Mitigating Traffic Remapping Attacks in Autonomous Multihop Wireless Networks

Jerzy Konorski and Szymon Szott

***Abstract*—Multihop wireless networks with autonomous nodes are susceptible to selfish traffic remapping attacks (TRAs). Nodes launching TRAs leverage the underlying channel access function to receive an unduly high Quality of Service (QoS) for packet flows traversing source-to-destination routes. TRAs are easy to execute, impossible to prevent, difficult to detect, and harmful to the QoS of honest nodes. Recognizing the need for providing QoS security, we use a novel network-oriented QoS metric to propose a self-enforcing game-theoretic mitigation approach. By switching between TRA and honest behavior, selfish nodes engage in a noncooperative multistage game in pursuit of high QoS. We analyze feasible node strategies and design a distributed signaling mechanism called DISTRESS, under which, given certain conditions, the game produces a desirable outcome: after an upper bounded play time, honesty tends to become a selfish node's best reply behavior, while yielding acceptable QoS to most or all nodes. We verify these findings by Monte Carlo and ns-3 simulations of static and mobile nodes.**

***Index Terms*—Autonomous nodes, game theory, IEEE 802.11, Quality of Service (QoS) security, selfish attacks, wireless networks.**

I. Introduction

WIRELESS networks with autonomous nodes, which we refer to as multihop autonomous wireless networks (MAWiNs), are an active research field. MAWINs embody the self-organizing network concept [1] in autonomous mobile mesh networks [2], [3], autonomous vehicular networks [4], autonomous sensor networks [5], and flying ad hoc networks [6]. In large-scale IoT systems, multihop cooperative relaying has been observed to improve the throughput, reliability, and energy efficiency of the data exchange between end-user devices (e.g., smart meters) and gateway nodes (e.g., data aggregation points) [7]–[11].

Besides classical threats to wireless transmission, MAWiNs face unique security threats due to node autonomy. The sustained operation of such networks relies on the nodes' benevolent compliance with cooperative protocols, such as fair channel access, transit packet forwarding, and route discovery. Nodal cooperation entails certain costs in terms of energy expenditure and Quality of Service (QoS) received by source (locally generated) traffic, e.g., fair channel access requires deferment of one's packet transmission, which causes delays. Autonomous nodes thus tend to exhibit rational (selfish) behavior, seeking a favorable tradeoff between received QoS and incurred costs. This makes MAWiNs susceptible to selfish attacks that abuse the employed network protocols to the attacker's benefit.

Selfish attacks, which attempt to acquire undue network resources through aggressive competition, range from the link layer to the transport layer. These attacks usually consist of the manipulation of sensitive protocol parameters, e.g., the contention window of IEEE 802.11 [12] or congestion control settings of TCP [13]. They have been countered by several detection- or prevention-type mechanisms [14] and often investigated using game theory [15], e.g., for incentivizing selfish IoT devices to participate in cooperative communication [16], [17]. A less known variety of selfish attacks by the name *QoS abuse* [18] or traffic remapping attack (TRA) [19] emerges in environments supporting traffic class-based QoS differentiation to enforce user-network QoS contracts such as service-level agreements (SLAs) [20]. By falsely assigning traffic to classes, an attacker node abuses provisioned QoS policies and can receive a higher QoS level for its source traffic at the cost of honest nodes' source traffic. MAWiNs make a perfect scene for TRAs, especially if they offer QoS differentiation as part of the network's mission rather than a metered service, which makes launching a TRA costless. Thus, on top of classical problems with network resource deficiency and/or mismanagement, threats to contractual QoS can arise from QoS abuse and should be addressed by a new class of defense mechanisms that can be collectively termed *QoS security*. Their task is to protect information security, in the sense of enforcing QoS guaranteed to honest nodes, in the presence of QoS abuse.

In wireless networks using IEEE 802.11, TRAs can exploit the enhanced distributed channel access (EDCA) function. EDCA defines four access categories (ACs), each with its own parameters controlling the priority and duration of medium access [12]. Packets are mapped to ACs based on the differentiated services code point (DSCP) in their IP header, which reflects the traffic's Class of Service (CoS) [21]. For simplicity assume that DSCP can be either expedited forwarding

Manuscript received 10 September 2021; revised 26 November 2021; accepted 7 January 2022. Date of publication 18 January 2022; date of current version 25 July 2022. This work was supported in part by PLGrid Infrastructure. The work of Jerzy Konorski was supported by the National Science Center, Poland, under Grant UMO-2016/21/B/ST6/03146. The work of Szymon Szott was supported by the Polish Ministry of Science and Higher Education with the subvention funds of the Faculty of Computer Science, Electronics and Telecommunications, AGH University. *(Corresponding author: Szymon Szott.)*

Jerzy Konorski is with the Department of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 80-233 Gdańsk, Poland (e-mail: jekon@eti.pg.edu.pl).

Szymon Szott is with the Faculty of Computer Science, Electronics and Telecommunications, AGH University of Science and Technology, 30-059 Krakow, Poland (e-mail: szott@agh.edu.pl).

Digital Object Identifier 10.1109/JIOT.2022.3143713

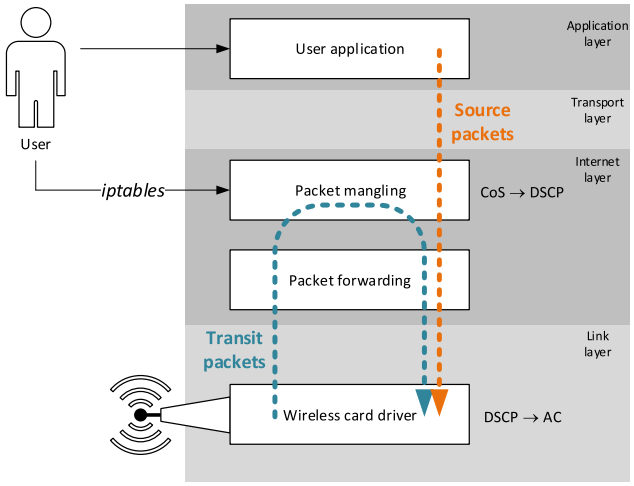


Fig. 1. Packet flow and TRA execution at an attacker node in the TCP/IP model.

(EF) or best effort (BE). The CoS-to-DSCP mapping is implemented by the Internet layer packet mangling software, such as Linux `iptables`. TRAs can be easily executed by setting DSCP = EF in source traffic whose CoS maps to BE and DSCP = BE in forwarded (transit) traffic whose CoS maps to EF (cf. Fig. 1). In contrast, AC parameter modification requires tampering with the DSCP-to-AC mapping embedded in wireless card drivers. Furthermore, TRAs are difficult to detect: determining if higher layer traffic matches its DSCP designation requires deep packet inspection [22] and global knowledge of the DSCP assignment policy.

In single-hop settings, TRAs have been shown to drastically reduce the throughput of honest nodes unless the latter employs a carefully designed MAC-layer discouragement scheme [22]. The multihop nature of MAWiNs poses several additional challenges for a defense scheme.

1) A selfish node can both promote its source traffic and demote transit traffic.
2) A locally performed TRA has an end-to-end impact: once assigned a false QoS designation, a packet retains it further down the route.
3) The impact of TRA is unclear *ex ante*, due to the complex interplay of multiple layers: PHY (hidden nodes), MAC (channel contention), and transport (flow control); this interplay also blurs QoS perception and rules out straightforward detection-based countermeasures.
4) The absence of single-broadcast hearability rules out simple punitive measures such as threats of jamming.
5) Heuristic end-to-end countermeasures against TRAs are moderately effective [19]; in particular, countermeasures that work well in single-hop settings, such as ACK dropping, fail in multihop settings [23].

Being rationally motivated, easy to execute, impossible to prevent, difficult to detect, and harmful to honest nodes, TRAs call for incentive-based defense. Unfortunately, the lack of a central authority rules out common approaches based on reputation building or Stackelberg games [7], [8], [24], hence a novel game-theoretic methodology is also needed. In [25], we presented an early formulation of the multihop TRA problem and preliminary insights into its impact upon the nodes' cost metric. A multistage game-type TRA mitigation scheme was proposed, whose convergence and alignment with nodes' rationality was only supported by numerical and Monte Carlo simulation arguments. Building on a more rigorous network model we offer herein a provably convergent, rational, and effective TRA mitigation scheme. Our approach follows "brinkmanship game theory" [26]: credible threats force nodes to toggle between TRA and honest behavior, and so engage in a noncooperative game in pursuit of high QoS. Although our analytical results apply to networks with static nodes, simulations show the scheme is also effective with node mobility. Our main contributions are as follows.

1) Based on a MAWiN model with a static topology and traffic flows, we formally define *plausible opportunistic* TRAs and discuss their motivation and impact.
2) We develop a heuristic end-to-end QoS metric that only uses information about the network topology and traffic flows. We verify it by simulation and comparison with alternative heuristics.
3) We design a distributed DISTRESS mechanism to signal the threat of service suspension due to ongoing TRAs. DISTRESS requires little data analysis and internode synchronization and needs not to distinguish between TRA and objectively harsh traffic conditions.
4) Using the developed QoS metric as a payoff function, we analyze the game arising among ill-behaved nodes under DISTRESS and state conditions of its desirable outcome. We show that after an upper bounded play time, honesty tends to become an ill-behaved node's best-reply behavior, keeping QoS acceptable to most or all nodes. These findings are verified by extensive Monte Carlo and time-true simulations of static and mobile nodes.

The remainder of this article is organized as follows. In Section II, we outline related work on QoS abuse in wireless networks and highlight the unsolved problems which justify our research, including the need for a macroscopic MAWiN network model. In Section III-A, we formulate a topology and traffic flow model, next used in Section III-B to formalize the notion of TRA. In Section III-C, we develop a MAWiN performance model and propose an end-to-end QoS metric; the latter is shown in Section III-D to yield quantitative insight into the motivation and impact of TRAs. In Sections IV-A and IV-B, respectively, we describe the one-shot TRA game arising among ill-behaved nodes and propose a model of multistage play to discourage TRAs. "Good" multistage strategies are analyzed in Section IV-C and validated by simulations in Section V. Section VI concludes this article.

II. Related Work

Selfish attacks in MAWiNs have mostly been studied at the Internet layer. The main attack under consideration has been packet dropping, also referred to as *forwarding/relaying misbehavior*. This attack can be considered as launched either on all packets (full dropping) or only on selected packets (partial dropping). In the latter case, the dropping can be either

probabilistic or deterministic (e.g., may specifically target some packet types such as routing control packets, or some source-to-destination routes).

The packet-dropping attack has been widely analyzed. Due to node autonomy and lack of any administrative control, only "soft" countermeasures are possible. Some proposals involve micropayment (credit) schemes, where a virtual currency is earned for relaying and next used to buy similar services [27]. Others have focused on the explicit identification of attackers. This can be done passively, e.g., through a watchdog mechanism where nodes promiscuously listen to the channel and observe offending behavior [28], or actively, e.g., using additional end-to-end acknowledgments to determine which routes contain packet dropping attackers [29]. Attacker identification can be enhanced through a complex audit- and reputation-based schemes where a node derives a reputation score of any other node from first-hand (watchdog-based) experience, and possibly from reputation scores calculated by third-party nodes [30].

The main response to Internet layer attacks has been of a reciprocation nature, i.e., restricted forwarding of attackers' source packets. This gives rise to numerous analyses of the underlying forwarding game. Various strategies (e.g., tit-for-tat) have been considered to enforce honest packet forwarding; see [31] for a systematic treatment. A complementary response is to route traffic around attackers. However, this is beneficial to them, as they can expend less energy and bandwidth on forwarding [32].

At the link layer, most attacks have found the IEEE 802.11 channel access function [12] an easy target. Numerous studies have shown that launching a *backoff attack*, i.e., changing the transmission deferment parameters (such as idle carrier sensing or backoff times) yields the attacker a considerable increase in throughput and access delays at the cost of honest nodes [33], [34]. Link-layer attacks have mostly been studied in a single-hop setting, which is not surprising given their local-scope nature.

QoS differentiation opens new vulnerabilities to attacks referred to in the literature as "QoS abuse" [35], [36] or "class hijacking" [37], [38]. In this area, researchers have also studied selfishness in forwarding multimedia streams [39], nodes misreporting channel request parameters [40], and various cooperative forwarding strategies [41]. Campus network designers have long foreseen that too much high-priority traffic may overwhelm the available bandwidth and/or switch capacity [18]. In infrastructure-based networks under administrative supervision, an obvious solution is to allow traffic marking with CoS/DSCP only at the network edge, subject to valid traffic contracts, rather than at users' premises. However, QoS abuse, exemplified by TRAs, is much harder to defend against in ad hoc networks, which lack a well-defined user-to-network interface.

TRAs are tied to the link layer: despite being launched at the Internet layer (through modifying DSCP), they exploit the underlying channel access prioritization. Local-scope TRAs were considered in [22] and acknowledged as a threat to transmission opportunity sharing protocols [42]. Multihop settings are also vulnerable [43]; [44] discusses attacks in IEEE 802.11s mesh networks, [23]—in two-hop relay networks, while [19] provides an overview of TRAs in ad hoc networks along with a discussion of attack detection and defense measures. Additionally, [45] studies a practical relaying scenario where users may execute TRAs.

From a detection viewpoint, TRAs are more challenging in multihop settings than in single-hop ones. First, it is not always clear how local-scope manipulation of per-traffic class handling translates into end-to-end per-flow or per-packet performance. Second, Internet layer attacks bring less pronounced benefit to the attacker and less pronounced harm to the honest nodes than does aggressive competition for the radio channel under link-layer TRAs. Single-hop settings are also easier to defend: when a traffic remapping attacker has been identified, it can be punished by neighboring honest nodes via responding in kind, e.g., increased transmission rate or jamming [46]. In a multihop setting, however, the punishment of TRAs may prove ineffective if known local-scope defense mechanisms are directly mimicked. Thus, studies of selfish link-layer attacks in multihop wireless networks leave many insights to be gained.

In this article, we are interested in MAWiN-oriented defense mechanisms justifiable by noncooperative game-theoretic considerations, i.e., rendering TRAs nonbeneficial for attackers in terms of perceived QoS. This requires simple performance models of MAWiNs under TRAs that yield closed-form solutions and thus handy payoff functions for arising games. Few such models are known, none of them able to capture on a macroscopic level the complex interplay of channel access, node mobility, and intraflow competition due to multihop forwarding in the presence of hidden nodes. Existing models are usually limited to chain topologies [47], [48] or tied to specific analytical models of high complexity [49]; they do not consider traffic differentiation.

III. Network Model

In this section, we formalize the network and TRA description and develop an end-to-end performance model to quantify TRA motivation and impact. A summary of the notation used in this article is presented in Table I.

A. Topology, Routes, and Flows

A static MAWiN topology is represented by a directed graph $T = \langle N, L \rangle$, where N is the set of nodes, $L \subset N \times N$, and $(i, j) \in L$ iff $i \neq j$ and j is in the hearability range of i. Let N^* be the set of all directed acyclic routes in T and $R \subseteq N^*$ be the set of end-to-end routes in T as determined by the routing algorithm in use. Each route $r \in R$ is represented as a sequence of nodes $r = (i_1, \ldots, i_m)$ such that $i_1, \ldots, i_m$ are all distinct and $(i_{m'}, i_{m'+1}) \in L$ for all $m' = 1, \ldots, m-1$. Among these, i_1 and i_m are the source and destination nodes of r, denoted s_r and d_r, $i_2, \ldots, i_{m-1}$ are the transit nodes, and $\|r\| = m - 1$ is the hop length of r. We write $i \in r$ if r involves node i; for $i, j \in r$ write $i <_r j$ ($i \leq_r j$) if i precedes (precedes or coincides with) j on r. For $i \in r \backslash \{d_r\}$ denote by $\mathrm{succ}_{r,i}$ the immediate successor of i on r, and for $i \in r \backslash \{s_r\}$ denote by $\mathrm{pred}_{r,i}$ the immediate predecessor of i on r; for uniformity, define pred_{r,s_r} as s_r. (A node i' is said to be *hidden* from i

TABLE I
SUMMARY OF NOTATION USED

Symbol	Definition
ac	An e2e-flow's intrinsic AC
A	Set of attackers
$cost$	Nodal cost metric
$CH_i(r, ac)$	Set of h-flows competing with outgoing h-flow $(i, r, hac_i(r, ac))$
s_r, d_r	Source and destination nodes of route r
Δ	Set of in-distress nodes
Δ^*	Set of in-exposure nodes
$E_{R_F}(M)$	Set of nodes whose source traffic is forwarded by nodes in M
$E_{R_F^*}(M)$	Set of nodes forward-reliant on nodes in M
$fcost$	e2e-flow cost metric
F	Set of e2e-flows in the network
F^*	Set of survivable e2e-flows in the network
$G(k)$	Set of in-game nodes in stage k
Γ	Set of best-reply nodes
$\mathbf{h}_i$	Node i's history of membership in $A(k-1)$ and $A(k)$
H	Set of recognizable h-flows
I	Set of ill-behaved nodes
(j, r, hac)	An h-flow of e2e-flow (r, ac) incoming from node j
k	Stage of the TRA game
$mang()$	Packet mangling function (CoS-to-AC mapping)
map	Function determining ACs of outgoing h-flows
OH_i	Set of outgoing h-flows at node i
$pred_{r,i}$	Predecessor (previous-hop node) to node i on route r
$P_{r,i}$	Set of nodes that precede or coincide with node i on route r
σ	An action selection rule in the TRA game
$succ_{r,i}$	Successor (next-hop node) to node i on route r
r, $\|\|r\|\|$	An end-to-end route and its hop-length
(r, ac)	An e2e-flow of intrinsic AC ac following route r
$rank_i(r, ac)$	Performance metric for e2e-flow (r, ac) at node i
R	Set of all end-to-end routes in the network
R_F	Forwarding relationship
R_F^*	Forward-reliance relationship
$T = \langle N, L \rangle$	Network topology graph (set of nodes, set of links representing node hearability)

if $(i, i') \notin L$ and $\exists j \in N, r, r' \in R : j = \text{succ}_{r,i} = \text{succ}_{r',i'}$.) Denote $P_{r,i} = \{j | j \leq_r i\}$.

We model network traffic as composed of *end-to-end (e2e) flows*, each of which is a collection of packets of the same CoS $\in \{\text{EF}, \text{BE}\}$ and moving along the same route. The corresponding link-layer frames are handled by EDCA according to the assigned ACs contained in the AC fields of their headers. For ease of presentation, we restrict the used ACs to VO (real-time traffic such as voice/video) and BE (best-effort traffic), with VO having (statistical) priority over BE at the link layer. Since packet mangling amounts to a CoS-to-AC mapping, we define a function mang : $\{\text{EF}, \text{BE}\} \to \{\text{VO}, \text{BE}\}$ such that $\text{mang}(\text{EF}) = \text{VO}$ and $\text{mang}(\text{BE}) = \text{BE}$. An e2e-flow of a given CoS is represented as (r, ac), where $r \in R$ is its route and $ac = \text{mang}(\text{CoS})$ is its intrinsic AC as returned at s_r. Let $F \subseteq R \times \{\text{VO}, \text{BE}\}$ be the (quasistatic) set of e2e-flows offered by MAWiN users. Presumably, only nodes generating their own source traffic are interested in staying connected, therefore we assume that at least one e2e-flow is offered at each node, i.e.,

$$\{s_r | (r, ac) \in F\} = N. \tag{1}$$

For further analysis, it is necessary to formally state the fact that a source of a traffic flow is reliant on a set of nodes for forwarding its packets.

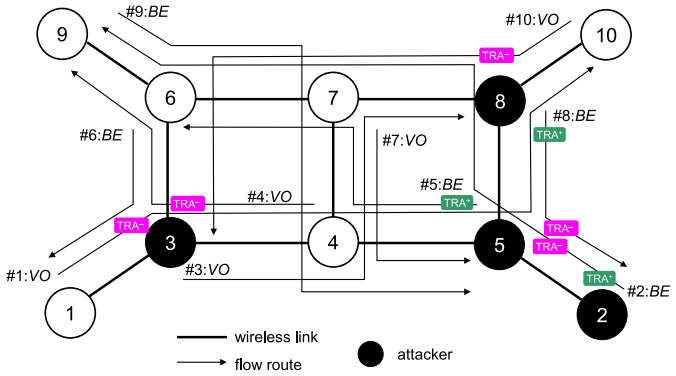


Fig. 2. Example MAWiN topology, e2e-flow routes, and experienced TRAs; node i is the source of e2e-flow #i with intrinsic AC indicated.

Definition 1: Let $R_F \subseteq N \times N$ be a binary relationship such that $(i, j) \in R_F$ iff j forwards i's source traffic, i.e., $\exists (r, ac) \in F : i = s_r \wedge j \in r \backslash \{d_r\}$ (in particular, $(s_r, s_r) \in R_F$). The transitive closure of R_F, denoted R_F^*, will be referred to as *forward-reliance*, i.e., $(i, j) \in R_F^*$ iff there exists a sequence of nodes $i_1, i_2, \ldots, i_k$ with $i_1 = i$ and $i_k = j$ such that i_{l+1} forwards i_l's source traffic, $l = 1, \ldots, k-1$.

Assume that a removal from the network of a forwarding node on r causes s_r to be removed as well. Then, $(i, j) \in R_F^*$ expresses node i's forward-reliance on node j in that a removal of j ultimately causes a removal of i. For $M \subseteq N$, let $E_{R_F}(M) = \{i \in N | \exists j \in M : (i, j) \in R_F\}$; the set of nodes forward-reliant on nodes in M is therefore $E_{R_F^*}(M)$. We have $M \subseteq E_{R_F}(M) \subseteq E_{R_F^*}(M)$, the first inclusion due to (1).

We use the notion of *hop (h-) flows* as the granulation level at which incoming traffic is recognized at a next-hop node. Packets of e2e-flow (r, ac) forwarded by $j = \text{pred}_{r,i}$, whose AC fields contain hac $\in \{\text{VO}, \text{BE}\}$, are recognized at node $i \in r$ as an h-flow (j, r, hac). (Possibly hac $\neq ac$, because AC fields can be modified hop-by-hop.) By convention, let e2e-flow (r, ac) be recognized at s_r as h-flow (s_r, r, ac). For example, if node 3 in Fig. 2 changes the AC fields of incoming packets, then e2e-flow #1, designated as (1, VO), is recognized as (1, r_1, VO) at node 1, (1, r_1, VO) at node 3, (3, r_1, BE) at node 4, etc., where $r_1 = (1, 3, 4, 5, 8, 10)$. Let $H \subseteq N \times R \times \{\text{VO}, \text{BE}\}$ be the set of recognizable h-flows.

Autonomous operation of node i is expressed as a function $\text{map}_i : H \to \{\text{VO}, \text{BE}\}$ according to which it sets ACs of h-flows. For an incoming h-flow (j, r, hac), where $j = \text{pred}_{r,i}$ and $i \in r \backslash \{s_r, d_r\}$, the new AC field forwarded by i further along r is given by $\text{map}_i(j, r, \text{hac})$.

B. Attack Model

We consider an attacker to be a selfish node that aims to receive a higher QoS level for its source traffic by performing a TRA, i.e., changing the traffic class of incoming transit or source flows. The Internet layer's packet mangling functionality is used as explained in Section I (Fig. 1) to interfere with the default CoS-to-AC mapping and modify the IP header fields of incoming packets, which are transmitted further along their path with a different MAC-layer priority. Except for the path's destination node, any node can potentially become an attacker. We assume that:

1) a MAWiN node is capable of assessing received QoS;
2) in terms of received QoS, a TRA can be beneficial to the attacker and harmful to other nodes;
3) a TRA can be performed at no expense and at no risk of detection or administrative punishment;
4) a subset of nodes are selfish and ready to become attackers.

A TRA can be formally described as follows.

Definition 2: A TRA that a node $i \in r\backslash\{d_r\}$ launches upon an incoming h-flow (j, r, hac), where $j = \text{pred}_{r,i}$, consists of changing its AC, i.e., configuring $\text{map}_i(j, r, \text{hac}) \neq \text{hac}$.

Such a definition captures the fact that the setting of AC fields under a TRA is both protocol compliant (the use of map_j is feasible) and ill-willed [inconsistent with $\text{mang}(\cdot)$].

We consider the behavior of a node that does not perform a TRA to be honest, whereas attackers can either upgrade or downgrade an incoming h-flow's AC. We formally define these behaviors as follows.

Definition 3: The behavior of node i with respect to h-flow (j, r, hac) can be classified as 1) *honest*, if the AC remains unchanged (i.e., $\text{map}_i(j, r, \text{hac}) = \text{hac}$); 2) *upgrading TRA* ($\text{TRA}^+$), if $\text{hac} = \text{BE}$ and $\text{map}_i(j, r, \text{BE}) = \text{VO}$; or 3) *downgrading TRA* (TRA^-) if $\text{hac} = \text{VO}$ and $\text{map}_i(j, r, \text{VO}) = \text{BE}$. Nodes that exhibit behavior 2) or 3) will be called *attackers*.

We adopt a simple model of an attacker: it will launch a TRA on all its source and transit flows provided that the former can be upgraded and the latter downgraded.

Definition 4: An attacker is called *plausible* if it never downgrades its own source traffic or upgrades transit traffic, i.e., $\text{map}_i(j, r, \text{hac}) = \text{hac}$ if ($\text{hac} = \text{VO}$ and $i = s_r$) or ($\text{hac} = \text{BE}$ and $i \neq s_r$), and *opportunistic* if it launches a TRA^+ or a TRA^- upon all h-flows it recognizes, subject to the plausibility constraints.

In our model, each attacker is assumed to be plausible opportunistic. Let $A \subseteq N$ denote the set of attackers. Given A, the new AC field $\text{hac}_i(r, ac)$ is derived as

$$\text{hac}_i(r, \text{BE}) = \begin{cases} \text{VO}, & s_r \in A \wedge P_{r,i}\backslash\{s_r\} \cap A = \varnothing \\ \text{BE}, & \text{otherwise} \end{cases}$$
$$\text{hac}_i(r, \text{VO}) = \begin{cases} \text{VO}, & P_{r,i}\backslash\{s_r\} \cap A = \varnothing \\ \text{BE}, & \text{otherwise.} \end{cases} \quad (2)$$

That is, $\text{hac}_i(r, \text{BE}) = \text{VO}$ if a TRA^+ at s_r and no TRA^- have been launched by the time the flow's packets reach i, and $\text{hac}_i(r, \text{BE}) = \text{BE}$ if no TRA or both a TRA^+ and a TRA^- have been launched. Similarly, $\text{hac}_i(r, \text{VO}) = \text{VO}$ if no TRA^- has been launched at nodes other than s_r, and $\text{hac}_i(r, \text{VO}) = \text{BE}$ if a TRA^- has been launched.[1]

For a 10-node MAWiN with $|N| = |F| = 10$, route hop lengths varying from $\|r\|_{\min} = 2$ to $\|r\|_{\max} = 5$, and $A = \{2, 3, 5, 8\}$, Fig. 2 displays TRAs experienced by each e2e-flow. One notes in particular that:

1) e2e-flows #3 and #6 are not attacked by the attacker node 3 due to the plausibility constraints;
2) likewise, e2e-flows #3, #7, and #9 are not attacked by their destinations (attacker nodes 8 and 5);
3) e2e-flow #1 with $ac = \text{VO}$ encounters three attacker transit nodes, of which the first launches a TRA^-, hence the second and third do not have to;
4) e2e-flows #2 and #8 experience a TRA^+ at their source nodes and a TRA^- at node 5; this is the maximum number of attacks an e2e-flow can experience.

[1]This type of downgrading attack is detectable at d_r by comparing the hac of the incoming h-flow with the flow's intrinsic AC (e.g., sent from s_r to d_r as encrypted metadata). While feasible, such detection is highly troublesome [19] and unable to pinpoint the attacker.

C. End-to-End Performance Model

Systematic evaluation of the impact of and countermeasures against TRAs requires an analytical performance model of a MAWiN in the presence of TRAs Motivated by the deficit of such models in the existing literature (cf. Section II), and building on the models of Sections III-A and III-B, we have developed an approximate rank-based model, described as follows. Each h-flow is assigned a rank depending on the number and priorities of h-flows it has to compete with for channel access. The collection of ranks of all h-flows constituting a given e2e-flow is then translated into an informative end-to-end QoS metric. At node i, the set of outgoing h-flows is

$$\text{OH}_i = \{(i, r, \text{hac}_i(r, ac))|(r, ac) \in F \wedge i \in r\backslash\{d_r\}\}. \quad (3)$$

For an outgoing h-flow $(i, r, \text{hac}_i(r, ac))$, the set $\text{CH}_i(r, ac)$ of competing h-flows consists of: 1) other outgoing h-flows at i, which compete via the local transmission queue; 2) outgoing h-flows at nodes in the hearability range of i, which compete via CSMA/CA; and 3) outgoing h-flows at nodes hidden from i, which compete via exclusive-OR reception at $\text{succ}_{r,i}$

$$\text{CH}_i(r, ac) = \text{OH}_i\backslash\{(i, r, \text{hac}_i(r, ac))\} \cup \bigcup_{j:(j,i)\in L} \text{OH}_j \cup \bigcup_{j:(j,\text{succ}_{r,i})\in L \wedge (j,i)\notin L} \text{OH}_j. \quad (4)$$

Per-hop performance at node i is determined by the pair $[\text{hac}, \text{CH}]_i(r, ac)$, where we use a succinct notation $[a, b]_i(x)$ instead of $[a_i(x), b_i(x)]$. We propose a per-hop performance metric $\text{rank}_i(r, ac)$ reflecting that an h-flow is better off at a node if it is VO, and competes with fewer and preferably BE h-flows. The metric ranks $[\text{hac}, vo, be]_i(r, ac)$ vectors, where $vo_i(r, ac)$ and $be_i(r, ac)$ represent the number of VO and BE h-flows in $\text{CH}_i(r, ac)$. Assume that a small rank is desirable.

To design $\text{rank}(\cdot)$, we used the Markovian model of EDCA [50] to calculate the normalized per-hop saturation throughput $S_i(r, ac)$ of e2e-flow (r, ac) at node i for various $\text{hac} = \text{hac}_{3i}(r, ac) \in \{\text{VO}, \text{BE}\}$, $vo = vo_i(r, ac) \in \{0, \ldots, 10\}$, and $be = be_i(r, ac) \in \{0, \ldots, 10\}$. For the resulting 14 520 pairs of (hac, vo, be) vectors, $\text{rank}(\cdot)$ represents a good fit if the following holds for a high percentage of pairs:

$$\text{rank}_i(r, ac)\big|_{\text{hac},vo,be} \leq \text{rank}_i(r, ac)\big|_{hac',vo',be'} \text{ iff } S_i(r, ac)\big|_{\text{hac},vo,be} \geq S_i(r, ac)\big|_{hac',vo',be'}. \quad (5)$$

A heuristic metric is

$$\text{rank}_i(r, ac) = \mathbb{1}_{\text{hac}=\text{BE}} \cdot \alpha \cdot (vo + \mathbb{1}_{vo>1 \vee be>2}) + \beta \cdot (vo + \mathbb{1}_{\text{hac}=\text{BE}}) + be \quad (6)$$

where $\mathbb{1}_{(\cdot)}$ is the indicator function, and the best fit (99.13% of the pairs) occurs at $\alpha = 40$ and $\beta = 10$. The preferences of h-flows are reflected: *vo* has more impact upon $\text{rank}_i(r, ac)$ than does *be* (because $\beta > 1$), and there is distinct separation between hac = VO and hac = 3BE (because $\alpha \gg \beta$).

For any $A \subseteq N$, rank$(\cdot)$ induces a heuristic e2e-flow cost metric we call *fcost*, additive for VO traffic delay and bottleneck-type for BE traffic throughput, defined as

$$fcost_{(r,ac)}(A) = \begin{cases} \frac{\sum_{i \in r \setminus \{d_r\}} \text{rank}_i(\text{hac}, r, ac)}{\|r\| - 1}, & ac = \text{VO} \\ \max_{i \in r \setminus \{d_r\}} \text{rank}_i(\text{hac}, r, ac), & ac = \text{BE} \end{cases} \tag{7}$$

where hac is given by (2) and the notation $fcost_{(r,ac)}(A)$ is meaningful, because hac depends on A. From (7), a nodal cost metric cost can be derived as a weighted sum

$$\text{cost}_i(A) = \sum_{(r,ac) \in F : s_r = i} \gamma_{r,i} \cdot fcost_{(r,ac)}(A) \tag{8}$$

where $\gamma_{r,i} \geq 0$ and $\sum_r \gamma_{r,i} = 1$. The status of an attacker (honest) node whose cost relative to the $A = \varnothing$ case has increased is *lose* (*mind*); otherwise, it is *do not lose* (*do not mind*).

To validate the rank-based model, we implemented the network topology and flow set of Fig. 2 in the ns-3 simulator, assuming error-free radio channels, static routing, and constant bit-rate saturation-level UDP traffic of 1500 B packets. Each simulation run lasted 200 s with an additional 50 s warm-up time and was repeated five times. Nodes were classified as *mind* or *lose* if the throughput of their BE flows dropped by 5% or more, or if the per-hop delay of their VO flows increased by more than 20 ms and exceeded 100 ms. We assessed *congruity*, defined as the proportion of nodes whose status (*mind*, *lose*, *do not mind*, or *do not lose*) upon TRAs launched by a random attacker set agrees between the simulation and the rank-based model. Fig. 3 presents the cumulative distribution function (CDF) of congruity obtained after simulating all 256 possible attacker sets,[2] producing a mean congruity of 0.89.

For comparison, consider a heuristic inspired by the $|N|$-person Prisoners' Dilemma (PD) game [51]: if the number of attackers exceeds (does not exceed) a certain threshold then all the attacker nodes' status is guessed as *lose* (*do not lose*) and the honest nodes' as *do not mind* (*mind*). The corresponding CDFs depicted in Fig. 3 for the threshold varying from 0 to $|N|$ produce mean values between 0.49 and 0.54, not far from a fair coin toss. As another baseline, an unrealistic "informed gambler," who knew an attacker (honest) node's statistical chance of acquiring a *lose* (*mind*) status under a random attacker set, might guess the node's status for a given A by tossing an appropriately biased coin. Congruity would then be measured by the expected number of guesses that match the simulation. The corresponding CDF in Fig. 3 produces a mean value of 0.82, inferior to our model's. We conclude that the rank-based model is a reasonably good predictor of the impact of TRAs in MAWiNs with saturation-level traffic.

It will be convenient to identify nodes directly impacted by a given attacker set.

[2]Nodes 1 and 10 cannot launch a TRA$^+$ or a TRA$^-$ due to the plausibility constraints of Definition 4.

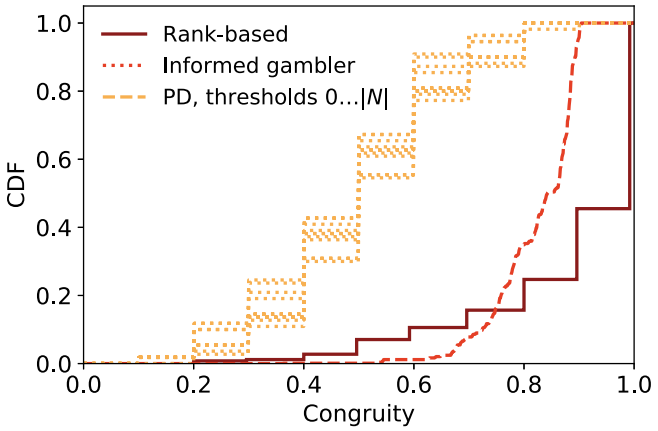


Fig. 3. Congruity between simulations and various analytical models.

Definition 5: A node whose status is *lose* or *mind* is said to be *in distress*. Let $\Delta(A)$ be the set of such nodes in the presence of the attacker set $A \subseteq N$.

Hence, the set of in-distress nodes contains nodes whose costs have increased in comparison to the $A = \varnothing$ case: $\Delta(A) = \{i \in N | \text{cost}_i(A) > \text{cost}_i(\varnothing)\}$. Note that $\Delta(A) = \varnothing \neq A$ is possible, e.g., if $A = \{1, 10\}$ in Fig. 2.

D. Attack Incentives and Impact

In realistic MAWiN settings, TRAs pose a threat whose credibility (i.e., incentives to launch) and seriousness (i.e., harmful impact upon honest nodes) we now quantify. We ask if, regardless of the currently ongoing TRAs, an honest node turning attacker perceives a QoS improvement and causes some other nodes to perceive a QoS degradation. Neither of these effects is certain, as it depends on a node's position in the network topology. Referring to Fig. 2, suppose that $A = \varnothing$ and node 3 turns attacker. Since flow #3 is VO, the attack amounts to a TRA$^-$ upon flows #1 and #4. While these two flows suffer, for all remaining flows the contention softens and their QoS improves. Hence, the TRA is harmless for other nodes. Consider an alternative scenario where it is node 5 that turns attacker. Its source traffic (flow #5) now enjoys elevated priority when forwarded at nodes 5, 4, and 7, but experiences increased contention from itself at node 5 (being forwarded by node 4 and via exclusive-OR reception from node 5 at node 4) and at node 4 (being forwarded by nodes 5 and 7). The likely net effect of this is a QoS degradation.

To investigate the above effects and their scaling with the network size $|N|$, both numerical calculations using the rank-based cost metric (8) and ns-3 simulations were conducted. In the numerical calculation, we assumed $|N| \leq 200$, uniformly distributed route hop lengths with $\|r\|_{\min} = 1$ and $\|r\|_{\max} = 5$, and $|A| = 1, 2, 5, 10$, or 20. For a fixed parameter configuration, the results were averaged over 10 000 instances of random network topologies, e2e-flow routes, and attacker sets. The transit nodes for a route were chosen at random in geographical proximity to the source node. We examined the scaling with $|N|$ of:

1) the incentives to launch a TRA, measured as the percentage of attacker nodes whose cost metric did not

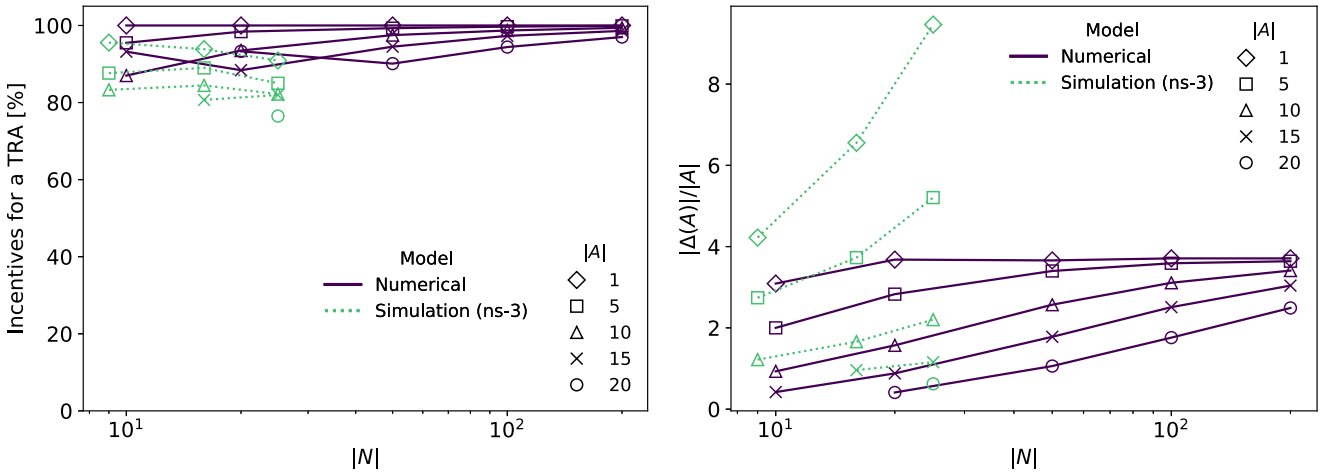


Fig. 4. Incentives to launch a TRA (*left*), harmful impact ("direct victims") of a TRA (*right*); $\|r\|_{\min} = 1$ and $\|r\|_{\max} = 5$.

worsen when turning attacker, i.e., nodes $i \in A$ satisfying $\text{cost}_i(A) \leq \text{cost}_i(A \backslash \{i\})$;

2) the harmful impact of a TRA launched in the presence of several ongoing TRAs, measured as $|\Delta(A)|/|A|$, i.e., the average *in-distress* nodes per attacker node.

The results depicted in Fig. 4 indicate that the threat of TRAs is not limited to small-size networks. The incentives for a TRA remain 100% for $|A| = 1$ and decrease with $|A|$, but slightly increase with $|N|$ on account of more dispersed attacker nodes. A similar scaling is visible for the harmful impact of a TRA.

For the ns-3 simulations, we assumed square grid topologies with $|N| = 9$, 16, and 25. Each node was the source of an e2e-flow following a minimum-hop route to a randomly chosen destination, and half of the flows were VO (other settings are described in Section V). As before, we used end-to-end throughput and delay as QoS metrics for BE and VO flows, respectively, and the same rules for deciding node status. The results are marked in Fig. 4 with dotted lines. The incentives for TRAs are lower now, since the edge nodes have no transit traffic to downgrade. Meanwhile, in-distress nodes are more numerous, reflecting interflow competition effects unaccounted for by (8). Nonetheless, these results confirm that the incentives for and harmful impact of TRAs are significant for large $|N|$.

IV. TRA Game Description

A selfish node performs a TRA whenever this improves its cost, anticipating similar conduct of other nodes. This gives rise to a noncooperative *TRA game*, whose one-shot and multistage variants we now describe. We propose to mitigate TRAs by introducing a distributed exposure signaling mechanism called DISTRESS, under which good multistage strategies produce few attacker nodes when the game terminates.

A. One-Shot TRA Game

In the noncooperative one-shot TRA game, the nodes are players, $\text{map}_i \in \{TRA, honest\}$ is node i's action, and *cost* is the (negative) payoff function (i.e., small costs are pursued). A given action profile $(\text{map}_i, i \in N)$ is equivalent of the set $A \subseteq N$ of plausible opportunistic attackers (nodes launching TRA). Using a ⟨players, action space, payoffs⟩ representation, the game is defined as

$$\left\langle N, 2^N, \text{cost} : N \times 2^N \to \mathbf{R}^+ \right\rangle. \tag{9}$$

Some interesting action profiles are: $\varnothing$ (all-honest), and N (all-TRA). In the latter, any e2e-flow (r, BE) experiences a TRA^+ at s_r, and any e2e-flow (r, VO) experiences a TRA^- at the first encountered node in $r \backslash \{s_r, d_r\}$.

Contrary to the intuition that it is always beneficial to upgrade source traffic and downgrade competing transit traffic, the TRA game is not an $|N|$-person PD. Specifically, due to the complexity of mechanisms determining MAWiN performance, the *TRA* action does not dominate *honest*, nor is it necessarily harmful to honest nodes. Moreover, $A = \varnothing$ need not be Pareto superior to $A = N$; for some traffic patterns, the reverse is true [25].

The following definition identifies nodes indirectly impacted by a given attacker set.

Definition 6: A node forward-reliant on a node in distress (cf. Definitions 1 and 5) is said to be *in exposure*. Let $\Delta^*(A)$ be the set of such nodes in the presence of the attacker set $A \subseteq N$.

Hence, the set of in-exposure nodes contains nodes which are forward-reliant on nodes currently in distress: $\Delta^*(A) = E_{R_F^*}(\Delta(A))$. The rationale behind Definition 6 is the following. Nodes in distress perceive unsatisfactory QoS and so lose incentives to continue packet forwarding services. Thus, they pose a credible threat of imminent *service suspension*, to which exposed are they themselves along with the set of source nodes whose traffic they forward. In the case of service suspension by a node in distress, each of these source nodes registers an infinite e2e-flow cost (8), and also loses incentives to continue packet forwarding services. By recursion, similarly exposed are all nodes forward-reliant on nodes in $\Delta(A)$, i.e., $\Delta^*(A)$.

TRAs can be mitigated by leveraging node exposure in a way not unlike an immune response is triggered by a foreign toxin. Namely, even a small attacker set creates a ripple effect

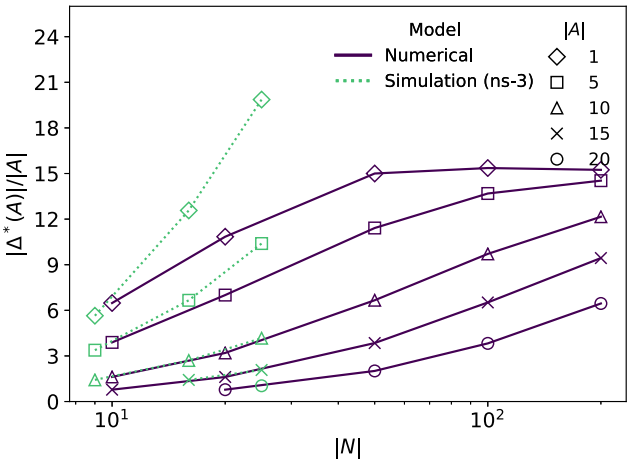


Fig. 5. Size of the "immune response"; $\|r\|_{\min} = 1$ and $\|r\|_{\max} = 5$.

Algorithm 1: DISTRESS Mechanism

Data: $A(k-1)$ – set of attackers in stage $k-1$
Result: $\Delta^*(A(k-1))$ – set of nodes in exposure at the end of stage k

$M \leftarrow \varnothing$; // no node marked as in-exposure
repeat
  for $i \in N \backslash M$ **do**
    if $(cost_i(A) > cost_i(\varnothing)) \vee$ ((DISTRESS(j) received) $\wedge$ $((i,j) \in R_F)$) **then**
      $M \leftarrow M \cup \{i\}$; // node i marked as in-exposure
      send DISTRESS(i) to $E_{R_F}(\{i\})$
    end
  end
until $E_{R_F}(M) = M$;
$\Delta^*(A(k-1)) \leftarrow M$

For ease of specification, a DISTRESS flag is assumed to be sent only once and forwarded reliably to the intended recipient.

across the network, causing exposure in a much larger set of nodes than those in distress. Instead of suspending service, nodes in exposure start playing the TRA game, occasionally selecting *TRA* rather than *honest*, which may cause exposure in the initial attackers. If exposure, i.e., the threat of imminent service suspension, is reflected in the game payoffs as a large enough (say infinite) cost, such play brings most or all attackers back to honesty, which the nodes in distress alone may be too few to achieve. A rigorous argument is given in Section IV-C.

For various $|N|$, we examined the size of the "immune response" triggered by a TRA, measured as $|\Delta^*(A)|/|A|$, the average in-exposure nodes per attacker node. Using cost metric-based calculation, we verified that it remains nontrivial and does not distinctly decrease at least up to $|N| = 200$ (cf. Fig. 5). In the ns-3 simulations of square grid topologies up to $|N| = 25$, $\Delta^*(A)$ was inferred by keeping track of the source nodes of flows currently forwarded by each node. The results (marked with dotted lines) show a nontrivial size of the "immune response," which even scales with $|N|$.

To incorporate exposure into the game payoffs, we redefine nodal costs (8) and the TRA game (9) as

$$\text{cost}'_i(A) = \begin{cases} \text{cost}_i(A), & i \notin \Delta^*(A) \\ \infty, & i \in \Delta^*(A) \end{cases} \tag{10}$$

$$\left\langle N, 2^N, \text{cost}' : N \times 2^N \to \mathbf{R}^+ \right\rangle. \tag{11}$$

B. Multistage Play Under the DISTRESS Mechanism

Mitigation of TRAs using the above approach requires that nodes signal exposure to one another and can toggle between *TRA* and *honest* in response to other nodes' play, as modeled by a multistage game. Let the TRA game (9) be played in stages $k = 1, 2, \ldots$, and let $A(k) \subseteq N$ be the set of attackers in stage k. Each stage k is assumed long enough for each node i to produce an accurate estimate of $\text{cost}_i(A(k))$ and signal exposure throughout the network if needed, hence to also determine $\text{cost}'_i(A(k))$.

Assume that there are no attackers prior to stage 1, i.e., $A(0) = \varnothing$. In stage 1, a set $I \subset N$ of *ill-behaved* (selfish) nodes spontaneously select *TRA*, i.e., $A(1) = I$; the other nodes are further called *well-behaved*. The stage-1 TRAs may bring about distress in some (possibly also ill-behaved) nodes, i.e., induce the set $\Delta(A(1)) = \Delta(I)$. At the end of a generic stage $k-1$, each node i estimates its current cost metric and if it finds itself in distress, i.e., $i \in \Delta(A(k-1))$, then marks itself as in-exposure and sends a DISTRESS(i) flag to all nodes whose source traffic it forwards; that is, copies of the flag are sent to all nodes of $E_{R_F}(\{i\})$, including node i itself. (The flag is also timestamped to avoid confusion with exposure signaling in another stage.) Having received DISTRESS(j) and checked that $(i,j) \in R_F$, node i ignores the flag if it is already in exposure; otherwise, marks itself as in-exposure and sends DISTRESS(i) to $E_{R_F}(\{i\})$ as above. It is easy to see that if M is the set of nodes so far marked as in-exposure then the process stops when $E_{R_F}(M) = M$. Thus, assuming that each flag is issued and reliably delivered to the intended recipient within one stage, at the end of stage k we have $M = \Delta^*(A(k-1))$. This mechanism, specified as Algorithm 1, will be termed distributed signaling of traffic exposure to service suspension (DISTRESS).

It is vital that the threat signified by signaled exposure be credible. Therefore, a received DISTRESS(j) flag, where $j \in r \backslash \{s_r\}$, should imply to s_r that j is indeed a transit node on r and not an off-route one that does not pose a threat. This is granted if a source routing protocol such as DSR [52] is employed, in which r is known to s_r. Otherwise, DISTRESS(j) can be appended to forwarded packets and at d_r returned to s_r through a (trusted) end-to-end feedback connection. Fig. 6 provides an illustration. Here, $R_F^* = \{(1,3), (1,4), (1,5), (1,6), (1,7), (1,8), (2,4), (2,5), (2,6), (2,7), (2,8), (3,6), (5,4), (5,7)\}$. Following a TRA at node 3 in stage $k-1$, node 4 sends DISTRESS(4) to $s_{\#1} = 1$ via $d_{\#1} = 10$ and to $s_{\#5} = 5$ via $d_{\#1} = 6$; subsequently, node 5 sends DISTRESS(5) to $s_{\#2} = 2$ via $d_{\#2} = 9$ and to $s_{\#1} = 1$ via $d_{\#1} = 10$; the latter flag is ignored by already in-exposure node 1 (to minimize the communication overhead, it could have been suppressed at node 10). At the end of the present stage, $\Delta^*(\{3\}) = \{1, 2, 4, 5\}$.

We remark that the DISTRESS mechanism is lightweight in terms of the required synchronization and communication

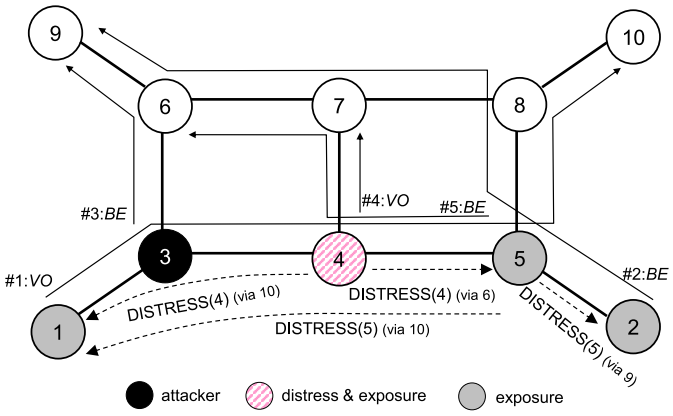


Fig. 6. Illustration of the DISTRESS mechanism; e2e-flow #*i* originates from source node *i* and has indicated intrinsic AC; node 4 is in distress due to a TRA^+ at node 3.

overhead (roughly $\mathcal{O}(|R|)$ per node in the worst case). Exposure signaling is triggered asynchronously by nodes in distress based on local QoS perception. The cause of the distress, either a TRA or temporarily harsh traffic conditions (e.g., transmission impairments, frequent collisions, or buffer overflow), does not influence a node's behavior. Such a distinction is a troublesome aspect of many known misbehavior mitigation schemes [22], [53], because responding to the distress caused by exogenous factors may result in punishment of honest nodes. In our solution, exposure signaling can only encourage a node to select *honest*, therefore does not affect the behavior of an already honest node unintentionally causing distress. By processing a received DISTRESS flag as described above, such a node simply acknowledges an objectively existing threat of imminent service suspension and no punishment occurs. Importantly, exposure signaling is costless, hence performed without incentive calculation, while fake signaling despite satisfactory QoS perception is not beneficial.

The above considerations also indirectly imply that the effectiveness of the DISTRESS mechanism is unaffected by the network traffic volume, in particular, background traffic competing with the e2e-flows: under light traffic conditions, no node finds itself in distress and the mechanism is not triggered; otherwise, DISTRESS signaling simply encourages honest behavior.

C. Good Multistage Strategies

A multistage strategy prescribes a node which of the two actions (*TRA* or *honest*) to select in each stage, based on the current history of play. To specify a desirable course of play under DISTRESS, we use two auxiliary definitions. The first describes flows whose source nodes are not forward-reliant on *in-distress* nodes and so are expected to survive a service suspension. The second describes a node that cannot benefit from selecting a different action, given the other nodes' actions.

Definition 7: An e2e-flow is called *survivable* if its source node is not in exposure. Let $F^*(A)$ be the set of such flows in the presence of the attacker set $A \subseteq N$.

Definition 8: A node is called *(weakly) best-reply* if it cannot unilaterally improve its nodal cost (10) by selecting a different action. Let $\Gamma_{\text{cost}'}(A)$ be the set of such nodes in the presence of the attacker set $A \subseteq N$.

Thus, we have $F^*(A) = \{(r, ac) \in F | s_r \notin \Delta^*(A)\}$ and $\Gamma_{\text{cost}'}(A) = \{i \in N | \text{cost}'_i(A) \leq \text{cost}'_i(A^{[i]})\}$, where $A^{[i]} = A \backslash \{i\}$ if $i \in A$ and $A^{[i]} = A \cup \{i\}$ if $i \notin A$. Note that if $\Gamma_{\text{cost}'}(A) = N$ then A constitutes a (weak) Nash equilibrium (NE) [51] of the one-shot TRA game (11).

We now formulate the following postulates.

1) *Opt-Out:* While ill-behaved nodes may occasionally select *TRA*, well-behaved nodes select *honest* at all times; that is, being nonselfish, refuse to play the game. Thus, $A(k) \subseteq I$ for all k.
2) *Termination:* After k_0 stages, the game terminates and no node thereafter changes its action. That is, $A(k) = A(\infty)$ for all $k \geq k_0$, where k_0 is finite, known in advance, and preferably small.
3) *Rationality:* Ill-behaved nodes tend to select (weakly) best-reply actions; ideally, $I \subseteq \Gamma_{\text{cost}'}(A(\infty))$, i.e., $A(\infty)$ is a weak NE of the one-shot game restricted to the ill-behaved nodes. A suitable quantitative measure is the fraction of ill-behaved nodes that are the best reply, i.e., $|\Gamma_{\text{cost}'}(A(\infty))|/|I|$.
4) *Efficiency:* Ill-behaved nodes eventually cause one another no distress; ideally, $\Delta(A(\infty)) \cap I = \varnothing$. A suitable quantitative measure is the fraction of ill-behaved nodes that are not in distress, i.e., $|I \backslash \Delta(A(\infty))|/|I|$.
5) *Defensibility:* Well-behaved nodes are eventually defended against distress caused by ill-behaved nodes' TRAs; ideally, $\Delta(A(\infty)) \subseteq I$. A suitable quantitative measure is the fraction of well-behaved nodes that are not in distress, i.e., $|(N \backslash I) \backslash \Delta(A(\infty))|/|N \backslash I|$.
6) *Survivability:* Eventually, few e2e-flows rely upon forwarding by nodes in exposure. A suitable quantitative measure of survivable network throughput is the fraction of survivable flows, i.e., $|F^*(A(\infty))|/|F|$.

To satisfy these postulates, a multistage strategy has to employ well-designed *action selection* and *participation* rules. The DISTRESS mechanism enables more informed rules by enriching the history of play: apart from recent actions, a node may recall in-distress conditions and received DISTRESS flags (i.e., in-exposure conditions) in recent stages. We confine a node's memory to the last two stages; the simulations in Section V indicate that it can produce satisfactory quantitative measures related to the above postulates.

We allow node i selecting an action for stage $k+1$ to recall its membership in the sets of current attackers, current in-distress nodes, and recent in-exposure nodes, i.e., $A(k)$, $\Delta(A(k))$, and $\Delta^*(A(k-1))$, without the knowledge of the entire sets that the DISTRESS mechanism does not guarantee. Subject to this restriction, a wide class of feasible action selection rules can be expressed as follows:

$$A(k+1) = \sigma_{A(k), \Delta(A(k)), \Delta^*(A(k-1))} \tag{12}$$

where

$$\sigma_{X,Y,Z} = \bigcup_{(x,y,z) \in \Phi \subseteq \{-1,1\}^3} X^x \cap Y^y \cap Z^z$$
$$\forall X \subseteq N : X^1 = X, X^{-1} = N \backslash X.$$

Determined by the index set Φ, there are $2^8 = 256$ distinct action selection rules. E.g., if $\Phi = \{(-1, 1, -1)\}$ then $\sigma_{X,Y,Z} = X^{-1} \cap Y \cap Z^{-1}$, hence $A(k+1) = \Delta(A(k))\backslash(A(k) \cup \Delta^*(A(k-1)))$, and if $\Phi = \{(-1, 1, -1), (1, 1, -1)\}$ then $\sigma_{X,Y,Z} = (X^{-1} \cap Y \cap Z^{-1}) \cup (X \cap Y \cap Z^{-1}) = Y\backslash Z$, hence $A(k+1) = \Delta(A(k))\backslash\Delta^*(A(k-1))$. Note that $\Phi = \varnothing$ and $\Phi = \{-1, 1\}^3$ correspond to "persistent honest" and "persistent TRA" strategies, respectively, and that (12) subsumes action selection rules with a reduced set of arguments, e.g., $\Phi = \{(-1, y, z), (1, y, z) | (y, z) \in \Phi'\}$, where $\Phi' \subseteq \{-1, 1\}^2$, corresponds to an action selection rule that does not explicitly condition $A(k+1)$ on $A(k)$, i.e., of the form $A(k+1) = \sigma_{\Delta(A(k)),\Delta^*(A(k-1))}$.

Participation in the game can change stage by stage as governed by some in-game condition; let $G(k)$ be the set of in-game nodes in stage k that select action according to (12), whereas the rest, i.e., $G^{-1}(k)$, retain the previous-stage action. In line with the opt-out postulate, action selection rules and in-game conditions only apply to ill-behaved nodes, i.e., $G(k) \subseteq I$, which we do not reflect in the ensuing formulas to keep them simple. The dynamics (12) become

$$A(k+1) = I \cap \left(G^{-1}(k) \cap A(k)\right) \cup (G(k) \cap \Sigma) \quad (13)$$

where $\Sigma = \sigma_{A(k),\Delta(A(k)),\Delta^*(A(k-1))}$. If (13) is a deterministic finite-order recurrence, then the sequence $(A(k), k = 0, 1, 2, \ldots)$ eventually becomes periodic and detection of this may terminate the game. It is enough to formulate the in-game condition for a given node that only depends on its recent membership in A, $\Delta(A)$, and $\Delta^*(A)$. Specifically, let $\mathbf{h}_i(k) = (\mathbb{1}_{i\in A(k-1)}, \mathbb{1}_{i\in A(k)})$ be node *i membership history* with respect to $A(k-1)$ and $A(k)$. We formulate the following in-game condition for node i in stage $k+1$:

$$\forall 1 \leq c \leq \min\{c_{\max}, k-1\} : \mathbf{h}_i(k) \neq \mathbf{h}_i(k-c). \quad (14)$$

That is, a node is out-of-game if its membership history has repeated itself within recent $c_{\max}$ stages (since well-behaved nodes stay honest at all times, they formally become out-of-game as of stage $k = 1$).

We now show that under certain conditions the game is guaranteed to terminate.

Proposition 1: If $c_{\max} \geq 4$ then termination is guaranteed with $A(k) = A(\infty)$ and $G(k) = \varnothing$ for all $k \geq 8$.

Proof: Observe that out-of-game nodes repeat previous-stage actions, thus if $i \notin G(k)$ and $i \notin G(k+1)$ then $i \notin G(k')$ for all $k' \geq k$. This is due to $\mathbf{h}_i(k) = \mathbf{h}_i(k+1)$ being true for all $k' \geq k$, in violation of (14) with $c = 1$.

For any node $i \in I$ consider an infinite sequence $\mathbf{a} = (a_0, a_1, a_2, \ldots)$, where $a_0 = 1$ and $a_k = \mathbb{1}_{i\in A(k)}$ for $k > 0$, inducing a sequence of node membership histories $(a_0, a_1), (a_1, a_2), \ldots$ Call $\mathbf{a}$ *proper* if it is compatible with (14), i.e., if $\exists 1 \leq c \leq \min\{c_{\max}, k-1\} : (a_k = a_{k-c}) \wedge (a_{k-1} = a_{k-1-c})$ then $a_{k+1} = a_k$ (hence, $G(k+1) = \varnothing$). Let Π be the set of all proper sequences. Denote $k_0(\mathbf{a}) = \max\{k | a_k \neq a_k - 1\}$ and, with a little abuse of notation, $k_0(S) = \max\{k_0(\mathbf{a}) | \mathbf{a} \in S\}$ for $S \subseteq \Pi$. We need to prove that $k_0(\Pi) = 8$.

Let Π_n be the set of all n-symbol prefixes of the form $(a_0, \ldots, a_{n-1})$ of sequences in Π. Based on (14), one verifies that if $k_0(\Pi_n) = k_0(\Pi_{n+3})$ then $k_0(\Pi_n) = k_0(\Pi)$. Inspection shows that among the infinity of sequences $\mathbf{a}$, only 18 are in Π, and the smallest n satisfying $k_0(\Pi_n) = k_0(\Pi_{n+3})$ is 8, with $k_0(\Pi_8) = k_0(\Pi_{11}) = 8$. Maximum $k_0(\mathbf{a})$ is achieved at $\mathbf{a}^* = (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, \ldots)$, inducing a sequence of node membership histories (1, 1), (1, 0), (0, 1), (1, 0), (0, 0), (0, 1), (1, 1), (1, 0), (0, 0), (0, 0), ..., where the underlined histories correspond to out-of-game stages. ■

It turns out that under certain conditions, the above specification includes multistage strategies exhibiting ideal rationality and defensibility. We will need two more definitions. First, we define a nodal cost function under which the benefit of an attacker always causes distress in some other node. Second, we define a flow set such that a service suspension at any node threatens every flow's survival.

Definition 9: The cost function $\text{cost}_i(\cdot)$ satisfies *all-honest dominance* if $\varnothing$ is Pareto effective (not Pareto dominated by any $A \subseteq N$), i.e., for all $i \in N$ and $A \subseteq N$, $\text{cost}_i(A) < \text{cost}_i(\varnothing)$ implies $\text{cost}_j(A) > \text{cost}_j(\varnothing)$ for some $j \neq i$.

Definition 10: The flow set F satisfies *full forward-reliance* if $R_F^* = N \times N$, i.e., each source node is forward-reliant on every other node (cf. Definition 1).

In general, all-honest dominance and full forward-reliance are not guaranteed; clearly, the latter is impossible if $R = \{r | (r, ac) \in F\}$ contains single-hop routes. However, if both features are present in a given network, then we can show that there exists at least one action selection rule which is ideally efficient (no ill-behaved nodes cause distress), ideally defensible (all well-behaved nodes are defended against distress), and ideally rational (all ill-behaved nodes select best-reply strategies).

Proposition 2: If all-honest dominance and full forward-reliance are satisfied, then there exists at least one action selection rule $\sigma_{(\cdot)}$ for which:

1) $\Delta(A(\infty)) = \varnothing$, consequently, $\Delta^*(A(\infty)) = \varnothing$ and $\text{cost}_i'(A(\infty)) = \text{cost}_i(\varnothing)$, i.e., when the multistage game terminates, no node is in exposure and nodal costs are the same as under all-honest (this implies ideal efficiency and defensibility);
2) $A(\infty)$ is a weak NE of the one-shot game (11) restricted to I, i.e., $I \subseteq \Gamma_{\text{cost}'}(A(\infty))$ (this implies ideal rationality).

Proof: Clearly, all-honest dominance implies $\text{cost}_i(\varnothing) \leq \text{cost}_i'(A)$ for all $A \subseteq N$ and $i \in N$, i.e., with respect to $\text{cost}_i'(\cdot)$, $\varnothing$ weakly Pareto dominates every other action profile, and as such is a weak NE of the one-shot game (11). The same pertains to any $A \subseteq N$ such that $\Delta(A) = \varnothing$ (indeed, for any such A, $\text{cost}_i(A) = \text{cost}_i(\varnothing)$ for all $i \in N$). Since under full forward-reliance it holds that $\Delta(A) = \varnothing$ iff $\Delta^*(A) = \varnothing$, it is enough to show that $\Delta^*(A(\infty)) = \varnothing$.

Let $k - 1 = \min\{k' | G(k') = \varnothing\}$, then from (14), it follows that $A(k-1) = A(k) = A(k+1) = A(\infty)$, where $A(\infty) = \sigma_{A(\infty),\Delta(A(\infty)),\Delta^*(A(\infty))}$. If $A(\infty) = \varnothing$ then the proposition trivially holds true, so assume $A(\infty) \neq \varnothing$. Take $\Phi = \{(-1, -1, -1), (-1, 1, -1), (1, -1, -1), (1, 1, -1)\}$, i.e., $\sigma_{X,Y,Z} = Z^{-1}$ and $A(k+1) = I \cap (N\backslash\Delta^*(A(k-1)))$. Then, either $\Delta(A(\infty)) = \Delta^*(A(\infty)) = \varnothing$ and the proposition

holds true or $\Delta(A(\infty)) \neq \varnothing$, which implies $\Delta^*(A(\infty)) \neq N$, impossible under full forward-reliance. ■

Proposition 2 states conditions of the existence of ideally rational, efficient, and defensible action selection rules. Simulations show that these conditions are often satisfied in randomly generated MAWiN instances; otherwise, good rules (12) nevertheless exist that ensure satisfactory characteristics across various MAWiN topologies and flow sets F (cf. Section V). These rules can be adopted *á priori*, relieving nodes from seeking good rules for a specific topology and flow set, which they are typically unaware of.

Note that $\Delta(A) = \varnothing$ implies that A is a weak NE of (11), but the converse is not true; in fact, simulations show that a vast majority of Nash equilibria A feature $\Delta(A) \neq \varnothing$.

V. Simulations

Simulations involved network topologies with both static and mobile nodes, respectively, using the Monte Carlo method based on the network model of Section III and the ns-3 simulator implementing a full MAWiN protocol stack. The goal of the Monte Carlo simulations was to assess the rationality, efficiency, defensibility, and survivability measures in realistic settings, when the two assumptions of Proposition 2 (all-honest dominance and full forward-reliance) were not necessarily satisfied. The ns-3 simulations were carried out to investigate the impact of fast-changing MAWiN topology and flow routes on the effectiveness of the DISTRESS mechanism.

A. Static Nodes

For the analysis of static topologies, we implemented the network model of Section III (including network topology, routing, flow configuration, attack behavior, and rank-based estimation of flow cost) as well as the multistage TRA game and DISTRESS mechanism of Section IV in a Monte Carlo simulator. Each simulation run consisted of a stage-by-stage play of the TRA game, with nodes deciding their action (*TRA* or *honest*) in each stage. One thousand MAWiN instances were generated with $|N| = |F| = 10$ and e2e-flow routes of uniformly distributed hop lengths with $\|r\|_{\min} = 1$ or 2 and $\|r\|_{\max} = 5$. Full forward-reliance occurred in 6.5% and 55.2% of the MAWiN instances with $\|r\|_{\min} = 1$ and $\|r\|_{\min} = 2$, respectively. We observed that:

1) all-honest dominance was never violated (violations are in general possible but unlikely, e.g., when traffic flows do not impact one another's performance);
2) for $\|r\|_{\min} = 1$ and $\|r\|_{\min} = 2$, weak Nash equilibria amounted to 40.2% and 94% of all action profiles $A \subseteq N$, respectively; however, those with $\Delta(A) = \varnothing$ were a rarity, amounting to 0.1% and 0.3%, respectively.

For each MAWiN instance, 100 independent multistage game runs were conducted with $I \neq N$ chosen at random subject to $\Delta(I) \neq \varnothing$. All 256 feasible action selection rules were tried. It was observed that:

1) with $\|r\|_{\min} = 1$ and $\|r\|_{\min} = 2$, respectively, 44 and 54 action selection rules (including the trivial persistent honest) ensured 1) and 2) of Proposition 2 even in the absence of full forward-reliance;

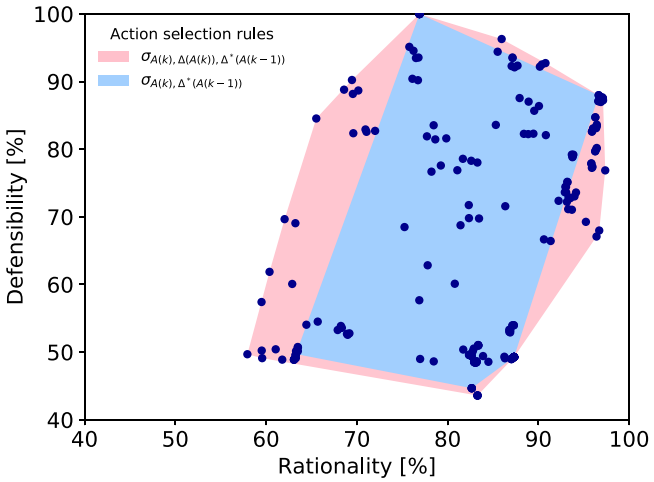


Fig. 7. Rationality and defensibility measures for the 2^8 feasible action selection rules; $|N| = |F| = 10$, $\|r\|_{\min} = 1$.

2) conditioning $A(k+1)$ on $A(k)$ besides $\Delta(A(k))$ and $\Delta^*(A(k-1))$ did not extend the interesting range of key after-game (asymptotic) characteristics;
3) on the other hand, conditioning $A(k+1)$ on $A(k)$ alone, i.e., disregarding information provided by the DISTRESS mechanism, produced the worst measures of rationality and defensibility.

To explain the first observation, consider, e.g., $A(k+1) = I \cap \Delta(A(k))$. It must be that $A(\infty) = \Delta(A(\infty))$, but $A(\infty) = \Delta(A(\infty)) \neq \varnothing$ is possible only if eventually all the attacker nodes and none of the honest ones are caused distress, a highly improbable situation. The latter two observations are illustrated in Fig. 7, where each dot represents a pair of after-game (rationality, defensibility) measures for a given action selection rule, averaged over the generated MAWiN instances and game runs. The outer contour encompasses all action selection rules (12) and the inner one only rules of the form $A(k+1) = \sigma_{\Delta(A(k)),\Delta^*(A(k-1))}$. The latter captures most of the Pareto front, including the best rationality and defensibility measures. Rules of the form $A(k+1) = \sigma_{A(k)}$ correspond to the two lower corners of the outer contour, the farthest from the Pareto front.

For more detailed analysis, several representative action selection rules have been chosen. They are listed below in the order of diminishing survivability and tendency to launch TRAs, and improving efficiency and defensibility.

(a) $A(k+1) = N$ ("persistent TRA").
(b) $A(k+1) = \Delta(A(k)) \cap \Delta^*(A(k-1))$.
(c) $A(k+1) = \Delta(A(k)) \oplus \Delta^*(A(k-1))$, where $\oplus$ denotes disjunctive union.
(d) $A(k+1) = (N \backslash \Delta^*(A(k-1))) \cup \Delta(A(k))$.
(e) $A(k+1) = N \backslash \Delta^*(A(k-1))$.
(f) $A(k+1) = \Delta(A(k)) \backslash \Delta^*(A(k-1))$.

These rules were observed to differ visibly in the speed of convergence to the after-game characteristics; for example, stage-by-stage trajectories for rules (e) and (f) are shown in Fig. 8. Table II presents relevant after-game characteristics, averaged as above. One notes in particular that:

TABLE II
SIMULATION RESULTS: AVERAGE AFTER-GAME CHARACTERISTICS FOR ACTION SELECTION RULES (A)–(F); $\|r\|_{\text{MIN}} = 1$

Action selection rule	Honest in I [%]	Rationality [%]*	Efficiency [%]	Defensibility [%]	Survivability [%]	Game duration [stages]
(a)	0	87.3 (79.4)	68.9	49.3	26.5	3
(b)	31.1	82.9 (66.8)	72.9	48.6	29.3	3.8
(c)	42.6	64.4 (37.0)	76.6	54.0	36.9	4.6
(d)	49.0	93.2 (79.2)	81.5	75.2	50.7	4.9
(e)	77.1	97.1 (90.7)	91.2	87.4	73.3	5.1
(f)	100	76.9 (48.6)	100	100	100	3.7

* In parentheses are percentages of game runs leading to Nash equilibria within I.

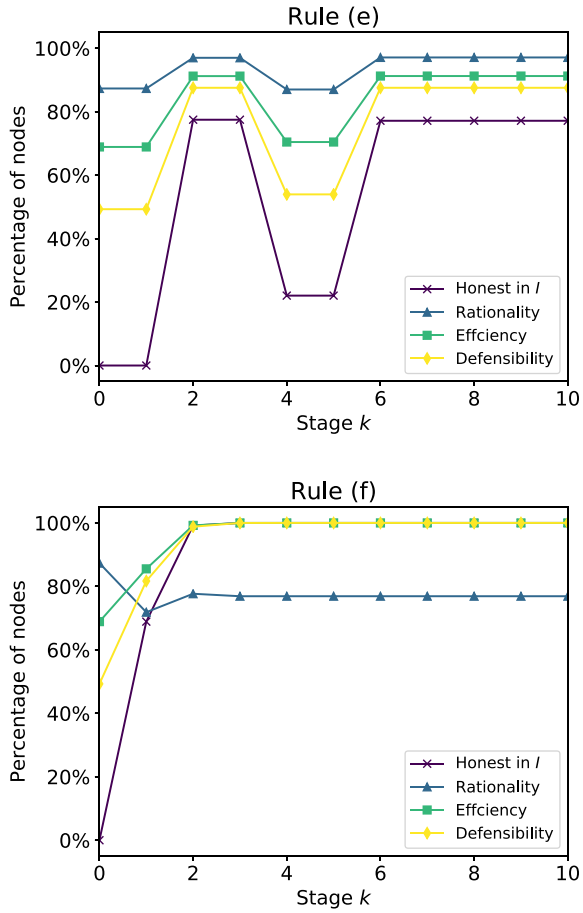


Fig. 8. Stage-by-stage trajectories of relevant characteristics for action selection rules (e) and (f); $\|r\|_{\min} = 1$.

1) rule (e) is the most likely to be adopted by rational ill-behaved nodes, as it leads to highly efficient Nash equilibria in the vast majority of game runs. It also produces good defensibility and survivability;
2) on the other hand, rule (f) produces ideal efficiency and survivability, but is far from rational, thus likely to be dismissed by ill-behaved nodes;
3) rule (a) ("persistent TRA") is moderately rational, but, due to the DISTRESS mechanism, very inefficient. This latter fact is fortunate, as rule (a) produces disastrous defensibility and survivability;
4) rules adversely affecting defensibility and survivability, such as (a)–(c), are not very rational and so unattractive to ill-behaved nodes. Rule (d) is moderately attractive, but from rationality and efficiency viewpoints is Pareto dominated by rule (e).

Hence, under DISTRESS, ill-behaved nodes are likely to follow rule (e), in which in-exposure nodes cannot be attackers.

TABLE III
NS-3 SIMULATION PARAMETERS

Parameter	Value
Total number of nodes	16
Node placement	grid, random
Area size	20 x 20 m
Grid spacing	8 m
Mobility model	random waypoint
Waiting time	20 s
Velocity	0 – 1.4 m/s
PHY/MAC	IEEE 802.11ac
RTS/CTS	Enabled
Channel width	20 MHz
Modulation	256-QAM
Coding rate	3/4
aCWmin	63[1]
Routing	OLSR[2]
Transport protocol	UDP
Traffic generator	CBR
Traffic rate	2 Mb/s

[1] To reduce the effect of hidden nodes.
[2] OLSR's signaling messages were prioritized over VO flows.

B. Mobile Nodes

To study the impact of node mobility, we implemented the multistage play of Section IV-C under rule (e) in the ns-3 simulator, using the settings of Table III. Each node was the source of an e2e-flow, half of them of high priority. We considered two topologies for initial node placement: 1) *grid*—all nodes arranged on a square grid and 2) *random*—all nodes uniformly distributed in the area. The adopted high modulation and coding scheme limits the nodes' transmission range to approximately 10 m. For a more realistic IEEE 802.11 range of 100 m, the maximum evaluated velocity would scale to 14 m/s (50 km/h). In summary, the chosen settings created conditions when TRAs are likely to negatively impact the performance of honest nodes.

With node mobility, $\Delta(A)$ and $\Delta^*(A)$ can change stage by stage although A remains the same, due to changing MAWiN topology and flow routes. Except for quasistatic environments, where a typical TRA game duration (on the order of a few stages) fits between successive route changes,

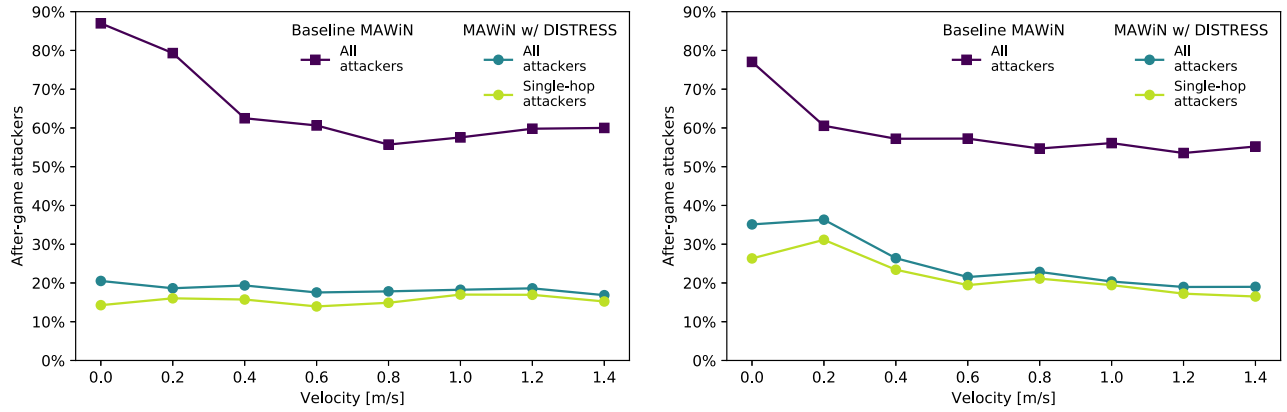


Fig. 9. Percentage of after-game attackers in N for varying node velocities in the case of grid (a) and random (b) initial topologies.

this may complicate ill-behaved nodes' strategic behavior. For preliminary insight, we assume that they nevertheless stick to rule (e); in particular, they calculate $\text{cost}_{3i}(\varnothing)$ only once for distress perception, at game start, and maintain the current action (TRA or honest) indefinitely when the out-of-game condition is satisfied. The key question was whether the DISTRESS mechanism would still be able to restrain TRAs. As an evaluation metric for our DISTRESS mechanism, we used the percentage of after-game attackers, which reflects how many of the network's ill-behaved nodes remain attackers after the game has terminated. Using this metric, we compared the performance of a MAWiN under the DISTRESS mechanism with a baseline MAWiN, where nodes do not fear service suspension and remain attackers if such behavior improves the QoS metrics (8) of their source flows.

In Fig. 9, each point is an average of 100 independent simulation runs with half the nodes being ill-behaved ($|I| = |N|/2$). Simulations confirmed that even for the maximum node velocity the adopted settings created a quasistatic environment—route changes during the TRA game were occasional or none and the play closely resembled that of Section IV-C. Hence, irrespective of node velocity and initial placement, after-game attackers were indeed distinctly fewer than for the baseline MAWiN with the DISTRESS mechanism disengaged; they were mostly limited to ill-behaved sources of single-hop flows, which, having no forwarding services to rely upon, remained unaffected by the DISTRESS mechanism.

To evaluate our proposed mechanism against varying attack intensity, we note that Definitions 2–4 do not leave room for any gradation of TRA intensity: a node either behaves honestly or executes a plausible opportunistic TRA. Therefore, the overall attack intensity in the network is sufficiently reflected by the percentage of ill-behaved nodes in N. Fig. 10 presents the respective simulation results for a high-mobility (1.4 m/s) scenario of the grid topology. DISTRESS is uniformly able to incentivize honest behavior in all (or almost all) of those ill-behaved nodes which are the sources of multihop flows. As before, only the sources of single-hop flows remain attackers.

Finally, even though a node's placement in the network topology does influence the potential benefits of becoming an attacker (as is visible in Fig. 2), one suspects that the

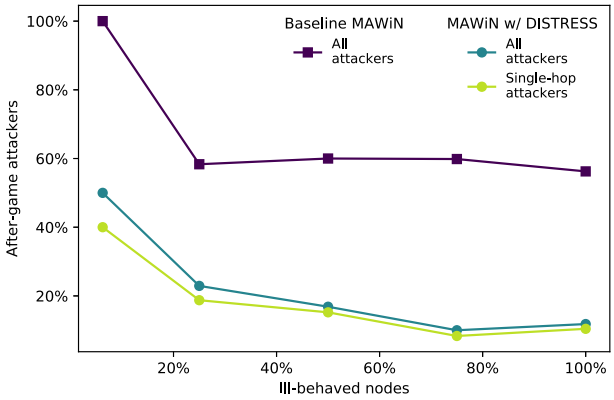


Fig. 10. Percentage of after-game attackers in N for a varying percentage of ill-behaved nodes in the grid topology with high mobility.

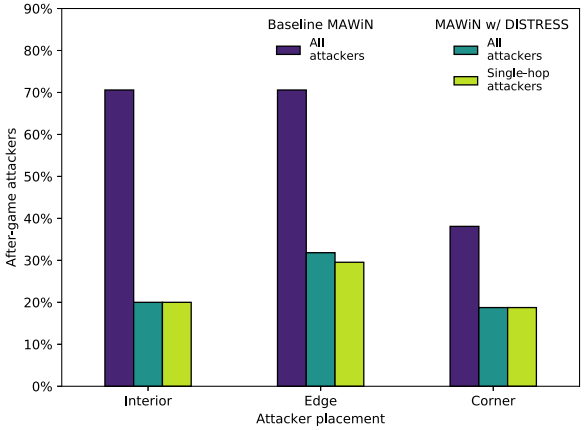


Fig. 11. Percentage of after-game attackers depending on initial ill-behaved node placement in the grid topology with high mobility.

effectiveness of the DISTRESS mechanism does not depend on the placement of attackers. This is because DISTRESS signaling is network-wide and affects the cost metric (11) of each node regardless of its location. Fig. 11 shows that indeed the initial placement (interior, edge, or corner) of ill-behaved nodes in a grid-topology MAWiN does not impact the percentage of after-game attackers.

VI. Conclusion

A TRA is hard to defend against in MAWiNs due to their multihop topology, node autonomy, and complex interplay of factors affecting end-to-end performance. We have proposed a systematic game-theoretic approach to TRA mitigation. The adopted model of a MAWiN under plausible opportunistic TRAs allows defining a noncooperative multistage TRA game arising among selfish nodes, in which the payoff function is provided by a novel network-oriented end-to-end QoS metric. We have augmented this function to reflect the threat of forwarding service suspension due to ongoing TRAs, as disseminated by a robust and low-cost distributed signaling mechanism called DISTRESS.

Our work distinguishes itself by proposing the first distributed self-enforcing mitigation approach for TRAs in MAWiNs. Existing solutions are not directly comparable: they counteract other types of attacks, rely on attack detection, require centralized control, or have been designed for single-hop networks and cannot cope with the multihop nature of TRAs. However, an advantage of the proposed framework is that by analyzing all feasible action selection rules (12), it enables an exhaustive search of a wide class of selfish nodes' multistage strategies. Therefore, optimum rules can be found according to the selected criteria, so that comparisons with particular solutions, existing or to be found in the future, are less relevant.

Our framework also enables a precise statement of postulates regarding a desirable game outcome: opt-out (well-behaved nodes need not play), termination (the finite game duration is guaranteed), rationality (ill-behaved nodes select best-reply behavior), defensibility and efficiency (well- and ill-behaved nodes receive satisfactory QoS), and survivability (little traffic is threatened by forwarding service suspension). We have argued that ill-behaved nodes are likely to use a strategy that, under certain assumptions regarding MAWiN topology and traffic flows, guarantees that these postulates are satisfied. The game outcome remains desirable even for a broader class of static-topology MAWiNs, as demonstrated by Monte Carlo simulations; time-true simulations using ns-3 extend this conclusion to networks with mobile nodes.

A straightforward extension of the DISTRESS mechanism to dynamic routing is possible. Suppose a source node toggles between the available routes for its e2e-flow according to current traffic and propagation conditions. The forward-reliance relationship is then less restrictive: a DISTRESS flag received from a transit node on an available route can be interpreted by the source node as a noncommittal signal to resend DISTRESS flags further, depending on the projected usage of that route in the near future. Only upon reception of DISTRESS flags from all available routes does the source node mark itself as in-exposure. Details of handling noncommittal signals warrant a separate study.

Finally, mechanisms providing QoS security, similar to DISTRESS, might produce a viable game-theoretic defense against QoS abuse in other distributed settings offering QoS differentiation; this is left for future research.

References

[1] A. A. Atayero, O. I. Adu, and A. A. Alatishe, "Self organizing networks for 3GPP LTE," in *Proc. 14th Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2014, pp. 242–254.

[2] K. Haseeb, I. Ud Din, A. Almogren, N. Islam, and A. Altameem, "RTS: A robust and trusted scheme for IoT-based mobile wireless mesh networks," *IEEE Access*, vol. 8, pp. 68379–68390, 2020.

[3] R. Pirmagomedov *et al.*, "Applying blockchain technology for user incentivization in mmWave-based mesh networks," *IEEE Access*, vol. 8, pp. 50983–50994, 2020.

[4] H. Peng, Q. Ye, and X. Shen, "Spectrum management for multi-access edge computing in autonomous vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 7, pp. 3001–3012, Jul. 2020.

[5] J. Rodriguez-Robles, A. Martin, S. Martin, J. A. Ruiperez-Valiente, and M. Castro, "Autonomous sensor network for rural agriculture environments, low cost, and energy self-charge," *Sustainability*, vol. 12, no. 15, p. 5913, 2020.

[6] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100359.

[7] A. Bader and M.-S. Alouini, "Localized power control for multihop large-scale Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 503–510, Aug. 2016.

[8] M. S. Omar, S. A. R. Naqvi, S. H. Kabir, and S. A. Hassan, "An experimental evaluation of a cooperative communication-based smart metering data acquisition system," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 399–408, Feb. 2017.

[9] G. Ramezan, C. Leung, and Z. J. Wang, "A survey of secure routing protocols in multi-hop cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3510–3541, 4th Quart., 2018.

[10] Z. Liu and Y. Wu, "An index-based provenance compression scheme for identifying malicious nodes in multihop IoT network," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4061–4071, May 2020.

[11] G. Chen, J. P. Coon, A. Mondal, B. Allen, and J. A. Chambers, "Performance analysis for multihop full-duplex IoT networks subject to Poisson distributed interferers," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3467–3479, Apr. 2019.

[12] *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 Standard 802.11-2016 (Revision of IEEE Std 802.11-2012), 2016.

[13] M. Allman, V. Paxson, and E. Blanton, "TCP congestion control," Internet Eng. Task Force, Fremont, CA, USA, RFC 5681, 2009.

[14] M. Li, S. Salinas, P. Li, J. Sun, and X. Huang, "MAC-layer selfish misbehavior in IEEE 802.11 ad hoc networks: Detection and defense," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1203–1217, Jun. 2015.

[15] A. Akella, S. Seshan, R. Karp, S. Shenker, and C. Papadimitriou, "Selfish behavior and stability of the Internet: A game-theoretic analysis of TCP," in *Proc. Conf. Appl. Technol. Archit. Protocols Comput. Commun. (SIGCOMM)*, 2002, pp. 117–130.

[16] F. Afghah, A. Shamsoshoara, L. Njilla, and C. Kamhoua, "A reputation-based Stackelberg game model to enhance secrecy rate in spectrum leasing to selfish IoT devices," in *Proc. IEEE INFOCOM Workshops*, 2018, pp. 312–317.

[17] X. Zhang, P. Huang, L. Guo, and M. Sha, "Incentivizing relay participation for securing IoT communication," in *Proc. IEEE INFOCOM IEEE Conf. Comput. Commun.*, 2019, pp. 1504–1512.

[18] T. Szigeti, C. Hattingh, R. Barton, and K. Briley, Jr., *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*. Indianapolis, IN, USA: Cisco Press, 2013.

[19] S. Szott and J. Konorski, "Traffic remapping attacks in ad hoc networks," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 218–224, Apr. 2018.

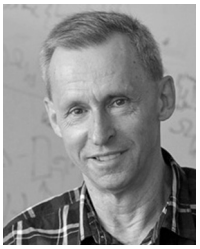
[20] S. Waldbusser *et al.*, "Terminology for policy-based management," Internet Eng. Task Force, Fremont, CA, USA, RFC 3198, Nov. 2001.

[21] R. Stankiewicz, P. Cholda, and A. Jajszczyk, "QoX: What is it really?" *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 148–158, Apr. 2011.

[22] J. Konorski and S. Szott, "Discouraging traffic remapping attacks in local ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3752–3767, Jul. 2014.

[23] S. Szott and J. Konorski, "Selfish attacks in two-hop IEEE 802.11 relay networks: Impact and countermeasures," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 658–661, Aug. 2018.

[24] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, 2nd Quart., 2016.
[25] J. Konorski and S. Szott, "Modeling a traffic remapping attack game in a multi-hop ad hoc network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2017, pp. 1–7.
[26] H. Jahan, M. Hassan, and S. K. Das, "A brinkmanship game theory model for competitive wireless networking environment," in *Proc. IEEE Local Comput. Netw. Conf.*, 2010, pp. 120–127.
[27] N. Samian, Z. A. Zukarnain, W. K. Seah, A. Abdullah, and Z. M. Hanapi, "Cooperation stimulation mechanisms for wireless multihop networks: A survey," *J. Netw. Comput. Appl.*, vol. 54, pp. 88–106, Aug. 2015.
[28] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3718–3731, May 2016.
[29] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
[30] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 1893–1907, Aug. 2016.
[31] K. R. Liu and B. Wang, *Cognitive Radio Networking and Security: A Game-Theoretic View*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[32] E. Ayday and F. Fekri, "A protocol for data availability in mobile ad-hoc networks in the presence of insider attacks," *Ad Hoc Netw.*, vol. 8, no. 2, pp. 181–192, 2010.
[33] J. Parras and S. Zazo, "Wireless networks under a backoff attack: A game theoretical perspective," *Sensors*, vol. 18, no. 2, p. 404, 2018.
[34] W. F. Fihri, H. E. Ghazi, B. A. E. Majd, and F. E. Bouanani, "A machine learning approach for backoff manipulation attack detection in cognitive radio," *IEEE Access*, vol. 8, pp. 227349–227359, 2020.
[35] G. Potrino, F. de Rango, and A. F. Santamaria, "Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2019, pp. 1–6.
[36] F. De Rango, M. Tropea, and P. Fazio, "Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy," in *Proc. IEEE INFOCOM Workshops*, 2020, pp. 842–847.
[37] R. Haywood, S. Mukherjee, and X.-H. Peng, "Investigation of H.264 video streaming over an IEEE 802.11e EDCA wireless testbed," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–5.
[38] A. Politis, P. Kyramaridis, and C. Hilas, "A MAC-centric approach to detect and mitigate EDCA misbehavior attacks," *J. Eng. Sci. Technol. Rev.*, vol. 9, no. 5, pp. 93–96, 2016.
[39] J. Li, X. Gao, Q. Yang, W. Gao, and K. S. Kwak, "Neural-network aided dynamic control for delivering media streams in selfish wireless networks with unknown node-selfishness," *IEEE Access*, vol. 6, pp. 31759–31771, 2018.
[40] G. Fang, M. A. Orgun, R. Shankaran, E. Dutkiewicz, and G. Zheng, "Truthful channel sharing for self coexistence of overlapping medical body area networks," *PLoS ONE*, vol. 11, no. 2, 2016, Art. no. e0148376.
[41] J. C. Kirchhof, M. Serror, R. Glebke, and K. Wehrle, "Improving MAC protocols for wireless industrial networks via packet prioritization and cooperation," in *Proc. IEEE WoWMoM*, 2020, pp. 367–372.
[42] A. C. Politis and C. S. Hilas, "Sharing transmission opportunity in ad-hoc WLANs supporting VoIP," in *Proc. 7th Int. Conf. Modern Circuits Syst. Technol. (MOCAST)*, 2018, pp. 1–4.
[43] A. Saxena and M. Khule, "Remapping attack detection and prevention for reliable data service in MANET," in *Proc. Int. Conf. Recent Adv. Comput. Commun.*, 2018, pp. 125–134.
[44] S. Szott, "Selfish insider attacks in IEEE 802.11s wireless mesh networks," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 227–233, Jun. 2014.
[45] J. Choi, "Detection of misconfigured BYOD devices in Wi-Fi networks," *Appl. Sci.*, vol. 10, no. 20, p. 7203, 2020.
[46] P. Patras, H. Feghhi, D. Malone, and D. J. Leith, "Policing 802.11 MAC misbehaviours," *IEEE Trans. Mobile Comput.*, vol. 15, no. 7, pp. 1728–1742, Jul. 2016.
[47] Y. Shimoyamada, K. Sanada, N. Komuro, and H. Sekiya, "End-to-end throughput analysis for IEEE 802.11e EDCA string-topology wireless multi-hop networks," *Nonlinear Theory Appl. IEICE*, vol. 6, no. 3, pp. 410–432, 2015.
[48] K. Sanada, N. Komuro, Z. Li, T. Pei, Y. J. Choi, and H. Sekiya, "Generalized analytical expressions for end-to-end throughput of IEEE 802.11 string-topology multi-hop networks," *Ad Hoc Netw.*, vol. 70, pp. 135–148, Mar. 2018.
[49] S. Rezaei, M. Gharib, and A. Movaghar, "Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework," *IEEE Trans. Commun.*, vol. 66, no. 11, pp. 5430–5443, Nov. 2018.
[50] S. Szott, M. Natkaniec, and A. R. Pach, "An IEEE 802.11 EDCA model with support for analysing networks with misbehaving nodes," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, p. 71, Apr. 2010.
[51] P. D. Straffin, *Game Theory and Strategy*. Washington, DC, USA: Math. Assoc. America, 1993.
[52] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," Internet Eng. Task Force, Fremont, CA, USA, RFC 4728, 2007.
[53] J. Konorski and K. Rydzewski, "Guessing intrinsic forwarding trustworthiness of wireless ad hoc network nodes," in *Ad Hoc Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 306, J. Zheng, C. Li, P. H. J. Chong, W. Meng, and F. Yan, Eds. Cham, Switzerland: Springer, 2019, pp. 314–331.



Jerzy Konorski received the M.Sc. degree in telecommunications from Gdańsk University of Technology, Gdańsk, Poland, in 1976, and the Ph.D. degree in computer science from the Polish Academy of Sciences, Warsaw, Poland, in 1984.

In 2002, he was the Visiting Erskine Fellow with the University of Canterbury, Christchurch, New Zealand. He is currently an Associate Professor with the Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology. He has authored over 170 papers in the area of computer communications, led academic projects funded by the EU, U.S. Air Force, and National Science Center, Poland, and served on the TPC for over 150 international conferences. His research and teaching expertise includes probability and statistics, information systems, data transmission, operational research, distributed environments, computer networking, and decision theory. His current research focuses on game theory in wireless networks and security architectures and reputation and trust building systems in distributed networking environments.

Szymon Szott received the M.Sc. and Ph.D. degrees (Hons.) in telecommunications from the AGH University of Science and Technology, Krakow, Poland, in 2006 and 2011, respectively.

He is currently working as an Associate Professor with the Institute of Telecommunications, AGH University of Science and Technology. In 2013, he was a Visiting Researcher with the University of Palermo, Palermo, Italy, and Stanford University, Stanford, CA, USA. He has authored or coauthored over 70 research papers. His professional interests are related to wireless local area networks (channel access, quality of service, security, and intertechnology coexistence).

Dr. Szott is a reviewer for international journals and conferences. In the past, he has been a member of ETSI's Network Technology Working Group Evolution of Management toward Autonomic Future Internet, an IEEE 802.11 Working Group Member, and on the management board of the Association of Top 500 Innovators. He has been involved in several European projects (DAIDALOS II, CONTENT, CARMEN, MEDUSA, FLAVIA, PROACTIVE, and RESCUE) as well as grants supported by the Ministry of Science and Higher Education and the National Science Centre.