XIX Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2009
Oddział Gdański PTETiS
Referat nr 24

WYKORZYSTANIE PROTOKOŁU UDP DO MONITOROWANIA OBIEKTÓW ZA POŚREDNICTWEM PUBLICZNEJ SIECI INTERNET

Michał PORZEZIŃSKI[1] , Grzegorz REDLARSKI[2]

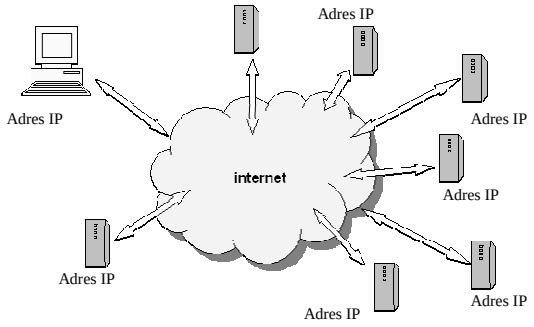
1. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: (58) 347-29-35 fax: (58) 347-18-02 e-mail: m.porzezinski@ely.pg.gda.pl
2. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: (58) 347-23-17 fax: (58) 347-18-02 e-mail: g.redlarski@ely.pg.gda.pl

Streszczenie: W referacie przedstawiono ideę monitorowania stanu rozproszonych obiektów za pośrednictwem publicznej sieci Internet z wykorzystaniem bezpołączeniowego protokołu UDP. Omówiono właściwości metod przesyłania danych oraz rodzaje i źródła błędów komunikacji powodujących ich utratę. Przedstawiono metodykę i wyniki przeprowadzonych badań niezawodności komunikacji w publicznej sieci Internet oraz najistotniejsze, wynikające z nich wnioski.

Słowa kluczowe: Internet, monitorowanie, UDP

1. WPROWADZENIE

Podczas eksploatacji urządzeń technicznych bardzo często zachodzi potrzeba monitorowania ich aktualnego stanu i sygnalizowania wystąpienia ewentualnych uszkodzeń. Klasycznym rozwiązaniem systemu nadzoru, stosowanym w przemyśle, jest wykorzystanie gotowego opro-gramowania typu SCADA (Supervisory Control and Data Acquisition) komunikującego się ze sterownikami PLC za pomocą lokalnej sieci komputerowej. W większości wypadków takie rozwiązanie jest w pełni zadowalające. Istnieją jednak systemy charakteryzujące się znacznym rozproszeniem nadzorowanych obiektów, obejmujące swoim zasięgiem duży obszar. W takim przypadku typowe rozwiązania przemysłowe mogą być zbyt drogie lub niewystarczające i uzasadnione może być wówczas opracowanie specjalizowanego systemu nadzoru [4]. Stosunkowo tanim i skutecznym rozwiązaniem jest wykorzystanie do tego celu infrastruktury sieci Internet. Podstawową zaletą tego rozwiązania jest wykorzystanie powszechnie dostępnej, taniej, sprawdzonej w działaniu infrastruktury warstwy fizycznej i stosowanych w niej rozwiązań. Struktura sieci jest dla systemu zarządzania całkowicie niewidoczna, a sieć oferuje gotowe usługi transportowe bazujące na adresowaniu IP (rys.1). Inną, istotną zaletą takiego rozwiązania jest użycie znanych, sprawdzonych w działaniu i wbudowanych w wiele popularnych systemów operacyjnych protokołów rodziny TCP/IP. Do podstawowych pośród nich, mogących znaleźć zastosowanie w systemie nadzoru należą: UDP i TCP [4], które wspólnie zaliczane są wyłącznie do warstwy transportowej modelu TCP/IP (rys.2).



Rys. 1. Idea wykorzystania sieci Internet do monitorowania stanu rozproszonych obiektów

Mechanizmy funkcjonowania	Warstwa TCP/IP
HTTP, SNMP, SMTP i in.	Aplikacji
TCP, UDP	Transportowa
IP, ICMP	Internetu
Network access driver	Dostępu do sieci

Rys. 2. Uproszczony model stosu protokołów TCP/IP

Protokół TCP oferuje usługę niezawodnego przesyłania danych [2]. Wymaga jednak wcześniejszego nawiązania połączenia i utrzymania go, co wiąże się z koniecznością zarezerwowania odpowiednich zasobów na urządzeniach biorących udział w wymianie danych. W przypadku stacji operatorskiej, która monitoruje dużą liczbę obiektów, a informacja o stanie obiektów przesyłana jest stosunkowo rzadko, rozwiązanie takie może być nieefektywne.
Bardziej efektywną metodą jest wykorzystanie bezpołączeniowego protokołu UDP. Przy projektowaniu systemu monitorowania należy uwzględnić jednak fakt, że UDP jest z definicji protokołem zawodnym. Do ochrony przed potencjalnymi błędami transmisji danych wykorzystuje on jedynie mechanizm sumy kontrolnej. Tak więc utrata danych może być również wynikiem szeregu innych zdarzeń, które mogą wystąpić w sieci [3].

Recenzent: Dr hab. inż. Dariusz Świsulski – Wydział Elektrotechniki i Automatyki
Politechnika Gdańska

2. METODY MONITOROWANIA

W systemach monitorowania do przekazywania informacji o stanie nadzorowanego obiektu można stosować metodę zdarzeniową, metodę cyklicznego odpytywania oraz ich odmiany.

Metoda zdarzeniowa polega na wysyłaniu informacji przez stronę nadzorowaną w chwili zmiany stanu nadzorowanego obiektu. Jej zaletą jest brak konieczności posiadania stałego adresu IP przez stronę nadzorowaną oraz znikome obciążenie sieci. Metoda ta nie może być jednak stosowana w czystej postaci, w przypadku protokołu UDP. Utrata danych nie zostanie bowiem zauważona i istnieje duże prawdopodobieństwo, że stacja monitorująca będzie posiadać nieprawdziwą informację o stanie obiektu. Wprowadzenie na poziomie warstwy aplikacji mechanizmu potwierdzania odebranych danych przez stację zarządzającą, nie rozwiązuje w całości problemu, gdyż w przypadku długotrwałej przerwy w łączności stacja monitorująca nie ma możliwości wykrycia takiego stanu. Skutecznym rozwiązaniem problemu jest dopiero wprowadzenie po stronie stacji monitorującej licznika czasu, w którym muszą zostać odebrane kolejne dane z informacją o statusie nadzorowanego obiektu. Brak informacji w zadanym okresie czasu może zostać zasygnalizowany jako brak łączności.
W przypadku metody odpytywania, polegającej na wysyłaniu przez stację zarządzającą zapytań o stan nadzorowanego obiektu, brak odpowiedzi może być łatwo wykryty i zapytanie o stan obiektu może zostać powtórzone. W przypadku braku uzyskania odpowiedzi w zadanej liczbie prób może zostać zgłoszony stan braku komunikacji. Konieczne jest jednak posiadanie przez stronę nadzorowaną stałego adresu IP, który musi być znany stacji nadzorującej. W metodzie tej występuje także znacznie większe obciążenie sieci, co w przypadku nadzorowania bardzo dużej liczby obiektów może być istotnym graniczeniem.

Często wybieranym rozwiązaniem jest połączenie obu metod. Wówczas okres odpytywania może być dłuższy (tak, by zagwarantować wykrycie braku komunikacji w zadanym czasie), podczas gdy czas reakcji na zmianę stanu pozostaje nadal krótki. Rozwiązanie takie stosowane jest w przypadku protokołu SNMP (wykorzystującego protokół UDP jako warstwę transportową), w którym oprócz klasycznego mechanizmu odpytywania funkcjonuje również mechanizm zdarzeniowy wykorzystujący tzw. pułapki [5]. Protokół ten, choć dedykowany jest do zarządzania elementami sieci komputerowej może być z powodzeniem stosowany również do nadzoru innych obiektów technicznych [3].

W każdej z metod istotnym elementem są jej parametry tj.: okres odpytywania, liczba prób, okres oczekiwania na potwierdzenie. Optymalny dobór tych parametrów jest możliwy dopiero po określeniu charakteru błędów, jakich należy się spodziewać w danej sieci.

3. ŹRÓDŁA BŁĘDÓW

Charakteryzując potencjalne błędy powodujące utratę danych protokołu UDP należy rozważać dwa aspekty. Pierwszy związany jest z błędami przypadkowymi powstającymi zwykle na poziomie warstwy fizycznej sieci komputerowej, a drugi z błędami związanymi z funkcjonowaniem urządzeń obsługujących wyższe warstwy protokołu.

Przyczyn powstawania błędów transmisji na poziomie warstwy fizycznej sieci komputerowej należy upatrywać przede wszystkim: w zakłóceniach EMI i RFI, w nieprawidłowym funkcjonowaniu struktury sprzętowej urządzeń wchodzących w skład danej sieci, będącym często skutkiem źle zaprojektowanej topologii fizycznej sieci, uszkodzeniami mechanicznymi torów transmisyjnych oraz awariami zasilania.

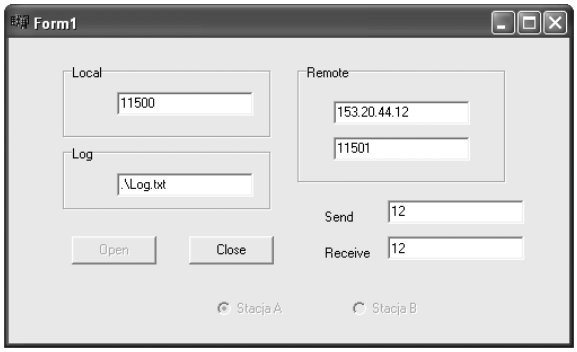
Najczęstszych przyczyn nieprawidłowo zaprojektowanej topologii fizycznej sieci komputerowej należy upatrywać w przekroczeniu dopuszczalnych parametrów użytych mediów transmisyjnych (np. długości okablowania), nieprawidłowej realizacji połączeń kablowych (np. o zbyt dużej wartości impedancji przejścia), zbyt wąskiej szerokości pasma transmisyjnego w stosunku do liczby urządzeń mających dostęp do współdzielonego medium czy wreszcie, w stosowaniu niewłaściwych urządzeń sieciowych. Wszystkie wymienione czynniki mogą być przyczyną występowania zwiększonej liczby kolizji w sieci. W efekcie tego może nastąpić nie tylko spadek wydajności sieci, ale również zwiększona utrata danych, przesyłanych za pośrednictwem protokołu UDP .

Uszkodzenia urządzeń sieciowych powodujące utratę transmisji często są związane z awariami interfejsów komunikacyjnych oraz różnego rodzaju podzespołów wewnętrznych tych urządzeń oraz, z awariami zasilania. Powyższe czynniki oraz losowe uszkodzenia mechaniczne torów transmisyjnych powodują, że dana ścieżka transmisyjna, staje się niedostępna. Przypadek taki wymaga czasu niezbędnego na wyszukanie innej (sprawnej) drogi transmisji w celu ponownego i szybkiego osiągnięcia zbieżności danej sieci.

Utrata pakietów IP w urządzeniach sieciowych, takich jak przełączniki i routery może być także wynikiem nadmiernego obciążenia spowodowanego dużą liczbą przesyłanych danych w krótkim przedziale czasu i związanego z tym przepełnienia się ich wewnętrznych buforów.

4. TESTOWANIE TRANSMISJI DANYCH

Do badania niezawodność transmisji danych UDP w sieci Internet, wykorzystano specjalnie przygotowane oprogramowanie o nazwie TestUdp, którego widok okna przedstawiono na rysunku 3.

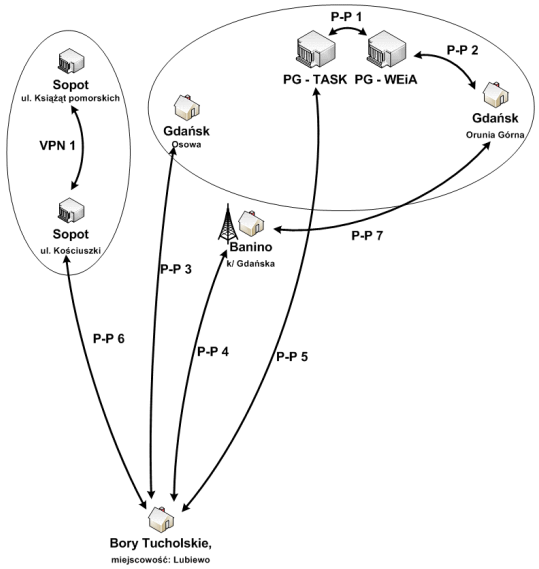


Rys. 3. Widok okna programu do monitorowania pracy sieci

Oprogramowanie to wymaga uruchomienia w punktach diagnostycznych pomiędzy którymi zachodzi proces transmisji danych. Jedna z aplikacji (Stacja A) pełni wówczas rolę hosta nadawczego (lokalnego), a druga (Stacja B) rolę hosta odbiorczego (zdalnego), który odsyła odebrane dane z powrotem do nadawcy. Konfiguracja oprogramowania wymaga podania adresu IP hosta zdalnego, oraz określenia numerów

portów, które mają być wykorzystane w procesie transmisji. Liczba segmentów UDP wysłanych w 10 s odstępach czasu (pole Send) oraz odebranych (pole Received) wizualizowana jest w sposób ciągły. Szczegółowe informacje na temat uzyskanych wyników badań, tj.: data i godzina (czas) transmisji, numer segmentu danych, opóźnienie transmisji oraz informacja na temat udanej lub nieudanej próby transmisji, gromadzone są w pliku tekstowym pełniącym rolę logu zdarzeń.

Prowadząc badania niezawodności transmisji danych w sieci Internet, ograniczono się do kilku punktów węzłowych (rys. 4) pomiędzy którymi w różnych przedziałach czasu ustanawiano proces wymiany danych protokołu UDP.



Rys. 4. Mapa połączeń realizowanych podczas badań

Uzyskane wyniki zaklasyfikowano do dwóch grup tematycznych. W pierwszej z nich wymiana informacji zachodziła pomiędzy dwoma punktami węzłowymi przewodowej sieci VPN. Z kolei w drugiej badano niezawodność transmisji w sieci Internet (połączenia oznaczone symbolem P-P), uwzględniając możliwość wymiany informacji w oparciu o technologię przewodową i bezprzewodową oraz możliwość korzystania z łączy transmisyjnych różnych dostawców usług internetowych. Analizę wyników badań w obydwu przypadkach przedstawiono w dalszej części opracowania.

5. ANALIZA NIEZAWODNOŚCI TRANSMISJI DANYCH W SIECI INTERNET

Prowadząc badania niezawodności transmisji protokołu UDP w sieci Internet nieznana była droga transmisji danych pomiędzy punktami węzłowymi (rys. 4), z wyjątkiem połączenia P-P 1, w przypadku którego korzystano z wysokiej klasy łączy, uczelnianej sieci LAN. Dostępne były jedynie informacje na temat dostawców usług internetowych po obu stronach oraz położenia geograficznego danego punktu węzłowego.
W wyniku badań (tab. 1) stwierdzono, że uzyskane wyniki mają charakter losowy ze względu na wielkość opóźnienia transmisji i liczbę traconych danych UDP. Podczas wszystkich przeprowadzonych procesów transmisji występuje ponadto utrata segmentów danych UDP (jeśli proces transmisji zostaje uruchomiony na odpowiednio długi okres czasu), których liczba w zdefiniowanej jednostce czasu (np. 1 h) jest różna i zależna od aktualnego stanu łączy pomiędzy punktami węzłowymi (np. uczelniane łącza P-P 1, okazują się bardziej niezawodne od łączy wykorzystywanych w procesie transmisji P-P 4 realizowanej z udziałem sieci bezprzewodowej).

Tablica 1. Wyniki analizy niezawodności transmisji danych opartej na protokole UDP

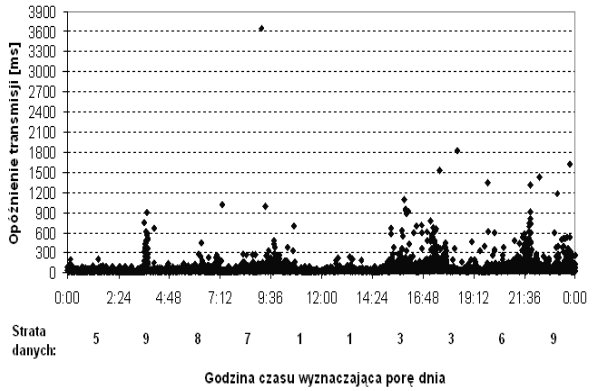
Nr połączenia (rys. 4)	Czas połączenia **[hh:mm:ss]**	**Liczba danych**	**Liczba błędów (1/2/3/4/5)***	**Liczba błędów [%]**	**Opóźnienie średnie [ms]**	**Opóźnienie max [ms]**	**Opóźnienie min [ms]**	**Informacja o węzłach**
P-P 1	23:32:10	8474	10 (5/0/0/0/1)	0,12	0,056	47	10	Sieć uczelniana – Sieć uczelniana
P-P 2	10:46:31	3817	38 (38/0/0/0/0)	0,99	2,003	4641	0	Sieć uczelniana – sieć kablowa (TV)
P-P 3	07:08:40	2597	11 (3/0/1/0/1)	0,42	186,49	1829	31	Neostrada TP – Neostrada TP
P-P 4	06:38:16	1969	148 (118/12/2/0/0)	7,52	200,67	1482	15	Sieć bezprzewodowa – Neostrada TP
P-P 5	02:07:31	766	1 (1/0/0/0/0)	0,13	38,56	250	31	Sieć uczelniana – Neostrada TP
P-P 6	50:17:31	18106	149 (142/2/1/0/0)	1,16	0,0612	78	0	Sieć uczelniana – Neostrada TP
P-P 7	26:03:23	9374	54 (54/0/0/0/0)	0,58	52,84	3650	15	Sieć bezprzewodowa – Neostrada TP
VPN 1	26:52:30	9676	190 (186/2/0/0/0)	1,96	36,13	31	125	TP S.A. – TP S.A.

* Liczba błędów występujących kolejno po sobie: pojedynczych/podwójnych/potrójnych ...

Czas opóźnienia transmisji może być różny w przypadku różnych pakietów danych i zależny jest on od pory dnia, co wynika niewątpliwe ze zmiennego w tym czasie obciążenia łączy przesyłowych. Na podstawie rysunku 5. przedstawiającego przykład takiej sytuacji, dla procesu transmisji P-P 7, można stwierdzić, że w godzinach zwiększonej aktywności na łączach (godziny pracy i pora wieczorna) występują większe opóźnienia.

Ponadto można zauważyć, że w godzinach pracy (od 7.12 do 16.48) następuje znacznie mniejsza utrata danych (15 strat), aniżeli poza tymi godzinami (37 strat).
Analiza wyników pokazuje również, że większość błędów to błędy pojedyncze związane najprawdopodobniej z przypadkową utratą danych. Należy się jednak liczyć również z możliwością występowania dłuższych przerw w funkcjonowaniu kanałów transmisyjnych, rzędu od kilkunastu do kilkudziesięciu sekund.

Jednym z rozwiązań poprawiających niezawodności transmisji opartej na protokole UDP jest tworzenie redundantnych kanałów transmisyjnych. Polega ono na ustanawianiu dodatkowych sesji w zakresie przesyłu tych samych segmentów danych.



Rys. 5. Dobowa charakterystyka czasów opóźnienia transmisji i utraty danych UDP na przykładowym łączu w sieci Internet

Przykład analizy wyników badań, dla N = 1, 2,..., 4, torów redundantnych przedstawiono w tablicy 2.

Tablica 2. Mechanizm redundancji w procesie transmisji danych

N	Liczba danych	Liczba błędów	Maksymalne opóźnienie [ms]
1	18106	62	94
2	18106	36	94
3	18106	69	46
4	18106	149	78
$1 \wedge 2$	18106	10	–
$1 \wedge 3$	18106	6	–
$1 \wedge 4$	18106	4	–
$2 \wedge 3$	18106	13	–
$2 \wedge 4$	18106	5	–
$3 \wedge 4$	18106	20	–
$1 \wedge 2 \wedge 3$	18106	6	–
$1 \wedge 2 \wedge 4$	18106	4	–
$1 \wedge 3 \wedge 4$	18106	4	–
$2 \wedge 3 \wedge 4$	18106	5	–
$1 \wedge 2 \wedge 3 \wedge 4$	18106	4	–

Innym rozwiązaniem może być zastosowanie redundancji polegającej na zwielokrotnieniu liczby wysyłanych danych zawierających tą samą informację. Z uwagi na charakter przerw w łączności, które mogą obejmować nawet do kilkudziesięciu sekund, uzasadnione jest powtarzanie informacji z odpowiednio dużym odstępem czasowym, co zmniejsza prawdopodobieństwo całkowitej utraty informacji.

6. PODSUMOWANIE

Rozwijająca się dynamicznie infrastruktura publicznej sieci Internet może stanowić podstawę budowy niedrogich systemów monitorowania obiektów, które są rozproszone na dużym obszarze.

Przeprowadzone badania pokazały, że jakość transmisji danych w oparciu o standardowy protokół UDP jest wystarczająca do realizacji typowych systemów monitorowania, w których do zaakceptowania jest czas reakcji rzędu minuty.

Z uwagi na zaobserwowany losowy charakter błędów transmisji skutecznymi metodami poprawy niezawodności transmisji jest tworzenie redundantnych kanałów transmisyjnych oraz powtarzanie informacji w odpowiednio dobranych odstępach czasowych.

Osobnym zagadnieniem jest ochrona przesyłanej informacji i zabezpieczenie systemu przed sabotażem ze strony innych użytkowników sieci. Stosowane w tym celu rozwiązania opierają się na różnych metody autoryzacji źródła informacji, jej szyfrowaniu i stosowaniu znaczników czasowych lub numeracji pakietów.

Rozwiązaniem zwiększającym bezpieczeństwo może być również zastosowanie wirtualnej sieci prywatnej VPN, umożliwiającej utworzenie tunelu łączącego wybrane podsieci poprzez publiczny Internet.

Niezależnie od przyjętych metod ochrony zawsze istnieje ryzyko ataku DoS, przed którym obrona jest bardzo trudna lub zwykłego chwilowego przeciążenia sieci. Dlatego też bardzo istotne jest ciągłe monitorowanie drożności kanału przesyłu informacji i sygnalizowanie dłuższych przerw w łączności, które w przypadku stacji monitorujących oznaczają możliwość posiadania nieaktualnej informacji o stanie nadzorowanego obiektu.

7. BIBLIOGRAFIA

1. Ballew S.M.: Zarządzanie sieciami IP za pomocą routerów Cisco. Oficyna Wydawnicza ReadMe, Warszawa 1998, ISBN 83-87216-48-8.
2. Comer D.E.: Sieci komputerowe TCP/IP. Tom 1 Zasady, protokoły, architektura, WNT Warszawa 1997, ISBN 83-204-2056-3.
3. Porzeziński M.: Wykorzystanie protokołu SNMP do zdalnego monitorowania i sterowania elementami instalacji KNX, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej 2008.
4. Porzeziński M., Mazur L.: Remote monitoring and control of technical systems using internet network technology, Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety TEHOSS, Gdańsk 2005
5. Stallings W.: Protokoły SNMP i RMON. Vademecum profesjonalisty. Wydawnictwo Helion, 2003, ISBN 83-7197-920-7.

USAGE OF THE UDP PROTOCOL FOR OBJECTS MONITTORING THROUGHT THE PUBLIC INTERNET NETWORK

Key-words: Internet, monitoring, UDP

The idea of monitoring of distributed objects state by the UDP protocol in the Internet network has been presented in this paper. The methods of data transferring, sorts and sources of transmission errors have been described. Moreover the computer program to tests of reliability in transmission process and the main results of the tests has been presented.