Postprint of: Konorski J., Szott S.. Selfish Attacks in Two-Hop IEEE 802.11 Relay Networks: Impact and Countermeasures. IEEE WIRELESS COMMUNICATIONS LETTERS, 2018, Vol. 7, nr. 4, pp. 658-661
DOI: 10.1109/LWC.2018.2809726



# Selfish Attacks in Two-hop IEEE 802.11 Relay Networks: Impact and Countermeasures

Szymon Szott, *Senior Member, IEEE.* and Jerzy Konorski

***Abstract*—Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non velit lacus. Donec viverra bibendum tortor, ac imperdiet nibh interdum eu. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Vestibulum id ex vitae sapien dictum luctus id in massa. Aliquam posuere, risus sit amet tincidunt feugiat, orci erat condimentum libero, id aliquet est nisl non nibh. Duis vel.**

***Index Terms*—Relay networks, IEEE 802.11, EDCA, QoS, game theory, selfish behavior, traffic remapping**

## I. Introduction

THE coverage of IEEE 802.11 networks can be extended if stations connected to an access point (AP) act as relays, i.e., they share their connection with other, neighboring stations, who either cannot reach an AP themselves or have a poor connection to it. This approach creates a two-hop relay network which is known to have many advantages in terms of network coverage and performance [1].

A two-hop relay network requires cooperation from the relaying station. However, even if the relay agrees to cooperate, it may want to provide preferential treatment for its own over relayed traffic (Fig. 1). This can be achieved through *selfish attacks* in which the attacker abuses network mechanisms to achieve an undue increase of the quality of service (QoS) [2]. For example, by refusing to forward offered transit packets (the *packet dropping* attack) the relay conserves bandwidth for source packets. However, more subtle misbehavior can be thought of that undoubtedly brings an attacker a better QoS without exposing it to easy detection. First, packet scheduling in the forwarding path can be biased in favor of source traffic. Second, source packets can be unduly prioritized at the MAC-layer. Since it is the MAC mechanisms that ultimately decide the order and delays of medium acquisition by successive packets (Section II), in what follows we focus on MAC-layer attacks which we define in Section III.

Selfish MAC-layer attacks pose a serious threat to IEEE 802.11 networks for several reasons: they are easy to perform, secure routing protocols do not prevent them, and their detection involves using complex methods [2]. These attacks have been studied in single-hop networks [3]. However, the two-hop relay topology introduces an important novelty, in that the relay can tamper with the QoS of either source traffic, or transit traffic, or both (Fig. 1). We consider the applicability of these attacks and their variants in the two-hop relay topology (Section IV), quantify their impact (Section V), and study defense measures (Section VI).

S. Szott is with AGH University, Poland.
J. Konorski is with the Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Poland.

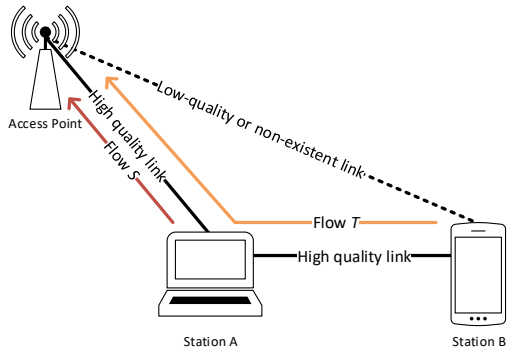


Fig. 1: Conceptual setting for selfish attacks in a two-hop relay network. Station A, as the relay, can increase its QoS perception by executing a selfish attack: promoting source traffic (flow $S$), demoting transit traffic (flow $T$), or both.

TABLE I: IEEE 802.11 high-rate direct-sequence spread spectrum (HR/DSSS) EDCA parameters: minimum and maximum contention window (CW), arbitration inter-frame space number (AIFSN), and transmission opportunity (TXOP) limit.

| AC | $CW_{min}/CW_{max}$ | $AIFSN$ [slots] | $TXOP_{limit}$ |
|---|---|---|---|
| VO | 7/15 | 2 | 3 ms |
| VI | 15/31 | 2 | 1.5 ms |
| BE | 31/1023 | 3 | single frame |
| BK | 31/1023 | 7 | single frame |

## II. QoS Provisioning in IEEE 802.11 Networks

QoS provisioning in IEEE 802.11 is achieved through the enhanced distributed channel access (EDCA) function. In EDCA, higher-layer traffic classes are mapped to one of four access categories (ACs), in order of decreasing priority: voice (VO), video (VI), best effort (BE), or background (BK). Each AC is characterized by four parameters (Table I), resulting in a configuration providing statistical prioritization with respect to channel access and duration.

Traffic classification into ACs is based on the Distributed Services Code Point (DSCP) set in a packet's IP header (in the `Type of Service` field in IPv4 or `Traffic Class` field in IPv6). DSCP values can be configured, according to higher-layer policies, using network-layer packet mangling software (such as Linux `iptables`) for all packets belonging to a given flow.

## III. Selfish Attacks in IEEE 802.11 Networks

The QoS provisioning model of IEEE 802.11 networks enables two types of selfish attacks: backoff attacks (BOAs) and traffic remapping attacks (TRAs). Both can be executed

either as *source traffic upgrading* or *transit traffic downgrading* (Fig. 1), which we denote ($^+$) and ($^-$), respectively.

### A. Backoff Attacks

BOAs belong to the class of MAC parameter manipulation attacks – out of the available medium access parameters (Table I) the contention window (CW) has proved to be the easiest to manipulate [4]. The CW governs the backoff mechanism, wherein each station *backs off* before accessing the channel by waiting a random number of time slots. An attacker may attempt to influence this random behavior so as to improve its QoS, either by decreasing CW for the AC of source traffic (BOA$^+$) or increasing it for transit traffic (BOA$^-$).

BOAs have two key advantages. First, modifying MAC parameters is often available as part of the command-line or graphical configuration interface. Second, detecting BOAs is challenging to detect due to both the randomness inherent to the backoff function as well as the practical difficulties in performing precise time measurements.

The BOA$^+$ attack has mostly been studied in a single-hop infrastructure-based WLAN setting and shown to effectively promote the attacker's traffic [4]. In a relay setting, a BOA$^-$ can additionally be applied to transit traffic to discriminate it in favor of source traffic. Initial reports have shown that such attacks can improve the attacker's source throughput more effectively compared to BOA$^+$ in multi-hop networks [5]. Detailed research is required to quantify the impact of BOAs in two-hop relay settings and in combination with TRAs.

### B. Traffic Remapping Attacks

TRAs consist in claiming a different medium access priority through false DSCP settings so that traffic can be mapped onto a different AC. TRAs are simpler to perform than BOAs: a user application can using packet mangling software to change the current DSCP of any packet.

TRAs have been studied in single-hop ad hoc networks [3], where a distributed discouragement scheme, based on the threat of detection and punishment, allows TRAs only if they are harmless to honest stations; otherwise it induces selfish stations to learn that a long-sustained TRA is counterproductive. For relay networks, TRAs can be performed also on transit traffic to lower its priority (TRA$^-$). Such a possibility has thus far only been studied in a multi-hop scenario [5] necessitating further research.

## IV. Two-Hop Relay Topology

We make the following assumptions for analyzing the network in Fig. 1. Stations B and the AP are out of communication range. The placement of A in the topology allows the execution of any one of the previously discussed attacks. For ease of presentation we reduce the configuration space assuming that only two ACs are used: VO and BE, representing high and low priority traffic, respectively. The interesting case for analysis is when, at A, the transit traffic is VO and the source traffic is BE. We evaluate the attack performance under saturation traffic with TCP used at the transport layer.

TABLE II: Comparison of attacker's MAC-layer configuration for the BOAs and TRAs in the setting of Fig. 1. The last two columns indicate, respectively, which EDCA queue is used and what is its configuration. The latter denotes priority in medium access during frame transmission, the former – the QoS designation of the frames.

| Attack strategy | Flow | Intrinsic AC | Used AC | AC configuration |
|---|---|---|---|---|
| None (honest behavior) | T | VO | VO | VO |
| | S | BE | BE | BE |
| BOA$^+$ | T | VO | VO | VO |
| | S | BE | BE | VO |
| BOA$^-$ | T | VO | VO | BE |
| | S | BE | BE | BE |
| TRA$^+$ | T | VO | VO | VO |
| | S | BE | VO | VO |
| TRA$^-$ | T | VO | BE | BE |
| | S | BE | BE | BE |
| 2xTRA (TRA$^+$ and TRA$^-$) | T | VO | BE | BE |
| | S | BE | VO | VO |

### A. Uplink and Downlink Scenarios

In the *uplink scenario*, there are two TCP flows upon which A can execute the attacks: $S$, referred to as the source flow, and $T$, referred to as the transit flow. A's goal is to improve its uplink throughput (i.e., that of $S$). There are also auxiliary traffic flows carrying TCP ACK segments and originating at the AP, complementary to the TCP terminating at the AP: $S'$ and $T'$ (omitted from Fig. 1 for clarity). These two flows are important: even though they have a low rate, they impact the regularity of the TCP transmissions and thus end-to-end throughput of flows $T$ and $S$.

A *downlink scenario* can also be considered, where the saturated traffic flows are $T$ and $S'$. Note that again A can directly influence $T$ and $S$, the latter now consisting of TCP ACKs. However, A's goal is now to improve its downlink throughput (i.e., that of $S'$). Single-hop network studies have shown that MAC-layer attacks have no serious impact on downlink throughput [6]. Whether this holds for two-hop relay settings is an open question that we want to address.

### B. Attack Strategies

For each of the possible attack strategies it is helpful to have a specification regarding which AC queues are used at the attacker, how they are configured, and which traffic is sent using which AC (Table II). For BOAs, we assume setting valid EDCA configurations, e.g., in BOA$^+$ the BE AC is configured with VO parameters. Note that despite the pairs (BOA$^+$, TRA$^+$) and (BOA$^-$, TRA$^-$) sharing the same AC configuration, the attacks are not interchangeable. TRAs modify the QoS designation of each packet according to the 'Used AC' column in Table II. This impacts potential subsequent transmissions of the frame carrying this packet, as well as the QoS designation of the returned TCP ACKs.

BOAs and TRAs can also be combined into more sophisticated attack strategies. In particular, BOA$^+$ and BOA$^-$ (2xBOA) can be combined to produce a priority switch between the source and transit traffic flows ($S$ and $T$). A similar

priority switch is produced by a combination of $TRA^+$ and $TRA^-$ (2xTRA).

In combinations of BOA and TRA, the TRA component assigns both flows to the same AC queue, for which the BOA component increases or decreases CW and other EDCA parameters; the provided QoS will be affected depending on various factors including the number of contending stations. Hence combinations of BOA and TRA come under performance optimization rather than network security, and as such are outside our scope. In light of the above analysis, we consider only 2xBOA and 2xTRA in our analysis.

## V. Attack Impact Analysis

To study the impact of the considered attacks we used the ns-2.28 simulator. A multi-hop IEEE 802.11 HR/DSSS[1] network served the three stations in Fig. 1. The provided QoS is defined based on a flow's intrinsic AC: as packet delay for VO traffic, i.e., $T$ (which according to ITU-T recommendations should not exceed 100 ms), and as achieved throughput for BE traffic, i.e., $S$ or $S'$ in the uplink or downlink scenario, respectively[2]. The selfish relay A attempts to maximize the throughput of $S$ or $S'$ at the cost of the victim flow $T$ while maintaining a low risk of detection. We have simulated all attack strategies available to A (Table II). For clarity, we have omitted from the figures attack strategies combining BOA and TRA (previously indicated as irrelevant), as well as 2xBOA, which was found only a marginal improvement over stand-alone $BOA^-$, because the contribution of $BOA^+$ turned out to be negligible.

### A. Uplink Scenario

In the uplink scenario, from A's perspective, significant throughput gains of $S$ can be achieved by attacking (Fig. 2a). However, it is visible that $BOA^+$ (where A uses both BE and VO queues configured with VO parameters) is not beneficial in two-hop relay settings. This is because, regardless of the inter-queue contention that worsens the overall performance, the VO queue used by $T$ retains its relative priority: the TCP ACKs for $T$ are handled as VO traffic at the AP, creating a smaller round-trip time (RTT) than that experienced by $S$ (whose TCP ACKs are handled as BE traffic). Under $TRA^+$, flow $S$ approaches the throughput achieved by $T$ with A's honest behavior (the reference line in Fig. 2b). The downgrading attacks provide even better gains, which supports the hypothesis that promoting source traffic is less important than demoting transit traffic and elimination of inter-queue contention (note that compared to $BOA^-$, $TRA^-$ yields slightly better gains because it causes the AP to handle TCP ACKs for $T$ as BE traffic). However, 2xTRA is strikingly beneficial.

The throughput gains of $S$ are accompanied by the loss in throughput by $T$ (Fig. 2b). In most cases the loss ranges between 30% and 50% with the exception of 2xTRA where 90% of the throughput is lost. Delay in all but the last case is below the ITU-T requirement of 100 ms (Fig. 2c). This shows that some selfish attacks can be harmless (inflict no QoS degradation for $T$), even in indiscriminate saturation conditions.

### B. Downlink Scenario

In the downlink scenario both $BOA^+$ and $TRA^+$ provide a small (3–5%) throughput gain for $S'$ by increasing the sending rate of the corresponding TCP ACKs at the price of increasing the collision rate due to smaller CW values (Fig. 2d). $BOA^-$ and $TRA^-$ reduce the collision rate due to larger CW values, therefore are much more beneficial for A; $BOA^-$ slightly less so because, as explained in Section V-A, the VO queue used by $T$ still has relative priority despite being configured with BE parameters, whereas $TRA^-$ eliminates the inter-queue contention at A. Unexpectedly for A, 2xTRA performs no better than $TRA^-$. The reason is that the $TRA^+$ component has TCP ACKs for flow $S'$ handled as VO traffic at A. Thus $S'$ experiences a lower RTT and its transmit window is excessively expanded; the resulting increased collisions at the AP ultimately lower the throughput of $S'$. In all considered downlink cases, $T$'s delay, though sometimes elevated beyond the reference value (representing A's honest behavior), meets the ITU-T requirement of 100 ms (Fig. 2f).

## VI. Defense Measures

There exist many approaches to defend against selfish MAC-layer attacks in IEEE 802.11 networks, such as mitigating their impact, e.g., by rerouting traffic over a different path (if one can be found) [2]. Another approach is to provide incentives for cooperation. In two-hop relay networks this can be achieved through punishment of the attackers by the AP. Once the AP identifies flows as belonging to attackers, it can employ such measures as dropping ACK frames for the attacker's source packets, shaping the attacker's source traffic, or banning the attacker from further communication (by deauthentication and blacklisting). All of these actions can be considered a form of denial of service (DoS).

We evaluate two of these DoS measures in the topology of Fig. 1 in the uplink scenario. Both methods, as will be shown, involve only a small computational overhead on behalf of the punisher and no transmission overhead at all.

The first measure, dropping ACK frames [4], has the punisher refrain from sending MAC-layer ACK frames for correctly received DATA frames belonging to the attacker's source flow. The degree of penalty can be scaled by acknowledging an $\alpha \in [0, 1]$ portion of frames.

The second measure is traffic shaping, where the punisher applies traffic control to the attacker's TCP flows, e.g., in the form of a leaky bucket filter with a controlled output rate. This rate can be proportional, by $\alpha \in [0, 1]$, to the attacker's rate during an attack, so that for $\alpha = 1$ the throughput of $S$ is equal to that shown in Fig. 2a.

The results presented in Fig. 3 show that ACK dropping was able to scale $S$'s throughput for the downgrading attacks. However, for the upgrading attacks, dropping ACKs can inadvertently optimize $S$'s TCP flow with respect to the effect

[1] Selected simulations were performed also for IEEE 802.11 OFDM with the same qualitative results.

[2] The 95% confidence intervals are either presented in the figures or were too small for graphical representation.

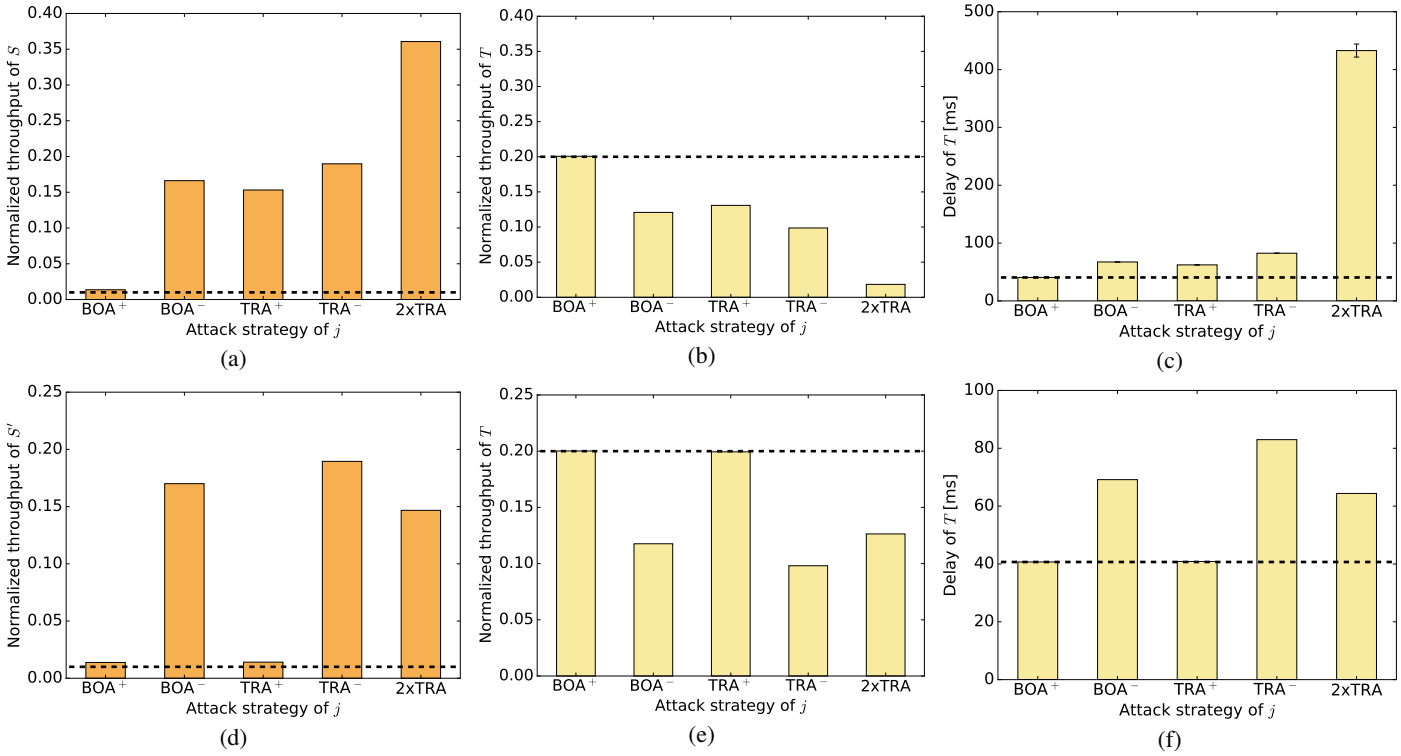


Fig. 2: Impact of A's attack strategy in the uplink (top) and downlink (bottom) scenario of the Fig. 1 topology ): throughput of $S/S'$ (left), throughput of $T$ (middle), and delay of $T$ (right). The reference line is for the case of A's honest behavior.

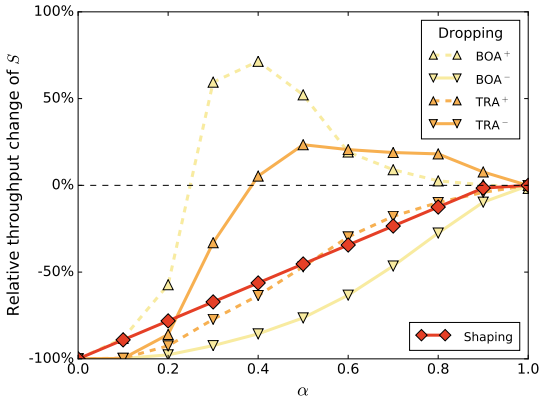


Fig. 3: Change of throughput of $S$ caused by punishment at the AP in comparison to unpunished attack.

of hidden stations and thus cause an unexpected *increase* of $S$'s throughput for $\alpha \in [0.4, 0.9]$. We have also evaluated the performance of flow $T$ (not shown) and observed that for TRA$^-$ the throughput is reduced for both $S$ and $T$; clearly, ACK dropping has caused *network* performance degradation. In contrast, traffic shaping allowed to successfully (almost linearly) control the throughput of $S$. Similar results were obtained in the downlink scenarios (thus they are not presented here).

## VII. Conclusions

Based on our analysis we can state the following: 1) as long as the QoS requirements of high-priority traffic are met, the selfish attacks can be considered harmless; this was always the case except for 2xTRA in the uplink scenario, 2) unlike in single-hop networks, BOA$^+$ brings the attacker no benefit in two-hop relay networks because it does not modify the packet's QoS designation, 3) downgrading attacks perform better than their upgrading counterparts, particularly in the downlink scenario, 4) BOA$^-$ and TRA$^-$ perform similarly; however, only the latter has a potential multi-hop impact, 5) combined attack strategies are only beneficial in the case of 2xTRA in the uplink scenario; adding TRA$^+$ to TRA$^-$ in the downlink scenario is counterproductive, whereas adding BOA$^+$ to BOA$^-$ (2xBOA) does not bring any benefits regardless of scenario, 6) ACK dropping, while effective in single-hop WLANs, cannot be viewed as a valid punishment in two-hop relay networks because of its unpredictable behavior.

## References


[1] A. Garcia-Saavedra, B. Rengarajan, P. Serrano, D. Camps-Mur, and X. Costa-P?rez, "SOLOR: Self-Optimizing WLANs With Legacy-Compatible Opportunistic Relays," *IEEE/ACM Transactions on Networking*, vol. 23, no. 4, pp. 1202–1215, 2015.

[2] S. Szott, "Selfish insider attacks in IEEE 802.11s wireless mesh networks," *IEEE Communications Magazine*, vol. 52, pp. 227–233, 2014.

[3] J. Konorski and S. Szott, "Discouraging traffic remapping attacks in local ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 3752–3767, 2014.

[4] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. of INFOCOM*, 2005.

[5] S. Szott, M. Natkaniec, and A. Banchs, "Impact of Misbehaviour on QoS in Wireless Mesh Networks," in *Proc. of IFIP Networking*, 2009.

[6] S. Szott, M. Natkaniec, R. Canonico, and A. R. Pach, "Impact of Contention Window Cheating on Single-Hop IEEE 802.11e MANETs," in *Proc. of WCNC*, 2008.