GDAŃSK UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRONICS, TELECOMMUNICATIONS AND INFORMATICS

The author of the PhD dissertation: Krzysztof Gierłowski
Scientific discipline: Telecommunications

DOCTORAL DISSERTATION

Title of PhD dissertation:
Cross-layer integration of network mechanisms for increasing efficiency of multimedia session support in IEEE 802.11s environment

Title of PhD dissertation (in Polish):
Międzywarstwowa integracja mechanizmów sieciowych dla efektywnej obsługi sesji multimedialnych w środowisku IEEE 802.11s

Supervisor *signature*	Second supervisor – *signature*
Professor Józef Woźniak	-
Auxiliary supervisor – *signature*	Cosupervisor – *signature*
-	-

Gdańsk, year 2016

Table of Contents

List of Figures

List of Tables

List of Acronyms and Symbols

Abbreviations:

- 5G – 5th Generation
- AAA – Authentication, Authorization, Accounting
- AAD – Additional Authenticated Data
- AC – Access Class
- AC_BE – Access Class: Best Effort
- AC_BK – Access Class: Background
- AC_VI – Access Class: Video
- AC_VO – Access Class: Voice
- ACS – Access Control and Security
- AE – Address External
- AEK – Authenticated Encryption Key
- AES – Advanced Encryption Standard
- AID – Association ID
- AIFS – Arbitration Inter-Frame Space
- AMI – Advanced Metering Infrastructure
- AMPE – Authenticate Mesh Peering Exchange
- AODV – Ad-hoc On-demand Distance Vector
- AP – Access Point
- APSD – Automated Power Save Delivery
- ARP – Address Resolution Protocol
- ARPREP – Address Resolution Protocol Reply
- ARPREQ – Address Resolution Protocol Request
- AS – Authentication Server
- BPDU – Bridge Protocol Data Unit
- BSA – Basic Service Set Area
- BSS – Basic Service Set
- BSSID – Basic Service Set Identifier
- CCN – Congestion Control Notification
- CF – Contention Free
- CFP – Contention Free Period
- CM – Configuration Message
- CSMA/CA – Carrier Sense Multiple Access / Collision Avoidance
- CTS – Clear To Send
- CW – Contention Window
- DA – Destination Address
- DFS – Distributed Coordination Function
- DFS – Dynamic Frequency Selection
- DIFS – Distributed Coordination Function Inter-Frame Space
- DLS – Direct Link Setup
- DNS – Domain Name System
- DNSREQ – Domain Name System Request
- DNSREQExt – Domain Name System Request Extension
- DNSRESP – Domain Name System Response
- DNS-SD – Domain Name System – Service Discovery
- DS – Distribution System
- DSM – Distribution System Medium

- DSS -Distribution System Service
- ECC – Elliptic Curve Cryptography
- ECT – ExtMP Communication Technology
- EDCA – Enhanced Distributed Channel Access
- EGL – ExtMP Gate List
- EIFS – Extended Inter-Frame Space
- ESOP – End Of Service Period
- ESS – Extended Service Set
- ExtMP – External Mesh Peering
- FC – Frame Control
- FCG – Finite Cyclic Group
- FCS – Frame Check Sequence
- FFC – Finite Field Cryptography
- FQDN – Fully Qualified Domain Name
- GANN – Gateway Announcement
- GSM – Global System for Mobile Communications
- HCCA – Hybrid Coordination Function Controlled Channel Access
- HCF – Hybrid Coordination Function
- HLSA – Higher Layer Service Advertisement
- HT – High Throughput
- HWMP – Hybrid Wireless Mesh Protocol
- IBSS – Independent Basic Service Set
- IE – Information Element
- IEEE – Institute of Electrical and Electronics Engineers
- IFS – Inter-Frame Space
- IoT – Internet of Things
- IP – Internet Protocol
- IPv4 – Internet Protocol version 4
- IPv6 – Internet Protocol version 6
- ISM – Industrial, Scientific, Medical
- ISO – International Organization for Standardization
- ITU – International Telecommunication Union
- ITU-T – International Telecommunication Union - Telecommunication Standardization Sector
- KVP – Key-Value Pair
- LAN – Local Area Network
- LLC – Logical Link Control
- LTE – Long-Term Evolution
- MAC – Medium Access Control
- MAN – Metropolitan Area Network
- MANET – Mobile Ad-hoc Network
- MBCA – Mesh Beacon Collision Avoidance
- MBSS – Mesh Basic Service Set
- MCAE – Mesh Control Address Extension
- MCCA – Mesh Coordinated Channel Access
- MCF – Mesh Coordination Function
- MDA – Mesh Destination Address
- mDNS – Multicast Domain Name Service
- MG – Mesh Gate
- MGG – Mesh Gate Group

- MGG ID – Mesh Gate Group Identifier
- MGGA – Mesh Gate Group Advertisement
- MIC – Message Integrity Control
- MKT – Mesh Temporal Key
- MMPDU – MAC Management Protocol Data Units
- MOS – Mean Opinion Score
- MPDU – MAC Protocol Data Unit
- MPM – Mesh Peering Management
- MSA – Mesh Source Address
- MSDU – MAC Service Data Unit
- NAV – Network Allocation Vector
- ND – Neighbor Discovery
- OSI – Open Systems Interconnection
- OTS – Off The Shelf
- PCF – Point Coordination Function
- PERR – Path Error
- PES – Packetized Elementary Stream
- PGD – Proxy Group Database
- PGU – Proxy Group Update
- PHY – Physical Layer
- PID – Proxy ID
- PIFS – Point Coordination Function Inter-Frame Space
- PLC – Packet Loss Concealment
- PMK – Pairwise Master Key
- PMKID – Pairwise Master Key Identifier
- PMKSA – Pairwise Master Key Security Association
- PPP – Point-to-Point Protocol
- PPREP – Proactive Path Reply
- PPREQ – Proactive Path Request
- PQDN – Partially-Qualified Domain Name
- PREP – Path Reply
- PREQ – Path Request
- PS – Power Saving
- PSAP – Public Safety Access Point
- PSP – Peer Service Period
- PtMP – Point-to-MultiPoint
- PtP – Point-to-Point
- PXU – Proxy Update
- QoE – Quality of Experience
- QoS – Quality of Service
- RA – Receiver Address
- RANN – Root Announcement
- RF – Radio Frequency
- RFC – Request For Comment
- RM-AODV – Radio Metric Ad-hoc On-demand Distance Vector
- RSN – Robust Security Network
- RST – Rapid Spanning Tree
- RSTP – Rapid Spanning Tree
- RTS – Ready To Sent

- SA – Source Address
- SAE – Simultaneous Authentication of Equals
- SAL – Station Assignment List
- SIFS – Short Inter-Frame Space
- SIV – Synthetic Initialization Vector
- SN – Serial Number
- SS – Station Service
- SSID – Service Set Identifier
- ST – Slot Time
- STA – Station
- STP – Spanning Tree Protocol
- TA – Transmitter Address
- TBR – Tree-Based Routing
- TBTT – Target Beacon Transmission Time
- TC – Topology Change
- TCP – Transmission Control Protocol
- TDLS – Tunneled Direct Link Setup
- TFS – Timing Synchronization Function
- TID – Traffic ID
- TO – Target Only
- TPC – Transmit Power Control
- TS – Traffic Stream
- TSPEC – Traffic Specification
- TTL – Time To Live
- TXOP – Transmission Opportunity
- UDP – User Datagram Protocol
- UMTS – Universal Mobile Telecommunications System
- UP – User Priority
- USN – Unknown Target HWMP SN
- VoIP – Voice over IP
- WAN – Wide Area Network
- WAVE – Wireless Access In Vehicular Environments
- WLAN – Wireless Local Area Network
- WMAN – Wireless Metropolitan Area Network
- WMN – Wireless Mesh Network
- WWAN – Wireless Wide Area Network
- XaaS – Everything as a Service

Symbols:

- E-Model:
  - I_e – equipment impairment factor
  - B_{pl} – packet-loss robustness factor
  - A – advantage factor
- Nakagami model:
  - m – Nakagami distribution shape factor
- Modified grid placement model:
  - N – number of grid intersections
  - s – size of a placement area
  - I_i – i^{th} grid intersection
  - x_i, y_i – coordinates of grid intersection I_i

Streszczenie

Obserwowana w ostatnich latach popularyzacja uniwersalnych, mobilnych urządzeń elektronicznych w rodzaju laptopów czy smartphone'ów oraz powszechne zastosowanie podejścia Everything as a Service (XaaS) spowodowały znaczący wzrost zainteresowania powszechnością dostępu do infrastruktury sieciowej (ubiquity of network access). Zainteresowanie to przyczyniło się w znacznej mierze do przyspieszenia tak standaryzacji jak i implementacji oraz szerokiego wdrożenia technik komunikacji bezprzewodowej różnych klas, poczynając od sieci komórkowych (należących do klasy bezprzewodowych sieci rozległych – Wireless Wide Area Networks, WWANs), poprzez łatwo dostępne dla użytkowników indywidualnych rozwiązania klasy lokalnej (Wireless Local Area Networks, WLANs), a kończąc na różnego typu rozwiązaniach sieci osobistych (Wireless Personal Area Networks, WPANs oraz Body Area Networks, BANs).
Na szczególną uwagę zasługują tu rozwiązania klasy lokalnej (WLAN), które dzięki swojej niewielkiej cenie oraz możliwości funkcjonowania w nielicencjonowanych pasmach radiowych (ISM – Industrial, Scientific, Medical), pozwalają na stosunkowo nieskomplikowane i tanie tworzenie własnych systemów dostępowych. Cechy te doprowadziły do ogromnej popularności rozwiązań WLAN, a w szczególności sztandarowego ich przedstawiciela – techniki WiFi, będącej implementacją standardu IEEE 802.11.
Sieci standardu IEEE 802.11 dobrze nadają się do tworzenia bezprzewodowych systemów dostępowych o architekturze punkt-wielopunkt, gdzie wiele urządzeń mobilnych uzyskuje dostęp do infrastruktury sieciowej pod kontrolą dedykowanego urządzenia dostępowego zwanego punktem dostępowym. Zainteresowanie powyższym standardem doprowadziło do jego gwałtownego rozwoju i w chwili obecnej, dzięki połączeniu możliwości pracy w paśmie nielicencjonowanym, wysokich oferowanych przepływności (teoretycznie do 3,5 Gb/s na pojedynczego klienta i do 7 Gb/s na wszystkich klientów danego punktu dostępowego) oraz obecności kompatybilnych interfejsów sieciowych w szerokiej gamie mobilnych urządzeń elektronicznych, stał się on naturalnym wyborem do budowy bezprzewodowych systemów dostępowych.
Sytuacja taka dała początek intensywnym pracom badawczym i standaryzacyjnym, dotyczącym mechanizmów zarządzania systemami dostępowymi wykorzystującymi standard IEEE 802.11 oraz ich integracji z innymi technikami sieciowymi, celem ułatwienia tworzenia i utrzymania złożonych systemów sieci dostępowych. Wśród inicjatyw tego rodzaju znajduje się cały szereg dodatków rozszerzających funkcjonalność podstawowej specyfikacji IEEE 802.11, takich jak np.: IEEE 802.11k (monitorowanie zasobów sieci bezprzewodowej), IEEE 802.11v (zarządzanie siecią bezprzewodową), IEEE 802.11r (szybkie przełączanie pomiędzy punktami dostępu), IEEE 802.11u (współpraca z innymi systemami sieciowymi) czy wciąż nie ukończony IEEE 802.11aq (detekcja parametrów sieci przed podłączeniem). Dzięki wykorzystaniu tak rozbudowanej funkcjonalności, sieci WLAN oparte na rozwiązaniach IEEE 802.11 mogą zostać z powodzeniem wykorzystane do budowy wydajnych, zarządzalnych systemów dostępowych będących w stanie zaoferować dostęp sieciowy bardzo szerokiej gamie użytkowników.

Systemy tego rodzaju wymagają jednak na stałej infrastruktury sieciowej, instalowanej i następnie utrzymywanej przez operatora. W jej skład wchodzi zwykle znacząca liczba stacjonarnych urządzeń dostępowych (punktów dostępowych, Access Points – APs) oferujących urządzeniom klienckim możliwość uzyskania dostępu sieciowego w trybie punkt-wielopunkt (Point-to-MultiPoint, PtMP) na określonym obszarze, pozostającym w zasięgu komunikacyjnym danego AP. Utrzymywana przez urządzenia AP bezprzewodowa sieć dostępowa musi ponadto być w stanie zapewnić obsługę ruchu sieciowego na odpowiednim poziomie jakościowym (Quality of Service, QoS), jeśli użytkownicy urządzeń klienckich mają być w stanie korzystać z różnorodnych aplikacji i usług udostępnianych

obecnie w sieciach komputerowych zachowując zadowalający poziom ich postrzeganej jakości (Quality of Experience, QoE). Sprawę odpowiedniego oszacowania niezbędnego poziomu QoS utrudnia jednak fakt, iż wymagania wspomnianych usług i aplikacji różnią się od siebie, a ponadto różne grupy użytkowników zainteresowane będą różnymi ich zbiorami.
Kolejnym aspektem niemożliwym do pominięcia przy tworzeniu systemu dostępowego przy wykorzystaniu rozwiązań PtMP jest minimalizacja stopnia wzajemnego wpływu, jaki wywierają na siebie urządzenia należące do sąsiednich komórek systemu (czyli obszarów tworzonych przez urządzenia dostępowe i ich klientów), realizowana np. poprzez wybór ortogonalnych kanałów częstotliwościowych wykorzystywanych przez sąsiadujące komórki systemu. Często wykorzystywanym rozwiązaniem jest też zastosowanie anten kierunkowych, dedykowanych do konkretnych punktów instalacji, w celu zarówno poprawy jakości pokrycia sygnałem interesującego nas obszaru, jak i uniknięcia wspomnianych interferencji między komórkami.
Aby system dostępowy WLAN złożony z wielu AP był w stanie świadczyć użytkownikom usługę dostępu sieciowego w spójny i niezawodny sposób, tworzące go urządzenia powinny ponadto zostać skonfigurowane w sposób pozwalający im funkcjonować jako elementy zintegrowanego środowiska sieciowego – często wymieniane aspekty tego rodzaju integracji obejmują zagadnienia takie jak, np.: uwierzytelnianie, autoryzacja i rozliczanie (Autentication, Authorization, Accounting – AAA), konfiguracja klienta, monitorowanie ruchu sieciowego i środowiska radiowego, zarządzanie ruchem sieciowym, szybkie przełączanie pomiędzy punktami dostępu, itp.

Z powyższych rozważań wynika, że odpowiednie umiejscowienie oraz konfiguracja urządzeń AP jest sprawą kluczową: muszą one zarówno zapewnić zadowalający poziom fizycznego sygnału radiowego na obszarze mającym zostać objętym działaniem systemu, jak i być w stanie obsłużyć odpowiednią liczbę podłączonych do nich klientów bezprzewodowych, często zróżnicowanych typów, o różnych możliwościach (zarówno pod względem wydajnościowym, jak i obsługi opcjonalnych mechanizmów wykorzystywanego standardu WLAN) oraz potrzebach. Jednakże widoczne jest również, iż potrzeby te mogą ulegać znacznym zmianom, i to zarówno w dłuższym jak i krótkim okresie czasowym.
Urządzenia tego typu muszą oczywiście zostać połączone z użyciem odpowiednio wydajnej sieci dystrybucyjnej, pozwalającej na dalsze przenoszenie ruchu sieciowego obsługiwanych użytkowników bezprzewodowych. Co więcej, poza wspomnianym podłączeniem do sieci dystrybucyjnej, punkty dostępowe muszą także posiadać podłączenie do odpowiedniej sieci zasilającej.
Wymagania powyższe powodują, iż w wielu wypadkach instalacja urządzeń AP nie będzie możliwa we wszystkich lokalizacjach niezbędnych do kompletnej realizacji wszystkich założeń tworzonego systemu, dotyczących np. kombinacji oferowanej jakości obsługi, pojemności systemu oraz obszaru jego funkcjonowania. Może to prowadzić do obecności obszarów w obrębie działania systemu na których jakość świadczonych przez niego usług jest ograniczona, lub też dostęp do sieci nie jest możliwy, a których wykrycie może być trudnie, a usunięcie nie jest możliwe z przyczyn technicznych lub nie jest ekonomicznie uzasadnione.

Daje się także zaobserwować fakt, iż fizyczna struktura systemów typu PtMP ma charakter statyczny, ze stałymi punktami instalacji urządzeń dostępowych, dobranymi odpowiednio antenami, doprowadzoną instalacją zasilającą oraz łączami sieci dystrybucyjnej itd. Co więcej, ewentualne zmiany elementów powyższej struktury spowodują najprawdopodobniej konieczność powtórnego przeprowadzenia złożonych prac projektowych, a następnie rekonfiguracji znacznej liczby urządzeń. Efekt ten jest dobrze widoczny, np. w przypadku gdy konieczne jest dodanie nowych urządzeń AP w obrębie funkcjonującej już infrastruktury systemu w celu zwiększenia jego pojemności (rozumianej jako maksymalna liczba jednocześnie obsługiwanych użytkowników) lub poprawy jakości zasięgu – wymaga to np. zmiany przypisania kanałów częstotliwościowych urządzeń AP i to nie tylko na obszarach podlegających bezpośredniej modyfikacji, lecz, ze względu na wzajemne zależności pomiędzy sąsiadującymi komórkami, na obszarze praktycznie całego systemu. W wielu wypadkach niezbędne okazuje się ponowne przeprowadzenie planowania radiowego, a czasem nawet przebudowa istniejącej sieci dystrybucyjnej systemu.

Widać stąd, iż szeroko pojęta elastyczność systemów dostępowych wykorzystujących stałą infrastrukturę urządzeń dostępowych pracujących w trybie PtMP i instalowanych przez operatora jest w znaczący sposób ograniczona, podczas gdy ich zaletą pozostaje przewidywalność działania, okupiona jednak potencjalnie długotrwałym i kosztowym procesem planowania i weryfikacji.

Rozwiązaniem wielu z powyższych problemów może być zastosowanie bezprzewodowych sieci o strukturze kratowej (Wireless Mesh Networks, WMNs), które zastępują prostą, gwiaździstą architekturę PtMP z wydzielonym urządzeniem dostępowym, strukturą połączeń bezpośrednich nawiązywanych pomiędzy urządzeniami pozostającymi w zasięgu wzajemnej komunikacji bezprzewodowej (sąsiadującymi) możliwą do wykorzystania dzięki wprowadzeniu obsługi transmisji wieloskokowej. Powyższa, radykalna zmiana podejścia, skutkuje koniecznością wprowadzenia szeregu nowych mechanizmów utrzymaniowych sieci, o stopniu komplikacji daleko większym niż ma to zwykle miejsce w przypadku systemu PtMP, lecz jednocześnie oferuje wiele zalet, jak np.:

- możliwość wyznaczenia wielu redundantnych ścieżek transmisji danych, pozwalających na elastyczne zarządzanie ruchem oraz odtworzenie łączności w przypadku awarii,
- możliwość wykorzystania urządzeń klienckich do przekazywania ruchu tranzytowego (w teorii każdy podłączający się klient zwiększa zasoby sieci), co pozwala na uzyskanie znacznej poprawy jakości pokrycia sygnałem terenu działania systemu, a także na jego zwiększenie bez konieczności instalacji stałej infrastruktury przez operatora,
- zdolność do automatycznego tworzenia struktury sieci (self-organization) i odtwarzania funkcjonalności sieci po awariach (self-healing), a także minimalizacja konfiguracji niezbędnej w procesie podłączenia do systemu (client zero-configuration).

Podejście WMN może być stosowane w systemach sieciowych wykorzystujących różnorodne techniki transmisyjne oraz przeznaczonych do zastosowań różnego typu, lecz w praktyce, najczęściej spotykane jest w przypadku wdrażanych na podstawie wcześniejszego projektu, bezprzewodowych sieciach dystrybucyjnych, w przypadku których węzły sieci instalowane są przez operatora. Wdrożenie sieci na podstawie wyników przeprowadzonego wcześniej procesu projektowania sieci, uwzględniającego np. planowanie radiowe, umożliwia uzyskanie wysokiej efektywności działania systemu, podczas gdy struktura kratowa, w połączeniu ze zautomatyzowanymi mechanizmami utrzymania sieci właściwymi dla podejścia WMN, daje możliwość szybkiej reakcji na awarie lub nieprzewidziane wcześniej zakłócenia łączności. W rezultacie możliwe jest uzyskanie systemu dystrybucyjnego, łączącego wysoką wydajność i niezawodność. Tego rodzaju implementacje mechanizmów WMN są bardzo często zamkniętymi rozwiązaniami firmowymi, nie podlegającymi standaryzacji. Wykorzystywane techniki transmisji bezprzewodowej mogą być w tym przypadku bardzo różne, lecz najczęściej należą do grupy bezprzewodowych sieci lokalnych (WLAN) lub metropolitalnych (Wireless Metropolitan Area Network, WMAN), a nawet radioliniowych połączeń punkt-punkt.

Drugim rodzajem sieci WMN są systemy wykorzystujące mechanizmy samoorganizacji w celu dynamicznego tworzenia struktury sieci w oparciu o urządzenia klienckie oraz logiczne łącza bezprzewodowe możliwe do zestawienia pomiędzy nimi, przy minimalnym udziale infrastruktury dostarczonej przez operatora systemu. Rozwiązania tego rodzaju są, z definicji, przeznaczone do zastosowania w roli systemów dostępowych lub umożliwiających komunikację w obrębie izolowanych grup użytkowników (np. systemy komunikacji awaryjnej lub wojskowej). Wykorzystanie urządzeń klienckich w celu przekazywania ruchu tranzytowego jest zarówno zaletą jak i wadą tego rodzaju sieci – ich stosunkowo duża liczba oferuje redundancję, zwiększenie zasięgu oraz daleko idące uniezależnienie sieci od stałej infrastruktury, lecz jednocześnie nawet przybliżona lokalizacja węzłów sieci jest trudna do oszacowania (a wraz z nią efektywne i interferencyjne zasięgi generowanych sygnałów radiowych), zgodność stosowanych przez nie procedur ze standardem nie może być zagwarantowana, a komplikacja struktury sieci utrudnia monitorowanie i zarządzanie.

Przedmiot naszego zainteresowania w poniższej rozprawie, rozszerzenie IEEE 802.11s standardu IEEE 802.11-2007, definiuje komplet mechanizmów niezbędnych do zaimplementowania oraz wdrożenia

funkcjonalnej sieci WMN drugiego z opisywanych rodzajów. Kompleksowość podejścia zaprezentowana przez autorów powyższej specyfikacji, w połączeniu z wykorzystaniem w roli techniki transmisyjnej niezwykle popularnej techniki WiFi, czyni z opisywanego rozwiązania WMN niezwykle interesującą propozycję, zarówno dla niewielkich sieci domowych, jak i rozbudowanych sieci dostępowych stanowiących ponadto część systemów złożonych.
W dążeniu do zapewnienia wysokiego stopnia uniwersalności opracowanego rozwiązania, system WMN oparty na specyfikacji IEEE 802.11s oferuje funkcjonalność transmisji danych w warstwie 2 modelu ISO-OSI wraz z mechanizmami wymiany danych z sieciami zewnętrznymi wykorzystującymi techniki tejże warstwy i zgodnymi z wymaganiami standardu IEEE 802.1D (czyli np. popularnymi sieciami Ethernet). W obu wypadkach omawiana sieć WMN postrzegana jest (przez protokoły warstw wyższych oraz sieci zewnętrzne) jako funkcjonalny odpowiednik sieci Ethernet. Podejście takie pozwala zarówno na wykorzystanie w sieci IEEE 802.11s dowolnego protokołu warstwy sieciowej, zdolnego do funkcjonowania w środowisku sieci Ethernet, jak i na łatwą integrację z większością obecnie funkcjonujących złożonych systemów sieciowych wykorzystujących techniki właściwe dla sieci lokalnych (Local Area Network, LAN).

Zastosowanie powyższych rozwiązań, czyni z IEEE 802.11s technikę łatwą we wdrożeniu i zapewniającą wysoki stopień elastyczności zastosowania. Wydaje się, że może ona stanowić atrakcyjne rozwiązanie pozwalające uniknąć wielu ze wspomnianych wcześniej ograniczeń klasycznych systemów IEEE 802.11 pracujących w trybie PtMP, a jednocześnie łatwe do wdrożenia w ich miejsce.

Niestety, pomimo wspomniany wyżej zalet oraz faktu, iż specyfikacja IEEE 802.11s została opublikowana w 2011 r., a jej obligatoryjne elementy zostały zaimplementowane w popularnych seriach sterowników interfejsów bezprzewodowych systemu Linux (ath5k i ath10k), wdrożenia omawianego rozwiązania należą do rzadkości.

W tej sytuacji, dokonawszy wstępnej analizy potencjalnych zalet i wad sieci WMN, w rozprawie sformułowano następującą tezę:

Kratowa struktura sieci pozwala na elastyczne wykorzystanie zasobów sieci, w stopniu większym niż w klasycznych rozwiązaniach punkt-wielopunkt ze stałą infrastrukturą szkieletową.

Jednakże, biorąc pod uwagę znaczącą liczbę oraz stopień złożoności mechanizmów niezbędnych do efektywnej realizacji transmisji danych w sieci WMN oraz integracji tejże sieci w ramach rozbudowanego systemu sieciowego, a także uwzględniając fakt, iż w niniejszej rozprawie koncentrujemy naszą uwagę na konkretnej specyfikacji sieci powyższego typu (IEEE 802.11s), lokującej wszystkie te mechanizmy w warstwie 2 modelu ISO-OSI, zdecydowano się rozszerzyć stawianą tezę o dodatkowe stwierdzenie:

Wprowadzenie, w sieciach mesh, integracji mechanizmów kontrolno-zarządzających warstw realizujących usługi przenoszenia ruchu sieciowego z analogicznymi mechanizmami warstw wyższych pozwoli na poprawę jakości obsługi ruchu sieciowego oraz efektywności wykorzystania zasobów sieci.

W celu weryfikacji powyższych tez, w rozdziale 2 zawarto przegląd ogólnej architektury oraz najważniejszych mechanizmów sieci standardu IEEE 802.11. Przedstawiono ogólny opis podstawowych rozwiązań technicznych zastosowanych w przypadku tej techniki sieciowej, włączając w to mechanizmy dostępu do medium transmisyjnego, zarządzania zasobami oraz kontroli funkcjonowania sieci. Powyższy ogólny opis zawiera także szczegóły wybranych mechanizmów, niezbędne jako podstawa pozwalająca zaprezentować w dalszych rozdziałach proponowane, oryginalne rozwiązania techniczne, wykorzystujące elementy integracji międzywarstwowej.

Końcowa część rozdziału 2 poświęcona została prezentacji wyników eksperymentów symulacyjnych, wskazujących na stosunkowo małą elastyczność klasycznych rozwiązań IEEE 802.11 pracujących w trybie PtMP w przypadkach gdy system musi funkcjonować w warunkach różniących się od założonych w trybie projektowania. Przedstawione, przekładowe scenariusze dotyczą np. spodziewanej jakości obsługi ruchu sieciowego wybranych usług multimedialnych w wybranych scenariuszach, wpływu prawidłowości oszacowania obszaru na którym rozlokowani są klienci systemu oraz ewentualnie występujących awarii urządzeń dostępowych. Scenariusze symulacyjne przedstawione w rozdziale drugim stanowią punkt odniesienia dla porównań oraz analiz przedstawionych w dalszych rozdziałach i dotyczących standardowego systemu WMN IEEE 802.11s oraz jego zmodyfikowanych wersji, uwzględniających zaproponowane w pracy, oryginalne mechanizmy wykorzystujące zasady integracji międzywarstwowej.
Uzyskane wyniki eksperymentów potwierdzają wspomniane wcześniej wady systemów tego typu, wynikające z ograniczonej elastyczności zarządzania zasobami, będącej skutkiem silnej, bezpośredniej zależności pomiędzy dostępnymi w danej lokalizacji zasobami, a miejscem fizycznej instalacji urządzeń dostępowych.

Rozdział 3 poświęcono prezentacji i przeglądowi mechanizmów zawartych w specyfikacji IEEE 802.11s, koniecznych do funkcjonowania sieci WMN wykorzystującej (opisane w rozdziale 2) mechanizmy komunikacyjne standardu IEEE 802.11. Rozdział rozpoczęto ogólną charakterystyką specyfikacji IEEE 802.11s, wraz z jej potencjalnymi zastosowaniami praktycznymi. W kolejnym podrozdziale przedstawiono listę najważniejszych, dodatkowych mechanizmów wprowadzonych w opisywanym rozszerzeniu standardu IEEE 802.11, obrazujących stopień komplikacji kompleksowego rozwiązania WMN w porównaniu do klasycznej sieci IEEE 802.11 pracującej w trybie PtMP.
Dalsza, rozbudowa część rozdziału 3, poświęcona została szczegółowemu opisowi tych ze wspomnianych wcześniej mechanizmów rozwiązania IEEE 802.11, które będą przedmiotem zaproponowanych dalej, oryginalnych modyfikacji wykorzystujących integrację międzywarstwową. Opis powyższy jest dość szczegółowy, ze względu na konieczność zarówno wskazania elementów specyfikacji IEEE 802.11s ograniczających szeroko pojętą efektywność działania sieci WMN, jak i przedstawienia specyfikacji proponowanych mechanizmów i modyfikacji w rozdziałach kolejnych. Szczególną uwagę poświecono mechanizmom ustalania sąsiedztwa (peering), wyznaczania tras (path discovery) oraz komunikacji międzysieciowej (interworking). Z powyższych względów, przedstawiono również opis protokołu RSTP, który wprawdzie nie jest częścią specyfikacji IEEE 802.11s, lecz ma bezpośredni i znaczący wpływ na efektywność realizacji komunikacji międzysieciowej w środowisku opisywanej sieci WMN.
Końcowa część rozdziału 3 zawiera wyniki badań symulacyjnych, realizowanych dla scenariuszy dobranych w sposób pozwalający na łatwe dokonanie porównań pomiędzy sieciami IEEE 802.11 pracującymi w trybie PtMP, a sieciami WMN wykorzystującymi rozwiązanie IEEE 802.11s. Ze względu na wyraźnie widoczną zależność efektywności działania sieci WMN od jej aktualnej struktury, powyższe badania przeprowadzono dla 4 umownych typów struktury sieci, również opisanych w niemniejszym rozdziale.
Wyniki badań wskazują na ograniczoną efektywność funkcjonowania jednokanałowej sieci WMN jaką jest IEEE 802.11s, w przypadku konieczności wykorzystania ścieżek transmisji danych wymagających wielu retransmisji w węzłach pośredniczących. Jednocześnie, wskazują one na możliwość znacznie większą elastyczność w zarządzaniu siecią, w porównaniu do opisywanych w poprzednim rozdziale systemów PtMP. Niestety, badania wykazują, iż kilka elementów specyfikacji systemu IEEE 802.11s, wprowadzonych w celu uzyskania wysokiego stopnia kompatybilności z protokołami warstw wyższych oraz zewnętrznymi systemami sieciowymi, wpływa na drastyczne pogorszenie elastyczności zarządzania zasobami, efektywności ich wykorzystania, a w efekcie czyni sieć IEEE 802.11s skalowalną jedynie w minimalnym stopniu. W efekcie, badania wskazują na bardzo ograniczoną możliwość efektywnej realizacji usług multimedialnych w tym środowisku.
Wyniki analizy teoretycznej mechanizmów sieci IEEE 802.11s przedstawionej w niniejszym rozdziale oraz powyższych badań symulacyjnych, posłużyły do opracowania propozycji oryginalnych

modyfikacji specyfikacji IEEE 802.11s z wykorzystaniem rozwiązań integracji międzywarstwowej, pozwalających na uniknięcie wykrytych ograniczeń efektywności działania oraz elastyczności zarządzania zasobami. Propozycje te opisano w rozdziałach 4-6.

W rozdziale 4 skoncentrowano się na, wykrytych w wyniku badań symulacyjnych opisanych w rozdziale 3, problemach dotyczących efektywnej obsługi protokołów warstw wyższych wykorzystujących komunikację adresowaną grupowo (broadcast, multicast). Fakt, iż należą do nich protokoły rozwiązywania adresów IPv4/IPv6 do odpowiadających im adresów MAC, takie jak ARP i IPv6 Neighbor Discovery, powoduje, iż efektywność nawiązywania komunikacji IP w intersujących nas systemach IEEE 802.11s ulega znacznemu pogorszeniu. Podobny problem dotyczy mechanizmów rozwiązywania nazw hostów bez użycie scentralizowanego serwera, takich jak np. Multicast DNS.
W tej sytuacji zaproponowano 2 metody pozwalające zastosować integrację międzywarstwową w celu minimalizacji liczby wiadomości przesyłanych w systemie w ramach powyższego procesu, ze szczególnym uwzględnieniem minimalizacji liczby wiadomości przesyłanych rozgłoszeniowo. W efekcie uzyskano znaczną minimalizację liczby niezbędnych transmisji w sieci bezprzewodowej oraz skrócenie czas jego realizacji, co potwierdzają przedstawione wyniki badań symulacyjnych.

Rozwiązanie opisane w rozdziale 5 stanowi koncepcyjne rozwinięcie metod zaproponowanych w rozdziale poprzednim, poprzez zastosowanie ich podstawowych założeń do rozbudowy funkcjonalności proaktywnych protokołów wyznaczania tras w sieci IEEE 802.11s, w celu udostępnienia możliwości rozgłaszania informacji o dostępności usług wysokiego poziomu. Tego rodzaju zastosowanie integracji międzywarstwowej pozwala na uzyskanie przez potencjalnych klientów usługi szeregu informacji dotyczących spodziewanej jakości jej realizacji, z uwzględnieniem specyfiki środowiska sieci WMN. W przypadku standardowej specyfikacji IEEE 802.11s uzyskanie tego rodzaju informacji nie jest możliwe, ze względu na zastosowanie ścisłej izolacji mechanizmów WMN od mechanizmów warstw wyższych.

Rozdział 6 prezentuje propozycje modyfikacji mechanizmów komunikacji międzysieciowej systemu IEEE 802.11s, w celu likwidacji najpoważniejszych problemów dotyczących efektywności oraz elastyczności działania opisywanej sieci WMN wskazanych w rozdziale 3 – nieefektywnej transmisji danych z wykorzystanym długich ścieżek oraz dezaktywacji redundantnych punktów wymiany danych z sieciami zewnętrznymi.
Zaproponowana metoda wykorzystująca elementy integracji międzywarstwowej, pozwala na utrzymanie aktywności wszystkich punktów potencjalnej wymiany danych sieci WMN zewnętrznymi sieciami, co umożliwia ograniczenie długości ścieżek transmisyjnych przy komunikacji międzysieciowej, pozwala na rozłożenie ruchu międzysieciowego pomiędzy wiele punktów jego przekazywania rozłożonych na znacznym obszarze, oraz pozytywnie wpływa na szybkość odtwarzania łączności po awarii urządzenia odpowiedzialnego za przekazywanie ruchu międzysieciowego. W ten sposób uniknięto większości ograniczeń (wskazanych w rozdziale 3) dotyczących efektywności obsługi ruchu międzysieciowego. Proponowana modyfikacja pozwala na wykorzystanie w systemie IEEE 802.11s elastyczności w zarządzaniu zasobami, jakiej teoria pozwala oczekiwać po rozwiązaniach typu WMN. Zaobserwowany w zmodyfikowanej sieci wzrost jakości realizacji usług multimedialnych stawia ją na równi z dobrze zaprojektowanymi systemami PtMP, a w porównaniu z systemami tego typu gdzie oszacowanie lokalizacji użytkowników nie było dokładne, oferuje znaczącą przewagę.
Druga z zaproponowanych metod, umożliwia wykorzystanie zasobów oferowanych przez sieci zewnętrzne, w realizacji komunikacji pomiędzy urządzeniami należącymi do tej samej sieci IEEE 802.11s. Zastosowanie integracji międzywarstwowej oraz elementów wirtualizacji łączy międzywęzłowych pozwala na znaczące zmniejszenie długości ścieżek transmisyjnych w systemie bezprzewodowym, znacząco redukując zużycie jego zasobów, podnosząc efektywność ich wykorzystania oraz oferując użytkownikom znacząco lepszą jakość usług wysokiego poziomu.

Wyniki pracy podsumowano w rozdziale 7, wskazując na przyjęte założenia, podsumowując wyniki analiz teoretycznych oraz badań symulacyjnych oraz potwierdzając celowość i skuteczność wprowadzenia proponowanych rozwiązań integracji międzywarstwowej.

Podsumowując, oryginalne osiągnięcia zawarte w poniższej rozprawie, obejmują:

1. Przegląd i analizę mechanizmów standardu IEE 802.11, dokonaną w celu ułatwienia późniejszego porównania mechanizmów standardu bazowego i rozszerzeń wprowadzonych przez specyfikację IEEE 802.11s.
2. Eksperymenty przeprowadzone w środowisku symulacyjnym, ilustrujące poziom efektywności i możliwej do uzyskania jakość obsługi ruchu sieciowego generowanego przez usługi multimedialne, oferowaną przez mechanizmy standardu IEEE 802.11. W załączonych wnioskach skoncentrowano się na aspektach dotyczących elastyczności zastosowania oraz zarządzania zasobami dla zróżnicowanych struktur sieci oraz w warunkach zróżnicowanego obciążenia ruchem.
3. Przegląd mechanizmów pozwalających na funkcjonowanie sieci WMN wprowadzonych przez specyfikację IEEE 802.11s, uzupełniony o szczegółowy opis tych z nich, które mają szczególne znaczenie dla tematyki rozprawy lub też mają bezpośredni wpływ na specyfikację oryginalnych rozwiązań integracji międzysieciowej, zaproponowanych w poniższej pracy.
4. Implementację brakujących mechanizmów oraz usunięcie błędów zawartych w częściowym modelu symulacyjnym sieci IEEE 802.11s stanowiącym część biblioteki INETMANET 2.0.
5. Eksperymenty symulacyjne dotyczące efektywności funkcjonowania sieci IEEE 802.11s oraz możliwego do osiągnięcia poziomu Quality of Experience (QoE) wybranych usług multimedialnych, przeprowadzone dla 4 odmiennych rodzajów struktury sieci WMN.
6. Wskazanie elementów specyfikacji IEEE 802.11s skutkujących nieefektywnym wykorzystaniem zasobów sieci, nieefektywną obsługą protokołów warstw wyższych wykorzystujących transmisję rozgłoszeniową oraz brakiem skalowalności systemu.
7. Opracowanie szczegółowej specyfikacji oryginalnych modyfikacji mechanizmów IEEE 802.11s, wykorzystujących rozwiązania integracji międzywarstwowej w celu likwidacji powyższych ograniczeń rozwiązań standardowych.
    a. mechanizm odwzorowania adresów IP na adresy MAC wykorzystujący mechanizmy integracji międzywarstwowej warstw 2-3 modelu ISO-OSI,
    b. mechanizm odwzorowania nazw mDNS na adresy IP i MAC, wykorzystujący mechanizmy integracji międzywarstwowej warstw 2-3 i 7 modelu ISO-OSI,
    c. mechanizm rozgłaszania obecności i wyboru serwerów usługowych wykorzystujący mechanizmy integracji międzywarstwowej warstw 2-3 i 7 modelu ISO-OSI,
    d. mechanizm pozwalający na zachowanie wielu punktów przekazywania ruchu pomiędzy systemem IEEE 802.11s, a zewnętrzną siecią warstwy 2 modelu ISO-OSI,
    e. mechanizm pozwalający na przekazywanie wewnętrznego ruchu sieci WMN z użyciem sieci zewnętrznych.
8. Implementację modeli symulacyjnych 5 powyższych oryginalnych mechanizmów wykorzystujących elementy integracji międzywarstwowej, w środowisku symulatora OMNeT++ 4.6.
9. Weryfikację poprawności funkcjonowania oraz zysków wynikających z zastosowania proponowanych modyfikacji z użyciem scenariuszy symulacyjnych pozwalających na łatwe dokonanie porównań z niezmodyfikowaną siecią IEEE 802.11s.

1 Cross-layer integration of network mechanisms in IEEE 802.11s environment

Continuous development and standardization of Wireless Local Area Network (WLAN) technologies designed to utilize unlicensed frequency bands have resulted in their widespread popularization as cost-effective, easy to deploy and compatible means of communication. The trend has been further intensified by popularization of mobile computing devices and Everything as a Service approach, creating a need for a robust, efficient and ubiquitous method of wireless network access. WLAN point-to-multipoint (PtMP) solutions, of which a widely popular WiFi (IEEE 802.11 [1]) standards family is a most notable member, are currently a popular solution used for this purpose. With its IEEE 802.11 g/a/n/ac [2,3,4,5] transmission-related extensions, offering theoretical transmission speeds up to 3.5 Gb/s per client (up to about 7 Gb/s per access point) and almost universal presence of compatible hardware in both nomadic and mobile of-the-shelf devices, the incentives to use WiFi WLANs as elements of network access systems are undisputed.
Such situation prepared the field for development of a significant number of IEEE 802.11 standard amendments aimed to enable seamless WLAN integration in compound network systems. For this purpose their transmission capabilities need to be supplemented by appropriate network discovery and selection, monitoring, management and interworking mechanisms. Most notable of such standardization initiatives for IEEE 802.11 family include: IEEE 802.11k (Radio resource measurement enhancements) [6], IEEE 802.11v (Wireless network management) [7], IEEE 802.11r (Fast BSS transition) [8], IEEE 802.11u (Interworking with external networks) [9] or as yet unreleased IEEE 802.11aq (Pre-association discovery) [10]. With these extensions a number of IEEE 802.11-based WLANs can be used to create a high-speed, managed access system able to provide a reliable network access to a broad group of users.

Such systems depend, however, on the fixed infrastructure of wireless access points (APs), which must be deployed through the intended coverage area in a considerable number, sufficient to provide both physical signal coverage and ability to provide an adequate Quality of Service (QoS) to an expected number of users. The adequate QoS level for a specific deployment is in turn dependent on the, potentially changing, set of applications and services users are expected to access with a satisfactory Quality of Experience (QoE).
Moreover, access points need to be correctly configured to reduce the interference between members of the neighboring cells (formed by APs and their associated wireless clients) for example by choosing orthogonal frequency channels. The use of antennas dedicated to fulfill the requirements of the specific deployment scenario and varied between specific APs in the system is the common practice.
The configuration of access points must also allow them to function as elements of a single manageable system, which provides its users with a service in a uniform, consistent manner – aspects such as authentication, authorization and accounting (AAA), client configuration, monitoring of traffic and Radio Frequency (RF) conditions, traffic management, wireless client handover, etc. need to be observed.
Moreover, such APs need to be connected to a power grid and a high-speed communication infrastructure of a distribution network. Both of these requirements tend to limit a number of locations where installation of such devices is possible or economically feasible. The described limitations can easily lead to a presence of areas exhibiting a poor coverage conditions within the access system, which could be difficult to pinpoint and/or not economic to correct.
This considerable number of operator deployed devices needs to be monitored and maintained, while any change in the infrastructure of such a network will most probably result in the need to redesign and reconfigure a significant part of its infrastructure – an effect manifesting itself in

particularly troublesome manner when there is a need to install additional APs within the already deployed structure, in attempt to provide a better signal coverage or increase the capacity of the system (understood as a number of clients the infrastructure is able to support). Due to a high number of devices and mechanisms interacting in complex ways, such changes most often require a repeated radio planning and sometimes even a redesign of the distribution network supporting the wireless access infrastructure.

An answer to many of these problems can possibly be found in Wireless Mesh Network (WMN) technologies, which substitute a mesh of connections between neighboring devices and multihop transmission capability in place of the simple point-to-multipoint structure of popular WLAN access systems. This change of approach results in technologies requiring much more complex mechanisms to function, but at the same time providing significant advantages, such as:

- redundancy of transmission paths, allowing for a traffic management and failure recovery to be performed,
- ability to use client devices to forward transit traffic, resulting in a very good signal coverage, possible increase of network's available resources with each connecting client and ability to create a sizable network without or with a very limited operator provided infrastructure,
- self-organization and self-maintenance of the network and minimal configuration of the connecting clients.

The WMN approach is known to be used in variety of network systems and environments, but can most often be found in pre-designed, wireless distribution networks, where all devices are deployed by an operator according to a strict radio and traffic planning which allows the network to maintain a high efficiency, while the mesh structure and its automatic maintenance mechanisms provide the additional ability to quickly react to an unexpected interference and failures, thus creating a robust network of a very high availability. The technologies employed in such systems however, are most often proprietary ones, developed and owned by wireless device manufacturers. Wireless Local Area Network, Wireless Metropolitan Area Network (WMAN) transmission technologies or even microwave links are used as a basis of mesh solutions of this type.
The second type of WMN networks are self-organizing and self-maintaining systems created on the basis of connecting client devices with minimum operator-provided infrastructure. Such systems are, by definition, intended as access networks or isolated client groups. Their use of client devices is both a strength and a weakness as the number of devices capable of forwarding traffic provides advantages of redundancy, coverage and independence of infrastructure, but at the same time the placement of devices and their effective and interference ranges are hard to predict, their standard adherence cannot be guaranteed and the management of a potentially very complicated network structure is difficult.

The solution of our interest, an IEEE 802.11s [11] standard amendment defining a comprehensive set of mechanisms sufficient to create a self-organizing, multihop wireless mesh network based on IEEE 802.11 technology is an example of the second type of WMN systems mentioned above. The completeness of the standard, combined with a widely popular WLAN transmission technology used as its basis makes it an interesting proposition for both small home networks and sizable WLAN elements of compound network systems.
This ready to be implemented solution have been designed to provide communication capabilities at ISO-OSI layer 2, complete with robust interworking mechanisms making its integration with modern layer 2 networks easy, by emulating an Ethernet Local Area Network (Ethernet LAN). Also, the fact that the service is provided at data link layer allows the use of any network (and higher) layer protocol fit to use the Ethernet LAN.
As one of the key requirements necessary for an effective use of such an end-device-dependent technology, is its transparency to users, IEEE 802.11s standard includes a high degree of auto-configuration capability in both its internal mechanisms and in procedure of connecting new clients.

Such approach makes it a robust and easy to use access network technology, taking over most tasks necessary for creating and maintaining user's layer 2 network connection.
It seems, that such an easy to integrate, robust, self-organizing network created of end-user devices could be an effective solution for dynamically extending and improving coverage of classical, point-to-multipoint, AP-based access systems. As such, the technology looks like a perfect element for realizing the ubiquity of network access postulate, which is present in many new network design trends [15].

However, despite the above advantages and the fact that the IEEE 802.11s standard amendment has been published in 2011 and that its partial implementation has been present in the popular ath5k and ath10k series of Linux wireless drivers for years, the deployments of the solution are scarce in both private/Small-Office-Home-Office (SOHO) and enterprise environments.

In this situation, seeing both potential advantages of self-organizing wireless mesh networks in general, a following thesis has been proposed:

A wireless mesh network structure allows its available resources to be used in a more robust manner than in case of classic Point-to-Multipoint wireless access networks relying on a static set of infrastructure devices.

However, taking into account the expected complexity of mechanisms necessary for operation of WMNs and unpredictability of their operating environment, combined with the fact that in this dissertation we are interested in a specific WMN implementation (IEEE 802.11s [11]) which places all of its mechanisms in an ISO-OSI layer 2, the above thesis has been supplemented by an additional statement:

By utilizing a cross-layer integration of a wireless mesh network's data transmission management mechanisms with management mechanisms of higher layer procedures, it is possible to improve the quality of network communication and efficiency of resource usage.

In the next chapter of this thesis a description of critical mechanisms of the IEEE 802.11 standard (supporting an ad-hoc and the widely popular PtMP infrastructure mode) has been provided, followed by an overview of mesh specific extensions introduced by IEEE 802.11s amendment. The list of such additional mechanisms required to support a self-organizing mesh network structure is considerable and includes over ten mechanisms and a considerable number of additional frame types and formats. Following this overview of basic IEEE 802.11s elements is a more detailed description of mechanisms bearing special importance to the topic of this thesis: mesh management procedures such as mesh discovery and peering management, reactive and proactive path discovery mechanisms, traffic forwarding procedures and interworking methods, complete with relevant network data structures such as frame formats.
This theoretical preview of the IEEE 802.11 infrastructure mode and the IEEE 802.11s mesh network mechanisms is supplemented by a simulation assessment of basic parameter values related to quality of network transmission possible to sustain in each environment, complete with an indication of the most important factors influencing these values.

The above evaluation serves to pinpoint a number of assumptions, protocol design decisions and specifics of functionality provided by IEEE 802.11s mesh network, which can serve as possible explanations for its limited popularity. They are mostly relevant to the aim of making the standard as compatible as possible, both in terms of integration of the WMN with external networks and ability to accommodate the widest possible range of higher layer protocols and services. As the analysis indicates, these goals seems to have been accomplished, but at the cost of efficiency of the WMN itself. Some of the most distinct problems seem to be related to some avoidable inefficiencies

in support of IPv4/IPv6 protocols made in accordance with promoting compatibility of the solution by maintaining strictly layered, black-box approach in exposing the WMN functionality to higher layer protocols, which can be quite wasteful in case of resource limited wireless multihop network.
Another set of inefficiencies resulting in limited scalability of the WMN can be attributed to a similar aim of maintaining a compatibility with widely popular, wired, IEEE 802.1D-compliant LAN technologies (such as Ethernet). It is evident that IEEE 802.11s interworking mechanisms have been designed with the above objective as one of its topmost priorities, again resulting in unnecessarily wasteful resource management.
Of course the indicated problems do not prevent the IEEE 802.11s network to be employed in many specific deployment scenarios, where the precise level of QoS parameters is not of paramount importance and the traffic volume is not likely to cause a congestion in the resource limited WMN system. However, the simulation and testbed results seem to indicate, that they are likely to nullify the unique WMN advantages over the classic PtMP systems and bring its level of service below the adequate level in a general-purpose deployment scenario, which today includes the widespread use of varied multimedia services.

Many of the most popular end-user services accessed in modern computer networks can be defined as multimedia services. While the definition vary, the term is often associated with services providing their end-user with a content that uses a combination of different content forms such as text, audio, images, animation, video and interactive content. The content presented by multimedia services can be further divided into linear and non-linear categories, with the former being a static content to be presented to a user while the presentation of the latter can be influenced by the user in an interactive manner.
A majority of modern multimedia services employ content types whose transmission consumes a significant amount of network resources due to the volume of data to be transmitted within a strictly specified time limit (such as an audio/video content), creating a need for a network communication adhering to a strictly defined and stable level of QoS parameters if the user's QoE is to remain high.
While in case of linear content there is a number of techniques which can relax the QoS requirements, in case of interactive services, based on non-linear content, such as a Voice Over IP (VoIP), videoconferencing, Virtual Reality (VR) etc., the QoS requirements must remain strict. Due to their high network resource consumption combined with high QoS requirements, multimedia services remain a class of services which is difficult to deploy in wireless networks while being in widespread demand.

Analyzing both mechanisms of the IEEE 802.11s WMN standard, its inefficiencies indicated below and requirements of the modern multimedia services, it seems probable, that the analyzed mesh standard can benefit from the use of a cross-layer approach, making it a valuable alternative to a classic PtMP WLAN systems.
Because an extensive amount of research [24-31] has already been devoted to cross-layer solutions based on changing the parameters of a specific high layer service to make it feasible in a particular network conditions (for example by making changes in encoding schemes and their parameters), the cross-layer solutions proposed in this thesis are intended to be general in their application scenarios and change selected procedures of mesh traffic management to provide a better quality of service or increase the efficiency of the WMN operation as a part of a larger, compound network system.
The term "cross-layer" is also used in a broad meaning, as the proposed methods utilize such an approach in a number of different ways:

- according to the most popular definition of the term – with higher ISO-OSI layers making use of information specific to lower layers and normally not exposed outside their internal mechanisms,
- by performing a cross-layer integration with higher ISO-OSI layer specific information being (partially or fully) performed using lower ISO-OSI layer signaling mechanisms,

- with additional network integration elements, where lower ISO-OSI layer mechanisms of a specific network take advantage of services provided by higher ISO-OSI layers of another network,
- by integrating a compound network management protocols with internal WMN mechanisms, despite the black-box approach used in IEEE 802.11s network.

Because many of the IEEE 802.11s advantages are attained by strictly observing the layered network model and making the WMN network a black-box with strictly defined and highly compatible with popular LAN network technologies points of contact with outside systems, it would seem counterproductive to employ cross-layer methods in this particular environment. However, the proposed mechanisms have also been designed with compatibility in mind, in terms of ease of deployment within the WMN, interworking with external networks and integration with other protocols.
It should be also taken into account, that efficiency of WMN operation is strongly dependent on the structure of such network, including spatial placement of nodes, their transmission and interference ranges combined with source and destination point of transmissions within the mesh. To take it into account, three different methods of generating mesh topology have been used in simulation experiments, reflecting the most common mesh deployment scenarios.
The conducted experiments and their results tend to indicate, that perhaps the IEEE 802.11s black-box approach, while elegant in its design and implementation, induces unnecessary limitations making the WMN less likely to be employed in practice.

In general, the obtained results indicate, that a wireless mesh network of the IEEE 802.11s standard is able to provide the service level necessary for deployment of popular multimedia services, in a manner comparable with the classic PtMP WiFi access, when communication conditions are comparable and the network is not congested. Moreover, by employing the proposed cross-layer modification to IEEE 802.11s mechanisms it is possible to extend the range of conditions where the WMN network is capable of doing so, thereby allowing the use of mesh-specific advantages of this technology.

Most of the results and solutions presented in this dissertation have been published as journal articles and conference papers. The list of relevant publications is as follows:

[12] Gierłowski K.: integracja międzywarstwowa protokołów RM-AODV, Multicast DNS i IPv6 Neighbor Discovery w środowisku sieci standardu IEEE 802.11s, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 8-9/2016

[13] K. Gierłowski, "Cross-layer mDNS/ARP Integration for IEEE 802.11s Wireless Mesh Network," 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), Colmar, 2016, pp. 33-40; IEEE Xplore.

[14] Gierłowski K., Hoeft M., Gumiński W.: „Laboratorium mobilnych technik bezprzewodowych", Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr. 8-9 (2015), s. 1141-1150

[15] Gierłowski K.: „Ubiquity of Client Access in Heterogeneous Access Environment", Keynote of IEICE Wireless Networks Workshop 2013, Journal of Telecommunications and Information Technology, issue 3 (2014), s. 3-16

[16] Gierłowski K.: „Mechanizmy odkrywania usług i integracji międzysieciowej w samoorganizujących systemach bezprzewodowych standardu IEEEE 802.11s", Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr. 8-9 (2013), s. 1120-1130

[17] Gierłowski K.: "Interworking and Cross-layer Service Discovery Extensions for IEEEE802.11s Wireless Mesh Standard", Journal of Telecommunications and Information Technology, nr. 3 (2013), s. 97-105

[18] Gierłowski K.: “Service and Path Discovery Extensions for Self-forming IEEE 802.11s Wireless Mesh Systems”, 17th Polish Teletraffic Symposium 2012, Zakopane 2012
[19] Hoeft M., Gierłowski K., Gierszewski T., Konorski J., Nowicki K., Woźniak J.: “Measurements of QoS/QoE Parameters for Media Streaming in a PMIPv6 Testbed with 802.11 b/g/n WLANs”, Metrology and Measurement Systems, nr 2, s. 283-294, 2012
[20] Gierłowski K., Kostuch A., Woźniak J., Nowicki K.: “Testbed Analysis of Video and VoIP Transmission Performance in IEEE 802.11 b/g/n Networks”, Telecommunication Systems, Issue 3, Vol. 48, p. 247-260, 2011
[21] Kostuch A., Gierłowski K., Woźniak J.: “Performance Analysis of Multicast Video Streaming in IEEE 802.11 b/g/n Testbed Environment”, Wireless and Mobile Networking : Second IFIP WG 6.8 Joint Conference, WMNC 2009, Gdańsk 2009
[22] Gierłowski K., Nowicki K., Pieklik W., Pawałowski P.: “An Integrated E-Learning Services Management System Providing HD Videoconferencing And CAA Services”, 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2012), Poznań, 18-20.07.2012, p. 1-6
[23] Gierłowski K., Woźniak J.: „Analiza szerokopasmowych sieci bezprzewodowych serii IEEE 802.11 i 16 (WiFi i WiMAX) z transmisją wieloetapową”, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 8-9/2008, s. 925 – 935, 2008

The listed papers include both results of research preliminary to specification of original mechanisms proposed in this dissertation [15,19-23] and results relating to the proposed, cross-layer mechanisms directly [12,13,16-18]. Additionally, there is a description of an advanced testbed designed to allow verification of the proposed experiments in real-world metropolitan conditions [14] complete with an example experimental scenario concerning the cross-layer interworking solutions proposed in chapter 6.

2 IEEE 802.11 Wireless Local Area Network – architecture and main components

The wireless mesh technology which has been chosen as an environment of interest for this thesis, is an extension of a Wireless Local Area Network (WLAN) 802.11 standard [1] published by Institute of Electrical and Electronics Engineers (IEEE).
To consistently and clearly present mechanisms of the abovementioned mesh technology, an introduction describing the base WLAN technology is in order. In the following chapter, a description of an overall architecture of the IEEE 802.11 system, its modes of operation, most important mechanisms and functions are presented, to provide background information for a description of the IEEE 802.11s mesh network provided in the next chapter.

2.1 Layer reference model

IEEE 802.11 standard specifies two distinct elements of WLAN system: medium access control (MAC) mechanisms of data link layer (ISO-OSI layer 2) and physical layer mechanisms (ISO-OSI layer 1). This architecture, including appropriate service access points (SAPs) allowing interoperation of mechanisms located in different layers is presented on the figure below (Fig. 1).

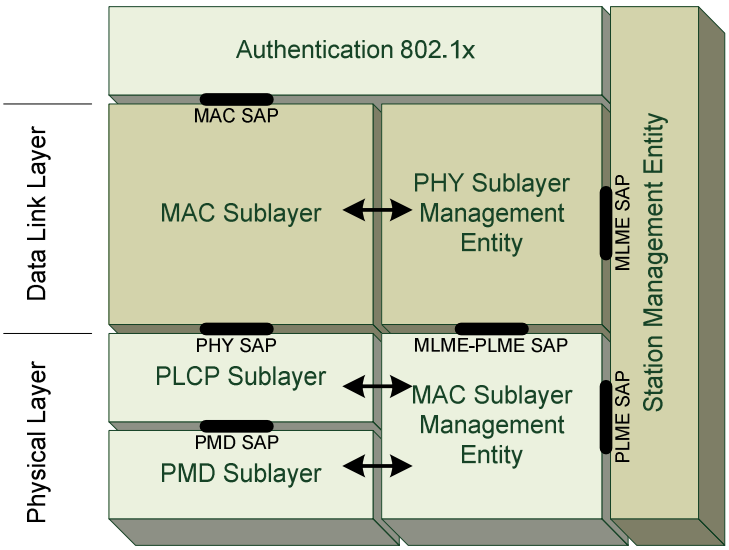

Fig. 1 IEEE 802.11 Layer reference model

In this thesis we are mainly interested in MAC sublayer mechanisms, specifically including management functions. Physical layer details of IEEE 802.11 WLAN operation are outside of scope of this work so their detailed description is omitted for the sake of clarity.
IEEE 802.11 MAC sublayer mechanisms on the other hand are a base on which IEEE 802.11s mesh mechanisms are directly dependent, so we dedicate this chapter to summary description of their functionalities and interactions.

2.2 Overall architecture

In case of IEEE 802.11-based wireless local area networks, the main building blocks of a network system are:

- Station (STA) – a device equipped with IEEE 802.11 compliant network interface, able to communicate in wireless fashion within its own BSS (see Fig. 2).
- Basic Service Set (BSS) – a logical entity composed of IEEE 802.11 compliant devices able to directly communicate by means of wireless transmission. Devices of a single BSS should share the common configuration and remain in Basic Service Area (BSA), loosely defined as a coverage area of a BSS (area where BSS services can be provided to a STA). Precise definition of BSA changes depending on wireless network's mode of operation.

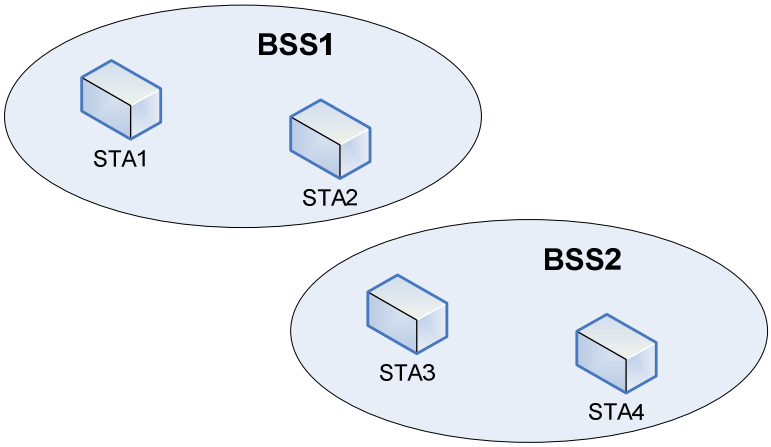

Fig. 2 IEEE 802.11 Basic Service Set (BSS) entities

A WLAN system, functioning according to current IEEE 802.11 standard, provides two basic modes of operation (Fig. 3):

- Ad-hoc mode – a distributed system, where wireless client stations communicate directly. Communication outside of BSS is impossible without higher layer (ISO-OSI layer 3+) mechanisms. A special type of BSS – Independent Basic Service Set (IBSS) – is used in this mode. BSA consists of stations (STA) located in direct, mutual transmission range.
- Infrastructure mode – a dedicated device (access point – AP) is used as an intermediary for transmissions in infrastructure mode. All transmissions are directed to AP which than retransmits them to their destinations (2 hop transmissions), or need to be negotiated with the AP if they are to be conducted directly (1 hop transmissions). It should be noted, however, that direct transmission mode is a relatively new development, introduced in IEEE 802.11-2007 version of the standard. Due to necessity of contacting AP during all transmissions, BSA can be defined as coverage area of an access point.
  The main rationale for introducing this mode and AP is the need to provide ability to communicate with external networks (outside of current BSS) at ISO-OSI layer 2. Such communication is accomplished by connecting APs to a Distribution System (DS) which provides connectivity with other BSSs and networks of different technologies.

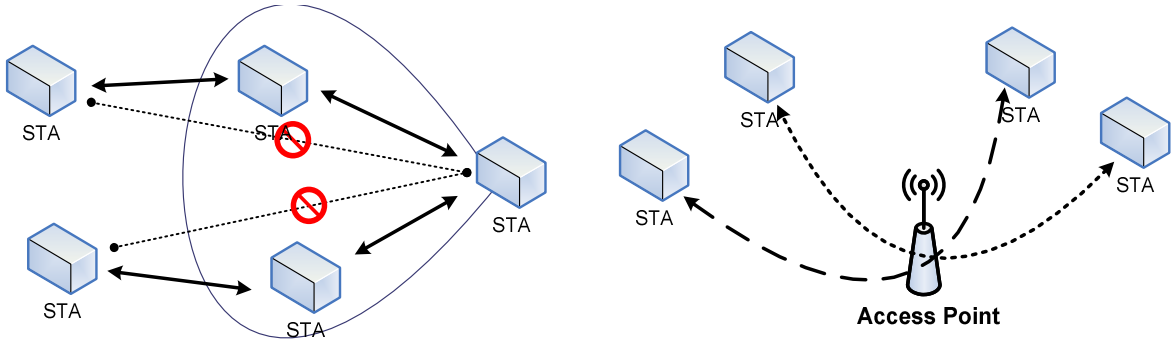

Fig. 3 Ad-hoc (left) and Infrastructure (right) modes

The introduction of access points (APs) and their ability to provide wireless stations with layer 2 communication outside boundaries of their current BSS is presently the main reason for vast popularity of infrastructure mode IEEE 802.11 networks. It should also be noted, that some modes of media access control (namely HCCA – Hybrid Coordination Function Controlled Access) relay on presence of a centralized controller (AP). Unfortunately their implementation is extremely rare in currently available commercial hardware.
In contrast, lack of such abilities and generally underdeveloped configuration and control mechanisms of ad-hoc mode has made its use incidental.

In modern versions of IEEE 802.11 standard (starting with IEEE 802.11-2007) BSSs can be further divided into BSSs supporting QoS mechanisms described in IEEE 802.11e amendment [32] (QoS BSS) and BSSs without such support.

The ability to provide connectivity between BSSs depends on presence of a Distribution System (DS), connecting the access points. An access point can be described as a compound entity, merging STA and DS-specific functionality (Fig. 4, further described in Section 2.3).

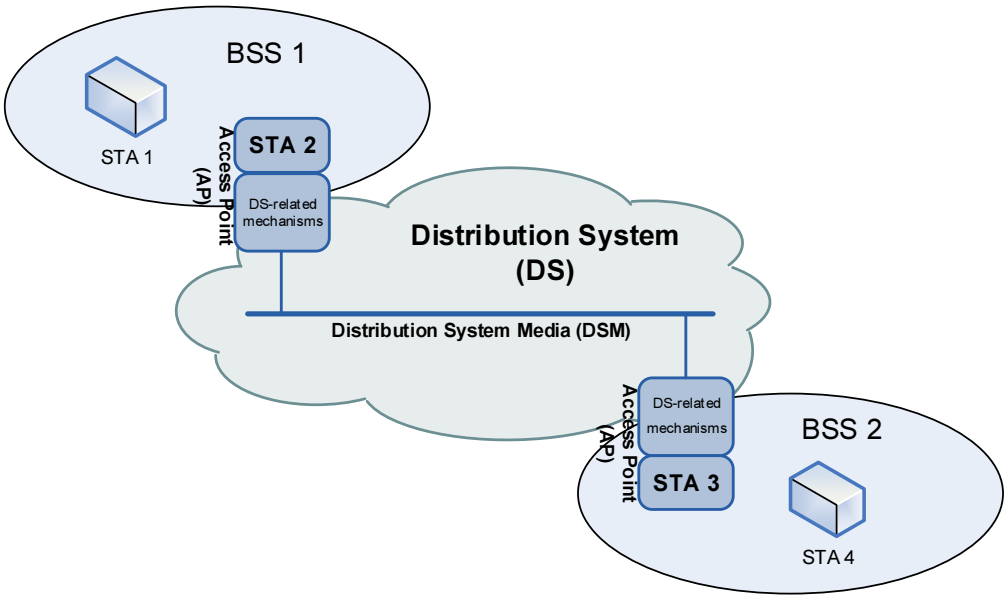

Fig. 4 IEEE 802.11 Distribution System

A Distribution System itself is not defined by IEEE 802.11 standard and can be create with use of various network technologies (Distribution System Medium - DSM), as long as they can support a mandatory set of services, which DS is compelled to provide in an IEEE 802.11 network system (see Table 1).
A concept of DS is crucial to creating more complex network systems based on IEEE 802.11 standard, as it enables a possibility of forming an Extended Service Set (ESS) composed of a number of individual BSSs. At the same time the lack of strict requirements concerning DSM, brings a degree of flexibility to the task.

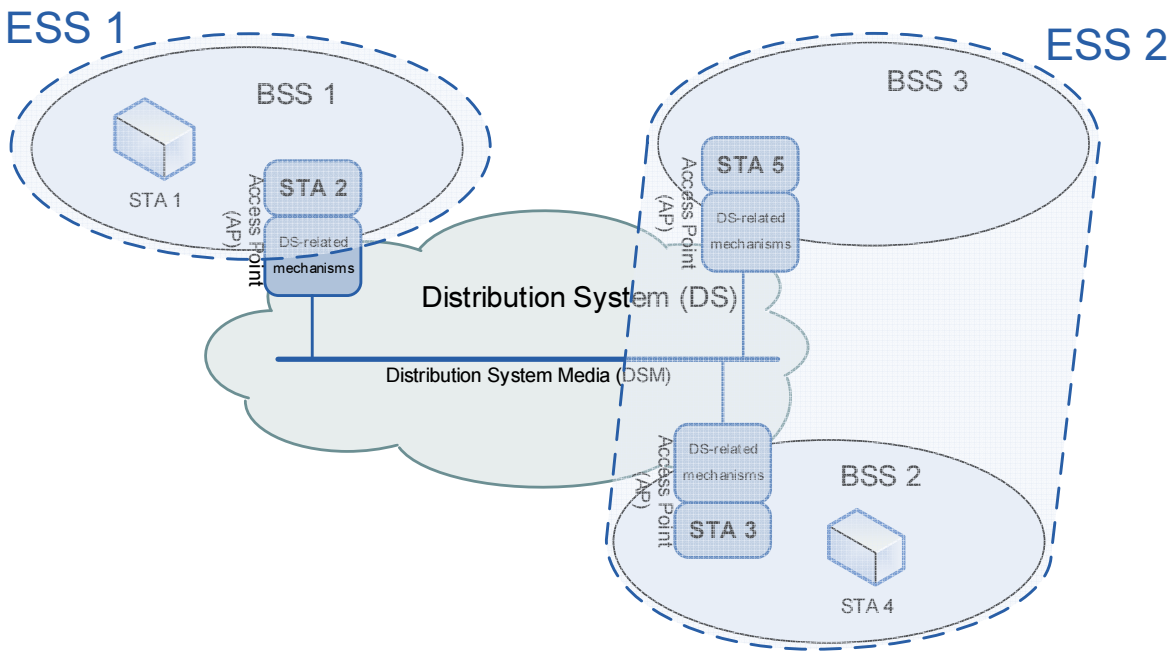

Fig. 5 IEEE 802.11 Extended Service Set (ESS)

An Extended Service Set is an union of BSSs connected by DS (Fig. 5). All stations within an ESS can communicate at ISO-OSI layer 2 and retain this communication despite moving between BSSs. BSSs within ESS can be located in an arbitrary way to provide:

- continuous coverage for a given volume of space – when BBAs of BSSs partially overlap,
- access at a number of spatially separated locations – when BSAs are separate – there is no limit to a distance between BSAs, as long as DS functions are available to all necessary APs,
- redundancy – when BSAs are spatially collocated.

The last of the main architectural elements of an IEEE 802.11 system is a portal (Fig. 6). It is an entity responsible for providing connectivity between DS and external, non-802.11 networks. As such it is, similarly to APs, a member of a DS, but it does not belong to BSS (and by implication to ESS). Instead it must belong to an external network.

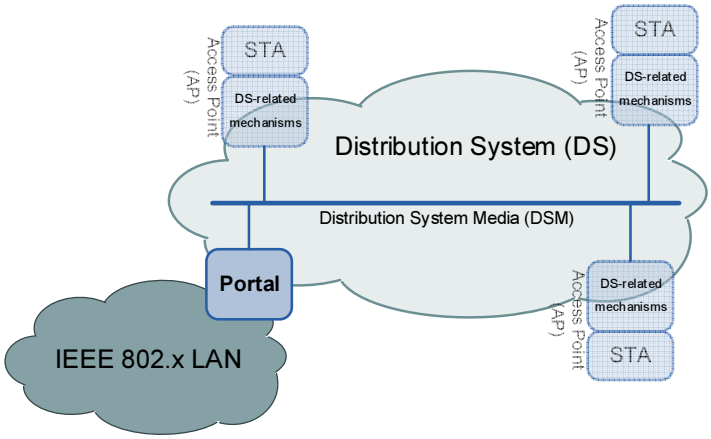

Fig. 6 IEEE 802.11 Portal

2.3 Wireless system services

Services which IEEE 802.11 based wireless system must provide are listed in Table 1 and fall under five categories:

- medium access control and service data unit (MSDU) delivery,

- WLAN access control and security,
- spectrum management,
- QoS support,
- higher layer synchronization.

All of the above services are supported by appropriate fame types, divided into three types: data, management and control.

Table 1 Services of IEEE 802.11 network. DSS – Distribution System Service, SS – Station Service.

Service	Location	Description
Distribution	DSS	Service used in the frame delivery process to determine destination address in infrastructure networks.
Integration	DSS	Frame delivery to an IEEE 802 LAN outside the wireless and DS networks.
QoS Traffic Scheduling	SS, DSS	Scheduling of intra-BSS frames.
Association	DSS	Used to establish the AP which serves as the gateway to a particular mobile station.
Reassociation	DSS	Used to change the AP which serves as the gateway to a particular mobile station.
Disassociation	DSS	Removes the wireless station from the network.
Authentication	SS	Establishes identity prior to establishing association.
Deauthentication	SS	Used to terminate authentication, and by extension, association.
MSDU delivery	SS	Delivers data to the recipient.
Data confidentiality	SS	Provides security protection of user traffic
Dynamic Frequency Selection	SS	Required for 5 GHz band.
Transmit Power Control	SS	Required for 5 GHz band.
Higher layer timer synchronization	SS	Provides time synchronization mechanisms for higher layers

2.3.1 Distribution System Services

Distribution system services are provided to elements of IEEE 802.11-based WLAN by Distribution System mechanisms. They are present only in case of BSS/ESS network, because in case of IBSS (ad-hoc) mode, there is no distribution system.

2.3.1.1 Distribution service

The service is responsible for delivery of every frame generated within an ESS to a proper BSS (or external layer 2 network accessible through a portal), where it can be received by its intended recipient.

While it is clear, that such service needs to be invoked when frame sender and recipient are located outside of sending station BBSs (the frame should enter DS by one AP and leaves it by another), it should also be noted that frame addressed to a destination station located in the same BSS as sending station also enter a DS and distribution service is involved in their proper handling. In such case frame enters and leaves DS through the same AP.

To fulfill its task, the distribution service must be able to locate the BSS of which the destination STA is currently a member and forward the frame to an AP appropriate for that BSS. APs in turn, must provide distribution service with sufficient information about STAs locations, which they, in turn, receive as a result of activity of three association related services: association, association and disassociation.

The standard does not specify how distribution service delivers frames to destination AP, as it is dependent on particular network technology utilized in DS.

2.3.1.2 Integration service

Integration service is responsible for handling messages, which were classified by distribution service for delivery to an external layer 2 network connected through a portal, instead of an another BSS within an ESS (reachable through an AP).
This service is invoked after distribution service delivers frame to an appropriate portal and must perform actions necessary to successfully forward such a frame from DSM to a media appropriate for the external network.
Particulars of the service are not defined by the standard, as they are dependent on involved (DSM and external) network technologies.

2.3.1.3 QoS traffic scheduling

The service responsible for scheduling intra-BSS frame transfers, when BSS supports IEEE 802.11e-compatible QoS aware medium access functions. At each transmission opportunity (TXOP), QoS traffic scheduling service selects a frame for transmission from one of multiple traffic queues, depending on variety of configuration parameters and current network state.
As a both Distribution System and station-specific service, it is present in both APs and STAs.

2.3.1.4 Association service

As described before, to successfully forward traffic within an ESS, distribution service needs to know, through which AP any given STA can be accessed. The process of creating a logical relationship between a STA and a BSS (with its serving AP) is called an association and is handled by an association service. This service also provides ESS distribution service with AP-STA mapping for delivery of inter-BSS traffic.
An STA can be associated with a single AP only at a given time. An association is required before a STA can send any data frames and is initiated by a STA.

2.3.1.5 Reassociation service

To support STA mobility by providing them with ability to move between BSSs within the same ESS a reassociation service has been defined. It allows STA to move its association to a different AP (and BSS) and keep distribution service informed about its current location, to properly forward inter-BSS traffic.
Reassociation service can also be used to change association parameters while remaining within the same BSS.

2.3.1.6 Disassociation service

This service is used to terminate existing association and remove information about a given STA from distribution service database.
The disassociation can be invoked by both non-AP STA and AP and cannot be refused, so it should be treated more as information and not a request. For efficient functioning of the system a STA leaving the system should inform AP about the fact by employing this service. The standard, however, cannot (and do not) require such behavior for correct functioning of the system as the frequent cause for stations to leave a system is a loss of physical communication ability (transmission range) with its AP. It is clear that a station in such situation cannot successfully employ a disassociation procedure.

2.3.2 Station Services

Station services are IEEE 802.11 services which are provided by STAs. Taking into account, that an AP also includes STA functionality, they must be provided by all IEEE 802.11 system devices.
A distinctive group of WLAN access control and security (ACS) related services is formed by authentication, deauthentication and traffic protection mechanisms. Operation of these services

depend on presence of IEEE 802.11i amendment describing security extensions for IEEE 802.11-based network which allow creation of a Robust Security Network (RSN) – an IEE 802.11 network utilizing modern security procedures.
Another distinctive group of station services refers to spectrum management tasks, mandatory for 5 GHz ISM band.
Two remaining services provide services for higher layers: time synchronization and transmission of higher layer data traffic.

2.3.2.1 Authentication (ACS service)

The authentication service allows a STA to establish their identity with other STAs with which they communicate. That can also include APs, as they contain both DS and STA elements.
Without successful authentication (accepted by both involved stations) the association will not be possible. Infrastructure mode BSS is controlled by an AP (which retransmits or controls all data transmissions), and all client STAs must associate with AP, making it a centralized access-control element.
It should be noted, that the service does not provide any type of end-to-end (sender-to-receiver of a message or user-to-user) authentication, only direct, link level authentication between directly communicating system devices.
The process of authentication can significantly vary depending on many factors and configuration parameters. Without the IEEE 802.11i amendment, two authentication methods are defined: Open authentication (always successful) and Shared Key authentication (utilizing the secret key as confidentiality services use). When a Robust Security Network (RSN) procedures are introduced (IEEE 802.11i amendment), extensible authentication procedures based on an Extensible Authentication Protocol's (EAP) [33] must be used. That allows use of any EAP-supported authentication method as long as it is mutually acceptable for involved parties.
It should be noted, however, that while successful authentication is required for association in BSS, the actual process may not include any means of verifying station identity and can be always successful. Without RSN extensions there is an Open authentication variant, while in EAP-OPEN method can be employed under RSN – both procedures always succeed (regardless of station's identity), as long as protocol procedures are successfully concluded.

To facilitate BSS transition for mobile STAs, a preauthentication procedures has been defined. They allow an STA to authenticate with a new AP, while still retaining association with a current one. In case of IEEE 802.11 system, where only hard handover is possible (as a single STA can only be associated with a single AP) it is a very beneficial possibility – there is no need to perform, possibly time consuming, authentication process during lack of user connectivity period characteristic for a hard handover.

2.3.2.2 Deauthentication service (ACS service)

This service is invoked, when an existing authentication needs to be terminated. Similarity to disassociation, deauthentication message is not a request, but a notification sent by station terminating the authentication to the other STA of authenticated pair. As such, it cannot be refused. In case of infrastructure BSS, a deauthentication results also in disassociation, as a valid authentication is a requirement for it.
Deauthentication message must be in all types of IEEE 802.11 networks, including ad-hoc IBBS, where authentication is optional.

2.3.2.3 Data confidentiality, key management, data origin authenticity, replay detection (ACS services)

As in case of authentication, these services can vary depending significantly. In case of a non-RSN network, a simple confidentiality and integrity protection is present, based on RC4 encryption with

a static key and CRC32 checksum respectively. Both contain numerous architectural and implementation errors, leading to almost complete lack of utility.
In case of RSN network, a number of mechanisms cooperate to provide:

- strong data confidentiality with use of an Advanced Encryption Standard (AES) encryption in counter mode (CTR) [34],
- cryptographic data integrity with use of AES in cipher block chaining (CBC) mode [35],
- automatic key management and delivery (4-Way Handshake and Group Key Handshake),
- data origin authenticity due to authentication and pairwise key agreements between communicating entities,
- replay detection due to packet counter integrated with data integrity mechanisms.

The above functions (except key management) are aggregated into protocols named Temporal Key Integrity Protocol (TKIP) and Counter Mode With Cipher Block Chaining Message Authentication Code Protocol (CCMP), one which need to be employed by a station, if the RSN security is to be archived.

2.3.2.4 Transmit Power Control (Spectrum management)

In case of WLAN operating in 5 GHz band, regulatory requirements concerning maximum transmit power and mitigation must be observed, to reduce likelihood of interference with other wireless services, for example satellite systems.
Transmit Power Control (TPC) service is necessary for this task and it is responsible for specifying the allowed range of transmission power levels for a transmission channel at a given location, choosing an AP of a BSS in accordance with allowed power levels, and adaptation of transmission power based on a range of information (including path loss and link margin estimates).

2.3.2.5 Dynamic Frequency Selection (Spectrum management)

In some locations radio regulations require wireless systems operating in 5 GHz band to include a mechanism which will prevent co-channel operation with radar systems and provide uniform utilization of frequency channels. Dynamic frequency selection (DFS) mechanism has been introduced to meet these requirements. DFS is able to test for radar emissions before and while operating on a given channel, report the results to interested parties, discontinue operations of IEEE 802.11 WLAN on a given channel, when radar emissions are detected, and quiet a selected channel (inform all parties on the channel to temporarily cease operation) to more precisely (without interference from other STAs) test for radar operation.

2.3.2.6 Higher Layer Timer Synchronization

Modern higher layers applications can require a more precise or more granular time synchronization then can be provided by a standard BSS timing synchronization function (TFS – utilized by, for example, IEEE 802.11 power saving mechanisms). In such case IEEE 802.11 network can provide such service with use of Higher Layer Timer Synchronization service. Synchronization is based on immediate signaling to higher layers a reception of a last symbol of MAC data frame with previously registered multicast destination address (Address 1 header field – see 2.4.4).

2.4 MSDU Delivery – 802.11 data plane architecture

IEEE 802.11 MAC Service Data Unit (MSDU) delivery is a station-based service, which means that it must be supported by all elements of a wireless system. This service is responsible for enabling two Logical Link Control (LLC) entities to exchange information in a form of MSDUs by use of services provided by physical layer (PHY).
In case of IEEE 802.11 network, MSDU delivery is asynchronous and connectionless. By default the delivery is carried out on a best-effort basis, but in case of QoS STAs, there are mechanisms to

provide differentiated services if such STA functions as a part of QoS BSS. In such a case traffic identifier (TID) is used to provide differentiated services on MSDU basis.
Standard also describes mechanisms and procedures for transmission with QoS guarantees, by use of dynamically created traffic streams (TS), grouping MSDUs into sets described in traffic specifications (TSPEC). TSPEC describes both basic traffic stream characteristics and its QoS requirements.
Depending on presence or lack of QoS mechanism in MSDUs are transmitted between devices in QoS or non-QoS data frames (see 2.4.5.3).

2.4.1 Delivery service classes

IEEE 802.11 MSDU delivery service defined 2 classes of service, controlling the overall method of MSDU handling and possibility of MSDU reordering.
In case of legacy, non-QoS destination STAs non-QoS fames are used. Different class is used to transmit unicast and group-addressed (multicast/broadcast) frames, due to different requirements of their delivery (group-addressed frames are not acknowledged).
In case of QoS destination STAs QoS frames are employed, and delivery service class can be explicitly specified:

- QoSAck – correctly received frames are to be acknowledged regardless of type. One of two modes of acknowledgement can be required: normal or block ACK. This class (in normal ACK mode) corresponds to unicast frame delivery in non-QoS STA.
- QoSNoAck – no frames are to be acknowledged. Corresponds to group-addressed frame delivery in non-QoS STA.

2.4.2 QoS support

To support QoS mechanisms, MSDU delivery service utilizes TID value assigned to each MSDU.
MSDU TID values 0-7 define 8 user priorities (UP) which correspond to priority values defined in IEEE 802.1D specification. These are later assigned to 4 different access classes (AC) which directly determine future queuing and medium access parameters for an MSDU. These values are allowed for QoS STAs functioning in QoS BSS or IBSS.
MSDU TID values 8-15 identify a specific traffic stream, which should be previously defined and created with use of network's management mechanisms. Future handling of such marked MSDUs depend on TSPEC parameters of a given TS. These values are allowed for QoS STAs functioning in QoS BSS.
Apart from these values of TID, which are sent in frame header of QoS frames, there are also two values of TID processed internally within a STA: Contention and ContentionFree. They are employed in case of transmissions utilizing non-QoS data frames, which lack QoS Control field (see 2.4.5.3) necessary to include TID. Such frames are used by non-QoS STAs, which also include QoS-capable STAs functioning in non-QoS BSS or IBSS.
TID value of Contention is assigned to MSDU if its frame has been received during contention access period. In case of outgoing MSDU this value results in transmission as TID 0 (lowest possible priority) during contention phase.
TID value of ContentionFree is assigned if a frame has been received during contention-free access period. This value in case of outgoing MSDU results in frame being sent during contention-free phase if point coordinator (PC) is present and as contention-based TID 0 otherwise.

2.4.3 MSDU reordering

In case of non-QoS frames, both unicast and group-addressed MSDUs are always delivered in order, but only within their group. It is highly probable that there will be change in the order of received

MSDUs between unicast and group-addressed ones, due to power-save related buffering of the second group.
In case of QoS frames, unicast MSDUs are delivered in order only within their access class (AC). Order of MSDUs belonging to different classes will most probably be changed. Group-addressed MSDUs transmitted by multicast or broadcast frames will also retain their order only relative to other group-related MSDUs.

2.4.4 IEEE 802.11 MAC frame format

All STAs must be able to construct and decode a subset of described frame types, depending on their supporting functionality. There is a mandatory set of frame types which must be supported by all STA, but at the same time the standard allows for future amendments or even proprietary extensions.
Overall IEEE 802.11 frame format (Fig. 7) consists of MAC frame header, data and frame check sequence (FCS) field. Frame header includes control, duration, addressing information, sequence numbering and, in case of QoS data frames, QoS information. FCS is a 32bit CRC value calculated over all MAC header fields and the Frame body, for the purpose of detecting transmission errors. Data field carries user data or frame-type/subtype specific information and can have length of 0 bytes.

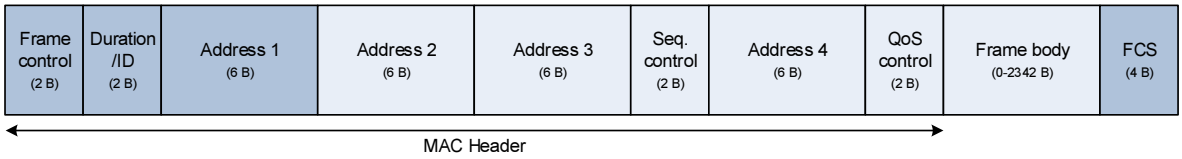

Fig. 7 Overall IEEE 802.11 frame format

The overall structure of IEEE 802.11 frame has been presented on Fig. 7. A set of mandatory fields, which are present in all frames consists of:

- Frame control field (FC) – carries information identifying content of the frame (type-subtype – necessary for correct decoding due to changing frame structure) and connected to mechanisms directly associated with frame transmission, such as fragmentation, retransmission, data unicast/group traffic reordering, power saving and distribution system support.
- Duration/ID field – one of key elements of medium access control mechanisms, allowing prediction of medium utilization time for a current frame,
- Address 1 field – the only address filed present in all frame types/subtypes, identifies intended frame receiver,
- Frame check sequence (FCS) field.

The remaining fields are present only in some of the IEEE 802.11 frame types/subtypes.

2.4.5 Frame types

There are three base frame types defined in the current IEEE 802.11 standard:

- Control frames – used in direct transmission control: RTS/CTS mechanism, acknowledgements, power-save polling and contention free period polling,
- Management frames – used for all management tasks (e.g. network discovery, authentication, association), except procedures utilizing control frames. The type also includes action frames (see below) utilized by a number of optional network mechanisms.
- Data frames – utilized for higher layer data transmission. Depending on presence or lack of QoS support on sending STA, a QoS Data Frame or non-QoS Data frame (respectively) can be used.

They are identified by appropriate value of Type subfield of FC frame header field.

2.4.5.1 Control frames

Control frame exchanges are key elements of medium access and transmission protocols. Due to their frequent occurrence, their length has been kept at minimum, as it has significant impact on transmission performance. Their usage and medium access control rules for their transmission are strictly defined specifically for each subtype. There are 8 subtypes of control frames identified by Subtype subfield of FC frame header field.

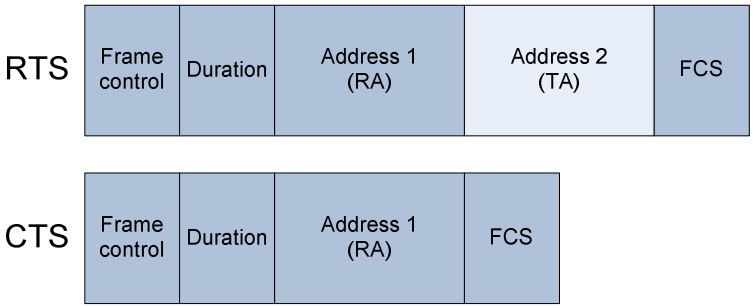

Fig. 8 RTS/CTS Control frames

Ready to send (RTS) frame consists of frame control (FC), duration, FCS fields and receiver (RA) and transmitter address (TA). It is used as a part of RTS/CTS medium reservation protocol and indicated the sending STA (TS) intent to transmit a data frame to RA.
Very short **clear to send (CTS)** frame (FC, duration, RA, FCS) is sent as an affirmative answer to RTS request, indicating that RTS sending station can proceed with data frame transmission within time frame indicated by duration field.
RTS/CTS will be further described in 2.5.1.2.

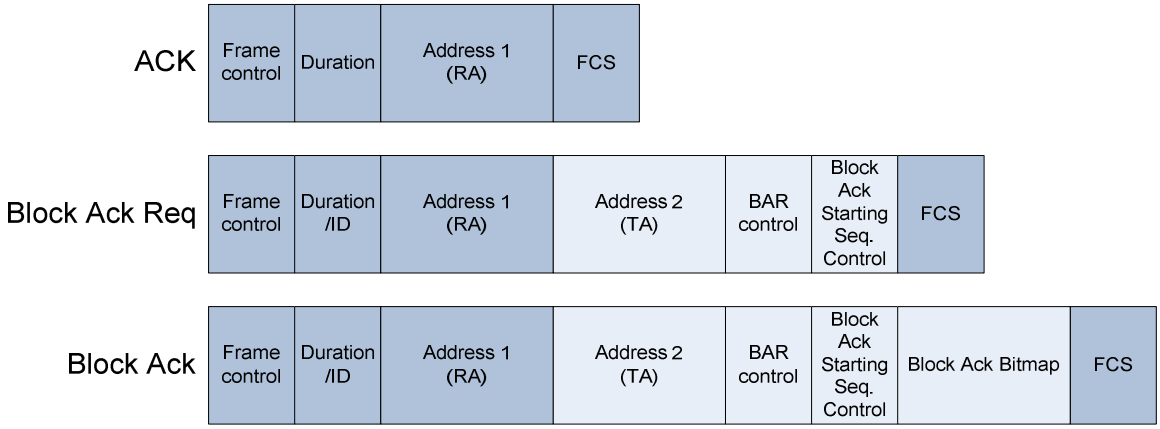

Fig. 9 Acknowledgement Control frames

Acknowledgement frame (ACK) is used by receiver to acknowledge a correctly received frame to prevent its retransmission by its sender. This frame also consists only of FC, duration, RA and FCS fields, which corresponds to the shortest possible IEEE 802.11 frame.
If block acknowledgement modes are employed (see 2.5.4.2), two more messages are introduced to support them: BlockAckRequest (allowing sender to request an acknowledgement of a group of frames) and BlockAck (sent in response by receiver, to acknowledge the group of frames in question). Due to an additional complexity of block acknowledgement mechanisms, these frames are somewhat longer, containing (in addition to ACK frame filelds) two 2 octet control fields and in case of BlockAck contains 128 octet Bitmap field. We have to keep in mind, however, that BlockAck allows its sender to acknowledge up to 64 received frames at a time.

If a BSS network is utilizing power saving mechanisms, **PS-Poll** control frame is utilized by stations to request a transmission of unicast frames addressed to them, which have been buffered at an access

point during their power-save sleep period. Frame consists of FC, ID (in place of duration field), two address fields indicating BSS and transmitting station address and FCS.

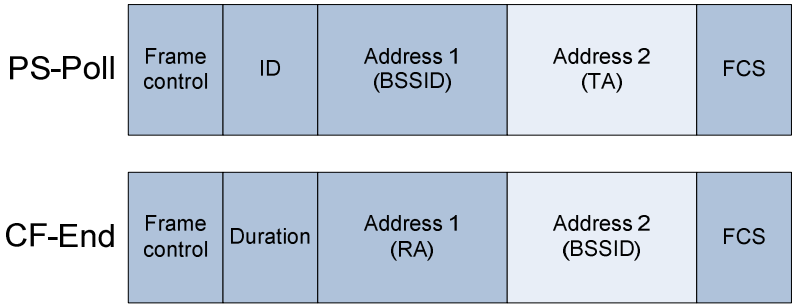

Fig. 10 PS-Poll and CF-End Control frames

CF-End and **CF-End+Ack** control frames are utilized to end a contention free period (see 2.5.2 and 2.5.5). The second one allows its sender to simultaneously acknowledge reception of a frame. These frames consist of FC, duration, RA, TA (indicating a BSS as the frames can only be sent by AP) and FCS.

As can be seen from the above list and short description of their usage, control frames are utilized in time-critical functions of transmission control mechanisms of the network. As such they are kept as simple and short as possible for reasons of reliability and efficiency. For similar reasons they are also never encrypted.

2.4.5.2 Management frames

Management frames are utilized to carry MMPDUs (MAC Management Protocol Data Units) used by IEEE 802.11 network management mechanisms, which do not require very low latency communication offered by control frames. The mechanisms include:

- Network discovery in its passive (beacon frames) and active (probe request/response frames),
- Authentication (authentication/deauthentication frames),
- Association (association/reassociation/disassociation frames),
- Power saving (ATIM frames).

Different kinds of management frames are identified by value of Subtype subfield of Frame Control (FC) frame header field (). The limited length of Subtype subfield (only 16 different values) created a considerable difficulty, as the requirements for new management frame subtypes already exceeded this number.

To work around this limitation, an Action subtype of management frame has been introduced. Its format includes additional Category field (1 octet in length) located in the frame body, to describe the type of management information contained therein.

Action management frames are utilized by the following standardized mechanisms:

- Block Acknowledgement management (ADDBA Request/Response, DELBA),
- Direct Link Protocol (DLS Request/Response/Teardown, ADDTS Request/Response, DELTS, Schedule),
- Spectrum Management (Measurement Request/Response, Transmission Power Control Request/Response, Channel Switch Announcement).

There is also an identifier space within the action management frame subtype reserved for proprietary usage.

The overall format of management frames is shown in the Fig. 11 below. It consists of FC, Duration, Address 1 to 3, Sequence Control, Frame Body and FCS fields – a frame structure much extended compared to control frames. Address 1 is used to indicate recipient of the frame, while Address 2

and Address 3 identify its sender and BSS to which the frame belongs – it is necessary to allow STAs to filter out group-addressed management frames from outside their BSS.

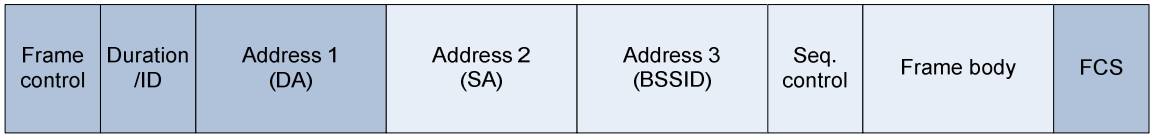

Fig. 11 Management frame format.

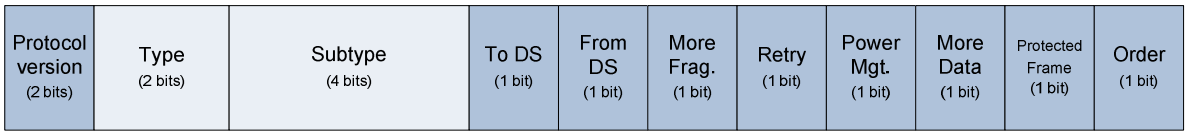

Fig. 12 Frame Control (FC) field

The data field of management frames consists of Information Elements (IE) – data structures consisting of identifier and information. For each type of management frame the necessary IEs are strictly defined and must be present in actual frame. Additional IEs however are allowed, and if a STA does not recognize a given non-mandatory IE it should ignore it. Such solution makes the format an easily extensible one, as both new IEs can be defined, and the contents of a particular frame subtype can be changed dynamically by including or removing Information Elements as necessary.

2.4.5.3 Data frames

Data frames carry higher layer MSDUs between two IEEE 802.11 network devices. There are two main groups of data frames:

- QoS data frames – frames generated by QoS-aware stations when sending date to other QoS-aware stations. Frames include QoS Control field.
- Non-QoS data frames – frames generated by legacy stations, unaware of QoS extensions included in IEEE 802.11-2007 standard or QoS-aware stations when sending to legacy stations. Frames lack QoS Control field.

Furthermore, to improve performance of network mechanisms, a two of Contention Free mode control messages (see 2.5.2 and 2.5.5 – CF-Poll, CF-Ack) has been allowed to be carried in the data frames, forming their different subtypes (identified by Subtype subfield of FC frame header field):

- Subtypes carrying MSDU:
  - Data / QoS Data
  - Data+CF-Ack / QoS Data+CF-Ack
  - Data+CF-Poll / QoS Data+CF-Poll
  - Data+CF-Ack+CF-Poll / QoS Data+CF-Ack+CF-Poll
- Subtypes used exclusively for MAC control purposes:
  - Null (no data) / QoS Null (no data)
  - CF-Ack (no data) / QoS CF-Ack (no data)
  - CF-Poll (no data) / QoS CF-Poll (no data)
  - CF-Ack+CF-Poll (no data) / QoS CF-Ack+CF-Poll (no data)

2.4.6 Fragmentation

MAC layer supports fragmentation of large MSDUs or even management frame content (MAC Management Protocol Data Unit – MMPDU) which is larger than maximum available data field size (which can vary depending on, for example, security mechanisms employed). The fragments are then reconstructed by the receiver.

Transmission mechanism requires acknowledgement of all transmitted fragments but such solution allows for retransmission of a single fragment instead of entire fragmented MSDU or MMPDU.

2.4.7 Data frame address usage

In case of management and control frames, the usage of header address fields is strictly defined for a particular frame type and subtype. In case of data frames, however, there is a number of possible scenarios of data transmission, which result in different address fields usage. Possible variants have been presented in the table below.

Table 2 Data fame addressing

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Usage scenario
0	0	RA = DA	TA = SA	BSSID	-	
0	1	RA = DA	TA = BSSID	SA	-	
1	0	RA = BSSID	TA = SA	DA	-	
1	1	RA	TA	DA	SA	Reserved for mesh use

Addressing scenarios are identified by ToDS and FromDS fields contained within Frame Control header field.

As we can see, frame header address fields can contain different information entities depending on scenario, but their overall, logical meaning remains unchanged:

- Address 1 – direct receiver address. Address of station which should receive a given wireless frame. Can contain group address, in which case BSSID is checked to ensure that only group transmissions from station's current BSS will be received. Can also contain BSSID if data is meant to be transmitted to DS.
- Address 2 – direct sender address. Address of a station physically sending a given frame. This information is used in acknowledgement mechanism, as ACK frame receiver address. Can contain BSSID in frames being sent into BSS from DS.
- Address 3 – contains additional address information. Identifies BSS when data frame is transmitted within its bounds (without entering DS). In case of frames originating or intended to be sent outside of BSS (through DS) it identifies original sender or final receiver of data (respectively). It is necessary as in such case they are different from direct sender and receiver addresses.
- Address 4 – only used in case of transit data frames (which both originate and are sent to stations outside BSS) when it contains address of station which initially generated the frame (original sender), while Address 3 field contains address of final destination. It is worthy of note, that this specific scenario is outside of scope of the standard and exact use of this field is not defined. Such situation resulted in multiple proprietary solutions utilizing this field in incompatible manner.

2.5 Media Access Control Sublayer

Access to physical wireless medium offered by physical (PHY) ISO-OSI layer of IEEE 802.11 standard, needs to be controlled to allow its sharing between multiple users. This task is handled by Media Access Control Sublayer (MAC Sublayer) which overall architecture and component functions are presented on the figure below (Fig. 13).

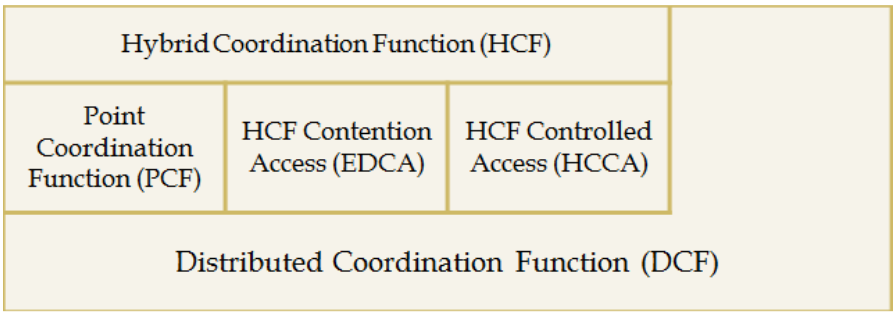

Fig. 13 IEEE 802.11-2007 Media Access Functions.

The fundamental media access function of MAC Sublayer is called Distributed Coordination Function (DCF) and provides access to shared media using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [1] method. The period of time during which DCF is utilized to provide shared medium access for STAs is called a Contention Period (CP).
Moreover, a number of additional MAC Sublayer functions have been defined based on DCF – Point Coordination Function (PCF), Enhanced Distributed Channel Access (EDCA) and HCF Controlled Channel Access (HCCA). These utilize DCF functionality to provide alternative medium access methods and are described in following sections.
The procedures and mechanisms described below are applicable in transmission of:

- data frames used to transmit MSDUs (MAC Service Data Units) received from higher layers,
- management frames used to transmit MMPDUs (MAC Management Protocol Data Units) generated by MAC layer management entities.

The remaining type of wireless frames – control frames – have their own usage and medium access rules, depending on their specific function.

2.5.1 Distributed Coordination Function (DCF)

Under DCF rules, if a STA want to transmit a data or management frame it must check medium to detect if another station is currently transmitting. If the medium is free for a defined time period (DCF Interframe Space – DIFS) the STA can transmit a frame. If another device transmission is detected, the STA must wait for the transmission to finish.
After the other device finished its transmission the STA must perform a backoff procedure – choose a random backoff time value and decrement it if a medium remains free for a time longer than DIFS. When backoff timer reaches zero the STA can transmit a frame.
STA must perform backoff procedure after successful transmission of a frame, before it can begin new transmission attempt. Successful transmission is defined as receiving ACK for a unicast frame and finishing sending a group-addressed frame.

Despite the above mechanism, there is a possibility of two STA will try to transmit their frames in overlapping time intervals leading to failure of both transmissions. Potential reasons for such situation include simultaneous transmission start or limited efficiency of physical medium state detection (see below). Such situation is described as a collision and results in necessity to retransmit both colliding frames.
The adverse effect of collisions on transmission performance is only made worse by the fact that transmitting stations are unable to detect this condition in progress and abandon failed transmission, thus freeing the medium. This is due to physical limitations of their transceiver units which are unable to monitor wireless medium during their own transmissions (half-duplex radio modules).
Additional mechanisms may be employed to further minimize the probability of collision, such as RTS/CTS exchange prior to transmission.

2.5.1.1 Medium state detection (Carrier Sense)

As its name implies CSMA/CA relies on stations monitoring the state of transmission medium (Carrier Sense - CS) to determine if it is currently free or utilized. Mechanisms employed for this purpose in case of IEEE 802.11 standard are two-fold: physical monitoring of wireless medium and virtual (logical) medium state maintained by MAC Sublayer based on information contained received in wireless frames.

Procedures monitoring a current state of a physical medium (Physical CS) are conducted by a PHY layer mechanisms and their results are subsequently reported to a MAC sublayer. Unfortunately, variety of physical and technological constraints limit the reliability of such a detection method. Already mentioned half-duplex radio modules which make physical medium state detection possible only while a given STA is not transmitting actively can be one example. Another example is a hidden station effect [36], when sending STA is outside of range of a transmission while receiving STA is in its range – is such scenario sending STA will detect free medium in begin its transmission leading to collision at the receiving station.

To minimize adverse effect of these and similar problems, a virtual medium state (Virtual CS) is being maintained by mechanisms of MAC Sublayer. Each station maintains Network Allocation Vector (NAV) indicating how much longer the medium should be considered busy, regardless of its physically detected state.

Each wireless frame header contains Duration/ID field (except PS-Poll frame, where the field is used for station identification and different rules apply), which contains information how much longer the current operation of sending station will take and when medium will be freed. Other stations hearing the frame must update their NAV value if the field indicates grater NAV value than currently set.

The standard details how Duration field should be set for various operations, but as a rule, it is set to cover a whole operation, instead of only a current frame transmission. For example:

- Data frame sets NAV to cover its transmission and its acknowledgement,
- Beacon frames starting Contention Free Period (CFP – see below) set NAV to cover entire CFP,
- Frame fragments set NAV up until ACK of the next fragment.

Such solution highly raises chances of successful (collision free) completion of multi-stage operation, as it is sufficient for other stations to receive a single of its frames, to protect the whole operation.

2.5.1.2 RTS/CTS

In presence of virtual medium state mechanism, frame collision probability is significantly reduced. However they can still occur and cause failure of both colliding transmissions. Moreover, hidden station effect can also lead to collision at receiving station.

To protect against this effect and as additional protection of long transmissions (costly in terms of medium usage) an RTS/CTS mechanism has been introduced. Its use is controlled by RTS Threshold parameter and all transmission of frames exceeding this length are required to utilize RTS/CTS mechanism.

If RTS/CTS is to be used, the initial medium access procedure is performed according to general DCF rules, but instead of the data fame, an RTS control frame is transmitted by the sender. RTS control frame is very short, so even if collision occurs it does not lead to significant medium utilization waste. The receiving STA, upon reception of RTS control frame immediately (after SIFS time, without media state detection) responds with CTS control frame. If the sending station receives CTS it can immediately send the data frame, which receiving STA then acknowledges according to general DCF rules.

Each of the frames in the above exchange set NAV to cover entire exchange up to and including the final ACK. Due to two-way exchange of RTS/CTS control frames, all stations within interference range of both sending and receiving STA is notified and update their NAV, thereby refraining from transmitting until RTS/CTS announced transmission is finished.

This solution induces additional overhead due to RTS/CTS exchange prior to transmission, but in case of long frames and/or in presence of hidden station it is still advantageous. We have to keep in mind that RTS/CTS control frames are very short and thus possible collision will result in loss of short control frame instead of possibly much longer data frame. Moreover RTS/CTS frames are received and interpreted by stations regardless of their current BSS, which facilitates their coexistence in terms of medium sharing.
To balance costs and advantages of the RTS/CTS mechanism the RTS Threshold parameter should be chosen with care.

2.5.1.3 Interframe space times and slot time

Many IEEE 802.11 medium access control mechanisms relay on different time periods, which must be observed while conducting specific operations – for example: medium should be monitored by a specific time before it is considered to be free, frame should be acknowledged in specific period of time or else its transmission is considered to be failed etc. As a result, a number of named time periods have been defined for use with MAC mechanisms. Their precise lengths depend on a given type of PHY layer employed.
The most basic is a slot time (ST). It is defined as a PHY layer parameter and is defined as the sum of the RX-to-TX turnaround time and the energy detect time.
The rest of defined time periods are jointly referred as Interframe Space times (IFS). There are 4 specific periods defined within this group for non-QoS STA (supporting only DCF and PCF medium access modes):

- Short Interframe space (SIFS)
- PCF Interframe space (PIFS)
- DCF Interframe space (DIFS)
- Extended Interframe space (EIFS)

In case of QoS STA, an additional sub-group of time intervals is defined, under a common name of Arbitration Interframe space (AIFS). The AIFS period is different for each of defined Traffic Classes (see 2.5.4), which is indicated by notation AIFS[AC].

SIFS is the shortest time of all IFSs. It is used when a STA needs to retain medium access to complete a multi-stage operation which shouldn't be interrupted. Such operations are called "atomic operations" and include, for example: RTS/CTS exchanges with subsequent protected frame transmissions, fragmentation bursts, pooling by Point Coordinator during Contention Free Period of PCF (see 2.5.2), acknowledging a frame, etc.
Due to the fact, that all other IFS times are longer than SIFS, no other STA can interrupt a sequence of operations separated by SIFS intervals by gaining medium access, as the standard requires them to wait longer then SIFS before taking up such activity. In other worlds the use of SIFS in atomic operations protects them from being interrupted. It should be noted, however, that to begin such operation STA needs to acquire medium access using general DFS rules.

PIFS time is used to begin a Contention Free Period (CFP) when PCF access rules apply. CFP begins with a Beacon management frame containing a specific indication of the fact. As the ability to initiate CFP should have priority over all other medium access operations except already started atomic operations, Point Coordinator which wishes to initiate CFP must sense medium state and find it free for PIFS duration, before it broadcasts the CFP-initiating Beacon frame. PIFS duration is longer than SIFS, but shorter than any other of IFS times, and thus a necessary priority is obtained.

DIFS time is used by stations operating under DCF rules to transmit data and management frames. Before attempting to transmit such frame, STA must check medium state and find it free for a duration of DIFS. DIFS is longer than both SIFS and PIFS, giving operations conducted with their use a priority over standard data and management traffic.

EIFS is the longest IFS time period, resulting in the lowest priority of operation which requires its use, but the purpose of EIFS is somewhat different than other IFS times – its length is not chosen to provide a specific priority but for seamless support of frame transmission in complex radio propagation environment.
The need for EIFS is based on the fact that a wireless frame can be received correctly by some of the stations, while other STAs will detect the same transmission as failure. It is possible that a frame will be correctly received by its intended receiver, but other stations will detect is as malformed (for example due to incorrect FCS). The possible reasons include hidden station effect which results in localized collisions and different propagation conditions for different stations, resulting in transmission errors in case of some STAs.
Without EIFS station detecting a failed frame transmission would potentially be able to commence its own transmission after DIFS time. That would lead to collision with acknowledgement of the previous frame, if it was in fact correctly received by its intended receiver (Fig. 14).

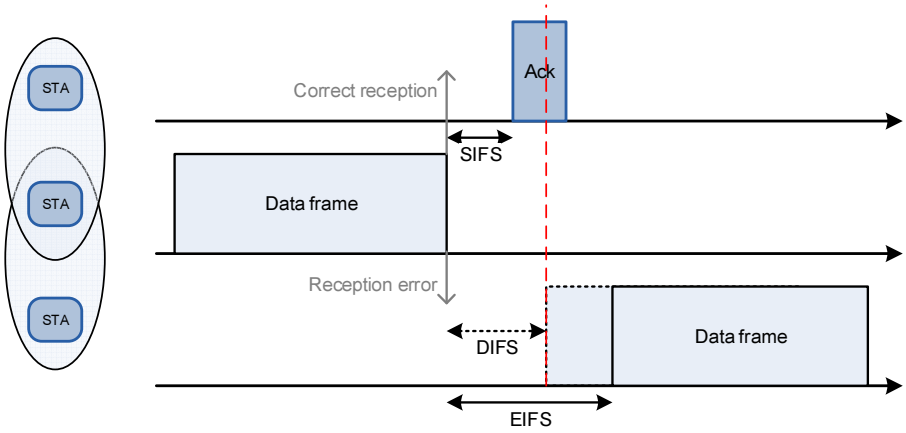

Fig. 14 EIFS-based ACK protection

Due to this possibility, the EIFS time should be used instead of DIFS if the station detected that previous transmission on the wireless medium has failed. Moreover, the EIFS time is measured regardless to NAV, as it is highly probable that due to the fact that last frame has been received with errors that NAV has not been correctly updated.
The length of EIFS is defined as EIFS = SIFS + ACKTime + DIFS, where ACKTime is a time needed to transmit an ACK control frame.
In other words EIFS is a time period which covers a time for receiver to acknowledge the last frame (SIFS + ACKTime) and a mandatory medium detection time normally used under DCF rules before a STA can begin its transmission (DIFS). Such usage of EIFS makes the described effect of incorrectly detecting success or failure of other station transmission safe in terms of medium access procedures.

2.5.1.4 Backoff

As described before, when a station needs to send a data or management frame, it should ensure that medium is free for an appropriate interval (DIFS), while also taking into account the possible need to utilize EIFS interval. If the medium is and remains free, the station can simply begin its transmission. In other case, when medium is detected as busy any time during the specified interval, the STA should employ backoff procedure.
The backoff procedure requires STA to choose a random backoff time measured in slot times, as defined earlier. The backoff time is to be chosen, in a pseudo-random manner, from an interval of [0,CW], where CW is an integer depending on number of times the backoff procedure is repeated by a given STA. Such procedure minimizes probability of collision between STAs that are backing off due to the same event.

To further improve efficiency of the mechanisms under high-load conditions, a set of rules concerning choosing CW value have been defined. The possible range of CW values must fall into [CW_{min}, CW_{max}] interval and the starting value of CW is CW_{min}. CW is also reset back to this value following successful transmission of a frame or abandonment of its further transmission attempts. With each retransmission attempt of the frame, CW is incremented to its next, higher value following the exponential growth rule ($CW = 2^{retransmission}-1$) until it reaches CW_{max}. Further retransmissions use constant CW value equal to CW_{max}. By default the number of retransmissions is limited to 7, but in many implementation the value may be modified by the user.

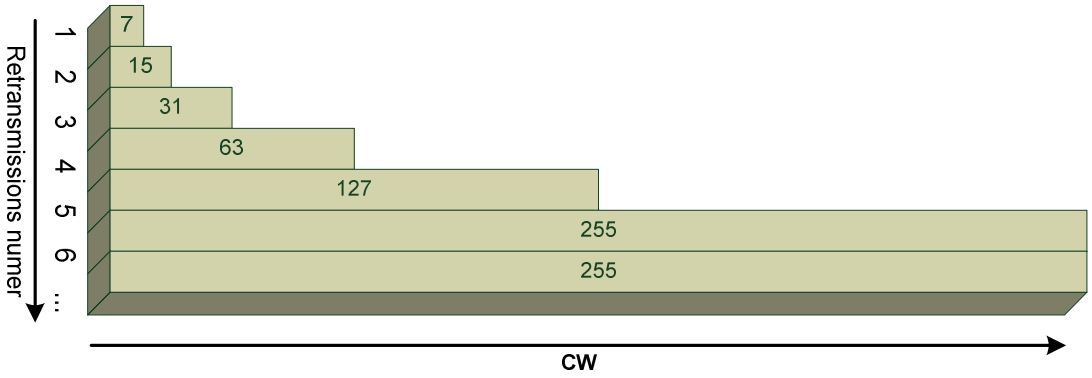

Fig. 15 CW parameter growth with retransmission number

Due to their largely different impact on wireless medium access efficiency under contention rules, short and long frames are threated separately by the mechanism. Short frames are defined as these, whose length is not grater then RTS Threshold parameter (see 2.5.1.2), while longer frames are classified as long. This division is utilized by both backoff and retransmission mechanisms, as each type of frame has its own retransmission counter defined which holds number of retransmissions attempts to date and, by rules described above, current CW value.

2.5.1.5 Frame transmission rules

Due to characteristics of wireless medium and the fact that the transmitter cannot monitor its state during its own transmission, the only means to verify correctness of frame reception is an acknowledgement generated by receiver.
In case of non-QoS BSS and IBSS systems all unicast frames (and their fragments) should be acknowledged by receiver by sending a separate ACK frame to its sender. If the frame (or fragment) is not acknowledged by the time needed to transmit and acknowledge it , the frame transmission is considered failed and retransmission procedures are used.
Group-addressed frames are not acknowledged when being sent to wireless STA. When they are sent to DS they are acknowledged by AP. Group addressed frames cannot be fragmented.
In case of QoS system, delivery service class dictates the method of acknowledgement. In case of QoSNoAck class no unicast frames are acknowledged. In case of QoSAck class unicast frames must be acknowledged and while the frame-by-frame (and fragment-by fragment) method of non-QoS system can be employed, there is also the Block Acknowledgement option.

When a frame to be transmitted is larger than a fragmentation threshold parameter of a BSS, the frame must be divided into fragments which are then transmitted as a fragmentation burst.
Each fragment has a complete format of a data frame and all but last have More Fragments field of Frame Control frame header field set, to indicate more fragments of the same frame are following. The first fragment is sent and acknowledged by general rules of a given system, but following are sent after SIFS time disregarding normal medium access procedures (fragmentation burst), which ensures uninterrupted transmission of a whole fragmented frame.

2.5.1.6 Error recovery

In wireless communication the probability of failed transmissions and error states is relatively high and thus error recovery procedures are of critical importance. Moreover, their complication should be kept at minimum, as they are likely to be extensively utilized and should impair efficiency of the system in minimum possible way.

In case of IEEE 802.11 standard it is always the sender or initiator of a given exchange or operation that is responsible for error recovery. It is his responsibility to detect the failed transmissions by observing lack of acknowledgement or other expected protocol response (for example CTS after RTS) in defined time limit.

When the sender detects that a given transmission has failed, it activates recovery procedure and tries to retransmit a failed frame. To limit a number of possible retransmission of a frame, each of them has an associated counter which record a number of transmission attempts made for that frame. When the counter reaches a configurable value the frame is discarded as impossible to successfully transmit to receiver.

It is evident, that necessity of retransmission of short and long frames will create in different effect on medium utilization and access. Due to this fact, IEEE 802.11 standard allows the short (frame lengths up to RTS Threshold) and long frames to be treated differently in terms of maximum number of allowed retransmissions as the parameter controlling this number is defined separately for each of these types.

2.5.2 Point Coordination Function (PCF)

Optional Point Coordination Function (PCF) aims to provide a Contention Free Period (CFP) for an infrastructure BSS, during which medium access is strictly controlled instead of contention-based.

A Point Coordinator (PC) entity located at access point reserves a regularly reoccurring time period by setting NAV in all stations within range (regardless to BSS they belong to). This is done by including appropriate information in Beacon management frames transmitted periodically by all APs.

Within this period the access is controlled exclusively by PC which polls its registered stations, allowing them to transmit a frame. A number of dedicated control frames (CF-Poll, CF-Ack, CF-End) have been defined to support this mode. There is also a number of data frame types which, apart from their data content, carry (piggybacking) CF messages for reasons of performance (see 2.4.5.3).

The exact list of stations to poll is left entirely to PC discretion – there is no standardized method for stations or system's administrator to influence that choice, so it cannot be used as configurable QoS control mechanism.

Despite clear advantages of this optional mode (efficiency of medium utilization) it has been implemented only in insignificant number of devices and thus has no practical utility in real world deployments.

2.5.3 QoS-aware Medium Access

With inclusion of IEEE 802.11e [32] amendment in 802.11-2007 standard a new, QoS aware, access function has been introduces. The function, called Hybrid Coordination Function (HCF) must be present in all QoS STAs and utilizes two distinct access methods:

- Enhanced Distributed Channel Access (EDCA) for contention-based access,
- HCF Controlled Channel Access (HCCA) for contention-free transmissions.

HCF uses term Transmission Opportunity (TXOP) to describe situation, when QoS STA is allowed medium access under HCF rules. A single TXOP can allow STA to transmit a single frame (as it was the case in DCF or PCF) or give STA permission to transmit as many frames as it needs in a given time interval.

Moreover, Admission Control procedures can be used in conjuration with EDCA and HCCA access, allowing stations to describe their traffic requirements and request guaranteed service.

2.5.4 Enhanced Distributed Channel Access (EDCA)

Enhanced Distributed Channel Access is an extension of DCF which provides prioritized access to wireless medium. EDCA medium access mechanisms and procedures are generally the same as in case of DCF access, apart from a number of modifications described below.

Table 3 EDCA Priority classes

Priority	UP	802.1D	AC	Description
Lowest	1	BK	AC_BK	Background
	2	-	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

Each MSDU obtained from higher layers or MMPDU (MAC Management Protocol Data Unit) generated by management entities can be classified as belonging one of 8 different Access Priorities. These are then assigned into 4 Access Classes (AC).
Each access class has its own, independent outgoing frame queue and its own, independent EDCA Function (EDCAF) contending for medium access. Each EDCAF contends for TXOP independently, in a manner similar to DCF but parameter values of CSMA/CA protocol are different depending on Access Class of a particular frame resulting in access priority differentiation. For all practical purposes, one QoS STA operating under EDCA rules can be treated as 4 independent stations. There is however one exception to this rule, as potential collisions between different EDCAFs of a single STA are handled internally (internal collision) and are not observable on physical medium. They also do not cause retransmission counter to be incremented.

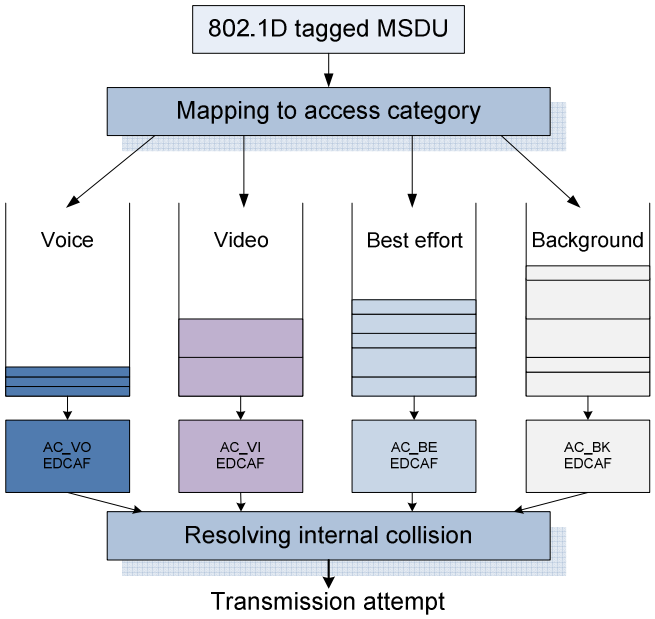

Fig. 16 EDCA medium access functions

Moreover, default parameter values for each AC can be changed and are published in Beacon management frames, Probe responses and (Re)Association frames which ensures their distribution to all STAs belonging to BSS. List of default parameter values for defined ACs is presented in the table below (Table 4).

Table 4 EDCA Class parameters

AC	CW_{min}	CW_{max}	AIFS[AC]	TXOP
AC_BK	aCW_{min}	aCW_{max}	7	0
AC_BE	aCW_{min}	aCW_{max}	3	0
AC_VI	$(aCW_{min}+1)/2-1$	aCW_{min}	2	0; 3.008 ms; 6.016 ms
AC_VO	$(aCW_{min}+1)/4-1$	$(aCW_{min}+1)/2-1$	2	0; 1.504 ms; 3.264 ms

The parameters used to differentiate 4 Access Classes include:

- AIFS[AC] – Arbitration Interframe Space. Time interval used by EDCA in place of DIFS employed by DCF. As can be seen, its value is different for each of AC and this differentiation directly influences the probability of obtaining medium access, especially under low traffic conditions.
- CW_{min}, CW_{max} – EDCA also employs different intervals for choosing CW value depending on AC. This results in shorter backoff times used for transmission of high priority frames.
- TXOP – one of main differences between EDCA and DCF is the former ability to obtain medium access for transmission of more than one frame at a time. TXOP parameter describes the time interval for which STA obtains medium access or indicated that only one frame can be transmitted (TXOP value 0).

It is easy to observe that parameters not only ensure differentiation of priority in obtaining medium access for frames in 4 supported classes, but also take into account requirements of services expected to use each class:

- Background (AC_BG) – the lowest possible priority, with initial medium sensing time about 3.5 times longer than DIFS. Intended for carrying traffic without influencing network's ability to handle higher priority data.
- Best Effort Classes (AC_BE) – standard data transmission priority, comparable to DCF service level, however with slightly smaller access priority due to AIFS[AC_BE] being a bit longer than DIFS. Appropriate for non-time sensitive traffic.
- Voice Class (AC_VO) – highest probability of obtaining TXOP, but for relatively short time. Such parameters correspond to requirements of real-time, interactive VoIP traffic, which requires small delay and jitter but also small bandwidth.
- Video Class (AC_VI) – probability of obtaining TXOP is lower than in case of VO Class, but TXOP interval is longer. This corresponds to requirements of non-interactive video streaming, in which case low delay and jitter are preferred but not strictly necessary, while high bandwidth in undeniable necessity.

If higher layers do not specify the desired Access Priority for a given MSDU it is handled by AC_BE class. Management frames however, are treated as priority traffic by assigning them to AC_VO, well suited for rapid transmission of small messages.

The extensions described above result in necessity to modify a number of dependent mechanisms. Most of the modifications are self-explanatory, such as consistent usage of specific AIFS[AC] in place of DIFS including EIFS interval calculation, AC dependent CW interval selection, etc. However, a number of differences originate from including completely new procedures or functionalities or correct deficiencies of the original medium access method. Some of the most important examples are discussed below.

2.5.4.1 *Virtual CS support changes*

The new ability to transmit many frames after receiving medium access in a form of non-zero time TXOP required small changes in NAV support. If TXOP length is zero, the classic DCF method is used. However, when TXOP is non-zero (which allows multiple frame transmissions), the first frame sets

NAV to the end of the current TXOP, reflecting the fact that medium access has been obtained for a given time interval, not for a single frame transmission.
Another slight modification in NAV support requires STAs to set NAV in response to all detected frames, even these which are considered malformed due to failed integrity check. This approach can potentially lead to incorrect NAV assignments, but additional protection of potentially long TXOPs in difficult propagation environments is understandable, given their use in support of real-time services.

Another change introduces NAV Distribution (or CTS-to-self) mechanism. If full RTS/CTS exchange is too costly or not necessary (the hidden terminal effect does not occur) it is often enough to employ simplified solution for distributing NAV information to neighboring stations. This approach consists of sending only a single CTS control frame with receiver address set to a sending station address in place of two-way RTS/CTS exchange. As in case of RTS/CTS mechanism, the starting frame (CTS-to-self frame in that case) can be sent by STA after obtaining access to medium using general DFS rules. After transmission of CTS-to-self frame, the station immediately (after SIFS time, without media state detection) sends the data frame. That way the sending STA retains most advantages of the full RTS/CTS exchange, while considerably shortening the preliminary control frame exchange by eliminating RTS frame. The sending STA still informs its neighboring stations and about upcoming large frame transmission, sets their NAV accordingly and risks only short CTS control frame to possible collision in its vicinity. What the solution lacks is protection from collisions at receiving STA in presence of hidden stations.

2.5.4.2 Frame acknowledgement policies

As mentioned in Section 2.4.1 IEEE 802.11-2007 standard allows use of different delivery service classes in case of QoS BSS. If QoSNoAck delivery service class is selected, no transmitted frames are acknowledged. If QoSAck class is in effect, there are a number of acknowledgement policies which can be used.
The default polity is the same as in case of DCF – each unicast data or management frame must be acknowledged by ACK control frame for the transmission to be considered successful.
If is, however, possible to utilize one of Block Ack modes, which allow receiving station to acknowledge a group of frames with a single control frame. Such solution raises system performance significantly, as the sending station can transmit a number of frames without waiting for acknowledgement and the receiver STA does not need to send nearly as much ACK control frames.
There are two block acknowledgement policies defined by the standard:

- Immediate Block Ack – appropriate for low-latency, high-bandwidth transmissions,
- Delayed Block Ack – suitable for moderate-latency traffic. Cost-effective solution, possible to implement on legacy (IEEE 802.11-1999) hardware.

Both of the above policies allow STA that receives a TXOP to transmit a number of frames (within TXOP limit) separated by SIFS intervals, without waiting for acknowledgements. To utilize one of these policies, their use must be negotiated between communication stations, with use of ADDBA Request / Response management frames. The above exchange allows for parameter negotiation (for example maximum number of frames to be transmitted before acknowledgement is necessary) and specifies the first MSDU to be transmitted with the negotiated acknowledgement rules in effect.
After the initial negotiation is successfully completed, the block transmission can be used. As mentioned before the sending station obtains TXOP and within it transmits a number of frames separated by SIFS time (a Data Block). It is advisable that the sending STA would use some kind of NAV setting procedure to protect such transmission (RTS/CTS, CTS-to-Self).

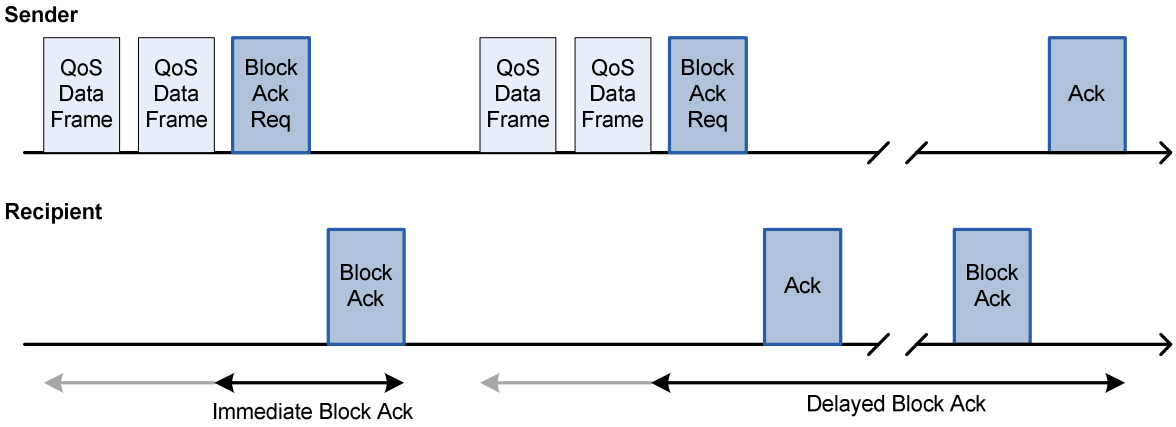

Fig. 17 Block Ackowledgement procedure.

The sending STA ends the Data Block with Block Ack Request control frame. The response of receiving STA differs depending on the specific Block Ack policy used.
In case of Immediate Block Ack, the receiving station immediately (after SIFS) responds with Block Ack frame, containing sequence number of the first frame to be described by a bitmap field which uses individual bits to indicate which frames were successfully received.
In case of Delayed Block Ack, the receiving station acknowledges the Block Ack Request using a standard Ack frame and subsequently tries to obtain its own TXOP to transmit Block Ack frame constructed in already described fashion. Its reception by initially sending station must, in turn, be acknowledged with the Ack frame.

2.5.4.3 Direct Link Setup (DLS)

One of the most prominent characteristics of IEEE 802.11-based BSS (infrastructure) is a necessity to relay all transmissions between wireless STAs through an AP. Such requirement is the result of the data handling process in IEEE 802.11 infrastructure network, where it is a DS Distribution Service (see 2.3.1.1) which is responsible for proper traffic directing both between different and inside a given BSS. It is also possible that at the moment when sending STA obtains medium access and starts transmitting, a destination STA would be inactive due to use of power saving mode, thus missing the transmission. Relaying through AP solves both of these problems, as DS Distribution Service is located at AP and AP can also bring any station out of power saving mode to complete the transmission. Moreover AP is able to buffer any data intended for inactive stations for later delivery.
Such approach however is rather costly in terms of archived throughput, as it reduces it by over 50% due to double transmission (STA-AP-STA) and the fact that in case of multi frame transfers they compete for medium access.
In this situation, to prevent retransmission through AP while also avoiding the problems described above, a Direct Link Setup procedure has been introduced in IEEE 802.11e [32] amendment. It allows two STAs in BSS to communicate directly, while keeping AP informed of the fact.

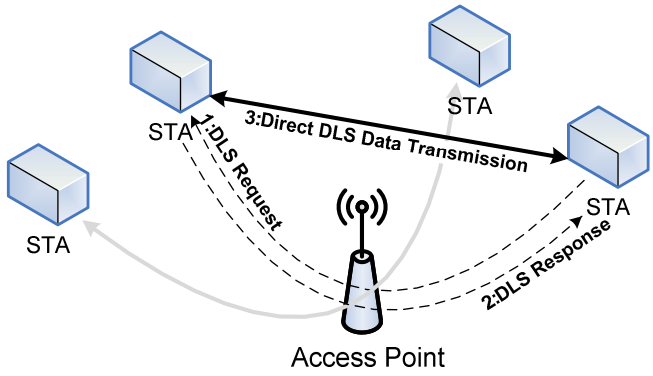

Fig. 18 Direct Link Protocol.

The involved stations exchange DLS Request / Response management messages in classic manner, using AP retransmission. This exchange informs AP (and DS Distribution service) of the intended transfer and allows it to bring the destination STA out of power save mode if necessary.
The initial exchange of management frames described above, allows involved stations to choose mutually acceptable physical and MAC layer parameters, such as modulation, data rate etc. If the transmission is to be secured, following Peer Key Handshake procedure allows creation of a direct security association between STAs.
After these procedures the direct transmission between STAs can proceed, but it still requires the use of the standard medium access methods and transmission procedures allowed within a given BSS.
To discontinue direct link activity, STA must inform both corresponding STA and AP by sending DLS Teardown management message. In case of error condition (such as one of the STAs disappearing from BSS), AP can initiate the teardown.
Unfortunately, while the described procedures have been present since IEEE 802.11e [32] specification, it has not been implemented in practice on any large scale. The specification has later been superseded by an optional Tunneled Direct Link Setup (TDLS) mechanism introduced in IEEE 802.11-2012 [37] revision of the standard. However, this version of the described mechanisms is also practically impossible to be found in Off-the-Shelf hardware.

2.5.5 HCF Controlled Channel Access (HCCA)

HCF Controlled Channel Access is the controlled medium access mode, similar to PCF, introduced as a part of HCF. The basic approach remains the same – there are periods of time, called Controlled Access Phases (CAPs) during which a centralized entity controls access to medium and polls STAs to allow them to transmit their data.
In case of PCF, such time intervals were called Contention Free Periods (CFPs, Fig. 19) and could be invoked for a specified time by Point Coordinator following a beacon frame (see 2.5.2). In contrast HCCA allows CAP to begin at any time. The controlling entity, called Hybrid Coordinator (HC), seizes the medium after PIFS time which gives it priority before any EDCA transmissions.

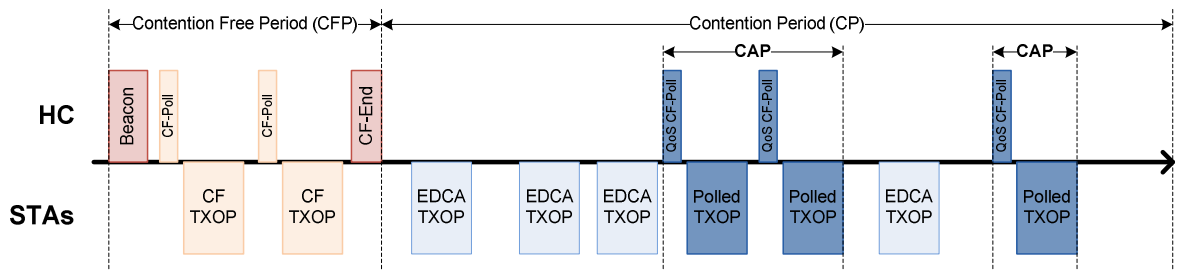

Fig. 19 HCCA medium access

The HC then polls selected STAs by sending QoS CF-Poll control frames, which grant a given station TXOP to send their data or management frames. STAs are required to respond after SIFS or their TXOP will be forfeit after PIFS and next QoS CF-Poll will be sent to maintain medium control by HC. If STA does not have frames to send it should respond to poll by sending Null Data frame.
The NAV is set by HC by sending appropriate information in QoS CF-Poll frames. Each poll sets NAV to cover TXOP interval assigned to a polled STA. Other STAs are of course required to observe the NAV and refrain from attempts to gain medium access, but they also should provide standard responses required from them as a part of control exchanges – acknowledging data / management frames, responding to RTS etc.
To provide HC with better knowledge of STA traffic requirements, STAs include their outgoing queue size in data frames send in response to poll. They can also forfeit their remaining TXOP time, by setting NAV to cover only the current frame plus time necessary for its acknowledgement instead of setting it for the end of granted TXOP interval, as they are required to do otherwise.
HC is responsible for ending the CAP, by sending QoS CF-Poll with Duration field = 0 to himself or CF-End – both of these frames end CAP and clear the NAV. If it fails to do so, the medium can be used again according to EDCA rules after AIFS[AC] time following end of NAV set by last poll.

As can be seen from the above description HC retains a complete medium control during CAP and is responsible for assigning TXOPs to stations. If Admission Control procedures (see below – 2.5.6) are used in BSS, HC can use thus obtained information about STA traffic requirements. If Admission Control is not used, STAs can request polling by appropriately setting information about their outgoing queue length (Queue Size field) or desired TXOP time (TXOP Duration Request field) in header of their outgoing QoS Data frames.

It should be noted, that both PCF and HCCA can be used at the same BSS, so both CFP and CAP periods may be present.

2.5.6 HCF Admission Control

Quality of service extensions initially described in IEEE 802.11e and later incorporated in base IEEE 802.11-2007 standard include Admission Control (AdC) support for QoS-aware medium access functions – EDCA and HCF. Their presence allows enforcement of resource management policy in wireless BSS, which in turn results in superior efficiency of QoS support and even ability to provide QoS guarantees for wireless traffic.

A centralized control entity is required to provide AdC and it is Hybrid Coordinator located at AP which is employed for this task. Due to this fact, only infrastructure BSS networks support AdC functionality.
Admission Control mechanisms can be used in both EDCA and HCCA environments, but only with combination with the latter it is possible to provide QoS guarantees, while in the former case AdC-gathered information is used to optimize traffic prioritization.

If AdC procedures are in effect, each STA must provide description of Traffic Streams (TS) it is going to transmit and their QoS requirements. It is done by sending ADDTS Request management frame, containing Traffic Specification (TSPEC) information element. Not all TSPEC field values need to be specified – the mandatory set depends on medium access type (EDCA or HCCA). Moreover, some parameters are optional – if they are not specified, HC is free to choose their values according to its resource management mechanisms.
Based on this information a given TS can be granted access or rejected by HC, which informs the STA on its decision by sending ADDTS Response management frame. ADDTS Response can also contain configuration parameters for the STA to use in its activities. If access is granted, information obtained

during ADDTS exchange is then used by medium access procedures to satisfy QoS requirements of a given TS.

2.5.6.1 EDCA Admission Control

In case of EDCA, any of ACs can be marked as requiring AdC which is than reflected in Beacon, Probe Response and (Re)Association Response management frames. However, if a given AC requires AdC, so should all higher ACs. It is a necessary precaution which prevents a higher priority classes from uncontrollably seizing resources allocated by lower priority AdC-enabled class.
If a connecting STA does not support AdC mechanisms or its request for access is rejected by AdC procedures it should attempt to gain access using lower priority AC.
When AdC decides (based on available resources) that a given TS can be admitted into an indicated AC, a Medium Time parameter is calculated by HC and the STA is informed of its value. Medium Time parameter describes an amount of time for which a given TS can have medium access during a given time interval (which can be understood as a contract conformance checking interval). The transmission of TS associated traffic is then handled according to EDCA rules, with a given AC access parameters, but if TS exceeds specified Medium Time, it cannot obtain medium access in a given AC during current interval. It can, however, temporarily use lower AC (which does not require AdC) to transmit the surplus traffic.
This mechanism prevents TS from exceeding a network resource consumption declared during its creation and is a basis for network resource management in EDCA environment.

2.5.6.2 HCCA Admission Control

If AdC procedures apply to HCCA access, STA must provide description of its intended traffic streams before it is allowed to send data during CAP. If a TS is accepted by HC, it is responsible for providing TXOPs necessary to fulfill QoS requirements specified for a given TS during ADDTS exchange. Already accepted TS must not be changed or dropped by HC until it is released by requesting STA, barring error conditions such as loss of communication with its owner.
HC scheduler takes into account parameters describing TS traffic characteristics specified by STA during its creation, current information about traffic conditions gathered by itself and obtained from STAs (such as their queue lengths) and physical transmission capabilities (available data rates).
HC publishes the intended polling schedule using Schedule information element in dedicated Schedule management frames. To offload some of the scheduling tasks, HC can provide aggregated TXOPs for a STA instead of providing TXOP specifically for each TS. Such aggregation forces STA to make scheduling decisions concerning TXOP allocation for its particular traffic streams, but it significantly lowers HC computational requirements and offers STA an additional flexibility in utilizing its assigned TXOPs.

2.5.7 Efficiency of IEEE 802.11-2007 mechanisms in handling of QoS traffic

As the IEEE 802.11s specification relies on many of IEEE 802.11-2007 transmission mechanisms and because the main topic of this thesis requires a comparison between PtMP and mesh IEEE 802.11 network deployments, the following chapter provides an overview of PtMP efficiency in handling of a few selected types of network traffic. Its results will later be compared with an IEEE 802.11s-based communication system's efficiency in comparative conditions (3.8.4), to indicate both advantages and limitations of the discussed mesh technology. This comparison will also provide a basis on which the need for proposed, cross-layer optimizations are going to be argued and their efficiency evaluated (4.1.4, 4.2.3, 5.1.4, 6.1.3 and 6.2.5).

Taking into account a fact that only a subset of the IEEE 802.11-2007 standard's functionality is commonly implemented in the Off-the-Shelf (OTS) hardware, it has been decided to concentrate the following simulation assessment of WiFi traffic handling performance on configurations and the feature sets which can realistically be expected to be used in practical deployments.
The most important difference between the described IEEE 802.11-2007 mechanisms and the functionality we can expect to use in a real system is the result of a partial implementation of IEEE 802.11e QoS-related functions. As the IEEE 802.11e standard amendment defines a significant number of new mechanisms, many of which can be considered complex and work-consuming in implementation, a separate specification named Wireless Multimedia Extensions (WME) or WiFi Multimedia (WMM) has been prepared. The WME specification contains only a selected set of IEEE 802.11e mechanisms, which reduces the specification document size from over 300 pages to about 30.
The WME includes basic EDCA mechanisms (including traffic prioritization and block acknowledgements) and a number of advanced power saving functions. The HCCA controlled access and Traffic Streams are omitted entirely and Direct Link Setup has been added a few years later as an additional, optional specification under a name of Tunneled Direct Link Setup (TDLS).

In such situation, the experiments described below exclude the unimplemented HCCA mechanisms to concentrate on widely used EDCA medium access method with its four traffic classes. They have been performed exclusively in the infrastructure mode (point-to-multipoint), leaving out the extremally rarely used and poorly implemented ad-hoc mode.

2.5.7.1 Simulation environment

All experiments have been performed in OMNeT++ 4.6 environment, while the simulation models used in modelling of presented scenarios have been developed expanding the ones provided by INETMANET 2.2 library.
All IEEE 802.11 access points and stations are equipped with a single IEEE 802.11a interface each, which provides a maximum transmission rate of 54 Mb/s in the 5 GHz ISM band. Due to the nature of the mechanisms proposed in this dissertation (as described in chapters 4-6, network management instead of the transmission itself), the results obtained for IEEE 802.11a transmission technology will retain their correctness also for more advanced specifications such as IEEE 802.11n [38] or IEEE 802.11ac [5].
The propagation model used is the Nakagami model [39]. It has been chosen as much more appropriate for multipath environment with Rayleigh fading than the popular Free Space model [40]. The alternatives taken into consideration were Rayleigh [41] and Ricean [42] models – however the chosen model should provide the closest match for real communication conditions in expected IEEE 802.11s wireless mesh deployment scenarios (see 3.1.1), such as office building interiors or ad-hoc concentrations of wearable devices in diverse metropolitan area conditions. The m parameter of Nakagami model has been set to the value of 3, based on a series of experimental measurements in the abovementioned environments.
All simulation scenarios presented in this dissertation have been repeated multiple times (precise values are indicated in their specific descriptions) with different random seeds, to obtain 95% confidence intervals (included in figures) small enough to indicate statistically meaningful results.

The first experiment illustrates IEEE 802.11 PtMP architecture performance in handling of three basic types of traffic as defined by (unfortunately no longer developed) IEEE 802.11T draft specification [43], intended to provide a standardized methods of wireless performance prediction: Voice over IP (VoIP), video streaming and data traffic. Specific parameters of VoIP and video transmissions have been selected taking into their popularity in real-world systems, and feasibility of their use in an IEEE 802.11a wireless network environment.

For the VoIP traffic, a G.711 PLC [44] codec has been chosen, due to its popularity, good voice quality and relatively high resilience to packet loss. The Packet Loss Concealment (PLC) [45] provides it with limited capability of reconstructing missing voice packets by extrapolating from previous ones. The codec generates a constant bitrate (CBR) 64 kbit/s data stream, using 40 B packets sent with 20 ms interval.

Video streaming has been performed using H.264 codec [46], generating a variable bitrate (VBR) data stream with maximum required throughput of 2 Mbit/s, which is sufficient to support a wide-screen 480p motion picture (resolution of 848x480). The transmission utilizes 188-byte data packets, forming a Packetized Elementary Stream (PES), which are carried in IP packets – each IP packet contains 7 PES packets resulting in IP packet size of 1316 B (not including headers). As in this instance we are considering a non-interactive video service, the receiving buffer size has been set to accommodate 5 seconds of maximum bitrate transmission.

Data transmission experiments have been intended to determine a maximum throughput possible in a given scenario, and for this purpose a inelastic UDP stream with bitrate exceeding maximum theoretical throughput of the IEEE 802.11a interface has been employed. In this case the size of UDP packets is equal to 1470 B.

2.5.7.2 Experiments in IEEE 802.11 PtMP network with no background traffic

While the assessment conducted in a network system carrying only the single traffic stream which is not exceeding its capacity is generally of limited utility, however it allows us to determine the communication technology's basic capabilities and establish a set of reference results. This will allow us to better interpret the subsequent results obtained for different traffic load levels.

The network setup reflects a common scenario with a wireless STA connected to an IEEE 802.11 access point (AP) and communicating with a remote host located in wired network or a second wireless STA located within its reliable communication range. The distance between these two stations has been selected to be 40 m based on results of STA to infrastructure transmission experiments described below.

In such system, a series of measurements of transmission delay, packet loss and Mean Opinion Score (MOS) parameters have been performed for different EDCA traffic classes (AC_BK – Background, AC_BE – Best effort, AC_VI – Video, AC_VO – Voice) and distance between the access point and its associated STA increasing from 0 m to 200 m. Simulation for each EDCA class / distance combination have been repeated 50 times with different random seeds, which proved to be enough to obtain 95% confidence intervals small enough (under stable network conditions) to indicate meaningful results. Each simulation scenario covered 60 seconds of simulated time.

Mean Opinion Score values for VoIP communication have been calculated in accordance with ITU-T G.107 specification, often called E-model [47]. Parameters of E-model have been selected to match the WLAN environment and the codec employed, based on values provided in ITU Study Group 12 documents [48] and ITU-T G.113 recommendation [49]:

- Equipment impairment factor (I_e) = 0
- Packet-loss robustness factor (B_{pl}) = 34
- Advantage factor (A) = 8

While the E-model method of objective assessment of QoE is a well-established one, it is intended sorely for audio transmissions. With the necessity to obtain a similar indicator of QoE level for the

described non-interactive video streaming service, a conducted literature study [50-59] allowed to us to accept the solution described in [60] as the method utilized to assess the video MOS values based on IP packet loss level, under condition, that receive side buffering is enough to prevent loss of quality due to an excessive transmission delay. In case of a non-interactive video streaming service such a condition is relatively easy to fulfill and as a result all video-related experiments have been conducted with a 5 s receive buffering.

When interpreting the results presented below, we should keep in mind that IP transmission delay values have been calculated only for IP packet which were successfully delivered, so a steep raise of a mean IP packet loss percentage can actually result in a reduced mean IP transmission delay, which should not be interpreted as improvement of transmission quality.
Additionally, we should remember, that all values presented below are calculated for the amount of time which a given STA stays connected to AP, which in good conditions is the whole time of a simulation scenario (60 s). However, in poor propagation conditions a STA can disconnect from AP before the end of the simulation, due to a loss of 3 consecutive Beacon frames. In such situation, the statistics are calculated for the limited time it has been connected, often resulting in falsely optimistic results, so caution is advices in interpreting results for extreme ranges.

VoIP STA to infrastructure transmission

The first experiment illustrate a 60 s VoIP transmission using a G.711 PLC codec as described above. The resulting 64 kbit/s data stream has been transmitted to AP using different EDCA traffic classes.

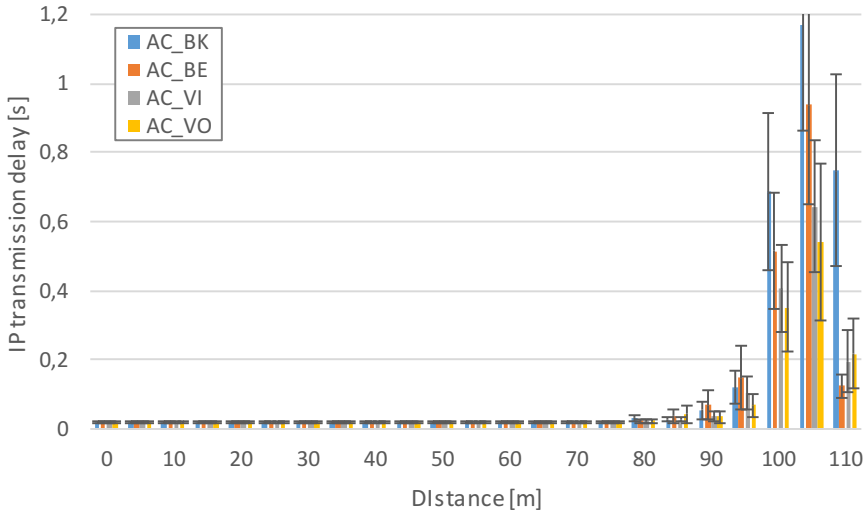

Fig. 20 IP transmission delay as a function of a distance from an AP for a STA to infrastructure VoIP transmission in an unloaded network

It can be seen, that IP transmission delay in unloaded IEEE 802.11 PtMP network does not normally exceed 0,02 s. Only when the distance between communicating devices approaches the limit of effective communication range, the transmission delay will sharply increase due to necessity of retransmitting lost or erroneously received data frames and filling up sending queues. Confidence intervals for distances over 95 m indicate severe instability of network operation and at these ranges it should be considered unfit to support a VoIP transmissions because of both the high delay and the mentioned lack of stability.
It can also be observed, that in case where there is no background traffic to contend for medium access with our observed traffic stream, in good communication conditions (under 90 m) the delay values offered by different EDCA traffic classes are almost identical. However, in difficult communication conditions Voice and Video traffic classes will provide smaller delays – an effect which can easily be explained with their shorter AIFS times.

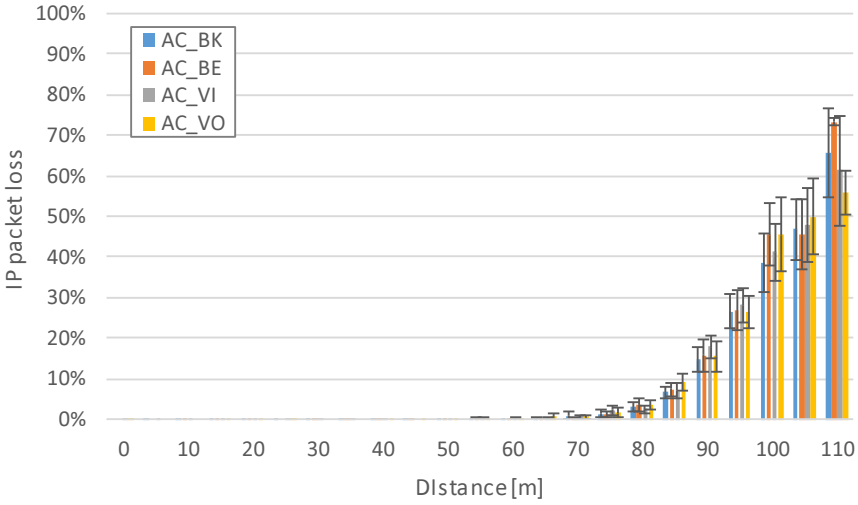

Fig. 21 IP packet loss as a function of a distance from an AP for a STA to infrastructure VoIP transmission in an unloaded network

The IP packet loss results for the scenario can be expected, based on the above transmission delay results. For ranges of up to 70 m packet loss remains under 1% (which can be interpreted as good traffic conditions for a WLAN network) and for longer ranges raises abruptly as the number of allowed retransmissions for a single wireless frame ceases to be sufficient for its delivery. At a range of up to 85 m, VoIP communication can still be expected to be of good quality, and for ranges of up to 95 m, where packet loss remains under 30%, it can be considered feasible. Over that range, with packet loss of 40-75% the network is unable to provide transmission capability necessary for a quality VoIP communication.

Analyzing both transmission delay and IP packet loss figures, the fact that at ranges of 100-110 m network's management protocols still maintain the link despite its unstable operation is an alarming observation. Commonly, implementations of IEEE 802.11 STA will not initiate a network discovery to find an AP providing a better service level until such a STA has been disconnected from its current AP. As a result, a STA remaining connecting to an AP and then increasing its distance from AP will be locked to it despite drastically low QoS and possible presence of other APs able to provide a better service level.

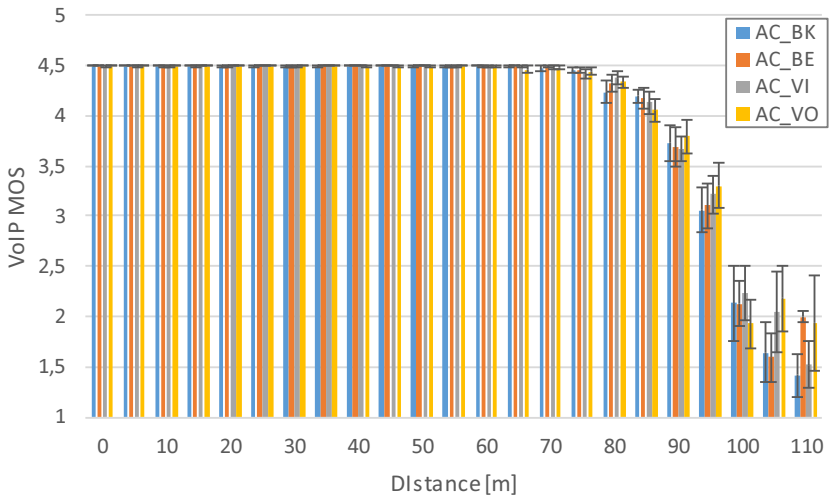

Fig. 22 VoIP MOS as a function of a distance from an AP for a STA to infrastructure VoIP transmission in an unloaded network

The results of MOS assessment are not surprising considering delay and packet loss analysis presented above – for ranges of up to 75 m, where both of these parameters remain at low values, all EDCA classes are able to provide as good VoIP communication quality as can be expected with the employed coded (4.5).
At 80 m, where packet loss percentage begins to raise, there is a sharp fall of MOS value for all classes. Above this range, with both packet loss and transmission delay parameters raising, all traffic classes provide similar MOS level (as there is no background traffic to contend with VoIP transmission), with a slight advantage of high priority (AC_VO/AC_VI) classes. Over 95 m, MOS values being less than 2 for all classes, VoIP transmission should be considered infeasible.

Having analyzed the scenario where VoIP transmission is conducted between wireless STA and host located in wired infrastructure in absence of external interference and background traffic, we were able to determine a range of 70 m as a maximum which does not adversely impact the quality of VoIP communication and a range of 95 m as a maximum which can be expected to provide propagation conditions sufficient to maintain a fair quality VoIP communication. The above values, dependent on the quality of the simulated hardware, chosen propagation model and its parameters and general capabilities of IEEE 802.11 medium access and transmission mechanisms, will be used in future experiments as reference ranges in construction of various network.

VoIP STA to STA transmission

Taking result of the above experiment into account, a second experiment have been conducted, where VoIP transmission is maintained between two wireless STAs located at a given distance from the AP and within a high-quality communication range from each other (60 m), based on results of the previous experiment.

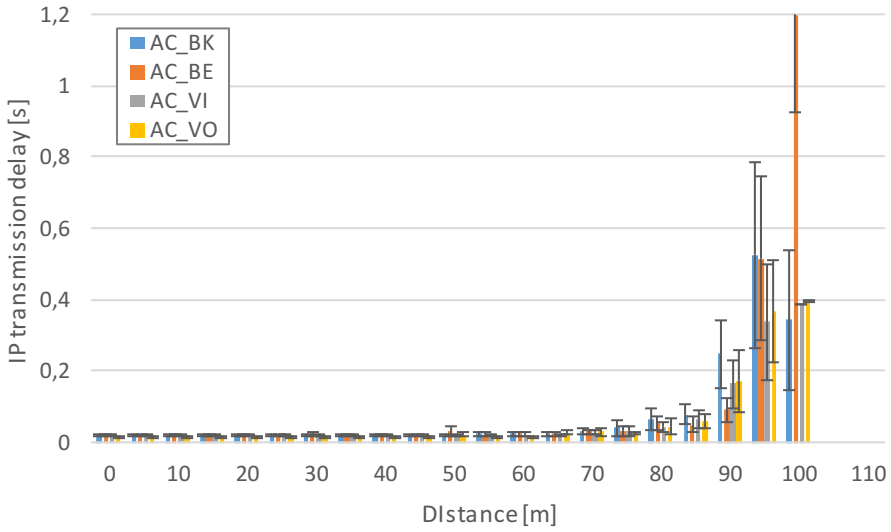

Fig. 23 IP transmission delay as a function of a distance from an AP for STA-STA VoIP transmission in an unloaded network

As the STA-STA communication in the infrastructure mode can be interpreted as 2-hop transmission with AP serving as a forwarding device, we could expect the transmission delay to be at least double of that from the previous (STA to infrastructure) scenario – however it is not the case as for ranges of up to 70 meters the mean value of delay for all traffic classes is about 0,034 s while in the previous case it slightly exceeded 0,02 s. Such effect can be explained by only a fraction of the recorded IP transmission delay being a direct result of wireless medium access and transmission delay. Such

component must indeed at least double compared to the previous scenario, as now the complete transmission path requires two wireless transmissions. Moreover, they are likely to interfere with each other resulting in effect similar to intra-path interference effect (further described in 3.1.1) however small in this case, due to low throughput of the transmit stream involved.
Due to the already mentioned fact, that the communication now requires two wireless transmissions conducted at the indicated range, first indications of raising transmission delay can be observed at a range of 50-60 m instead of 70-80 m. The following growth of transmission delay and degradation of transmission stability is also observed earlier, as at the range of 90 m we are already over the suggested 150 ms delay limit of a quality VoIP communication. The wireless link cannot be maintained over the range of a 100 m.

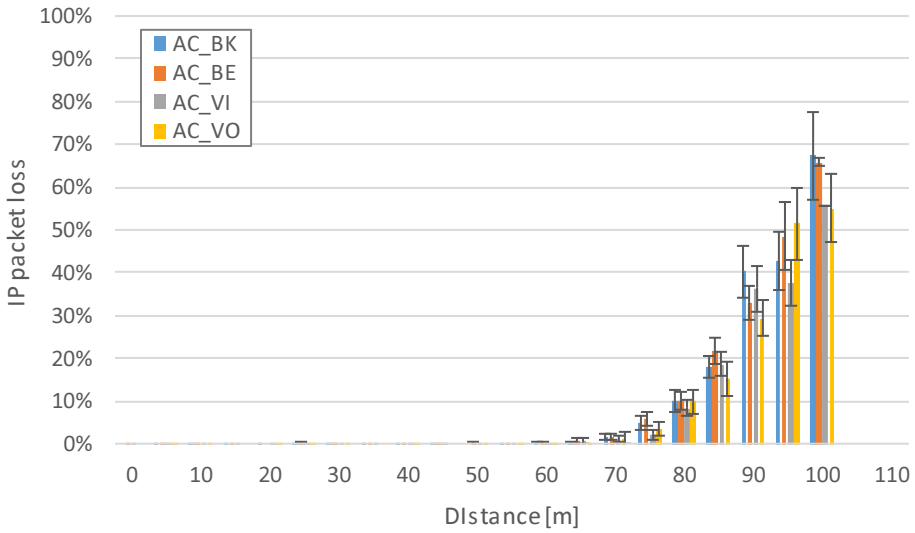

Fig. 24 IP packet loss as a function of distance from an AP for a STA-STA VoIP transmission in an unloaded network

The IP packet loss results follow similar patter as in case of the previous scenario, however Background and Best effort traffic classes start to show a noticeably higher packet loss values then high priority traffic classes until range of 95 m, where all classes reach packet loss of over 45% and width of confidence interval starts to indicate an unstable network conditions. This effect can be attributed to the 2-hop transmission and can be expected to be much more pronounced with a higher throughput of a video transmission or in presence of a background traffic.

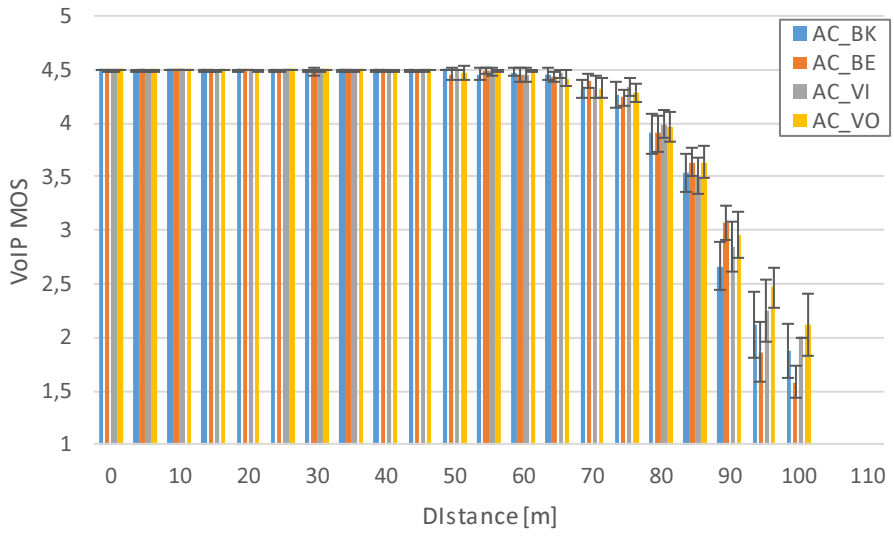

Fig. 25 VoIP MOS as a function of distance from an AP for a STA-STA VoIP transmission in an unloaded network

In this scenario, the presence of 2 wireless hops on the transmission path and some amount of intra-path interference, causes Voice and Video traffic classes to slightly outperform others. Until the range of 80 m, where packet loss raises over 5% and begins to increase quickly, both of them show a good MOS values of at least 4.0. Traffic classes of lesser priority consistently provide a slightly smaller MOS values. In overall, VoIP communication quality is very similar to the case of a single-hop wireless transmission shown in the previous scenario, with but first signs of MOS degradation are observable in 20 m shorter range (50 instead of 70 m) and it is much faster over 80 m range.
The maximum range at which the communication is still possible is reduced from a 110 m observed in 1-hop STA to infrastructure scenario to a 100 m.

Video STA to infrastructure streaming

Video streaming experiments follow the same pattern as VoIP experiments described above. In the first scenario a single STA connected to an AP performs a transmission of non-interactive video content to a host located in an infrastructure network behind the AP. The resulting H.264 VBR stream has maximum throughput of 2 Mbit/s and utilizes IP packets with a data field of 1316 B, as already described. The receiver allocates a receiving buffer sufficient to hold 5 seconds of transmission.
During the experiment such transmission is successively conducted with use of each of EDCA traffic classes and for different distances between transmitting STA and the AP it is associated to. The results shown below include IP transmission delay, IP packet loss and Video MOS of the described transmission.

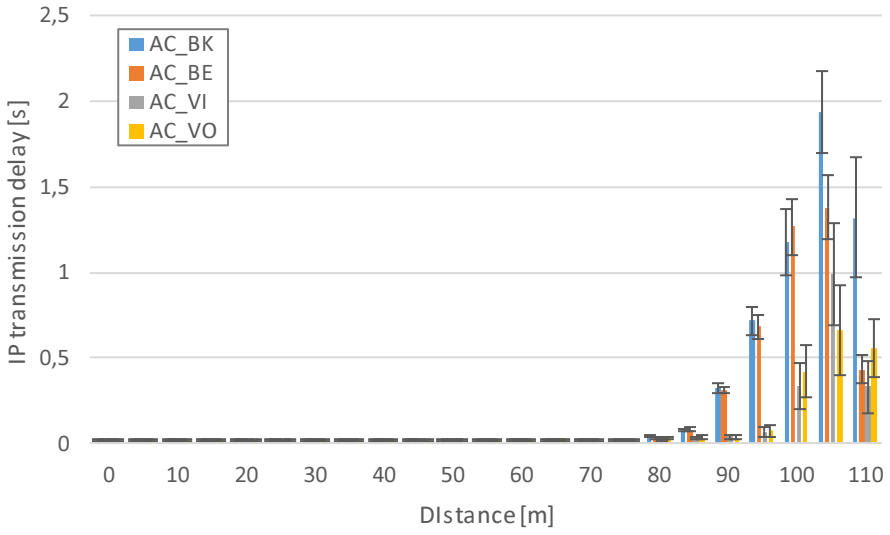

Fig. 26 IP transmission delay as a function of a distance from an AP for a STA to infrastructure video transmission in an unloaded network

As shown in Fig. 26, the IP transmission delay retains the same type of dependency from the range between an AP and its associated STA as in case of VoIP transmission described above. However, due to a much higher throughput of the video transmission, in case of Background and Best effort traffic classes the growth of IP transmission delay is much more pronounced than in case of low throughput VoIP stream. It can be observed, that in their case the delay is raising noticeably starting from the distance of 85-90 m and at 105 m is between 1-2 s.
At the same time, Video and Voice traffic classes do not show this effect and retain delay values similar to these of VoIP transmission. At a 100 m their delay it begins to raise noticeably, however the width of confidence intervals at this range indicate that we should consider the conditions of the network transmission to be highly unstable.

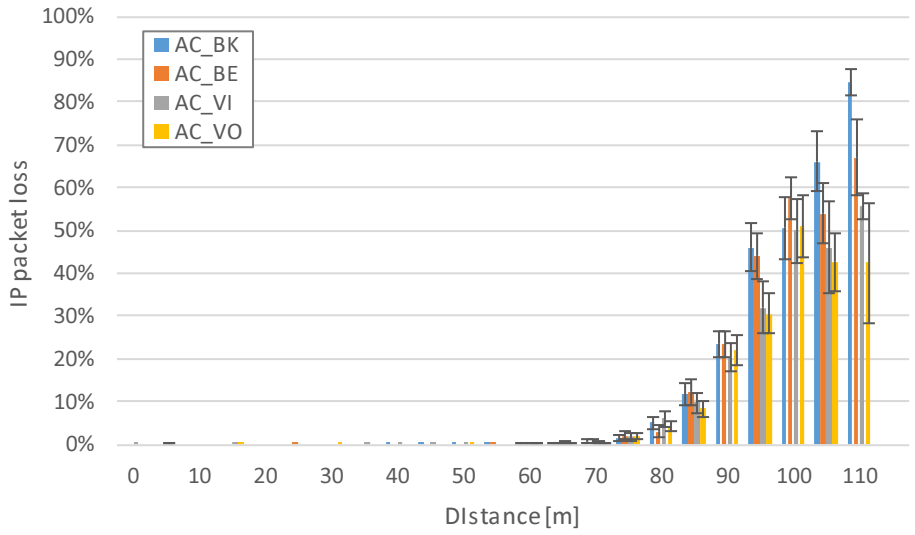

Fig. 27 IP packet loss as a function of distance from an AP for a STA to infrastructure video transmission in an unloaded network

In case of non-interactive video transmission, an IP packet loss level tends to be significantly more important than a packet transmission delay, as the use of receive buffer will prevent playback degradation due to, even a very considerable (in our case 5 s), transmission delay. However, as in this scenario both transmission delay and packet loss is caused by difficult propagation conditions causing a need for an excessive number of retransmissions or even exceeding retransmission limits and losing the packet, it is logical that at a range where the IP transmission delay raises sharply, the same can be expected of IP packet loss. Obtained results confirm this effect, as IP packet loss shows a quick growth at a range over 80 m, similarly to the growth of the IP transmission delay.
When we compare the IP above packet loss characteristics, with the experiment showing a maximum UDP throughput for a particular range presented in further part of this Section (Fig. 32), we notice that for AC_BK and AC_BE, over the range of 85 m the maximum throughput of the transmission drops below the required 2 Mbit/s, which we can observe in Fig. 27 as a rapid growth of IP packet loss percentage. The same effect is observable for AC_VI and AC_VO starting from the range of 90 m.

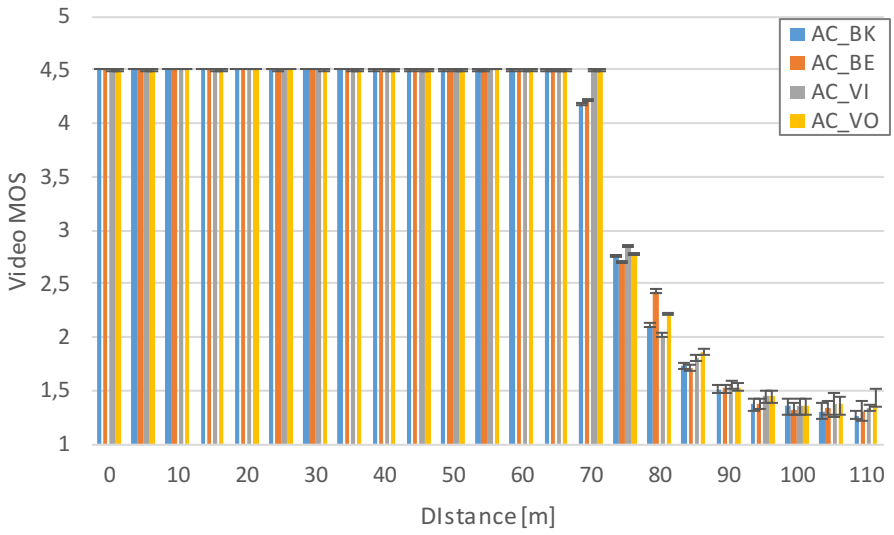

Fig. 28 **Non-interactive video streaming MOS as a function of distance from an AP for a STA to infrastructure VoIP transmission in an unloaded network**

With 5 s receiving buffer, MOS values for the video transmission are mainly influenced by packet loss, instead of transmission delay of IP packets which have been successfully received by its destination. In accordance with this observation, the MOS remains high for all traffic classes for ranges below 70 m, as in that range they encounter virtually no IP packet loss. In case of longer ranges, MOS values drop quickly with raising IP packet loss percentage – a loss of 5 % being sufficient to lower MOS value below 2. With no retransmission at AP or a presence of background traffic, the traffic class used proves to be of limited importance.
The maximum range of a high quality video streaming shows to be 70 m, which is with accordance with results obtained for VoIP communication in the earlier experiment. At ranges over 85 m, the video service should be considered unfit for use, which happens 10 m earlier than in case of a low throughput VoIP transmission.

Video STA to STA streaming

The second experiment repeats the same general scenario, but this time video transmission is conducted between two wireless STAs associated with the same AP, located in mutual communication range at a distance of 60 m. As already described in relation with VoIP experiments, such setup can be seen as a 2-hop transmission with AP serving as a transit station, and the traffic stream competing for medium access with itself due to its retransmission at AP in a manner similar to an intra-path interference effect well known in single-channel multihop wireless networks.

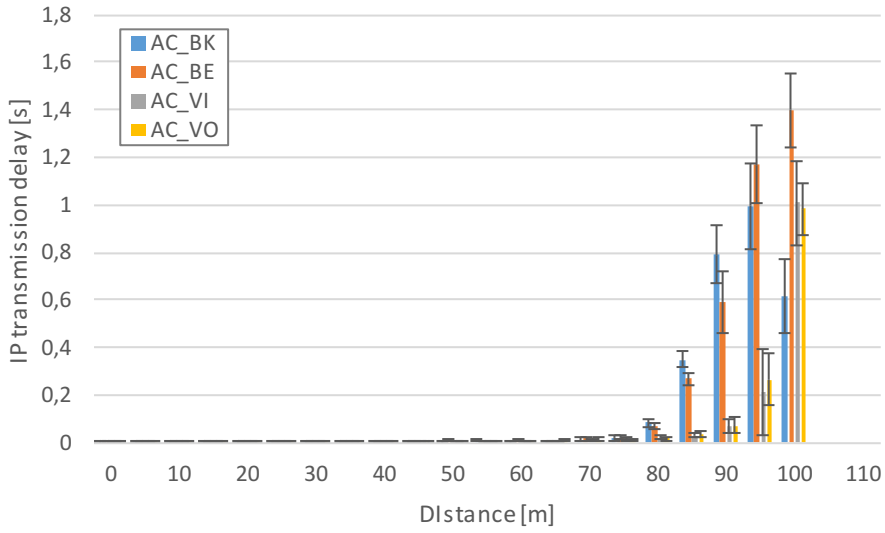

Fig. 29 IP transmission delay as a function of a distance from an AP for STA-STA video transmission in an unloaded network

In case of STA-STA video transmission, we can notice all the effects already observed in case of STA to infrastructure scenario presented above. Additionally, difficult propagation conditions observable at longer ranges will impact the transmission twice, as despite the fact that both stations are located within easy communication range (0 m) from each other, they need to communicate through the AP. With a much higher throughput than a VoIP transmission, the competition for medium access at both sending STA and retransmitting AP is causing low priority traffic classes (AC_BK and AC_BE) to provide a significantly degraded service at a range 85 m and greater, especially compared to high priority classes (which show significant degradation only at the maximum archivable range of communication).
The transmission queue growth and overflow due to the maximum transmission bandwidth of a STA being reduced below the required 2 Mbit/s (see Fig. 33) at longer ranges, will only be is observable at source STA, as the traffic stream arriving at AP is of already reduced throughput. With both

wireless hops (to and from AP) of approximately the same quality, there is no systematic queue growth at AP.

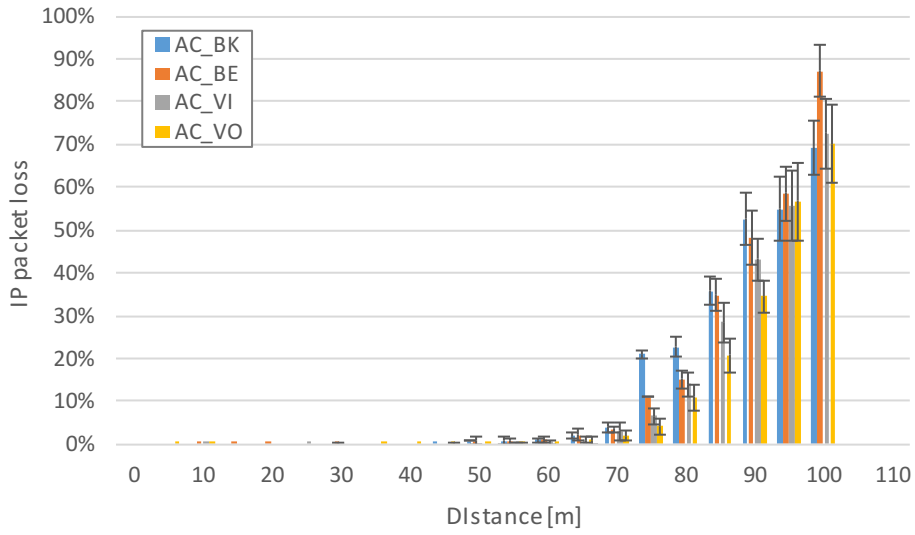

Fig. 30 IP packet loss as a function of distance from an AP for a STA-STA video transmission in an unloaded network

Packet loss statistics also follow the pattern observed during previous scenario, however in case of STA-STA transmission, the IP packet loss becomes observable earlier and its percentage is higher. This is only to be expected as, according to results shown in Fig. 33, the maximum throughput of the 2-hop STA-STA transmission is expected to be below ½ of its value for a direct STA to infrastructure communication. Also, it is noticeable, that in presence of other traffic contending for access to a wireless medium, high priority traffic classes are able to provide a significantly smaller traffic loss, compared to low priority ones, which is especially noticeable in 50-90 m range.

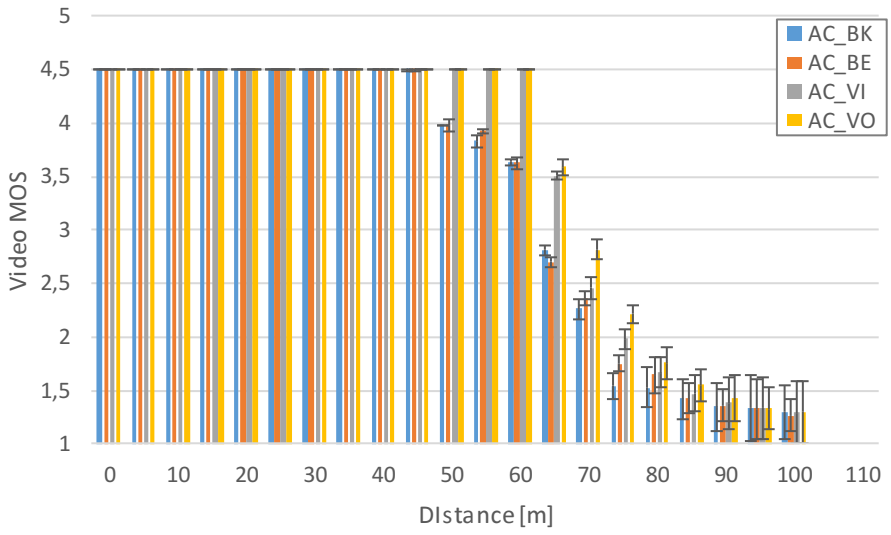

Fig. 31 Non-interactive video streaming MOS as a function of distance from an AP for a STA-STA video transmission in an unloaded network

The abovementioned ability of AC_VI and AC_VO to provide a better service level (especially in terms of a packet loss) in presence of contending traffic significantly influences the resulting video MOS values. With at least 0.5 difference in MOS value between low and high priority traffic classes in ranges between 50 and 70 m, the advantage of the later is easily observable. At higher ranges, the already mentioned, maximum available bandwidth limitation due to low SNIR brings MOS for all traffic classes below 2.0 (poor), which reduces the range in which the service can be accessed with an acceptable QoE by about 15 m, compared to STA to infrastructure scenario.

The maximum transmission range in this scenario is limited to a 100 m (10 m shorter then in case of STA to infrastructure communication).

UDP data transmission

The first data transmission scenario consists of single wireless STA generating an inelastic, UDP traffic stream addressed to a host in the cable infrastructure network behind its serving AP – a single, 1-hop transmission.

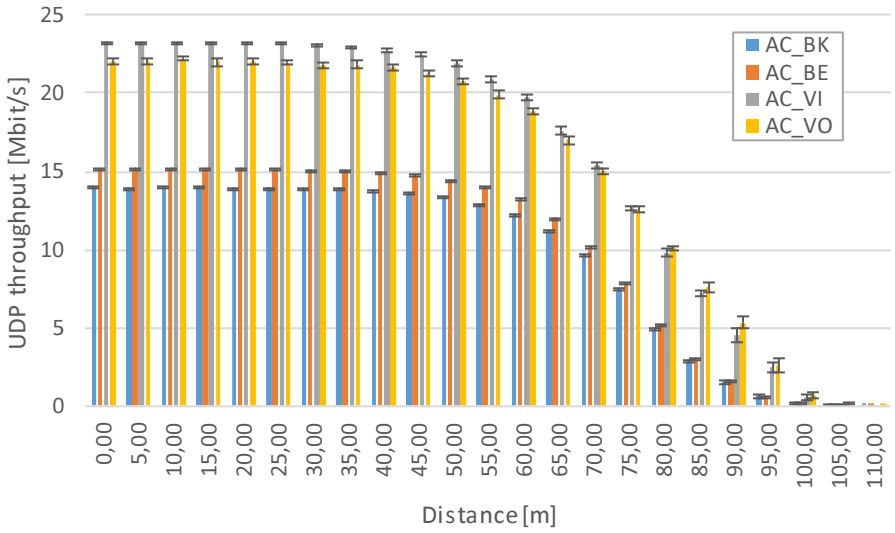

Fig. 32 STA to infrastructure UDP throughput as a function of a distance from an AP

As can be seen in Fig. 32 Voice and Video traffic classes allow for significantly better throughput to be obtained, due to their preferential medium access parameters (shorter AIFS timers and lower $CW_{min/max}$ limits), but mainly due to their non-zero TXOP values. At extreme range of the AP's coverage it can also be observed, that AC_VO outperforms AC_VI, because its more preferential medium access parameters become more important than longer TXOP of AC_VI, as the number of required retransmissions increase due to small SNIR (Signal to Noise and Interference Ratio) value of the received radio signal.
The specific throughput values obtained remain consistent with expectations, taking into account maximum transmission rate of 54 Mbit/s, medium access overhead, link-layer acknowledgements and the propagation environment (Nakagami model, m=2). They are also consistent with measurements obtained for several real-world systems operating without above-average external interference.

The second scenario consists of two wireless STAs located (as in case of previous VoIP and video experiments), within mutual communication range (40 m).

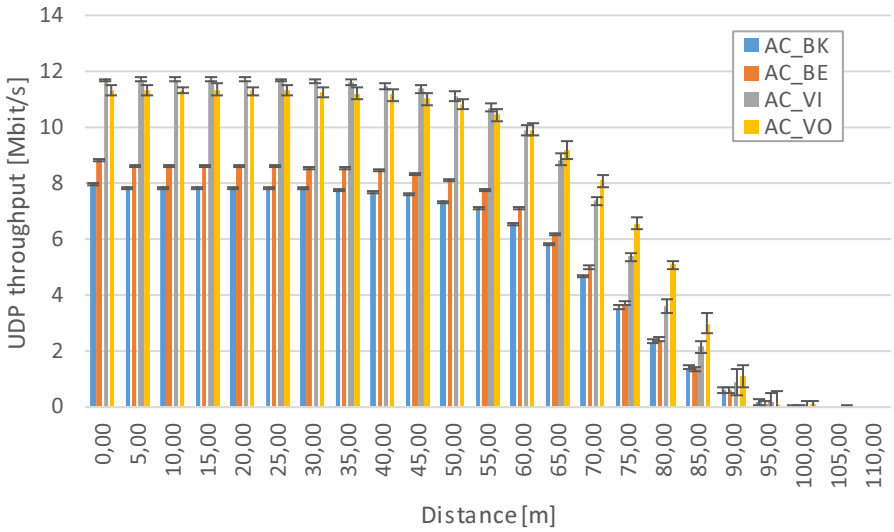

Fig. 33 STA-STA UDP throughput as a function of a distance from an AP

The throughput in this case is consistently a bit less than half of that observed in STA to infrastructure scenario, until we reach the extreme range of the AP's coverage, where it decreases faster than in case of 1-hop transmission. As expected, a 2-hop transmission sharing the same wireless channel leads to a need to divide its resources, halving the possible throughput. Moreover, contention-based medium access mechanisms cause a certain amount of inefficiency, responsible for reducing the throughput even further (especially at extreme range, where retransmission probability is high), however the effect is limited due to a chosen UDP packet size of 1470 B.

2.5.7.3 Experiments in IEEE 802.11 PtMP network with background traffic

Having analyzed effects of communication range on a quality of chosen multimedia services, we proceed to analyze similar impact of a background traffic. For this purpose a number of wireless stations, have been added to the previous scenario. All of these stations are connected to the same AP and each is generating a 6 Mbit/s inelastic UDP traffic stream to a host located in infrastructure network. Such a selection of a source throughput results, compared with assessment of the network's effective bandwidth (Fig. 32), means that it should reach saturation conditions with as few as 4 active background traffic sources. Further increase of the number of such traffic sources will allow us to illustrate the impact which a number of competing clients makes on the efficiency of IEEE 802.11 network operation under saturation load.
The experiment has been repeated with such background traffic using various EDCA traffic classes and the charts, in contrast with charts from the previous section, show traffic classes of the background traffic. Each of evaluated services, VoIP and non-interactive video streaming, utilizes a traffic class indicated for such service type in IEEE 802.11 standardization documents [32]: AC_VO and AC_VI respectively.

As previous experiments indicate that a transmission quality required to support the selected set of multimedia services can be maintained in 70 m range, all wireless stations in the following scenario are located at 70 m from the AP.

VoIP STA to infrastructure transmission

In case of a single-hop, STA to infrastructure VoIP transmission, it can be clearly seen, that a traffic using Background and Best effort classes has a limited impact on VoIP transmission utilizing a Voice

traffic class. On the other hand, background traffic of Video and Voice classes influences IP transmission delay and IP packet loss significantly.

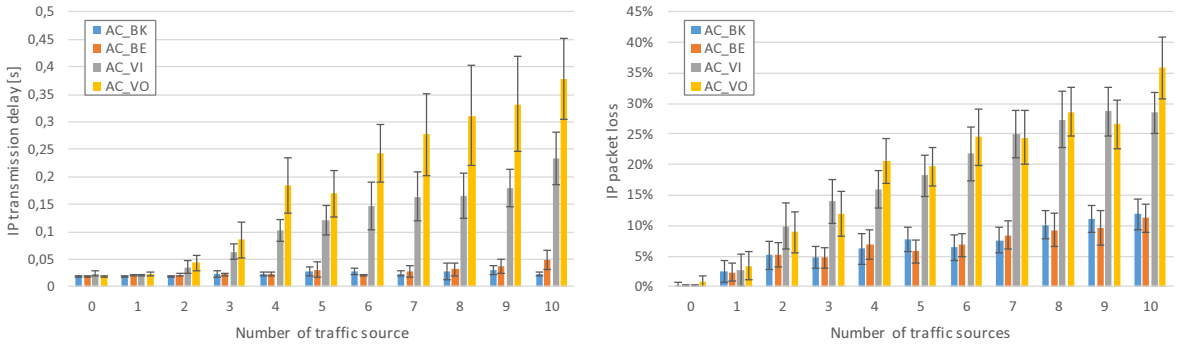

Fig. 34 IP transmission delay and packet loss as a function of a number of 6 Mbit/s background traffic sources for a STA to infrastructure VoIP transmission

As shown in Fig. 34, low bandwidth of VoIP transmission combined with use of AC_VO traffic class, makes the service resilient to even relatively high-bandwidth competing traffic streams in low priority classes. As observed before, AC_BK and AC_BE-class background traffic has almost no impact on a delay of AC_VO VoIP transmission and limited impact on its IP packet loss.
On the other hand, the impact of AC_VI and AC_VO-class background traffic is clearly observable, causing about 5% packet loss per each 6 Mbit/s traffic source present. After the network reaches saturation conditions (4 sources with 24 Mbit/s aggregated traffic), further increase of the number of traffic sources sill results in further degradation of transmission quality, combined with an observable increase of the width of confidence intervals, indicating reduced stability of traffic conditions.
In overall, 3 and more traffic sources (which equals to about 18 Mbit/s of background traffic) will lead to an observable degradation of quality of the VoIP service, mostly due to IP packet loss. With over 4 traffic sources active, also the transmission delay exceeds a 150 ms maximum, suggested for VoIP communication.

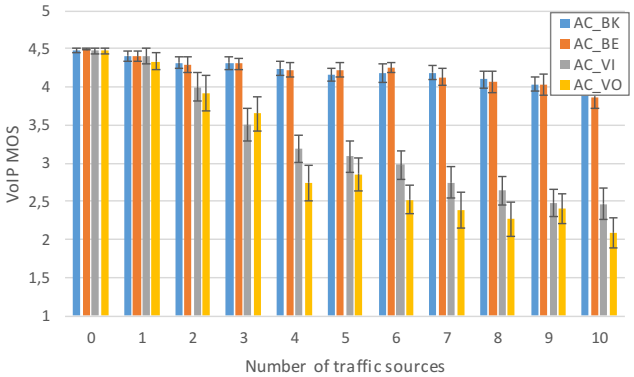

Fig. 35 VoIP MOS value as a function of a number of 6 Mbit/s background traffic sources for a STA to infrastructure transmission

The above characteristics directly influence resulting MOS values shown in Fig. 35. Low priority background traffic proves to be unable to impact the VoIP transmission sufficiently to bring its QoE visibly below a good (4.0) level, regardless of the number of traffic sources, which clearly proves utility of AC_VO traffic class for a VoIP service.
Background traffic in high priority traffic classes will result in VoIP service degradation as the network approaches saturation conditions. For number of background traffic sources less than 3 (18 Mbit/s),

MOS does not drop significantly below 4.0. With growing number of background traffic sources, it quickly drops to about 2.5. However, the MOS does not fall below 2.0, even for 10 sources (60 Mbit/s of generated background traffic).

Video STA to infrastructure transmission

Higher throughput (2 Mbit/s) and lower traffic class (AC_VI) of video streaming transmission makes it more susceptible to disruption due to activity of background traffic sources. However, different EDCA background traffic classes influence its impact on the video transmission in a manner akin to the one observed in previously described VoIP scenario, with background traffic in AC_BK/AC_BE classes showing lower and in AC_VI/AC_VO significant impact on the video transmission.

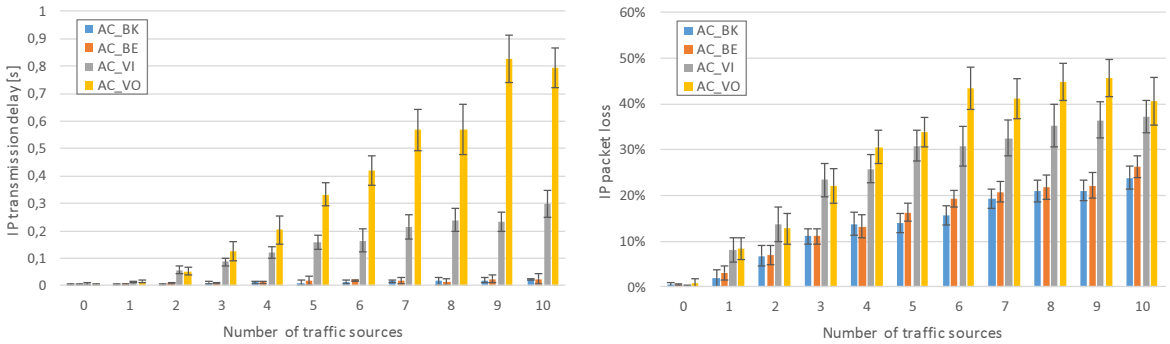

Fig. 36 IP transmission delay and packet loss as a function of a number of 6 Mbit/s background traffic sources for a STA to infrastructure video transmission

From Fig. 36 we can observe, that IP packet loss percentage that AC_VO background traffic significantly impacts both IP transmission delay and packet loss of a video transmission. The impact of even low priority traffic on the packet loss of a 2 Mbit/s transmissions utilizing an AC_VI traffic class is clearly observable. The difference is cause both by a higher throughput of the transmission, and its slightly lower priority traffic class, with less preferential medium access parameters. It is evident, that background traffic in the higher priority AV_VO traffic class, has an significantly higher impact on the video traffic than any other class.

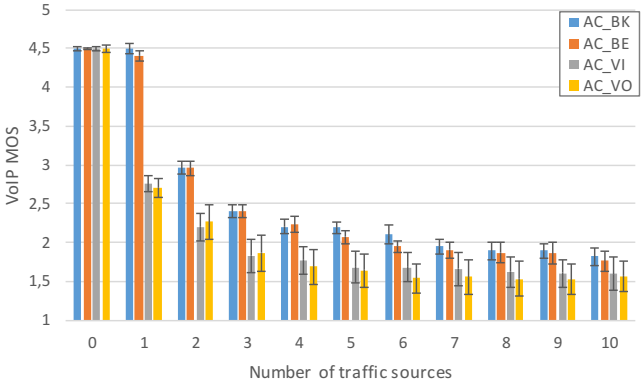

Fig. 37 Non-interactive video streaming MOS value as a function of a number of 6 Mbit/s background traffic sources for a STA to infrastructure transmission

While the H.264 non-interactive video streaming with 5 s receive buffering is not degraded by transmission delay cause even by AC_VO traffic, it is highly susceptible to packet loss. Even a single traffic source of AC_VO or AC_VI is enough to reduce the MOS to about 3.0 (fair), while a higher number will quickly bring it down below a value of 2.0 (poor). In case of a traffic using AC_BK or

AC_BE, a single 6 Mbit/s source does not seem to degrade the video QoE, but when the network load approaches saturation point, even such traffic will bring it between 2.0 and 2.5.

VoIP STA to STA transmission

With additional retransmission of the VoIP stream necessary in STA-STA scenario, the impact of background traffic is much more evident, despite the low bandwidth of the VoIP stream.

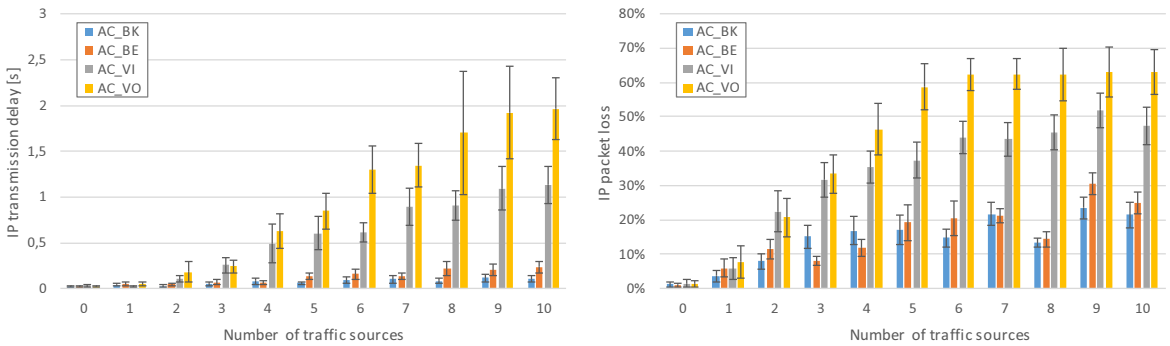

Fig. 38 IP transmission delay and packet loss as a function of a number of 6 Mbit/s background traffic sources for a STA-STA VoIP transmission

Even cursory analysis of IP transmission delay and packet loss for STA-STA communication shows, that background traffic influences the analyzed stream in a very similar way as was the case in the STA to infrastructure transmission, but with even higher the delay and packet loss values.

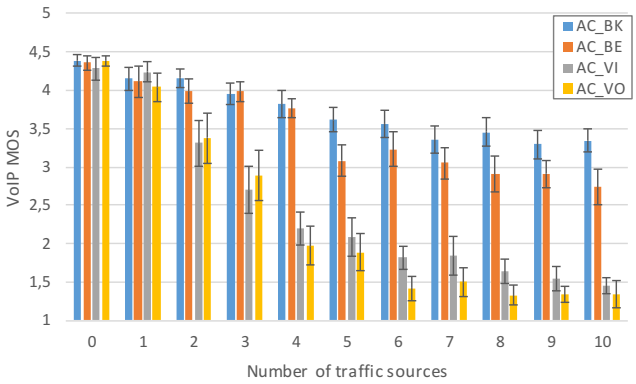

Fig. 39 VoIP MOS value as a function of a number of 6 Mbit/s background traffic sources for a STA-STA transmission

As can be expected, the resulting MOS values of VoIP transmission are generally lower, with even AC_BE and AC_BK traffic being able to visibly influence video MOS values with high number of traffic sources. Also, for the first time, an observable difference between the impact of AC_BK and AC_BE can be observed, despite their much lower priority then AC_VI used for VoIP traffic.
The impact of high priority background traffic is observable as the network approaches saturation point, in which case VoIP MOS quickly drops under 2.0 (poor). With growing number of traffic sources the MOS value stabilizes at about 3.0 in case of low priority background traffic – which makes its effect observable in contrast with 1-hop scenario, and below 1.5 in case of high priority background traffic – which makes the VoIP service unfit for use.
This scenario makes it evident, that additional transmission hop in presence of a background traffic significantly reduces the QoE and makes it susceptible for even low priority contending traffic streams.

Video STA to STA transmission

A combination of a relatively high throughput and necessity of retransmitting packets by an AP makes the scenario of STA-STA video transmission the most susceptible to disruption by a background traffic. In this case even sources utilizing low-priority traffic classes (AC_BK/AC_BE) can be expected to influence IP transmission delay and packet loss of the AC_VI video traffic stream.

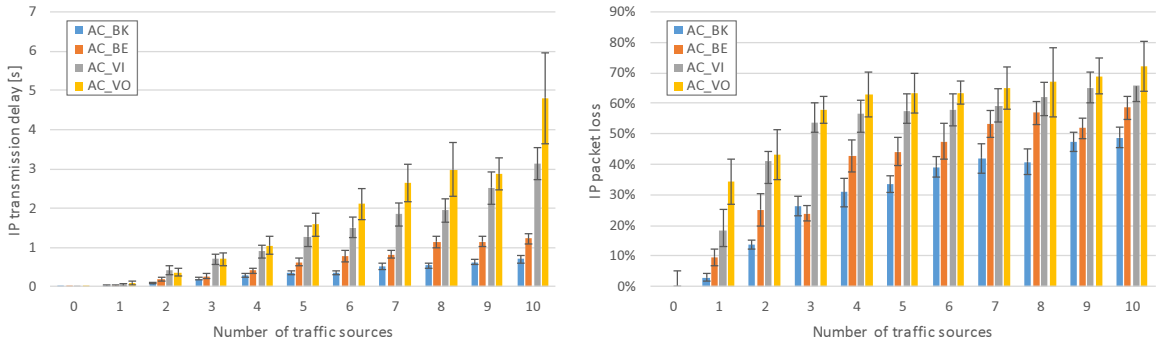

Fig. 40 IP transmission delay and packet loss as a function of a number of 6 Mbit/s background traffic sources for a STA-STA video transmission

If we compare this scenario with a previously described STA to infrastructure video streaming, we will observe about twice as high percentage of packet loss and up to 10 times as high IP transmission delay when background traffic sources utilize one of high priority classes (AC_VI/AC_VO). Moreover, the delay caused by a background traffic using low priority classes is clearly visible and grows significantly with the number of its sources (and its volume) – an effect absent in previous scenarios.

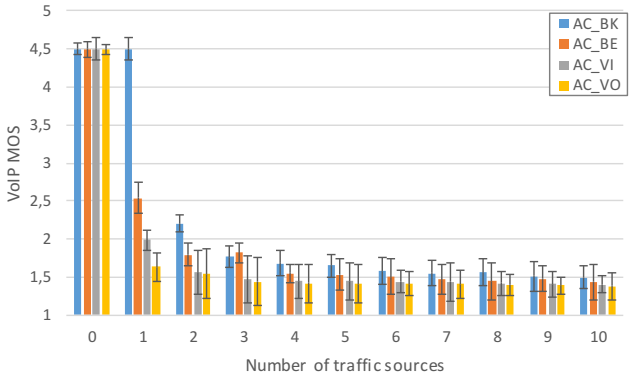

Fig. 41 Non-interactive video streaming MOS value as a function of a number of 6 Mbit/s background traffic sources for a STA-STA transmission

In this scenario, even a single high priority background traffic source (6 Mbit/s) can bring the video MOS value below 2.0, indicating poor service quality. In case of low priority traffic, the effect is less pronounced (especially for an AC_BK class). However, in case of more than 2 traffic sources (12+ Mbit/s) the service should be considered unfit for use regardless of the EDCA class of the background traffic – it is due to a high level of IP packet loss, for which the video streaming is highly susceptible. The scenario further confirms a much higher susceptibility of high throughput multimedia services to even low priority background traffic, in multihop environments.

Group addressed traffic delivery

Apart from multimedia services analyzed above, a simple experiment has been performed regarding the delivery of group addressed traffic. Such traffic type (multicast and broadcast) is delivered

without transmission acknowledgements, resulting in IP packet loss rates significantly higher than in case of unicast traffic. A broadcast transmission has been performed between a single STA and an AP, at ranges of under 1 meter, and then at 30 and 70 m. Each of scenarios has been repeated with an increasing number of background traffic sources, each generating 6 Mbit/s of UDP traffic.

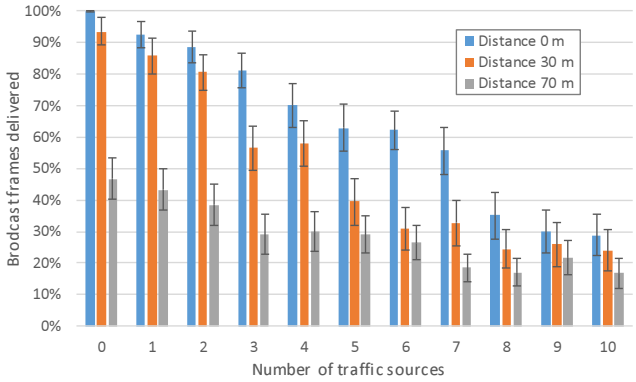

Fig. 42 Broadcast traffic delivery ratio in an IEEE 802.11 PtMP environment

As show in Fig. 42, the broadcast traffic delivery rate in our assumed propagation environment, is highly dependent on transmission range, as when in unicast transmission frame errors result in increased transmission delay due to retransmissions, in case of broadcast traffic they immediately cause packet loss.

Background traffic has similar effect, resulting in broadcast packet delivery as low as < 20% for 70 m range and saturated network. In most working conditions we must consider at least 30 % broadcast packet loss.

From the above results and due to a number of additional issues, related to, for example power saving procedures addressed in research preliminary to preparing this thesis [20], the use of a group addressed communication in an environment of the IEEE 802.11 network does not seem to be an efficient solution promising even an adequate level of the Quality of Experience. As can be seen in Fig. 42 the problems become severe if any of the high traffic load or a long range (lesser quality) links are present.

In this situation it seems that an unicast delivery of multimedia traffic can be considered a viable solution even in a IEEE 802.11 PtMP environment, despite the obvious inefficiency of such solution, requiring a separate traffic stream to be maintained for each client connected to the service. However, with limited capacity of real-world access point implementation, able to successfully support only a limited number of clients, a growing bandwidth of available physical layer solutions and efficiency of modern compression algorithms, such approach is indeed practicable.

It can also be expected, that in case of an IEEE 802.11s mesh network described in the following chapters, the problem with a quality of group addressed traffic delivery can pose an even greater challenge in deployment of multimedia services.

2.5.7.4 *Efficiency of IEEE 802.11 management mechanisms in multi-AP network deployments*

With the efficiency of IEEE 802.11-2007 data plane mechanisms already verified in previous simulation scenarios, it remains to be seen, how efficient are its management mechanisms. This aspect should be of a particular interest, as IEEE 802.11s mesh network employs almost exactly the same data plane procedures (especially medium access mechanisms – see 3.7.1), while majority of differences between IEEE 802.11-2007 infrastructure mode and IEEE 802.11s mesh network lays in its self-organization and autoconfiguration capabilities.

The above observation seems to suggest, that the use of a multihop transmission of an IEEE 802.11s mesh in place of a single-hop AP-STA communication cannot provide a superior quality of communication for multimedia services. This assessment is further reinforced by comparing single-hop STA to infrastructure scenarios with 2-hop STA to STA scenarios. In this situation, it is clear, that possible mesh network advantages should be expected in its expected superior coverage, redundancy and ability to reconfigure its mechanisms according to the current network state.
Based on these expectations, a number of scenarios illustrating IEEE 802.11-2007 PtMP network operation in an event of change in network structure (device failure or deactivation) have been presented below. The scenarios also provide a rough assessment of coverage area and quality available with a given number of infrastructure devices. It is thus obtained information will be used for comparison with IEEE 802.11s mesh network performance in similar conditions, presented in 3.8.4.

Latency of recovery from a single access point failure

As an IEEE 802.11 PtMP network requires a dedicated access point for its operation, a failure of such device will render an entire PtMP network inoperative. In such case wireless STAs will be required to find another AP to connect to, if there is one able to provide a network coverage for a particular STAs location.

The process of detecting of AP failure is not strictly specified in the standard, but the task is most often performed by detecting the loss of three consecutive Beacon management frames, which are, by default, sent with interval of 100 ms, resulting in minimal failure detection time of 300 ms.

The STA must subsequently find a new AP to connect to, which requires it to perform a network scanning over a set of preconfigured frequency channels. The latency of the process is mainly dependent on the length of the channel list and the amount of time a given STA spends checking each frequency channel (dwell time). The dwell time depends on two parameters:

- MinChannelTime – indicates a minimum time a STA must spend on each frequency channel while performing a scan,
- MaxChannelTime – sets the upper limit of a time a STA can spend on each frequency channel while performing a scan.

The specific values for the above parameters are not defined by the IEEE 802.11-2007 specification and must be considered implementation specific.
The popular values of MinChannelTime include 10-30 ms [61,], but there are implementations and simulation models which set this parameter as high as 150 ms [62,63].
The MaxChannelTime values are often in range 200-300 ms [61], but some implementations are known to use values as low as 28 ms [64].

The scanning can be conducted in two modes:

- Passive scanning – by listening to Beacon management frames broadcasted by APs. The dwell time must take into account the interval in which Beacon frames are sent (100 ms by default).
- Active scanning – by sending Probe Request management frames and awaiting Probe Response management frames. The dwell time must accommodate an amount of time necessary for the above frames to be exchanged, but can generally be shorter than in case of passive scanning. Due to this advantage, it is the default method of network discovery, however the decision depends upon a particular implementation.

The actual dwell time depends on a used mode of scanning (passive or active) and a particular algorithm employed by the STA (which also is not precisely defined in IEEE 802.11-2007

specification), and will impact the overall network discovery latency both by introducing a direct delay of dwell time for each scanned channel and by influencing the probability of missing an existing AP on a particular channel, due to not receiving its valid response within the dwell time used, possibly preventing STA from regaining network connectivity and requiring the scanning process to be repeated. Both difficult propagation conditions and heavy traffic load can negatively impact the probability of performing a successful network discovery within an allocated dwell time [61].
In case of complex networks, providing redundant coverage, missing an AP in the process of network discovery can also have a different effect, as can also lead to the STA connecting to an AP providing a lower level of service despite the (undetected) presence of a better one. Such occurrence will keep the standard IEEE 802.11-2007 STA connected to such erroneously selected AP, as the scanning process will not be repeated until the STA again suffers a loss of network connectivity.

With the network discovery complete, the STA must perform authentication and association phases, before network connectivity can be restored. While the association process is relatively simple, most often requiring a single exchange of Association Request and Association Response management frames, the authentication phase complication and latency can vary greatly, depending on authentication method employed. It is possible for the process to be finished under 20 ms in case of utilizing exclusively AP-integrated functionality and resources [65], or to require multiple seconds, due to a necessity of communicating with external authentication server over wide-area IP network. Due to possibly high impact of the authentication-related delay combined with its implementation and configuration dependent nature, we are going to leave it out from the following assessment scenario.
Due to evidently high latency of the network discovery phase, a number of optimizations have been proposed [15,66,67], but their employment requires introduction of additional STA mechanisms, so their deployment is limited to particular brands of hardware.

In Fig. 43 an assessment of a mean time necessary to restore a network connectivity in case of a standard IEEE 802.11-2007 STA after a complete failure of its currently serving AP. A single redundant AP is available for the STA.
The results have been obtained in the already described (see 2.5.7.1) simulation environment and for randomly assigned frequency channels from an European set of 5 GHz ISM band. The 5 GHz ISM band provides [68]:

- 4 independent 20 MHz frequency channels in U-NII-1 portion – dedicated for indoors use,
- 4 independent 20 MHz frequency channels in U-NII-2A portion – intended for mixed indoor/outdoor use,
- 11 independent 20 MHz frequency channels in U-NII-2C portion – intended for outdoor use.

The simulation has been performed for low and saturation network load and STA located at randomly chosen location within 80 meters of AP, which (based on previous scenarios) should provide adequate propagation conditions. The parameters of MinChannelTime and MaxChannelTime has been set to middling values of 20 and 250 ms respectively.
Each scenario has been repeated a 100 times to obtain statistically meaningful results.

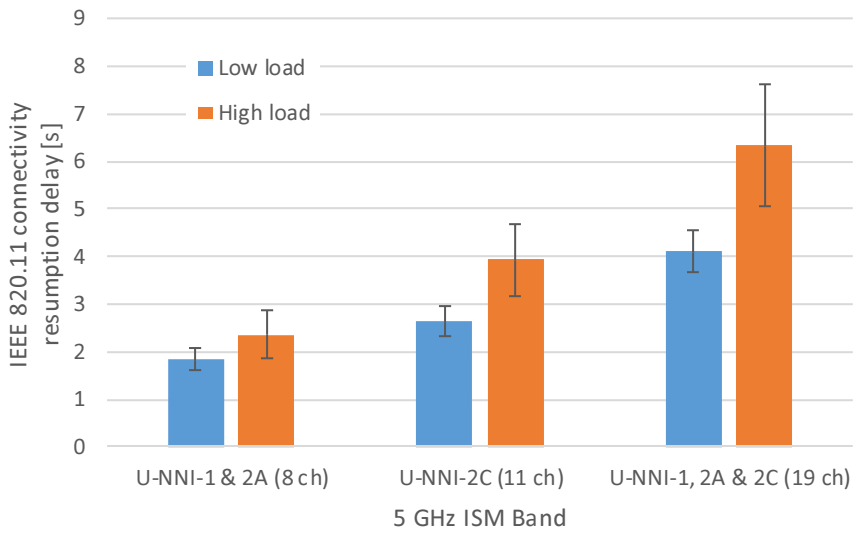

Fig. 43 IEEE 802.11 network discovery latency

It is evident, that STA recovery from an AP failure, without additional information concerning available APs and their parameters is a time consuming process. A number of channels which a STA must check has a direct impact on the delay, while a high traffic load, leading to management frame losses can increase the reconnection delay significantly. Relatively broad 95% confidence intervals for high network load scenarios are caused by a significant impact of losing a management frame, which can result in necessity of repeating the entire scanning process.

Impact of access point failure in a multi-AP network

With the previous scenario providing assessment of the expected length of connectivity disruption due to AP failure, we are going to proceed with a scenario illustrating how failure of a given number of AP in a multi-AP access network will affect quality of multimedia service provided to its users.
For this purpose and based on the AP range estimation from preceding experiments, we analyze a 10 access point network deployed over a 500x500 m area. All access point and a single host computer are connected with a Gigabit Ethernet wired network. All other parameters are the same as they were in case of previous scenarios.
In such environment, 30 IEEE 802.11g wireless stations are deployed, which proceed to associate with the network and commence a 60 s VoIP or video streaming transmission (transmission parameters are also the same as is previous scenarios). After all STAs finish their transmissions, a random AP is deactivated, possibly causing some STAs to lose connectivity with the network and attempt a reconnection. Then connected stations repeat their transmission. Stations which are unable to connect are counted as MOS 1.0 indicating a unacceptable level of service.
The described scenario takes into account only transmission capabilities provided to stations in a given network setup, disregarding the impact of the disconnected station's delay in finding an alternative access point and reconnecting to the network, which can be expected (based on the previous experiment) to reach an average of about 2 s.

Three AP placement methods are considered:

- Random AP placement – APs are placed in the described area randomly, with uniform probability,
- High quality coverage AP grid – APs are placed at free intersections of a rectangular grid, with grid lines being 110 m apart. Such placement allows neighboring APs to provide a good quality transmission over the area if they are placed at neighboring intersections and significant overlap of their fair transmission coverage area.

- Maximum coverage AP grid – APs are placed at free intersections of a rectangular grid, with grid lines being 190 m apart. Such placement allows neighboring APs to provide a fair quality transmission over the area, if they are placed at neighboring intersections. The coverage overlap is very limited.

Neighboring Access Point are configured to use orthogonal frequency channels, if possible, from 5 GHz ISM U-NNI-1 and U-NNI-2A bands (8 orthogonal channels).

The abovementioned distances have been selected based on the previously conducted experiments concerning IEEE 802.11 PtMP efficiency in our chosen propagation environment.
In case of a fully installed (all intersections occupied):

- high quality coverage grid – STA should be no farther than 65 m from the AP,
- maximum coverage grid – STA should be no farther than 95 m from the AP.

Which is in accordance with the range of 70 m being a maximum distance between two communication stations, at which there is still no degradation of transmission parameters due to propagation conditions and the maximum association range of an AP being a 100 m.

As such access networks are most often deployed according to pre-designed rules, three different wireless station placement scenarios have been considered:

- Random STA placement – STAs are placed in the described area randomly, with uniform probability, illustrating access network created with no prior knowledge of its client locations,
- Random STA placement within good coverage area – STAs are also placed randomly, but only within network's good coverage area (up to 40 m from AP),
- Random STA placement within coverage area - STAs are also placed randomly, but only within network's coverage area (up to 90 m from AP).

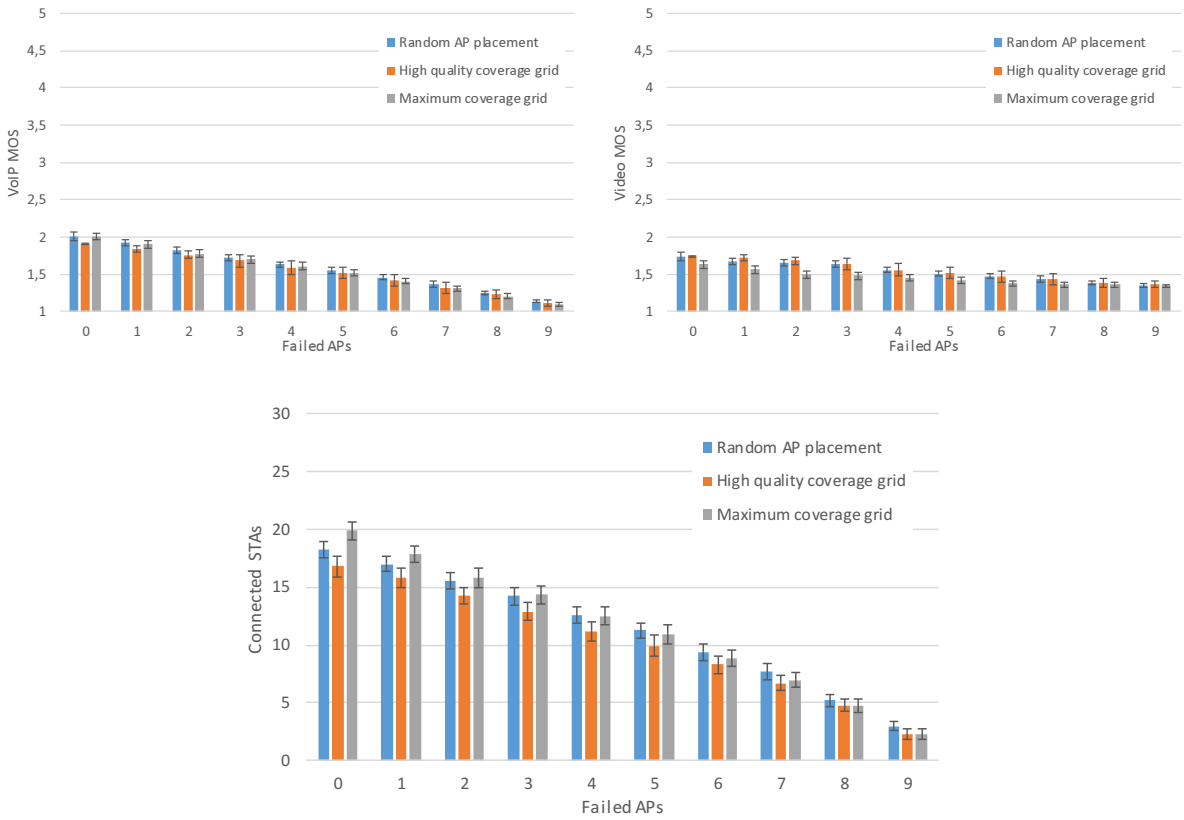

Fig. 44 Assessment of mean VoIP and non-interactive video QoE values for a random station placement

In case of random STA placement, only a fraction of STAs will be located within the coverage of APs (Fig. 44) and an even smaller fraction within a range allowing the communication between STA and AP to be of good quality (as shown in previous experiments – about 70 m).
As can be expected a maximum coverage grid AP deployment policy results in a highest number of connected stations, which becomes less observable with decreasing number of active APs. In contrast, high quality coverage grid AP placement policy results in much lesser overall coverage, while random AP placement provides a middle ground solution. However, the differences are not pronounced and for 10 APs all methods leave at about 1/3 of STAs outside the system's coverage area.

As a result, mean values of both VoIP and non-interactive video MOS are between 1.5 and 2.0 which indicates poor perceived quality of these multimedia services.
VoIP MOS values are a bit higher then video MOS mainly due to much smaller resource requirements of 64 kbit/s VoIP transmissions, despite their susceptibility to disruptions resulting from transmission delay, which are of much lesser importance in case of video transmissions. In case of video traffic streams, their 2 Mbit/s throughput makes separate traffic streams interfere with each other both within the same BSS and between different BSS networks operating on the same channel (as interference range is much higher than effective communication range).
Low throughput of VoIP streams also makes the high quality coverage grid AP deployment pattern the least effective solution, as it provide the smallest effective coverage of the system, thus reducing the number of connected STAs and in effect, the overall mean VoIP MOS value. In case of video streaming, its much higher transmission bandwidth raises the importance of obtaining good propagation conditions, which provide a significant MOS gain, outweighing the impact of lesser number of connected stations.
Simulated AP failures result in observable but relatively insignificant decrease of overall, mean MOS values of the system, as the initial value of this parameter for a complete 10 AP system is already small.

Based on the above results, it is not surprising, that deployment of multi-AP IEEE 802.11 access networks is, most often, based on previous radio planning phase. The results of the next scenario, shown in Fig. 45, illustrate the situation where all stations are located within a good coverage area (up to 70 m) from AP. As subsequent access points are disabled, the number of connected stations decreases most rapidly in case of a maximum coverage grid AP placement policy, as APs are located with minimal overlap of their coverage areas. Random AP placement and high quality coverage grid policy show slower decrease, due to more substantial overlap of coverage areas, with random placement providing marginally more substantial but less predictable resiliency level (as indicated by its wider confidence intervals).

The fact that, initially, all STAs have good connectivity with their APs, results in VoIP and video MOS values over 4.0 (good) and 3.0 (fair) respectively. The lower value of video MOS is caused by higher bandwidth requirements of such transmissions, leading to higher transmission resource consumption and contention between different traffic streams within the system.
In case of VoIP service,

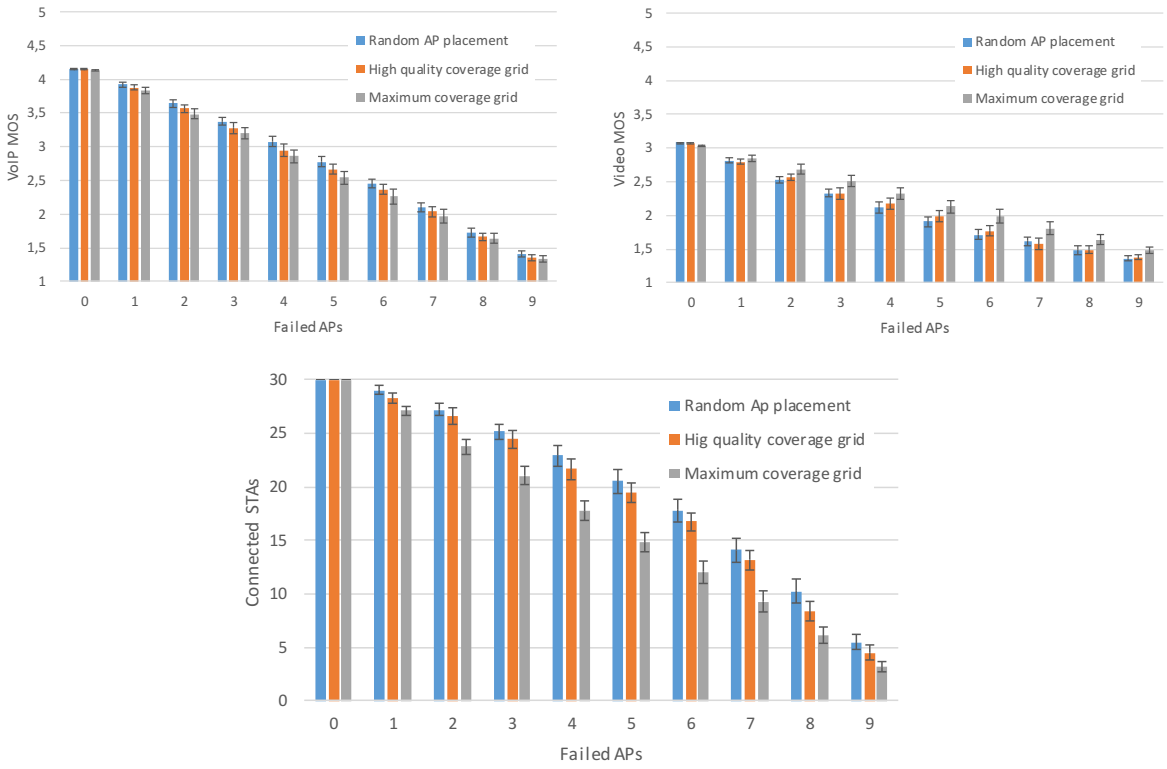

Fig. 45 Assessment of mean VoIP and non-interactive video QoE values for a random station placement within a good coverage area of a multi-AP network

In case of video streaming, it can be observed, that AP placement policies where deactivation of subsequent APs results in rapid decrease of a number of connected stations, surprisingly display a visibly slower decrease of overall, mean MOS value of the system. This effect can be explained by the fact, that disconnected stations, unable to initiate their video streaming transmissions, do not consume system resources which in turn become available for the still connected stations. Such effect has not been observable in previous scenario, due to significantly more dispersed STA locations.

In the last scenario, wireless stations have been placed randomly within adequate coverage range (100 m) of system's access points. The results shown in Fig. 46 confirm, that initially all 30 stations are successfully connected to the network, which results in a mean VoIP MOS value higher than in case of random station placement scenario, where some STAs were initially unable to connect. However, mean video streaming MOS values are very lowest of all station placement scenarios – in their case, with all 30 stations concentrated within coverage range of APs and thus able to connect to the network and commence their 2 Mbit/s transmissions maximizes interference. At the same time there is a considerable probability, that a STA will be located outside of a range within which a good quality of communication is possible. Combination of these factors results in mean video streaming MOS value at about 1.5, which effectively makes the service unusable.

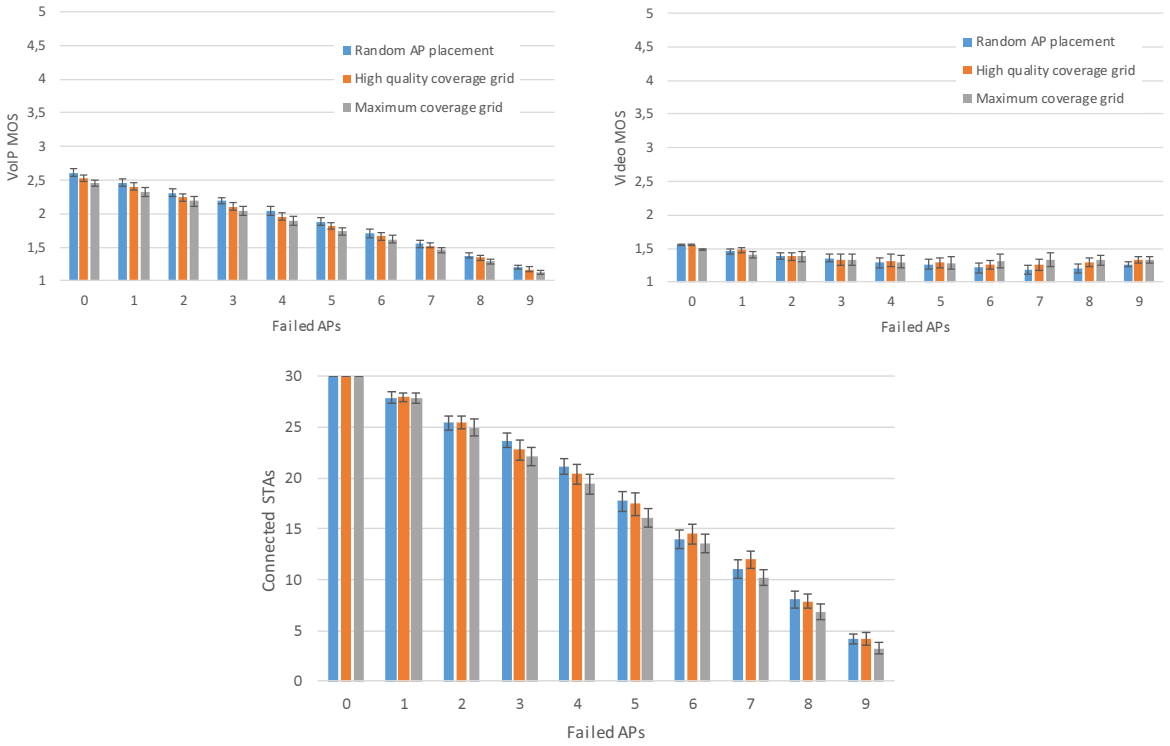

Fig. 46 Assessment of mean VoIP and non-interactive video QoE values for a random station placement within an adequate coverage area of a multi-AP network

As subsequent access point fail, the mean VoIP MOS decreases, as can be expected. The same trend initially be observed in case of the mean video streaming MOS values, but with less than 4 active APs remaining, it actually begins to increase, due to disconnection of a high number of stations and thus reduced interference between their transmissions.

2.5.7.5 *Interpretation of simulation results*

The above experiments allowed us to obtain a number of values and conclusions regarding efficiency of handling of multimedia traffic in IEEE 802.11 PtMP networks. This information will be used for comparison with IEEE 802.11s mesh network performance in similar environments, to verify if indeed there are cases where multihop mesh communication can provide a better level of service than a simple PtMP access.

The most notable observations include:

- For the propagation model used, which provides good approximation of real communication environment with significant attenuation and multipath effects, the network shows a sharp growth of IP packet loss ratio and IP transmission delay near its maximum possible communication range. Moreover, the values of these parameters show chaotic behavior at such ranges, making the offered level of service highly unstable.
- In the abovementioned environment, the maximum range at which a transmission quality does not show a noticeable degradation due to the distance to AP is observed to be about 50 m.
- In the described propagation environment, the effective throughput archivable for an IEEE 802.11a station in a STA to infrastructure transmission scenario does not exceed 24 Mbit/s and slightly less than half that value in STA-STA transmission scenario.

- The fact that a STA remains associated with AP even in poor propagation conditions can be a serious disadvantage, as it will prevent it from searching for another AP, possibly offering a much better connectivity.
- Background traffic in high priority classes (AC_VI and especially AC_VO) introduces much more pronounced disruption to other transmissions then the same traffic in low priority classes (AC_BK and AC_BE), especially in case of limited availability of network resources (saturation conditions).
- Due to lack of implementation of Tunneled Direct Link Setup (TDLS), station to station traffic needs to be retransmitted by AP, which effectively changes such PtMP environment from 1-hop into 2-hop network. In such 2-hop environment the adverse effect of a background traffic is much more pronounced, making even a low priority (AC_BK, AC_BE) traffic a significant factor influencing the QoE of a multimedia service.
- The IP traffic delay is only partly due to a delay introduced by IEEE 802.11 medium access mechanisms and wireless transmission. A significant part of the recorded delay can be attributed to IP mechanisms located in network ISO-OSI layer.
- The impact of a background traffic generated by other STAs in the PtMP network causes less chaotic degradation of a quality of multimedia transmissions than adverse propagation conditions at its extreme ranges.
- MOS values of non-interactive video streaming do not show much dependence on IP transmission delay values (due to ability to employ a receive buffer of considerable size). However, video transmission reacts sharply to even relatively small IP (1-3%) packet drop rates. Moreover, a relatively high throughput of video traffic stream makes it generally more susceptible to disruption due to background traffic presence.
- It is advised to limit the use of high priority classes within the network to services which strictly require them, as the impact such a traffic has on other traffic streams is much more pronounced than in case of lower priority classes. That observation confirms the decision to use AC_VI traffic class for video transmissions, instead of AC_VO class, despite the fact that the latter is able to provide a limited improvement in transmission parameters and resulting MOS values, for relatively low throughput video streams chosen for experiments (2 Mbit/s).
- An IEEE 802.11 in infrastructure mode requires a relatively high number of access points to provide a good quality coverage of a sizable area. Due to this fact, it is imperative to design such system taking into account expected locations of client STAs.
- Without employing a high number of redundant devices, failure of an AP results in degradation of multimedia service quality, even in case, when a given STA will be able to connect to another access point.
- The process of reconnecting to the network following an AP deactivation or failure is quite lengthy (seconds), and highly dependent on the time required by the network discovery procedures.

The significant increase of susceptibility of both VoIP and video multimedia traffic to both range and background traffic-originating disruption in STA to STA communication scenarios, does not make the use of a single-channel, multihop communication network a promising solution for these types of services. However, there are possible advantages to be found in peer-to-peer structure of mesh network, as long as it is supported by efficient set of self-organization and automatic management mechanisms – a set of IEEE 802.11s deployment scenarios, designed to allow a comparison with these presented above, is provided following the IEEE 802.11s standard description (see 3.8.4).

2.5.8 Conclusions

Having in mind the statements of the thesis presented in chapter 1 and based on results of both the theoretical analysis and simulation-based experiments presented above, we must conclude that the robustness of the classic PtMP wireless access systems created with currently available IEEE 802.11-compatible hardware is strictly limited.

The results of scenarios presented in Section 2.5.7.4 clearly indicate, that the ability of wireless clients to obtain a network connectivity and its quality is strongly dependent on the placement of a static set of access points. When we assume that it has been done correctly and the characteristics of client behavior did not change the results are satisfactory (Fig. 45). However, if we are unable to successfully asses the user behavior or locate appropriate infrastructure devices in accordance with the assessment, the quality of service provided will be unacceptable, especially as far as multimedia services are concerned (Fig. 44 and Fig. 46).

The above requirement results in three specific problems:

- inability of wireless clients to connect at the network at all,
- clients maintaining connection with an access point providing poor service level due to propagation conditions,
- clients connecting to a specific access points while leaving others underutilized.

The first problem is clearly visible in Fig. 44, where random client placement results in only about 60% of them being able to connect in our scenario.

The second one can be illustrated with results presented in sections 2.5.7.2 and 2.5.7.3 where it is clearly visible, that the quality of wireless transmission degradants significantly at longer ranges. Moreover, at extreme ranges the quality of transmission is clearly at unacceptable level, but standard IEEE 802.11 mechanisms prevent client from seeking a better point of network access until the current connection is terminated, which is especially troublesome for mobile clients. There are standard amendments designed to mitigate that problem (for example IEEE 802.11v [6]), but their mechanisms must be implemented in client devices, and their popularity is strictly limited.

The third problem is caused by the static way in which the resources of the network infrastructure must be assigned, by placing the access point devices to provide coverage in specific areas. Even when it is unlikely, that a given area will contain a significant number of clients, it must be covered by a dedicated access device. This leads to a frequently difficult decision if we are confronted with a complicated propagation environment (for example building interiors, industrial spaces, narrow streets, etc.) – should we significantly increase the number of infrastructure devices or should we leave some areas without coverage (coverage holes). As a result, infrastructure devices must be used to directly provide both coverage and capacity of the system.

In this situation, it is clear that the robustness resource management in a IEEE 802.11 PtMP network is strictly limited to the point, where an appropriate assignment of network resources and related compromises between number of deployed devices and completeness of the coverage are one of the main elements of the network design process.

The situation looks even worse if we factor in the possibility of device failure, which requires redundant devices to be installed in parallel with the active infrastructure to be activated in case of the active device failure or the access points to be placed in a manner which provides redundant coverage. Without such additional measures, failure of AP will quickly result in disconnected stations – as shown in Fig. 44 to Fig. 46, leaving less than 15% stations connected when only a single AP per considered system remains.

Of the mentioned methods of providing redundancy the former directly results in inefficient hardware resource utilization, as with such active-passive redundancy approach a high number of installed devices is always inactive. Unfortunately, the latter solution is also not without drawbacks, as concentration of an increased number of access points over the specific area increases the available transmission resources of the network only as long as they are able to operate using orthogonal frequency channels, and the number of such channels in ISM bands is strictly limited. In

other cases transmissions of clients connected to different APs will need to contend for channel access. Combined with a long time required for the wireless client to recover from the AP failure (even when an alternative is available) and a lack of IEEE 802.11 mechanisms dedicated to provide failover functionality for access point, make this standard significantly inefficient in widely understood resource management in situations for which the network has not been predesigned.

Apart from the above characteristics related to placement of infrastructure devices and related coverage issues, we should remember that in IEEE 802.11 PtMP mode (called infrastructure mode) an AP is required not only for communication with external network (through the DS and portal), but also for communication between clients in the same network. In the infrastructure mode, the AP operates as an immediate forwarding station even when communicating STA are in mutual communication range, thereby converting the 1-hop PtMP network into a 2-hop structure. The adverse effect of such operation can be seen in STA-to-STA scenarios presented in this chapter. While there are standardized mechanisms able to eliminate this inefficiency, such as the ad-hoc mode (2.2) or Direct Link Protocol (2.5.4.3), they are either not widely implemented (the latter) or their operation remains unstable due to both design and implementation issues (the former).
The analysis of an evolution of IEEE 802.11 standard indicates, that multiple management-related mechanisms have been defined following the IEEE 802.11-2007 standard revision (IEEE 802.11k [6], IEEE 802.11v [7], IEEE 802.11u [9], IEEE 802.11r [8]), and thus are present as elements of the current IEEE 802.11-2012 revision. However, their adoption in wireless device implementations available on the market are strictly limited. The situation reminds that related to the IEEE 802.11e [32] specification, from which only few selected elements have ever been implemented in practice (such as Block Ack and power saving mechanisms), while other exist only theoretically (for example HCF and admission control).

3 IEEE 802.11 Wireless Mesh Networking

The document providing specifications of Wireless Mesh Network (WMN) mechanisms necessary to introduce a mesh mode to the popular IEEE 802.11 WLAN standard is designed:
STANDARD for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 10: Mesh Networking.
At the time of writing this thesis, the current version of the above document is an IEEE 802.11s-2011. It is an amendment to the base IEEE 802.11-2007 standard, describing modifications to wireless LAN medium access control (MAC) and physical layer (PHY) specifications, necessary to support mesh networking in IEEE 802.11-based WLAN environment.
According to IEEE 802.11 Task Group S initial declarations, the purpose of the document is to define a IEEE 802.11 Mesh Basic Service Set using the IEEE 802.11 MAC/PHY layers that supports both group addressed and unicast delivery over self-configuring multihop topologies [69], providing data transmission capabilities at ISO-OSI layer 2 (data link layer).

When analyzing the above definitions, we should remember that the IEEE 802.11-2007 standard has been extended and modified by a considerable number of amendments to date, so for the purpose of defining mesh extensions, the authors of the current IEEE 802.11s specification assumed, that by the base standard we understand the following set of specifications:

- IEEE P802.11-2007 [70] – The current base standard for IEEE 802.11 networks. Includes amendments a, b, d, e, g, h, i & j.
- IEEE P802.11k-2008 [6] – Radio resource measurement enhancements.
- IEEE P802.11r-2008 [8] – Fast BSS transition.
- IEEE P802.11y-2008 [71] – 3650–3700 MHz Operation in the U.S.
- IEEE P802.11w [72] – Protected Management Frames.
- IEEE P802.11z [73] – Extensions to Direct Link Setup.
- IEEE P802.11p [74] – WAVE - Wireless Access for the Vehicular Environment.
- IEEE P802.11v [7] – Wireless network management.
- IEEE P802.11u [9] – Interworking with non-802 networks.

As we can see, the new mesh specification is aimed to utilize, or at least coexist, with the all mechanisms available for the IEEE 802.11 standard both currently and in the future.

In the following sections of this chapter, the overall description of Wireless Mesh Networks will be provided along with their popular usage scenarios. The overview of IEEE 802.11s as a WMN will then commence the part dedicated to description of specific mechanisms of this technology.
This description is divided into two parts: the overall information regarding mesh mechanisms introduced by the IEEE 802.11s amendment [11] and specific description of these of its mechanisms which are particularly important to the subject of this thesis (3.4 - 3.8) and proposed modifications of the standard.
The chapter is concluded with simulation and experimental results concerning the efficiency of IEEE 802.11s mesh operation while handling the multimedia traffic (3.8.4) in network topologies generated according to several method reflecting its probable usage scenarios.

3.1 Wireless Mesh Networks (WMNs)

The definition of Wireless Mesh Network (WMN) clearly indicates that such entity is capable of performing transmissions in a multihop manner, consecutively forwarding data units over a number

of wireless links. It is also widely understood that WMN network should possess some degree of automation regarding creation and maintenance of its network structure. However, apart from these well recognized features, the specific characteristics of a WMN and its relation to other types of non-PtMP wireless system is not uniform across various sources.
In particular the relation of Wireless Mesh Networks (WMNs) to wireless ad-hoc networks, Mobile Ad-hoc Networks (MANET) and Wireless Sensor Networks are often a subject to change depending on the source.
To prevent the possible misunderstanding, the term Wireless Mesh Network is used in this thesis to describe a network of following characteristics:

- utilizes a broadband wireless transmission technology of Wireless Personal Area Network, Wireless Local Area Network or Wireless Metropolitan Area Network class,
- the mechanisms necessary for creation of the network structure and its maintenance are capable of unsupervised operation following an initial configuration not exceeding in its complexity the configuration needed in case of popular PtMP WLAN systems,
- is capable of performing a multihop traffic delivery, using data transmission paths discovered automatically by appropriate network mechanisms,
- the conservation of node's computational and power resources is not of high importance,
- node mobility, while possible, is not an inherent trait of the system and thus is not likely to be specifically addressed by presence of dedicated mobility management mechanisms,
- should be capable of integrating with external network systems utilizing popular link layer and network layer protocol to perform an inter-network traffic delivery,
- the system is intended to provide a general purpose network connectivity, not specifically optimized for a single or a specific group of services.

As such, the WMN can be seen as a specific type of MANET, which is often used as a general term indicating a self-organizing and self-maintaining network which is capable of automatically adapting to significant and rapid changes in its structure. However it should be clear, that the WMN is not specifically designed to accommodate the nodes with a very significant degree of mobility relative to WMN structure and requirement of seamless communication during the process.
At the same time, the WMNs can be expected to be significantly different from Wireless Sensor Networks, which are designed with efficient support of data acquisition services in mind, resulting in frequent presence of strong assumptions concerning the type of network traffic (for example, a strongly unsymmetrical traffic flows, from sensors to a specified collecting node, low throughput), importance of power conservation (with node/network lifetime on battery power being a parameter of high importance, and with possible presence of energy harvesting mechanisms) and often inherently cross-layer design incapable of supporting general purpose network and transport protocols.
While the WMNs are capable of creating and maintaining spontaneous network systems, referring to them as ad-hoc networks should be avoided, to prevent confusion with an ad-hoc mode of the popular IEEE 802.11 technology, incapable of supporting a multihop communication scenario.

Wireless Mesh Networks as defined above are able to offer a number of advantages when deployed in correct manner. The most significant of these include many properties of an autonomic network system and benefits in coverage area and quality:

- Self-organization - the network creation is highly automated, which allows the mesh of wireless connections between a potentially high number of participating nodes to be created and maintained without user intervention. Moreover, multihop transmission paths are created and maintained by internal WMN mechanisms and can be selected according to variety of requirements,
- Self-configuration – despite the fact, that WMN presents a much more complicated network and protocol structure then the classic PtMP access networks utilizing infrastructure-based

Access Points (APs), the initial WMN client configuration is potentially less complicated for the user, due to robust link establishment mechanisms. The possible configuration changes required after the initial connection are most often handled fully automatically,

- Self-healing – with a high number of mesh links available, the WMN can provide a high degree of redundancy in transmission path selection. Combined with specialized path maintenance mechanisms, capable of reacting to path failures, there is a very high probability of maintaining the transmission in case of unpredicted events.
- Self-optimization – with the network structure and traffic conditions being subject to possibly severe and unpredicted changes, WMN mechanisms are capable of performing an event-based or periodic path rediscovery to take such changes into account, by altering the layout of data transmission paths through the network,
- Self-management – with a number of necessary mechanisms and their level of complexity being higher in case of WMN compared to classic PtMP access networks, there is a need to integrate these elements without introducing additional management tasks for the user to perform,
- Blanket coverage – due to any node being able to provide connectivity for a newly connected nodes, the area over which the WMN is deployed will most likely to exhibit a full signal coverage without any coverage holes due to unpredicted propagation conditions or difficulties in deploying the infrastructure,
- Limited need for infrastructure – when external connectivity in not required the WMN can provide coverage without the need for any kind of operator provided infrastructure, and even with external connectivity requirement the need for infrastructure is greatly limited,
- Mobility support – the fact that the client can simultaneously maintain wireless links to multiple neighboring WMN nodes allows for soft-handover operation. However WMN procedures are rarely include specific optimizations for handling seamless mobility.

However, the multihop transmission in erratic wireless environment, unpredictability of the network structure changes and the complexity of mechanisms required for WMN to operate create a number of serious drawbacks:

- Intra-path interference – use of multihop transmission paths requires transit nodes to retransmit the data which they have received as soon as possible. When orthogonal channels are not available for consecutive hops on the transmission path, the incoming and outgoing transmissions will need to share the same transmission medium, leading to intra-path interference at each such transit node. As a result, shorter mesh paths (in terms of number of hops) are generally more likely to provide adequate values of QoS parameters.
- Inter-path interference – the interference is also possible between two different transmission paths, if they have been established in each other's interference range. Due to changing network structure and dynamic manner of data transmission path discovery, the inter-path interference is much more difficult to predict then the intra-path interference, while its impact tends to influence a sizable area of the network. Sorter (in terms of their spatial length) and more spatially separated mesh paths are generally preferred for limiting the inter-path interference.
- Unplanned, changing network structure – with the network structure created dynamically and being subject to unpredictable changes, the possibility of performing a network optimization process is very limited. Moreover, the need to discover paths through the mesh structure for purposes of data transmission and both intra-path and inter-path interference dependent on their specific layouts, the fact network structure itself is likely to be modified can lead to changes in QoS characteristics of data transmissions or even to temporary losses of connectivity,
- Need for distributed method for medium access – with the nodes of the network forming a peer-to-peer mesh structure, without a selected node acting as a coordinator, the possibility

of introducing a controlled channel access is limited. There is a number of proposed solution available, but in case of client-based, self-organizing mesh networks such solutions are rarely employed due to a complicated implementation and potential instabilities in changing environment,

- Unpredictable traffic conditions – with the difficulties listed above, it is evident that each traffic flow within the mesh will significantly impact a number of others in a fashion which is difficult to predict.
- Dependence on client devices – as the communication within the WMN is likely to be dependent on client devices performing the role of transit network nodes, it is imperative for such devices to operate strictly according to WMN specification. However, apart from the possibility of encountering faulty implementations of WMN mechanisms, it should also be noted it is rarely to a direct advantage of a node to forward a transit traffic. In this situation it is possible that we can encounter disruptions to the WMN operation caused by both unintended and deliberate divergences from the standard.
- Complexity of required mechanisms – the complexity of network mechanisms required for WMN operation can be roughly estimated as complete set of ISO-OSI layer 1-3 mechanisms, accompanied with a significant set of support and management solutions, such as dynamic routing and Authentication, Authorization and Accounting (AAA). The fully functional implementation of the WMN can be expected to be a complex task.

From the above summarization of the WMN advantages and drawbacks it is evident that while the former are considerable, the WMN deployment needs to be preceded by an appropriate planning aiming to take the maximum advantage of strong points of a particular WMN technology while minimizing the impact of its drawbacks.
The most common use cases are described below, and while the specifics of a deployment will change from cast to case and with each different WMN technology. If there is a general rule, it will be to minimize the length of transmission paths within the WMN system.

3.1.1 Wireless Mesh Network usage scenarios

Wireless Mesh Network, as defined above, can still describe a number of significantly different network types employing mechanisms and technologies based on different design principles.

The type which is currently most often employed in production grade systems is a pre-designed mesh network. Such mesh network consists of operator installed devices and is most often employed as a distribution network. The fact that all devices within such mesh are under operator's control allows for the system to be constructed to fulfill specific design parameters, such as required throughput or redundancy level, while minimizing the wireless mesh disadvantages (for example, intra-path interference). At the same time, the mesh-specific mechanisms remain available to provide a high degree of self-management, self-optimization and self-healing capability. Wireless transmission technologies used in such networks are range from high-end implementations of popular WLAN technologies, through WMAN solutions, ending with relatively rare point-to-point microwave links.
Client-client operated devices are not directly connected to the WMN of this type, but a dedicated access network technology is employed for that purpose, interconnected with the distribution WMN by dedicated gateway devices.
This type of the WMN environment is to be considered the most deterministic of them all, additionally allowing the use of optimization procedures based on general network knowledge.

The radically different approach to network creation is taken in case of spontaneous client-based mesh networks. In this case the mesh network structure is constructed using exclusively client operated devices, taking advantage of the self-organization, auto-configuration and self-

management capabilities provided by WMN mechanisms. The ability to create and operate a multihop network without any pre-deployed infrastructure makes such type of WMN a very useful solution for specific deployment scenarios, such as emergency communication systems, military short range communication, ad-hoc user groups etc. However dependency on the client devices also makes this type of network a highly non-deterministic environment, combining a considerable list of hard to predict effects, such as: unpredictable structure changes (due to device movement or its sudden activation/deactivation), propagation conditions changes combined with relatively simple radio hardware available at client devices, resulting transmission path modifications, inability to ensure standard compliance etc.
The ability to successfully employ a specific high layer service in such environment can be difficult to predict, and use of services designed to accommodate unpredictable QoS scenarios is advised.

However, the WMN based exclusively on client devices is rarely employed without any point of contact with external networks. While currently not as popular as pre-designed distribution networks, the access network combining a limited operator provided infrastructure with client-based WMN network is an interesting solution, worthy of popularization, as it can easily provide a number of advantages over the classic PtMP access solutions, as long as the length of its transmission paths can be kept relatively short. The possible advantages of a short-path access WMN can include:

- coverage being both more through (lacking unpredictable coverage holes) and extended in range with no additional infrastructure investments,
- capacity of the access network (understood as a number of clients) being significantly extended without additional, operator provided access devices,
- ability to recover from failures of infrastructure access points and from degrading propagation conditions,
- support for client mobility, as moving client will retain its identity through the WMN and its active communication sessions will be maintained by use of procedures similar to a soft-handover,
- minimization of infrastructure requirements – as each connected client serves as a pint of access for new clients, most of the coverage can be expected to be provided in such way. That allows minimization of a number of infrastructure access points, which could become dependent more on the traffic volume to be exchanged between client and infrastructure, then on the intended coverage area,
- easier client configuration and management – the client simply needs to be configured to access the WMN (which is a simple procedure from the user's point of view), to obtain support of WMN's management mechanisms in further maintaining its configuration,
- ease of network extension and self-extension – the network can be easily extended with minimum infrastructure investment or can even be counted on to naturally extend its coverage and capacity with the influx of clients.

Apart from the role of an general access network, the client-based WMN with infrastructure support can also be employed in a number of more specialized systems. The following usage scenarios can serve as frequent examples.

Home/building/industry automation – with its capability for self-organization, auto-configuration and self-healing, the WMN is a very good solution for automation networks. The ability to provide redundant, failure resistant, automatically configuring and extending network connectivity between multiple automation devices dispersed in a home, office building or industrial space is an enabler functionality for such applications. However, is there are strict delay-related requirements placed by the applications, the WMN may not be able to fulfill them reliably. The example of a solution dedicated for such environment is a ZigBee technology [76].

Environmental monitoring – with multitude of sensors dispersed over a considerable area (especially one without existing communication infrastructure), the requirement to build a dedicated infrastructure to provide them with network connectivity is not feasible. The WMN can provide such connectivity by means of multihop transmission. However, this application is more often a task for WSN instead if WMN, except the scenarios where high bandwidth, diversity of applications or more symmetric traffic flows then expected in WSN are encountered. It should also be noted, that the currently most popular method of providing connectivity for such sensors in an urbanized environment depends on use of PtMP Wireless Wide Area Network (WWAN) access, such as GSM, UMTS and LTE.

Advanced Metering Infrastructure – which can be seen as a specific case of the monitoring scenario, however the expected high number and density of metering devices makes the use of direct connectivity to external operator provided WWAN infeasible. Due to these characteristics, the AMI infrastructure (Fig. 47) often includes a WMN network providing connectivity between end-user devices and an aggregating device, which in turn employs a single WWAN connection to a processing and control center.

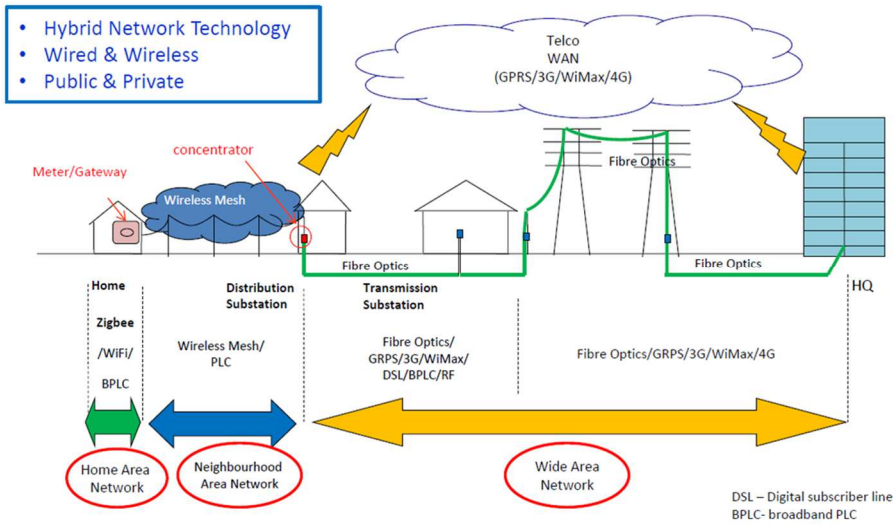

Fig. 47 An example AMI architecture [77]

Internet of Things (IoT) – as the IoT systems are beginning to emerge in practice, the WMN solutions seem to be considered for use in this environment (currently utilizing mainly PtMP communication model for end-devices) due to universality of their possible usage. However, advanced power conservation mechanisms are expected to be an enabler of WMN use in this environment.

Access integration network – with a number of access technologies available to a group of clients, each with its own advantages and limitations, it is possible to employ a WMN as an integrating network (Fig. 48), allowing sharing of available network connections within a group of users. Such solution allows for increased reliability of access and changing the access link based on service requirements and the current traffic conditions.

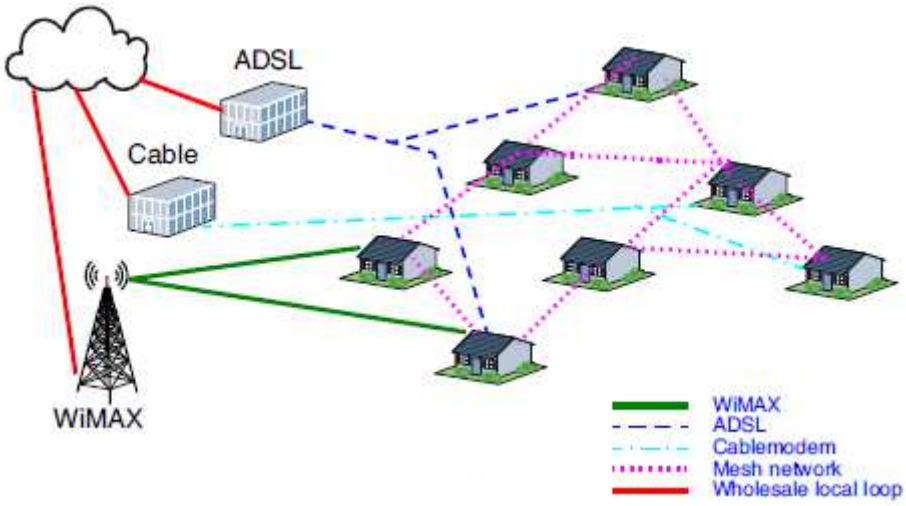

Fig. 48 WMN access integration network example

Military and emergency communication – despite the fact that military and emergency communication scenario has already been mentioned as examples of isolated WMN use, their most common deployment scenario also includes integration with external networks when they are available (Fig. 49). The use of WMN (instead of direct use of a long range communication technology) allows for power saving, easily portable hardware, lower probability of signal interception and scalability of the resulting communication system.

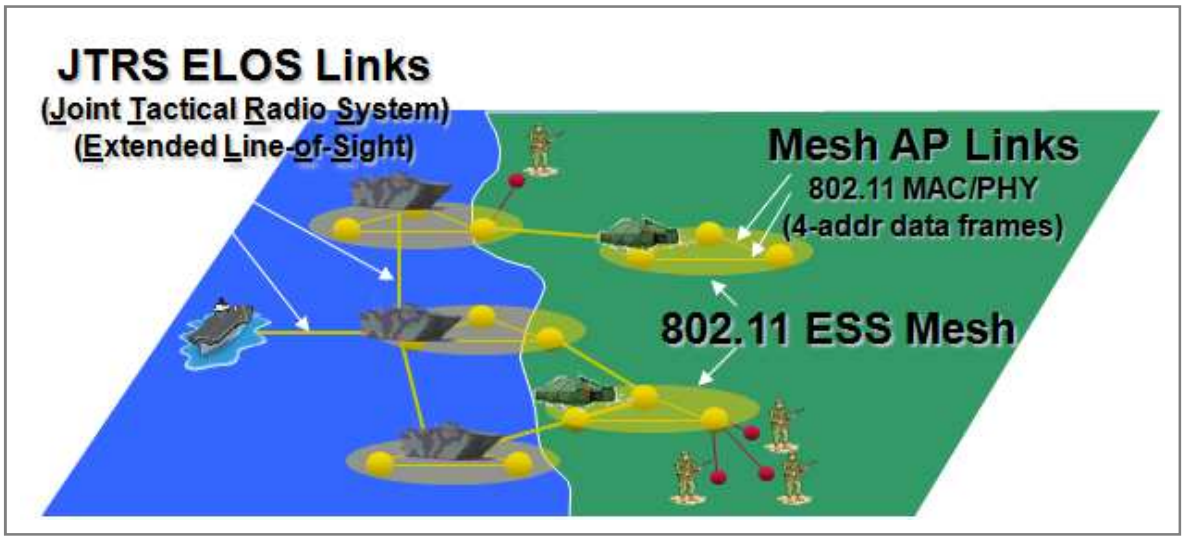

Fig. 49 An example military WMN deployment scenario [78]

5th Generation Networks (5G) – with the ubiquity of broadband network access aim clearly present in the 5G descriptions and specifications, the WMN solutions are specifically listed as one of the technologies to employ to fulfil that purpose.

From the above preview of popular WMN deployment scenarios it is evident that one of the most important functionalities of such network technology should be the ability to function as a part of a compound network system and exchange traffic with external networks. Additionally, it can also be seen, that we can expect to encounter both service clients and providers within the MWN network.

3.1.2 The IEEE 802.11s system as a Wireless Mesh Network

The IEEE 802.11s specification offers a comprehensive set of mechanisms necessary to operate an WMN network based on the IEEE 802.11 wireless technology. Moreover, it also integrates the WMN mechanisms with the existing IEEE 802.11 solutions, making them an integral (though optional) part of the standard – the third mode of operation defined for an IEEE 802.11 wireless interface, apart from the most common PtMP infrastructure mode and the rarely used and usually poorly implemented ad-hoc mode.

The IEEE 802.11s specification defines a self-contained set of mechanisms sufficient to create and maintain a client-based WMN system, operating at ISO-OSI layer 2 (data link layer) and capable of exchanging traffic with external ISO-OSI layer 2 network systems, including the widely popular Ethernet networks.

In keeping with the fact, that the mesh capabilities have been introduced into the IEEE 802.11 standard as one of possible operation modes of a wireless interface, the IEEE 802.11s amendment retains the ability to create and participate in the Mesh Basic Service Set (MBSS) for devices equipped with a single IEEE 802.11 interface. Due to this design decision, the IEEE 802.11s MBSS is a single channel network (as concurrent use of multiple frequency channels implicates the presence of multiple physical IEEE 802.11 interfaces), where all transmissions are conducted with use of the same RF channel shared between all stations in the network.
This is a serious limitation compared to a theoretically possible WMNs with a multichannel capability, able to concurrently use different (orthogonal) frequency channels for communication between different mesh node pairs at the same time, thereby providing the WMN with access to a vastly increased transmission resource pool and reducing intra-mesh interference.
However, in case of a self-organizing WMN network, intended to make use of client devices to create its structure, it has been decided that additional complexity of the necessary mechanisms could easily lead to both implementation and operation difficulties, hindering its popularization process and making its operation unstable in a highly nondeterministic environment of the ISM RF band. Thus the Common Channel Framework mechanism proposed in IEEE 802.11s draft specification and allowing per-frame transmission channel switching has been left out of the final specification.

Recognizing the importance of interworking in WMN usage scenarios, the design of the IEEE 802.11s mechanisms aims to provide a high level of compatibility with both external networks and higher layer protocols and services. The compatibility with external networks is obtained by isolating its internal mechanism operation from the outside systems and presenting the mesh network as an IEEE 802.1D-compliant [79] Local Area Network (LAN). Similar approach it taken regarding compatibility with higher layer mechanisms – by adopting a strictly layered approach, isolating internal mesh mechanisms and presenting the mesh network as a standard LAN interface.
Such black-box approach allows for a deployment of the IEEE 802.11s mesh into a compound Bridged Network (as defined in IEEE 802.1D and described in 3.8.3) to be an uncomplicated procedure, but can also impose considerable limitations regarding scalability of the mesh network (as described in 6).

In overall, the comprehensiveness of IEEE 802.11s mesh mechanisms make it capable of being employed in most of the usage scenarios described earlier, including the most challenging client-based, self-organizing network with interworking support. At the same time, its single channel operation and strict connection with IEEE 802.11 transmission technology (operating in unlicensed ISM frequency bands) makes it relatively poorly suited for pre-design distribution systems. However, it should be noted, that such systems often utilize selected IEEE 802.11s management mechanisms combined with other transmission technologies, for example products of a well-known Mikrotik

company [80] employ a slightly modified IEEE 802.11s path selection mechanisms with TDMA medium access.
Review of the IEEE 802.11s specification and other published WMN standards seems to indicate that the specification is the most comprehensive one available, outdistancing solutions described in IEEE 802.16 [75] and ZigBee [76] specifications.
The subsequent sections of this chapter will provide a general overview of the IEEE 802.11s architecture and its composing mechanisms. This overall description is followed by a detailed description of IEEE 802.11s mechanisms being relevant to the new, cross-layer mechanisms proposed in this thesis.
The descriptions of several methods which can be used to generate IEEE 802.11s mesh network topologies reflecting its most probable usage scenarios are described next. The chapter is concluded with a performance assessment of the standard IEEE 802.11s mechanisms in network topologies generated according to the described methods.

3.2 IEEE 802.11s overall architecture

The IEEE 802.11s standard amendment defines a new IEEE 802.11 structural entity – Mesh Basic Service Set (MBSS) – as a single set of independent mesh stations forming a self-contained network. A basic element of IEEE 802.11s mesh network is a mesh station (mesh STA). It is an IEEE 802.11 QoS STA, which supports mesh services necessary to participate in wireless mesh network (see 3.3) and a subset of QoS functionality defined in IEEE 802.11e extension:

- use of QoS frame format,
- EDCA medium access (which is a part of Mesh Coordination Function – MCF).

Optionally a block and no acknowledgement can be supported.
Mesh STA does not support a number of more advanced IEEE 802.11e mechanisms, such as:

- HCCA medium access,
- Traffic specifications (TSPEC) and traffic stream management (TS),
- admission control,
- Automated power save delivery (APSD),
- (Tunneled) Direct link setup (DLS/TDLS).

In some cases this lack of support is a logical result of different network structure (APSD, DLS/TDLS), but in others (HCCA, TSPEC, TS, Admission control) it is simply a result of an inclination to simplify the mesh STA. While an understandable trend from commercial point of view, lack of more advanced QoS-related functionality in its basic building blocks does not favorably impact an ability of MBSS to reliably provide multimedia services.

To form MBSS mesh structures, wireless mesh stations establish peer links with their mesh-capable physical neighbors, creating a network structure of linked mesh stations.
Furthermore, in a mesh network, messages can be delivered between stations which are not in direct communication with each other. It is possible by using multihop transmission over the abovementioned peer link structure. As far as data delivery is concerned, all stations in the same MBSS can be considered to be connected at ISO-OSI layer 2. The described ability clearly indicates, that a given mesh station can be not only a source or sink, as is the case in classic IEEE 802.11 BSS/IBSS, but also a forwarder of network traffic.

The ability to provide layer 2 communication between all mesh STA within an MBSS results in introduction of the concept of MBSS LAN, as an IEEE 802.11s MBSS is perceived by higher layer entities as a single layer 2 network, with functionality of a classic, wired LAN. Internal structure of MBSS is intentionally hidden from higher layers.

A mesh station connected to a particular MBSS can communicate with all stations in the same MBSS, but not with destinations located outside its boundaries. To provide mesh STAs with connectivity outside their MBSS a distribution system must be used, in a manner analogue to the one employed in case of classic IEEE 802.11 network.
To allow MBSS elements to utilize distribution system for external communication, a dedicated mesh stations, called mesh gates, are defined, which include both mesh and DS functionality. Their presence allows mesh stations belonging to a given MBSS to communicate with IEEE 802.11 entities outside its boundaries – for example: mesh stations belonging to other MBSS or classic IEEE 802.11 BSS networks (Fig. 50).

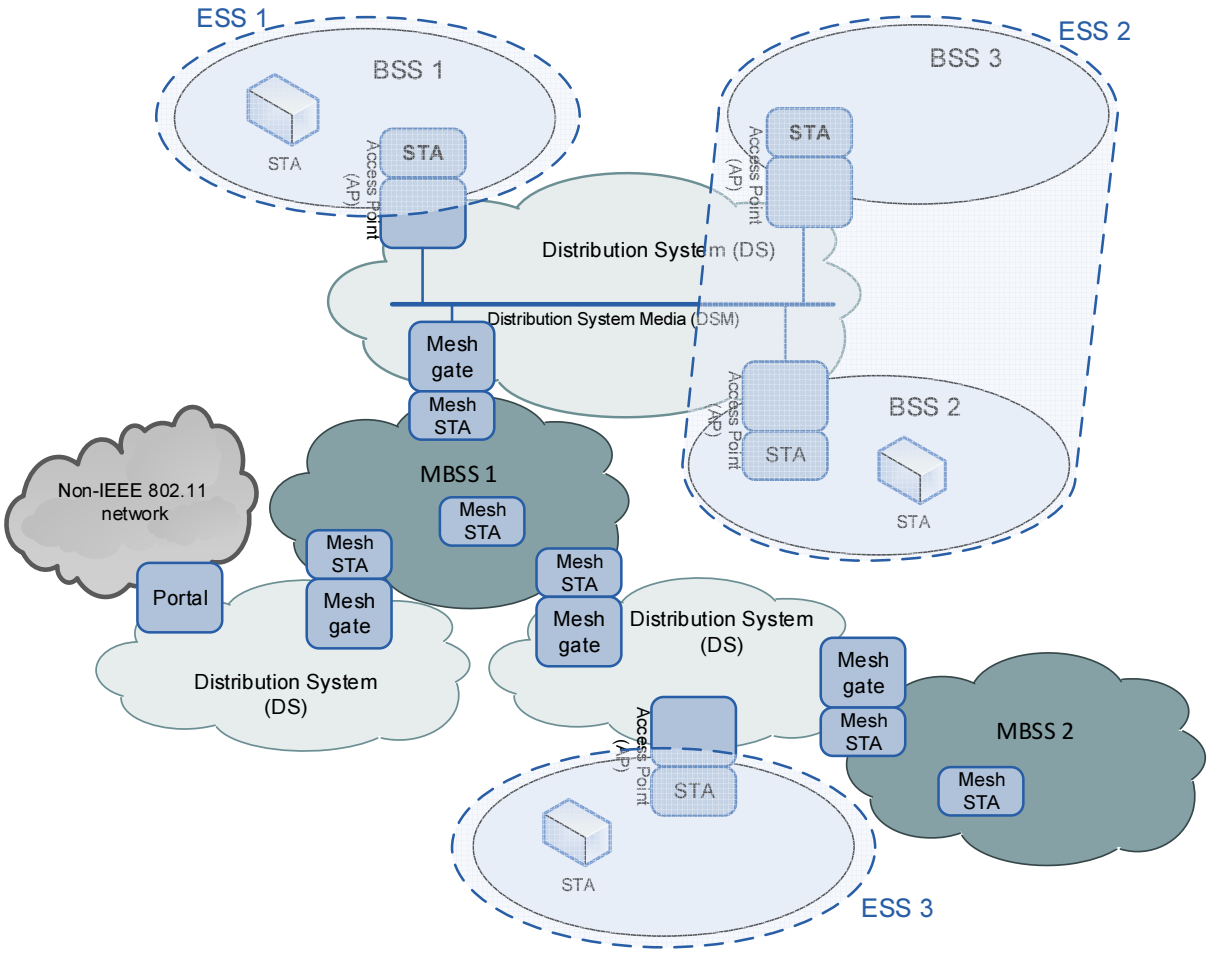

Fig. 50 IEEE 802.11s network architecture elements

The distribution system can be used to provide communication between IEEE 802.11-compliant entities, but to connect such entity (a mesh network for example) to non-IEEE 802.11 network (which utilizes different layer 2 technology), a portal entity must be employed.
Portal is an element, which allows communication between IEEE 802.11 DS and network utilizing different technology, for example popular IEEE 802.3-based solutions.

From the above description, it is evident that, while the MBSS itself is a completely new and complex element, base IEEE 802.11 system architecture, use of distribution system to connect IEEE 802.11 networks and use of portals to interact with different layer 2 technology networks is not changed compared to classic IEEE 802.11 standard.

It should be noted, however, that the complexity of MBSS internal mechanisms and protocols requires a much more complex entity at its point of contact with DS. In case of classic IEEE 802.11 BSS, a comparatively simple access point (AP) has been employed, while in case of MBSS a mesh gate must be used – a much more universal and complex entity. The complexity is partly a result of necessity to fully participate in internal MBSS operation, but is also affected by the fact, that complex MBSS network structure can have multiple points of contact with a single or multiple distribution systems.

It is possible to combine functions of mesh gate, portal and access point in a single device, which can also include, in that case, a self-sufficient DS.
A device used to connect mesh network to a wired (for example: Ethernet-based) infrastructure, will incorporate the compound architecture depicted in Fig. 51, which includes mesh gate, self-sufficient DS and portal.

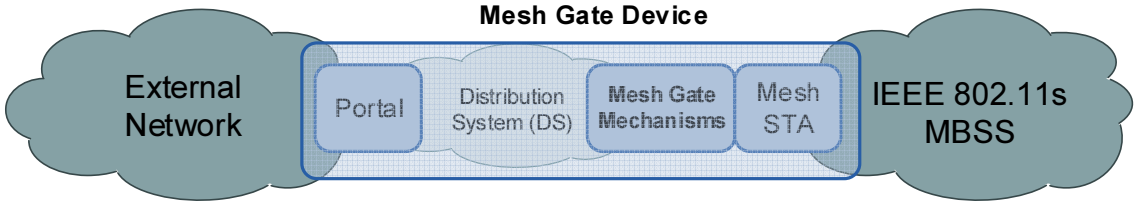

Fig. 51 Mesh gate device connecting MBSS to an external network

Another popular scenario connectivity scenario requires an ability to provide classic IEEE 802.11 stations with network connectivity using wireless mesh. In such case a device consisting of a mesh gate, distribution system and access point can be used (Fig. 52).

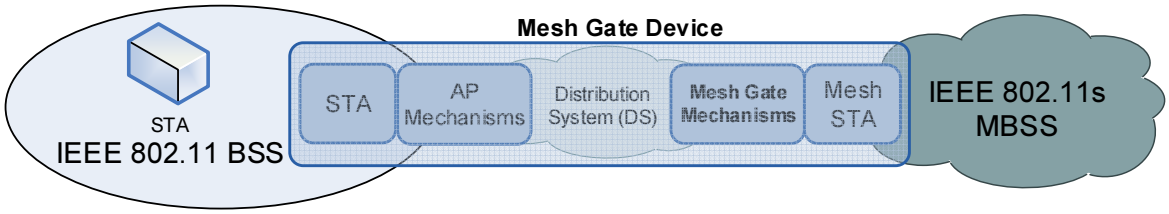

Fig. 52 Mesh gate device providing standard IEEE 802.11 BSS services

Of course, it is also possible for a mesh gate to connect two independent IEEE 802.11s MBSS mesh structures as shown in Fig. 53.

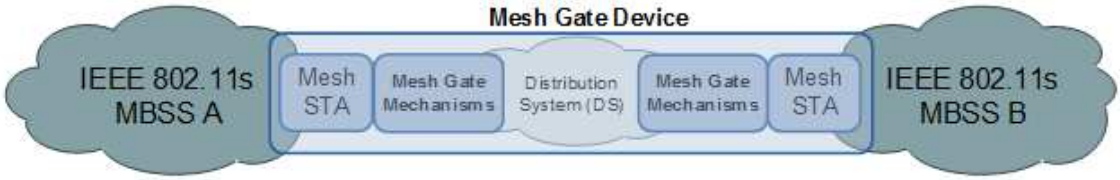

Fig. 53 Mesh gate device connecting two IEEE 802.11s MBSS networks.

3.3 Overview of mesh services

In similar way as Distribution System Services and Station Services are defined in a base IEEE 802.11 standard, an IEEE 802.11s extension defines additional mesh services which are necessary to provide MBSS functionality. Not all of the defined mesh services are obligatory, as some provide functionality which is considered optional by IEEE 802.11s extension.

The list of defined mesh services include:

- Mesh discovery,
- Mesh peering management,
- Mesh security,
- Mesh beaconing and synchronization,
- Mesh coordination function,
- Mesh power management,
- Mesh channel switching,
- MBSS addressing,
- Mesh path selection and forwarding,
- Interworking with external networks,
- Intra-mesh congestion control,
- Emergency service support in MBSS.

Sort descriptions of these services are provided below, while the following sections will describe mechanisms particularly important to the main subject of this thesis in detail.

3.3.1 Mesh discovery

To allow wireless stations to detect the presence of mesh MBSS and its building mesh stations, each of such stations transmits Beacon frames periodically, which is a basis of passive method of mesh detection.
Also, each of MBSS stations respond to Probe Request management frames with Probe Response messages, which allows stations to perform mesh discovery in active manner.
The described method closely corresponds to BSS/IBSS discovery procedure, but in our case there are two differences.
The first is presence of Mesh ID element in Beacon and Probe Response management frames, which contains mesh-related information.
The second is the necessity for all mesh STAs to transmit Beacon frames and respond to Probe Requests. Such approach is required, because STA wishing to participate in MBSS must choose a set of particular MBSS stations, with which it will attempt to establish peer relationship. To do that, STA need information about all mesh STAs in its physical neighborhood and their mesh-related capabilities (such as current ability to create new peer relationships or lack thereof).
In case of infrastructure BSS, which is a centrally coordinated network, these tasks could safely be conducted by an access point. In case of distributed IBSS, an optimized, distributed scheme has been employed, based on the fact, that only the presence of IBSS itself needed to be advertised, not the presence of particular participating stations.

3.3.2 Mesh peering management

Within an MBSS two mesh STA can communicate directly only if they have a common peer relationship. After mesh discovery, a STA wishing to participate in MBSS need to create such relationship with one or more mesh STA, from a target MBSS.
To do this, STA employs mesh peering management functions, which are used to create, maintain and close peerings between mesh STAs.

3.3.3 Mesh security

Security functions for MBSS defined in IEEE 802.11s extension allow mutual authentication of mesh STA pairs which are to create peer relationships. Security protocols perform STA authentication and create a common pairwise master key (PMK) for a specific peering. That key is then used by authenticated mesh peering exchange protocol to establish an authenticated peering and derive session keys to be used for transmission security mechanisms.

3.3.4 Mesh beaconing and synchronization

The discussed mesh standard introduces an extensible synchronization framework, which allows the use of any synchronization method supported by all MBSS stations, thereby providing means to seamlessly introduce solutions to meet specific application requirements. For a method to be used, all stations within a MBSS must support it – if a station is not compliant with currently active method it cannot establish peer relation with STA of a given MBSS.
The information about active synchronization method is included in Mesh ID element, which provides this information to candidate stations early during mesh discovery phase.
A neighbor offset synchronization method is defined as a default solution, and must be supported if a STA is to be considered IEEE 802.11s compliant. If it is used, a given STA maintains time offsets between their own internal timer, and timers of all STAs with which it maintains synchronization and employs clock drift adjustment procedures to update its own timer. The method is based on exchange of timestamps in periodically transmitted Beacon and Probe Response Management frames.
It is worthy to note, that a given STA can maintain synchronization not only with its peer neighbors, but also with physical neighbors outside its current MBSS. This possibility allows for an efficient Beacon collision avoidance (MBCA) and coordinated channel access (MCCA), which must take into account all STAs contending to use a shared transmission medium.

Synchronization functions are employed by a number of mesh mechanisms, including:

- Mesh power management,
- Mesh coordinated channel access (MCCA – an optional element of Mesh coordination function),
- Mesh beacon collision avoidance (MBCA).

Two former functions are described separately as they are simply recipients of synchronization services. MCBA on the other hand is closely related to synchronization function, as it affects periodic sending of Beacon frames.
Mesh Beacon Collision Avoidance (MBCA) addresses the problem of highly probably Beacon frame collisions between physically neighboring stations in 2-hop neighborhood. As described in 3.3.1, all stations in MBSS (in contrast with BSS/IBSS networks) are required to periodically transmit such frames – crucial mesh functions: discovery and synchronization are dependent on this behavior.
Such high number of intra-MBSS Beacon frame sources, combined with possible hidden station effect and uniform Beacon frame transmission interval within an MBSS, can lead to their high and consistent loss ratio. Moreover, outside sources of Beacon frames, such as other BSS, IBSS and MBSS networks raise probability of Bacon frame loss even higher.
Taking into account that discussed management frames are transmitted by means of unacknowledged broadcast, the described problem requires an efficient solution.

3.3.5 Mesh coordination function (MCF)

IEEE 802.11s is an extension of on IEEE 802.11-2007 standard and as such it is aware of medium access method defined there (see 2.5).
Of these access methods, however, PCF and HCCA cannot be effectively supported in mesh environment, as they require a central coordinator and provide controlled access in 1-hop neighborhood only.
The remaining, contention based access methods, DCF and EDCA could be employed. As there seems to be no advantage in employing non-QoS aware DCF, EDCA access method has been selected as default for IEEE 802.11s mesh networks.
Moreover, with an aim to optimize the efficiency of frame transmission, a new (optional) reservation-based access method has been introduced – Mesh controlled channel access (MCCA).
These two methods (EDCA and optional MCCA) form a compound medium access method for IEEE 802.11s-compliant mesh networks – Mesh coordination function (MCF).

3.3.6 Mesh power management

Mesh power management mechanisms aim to provide an energy saving functionality in MBSS environment.
Such functionality in WLAN-based IEEE 802.11s mesh is not as important as in case of other multihop networks (for example various sensor network technologies). The main aim of IEEE 802.11s mesh is to provide universal, robust, broadband connectivity for modern services, including transmission of multimedia content. It is assumed, that many mesh stations are in fact stationary devices, directly connected to wired power grid. However, the growing number and capabilities of mobile devices require that energy saving aspects of wireless transmission are addressed.

The basic procedure for sending frames to mesh stations which utilize power management is similar as in case of an IBSS – sending stations must buffer frames to be delivered to inactive station, until it activates. However, the task of ensuring that a given mesh STA will activate with appropriate frequency and informing its correspondents that it is active and ready to receive is more complicated than in case of classic BSS/IBSS networks.
The source of complication is an ability of a mesh STA to form multiple peer relations with its neighbors, as power saving level and current state for each peer link must be maintained separately. Moreover, as some mechanisms (for example MCCA, MBCA, mesh discovery and peering management) require interaction non-peer STAs, a power saving policy concerning these external entities must also be declared and executed.
Mesh STA can set one of three different activity levels for each peer links it maintains:

- Active mode – station will always be in Awake state,
- Light sleep mode – station can enter Doze state, but it must activate to receive all Beacon frames from a given peer,
- Deep sleep mode – station can enter Doze state, and it is permitted for it not to listen for Beacon frames from a given peer. It must only activate periodically to send its own Beacons (but with much lower frequency then in Active mode) and provide short activity time called Mesh awake window, to allow incoming communication.

For communication with non-peer STAs, possible options are limited to Active mode or Deep sleep.

With the above activity levels defined, station switches between Active and Doze states – the former meaning that STA is fully powered and functional, while the later represents energy saving state, when radio transceiver is powered off and no communication can take place. The sequence is determined by presence of so called Peer Service Periods (PSP).
PSP is a time interval during which a given STA should be ready to transmit or receive over a particular link. They can be initiated by any of the peers and the initiator is able to indicate which STA will be owner of PSP and thus able to use it for transmission. The other peer must remain in Active state and is only able to receive over the link during such PSP. The owner of PSP is able to terminate it at any moment.
To ovoid the necessity to transmit additional frames for purposes of PSP signaling, their initiation and termination is indicated by setting appropriate field values in headers of QoS Data or QoS Null frames.

Non-peer stations are treated with much lower priority, as a STA which maintains any of sleep levels (light or deep) for any of its peer links is considered to use Deep sleep level for non-peer stations. In such case, non-peer stations can only initiate communication with it during infrequent Mesh awake window.

3.3.7 Mesh channel switching

Discussed WLAN mesh standard defines a single channel mesh, where all wireless links between STAs in MBSS utilize the same frequency channel. It allows a significant simplification of mesh discovery,

peering management, synchronization and path selection mechanisms. It also makes a mesh network less aggressive in consuming radio frequency resources, as such self-configuring and automatically expanding network will only occupy a single channel – with ability to support multichannel link differentiation, mesh would display tendency to occupy all usable frequency channels while covering significant areas.
On the other hand, limitation to a single channel trends to radically limit mesh performance, due to both inter-path (between independent multihop transmission path) and intra-path (between subsequent hops on a single multihop path) interference.
Adverse effects of described intra-mesh interference can be minimized by use of various internal coordination mechanisms, starting from MCF, through appropriate path selection mechanisms and ending with intra-mesh congestion control. However, single channel operation makes mesh network susceptible to interference from external sources, which do not employ any coexistence procedures. In such situation it is imperative to be able to choose the best possible frequency channel for mesh MBSS and be able to dynamically change it, if the need arises.
The first of these tasks (channel selection) is considered to be outside the scope of IEEE 802.11s standard extension. Radio resource monitoring procedures though, are included as a part of IEEE 802.11k extension – part of a base IEEE 802.11-2007 specification. Their presence should provide ample information for channel selection algorithms, if a method of distributed metering would be defined.
The second task, global mesh frequency channel switching itself, has been addressed by IEEE 802.11s procedures. The functionality includes change of base frequency of the channel and its width between 20MHz and 40 MHz.
To perform the channel switch without disrupting operation of the mesh network and data transmission services provided to users, the switch must be scheduled in such way, that all mesh stations (including these utilizing power save procedures) are informed before its execution.
The need for a channel switch is propagated through a MBSS by sending Channel Switch Announcement multihop action frames to all mesh stations in a broadcast manner. Such frames contain Channel Switch Announcement and Channel Switch Parameters information elements, describing details of the planned channel change. The information includes the time remaining until channel change, which receiving stations use to schedule the event.
Moreover, after receiving the described action frame, mesh stations include the above information elements in Beacon and Probe response frames that they transmit, each time updating value of time remaining until channel switch. Such solution ensures, that all stations within MBSS are informed of planned channel switch, without introducing an excessive signaling traffic.
When the scheduled time is reached the switch is executed without disrupting peer relationships between mesh stations and with minimal disruption of data transmission service provided by the network.

3.3.8 MBSS addressing

As described before, an IEEE 802.11-2007 standard defines four address fields in its MAC header. The procedures concerning first three are precisely defined in the standard, but the use of the fourth one is not specified. With introduction of IEEE 802.11s multihop transmission capabilities, additional addressing procedures had to be defined. While Control frames and most of Management frames do not use multihop transmission and thus still require no more than 3 address fields, Data frames (carrying MAC Service Data Units – MSDUs) and Multihop category of Action Management frames (carrying MAC Management Protocol Data Units – MMPDU) may require as much as 6.

As only four address fields (Address 1 to Address 4) are located in standard IEEE 802.11-2007 MAC header, an extension of base frame structure (Mesh Control Field) needed to be defined to accommodate 3 remaining addresses.

It should be noted, that address 4 field present in standard IEEE 802.11-2007 MAC header only when ToDS and FromDS bits of Frame Control field are set (see 2.4.7) and its use is discouraged due to compatibility reasons described below.
For the detailed description of IEEE 802.11s mesh frame format please consult Section 3.4.

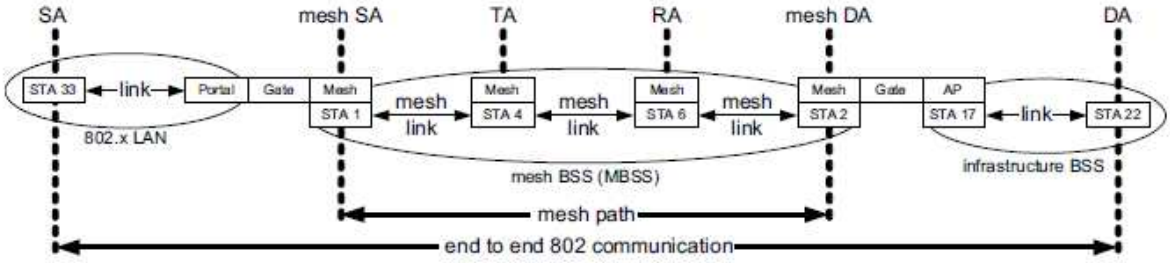

Fig. 54 Mesh address types and their significance areas

In case of unicast frames, addresses 1 and 2 describe endpoints of current transmission over a single wireless link: address 1 field holds receiver address (RA), while address 2 – transmitter address (TA). Address 3 and 4 fields describe endpoints of mesh path, describing its destination (address 3 – MDA) and source (address 4 – MSA) within current MBSS.
Address 5 and 6 fields are used in handling of traffic involving the use of mesh gateways – traffic originating and/or to be delivered to devices outside of current MBSS. In such cases these addresses describe end-to-end path: address 5 field contains final destination address (DA) and address 6 field – original frame source address (SA). It is worthy of note, that mesh stations do not need to interpret addresses 5 and 6, as they are able to forward the traffic within MBSS using only addresses 1-4. Addresses 5 and 6 are interpreted only by original source, final destination and mesh gateways.

In case of group addressed frames address field 1 contains destination group address, address field 2 have the same meaning as in case of unicast transmission (TA) and address 3 holds sender address within the MBSS. These three addresses are sufficient for MBSS-originated group addressed traffic.
If the group addressed frame originated from outside of MBSS, address field 4 needs to be used to indicate original frame sender (SA).

When the rules described above indicate the use of Address 4 field, we should remember that it should be located in one of two possible places: in standard IEEE 802.11-2007 MAC header or in Mesh Control field. The rules for Address 4 field placement are such that only unicast Mesh Data frames can place it in Address 4 field of an IEEE 802.11-2007 MAC header. All other frame types either do not use it (intra-MBSS group addressed frames) or should place Address 4 field in Mesh Control field (all inter-MBSS frames and group addressed multihop management frames).

Such decisions have been made for compatibility reasons – in base IEEE 802.11-2007 standard, usage of an Address 4 field located in a standard IEEE 802.11-2007 MAC header has not been defined, which resulted in multiple proprietary, incompatible solutions utilizing this field. In this situation authors of IEEE 802.11s extension decided to avoid its use if possible. With maximum of two additional address fields to be found in Mesh Control field, the only case when the use of a standard Address 4 field is necessary is an inter-MBSS unicast data frame – as it requires 6 address fields. However, apart from the mentioned frame type, also an unicast intra-MBSS data frame uses this solution. The only explanation that comes to mind is an intention to unify the structure of unicast data frames, regardless of their point of origin or destination.

Complete rules concerning the use of IEEE 802.11s address fields in multihop frames are presented in below.

Table 5 MBSS use of address fields (MCAE – number of Mesh Control Address Extension fields)

Supported frames	ToDS FromDS fields	MCAE	Address 1	Address 2	Address 3	Address 4 (MAC header)	Address 4 (Mesh Control)	Address 5	Address 6
Mesh Data (unicast)	1 1	-	RA	TA	DA = MDA	SA = MSA	-	-	-
Mesh Data (group addr.)	0 1	-	DA	TA	SA = MSA	-	-	-	-
Mesh Data (inter-MBSS unicast)	1 1	2	RA	TA	MDA	MSA	-	DA	SA
Mesh Data (inter-MBSS group addr.)	0 1	1	DA	TA	MSA	-	SA	-	-
Multihop Action (unicast)	0 0	1	RA	TA	DA = MDA	-	SA = MSA	-	-
Multihop Action (group addr.)	0 0	-	DA	TA	SA = MSA	-	-	-	-

One cannot fail to notice that rules concerning placement of Address 4 field are not easy to follow, but they seem to minimize the probability of conflict with proprietary solutions. However, the risk of such conflict has never been precisely assessed and seems to decrease with rapid disappearance of non-standard hardware from both the market and deployed systems.

3.3.9 Mesh path selection and forwarding

As the mesh network is to provide a multihop communication between stations, it is necessary to utilize path discovery mechanisms to select the most appropriate data paths between sending (MSA) and receiving (MDA) mesh stations.

The standard allows the use of custom mechanisms for the purpose, as long as all stations within an MBSS utilize the same mechanism. The information about path discovery mechanisms currently utilized within a given MBSS is provided in Mesh ID element in Beacon and Probe response frames, which allows candidate stations to decide if they are capable of connecting to such mesh network, early during mesh discovery phase.

While mesh devices can support many path discovery mechanisms, for reasons of compatibility there is one mandatory solution, which must be supported by all IEEE 802.11s compliant devices – Hybrid Wireless Mesh Protocol (HWMP). This path discovery protocol can simultaneously utilize both proactive and reactive path discovery mechanisms and uses a link metric to select the most appropriate path.

Reactive patch discovery sub-protocol used in HWMP is Radio Aware Ad-hoc On-demand Distance Vector (RA-AODV). It is a modification of well-known AODV [81] protocol. One of the most significant modifications is its ability to utilize link metric currently active in MBSS (by default – Airtime Metric mentioned below).

The proactive sub-protocol of HWMP is an optional element, which requires presence of a distinct mesh station, which performs role of root station. The station proceeds to employ Tree-Based Routing (TBR) protocol, to proactively create and maintain forwarding information in all MBSS stations, which allows them to communicate with such station.

Due to the fact, that it is highly probable that, in case of MBSS connected to outside network, a significant amount of traffic will be exchanged with extra-mesh destinations, the HWMP root is advised to be located at mesh gate station. Such solution will provide all stations with proactively maintained paths to gate station leading to fast response times in of frequent extra-mesh communication.

HWMAP proactive path discovery does not provide paths between non-root MBSS stations, for which purpose reactive path discovery must be used. Due its very nature, reactive mechanism is not activated until the need for communication between a given pair of station arises, which, in case of more complex MBSS networks, can lead to considerable delay in establishing communication between such mesh stations.
A partial solution for this problem is provided by an ability of HWMP to substitute considerably less efficient, but constantly available proactive path information in place of temporarily absent reactive path. Such proactive path will allow communication between two mesh stations, by first forwarding traffic from its source to root station, then from root station to its final mesh destination (Fig. 55). As reactively discovered route becomes available, the traffic begins to be forwarded along this more efficient path.

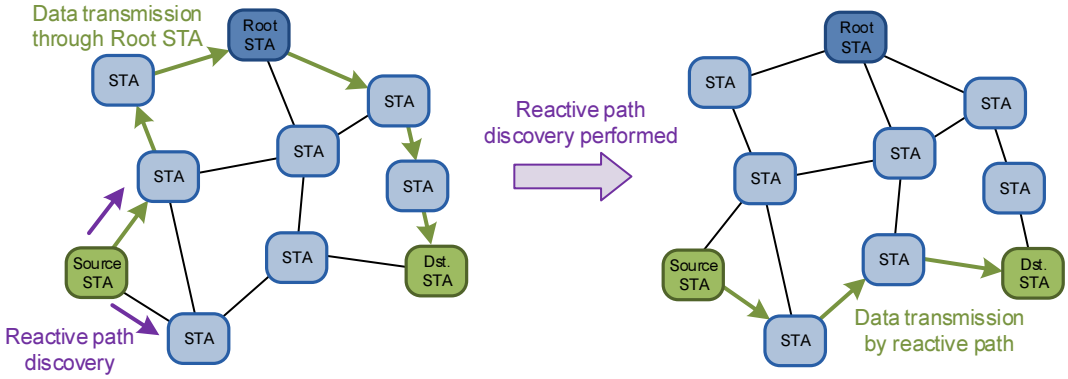

Fig. 55 Non-root STA to non-root STA hybrid path selection process

While such solution allows sending mesh station to commence transmission immediately, it crates two main problems. The first is the proactive route through root station being almost always much longer (in terms of utilized wireless links) than necessary. It results in poor quality of end-to-end transmission (bandwidth and frame loss rate) while causing high network resource utilization.
The second is data reordering when switching from temporary proactive route to final reactive one, as, most probably, the data sent by reactive path will arrive to destination before the data sent earlier by much longer proactive one. To mitigate the problem, a receive buffer at destination STA must be employed.
Both of these problems are compounded by the fact, that only one proactive route (to a single root STA) is to be maintained in mesh stations. In case of larger mesh structures it causes very long paths to be used in some cases even for stations located in 2-hop neighborhood.
The above problems make proactive/reactive path switching solution highly undesirable for real-time multimedia traffic.

The link metric employed by path discovery mechanisms can also (like the path discovery mechanism itself) be selected from a set of metrics supported by all mesh stations within a given MBSS. The selected metric is also included in Mesh ID element of Beacon and Probe response frames, as only one metric can be used in a given MBSS at a given moment. The default, mandatory metric needed for IEEE 802.11s compliance is called Airtime Metric and takes into account both link speed and quality (defined as error rate).

Activity of path selection mechanisms results in presence of forwarding information in mesh stations, necessary to allow transmission of a wireless frame to its mesh destination. Such information consists of destination mesh station address (MDA), next-hop address, precursor list and lifetime the information.
Forwarding rules for both individually and group addressed frames are clearly defined by the standard. Delivery of group addressed frames is conducted in an unreliable manner, due to lack of

reception acknowledgement procedure. Reception of individually addressed frames by next-hop mesh station must be acknowledged.
It should be noted, that they is no support for handling multicast traffic in IEEE 802.11s specification. Such frames will be transmitted using broadcast rules, resulting in inefficient utilization of network resources and unreliable delivery, which makes such method of providing multimedia content to larger groups of receivers ineffective.

Activity of path discovery mechanisms and forwarding functionality results in transparent layer 2 communication between all stations in MBSS, forming so called MBSS LAN.

3.3.10 Interworking with external networks

To be able to communicate with external networks a mesh BSS must contain mesh gate stations. Such stations allow communication between MBSS and distribution system (DS) used to interconnect IEEE 802.11 compliant networks.
To provide communication with networks utilizing other technologies a portal entity must be present in DS. It is often the case, that mesh gate station additionally supports portal functionality, to provide direct connectivity with, for example, wired infrastructure.

Mesh gates can announce their presence in the mesh by one of two mechanisms:

- Gate Announcement – when only reactive routing is employed in MBSS,
- HWMP Proactive path discovery – when a given mesh gate is also a root station.

It is logical for a mesh gate to announce its presence when it has access to a portal through a DS or contains a portal functionality itself. Is such case, the knowledge of a mesh gate presence allows other stations in MBSS to communicate with external networks, by selecting the appropriate one and building a path towards it.

To provide mesh stations with outside connectivity, mesh gate functions as a proxy for destinations outside MBSS, ensuring that forwarding information present within an MBSS concerns only addresses that belong to that MBSS.

From outside point of view, due to its internal functionality (layer 2 communication between all mesh STAs) extended by presence and functionality of mesh gateways, a mesh BSS operates like IEEE 802 LAN segment, compatible with IEEE 802.1D specification – it appears as a single access domain. The mesh structure and mechanisms are hidden form both external layer 2 networks and all higher ISO-OSI layer mechanisms.
Such ability can be a large advantage due to ease of integration with external IEEE 802 networks and forming complex layer 2 networks systems. Also, all network protocols able to function in popular IEEE 802 systems (such as Ethernet), will function in MBSS without any modification.
Strong separation of mechanisms both at MBSS boundaries and between ISO-OSI layer 2/layer 3 mechanisms provides high compatibility of discussed mesh technology.
On the other hand, for mechanisms and protocols located in higher layers of ISO-OSI model, there is no indication to differentiate between stations in a single MBSS as they all appear to be connected to a single LAN. In case of non-mesh solutions (both wired and wireless BSS networks) this scenario corresponds to highly similar communication conditions for all such stations. In case of MBSS it is not the case, as the conditions vary drastically depending on a number of factors (for example: mesh path length).

It is possible for a MBSS to have more than one mesh gate to a single DS. In a sense of IEEE 802.1D specification it corresponds to more than one “port” being available between two IEEE 802 networks. In such situation it is necessary to employ a loop preventing protocol as a part of mesh gate functionality. The typical solution is to employ Rapid Spanning Tree Protocol (RSTP) as defined in IEEE

802.1D-2004 specification. As a result, MBSS can have only one active port (mesh gate) to a single DS.

3.3.11 Intra-mesh congestion control

Due to limited resources of wireless network and changing link quality, a method of providing flow control for multihop communication have been introduced into IEEE 802.11s extension, as an optional functionality. The aim is to reduce the likelihood of buffer overflow at forwarding mesh stations and lessen its negative impact on network performance and resource utilization efficiency.
Three base mechanisms are utilized for this purpose:

- Local congestion monitoring and congestion detection,
- Congestion control signaling,
- Local rate control.

Of these three mechanisms only Congestion control signaling is defined by the standard, while detection and rate control mechanisms are outside of its scope.

As is the case with path selection related mechanisms, a custom congestion control solutions can be used in the IEEE 802.11s mesh. Similarly, a default congestion control signaling protocol has been defined, which must be supported by all stations if congestion control is activated in a given MBSS.

The signaling protocol can be used by a station if it detects congestion in a specific MCF traffic class (see 3.5.1) for a specific mesh destination address. If such congestion is detected, the STA can send a Congestion Control Notification (CCN) frame to the transmitter (TA) of the traffic which is causing congestion and to other neighboring STAs. Such frame contains one or more Congestion Notification elements, each of which, apart from the above information should also include the expected duration of an indicated congestion condition.

Mesh station receiving a CCN frame should stop or reduce rate of sending traffic intended for a specified destination, for the duration indicated in received CNN frame. It may also decide to send its own CCN notification to the transmitter from which it receives traffic causing congestion and its own neighbors in turn. If STA decides to do so, it must update the expected congestion duration, so it will expire in all notified stations at the same moment.

When the congestion condition expires, stations utilizing rate control mechanisms as a result of such notification should resume normal operation.

3.3.12 Emergency service support in MBSS

Due to wide variety of IEEE 802.11s wireless mesh usage scenarios (many providing coverage for a considerable areas, such as a whole suburb district or university campus) and popularity of its base (IEEE 802.11) technology, it can be considered a valued candidate for ubiquitous networking infrastructure. This approach aims to ensure that a user is always connected to the network and can access services regardless of its current location or access technology.
One of services which are considered to be essential for users, and as such have to be provided in the described environment, are emergency services. The term covers widely defined (video, voice, data) communication dedicated with dispatch centers coordinating medical, firefighting and law enforcement response.
To support emergency service related communication in IEEE 820.11s mesh, the standard provides means to indicate if a given STA supports emergency services – appropriate information is included in Beacon and Probe Response frames.
When an outside STA needs to access emergency service, it proceeds to create a peering with mesh STA supporting emergency services, while indicating the necessity of emergency services access by including appropriate indication on an Open frame initiating peering exchange. Mesh STA which

accepted such peering is than responsible for transferring the data to an emergency server – for example to a Public Safety Access Point (PSAP – a call center responsible for answering communications intended for emergency services).

It is worthy of note, that the above description of emergency service support contains not a brief introduction (as is the case with all previous mesh services), but a full description of procedures defined by the standard.

3.4 New frame formats

Introduction of many new network mechanisms, both these necessary for MBSS network to function and optional ones, required the IEEE 802.11-2007 base frame formats to be extended. The extension is required not to disturb the compatibility with the base standard, so the changes can be classified into the following groups:

- Definition of new values for existing frame fields – the new values are chosen from ranges which were reserved in the base standard for the purposes of future extensions.
- Definition of new frame types and their formats – possible due to introduction of the new values mentioned above in the frame fields responsible for frame type identification.
- Extension of structure of existing frame types, which the base standard designed to be extensible (for example Beacon and Probe Response frames).

Due to the overall IEEE 802.11-2007 standard policy, stating that network entities should ignore frames which they are not able to interpret (unless specifically instructed otherwise – in case of security mechanisms for example), the presence of IEEE 802.11s specific frames should not create incompatibilities with standard IEEE 802.11-2007 network installations.

In the following description we will omit detailed description of changes specific to mechanisms which are loosely connected to the main subject of this thesis. We will concentrate on most notable overall format changes introduced by IEEE 802.11s mesh extension and these associated with mechanisms of direct interest to us.

3.4.1 General frame format

Despite the changes necessary to accommodate new mesh mechanisms, the base format of IEEE 802.11 frame remains unchanged and depends on the version of the IEEE 802.11 standard which is used by the mesh as a transmission technology.
It should be noted, that all Data frames employed within an MBSS are exclusively of QoS Data frames which means they include QoS Control field (see 2.4.5.3). In the following text of this dissertation, if a Data frame transmitted within MBSS is mentioned, it is assumed that it is a QoS Data frame.

3.4.1.1 QoS Control field

The IEEE 802.11s amendment extends the usage of this field to accommodate its new mechanisms, while retaining backwards compatibility. In case of IEEE 802.11-2007, there are 4 different structures of QoS Control field defined (differentiated by the IEEE 802.11 MAC Type/Subtype field values), and the IEEE 802.11s defines another one intended to be used in MBSS environment The structure of the QoS Control field used in MBSS network is presented in Fig. 56.

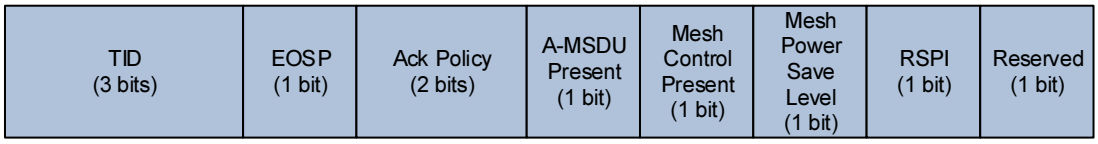

Fig. 56 QoS Control field structure for MBSS environment

TID subfield identifies Traffic Class or Traffic Stream to which the frame belongs, which is a basis for traffic QoS prioritization or guarantees under, respectively, EDCA and HCCA rules.
AckPolicy subfield indicates acknowledgement policy for the frame.
A-MSDU Present subfield allows MSDU aggregation to be used by indicating if MSDU or A-MSDU resides in the Frame Body.
Mesh Power Control functions employ a set of three subfields of QoS Control field: Mesh Power Save Level, End of Service Period (ESOP) and Receiver Service Period Initiated (RSPI).
If appropriate Frame Control subfield indicates that transmitting STA is about to enter sleep mode, the Mesh Power Save Level subfield is used to indicate if it will be Light Sleep or Deep Sleep mode.
End of Service Period (ESOP) and Receiver Service Period Initiated (RSPI) values in QoS Data or QoS Null frames can be used to initiate a Peer Service Period (see 3.3.6) and indicate its owner (station allowed to use it to transmit over the link). ESOP field is additionally used to terminate a currently active PSP.
Mesh Control Present subfield indicates lack or presence of a completely new addition to IEEE 802.11 frame format – Mesh Control field.

3.4.1.2 Mesh Control field

Mesh Control field is present in mesh Data frames which contain a complete MSDU, a first fragment of fragmented MSDU or an A-MSDU. Additionally it is used in Multihop Action Frames (see 3.4.4) introduced by IEEE 802.11s extension. In other words, it is present in frames which commence a possibly multihop transmission of an independent data portion (MSDU in case of data frames and MMPDU in case of multihop action frames) and contains elements necessary to perform a multihop delivery – addressing, time-to-live (TTL) and multihop sequence numbering information.

Mesh Control field is of variable length (6, 12 or 18 octets) depending on the number of address subfields (0-2) which it includes. Its overall structure is presented in the figure below.

Fig. 57 Mesh Control field structure

As mentioned before (3.3.8), mesh BSS uses up to 6 address fields. With only 4 address fields in the header of a standard IEEE 802.11 frame, the remaining necessary fields are included in Mesh Control field. Additionally, as the Address 4 field of a standard 802.11 MAC frame is not utilized in some addressing scenarios despite its availability (due to compatibility reasons) there is a need for up to 2 additional address fields.
The additional address information is located at the end of Mesh Control field in form of Mesh Extension Address subfields. As their number is subject to change, it is indicated by Address Extension Mode value – part (2 bits) of Mesh Flags subfield. Its remaining 6 bits are currently not used.
Mesh TTL value is used to limit a maximum number of forwarding hops the frame is allowed to take before it is dropped as means of preventing infinite loops.
Mesh Sequence Number (4 octets) is used as a counter for duplicate detection and recovery procedures in multihop transmissions. It is incremented by one with each MSDU/MMPDU transmitted by a given station using frame format with Mesh Control field present.
It should be noted, that IEEE 802.11-2007 standard mechanisms for duplicate detection are also present in MBSS, but their functionality covers only a single hop. In case of multihop environment they are not sufficient, as a station can receive multiple copies of the same MSDU from its multiple neighbors.

3.4.2 Data frames

As stated before, all Data frames transmitted within MBSS are QoS Data frames and as such contain QoS Control field. As IEEE 802.11s extension is based on base IEEE 802.11-2007 standard and Mesh Coordination Function (see 3.5.1) supports both contention based (EDCA) and controlled (HCCA) medium access methods , all subtypes of QoS Data frame are supported in MBSS:

- Subtypes carrying MSDU / A-MSDU:
  - QoS Data
  - QoS Data+CF-Ack
  - QoS Data+CF-Poll
  - QoS Data+CF-Ack+CF-Poll
- Subtypes used exclusively for MAC control purposes:
  - QoS Null (no data)
  - QoS CF-Ack (no data)
  - QoS CF-Poll (no data)
  - QoS CF-Ack+CF-Poll (no data)

All of the above Data frame subtypes contain QoS Control field described in 3.4.1.1. Moreover all subtypes carrying MSDU or A-MSDU include Mesh Control field at the beginning of Frame Body.

3.4.3 Control frames

The format of Control frames is minimalistic and highly specific to their particular subtype. In case of MBSS it remains unchanged, except 3 specific cases:

- Block Ack Request and Block Ack frames – IEEE 802.11e [32] extension defined new variants of these frames, due to introduction of new frame acknowledgement procedures.
- PS-Poll frame – as the standard power management mechanisms of IEEE 802.11-2007 standard are not employed in MBSS, PS-Poll control frame type is also not used. Mesh Power Management procedures are used instead.

As can be seen, there are no significant differences between wireless links in PtMP and MBSS environment. Such situation is to be expected, as the purpose of Control frames is to exercise a direct control over wireless transmission's atomic procedures, which are not modified by mesh extension, but used transparently if possible.

3.4.4 Management frames

The format of management frames is largely unchanged compared to previously described IEEE 802.11-2007 standard. It should be noted, however, that a slight change in the specification removes explicit bindings between address fields of the above overall management frame structure and DA, SA and BSSID identifiers. The contents of the address fields are defined separately, depending on the specific management frame type.

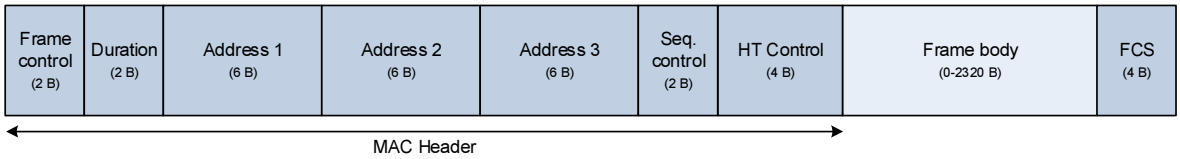

Fig. 58 Management frame overall format

Management frames are identified by appropriate value of Type subfield of Frame Control (FC) MAC header field. Furthermore, a specific kind of management frame is identified by Subtype subfield of FC field. Limited length of Subtype subfield results in most new management frame varieties being

defined as Action subtype, which introduces an additional Category field (1 octet) at the beginning of the frame body, for their identification (Fig. 59).

Fig. 59 Management Action frame format

As before, the structures of particular subtypes of management frames and categories of Action subtype define the (obligatory or optional) presence of fields/information elements and their appropriate sequence in their Action details fields. It is important to remember, that if a given Management frame type allows/requires Information Elements of some specific type (as most of them do), it can be extended by including newly defined IE types, without losing compatibility. The new IEs will be processed by STAs able to do so and ignored by other stations.
The Action details field can be optionally terminated with Management MIC Element (MME) providing data integrity and reply protection. Such functionality is available for specific types of group addressed management frames, called robust management frames: Action, Disassociation and Deauthentication.

It should be noted that all of management frame types present in IEEE 802.11-2007 standard are designed to be used in single hop environment, as it was the only environment of wireless network operation defined there. Some of their number is still used in MBSS to perform management tasks concerning physically neighboring stations (for example tasks concerning mesh discovery), however their format have often been extended to accommodate new management information. Such extension has been possible, because the format of management frames has been designed to be extensible (in contrast with, for example, Control frame format). The methods used in case of IEEE 802.11s specification include:

- extension of type/subtype identifier space by use of Action management frame subtype,
- use of Information Elements to provide ability to dynamically change the exact format of a particular subtype.

For the purpose of the discussed extension, 22 new Information Elements have been defined, to be used in both newly created Action frame categories and to extend existing management frame formats. Most important of them include:

- Channel Switch Announcement / Extended Channel Switch Announcement – used by Mesh Channel Switching mechanism (3.3.7) to schedule mesh-wide changes of used frequency channel,
- Mesh Peering Open / Confirm / Close – necessary to create peer links between neighboring mesh nodes (Mesh Peering Management – 3.3.2),
- Mesh Group Key Inform / Acknowledge – utilized by security mechanisms to secure group addressed communication,
- Mesh Link Metric Report – necessary to disseminate link metric information between neighboring peers,
- HWMP Mesh Path Selection – utilized by HWMP Mesh Path Selection (3.3.9) mechanism,
- Gate Announcement – used to distribute Mesh Gate presence information,
- Congestion Control Notification – employed by optional Intra-mesh congestion notification protocol (3.3.11),
- MCCA Setup Request / Reply – utilized to perform (request and confirm) medium access reservations with optional Mesh Controlled Channel Access (MCCA) mechanism,
- MCCA Advertisement / Advertisement Request – used by MCCA mechanism to disperse medium reservation information to all affected STAs,

- TBTT Adjustment Request / Response – used in Mesh Beacon Collision Avoidance (MBCA) process, preventing excessive collisions between Beacon frames sent by mesh STAs in 2-hop neighborhood,
- Proxy Update / Update Confirmation – employed by Proxy Mesh Gates as a part of interworking procedures (see 3.8.2.3).

More detailed discussion of their formats and usage will be provided as a part of description of particular mesh mechanisms.

Apart from existing management frame subtypes and specific Action frame categories, three new categories of Action frames have been defined for IEEE 802.11s MBSS-specific mechanisms:

- Self-protected Action frames – frames of this category are not robust frames and thus their potential protection is decided by external means specific to the particular mechanism which employs them. They are used mainly before peering relationship is established between STAs and standard MBSS security mechanisms become available – for example in process of mesh peering (see 3.6.3) and include various Mesh Peering and Mesh Group Key frames.
- Mesh Action frames – robust Action frames intended to be used in variety of MBSS mechanisms, such as path selection, interworking, congestion control, controlled channel access, etc. They require a peering relationship to be already established between communicating STAs.
- Multihop Action frames – a unique category of robust Action frames, used to communicate between STAs which are not direct neighbors and thus being forwarded through an MBSS in multihop manner. Employed in communication between mesh gates (see 3.8.2).

In all of these three categories, the octet immediately following the Category field indicates a particular action type within a given category.

The last of the three Action frame categories however, requires additional attention – a Multihop Action category. It utilizes a MAC header with 4 address fields (instead of standard 3-address header as other management frames – see 3.3.8), which allows it to be exchanged between mesh stations outside of a mutual 1-hop neighborhood.
The standard IEEE 802.11-2007 frame header already includes 4 address fields and should be able to accommodate this frame subtype, but its 4th address field is not used due to compatibility reasons. As already mentioned in Section 3.3.8, multiple proprietary solutions utilize it (due to lack of earlier specification for its use), which is likely to cause conflicts unacceptable in case of management-related communication. In this situation, the 4th required address is included in Mesh Control field (see 3.4.1.2).
Despite the considerable number and complexity of MBSS-specific mechanisms only one of them currently utilizes multihop management functionality offered by Multihop Action frames – Mesh Gate Proxy mechanism (see 3.8.2.3).

Although Multihop Action is the only management frame capable of being addressed to non-neighboring mesh stations, it is not the only management frame which can be used to perform management operations concerning such stations. While the remainder of management frames cannot be addressed to non-neighbor mesh STAs, they can result in mandatory generation of new management frames by its receivers (Fig. 60). This technique can be used for wide dissemination of management information and performing management operations concerning large station sets.

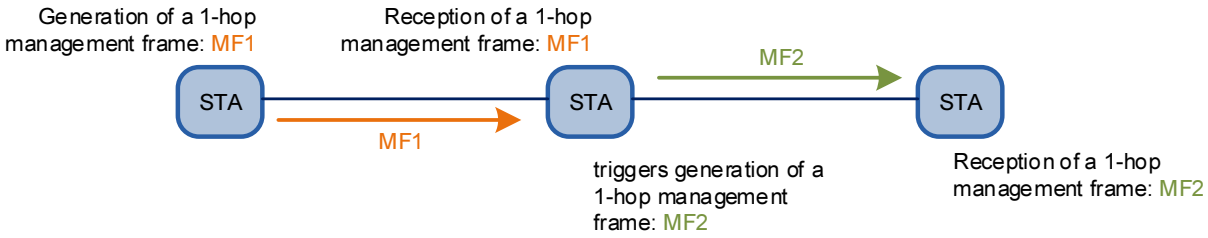

Fig. 60 MBSS-wide propagation of a message with use of 1-hop management frames

Multihop Action frames, on the other hand, are processed only by their final MDA destinations, while the transit STAs forward them without processing their contents.

3.5 MAC sublayer functionality extensions

While the already described, IEEE 802.11-2007 MAC sublayer functionality covers all mechanisms necessary for controlling a data transmission over the wireless medium (WM), they are designed for a point-to-multipoint architecture of an infrastructure network and a simple point-to-point links of ad-hoc system.
In case of obligatory, contention-based medium access methods (DCF and EDCA), the mechanisms used in infrastructure and ad-hoc systems can be used in an MBSS environment with almost no modifications. The reason is the simplicity of the service provided by such methods and resulting lack of necessity to take the network structure into account.
However, in case of contention free access (PCF and HCCA) and its aim to provide guaranteed service for higher layers, the mechanisms of infrastructure and ad-hoc modes need to be substantially extended if they are to be effective in a multihop mesh network environment.
Due to this need for additional specification regarding MAC sublayer functionality for an IEEE 802.11s mesh mode, a separate coordination function has been defined for this new type of IEEE 802.11 network – a Mesh Coordination Function (MCF), describing both contention-based and contention free methods of WM access.

3.5.1 Mesh Coordination Function (MCF)

Under Mesh Coordination Function (MCF) rules, the medium access rights are allocated for a time interval called TXOP and defined by its starting time and duration. Depending on the mechanisms used by a STA to obtain an access to a WM, the TXOP can be:

- the EDCA TXOP – obtained according to EDCA rules described in Section 2.5.4,
- the MCCA TXOP – obtained during a controlled channel access interval, according to MCF Controlled Channel Access (MCCA) rules described in the following section.

While support for EDCA and resulting EDCA TXOPs is obligatory in an IEEE 802.11s MBSS, the MCCA support is optional. Moreover, it is possible to mix MCCA and non-MCCA stations within a single MBSS without additional restrictions – however it should be noted, that the presence of non-MCCA STAs in an interference range of MCCA STAs will negatively impact the efficiency of MCCA operation.

3.5.2 MCF Controlled Channel Access (MCCA)

The MCF Controlled Channel Access (MCCA) mechanisms allow stations to make WM reservations for their future transmission using IEEE 802.11 management frames.
To make a reservation for WM access, a STA sends an unicast MCCA Setup Request frame to an intended recipient of the traffic which it plans to transmit. The fame contains a detailed information about the period for which the reservation is intended, called MCCA Opportunity (MCCAOP). The STA, which initiates the procedure by sending such frame becomes known as an MCCAOP owner.

The recipient of the MCCA Setup Request frame (called MCCAOP responder) verifies if the reservation can be established (for example: it does not interfere with other reservations) and responds with an unicast MCCA Setup Reply frame.
With the reservation established between the owner and the responder (or responders, in case of a group addressed transmissions), these stations start advertising relevant information to their neighbors, whose transmissions could interfere with transmission during the reserved MCCAOP.
All MCCA-enabled stations (including stations from other MBSS networks), should track the above advertisements and refrain from transmissions during MCCAOP reservations for which they are not the owners.
The owner of the MCCAOP reservation can, during its interval, perform a transmission to the responder, after obtaining channel access according to EDCA rules. The owner will use a customized set of EDCA attributes for obtaining the access during its MCCAOP and should not encounter competition from other MCCA-enabled stations, due to earlier advertisement of the reservation. It is possible that it will encounter access attempts from non-MCCA STAs, but such conflicts should be resolved due to the obligatory EDCA procedure, for which MCCAOP owner employs a preferential set of parameters.

The MCCA procedure outlined above seems to be reasonably uncomplicated, however, due to necessity of obtaining time synchronization, maintaining compatibility with other mechanisms of the IEEE 802.11s MBSS, coexistence with non-compliant stations, efficiency of operation and preventing starving of non-MCCA stations, there is a significant number of elements which must be addressed for it to work:

- Support for individually and group addressed transmissions – resulting in different reservation signaling procedures,
- Specification of reservation setup and teardown – necessary to perform the signaling necessary for obtaining the reserved MCCAOP,
- Mechanisms for advertising the reservation – used to prevent interferences from other MCCA-enabled stations. The robust signaling mechanisms support proactive/reactive and full/differential (partial) advertising procedures, supplemented by piggybacking the advertisements in Beacon frames,
- Possibility of early release of the reservation – introduced to allow the MCCAOP owner to end the reserved period early, preventing it from unnecessary consuming WM resources,
- Dead reservation detection – mechanism for detecting and removing MCCAOP reservations which are not used but have not been properly torn down,
- Time synchronization – required to specify and track MCCAOP reservation intervals,
- EDCA channel access, with custom access attributes – used to perform an addition WM channel access control, to accommodate non-MCCA stations and unexpected situations,
- Reserved Allocation Vector (RAV) array – per neighbor WM allocation vector, to used extend the existing physical and virtual channel allocation mechanisms,
- Maximum MCCA Access Fraction – limitation of MCCA-controlled WM time, necessary to prevent starving of contention-based WM access,
- Reservation tracking limit per STA – limitation of a number of reservations a given station is required to keep track of, used to prevent overloading of less capable STAs.

From the list above it is evident, that mechanisms required for implementing MCCA medium access are numerous, complicated and tightly interrelated both within their group and with other IEEE 802.11 mechanisms. It is probably due to this fact, that there are currently no MCCA implementations for off-the-shelf (OTS) hardware and even simulation models are limited to partial implementations.

3.6 Mesh Discovery and Peering Procedures

The IEEE 802.11s amendment specifies a comprehensive set of mechanisms required to create a self-organizing wireless mesh network utilizing dynamically established peer-to-peer links between participating stations. For the purpose of creating such a network structure, it is necessary to provide IEEE 802.11 stations with procedures allowing them to detect the presence of a mesh network and form the links to their peers in an efficient and automated manner.
The process of connection to an IEEE 802.11s MBSS network can be divided into three distinct stages:

- Mesh network discovery – STA searching for the network obtains information about MBSS networks available, their basic configuration parameters and requirements they set for connecting stations,
- Authentication – connecting STA needs to authenticate to the MBSS, before it is allowed to connect,
- Mesh Peering – authenticated STA forms peer link to a STA already connected to MBSS, thereby becoming part of an MBSS network structure.

The overall process stages may seem similar to these performed in case of connecting to a classic, PtMP WiFi network, but due to different architecture of a mesh network, their specifics (described below) are also dissimilar.

3.6.1 Mesh Discovery

If a station is to be a part of an MBSS, it is necessary for it to perform a Mesh Discovery procedure to verify if an appropriate MBSS exists and obtain configuration information required to join its network structure, or to check if it is permissible for the STA to establish a new one.

Mesh STA can use both passive and active scanning to discover presence of MBSS, using the same procedure as in case of infrastructure and ad-hoc IEEE 802.11 modes, but extending the employed data structures to include mesh-specific information.

The specific MBSS is uniquely identified by a 0-32 byte binary identifier called Mesh ID used in all mesh discovery procedures which in turn employ Beacon and Probe Request/Response frames. This identifier is also used in mesh peering procedures described in following sections, which are used to create transmission links between STAs in an MBSS.

When Mesh ID is used to perform MBSS discovery, SSID element (used for network identification in infrastructure and ad-hoc modes) in Beacon, Probe Response and Probe Request must be set to so called wildcard SSID – a 0 byte length SSID field. In case of two former frame types it indicates that a sending STA is not a part of a classic BSS or IBSS to prevent non-mesh capable STAs from attempting to join the MBSS network. In the latter frame type it allows the sender to obtain responses irrespective of SSID value which is not used in the MBSS discovery process.

As a result of passive or active MBSS scanning STA will obtain Mesh Configuration Element (Fig. 61) used to advertise mesh services and containing:

- mesh profile which carries information about an MBSS as a whole,
- additional information specific for a particular mesh STA which generated the Beacon or Probe Response frame – Mesh Formation Information and Mesh Capability.

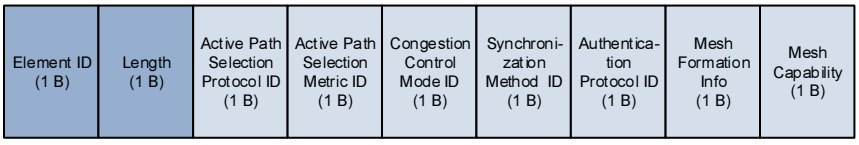

Fig. 61 Mesh Configuration element

Mesh Profile contains parameters, which must be the same for all STAs in a given MBSS, as they specify critical, network wide mechanisms. STA planning to join a specific MBSS must assume the same mesh profile values as these active within the MBSS.
Mesh profile parameters include:

- Active path selection protocol identifier – indicates path selection protocol which is used for path discovery in the MBSS. Currently only HWMP protocol (see 3.7.3) is defined as ID 1.
- Active path selection metric identifier – identifies type of metric to be used for link/path assessment and selection. Currently only Airtime metric (see 3.7.2) is defined as ID 1.
- Congestion control mode identifier – specifies congestion control protocol currently used in the MBSS. While there is a simple solution for this task specified in the standard, the default value for this field is 0, which indicates that no such protocol is in use.
- Synchronization method identifier – specifies method used for obtaining time synchronization between STAs in the MBSS. Neighbor offset synchronization method is defined in the standard and is used by default (ID 1), however it is possible to omit such functionality by specifying ID 0 in this field.
- Authentication protocol identifier – specifies authentication method used to verify eligibility of stations to establish mesh peerings within the MBSS. Currently three possibilities are defined: No authentication (ID 0), Simultaneous authentication of equals (SAE) defined by the standard (ID 1) and IEEE 802.1X authentication requiring presence of an Authentication Server within the MBSS (ID 2).

All of the above Mesh Profile fields have length of 1 byte allowing for 254 different identifiers and a value of 255 which indicates presence of additional Vendor Specific element, containing information about a particular mechanism (which does not have a specific ID assigned in the standard).

While Mesh Profile describes the MBSS, Mesh Formation Information (Fig. 62) and Mesh Capability (Fig. 63) fields contains information specific for a particular STA which generated a particular Beacon or Probe Response frame.
Mesh Formation Information holds information describing sending STA's condition as a part of MBSS network structure:

- Connected to Mesh Gate field (if set) indicates that a given STA has a current path to Mesh Gate,
- Number of Peerings field describes the number of peer links that a given STA maintains at the moment,
- Connected to AS field informs, if a given STA has a current communication path to an Authentication Server which can be used to perform authentication using IEEE 802.1X protocol.

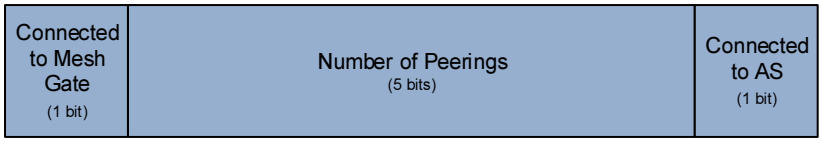

Fig. 62 Mesh Formation Information field

Mesh Capability field holds information concerning sending STA's link establishment capabilities:

- Accepting Additional Mesh Peering field indicates, if sending station allows for additional mesh peering to be established with it. If this indicator is not set, no new peering requests should be sent to the STA.
- MCCA Supported – indicates whatever a given STA supports Mesh Coordination Function Controlled Channel Access (MCCA, see 3.3.5) procedures.
- MCCA Enabled – indicates whatever a given STA currently employs MCCA procedures.
- Forwarding – indicates if the STA can be used to forward data frames.

- MBCA Enabled – indicates if the STA currently employs Mesh Broadcast Collision Avoidance (MBCA, see 3.3.4) procedures.
- TBTT Adjusting – indicates if the STA is currently in process of adjusting its Target Beacon Transmission Time (TBTT) as part of MBCA procedures, due to a high number of Beacon collisions detected.
- Mesh Power Save Level – if Power Management procedures are used by the STA, this field indicated whatever deep sleep mode is supported (value 1).

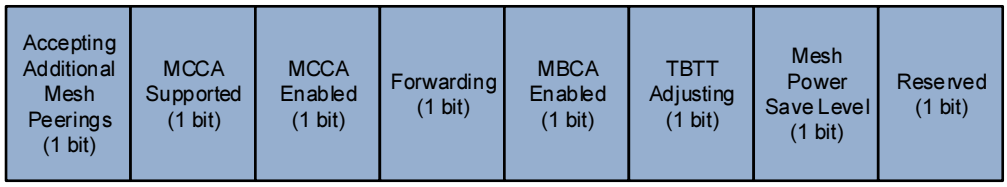

Fig. 63 Mesh Capability field

The STA performing a Mesh Discovery can, based on the results obtained from received Beacon and Probe Response frames, decide to establish a new or join an existing MBSS.
If the station decides to join an existing MBSS it prepares a list of valid candidate stations which includes STAs satisfying the following conditions:

- they use the same Mesh Profile as the STA performing discovery. It should be noted, that if the STA performing discovery is not a member of any MBSS, it can freely change its Mesh Profile to match discovered station,
- they accept mesh peerings as indicated by Accepting Additional Mesh Peerings field,
- they have compatible Basic Rate Sets (and Basic MCS Sets in case of High Throughput capable stations),
- it is possible to successfully perform Authentication procedure (based on Authentication Protocol ID and Connected to AS fields).

Station that obtained non-empty candidate station list, can perform (optional) Authentication procedure followed by Mesh Peering procedure to join an MBSS.
If the station becomes a member of MBSS (by joining an existing or establishing a new one) it starts to advertise the MBSS presence in periodically sent Beacon frames and reactively sent Probe Responses.
Station which is a member of MBSS can continue to perform Mesh Discovery procedures to detect presence of other MBSS networks or additional possible peerings within its current MBSS.

3.6.2 Authentication

Depending on a particular MBSS configuration two stations attempting to establish a mesh peering may require a common Pairwise Master Key Security Association (PMKSA) confirming that they successfully performed an authentication process.
Apart from the option to create an unsecured mesh MBSS, when there is no authentication and no PMKSA is required, are two authentication mechanisms currently defined by the standard to perform the task:

- Simultaneous Authentication of Equals (SAE), which is an obligatory mechanisms to be supported by all IEEE 802.11s compatible STAs,
- IEEE 802.1X, which can be optionally supported and requires a dedicated Authentication Server to be present in the MBSS.

As a result of completion of either procedure, both stations establish a bidirectional PMKSA, which both confirms the fact that they successfully authenticated each other and holds keying material

necessary for derivation of additional keys used to secure the mesh link such STAs may establish within a particular MBSS.

The complete structure of PKMSA includes the following elements:

- Pairwise Master Key Identifier (PMKID) – cryptographically generated, unique identifier of a PKMSA,
- Mesh STA's MAC address – local station's MAC address,
- Peer mesh STA's MAC address – authentication peer's MAC address,
- Pairwise Master Key (PMK) – a key cryptographically generated in the process of successful authentication and proving its proof,
- Authenticated Encryption Key (AEK) – a key derived from PMK, used by Authenticated Mesh Peering Exchange (AMPE) protocol employed to create secure mesh peerings and described in the following section,
- Lifetime – length of time after with the PMKSA can no longer be used due to security reasons,
- Selected Authentication and Key Management Suite – describes set of algorithms used to perform the authentication and selected for key management tasks.

As described in the previous section, a station that wishes to join an MBSS performs a detection procedure and creates a candidate list. As a part of this procedure, such STA obtains authentication requirements of detected MBSS systems through Authentication Protocol Identifier present in Mesh Configuration element of Beacon or Probe Response frames.
Depending on the indicated configuration the STA may:

- immediately commence peering procedure according to Mesh Peering Management (MPM) protocol, if the MBSS does not use authentication,
- attempt SAE authentication procedure described below to obtain PMKSA if the MBSS configuration indicate SAE as an active authentication protocol,
- perform temporary peering procedure using MPM protocol to obtain a limited MBSS connectivity allowing it to conduct an IEEE 802.1X authentication with an MBSS-side Authentication Server, if the IEEE 802.1X authentication is used by the MBSS.

3.6.2.1 Simultaneous Authentication of Equals

By the use of Simultaneous Authentication of Equals (SAE) protocol, two stations can prove to each other the knowledge of a secret password, thus completing the authentication process. The protocol is based on Dragonfly Key Exchange [82] – a password-authenticated key exchange based on a zero-knowledge proof. As a result of successful authentication, a shared Pairwise Master Key becomes known to participating stations.
Peer-to-peer architecture of SAE does not require the existence of a designated authentication authority, which is a strong advantage in case of self-organizing mesh system. The protocol is also well designed for wireless environment from security standpoint, as it is not susceptible to man-in-the-middle attacks (easily lunched in such environment), as the attacker is unable to determine the authentication password or resulting PMK by either observing, modifying, forging or replaying authentication frames sent to an uncorrupted STA. Moreover, the protocol is resistant to dictionary/brute force attacks as the attacker can attempt only one guess at the password in an online, active attack – it is not possible to obtain a password in using an offline analysis.
The protocol also prevent the use a compromised PMK to obtain a password or PMK of another SAE session, and the use of a compromised password to recover PMKs from earlier sessions.
The described features, combined with denial-of-service protection based on Anti-clogging Token, make the SAE a robust and resilient solution, well suited for wireless network environment.

The protocol uses Authentication management frames (Type: Management, Subtype: Authentication) and requires successful completion of two stop procedure by both participating stations.
Any of the stations begins the SAE exchange by sending a Commit Message of the following content in Authentication management frame:

- Standard IEEE 802.11 frame header (in particular TA and RA address fields),
- Authentication algorithm number = 3 (SAE),
- Authentication transaction sequence number = 1 (Commit Message),
- Status code = 0 (Success),
- Finite Cyclic Group (FCG) - Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC) cryptographic group specification,
- (optional) Anti-Clogging Token – needs to be present for the frame to be accepted when a Denial of Service protection is responding to a high number of requests (see below),
- Scalar – value generated as a part of a Dragonfly Key Exchange,
- Element – value generated as a part of a Dragonfly Key Exchange.

First two fields, supplemented by the general IEEE 802.11 frame header, identify stations (TA and RA fields of general frame header), SAE authentication algorithm and Commit Message (transaction sequence = 1). The frame is sent as a result of initial cryptographic calculations, which produce the results placed in FCG, Scalar and Element fields. As the calculations have been successfully conducted and the frame is prepared, the Status code field indicates Success (0).

Station receiving SAE Commit Message should check its basic correctness and respond by sending its own SAE Commit Message prepared according to the same rules. Then it should process the content of the cryptographic fields contained in both received and sent SAE Commit messages and respond with SAE Confirm Message of the following format:

- Standard IEEE 802.11 frame header (in particular TA and RA address fields)
- Authentication algorithm number = 3 (SAE)
- Authentication transaction sequence number = 2 (Confirm Message)
- Status code – depending on SAE Commit Message processing and current state of the sending STA
- (optional) Anti-Clogging Token – optionally present when a Denial of Service protection is responding to a high number of requests (see below),
- Send-Confirm – integer value calculated to provide protection against traffic reply attacks,
- Confirm – cryptographic value calculated as a part of Dragonfly Key Exchange.

The contents of Confirm field of the above message allows the sender of the original SAE Commit Message to verify the that both stations used the same authentication password during SAE procedures. The station accepts the authentication to be successful when it receives a correct Confirm Message with a Successful (0) Status code from its authentication partner.

As the SAE Commit Message must be accepted from any station and its reception triggers a computation intensive process, it may be used as means for Denial of Service attack, executed by flooding the station with SAE Commit Messages from different forged MAC addresses. To mitigate the impact of such attacks, stations maintain a counter of currently open SAE authentication exchanges. If the counter exceeds a configured threshold, further SAE Commit Messages will be rejected by sending its originator a SAE Confirm Message with a Status code of 76 (“Anti-Clogging Token Requested”) and Anti-Clogging field containing a token bound to its specific MAC address. In this state, for a SAE Commit Message to be processed it must contain a token received in response to a previous SAE Commit Message.

3.6.2.2 IEEE 802.1X authentication in MBSS environment

As the IEEE 802.1X authentication architecture follows a client-server model, with strictly defined initiator (Supplicant) and responder (Authentication Server – AS), it requires the latter to be present in the MBSS. Moreover, the communication between the joining station and the AS must be possible to perform authentication. Combined with the fact, that, according to IEEE 802.11s rules, in a secure MBSS the authentication process must precede the peering process (which in turn is required to enable connectivity between new station and the MBSS containing the AS), these requirements seem to make the IEEE 802.1X authentication procedure impossible or at least difficult to employ.

The first difficulty to overcome is the client-server architecture of the IEEE 802.1X authentication. To successfully employ it, two stations attempting a peering need to decide which one is going to function as initiator, and which one as responder. For this purpose, during the mesh discovery process, a Connected to AS field of a Mesh Formation Information element (present as a part of Mesh Configuration element in all Beacon and Probe Response frames) is examined – if set to 1, it indicates that a given STA has a connection to Authentication Server. If only one of the stations attempting the peering has this value set to 1, it will function as responder, and the other as initiator. When both stations have connection to AS (which is common when stations which already belong to MBSS form additional peerings), the one with higher MAC address will act as a responder. If none of the stations have connection to AS, IEEE 802.1X authentication is impossible and should not be attempted.

To second problem, the need for an established communication link before the authentication process, is solved by introducing a two stage peering process. The connecting station will first perform a temporary peering using the unsecured MPM protocol, which will allow it to form a communication link with an appropriate (having Connected to AS field set) candidate station belonging to a chosen MBSS.
The authentication itself is performed using EAP [32] protocol and results in establishing a PMK shared by both stations participating in the temporary MPM peering. This PMK is then extended by stations to form a PMKSA described earlier and the temporary peering is closed following MPM rules. As both stations now possess the PMKSA created as a result of IEEE 802.1X authentication, they can proceed to form a secure peering using AMPE protocol described in following sections.

3.6.3 Mesh Peering Management (MPM)

For a station to become a part of an MBSS structure consisting of more than a single station, it is necessary for it to create transmission links with other STAs in the MBSS. For this purpose, following a successful Discovery and Authentication procedures, a Mesh Peering procedure must be completed for each direct station to station link.

Mesh peering can be performed according to one of two similar procedures, depending on whatever the MBSS requires authentication of mesh stations. Mesh Peering Management procedures (MPM) are used if no authentication is required, while their extended version: Authenticated Mesh Peering Exchange (AMPE) is employed if such requirement exists.

An entity called Mesh Peering Instance Controller is responsible for managing STA's peerings, by creating, managing and destroying separate instances of MPM/AMPE protocol maintained by for each peering, identified by Mesh Peering Instance Identifier – a set of the following fields:

- localLinkID – integer identifier of the peering, uniquely identifying it within a particular STA,
- localMAC – MAC address of the local STA,
- peerMAC – MAC address of the peer mesh STA.

Apart from the above identifier, the peering instance stores additional information:

- peerLinkID – integer identifier which the peer mesh STA uses as its localLinkID of the peering instance,
- configuration and capability information obtained as a result of the peering procedures.

3.6.3.1 Mesh Peering Management

Assuming that its Mesh Profile specifies that no authentication is to be used in a given MBSS, Mesh Peering Management (MPM) procedures are employed.
If a station has non-empty candidate station list (see 3.6.1) MPM procedures can be initiated by:

- receiving a Mesh Peering Open frame from a STA within a candidate list,
- decision of higher layer management entities not defined by IEEE 802.11 standard, resulting in sending a Mesh Peering Open frame to a STA within a candidate list.

For the peering procedure to be complete, it is necessary for the pair of stations to successfully send a Mesh Peering Open frame to each other and have it confirmed by receiving an appropriate Mesh Peering Confirm frame.
Removal of an existing peering can be accomplished by sending Mesh Peering Close message. However, it should be noted that the peering instance will not be deleted immediately, but need to be maintained for a specified time, to allow for graceful termination of dependent mechanisms.

Frames used in MPM belong to management frames of Action subtype and Self-protected category (Self-protected Action), which is intended for direct STA-STA communication and assumes that possible protection of its frames is provided by and upon decision of protocols which use this frame type. It should be noted that such approach is different from both Public category frames (which are intended to be readable for all STAs) and many other sub-categories of Action category which have Robust property (as they assume that protection mechanisms are externally provided and already in place).

Self-protected Action management frames currently the following mesh peering-related frames, identified by Action Details field of Action Element:

- Mesh Peering Open – used to initiate Mesh Peering procedure. Contains already mentioned Mesh ID and Mesh Configuration elements, a Mesh Peering Management element (see below), as well as a set of parameter values supported by the sender for all parameters necessary to establish an IEEE 802.11 wireless link between stations.
- Mesh Peering Confirm – used to confirm reception and acceptance of Mesh Peering Open frame. It contains a confirmation of peering parameters.
- Mesh Peering Close – used to terminate an existing peering. Identifies a specific peering and describes reason for its termination by including a Mesh Peering Management Element.

Apart from the frames listed above, there are two additional Self-protected Action frames defined, allowing selection of group cipher suite if protection of group-addressed frames is required in MBSS: Mesh Group Key Inform which initiates a group cipher suite selection process, and Mesh Group Key Acknowledge, which finalizes it.

3.6.3.1.1 Creating a new mesh peering

Station which decides to initiate a peering with another STA from its candidate list will create and send a Mesh Peering Open management frame containing the following fields, describing its transmission capabilities, identifying the MBSS and specifying the peering to be created:

- Capability
- Supported Rates

- Extended Supported Rates
- Power Capability
- Supported Channels
- **Mesh ID**
- **Mesh Configuration**
- **Mesh Peering Management**
- ERP Information
- Supported Regulatory Class
- HT Capabilities
- HT Operation
- 20/40 BSS Coexistence element
- Extended Capabilities element
- Interworking
- Vendor Specific elements

As can be seen from the above list it includes all parameters necessary for negotiating an IEEE 802.11 wireless link, as its structure is a close copy of an Association Request management frame used in infrastructure mode. However, it is further extended to include mesh-specific parameters necessary for:

- identifying the MBSS – Mesh ID and Mesh Configuration elements, which uniquely identify the MBSS and describe its critical configuration parameters which joining STA mush adhere to (see 3.6.1),
- establishing the peering itself – Mesh Peering Management element (Fig. 64) supplemented by the base IEEE 802.11 frame header (TA and RA fields), which allows peering identification to be established.

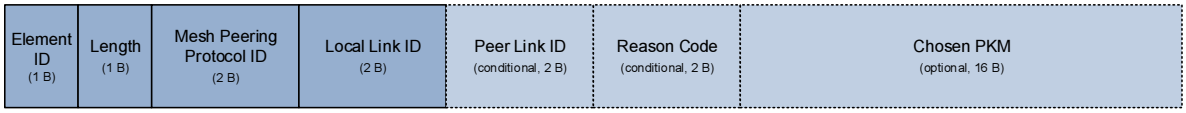

Fig. 64 Mesh Peering Management element

As shown in Fig. 64 Mesh Peering Management element provides information necessary to uniquely identify the peering and can optionally provide additional information concerning reason of its rejection or termination:

- Mesh Peering Protocol ID indicates peering protocol used to maintain the peering: MPM or AMPE,
- Local Link ID contains local ID of the peering (in previously described form),
- Peer Link ID is optional (its presence is indicated by appropriate value of Length field) and if present contains ID of the peering assigned by peer STA,
- Reason Code if present in Mesh Peering Close frames and specifies reason for peering termination or rejection,
- Chosen PMK is present only in case of AMPE and indicates ID of Pairwise Master Key used to protect the frame.

Station receiving such a Mesh Peering Open frame will verify if the Mesh ID and Mesh Configuration values match ID and configuration of its MBSS – if there are any inconsistencies the peering attempt will be rejected by sending Mesh Peering Close (see Peering termination section below) message with a reason code of MESH-CONFIGURATION-POLICY-VIOLATION.
Mesh Peering Instance Controller of receiving station then checks if it is allowed by configuration parameters to accept additional peerings and if it is so, it decides if this particular peering should be

accepted. Negative decision on any of these steps also results in sending of Mesh Peering Close frame with, respectively, MESH-MAX-PEERS or MESHPEERING-CANCELED reason codes.

If the decision is to accept the peering, a Mesh Peering Confirm frame is sent to the peering initiator, containing confirmation of peering parameters and Association ID assigned to peering initiator by receiving STA, necessary for proper operation of Power Saving mechanisms of IEEE 802.11 wireless link:

- Capability
- Association ID (AID)
- Supported Rates
- Extended Supported Rates
- **Mesh ID**
- **Mesh Configuration**
- **Mesh Peering Management**
- HT Capabilities
- HT Operation
- 20/40 BSS Coexistence element
- Extended Capabilities element
- Vendor Specific elements

As in case of Mesh Peering Open management frame, Mesh Peering Confirm frame structure is closely
Based upon Association Response management frame and serves analogous purpose. The list of fields is truncated compared to Association Response frame, because a number of mechanisms designed to supplement IEEE 802.11 network in infrastructure mode is not applicable in case of an MBSS (for example: Fast BSS Transition, as a mobile STA in an MBSS will change its peerings instead of changing a BSS). Additional mesh-specific elements are the same as in case of Mesh Peering Open management frame – they confirm mesh identification and its obligatory parameters (Mesh ID and Mesh Configuration elements) and provide Mesh Peering Open frame sender with peer-specific peering identification parameters (Mesh Peering Management element).

Additionally, accepting STA sends a Mesh Peering Open frame to the initiator of the exchange, with parameters describing the wireless link holding the same values as in previous Mesh Peering Open/Mesh Peering Confirm exchange and Mesh Peering Management field modified to reflect the fact that now the previously accepting STA has become a peering initiator.
This Mesh Peering Open frame must be received by the STA which originally initiated the peering procedure, by sending appropriate Mesh Peering Confirm frame.

When both STAs have sent Mesh Peering Open frame and have received its confirmation in form of Mesh Peering Confirm frame, the peering is established.

3.6.3.1.2 Peering termination

If station needs to terminate an existing peering or if a peering procedure needs to be aborted in progress, a Mesh Peering Close frame is sent, containing Mesh ID and Mesh Peering Management element:

- Mesh Peering Protocol ID indicates peering protocol used to maintain the peering: MPM or AMPE,
- Local Link ID contains local ID of the peering to be terminated,
- Peer Link ID is optional (its presence is indicated by appropriate value of Length field) and if present contains ID of the peering to be terminated assigned by peer STA,
- Reason Code specifies reason for peering termination,

- Chosen PMK is present only in case of AMPE and indicates ID of Pairwise Master Key used to protect the frame.

There are currently 66 different Reason Code values defined for Mesh Peering Close frame, covering various errors which can be encountered by a number of different mesh mechanisms resulting in peering termination, and a set of reasons connected with decisions taken by mesh management mechanisms.

Upon reception of a valid Mesh Peering Close frame, indicating termination of an existing peering, a STA needs to respond with its own Mesh Peering Close frame describing the peering being terminated from its own perspective (Local Link ID, etc.).

3.6.3.2 Authenticated Mesh Peering Exchange

The Authenticated Mesh Peering Exchange (AMPE) protocol is designed to establish an authenticated mesh peering between two STAs in a secure manner. The prerequisite for AMPE is the existence of Pairwise Master Key Security Association (PMKSA) before initiation of the protocol, so an authentication of participating stations must have already been performed.
The AMPE provides a mesh peering protected by an appropriate Temporal Key Security Association (TKSA) and a Group Temporal Key Security Association (GTKSA) for each of two participating STAs. As a result both stations can fully participate in a secured MBSS activities, being able to process both unicast and group-addressed, protected traffic. For this purpose the protocol needs to perform three specific tasks:

- security capabilities selection allowing two STAs to agree upon the security parameters used in the particular instance (and, as a result, for a particular mesh peering),
- key confirmation, providing verification that both STAs possess a correct PMK and that the integrity of protocol frames exchanged between is maintained,
- key management, responsible for generating and maintaining of temporal keys used in TKSAs and as MGTK.

The described protocol utilizes the same management frames as MPM protocol described above, but each of its messages is extended by adding additional:

- RSN element (Fig. 65) located before Mesh ID,
- Message Integrity Control (MIC) added after Vendor Specific elements,
- Authenticated Mesh Peering Exchange (AMPE, Fig. 66) element added at the end of the frame.

The exchange Mesh Peering frames in case of AMPE is the same as in case of MPM, however, the additional fields listed above allow AMPE to fulfil additional, security related tasks.

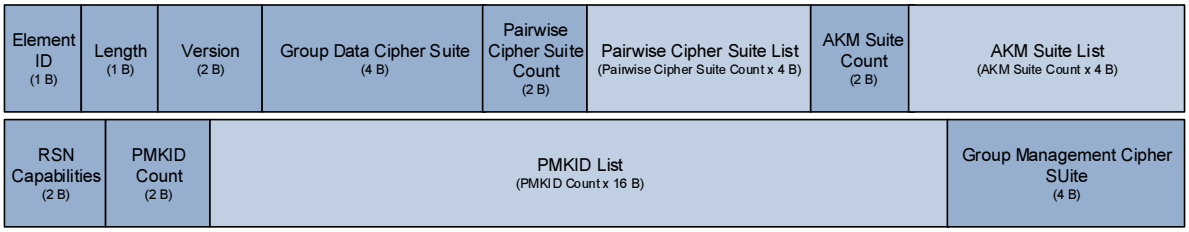

Fig. 65 RSN element

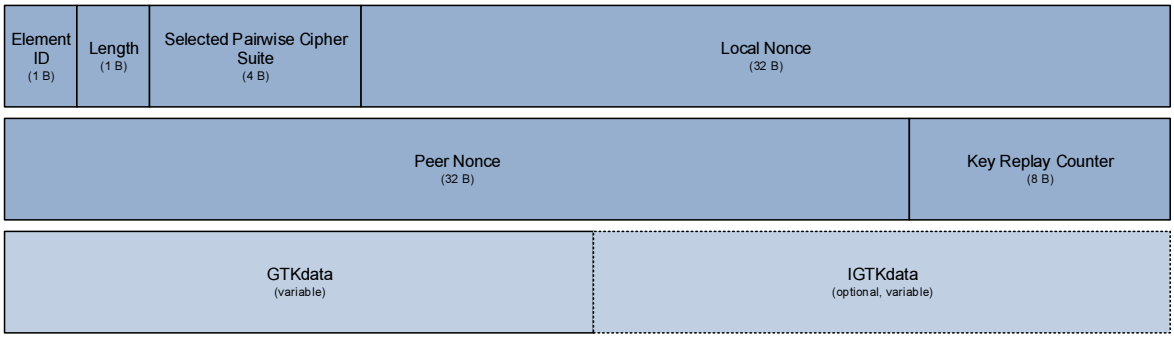

Fig. 66 Authenticated Mesh Peering Exchange element

3.6.3.2.1 Key confirmation and integrity protection

Mesh Peering Management frames used in AMPE protocol are protected according to AES-SIV specification [83]. This method allows to perform authenticated encryption of a data block and authenticate additional block of data (Additional Authenticated Data – AAD).

When encrypting it takes a key, plaintext data to encrypt and authenticate and AAD data blocks. As a result a Synthetic Initialization Vector (SIV) and encrypted ciphertext are obtained.

When decrypting/verifying it takes a key, SIV, ciphertext and AAD data blocks. As a result a decrypted plaintext and verification confirmation is obtained, indicating that both resulting plaintext and accompanying AAD data blocks are not modified.

When building an AMPE versions of Mesh Peering Management, Authenticated Mesh Peering element is a plaintext to be encrypted and all content of the frame, starting from Category indication (inclusive) and ending with MIC element (exclusive), supplemented with values of localMAC and peerMAC of the intended peering are treated as AAD. Resulting SIV is used as MIC field, while Authenticated Mesh Peering Exchange element is transmitted in its encrypted form.

As for the process to be completed successfully both stations must possess the same encryption key, and Authenticated Encryption Key (AEK, part of PMKSA) is used for this purpose, only stations which are successfully authenticated and possess a valid PMKSA can perform an AMPE peering.

3.6.3.2.2 Security capabilities negotiation

Security capabilities negotiation is carried out with use of RSN and AMPE elements shown in Fig. 65 and Fig. 66. Both pairwise cipher suite selection and group cipher suite selection procedures described below are performed simultaneously during AMPE peering.

Pairwise cipher suite selection

In the Mesh Peering Open frame, the sending station includes a list of its supported pairwise cipher suites in descending order of preference.

Upon reception of such frame, the receiving STA will calculate an intersection of the received list and its own preference-ordered list of supported pairwise cipher suites and select from the resulting set of mutually supported cipher suites the one which is of the highest preference for the STA with highest (lexicographically) MAC address.

This selection is then indicated in Selected Pairwise Cipher Suite field in the AMPE element of Mesh Peering Confirm frame, finalizing the selection.

It should be noted, that MPM protocol requires two symmetric Mesh Peering Open – Mesh Peering Confirm exchanges. AMPE protocol should verify that pairwise cipher suite selection-related results of both exchanges are identical – if they are not, the peering fails with MESH-INVALID-SECURITY-CAPABILITY reason code sent within Mesh Peering Close management frame.

Group cipher suite selection
To perform a selection of a group cipher suite the sender of Mesh Peering Open frame indicates its chosen group cipher suite in RSN element of the frame.
Upon reception of Mesh Peering Open management frame, receiving STA verifies if it supports the indicated group cipher suite. If it is supported, a Mesh Peering Confirm frame can be sent, indicating the group cipher suite used by its sender.
If either the receiver of Mesh Peering Open or Mesh Peering Confirm does not support the cipher suite indicated by its peer, it terminates the peering with Mesh Peering Close message showing MESH-INVALID-SECURITY-CAPABILITY reason code.

3.6.3.2.3 Key Management
To successfully perform AMPE peering, involved stations need to be authenticated, which results in creation of PMKSA mentioned before.
A part of PMKSA, an Authenticated Encryption Key statically derived from PMK is used for protection of Mesh Peering Management frames as described earlier in this section.
An additional key, a Mesh Temporal Key (MKT) is also derived from PMK using additional information describing a particular peering and random Nonce values, exchanged during peering creation in appropriate fields of the encrypted Authenticated Mesh Peering Exchange element.
MKT is used to protect communication between two mesh stations and can be refreshed by the stations at any time by re-invoking the described AMPE peering procedure.

3.7 Multihop path selection and frame forwarding

As one of the most characteristic functionalities of wireless mesh networks is their ability to deliver data to its specified destination in a multihop manner, mechanisms directly dedicated to support this functionality are of fundamental importance. They define the core of a discussed wireless mesh solution, based on wireless transmission capabilities of underlying technology and supplemented by various configuration and management mechanisms.
In case of IEEE 802.11s wireless mesh standard, these core mechanisms, directly providing multihop data delivery capability, are a path selection and frame forwarding.

Frame forwarding procedures are responsible for preparing received wireless frames of specific types for a next transmission necessary to eventually deliver them to their indicated destination. They are not responsible for tasks related to a wireless transmission itself, as these are handled by dedicated mechanisms of the underlying wireless transmission technology. For their operation, frame forwarding mechanisms require a number of information databases, most important being:

- forwarding information table – providing next-hop information for an indicated frame destination,
- precursor list – detailing permissible transmitters of frames intended to be forwarded to an indicated destination, used for security and error handling.

These databases need to be populated and maintained by path selection mechanisms, responsible for obtaining the data required for efficient operation of frame forwarding mechanisms.

To facilitate the following description of multihop frame forwarding and path selection mechanisms, it seems advisable to clearly define a number of terms used through the text:

- Frame originator/source – an entity (within or outside an MBSS) which originally created the frame. Identified by a Source Address (SA).
- Frame destination/target – an entity (within or outside an MBSS) which is a final destination of the frame. Identified by a Destination Address (DA).

- (Mesh) path – multihop transmission path through a number of stations within a given MBSS.
- (Mesh) path originator – a mesh STA which initiated a path discovery process to establish a mesh path to a mesh target station. Most often a mesh source station.
- (Mesh) path destination/target – a mesh STA to which a mesh path originator attempt to establish a path.
- Mesh source station – a mesh STA which is the first in a given MBSS to send a frame to another STA. It may or may not be a frame source. is a mesh path originator. Identified by a Mesh Source Address (MSA).
- Mesh destination station, mesh target station – a mesh STA which is the last in a given MBSS to send a frame to another STA. It may or may not be a frame target. Identified by a Mesh Destination Address (MDA).
- Frame transmitter – a mesh STA which transmits a frame over the wireless medium. Identified by a Transmitter Address (TA).
- Frame receiver – a mesh STA which receives a frame over the wireless medium. Identified by a Transmitter Address (RA).

3.7.1 General multihop forwarding procedures

Multihop frame forwarding service within an IEEE 802.11s MBSS is supported in case of two broad types of frames: Mesh Data frames (QoS Data frames with Mesh Control Present subfield in the QoS Control field is set) and Multihop Action Management frames. There is also a number of other frame types used in procedures resulting in an MBSS-wide transmission (for example path discovery), but frames used there are not forwarded, but received after passing each transmission link and after processing their content, a new a messages are generated to be sent further.
Both of the abovementioned frame types utilize variable-size Mesh Control field (show in Fig. 67, located at the beginning of IEEE 802.11 Frame Body) to extend the information provided by a general IEEE 802.11 MAC header with elements required for multihop frame forwarding.

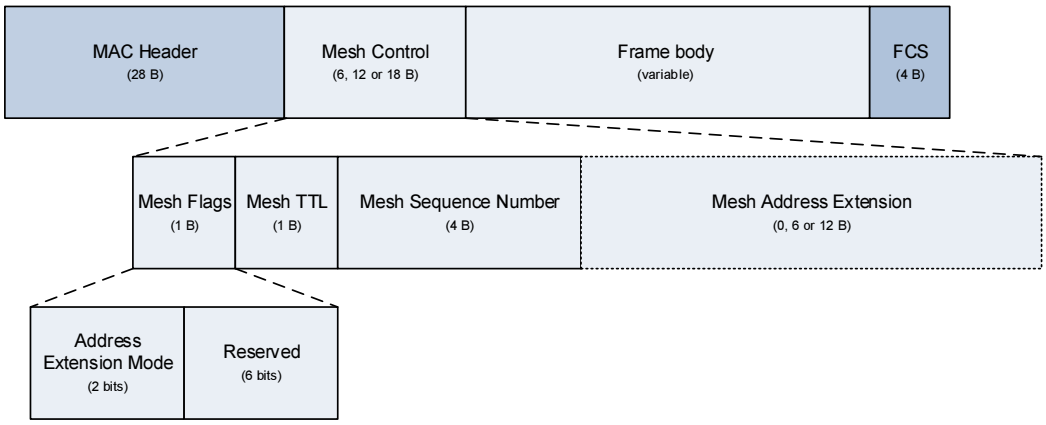

Fig. 67 Mesh Control field

Mesh Control field provides Mesh Time to Live indicator (Mesh TTL) indicating a remaining number of mesh links which a given frame can traverse before it is dropped in order to prevent infinite frame looping.
Mesh Sequence Number is an identifier assigned to a particular frame by its originating STA within an MBSS and used by other STAs to detect its duplicates, which are then silently dropped. The identifier is maintained separately by each originating mesh station and is based on a modulo-2^{32} counter.

Mesh Flags field currently contains only a single subfield specifying an Address Extension Mode used for the frame. Depending on its value, Mesh Control field can contain from 0 to 2 Mesh Address Extension subfields, which are used for different purposes depending on type of the frame and type of its destination address (individually or group addressed), as described in Section 3.3.8.

3.7.1.1 Individually addressed frame forwarding

Stations in an IEEE 802.11s MBSS are using two information tables to perform unicast frame forwarding services:

- forwarding table – indicates a next-hop STA in a path to a particular destination address,
- precursor list – used to identify legitimate transmitters of unicast frames and in process of recovery from link failures.

It should be noted, that frame forwarding services of MBSS network described in this section, allow a frame to be delivered within an MBSS boundaries – from a STA belonging to a particular MBSS to a STA in the same MBSS. Interworking procedures used to handle inter-mesh traffic will be described in Section 3.8.

The base information required to forward a frame towards its MBSS destination is kept in STA's forwarding table. This table contains forwarding information if form of entries specifying:

- Destination MAC address – a destination MAC address to be compared with Mesh Destination Address (MDA) to determine, if a particular entry is to be used in forwarding of specific frame,
- Next-hop – a MAC address of a peer STA which should receive the frame ,
- Path metric – metric of the path from the current STA to a destination indicated by destination MAC address,
- Number of hops – number of hops from the current STA to destination indicated by destination mac address,
- HWMP Sequence Number – used to determine relative freshness of the forwarding table entry compared to a newly received updates,
- Lifetime – time for which the information record should be considered to be valid.

The forwarding information table is populated by a path selection protocol (see Section 3.7.3) and the records can be refreshed by the same protocol or by processing of multihop frames being successfully forwarded by the STA to a particular destination. Entries which are not updated and their lifetime expires are removed.

The precursor list contains addresses of peer stations allowed to forward to this STA multihop frames addressed to a specified destination. The entries contain a destination STA MAC address, precursor STA MAC address and lifetime for the entry. The precursor list is also populated by path discovery mechanisms.

When a STA originates an unicast multihop frame, it fills its address fields according to rules described in Section 3.3.8. In case of unicast frames, Address 3 indicates a Mesh Destination Address (MDA) while Address 4 holds a Mesh Source Address (MSA). Address 2, which indicates an address of a transmitting station for a particular hop is also set to MAC address of the originator.
The sending station will also set a Mesh TTL field to control the maximum hop-count of the frame and a Mesh Sequence Number to identify the frame and allow receiving stations to discard its potential duplicates (a mechanism required mainly in case of group addressed frames).
The station then consults its forwarding table and sets Address 1 to an address taken from a Next-hop field of an entry corresponding to an appropriate destination MAC address, indicating a peer which will be a direct receiver of the upcoming frame transmission.

The frame is then transmitted using a wireless medium to be received by the next-hop STA indicated in Address 1 field. The transmission is carried out according to a standard unicast rules, normally requiring an acknowledgement to be sent by the receiving STA, and subject to retransmission if the acknowledgement is not obtained by the sender within a specific time.

When a STA successfully receives a valid wireless frame, it compares its MAC address with Address 1 field and processes the frame only if they match.
The station then checks if the frame has been transmitted by one of its peer stations, by comparing its peer list with Address 2 of the frame. Frames transmitted by non-peer stations are silently discarded.
As a next step, the STA consults its precursor list table, to determine if the frame has been transmitted (indicated by its Address 2 field) by a STA allowed to send it the frames for a particular MDA. If not, the frame should be discarded.
The station then compares its own address with frame's Address 3 field, to determine if it is a final destination of the frame within an MBSS. If it is, the frame is handed to higher layers for further processing.
It not, the station will decrement the value of a Mesh TTL field of the frame (located in its Mesh Control field). If its value is reduced to 0 as a result of this operation the frame is discarded.
Next, the STA will perform a forwarding frame lookup to determine a next-hop address for a particular MDA and update Address 1 field accordingly. Address 2 field will also be updated to the stations own address to properly indicate the transmitting station.

Additionally, the successful completion of the forwarding procedure described above results in refreshing of the appropriate entries in forwarding and precursor lists.
Moreover, the described procedures assume that appropriate information is already present in forwarding and precursor tables due to activity of path selection mechanisms triggered by a mesh source station of the frame or working proactively.
The situation when a mesh STA receives an unicast frame (STA is not its originator) which should be forwarded and the frame's destination address is not listed in forwarding information database is considered an abnormal one. Mesh path selection mechanisms should ensure that forwarding information databases of all STAs on the transmission path contain appropriate entries. To rectify the situation, the STA has a choice to perform any combination of the following:

- discard the frame,
- initiate path selection procedures for the indicated destination address,
- inform its precursor STA of unreachability of the destination to trigger path recovery procedures (see 3.7.3.3).

3.7.1.2 Group addressed frame forwarding

As the IEEE 802.11s standard lacks support for multicast transmission, all group addressed frames are forwarded as broadcast frames using a three address version of IEEE 802.11 MAC header is used, with:

- Address 1 indicating the destination group address (MDA), which is, due to lack of multicast support in IEEE 802.11s standard, the same as the receiver address (RA) – all receivers must process the frame,
- Address 2 identifying the currently transmitting station (TA),
- Address 3 specifying an initial originator of the frame (MSA).

An appropriate Mesh TTL and Mesh Sequence Number will also be set and the resulting frame will be transmitted over a wireless link.

All stations which successfully receive the frame will proceed to process it, by first checking if it has been sent by one of their peer stations. If not, the frame is silently dropped.
Next, the receiving STA will check if it already received a copy of the frame, by examining an MSA and Mesh Sequence Number (MSN) value pair and comparing it to a list of such pairs recorded from recently received frames. If the frame is a duplicate, it will be dropped, if not, its MSA/MSN value pair will be recorded. This process is a strict necessity for group addressed frames, as each of receiving stations will retransmit them once, resulting in each STA receiving the frame multiple times. The Mesh TTL field will then be decremented by 1 and checked if it reached 0. If it is the case, the frame will be dropped, limiting the range of the broadcast flooding. The frame with non-zero Mesh TTL value will be updated by placing the STA's address in Address 2 field (to properly identify the new frame transmitter) and transmitted over the wireless link.

It should also be noted, that broadcast frames are transmitted in an unreliable manner, without requiring the receiving STA to confirm their reception using an appropriate acknowledgement mechanism. Such approach reduces the management overhead of a broadcast transmission, but at the same time the probability of the broadcast missing a single STA or even a part of the network can be considerable. The risk of such occurrence is reduced by the fact, that each station is likely to receive the same frame from all of its peer stations.
To further reduce the risk of losing a group addressed frame, a transmitting STA can optionally forward such frame as a number of unicast frames individually addressed (Address 1, with Address 3 indicating group MDA and Address 4 - MSA) to each of its peer STAs instead of employing a single group addressed transmission.

3.7.2 Metric

In case of unmodified AODV metric used for path selection is a number of transmission hops on a given path. Such solution does not take into account the quality of links traversed which makes it poorly suited for wireless environment, where different links can provide a radically different transmission quality. To address these issues, RM-AODV employs Airtime Metric as a measure of link quality, taking into account both their current maximum data rate and transmission error rate - see equation (1).

$$c_a = \left[O + \frac{B_t}{r}\right] \frac{1}{1-e_f} \tag{1}$$

where C_a is link Airtime Metric value, O - technology dependent transmission overhead, r - link throughput, B_t – size of the test frame and e_f - frame error rate for a given B_t .
Link load is not taken into account directly, due to rapid and unpredictable changes of this parameter in case of wireless multihop systems, but its impact is reflected by link error rate parameter (which is significantly higher in case of highly loaded links). Airtime Metric can be seen as an amount of link resources necessary to transmit a frame.

3.7.3 Hybrid Wireless Mesh Protocol

The default path discovery solution chosen for the IEEE 802.11s system is called a Hybrid Wireless Mesh Protocol (HWMP). It consists of both reactive and proactive path discovery mechanisms, both able to function concurrently to provide fast response, adherence to changing transmission conditions and minimization of management overhead.
However, the standard allows for extensibility of path selection protocols, including the ability to use alternate path discovery solutions, as long as the same, single solution is utilized uniformly through

the mesh network. Despite the fact, the obligatory HWMP protocol must also be supported by all IEEE 802.11s devices, for the sake of compatibility.
Peering management mechanisms (described in Section 3.6.3) are responsible for assessing node capabilities and deciding, if connecting station is able to participate in a given mesh procedures. The same mechanisms are then responsible for configuration of the newly connected node to use the appropriate path selection protocol.

The basic, obligatory path discovery mechanism of HWMP is a reactive Radio Metric Ad hoc On-Demand Distance Vector (RM-AODV) protocol based on a well-known AODV protocol [81] designed for IPv4 systems. The classic AODV protocol has been modified to use ISO-OSI layer 2 addresses and utilize a link metric instead of a simple hop count.
Proactive mechanisms of HWMP are optional and provide capability to distribute and maintain forwarding information for a number of chosen STAs, named root stations. Due to continuous management traffic generation required by proactive mechanisms, they have several deployment options and configuration parameters, making it possible to deploy them in a manner appropriate for a specific mesh structure and user requirements.

HWMP protocol utilizes HWMP Path Selection Mesh Action Management frames (frame type: Management, subtype: Action, category: Mesh Action, Mesh Action: HWMP Path Selection). The specific function of HWMP Path Selection frame is determined by presence of appropriate Information Elements (IEs) in its data field:

- Path Request IE (PREQ IE) – sent by initiators of path discovery process. Creates a so called reverse path (path towards the initiator of the discovery). Can also be used for to initiate a path verification process.
- Path Response IE (PREP IE) – sent in response to PREQ IE. Creates forward path towards the target of a path discovery process.
- Path Error IE (PERR IE) – sent by STAs on an active transmission path to indicate unexpected unreachability or lack of appropriate forwarding information.
- Root Announcement IE (RANN IE) – used in one of proactive mechanisms of HWMP protocol, allows an easy assessment of distance to a specified root station.

All of the above IEs are, most often, transmitted through the MBSS in a multihop manner, but it should be noted, that HWMP Path Selection frame is not a Multihop Action frame and as such is not a subject to forwarding procedures described in Section 3.7.1. It is an Information Element contained in such frame (sometimes called a message – for example a PREQ message), which is retransmitted through the network by intermediate stations, not the frame itself.

With multiple stations maintaining their own forwarding-related databases, it is imperative to be able to assess the freshness of received information relative to information already possessed. For this purpose, a HWMP Sequence Number (HWMP SN) is introduced, which is always appended to any forwarding related information being sent or stored.
Each MBSS station maintains its own HWMP SN counter (modulo 2^{32}). When a given station generates a forwarding-related information to be transmitted to other stations (which effectively includes sending any of the HWMP-related IEs mentioned before, although there are special cases), it will increment its current HWMP SN counter and attach the resulting value to the transmitted information.
When a station adds new information to its forwarding table based on received HWMP IE, it will append it with a HWMP SN received with the IE. Such entry then cannot be updated or removed based on information with lower HWMP SN, as it is understood that it is based on more recent knowledge.

3.7.3.1 Reactive routing: Radio Metric Ad-hoc On-demand Distance Vector protocol

In keeping with reactive nature of RM-AODV protocol, a path discovery procedure is initiated when a station being in possession of a frame to be forwarded does not possess a relevant entry in its forwarding table. The procedure is obligatory if the station is a mesh source station for the frame (the first station of the particular MBSS to possess the frame, often its initial sender) and optional, if the station is an intermediate station on the mesh path, which should, but does not have an appropriate forwarding information.

3.7.3.1.1 Initiation of a new path discovery procedure

The STA initiates a reactive path discovery by preparing and sending a HWMP Path selection frame containing a Path Request Information Element (PREP IE, Fig. 68). Normally this frame type is sent to all peer stations as a broadcast frame. However, due to the fact, that broadcast transmissions are handled in an unreliable manner (without acknowledgements and retransmissions), a STA can decide to use a number of unicast frames addressed individually to all its peer stations instead.
Before sending the PREP IE, the originating station will also increase its HWMP SN by 1, and use this new value in Originator HWMP SN field of the IE to indicate that updated information present in the IE requires attention of its recipients.

As all IEEE 802.11 IEs, the PREP IE type begins with Element ID identifying it as a PREP IE, followed by an Length field indicating its length in bytes.
The subsequent Flags field indicates the specific type of path selection procedure, as the PREP IE is used in various procedures of both reactive and proactive HWMP path selection.
In case of RM-AODV path discovery means setting Gate Announcement and Proactive PREP fields to 0, as they indicate proactive use of the PREP IE.
Addressing Mode bit will indicate if the IE has been sent by a broadcast frame (0) or as a group of unicast frames (1) as described before.
The Address External (AE) bit will indicate if the frame to be delivered, which made the STA initiate the path discovery process has been generated by the STA itself (value 0) or if it has been received by the STA from external network (value 1, possible when the STA is a mesh gate). In the latter case the STA will perform a path discovery as a proxy for the external frame original sender, by using its own address as Originator Mesh STA Address and the original sender's address in Originator External Address field. This last field is only present when the AE bit is set. Detailed description of interworking procedures has been provided in Section 3.8).

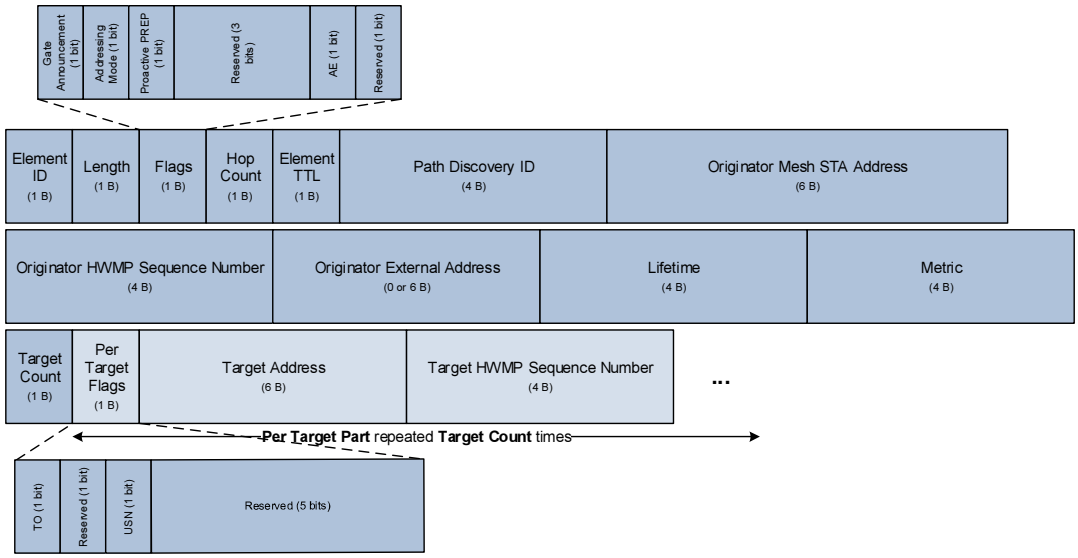

Fig. 68 Path Request (PREQ) Information Element

As the PREP IE will be transmitted through the MBSS in multihop manner, an Element TTL field is present to prevent infinite forwarding of IE and allows limiting a PREP dissemination through an MBSS structure. The Element TTL field will be decreased by 1 at each receiver. If it reaches 0, the IE will not be retransmitted further.

Each new path discovery initiated by a given STA is usually preceded by incrementing a HWMP SN, as it results in dissemination of updated information concerning the path originator STA through the MBSS. Its value is included in Originator Mesh STA HWMP SN field, while the STA itself is identified by its MAC address in present in Originator Mesh STA Address field.
Additionally, each path discovery procedure initiated by a particular STA is assigned an unique Path Discovery ID (DPID), which combined with the path originator STA address will identify it in a precise manner within a specific MBSS. This additional identifier is necessary, because it is not required for a path originator STA to assign an unique HWMP SN for each path discovery procedure.

As a single path discovery procedure can be used to establish mesh paths to multiple mesh destinations, a Target Count field is used to indicate the number of path discovery targets.
Each of them is described by a set of three fields:

- Per Target Flags – contains a Target Only and Unknown Target HWMP SN indicators:
    - Target Only (TO) – when set to 1, only requested path target STA can send response to the PREQ IE, when set to 0, also an intermediate STA which has a path to the target STA can send such response. This procedure is described in more detail in 3.7.3.1.6.
    - Unknown Target HWMP SN (USN) – if the path originator has any information concerning a target in its databases (for example a path with expiring lifetime which it wants to refresh), the field is set to 0, and the HWMP SN of such information is included in Target Sequence Number field. If the path originator does not have any information concerning the target, the indicator is set to 1.
- Target Address – uniquely identifies the target of path discovery procedure by providing its MAC address.
- Target Sequence Number – if USN field is set to 0, the field holds a HWMP SN of the most recent information the originator has about the target.

As the procedure which employs PREQ IE aims to discover the best path between the path originator and target stations, the message need to include some indicator of preference which can be used to differentiate between multiple possible paths. Two fields are dedicated to this task: Hop Count and Metric. Hop count field, initially set to 0 by the path originator will be incremented by one at each intermediate station it will traverses when sent and indicates a number of wireless links it passed through.
Metric field is initially set to a configured initial value (most often 0) by the path originator STA and will be incremented by each intermediate STA the PREQ IE will arrive at by the value of a link metric it arrived through. The resulting value represent an additive path metric based on a set of link metrics and is a main criteria in choosing the path and assessing its quality.

The PREQ IE constructed according to the described rules is subsequently sent by the originating STA to all of its peer STAs as a broadcast HWMP Path Selection frame (or a set of unicast frames).
Each receiving peer STA needs to make two decisions:

- should the information contained in the received PREQ IE be used to update its forwarding information table?
- should the received PREQ IE be retransmitted to its peer stations?

3.7.3.1.2 Updating of a forwarding information table

To make these decisions, the receiving STA checks its forwarding table, to see if it already contains information about the path originator with a greater HWMP SN then received in PREQ IE. If so, the PREQ IE is considered to be outdated and is discarded, as a PREQ IE based on more recent knowledge has already have been received from the originator. Such PREQ IE will not be used to update the STA's forwarding information and it will not be retransmitted.
If the receiving STA does not have any forwarding information concerning the originator STA or the information has lower HWMP SN then the received PREQ IE, it means that the received information is more recent that the one the receiving STA already has. In this case the information from PREQ IE will be used to update the STA's forwarding table and then will be retransmitted to its peer stations.

If the receiving STA has information about the path to the originating STA with the same HWMP SN as the information in the received PREQ IE, the STA will assume that the received information has been generated by the originator STA based on equally current knowledge as the one already received. Such assumption means that any change in the content of the information contained in the PREQ IE must be a result of the path it had taken to reach the receiving STA. Thus the STA will only be interested in the content of the PREQ IE if it provides information about a better path to its originator – if such PREQ IE contains a path metric value to the originator STA which is:

- higher than the one in forwarding table – the PREQ IE contains current information (the same HWMP SN), but it is also discarded, because the STA already received PREQ IE which arrived through the better path (smaller path metric).
- the same or a lower than the one in forwarding table – the PREQ IE contains a current information (the same HWMP SN) and arrived by the best path (smallest metric) yet. Such PREQ IE will be used to update the STA's forwarding information.

If the STA decides to accept the PREQ IE, it updates its forwarding information by recording:

- MAC address of the PREQ IE originator STA, as destination address,
- the station that it received PREP from, as its currently known best next-hop on a path to PREQ IE originator,
- the hop count of the IE incremented by 1 (to take the last hop into account), as a hop count of the best currently known path towards the PREQ IE originator,
- the metric of the IE incremented by a metric of the link to a peer it arrived from, as a path metric of the best currently known path towards the PREQ IE originator.

This information will be considered current in the time frame indicated by Lifetime field of the accepted PREQ IE, set by its originator.

3.7.3.1.3 Retransmission of a PREQ IE

Having decided if it should use the PREQ IE to update its forwarding table, the STA must also make a decision whatever the IE should be retransmitted.
If the PREQ IE has been used to update the STA's forwarding information, the STA will retransmit it to its peer stations, as it contains previously unknown information resulting in discovery of a better path that was known before.
The PREQ IE will also be retransmitted if the STA decided, that while it does not provide information resulting in discovery of a new best path to the originating STA, the information is contains still current and the STA has not yet retransmitted a PREQ IE in a given path discovery procedure. In other worlds, the PREQ IE will also be retransmitted if its HWMP SN is equal to the HWMP SN associated with its originator in the STA's forwarding table and the Path Discovery ID/Originator Mesh STA Address combination has not yet been encountered by the receiving STA.

It the decision is to retransmit the PREQ IE, its content will be updated (new hop count and metric values) and then PREQ IE will be re-sent (by broadcast or a set unicast messages) to all peer stations of a given STA.

3.7.3.1.4 Establishment of a reverse path

As a result of the described procedure the PREQ IE will be flooded through the MBSS (as shown in Fig. 69 by red, dotted arrows), and will possibly reach each of the STAs (within an area limited by the value of Element TTL field) from multiple peers, due to the fact that different copies of this message will arrive by a number of different paths. It will be accepted and re-transmitted more than once only if the new copy arrived by a better path – in such case it will also overwrite the forwarding information based on a copy of a given PREQ IE which arrived earlier, but through a less preferable path.
The PREQ IE flooding procedure results in creation of a forwarding information entry indicating a next-hop in path towards the path originator in all receiving stations, thereby forming a so-called reverse path, shown as blue arrows in Fig. 69.

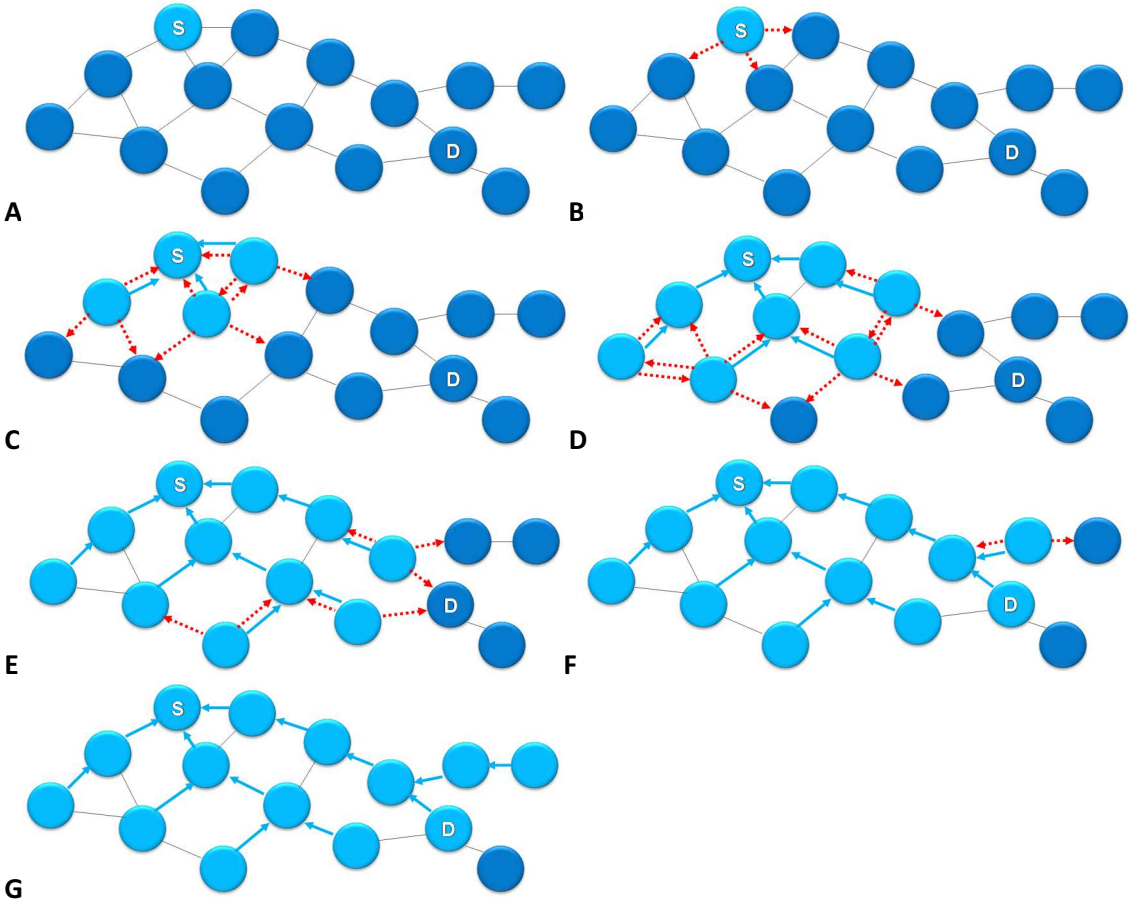

Fig. 69 RM-AODV reverse path formation steps

It should be noted, that the described procedure is, by default, conducted with use of HWMP Path Selection Frames sent to a broadcast address and such frames are not subject to reception acknowledgement and retransmission procedures. This solution have been chosen to lower the resource consumption and process delay at a cost possibility of missing an optimal path due to a loss of Path Selection frames.

3.7.3.1.5 Response to a path request

When an intended target of the path discovery procedure (destination station) receives and accepts a PREQ IE, it updates its forwarding information for the path originator STA completing the reverse path from the path target to path originator. Then, instead of re-broadcasting the PREQ IE, it generates a Path Replay Information Element (PREP IE) shown in Fig. 70.
It should be noted, that it is possible that the transit stations will re-broadcast PREQ from the same discovery procedure multiple times and the destination node will generate multiple PREP messages, if they receive multiple subsequent PREQ IEs with a decreasing path metric. However, due to the fact that smaller metric most often corresponds to shorter transmission delay, it is not likely.

Target HWMP Sequence Number of the PREP IE will be set to a current value of the responding STA's HWMP SN counter, to indicate the freshness of information contained therein. Originator HWMP Sequence Number contains the HWMP SN value obtained from the PREQ IE which triggered the response. It will allow the path originator to associate the response with a specific state of its forwarding table which required initiation of this specific path discovery.

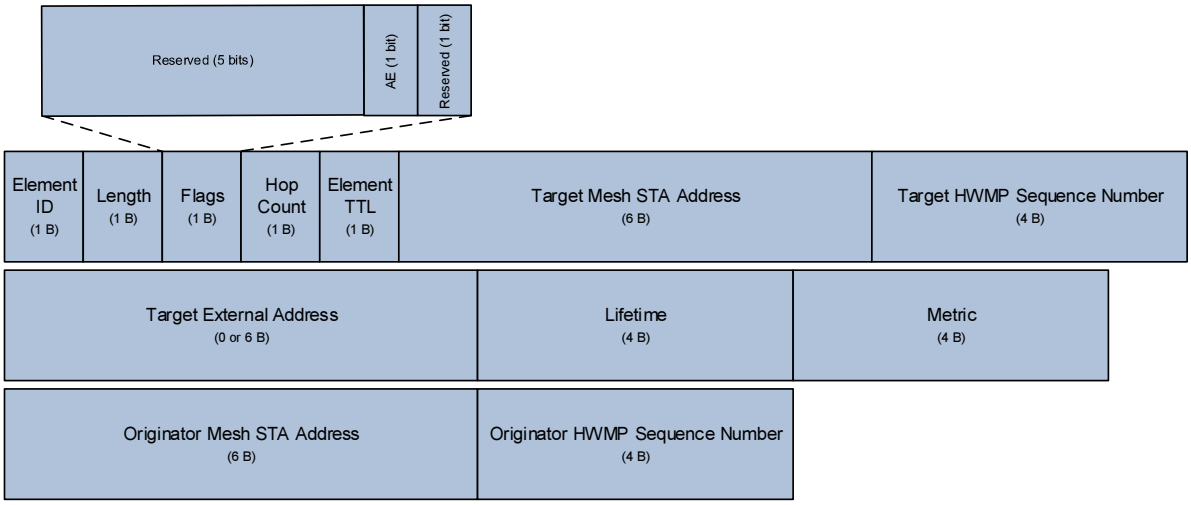

Fig. 70 Path Reply (PREP) Information Element

The structure of PREP IE follows the standard IE requirements, beginning with Element ID (identifying IE as a PREP IE) and Length fields.
The following Flags field includes only an Address External (AE) indicator, used to specify if the responding station is indeed the final destination requested in PREQ IE Target Address field (value 0) or is it a mesh gate responding to PREQ IE as a proxy for an external destination (value 1) as per interworking procedures described in Section 3.8.2. The optional Target External Address will be present and set to the target address of the path discovery only if the STA responds as a proxy.
Element TTL value will limit a number of time the PREP IE can be retransmitted by successive intermediate stations, before it is dropped. The field should be set to a value at least as high as hop count of PREQ IE which triggered the response. Hop count field is set to 0 by the sending station and will provide information about the number of wireless links the IE traversed. Similarly, the Metric field will be set to a configured initial value and incremented by consecutive link metric values, as the PREP IE is sent through the MBSS.

Target Mesh STA Address field will contain an address of the responding STA. If the responding STA is also a path discovery target, the address will be the same as the Target Address specified in PREQ IE. However, if the Target Address is external to the MBSS and the response is generated by a mesh gate proxying for such address, the field will contain an address different from the Target Address

specified in the Path Request. In such case AE flag will be set to 1 and the requested target address will be present in Target External Address field, indicating an extra-MBSS destination.

The PREP IE is sent to PREQ IE originator as an unicast HWMP Path Selection frame, along the just discovered (reverse) path shown in Fig. 71 by blue arrows. The PREP IE is forwarded (red dotted arrows) by intermediate stations along the reverse path, each of them updating its forwarding table following the same rules as in case of a PREQ message and thus creating a forward path towards the path target STA (orange arrows).

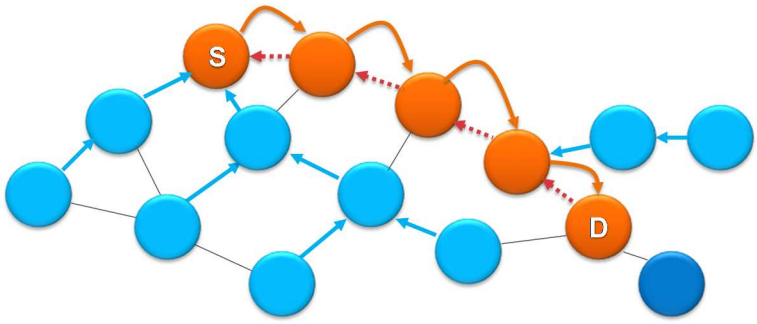

Fig. 71 RM-AODV forward path formation

Additionally, each intermediate STA which updated its forwarding table due to the reception of the PREP IE also updates its precursor list by:

- adding the next hop peer (the one it is going to forward the PREP IE to) to the list of precursors for forwarding towards the path target,
- adding the peer from which it received the PREP IE to the list of precursors for forwarding towards the path originator.

As PREP reaches the source station, a bi-directional path between the initiator of the discovery procedure and its target is formed, by ensuring the presence of a current next-hop forwarding information in all transit nodes, accompanied by appropriate precursor list entries.

It is evident that such a broadcast-based, reactive procedure can lead to a considerable communication establishment latency, especially in case of large mesh networks and distant destinations.
Moreover, broadcast procedures tend to consume a substantial amount of resources. To optimize the described procedure, it is possible to allow transit stations which already have current next-hop information toward the destination station, to respond with PREP. That allows the source station to learn the forward path to destination quickly, but its PREQ still must be broadcasted all the way towards the destination station, to form the reverse path from destination to source.

3.7.3.1.6 Intermediate station PREP response mechanism

To provide faster path discovery in reactive mode, HWMP protocol allows for an optional extension of the procedure described above. The procedure needs to be specifically allowed by source station, by setting the Target Only (TO) field of the PREQ message to 0.
When this extension is in effect, if a station receives a PREQ IE for a target MAC address for which it already has a current path available, such station is allowed to send back a PREP message even if it is not an intended target station of the PREQ message (owner of destination MAC address).
Such intermediate station is then required to follow the standard PREQ IE flooding procedure, by rebroadcasting the PREQ IE according to normal broadcast rules, but only after setting TO field to 1, to prevent further intermediate stations from sending additional PREP messages.

3.7.3.2 Proactive routing

Apart from the obligatory RM-AODV protocol, the IEEE 802.11s standard defines an optional proactive path discovery solution, which can be deployed concurrently with RM-AODV.
This solution, sometimes called Tree-Based Routing (TBR) protocol, consists of two independent mechanisms: Proactive Path Request (PPREQ) and Root Announcement (RANN). Both can be used to proactively create and maintain mesh paths between a selected mesh station (Root Mesh Station) and all other stations in the mesh. Moreover, they reuse a significant number of mechanisms of RM-AODV protocol, thereby simplifying their implementation.

3.7.3.2.1 Proactive PREQ mechanism

In case of the first approach, Proactive PREQ, a selected root station periodically originates Proactive Path Request (PPREQ) messages, which can be defined as PREQ messages with a broadcast address (all bits set to 1) specified as Target Address and with Target Only (TO) indicator set to 1 (to prevent intermediate stations from generating responses).
Such messages are re-broadcasted through the network according to the same rules as PREQ messages in case of RM-AODV reactive protocol (using HWMP Path Selection frames), which results in creation and periodic refresh of unidirectional, reverse mesh paths leading towards root station in all stations within the range of the broadcast (as limited by Element TTL field of PREQ IE).

If mesh station predicts that a bi-directional path will be required, it can respond to PPREQ message with an unicast PREP IE, which will be forwarded to root station and create a forward path in opposite direction (from the root station to the responding station).

Root station can also request that all stations respond in such fashion, by setting the Proactive PREP flag of the PPREQ message to 1. As a result a complete set of bi-directional paths between the root station and all mesh stations within the PPREQ broadcast range will be created. The root station will also obtain a complete list of mesh STAs within such range.

Due to a relatively high consumption of resources in case of the described PPREQ method, an alternative, lightweight solution has been included in the standard – the Root Announcement mechanism (RANN).

3.7.3.2.2 Root Announcement mechanism

Instead of a Proactive PREQ mechanism described above, a root station can choose to utilize a less involving mechanisms for purposes of building a proactive forwarding tree – a Root Announcement (RANN) mechanism.
Its introduction has been caused by a relatively high level of management traffic generated by a Proactive PREQ method. To offset these drawback, the RANN mechanism, while based on essentially the same idea, introduces three important changes.
The first one is the use of a new Root Announcement Information Element (RANN IE, Fig. 72) of simplified structure compared to the PREQ IE.

3.7.3.2.3 Root Announcement (RANN)

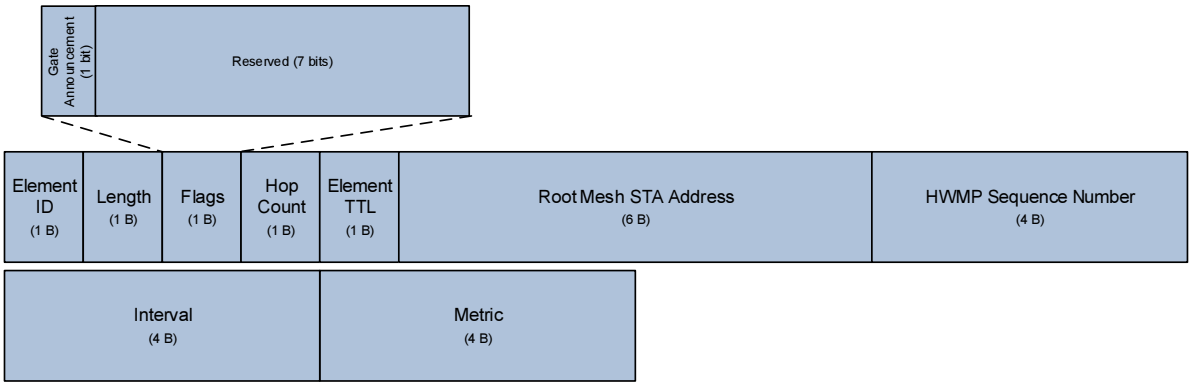

Fig. 72 Root Announcement (RANN) Information Element

Apart from already described Element ID and Length fields required for any IE, there are also other fields with which we are already familiar from our analysis of PREQ IE:

- Flags, containing only a single Gate Announcement indicator, allowing RANN IE to be used for interworking purposes in the same way as Proactive PREQ IE (see interworking procedures description in Section 3.8),
- Hop Count – a number of wireless links the IE already traversed in the MBSS, a distance (in hops) to the root station which originated the IE,
- Element TTL – the value indicating the number of wireless links the IE can traverse, before it is dropped. Can be used to limit the area of RANN IE propagation,
- Metric – a sum of link metrics of wireless links the RANN IE already traversed in the MBSS, a metric of a path to the root station which originated the IE,
- Root Mesh STA Address – the identifier of a mesh root STA which originated the RANN IE, in form of its MAC address,
- HWMP Sequence Number – indicates relative freshness of the information about the originating root station.

A single new Interval field is introduced, describing a time interval between generation of subsequent RANN messages by the specific root station.

The second change is that while RANN IE can be sent using HWMP Path Selection management frames, it can also be transmitted as a part of Beacon management frames, which are periodically broadcasted by each mesh station as a part of mesh discovery procedures, resulting in significant resource conservation. The tradeoff here is the fact that Beacon frames are sent by a station in periodic manner using a set interval, which will introduce a delay in propagating the a RANN message at each retransmitting station. The delay will be difficult to determine, as it depends on timing relations between Beacon transmission at different stations, but, in most cases (depending on configuration and activity of MBC mechanism, see 3.3.4) should not exceed 0.1 s per hop – a value which would not be acceptable in case of a reactive path discovery mechanism, but should not cause problems for proactive support mechanism such as RANN.

The third difference is between RANN and Proactive PREQ procedures is, that while RANN messages are propagated through the network using the same procedure as PPREQ messages, their reception does not result in creation or update of forwarding information at receiving stations. Instead they are used to obtain a current matric value for a possible path to the origination root station, which in turn can be used to decide, if active update of forwarding information should be undertaken.

For this purpose an information identifying a peer STA from which RANN message has been received is stored, and the path metric contained in RANN IE is compared with metric of the current path that

the station has to the specific root station. If the receiving station does not have a path to the root station or if its metric is worse than RANN metric, the station can perform a reactive path discovery to create or update such path. However, due to the information obtained by RANN message reception, such discovery can be performed by sending a single individually addressed PREQ instead of a group addressed one, as is the standard procedure.
This optimization is possible due to the fact, that while the RANN receiving STA does not update its forwarding information, it remembers from which peer STA it received a RANN message with a best metric for a particular root station. Making use of this information, the station sends a unicast PREQ message to the root station, by transmitting it to such a peer STA. The PREQ message is then forwarded by consecutive mesh stations retracing RANN path to the root station, updating forwarding information along the way and thus forming a reverse path towards the PREQ originator. Upon reception of the PREQ, root station responds with a standard unicast PREP, which forms the forward path in opposite direction.
Due to strictly unicast nature of such discovery, it combines the best features of proactive and reactive approach, as is both efficient (no broadcast flooding and triggered as required) and reliable, as unicast frames are subject to reception acknowledgement and retransmission.

3.7.3.3 Path error handling

Due to inherently dynamic structure of a self-configuring mesh network it is evident, that forwarding information is subject to change. While periodic update of this information is compelled by an information lifetime limit associated with each particular entry, such a timer-based approach cannot provide a reaction time sufficient to offer a data transmission service of a quality adequate for modern application layer services.
The requirement of rapid reaction to data transmission path failures results in introduction of an event-based path invalidation mechanism, based on back-propagating of error message from the point of failure towards the traffic source.
There are currently three scenarios which can result in initiation of a path error handling procedures:

- an active next hop link at an intermediate station on a mesh path becoming unusable,
- a lack of forwarding information at an intermediate station on a mesh path,
- a lack of proxy information at the mesh gate concluding a mesh path (see Section 3.8 for description of interworking procedures).

The station which detects one of the problems listed above should generate a Path Error Information Element (PERR IE) describing the problem and affected destination addresses. Such IE will then be sent using a HWMP Path Selection frame.
The structure of PERR IE is relatively simple. Apart from the obligatory Element ID and Length fields described before, supplemented by Element TTL field universally found in HWMP-related IEs, it contains only a Number of Destinations field indicating a number of following unreachable destination descriptors. Each of unreachable destination descriptors consists of 4-5 fields:

- Flags field, containing only a single Address External (AE) indicator – the AE bit is set to 0 if the message is generated to indicate lack of forwarding information and set to 1 if the reason is lack of proxy information at mesh gate.,
- Destination Address – an address of a mesh destination which is unreachable or an address of a mesh gate which lacks the necessary proxy information,
- HWMP Sequence Number – specifies the relative freshness of the information contained in the IE,
- (optional) Destination External Address – field present only when the error is caused by a lack of proxy information (AE bit is set to 1), and indicates the external, final destination address of the frame which cannot be delivered,
- Reason Code – describes the type of error indicated in the descriptor.

The PERR IE is sent by the STA detecting the problem, in an individually addressed HWMP Path Selection frame, to stations upstream on the transmission path.
If the reason for the error is a link failure, the PERR IE is sent to all peer stations which are listed as precursors on paths to destinations which become unreachable due to the indicated link failure. In this case, the HWMP SN of forwarding information entries which have been invalidated is incremented by 1 before including it in respective error descriptors in the PERR IE, to indicate that it represents a change in the current MBSS topology.
When the reason for the error is lack of forwarding information, the list of relevant precursors and HWMP SN values are unavailable. In this situation the PERR IE is sent to the peer station which is a transmitter of the undeliverable frame. The HWMP SN field is set to a reserved value of 0.
The case when the error is caused by lack of proxy information will be described separately.

Stations receiving the PERR IE will analyze the unreachable information descriptors separately and accept each one only if they have a forwarding information entry for destination indicated in the descriptor for which their next hop is the peer station which transmitted them the PERR IE.
If a particular descriptor is accepted, the STA will check if the HWMP SN in the descriptor is greater than HWMP SN of the entry and if it is so – invalidate the appropriate forwarding information entry as the error indication contains a more recent knowledge.

If the received PERR IE caused invalidation of the forwarding information, a new PERR IE will be generated describing the changes. The reason codes will be copied from the received PREP IE, but the HWMP SN of the unreachable destination descriptor will be incremented by 1, to indicate that it refers to a system state more recent (due to invalidation of forwarding information at current STA) then the received PERR IE.

The above procedure will cause the PERR IE to be transmitted towards the traffic source along the mesh path, invalidating forwarding information entries made out of date by the failure. When the PERR IE will reach the originator of the traffic and invalidate its forwarding entries, such station will initialize the path selection procedure to obtain new forwarding information based on a changed MBSS topology.

In case of unreachable destination descriptors concerning proxy information (AE bit set to 1), their reception do not result in invalidation of forwarding information regarding the mesh gate indicated in Destination Address. However, they are copied transparently to a new PERR IEs at intermediate stations and transmitted to all precursors on paths to a given mesh gate. When such PERR IE reaches the beginning of the mesh path leading to the gate, it will cause invalidation of a proxy information entries which indicate a given mesh gate (as indicated by Destination Address field) as a proxy for an external address indicated in Destination External Address field and have a HWMP SN lower than the arriving unreachable destination descriptor.

3.8 Interworking

As stated before, IEEE 802.11s standard aims to provide easy integration of mesh network with other network technologies, in particular Ethernet wired technologies. An IEEE 802.11s MBSS integrates with external networks as another IEEE 802 access domain, complete with support for IEEE 802.1D interworking mechanisms such as bridging.
However, in contrast to other popular IEEE 802 technologies (for example Ethernet), the MBSS operation is not primarily based on broadcast data delivery, as such approach is not acceptable due to limited resources of a wireless system.

In this situation, delivery of data to addresses unknown within MBSS cannot be conducted by simple broadcasting it to all stations for the bridging ones to receive and forward to external systems as it is done in cable-based IEEE 802 technologies (Fig. 73) [79].

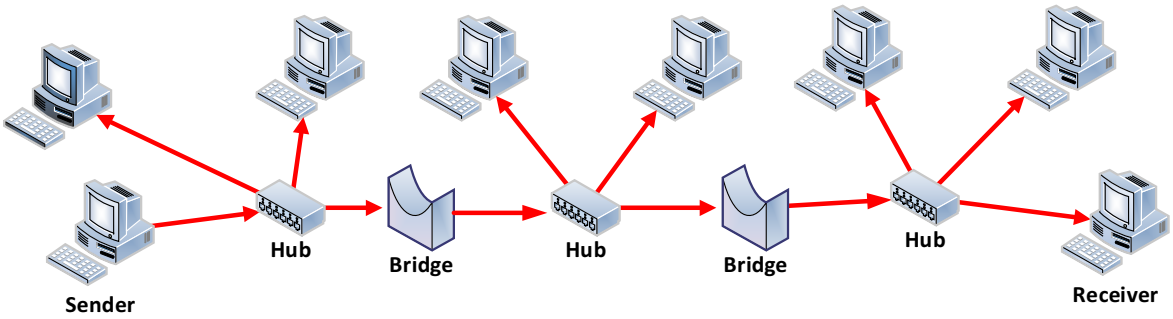

Fig. 73 IEEE 802.1D traffic delivery for unknown destination.

To emulate this popular method of delivery, mesh stations connected to external networks, named mesh gates (MGs), support an extended suite of mesh mechanisms.
Presence of mesh gates is advertised in the MBSS by dedicated Gate Announcement frames (GANN, see 3.8.1.1) distributed in fashion similar to already described RANN messages or, if proactive routing is used and MG is also a Root Station, by extending proactive PPREQ/PPREP messages with a special Gate Announcement field (see 3.8.1.2).
Each MG maintains a dedicated database (Proxy Information) of addresses known to be located in external networks accessible through a given gate. Moreover, it forwards its contents to other mesh gates through MBSS with use of Proxy Update (PXU) messages (see 3.8.2.3). That makes all MGs aware, which gate should receive frames addressed to a particular external destination. If any of them receives frame proxied by other MG (for example due to incorrect proxy information at the sending STA), it will forward it to the correct gate through MBSS (Fig. 74).

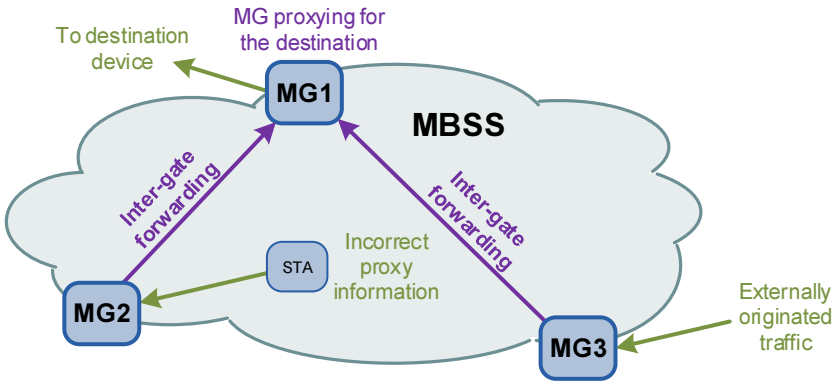

Fig. 74 Inter-gate forwarding

It should be noted however, that both proxy information exchange and gate to gate data forwarding is conducted through MBSS and thus consuming limited RF resources.
Moreover, due to the fact that MG is functional equivalent of IEEE 802.1D bridge, if more than one gate is connected to a given external network, only one such gate can be active at a time, as multiple active gates could lead to creation of loops when forwarding group addressed frames or unicast frames for previously unknown external addresses. For this purpose a dedicated protocol must be employed at mesh gates – in compliance with IEEE 802.1D specification it is a well-known Rapid Spanning Tree Protocol (RSTP) [79]. This protocol will interpret mesh gates as ISO-OSI layer 2 network ports and will disable all mesh gates connecting an MBSS and a particular external ISO-OSI layer 2 network, except one. Disabled MGs will not provide any mesh gate-specific service except participation in RSTP protocol. The mesh gate which is chosen by the RSTP protocol to remain functional is called an active mesh gate.

Mesh station which cannot discover a MBSS path to a given address, assumes that it is located in external network. In such case it sends the data frame to all known MGs, for further delivery - due to RSTP activity, the frame is delivered to each external network only once, as only one mesh gate is active per such network. To optimize further data delivery, MG appropriate for a given destination sends PXU message to the station, which allows it to create its own Proxy Information entry instructing it to use a single, specific MG in continued transmission to a given external address.

The described method does not require complicated mechanisms to be present which makes it easy in implementation and provides seamless integration of MBSS with widely popular Ethernet networks. However, due to particulars of MBSS operation and strictly limited radio resources available for MBSS stations, its deployment in real-world scenarios can lead to inefficient operation of the network.
Operation of RTSP protocol results in deactivation of all save one mesh gates between MBSS and a given external network. Such operation does not have significant adverse impact on network systems utilizing wired communication, due to their star topology, link independence and relatively high level of available resources. In case of MBSS however, it can potentially result in significant efficiency loss and limited scalability, due to necessity of using long transmission paths. Detailed description and assessment of the problem will be presented in chapter 6.

3.8.1 Gate announcement procedures

For the mesh stations to learn the presence of gates one of three different procedures may be employed:

- Gate Announcement protocol – a dedicated protocol for advertising presence of mesh gates,
- Proactive PREQ mechanism of HWMP protocol (see 3.7.3.2) – advertising a mesh gate presence and creation of paths towards it using the proactive TBR protocol, applicable when mesh gate functions as a HWMP root station.
- Proactive Root Announcement protocol (see 3.7.3.2.2) – a combined advertising a mesh gate and a root station presence, applicable when mesh gate functions as HWMP root station.

3.8.1.1 Gate Announcement protocol

The Gate Announcement (GANN) protocol utilizes a simple broadcast flooding to propagate the information about presence, hop distance to and MAC address of a particular mesh gate. No additional information about mesh gate is provided, nor any forwarding information if obtained by stations due to use of GANN protocol.
Recognizing, that an MBSS may include multiple mesh gates and that unconstrained broadcast flooding may negatively impact scalability, the GANN protocol utilizes a Time To Live (TTL) parameter to limit the area of GANN broadcast.

A mesh gate which does not advertise its presence by any other possible mechanism may advertise its presence using GANN protocol. To do so, it employs a dedicated Gate Announcement Mesh Action Management frames (type: Management, subtype: Action, category: Mesh Action, Mesh Action: Gate Announcement). They follow the overall format of Mesh Action frames and contain a single Gate Announcement Information Element (GANN IE, Fig. 75) in their data field.

Element ID (1 B)	Length (1 B)	Flags (1 B)	Hop Count (1 B)	Element TTL (1 B)	Mesh Gate Address (6 B)	GANN Sequence Number (4 B)	Interval (1 B)

Fig. 75 Gate Announcement (GANN) Information Element

The GANN IE begins with a standard set of Element ID and Length fields, common to all IEs and identifying a particular IE type and providing its length. The Flags field of GANN IE is current not used for any standardized purpose.
The information used by GANN protocol is present in remaining fields of GANN IE. Hop Count indicates how many mesh links the message has traversed from the originating mesh gate to the STA transmitting the IE. It is the only indication allowing the receiving STA to assess the possible preference of a particular mesh gate.
Element TTL is set by the originating mesh gate allows for limiting the area of broadcast flooding by indicating the remaining number of mesh links that the IE is allowed to traverse.
The Mesh Gate Address uniquely identifies the advertising mesh gate by providing its MAC address, which can then be used by the receiving STA in its path discovery procedures, if it decides to utilize the particular mesh gate.
GANN Sequence Number is a gate-specific counter used to identify a particular GANN advertisement for purposes of handling a broadcast flooding.
Interval field specifies a time interval the mesh gate waits between sending a consecutive Gate Announcement frames.

Stations receiving the described Gate Announcement frame process it according to standard broadcast flooding rules (retransmitting the frame it they have not already retransmitted the such frame from the same sender with the same or higher Sequence Number). Additionally the Element TTL field is taken into account – it is decremented by 1 upon reception and the frame in not retransmitted if it has reached 0.
The values of Mesh Gate Address and Hop Count fields inform the receiving STA of the presence and distance to the sending mesh gate, fulfilling the objective of GANN protocol. Additionally a value of the Interval field can be noted, for purposes of efficient detecting stale mesh gate information.

Due to limited information provided by GANN protocol, especially compared to HWMP-based mechanisms described below, it is intended to be used as a lightweight solution for MBSS networks utilizing exclusively reactive path discovery solutions. If the proactive mechanisms of HWMP protocol are employed in the MBSS, it is preferred to utilize one of the related methods described below.

3.8.1.2 HWMP-related gate announcement methods

If proactive mechanisms of HWMP protocol are in use in the MBSS, it is possible to use their management messages for purposes of gate announcement. For such solution to be possible, the mesh gate must also be a root station of HWMP protocol and thus employ Proactive Path Request (Proactive PREQ) or Root Announcement (RANN) protocol.

If Proactive PREQ method is in use, the root station (gateway) periodically broadcasts PPREQ massages through the MBSS. As a result, all receiving stations obtain a proactively maintained mesh paths to the root station. Optionally, the root station can also indicate that receiving stations must respond with Path Reply (PREP) messages, which results in creation of bi-directional mesh paths between the root stations and all stations within PPREQ broadcast range (limited by Element TTL field of PPREQ IE).
Additionally, all receiving stations obtain information about distance to the root in terms of both the number of consecutive mesh links (Hop-Count field) and the routing metric (Metric field). The root station in turn, if it chosen to require PREP from stations, receives the complete list of STAs in its broadcast range, complete with their MAC addresses and comprehensive distance information (Hop-Count and Metric fields).

The above mechanism can also be employed to advertise the presence of a mesh gate if it is also a root station. For this purpose a Gate Announcement indicator has been defined in Flags field of PREQ frame. If set to 1 it indicates that the sending root station is also a mesh gate.
This procedure allows the stations to obtain a more comprehensive information (in particular a routing metric) about mesh gates utilizing it than GANN protocol. Moreover, by integrating it into an already deployed proactive protocol stations automatically obtain proactive mesh paths to the mesh gate (unidirectional or bidirectional) and there is no need for any additional management traffic.

Due to relatively high resource consumption required by the described Proactive PREQ mechanism, a lightweight alternative has been introduced for advertising the presence of root stations – a Root Announcement (RANN) protocol. Its relatively small Root Announcement management frames can be propagated by broadcast flooding or attached to periodically sent, one-hop Beacon frames (part of mesh discovery procedure). As a result, receiving stations obtain the similar information about originating root station as in case of PPREQ mechanisms, but no mesh path is constructed. However, it is possible for the receiving STA to follow up with strictly unicast reactive mesh path discovery, as described in earlier sections.
The described RANN mechanism can be used to propagate mesh gate information in a way similar to PPREQ mechanisms, as RANN management frames also contain Gate Announcement indicator in the Flags field of RANN IE.
The RANN procedure extended to advertise presence of mesh gates functioning as HWMP root stations provides the same amount of information as PPREQ mechanisms, except no mesh paths are actually created and need to be discovered reactively by interested stations. It should be also noted, that the reactive discovery following RANN announcement is possible without additional broadcast flooding.

3.8.2 Proxy mechanisms for inter-MBSS traffic handling

As previously described in mesh forwarding overview (Section 3.7.1) and the general overview of IEEE 802.11s interworking mechanisms above, the mesh path selection mechanisms are responsible only for providing a data transmission path within a particular MBSS network. Mesh stations which are not active mesh gates, originators or final destinations of inter-MBSS traffic do not need to employ any procedures except these described in mesh forwarding overview section. Such STAs process only 3 static (Address 1 through Address 3) and 1 optional (Address 4) of the standard IEEE 802.11 MAC header's address fields while handling unicast traffic, and the same number of fields, but Address 4 field is relocated from MAC header to a Mesh Control structure in case of group addressed traffic.
If the frame's origin or destination is external to the MBSS, two additional address fields are included in its Mesh Control field – Address 5 (frame destination address, DA) and Address 6 (frame originator address, SA). They are, however, processed only by source/destination STAs (if they are internal to the MBSS) and mesh gates. The remaining mesh STAs do not need to employ any additional mechanisms to handle the inter-mesh traffic.
The IEEE 802.11s inter-MBSS traffic handling procedures follow an overlay model and are deployed only in these mesh stations which have to be aware of the inter-MBSS nature of a given frame to ensure its proper handling, namely:

- frame originator STA in case of frame addressed to an address outside of the MBSS – frame destination address in unknown in the MBSS and its path selection mechanisms will respond with information that the address is unreachable,
- frame destination STA in case of a frame originated outside of the MBSS – the final receiver of the frame should be informed of the address of its originator, while forwarding

mechanisms and addressing fields described above will only inform about the STA which discovered the path through the MBSS used for frame delivery within its boundaries,

- mesh gate forwarding the frame between the external network (or more precisely Distribution System – DS) and the MBSS – the mesh gate is responsible for forwarding the frame between the DS and the MBSS, functioning as both an MBSS STA required to support its internal procedures and an interworking device responsible for forwarding the frame between various networks based on its source and destination MAC addresses.

These stations will perform all operations involved in handling the inter-mesh traffic, by processing Address 5 and Address 6 fields ignored by other stations, and ensuring that remaining address fields used in intra-mesh forwarding are correctly set, resulting in its proper handling within the MBSS.

Each of the above mesh stations maintains a Proxy Information Database (PID) containing a list of external MAC addresses along with corresponding MAC addresses of a mesh stations located in the same MBSS and able to process the inter-MBSS addressing information, to which the frame should be sent to ensure its delivery. As a result, the indicated mesh station acts as a proxy for the corresponding external address by being a mesh destination of its incoming traffic or a mesh source of its outgoing traffic.
Each entry of this list also includes a sequence number necessary to assess freshness of potential future updates in relation to currently used information and a lifetime value, necessary to eventually remove stale (not updated for an extended period of time) proxy information.

While the previously described Forwarding Information Database serves to deliver the frame within the MBSS, the PID indicates the correct MBSS exit point for inter-MBSS traffic.

3.8.2.1 Unicast frame delivery

When a mesh STA (including a mesh gate) possesses an unicast frame intended to an unknown destination, meaning a destination for which it currently does not have either forwarding or proxy information, it will assume that it is an intra-MBSS destination and will attempt to obtain an appropriate mesh transmission path to the appropriate MAC address.
Four possible scenarios can be a result of such attempt:

1. The station will obtain a path to the final destination within the current MBSS – this scenario results in intra-mesh delivery.
2. The station will obtain information that the destination address is unknown within the MBSS – no STA (including mesh gates) owns the address or has any information regarding the address in its PID.
3. The station will obtain a path to a specific mesh gate – the responding mesh gate has information about the specified destination address in its PID, indicating that it is a proxy for the indicated address.
4. The station will obtain a Proxy Update (PXU) containing indicating a mesh gate – the responding STA (not necessarily a mesh gate) has a PID entry indicating the mesh gate currently acting as a proxy for the specified destination address.

Scenario 1 results in an intra-MBSS delivery, which has already been described in Section 3.7.1. However, in all of the described scenarios a frame that the station attempts to send could have been obtained from a network external to its IEEE 802.11s MBSS as the STA could be a mesh gate. That possibility makes Scenario 1 one of interworking scenarios. In such case, in contrast with strictly intra-MBSS transmissions (where 4 address fields are sufficient), the frame will utilize 6 address fields.
Address fields 1-4 will describe the frame path through the MBSS:

- Address pair 1-2 – current receiver and transmitter, changing with each hop (RA/TA),

- Address pair 3-4 – mesh path: MDA (destination within the MBSS) / MSA (sending STA within the MBSS – the mesh gate),

while Address 5 and 6 will contain respectively originator and final destination MAC address. This addressing scheme is a general policy for handling an inter-MBSS traffic and will also be used in all interworking scenarios described below.

In Scenario 2 the sending STA (which can also be a mesh gate and the frame can be of extra-MBSS origin) does not obtain any information except that the specified destination MAC address does not belong to any MBSS STA. The STA will attempt to deliver the frame by sending it to all mesh gates it is aware of as a set of unicast frames. Their address fields 1-4 will describe the frame path through the MBSS:

- Address pair 1-2 – next transmission: RA/TA,
- Address pair 3-4 – mesh path: MDA (destination mesh gate) / MSA (sending STA, which can also be a mesh gate),

while Address 5 and 6 will contain respectively originator and final destination MAC address.

The described scenario can occur even in case when the MBSS is not connected with any external network and has no mesh gates, in which case the frame is undeliverable and will be dropped. The same result will occur if the sending STA does not have information about mesh gates despite their existence.
It should be noted, that despite individual addressing of discussed traffic, this scenario creates a risk of crating forwarding loops. Because no specific information about the intended destination address is known, IEEE 802.1D compliant interworking devices (including IEEE 802.11s mesh gates) will forward such frame to all their active ports performing an equivalent of a broadcast frame delivery to ensure that it will eventually reach its destination. With more than one point of contact between two networks, such approach will result in an equivalent of a broadcast loop. To eliminate the described risk, the RSTP protocol is employed to ensure that only a single mesh gate will remain active between an MBSS and a given external ISO-OSI layer 2 network.

In Scenario 3 the sending station's path discovery attempt has been received by a mesh gate which is currently considered the best one to deliver the frame, and so has an appropriate entry in its PID – indicating its own address as a proxy for the destination MAC address specified in path request message.
Such mesh gate will respond to the path discovery attempt as a proxy for the external address owner, resulting in mesh path being established between the sending STA and the mesh gate. The response will contain an AE (Address External) field set in Flags field of its PREP Information Element to indicate that interworking mechanisms are in effect and the responding station is a proxy mesh gate not a final destination. Additionally the Target Mesh STA address will contain the address of the proxy mesh gate instead of the destination address requested by the station which initiated the delivery, which in turn will be added as an additional Target External Address field of PREP IE.
Station receiving such a replay will add the proxy mesh gate address to its forwarding table indicating the presence of a mesh path to the gate and an entry linking the intended external destination address with the proxy mesh gate address to its PID.
The frame can then be sent, as the sending station knows both the appropriate mesh gate to deliver it (PID entry) and the mesh path to the indicated mesh gate (forwarding table entry). The addressing of the frame follows the same rules as in case of Scenario 2.

The Scenario 4 occurs, when the response is provided by a mesh STA which is not an appropriate mesh gate to forward the traffic to the indicated destination address, but whose PID contains the relevant entry. Such STA can send a Proxy Update to the station performing the path discovery indicating an address of a correct mesh gate to handle the frame intended for a particular external address.

The sending station can update its PID based on received PXU and send the frame to the indicated mesh gate, performing a mesh path discovery procedure if no forwarding information for its address if present. The addressing scheme for this scenario also follows the same rules as in case of Scenario 2.

Apart from the above scenarios, which assume lack of any information regarding the intended destination address of the frame on the part of the sending station, there is also a possibility it has some relevant information in its forwarding and/or proxy database.
If the information is complete, the frame will be delivered accordingly. The information to be considered complete consists of:

- The destination address listed in STA's forwarding database – the destination STA is located in local MBSS and the frame will be delivered following intra-MBSS forwarding rules.
- The destination address listed in STA's proxy information database and the indicated proxy mesh gate listed in STA's forwarding database – the destination address is external to the MBSS, but the indicated proxy mesh gate address is known and the path to the indicated gate is also available. The frame will be forwarded to the mesh gate using 6 address frame format.

There is also a possibility that an incomplete information is available:

- The appropriate information regarding the destination address is present in STA's PID, but no forwarding information for the address of the indicated mesh gate is present in its forwarding database – the destination address is external to the MBSS, and the frame will be delivered to the indicated proxy mesh gate, following a path discovery procedure initiated to obtain a mesh path to its address. A 6 address frame format will be used in the frame's transmission.

3.8.2.2 Group addressed frame delivery

Due to the lack of specific multicast support all group addressed are transmitted through the mesh by means of broadcast flooding (as described in 3.7.1.2), which also makes their interworking transmission procedures relatively simple compared to mechanisms required in case of individually addressed frames. There is no need to differentiate between intra and inter-MBSS delivery, as all group addressed frames need to be delivered to all stations in MBSS, including all active mesh gates.

When a STA generates a group addressed frame, it will use the intra-MBSS procedure and frame format to do so, with Address 1 indicating a destination group address (DA, there is no need for RA as according to broadcast flooding rules, all STAs must receive a group addressed message), Address 2 indicating a transmitter for a particular hop (TA) and Address field 3 specifying an original mesh sender of the frame (MSA equal to SA as the mesh STA originated the frame). Such frame will be delivered to all MBSS STAs including active mesh gate, which in turn will forward the frame to external network. With Address 1 and Address 3 fields specifying the destination group address and frame source respectively, the mesh gate has all necessary information to forward the frame.
If the frame is received by a mesh gate from external network, the 3 field addressing scheme will be insufficient as Address 3 field will indicate only mesh source address (MSA), with no information about the original sender of the frame located outside of an MBSS. To provide this information an additional Address 4 field is added to the described frame format, containing the external SA.

This simple method is sufficient to provide support for broadcast frames and in general for any group addressed frame, however, without additional assumptions, there would be a risk of broadcast loops. Because of this risk it is assumed that only one mesh gate can remain active between an MBSS and a given external ISO-OSI layer 2 network. The task of selecting such gate is assigned to RSTP protocol.

3.8.2.3 Proxy information exchange

Proxy Information Database (PID) is partially populated with information received from path selection mechanisms. In case of HWMP protocol, the information transmitted in PREQ, PREP and PERR Information Elements, when their Flags field contains an AE (Address External) bit set to 1.
In such case the STA which generated the particular IE (identified by Address 4 field of the frame, MSA) is only a proxy for an external originator (PREQ IE), target (PREP IE) or forwarder (PERR IE) of the frame which caused the IE to be sent. The external addresses are provided in optional field present only when AE bit is set to 1 and allow easy creation of PID entries:

- PREQ IE: Originator External Address proxied by STA identified by the frame's Address 4 field,
- PREP IE: Target External Address proxied by STA identified by the frame's Address 4 field,
- PERR: Destination External Address (PERR) proxied by STA identified by the frame's MSA Address 4 field.

Such solution ensures, that when a mesh gate performs a path discovery on behalf of an external frame originator, it will create both mesh reverse paths towards its own address (by creating forwarding information entries in forwarding information databases of other STAs) and PID entries marking this address as a proxy for the external originator's address.
Similarly, if the mesh gate responds to PREQ message on behalf of an external address, it will send a PREP message creating a forward mesh path towards its own address and provide the path selection process initiator with information defining its own address as a proxy for the requested external address.

Apart from integration with path Selection mechanisms, PID is populated and maintained by exchange of dedicated Proxy Update (PXU) elements, transmitted in unicast Multihop Action management frames. The frame can contain multiple PXU elements directly following the Mesh Control field, and their presence makes such frame a Proxy Update management frame. Each PXU IE can contain multiple Proxy Information entries used to create, update or delete PID entries at receiving STA.

The PXU elements will be sent by a mesh gate to other mesh gates it is aware of, when it changes entries in its Proxy Information Database. Mesh gates may also generate Proxy Update frames periodically. This procedure results in loose synchronization of PIDs belonging to different mesh gates within the MBSS.
A mesh gate will also send a PXU to a mesh STA from which it has received a PREQ message requesting a path discovery for an external address the gate has information about in its PID. Such PXU will be sent if the mesh gate is a proxy for the indicated address, but also if its PID indicates that the address is proxied by some other mesh gate. Such procedure ensures that a mesh STA will receive a PXU necessary for it to send the frame through a mesh gate appropriate for a specific external address, even if it is outside its announcement range.

The structure of PXU IE (Fig. 76) begins with Element ID and Length fields obligatory for IE in general and indicating its type an length.

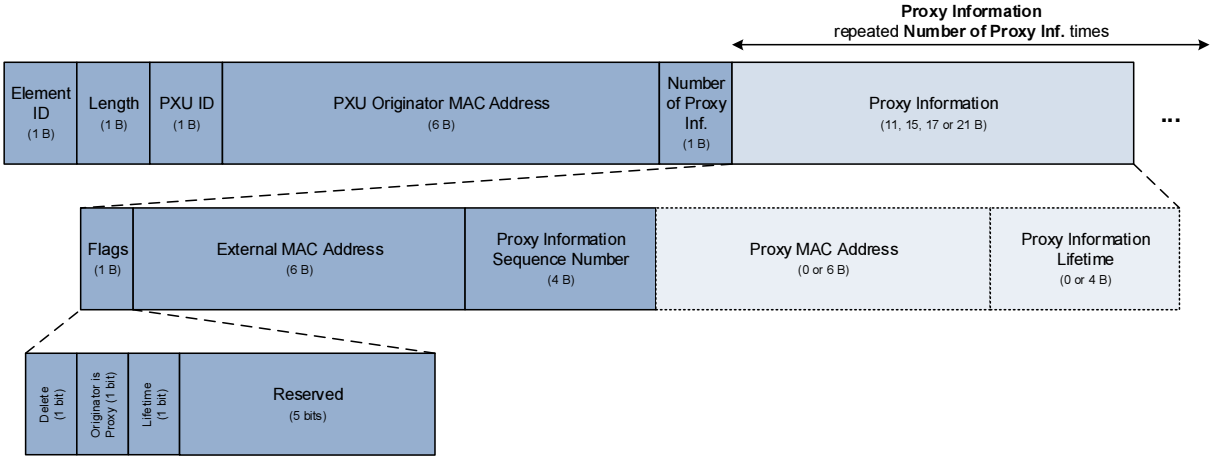

Fig. 76 Proxy Update (PXU) element

They are followed by:

- PXU ID – identifier of a particular PXU IE maintained by PXU originator indicated in the following field,
- PXU Originator MAC address – MAC address of the STA which originated the particular PXU,
- Number of Proxy Information elements – defines the number of following Proxy Information elements,
- The indicated number of Proxy Information sets.

Each Proxy Information set consists of:

- Flags field,
  - Delete – value 0 indicates request to add proxy information, value 1 – to delete it,
  - Originator Is Proxy – specifies if PXU originator is also the proxy mesh gate for this particular Proxy Information set (value 0 – the proxy mesh gate address is specified in Proxy MAC Address field, value 1 – PXU originator is also the proxy mesh gate, the Proxy MAC Address field is omitted in this set),
  - Lifetime – indicates if the set contains Proxy Information Lifetime field (value 0 – the field is omitted, value 1 – the field is present).
- External MAC Address field – specifies the external MAC address for which this Proxy Information set contains proxy information,
- Proxy Information Sequence Number – allows the receiving STA to assess the relative freshness of this Proxy Information set, compared to the data contained in its PID,
- Proxy MAC Address – if the Proxy Information set indicates a proxy mesh gate other than the PXU originator, this field specifies the proxy mesh gate address. For this field to be present Flags field Originator Is Proxy indicator must be set to 0,
- Proxy Lifetime Information – if the Proxy Information set contains a proxy information entry to be added to receivers PID, this field specifies desired lifetime of the entry. For this field to be present, Flags field Lifetime indicator must be set to 1.

The described Proxy Update frame structure is designed for both efficiency and robustness.
It is possible to aggregate both multiple Proxy Information sets in one IE and multiple PXU IEs in a single frame, with support not only for adding proxy information entries with or without a specified lifetime but also for deleting them at need.
Moreover it is possible to exchange both proxy information concerning external addresses proxied by the PXU originator and proxy information referring to external addresses proxied by other mesh gates.

The ability to omit unnecessary fields instead of ignoring them results in possible size reduction of a Proxy Information set element by almost 50%.

The originator of PXU IE should retransmit a PXU identified by a particular ID until its recipient will provide confirmation off the reception by sending back a Proxy Update Confirmation (PXUC) IE shown in Fig. 77. The rules for framing of this IE are the same as in case of PXU IE and result in creation of an individually addressed Proxy Update Confirmation Multihop Action management frame.

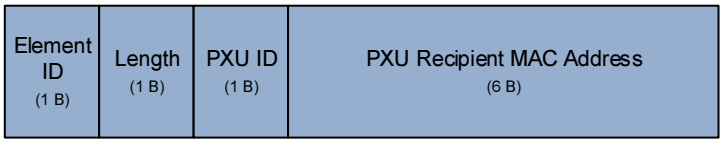

Fig. 77 Proxy Update Confirmation (PXUC) element

Each PXUC IE present in Proxy Update Confirmation frame confirms reception of a single PXU IE (identified by PXU ID field) by a recipient STA identified by its MAC address provided in PXU Recipient MAC Address field.

3.8.3 Rapid Spanning Tree Protocol (RTSP)

As described in previous sections, the IEEE 802.11s wireless mesh network can be easily integrated with other IEEE 802.1D-compliant network technologies to form a complex, ISO-OSI layer 2 network system, interconnected by bridge devices – a Bridged Local Area Network (Bridged LAN). In that context, the MBSS system can generally be seen as a shared media LAN, and more specifically, as an (emulated) Ethernet network.
In a complex Bridged LAN, there is a high probability that its structure, consisting of many LAN networks connected by bridge devices, will allow a data frame to be delivered to its destination by choosing one of multiple different paths. In such situation, there is a possibility of transmission loops, which must be prevented from occurring if the efficiency of the network operation is to be maintained.

For this purpose, the IEEE 802.1D standard specifies a Rapid Spanning Tree Protocol (RSTP), first defined in IEEE 802.1w standard extension and later incorporated into the base IEEE 802.1D-2004 standard in place of previously specified Spanning Tree Protocol (STP).
The RSTP will prevent transmission loops in a Bridged LAN environment, by selecting a root bridge device and then constructing a single transmission tree spanning all networks in the Bridged LAN. Bridge ports which are not required to maintain this tree structure are set to discarding state and cannot be used to forward traffic (discarding ports). This tree-based topology makes transmission loops impossible, as there is only one possible transmission path between any two different LAN networks in such Bridged LAN system.

The IEEE 802.11s MBSS specification, in accordance with IEEE 802.1D-2007 standard, indicates the RSTP as a preferred mechanism for avoiding transmission loops when connection an MBSS network with external LANs. For that purpose, the RSTP protocol should be implemented in each IEEE 802.11s mesh gate, as it is a mesh gate STA which performs the role of a bridge device connecting the MBSS to a Distribution System (DS), and through it to other IEEE 802.1D-compliant LANs.
The mesh gate should threat its connections to an MBSS and a DS as a bridge ports connected to shared media LANs, making it a two-port bridging device.

3.8.3.1 Basic RSTP characteristics

For the RSTP protocol to function each of bridging devices and their network ports must be possible to identify in an unique manner. For that purpose a the standard introduces Bridge Identifier (Bridge ID) uniquely identifying a bridge device within a Bridged LAN. A particular bridge port is identified by a Port Identifier (Port ID) unique within a particular bridge.

As a result of RSTP activity, ports of a bridge can assume one of three different states:

- Discarding – port does not receive or send frames except for BPDU frames described below. I cannot be used to forward traffic between networks. A normal state for a port which is not a part of the spanning tree structure,
- Learning – similar to discarding state, but the port additionally learns MAC addresses from detected frames. A transient state most common for a port changing its state form discarding to forwarding,
- Forwarding – port receives and sends frames and can be used for traffic forwarding, MAC address learning and BPDU operations are also conducted. A normal state of an active bridge port.

The above port states are a direct result of RTSP protocol classifying all bridge ports into one of the following 6 port types:

- root port – a forwarding port which leads towards the root bridge by the best path. There can be only one such port in a specific bridge,
- designated ports – forwarding ports, which connect their respective LAN networks to the spanning tree. There can be only one such port per each connected LAN,
- alternate ports – discarding ports, any of which can be used as a root port if the current root port connection fails,
- backup ports – discarding ports, any of which can be as a designated port, if the current designated port fails,
- edge ports – ports manually configured by administrator as edge ports are exclusively used to connect end-user devices (no bridges can be connected to such port) and thus can immediately assume and always remain in forwarding state, performing a function of designated ports,
- disabled ports – ports deactivated by administrator, ignored in RSTP procedures.

As can be seen from the above list, only edge ports, root ports and designated ports remain in forwarding state and can be used to receive and forward traffic between LAN networks. All other ports are set to discarding state, preventing such activity.
Edge ports can assume forwarding state immediately, without performing a time consuming procedure of designated port selection, as with only a single bridge port connected to a particular network, there is no risk of forming a transmission loop. However, is an edge port receives a message from another bridge (see below) it immediately loses its edge port status and must adhere to a full scope of RSTP procedures.

Changing the perspective from a bridge to a LAN network in the Bridged LAN environment, each of them will only have forwarding bridge ports of the following types:

- a single designated port or an edge port – connecting a given LAN to a bridge device on the best path towards the root bridge (such device is called a designated bridge),
- optionally, a number of root ports, present if the LAN is not a leaf of the spanning tree – each being the only connection point leading to the root bridge for networks located farther away from the root then the specific LAN.

The presence of root ports indicate that the LAN will be a transit network for a traffic generated in the connected branches of the spanning tree that is addressed to destinations outside a given branch.
Neighboring (connected to the same LAN network) bridge devices are communicating by exchanging Configuration Messages (CMs) and Topology Change Notification Messages (TCNs). These messages are transmitted by all ports of the bridge regardless to their state (forwarding or discarding) in ISO-OSI layer 2 frames called Bridge Protocol Data Units (BPDUs). BPDUs are addressed to a reserved Bridge Group Address (01-80-C2-00-00-00), which indicates that the BPDU is to be received by all bridge devices regardless to the state of the port they arrive at, but should never be forwarded between different LAN networks.

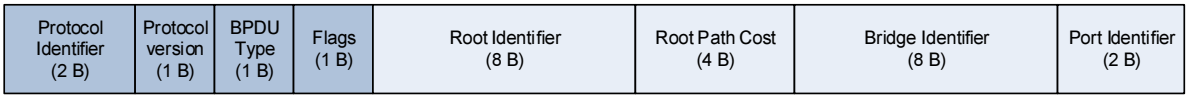

Fig. 78 BPDU stucture

As BPDU frames can be used for variety of tasks, the specific type used by RSTP is called RST BPDU and identified by an appropriate value in its Protocol Identifier (value 0, indicating STP and RSTP), Protocol Version Identifier (value 2, specifying RSTP) and BPDU Type (value 2, indicating RST BPDU) fields.
The remaining fields contain a number of flags and a message priority vector critical for RSTP operation and described below in more detail.
For the compatibility with bridge devices supporting only an older Spanning Tree Protocol (STP) [79] mechanisms, the RSTP can also use Configuration BPDUs and Topology Change BPDUs in place of RST BPDUs to convey CMs and TCNs respectively. However, mixing RSTP and STP bridge devices in a single Bridged LAN results in a loss of many RSTP advantages, network convergence time among them.

The algorithm used to build the tree structure in RSTP is based on comparison of so called priority vectors, in general containing the following parameters:

- Root Bridge ID – specifies a Bridge ID of the root device of the spanning tree being constructed,
- Root Path Cost – indicates the cost of the path from the specific bridge to a root bridge indicated by Root Bridge ID element,
- Bridge ID – unique identifier of the specific bridge within the Bridged LAN,
- Port ID – unique identifier of the specific bridge port within the bridge indicated by Bridge ID element,
- Port ID – unique identifier (within its bridge) of the port which received the priority vector. This element is present only under specific circumstances and is never transmitted.

The comparisons require comparing corresponding elements of the priority vectors, with the elements organized in decreasing order of priority (leftmost element has the highest priority). The elements of lesser priority are significant only if all the elements of higher priority are equal. The vector which has a lower value in the significant element is considered to be a better one.
As the bit order used to encode values of the vector elements place the most significant bits first, instead of comparing specific vector elements, a priority vectors can be interpreted as a single multi-byte value and compared that way.

3.8.3.2 RSTP operation overview

According to RSTP rules, each bridge port maintains a separate instance of a priority vector, called a port priority vector, whose elements describe the knowledge that the bridge has regarding a network which is directly connected to that particular port:

- Root Bridge ID – Bridge ID of the root device of the spanning tree,

- Root Path Cost – cost of the path from the bridge to the root device,
- Designated Bridge ID – Bridge ID of the designated bridge (a bridge offering the least costly path to the root device) for the network,
- Designated Port ID – Port ID of the designated port for the network (a port within a designated bridge through which it is connected to the specific network),
- Bridge Port ID – Port ID of the port maintaining this priority vector.

The first two elements provide information significant within the whole Bridged LAN structure, while the following two have significance within a specific LAN network connected to the particular port.
The port priority vector is updated based on information received from neighboring bridge devices within the Bridged LAN structure, so it reflects the current knowledge state of the particular bridge device. It should be noted, that such local knowledge can differ from the actual system state in time periods before the RSTP reaches convergence following Bridged LAN's topology changes.

Apart from maintaining the described port priority vector, a designated priority vector is generated for each bridge port, containing the information about the specific bridge and port:

- the root bridge identity (Root Bridge ID),
- cost of the path from the generating bridge to the root device (Root Path Cost),
- identification of the bridge being advertised (Bridge ID),
- identification of the port being advertised (Port ID),
- identification of the port providing information to generate the vector – element present only internally (not transmitted) and equal to Port ID.

It is the content of the designated priority vector, which is truncated to the first 4 elements to form a message priority vector, which is transmitted to neighboring bridges in RSTP Configuration Messages (CMs).

The port priority vector is subject to change, depending on message priority vectors received by the port from other bridge devices connected to the same LAN. If a bridge port receives a CM containing a message priority vector better than its current port priority vector, the port priority vector is updated using received information.
Such action reflects the fact that the receiving port's priority vector does not describe parameters of this specific port, but parameters of the network the port is connected to. As a result, each port connected to a given LAN should end with the same port priority vector – the best one of priority vectors proposed by ports connected to the particular LAN.

The procedure of comparing the received message priority vectors and port priority vectors serves to achieve a number of specific tasks:

- selection of the root bridge device of the spanning tree,
- selection of a root port for each bridge,
- selection of a designated bridge and port for each LAN,
- selection of alternate and backup ports at each bridge.

The first three of the listed tasks are necessary for creation of the spanning tree, while the last allows for faster recovery from network failures or topology changes.

3.8.3.2.1 Root bridge selection

The first task required for establishing a spanning tree in a Bridged LAN environment is a selection of a root bridge device. According RSTP rules, the bridge device with lowest Bridge ID will become a root device and the selection process itself is based on the first element of a priority vector – Root Bridge ID.

At the start of the procedure, each bridge device sets priority vectors for all of its ports according to its starting knowledge, which is limited to the bridge device itself. In this situation, the lowest Bridge

ID known to the device is its own, so it becomes the value placed in the first element of its port vectors and sent to neighboring bridge devices in Configuration Messages.

When a bridge device's port receives a CM containing a priority vector better than its own, it will overwrite its own vector with the received one. As the Root Bridge ID is a vector element of the highest priority, its change for more preferable value will always be accepted, overwriting this value in the port priority vector of the receiving port and, additionally in priority vectors of all ports in the receiving bridge. Resulting fast dissemination of information about the bridge with the most preferred Bridge ID through the Bridged LAN fulfills the task of the root bridge selection.

3.8.3.2.2 Root port selection

While Root Bridge ID element allows for selection of the root bridge of the spanning tree, the tree itself needs to be created. For this purpose, each bridge in the Bridged LAN must select a root port – a port which provides the best path towards the root of the tree.
The second element of the port priority vector (Root Path Cost) describes the cost of reaching the root bridge when sending frames through the specific bridge. The value of this parameter is a sum of costs associated with LAN networks which need to be traversed to reach the root bridge device. The costs associated with LAN networks can be in range from 1 to $2*10^8$ and, by default are based on a maximum throughput of the specific network technology, but can be customized by an administrator.

A procedure allowing the correct Root Path Cost value to be available at every bridge in the Bridged LAN is performed concurrently with root bridge selection.
The root bridge sets Root Path Cost value of its port priority vectors to 0 as there are no networks which must be traversed to reach the root bridge. This value is distributed by sending it in a CMs, as a second element of message priority vector, through all bridge ports.
Each receiving bridge device checks if Root Path Cost value of the received message priority vector is lower to the corresponding value of the receiving port's priority vector. If it is not, no action is taken regarding the root port, but if it is:

- the port which received such Configuration message is selected as a root port of the bridge,
- the received message priority vector Root Path Cost element value will be increased by the cost value of the network it arrived by and used to overwrite the value of Root Path Cost for all ports of the bridge.

The receiving bridge will then proceed with periodic sending the designated priority vector information to all of its neighbors, providing them with its own, updated Root Path Cost.

3.8.3.2.3 Selection of designated bridge and port

As the designated bridge is a bridge which can provide the best path from the specific LAN network towards the root bridge, its selection is closely related to the procedure of choosing the root port – the bridge device from which the Configuration Message resulting in choosing a root port has been sent will be selected as designated bridge for the network through which the message has been sent. It would seem that no further steps beyond these described in root port selection procedure are required for a designated bridge selection.
However, it is possible that there is more than one bridge device connected to the same LAN, advertising the same Root Path Cost. Such situation does not complicate the root port selection procedure, as by selecting the root port, we are choosing the next network (not device) on the path to the root. In case of a designated bridge selection procedure we are selecting a single, specific bridge device.
To allow us to choose between two bridge devices with identical values of Root Path Cost, their Bridge ID values are compared, the lower one being preferred.

Moreover, there is also a possibility, that more than one port of a designated bridge chosen according to the above procedure is connected to the network in question. Only one of these ports can be used to construct the spanning tree, so a designated port of the designated bridge must be selected. Following the overall rules of the RSTP, a value of the next element of priority vector is used for this purpose (Designated Port ID), with lower value being preferred. As a result, a designated bridge port with a lowest Port ID which is connected to the specific network is selected as the network's designated port.

3.8.3.2.4 Selection of alternate and backup ports

While the selection of root bridge, root port, designated bridge and designated port is strictly required to construct a tree spanning all LAN networks within a Bridged LAN, selection of alternate and backup ports is theoretically not necessary but nevertheless required by the RSTP standard to allow for fast recovery in case of network failure or topology change.

An alternate port is a port which can provide an alternate path from a specific network to the root bridge. As the active path from the specific network to the root device leads through its designated bridge, any other bridge connected to the network provides an alternate path.
As a result, any port connected to a particular network, whose bridge is not a designated bridge is an alternate port. If a port is not a root port and receives from the network Configuration messages indicating that another bridge is a designated bridge for this network, it should consider itself an alternate port.

A backup port can be used to provide a given network with alternate connection with its designated bridge. If a designated bridge for a specific network is connected to it by more than one port, only one of them is selected as designated port – the rest must assume role of backup ports. So, if a port is not a root port and receives a CM indicating that another port in its own bridge is a designated port for the same network it connects to, it should consider itself a backup port.

Both alternate and backup ports are not a part of the spanning tree structure of the Bridged LAN and are set to discarding state.

3.8.3.2.5 Relations between RSTP selection procedures

The above description divides the basic RSTP operation into specific, task-related procedures. However, it should be noted that all of these tasks are based on exchange of the same Configuration Messages and are performed in parallel.

If a port receives a Configuration message with a better (lower):

- Root Bridge ID – root selection, root port selection and designated bridge/port selection procedures are performed, as the very root of the tree has been changed and its structure must be completely rebuilt,
- Root Path Cost (but the same Root Bridge ID) – root port selection and designated bridge/port selection procedures are performed, as the new path towards root can lead through a different network and it is possible that a designated bridge in one of its connected network is going to change,
- Designated Bridge ID (but the same Root Bridge ID and Root Path Cost) – designated bridge/port selection procedures are performed, as a new bridge will be chosen for a designated bridge of one of its connected networks,
- Designated Port ID (but the same Root Bridge ID, Root Path Cost and Designated Bridge ID) – designated port selection procedure is performed, as the designated bridge in one of its connected network is now connected to it by a more preferred port.

3.8.3.3 RSTP convergence and transient loop prevention

Apart from constructing a transmission tree spanning all LAN networks in the Bridged LAN, the RSTP must also interact with other IEEE 802.1D bridging mechanisms, such as address learning and MAC forwarding table maintenance. Such interaction is necessary to prevent transient traffic loops following topology change events. Such problems can occur due to:

- time required for the RSTP to reach convergence, during which the transmission tree cannot be assumed to be correctly constructed,
- obsolete entries in MAC forwarding tables of some bridge devices, still reflecting the network state from before the spanning tree recalculation.

When there is a need to change the spanning tree structure, for example due to failure of an existing link or an activation of a new one, there is a period of time, when some bridging devices in the Bridged LAN are already reconfigured to react to the change of physical topology of the network, while others still retain a previous (now obsolete) configuration. It is possible, that if previously discarding ports would be changed to a forwarding state during this such time period, transient transmission loops would occur, until all devices would assume the new configuration.
To prevent such an occurrence, an older STP protocol introduced a lengthy delay between changing a port role to one which requires the port to be in forwarding state and the resulting change of the port state itself. This delay endured that all bridge devices within the Bridged Network have been reconfigured to reflect new conditions (the STP protocol reached convergence) before any actual change in port state had occurred.
In case of the RSTP a Proposal/Agreement sequence between neighboring bridge devices and a Sync mechanisms are used instead, which results in much faster reconfiguration of the network.

When a change in physical network topology results in selection of a new designated or root port, such ports are initially in discarding state to prevent transient transmission loops. Until they reach forwarding state, they will set a Proposal flag in BPDUs they send.
A bridge receiving BPDUs with a Proposal flag set will start a Sync process by setting all of its ports (except edge ports) in discarding state. The bridge will then confirm its readiness to allow the sender of the BPDU to activate its new designated port by sending back a copy of its BPDU with Proposal flag cleared and Agreement flag set. Such transition can be safely made, because all other ports of the agreeing bridge (leading further down the tree to bridge devices which are not yet aware of the topology change and could form a loop) are in discarding state.
When discussed ports change their state to forwarding, the bridge that had agreed to the change will start sending updated topology information with the Proposal flag set. This way the topology change is propagated down the tree, but at each step, before activating new root port of a bridge, all its other ports are blocked to prevent loops through devices which not yet received new topology information.

To ensure that no bridge device retains obsolete MAC forwarding table entries, they must be notified of the topology changes. To ensure that this general goal is achieved, two separate tasks must be undertaken: topology change detection and topology change propagation.
To detect a topology change, each bridge monitors if any of their non-edge ports previously being in other state, changed its state to forwarding. As such an event can occur when a new root port or a new designated port is chosen, it definitely represents a change in the spanning tree topology.
It should be noted, that loss of connectivity is not interpreted as a topology change by RSTP, as such an occurrence cannot directly cause formation of transmission loops and a topology change will be detected when the RSTP protocol reacts to the loss by reconstructing the tree.

If a topology change is detected by a bridge, it will flush addresses reachable through its root and (non-edge) designated ports from its MAC forwarding table. The bridge will then inform its neighboring bridge devices that a topology change has been detected by setting (for a specified period of time – TC While time) a Topology Change (TC) flag in its BPDUs sent out the root and designated ports.
If another bridge receives a BPDU with TC flag set, it will flush its MAC forwarding table, except for addresses reachable through the port the BPDU arrived through. It will then proceed to send its own root and designated port BPDUs with a TC flag set for a TC While time.
That way an information about topology change is quickly propagated through the spanning tree, allowing all bridge devices to remove obsolete information from their forwarding tables.

3.8.4 IEEE 802.11s mesh network performance assessment

One of the most promising mesh solutions currently being developed is an IEEE 802.11s standard, aimed to create a broadband, fully auto-configurable, dynamically extending, and secure mesh solution, based on widely popular WiFi wireless local area network (WLAN) technology. It is designed to serve in wide variety of environments, starting with small ad-hoc, isolated networks (for example: groups of laptops or smartphones), through industrial/sensor network deployments, office LANs, and ending with large, self-extending, public access systems.
The fact that this solution is based on cheap and popular WiFi technology and can be deployed on existing hardware makes it one of very few mesh solutions able to successfully appear and remain on popular WLAN market. Additionally, a number of design decision have been made to make an IEEE 802.11s mesh as compatible and as easy as possible to integrate with existing network systems. Examples include: mesh gates - specialized network nodes responsible for integration with external networks, hybrid routing protocol - ensuring that there are relatively small delays in routing to external destinations, higher layer transparency - making mesh network seem as a single Ethernet broadcast domain, complete with 802.1D [79] compatibility (bridging and spanning tree protocol). It is evident, that standard authors aimed to provide a robust building block for modern networks systems, both functional and inexpensive to deploy.
Due to its robustness, an IEEE 802.11s-based mesh can be deployed in a variety of previously described roles, including the most complex - self-organizing office/building/campus infrastructure and access system.
Despite the above advantages, a number of areas in the discussed standard lack sufficient support, which can lead to significant inefficiency and degradation of service quality in real-world IEEE 802.11s network deployments.
The first serious limitation is the fact, that the standard in its current form does not include support for creating multichannel mesh networks, which leads to severe throughput degradation due to both intra and inter-path interference.
This limitation is especially important in case of dense mesh networks, where each transit node directly affects a high number of neighboring nodes. The inability to perform concurrent transmissions within a given neighborhood by spreading them across a number of orthogonal frequency channels or for a single node to concurrently receive and transmit on different channels (by using multiple wireless interfaces) results in highly inefficient RF resource utilization.
In this situation, each additional hop on the transmission path consumes high amount of limited RF resources, not only resulting in lowering QoS parameters of a given transmission (due to intra-path interference), but also affecting all neighboring transmission paths (causing inter-path interference).

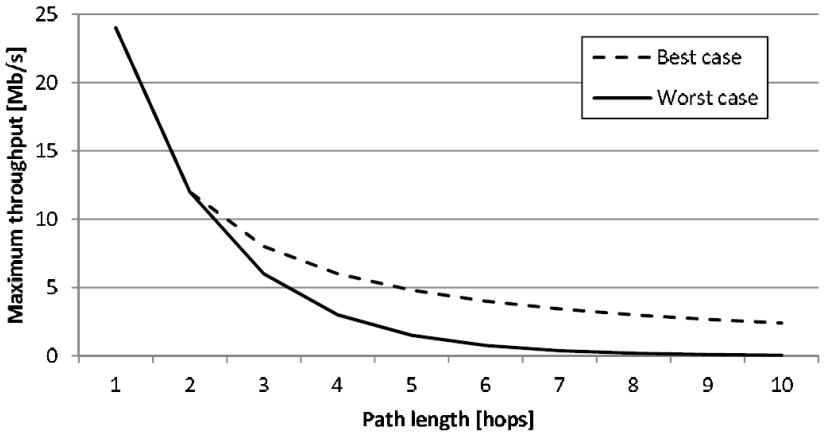

Fig. 79 Theoretical assessment of a maximum throughput of a single channel multihop network [84]

Fig. 79 illustrates the theoretical maximum throughput as a function of number of hops in a single channel WiFi mesh, where only one transmission is currently conducted (there is no inter-path interference). Two cases have been considered:

- an optimistic case - where it is assumed, that each of transit nodes has only two neighbors in both its communication and interference range: its predecessor and the next node on transmission path,
- a pessimistic case - where it is assumed that all nodes are within interference range of each other.

As can be seen from the above description, in case of single-channel mesh network, it is crucial to keep the number of hops on a length transmission path as low as possible, as it will improve both the efficiency of resource usage and a QoS level available for users. To verify the above statements and assess the impact of the mesh path length on the quality of our example multimedia services, a number of experiments have been conducted below, taking into considerations such aspects as mesh network structure, background network traffic level, and transmission distance. Additionally a few interesting elements of an MBSS system, of possibly significant impact on the general user satisfaction level, have been highlighted in comparison with the classic PtMP environment described earlier – they include the process of recovery from a failure of an internetworking device (AP in a PtMP system and a mesh gate in an MBSS network) and client-extended coverage capabilities.

3.8.5 IEEE 802.11s mesh network topologies for simulation experiments

To illustrate the described mesh efficiency problems and analyze them in greater detail a series of simulation scenarios have been performed in the following wireless mesh structures:

Random network created with uniform placement model

Using this method, an area of size $|A|$ is chosen and n nodes are placed within with uniform probability of:

$$P = \frac{n}{|A|} \tag{2}$$

The main problem of this model is a requirement of high node density if we are to ensure high probability of creation of a well-connected network. In [85] and [86] authors estimate that nodes

need to have an average degree of respectively 10.8 and 13.78 if we aim to obtain a network which is connected with probability of 0.99.
A significant number of modifications have been proposed for this model, to obtain a well-connected network without the requirement of high node density [87-89], but they tend to have limited utility in modeling real-world conditions [90].
This model will be used as an approximation of ad-hoc gathering of clients over a specified area of uniform propagation conditions – for example an outdoor event.
As size of such area will be limited due to requirement of uniform propagation conditions and taking into account a relatively long communication range of IEEE 802.11 technology, we can expect to obtain a sufficiently high node density for an unmodified uniform placement model. In subsequent experiments using this model, a two-dimensional, rectangular area will be used.
Despite relative simplicity of the random placement method, it provides an adequate approximation of mesh node placement in some of the real-world IEEE 802.11s deployment scenarios [90].

Random network created with modified grid placement model

In standard grid placement model, nodes are located at intersections of rectangular grid.
Parameters of the grid, such as distance between grid lines, are typically chosen depending on node communication radius to obtain a well-connected network with a non-border node degree of 4.

In the presented research a modified grid placement model will be used, where first an intersection of a two-dimensional, rectangular grid is selected for a node placement with uniform probability of:

$$P(I_i) = \frac{1}{N} \tag{3}$$

where I_i is a chosen intersection and N is a total number of intersections.
Then a node is randomly placed, with uniform probability, within a rectangular area A defined as

$$\left(x_i - \frac{s}{2}, y_i - \frac{s}{2}\right), \left(x_i + \frac{s}{2}, y_i + \frac{s}{2}\right) \tag{4}$$

where x_i and y_i are coordinates of the chosen intersection I_i, while s is a parameter describing size of the placement area.
It should be noted, that described modification allows for multiple nodes to be placed in neighborhood of the same grid intersection and for a number of grid intersection neighborhoods to remain empty.
This model will be used as an approximation of scenarios with semi-organized placement of nodes such as open-space offices.

Network model parameters

Based on the previously conducted experiments concerning IEEE 802.11 PtMP efficiency in our chosen propagation environment, it has been possible to choose the range of 70 m as a maximum distance between two communication stations, at which there is still no degradation of transmission parameters due to propagation conditions (no background traffic). The range at which a multimedia service is still usable with an acceptable QoS is dependent on the service, and has been shown to be:

- 95 m for the low throughput G.711 PLC VoIP transmission,
- 85 m for the 2 Mbit/s H.264, non-interactive video streaming.

Taking these values into account, a two versions of each of the above network types have been selected for further experiments:

- Sparse grid network – based on a modified grid placement model, with grid lines 85 m apart and *s* parameter being 10 m. Such network guarantees a possibility of a link formation along the grid lines and randomly offers a chance of forming a low quality links diagonally within a grid. At the same time placing mesh STAs at relatively long ranges can serve to limit inter-path interference within a mesh.
- Dense grid network – based on a modified grid placement model, with grid lines 65 m apart and *s* parameter being 10 m. Such network guarantees a possibility of a good quality link formation along the grid lines. Additionally it offers a chance of forming a good quality links diagonally within a grid. At the placing mesh STAs at such limited range can result in increased inter-path interference within a mesh.
- Sparse random network – a network of randomly placed nodes where a mean distance between neighboring mesh nodes of the resulting MBSS structure is close to 70 m. Such structure results in lower node degrees. The level of intra-path interference can be expected to be lower, but at the same time, the quality of wireless links will also suffer due to longer ranges at which they are forced to operate (and still be used by path selection mechanisms).
- Dense random network – a network of randomly placed nodes where a mean distance between neighboring mesh nodes of the resulting MBSS structure is close to 45 m. Such structure results in relatively high node degrees and a well-connected network. However, a significant level of intra-path interference can be expected.

Network creation parameters chosen above also enable easy comparison with results of IEEE 802.11 PtMP experiments using network creation policies described as a high quality grid, maximum coverage grid and random AP placement, specified in 2.5.7.4.

3.9 Experiments

To compare the Quality of Service possible in IEEE 802.11s MBSS with the quality archivable in case of IEEE 802.11-2007 PtMP network, a set of experiments corresponding to these already described for the latter technology (see 2.5.7) has been performed for the mesh network.
However, this time we will limit the extent of our experiments to EDCA traffic classes most appropriate or a given service type: AC_VO (Voice) for a VoIP service and AC_VI (Video) for a non-interactive video streaming. All parameters of the above services remain the same as in case of previous experiments (see 2.5.7.1), to facilitate performing a comparison between PtMP and mesh systems.

3.9.1 Direct STA-STA communication

As there are no centralized access points in an MBSS, so all transmissions between different mesh stations are conducted according to the same rules – by obtaining a transmission path using HWMP protocol. As a result, if previous STA to STA scenarios (see 2.5.7.3), with communicating STAs located in mutual, direct communication range were performed in MBSS environment they would be able to communicate directly (1-hop), instead of using AP retransmission (2-hop). Resulting MOS values (Fig. 80) are clearly superior to these obtained with use of a classic IEEE 802.11 PtMP setup.

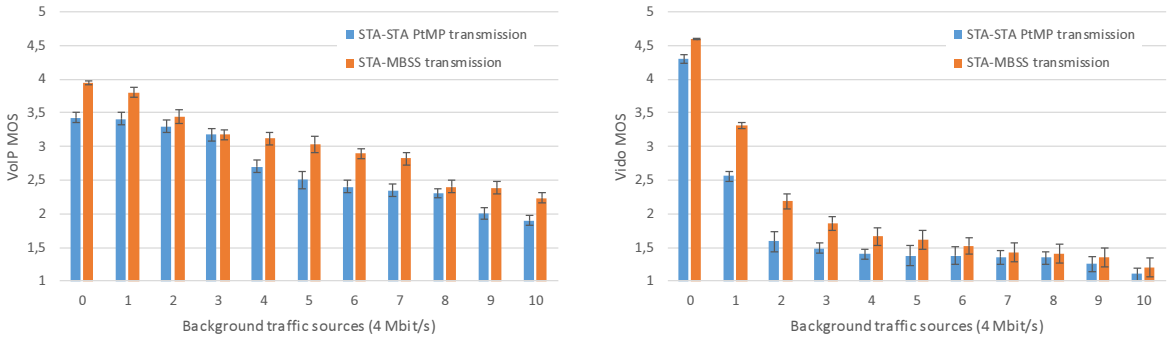

Fig. 80 MOS values for STA-STA transmissions between neighboring STAs in IEEE 802.11 PtMP and IEEE 802.11s MBSS networks (left chart – VoIP, right chart – video)

Thus the ability of direct STA to STA communication can be considered the first of IEEE 802.11s mesh network advantages over the classic IEEE 802.11 PtMP infrastructure mode. It should be noted, that IEEE 802.11 standard defines an optional Tunneled Direct Link Setup (TDLS) protocol, which enables similar, direct STA-STA communication, but its implementation is very limited in real-world hardware, while analogous functionality of the IEEE 802.11s specification obligatory and thus available in all implementations.

3.9.2 Experiments in IEEE 802.11s MBSS network with no background traffic

As before, the first set of experiments will be conducted in a network without any additional background traffic. For each experiment a set of 40 mesh stations has been placed over a 500 m x 500 m area, following the rules specified for all 4 of network structure types described above: dense and sparse versions of both grid-based and random structures. The number of station has been chosen to remain the same as it was in case of earlier PtMP experiments (see 2.5.7.4, 10 APs and 30 STAs).
For each simulation run a single existing mesh STA has been selected as a destination, while an additional mesh station have been randomly placed within the area, at a specified distance from the destination STA (if the distance would require the STA to be placed outside of the test area or the selected STAs were unable to communicate, the process of selecting a destination STA has been repeated). After a 10 s warmup time (allowing the mesh mechanisms to create an MBSS structure) a multimedia transmission between them has been initiated and maintained for 60 s.
The transmissions conducted were of the same type and parameters as in case of PtMP network experiments described earlier: a VoIP (G.711 with PLC) or a non-interactive video streaming (2 Mbit/s H.264). The exact parameters of these multimedia services have been described in 2.5.7.1.
Each such experiment has been repeated 50 times to obtain statistically meaningful results and 95% confidence intervals have been marked on the following charts.

UDP data transmission

To help analyze the following results and verify the correctness of the assessment stated in [84] and shown in Fig. 79 for our mesh structures and propagation environment, a maximum UDP throughput test, analogical to the one performed for PtMP environment has been conducted. However, instead of path length in hops, the following results use a distance between communication stations in meters. Such approach will allow an easier comparison between different services (inelastic data, VoIP, non-interactive video) deployed in different mesh structures described in Section 3.8.5.

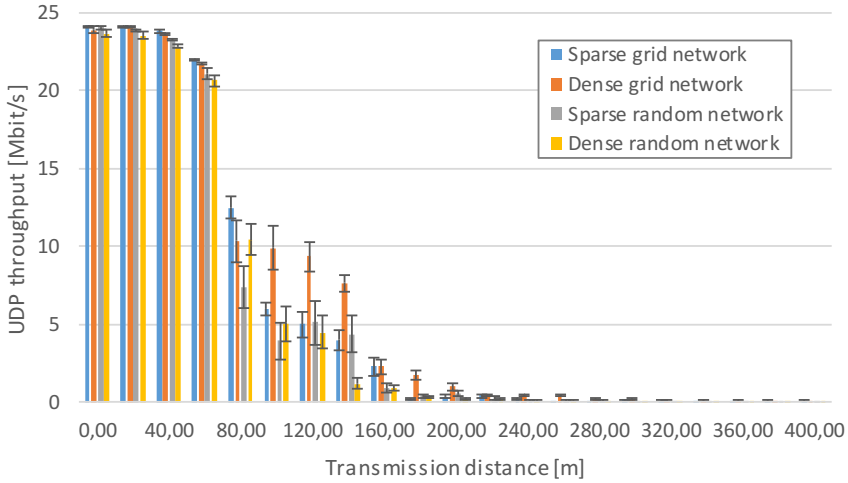

Fig. 81 IEEE 802.11s UDP throughput for different network structures and transmission distances

The obtained results for our particular propagation environment and network structures are in general keeping with the abovementioned overall assessment (with a roughly estimated length of a single hop between 60-90 m). That characteristic alone, by illustrating the limited availability of transmission resources in a single channel mesh network, clearly illustrates the need to minimize transmission path length within the MBSS, as the negative impact of additional retransmissions becoming necessary at the transmission path is clearly visible. Of the considered network structures grid-based deployments seem to generally provide a higher throughput with growing distance between communicating stations. A dense grid structure shows a particularly good results, due to a high quality of communication links between its stations due to limited distance between them.
At the same time, we must observe, that the available transmission bandwidth, while fully capable of supporting relatively low-bandwidth VoIP communication over considerable distances, will prove insufficient for a 2 single Mbit/s video transmission at a range of 160-180 m.

VoIP transmission

The mesh network structure has been generated using 4 different method described earlier (see 3.8.5), and a single VoIP transmission has been conducted in absence of background traffic, expect that generated due to activity of MBSS protocols.

Looking at charts presented in Fig. 82, it can be seen that, in absence of a background traffic, a forwarding delay component of IP transmission delay is relatively small (about 3-4 ms per transmission hop), compared to initial layer-3/layer-2 processing at source STA. This advantageous property can be attributed to IEEE 802.11s mesh operating strictly within ISO-OSI layer 2 in contrast to mesh solutions performing ISO-OSI layer 3 routing at transit nodes. It is even smaller per hop, than in case for AP processing in a STA to STA PtMP communication scenario. The delay is well within the requirements for VoIP communication.

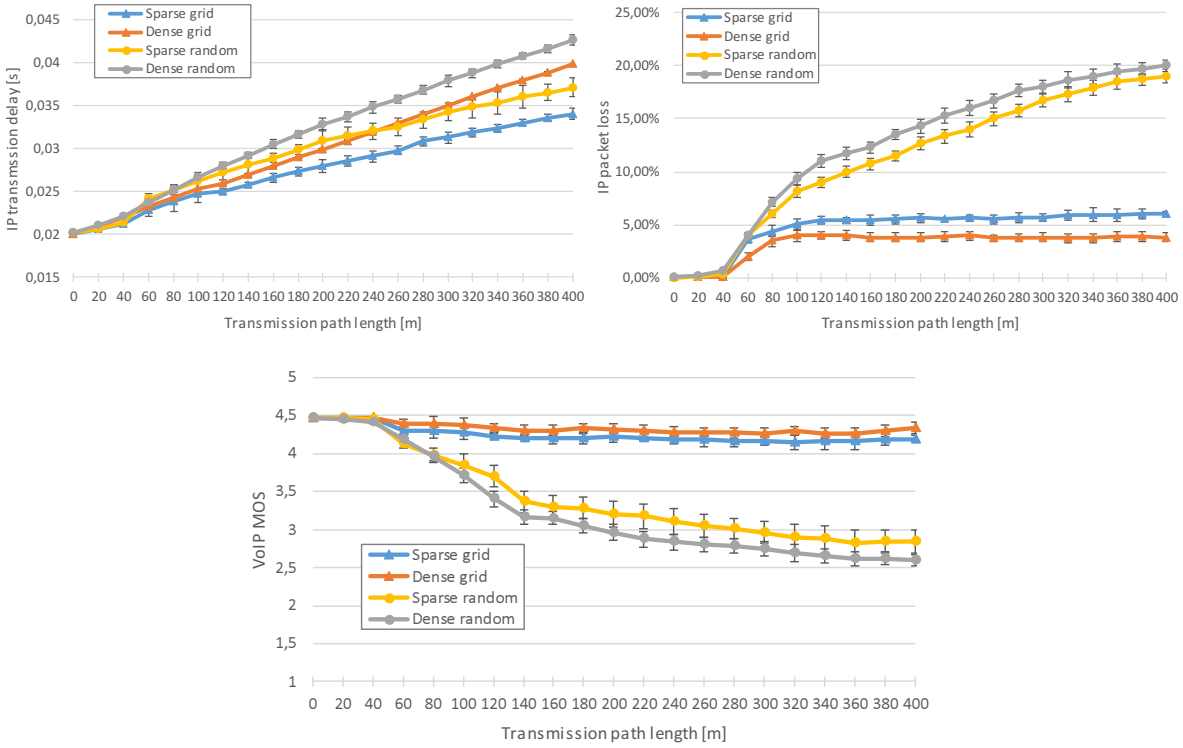

Fig. 82 VoIP transmission with no background traffic

It can be seen, that grid-based mesh structures generally provide lower and more stable delay and packet loss characteristics then randomly generated ones. While difference in the total IP packet transmission delay are not very significant, the greater width of confidence intervals is a direct result of the unpredictability of the randomly generated structures with mesh paths utilizing a combination of both short and long range transmission hops. The effect is especially distinct in case of the sparse random structure, with its higher probability of utilizing relatively longer and lower quality links. In contrast, the difference in packet loss ratio is prominent with random mesh structures reaching 10% loss at about 100 m which is continues to grow until the final range of the test (400 m) when it reaches 20%. Grid structures in the same conditions maintain a stable loss value of 5% (sparse grid) or lower (dense grid), which does not show a noticeable increase with a growing length of the transmission range.

A comparison of grid-based network structures and the ones generated on strictly random basis clearly shows the advantage of the former, with dense grid offering both the lowest transmit delay and packet loss ratios. The effect points out to a higher importance of utilizing exclusively good quality links (shorter ranged) than attempting to minimize the impact of intra-path interference effect by spacing STAs further apart, at least in case of such a low bandwidth transmission.

In overall, the quality of communication is surprisingly good, with MOS remaining at about 4.3 at 400 m in case of grid structures and between 2.5-3.0 in case of random ones.

So far, results seem to contradict the expectations of high importance which should be ascribed to minimizing the length of MBSS transmission paths. However, we should remember, that the scenario illustrates a highly theoretical case of a single 64 kbit/s transmission in an otherwise unloaded mesh network.

Video transmission

The same scenario has been repeated for a non-interactive video streaming service, with its 2 Mbit/s bandwidth requirement and high susceptibility to a packet loss. In that case, a relation between service quality and the length of the used transmission path is clearly evident (Fig. 83).

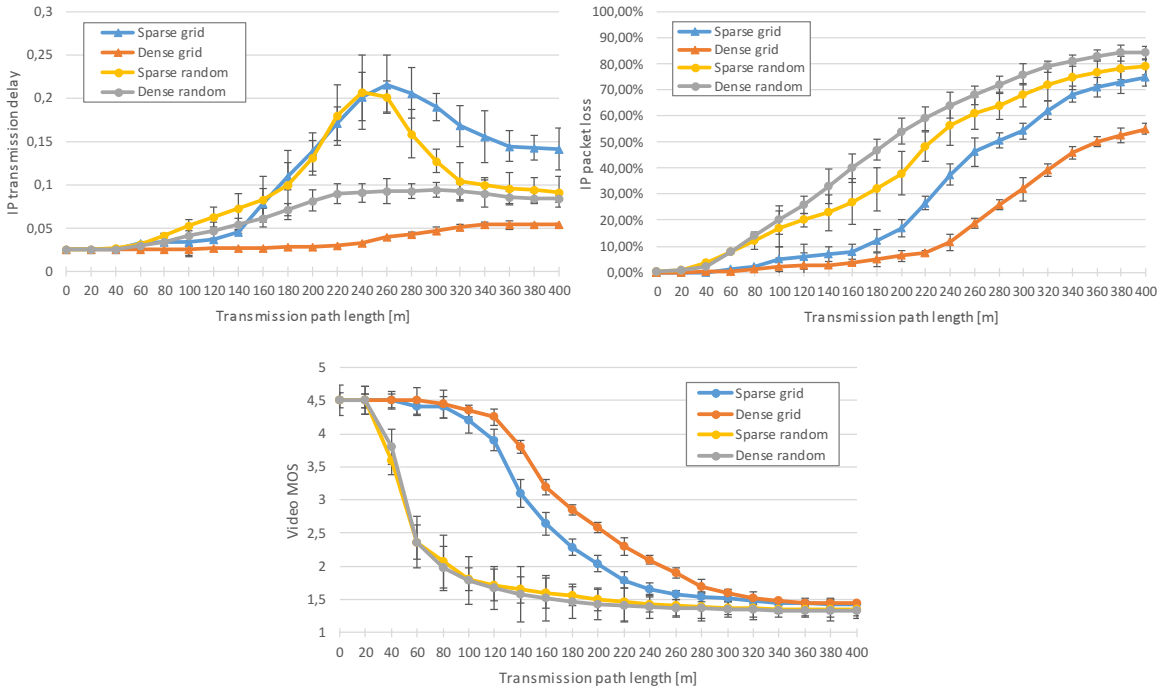

Fig. 83 Non-interactive video streaming with no background traffic

The delay characteristics of video transmission shows an easily observable growth with increasing distance between communication stations except for the dense grid mesh structure, where regular placement of mesh stations within high quality transmission range helps to minimize the effect. The sudden decrease of IP transmission delay following its rapid growth to over 200 ms can easily be explained by referring to a packet loss chart and remembering, that the delay is calculated only for actually delivered packets. With packet losses exceeding 30-50% (depending on the structure) at 220 m and continuing to grow, it is the delay characteristic ceases to be meaningful for these ranges. Significant width of confidence intervals seems to confirm this interpretation.

The only mesh structure which does manage to maintain a relatively limited transmission delay (mostly under 50 ms) is, again, a dense grid structure. However even in its case, packet loss ratio starts to climb at about 160 m and exceeds 10% at 220 m, to eventually grow to over 50% at the maximum considered range of 400 m.

With the packet loss increasing rapidly in case of random mesh structures to reach 80-90% at 400 m, these structures seem to have a limited use for higher bandwidth multimedia services. Grid structures also show similar growth, in their case, however, it remains under remotely acceptable 10% until the range of 170 m for a sparse grid and 200 m for a dense one.

Such results are consistent with previous assessment of the available network bandwidth (Fig. 81), which is expected to prove insufficient for the video transmission at ranges over 160-180 m.

The MOS of the video streaming service confirms the above expectations, in case of random mesh structures dropping almost immediately (at about 60 m) under 2.5 and then decreasing under 1.5 at a range of 180 m. Grid-based mesh deployments retain a good quality much longer, showing a MOS values of over 4.0 up to 140 m and then experiencing a steady decrease, but remaining of acceptable quality up to a range of 200-260 m.

From the above experiments, it is evident, that a particular structure of MBSS can be of high importance for efficient handling of network traffic in difficult propagation conditions – with necessity of performing relatively long range transmissions between MBSS stations, the quality of communication can be severely degraded. The low performance of a dense random network indicates that even a limited number of such links is sufficient to degrade the quality of transmission significantly.
At the same time, the multihop transmission capability of MBSS network seems to be able to significantly increase the range in which a multimedia service can be provided with adequate quality, especially in case of low throughput traffic streams.
However, with sufficiently high bandwidth requirements, even in case of an MBSS network with no background traffic, the impact of interference between transmissions of different STAs becomes clearly evident and limits the available bandwidth severely. This observation tentatively confirms both the danger of intra-path interference and the need to minimize lengths of wireless transmission paths through MBSS. Still, a care should be taken to avoid the use of long-range/low-quality mesh links.

3.9.3 The impact of background traffic

Having assessed the basic ability of MBSS network to provide a sufficient Quality of Service for VoIP and video transmissions without degrading effects of background traffic, we will now proceed with experiments taking this factor into consideration.
Based on results obtained for an unloaded network scenario, we are going to limit presented results to distances of 60, 160 and 300 m between communication stations. The background traffic has been generated by performing a number of concurrent 1 Mbit/s UDP transmissions within the mesh structure, each of them between stations at least 200 m apart and using the same traffic class as the multimedia service. The experiments have been conducted for 2, 4 and 8 such background traffic streams. The results are presented in Fig. 84 and Fig. 85, with an uniformly selected scale to facilitate easy comparison between different scenarios and services.

The conclusions indicating that a low-throughput VoIP service can be successfully deployed in an MBSS environment seem to be confirmed by results shown in Fig. 84, which demonstrate the impact on a background network traffic on the service of this type. For all considered network structures the obtained MOS values remain relatively high. The problem of limited maximum throughput of long mesh transmission path is clearly of little importance in case of a single VoIP traffic stream.
Another previous observation confirmed in this experiment is that random network structures (C and D) generally tend to provide a lower level of service, as indicated by their higher packet loss ratios. Grid-based structures (A and B), with their grid line distances based on preliminary PtMP experiments are able to provide a better service, by eliminating the need to use a long-distance low-quality links. The confidence intervals are also wider in case of random networks underscoring relatively lower predictability of multihop communication in such structures.
The adverse impact of background traffic can be observed to be relatively higher in case of longer mesh paths, which is expected due to a potentially larger area of mutual interference between different traffic streams. Also the impact of such traffic is shown to be higher in sparse structures (A and C), which indicates that its degrading effect is more pronounced in case of low quality links. This effect clearly outweighs the possibly advantageous effect of spreading mesh stations over a larger area, thereby reducing the other stations' interfering signal strength due to a longer range.

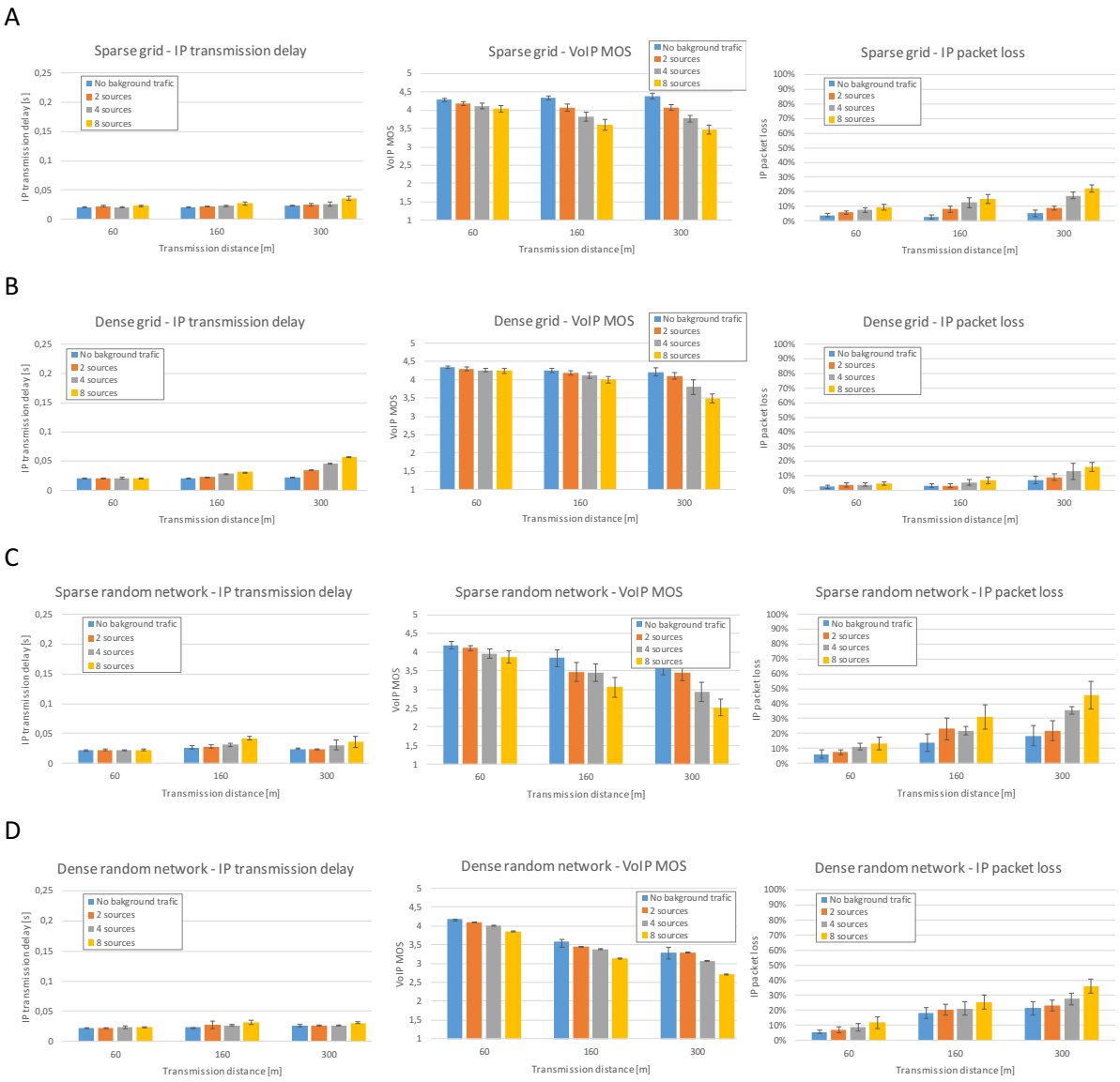

Fig. 84 Impact of background traffic on a VoIP transmission in different (A – sparse grid, B – dense grid, C – sparse random, D – dense random) structures of IEEE 802.11 MBSS network

In case of results for a 2 Mbit/s video service (Fig. 85), the already observed effect of a mesh transmission path's maximum throughput being reduced with distance is clearly confirmed. Similarly, so it the effect of decreasing the observed transmission delay due to excessive packet loss.

The relatively high throughput of the video service, the impact of both distance and background traffic is high, resulting in low MOS scores for any but a low range transmissions with no background traffic in grid-based networks (A and B). The effect of the later is very significant even with a 60 m transmission path. In case of longer paths the effects of the background traffic is less observable in MOS score which is already low, but can be clearly seen in packet loss charts.
In case of randomly generated networks (C and D) the MOS score is consistently lower than in case of grid-based networks (A and B). Moreover, in their case, the adverse effect of background traffic is clearly observable even for long paths, despite their already high packet loss.
The worst case seems to be a sparse random network (C), in which the quality of communication degradants very quickly with both range and background traffic.

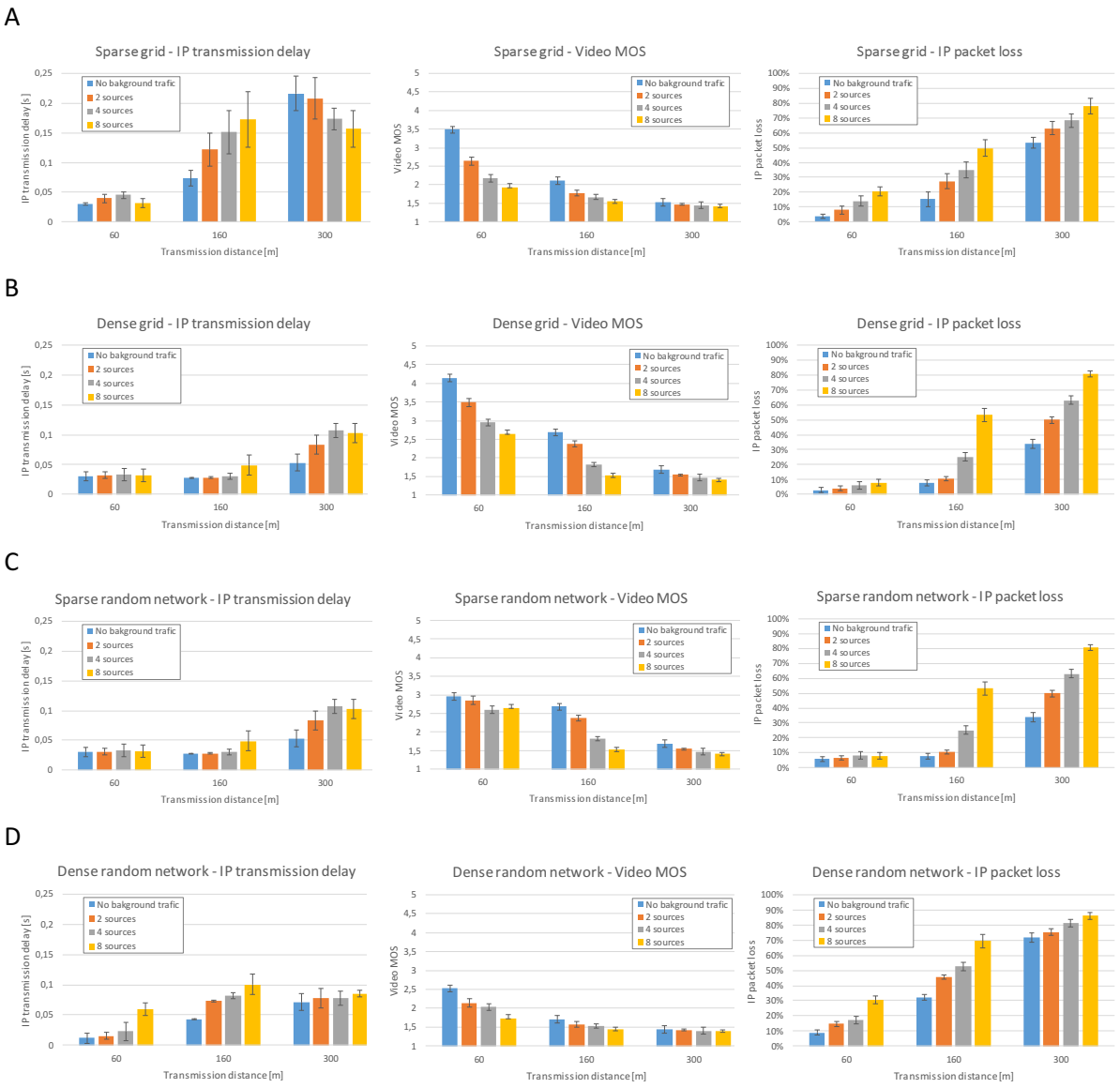

Fig. 85 Impact of background traffic on a non-interactive video transmission in different (A – sparse grid, B – dense grid, C – sparse random, D – dense random) structures of IEEE 802.11 MBSS network

The experiments in the MBSS network with background traffic confirm the general conclusions derived from earlier experiments. Due to both intra-path and inter-path interference, it is highly advisable to keep mesh transmission paths as short as possible in terms of number of hops, as long as it does not cause the path to utilize high-loss wireless links.

3.9.4 Deployment of an MBSS system in place of IEEE 802.11 PtMP multi-AP network

Because in case of an IEEE 802.11s MBSS system, each participating STA is capable of operating as a transit station, each such station provides its own coverage area from within which other STAs can perform a mesh peering and connect to the MBSS network. As a result a coverage area of a sufficiently populous MBSS network lacks coverage holes frequent to PtMP systems deployed in difficult propagation environments. To allow us to compare the coverage and its associated QoE of our selected multimedia service in PtMP and MBSS environment, a scenario analogous to the one

described in 2.5.7.4 has been performed. Of the 40 mesh STAs used in all of our mesh experiments, we have randomly selected 10 to function as mesh gates and thus provide all mesh stations with connectivity with external wired infrastructure, where a host being a destination of a multimedia transmission is located.
All 40 stations have been placed within a 500x500 m area (as before), adhering to previously described (see Section 3.8.5) rules of creating grid-based and random mesh structures.
As before, each station capable of communication with external network attempts to use the VoIP or non-interactive video streaming service described in 2.5.7.1. The results include a number of mesh stations (excluding 10 STAs selected as mesh gates, Fig. 86) capable of internetwork connectivity and MOS scores for each of tested services (Fig. 87).

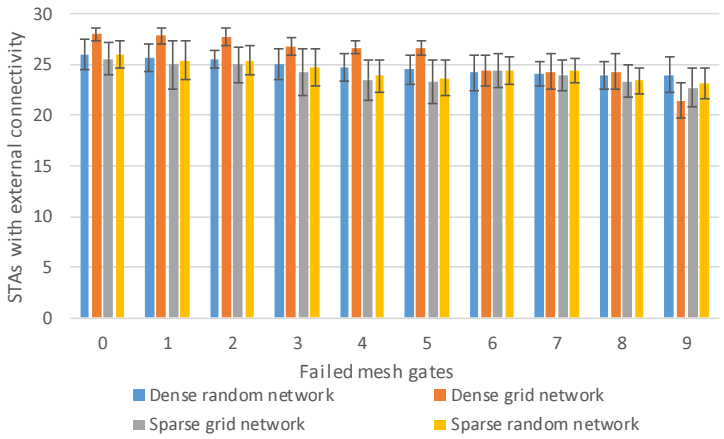

Fig. 86 Number of STAs retaining connectivity with external network as a function of failed mesh gates

The experiment confirms a much more through coverage available in case of an IEEE 802.11s MBSS system, compared to a very similar deployment performed using a classic PtMP IEEE 802.11 devices. Almost all devices retain their connectivity with external network even when the number of remaining mesh gates is significantly reduced. The dense grid network provides the most trough coverage, however it also shows the most observable reduction of stations retaining their ability to communicate with external networks. In contrast, a random network structure seems to ignore the deactivation of mesh gates.

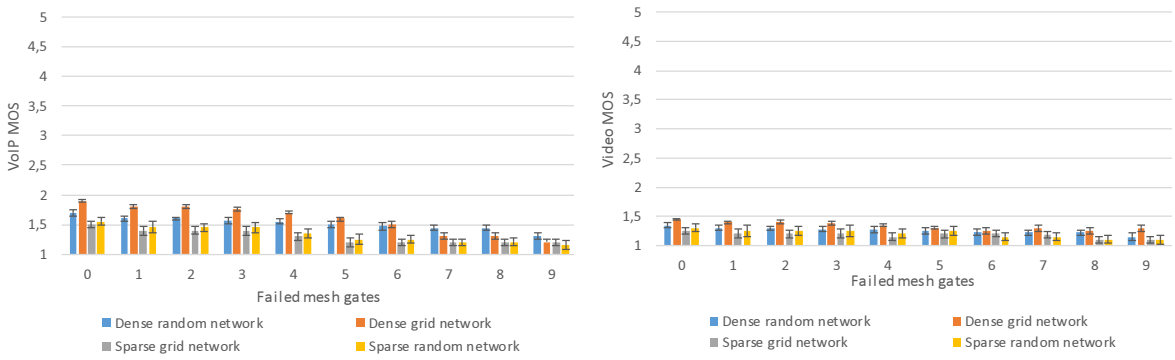

Fig. 87 MOS scores for an internetwork VoIP transmission and a non-interactive video streaming in the IEEE 802.11s MBSS as a function of failed mesh gates

However, despite such a considerable gain in a percentage of connected wireless stations, MOS scores for the VoIP and especially for the video transmission indicate their almost complete failure in this environment, as far as the resulting QoE is concerned. Based on the presented description and previously described scenarios, the explanation is very simple and focuses on two particular traits of IEEE 802.11s specification:

- the single-channel mesh operation,
- the use of standard RSTP protocol to disable all mesh gates connecting the MBSS with the same external network, except one.

Both of these characteristics have been introduced to maximize compatibility of IEEE 802.11s systems. The first one, allows for an uncomplicated, single-radio devices to participate in an MBSS system. However, due to the fact that an interference range is generally greater than an effective communication range, single-channel operation causes large number of mesh STA to contend for the same frequency channel, causing both intra-path and inter-path interference. Fortunately, with new specifications being added to the IEEE 802.11 standard, it begins to evolve from a solution depending on choosing of orthogonal frequency channels for independent operation between different devices, to a solution utilizing a very limited number (possibly only 1) of channels of considerable width – with IEEE 802.11ac specification the channel width has been extended from 20 MHz to 160 MHz. Such a change was possible due to development and implementation of mechanisms allowing multiple devices to share a high-width frequency channel by utilizing only parts of its width depending on activity of other devices, and performing the above decisions on frame by frame basis. This evolution towards a single channel WLAN technologies combined with development of the abovementioned coexistence mechanisms should positively influence the efficiency of a single-channel mesh operation, without a necessity of extending its own mechanisms and procedures.

The second characteristic has been introduced to make an IEEE 802.11s MBSS compatible with IEEE 802.1D specification, thus allowing its easy integration with other popular LAN technologies (for example: Ethernet networks). However, due to characteristics of IEEE 802.11s MBSS operation and limited transmission resources of a wireless network, the simple expedient of disabling network interconnection points is a costly decision. In this particular scenario, it limited all mesh STAs to a single mesh gateway able to forward their traffic to its destination, causing creation of long mesh transmission paths and concentrating all of these paths around the remaining mesh gate. As indicated by earlier experiments, such situation combines two main adverse effects for an efficient mesh transmission – a high number of retransmissions over the transmission paths (directly resulting in increased intra-path interference and indirectly extending the areas where inter-path interference is likely) and concentration of traffic over a relatively small area (directly increasing inter-path interference for path in the area). Surprisingly, the good coverage provided by the mesh network works to our disadvantage in this instance, because in case of MBSS fragmentation into a number of disjoined structures, each of them would be allowed by the RSTP protocol to activate its own mesh gate.
Due to the severity of this last IEEE 802.11s limitation, a cross-layer solution described in Section 6.1 has been dedicated to solving this problem by enabling multiple mesh gates to remain active. Apart from this solution, another of proposed cross-layer mechanisms (see Section 6.2) will allow inactive mesh gates to forward traffic to the active one using transmission technologies other than wireless transmission, if such are available.

3.9.5 Inefficiency of IP support due to the group addressed traffic delivery method

As already demonstrated in IEEE 802.11 PtMP environment, the unreliable (without acknowledgements) delivery of group addressed traffic results in a very high packet loss (see 2.5.7.3). Moreover, the link quality and the level of traffic load impacts the delivery ratio both negatively and severely. Additionally, in the IEEE 802.11s specification, there are no specific procedures dedicated to handling a multicast traffic, which is delivered the same way as a broadcast traffic – by flooding the mesh structure, with all mesh stations retransmitting the group addressed frame once.

It may seem strange, why no multicast specific traffic delivery optimizations have been included in the standard, however, it becomes clear when we look at the broadcast delivery ratio for the PtMP environment (see Fig. 42). With such a high loss rate, the redundancy of broadcast flooding greatly increases the chances of successful delivery of the broadcast frame to all mesh STAs (especially in dense mesh structures) – any optimizations leading to a reduction of the number of retransmissions would lead to an increase of the chance of performing an incomplete broadcast.
In this situation and based on previous research [20] it has been decided to omit detailed experiments concerning the efficiency of group addressed and concentrate on its effects on the quality of support of IP suite of protocols.

With group addressed traffic deemed unfit for direct use in deploying multimedia services in mesh networks functioning in real-world propagation conditions, the use of many unicast streams is advised instead. For this purpose, an ability of establishing an IP communication with a set of mesh STAs quickly and efficiently would be of practical use. Unfortunately, it seems that the described problems with a group addressed traffic delivery will influence even this task, because operations such as obtaining an IP to MAC address mapping using ARP protocol requires a broadcast transmission. At the same time, timeout values for protocols such as ARP protocol, governing the delay which must elapse before the procedure can be retries are specified in seconds (in case of the ARP protocol – 1 s). The situation is even worse for higher layer protocols such as Multicast DNS (mDNS) for which the timeouts are even longer (a minimum of 2 s), and whose operation requires two multicast transmissions, each resulting in broadcast flooding through the MBSS.

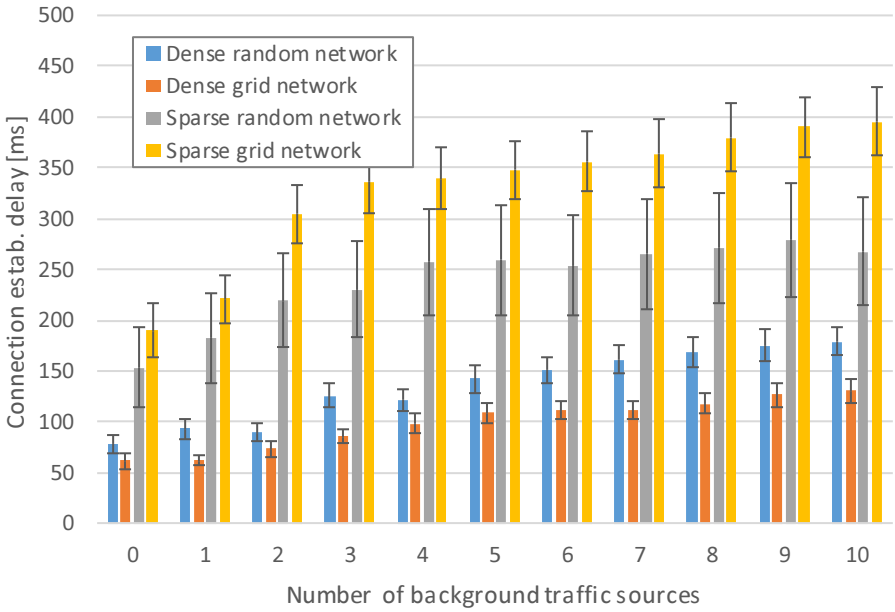

Fig. 88 Latency of IP to MAC address resolution procedure (ARP protocol) in MBSS environment

In Fig. 88 a mean latency of IP to MAC address resolution in different mesh structure types (as described in 3.8.5) has been presented. The results have been obtained by performing 100 simulation runs, each time generating a mesh structure of 50 STAs and performing an ARP address resolution procedure. Because of the, already presented, dependence of a broadcast delivery ration on the network load level, the experiment has been extended to include 0-10 UDP traffic sources located at randomly selected STAs, each generating a 1 Mbit/s traffic stream to a randomly selected destination STA. It is evident, that the mean latency of such a simple and routine task as ARP-based address resolution can be quite large in the MBSS environment, especially in case of sparse network structures (utilizing a longer ranged, lower quality links) and higher traffic loads. One of the main

causes of such a high mean latency are failed broadcast transmissions, which do not occur very frequently, but their impact on the latency of the process is very high.
It is somewhat disturbing, that an IEEE 802.11s mesh standard, designed with compatibility and ease of integration in mind, provides such an inefficient support for the IP protocol, which can be considered as one of the base solutions employed in integration of modern network systems.
A more detailed discussion of the results, as well as similar experiments for the Multicast DNS service will be presented in chapters 4.1 and 4.2, which describe a proposition of cross-layer integration solutions, designed to mitigate the above problem, thereby allowing an efficient establishment of multiple IP communication sessions with different mesh STAs.

3.9.6 Recovery from a mesh gate failure

One of the expected advantages of a mesh network is a redundancy of its communication capabilities. If one of stations or links on the transmission path fails, the HWMP protocol will initiate an path error handling procedure (see Section 3.7.3.3) to establish a new transmission path, taking into account the changed structure of the network. The procedure requires an unicast message to be delivered to the source station and then a new path discovery process to be successfully completed (which, in case of reactive HWMP procedure, requires one broadcast and one unicast message transmission).
To verify this ability and compare its results with results of a similar experiment described before for IEEE 802.11 PtMP environment, two separate scenarios have been analyzed:

- recovery from a failed STA on the current transmission path,
- recovery from a failed mesh gate.

The second scenario relates almost exactly to the AP failure scenario analyzed for PtMP environment.

For the mesh transmission to recover from its current transmission path failure, a number of tasks must be completed sequentially:

- detection of link failure – not specified in the standard, however most often performed by monitoring Beacon frames transmitted by other STAs, loss of a configured number of consecutive frames result in link failure indication. With the common value of 3 such frames and the default 100 ms interval between successive beacon frames, the process takes a maximum of 400 ms. However, if the link is currently used for data transmission, its failure can be detected by a consecutive loss of a specific number of data frames.
- invalidation of the existing path – the station which detected the link failure, sends a Path Error IE in an uncast management frame, to the traffic source. It is also possible for such station to attempt to find a continuation of the previous path by itself, but we will disregard this ability to provide the worst case estimate for the connectivity resumption. Due to a high priority of such message and the fact that it is inserted at the head of the sending queue, the latency of such process is mainly dependent on the mesh path length, propagation conditions and current traffic load.
- new path selection – performed according to the procedure described in Section 3.7.3.1, depends on the same factor as the previous step.

To estimate the mean latency of a mesh path recovery in our simulated system described in Sections 2.5.7.1 and 3.8.5, a 100 simulation runs have been conducted for each of 4 considered types of mesh topology. A low throughput (G.711 VoIP transmission, 64 kbit/s) intra-MBSS IP transmission between initiated and sustained two randomly selected mesh STAs. Additionally a number of 1 Mbit/s UDP traffic sources have been deployed at randomly selected mesh STAs, each configured to send its traffic stream to another, randomly selected mesh STA.

After 10 s a random intermediate STA on the path has been disabled. The results shown in Fig. 89 indicate the delay until the transmission have been resumed, but do not include the detection phase, due to lack of its standardization.

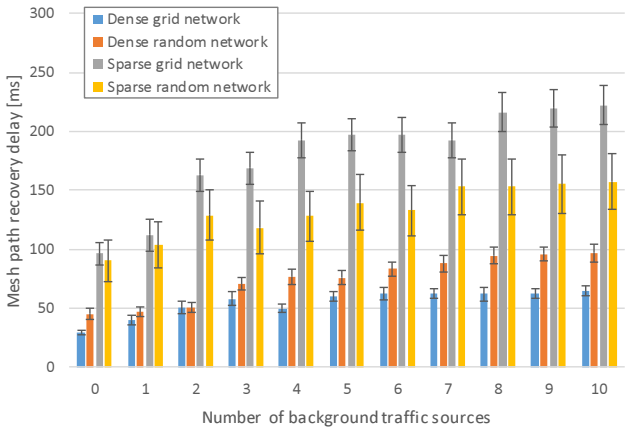

Fig. 89 A mean mesh path recovery time for IEEE 802.11s MBSS (failure detection time not included)

As the procedure requires an exchange of an unicast PERR, a broadcast PREQ and an unicast PREP, the procedure is susceptible to an already described unreliable broadcast communication problems (path discovery retry timeout is by default set to 1 s). This partial dependence on broadcast communication allows the procedure to be adversely influenced by sparse network structures (with their low quality links) and heavy traffic loads.

The recovery from an active mesh gate failure depends on the completion of the following tasks:

- RSTP detection of mesh gate failure,
- RSTP handshake resulting in activation of an alternative mesh gate (if present),
- path discovery initiated by a new mesh gate,
- update of STA's proxy information.

The main difference between a mesh path failure scenario described above, and a mesh gate failure scenario is the fact, that before a discovery of the new path can take place, a new mesh gate must be activated, as the failure of the previous one leaves the STA without a mesh destination to forward traffic to, instead of just making a currently used path invalid.
The activation of the new mesh gate is dependent on the RSTP protocol, which should detect the failure of the currently active mesh gate and allow another to come online. The amount of time required for this task can greatly differ depending on the specifics of the mesh failure. If the mesh gate fails in a manner allowing bridging devices of the external network to detect the fact due to a loss of a physical link to a mesh gate, the detection is possible in as low as 5 ms, although the value is highly implementation dependent and are often in range of 30-150 ms, but can reach much as 2 s [93] (despite the fact that IEEE 802.3 [94] specification set a maximum of 700 ms. However, if the mesh gate malfunction can only be detected due to a failure to receive its expected RSTP BPDU messages, the time required for detection is equal to 3 times RSTP Hello interval (by default 2 s) which results in a detection delay of 6 s.
When the failure is detected and there are alternative devices which can be activated to restore the connectivity, the specification of RSTP protocol informs, that the properly implemented and configured protocol allows such a restoration to be performed within 50 ms.
The next task, a mesh path establishment between a newly activated mesh gate and STAs within the MBSS, is conducted in a proactive manner. Following its activation, a new mesh gate performs a Proactive PREQ broadcast, answered by each STA with an unicast PREP message. The same simulation scenario as in case of a general mesh path failure described above, has been performed

for the process of creating a bidirectional, proactive path between a mesh STA and a host located in external network connected to the MBSS by a mesh gate.
The last step, updating of the STA's proxy information to indicate the new mesh gate as the mesh destination proxying for the external destination address, requires another unicast message (PXU).

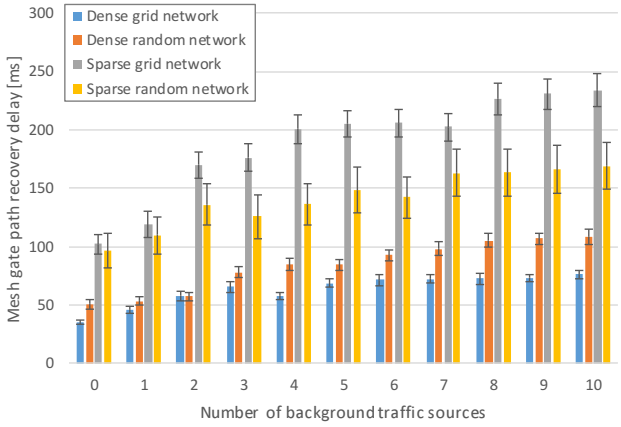

Fig. 90 A mean time of recovery from a mesh gate failure for IEEE 802.11s MBSS (failure detection time not included)

The results, show in Fig. 90, are easily predictable based on previously presented results concerning a general case of mesh path recovery (Fig. 89). It can be observed, that the inclusion of a more sizable PXU message in place of a small PERR increases the overall mean time of the process slightly, but the impact of this change is negligible. However, the remaining broadcast-unicast exchange is still susceptible to delays caused by a broadcast message loss in sparse network structures and/or under heavy network load.
In overall, the total time (including detection phase) required for recovery from a mesh gate failure can be expected vary from 65 ms to over 6 s, mainly due to unpredictable mesh gate failure detection time, depending on the operation of the RSTP protocol (external to IEEE 802.11s specification) and a structure and configuration of external network.
The above results indicate, that an MBSS-connected STA may be able to recover from a mesh gate failure much faster than a STA connected to a failing IEEE 802.11 AP (a roughly estimated minimum of 65 ms, compared to equally roughly estimated network discovery times of about 2 s or more, see Fig. 43) or in both cases the delays may be comparative (over 6 s in case of MBSS and about 2-8 s in PtMP system). It is clear, that in case of MBSS, the main factor which can prevent an efficient and fast recovery from the network interconnection point failure is a time required for a detection of such an event, necessary for before the activation of a new mesh gate can be allowed by the RSTP protocol.

3.10 Conclusions

Even the most cursory analysis of the IEEE 802.11s mesh standard indicates, that this solution should offer much more robustness in the use of its available resources then a classic PtMP IEEE 802.11 installation. With physical layer mechanisms the same in both cases and medium access sublayer mechanisms directly related to medium sharing being essentially the same (despite some extensions defined in case of the mesh standard, due to an almost complete lack of their implementation – see 3.5), the deciding factor must be the ability to manage the created network system.
With the classic PtMP IEEE 802.11 systems long since having management problems due to absence of standardized and popularly implemented means of controlling the activity of a network client, the mesh standard, with its mandatory self-organization and autoconfiguration mechanisms can be expected to have a significant advantage.
The above statement is made with a full knowledge of the existence of IEEE 802.11v [7] standard amendment enabling standardized wireless client control. However, due to the necessity of obtaining a popular support for this extension in client devices before it can be effectively used for tasks related to resource management, this solution cannot be considered practicable in most real-world usage scenarios. Apart from the IEEE 802.11v extension there are multiple proprietary solutions based on centralized network controllers, which, with use of non-standard AP behavior attempt to provide some degree of control over standard wireless clients [91,92]. However, their operation is not standardized and as such they cannot be considered a general solution.

In this situation the IEEE 802.11s mesh network, with its capability of performing multihop transmissions over a self-organizing topology of wireless stations and mesh links can be expected to provide a number of advantages as far as the robustness of resource management is concerned.
First and foremost, the IEEE 802.11s Mesh Basic Service Set network is created by allowing connecting client devices to become part of the traffic forwarding infrastructure. In theory, each connection client station extends the resources of the network, which should provide it with excellent scalability.
The analysis and simulation experiments performed above confirms this capability as far as the coverage of the network is concerned – each connected station can (and by default will) forward wireless frames in accordance with configuration information obtained due to activity of IEEE 802.11s mechanisms and protocols.

The first of advantages of such a capability can be observed in a STA to STA communication scenario presented in Section 3.9.1. In contrast to a standard IEEE 802.11 network configured in an infrastructure mode, a direct communication between neighboring STAs is not only possible, but a normal mode of data forwarding within a mesh structure. The situation is only a special case of the more general scenario of intra-MBSS communication between different stations and in all such cases a path selection protocol (by default HWMP) will select an appropriate mesh path between stations intending to communicate. The path will take into account a current state of MBSS network, including its currently available resources, providing that link metric currently active in the MBSS provides such capabilities (as the default Airtime Metric does, see 3.7.2). With no central data device required for data forwarding, the distributed ability to select data transmission paths based on various criteria results in high robustness in management of the network's remaining transmission resources. This characteristic, combined with an ability to perform various network maintenance tasks, such as a path selection, on demand (reactively), seems to indicate a considerable scalability level of the described mesh network.

Another advantage of the ability to use client devices as traffic forwarding network nodes can be seen in Fig. 86. With the network environment identical to the one considered in case of PtMP network and with both 10 mesh gate devices (considered to be an equivalent to access points) and

30 client stations deployed in random manner, it provides the connectivity ratio of 80-90%, which PtMP can only outperform in case of scenarios in which stations are placed within range of functioning APs (simulating a perfectly designed coverage) with no more than 3 failed access points. In case of a random station placement the best results in PtMP case is about 66% connectivity with all 10 AP functional. Moreover, any decrease of the number of active APs will results in a clearly observable reduction of connectivity ratio – with extreme case of 9/10 failed APs, it drops to about 15%. In case of the MBSS structure, failure of an active mesh gate will have only a slight chance of depriving the STA of external network connectivity – with the same case of 9/10 failed mesh gates, the connectivity ratio still exceeds 75%. Of course, in both cases, the specific result will be dependent on the specific network topology (in case of mesh network, this dependence is even more pronounced).
This scenario shows what seems to be a clearly superior case of resource management, both in terms of acquitting coverage resources from connecting clients and utilizing them to provide a blanket coverage of system's operation area, without the necessity of deploying additional devices to cover coverage holes or provide failure recovery capabilities.
However, if we look at Fig. 87, we can see that such a high connectivity ratio through the area of the system, does not translate to the quality of communication provided by the system. To provide an easy comparison with the PtMP systems, the scenario is limited to an inter-MBSS transmissions only and it is clear, that the system is not able to provide transmission resources adequate to support even low-throughput VoIP transmissions with any acceptable quality, leaving aside the complete inability to support 2 Mbit/s video streaming. However, despite the very low MOS scores of both services, we must observe, that their further degradation with the growing number of failed mesh gates is minimal.
The reason for such a poor result is clear when we refer to IEEE 802.11s interworking mechanisms description (3.8) and expected results of RSTP protocol operation (3.8.3) in particular – to provide compatibility with IEEE 802.1D-compliant networks at ISO-OSI layer 2, the RSTP protocol is utilized by mesh gates for the purpose of preventing forwarding loops. As a result only a single mesh gate can remain active between a given layer 2 network and the specific MBSS system. This information explains the low MOS scores visible in Fig. 87 – with only a single mesh gate active, all traffic must be forwarded through MBSS to such an STA, resulting in long transmission paths and concentration of traffic around the mesh gate. Especially in case of high-throughput transmissions, inter-path (increased by concentration of mesh transmission paths) and intra-path (increased by long mesh paths – see Fig. 79) interference causes transmission to quickly consume available transmission resources and leads to a local network saturation condition in vicinity of the gateway.

The situation is only made worse by the fact, that IEEE 802.11s is a single-channel mesh standard, which performs all transmissions using the same, shared frequency channel, making the transmission resources available to the MBSS network strictly limited. Such a standardization choice, initially caused by the desire to keep the solution simple and allow popular, single-radio devices to participate, can be expected to lose its most important drawbacks, with observable trend towards high-bandwidth, single channel transmission technologies, utilizing frequency channels of 160 MHz and employing sophisticated coexistence procedures (for example IEEE 802.11ac [5]).
With the IEEE 802.11g transmission technology, however, the transmission resources available to a given MBSS network are strictly limited, leading to the, already mentioned, degradation of transmission quality over long mesh paths. The intra-path interference, caused by the fact that an intermediate mesh STA needs to simultaneously receive and send data frames following such a path, leads to a situation when data frames of a given traffic stream contend for an access to the shared wireless medium access. As illustrated in Fig. 79 such effect can occur between transmissions of neighboring stations on the path or between transmission of a larger number of STAs, depending on their relative spatial placement and propagation conditions. Interference range of transmissions being larger than their communication range, it is highly probable that intra-path interference will be dependent on the length of the path. This dependency have been confirmed by simulation

scenarios presented in Section 3.9.2. The results clearly show, that transmission quality required for multimedia services can be sustained only for mesh paths of limited length.
The inability to use multiple independent frequency channels within an MBSS and significant interference range of wireless transmissions also result in inter-path interference, when wireless transmissions belonging to a different transmission paths contend for medium access or cause frame loss due to signal interference. In contrast to the intra-path interference (in a single-channel mesh) this effect can be minimized by changing the spatial placement of mesh paths, to keep their sending and intermediate stations out of interference range. As the IEEE 802.11s MBSS utilizes the Airtime Metric (see 3.7.2) which takes the quality of mesh links into account, the standard IEEE 802.11s path selection mechanisms perform this function without additional modifications. However, even in case of inter-path interference, the reduction of mesh path length will bring beneficial results, by reducing the number of its links affected by this effect and the area over which a given path causes it. Results illustrating the influence of inter-path interference have been presented in Section 3.9.3 and show that longer mesh paths are more susceptible to adverse effects of intra-path interference.

The described combination of the inefficiency of long transmission paths in a single-channel mesh network and the RSTP-induced reduction of the number of active mesh gates between a given MBSS and a specific external layer 2 network drastically reduce the practical utility of the IEEE 802.11s standard. With such limitations in place, the scalability of the network created with use of a technology which should be, due to the possible robustness of its resource management, an extremely scalable one, is almost non-existent.

With an exquisite care devoted to make the IEEE 802.11s specification compatible with popular LAN technologies and highly robust in its support for higher layer protocols, the efficiency problems concerning support for IP to MAC address resolution (necessary for IP operation in an ISO-OSI Layer 2 network) are both surprising and worrying. The preliminary results presented in 3.9.5 indicate that ARP protocol's dependence on group addressed transmissions, perfectly valid in case of highly reliable cable-based networks, is a significant hindrance in a much less reliable MBSS environment.

In overall, the technical preview presented in this chapter indicates that IEEE 802.11s mesh network should be able to provide robust self-organization, autoconfiguration, failure recovery and resource management, creating a highly scalable access network system. However, a number of standardization decisions, mainly regarding compatibility with both external network systems and higher ISO-OSI layers (black box approach), result in a drastic reduction of the utility of an IEEE 802.11s MBSS system, which has been confirmed by performed simulation experiments.
In the following chapters, a number of modifications of IEEE 802.11s specification have been proposed, addressing such specific issues, as:

- the inability to maintain more than a single active mesh gate between an MBSS and a specific ISO-OSI layer 2 network,
- the requirement, that STA to STA transmission within an MBSS cannot take advantage of external network connectivity,
- the inefficiency of support for a number of popular higher-layer protocols which utilize a group addressed communication.

As one of the main characteristics of the IEEE 802.11s specification is keeping a strict separation both between the MBSS and external mechanisms and between different IEEE 802.11s internal mechanisms within its ISO-OSI layer, the proposed modifications have taken a cross-layer approach, as presented in their specific descriptions in the following chapters.

4 Cross-layer address resolution extensions for IEEE 802.11s mesh networks

The ability of the IEEE 802.11s MBSS to provide a data link layer connectivity allows the network to support a vast majority of popular network layer protocols and as a result, practically all popular application layer services. This characteristic is one of main advantages of the discussed WMN standard. However, we should remember, that the protocol compatibility of the network system with a high layer protocol or service does not necessarily mean that it is well suited for their deployment. It is often the case, that a less universal solution is able to provide much better support within its compatibility limits than its all-purpose alternative.
As the vast majority of network traffic today is exchanged using an IP protocol [95], including modern multimedia services, it seems an important matter to verify if the IEEE 802.11s support for this protocol and its associated network services is ensured in an efficient manner.
Having analyzed the forwarding (not to be confused with wireless transmission) process itself, and finding it at comparable level of efficiency with other popular LAN networks (such as an Ethernet), with additional configurable support for large frame sizes and different modes of traffic aggregation, EDCA prioritized access and optional congestion control mechanisms, it has been decided to look upwards on the protocol stack, to include IP support services in the analysis.
As the IP connectivity is dependent on the ability to translate IP addresses into ISO-OSI layer 2 addresses appropriate for an underlying technology, it has been decided to verify if the process can be efficiently performed in case of an MBSS network. The protocol responsible for the task is the Address Resolution Protocol (ARP) in case of IPv4 and the Neighbor Discovery (ND) protocol in case of IPv6. Both of these protocols function in a similar manner, and while only the case of ARP is described below in detail, the corresponding analysis for IPv6 ND can be found in [12].
Having discovered that the process of IP to IEEE 802.11 MAC address resolution is not performed in an efficient manner in the described wireless mesh environment (as already described in 3.9.5), which leads to both unnecessary network resource consumption and both high and unpredictable latency in initial IP communication within the MBSS, a cross-layer integration procedure for IP to MAC address resolution has been proposed to correct the problem.
Following the same line of reasoning, the application layer address to IP address resolution procedures have been analyzed in similar manner. Having reviewed a number of most popular application layer address resolution mechanisms, a Multicast Domain Name Service (mDNS) protocol has been selected for detailed analysis, as it is both a very widely supported solution and one designed to function in self-configuring access or workgroup networks, able to provide such functionalities as application layer service discovery and zero-configuration operation. At the same time it is based on group based communication, which is currently poorly supported within the MBSS and generally not well suited for WMN environment.
As predicted, problems similar to these encountered in case of the ARP address resolution have been discovered in case of mDNS name resolution and service discovery also. To provide an adequately efficient support for the mDNS application layer name resolution and dependent services, the cross-layer integration solution proposed for ARP support has been extended to span data link (layer 2), network (layer 3) and application layer (layer 7).
As a result a procedure allowing to discover a mesh path to a DNS-named host or service along with relevant Name->IP->MAC address mappings with a single exchange of messages has been prepared.

At the same time it is surprising to discover, that the prized ability of IEEE 802.11s to accommodate a wide range of network layer protocols results in an inefficient support for the only few which are likely to be encountered in production-grade network systems.

4.1 IP to MAC address resolution extension for IEEE 802.11 MBSS environment

In case of IPv4 protocol packet both source and destination network nodes are described by 32-bit IPv4 addresses identifying them at a third (network) ISO-OSI layer. However, if the packet is to be successfully delivered to a destination node, it must usually traverse at least one network link utilizing ISO-OSI layer 2 protocols and addresses – for example an Ethernet link or, in our case, an IEEE 802.11s mesh MBSS. In this situation it is evident that a mechanism which will allow a network node to obtain a mapping between a given layer 3 address and its corresponding layer 2 address is a necessity.
There two basic types of such mechanisms:

- direct mapping – used in situation where a lower layer address can be directly obtained by analyzing a higher layer address. Unfortunately it has a number of limitations, one of the most prominent being requirement for a lower layer address to be shorter than higher layer address. With 32-bit IPv4 address and 48-bit IEEE 802 Media Access Control (MAC) addresses the method is clearly not usable in case of IPv4 networks in their popular usage scenarios.
- dynamic resolution – allows a node to obtain a lower layer address corresponding to a higher layer address, most commonly by querying one or more other network devices.

In case of IPv4 networks a dynamic resolution is used and performed by IP Address Resolution Protocol (ARP) defined in RFC826 [96].

4.1.1 IP Address Resolution Protocol (ARP) overview

The protocol utilizes broadcast querying of devices in local layer 2 network segment and caching mechanism to avoid performing address resolution each time an IP packet is to be sent.
ARP messages are sent in format presented in Fig. 91, which provides the ability to support both different higher layer protocols and lower layer transmission technologies.

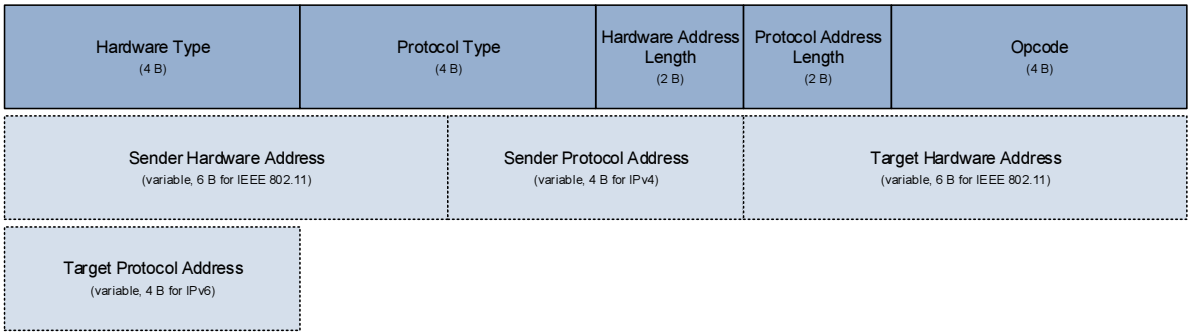

Fig. 91 Address Resolution Protocol message format

The fields used in the ARP message have the following functions:

- Hardware Type (2 bytes) – indicates the type of the lower layer (transmission technology) address,
- Protocol Type (2 bytes) – specifies the type of the higher layer (network protocol) address,
- Hardware Address Length (1 byte) – as different types (and lengths) of hardware address are supported, there is a need to specify the length of subsequent Hardware Address fields,
- Protocol Address Length (1 byte) – similarly to hardware addresses, different protocol address types are also supported, so the length of subsequent Protocol Address fields also needs to be specified,
- Opcode (1 byte) – indicates the type of ARP message: ARP Request (1), ARP Reply (2)

- Sender Hardware Address (variable length) – lower layer address of the sender of the message,
- Sender Protocol Address (variable length) – higher layer address of the sender of the message,
- Target Hardware Address (variable length) – lower layer address of the intended receiver of the message,
- Target Protocol Address (variable length) – higher layer address of the intended receiver of the message.

It can be seen from the above list of fields, that the ARP protocol allows for the higher layer protocol and lower layer transmission technology to be specified, making it possible to accommodate different combination of such protocols and technologies, complete with support for varied address lengths. Such ability theoretically allows the ARP protocol to be used in deployment scenarios which do not include the use IPv4 protocol. However, it is almost unknown to encounter such deployment, making the ARP a de facto IPv4-specific solution.

Generic, simplified procedure for obtaining layer 2 (MAC) address corresponding to a given layer 3 (IP) address using ARP protocol is as follows:

1. Source device checks if a given IP to MAC address mapping is present in ARP protocol cache. If so, device uses the information to create layer 2 frame appropriate for sending IP datagrams to a given IP address and the resolution process ends.
2. Source device generates an ARP Request Message containing its MAC and IP address in Sender Hardware Address and Protocol fields and IP address to be resolved in Target Protocol Address field.
3. Source device sends the above ARP Request Message as layer 2 broadcast frame.
4. All local devices receive ARP Request and each device checks if it owns IP address indicated in Target Protocol Address field.
5. If it does not, device drops the packet and takes no further action.
6. Device that owns the IP address indicated in Target Protocol Address field generates ARP Reply Message by copying values of Sender Hardware Address and Sender Protocol Address fields to Target Hardware Address and Target Protocol Fields and putting its own MAC and IP addresses in Sender Hardware Address and Sender Protocol Address fields respectively. Device also updates its ARP cache with information concerning ARP Request sender's IP to MAC address mapping.
7. Destination device sends ARP Reply prepared in step 5 as an unicast frame to MAC address which has been indicated in Sender Hardware Address of ARP Request Message.
8. Source device receives ARP Reply Message and updates its ARP cache with IP to MAC address mapping of destination device, based on values of Source Hardware Address and Source Protocol Address fields of ARP Reply Message.

If source device does not receive ARP Response Message in preconfigured time interval it will retry the procedure. If the procedure is repeated without success a preconfigured number of time it will fail and appropriate information will be entered into ARP cache. In such situation sending IP packet to a given IP address will not be possible and it will be dropped by the sender.

To ensure that information in ARP cache is current each device will periodically check its contents and if a given entry is unused for a specific time it will change its state to STALE. If such entry is to be used again, it is to be verified – the procedure is the same as in case of discovering a new mapping, but due to the fact that source device already possesses probable MAC address of the destination, ARP Request Message is first send as unicast frame (instead of broadcast). Only if there is no response to a number of unicast query attempts, device will revert to sending broadcast queries.

4.1.2 ARP Resolution in IEEE 802.11s MBSS environment

ARP protocol has been designed to support both different higher and lower layer protocols, so it will function in MBSS network without need for any modifications. Moreover, IEEE 802.11s standard aims to retain a high level of compatibility with widely popular Ethernet networks, so ARP protocol will operate in environment virtually identical to this most popular scenario.
However, while MBSS offers higher layers (including ARP protocol which is placed in 2.5 ISO-OSI layer) a set of functionalities and access methods identical with Ethernet network, mechanisms and protocols which are used to provide them are, of necessity, significantly different.

ARP resolution procedure in MBSS environment will proceed as follows:

1. Source station checks ARP cache for valid IP to MAC address mapping. If found the resolution procedure finishes successfully.
2. Source station creates ARP Request Message.
3. ARP Request Message is sent as a broadcast frame, and flooded through the MBSS with each station retransmitting the frame once as per rules described in 3.7.1.2.
4. Receiving stations check if they received the broadcast frame already (as the broadcast procedure will most likely cause stations to receive multiple copies of the frame, retransmitted by different neighboring STAs). If not, the station checks if the specified Target Protocol Address field contains their IP address:
    a. If it is so, the station generates ARP Reply message and sends it to source station as an unicast frame. To do so, it requires a mesh transmission path to be available, so it checks its forwarding table – if such path is:
        i. PRESENT – ARP Replay Message is sent using this path,
        ii. ABSENT – path discovery is initiated according to HWMP procedures. When path is found, it is used to send ARP Replay Message.
    b. If the STA does not own the address specified in Target Protocol Address field, but is a mesh gate, it will perform an ARP address resolution using its external interface. If it is successful the mesh gate will generate ARP Reply message like in case 4a of this procedure.
5. Source station receives ARP Replay Message and updates its ARP cache with IP to MAC address mapping.

From the above description we can see, that ARP resolution requires a broadcast transmission to be performed (steps 3 and 4-a). Such transmission results in flooding entire MBSS with the message, as it is retransmitted by every station, as IEEE 802.11s standard, for the sake of simplicity and ease of implementation, does not include any broadcast optimization mechanisms such as, for example these included in OLSR protocol [97]. Broadcast transmission according to these rules will certainly result in unnecessary resource consumption, as:

- flooding will continue even after intended destination station receives and processes ARP Request Message,
- it is highly probable, that a given station will unnecessarily receive multiple copies of the broadcast message from different transmitters – a problem more prominent in dense mesh structures.

We should also keep in mind, that broadcast messages in IEEE 802.11s MBSS are not acknowledged, so it is possible, that some of the stations will not receive the message as a broadcast frame used to transmit it will be lost with a simple collision. Of course, the already mentioned fact, that it is highly probable that a station will receive multiple copies of the broadcast message from different transmitters, tends to mitigate the problem so it will be more prominent in sparse networks. High network load will also raise the probability of not receiving a broadcast message significantly.

We should also look with more detail at step 4-a-ii which requires that the station performs HWMP path discovery. The specifics of this process will differ according to configuration of MBSS – three different cases should be analyzed:

A. HWMP **does not use proactive** path discovery,
B. HWMP **uses proactive** path discovery and source station **is not a root** station,
C. HWMP **uses proactive** path discovery and source station **is a root** station.

In scenario A the destination station must perform reactive path discovery to send an unicast ARP Reply Message to the source station. In adherence to RM-AODV procedures it requires flooding the MBSS with a broadcast PREQ message and waiting for an unicast PREP response from the source station. This procedure will result in source and destination stations of ARP discovery obtaining a bidirectional, unicast transmission path between them. However, we must observe, that the described path discovery procedure, being based on broadcast transmission through MBSS, also encounters adverse effects already described above in connection with ARP Request broadcast transmission.

In scenario B the destination station can choose to send the unicast ARP Reply Message to root station for indirect delivery to ARP resolution process source station. It may also utilize reactive path discovery described in scenario A or use both methods simultaneously: send ARP Reply Message using proactive path and initiate reactive path discovery in expectation, that a bidirectional data transmission will follow ARP resolution procedure.
If destination station chooses to use a proactive patch to root station, ARP Reply Message can be send immediately. It will, however, be delivered using a path that is most probably longer than is necessary.
Also, the destination station should check if Proactive PREP mechanism is used by root station and if Proactive PREP field on its Proactive PREQ announcements is set. If RANN mechanism is used or Proactive PREP field is not set then there is no guarantee that root station has a valid path to the station which initiated the ARP resolution process. Lack of such path will require the root station to initiate a reactive path discovery to deliver the message.

In scenario C the destination station already has a proactively maintained transmission path to ARP resolution process source station and can send the unicast ARP Replay Message immediately.

Intermediate station PREP response mechanism
We should also remember about possible impact of rarely implemented optional functionality of HWMP reactive path discovery, which allows a PREQ response to be generated not only by the destination station of path discovery process, but also by any intermediate station, which already has a path to a given destination. This functionality need to be specifically allowed by source station od path discovery process (Target Only field of PREQ Message set to 0) and intermediate stations are not required to provide path data they possess, but only allowed to do so.
Moreover, intermediate station which responds to PREQ in this manner, still broadcasts the PREQ Message to its neighbors, this time with Target Only field set to 1, to prevent other intermediate stations from generating additional responses based on their own path knowledge.
This optional mechanisms can significantly speed up reactive path discovery process, but practice shows that it is rarely implemented and can lead to inefficient path selection if MBSS structure or link metrics are changing frequently. While the first of above problems is of lesser significance in our research concerning static mesh networks, high-throughput multimedia flows can impact the airtime metric significantly. Due to this fact it is not recommended intermediate station PREP response option in MBSS expected to carry traffic streams of moderate or high bandwidth. In this situation we will disregard this optional functionality in further analysis assuming that source station of path discovery will always send PREQ Messages with Target Only field set to 1.

From the above theoretical description it is clear, that ARP resolution in IEEE 802.11s MBSS environment requires two separate procedures to be performed between source and destination stations (ARP Request-Reply and path discovery for purpose of sending the unicast ARP Reply). Moreover, at least one of these procedures involves broadcast transmission, while most often both of them have this requirement.

4.1.3 Cross-layer address resolution procedure

As the ARP address resolution is a mechanism of crucial importance for IP networks and can be expected to have a direct impact on initial communication establishment delay between two IP hosts, a cross-layer modification of the above procedure have been developed. Its aim is to integrate procedures required in IEEE 802.11s MBSS for ARP address resolution in ISO-OSI layers 2 (HWMP path discovery) and 2.5 (ARP Protocol) as shown in Fig. 92, thereby reducing number of necessary message exchanges (especially exchanges involving broadcast transmission).

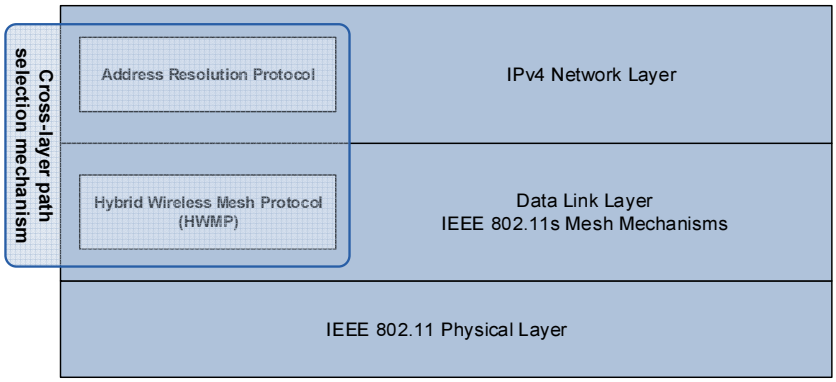

Fig. 92 Cross-layer address resolution procedure placement in ISO-OSI model

The proposed modification combines ARP Request message and HWMP PREQ message into a single entity (HWMP ARPREQ message) used to simultaneously request an IP to MAC address mapping to be created and establish a reverse data transmission path.
Similarly, ARP Reply message and HWMP PREP message have also been combined into one (HWMP ARPREP message), simultaneously providing IP to MAC address mapping information and establishing a forward transmission path from the source to the destination station.

4.1.3.1 Data formats

To retain compatibility with unmodified IEEE 802.11s MBSS, the messages mentioned above are constructed on a basis of standard HWMP messages.
HWMP ARPREQ message is based on HWMP PREQ message, which is normally transmitted in MBSS as an Action Management Frame of HWMP Path Selection type, containing Path Request Information Element (PREQ IE) shown in Fig. 68. The HWMP APRREQ message additionally includes an ARP Request Information Element (ARPREQ IE) following the PREQ IE. The new IE contains information fields intended to extend the information present in the standard PREQ IE to include all data provided by the ARP Request message.

Taking into account the overall mandatory rules regarding IEEE 802.11 Information Elements and the need to minimize the IE length, the proposed format for ARPREQ IE is shown in Fig. 93.

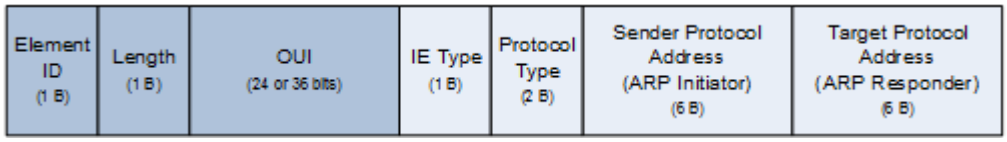

Fig. 93 ARPREQ Informaton Element

The initial Element ID and Length fields follow the general IEEE 802.11 structuring rules for Information Elements – they indicate the type of the IE as Vendor Specific IE (value 221 in 1 byte Element ID field) and provide its length in bytes (1 byte Length field).
As the IE is defined as a Vendor Specific IE, an Organization Identifier field (OUI) following the Length field contains an IEEE-assigned identifier of the organization defining the new IE. The OUI field length can be 24 or 36 bits depending on the type of identifier assigned by IEEE, and the specific type of OUI (and its expected length) is recognizable based on values of its commencing bytes.
As the Element ID / OUI fields specify only an organization defining the IE structure, it is necessary to include an additional field to indicate the particular type of the IE – the IE Type field of 1 byte length. As specified in Table 6, the ARPREQ IE is identified by a value of 0x00. The IE Type field is the last of obligatory IE fields required by IEEE 802.11 standard and the subsequent fields can be dedicated to carrying the ARP-related information.

We must observe, that by taking into account the specific environment for which the proposed cross-layer solution is intended, it is possible to eliminate the need for a significant number of the ARP Request message fields, thereby simplifying and reducing the size of the ARPREQ IE.
The Opcode ARP message field, used to differentiate between ARP Request and Reply messages is not needed in our case, as identification of ARP message type is performed based on the IE Type described above. Similarly, as the proposed solution is dedicated to the IEEE 802.11s environment, its MAC address format is compatible with Ethernet specification, so the value of Hardware Type ARP message field can be assumed to indicate Ethernet (value 0x0001) and the Hardware Address Length field can be assumed to be equal to 0x06. In this situation these fields also do not need to be included in the HWMP ARPREQ message, as their values can be predicted by the receiver. Additionally, with the PREQ IE preceding the ARPREQ IE in the HWMP ARPREQ message, the Originator Mesh STA Address field of the former provides the information normally contained in ARP message's Sender Hardware Address field.
Taking the above into account and further observing that Target Hardware Address field of ARP Request message can be assumed to be meaningless (as the address is unknown to the ARP Request originator), the only fields that need to be included into ARPREQ IE are:

- Protocol Type – as we are interested in support for IPv4 protocol, this field could also be omitted, but its presence allows the same solution to be used in case of IPv6 ND protocol's neighbor solicitation procedure. In case of IPv4 ARP address resolution this field should be set to a value of 0x0800 as per specification [98]. The value of this field is also used to determine the length of Protocol Address fields described below,
- Sender Protocol Address – must be set to an IPv4 address of the originator of the message, to allow the receiving STA to create a mapping between originating STA's IPv4 address and its MAC address obtained from the accompanying PREQ IE,
- Target Protocol Address – must be set to a destination IPv4 address and will be used by receiving STA to determine if it is a target STA of the address resolution procedure and should generate the ARP Reply message.

As the HWMP ARPREQ message described above is based on a standard HWMP PREQ message, the HWMP ARPREP message is created by extending the standard HWMP PREP message with newly defined ARP Reply Information Element (ARPREP IE) resulting in a PREP/ARPREP IE pair. This new message also employs an Action Management Frame of HWMP Path Selection type for its transport.

Element ID (1 B)	Length (1 B)	OUI (24 or 36 bits)	IE Type (1 B)	Protocol Type (2 B)	Sender Protocol Address (ARP Responder) (6 B)	Target Protocol Address (ARP Initiator) (6 B)

Fig. 94 ARPREP Information Element

The structure of ARPREP IE also follows the standard IEEE 802.11s rules concerning the format of Information Element entities, as described above. To designate the IE as ARPREP IE the IE Type field contains the value of 0x01 as per Table 6.
Because the ARPREP IE is being sent in pair with preceding PREP IE, the values of Hardware Address fields of the classic ARP message are provided by its Target Mesh STA Address and Originator Mesh STA Address fields. With Opcode indicated by IE Type, hardware type being known and hardware address length not used due to lack of relevant fields in APRREP IE, the only fields required to be passed using ARPREP IE are the same as in APRREQ described above:

- Protocol Type – indicating the IPv4 protocol, but possibly allowing support for the IPv6 or even other network layer protocols,
- Sender Protocol Address – an IPv4 address of the sender of HWMP ARPREP message (responder in ARP address resolution process),
- Target Protocol Address – an IPv4 address of the destination of HWMP ARPREP message (initiator of the ARP address resolution process).

It should be noted, that while the chosen format of ARPREQ IE does not contain all fields of ARP Request Message, missing field values are obtained from accompanying PREQ IE or PREP IE, so the resulting solution retains a potential compatibility with higher layer protocols other than IPv4 in a manner similar to a standard ARP Protocol. The only limitation is lack of support for different Hardware Address types, which has been decided to be unnecessary as we are only interested in supporting a single lower layer protocol of fixed address length.

4.1.3.2 *Address resolution procedure*

As the proposed solution integrates ARP Protocol with HWMP Protocol, we must define its procedures for both reactive path and proactive HWMP mechanisms.

ARP address resolution for reactive path discovery

1. Source station checks ARP cache for valid IP to MAC address mapping. If found, a standard path discovery procedure is performed and process finishes.
2. Source station creates ARPREQ Message following format described in 4.1.3.1.
3. ARPREQ Request Message is sent as a broadcast HWMP Path Selection frame.
4. Unmodified receiving stations interpret ARPREQ Message as PREQ Message ignoring unknown ARPREQ IE. Such station processes PREQ Message according to standard HWMP procedures, creating reverse path to source station. However, due to destination MAC address set to 00-00-5E-00-53-00 (reserved address which is not to be used in real-world network systems [99]), none of unmodified stations will generate PREP Message.
5. Modified stations process both Path Request IE and ARP Request IE.
    a. Path Request IE is processed following the same rules as in unmodified station, but the message is not transmitted until ARP Request IE is processed.
    b. ARP Request IE processed following the same rules as in case of standard ARP Request Message – station checks if its IP address matches Target Protocol Address of ARP Request:

i. NO – ARPREQ Message is released for further transmission following HWMP rules regarding PREQ Messages. Additionally, IP to MAC mapping for source station can be placed in local ARP cache.
ii. YES – ARPREQ Message is dropped and ARPREP Message is constructed. Its ARPREP IE is constructed according to ARP Protocol procedures, while its PREP IE is constructed following HWMP procedures appropriate for destination station of requested path. The message is subsequently sent to source station using reverse path created by ARPREQ Message.

6. Source station receives ARPREP Message and updates its ARP cache with IP to MAC address mapping based on ARPREP IE. Reception of the message and its PREP IE also finalizes HWMP-based path resolution procedure – a bidirectional path between source and destination stations has been established.

ARP address resolution for proactive path discovery

If proactive HWMP path discovery mechanisms are used, reactive HWMP mechanisms are also active, so in such case the procedure described above remains in effect. Additionally, two more HWMP mechanisms need to be addressed, as they can potentially provide an optional, extended functionality:

- HWMP Proactive PREQ,
- HWMP Root Announcement (RANN).

If HWMP Proactive PREQ mechanism is used, apart from modifications to the reactive path discovery procedure described above, root station can extend proactive PREQ messages which it periodically broadcasts with additional ARPREP IE. That way, it will provide stations in MBSS not only with proactively maintained paths towards root, but also with an IP to MAC mapping. In contrast to reactive path discovery scenario, this mapping does not need to provide IP / MAC addresses of the root node, but can be chosen in an arbitrary manner to distribute address mapping for a chosen IP address. Also, multiple mappings can be published by including multiple ARPREP IE elements.

If RANN mechanism is in use, it remains not modified, but we should remember that in such case there is a possibility that the reactive path discovery procedure will be performed differently – additional information obtained from RANN announcements will allow the source station to use an unicast (instead of broadcast) communication in step 3, if the destination station is a root station.
Even casual analysis indicates, that it would be possible to extend RANN mechanisms to include additional information, for example:

- information about IP to MAC mapping of the sending root station,
- indication if root station is modified,

but doing so would increase the size of messages generated by a mechanism designed to be a lightweight as possible and conflicts with intended characteristics of RANN mechanism.

4.1.3.3 Compatibility considerations

For the described procedures to be effective, both source and destination station must be modified according to described rules: source station – to initiate the modified address resolution procedures and destination station – to properly respond to newly defined messages. All other stations in MBSS however, need not be modified, as the proposed solution is transparent to them. Moreover, modified stations will continue to support standard IEEE 802.11s path discovery and ARP address resolution procedures, which will allow them to seamlessly interact with unmodified stations in these respects.

The only incompatibility induced by the proposed modification is lack of ability of unmodified station to respond to a reactive ARPREQ Message, which will cause the combined ARP/PREQ procedure to fail if the proposed modification is used and destination station is not modified.
Due to this fact, it is advised to deploy the modification to all stations in MBSS, which will provide all planed advantages. As an alternative, the described modification can be deployed to a selected subset of MBSS stations, in which case however it will be necessary for modified stations to initiate both combined and standard ARP resolution / PREQ path discovery (in this order). Additionally, destination station should refrain from sending a response to the standard ARP Request Message, if receives ARPREQ Message from the same source.
Such approach will result induce an additional, single broadcast transmission as both ARPREQ and standard ARP Request messages will be sent by source station, initiating both combined and subsequently standard ARP resolution procedure. As source station should receive ARPREQ Message first it will initiate only combined procedure, disregarding standard ARP Request message received later.
If, due to network conditions ARPREQ Message is lost or received out of order with standard ARP Request Message, the standard procedure will be terminated at its reception, usually not later, than during path discovery phase. This will result in another broadcast transmission (standard PREQ) increasing generated management traffic over MBSS lacking modified stations, but not will not delay the conclusion of modified procedure.
Modifications to Proactive PREQ mechanism of HWMP protocol does not induce any incompatibilities, as unmodified stations will process PREQ IE of proactively broadcasted ARPREQ Message, ignoring newly defined ARPREQ IE.

The above analysis of the compatibility of the proposed solution remains valid if the IEEE 802.11s standard amendment and subsequent revisions of the IEEE 802.11 standard of which IEEE 802.11s specification became a part will retain the ability to transparently carry unknown IEs within HWMP Path Selection frames. In case the ability will not be retained, it should be noted, that for the proposed solution to work, either all STAs must be modified to fully support it, or at least all STAs must have the ability to transparently carry unknown IEs as described above. The conducted research indicates that the presence of such an ability is a very valuable characteristic for the standard, allowing seamless integration of custom mechanisms at selected STAs without the loss of compatibility. This clarification has been included due to ambiguities regarding this matter observable in various implementation of HWMP mechanisms in both simulators (for example OMNeT++, NS-2, NS-3) and real-world devices (for example: Linux kernel, Mikrotik RouterOS).

4.1.3.4 Expected advantages

In MBSS containing only modified stations, the proposed modification should result in reduced management traffic, requiring only a single broadcast ARPREQ-unicast ARPREP exchange of messages (in place of a two, each requiring a broadcast-unicast transmission) for initial establishing of IP communication between two MBSS stations. The process should also take considerably less time, reducing the delay induced by the above process.
Increased reliability of the combined ARP resolution / path discovery process is also expected, due to reduction of number of necessary broadcast messages, which are propagated through MBSS in unreliable fashion.
The described advantages are expected to be more pronounced in sparse networks, as in dense one, station is likely to receive multiple copies of a broadcast message retransmitted from multiple neighboring stations. Also, the advantage provided by described modifications should be more significant in case of networks under considerable traffic load, as such conditions increase both transmission delay and probability of packet loss.

4.1.4 Experiments

To verify the expected advantages of the proposed solution, a series of experiments have been performed in the already described mesh structures (see 3.8.5). To allow the results presented here to be interpreted using information obtained from previously described experiments, the simulation scenarios have been conducted as before – in a network of a 30 stations equipped with IEEE 802.11g interfaces. The propagation conditions are also the same as in case of previous experiments, which result in creation of a relatively challenging communication environment for a mesh network, however one providing a good approximation of today's metropolitan area conditions in ISM band.
In such an environment, after a 10 s warmup period allowing mesh mechanisms to configure a functional MBSS system, an IP communication attempt have been performed by randomly choosing a pair of mesh STAs and attempting to send a single IP packet between them to assess the delay of IP communication establishment process in IEEE 802.11s MBSS environment.
As it has been expected, that a level of background traffic will impact the results, the above scenarios have been repeated for different level of such traffic, generated (as in case in previous experiments) by placing a number of 1 Mbit/s UDP traffic sources within the MBSS, configured to send their traffic streams to another, randomly selected mesh STA.
All other configurable parameters of protocols being employed (such as IP and ARP) are assumed to have default values specified in standardization documents or based on common practice found in popular operating systems – the most important parameters for the scenarios being ARP retry interval set to 1 s according to IETF standardization documents [96].
As the goal of the experiment is to verify the efficiency of the proposed cross-layer solution, the scenarios described above have been performed for both a standard, sequential procedure (ARP address resolution, followed by a HWMP reactive path discovery), and for the proposed, cross-layer procedure.
Each of such scenarios has been repeated 100 times for each of mesh topologies already employed in previous, mesh-related experiments and described in 3.8.5. The presented charts contain mean values and show 95% confidence intervals.

The results show in subsequent figures, illustrate a mean time necessary to establish an IP communication between two mesh stations, based on the knowledge of the destination STA's IP address and a mean number of wireless frame transmissions stations in the MBSS network have performed in order to obtain this goal.

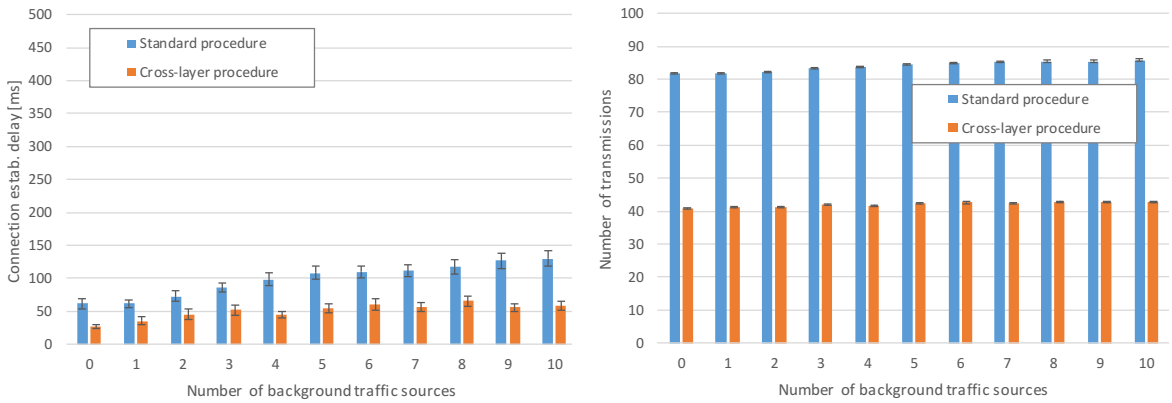

Fig. 95 IP connection establishment delay and a number of required wireless transmissions compared for standard and cross-layer procedures in a dense grid mesh structure

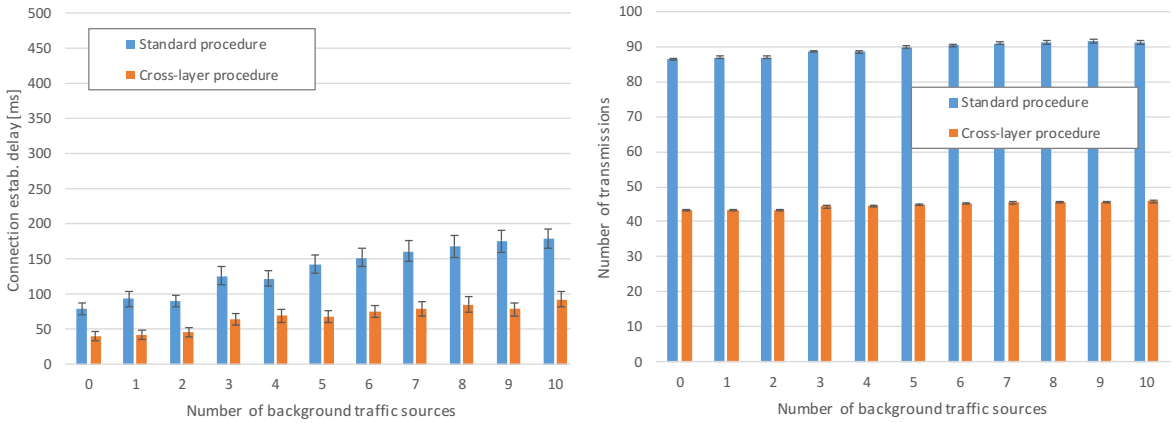

Fig. 96 IP connection establishment delay and a number of required wireless transmissions compared for standard and cross-layer procedures in a dense random mesh structure

The results for a mesh structures generated using a dense rules (both grid and random) show a moderate values of delay for a standard procedure (60-80 ms), which increase with the level of traffic load up to 140 ms in case of the grid structure and 190 ms in case of the random one. The random network displays a consistently higher delay values than the grid-based one.
Such situation is to be expected, as both of these structures relay on a relatively short-range links, able to sustain a low-loss transmissions, thereby minimizing the time required to complete the procedure. In case of a random network, there is a greater possibility of the network being required to use a lower quality links, resulting in higher latency.
The employment of the proposed cross-layer address resolution procedure results in all expected advantages, as both the number of required transmissions and the procedure's latency has been reduced by about 50%.

In the presence of such an adverse effect, the proposed cross-layer procedure provides significant advantages, due to elimination of 1 broadcast and 1 unicast frames. As a result, the latency is 50-55% smaller (25-75 ms), with significantly reduced confidence intervals, indicating the increased predictability of the process.

The chart displaying the mean number of wireless transmissions confirms the expected results of deployment of the proposed cross-layer procedure, with their number being reduced to less than half that of the standard procedure, and showing only limited growth with increasing network traffic load. With each full broadcast flooding in an MBSS structure of 30 STAs requiring 30 transmissions and an unicast message requiring the number of transmissions equal to at least twice the number of hops on the transmission path (transmission of the frame and an acknowledgement, increased in case of retransmissions), the decrease of the number of required messages is also about 50%. A slight increase of a mean number of messages is caused by both an increased number of retransmissions of unicast messages and a much less frequent but resulting in significantly higher number of additional transmissions, failure to deliver a broadcast frame.

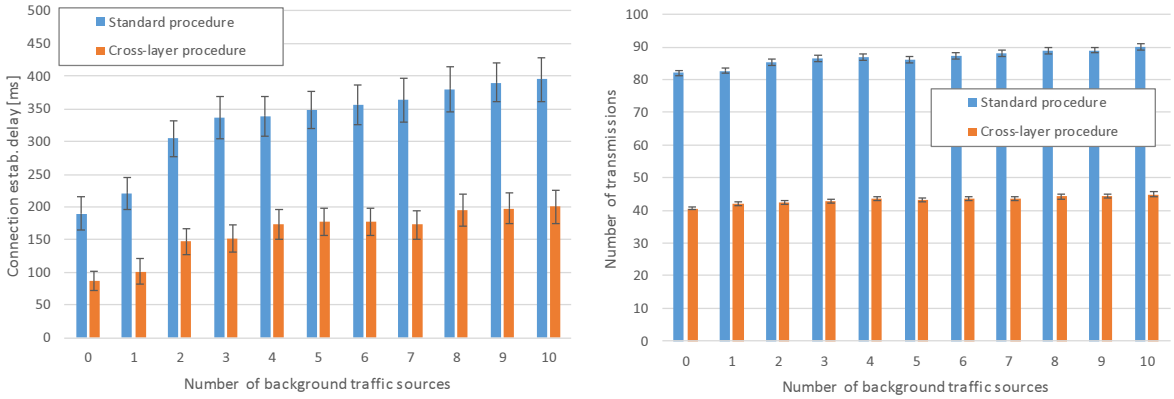

Fig. 97 IP connection establishment delay and a number of required wireless transmissions compared for standard and cross-layer procedures in a sparse grid mesh structure

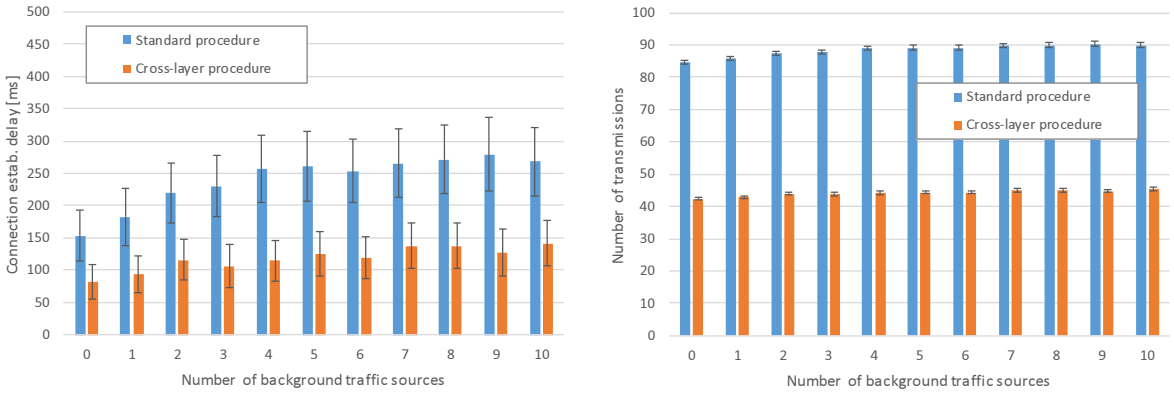

Fig. 98 IP connection establishment delay and a number of required wireless transmissions compared for standard and cross-layer procedures in a sparse random mesh structure

In case of sparse mesh structures, we observe a significantly higher delay values, due to their dependency on relatively longer ranged but lower quality links, which require a significant level of retransmissions of unicast messages and cause a much higher probability of a loss of a broadcast frame (see 2.5.7.3), which are transmitted in an unreliable (without acknowledgements) manner. This last characteristic, combined with a degree of a node lower than in case of dense structures, results in much higher probability that a loss of a broadcast frame will prevent a delivery of a broadcast message to its intended recipient.

The risk of the failure to deliver the broadcast frame to its recipients is normally mitigated by the redundant nature of the mesh broadcast flooding process, due to which each station should receive a copy of the broadcast frame from all (in general) of its neighbors. In case of a dense grid mesh structure, which can be expected to provide the highest level of such protection (a relatively high node degree and high-quality links), the failure to deliver such a message is an infrequent problem, however in case of sparse networks, the risk is becoming considerable.

Moreover, the loss of any message required to complete the address resolution procedure will require the STA to retry it. However, both ARP and HWMP reactive path discovery define the retry timeout to be set to 1 second – in case of ARP without provision allowing the timeout to be set to a lower value and still retaining compatibility with the protocol specification. Such timeout value will increase the delay of address resolution procedure enormously in case of a message loss, which is acceptable in wired networks due to tier low error rate, but in multihop wireless system with their packet loss values being a few orders of magnitude higher, it is a serious problem. If we refer to the results of previous experiments concerning broadcast transmission reliability (see 2.5.7.3), it

becomes evident that we can expect the standard procedure (with its 2 broadcast transmissions) to exhibit a considerable mean latency, especially in high network load conditions.
The effect is confirmed by results shown in Fig. 97 and Fig. 98 which display latency between 150-180 ms even in unloaded network, with its values reaching 280 ms in case of a sparse random network and almost 400 ms in case of a sparse grid structure.
Of course, also in this case the use of the proposed cross-layer procedure allows for about 50% reduction of the latency of the process and of the number of required wireless transmissions. This time, with gains in range of 150-200 ms the difference can be clearly observable for the end user.

The results of the presented experiments indicate the advantages of employing the cross-layer address resolution procedure in terms of both latency and generated traffic. Minimalization of communication establishment latency allows the efficient use of multiple unicast traffic streams as an element of multimedia service designed for IEEE 802.11s MBSS environment (as already mentioned in Section 3.9.5). Additionally, such efficiency improvement will be useful in a frequent case of a multimedia services which rely on a multimedia content obtained from a number of different locations through the system – such as modern web-pages, peer-to-peer content sharing solutions and various content delivery networks depending on active, client-based caching and sharing of data [100].
The proposed cross-layer solution clearly improves both the efficiency of resource utilization in the IEEE 802.11 MBSS system, by significantly reducing the amount of management traffic and minimizing the probability of the necessity of retrying the procedure due to a failed broadcast transmission. The resulting reduced latency and increased reliability of IP communication establishment procedure in turn positively influences the quality of experience for the end-user. The presented simulation results show, that the proposed solution mitigates the inefficiency of IP protocol support previously described in Section 3.10.

4.2 Cross-layer name resolution extensions for IEEE 802.11s MBSS environment

With a demonstrated advantages of ARP resolution/path discovery cross-layer integration, it would seem that further application of cross-layer integration of mechanisms frequently used in IP connection establishment process can provide even more significant advantages.
With ISO-OSI layer 2 path discovery mechanisms already integrated with layer 3 (IP) - layer 2 (IEEE 802.11s) address resolution by means of mechanism proposed in 4.1.3, a promising direction of research would be an attempt to extend this approach to span even more ISO-OSI layers.

If we analyze a standard procedure of establishing a communication between two nodes of IP network, we will discover that in most cases the destination node is not directly identified by its IP address, but by an alphanumeric hostname [101]. If such hostname is to be used for communication establishment in an IP network, it has to be translated into an IP address.
Moreover, it is not always the case that a given name is directly mapped to a single IP address, as there is a number of scenarios, where a name represents a group of servers (for example in case of round-robin traffic distribution [102]) or even an application layer service instead of a specific host (NetBIOS or DNS-based service discovery [103]).

In this situation it seems that extending the cross-layer IP to MAC address resolution procedure described previously (which effectively allows for a layer 2 path discovery to an IP address) by including name to IP address resolution is a logical step offering further efficiency gains. Such an extension would provide IEEE 802.11s MBSS path discovery mechanisms with an ability to discover mesh transmission paths to DNS-named hosts. The procedure would also eliminate yet another message exchange in communication establishment procedure by integrating mechanisms of ISO-OSI layers 2 (data link), 3 (network) and 7 (application) as show in Fig. 99.

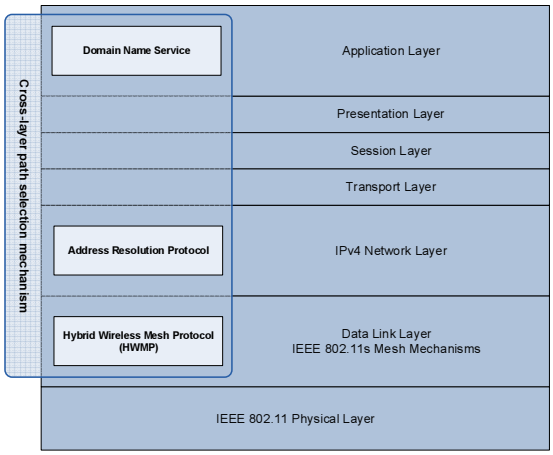

Fig. 99 Cross-layer name resolution extensions for IEEE 802.11s MBSS environment

Moreover, as name resolution mechanisms in modern IP networks often take an active part in service discovery, a cross-layer mechanism which would provide IEEE 802.11s specific enhancements to for this functionality should offer significant advantages in wireless mesh environment, where correct selection of service providing device is likely to have a considerable impact on both service quality and network resource consumption.

4.2.1 Name resolution mechanisms in IP networks

There is currently a number of standardized mechanisms for name resolution in the IP network environment. From literature studies and practical experience with production grade IP systems, it is possible to specify three widely supported and most often employed solutions:

- NetBIOS over TCP/IP name resolution and Windows Internet Name Service (WINS) [104,105],
- Unicast Domain Name Service (DNS) [106],
- DNS-based multicast solutions such as Multicast Domain Name Service (mDNS) [107] or Link Local Multicast Name Resolution (LLMNR) [108].

The mechanisms listed above are among the most popular solutions of the type and represent different approaches to the task of name to IP address resolution. Other solutions, such as or Peer Name Resolution Protocol (PNRP) [109] are not widely supported or often utilized in real-world systems.

4.2.1.1 NetBIOS over TCP/IP name resolution and Windows Internet Name Service

NetBIOS over TCP/IP name resolution in its base version is defined in IETF documents [104] and [105]. It offers an ability to use 15-byte names to identify network objects and obtain their IP addresses. Sixtieth byte of the name is used to describe the type of the object, for example a server providing a particular service or client of such service. It was once broadly deployed as name resolution service used by Microsoft operating systems in Local Area Networks. While detailed operation of this mechanism is significantly more complicated, its basic idea utilizes:

- broadcast distribution of name/type to IP address mappings over a single LAN segment,
- listening for and caching the above broadcast messages,
- ability to send queries to be answered by destination or caching nodes,
- selecting specific network nodes to facilitate the process.

The mechanism has been designed for relatively small, layer 2, wired network segments, where broadcast name resolution can be kept relatively reliable and its resource consumption will not have significant impact on other services. To provide name resolution services across different segments interconnected by layer 3 devices (IP routers), the basic standard has been extended to function using unicast communication in client-server model. Network nodes could be configured with WINS server address to register their name/type to IP address mapping in its database and to query it for such mappings of other network objects. Unicast communication allowed servers and clients to be located in different LAN segments and additional mechanisms have been introduces to provide database synchronization of WINS servers databases in multi-master mode. Moreover, compatibility issues between broadcast and unicast-based name resolution have been addressed by creating appropriate relaying mechanisms. The resulting WINS service allowed network nodes to utilize a combination of broadcast and unicast name resolution in relatively complicated network systems.
However, innate limitation of 15(+1)-byte, flat namespace and complication of the system (evident even from this short description) made it cumbersome in deployment and operation, especially in case of larger systems. Due to these problems the use of NetBIOS name service and WINS servers dropped drastically when a viable alternative solution became available – a Domain Name Service (DNS) with a number of extensions facilitating its use in dynamically changing network environment of LAN system.

4.2.1.2 Domain Name Service

Domain Name Service (DNS) has been designed for use in very large, but at the time relatively static, environment of Internet network. It had to support a large number of hosts spread over numerous administrative domains, but their address assignments and resulting name-to-address mappings

tended to remain unchanged for prolonged periods of time. To fulfil above requirements, DNS service supports a hierarchical (tree-based) namespace hosted in a distributed database. Elements of the namespace can be delegated to independent administrators and maintained on separate DNS servers, with logical references allowing localization of requested information by obtaining series of referrals, staring from a set of common root points (iterative name discovery). Alternatively, a client can submit a recursive DNS query, in which case the iterative name discovery can be performed on its behalf by a single DNS server and final answer will be returned if possible.
In its classic, unicast version, elements of namespace (DNS zones) could be maintained in a redundant set of synchronized servers, but the synchronization has been supported only in single-master mode, with only one writable replica. Also, no standardized methods of modifying content of a DNS database have been available, resulting in necessity of manual editing by administrator or use of custom made tools.
Such approach has been appropriate for intended working environment of the DNS service, but at the same time it made the DNS a poor choice for dynamically changing LAN environment. Subsequent numerous extensions of the standard, however, provided additional functionality, such as:

- DNS Dynamic Update [110]– ability for clients to dynamically modify DNS zone data,
- TXT [111] and SRV [112] records – ability to store additional information in DNS zone, such as application layer service access point descriptions and arbitrary string data.

With these standardized extensions DNS offers functionality sufficient to efficiently provide name resolution and service discovery for both Internet and LAN environments. Currently DNS is recognized as one of a group of crucial support services for IP-based systems, collectively abbreviated as DDI services (DHCP, DNS, IP Address Assignment) [113].
From a network communication point of view, DNS service follows a client-server architecture, with clients submitting unicast requests to a single (recursive name discovery) or multiple (iterative name discovery) DNS servers. It is a most common practice for end-clients to submit recursive name discovery requests to a small number (most often 1 or 2) of a preconfigured DNS servers.
Moreover, due to the popularity of the DNS service, its data structures are currently considered a standard for host and service naming purposes in IP networks, even when the DNS service itself is not used directly.

4.2.1.3 Multicast Domain Name Service

However functional and popular the DNS service is today, it still retains basic drawbacks of client-server solutions – the necessity to deploy and maintain a DNS server and to provide each client with a preconfigured server address and additional configuration such as local DNS domain name (needed for dynamic update and proper resolution of Partially Qualified DNS names). The client configuration requirement is often more troublesome than operating the DNS server itself, as necessary information must be entered manually on each client or a configuration service (such as, for example, a Dynamic Host Configuration Protocol) must be maintained in the network.
With such complications being common in case of network services based on client-server model, a number of auto-configuration solutions and network support services operating in distributed manner have been developed for IP networks. The trend is easily observable in case of IPv6 networks, but even in case of IPv4 there is a significant number of examples.
One group of such services addresses DNS name resolution problems mentioned above and includes such popular solutions as Multicast Domain Name Service (mDNS) standard developed by Apple Incorporated and Link Local Multicast Name Resolution (LLMNR) created by Microsoft Corporation.
Both of these solutions utilize multicast communication as a basis of a peer-to-peer name discovery while struggling to retain a high level of compatibility with a standard DNS service in regard to a provided functionality and employed information formats. As a result a compatibility with existing

applications can be preserved and the only operating system element which needs to be modified is a DNS service client (resolver).
Multicast Domain Name Service uses packet format compatible with classic client-server DNS, but instead of exchanging request-response messages between client and server, clients use multicast destination address for their DNS traffic. Additionally UDP port 5353 is used instead of classic TCP/UDP port 53, to unambiguously differentiate both services.
To improve performance all mDNS clients write information they obtain into their local DNS cache, even when the information they received has been intended as a response for request sent by another client. At the same time, clients are allowed to send answers only concerning their own DNS names (for which they are authoritative) and not based on their cached information. Responses are, by default, also send to multicast address, allowing all clients to update their cache information.
Clients can use two modes of submitting queries: one-shot queries and continuous querying. In case of one-shot queries, client simply sends a classic DNS UDP query to a well-known multicast address of 224.0.0.251 and port 5353. All mDNS clients which known the answer will respond with multicast response packet to the same address and port, unless they already detected a response to a given query sent from another client (in which case responding is optional). This method is highly compatible (standard DNS clients can be used if capable of using the multicast IP address and UDP port 5353) and allows for wide dissemination and caching of the response.
However, we should remember, that using a one-shot query, mDNS client will only process a first response received. While this sufficient for name-IP address resolution, another method must be used when we are interested in obtaining a combined information based on responses from multiple clients, for example a list of network devices providing a particular service. For such scenarios, clients should utilize the continuous querying method, which allows them to receive answers over a specified period of time and periodically repeat the query to maintain an up-to-date information.
It is worthy of note that, in contrast with classic client-server solution, there is no central authority in mDNS. Due to this fact, a distributed mechanisms for detecting and resolving name conflicts has been introduced. It requires a host to perform multiple multicast DNS queries over 750 ms to verify if its intended name is not already in use. If it is, there is an arbitrary procedure based on lexicographical precedence of disputed DNS name records of competing hosts to indicate which host will retain the name.
Even such cursory overview of mDNS operation clearly indicates that it is a solution intended for local IP systems of limited size, as indicated by, for example: lack of central authority, use of unreliable group message delivery and the method of resolving name conflicts. Moreover, mDNS supported namespace is limited to ".local" DNS domain and it should not be used to resolve names from other domains – for such purpose a classic DNS should be employed. The coexistence between these two mechanisms is a responsibility of a resolver, which should employ mDNS name resolution mechanisms for ".local" domain and classic DNS name resolution in all other cases. Unfortunately, it also means that this popular domain should not be deployed in systems using classic DNS servers, as it will be unreachable for mDNS aware resolvers.

The above overview of the most popular name resolution standards shows that there are currently two popular types of environment for such mechanisms to operate:

- Local Area Network environment, where we are interested in simplifying and automating configuration of clients (zero-configuration) and minimizing required infrastructure,
- internetwork environment, where mechanisms should allow for easy integration with a highly scalable network infrastructure.

It is evident that DNS-based name resolution mechanisms are currently the most popular solutions in both of these environments, with classic DNS being the most popular and mDNS gaining popularity in small, infrastructure-less deployments and access networks where zero-configuration requirement is of vital importance.

Due to the fact that IEEE 802.11s MBSS is based on wireless LAN technology, integrate with external network systems at ISO-OSI layer 2 and (as an access network technology) has been designed to provide a significant level of client auto-configuration, propositions of mechanisms included in this chapter concentrate on optimizing operation of a name resolution mechanisms currently encouraged for such environment – namely Multicast DNS with classic DNS compatibility.

4.2.2 Cross-layer serverless name resolution for IEEE 802.11 MBSS environment

As it is our purpose to provide IEEE 802.11s MBSS path discovery mechanisms an ability to discover ISO-OSI layer 2 paths to application layer hostnames belonging to MBSS nodes, we will be combining three separate processes necessary for initial establishment of IP communication in MBSS:

- name to IP address resolution,
- IP to MAC address resolution,
- MBSS path discovery

into one cross-layer procedure. Such approach should provide advantages similar to these already described in chapter 4.1, the proposed solution being a logical extension of mechanisms described there.
Due to a wide popularity of DNS-based name resolution and its associated name format, it has been decided then the proposed mechanism will be designed to retain compatibility with the DNS standard as far as name format is concerned which will facilitate the ability to seamlessly integrate it with a standard DNS infrastructure.
Taking into account the requirements specified above, it seems that a modification of the chosen Multicast DNS standard will provide functionality close to desired solution. Moreover, the mDNS employs peer-to-peer architecture, allowing an authoritative stations to respond to DNS resolution requests without the need of activating a dedicated server and performing relevant client configuration for all stations, which will simplify the intended cross-layer integration.

The standard Multicast DNS name resolution procedure in the MBSS environment must be considered inefficient as it requires the following steps:

1. Resolver checks if name to be resolved belongs to ".local" domain. If not, it is resolved using classic DNS.
2. Resolver checks if the answer is present in its local mDNS cache. If so, answer is provided locally and no inter-node communication takes place.
3. Resolver generates a DNS Request message containing a DNS Question for a specified name.
4. DNS Request message is encapsulated in an UDP packet, addressed to a multicast address 224.0.0.251 port 5353.
5. As IEEE 802.11s standard does not support multicast transmission, the packet is flooded through the network as in broadcast data frames as per standard broadcast procedure described in Section 3.7.1.2.
6. Stations receiving the broadcast data frame process it according to general IEEE 802.11s rules concerning broadcast transmission. At the same time, each retransmitting station passes the UDP multicast packet the frame contains to IP layer for further processing.
   If mDNS is not supported the network layer silently discards the packet. It should be noted, however, that the broadcast IEEE 802.11s frame containing such packet is still retransmitted as per general IEEE 802.11s broadcast rules.
   If a given station supports mDNS, the DNS message received is retrieved from UDP multicast packet and processed by mDNS mechanisms.
   a. If the message is a DNS Request:

i. If mDNS service knows the answer to any of the questions the DNS Request message contains, it generates a DNS Response message and sends it as UDP packet addressed to the same multicast address and port as the query. Such response is also flooded through the MBSS in a broadcast data frame.
ii. Any questions contained in DNS Request message for which a given station does not know the answer are silently ignored.

b. If the message is a DNS response:
   i. Information contained in DNS Response message can be included in DNS cache of the station's mDNS service.
   ii. If the station is the one which originated a specific DNS Request, the DNS Response is passed to the resolver.
      1. If the query was a one-shot query the name resolution process is considered complete.
      2. If the query was a continuous query, resolver can continue to wait for eventual subsequent responses.

It is by design, that DNS Responses are transmitted by means of multicast UDP traffic, as such approach allows all mDNS-capable stations to learn and cache transmitted information. This information can then be used by their resolvers, however stations are not allowed to generate responses based on cached information. It is a significant modification of the classic DNS behavior, where DNS servers are allowed to generate responses from cached data and this ability plays significant role in maintaining the service scalability and provides protection from short-term unavailability of authoritative servers. In contrast, Multicast DNS service has been designed for wired LAN installations of limited size, where scalability of the solution is of secondary importance to ease of configuration and data transmissions are expected to be low-latency, high-speed and highly-reliable. In such environment multicast or even broadcast transmission combined with data caching provides readily available information to all interested stations without the need of prior configuration (zero-configuration property), while elimination of the ability of non-authoritative stations to respond based on cache information simplifies cache management and name conflict resolution, while minimizing probability of propagating stale information.

However, in case of multihop wireless network, multicast or broadcast-based communication can be a significant disadvantage. In case of IEEE 802.11s MBSS multicast communication is not supported and all group addressed frames will be delivered by means of broadcast transmission, specifically by employing the already described flooding procedure (see Section 3.7.1.2). Due to lack of any broadcast optimizations in the IEEE 802.11 MBSS such transmission will result in unnecessary resource consumption. Moreover, broadcast frames are transmitted without acknowledgement procedure (see 2.4.1) which can lead to their unrecoverable and undetected loss. While lack of broadcast optimization procedures mitigates the problem in dense networks, where each station will most probably receive multiple copies of a given broadcast frame from its neighbors (each of which is required to rebroadcast the frame), in sparse networks the probability of performing only a partial broadcast remains high. In this situation, mDNS request-response exchange requiring transmission of two broadcast frames can be both resource intensive and unreliable.

Moreover, we should remember, that in case of mDNS there is no central authority maintaining complete, authoritative information concerning a given DNS domain, but each station is authoritative for its own DNS records. They will most often contain name-to-IP address mapping, but other information can also be included, such as a service advertisement information. Such a strictly distributed approach to database creation and maintenance, where each station holds an element of a distributed pool of name-to-address mappings, requires a mechanism to prevent name conflicts when multiple stations attempt to register the same name.

The name conflict prevention mechanism requires a new station to attempt to resolve its name with use of mDNS mechanism – such operation has to be repeated three times with timeout of 250 ms each time, resulting in 750 ms delay before station can begin responding to mDNS queries. Furthermore, if name conflict is detected during station operation, it is required to cease responding to queries, optionally modify the name (if it does not have a priority for its ownership) and repeat the above procedure.

From the above descriptions of mesh path discovery, ARP and mDNS mechanisms presented in previous sections it can be seen that a completion of the procedures necessary for IP communication establishment between named network stations of IEEE 802.11s MBSS requires a sequential completion of multiple message transmissions between the same pair of stations – source STA (initiating communication) and destination STA. The precise number and type transmissions depends on whatever a partial information is present in cache memory of participating network stations. In the worst case, when no information is present in DNS and ARP caches of source and destination stations, and when transmission path between them is not present in HWMP forwarding tables, the process requires no less than 4 broadcast and 2 unicast transmissions:

- a broadcast mDNS Request from source STA for IP address corresponding to destination STA's name,
- a broadcast mDNS Response from destination STA containing its IP address,
- a broadcast ARP Request from source STA for MAC address corresponding to destination STA's IP address,
- a broadcast Path Request (PREQ) for a path from destination to source STA (creating unidirectional paths towards destination STA) – necessary for sending a unicast ARP Reply,
- a unicast Path Reply (PREP) from source to destination STA (creating unidirectional path from destination to source STA),
- a unicast ARP Reply from destination to source STA containing destination node's MAC address.

It is evident that simple deployment of the mDNS in the IEEEE 802.11s environment will not be a particularly efficient solution in terms of volume of generated traffic, service latency and reliability.

4.2.2.1 Address resolution procedure

In order to efficiently employ an mDNS compatible solution in the IEEE 802.11s MBSS environment and limit the number of the sequential message exchanges required for initial establishment of IP communication between two STAs, a solution similar to the one described for the ARP integration scenario has been proposed.
As the mDNS Request messages are to be delivered to all stations within MBSS, as is the case with:

- a standard, reactive Path Request (PREQ) messages, used in path discovery process,
- ARP Request messages of the ARP protocol,

it is only natural to adopt a cross-layer integration approach and attempt combine all three above processes into one.
To do so a new DNS Request Information Element (DNSREQ IE) is defined and appended to a standard PREQ message, resulting in creation of a new HWMP DNSREQ Path Selection frame, containing a combined information sufficient to perform an mDNS address resolution, an ARP address resolution and a mesh path discovery.

Transmitting the response generated as a result of such a combined procedure is less straightforward, as the response to the mDNS Request message is normally distributed using a multicast transmission, while we aim to integrate it with:

- a standard, unicast Path Reply (PREP) message,
- a standard, unicast ARP Reply message.

In this situation we are going abandon the multicast manner of the mDNS Response and combine it with the standard PREP and ARP Reply messages, to be delivered within an unicast HWMP DNSRESP Path Selection frame, constructed by appending a DNS Response Information Element (DNSRESP IE) to the Path Reply Information Element (PREP IE) in data field of HWMP Path Selection frame. The DNSRESP IE will contain response information of both ARP and mDNS protocols.
Such approach will limit the ability of stations other than the originator and the target to cache the mDNS Response data, but in resource limited IEEE 802.11s MBSS environment a reduction of a broadcast management traffic and a better reliability of an acknowledged unicast transmission should offset the loss.
In effect, by integrating the mDNS name resolution, ARP address resolution and IEEE 802.11s path discovery we are creating a new, cross-layer procedure can be seen as a method allowing the discovery of mesh paths to DNS-named hosts within the IEEE 802.11s mesh network.

Source station which intends to communicate with another STA initiates the procedure of cross-layer path selection to an name-identified host or service by checking its available cache information:

1. The source STA checks if destination hostname is in its DNS resolver's cache. If so, hostname to IP address resolution is performed locally, based on cached data.
2. If IP address of the destination STA has been obtained in previous step, the source STA checks if destination IP address is in ARP cache. If so, IP to MAC address resolution is performed based on cached data.
3. If MAC address of destination STA has been obtained in previous step, the source STA checks if current path information is present in its forwarding table. If it is present, the procedure is successful – the source STA has current path to the specified DNS hostname. If not, a standard path selection procedure is performed using obtained destination MAC address.

If the source STA is missing cached information in any of first two steps, thereby preventing direct use of standard path selection procedure, the source STA creates the HWMP Path Selection message containing PREQ and DNSREQ IEs. The message is then flooded through the network according to standard IEEE 802.11s path discovery rules, as non-modified STAs recognize it as a standard PREQ message. However, as the only station which should generate reply is the one whose hostname matches the name specified in DNSREQ IE, target address field in PREQ IE must be set to the value of 00-00-5E-00-53-00 (address which is not to be used in real-world network systems [99]), thereby preventing the standard HWMP mechanisms from generating PREP based on PREQ IE.

4. Modified STAs process the DNSREQ IE prior to processing the PREQ IE. If a destination hostname field in the DNSREQ IE matches their own, they generate a message containing both a PREP IE and a DNSRESP IE, following the rules described below. The station also updates its ARP cache with information concerning source STA.

   If DNSREQ IE destination hostname field does not match STA's hostname, the HWMP Path Selection frame is processed based on its PREP IE, allowing creation of a reverse path to the source STA, as per standard HWMP rules.

This DNSRESP IE contains information normally provided by DNS and ARP Reply messages: IP and MAC addresses of the destination STA. It is sent to the source STA in a unicast HWMP Path Selection frame as specified for a standard PREP message.

5. All intermediate stations process a PREP IE according to standard IEEE 802.11s rules (forming forward path from source to destination STA). Modified station can additionally use DNSRESP IE information to update their DNS and ARP cache.
6. The source station processes a PREP IE to finalize the procedure of mesh path discovery and a DNSRESP IE to finalize procedures of DNS and ARP address resolution. Appropriate information is written to HWMP forwarding table and DNS/ARP caches.

Stations will provide responses to queries for FQDNs which they consider to be their own. However, in contrast to mDNS, there is no requirement to perform the verification procedure for FQDNs. In the MBSS environment such broadcast-based procedure will be unreliable, due to:

- relatively high probability of a broadcast transmission reaching only part of the MBSS, resulting in significantly extended latency of the procedure and limited probability of its successful operation,
- inability to easily monitor adherence to the standard, which would open an easy way for a malicious STA to perform a Denial of Service attack, by preventing registration of any names, or to register an already owned name anyhow.

The verification procedure is still advised to be performed, however with the above disadvantages and due to the lack of reliability, it is no longer obligatory. Moreover, the resulting ability of two stations registering the same name can be used to conduct an anycast-like name discovery, as the initiating station can obtain multiple responses, with these most likely to offer the best traffic conditions arriving first.

As can be seen from above description, the procedure requires only one broadcast and one unicast transmission. Moreover, when compared with classic, three stage communication establishment process, modified stations on the communication path between source and destination STAs retain the same opportunities to cache DNS and ARP data. Unfortunately, as already mentioned, all other modified stations lose opportunity to cache DNS data for destination station from DNSRESP, which is transmitted as unicast instead of broadcast. In some cases this lost opportunity could provide a STA with information it requires for communication establishment, but it is highly probable that such STA would still need to obtain an ARP mapping or discover mesh path to destination station, each of which requires the same number of messages to be exchanged as the complete cross-layer procedure described above.

4.2.2.2 New data structures

The new DNS Request Information Element (DNSREQ IE) will not strictly follow a standard DNS message format due to the need to minimize message size, as the maximum size of IEEE 802.11 IE is limited to only 255 bytes. Moreover, larger messages are more prone to transmission errors and, under unreliable broadcast transmission rules, to message losses. However, the DNSREQ IE structure (see Fig. 100) will allow a sending station to include one or more DNS questions in a DNS-compatible format and thus performing a path discovery for a number of names simultaneously (to account for such an ability in regard to name-to-address mappings provided by the mDNS standard).

Fig. 100 DNS Request Information Element

The DNSREQ IE begins with the mandatory Element ID, Length, OUI and IE Type fields required by the IEEE 802.11 standard in case of Vendor Specified IEs, which have been already described in Section 4.1.3.1. Of course in this instance the IE Type field will hold value 0x02 indicating the DNSREQ IE (as specified in Table 6). Subsequent DNSREQ-specific fields provide the information necessary to implement the described cross-layer procedure:

- Protocol Type (2 bytes) – indicates the version of IP protocol to which the initiating STA attempts to use for communication with the indicated destination STA. Determines the Sender Protocol Address field's length and the type of address returned in response to the query for IP address (IPv4 or IPv6). Values for this field are defined in ARP protocol specification.
- Sender Protocol Address (variable length, depending on Protocol Type) – an IP address of the initiator of the procedure,
- DNS Name Count (1 byte) – allows for multiple DNS Name fields to be included in a single DNSREQ IE and indicates their number. The special value of 0 indicates the fragmented DNS Name as described below,
- DNS Names (variable length) – the FQDN of the intended destination, encoded according to DNS rules [106].

Despite the requirement of compatibility with DNS data structures, it does not seem necessary to directly include standard DNS Question structure (as shown in Fig. 101) in the DNSREQ IE, as some if its fields are redundant in this situation and will unnecessarily increase the size of DNSREQ message.

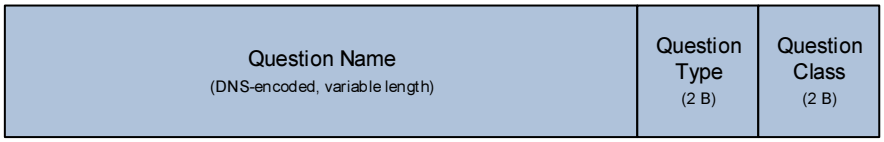

Fig. 101 Standard DNS Question structure

With the only Question Type (2 byte field) values relevant to the situation when we are interested in obtaining an IP address as a result of our query being:

- 0x0001 – IPv4 address,
- 0x001C – IPv6 address,

and the Protocol field described earlier specifying the IP protocol version, the Question Type field can be omitted. Additionally, the DNS Resource Record Class (2 byte field) can be left out also, as the only value defined for it is "Internet" (0x0001).

The single remaining Question Name field is a variable length one, containing an FQDN to be resolved, encoded according to specific DNS rules [106]. The encoding provides a number of features, in particular the ability to detect the end of the field without additional length-describing field, and a name compression mechanism when multiple questions are included in a single message. Due to the these modifications of the DNS Question format, the resulting data structure, consisting exclusively of the Question Name field, is named the DNS Name field of DNSREQ IE. It is preceded by a DNS Name Count field, specifying the number of DNS Names included in the IE, to support the functionality of the mDNS allowing to specify a number of DNS names to be resolved in a single message. In our case, it will result in ability to initiate a number of path discovery processes with a single HWMP DNSREQ message broadcast.

However, there is an additional difficulty in maintaining conformance with the DNS data structures, caused by the maximum allowed length of the encoded DNS FQDN being 255 bytes – the same value as the maximum allowed length of the complete IE structure. It clearly indicates that the compatibility cannot be maintained without additional mechanisms enabling the fragmentation of DNS Name field data. For this purpose an additional DNS Request Extension IE (DNSREQExt IE) has been defined (Fig. 102), possible to be used only directly following the DNSREQ IE. Its structure, apart from the already described mandatory fields with the IE Type indicating DNSREQExt IE by assuming

the value of 0x03, contains only a single, variable length DNS Name Continuation field, which contains the DNS Name data which could not be accommodated in DNSREQ IE due to its limited size.

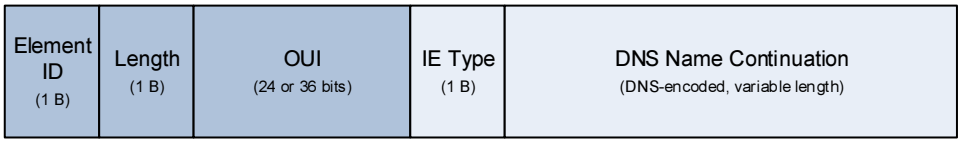

Fig. 102 DNS Request Extension Information Element

When there is a need to accommodate the DNS Name field exceeding the remaining capacity of the DNSREQ IE, its DNS Name Count field should contain a value of 0x00, indicating that a DNS Name field that follows continues until the end of DNSREQ IE, and that this HWMP DNSREQ Path Selection frame additionally contains an DNSREQExt IE carrying the remainder of the DNS Name data.
When there is a need to fragment the DNS Name field, only a single DNS name is allowed per HWMP DNSREQ frame, and the DNSREQ IE should be processed after reconstruction the complete DNS Name field.

The PREQ/DNSREQ IE pair present in the HWMP DNSREQ Path Selection frame contains all information necessary to perform a DNS name to IP address resolution, followed by IP to MAC address resolution complete with update of the destination station's ARP cache with information about the initiator of the path discovery process:

- mDNS address resolution:
  - DNS Name of DNSREQ IE – FQDN to be used as a Question Name in a DNS query for A or AAAA (as indicated by Protocol Type field) record,
  - Protocol Type of DNSREQ IE – used to choose the record type of the DNS query (A or AAAA),
- ARP address resolution:
  - Protocol Type of DNSREQ IE – protocol type indicating if ARP (IPv4) or other (for example IPv6 ND) procedures should be used,
  - Originator Mesh STA Address of PREQ IE and Sender Protocol Address of DNSREQ IE – provide information required to create an ARP cache entry for the initiator of the procedure,
  - the IP address obtained from mDNS query and the receiving STA's MAC address – to be delivered to the initiator STA, which will allow it to create an ARP cache entry for the destination STA.

Responses to HWMP DNSREQ Path Selection frames are provided with use of HWMP DNSRESP Path Selection frames, containing a combination of the Path Response IE (PREP IE) and the DNS Response IE (DNSRESP IE). The format of the latter IE is presented in Fig. 103 and also differs from a standard DNS Response message, for reasons already described in case of DNSREQ IE. The new IE allows the station to provide response to DNSREQ IE and is an element of DNSRESP massage, which contains:

- a Path Reply IE responsible for creating a data transmission path between the source to the destination station and extending the DNS Response IE-provided information with additional information required for a mapping between destination's IP address and its MAC address,
- followed by a DNS Response IE containing appropriate DNS name to IP address mappings.

The DNSRESP IE should be used only following PREP IE forming a HWMP DNSRESP Path Selection frame, and not transmitted individually.

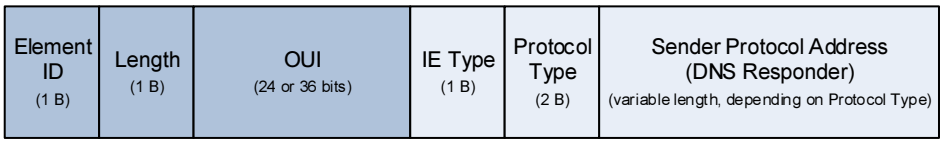

Fig. 103 DNS Response Information Element

The structure of DNSRESP IE includes the starting fields required by IEEE 802.11 standard, with IE Type field value set to 0x04 to indicate its type. These are followed by DNSRESP specific fields:

- Protocol Type (2 bytes) – indicates the version of IP address returned in response to DNS Name provided in DNSREQ IE and the length of the following Sender Protocol Address field. Specific values are these identical to these defined by ARP protocol for such a field.
- Sender Protocol Address (variable length, depending on Protocol Type) – the IP address corresponding to the DNS Name indicated in the received DNSREQ message.

The HWMP DNSRESP Path Selection frame must both result in creation of forward path from the originating STA to the destination STA of the path selection process, but also provide the originating STA with information sufficient to create address mapping between:

- the specified DNS FQDN name and corresponding IP address,
- the IP address indicated above and the MAC address of its corresponding destination STA.

As the HWMP DNSRESP Path selection frame begins with a standard PREP IE, it will be processed by unmodified stations as a HWMP PREP Path Selection frame and forwarded along the available reverse path from the target of the path discovery process to its originator. Along the way it will create the forwarding information resulting in creation of the forward path (as described in 3.7.3).
The STA which initiated the DNSREQ-based path discovery will additionally process the DNSRESP IE and obtain the following information, sufficient to finalize both mDNS and ARP address resolution:

- mDNS address resolution:
  - the FQDN of the intended target station, retrieved from the local temporary cache using the value of the Path Discovery ID field of PREP IE as a key (see description below),
  - Protocol Type and Sender Protocol Address of DNSRESP IE – indicating the type and value of the IP address corresponding to the above FQDN,
- ARP address resolution:
  - Protocol Type of DNSRESP IE – protocol type indicating if ARP (IPv4) or other (for example IPv6 ND) procedures should be used,
  - Target Mesh STA Address of PREP IE and Sender Protocol Address of DNSRESP IE – provide information required to create an ARP cache entry for the target of the procedure.

4.2.2.2.1 Resolver operation concerning partially and fully qualified domain names

The standard DNS service will provide answers to questions for Fully Qualified Domain Names (FQDNs), which uniquely identify a specific DNS record within DNS hierarchical naming structure. FQDN names consist of name of a specific record in DNS database including a complete DNS domain name in which it is located – for example: *host.eti.pg.gda.pl*. The rightmost element of FQDN must be a top-level domain.
However, FQDNs can be quite lengthy due to necessity of providing full domain name, so DNS resolvers will also accept Partially Qualified Domain Names (PQDNs), containing only a specific part of FQDN, starting with leftmost component – for example: *host* or *host.eti*. Moreover, there are no universally supported method for an application to inform the resolver, if a name provided in its query is partially or fully qualified.

In this situation, the standard resolver will perform name resolution not only for a name specified by an application, but also extend it, by appending it with:

- a suffix configured as “local DNS domain name”,
- suffixes from a list of “search DNS suffixes”.

The process will continue until one of the queries results in successful name resolution or resolver runs out of suffixes to append to a specified name.
However, in case of our proposed cross-layer solution, each such attempt could result in a broadcast transmission of a HWMP DNSREQ Path Selection frame. To minimize the management traffic generated in such case, it is advised to first attempt the procedure for the precise DNS name submitted by the application, and in case of its failure, use the multi-DNS Name capability described before.

4.2.2.2.2 Support for global DNS infrastructure

The standard mDNS mechanisms are limited to processing DNS Questions for the “.local” domain only, to allow the resolver to easily separate which names should be resolved using mDNS and which should be processed by the unicast DNS infrastructure.
This approach can be maintained in case of our cross-layer procedure wish similar advantages and employ a classic DNS server advertised with use of the cross-layer method proposed in the next chapter, to retain a zero-configuration capability.
The alternative solution, which should be considered less efficient, makes the proposed procedure the only method of DNS name resolution within the MBSS used to resolve any technically valid FQDN. The integration with classic DNS structure in this case, can be provided by a mDNS/DNS proxy located at one of mesh gates.

4.2.2.3 Compatibility considerations

The proposed procedure is based on the same principles as the previously described IP to MAC address cross-layer resolution procedure, and thus shares its principal compatibility characteristics.
However, it should be observed, that cross-layer integration spanning multiple ISO-OSI layers is more difficult to efficiently employ, due to the necessity of implementing mechanisms which are normally provided by intermediate layers’ mechanisms and the generally more sizable data units involved in management processes of higher ISO-OSI layers. The good example of such difficulties, can be the necessity of implementing a DNS Name field fragmentation procedures to cope with a limited size of IEEE 802.11 Information Elements.

4.2.2.4 Expected advantages

The proposed cross-layer path selection procedure allows for a significant reduction of management traffic and time necessary for initial IP communication establishment with a destination mesh stations specified by DNS names – instead of up to 4 broadcast and 2 unicast messages which must be exchanged sequentially, the process is accomplished with only 1 broadcast and 1 unicast message. Based on results of simulation experiments concerning the previous cross-layer integration method, covering only ARP protocol and HWMP path selection procedures, it can be expected, that the gains in terms of reduced latency and number of wireless transmissions will be even greater in case of this more comprehensive method.

4.2.3 Experiments

In order to easily compare the efficiency of the proposed cross-layer name resolution procedure, a set of experiments analogic to the one used in case of the cross-layer IP to MAC address resolution procedure have been performed. The basic summary of the experiments includes:

- the MBSS of 30 stations capable of communication (in case of network segmentation, the MBSS topology generation has been repeated),
- topology of the MBSS generated using 4 different methods (described in 3.8.5): dense grid, sparse grid, dense random and sparse random,
- 11 different levels of traffic load have been considered, generated by activating 0 to 10 of 1 Mbit/s UDP traffic sources located at randomly chosen mesh stations, with a randomly selected traffic destinations,
- a 100 simulation runs for each topology type and traffic load combination.

The timeout values of ARP and mDNS protocols, governing the delay before the procedure of address or name resolution can be retried in case of lack of answer, have been set to the minimal values allowed by the respective standards – 1 s for ARP and 2 s for mDNS.

During each simulation run, following a 10 s warm up period, allowing mesh mechanisms to create a functional MBSS system, a randomly chosen STA attempted to establish an IP communication with another randomly chosen mesh STA, using its DNS name and mDNS protocol as a means of resolving it to an IP address. The presented charts contain mean values obtained from the above simulation runs and show 95% confidence intervals.

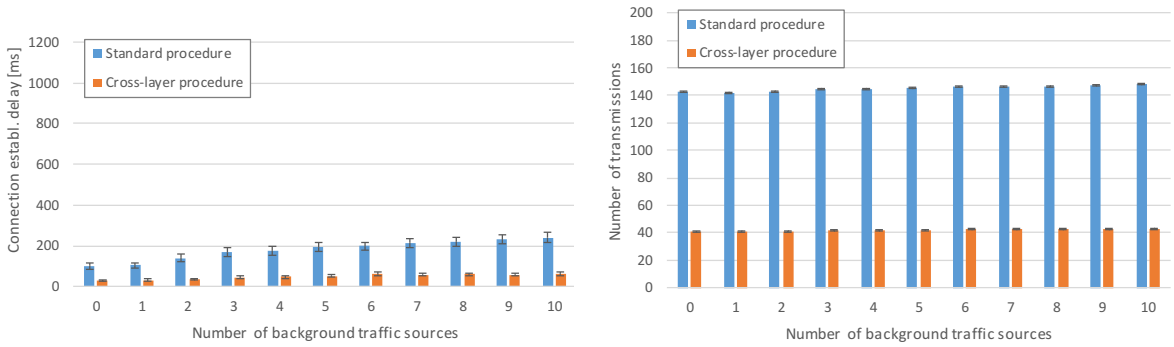

Fig. 104 The delay and a number of required wireless transmissions required for establishing an IP communication with a DNS named host compared for standard and cross-layer procedures in a dense grid mesh structure

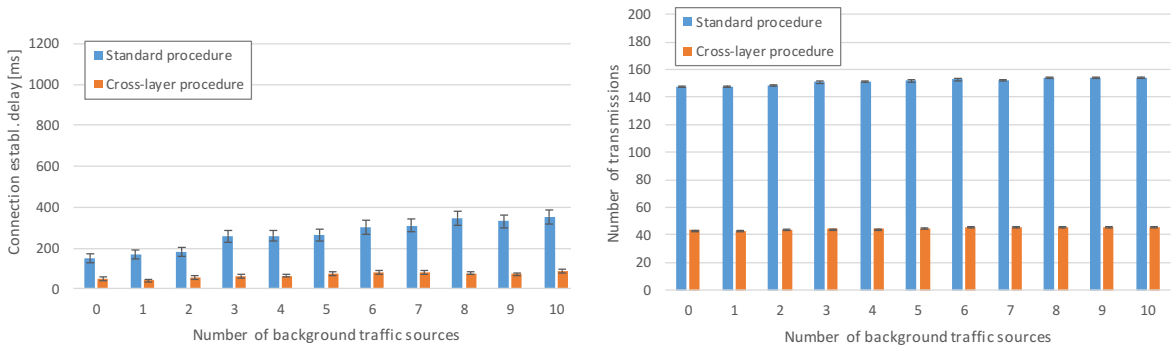

Fig. 105 The delay and a number of required wireless transmissions required for establishing an IP communication with a DNS named host compared for standard and cross-layer procedures in a dense random mesh structure

The results for dense network topologies show that even in this preferable (as indicated by previous experiments, see 4.1.4) environment, a standard 3 stage process of establishing communication with an IP host identified by a DNS name can generate a considerable latency, due to the necessity of delivering four broadcast and two unicast messages required for its completion. Even with no

network traffic present, the mean latency is between 100 ms and 150 ms. When a significant traffic load is present, the values will more than double, reaching 240 ms for the grid-based network and 350 ms for the random one. With such a considerable latency values in the dense mesh environment providing good quality links, we can expect the delay to grow to alarming values in case of sparse mesh structures.

In the described experiments, the cross-layer approach offers about 70-75% reduction of the mean latency of the process and about 70% reduction of the mean number of wireless transmissions required in case of these types of mesh structures, bringing the latency to a toughly acceptable values of 30-60 ms for a dense grid and 50-90 ms for a dense random network structure. The dependence of the latency of the cross-layer procedure on the traffic load is largely limited due to reduction of the required number of messages to be exchanged.

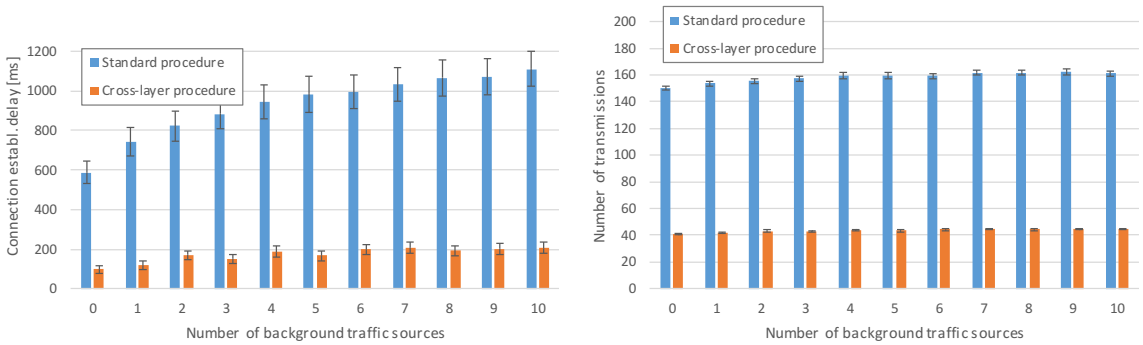

Fig. 106 The delay and a number of required wireless transmissions required for establishing an IP communication with a DNS named host compared for standard and cross-layer procedures in a sparse grid mesh structure

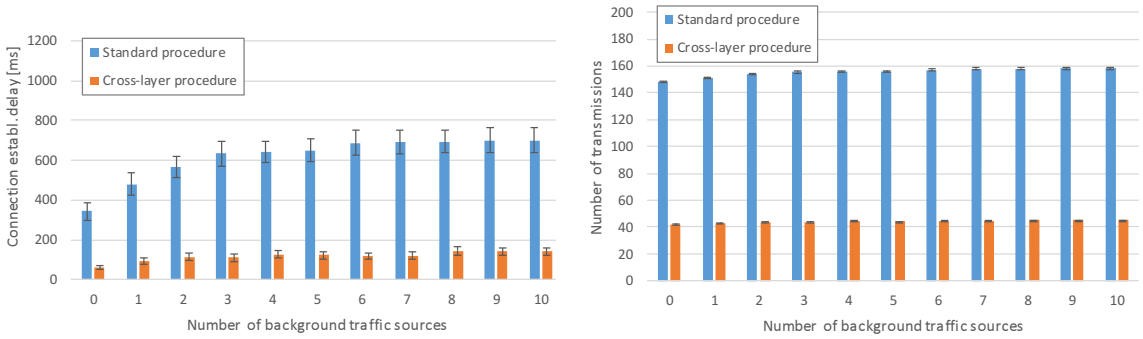

Fig. 107 The delay and a number of required wireless transmissions required for establishing an IP communication with a DNS named host compared for standard and cross-layer procedures in a sparse random mesh structure

The delay of the standard, sequential, mDNS/ARP/HWMP procedure of establishing communication with a DNS named host within the MBSS system, considerable even in case of dense topologies, in case of sparse network structures grows to values, which will certainly degrade the user experience even in case of services which do not require the establishment of numerous IP communication sessions. With the sparse random network exhibiting a latency between 350 ms and 750 ms (depending on the traffic load), which in case of a sparse grid network grow even more and reach the range of 600 ms to 1100 ms, the need for optimization cannot be denied.

The proposed cross-layer procedure allows the latency reduction of about 80%, bringing it to a level of 60-140 ms for the sparse random network and of 90-200 ms for a sparse grid structure. These values, while sill considerable, can be accepted for most purposes in this difficult network environment.

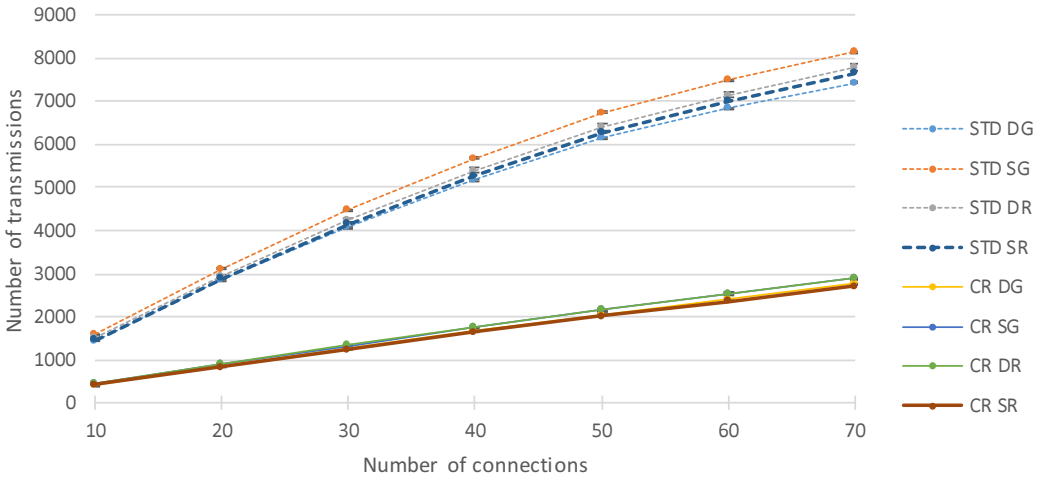

Fig. 108 Impact of mDNS caching on a number of wireless transmisisons requred for an mDNS-based communication establishement (DG – dense grid, SG – sparse grid, DR – dense random, SR – sparse random, STD – standard procedure, CR – cross-layer procedure)

Due to the fact, that the proposed cross-layer method of combining mDNS name resolution, ARP address resolution and HWMP mesh patch discovery prevents a network-wide reception of mDNS Response message and thus limits the ability of mesh stations to cache its content, an additional simulation scenario designed to assess the impact of this effect has been performed.
For this purpose, a 70 IP connections between a randomly chosen pairs of DNS named mesh STAs have been sequentially attempted, while recording the number of generated wireless transmissions. The scenario have been performed a 100 times for both the standard procedure and the proposed cross-layer one in each of the 4 described mesh structure types.
Due to high number of configuration values controlling cache maintenance, a set of values where standard procedures will perform most efficiently has been chosen for comparison with the cross-layer method – it is assumed then all stations start with empty cache, but entries entered into cache remain valid for the complete period of the simulation run. All other configurable parameters of discussed protocols are assumed to have default values specified in standardization documents or based on common practice found in popular operating systems.
As can be seen from results shown in Fig. 108, the ability to cache the mDNS Response message provides some reduction of the number of required wireless transmissions, however the gain does invalidate the advantages of the proposed cross-layer procedure. Moreover, it should be noted, that the proposed procedure could also make an extensive use of caching, for example allowing mesh stations to cache the contents of DNSREQ IE, thus providing all stations within the MBSS with IP to MAC mapping for the source station complete with the mesh path towards it. An additional field containing a source station's DNS name added to the DNSREQ IE, would complete the broadcasted information with DNS name to IP mapping. However, due to dynamically changing structure and configuration of a self-organizing wireless mesh network such an extensive caching of information is not advisable (following the same reasoning that forbids mDNS responses from cache). Moreover, additional sizable data fields (such as DNS name field) would significantly increase the size of DNSREQ IE.

The proposed cross-layer procedure provides even larger gain in both efficiency of resource utilization within the MBSS network and the resulting end-user experience, then the previously described, cross-layer IP to MAC address resolution procedure. As a result, it removes one of the IEEE 802.11s specification's weak points, by providing it with a capability of providing an efficient support for the popular IP protocol, despite the reliance of its mechanisms on a group addressed communication.

As an example of the scenario in which a minimalization of IP communication establishment delay can be useful, is the simple procedure of communication quality assessment, allowing the client to select a content or service-providing server from the preconfigured list. For this purpose, the client attempts to access its configured servers to request their service-quality related parameters (such as their current load, number of connected clients, content compression methods, etc.) or even performs an active testing of the communication quality using a variety of methods. Such assessment, especially the active testing, is often performed sequentially, to prevent different probe transmissions from interfering with each other.

The abovementioned process of advertising and selecting a most advantageous content or service provider is an important element of modern multimedia services, which makes the proposed solution an advantageous multimedia service support mechanisms for IEEE 802.11s MBSS environment. However, due to the importance of the service selection process, a dedicated cross-layer procedure for this purpose will be presented in the following (5) chapter.

5 Cross-layer service advertisement for IEEE 802.11s mesh networks

As described in the basic properties of the IEEE 802.11s wireless mesh specification, the MBSS network provides a data link layer service for its participating stations. At the same time it should be observed, that the service is provided over the changing, multihop structure of a self-organizing network, which requires the use of mechanisms and procedures more often found in network layer protocols.
Another difference between the IEEE 802.11s and other ISO-OSI layer 2 network solutions popular nowadays it the fact that the wireless transmission medium used by the standard is shared in a manner difficult to predict and control. Wired technologies can fully control access to their transmission medium using relatively simple mechanisms. In case of a self-organizing wireless mesh network operating in the ISM band, each transmission is susceptible, at each of its possibly multiple hops, to effects such as:

- intra-path interference – interference between two hops of the transmission itself, if the receiving and sending channels are not orthogonal. The IEEE 802.11s does utilize a single RF channel for both operations to allow it to be employed by stations equipped with a single wireless interface,
- inter-path interference – interference between transmissions belonging to different transmission paths present within interference range. In case of self-organizing network, with both structure and transmission paths is controlled by autonomous mechanisms, inter-path interference can be difficult to predict and will itself impact the route of further transmission paths,
- external interference – interference from external RF systems, while also present in simple point-to-multipoint installations, in case of mesh network becomes more difficult to measure (configuration of measuring stations and measurement data distribution), analyze (choosing of a centralized analysis point or employment of distributed analysis method) and react to (reconfiguration of network stations without disrupting the operation of other MBSS mechanisms),
- device failures – while in case of the simple system such occurrence will most probably result in service unavailability, as either the interested client or its single point of network access ceased to function, in case of mesh network the service can continue to be provided, but with a changed quality characteristics. If the MBSS is created based on client devices, the chance that a device will cease its operation or change its operational characteristics is also much higher than in case of system based on operator-provided infrastructure.

The above description clearly illustrates the fact, that the MBSS network is likely to provide a changing level of service. Moreover, the quality of service is very likely to be dependent on the physical path the transmission takes within the mesh structure, which in turn is dependent on a source and destination of a particular traffic flow within the MBSS.
At the same time, in order to provide the IEEE 802.11s MBSS with an ability to easily integrate into existing network structures and allow it to be used for a wide range of higher layer protocols, it is exposed to both external networks and higher layer protocols as a single Ethernet broadcast domain.

Such approach accomplishes the compatibility goals of the designers, however it may pose a significant complication for higher layer service discovery procedures, especially if a server selection is involved in the process.
The problem is caused by the fact, that most such solutions tend to assign clients to servers on the basis of:

1. belonging to the same local area network as the server (Multicast DNS Service Discovery, NetBIOS),
2. belonging to the same network layer addressing group (for example an IP network) as the server (Classic DNS Service Discovery with DNS Address Sorting or DNS Views), which often translates into the same local area network,
3. number and type of LAN systems between a client and the server (STP-based detection methods, link-state dynamic routing protocols such as OSPF),
4. number and type of network layer devices (for example: routers) between a client and the server (single packet connectivity tests),
5. connectivity test between a client and the server, which should be performed fast and without causing disruption of network operation (mostly application specific or proprietary solutions).

If we analyze the first four approaches, it can be seen that in all these four cases a single LAN network is being interpreted as an indivisible entity with specific characteristics attached. Moreover, these characteristics are often limited to the maximum theoretical throughput attainable by the technology it operates.
While such approach can prove sufficient in case of fast and stable wired networks or even wireless MAN and WAN systems capable of providing QoS guarantees for network traffic, it does not seems adequate for the complex environment of the MBSS network, where not only length of the transmission path within the MBSS but also its spatial placement and relation to other paths can drastically impact the quality of the transmission. At the same time, the design of IEEE 802.11s MBSS mechanisms aims to hide as much of its internal operation and structure as possible.
The fifth approach to server selection, based on actual testing of traffic conditions between a client and the server, can be expected to provide the best results as we are depending on definite measurements instead of trying to deduce the expected conditions based on network structure.
The downside of such approach stems from the necessity of performing active measurements of attainable transmission quality. While there is a number of methods for the task [114-121], their reliability tends to depend on the time taken to perform the measurement, and with a number of servers to choose from the process of selection can become quite lengthy. Moreover, in case of a wireless mesh network's changing environment, the results could retain its currency only for a limited time.

In the situation described above, with a complex MBSS internal network structure hidden from external mechanisms and the usual server selection mechanisms designed with an assumption (incorrect in this instance) that a LAN system can be considered as an uniform whole, it seems to be a scenario where employment of a cross-layer approach can bring substantial advantages.
It can be especially advantageous in case of servers located within the mesh network, because in their case, from a network layer point of view, they are all 1 hop away. Moreover, network layer server selection procedures cannot take into account an actual mesh transmission path length. Such approach can lead to inefficiently long transmission paths and dynamic organization of mesh network tends to make such paths very unstable which reduces reliability of methods based on actual testing of transmission parameters.

The scenario where application layer servers are located within the IEEE 802.11s mesh structure may seem to be not a very popular solution. However, closer analysis of the problem indicates a number of advantages of such approach.
The most common approach to deploying application servers in relation to a wireless access network today, is to connect the servers to a wired infrastructure, which in turn is used to provide internetwork connectivity for a wireless access network. However, we must take into account the fact, that such a wireless access network consists of a number of wireless access points, each providing 1 hop access to the wired infrastructure for its connecting clients. As such, the popular

scenario is in keeping with popular service detection and server selection mechanisms' requirements.
In case of an IEEE 802.11s MBSS network and its requirement that only a single mesh gate can remain active between the MBSS and a particular external network (due to RSTP activity as described in Section 3.8.3), such server placement policy will result in both unnecessarily long paths within the MBSS and traffic concentration in the vicinity of the active mesh gate.
An alternative of placing each server in a separate Bridged LAN and connecting it to the MBSS with a dedicated mesh gate results in the same general requirements for deployment as in case of directly connecting the servers to the MBSS, but brings more complication to the system structure. Additionally, it also does not provide any advantage concerning a server selection, as the MBSS is still threated as a single LAN network bridged to the one where the server is located, and as a result only one layer 3 hop (or two layer 2 hops) away from any client in the MBSS.
The same limitations will apply even in case of deployment of the Parallel Mesh Gate Group interworking method, proposed in later sections, which allows for more than one mesh gate to be active between a given MBSS and a single, external Bridged LAN which shortens mesh paths but still does not provide a mesh-aware server selection solution.

The cross-layer solution proposed in this Section is dedicated to a task of efficiently performing a service advertisement and discovery within the IEEE 802.11s MBSS boundaries, complete with the preferred server selection. Its deployment should help clients of the advertised service located in MBSS stations to:

- minimize the time necessary to access the service initially,
- provide them with selection of preferred servers, taking into account current transmission conditions within the MBSS,
- minimize number of message exchanges required for the client to perform service discovery and access procedures,
- provide the client with information which can be used to make a decision of MBSS-level path re-discovery or changing an access server during service access,

The proposed solution will also reduce the resource consumption of the MBSS by preventing the unnecessary long path from being established.

To fulfill this goal, the proposed mechanism will allow application level services and servers to proactively advertise the service they are offering using layer 2 mesh management mechanisms. Such approach allows a mesh structure aware dissemination of information about available services and facilitates a selection of the most appropriate server for a given client. Additionally, application servers can include elements such as, for example:

- server load information,
- information about supported access methods, authentication schemes and other client requirements,
- an initial configuration information for connecting clients

in advertisement messages, providing further information useful in server selection process and possibly resulting in reduction of initial service access time.

5.1.1 Compatibility with DNS Service Discovery (DNS-SD)

As there is a number of different service discovery solutions already available, intended for various deployment scenarios and network technologies, the first decision to make is whatever any of them is currently popular and robust enough to use its principles in our solution and design it to attain a level of compatibility with it. Such compatibility will be advantageous not only in terms of avoiding

the duplication of already existing functionality, but also can allow existing applications to use the proposed solution without a need for any modifications on their part.

Due to the same overwhelming popularity, which caused the previously described, cross-layer address resolution methods to be designed for compatibility with IPv4/IPv6 protocols, it has been decided that the proposed service discovery solution will be dedicated to the IP network environment.
From the analysis of currently employed solutions of this type, the most popular robust and being actively developed is the DNS-Based Service Discovery (DNS-SD) specified in RFC 6763 [103]. It employs a combination of PTR, SRV and TXT DNS records to provide:

- a list of instances of a particular service in a given DNS domain,
- a DNS name of a server providing a particular service instance,
- additional information concerning the service, possibly facilitating the process of accessing it.

Combined with a standard DNS support for A/AAAA records, the chosen server name can be translated into IPv4/IPv6 address, providing a complete ISO-OSI layer 3 information needed to access the service.

According to DNS-SD rules, a service instance is uniquely identified by a Service Instance Name, defined as a concatenation of a DNS domain name, a service name and a instance name within the service, separated by dot (".") characters :

```
Service Instance Name = <Instance>.<Service>.<Domain>
```

Such a name follows the DNS hierarchical name structure and provides similar advantages in creation of a distributed database or querying information relevant to a particular DNS domain.
The Instance element identifies a particular instance of the service, for example a specific printing device from among a set of such devices providing a printing service of a particular kind. The instance element can take as much as 63 octets and can contain any character supported under Net-Unicode [122] specification (with exception of ASCII control characters [123]).
The Service element identifies the particular service and is composed of two parts, each starting with an underscore ("_") character:

- the name of the service defined following the rules specified by RFC 6335 [124],
- an indication of the transport layer type used by the service – with "_tcp" being used for services employing TCP transport protocol, and "_udp" being used for all other protocols.

The Domain element defines the DNS domain for which a particular service instance is advertised.

This Service Instance Name is then made available by means of an SRV DNS record [112], which maps it to the following set of fields:

- Priority (16 bit) – a number in a 0-65535 range, used in a simple failure recovery mechanism: a client must first try to use server indicated by SRV record with the lowest priority value, and only if it is not reachable, then the one with higher priority value can be used.
- Weight (16 bit) – a number in a 0-65535 range, used in a simple server selection mechanism: from the servers indicated by entries with the same priority, a chance of selecting a particular one should be directly proportional to its weight value.
- Port (16 bit) – a transport layer service port of the service instance on the server indicated by Target field,
- Target (variable length) – an FQDN DNS name of the server providing the service instance.

As the SRV record returns a DNS name of the server, an additional query to obtain a corresponding IP address is often required, although the developers are encouraged to automatically provide a relevant A or AAAA records in an Additional Data section of DNS Responses for SRV queries.

While the SRV record provides information allowing a server of a particular service instance to be contacted through the network, it is also possible to provide client with additional information regarding the service using a TXT DNS records. Such records map a Service Instance Name into a text data field following a variant of a Key/Value Pair (KVP) format. The maximum length of the field is limited to 65535 bytes, but it is currently intended for to be kept under 200 bytes to be extended to 400 bytes (to fit in a single, standard DNS message as defined in RFC 1035 [106]) if necessary. It is absolutely not recommended for the field to exceed 1300 bytes (as such DNS Response would not fit within a standard Ethernet frame of 1500 bytes).
The data in the text field is composed of key/value pairs of he the length not exceeding 255 bytes including its key name and delimiting equality ("=") character. Each such pair starts with a key name, limited to characters of printable US-ASCII (as defined in RFC20 [123]), terminated by the first equality character encountered. The value part starts after the delimiter and is processed as an opaque binary data block, allowing a wide variety of information to be passed. Each of key/value pairs is preceded by a single byte indicating its length in bytes.

To access a specific instance of the service, known by its Service Instance Name, a client queries the DNS for a relevant SRV and TXT records. As a result, it obtains a list of SRV records, containing FQDN names and transport layer ports of the service providing hosts. The TXT record provides additional information about the service. If more than one SRV record is returned, the client must take into account the Priority and Weight fields in choosing the SRV record to use.
When the preferred SRV record is selected, its FQDN is translated to a corresponding IP address (performing an A and/or AAAA DNS query if necessary) and the connection to the server is made (which may require an ARP resolution to obtain a MAC address corresponding to a chosen IP).

However, it is often the case, that the name of a specific service instance is not known. To obtain it, a client will query a DNS for a PTR record corresponding to a name defined as: <service>.<domain>
Such a query will return a list of Service Instance Names for a particular service in a specified DNS domain, allowing the client to perform the server selection procedure described above.

The DNS-SD mechanisms can be deployed in both classic (client-server) or multicast DNS environment, in the latter case being capable of offering a zero-configuration service discovery for client on the local link.

Because of robustness of the data format used and the fact that the DNS-SD is a currently preferred method of performing service discovery tasks in today's internetwork, it has been decided to adapt its basic data structures and design the IEEE 802.11s-specific mechanism proposed here for easy integration with the DNS-SD.
Such a decision is in keeping with IEEE 802.11s approach emphasizing the need for seamless integration of MBSS networks into compound network systems and will allow application layer services to use the new service advertisement/discovery mechanisms with a minimal integration effort.

5.1.2 Information dissemination mechanism

To allow the servers to advertise their presence in the intended manner, a new type of message should be defined – a Higher Layer Service Advertisement (HLSA) message. It is to be generated by active application servers and contains information of content and format based on the popular DNS-

SD mechanism described above and thus will contain all information necessary for a client to perform a service discovery and select a particular server according to DNS-SD rules.
However, DNS-SD being a service discovery mechanism intended for ISO-OSI layer 3 connectivity in classic, wired network system, it does possess all the already described limitations of such solutions. Moreover, the server selection mechanisms contained therein (priority and weight values) are designed for recovery from server failure and load balancing in high-reliability and resource rich environments. To perform adequately in an IEEE 802.11s MBSS they need to be extended to take specific characteristics of such an environment into account.

For this purpose the DNS-SD-based HLSA message content should be extended by including an information describing current transmission conditions between a server generating the advertisements and a client receiving them. Additionally, as the proposed mechanism is intended to function in a proactive manner and may require a transfer of medium-sized messages, it is of significant importance to choose a resource-conserving message distribution scheme. Fortunately, the transmission of HLSA messages does not need a strict time guarantees.

Analyzing the above requirements and existing IEEE 802.11s proactive information distribution mechanisms, it seems that a HWMP proactive Root Announcement (RANN, described in more detail in Section 3.7.3.2.2) is a good solution for the task of distributing HLSA information.
In its standard version, it is used to proactively inform mesh stations about the metric of a best mesh path available to them leading to a chosen root station. The RANN messages (in form of RANN Information Elements) can be distributed using either dedicated HWMP Path Selection frames or by including it in Beacon management frames periodically generated by all mesh stations. Moreover, the propagation of RANN IEs through the MBSS is performed with relaxed requirements concerning the delays at intermediate stations, as they are not obliged to resend the received message as quickly as possible (which is the case with other frame types), but are allowed to introduce an arbitrary delay.

By making the server a RANN root station and extending the advertised information by supplementing the standard RANN IE with the HLSA message encoded in HLSA IE detailed below, receiving stations will obtain both service/server information corresponding to this provided by DNS-SD method and a current metric of a best path to a particular server – providing receiving clients with an assessment of expected quality of data connectivity with the indicated server of a particular service.
Moreover, we should remember that while a RANN IE advertisement does not results in creation of transmission paths, it provides receiving stations with a path information allowing them to use a RANN-assisted, strictly unicast path selection procedure to quickly establish such a path to the advertising root station (see Section 3.7.3.2.3).

When performing a joint RANN/HLSA advertisement with use of dedicated HWMP Path Selection frames, it would be sufficient to include the new HLSA IE in their data field following the standard single RANN IE describing its originating root station. Such HWMP Path Selection frame would be recognized by all MBSS STAs (including unmodified stations) as a RANN message and processed accordingly. The non-standard HLSA IE would be ignored by unmodified stations. The stations modified to support the HLSA mechanism would additionally process the HLSA IE and combine its information with the information provided by the preceding RANN IE from the same HWMP Path Selection frame.
However, as RANN advertisement can also be performed by including multiple RANN IEs in a single Beacon frame, a mechanism able to link a given HLSA IE to a particular RANN IE is required. As the RANN IE identifies its sending root station by providing its MAC address and because all services provided by a server within an MBSS will also require their client to use this address, it can be

provided in HLSA IE to both provide receiving clients with a necessary information required to access the service and create association with a relevant RANN IE.

When using the RANN mechanisms for service discovery, it is also advisable to take advantage of its TTL-based dissemination limit capability, which allows for the message to be transmitted only a limited number of hops. It is often the case, that it is possible to assess the maximum transmission path length still enabling the service to be provided with an adequate quality. By setting RANN and HLSA IE's TTL fields appropriately, the server's service advertisement can be limited to clients likely to be able to access the service it provides with satisfactory quality. The method will also lead to conservation of the MBSS resources, as both the advertisement itself will be limited spatially and clients will be prevented from choosing servers requiring the use of long mesh paths.

As an alternative to a RANN-based HLSA dissemination, a proactive PREQ mechanism can be used instead. However, there are several disadvantages to such approach. The proactive PREQ mechanism (described in Section 3.7.3.2.1) can use only dedicated HWMP Path Selection frames to transmit the advertisement and requires the receiving stations to process and resend it without any delay (like a traffic to be forwarded) which is unnecessary in this case and makes the advertisement compete for resources with user traffic. Additionally, the proactive PREQ mechanism not only provides all receiving stations with a metric of a path to the root, but also requires them to update their forwarding information relevant to reverse path towards it. Such requirement can be both resource intensive and disrupt the currently active traffic flows by altering their mesh paths.

5.1.2.1 Advertisement message format

As the method proposed here is intended to function in proactive manner and retain a basic compatibility of its data structures with the DNS-SD solution, the format of its messages contained in HLSA Information Elements is going to require the following elements:

- The SRV record which in turn is composed of:
  - Service Instance Name (variable length, contains a terminating marker),
  - weight (16 bits) and priority (16 bits) information,
  - transport layer port number (16 bits),
  - FQDN of the server (variable length).
- The FQDN to IP address mapping information (32 or 128 bits depending on IP protocol version).
- The IP address to MAC address mapping information (48 bits). This address will also be used to link the HSLA IE to a relevant RANN IE as described before.

Such information set can be easily generated by the server based on its DNS-SD information supplemented by fundamental information regarding its network interface. At the same time, it contains all information necessary to establish a network connectivity with the server.

Taking into account the overall mandatory rules regarding IEEE 802.11 Information Elements, the necessity of providing a sufficient information for the receiver to decode the message containing variable length fields and the need to minimize the IE length, the proposed format for HLSA IE is as shown in Fig. 109.

Fig. 109 Higher Layer Service Adverisement Informaton Element (HLSA IE) structure

The IE structure begins with the usual mandatory fields required by the IEEE 802.11s standard (and described in Section 4.1.3.1). The IE Type field value indicates that the IE is of HLSA IE type (value 0x05 as specified in Table 6).
The remainder of IE structure contains HLSA-specific fields. Despite the requirement of compatibility with DNS-SD data structures, it does not seems necessary to directly include the DNS SRV resource record in the HLSA IE, as many if its fields are redundant in this situation and will unnecessarily increase the size of HLSA message. With only DNS Resource Record Class (2 byte field) defined being "Internet" (value 0x0001) and the knowledge that we are encoding the information from the SRV Resource Record Type (2 byte field), these fields can be omitted. Moreover, with appropriate encoding, we are able to omit the Resource Data Length also.
In this situation, the first of the HLSA-specific fields present in the HLSA IE is a Service Instance Name, allowing the receiver to identify the service instance being advertised and decide if further processing of the message (other than retransmitting it) is necessary. The Service Instance Name is encoded using the standard DNS name notation, which allows the receiver to find the end of this variable length field without additional information.
Following are Priority and Weight fields, each of 2 byte length, copied from DNS-SD information, for purposes of compatibility and to allow a degree of an administrative control over the server selection, as described in their short description in the previous section.
The next is a second variable length field (Host FQDN), containing an FQDN of the advertising server. In contrast with a general DNS Resource Record format, the fact that we are only allowing an FQDN here instead of general DNS Resource Data (RData), allows us to disperse with RDLength field used to indicate its length. Instead we, one again, utilize a standard DNS name notation.

The above fields allow the receiving client to perform a service discovery and server selection according to rules of DNS-SD. The remainder of the HLSA IE, will extend this ability to cover the IEEE 802.11s mesh-specific aspects of the process.

The first of them contains a MAC address (6 bytes) of the server performing the advertisement, allowing for an easy linking of the DNS-SD-specific information with a mesh path metric information obtained from a corresponding RANN IE. The knowledge of the MAC address of the server will also be necessary for a possibly (if the server is selected by the client) following path discovery process and eliminates a need for an ARP/Neighbor Solicitation address resolution process, already mentioned in the description of cross-layer address resolution methods (Section 4.1.2).
The following IP Version (4 bits as defined in IP packet format [95]) and IP Address (4 or 16 bytes depending on IP version) field provide the receiving client with an IP address of the sending server, required for establishing an ISO-OSI layer 3 communication with it. In case of a standard DNS-SD service discovery, it is provided in Additional section of DNS Reply message or requires an additional DNS query to be performed for an A or AAAA record.

The single remaining base element of DNS-SD not yet supported by the proposed mechanism is an ability to provide additional information concerning the service with use of KVP encoded field of TXT record. Due to possibly large amount of data possible to be provided in such way (up to 64 kB) and the size of IEEE 802.11 IE being limited to 255 bytes, it would be cumbersome to allow for a complete, transparent delivery of such data using the proposed proactive mechanisms. Such functionality would require a fragmentation/reassembly procedures using additional IE data fields, at minimum providing an unique identification of the fragmented message, a fragment identifier and a total number of fragments. At the same time, an ability to proactively broadcast such a amounts of fragmented data using the methods clearly intended for transmission of small, self-contained messages would negatively impact both efficiency of the proposed solution and the mesh network.
In this situation, while implementing the DNS-SD TXT record support, we should take into account the fact that its specification intends the record to provide non-critical, supplemental information, which should not be necessary for a client to access the service. An original list of KVPs of the DNS-

SD TXT record should be filtered to limit the size of data to be included in HLSA IE. The method of such selection is outside the scope of this specification and is most likely to be application specific. However, as a means of preventing errors resulting from attempts to include oversized TXT information in HLSA IEs, it TXT field should accept information on a single KVP basis, until the IE's size limit is reached. The first KVP impossible to be fully included in the IE and all subsequent ones should be left out.

5.1.3 Expected advantages

The described HLSA IE combined with information obtained from a linked RANN IE, provides the receiving client with a complete information necessary to generate a list of services and relevant servers available, complete with a Priority/Weight and mesh path (metric and mesh hop length) information required for a DNS-SD-compatible and mesh-aware server selection.
Moreover, the client also obtains information about the IP address corresponding to the server's FQDN and about the MAC address corresponding to the above IP address, by processing a single RANN/HLSA advertisement.
In effect, the described proactive procedure provides not only a mesh-aware server selection but also all advantages of the cross-layer name resolution procedure described earlier, for the connection establishment process with the chosen server.
Additionally, the TXT field can be used to convey additional parameters of the specific server, such as, for example, its expected performance or a current load level, to be taken into account during server selection process.
As a result we can expect a number of valuable advantages, such as:

- a significant reduction of initial service access delay for connecting clients,
- easy selection of the nearest available servers resulting in shorter transmission paths, providing both good and stable transmission parameters and significant conservation of network resources,
- reduction of necessary network traffic generated by higher layer network mechanisms, such as (in case of IP network): DNS request-response, ARP broadcast request-reply, etc.

With the additional functionality of the RANN procedure, which enables the use of an unicast selection of path to the advertising server (root station), the proposed procedure is a comprehensive solution facilitating efficient access to a set of high layer service providing stations located within a mesh structure.

5.1.4 Experiments

To verify the operation of the described proactive service discovery procedure and allow an easy comparison with results obtained for the standard and previously proposed cross-layer methods, a simulation scenario similar to the one used to verify the previous method has been performed:

- the MBSS of 30 stations capable of communication (in case of network segmentation, the MBSS topology generation has been repeated),
- topology of the MBSS generated using 4 different methods (described in 3.8.5): dense grid, sparse grid, dense random and sparse random,
- 11 different levels of traffic load have been considered, generated by activating 0 to 10 of 1 Mbit/s UDP traffic sources located at randomly chosen mesh stations, with a randomly selected traffic destinations,
- a 100 simulation runs for each topology type and traffic load combination.

From the above 30 STAs, ten were randomly selected to host non-interactive video streaming service.

The system has been allowed a 10 s warm up period, allowing mesh mechanisms to create a functional MBSS system and servers to commence their HLSA advertisements.

During each simulation run, a randomly chosen STA attempted to discover a server and access the video streaming service by using:

- the standard mDNS DNS-SD method, employing it in a manner which minimizes its latency – by accepting the first received response to its service related query,
- the reactive, cross-layer mDNS-SD method described in chapter 4.2, also selecting the first received response,
- the cross-layer, proactive service advertisement method proposed in this chapter.

As before, the timeout values of ARP and mDNS protocols, have been set to the minimal values allowed by the respective standards – 1 s for ARP and 2 s for mDNS.

The latency of each method, measured from the moment the STA initiates service access procedures to the moment when it is able to send a request for a specific content (the server is selected, its IP and MAC addresses are known and a mesh path is established) are presented in Fig. 110 and Fig. 111.

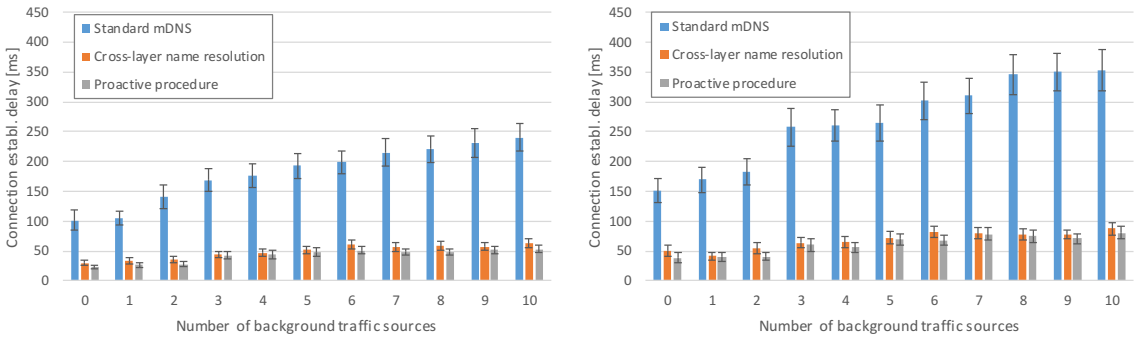

Fig. 110 Latency of a server selection process in the dense grid (left) and dense random (right) mesh structures

As can be seen in Fig. 110, the proactive procedure provides a significant reduction in the process latency compared to the standard mDNS-SD method, in case of dense mesh structures. It is only to be expected, as the STA proactively constructs and maintains a list of servers with their respective IP/MAC addresses and Airtime Metric values for the mesh path which will be used for communication. However, to conserve the resources of other stations in the MBSS, the HLSA procedure does not require all receiving stations to create/update their forwarding information for the advertising server. In presence of such a requirement the latency of the process would be equal to 0, however, all stations would be required to maintain mesh paths to all application servers present in the same MBSS. As it is, the proactive procedure utilizes the RANN-assisted unicast-unicast path discovery (see 3.7.3.2.3), which allows it to establish a mesh path to the selected server without the need for a broadcast transmission. This ability gives it to obtain a slight gain over the previously proposed cross-layer name resolution method, which also requires only a single exchange of messages, but the first of them (DNSREQ) is a broadcast one.
The advantage of both proposed methods over the standard procedure (requiring 4 broadcast and 2 unicast messages) is clearly visible and described at greater length in Section 4.2.3.

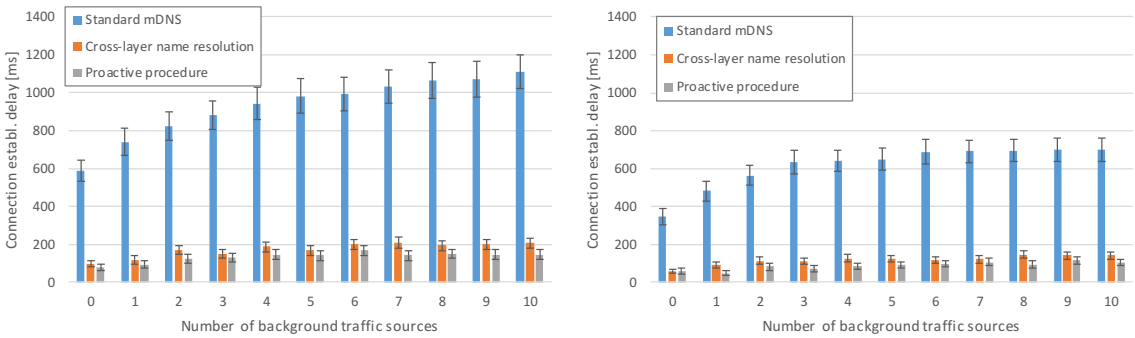

Fig. 111 Latency of a server selection process in the sparse grid (left) and sparse random (right) mesh structures

The same advantage is even more pronounced in case of sparse network structures due to their lower quality links and a higher probability of broadcast transmission failure (Fig. 111). Because of that characteristic, the proposed proactive procedure with its strictly unicast communication, shows a latency consistently lower than even the previously proposed reactive method.

Due to the fact, that in the presented scenario both the standard and the reactive cross-layer procedure is attempting to minimize the latency of the process, they both select the first received reply as the preferred server, based on the assumption, that the quickest response indicates the best available traffic conditions. As messages exchanged during the discovery procedure are subject to a message loss (especially in sparse network structures), that can lead to omitting a server due to a random event, which can negatively influence the resulting MOS score of the service.

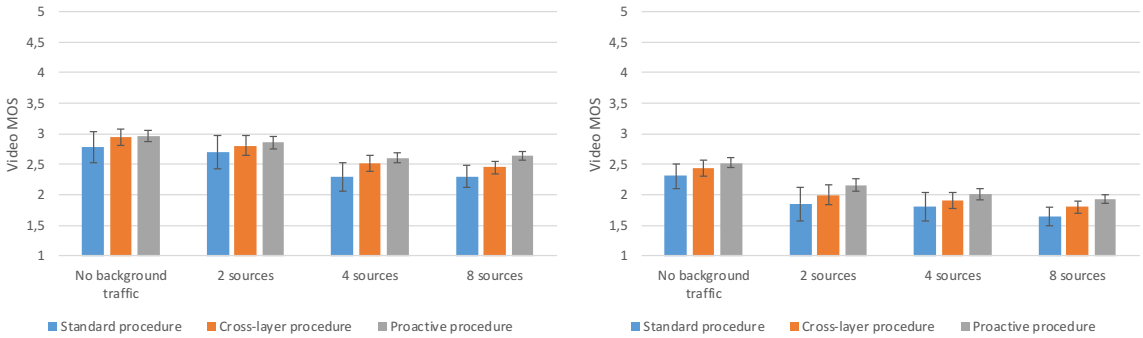

Fig. 112 Video MOS scores for servers selected using different procedures in the dense grid (left) and sparse grid (right) mesh structure

In contrast to the standard and the previously proposed reactive procedures, the proposed proactive method utilizes an Airtime Metric values reported by IEEE 802.11s mechanisms to assess the expected communication quality with a particular server. Additionally, its proactive operation prevents one-time loss of a message from influencing the selection in a radical manner. As show in Fig. 112, this allows for a slight increase of the mean MOS of a non-interactive video streaming service.

It should be noted, that the reactive-cross layer procedure could also utilize the Airtime Metric as its server selection criteria, but at a cost of increased latency, due to a necessity of collecting responses from multiple servers, without a prior knowledge of their number. However, such a solution would not protect the method from selection errors due to messages lost during the reactive server discovery.

6 Interworking extensions for IEEE 802.11s mesh network

As already demonstrated in Section 3.8.4, a wireless network utilizing the popular IEEE 802.11 technology has a strictly limited pool of radio resources to be shared between its clients. Moreover, due to employment of contention-based medium access method, the utilization efficiency of these resources is relatively low, especially when a sizable group of wireless clients simultaneously contends for medium access.
These problems are present even in case of a simple PtMP access networks, but in case of mesh systems, where a concentration of client devices is required for the mesh network creation, the conservation of radio resources and minimization of intra-mesh interference become matters of primary importance. At the same time, the analysis of interactions between transmission attempts made by devices in a wireless mesh environment is not straightforward, as it depends on a wide range of factors, such as:

- relative position of devices,
- propagation conditions between each pair of devices,
- transmission methods and parameters employed by specific devices: power, modulation, antenna properties,
- resulting communication and interference ranges of mesh devices.

Even with a complete knowledge of the abovementioned elements, it is not possible to accurately assess the level of service provided to users in a particular deployment, as the above interactions will occur depending on actual traffic patterns present in the WMN at a given moment, which in turn depend on:

- end-user services used in the mesh with their specific architecture, configuration and requirements:
  - peer-to-peer or server-based,
  - location of servers and clients,
- resulting traffic flows with their specific source and destination addresses, traffic volume and time characteristics,
- resulting mesh transmission paths created by path selection mechanisms, which depend on the protocol and metric used for the purpose.

Due to the fact that IEEE 802.11s is a single channel mesh network, designed to be possible to deploy with popular devices equipped with only a single radio interface, the radio resources are strictly limited and susceptible to both inter-path and intra-path interference, as the simple and efficient technique of configuring transmission paths through subsequent links which use orthogonal frequency channels to eliminate the latter is not possible to employ.

As a result of the quantity of the above parameters and their interactions, a significant number of optimization methods have been developed for various combinations of a particular network structures, parameters to be optimized (for example throughput, communication delay, power consumption, etc.) and specific disrupting factors (for example: high node/link failure rate, node mobility, external RF interference). These methods mainly include new or modified path discovery mechanisms, link/path metrics or methods to change IEEE 802.11 into multichannel mesh. However, they almost exclusively address only a very specific case of a mesh network deployment.
Yet, we should keep in mind that IEEE 802.11s is a general use technology, intended to be employed in a manner similar to the popular WiFi Access Point-based network – in a variety of deployment scenarios and supporting an unknown, but high and still growing, number of different services.

In the situation when there is a considerable number of case-specific optimizations proposed, it has been decided that an attempt should be made to provide some general solutions, which would offer an improvement in transmission quality in a broad spectrum of deployment scenarios.
It has been observed, that while the IEEE 802.11s technology is also a good choice for creating isolated, ad-hoc network systems, it can be expected that most of its deployments will have connections to a an external infrastructure. Such infrastructure will most often be a wired LAN network, but other solutions (like MAN or WAN wireless systems) are also possible. It should be expected, however, that such an external infrastructure installation will either have bandwidth resources exceeding that of the MBSS, will be able to provide a more predictable level of service or both.

The IEEE 802.11s technology should be expected to be well suited for such an environment, as its mechanisms allow for a significant flexibility in path discovery operations (as described in Section 3.7), taking advantage of both optimized paths created on demand by reactive routing procedures and fast connection establishment to critical mesh locations, provided by proactive solutions. Moreover, interworking with outside networks is a subject of much attention (as presented in Section 3.8), allowing seamless integration of mesh network with other IEEE 802 layer 2 ISO-OSI systems.
However, while IEEE 802.11s mesh network can provide connectivity with destinations located in external networks, it is unable to use resources provided by these networks to support connectivity between intra-MBSS destinations. Furthermore, it is unable to utilize multiple mesh gates connecting MBSS with the same external network segment (RSTP protocol disables frame forwarding in all but one – see Section 3.8), resulting in formation of unnecessarily long paths within the MBSS (as mesh gates conveniently located near a particular station are likely to be disabled by the RSTP).

The modifications proposed here are intended for usage scenarios where the IEEE 802.11s MBSS network is deployed with associated external infrastructure, preferably a high performance wired technology. The mentioned infrastructure can be a dedicated system designed to support the mesh-based wireless access network or simply a part of a compound network system of which the MBSS is a part. In case of such deployment scenario, the MBSS will most likely have multiple potential contact points with the wired infrastructure of which only a limited number will be active at a time due to the RSTP activity at mesh gateways.
Of course, it is possible to design the mesh-based access system in such way, that it will be administratively divided into a number of separate MBSS partitions, to ensure that most of wired-wireless connection points will remain active and the system will provide mesh-based connectivity for users while keeping mesh paths within a reasonable length.
It is not difficult to see limitations of a such static, administratively controlled solution used in deployment of technology which is intended to provide a self-organizing, auto-configuring and client-device dependent service:

- inter-MBSS connectivity between wireless stations is often inefficient, as it must be passed through an external infrastructure even if direct wireless communication would be possible,
- coverage provided by each MBSS is difficult to assess, as it is dependent on a number, capabilities and spatial distribution of participation client devices,
- with unpredictable coverage of composing MBSS networks, a compound coverage of the resulting network system is likely to be poor (coverage-holes effect between the MBSS systems) and difficult to predict and monitor,
- failure recovery capabilities of the compound network will be limited, due to removal of possible wireless links between client devices as they are distributed over a number of independent MBSS structures,
- client devices need to be configured to access and roam over a number of independent MBSS networks.

It is evident, that such an attempt to circumvent the limitation of a single traffic exchange point between an IEEE 802.11s MBSS and an external network nullifies most of the mesh network advantages. The extended coverage, ability to respond to device and link failures, simple configuration of client devices, ability to use mesh as a technology integrating multiple access networks (Fig. 48) are all reduced or lost. Adoption of such approach would be severely limiting especially in larger access networks and presence in of services hosted by wireless clients or distributed services extensively using client-to-client communication.

To allow an IEEE 802.11s mesh networks to make much more efficient use of connected external infrastructure without introducing the, hard to accept, limitations listed above, two modifications of IEEE 802.11s mesh path discovery and forwarding protocols are proposed, which can be summarized as follows:

- introduction of ability for a mesh station to use mesh gates which would normally be disabled by the RSTP protocol,
- introduction of ability to form a peering relationship between mesh gates, using external network as transmission medium.

The first proposition aims to offset the negative results of employing the standard RSTP procedure, which results in a complete deactivation of mesh gate mechanisms in all potential mesh gate stations between a given MBSS and a specific section of a Bridged LAN, save for a single one. By employing the proposed procedure, multiple mesh gates can remain active and take part in forwarding of the network traffic, resulting in both shorter mesh paths for inter-MBSS traffic and dispersing it over a set of mesh gates instead of concentrating in the vicinity of a single one.

The second proposed modification, External Mesh Peering, allows the use of fast wired connections, frequently present between mesh gates connected to fixed infrastructure, to form transmission paths between intra-MBSS destinations. Due to the fact that Airtime Link Metric for such a transmission link will be small (due to a higher throughput and lower error rate than that provided by the IEEE 802.11 wireless transmission technology), use of such links will be preferred. It is highly probable that such ability will result in significant reduction of the average path lengths for intra-mesh transmissions. Of course the precise gain depends on the presence of mesh gates able to communicate with use of external network and distributed through the MBSS in more or less uniform fashion. In fact, for the standard mesh deployment in large, multi-company office building, utilizing about 0.5-1 mesh gate for a single floor, the described mechanism will tend to reduce average mesh path lengths to 2-3 hops - which makes it suitable even for real-time multimedia communication.

6.1 Mesh Gate Groups

The problem of integrating a self-organizing mesh network within the compound structure of a Bridged LAN (as defined in IEEE 802.1D) is not a simple one if we take into account its dynamically changing structure, limited resources, contention-based operation and the resulting complexity of its mechanisms. In comparison with popular wired ISO-OSI layer 2 network technologies, the IEEE 802.11s mesh network should be considered a complex and not deterministic environment.
Creators of the IEEE 802.11s specification decided to solve the problem by completely isolating the internal mechanisms of the MBSS from the external network systems by employing mesh gates – fully functional mesh STAs, additionally equipped with external network connections and able to provide an IEEE 802.1D-compatible interface for these systems. As a result, an IEEE 802.11s MBSS is visible to external networks as a single, data link layer LAN connected to other LANs with use of 2-port bridges (see Fig. 113).

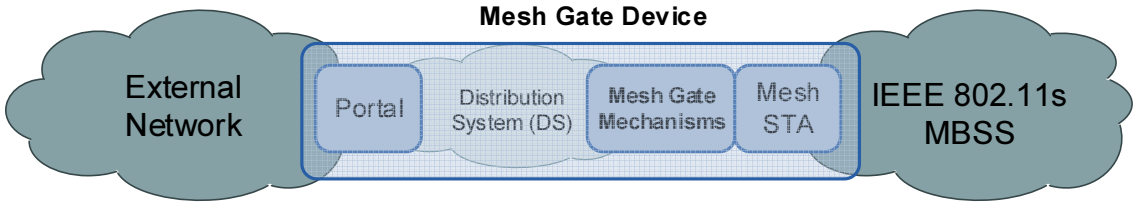

Fig. 113 Mesh gate as a logical element of an IEEE 802 system.

Such a solution greatly simplifies the task of network integration, but at the same time the complex, changing structure of an MBSS is interpreted using the procedures designed for a simple, static one typical for a wired LAN network.

Following the above approach, when an MBSS is integrated with a compound Bridged LAN consisting of many LAN networks interconnected at ISO-OSI layer 2 by means of bridges (or switches), measures must be taken to prevent creation of transmission loops. In case of IEEE 802.1D-compatible systems, the solution deployed for this purpose is the Rapid Spanning Tree Protocol (RSTP) described in more detail in Section 3.8.3. The use of RSTP is also directly mentioned in IEEE 802.11s interworking specification as a preferred mechanisms for the task.
The RSTP selects the root bridge from all bridge devices within the compound Bridged LAN and forms a communication tree spanning all its comprising LAN networks. The tree is created by selecting bridge ports which are necessary for its operation and disabling (by changing to discarding state) all other ports. The resulting communication structure provides only a single transmission path between any two of its comprising LAN systems, thereby making transmission loops impossible.
The protocol is designed to be fast reacting, robust and backwards compatible with the previously dominant Spanning Tree Protocol. It is indeed commonly and successfully used in a wide variety of compound LAN systems. However, it is clear that the design of its mechanisms it based on assumption that a LAN network can be interpreted as a single, uniform entity, regardless of specific entry and exit points chosen for traffic transmission.
The above assumption allows cost values (used in a tree construction) to be assigned at the level of specific LAN networks, not bridge ports. Moreover, in case of the need to select between otherwise equivalent devices or ports within the same network, a MAC address value is used as a tie-breaker. While the approach does not induce a significant inefficiency in case of popular wired networks, the same cannot be said for its deployment in a wireless mesh environment, as shown in Fig. 114.

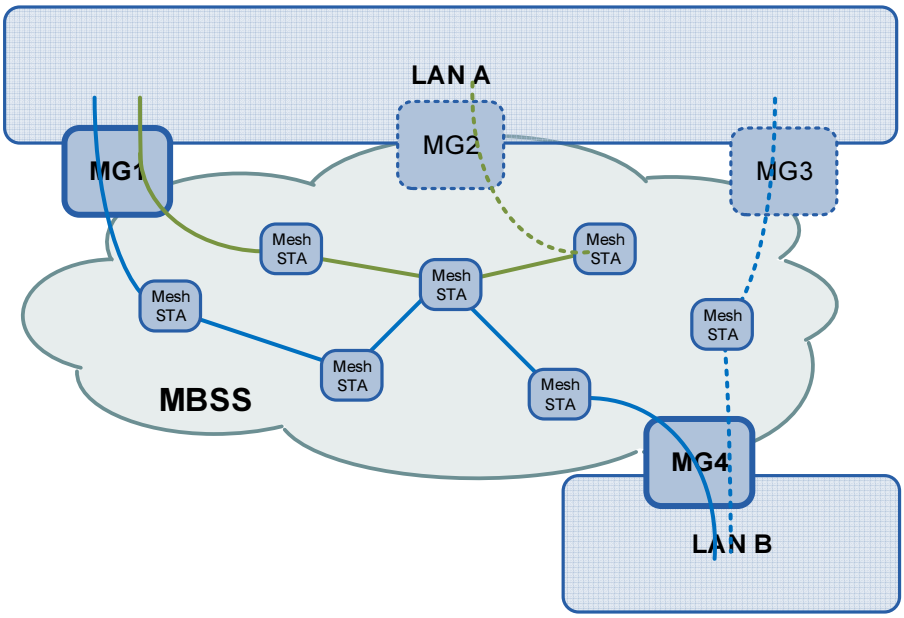

Fig. 114 RSTP deployment in an MBSS environment

With mesh gates being interpreted as 2-port bridge devices by the RSTP and multiple of them connecting LAN A with MBSS, only one of them can become a designated bridge for the MBSS and retain an active mesh port. As all of them are connected to the same LAN network, root path cost value will be the same for all of them, making their MAC addresses a deciding factor.
Assuming that the leftmost mesh gate (MG1) has the preferred MAC address, its mesh port will assume the forwarding state, while mesh ports of all other mesh gates between LAN A and MBSS will be set to discarding state. From the perspective of the MBSS, such mesh gates switch to inactive state becoming common mesh stations as they no longer possess a connection to outside network. As a result, any mesh traffic addressed to destinations in the Bridged LAN reachable through the LAN A will be required to use the single active mesh gate, which has been selected based on its MAC address with no regard to other factors, such as, for example an average mesh distance between the MBSS stations and the mesh gate. Resulting unnecessarily long mesh paths will provide a poor quality of service while causing a significant intra-path interference over the majority of the MBSS area.
The same mesh gate will also be used in case of a transit traffic entering the MBSS through mesh gate MG4 from LAN B and subsequent LAN networks located further down the spanning tree branch with similar results, despite the presence of conveniently located mesh gate MG3.
While it is theoretically possible to influence the selection of a particular mesh gate as a designate bridge by RSTP mechanisms, which could help by allowing the transit traffic to be forwarded along the MG4-MG3 path in this particular case, we must remember that the structure of MBSS is a dynamically changing one which makes solutions based on a static configuration cumbersome at best and possibly leading to even less desirable results.

From the above example, it is clear that in case of a mesh network the specific location of the bridging device both within the mesh structure and spatially relative to other stations is of significant importance. However, simply introducing a superior method of selecting a designated bridge will bring only limited advantages, as we will still limit the number of mesh gates which can be used to forward traffic. Such limitation can be expected to have a highly adverse effect on scalability of the mesh network, as in spatially larger MBSS deployments a high number of transmission paths will need to traverse a significant distance causing the interference over a large area. Such long mesh paths will also be subject to significant intra-path interference at each intermediate station.
To overcome this limitation, a modification of mesh gate operation is proposed below, allowing all mesh gates within the IEEE 802.11s MBSS to remain active and able to forward a network traffic.

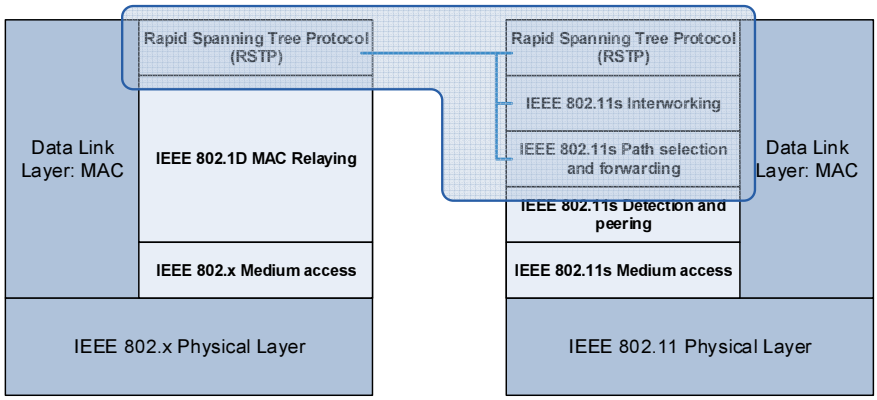

Fig. 115 Mesh Gate Groups solution cross-layer architecture

The proposed solution integrates a number of mechanisms of IEEE 802.11s and external networks as shown in Fig. 115. While all of these mechanisms are located in ISO-OSI layer 2, due to significant complexity of IEEE 802.11s specification (which incorporates mechanisms more often found in ISO-OSI layer 3, such as transmission path selection in complex multihop environment) a number of separate sub-layers can easily be found in its protocol stack. Moreover, its sub-layers, such as Path selection and forwarding, Interworking and an external RSTP protocol are strongly separated and made to operate with high degree of independence by premeditated design of standard creators (as described earlier, for example, in 3.8.2). In this situation, the proposed Mesh Gate Groups mechanism, integrating two separate elements of IEEE 802.11s specification interacting in layered fashion and an internetwork management protocol, follows a description of a cross-layer integration solution.

6.1.1 Parallel Mesh Gate Groups procedure

As described before, because of RSTP protocol activity, only a limited number of mesh gates can remain active in a given MBSS:

- a single designated mesh gate providing the MBSS communication in the direction of the root bridge of the spanning tree,
- a single mesh gate for each branch of the spanning tree relaying on the MBSS for its communication towards the root bridge.

While such approach makes transmission loops impossible, it can also introduce significant inefficiency in the MBSS operation – a serious problem for a wireless network of limited resources. To prevent the deactivation of possible traffic exchange point between the MBSS and external networks, it is proposed to modify the standard IEEE 802.11s mesh gate procedures by allowing all mesh gates to remain active. However, care must be taken not to reintroduce transmission loops the RSTP has been deployed to prevent.

Procedures proposed below are to be deployed in parallel with the standard IEEE 802.11s/RSTP mechanisms, which means that the mesh gates which would remain active in the unmodified system will still do so and provide the interworking service following the standard rules. Such approach allows the MBSS to both support unmodified client STAs in the standard way and prevent such STAs from disrupting the MBSS and the Bridged LAN by not conforming to the new mechanisms. It should be noted, however, that all mesh gates in the MBSS need to be modified to support new mechanisms, including the ones which retain support for legacy interworking procedures – without this provision, it would be impossible to ensure a loop free operation.

The core concept of the proposed solution is a Mesh Gate Group (MGG) defined as a set of mesh gates belonging to the same MBSS and being able to communicate without using the MBSS in

question – which means they are able to communicate using external network systems, along the spanning tree structure. Each MGG is uniquely identified within the MBSS by a Mesh Gate Group Identifier (MGG ID), an 8 byte value compatible with RSTP Bridge Identifier format.
With MGGs defined, modified client STAs will be able to use a proxy information indicating the MGG to which they should deliver the inter-MBSS traffic, instead of a specific mesh gateway. With a number of mesh gates in the indicated MGG, it is possible for such STA to select and use the most convenient one.

As the formation of Mesh Gate Groups and assignment of MGG IDs must be performed for the proposed solution to function, it has been decided to use information provided by RSTP protocol for this purpose:

- all mesh gates which receive RST BPDUs from an external network indicating that one of mesh gates of their MBSS is a designated bridge, belong to the same MGG identified by MGG ID equal to the ID of the indicated designated bridge. Mesh gates are able to identify MAC addresses of other mesh gates of their MBSS due to RST BPDUs being broadcasted in both the MBSS and the external network,
- all mesh gates which receive RST BPDUs from an external network indicating that a device outside of their MBSS is a designated bridge, belong to the same MGG identified by MGG ID equal to the Root Bridge ID.

As the standard interworking mechanisms allow only a single mesh gate in each MGG to remain active and advertise its presence, additional mesh gates of such MGG must advertise their presence using an additional procedure. However, as the proposed solution requires the presence of certain custom mechanisms at client STAs, the new mesh gate advertisement must not cause unmodified STAs to discover the presence of additional mesh gates.
To fulfill this requirement, a procedure based on RANN principles is introduced – a Mesh Gate Group Advertisement (MGGA). The protocol requires a mesh gate to participate in RANN protocol, periodically sending HWMP Path Selection frames with RANN IE as described in 3.7.3.2.3, with Gate Announcement indicator NOT SET. Additionally the gate needs to periodically sent IEEE 802.11 Multihop Action frame, addressed to a general broadcast address (FF:FF:FF:FF:FF:FF) and containing a Mesh Gate Group Advertisement Information Element shown below (Fig. 116).

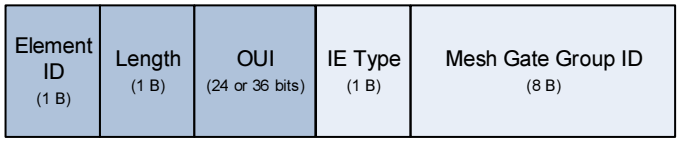

Fig. 116 Mesh Gate Group Advertisement Informaton Element (MGGA IE) structure.

The simple format of the MGGA IE contains:

- Element ID, OUI and IE Type indicating the Vendor Specified MGGA IE,
- MGG ID field (8 bytes) containing the MGG ID of sending mesh gate.

As the MGGA IE is transmitted in a Multihop Action frame, Hop Count and Element TTL fields can be omitted from the IE structure. The frame is identified as MGGA Advertisement frame by value 0x04 in its Multihop Action field.

By using a combination of RANN and MGGA Advertisement messages, each STA within the MBSS obtains a current metric value of a path to each of mesh gates, but only modified STAs are informed about the presence of active interworking mechanisms at indicated devices and their MGG membership. The association between RANN and MGGA advertisements is maintained by comparing MAC addresses contained in Root Mesh STA Address of RANN IE and Mesh Source Address of the IEEE 802.11 Multihop Action frame carrying the MGGA IE.

A modified mesh station should respond to a single chosen mesh gate from each MGG (as identified by MGG ID) by sending an MGGA Selection message, which is identical to MGGA Advertisement message, but transmitted as an unicast Multihop Action frame addressed to the selected mesh gate and identified by Multihop Action field value equal to 0x05. The MGG ID field of MGGA IE should:

- in case of client STAs – copy the MGG ID value received in MGGA Advertisement,
- in case of mesh gate (as mesh gates are also a fully functional modified STAs) – the value of MGG ID should indicate the MGG membership of the responding mesh gate.

By doing so, the STA is selecting such a specific mesh gate as the one it is going to use for inter-MBSS communication through the given MGG, so it should choose the one providing the best expected quality of service, based on path metric and hop distance provided in the received RANN message.
As a result of this procedure:

- each station will obtain a list of mesh gates with each of them representing different MGG,
- each of mesh gates will obtain a list of mesh stations it has been selected by and add this information to a Mesh Gate Group's Station Assignment List (SAL) described below.

While the modified mesh STA should select and respond to only a single discovered mesh gate within a MGG, it should be noted that the alternative choices are retained and can be quickly used in case of a failure of the selected mesh gate.

We should remember, that mesh gates are a fully functional mesh stations and will participate in the above selection process as both RANN/MGGA senders and responders. However, when a mesh gate belongs to a particular MGG, it should choose itself as its selected mesh gate for the particular MGG.

The Station Assignment List (SAL) consists of:

- mesh station addresses,
- their corresponding selected mesh gate addresses within a specific Mesh Gate Group,
- type of the mesh station: modified or standard IEEE 802.11s,
- in case that the station is also a mesh gate – its MGG ID and path metric between MGs, obtained from the RANN element of MGGA advertisement mechanism,
- lifetime of the entry – after which the entry is removed from SAL.

Mesh gates within the same MGG will communicate between themselves to synchronize their SAL lists in the same manner as in case of Proxy Information Database (see 3.8.2.3) to obtain a synchronized, MGG-specific SAL list.
To accommodate the possibility of a STA changing its selected station or leaving the MBSS structure, the mesh gate currently having the STA assigned will remove it from the SAL if its lifetime elapses. The lifetime value is restored to a starting value when the STA responds to MGGA message or, in case of unmodified stations, is found in the MBSS by a mesh path discovery process initiated by a RSTP-selected mesh gate (as described in the following Section 6.1.1.2).

Because the proposed modifications of IEEE 802.11s interworking mechanisms change the information that a mesh STA requires for inter-MBSS traffic delivery from a single RSTP-selected mesh gate address to an identifier of a Mesh Gate Group, the information stored in Proxy Information Database (PID) needs to be extended.
The new database is named Proxy Group Database (PGD) and while the current format of PID is retained in PGD, an additional database field added indicating the MGG which is a proxy for the specified external address. The PGD is synchronized between all mesh gates in the MBSS using the same mechanisms as PID, but utilizing Proxy Group Update (PGU) messages for synchronization of PGD between the mesh gates. The PGU message structure is the same as that of standard PXU, but with the additional MGG ID field is added.

While PGU is employed in place of PXU for synchronization between mesh gates and for updating PGD at modified stations (see below), the PXU is retained for compatibility with standard mesh stations.

As the PGD includes an MGG ID in addition to a MAC address of a mesh gate when indicating an entity responsible for performing proxy functions for a particular external MAC address, when a modified mesh gate obtains a proxy information resulting in necessity of creating or updating a PGD entry, it should:

- if the mesh gate is an RSTP-selected one – include in the entry the MGG ID of its MGG,
- if the mesh gate is not RSTP-selected – include in the entry the MGG ID of its MGG; as a proxying mesh gate address it should provide the address of RSTP-selected mesh gate of its MGG, instead of its own address.

The information concerning the RSTP-selected mesh gate of the particular MGG can be obtained by any mesh gate in the following way:

- if the RSTP designated bridge for the external network is a mesh gate belonging to the MBSS, the address of its MBSS interface should be used,
- if the RSTP designated bridge for the external network is not a mesh gate belonging to the MBSS, the address the MBSS interface of a designated bridge for the MBSS should be used.

As already mentioned, each of the mesh gates is in possession of a complete list of all mesh gates in its MBSS and their respective Bridge IDs due to RST BPDUs broadcasted over the MBSS.

When a proxy information needs to be sent to a STA (as described in the following sections), it must be verified is the STA is a standard or modified one (capable of using MGG ID information). The verification is performed by checking the SAL where the information is directly available, and the proxy information is sent in appropriate form:

- the unmodified STA will receive a standard Proxy Update (PXU) message indicating the MAC address of the RSTP-selected mesh gate which should be used to forward the traffic,
- the modified STA will receive a Proxy Group Update (PGU) message indicating the MGG ID of the appropriate MGG.

6.1.1.1 *Inter-MBSS outgoing unicast traffic delivery*

Following standard IEEE 802.11s rules, when a STA has an unicast frame to send, it will first check its PID information to determine the appropriate mesh destination of the frame. Depending on the location of the specified frame destination address it could be:

- a device identified by the specified destination MAC address and belonging to the same MBSS network,
- an active mesh gate device performing a role of proxy for the specified destination MAC address which is located outside of the MBSS boundaries.

Then a mesh destination address has been determined, the forwarding table is consulted to check, if the STA already has a current mesh path to the mesh destination address. If it does not, the STA will perform a path discovery procedure, which will establish an appropriate path.
However, it is also possible that a destination address located outside of the MBSS is not yet known to the STA nor any of mesh gates. In such case the destination address will be absent both for PID and forwarding table, and the attempt to discover the path towards it will also fail. In this situation, the STA will send the frame to all active mesh gates of the MBSS. The STA obtains the necessary list of active mesh gates due to activity of GANN protocol (described in 3.8.1.1) or inclusion of gate announcement in RANN or proactive PREQ messages originated by a mesh gate (described in 3.8.1.2). All of these methods are based on performing a proactive advertisement of a mesh gate presence.

In case of an MBSS following modified procedures, all mesh gates advertise their presence in such way that only modified STAs can process of their advertisements and interpret them as mesh gate announcements, while a single RSTP-selected mesh gate in each MGG also utilizes the standard method for compatibility with unmodified stations.
Modified stations able to process RANN/MGGA advertisements select a single mesh gate from each MGG based on RANN-provided path information and complete their SAL registration by sending MGGA Selection message.

The main difference between standard and modified STAs is the fact, that the latter use Proxy Group Database (PGD) providing MGG ID of the MGG which is responsible for handling traffic to a given external destination, instead of Proxy Information Database (PID) providing MAC addresses of specific mesh gate which performs this function. This approach allows the modified STA to choose the most convenient mesh gate from within the indicated MGG.

When sending a frame, a modified STA will first consult its PGD (instead of PID) to obtain an identifier of the MGG (instead of a specific mesh gate address) which is proxying for the frame's destination address. If such information is found, it indicates that the address is located in external network and the MGG ID of the appropriate MGG will be obtained. The STA will then proceed to forward the frame towards its selected mesh gate within the indicated MGG.
If relevant information is not available in station's PGU, it will temporarily assume that the destination is located within an MBSS and proceed with intra-MBSS delivery attempt, by checking the forwarding table and if no active path is found, initiating the mesh path discovery procedure. If the destination device indeed belongs to the MBSS the path will be established and the frame delivered. If the destination is outside the MBSS and but is currently proxied by a particular MGG (as indicated by the PGD synchronized between all mesh gates in the MBSS), the mesh gate selected by the particular STA from such this MGG will respond with PGU update and PREP response. The information specifying the mesh gate selected by a particular STA is available in SAL (synchronized between mesh gates of a particular MGG). The STA will include the information in its own PGD table and forward the frame accordingly (to its selected mesh gate from the correct MGG).
However, it is also possible, that the destination is in fact an external one, but as yet unknown to the MBSS interworking mechanisms. In such case the STA will forward the frame to all its selected mesh gates and in effect to all MGGs of its MBSS. Such frame will then be forwarded to external networks.

As in all cases the frame will be delivered to the same specific mesh gate within the appropriate MGG (the selected mesh gate of the particular STA) and then forwarded towards its external destination, the MAC table of an external bridge will indicate the port to which a selected mesh gate of the particular station is connected as appropriate for sending return traffic for such station.

6.1.1.2 *Inter-MBSS incoming unicast traffic delivery*

If we modify the IEEE 802.11s interworking mechanisms to allow all mesh gates to remain active, is highly probable that a frame transmitted through the Bridged LAN along the spanning tree will be received by more than one active mesh gate belonging to a specific MBSS. In such a case, only one of receiving mesh gates should forward the frame, as otherwise a risk of frame duplication and traffic loops occurs.
To prevent such occurrence, when a mesh gate receives a frame from external network two basic decisions must be taken:

- The mesh gate must decide if it should forward the frame or if the task will be performed by another mesh gate.

- The mesh gate must decide where the frame should be delivered within the MBSS.

The above task is a simple one if the destination of the frame is a STA within the MBSS – it is enough to check the Station Assignment List to obtain the information if the STA belongs to the MBSS and which mesh gate is its selected mesh gate. If the SAL indicated that the mesh gate is the one selected by the indicated STA, it should deliver the frame to its final destination. Because the selected mesh gate is used for both outgoing and incoming traffic between the specific STA and external networks within a particular portion (root or a specific branch) of the Bridged LAN, the compatibility with external learning bridge devices is maintained.
If the destination address is not listed in the SAL, it is still possible that it is an unmodified STA belonging to the MBSS, so if the mesh gate is RSTP-selected, it should perform a mesh path discovery for the destination address (as per standard procedure). If successful, it should add such unmodified STA to the SAL with its own MGG ID and mesh gate address (making itself STA's selected mesh gate to emulate the standard IEEE 802.11s procedure) and deliver the frame. If the mesh path discovery fails, the frame is to be considered a transit frame (originated outside the MBSS and with destination also located outside its boundaries).

If the frame has been identified as a transit frame the mesh gate will check its PGD (global for all mesh gates in the MBSS), containing all addresses known by MBSS interworking mechanisms to be external. If the address is found, the ID of Mesh Gate Group through which is can be reached is obtained, and the frame should be delivered to a mesh gate within that MGG to be forwarded correctly. Under no circumstances the frame should be forwarded to external network connected by any mesh gate within the same MGG.
If the address is not found in the PGD, then the location of the address is not known, so it must be delivered to all MGGs except the one to which a mesh gate now holding the frame belongs to, for forwarding to external networks.
Despite the fact, that the destination MGGs have been determined, either by obtaining this information from PID or by deciding that all MGGs should be used to forward the frame to their connected external networks, it seems that both of our initial questions are as yet unanswered. It is still to be decided if the particular mesh gate should forward or discard the frame and if forwarding is required, then to which specific mesh gate the frame should be forwarded.
However, due to the fact that all mesh gates are also fully functional, modified mesh STAs, each of them takes a part in the described RANN/MGGA mesh gate advertisement procedure and gets registered in each MGG's SAL. By accessing the SAL of its own MGG the mesh gate is able to obtain the list of mesh gates of a destination MGG. This information is supplemented by RANN-obtained metric values for paths between all members of its own MGG and all members of a destination MGG. The mesh gate will only forward the frame if it is an endpoint of the path with the best metric of all the paths mentioned above. The destination mesh gate will be the other gate indicated in the SAL entry.

6.1.1.3 Group-addressed traffic forwarding

Both outgoing and incoming group-addressed traffic processing is not modified by the proposed solution. It is forwarded only by mesh gates belonging to an RSTP-created spanning tree structure, according to the standard IEEE 802.1D and IEEE 802.11s rules. It will be flooded through the MBSS, eventually reaching all mesh gates. The only mesh gates which forward such frames from the MBSS to external networks are the designated mesh gate for the MBSS and these of its mesh gates which are designated bridges for other networks – in other words RSTP-selected mesh gates.
The standard method of handling of the group-addressed traffic has been retained, despite the fact that it would be possible to extend the proposed solution to support its optimized delivery. However,

such approach would have resulted in compatibility problems, as the presence of unmodified stations in the MBSS could cause broadcast loops.

6.1.1.4 Compatibility considerations

For the proposed solution to maintain a loop free topology of the Bridged LAN, all of mesh gates in the MBSS must be modified. However, the proposed solution make allowances for unmodified stations and includes mechanisms which allows them to function in the modified MBSS. Such ability makes it possible to deploy the proposed solution at will, without the need for all MBSS stations to be updated, which would be troublesome in a self-organizing mesh network based on client devices. To maintain the compatibility with unmodified stations, new mechanisms of the proposed solution have been designed to be transparent to such stations, while additional mechanisms emulate the standard IEEE 802.11s interworking service for them to use.

6.1.2 Expected advantages

The proposed procedure, which integrates the functionality of IEEE 802.11s path discovery and interworking mechanisms, with the management protocols of IEEE 802.1D-compatible external network systems, can provide a significant advantages in forwarding the inter-MBSS traffic, while maintaining compatibility with IEEE 802.1D mechanisms of external network.
The introduced ability to keep all available points of contact (mesh gates) between the MBSS and external network active ensures, that the mesh transmission path will be selected to the closest (in terms of path metric) mesh gate available. In effect, the length of required mesh paths will be shorter and intra-path interference generated as a result will be minimized.
Additionally, the intra-MBSS traffic will be divided between a higher number of mesh gates, instead of concentration in vicinity of a limited set of such gates left active by RSTP protocol.
As a result, one of factors limiting the scalability of the IEEE 802.11s has been eliminated, making it possible to employ it efficiently in, for example, sizable and complex access integration network scenarios (Fig. 48).
However, it should be observed, that only an inter-MBSS traffic delivery is optimized by the proposed solution. The intra-MBSS communication still remains a factor limiting the MBSS size, as such traffic still requires creation of long transmission paths spanning sizable portions its structure with associated intra-path and inter-path interference. The problem which will be addressed in the following chapter.
The solution can also be considered a safe one, as unmodified client stations within the MBSS will not cause disturbance in the operation of the Bridged LAN or the MBSS. They, however, will generate an increased amount of management traffic, which makes the solution unfit for partial-deployment scenarios.

6.1.3 Experiments

Taking into account the simulated results of deploying the IEEE 802.11s MBSS network in place of a set of preconfigured IEEE 802.11-2007 access point (see 2.5.7.4 and 3.9.4) is seems that the proposed solution increasing the number of mesh gates which remain active can be crucial for effective deployment of the mesh system in this widely popular usage scenario.
To verify this expectation the scenario described in 3.9.4 has been reproduced here, but with the proposed MGG solution implemented in all mesh gates within the MBSS.
The previously analyzed scenario has been analogous to the one described in 2.5.7.4 for IEEE 802.11 PtMP network and consisted of the 40 mesh STAs from which a randomly selected 10 function as

mesh gates to provide all mesh stations with connectivity with external wired infrastructure, where a host being a destination of a multimedia transmission is located.
All 40 stations have been placed within a 500x500 m area following both previously described grid-based mesh structure scenarios and a single scenario of uniformly random STA placement over the designated area. Each station capable of communication with external network simultaneously attempted to use the VoIP or non-interactive video streaming service described in 2.5.7.1. The results include a number of mesh stations (excluding 10 STAs selected as mesh gates) capable of internetwork connectivity and MOS scores for each of tested services. The test has been repeated for the decreasing number of mesh gates, to test the system's resilience to this important device failures.
The results presented in Fig. 86 and Fig. 87 indicated that while the coverage provided by the MBSS is much better than it was possible to obtain in case of PtMP network with the same number of interworking devices and that the MBSS is highly resilient to mesh gate failures, the Quality of Experience level was completely unacceptable. A cause for this effect was the fact, that only a single mesh gate remained active, leaving a single device capable of exchanging network traffic between MBSS and external networks. The effects, including increased both inter-path and intra-path interference (due to long transmission paths) and severe contention in the spatial area around the single active mesh gate, degraded the QOE for even the low-throughput VoIP service, while video streaming service become completely unusable due to insufficient available throughput.

The results of the scenario with mesh gates supporting the proposed MGG cross-layer solution, indicate that we have obtained the desired results. In Fig. 117 it is confirmed, that the number of mesh stations able to connect to the MBSS remains at the same level as in case of the standard IEEE 802.11s system, and the high resiliency to the failure of even 90% of mesh gates is also unimpaired.

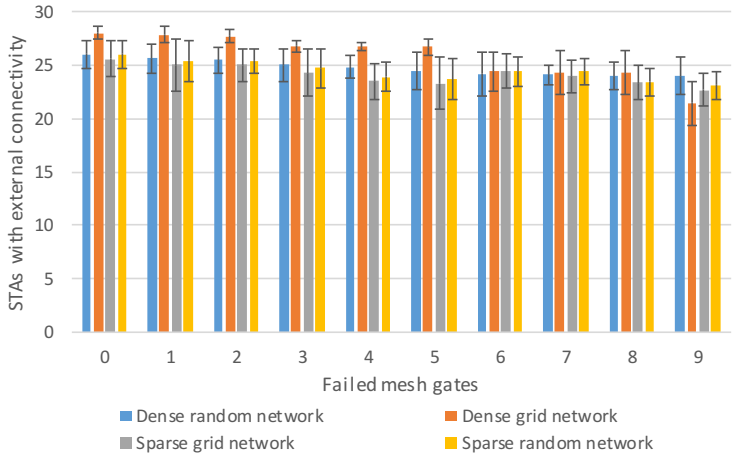

Fig. 117 Number of mesh STAs retaining internetwork communication capabilities as a function of a number of failed mesh gates

Additionally, the fact that each mesh STA constantly receives and caches not only advertisements of its currently selected mesh gate, but also of alternative ones, allows it to quickly change its selected mesh gate in case of its failure. When the recovery procedure requires only the STA changing its configuration and obtaining a mesh path to a new gate, the detection of a failed mesh gate requires only approximately the round-trip time of a mesh path between the STA and the mesh gate, as the last hop station between the failed mesh gate will send back PERR message when attempt to forward a specific number wireless frame to the mesh gate fails. The STA already has an MGGA advertisement of the alternative mesh gate and will proceed MGGA Selection procedure.
The Fig. 118 illustrates the reduction of a mean recovery time for a randomly selected station in case of a mesh gate failure in the abovementioned MBSS system structures modified to support the cross-layer MGG solution. The specific scenario is the same as in case of the experiment described in 3.9.6:

- a 100 simulation runs conducted for each of 4 considered types of mesh topology,
- a low throughput (G.711 VoIP transmission, 64 kbit/s) intra-MBSS IP transmission initiated and sustained between a randomly selected mesh STA and a host in external network,
- a number of 1 Mbit/s UDP traffic sources deployed at randomly selected mesh STAs, each configured to send its traffic stream to another, randomly selected mesh STA.

After 10 s a mesh gate currently used to forward the traffic between the MBSS and the external network have been disabled. The results shown in Fig. 118 indicate the delay until the transmission have been resumed, and include the detection phase (detection of 3 missing Beacon frames).

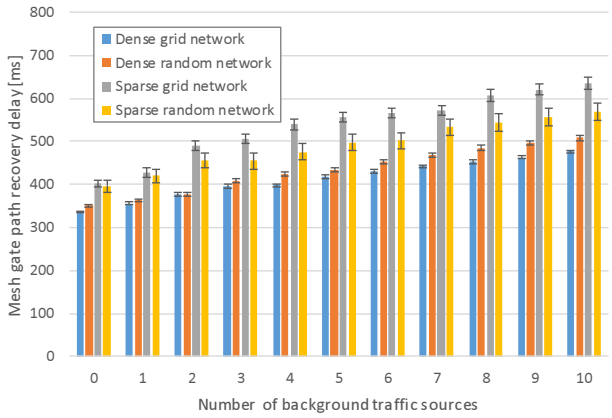

Fig. 118 The latency of mesh gate failure detection and recovery in an MGG MBSS environment

It is visible, that by keeping all mesh gates active, the MGG solution removed the dependency of the recovery procedure on the RSTP protocol operation. As a result it is no longer necessary to wait for the RSTP to activate a new mesh gate before a mesh path discovery can be attempted – when a precursor of the failed mesh gate on the transmission path detects its failure, it will send an appropriate PERR message. The sending STA receiving such a message will become aware of the failure and can immediately choose another mesh gate from the same MGG, send the MGGA Selection message (to prevent the new mesh gate from attempting to forward the traffic to the failed one) and resume the transmission. There is no need to update STA's proxy (PGD) information, as it indicates the MGG and not a particular mesh gate.

With resiliency to mesh gate failures equal to this of the standard MBSS and a slightly improved mesh gate failure recovery time, it remains to be seen, if the MGG provides advantages as the QoE of our selected multimedia services is concerned. To allow such a comparison, MOS scores for these services have been presented in Fig. 119 (VoIP) and Fig. 120 (video streaming).

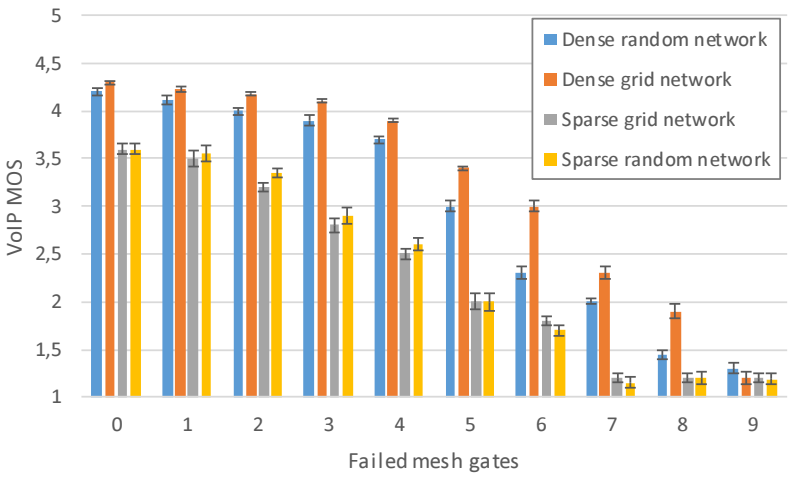

Fig. 119 MOS scores for a VoIP service deployed in the MBSS environment modified to support the MGG solution

The MOS scores for the low-throughput VoIP service indicate (Fig. 119), that the MGG-enabled MBSS is capable of providing a level of service surpassing that of the standard PtMP setup in all dense topologies (grid and random). While, the maximum MOS is not improved and remains at about 4.0-4.3 level, the high resiliency of the MBSS to mesh gate failures results in this high QoE level being sustained despite failure of a significant number of mesh gates. In contrast, in case of the PtMP network, each failed AP significantly influenced the mean MOS score of the system.

The cause for such a positive change due to the deployment of MGG is the fact, that an average length of the mesh path between a wireless STA and its serving mesh gate has been significantly reduced, in case of dense mesh structures from about 5-6 hops to as low as 2-3 hops. Resulting reduction of both intra-path and inter-path interference, combined with spreding of the traffic over a number of network interconnection points (instead of concentration in in the vicinity of a single active mesh gate) allowed such positive results to be obtained.

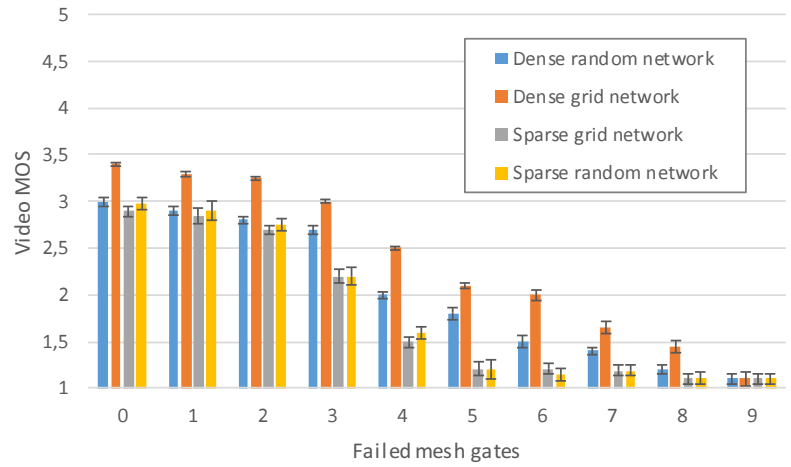

Fig. 120 MOS scores for a non-interactive video service deployed in the MBSS environment modified to support the MGG solution

In case of the video streaming transmission, its higher bandwidth requirements (2 Mbit/s) and high susceptibility to packet loss causes generally lower MOS scores to be obtained, however they are still preferable to the level of QoE available in the PtMP deployment, if we take the possibility of AP/mesh gate failures into account. The higher throughput of the video traffic stream causes the MOS degradation caused by failing mesh gate to appear earlier, and makes the superior performance of

the dense grid structure, with its high quality links, clearly visible even for a low number of failed mesh gates.

The above results show that an IEEE 802.11s MBSS mesh network modified to include the cross-layer Mesh Gate Group solution, can provide a superior Quality of Experience for both VoIP and non-interactive streaming video services compared to a classic PtMP network setup discussed in 2.5.7.4. The advantage is especially visible in case of failure of network interconnection devices such as access point and mesh gates, with the modified MBSS providing both quick resumption of communication and its relatively high quality for a decreasing number of mesh gates.

The deployment of the proposed solution within the IEEE 802.11s MBSS removes one of the most important obstacles preventing this technology from utilizing the robustness of resource management inherent to the mesh network structure in general. As shown in presented simulation results, the modification allowed the resources of all mesh gates present in the MBSS to be used for internetwork traffic exchange, multiplying the maximum inter-MBSS throughput available in the described scenario by the order of magnitude. Additionally the activation of all mesh gates, allowed a significant reduction of mesh path lengths, preventing the inherent inefficiency of using long mesh paths and minimizing both intra-path and inter-path interference. Additionally, the fact that all mesh gates remain active, allows the clients to discover inter-MBSS paths leading through different mesh gates, according to a network's resource state as indicated by the Airtime Metric of its links, thereby providing a more efficient resource usage.
Moreover, the constant activity of multiple mesh gates slightly decrease the, already small compared to the IEEE 802.11 PtMP environment, time required to react to a mesh gate failure. What is even more important, the latency of this reaction no longer directly depends on the operation of the external RSTP protocol and as a result, on the design and configuration of network external to the MBSS.
The results of the proposed modification for the quality of experience of the users attempting to utilize the selected multimedia service in the MBSS environment are evident – in the presented, rather universal scenario, its deployment causes the MBSS network to provide a quality of experience at a better level then a single-hop, multi-AP network. The improvement is evident in both the resulting coverage, failure recovery and MOS-estimated quality of multimedia services. If we take into account the fact that the IEEE 802.11s is a single-channel network, in our scenario utilizing 1/8 of the frequency channels available to the compared multi-AP setup (see 2.5.7.4), the advantage of efficiency and robustness of resource management presented by the modified mesh solution is unmistakable.
In this situation, comparing the above results with QoE MOS scores obtained for an unmodified IEEE 802.11s MBSS (see 3.10), it is clear that the described modification allows the MBSS to attain a much higher robustness in management of its available resources, in most cases surpassing even a pre-designed multi-AP IEEE 802.11 PtMP system. The only presented scenario where IEEE 802.11 PtMP system offers an advantage is the one where it has been assumed that the AP placement is close to ideal as far as coverage area and client locations are concerned – which illustrates the lacking robustness of such a solution.

6.2 External Mesh Peering (ExtMP)

Analyzing path selection mechanisms described in Section 3.7.3 we observe that their functionality is limited to selecting mesh paths – paths between two stations in a given MBSS. Connectivity with external networks is provided by making mash gates perform as proxies for external sources and destinations (see Section 3.8.2). The frame structure reserves a separate sets of address fields for intra-mesh delivery (fields Address 1 to Address 4 as described in Section 3.3.8) of both intra-MBSS and inter-MBSS traffic, with a separate set (Address 5 and Address 6) responsible for specifying initial source and final destination present only in case of inter-MBSS communication.
Such architecture makes the intra-MBSS path selection a self-contained mechanism, as it does not need to differentiate between intra-MBSS and inter-MBSS traffic, but simply deliver it between its points of entry and exit from a given MBSS.
We cannot help but notice, that while such approach offers significant advantages as it allows for a relatively simple architecture of necessary mechanisms and a high level of compatibility with external systems, it also introduces an important limitation – a transmission path between two stations within the same MBSS must be fully contained within its structure.
Such inability of providing communication between two stations within the same ISO-OSI layer 2 network by forwarding it through an external network does not seem to be a significant disadvantage, until we consider distinctive characteristics of a WMN in general and an IEEE 802.11s in particular:

- limited RF resources in form of a single, time-shared RF channel,
- intra-path interference due to forwarding at intermediate stations combined with a single channel operation, making long paths inefficient and lacking in transmission quality (see Section 3.8.4),
- inter-path interference due to highly probable presence of multiple transmission paths within an interference range of each other, also made more probable in case of long mesh paths.

Even this short list demonstrates, that long mesh transmission paths should be avoided if possible, as they are less efficient even in otherwise uncongested network (due to intra-path interference), while being both more susceptible to inter-path interference and creating it in large spatial areas of the network.
The effects described above make it clear, that the mentioned limitation establishes a serious spatial scalability constraint for an IEEE 802.11s mesh system, as with the larger area grows the length of necessary mesh paths, which usually more than overcomes any gains from spatial separation of mesh stations creating areas of mutually independent medium access (stations of a single MBSS outside of mutual interference range). It is dependent on traffic patterns (source-destination pairs) within the MBSS, but in any scenario except the unlikely one exclusively including transmissions to the sending station's loosely defined neighborhood, the MBSS will become increasingly less efficient.
To overcome this limitation while retaining a compatibility with the IEEE 802.1s specification, the External Mesh Peering (ExtMP) solution proposed here utilizes virtual links between IEEE 802.11s mesh gates to interconnect them through network systems external to the MBSS.
Virtual links provide mesh gates with communication capabilities necessary to use standard IEEE 802.11s mesh detection and peering mechanisms to form direct peer links over them. As a result a topology of an MBSS is extended with additional direct mesh links between mesh gates (called external mesh peerings or external mesh links). Such links do not utilize radio resources of the mesh system, but depend on resources provided by external networks. Of course, for the solution to be

applicable, it is necessary for a given MBSS to possess at least two mesh gates able to communicate by external means (without involving the MBSS in question).

The MBSS structure fully extended with virtual mesh links will have all its mesh gates able to communicate without using the MBSS connected with direct mesh links. Moreover, these links can be expected to provide a performance superior to that of a single RF channel multihop transmission provided by the MBSS in question and will not consume its transmission resources.
As virtual mesh links are created and maintained by standard IEEE 802.11s mechanisms, the preference for their use will be determined by the Airtime Metric. As a result, when the external infrastructure will be able to provide a better communication then a path through the wireless domain, such infrastructure will be used instead. It is expected, that with the generally recognized network design principles being followed, virtual links through the infrastructure network will be significantly preferred and used instead of most probably longer paths over probably slower wireless technology of the mesh.

6.2.1 External Mesh Peering architecture

Mechanisms necessary to implement the proposed External Mesh Peering solution can be divided into internal ExtMP procedures, responsible for IEEE 802.11 MAC frame exchange between participating mesh gates over the external communication network, and the interface between abovementioned mechanisms and IEEE 802.11s MBSS functions.

The internal ExtMP mechanisms are intended to provide communication between IEEE 802.11s mesh gates through an external network in a manner which will allow them to establish peer links. This functionality can be implemented using any communication technology which can provide data transmission capabilities between participating IEEE 802.11s mesh gate devices, with ISO-OSI layer 2 and layer 3 solutions being a natural choice.
On the basis of such a communication technology, a frame delivery service for IEEE 802.11 frames (described in Section 3.4.1) must be implemented, which will permit them to be exchanged between participating mesh gates in a reliable manner. When creating such service we must take into account, apart from the specification of the chosen communication technology, a number of ExtMP-specific requirements, such as:

- a considerable maximum size of an IEEE 802.11 frame (from 2304 B upwards, depending on the exact standard version and framing mode), which must be accommodated, but exceeds the maximum MTU size of popular Ethernet technologies (1500 B without jumbo frame support), creating a requirement for fragmentation and reassembly procedures,
- the ExtMP communication between mesh gates should not be effected through the MBSS network they belong to,
- IEEE 802.11 frames must be exchanged between ExtMP-connected mesh gates in a manner which allows standard IEEE 802.11s mechanisms to function, but at the same time care should be taken to prevent unnecessary traffic being generated by the ExtMP mechanisms. In particular it is not advisable to emulate the broadcast characteristics of physical wireless communication by a simple expedient of performing a broadcast transmission to all ExtMP-connected mesh gates.

With the ExtMP internal mechanisms able to efficiently perform the described function, they must also be able to integrate with IEEE 802.11s MBSS mechanisms. Because the external network is not to be connected with an MBSS as a separate network entity but is intended to be used as a transmission medium for an MBSS link, the existing IEEE 802.11s interworking mechanisms cannot

be used. Instead, the integration must be accomplished by employing an underlay or a cross-layer model.
The underlay integration model offers the best possible compatibility up to the point of being able to integrate ExtMP with completely unmodified IEEE 802.11s mesh gate, by exposing a virtual wireless interface, emulated at an approximate level of a boundary between physical and data link ISO-OSI layers. Unfortunately, such compatibility and seamless integration would occur at a cost of efficiency and reliability, especially in terms of the traffic to be exchanged between ExtMP-connected mesh gates and the fact that CSMA/CA procedures would need to be performed over the emulated transmission medium.
The alternative cross-layer integration model requires the IEEE 802.11s mechanisms to be modified for use of ExtMP-provided connectivity in place of its standard physical layer and elements of its MAC sublayer. This model of integration, however, allows for an implementation of ExtMP internal mechanisms to be more efficient than the one possible following the underlay model. However, due to complication of integration mechanisms necessary to employ an underlay model, combined with their expected low efficiency and reliability, it seems that a cross-layer approach is preferable. Fortunately, modifications are required only in case of mesh gates which are to participate in ExtMP communication, while other elements of an MBSS (including other mesh gates) do not need to be modified.

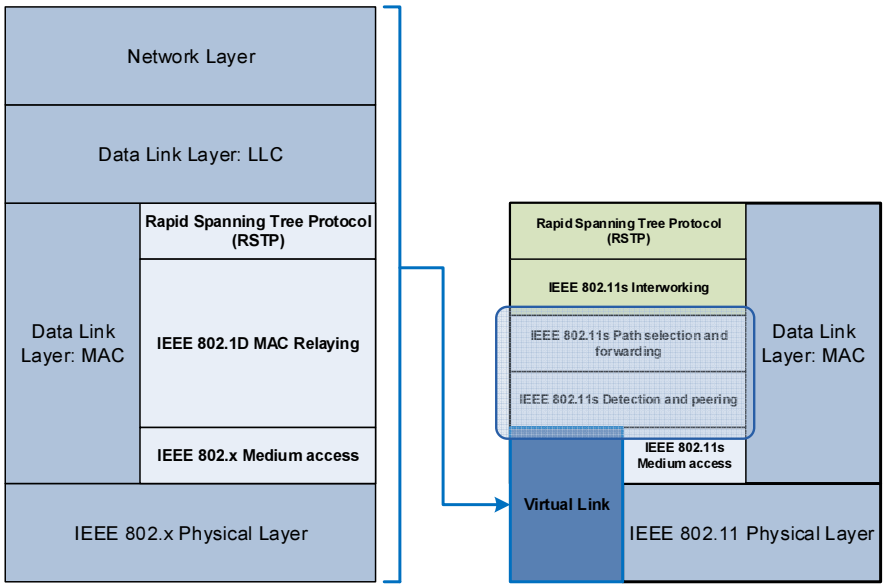

Fig. 121 ExtMP integration in mesh gate architecture

It should also be noted, that both active and inactive (disabled by RSTP protocol as described in Section 3.8.3) mesh gates can be used as endpoints of ExtMP connections, as the proposed solution integrates with intra-MBSS path selection and frame forwarding procedures and does not require a modification of mesh gate-specific interworking mechanisms (see Fig. 121). The requirement, for the ExtMP connection endpoints to be located at mesh gates is based on the need to obtain direct access to the external network connectivity and not on the need to rely on their interworking mechanisms.

6.2.2 ExtMP internal mechanisms

As the main task of ExtMP internal mechanisms is to allow an exchange of MAC layer IEEE 802.11 frames between devices performing the role of mesh gates for a specific MBSS, an ISO-OSI layer 2 or layer 3 technology is preferred for this purpose. An ISO-OSI layer 2 technology provides a minimum feature set necessary for straightforward implementation of required mechanisms, while an ISO-OSI layer 3 solution contains almost a complete set of necessary functions, reducing the implementation

requirements to integration tasks. Additional functionality offered by layers higher than a network layer is superfluous in this case, as provided communication capability is to be used by a data link layer mechanisms of IEEE 802.11 devices.
Whichever technology is chosen in a particular implementation of ExtMP internal mechanisms to provide external connectivity between participating mesh gates, it will be referred as ExtMP Communication Technology (ECT).

6.2.2.1 Configuring the ExtMP-connected mesh gate set

For the purpose of successfully exchanging IEEE 802.11 frames between mesh gates with use of a network external to their MBSS, it is necessary to create a list of mesh gateways which are to be connected in this manner. The list should contain addresses allowing the selected mesh gate devices to be identified by the ECT and is referred to as ExtMP Gate List (EGL).
The method of creating an EGL is considered outside the scope of this specification, but some of possible approaches include:

- a static configuration of mesh gate addresses – often a preferred method in case of up to medium size installations, as the list tends to be static in case of production-grade deployments,
- a management system assisted list deployment – a scenario when a preconfigured list is deployed to all mesh gates with use of an external management system, reducing the workload and making the configuration feasible in case of larger systems. The list itself also can be generated by the management system,
- link or network layer group-casting – broadcasting (or multicasting) the presence of ExtMP enabled gates using a particular multicast destination address, protocol type and/or port number,
- a service registration/discovery – an automatic registration of participating gateways using one of popular methods of service registration and subsequent discovery, for example: a Domain Name System Service Discovery (DNS-SD).

It can be expected that solutions based on a list generation and deployment will be preferred in most deployments (over automatic advertisement-based methods) as the EGL is not expected to change frequently and its correct selection will impact not only the MBSS operation, but also this of external networks used to carry ExtMP traffic. In this situation, its configuration will probably be directly supervised by a system administrator, instead of delegating it to fully automatic solutions.

6.2.2.2 IEEE 802.11 MAC frame encapsulation

For the IEEE 802.11 MAC frames to be exchanged between ExtMP-enabled devices, they must be encapsulated within data units appropriate for a chosen ECT. The data units in turn must:

- be correctly addressed (as described in the following section), allowing them to be delivered to appropriate mesh gate devices participating in the ExtMP infrastructure,
- clearly identify the service they belong to as ExtMP,
- be able to accommodate the maximum size of an IEEE 802.11 MAC frame.

While the addressing procedures are described in more detail in the next section, the methods of service identification and IEEE 802.11 MAC frame encapsulation capable of handling the necessary frame size can be numerous and will differ depending on ECT employed.
The maximum size of an IEEE 802.11 MAC frame exceeding the maximum SDU size allowed in many popular network technologies (such as Ethernet without jumbo frames support), so it is may be necessary to employ additional fragmentation/reassembly procedures if such an ECT is chosen for the purpose of ExtMP communication. On the other hand, a significant number of technologies already provide such functionality, for example ISO-OSI layer 3 protocols such as IPv4 and IPv6 or dedicated solutions such as Point-to-Point Protocol (PPP).

The next important element, service identification, allows ExtMP mechanisms of receiving device to distinguish and process only traffic being exchanged by ExtMP from traffic belonging to other services. They are universally present in popular network technologies, providing service differentiation capabilities of robustness depending on their intended deployment scenarios. Again, ISO-OSI layer 3 provide more robust functions in this aspect, as can be expected due to ISO-OSI described layer functions.
Examples of header fields used for service differentiation in a number of popular technologies, include:

- Ethernet II – EtherType header field (16 bits),
- IEEE 802.2 Logical Link Control (LLC) – Destination Service Access Point (DSAP) field (8 bits),
- IEEE 802.2 Logical Link Control with Subnetwork Access Protocol extension (LLC/SNAP) - Organizationally Unique Identifier (24 bits) an Protocol ID (16 bits) fields,
- IPv4 – protocol ID field (8 bits),
- IPv4/UDP/TCP – Destination Port field (16 bits),
- IPv6 – Next Header field of the last IPv6 header of the packet (8 bits),
- IPv6/UDP/TCP – Destination Port field (16 bits).

The encapsulation itself can also be handled in different manners, starting with a simple handing off the raw frame to be encapsulated as an Service Data Unit to the underlying technology (as in case of a proprietary Ethernet over IP solution [80]) and ending with use of dedicated protocols such as a Point-to-Point Protocol possibly further extended with a Link Control Protocol and a Network Control Protocol appropriate for a specific higher-layer service.

Due to relative simplicity of ExtMP requirements and the lack of transmission related parameters which need to be negotiated between communicating devices, the choice of the ECT is a very broad one. The specific selection will determine compatibility of a particular ExtMP implementation and can have some impact on its performance – manly due to possible presence of ECT-specific protocol overhead. However, the proposed solution will be able to function and provide its intended advantages as long as all mesh gate devices participating in ExtMP group employ a compatible ECT method.

6.2.2.3 Frame delivery

Following commonly recognized service differentiation rules, when sending the ExtMP traffic it should always be clearly identified as such using the service identification method appropriate for the used ECT, as described in the previous section. Also, only traffic identified as belonging to ExtMP should be handled to its mechanisms for processing.

With the ExtMP Gate List configured at each participating mesh gate device it is possible to perform an IEEE 802.11 MAC frame exchange satisfying the requirements of ExtMP, as all its traffic sources and destinations are clearly specified. Having that knowledge and being aware that all virtual mesh links created by the proposed solution must be bidirectional, ExtMP-enabled devices should drop all ExtMP traffic received from sources not listed in their EGL.

As IEEE 802.11s mesh mechanisms are designed to function in a physical environment where the transmissions from a given mesh station are received by all its neighbors within the effective transmission range, the most straightforward method for frame delivery in ExtMP would involve delivering each frame sent to ExtMP infrastructure to all participating mesh gates listed in the EGL. However, as we are already planning on employing a cross-layer integration approach for our solution, we should consider such an approach both inefficient and unnecessary.

Instead we introduce method functioning in a manner similar to IEEE 802.1D bridge learning to optimize exchange of individually addressed frames between ExtMP-enabled mesh gates.
As each of EGL entries corresponds to a mesh gate participating in ExtMP infrastructure and provides information about its ECT address, it is possible to supplement this information with a corresponding MBSS address of such a mesh gate. Such information can be statically provided during initial creation of the EGL (as described in Section 6.2.2.1), but a requirement to do so would bring an unnecessary administrative burden. Instead, the information can be obtained by linking the value of source address field of the ECT data unit with the Transmitter Address (TA) value obtained from IEEE 802.11 MAC frame it encapsulates. Such mechanism will supplement the EGL list of mesh gate ECT addresses with corresponding MBSS mesh gate addresses, allowing individually addressed IEEE 802.11 frames to be sent to appropriate mesh gates by means of a single unicast transmission, based on the RA information in their header.
It should be noted, however, that such address mapping table needs to be maintained to prevent stale information from disrupting the system's operation:

- each mapping should have an associated expiration time. Its elapse results in removal of the MBSS gate address information, but it is reset to the initial value with each reception of ECT data unit allowing to reconfirm the mapping information,
- in case of conflicts a new information should be used overwrite the existing mapping.

While IEEE 802.11 MAC frames individually addressed to mesh gates with a current mapping information can be delivered using the procedure described above, a group addressed frames or frames for addresses which do not have an appropriate mapping to a specific ECT address must be sent to all mesh gate devices listed in EGL.

While the specific method of data unit delivery within the ECT is not important for ExtMP mechanisms as long as a satisfying quality of service is maintained, it would be counterproductive to allow the ExtMP traffic to be exchanged between its participating mesh gates using their own MBSS network. Preventing such occurrence falls under a responsibility of a network administrator deploying the proposed solution and preparing EGL, however an extension to the IEEE 802.11s interworking mechanisms can be used to prevent such occurrence.
For this purpose, the interworking mechanisms of all mesh gates capable of forwarding traffic between external network and the particular MBSS (active mesh gates) should be modified to recognize ExtMP traffic and perform its analysis by comparing its ECT source and destination addresses with these specified in their own EGL. If a match is found, such data unit should be discarded. This procedure is likely to require a cross-layer analysis at mesh gate, depending on ISO-OSI layer of ECT employed (as IEEE 802.11s interworking mechanisms operate at data link layer) and will prevent ExtMP communication between mesh gates if it requires transmission through the MBSS in question.

It is possible that the structure or configuration of the infrastructure network will not allow all mesh gates of a particular MBSS to be connected using ExtMP while observing the above restriction. An activity of a Rapid Spanning Tree Protocol (RSTP) or equivalent solution is a particularly probable cause for such situation, if the MBSS is not an edge network (see Section 3.8.3).
While a modification of such a well-established protocol as the RSTP, which must remain highly-compatible and implemented on many devices within the compound network system does not seem practical a practical solution to such problem, it may be still possible to create multiple, separate ExtMP structures, each connecting a subsets of the MBSS's mesh gates. Moreover, it should be noted, that there are multiple methods and mechanisms capable of modifying the configuration of infrastructure network to better accommodate ExtMP requirements, such as:

- in case of ISO-OSI layer 3 network: modification of routing protocol configuration or static routing configuration, up to introduction of host specific routes,

- in case of both ISO-OSI layer 2 and layer 3 networks: deployment of VLANs to accommodate ExtMP traffic, combined with deployment of Multiple Spanning Tree Protocol (MSTP), which allows creation of separate communication tree for each VLAN.

6.2.3 Interface to an IEEE 802.11s MBSS

If the ExtMP infrastructure created by the described mechanisms is to be used as a replacement transmission medium for IEEE 802.11 mechanisms allowing virtual mesh links to be created, specific elements of the standard also need to be modified.

While IEEE 802.11 MAC frame delivery can be implemented by means of creating an ISO-OSI layer 2 virtual network interface for IEEE 802.11s mechanisms to use, such interface will be missing a number of characteristics specific to a wireless network interface, which mechanisms of the discussed standard expect to find and utilize.
Moreover, some of the IEEE 802.11 and IEEE 802.11s mechanisms should not be used with such an interface, as it their functionality is not required (for example, it is already implemented as an element of a virtual link mechanisms) or should be implemented in a modified way.
Due to this situation, a cross-layer integration model has been adopted, employing specific functions of the chosen ECT (implementation dependent, but most probably ISO-OSI layer 3) in place of IEEE 802.11 mechanisms responsible ISO-OSI layer 1 and 2 support.

As the underlying ECT mechanisms of the virtual interface already provide medium access control and the virtual link represents a potentially complex transmission path through the ECT, no Mesh Coordination Function medium access control mechanisms designed for wireless environment should be used for such interface. Instead the MCF queuing mechanisms should pass data directly to ExtMP data delivery mechanisms.

Further analysis of IEEE 802.11 standard indicates, that apart from the already mentioned changes, a number of IEEE 802.11 management mechanisms depending on periodic transmission of Beacon management frames should be modified.
Beacon management frames are by default sent over the wireless link frequently (10 times per second) but at the same time the range of such transmission is limited to a 1-hop neighborhood of the sender. They are used for variety of purposes related to mesh discovery (as described in 3.6.1) and obtaining a time synchronization between neighboring stations. This latter functionality is then utilized as a basis for a number of functions requiring a scheduling-based approach – for example: controlled channel access mechanisms and power management procedures.
In case of a virtual link, created with use of the infrastructure-grade technology, which is likely to provide a higher stability of connection and which utilizes its own ISO-OSI layer 2 mechanisms, many of Beacon frame functions are no longer needed or cannot be applied to a described virtual link:

- Mesh power management (described in 3.3.6) – not applicable and not needed as power management functionality will be provided on ECT level,
- Mesh Controlled Channel Access (described in 3.5.2) – not applicable, as it is designed to provide a physical medium access control in a shared wireless medium environment, while ECT utilizes its own mechanisms for medium access control tasks,
- Time Synchronization Function (see 3.3.4) – as the timing characteristics of transmission over the virtual link are different then these of a real wireless link between stations in mutual effective transmission range and can be a subject to change depending on changing traffic conditions along the ECT transmission path, it is discouraged to utilize TSF functionality over a virtual link. Moreover, an ExtMP-enabled mesh gate will always possess a classic wireless interface to obtain TSF synchronization with its actual physical neighbors.

Taking into account the above considerations, there remains a Mesh Discovery function (3.6.1) of the Beacon management frame, where its periodic 1-hop broadcast allows devices within effective transmission range to obtain information about fundamental capabilities, requirements and configuration characteristics of an IEEE 802.11s MBSS in general and the broadcasting station in particular. Such functionality must be maintained even over ExtMP virtual links, as it is necessary for initiation of the mesh peering process. However, we must observe, that in case of a EGL-preconfigured ExtMP infrastructure, the frequent Beacon broadcast will be delivered to all mesh gates listed in EGL by paths which sometimes span multiple transit networks. At the same time, the expected stability of infrastructure-grade ECT network communication and the fact that only mesh gates (which rarely exhibit significant mobility) are connected by ExtMP, eliminates the need for a frequent Beacon transmissions. Combined with absence of previously listed mechanisms depending on Beacon timing relations, it is possible to significantly reduce Beacon transmission frequency over ExtMP virtual links.
The precise Beacon transmission interval should be left as a configurable option for system administrator and its value will strongly depend on quality of ECT communication and possible deployment of Beacon-dependent RANN/GANN mechanisms (3.8.1) within the MBSS, which must be able to operate over the virtual link.

The last required set of modifications refers to the IEEE 802.11 wireless transmission capabilities negotiation process performed as a part of mesh discovery and peering management procedures. Due to the fact that ExtMP virtual link does not use a wireless medium and its associated physical layer mechanisms, many Information Elements and specific fields contained in the following management frames:

- Beacon, Probe Request, Probe Response,
- Mesh Peering Open, Mesh Peering Confirm,

are impossible to be filled in with meaningful information, while their specific content still can result in a failure to establish a peering. In this situation, these IEs need not to be present in the listed frames sent over the ExtMP virtual link, and if present, should be ignored on reception. Specific fields in otherwise supported IEs must of course be preset to maintain their format integrity, but need not to be filled with relevant information and should likewise be ignored.
The specific list of elements which should be supported or ignored in particular frame types is provided below.

Beacon management frame elements occurring in MBSS Beacons should be processed as follows:

- Information Elements to be supported:
    - Timestamp,
    - Beacon interval,
    - Service Set Identifier (SSID),
    - RSN,
    - EDCA Parameter Set,
    - QoS Capability,
    - QoS Traffic Capability,
    - Time Advertisement,
    - Interworking,
    - Advertisement Protocol,
    - Emergency Alert Identifier,
    - Mesh ID,
    - Mesh Configuration,
    - Mesh Awake Window,
    - Beacon Timing,
    - MCCAOP Advertisement Overview,
    - MCCAOP Advertisement,

    - Mesh Channel Switch Parameters.
- Information Elements to be ignored as directly related to physical layer mechanisms:
    - Supported rates,
    - Frequency-Hopping (FH) Parameter Set,
    - DSSS Parameter,
    - Country,
    - FH Parameters,
    - FH Pattern,
    - Power Constraint,
    - Channel Switch Announcement,
    - Quiet,
    - TPC Report,
    - ERP,
    - Extended Supported Rates,
    - Antenna,
    - RM Enabled Capabilities,
    - HT Capabilities,
    - HT Operation,
    - 20/40 BSS Coexistence,
    - Overlapping BSS Scan Parameters,
    - Extended Capabilities.
- Information Elements to be ignored as related to power management mechanisms:
    - Traffic indication map (TIM),
    - FMS Descriptor.
- Capability field – to be partially supported, as described below.

Mesh Peering Open management frame elements should be processed as follows:

- IEs to be supported:
    - Interworking,
    - Mesh ID,
    - Mesh Configuration,
    - Mesh Peering Management.
- IEs to be ignored as directly related to physical layer mechanisms:
    - Supported Rates,
    - Extended Supported Rates,
    - Power Capability,
    - Supported Channels,
    - ERP Information,
    - Supported Regulatory Class,
    - HT Capabilities,
    - HT Operation,
    - 20/40 BSS Coexistence element,
    - Extended Capabilities element.
- Capability field – to be partially supported, as described below.

Mesh Peering Confirm management frame elements should be processed according to the same rules as specified for Mesh Peering Open management frame. The only new element introduced in Mesh Peering Confirm management frame – Association ID (AID) – should be supported.

The **Capability field** specified in the above list as partially supported is a 2 byte long flag field, and consists of the following flags:

- Flags to be supported:
  - Privacy,
  - QoS.
- Flags to be ignored as directly related to physical layer mechanisms, medium access control mechanisms, power management or as not used in an MBSS network:
  - ESS,
  - IBSS,
  - Delayed Block Ack,
  - Immediate Block Ack,
  - CF Pollable,
  - CF-Poll Request,
  - Short Preamble,
  - PBCC,
  - Channel Agility,
  - Spectrum Management,
  - Short Slot Time,
  - APSD,
  - DSSS-OFDM.

6.2.4 Expected advantages

As a result the deployment of External Mesh peering method and creation of virtual mesh links leading through external infrastructure of sufficient quality we can expect the following advantages to be obtained:

- any management traffic exchanged between connected mesh gates, including the standard Proxy Update (PXU) messages, can be transmitted by a fast and reliable external network, leading to efficient synchronization of mesh gate-related information without consuming limited resources of the MBSS,
- inter-mesh outgoing traffic received by a mesh gate other than the mesh gate proxying for its destination and thus needed to be forwarded to its appropriate proxy mesh gate, can be transmitted outside the MBSS wireless domain,
- any mesh path can take advantage of a virtual link, making it possible for spatially distant stations to establish a path that includes a relatively small number of hops, some of which do not involve a wireless transmission,
- the previous also includes an inter-mesh traffic incoming through a mesh gate distant from its mesh destination.

The effectiveness of External Mesh Peering depends on a structure of the particular MBSS network combined with number, location and connectivity available to its mesh gates. However, in general it can succeed in changing the pattern of mesh transmission paths through its wireless domain to one reminding of a set of IEEE 802.11 infrastructure PtMP installations with direct connectivity option (introduced in IEEE 802.11e) enabled. Mesh gates fulfill the role similar to access points by:

- providing inter-MBSS connectivity for stations in their proximity (with a sufficient number of mesh gates present not exceeding 2-3 hops) – a functional likeness to an access point with coverage area extended by its nearby (1-2 hop) clients,
- providing intra-MBSS connectivity with distant stations with mesh paths exiting the wireless domain at the nearby mesh gate and entering it again at a mesh gate close to the destination

– a functional likeness to multiple access points connected with a shared DS, possibly being located outside of its mutual interference range.

At the same time, with appropriate placement of mesh gates, continuous path lengths through the wireless domain should not exceed 3 hops, which makes it possible to keep both intra-path and inter-path interference at levels allowing a transmission of a quality appropriate for multimedia transfers.

Due to expected preference of virtual links over wireless ones, we can expect a concentration of traffic paths in neighborhood of mesh gates. However, is will be reflected with increased Airtime Metric of relevant mesh links and the standard path selection mechanisms will respond to such traffic increase by selecting alternative paths as necessary.

6.2.5 Experiments

As the proposed ExtMP modification is intended to improve the quality of traffic transmission within the MBSS network, by providing an ability to substitute external network connectivity in place of native wireless links of the MBSS, a set of experiments already performed for a standard IEEE 802.11s mesh network (see 3.9.3) has been repeated for a mesh network with the proposed ExtMP modification.

In all 4 types of network topologies described in 3.8.5 (each consisting of 30 STAs and additional 10 mesh gates), a random STA has been selected as a traffic destination, while an additional STA has been added to the structure to act as a traffic source, generating multimedia traffic according to rules specified in 2.5.7.1 for VoIP and non-interactive video streaming services. The source station has been placed randomly, but at a predefined distance from the destination STA – in this experiments 60, 160 and 300 m (if the distance would require the STA to be placed outside of the test area, the process of selecting a destination STA has been repeated). The background traffic has been generated by performing a number of concurrent 1 Mbit/s UDP transmissions within the mesh structure, each of them between stations at least 200 m apart and using the same traffic class as the multimedia service. The experiments have been conducted for 2, 4 and 8 such background traffic streams.
All mesh gates have been modified according to the proposed ExtMP specification and are connected by otherwise unloaded Gigabit Ethernet network.
Results have been presented separately for VoIP (Fig. 122) and non-interactive video streaming (Fig. 123) services. To allow for easy comparison between the standard and ExtMP enabled mesh performance, both sets of results have been included in the charts – results for the standard IEEE 802.11s MBSS in diagonal stripes and results for the ExtMP-capable MBSS in solid colors.

The scale of charts in Fig. 122 and Fig. 123 has been set to an unified value, to facilitate comparison both between different mesh structures and between low-throughput VoIP and higher-throughput video services.

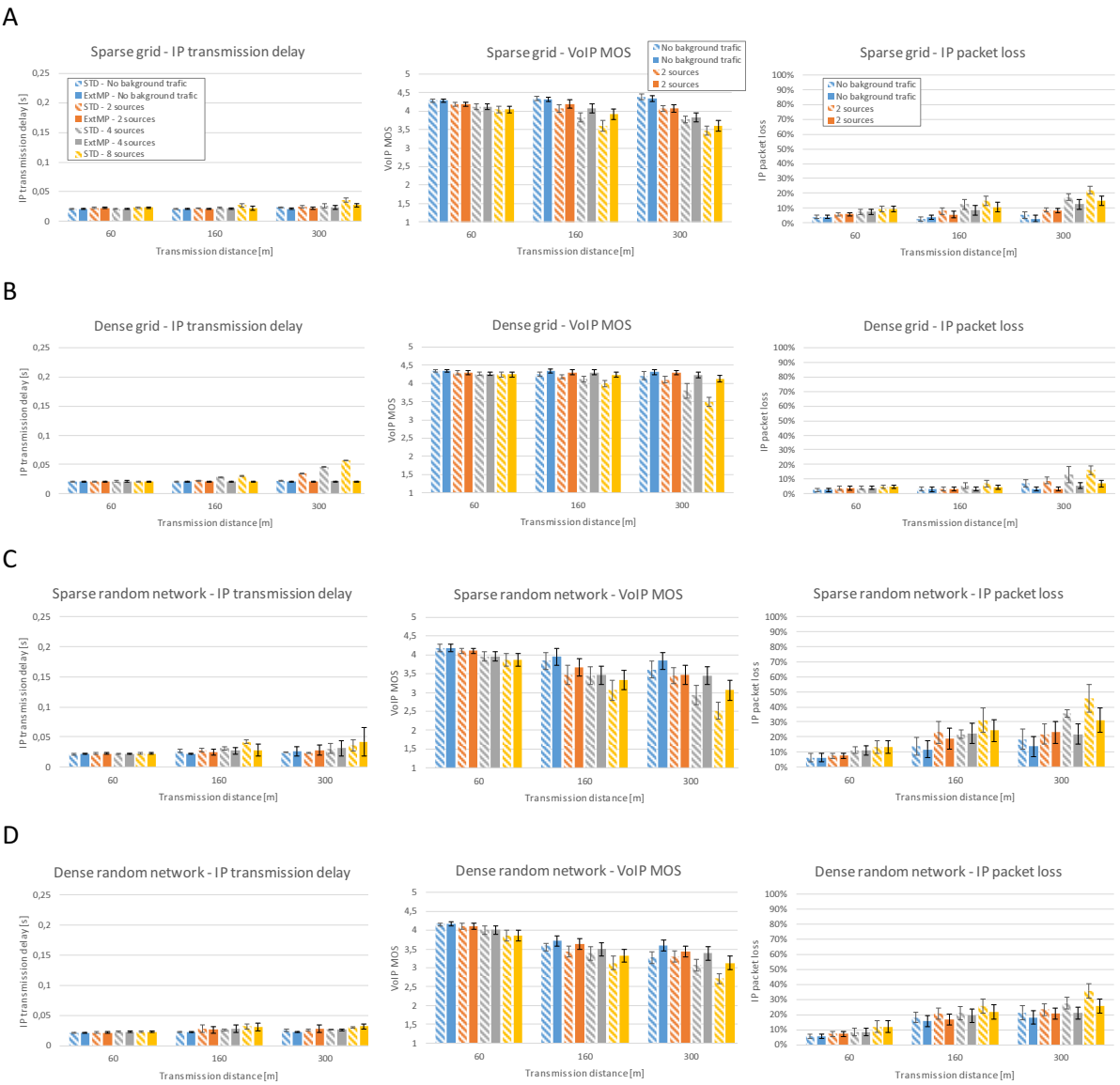

Fig. 122 VoIP transmission in presence of a background traffic, for different (A – sparse grid, B – dense grid, C – sparse random, D – dense random) mesh structures with and without ExtMP modification

The result for the VoIP service demonstrate, that deployment of ExtMP modification does indeed provide advantages in both IP packet loss ratio and IP transmission delay. Due to already high MOS scores for the VOIP service, the improvement becomes clearly visible for mesh paths between stations located at relatively long distance from each other (300 m). For such stations, the long, multihop path required by the standard mechanisms is replaced by a relatively short path leading to the nearest ExtMP mesh gate, which forwards the traffic outside the wireless domain to another ExtMP mesh gate near the destination STA. As a result, both intra-path and inter-path interference is minimized, and the scalability of the IEEE 802.11s MBSS is greatly improved. Theoretically, the length of the mesh path in ExtMP-enabled MBSS is not directly dependent on the distance between communicating stations, but on distances between them and their nearest mesh gates connected using external network infrastructure.

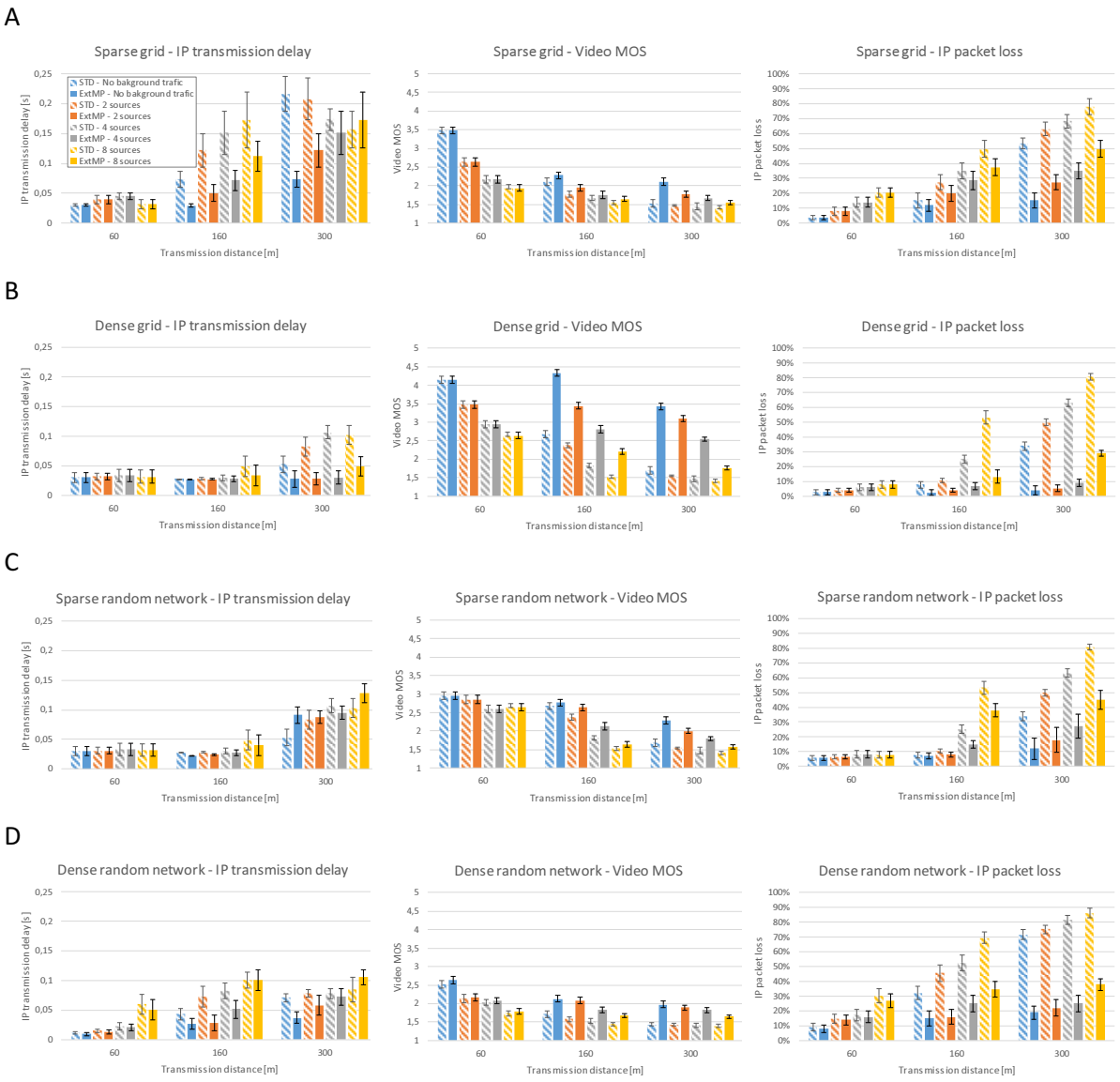

Fig. 123 Non-interactive video streaming transmission in presence of a background traffic, for different (A – sparse grid, B – dense grid, C – sparse random, D – dense random) mesh structures with and without ExtMP modification

With much higher resource requirements of the video streaming service, the difference between the standard MBSS and the one utilizing the proposed ExtMP mechanisms is much more pronounced. The characteristic showing the most improvement is IP packet loss, as in many cases the employment of ExtMP allowed the transmission to avoid the situation where the throughput limit of its transmission path falls below the 2 Mbit/s value required for the video stream. The above effect explains the drastic decrease of the packet loss rate, observable for long range transmissions (300 m). We can also observe a much less prominent difference between medium (160 m) and long (300 m) distance transmissions, due to the fact, that in many cases they do not utilize a significantly different number of wireless transmissions.
It can also be observed, that in case of sparse network structures, the resulting QoE does not rise sufficiently to indicate a good end-user experience, because the limited quality of remaining wireless links is enough to cause the degradation of service level.

Having confirmed the advantageous effect of the proposed ExtMP mechanism on the quality of unicast communication between mesh stations, it can also be observed, that similar advantages can also be expected in case of services utilizing broadcast communication – such as name and address

resolution mechanisms described in chapters 4.1 and 4.2. To verify this expectation, a subset of simulation experiments performed for these mechanisms has been repeated in ExtMP capable mesh.

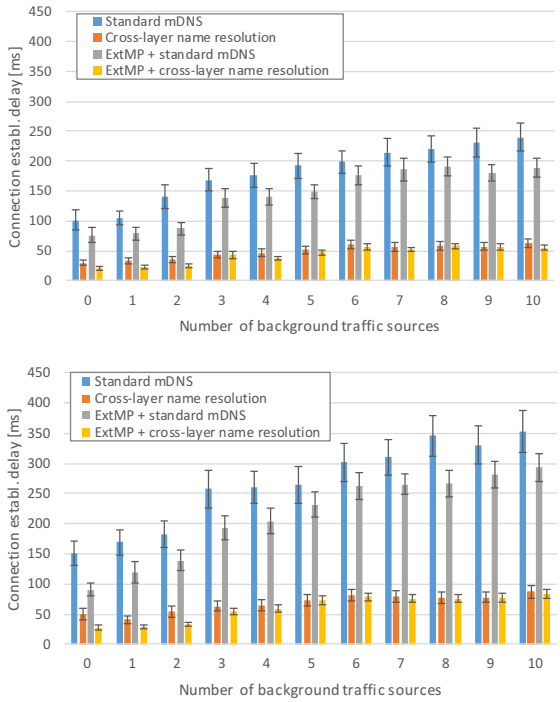

Fig. 124 Comparison of IP communication establishment latency gains for a combined use of the cross-layer mDNS address resolution and ExtMP mechanisms (left – dense grid network, right – dense random network)

The results presented in Fig. 124 indicate, that in case of dese network structures (both grid-based and random) the reduction of the process of establishing IP communication to a DNS-named STA, while present, is limited. With relatively high quality links and highly redundant broadcast flooding process, the advantage of somewhat shorter mesh paths offered by ExtMP is not of paramount importance, for the MBSS network of analyzed size. It can be expected, that in case of geographically larger mesh structures this advantage will increase, provided that there is a sufficient amount of ExtMP-connected mesh gates dispersed through the network.

While for the standard procedure the reduction of latency is at least observable, then in case of the cross-layer procedure proposed in 4.2 it becomes minimal, due to a significant reduction of necessary message exchanges. However, in no cases introduction of ExtMP increases the latency.

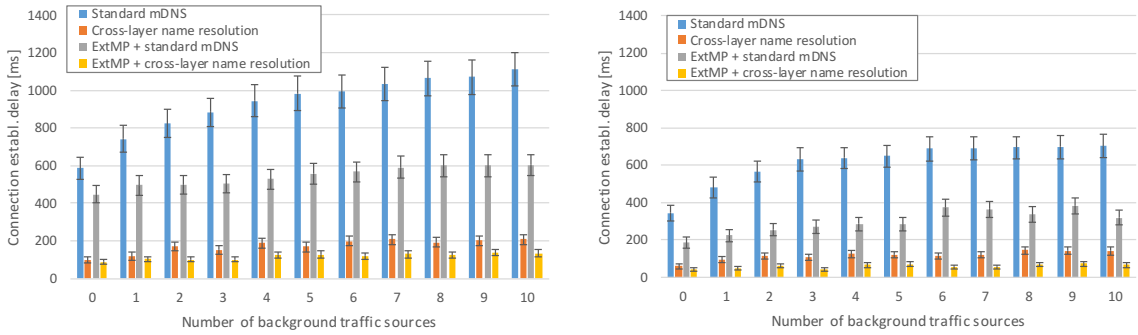

Fig. 125 Comparison of IP communication establishment latency gains for a combined use of the cross-layer mDNS address resolution and ExtMP mechanisms (left – sparse grid network, right – sparse random network)

As can be expected, in case of sparse mesh structures, the advantages of ExtMP become substantial, as high quality virtual links can be used in place of long-range and low-quality wireless ones. In case of the standard procedure (which requires 4 broadcast and 2 unicast transmissions between source

and destination stations) performed in a sparse grid structure, the reduction of mean latency of the process starts at about 20% at the absence of background traffic and growths to 48% in heavy traffic conditions.
In case of the sparse random network, despite its relatively lower mean latency, the use of ExtMP provides even higher reduction ratio – 45-58%.
The ability to substitute high quality Ethernet communication in place of low quality links present in sparse topologies results in latency reduction even in case of the abovementioned cross-layer procedure, despite the fact, that is requires only a single broadcast and a single unicast transmission.

The above results confirm usefulness and universality of the proposed ExtMP solution. By effectively reducing mesh path lengths through the wireless domain, it allows for a much more reliable transmission, reduces interference level and conserves limited mesh resources. Such an advantage, provided at multihop transmission level impacts a broad spectrum of higher layer services, including both these provided for end-users (for example VoIP and video transmissions) and these required for network operation, such as mDNS name resolution or obtaining IP to MAC address mappings with ARP protocol.
The fact, that communication between ExtMP mesh gates will, most probably, be conducted using external network infrastructure, allows for an advantage similar to that offered by MGG solution – despite the fact that only a single mesh gate will remain active, the ExtMP with is capable of making all mesh gates a direct mesh neighbors, connected by direct mesh links of a very good quality. Mesh paths towards the active mesh gate will be most probably lead from the discovering STA to the nearest ExtMP mesh gate (operating as a standard mesh STA but with a very good quality, direct link to an active mesh gate) and then by means of a virtual link to the active one. It should be noted, that such operation, however advantageous from mesh STAs point of view, could not be called an efficient solution compared to the MGG mechanism dedicated to optimize such communication scenario. Due to this fact, it is advised to deploy MGG and ExtMP concurrently, obtaining the advantages of shorter mesh paths for both inter-MBSS (MGG) and intra-MBSS (ExtMP) traffic.

The proposed cross-layer modification allows the IEEE 802.11s MBSS to both visibly improve the efficiency and robustness of the mesh resource usage and allow the system utilize resources of external networks for the purpose of handling its own intra-MBSS traffic. The proposed method does not require any modifications of eternal network systems and, due to the use of the cross-layer approach (integrating mesh path discovery and forwarding with a virtualized mesh interface utilizing an IP-based data transfer) can be used in a wide variety of external networks.

7 Conclusions

The aim of this dissertation was to provide an overview of the mesh mode introduced in the IEEE 802.11s of a very popular IEEE 802.11 wireless network standard and provide a comparison between the efficiency and robustness of its operation and that of the standard IEEE 802.11 Point-to-Point system.
As the preliminary research indicated, that while IEEE 802.11s specification indeed provided a comprehensive set of mechanisms allowing a fully functional and highly compatible Wireless Mesh Network (WMN) to be deployed, some elements of the specification can be expected to significantly decrease the robustness of the solution and its efficiency in supporting popular higher layer protocols and network integration scenarios.
In this situation a two-statement thesis has been proposed:

1. A wireless mesh network structure allows its available resources to be used in a more robust manner than in case of classic Point-to-Multipoint wireless access networks relying on a static set of infrastructure devices.
2. By utilizing a cross-layer integration of a wireless mesh network's data transmission management mechanisms with management mechanisms of higher layer procedures, it is possible to improve the quality of network communication and efficiency of resource usage.

To verify the above statements, an overview of the IEEE 802.11 network mechanisms has been provided, followed by a simulation assessment of its operation. The description of IEEE 802.11 mechanisms allowed the simulation scenarios to be defined in a manner which covers the most important aspects of its operation as far as the robustness of its mechanisms and resulting quality of service is concerned.
To make the results of the performed research applicable in real-world deployment scenarios, it has been decided to take into account a propagation environment better describing the most probable working environment of the described mesh standard. Due to this decision a Nakagami propagation model has been employed in place of the popular Free Space of Two Ray models, which is observable in the obtained simulation results, increasing their adherence to experimental results for systems operating in metropolitan environment with its complex and often adverse propagation conditions. By the same token, the set of utilized, optional mechanisms defined in IEEE 802.11 specification has been limited to the ones implemented in real-world Off-The-Shelf hardware.
The presented simulation scenarios shown that the quality of service offered by a standard IEEE 802.11 PtMP access network, composed of multiple access point devices is strongly dependent on their placement in relation to the location of wireless client devices. If it has been possible to predict the locations of client devices correctly and deploy APs in a way which places majority of clients within their high quality coverage area, the resulting quality of network communication will be good as shown by the results of simulation experiments. At the same time, it has been shown, that apart from the quality of communication being degraded with the increasing range between AP and client devices, it is also degraded by the presence of other network traffic contending for medium access. In this situation, the placement of APs should be such, that client devices are distributed between them evenly, and all PtMP networks within mutual interference range should utilize different, orthogonal frequency channels.
In case, when the above requirement are not satisfied however, we can expect a degradation of the quality of network service and, as a result a degradation of Quality of Experience for multimedia service users. Such characteristics make the IEEE 802.11 PtMP-based access network poorly suited to react to a changing environment. Changes such as unpredictable behavior of its users (both their spatial location and traffic requirements), external interference from other users of ISM band or device failures are capable of disrupting the efficiency of operation of a complex IEEE 802.11 PtMP

access systems drastically. The effect of unpredictable client placement and device failures have been definitely confirmed by results of presented simulation scenarios.

Having assessed the efficiency and quality of network communication offered by multi-AP IEEE 802.11 network systems operating in PtMP mode in both favorable and difficult scenarios, and thus having obtained a comparison baseline, the analysis of IEEE 802.11s mesh extension have been performed.
The overview of the newly introduced mechanisms have been performed, followed by a more in-depth description of the most important ones from the point of view of the thesis. This detailed description allowed both an analysis of expected advantages and weaknesses to be performed and provided a basis for a detailed specification of proposed cross-layer modifications developed to offset limitations of the standard IEEE 802.11s system.
Even the most cursory analysis of the IEEE 802.11s cannot miss the fact, that the solution is a single-channel mesh, in which case of its station use the same, shared frequency channel to communicate. Such approach allows for a popular deployment of the technology, as it simplifies its operation, potentially improves the reliability on heterogenous hardware, and allows popular, single-radio devices to participate fully in the mesh operations. Hoverer, such decision also drastically limits the wireless transmission-related resources available to the network.
In such a mesh type, it is clear that the use of multihop mesh transmission paths will lead to inefficiency of resource consumption and relatively poor QoS due to both intra-path and inter-path interference, especially compared to a simple 1-hop PtMP communication. However, it is also to be expected, that the coverage and ability to cope with device failures will be at much higher level, due to the use of client devices as intermediate retransmission points and advanced self-organization and autoconfiguration mechanisms. The described characteristics seem to indicate, that if the mesh paths can be kept at relatively low number of hops, the robustness of WMN resource management can outweigh disadvantages related to its limited resource pool.
Another of IEEE 802.11s limitations discovered in the process of the analysis of its mechanisms, it its dependence on the IEEE 802.1D-specified mechanisms for interworking purposes – especially RSTP protocol used to avoid traffic loops in compound ISO-OSI layer 2 networks. The protocol performs its basic function by disabling redundant network interconnection points between a given pair of layer 2 networks, leaving only one such device. As if such an approach was not bad enough, it does it without regard for a spatial or structural placement of such devices within the network – an approach understandable in case of high-throughput, high reliability, star-shaped wired networks, but not in case of a limited-resource wireless mesh.
All of these limitations have been confirmed by a series of simulation experiments performed in scenarios similar to these employed in case of IEEE 802.11 PtMP networks. As the performance of a mesh network clearly depends on the spatial layout of its devices, the experiments have been performed for layouts generated by 4 different methods/parameter sets, while keeping the layouts comparable to these used in PtMP scenarios.
The obtained results confirmed the abovementioned expectations, by indicating:

- very through and robust (resilient to changes, such as these brought by device failures) of the network coverage,
- inefficiency and poor QoS of long mesh paths,
- adverse impact of long-range mesh links,
- lack of scalability due to RSTP-induced limitation of the number of available internetwork traffic exchange points.

The simulation results additionally indicated a less obvious problem – due to unreliable manner of group addressed transmission (without acknowledgements and retransmissions), higher ISO-OSI layer protocols which depend on such communication can be expected to encounter message loss and resulting latency increase do to necessity of retrying their failed procedures. As such protocols include ARP and IPv6 ND protocols required for IPv4/IPv6 protocol operation, the effect can prove

to be a significant problem, especially when the direct use of multicast/broadcast multimedia transmissions is not advices due to the same unreliability effect, and a number of unicast flows should be substituted instead.
In overall, the IEEE 802.11s MBSS proves to be more robust in managing its available resources, but due to its single-channel operation and limitation of the number of active interconnection points with external networks, they are so limited, that the MBSS is unable to support the use of multimedia services, except extremally low-bandwidth ones in network structures of strictly limited size.

Having found and verified the above inefficiencies of IEEE 802.11s design, the number of modifications have been proposed to solve the abovementioned problems. Due to the fact, that the IEEE 802.11s specification assigns a high priority to maintaining a high compatibility level with both higher layer protocols and external layer 2 networks systems, and attempts to obtain such compatibility with isolation of different mechanisms (black-box approach) of mechanisms and hiding all of its them by emulating a functional equivalent of an Ethernet network, the proposed modification utilize a cross-layer integration approach.

The first of the proposed procedures integrates the ARP-based IP to MAC address resolution with the reactive path discovery mechanisms of the MBSS. Both of these procedures require a broadcast-unicast exchange of messages between initiating and responding STA, which allows their integration into a single such exchange, instead of two separate processes to be performed sequentially. Not only such a modification reduces the number of necessary messages and the latency of the process by half, but also visibly decreases the impact of an ARP's 1 s timeout, preventing the procedure to be retied in case of a failed transmission. As could be expected, the simulation scenarios performed for all mesh structure types mentioned earlier and various traffic levels, confirm the expected advantages of the modification in terms of both generated traffic and process latency, especially in difficult propagation conditions and heavy network load.
Having the above method performing due to expectations and recognizing that a significant percentage of IP communication is perfumed based on host names instead of IP addresses, another cross-layer integration method have been proposed, extending the already described one to include Multicast DNS name resolution. As a result a mechanism allowing a mesh path establishment to DNS-named hosts have been specified, combining an mDNS to IP address name resolution, an IP to MAC address resolution and a mesh reactive path discovery. The method substitutes a single broadcast-unicast message exchange in place of 4 broadcast and 2 unicast message transmissions. Such a substantial reduction of necessary messages, combined with the fact, that 4 of them required broadcast transmissions susceptible to loss due to unreliable manner of their transmission, allows for 70-80% of latency reduction and prevents delays in order of 1.2 s, caused by 1 s ARP and 2 s mDNS retry timeouts. Again, simulation experiments have been performed for the usual set of mesh topology types and under different network loads, and their results confirm the advantages of the proposed methods in all scenarios, which confirms the second statement of the thesis.
With DNS being used not only for simple name to IP address resolution, but also for service discovery and server selection purposes, the method clearly offers significant advantages in MBSS environment.

With the first two methods utilizing a cross-layer integration approach for more efficient name/address/path resolution in case of reactive MBSS procedures, the third one has been designed to address similar processes in their proactive version. The proposed modification of the HWMP proactive path discovery allows for a servers located within MBSS to advertise their presence, along with optional additional information. The process has been designed to be a highly compatible and resource efficient one.
As a result, client STAs will not only receive current information about available servers and services, but, due to the employ of cross layer integration principles, they will be informed of the current Airtime Metric of the mesh path which will be used for communication and the subsequent path

discovery process will be performed with an unicast-unicast message exchange (instead of the less efficient and more error prone broadcast-unicast one).
Simulation experiments comparing this proactive solution with both the standard, mDNS-based service discovery method and with the previously proposed, (reactive) cross-layer mDNS method have been performed to verify its operation and efficiency. Their results indicate, that the proposed proactive method allows for latency reduction slightly surpassing the reactive, cross-layer solution proposed previously. Additionally, due to the proactive manner of the service advertisement, it is less prone to errors causing a server to be omitted from selection due to a message loss.

Having addressed the discovered inefficiency of a number of IP network's critical protocol's support, further research concentrated on even more serious deficiencies in IEEE 802.11s network interworking mechanisms. As deactivation of a mesh gate results in both longer mesh paths for inter-MBSS destinations and forces the traffic to be forwarded by a decreased number of mesh gates creating a an increased contention in areas around functioning mesh gates, it is imperative to prevent such occurrences.
The proposed Mesh Gate Group cross-layer procedure, allows all mesh gates within an MBSS to remain active, without either compromising the compatibility of the modified MBSS with external networks or risking traffic loops. With increased number of mesh gates, the inter-MBSS traffic will use different mesh gates for different mesh STAs according to their respective cost as indicated by Airtime Metric. As a result not only the length of such paths will be much sorter (lesser intra-path interference), but they will also be spatially dispersed, decreasing inter-path interference. The proposed method will also function in case of a transit traffic, allowing the MBSS to be efficiently used as an element of distribution network, instead of only an access one.
The verification of the efficiency of the method, performed again for the usual set of network topologies confirms that while the coverage advantages of the standard IEEE 802.11s MBSS have been retained, the modified network is also able to provide the QoS of infrastructure network access required to support multimedia services with the QoE at the level similar to the one obtained in the reference, well designed PtMP network. Additionally the network's resilience to failures of infrastructure access devices (mesh gates in this instance) is much higher in case of the modified WMN. This result confirms the first statement of the thesis, especially if we take into account, that the MBSS network operates using a much smaller resource pool than the reference PtMP network – 1 frequency channel used by the modified IEEE 802.11s network instead of 8 of such channels used in the reference PtMP scenario. If we take into consideration the poor performance of unmodified IEEE 802.11s network in the same scenario, the results also confirm the second statement of the thesis.

The last of the proposed cross-layer integration procedures addresses the problem of a growing mesh transmission path lengths in larger MBSS structures, which is a significant limitation of the system's scalability. Taking into account, that according to the standard IEEE 802.11s specification, there can be no two active points of traffic exchange between the MBSS and the single, external ISO-OSI layer 2 network, the requirement that intra-MBSS mesh transmission paths must be fully contained within the MBSS is logical. However, in presence of more than one mesh gate connected to the external network, a virtual mesh peering can be established between them, offering a reliable transmission 'shortcut' outside of the wireless domain. The use of such a virtual link will not only conserve MBSS resources, but also can span a significant spatial distances.
Simulation experiments performed to verify the operation of this modification indicate a much better delay and packet loss characteristics of the transmission between mesh STAs located at a given distance from each other, compared to an unmodified IEEE 802.1s MBSS scenario. Moreover, due to a reduced number of retransmissions within the wireless MBSS domain, the adverse impact of the background traffic load is significantly reduced.
The described gains are obtained in case of all considered mesh topology types, one again confirming the second statement of the thesis. Also, while the obtained QoE scores for considered multimedia

services are relatively lower than is the perfect case of the pre-planned PtMP scenario, if we take into account that the MBSS utilizes only a single frequency channel and that the placement of the STAs is not pre-designed in any way, it can be argued that the robustness resource management of the modified MBSS is superior to the statically pre-planned PtMP network. Especially, if we consider the fact that the modified WMN is able to dynamically utilize the resources of different external networks connected at ISO-OSI layer 3, if it will allow it to conserve its own resources while maintaining (or increasing) the QoS level, but can also function without any static infrastructure. Thus, the scenario also confirms the first statement of the thesis.

The achievements and contributions of the dissertation can be summarized as follows:

1. The overview and analysis of the IEEE 802.11 standard mechanisms has been provided, as a comparison basis for further study of IEEE 802.11-based mesh systems.
2. Simulation experiments illustrating the efficiency and quality of IEEE 802.11 support for a selected set of multimedia services have been performed in a number of network structures. Conclusions regarding the robustness of resource management in case of different network loads and network structure changes (caused by unpredicted client placement and/or device failures) have been provided.
3. The overview of the IEEE 802.11s mesh network mechanisms has been included, followed by an in-depth description of these of its mechanisms which have direct bearing on the inefficiencies uncovered in the conducted research or whose particulars must be observed in specification of the proposed cross-layer integration methods.
4. A partial IEEE 802.11s simulation model provided by the INETMANET 2.0 model library has been extended with previously missing mechanisms and its errors corrected.
5. Simulation experiments of IEEE 802.11s MBSS operation in 4 different mesh topology types have been performed, verifying its efficiency of operation for different traffic scenarios and the resulting Quality of Experience for a selected set of popular multimedia services.
6. The set of inefficiencies of the IEEE 802.11s specification related to its interworking functions and support for a broad group of a higher layer protocols has been pinpointed and described.

   A number of original, cross-layer integration mechanisms intended to eliminate the discovered inefficiencies has been proposed and specified in detail for implementation and deployment in IEEE 802.11s system:
7. The original, cross-layer mechanism for the IP to MAC address cross-layer resolution procedure have been proposed and specified in detail, allowing the inefficiency in handling a broadcast-dependent ARP protocol (a critical part of IP protocol stack) to be minimized.
8. The original, cross-layer mechanism allowing the efficient DNS name to IP and MAC address resolution procedure to be performed in the mDNS/IEEE 802.11s environment, thereby minimizing inefficiencies in mDNS/ARP operation in such a WMN system.
9. The original, cross-layer service advertisement mechanism capable of low-latency and reliable application server advertisement within the IEEE 802.11s mesh structure, providing clients with precise communication path quality assessment.
10. The Mesh Gate Groups original interworking solution, utilizing the cross-layer integration approach to allow for multiple traffic exchange points to remain active between an IEEE 802.11s MBSS and an external ISO-OSI layer 2 network, greatly improving the systems scalability and robustness of resource management.
11. The External Mesh Peering, an original MBSS topology extension, employing cross-layer integration procedures and link virtualization mechanisms to allow mesh gates to from links through external networks, resulting in significant resource conservation within the MBSS system.

12. Simulation models of all 5 proposed cross-layer mechanisms have been implemented in OMNeT++ 4.6 simulation environment.

13. The expected advantages of all proposed cross-layer mechanisms have been verified in simulation scenarios allowing an easy comparison of the modified WMN efficiency with both unmodified IEEE 802.11s system and the classic IEEE 802.11 PtMP network.

Following the research presented in this dissertation it can be stated that the operation of the standard IEEE 802.11s mesh network does not allow us to confirm the first statement of the thesis. However, the introduction of the proposed cross-layer integration procedures removes the most troublesome limitations of the standard solution and increases the efficiency and robustness of its resource management and other operational aspects in a manner which allows us to confirm the first statement of the thesis on a basis of performed simulation experiments:

1. ***A wireless mesh network structure allows its available resources to be used in a more robust manner than in case of classic Point-to-Multipoint wireless access networks relying on a static set of infrastructure devices.***

At the same time, the fact that the introduction of proposed cross-layer integration procedures has been necessary to confirm the first statement, directly proves the second one.

2. ***By utilizing a cross-layer integration of a wireless mesh network's data transmission management mechanisms with management mechanisms of higher layer procedures, it is possible to improve the quality of network communication and efficiency of resource usage.***

In this situation we can consider both statements of the thesis to be proven.

8 References

1. IEEE, "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-1997, 1997
2. IEEE, "Supplement to IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band", IEEE Std 802.11a-1999, 1999
3. IEEE, „IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band", IEEE Std 802.11b-1999, 2000
4. IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11g, 2003
5. IEEE, "IEEE Standard for Information technology- Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz", IEEE Std 802.11ac-2013, Dec. 18 2013
6. IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs", IEEE Std 802.11k-2008, June 12 2008
7. IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: IEEE 802.11 Wireless Network Management", IEEE Std 802.11v-2011, Feb. 9 2011
8. IEEE, "IEEE 802.11r: Amendment 2: Fast Basic Service Set (BSS) Transition", IEEE Std 802.11r-2008, July 2008
9. IEEE, "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks-specific requirements - Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 9: Interworking with External Networks", IEEE Std 802.11u-2011, Feb. 25 2011
10. IEEE P802.11 - TASK GROUP AQ, "Status of Project IEEE 802.11aq: Pre-Association Discovery (PAD)", http://www.ieee802.org/11/Reports/tgaq_update.htm, retrieved 2016
11. IEEE, "IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking", IEEE Std 802.11s, 2011
12. Gierłowski K.: „Integracja międzywarstwowa protokołów RM-AODV, Multicast DNS i IPv6 Neighbor Discovery w środowisku sieci standardu IEEE 802.11s", Przegląd

Telekomunikacyjny + Wiadomości Telekomunikacyjne, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 8-9/2016
13. K. Gierłowski, "Cross-layer mDNS/ARP Integration for IEEE 802.11s Wireless Mesh Network," 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC), Colmar, 2016, pp. 33-40
14. Gierłowski K., Hoeft M., Gumiński W.: „Laboratorium mobilnych technik bezprzewodowych", Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr. 8-9 (2015), s. 1141-1150
15. Gierłowski K.: "Ubiquity of Client Access in Heterogeneous Access Environment", Keynote of IEICE Wireless Networks Workshop 2013, Journal of Telecommunications and Information Technology, issue 3 (2014), s. 3-16
16. Gierłowski K.: „Mechanizmy odkrywania usług i integracji międzysieciowej w samoorganizujących systemach bezprzewodowych standardu IEEEE 802.11s", Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr. 8-9 (2013), s. 1120-1130
17. Gierłowski K.: "Interworking and Cross-layer Service Discovery Extensions for IEEEE802.11s Wireless Mesh Standard", Journal of Telecommunications and Information Technology, nr. 3 (2013), s. 97-105
18. Gierłowski K.: "Service and Path Discovery Extensions for Self-forming IEEE 802.11s Wireless Mesh Systems", 17th Polish Teletraffic Symposium 2012, Zakopane 2012
19. Hoeft M., Gierłowski K., Gierszewski T., Konorski J., Nowicki K., Woźniak J.: "Measurements of QoS/QoE Parameters For Media Streaming in a PMIPv6 TESTBED WITH 802.11 b/g/n WLANs", Metrology and Measurement Systems, nr 2, s. 283-294, 2012
20. Gierłowski K., Kostuch A., Woźniak J., Nowicki K.: "Testbed Analysis Of Video And Voip Transmission Performance In IEEE 802.11 B/G/N Networks", Telecommunication Systems, Issue 3, Vol. 48, p. 247-260, 2011
21. Kostuch A., Gierłowski K., Woźniak J.: "Performance Analysis of Multicast Video Streaming in IEEE 802.11 b/g/n Testbed Environment", Wireless and Mobile Networking: Second IFIP WG 6.8 Joint Conference, WMNC 2009, Gdańsk 2009
22. Gierłowski K., Nowicki K., Pieklik W., Pawałowski P.: "An Integrated E-Learning Services Management System Providing HD Videoconferencing and CAA Services", 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP 2012), Poznań, 18-20.07.2012, p. 1-6
23. Gierłowski K., Woźniak J.: „Analiza szerokopasmowych sieci bezprzewodowych serii IEEE 802.11 i 16 (WiFi i WiMAX) z transmisją wieloetapową", Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 8-9/2008, s. 925 - 935, 2008
24. Sadaf T., Zareen S., Iqbal F., Shah G. A., Javed M. Y.: "Link Adaptive Multimedia Encoding in Wireless Networks: A Survey of Theory And Approaches," 2010 International Conference on Electronics and Information Engineering, Kyoto, 2010, pp. V2-5-V2-10
25. T. Ma, M. Hempel, D. Peng and H. Sharif: "A Survey of Energy-Efficient Compression and Communication Techniques for Multimedia in Resource Constrained Systems" in IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 963-972, Third Quarter 2013
26. Misra S., Reisslein M., Xue G.: "A Survey of Multimedia Streaming in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 18-39, Fourth Quarter 2008
27. Mao S., et al.: "Video Transport over Ad Hoc Networks: Multistream Coding with Multipath Transport," IEEE JSAC, vol. 21, no. 10, Dec. 2003, pp. 1721–37
28. van der Schaar M., et al.: "Adaptive Cross-layer Protection Strategies for Robust Scalable Video Transmission over 802.11 WLANs," IEEE JSAC, vol. 21, no. 10, Dec. 2003, pp. 1752–63

29. Park J., Lee H., Lee S.: "Cross-Layer Optimization for Scalable Video Coding and Transmission Over Broadband Wireless Networks," 2007 IEEE International Conference on Image Processing, San Antonio, TX, 2007, pp. III - 313-III - 316
30. Kofler I., Seidl J., Timmerer C., Hellwagner H., Djama I., Ahmed T.: "Using MPEG-21 for Cross-Layer Multimedia Content Adaptation", Volume 2. Springer J. Signal Image Video Process; 2008:355-370
31. Sutinen T., Vehkaperä J., Piri E., Uitto M.: "Towards Ubiquitous Video Services Through Scalable Video Coding And Cross-Layer Optimization", EURASIP Journal on Wireless Communications and Networking, 2012
32. IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements", IEEE Std 802.11e-2005, Nov. 11 2005
33. Aboba A., Simon D., Eronen P.: "RFC5247: Extensible Authentication Protocol (EAP) Key Management Framework", IEFT 2008
34. Lipmaa H., Wagner D., Rogaway P.: "Comments to NIST Concerning AES Modes of Operations: CTR-Mode Encryption", 2012
35. Ehrsam W., Meyer C., Smith J., Tuchman W.: "Message Verification and Transmission Error Detection by Block Chaining", US Patent 4074066, 1976
36. Hung F. Y. , Marsic I.: "Access Delay Analysis of IEEE 802.11 DCF in the Presence of Hidden Stations," *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*, Washington, DC, 2007, pp. 2541-2545
37. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Redline," in IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) - Redline , vol., no., pp.1-5229, March 29 2012
38. IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput", IEEE Std 802.11n-2009, Oct. 29 2009
39. Nakagami M.: "The m-distribution—A general formula of intensity distribution of rapid fading," in Statistical Methods in Radio Wave Propagation, W. C. Hoffman (ed.), pp. 3-36, Pergamon Press, London, 1960
40. Andersen J., Rappaport T., Yoshida S.: "Propagation measurements and models for wireless communications channels", IEEE Communications Magazine. 1995 Jan; 33(1)
41. Sklar B.: "Rayleigh fading channels in mobile digital communication systems" in IEEE Communications Magazine, vol. 35, no. 9, pp. 136-146, Sep 1997
42. Punnoose R., Nikitin P., Stancil D.: "Efficient Simulation of Ricean Fading within a Packet Simulator", InVehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd 2000, Vol. 2, pp. 764-767
43. IEEE P802.11 - TASK GROUP T, "Status of Project IEEE 802.11 Task Group T: Recommended Practice for Evaluation of 802.11 Wireless Performance", 2008
44. ITU-T Geneva Switzerland, "ITU-T G.711 - Pulse Code Modulation (PCM) of Voice Frequencies", Nov. 1988
45. ITU-T, "A High Quality Low-Complexity Algorithm for Packet Loss Concealment With G.711" ITU-T Recommendation, G.711 Appendix 1, 1999
46. ITU-T, "Advanced Video Coding for Generic Audiovisual Services", ITU-T H.264 (V11), 10/2016
47. ITU-T, International telephone connections and circuits – Transmission planning and the E-model – The E-model: a computational model for use in transmission planning, G.107, 06/2015

48. ITU-T, STUDY GROUP 12 – DELAYED CONTRIBUTION 106, COM 12 – D 106 – E, January 2003
49. ITU-T, “International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection – Transmission impairments due to speech processing, G.113”, 11/2007
50. ITU-T, “Opinion model for video-telephony applications”, ITU-T G.1070, 07/2012
51. ITU-T, “Methods for objective and subjective assessment of speech and video quality – Mean opinion score (MOS) terminology”, P.800.1, 07/2016
52. ITU-T, “Methods for objective and subjective assessment of speech and video quality – Models and tools for quality assessment of streamed media”, P.1200
53. ITU-T, “Methods for objective and subjective assessment of speech and video quality – Models and tools for quality assessment of streamed media - Parametric non-intrusive assessment of audiovisual media streaming quality”, P.1201, 10/2012
54. ITU-T, “Methods for Objective and Subjective Assessment of Speech and Video Quality – Telemeeting assessment”, P.13xx series
55. Mwela J., Oyekanlu E.: “Impact of Packet Loss on the Quality of Video Stream Transmission”, Thesis no: MSC-2010-6182, May 2010
56. Alahari Y., Prashant B.: “Analysis of Packet Loss and Delay Variation on QoE for H.264 andWebM/VP8 Codecs”, December 2011
57. Lin T.-L., Kanumuri S., Zhi Y., Poole D., Cosman P., Reibman A.: “A Versatile Model for Packet Loss Visibility and Its Application to Packet Prioritization,” IEEE Transactions on Image Processing, vol. 19, no. 3, pp. 722 –735, 2010.
58. Loguinov D.,Radha H.: “Measurement Study of Low-Bitrate Internet Video Streaming,” in Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement, 2001, pp. 281–293. [Online]. Available: http://doi.acm.org/10.1145/505202.505238
59. De Simone F., Tagliasacchi M., Naccari M., Tubaro S., Ebrahimi T.: “A H.264/AVC Video Database for the Evaluation of Quality Metrics,” in Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, 2010, pp. 2430 –2433.
60. Nawaz Minhas T., Gonzalez Lagunas O., Arlos P., Fiedler M.: "Mobile Video Sensitivity to Packet Loss and Packet Delay Variation in Terms of QoE," 2012 19th International Packet Video Workshop (PV), Munich, 2012, pp. 83-88.
61. Castignani G., Moret A., Montavont N.: “A Study of the Discovery Process in 802.11 Networks”, ACM Sigmobile - Mobile computing and communications review, 2011, 15 (1), pp.25-36.
62. Madwifi Project, http://madwifi-project.org, retrieved 2012
63. Varga A.: “The OMNeT++ Discrete Event Simulation System”, Proceedings of the European simulation multiconference (ESM’2001) 2001 Jun 6 (Vol. 9, No. S 185, p. 65).
64. Linux Wireless Ath5k, http://linuxwireless.org/en/users/Drivers/ath5k/__v10.html, retrieved 2016
65. Mazlan M., Ariffin S., Balfaqih M., Hasnan S., Haseeb S.: “Latency Evaluation of Authentication Protocols in Centralized 802.11 Architecture”, IET International Conference on Wireless Communications and Applications (ICWCA 2012), Kuala Lumpur, 2012, pp. 1-6.
66. Burgess D.: “Learn RouterOS”, Lulu.com, 2011.
67. Waharte S., Ritzenthaler K., Boutaba R.: “Selective Active Scanning for Fast Handoff in WLAN Using Sensor Networks”, Mobile and Wireless Communication Networks 2005 (pp. 59-70). Springer US.
68. ETSI, E. 300 328, “Electromagnetic Compatibility and Radio Spectrum Matters” (ERM):1-3.
69. Conner W., Kruys J., Kim K., Zuniga J.: „IEEE 802.11 s Tutorial”, IEEE 802 Plenary. 2006 Nov:93.

70. IEEE, "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2007, June 12 2007
71. IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: 3650-3700 MHz Operation in USA," in IEEE STD 802-11y-2008 , vol., no., pp.1-90, Nov. 3 2008
72. IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames", IEEE Std 802.11w-2009, Sept. 30 2009
73. IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Extensions to Direct-Link Setup (DLS)," in IEEE Std 802.11z-2010
74. IEEE, "IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments", IEEE Std 802.11p-2010, July 15 2010
75. IEEE, "IEEE Standard for Air Interface for Broadband Wireless Access Systems", IEEE Std 802.16-2012, Aug. 17 2012
76. ZigBee Alliance, http://www.zigbee.org/, retrieved 2016
77. Rajamanickam A.: "Telecommunications Strategy and Solutions for Smart Grid Implementation", Metering, Billing/CRM Asia 2013, 22-23 May, Bangkok, Thailand, 2013
78. Hauser J., Shyy D., Green M.: "802.11s Military Usage Case", IEEE 802.11-04/1006r0, 2004
79. IEEE, "IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges", IEEE Std 802.1D, 2004.
80. MikroTik Routers and Wireless, http://www.mikrotik.com/, retrieved 2016
81. Perkins C., Belding-Royer E., Das S., "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561 (Experimental), Internet Engineering Task Force, Jul. 2003.
82. Harkins D.: "RFC7664: Dragonfly Key Exchange", http://tools.ietf.org, 2015.
83. Harkins D.: "RFC5297: Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)", http://tools.ietf.org, 2008
84. StrixSystems, "Solving the Wireless Mesh Multihop Dilemma", whitepaper, http://www.strixsystems.com/products/datasheets/StrixWhitepaper_Multihop.pdf, 2005
85. Bettstetter C.: "On the Minimum Node Degree and connectivity of a Wireless Multihop Network", Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking and computing, Lausanne, Switzerland, 2002.
86. Li X., Wan P., Wang Y., Yi C.: "Fault Tolerant Deployment and Topology Control in Wireless Networks", Proceedings of the 4th ACM international symposium on Mobile ad hoc networking and computing, Maryland, USA, 2003.
87. Bettstetter C., Gyarmati M., Schilcher U.: "An Inhomogeneous Spatial Node Distribution and Its Stochastic Properties", Proceedings of 10th ACM-IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2007), Chania, Greece, 2007.

88. Liu X. , Haenggi M.: “Toward Quasiregular Sensor Networks: Topology Control Algorithms for Improved Energy Efficiency”, IEEE Transactions on Parallel and Distributed Systems, 2006.
89. Fang L., Du W., Ning P., ”A Beacon-Less Location Discovery Scheme for Wireless Sensor Networks”, Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM2005, 2005.
90. Milic B., Malek M.: “NPART-node Placement Algorithm for Realistic Topologies in Wireless Multihop Network Simulation”, Proceedings of the 2nd international conference on simulation tools and techniques 2009 Mar 2 (p. 9), ICST
91. MERU Networks, “The enterprise is ready for VOIP”, White paper, www.merunetworks.com, 2005
92. Cheetham B., Ettefagh A., Spegel M., Nasr K., Ravnikar E.: “Voice over WLAN for Converged Enterprise Networks”, 15th IST Mobile & Wireless Communications Summit, Greece, June 2006
93. Pallos R., Farkas J., Moldovan I., Lukovszki C.: “Performance of Rapid Spanning Tree Protocol in Access and Metro Networks”, Second International Conference on Access Networks & Workshops, Ottawa, Ont., 2007
94. IEEE, “IEEE Standard for Ethernet," in IEEE Std 802.3-2015 (Revision of IEEE Std 802.3-2012) , vol., no., pp.1-4017, March 4 2016
95. Postel J.: “RFC 791: Internet Protocol”, DARPA Internet Protocol Specification. http://tools.ietf.org, 1990
96. Plummer D.: “RFC 826: An Ethernet Address Resolution Protocol”, Internet Network Working Group, http://tools.ietf.org, 1982
97. Jacquet P., Muhlethaler P., Clausen T., Laouiti A., Qayyum A., Viennot L.: “Optimized link State Routing Protocol for Ad hoc Networks”, Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century, 2001
98. Hornig C.: “RFC 894: Standard for the Transmission of IP Datagrams over Ethernet Networks”, http://tools.ietf.org, 1984
99. Eastlake D., Abley J.: "RFC 7042: IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", https://tools.ietf.org/html/rfc7042, 2013
100. Paris J., Shah P.: “Peer-to-peer Multimedia Streaming Using BitTorrent”, 2007 IEEE International Performance, Computing, and Communications Conference 2007 (pp. 340-347), IEEE, 2007
101. Mockapetris P.: “RFC 1034: Domain Names: Concepts and Facilities”, http://tools.ietf.org, 2003
102. Brisco T.: “RFC 1794: DNS support for load balancing”, http://tools.ietf.org, 1995
103. Cheshire S, Krochmal M.: “RFC 6763, DNS-Based Service Discovery. Internet Engineering Task Force”, http://tools.ietf.org, 2013
104. Aggarwal A.: “RFC 1001: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods.”, IETF Network Working Group, http://tools.ietf.org, 1987
105. Aggarwal A.: “RFC 1002: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications”, IETF Network Working Group, http://tools.ietf.org, 1987
106. Mockapetris P.: “RFC 1035-Domain Names-Implementation and Specification”, http://tools.ietf.org, 1987
107. Cheshire S, Krochmal M.: “RFC 6762: Multicast DNS”, Internet Engineering Task Force (IETF) standard, http://tools.ietf.org, 2013
108. Aboba, B., Esibov, L. and Thaler, D.: “RFC 4795: Link-local Multicast Name Resolution (LLMNR)”, http://tools.ietf.org, 2007

109. Microsoft, “Peer Name Resolution Protocol (PNRP) Version 4.0”, https://msdn.microsoft.com/en-us/library/cc239047.aspx, retrieved 2016
110. Vixie P, Thomson S, Rekhter Y, Bound J.: “RFC2136: Dynamic Updates in the Domain Name System”, http://tools.ietf.org, 1997
111. Rosenbaum R.: “RFC1464: Using the Domain Name System to Store Arbitrary String Attributes”, http://tools.ietf.org, 1993
112. Gulbrandsen A, Vixie P, Esibov L.: “RFC 2782: A DNS RR for Specifying the Location of Services (DNS SRV)”, Internet Engineering Task Force (IETF) Standards Track, http://tools.ietf.org, 2000
113. Banerjee A., Wallace S.: “DDI: A Comprehensive IP Address Management Solution”, http://studylib.net/doc/14404783/ddi--a-comprehensive-ip-address-management-solution-white..., retrieved 2016
114. Corral, J. et al.: “End-to-end Active Measurement Architecture in IP Networks”, Proceedings of Passive and Active Measurement Workshop PAM’03, 2003
115. Cottrell L.: “Web reference Network Monitoring Tools”, http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html, retrieved 2016
116. Raisanen, V. et al.: “RFC 3432, Network Performance Measurement with Periodic Streams”, http://tools.ietf.org, 2002
117. Mahdavi, J., Paxson, V.: “RFC 2678, IPPM Metrics for Measuring Connectivity”, http://tools.ietf.org, 1999
118. Almes, G. et al.: “RFC 2680, A One-way Packet Loss Metric for IPPM”, http://tools.ietf.org, 1999
119. Koodli R., Ravikanth R.: “RFC 3357, One-way Loss Pattern Sample Metrics”, http://tools.ietf.org, 2002
120. Almes G. et al.: “RFC 2681: A Round-trip Delay Metric for IPPM”, http://tools.ietf.org, 1999
121. Shalunov, S. et al.: “RFC 4656: A One-way Active Measurement Protocol (OWAMP)”, http://tools.ietf.org, 2006
122. Klensin J., Padlipsky M.: “RFC5198: Unicode Format for Network Interchange”, http://tools.ietf.org, 2008
123. Cerf V.: “RFC20: ASCII Format for Network Interchange”, http://tools.ietf.org, 1969
124. Cotton M., Eggert L., Touch J., Westerlund M., Cheshire S.: ”Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry”, http://tools.ietf.org, 2011.

9 Appendix A

For the reasons of maintaining compatibility with the IEEE 802.11 standard, mechanisms proposed in this thesis use the Information Element (IE) data format specified therein. As suggested in the standard the Vendor Specific IE is employed, which in turn identifies a specific vendor-specified IE type with use of additional data fields:

- IEEE-assigned OUI identifying defining organization
- IE Type field specifying a precise IE type within the OUI.

It has been assumed that OUI will be the same for all methods described in this thesis, while the IE Type will be used to differentiate between newly defined IEs. Their full list, along with assigned IE Type values is provided in Table 6.

Table 6 IE Type definitions within an IEEE-assigned OUI

IE Type field value	IE Type
0x00	ARPREQ
0x01	ARPREP
0x02	DNSREQ
0x03	DNSREQExt
0x04	DNSRESP
0x05	HLSA
0x06	MGGI

In case of Mesh Gate Groups solution, it has been necessary to define new types of Multihop Action management frames. The specific type of such frame is indicated by a value of Multihop Action field of its header. The complete list of values, combining both standard and newly defined, is provided in Table 7.

Table 7 Multihop Action field value definitions

Multihop Action field value	IE Type
0x00	Proxy Update
0x01	Proxy Update Confirmation
0x02	Proxy Group Update
0x03	Proxy Group Confirmation
0x04	MGGA Advertisement
0x05	MGGA Selection