Selfish Attacks in IEEE 802.11aa Networks with Intra-AC Prioritization

Lukasz Prasnal
AGH University of
Science and Technology
Krakow, Poland
Email: prasnal@kt.agh.edu.pl

Szymon Szott
AGH University of
Science and Technology
Krakow, Poland
Email: szott@kt.agh.edu.pl

Marek Natkaniec
AGH University of
Science and Technology
Krakow, Poland
Email: natkaniec@kt.agh.edu.pl

***Abstract*—The 802.11 standard is prone to selfish attacks performed by insiders, i.e., correctly authenticated stations. The recently released 802.11aa amendment is likewise prone to such attacks because the mechanisms which it provides can be selfishly configured by insiders to raise their QoS. In this paper, we present the first security analysis of 802.11aa by investigating selfish insider attacks against the intra-AC prioritization feature. Our analysis shows that 802.11aa is susceptible to already existing attacks as well as attacks previously not considered. Furthermore, our research shows the extent to which an attacker can benefit from these types of selfish behaviors. Therefore, we can identify which mechanisms should be augmented with countermeasures to protect 802.11aa networks from selfish attackers.**

I. Introduction

Providing quality of service (QoS) support in Wi-Fi networks is a challenging task. To improve audio-video streaming in such networks, the recently released IEEE 802.11aa [1] amendment defines several new mechanisms. Among them is intra-access category (intra-AC) prioritization (Section II). This feature extends the enhanced distributed channel access (EDCA) traffic prioritization of the IEEE 802.11 standard [2] by introducing two new transmit queues (primary and alternate) for the two high priority ACs (voice, VO and video, VI) to enable differentiation of audio-video streams service.[1] There have already been several studies of 802.11aa [3]–[6]: all of them have focused on analyzing the performance of the QoS mechanisms defined therein. However, no security analysis of these mechanisms has yet been performed.

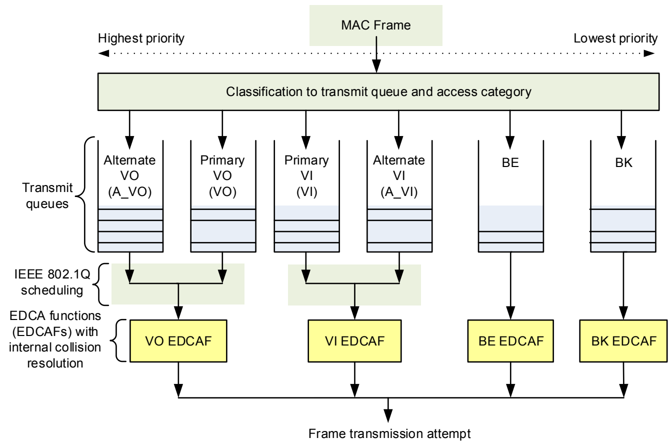


Fig. 1. Traffic prioritization in IEEE 802.11aa. The new transmit queues allow to differentiate the priority for two ACs: VO and VI.

It is well known that the 802.11 standard is prone to selfish attacks performed by insiders, i.e., correctly authenticated stations [7]. Such attackers aim to directly or indirectly increase their QoS by abusing network mechanisms. This is in contrast to malicious attacks that aim at destabilizing network performance. Selfish attacks are an emerging threat for Wi-Fi networks for several reasons: equipment vendors may attempt to illegitimately increase the performance of their devices [8]; there is a trend toward applying software-defined networking (SDN) principles in wireless card drivers [9], which paves the way for nonstandard and noncooperative behavior [10]; and although 802.11 provides authentication and encryption to protect the network from external attacks, it is still susceptible to selfish insider attacks. The recently released 802.11aa amendment is likewise prone to such attacks because, as we will show in this paper, the mechanisms which it provides can be selfishly configured by users to raise their QoS.

In this paper, we present *the first security analysis of 802.11aa* by investigating selfish insider attacks against the intra-AC prioritization feature. Similar analyses have been performed for previous amendments of 802.11: selfish attacks were studied in 802.11e (EDCA) networks [11]–[13] and 802.11s (mesh) networks [14], [15]. Our analysis shows that *802.11aa is susceptible to already existing attacks as well as attacks previously not considered* (Section III). Furthermore, our research shows *the extent to which an attacker can benefit from these types of selfish behaviors* (Section IV). We *discuss execution costs and detection methods* which allows us to *quantify the threat of each attack* (Section V). Finally, we summarize the main conclusions and outline future work on protecting 802.11aa networks from selfish insiders.

II. IEEE 802.11aa Basics

Intra-AC prioritization allows individual audio and video streams to be treated with different priorities [16]. In particular,

[1] The operation of the lower priority ACs, best effort (BE) and background (BK), remains the same.

higher priority (HP) is given to A_VO over VO and VI over A_VI (Fig. 1). The addition of two new transmit queues requires new scheduling functions situated above the EDCA functions (with separate instances for VO and VI), which decide between the 802.11aa transmit queues (primary and alternate). These schedulers are always configured so that the HP queue is selected more often that the lower priority (LP) queue. Two scheduling algorithms are suggested by 802.11aa: the strict priority algorithm (SPA) and the credit-based shaper algorithm (CBSA). SPA, the default algorithm, selects the LP queue only when the HP queue is empty. Alternatively, CBSA, defined in 802.1Q [17], can be used to provide more flexible bandwidth allocation. In this paper, we focus on CBSA, as the more interesting case. However, the main conclusions derived from the simulation analysis of CBSA (Section IV) apply likewise to SPA.

CBSA limits the rate of the LP queue by selecting it only if an internal parameter, called the *credit* value, is non-negative. In particular, CBSA selects a frame from the LP queue if (a) $credit > 0$ or (b) $credit = 0$ and the HP queue is empty. Otherwise, CBSA selects a frame from the HP queue. The value of *credit* is based on two external parameters: *portTransmitRate* – the transmission rate, in bits per second, supported by the underlying MAC service, and *idleSlope* – the rate of change of *credit*, in bits per second, when the value of *credit* increases. The latter determines the maximum portion of *portTransmitRate* available for the transmission of frames stored in the LP queue. Additionally, *sendSlope*, an internal parameter, determines the rate of *credit* change, in bits per second, when the value of *credit* decreases. It is calculated as the difference between *idleSlope* and *portTransmitRate*.

Credit is increased with a rate of *idleSlope* (a) during the transmission of a frame from the HP queue and (b) when there is no transmission while *credit* is negative. *Credit* is decreased with a rate of $sendSlope$ during the transmission of a frame from the LP queue. If $credit$ is positive and the LP queue is empty then it is reset to zero. Additional parameters (*loCredit* and *hiCredit*) limit the minimum and maximum values of *credit*. They are calculated based on the maximum size of a frame that can be transmitted, the maximum size of a burst of HP traffic that can delay a frame transmission, as well as the *idleSlope* and *portTransmitRate* parameters [6].

In order to achieve precise throughput division between priority and alternate queues of a given AC, we have proposed a modified implementation of CBSA, called wireless CBSA (WCBSA)[2] [18]. The main idea behind this solution is keeping the *credit* value unchanged during the acknowledgment procedure, retransmissions and medium access waiting times (e.g., the backoff procedure). Fig. 2 illustrates how *credit* changes in an exemplary traffic scenario.

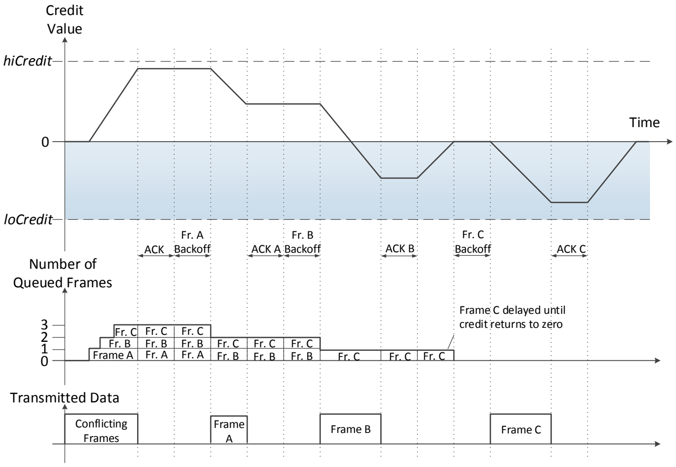


Fig. 2. Operation of WCBSA for three frames (A, B, and C) queued in the LP queue during the transmission of conflicting traffic.

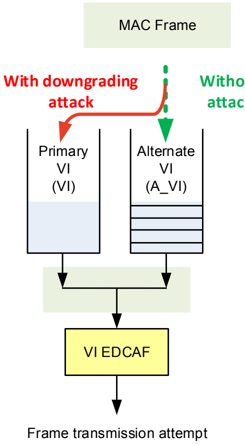


Fig. 3. Example of a downgrading attack. With 802.11aa disabled, the alternate queues are not used.

III. Types of Selfish Attacks

In this section we describe three categories of selfish attacks to which IEEE 802.11aa is intrinsically susceptible to: downgrading, traffic remapping, and parameter manipulation. The attack execution of the first and last of these is unique to 802.11aa, whereas the traffic remapping attack is already possible in EDCA networks, but 802.11aa extends its scope.

A. Downgrading Attack

In an 802.11aa network, a selfish station can perform a *downgrading attack*, i.e., disable its support for 802.11aa by modifying an internal configuration parameter, and become a legacy station. This attack is beneficial to the selfish station when the intra-AC queue selection procedure limits bandwidth of a given traffic priority. It occurs when sending VO or VI traffic which would be mapped to the LP queues (Fig. 3). We perform an analysis of this attack in Section IV-A.

[2] Note that CBSA was originally defined for wired networks. Therefore, improvements were necessary to adapt CBSA to wireless networks. Further details regarding the implementation of WCBSA can be found in [18].

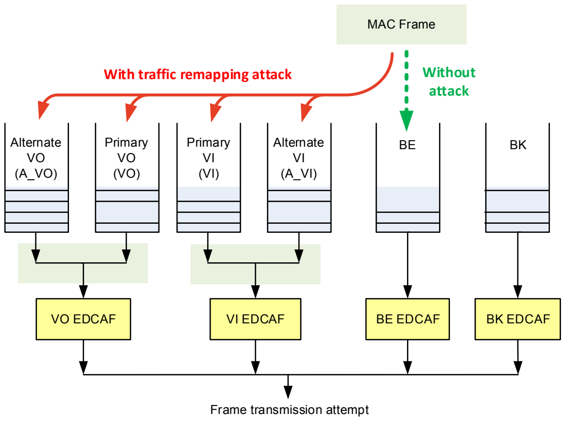


Fig. 4. Example of a traffic remapping attack. The attacker modifies the DSCP code of its best effort packets in order to upgrade their priority.

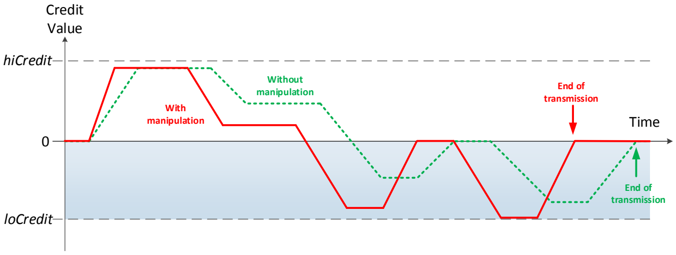


Fig. 5. Example of an *idleSlope* manipulation attack based on the conditions depicted in Fig. 2.

B. Traffic Remapping Attack

A selfish station can perform a *traffic remapping attack* by upgrading the priority of locally generated traffic. This can be achieved through modifying the QoS designation of transmitted traffic so that it can be mapped onto a higher priority queue (Fig. 4). Note that the downgrading attack (Fig. 3) can be considered a special case of the traffic remapping attack. We study the performance of the latter in Section IV-B.

C. Parameter Manipulation Attack

To increase its chances of accessing the radio channel, an attacker may manipulate the values of its medium access parameters such as the contention window minimum and maximum values. Among the parameters introduced by IEEE 802.11aa, *idleSlope* is particularly prone to manipulation since it has a direct impact on all the other 802.11aa parameters (Section II). By increasing *idleSlope*, the variance of the credit value increases (the slope is more steep) but over time a series of transmissions may be completed faster than with standard settings (Fig. 5). The advantages of this manipulation attack are studied in Section IV-C.

IV. Simulation Results

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
RTS/CTS, TXOPLimit	Turned off	Queue size	400 frames
Preamble length	16 μs	Slot time	9 μs
PLCP header length	4 μs	SIFS	16 μs
DATA payload	1000 B	PHY layer	OFDM (802.11a)
Data rate	54 Mbps	Basic rate	6 Mbps
Transport protocol	UDP	Traffic type	CBR
Parameter		**Value**	
CW$_{min}$ {VO, VI, BE, BK}		{3, 7, 15, 15}	
CW$_{max}$ {VO, VI, BE, BK}		{7, 15, 1023, 1023}	
AIFSN {VO, VI, BE, BK}		{2, 2, 3, 7}	

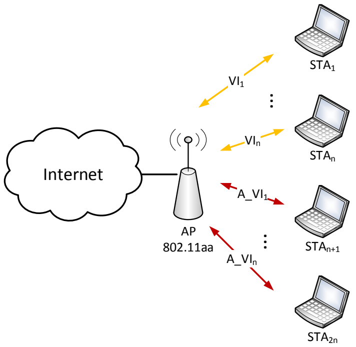
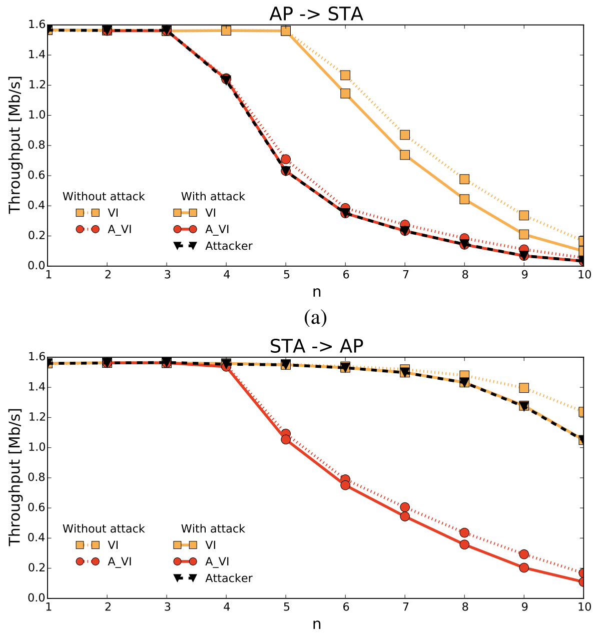


Fig. 6. Network topology in the downgrading attack scenario

The simulations were performed in ns-3 [19] which we extended to support IEEE 802.11aa intra-AC differentiation. In all scenarios, the network topology consisted of an AP with a varying number of stations (STAs), one of which was an *attacker* (we refer to the other stations as *honest*). We analyzed three simulation scenarios, one for each of the considered attacks: downgrading, traffic remapping, and *idleSlope* manipulation. The simulation parameters used in these scenarios are presented in Table I. Additionally, unless noted otherwise, *idleSlope* = 25% (based on our previous performance analysis [6]) and there was only one attacker.

A. Downgrading Scenario

In this scenario, we assumed bidirectional video transmissions, representative of a videoconference, between the AP and its associated stations (Fig. 6). Furthermore, we assumed that each of these stations used one of the 802.11aa transmit queues (VI or A_VI). We denote the number of stations using each queue as n. We set $idleSlope = 25\% \times \frac{1}{n}$ to provide fair division of the A_VI throughput. The attacker attempted to gain an advantage by disabling 802.11aa support and switching to EDCA. Thus, we assumed that the attacker belongs to the group of stations using A_VI. To observe the impact of the attack depending on network size, n varied from 1 to 10. Fig. 7 presents the throughput achieved by each station in this scenario. In the downlink direction (Fig. 7a), the flows were not significantly affected by the attack as the attacking station cannot affect the AP's settings. Specifically, there was no change in the attacker's throughput and only a slight decrease in throughput for the VI flows. In the uplink direction (Fig. 7b), the attacker can gain by redirecting traffic from the A_VI flows to the VI flows in terms of throughput.



(a)

(b)

Fig. 7. Per-station throughput difference as a consequence of the downgrading attack in the (a) downlink and (b) uplink directions

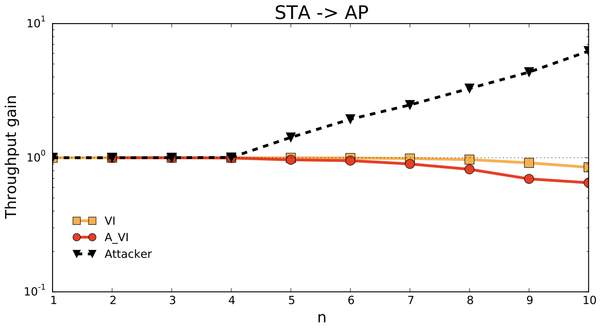


Fig. 8. Per-station throughput difference as a consequence of the downgrading attack

This means that there is one more VI flow (and one A_VI flow less) which reduces the per-station throughput for both VI and A_VI flows. The quantified gain from the attack is shown in Fig. 8, which presents the difference in throughput caused by the attack. Since the measured difference is relative, the gain in throughput is proportional to the number of stations in the network. Hence, the larger the network the larger the incentive to perform a selfish attack.

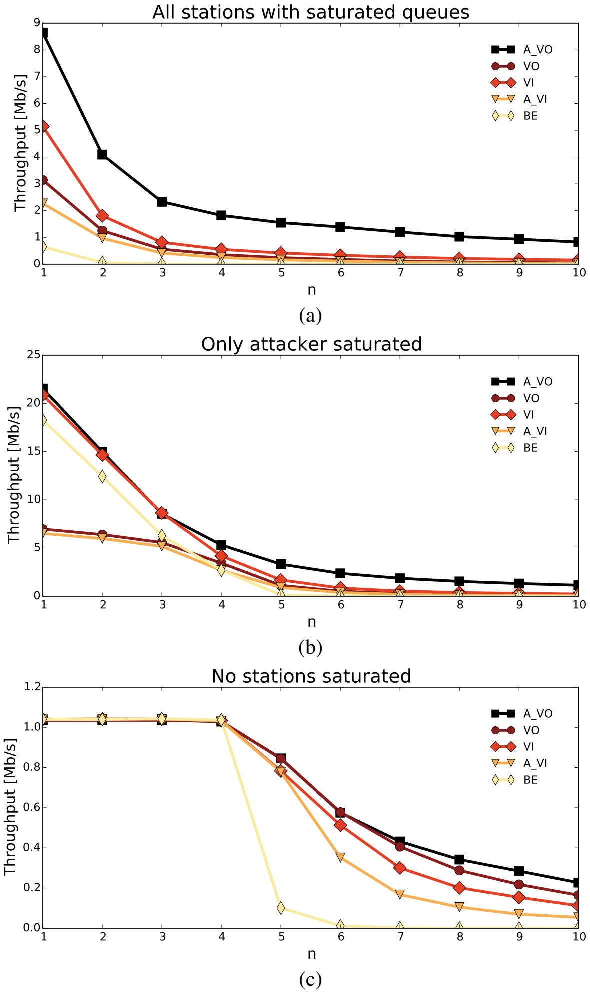
B. Traffic Remapping Scenario

To illustrate the effectiveness of the traffic remapping attack, we simulated a network in which n stations generated traffic belonging to all six ACs while one station sent BE traffic. To achieve higher throughput, this station became an attacker and behaved selfishly by diverting traffic to one of the other categories (Fig. 4). Fig. 9 presents the attacker's throughput in this scenario with the BE traffic throughput as the baseline (no attack) and A_VO to A_VI as the four remapping possibilities. We considered three different traffic scenarios in which stations had non-saturated queues (an offered load of 1 Mb/s) or saturated queues (30 Mb/s). When all queues were saturated (Fig. 9a), every type of traffic remapping attack gave proportionally better throughput. However, if only the attacker has a saturated queue (Fig. 9b), using either of the two lower-priority 802.11aa ACs (VO or A_VI) resulted in a *loss* of throughput.[3] This is because of the limits imposed by the 802.11aa parameters which thwart traffic in these ACs to favor A_VO and VI, respectively. Therefore, any traffic remapping attack is more beneficial for the attacker when the VO or A_VI 802.11aa ACs are avoided. Finally, when no stations had saturated queues (Fig. 9c), the attack did not bring any gains until the network became congested ($n > 4$). We performed additional studies by varying $idleSlope$ but found that it impacts mostly the lower priority 802.11aa ACs, which should be avoided anyway. In summary, all the remapping attack variants brought gains proportional to their priority (with the exception of VO and A_VI).

C. idleSlope Manipulation Scenario

In the final scenario, all nodes sent A_VI traffic with $idleSlope = 1/n\%$ which has been shown to maximize the overall network performance and achieve fair throughput sharing [18]. We analyzed an attack based on manipulating the value of $idleSlope$ for a station sending A_VI traffic. Fig. 10 presents the throughput of the attacker and the normal stations for three different network sizes. As can be expected, the attacker's throughput is proportional to the value of $idleSlope$. This is most evident in the largest network (Fig. 10c), whereas for smaller network sizes there exist operation points where the throughput does not change for a certain range of $idleSlope$ values (e.g., 50% to 80% in Fig. 10a). This is a peculiarity of the operation of 802.11aa visible in small networks (similarly to the honest station's throughput oscillation for low $idleSlope$ values) caused by the synchronization of WCBSA with other transmissions. Nonetheless, based on these results, we conclude that it is beneficial for a single attacker to maximize the value of $idleSlope$. In the described scenario, primary traffic is not present so this form of attack is identical to downgrading. The situation is different when multiple stations perform this attack. Fig. 11 presents the per-station throughput gain for a varying number of attackers (each with a maximum possible setting of *idleSlope*) where the following observations can be made. A normal (honest) station's throughput degrades when the number of attackers increases while attacking always gives a station an increase in throughput (irrespective of the number of attackers). Therefore, using game-theoretic terminology, an operating point with all stations attacking is a Nash equilibrium. However, this Nash equilibrium is Pareto ineffective, because the stations achieve the highest throughput when none of them are attacking. We conclude that incentive mechanisms are required to ensure that all stations are honest.

[3] In fact, using BK resulted in a higher throughput than these two 802.11aa ACs (not shown in the figure). This leads to the conclusion that there may be cases for downgrading the traffic priority from VO or A_VI to BE or BK.

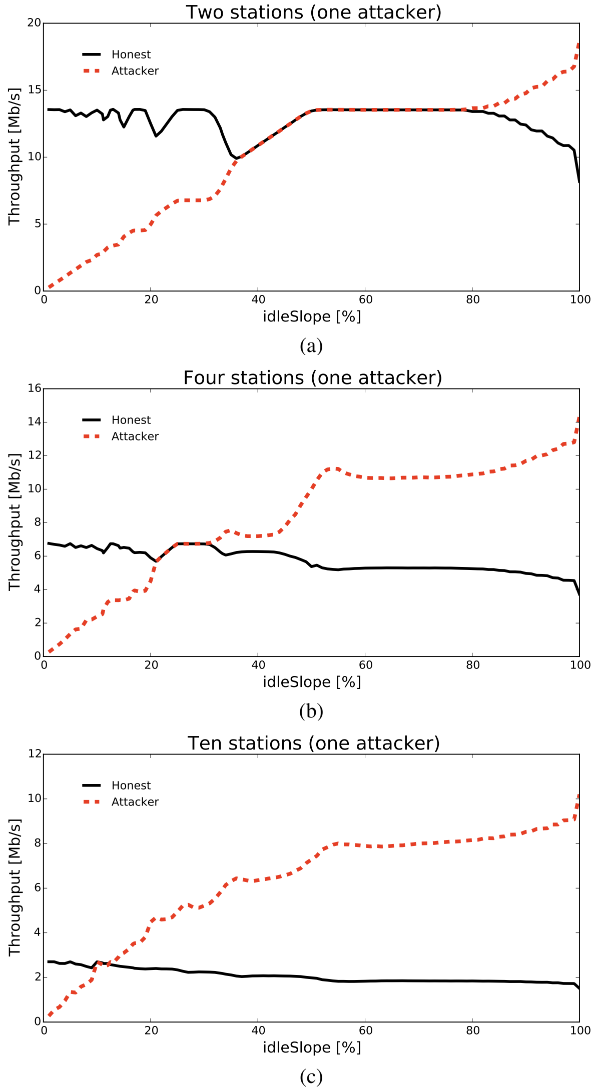


(a)

(b)

(c)

Fig. 9. Attacker's throughput in the traffic remapping attack scenario for three different network traffic conditions: (a) all stations have saturated queues, (b) only the attacker has a saturated queue, and (c) no stations have saturated queues. BE is the baseline for comparison (no cheating).



(a)

(b)

(c)

Fig. 10. Attacker's throughput in the *idleSlope* manipulation attack for three different network sizes: (a) two stations, (b) four stations, and (c) ten stations. In all cases there was only one attacker.

V. Attack Comparison

To compare the attacks, we use an attack tree (Fig. 12) – a method of security analysis described by Schneier in [20]. Each attack is subjectively rated by its execution cost c, risk of being detected r, potential QoS gain g, and the aggregated threat $t = \frac{g}{cr}$. The cost, risk, and gain are assessed on a scale of 1 to 3, with 1 being low and 3 being high.

The execution cost c is related to the attack's technical requirements. The traffic remapping attack ($c = 1$) requires only packet mangling software (such as Linux *iptables*), which may be independent of the wireless card driver. The other attacks require drivers that allow the configuration of selected parameters: either basic functionality disabling in the case of downgrading ($c = 2$) or internal parameter tuning in the case of *idleSlope* manipulation ($c = 3$).

The detection risk of an attack r depends on the required discovery method. Downgrading has the highest risk ($r = 3$) because the AP can easily detect that the station has disabled its 802.11aa functionality. Parameter manipulation attacks ($r = 2$) require a detailed watchdog mechanism coupled with statistical data analysis to determine a station's internal parameter. Finally, traffic remapping has the lowest risk ($r = 1$) because it requires traffic classification that consumes more time to be accurately detected.

The gain g is assessed in terms of the increase in QoS for the attacker. Gains are highly dependent on the network and traffic scenario but based on the outcomes of the simulation analysis we classify the attacks using the following reasoning. Both the downgrading and parameter manipulation attacks provide high throughput gains but are limited to cases where the attacker is sending traffic mapped to the secondary queues (VO or A_VI). Thus, for these attacks $g = 2$. However, the traffic remapping poses a threat regardless of the intrinsic traffic class of the attacker ($g = 3$).

To summarize, in terms of threat, the traffic remapping attack clearly has the highest score owing to its combination

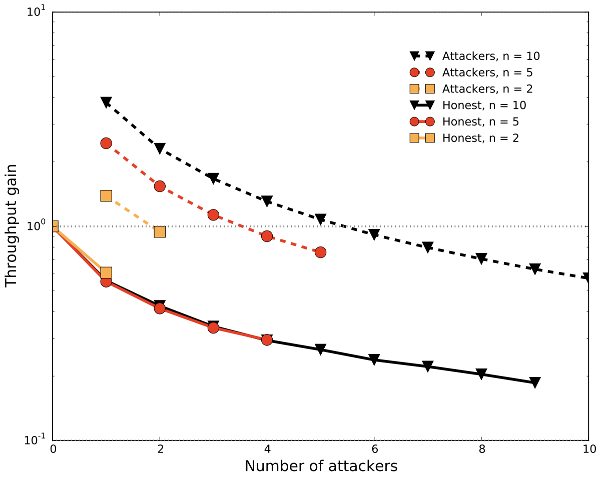


Fig. 11. Per-station throughput gain in the *idleSlope* manipulation attack for a varying number of cheating stations

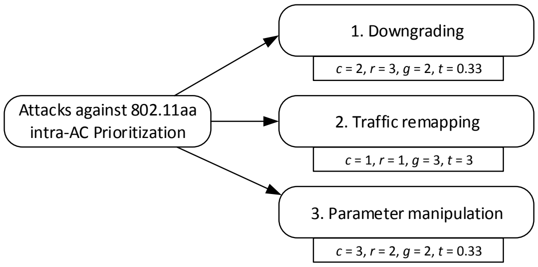

Attacks against 802.11aa intra-AC Prioritization
1. Downgrading
$c = 2, r = 3, g = 2, t = 0.33$
2. Traffic remapping
$c = 1, r = 1, g = 3, t = 3$
3. Parameter manipulation
$c = 3, r = 2, g = 2, t = 0.33$

Fig. 12. The attack tree for selfish attacks in 802.11aa networks using intra-AC prioritization

of low cost, low risk, and high gain. The other two attacks are a low threat mainly because they are limited to certain traffic scenarios.

VI. Conclusions, Countermeasures and Future Work

In this paper we have analyzed the impact of three categories of selfish insider attacks (downgrading, traffic remapping, and parameter manipulation) on 802.11aa networks. Traffic remapping has turned out to be the most beneficial for the attacker. Therefore, as future work we foresee investigating appropriate countermeasures to this type of attack in 802.11aa networks.

The most straightforward approach (in an infrastructure-based Wi-Fi network) would be to for the AP, having detected an attack (as described in Section V), to incentivize the attacker by shaping its incoming and outgoing traffic or even completely denying service to the offender. More elaborate approaches (especially for ad hoc settings) would require a game-theoretic analysis similar to [13].

An interesting observation can be made regarding the downgrading attack. Its occurrence can signify the presence of a legacy station which does not support 802.11aa intra-AC prioritization. Our results show that in this case overall network performance is decreased. Further research is required to determine optimum network configurations for scenarios with legacy stations.

Acknowledgments

This work has been carried out as part of a project financed by the Polish National Science Centre (decision no. DEC-2011/01/D/ST7/05166).

References

[1] "IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: MAC Enhancements for Robust Audio Video Streaming," *IEEE Std 802.11aa-2012*, pp. 1–162, 2012.

[2] "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, March 2012," 2012.

[3] K. Kosek-Szott, "A Throughput Model of IEEE 802.11aa Intra-Access Category Prioritization," *Wireless Personal Communications*, vol. 71, pp. 1075–1083, 2013.

[4] A. De La Oliva, P. Serrano, P. Salvador, and A. Banchs, "Performance evaluation of the IEEE 802.11aa multicast mechanisms for video streaming," in *Proc. of IEEE WoWMoM*, 2013.

[5] M. Santos, J. Villalon, and L. Orozco-Barbosa, "Evaluation of the IEEE 802.11aa group addressed service for robust audio-video streaming," in *IEEE International Conference on Communications (ICC)*, 2012.

[6] K. Kosek-Szott, M. Natkaniec, and L. Prasnal, "IEEE 802.11aa Intra-AC Prioritization–A New Method of Increasing the Granularity of Traffic Prioritization in WLANs," in *Proc. of IEEE ISCC 2014*, 2014.

[7] M. Raya, I. Aad, J. Hubaux, and A. El Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 1691–1705, 2006.

[8] G. Bianchi, A. Di Stefano, C. Giaconia, L. Scalia, G. Terrazzino, and I. Tinnirello, "Experimental assessment of the backoff behavior of commercial IEEE 802.11b network cards," in *Proc. of INFOCOM*, 2007.

[9] I. Tinnirello, G. Bianchi, P. Gallo, D. Garlisi, F. Giuliano, and F. Gringoli, "Wireless MAC processors: Programming MAC protocols on commodity Hardware," in *Proc. of IEEE INFOCOM*, 2012.

[10] S. Szott, J. Gozdecki, K. Kosek-Szott, K. Loziak, M. Natkaniec, and I. Tinnirello, "The risks of wifi flexibility: Enabling and detecting cheating," in *Proc. of Future Network and Mobile Summit*, 2013.

[11] S. Szott, M. Natkaniec, and A. R. Pach, "An IEEE 802.11 EDCA Model with Support for Analysing Networks with Misbehaving Nodes," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, p. 13, 2010.

[12] S. Szott, M. Natkaniec, and R. Canonico, "Detecting backoff misbehaviour in IEEE 802.11 EDCA," *European Transactions on Telecommunications*, vol. 22, pp. 31–34, 2011.

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

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

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

[16] K. Kosek-Szott, M. Natkaniec, S. Szott, A. Krasilov, A. Lyakhov, A. Safonov, and I. Tinnirello, "What's new for QoS in IEEE 802.11?" *Network, IEEE*, vol. 27, pp. 95–104, 2013.

[17] "IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks," *IEEE Std 802.1Q-2011*, pp. 1–1365, 2011.

[18] K. Kosek-Szott, M. Natkaniec, and L. Prasnal, "A Novel IEEE 802.11aa Intra-AC Prioritization Method for Video Transmissions," in *Proc. of IEEE GLOBECOM*, 2014.

[19] "Network simulator ns-3." [Online]. Available: http://www.nsnam.org/

[20] B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21–29, 1999.