COL-MOD: A New Module to Quantify the Weight of Damage Incurred by Collision Attacks

Mina Malekzadeh[1], Moghis Ashrostaghi[2]
(Corresponding author:Mina Malekzadeh)

Computer Department & Faculty of Electrical and Computer Engineering, Hakim Sabzevari University[1]
P. O. Box 379, Tohid Shahr, Sabzevar 9617916487, Iran
Computer Department & Mirdamad Institute of Higher Education, Gorgan, Iran[2]
(Email: corresponding_ m.malekzadeh@hsu.ac.ir)

(Received May 12, 2016; revised and accepted Sept. 3 & Oct. 3, 2016)

Abstract

The wireless technology is inherently susceptible to many types of attacks. There are few studies that have investigated the collision attacks. However, to the best of our knowledge, there is no prior work on investigating the consequences of the collision attacks on performance of the wireless networks. Hence, this work proposes a new module specifically for NS2 simulator which is capable of implementing and measuring the impact of the collision attacks on performance of the functional wireless networks. With the same conditions, we further design a testbed to measure the effectiveness of the collision attacks in real networks. Finally, in order to prove the accuracy of the proposed module, its results are compared with the results from the testbed. The purpose is to accurately determine the impact of the collision attacks which is essential for evaluation and testing the potential defense appliances against the attack. The results signify the extensive impact of the attack on disrupting the normal operation of the wireless networks.

Keywords: Collision attacks, NS2 module, wireless testbed, Ubuntu attacks

1 Introduction

Despite offering many benefits, wireless networks are exposed to many types of attacks including Collision attacks [3]. In collision attack, the attackers do not follow the rules implied in the Medium Access Control (MAC) protocol. Based on the MAC protocol, a collision occurs when two distinct transmissions happen simultaneously on the same media. When the packets collide, they are discarded and the retransmissions are required [1]. The attackers exploit the MAC protocol to launch the collision attacks. They deliberately induce collisions to the target media even by sending small packets [10]. Adversaries may only need to induce a collision in one octet of a transmission to disrupt the packet. Huge retransmission rate of the legitimate lost packets can severely slow down the victims normal operation and eventually render it unavailable for the intended users [12].

In this work, we provide an attempt to determine the severity and effectiveness of the collision attacks on IEEE802.11n MAC layer of the wireless networks. A new module called COL-MOD is created for NS2 tool to simulate a wireless network environment in which the collision attacks are implemented under different scenarios. Furthermore, a testbed is set up to implement the same attacks under the same scenarios against real wireless network. The purpose of the testbed is to validate the accuracy of the simulation results in term of how close the testbed results are to the simulation results.

The rest of the paper is organized as follows. Section 2 reviews the related researches. Section 3 describes both our proposed testbed setup and simulation environment. We present and analyze the experimental results in Section 4. We conclude this paper in Section 5.

2 Related Works

The Communications between the end users in wireless networks involve transmission of the signals through the open-air which exposes the wireless networks to a variety of attacks [11, 14] including collision attacks [2]. In [15] the authors attempt to detect some attacks including Jamming, exhaustion, and flooding. However, collision attacks are not considered. In [5] the authors consider two attacks called sinking behavior and collision behavior. However, they do not evaluate their findings in real world. Additionally, network topology, metrics, and types of attacks are the other parameters that differ from our work.

Impact of e-DoS attacks on energy consumption level of the targets is investigated in [13]. An energy model is designed to examine the impact of the attack on different layers of the protocol stack. However, the impact of collision attacks on performance of the wireless networks is not investigated. In [6], the authors use GloMoSim tool to simulate smurf attack which they consider as a type of DDoS attack. However, no testbed confirms the accuracy of the findings. The network security is also discussed in [4, 7, 8, 9].

Most of the previous studies show that the capacity of the DoS attacks seems endless to disable processing of the users requests. However, these studies only enable a limited investigation of the security policy problems associated with DoS attacks and cannot provide in-depth investigations in quantifying impact and severity of the collision attacks. Hence, as the primary contribution of this work, we build on these earlier approaches and extend them particularly by implementing the collision attacks against the IEEE 80.11n wireless networks. By modeling a simulation environment a testbed environment, the main motive is to precisely measure the damage created by the collision attacks and provide a careful comparison of the results from the simulation and the testbed experiments with different attack scenarios and system parameters. This will aid ISPs and network administrators in their evaluation and analysis of the effectiveness of the collision defenses applications.

3 Experimental Setup

In this section, we describe both our proposed simulation environment and testbed setup along with the tools that we have utilized to conduct the collision attacks against the IEEE802.11n wireless networks.

3.1 COL-MOD Module

In order to precisely determine the amount of damage produced by the collision attacks, we first need to quantify the baseline operation of the network which is referred to the network state at which there is no on-going attack. Therefore, by using NS2, we design a simulation environment.

In the baseline case, a wireless network topology with five legal nodes (numbered from 0 to 4), operates under normal conditions. Then we construct a new module and call it COL-MOD with different scalable capabilities to directly implement the collision attacks. We equip the attacker (node5) with the COL-MOD module to be capable of conducting the collision attacks against the target (node0 which also has the router functionality role). The simulation topology is shown in Figure 1.

The total simulation time is 60 seconds which is divided into three 20 seconds. The first 20 seconds (0-19s) is the normal duration at which the target wireless network operates normally. Then, the attacker launches the collision attacks for 20 seconds (20-39s). Finally, the last 20 seconds (40-60s) shows the network states after termination of the attacks. The DSDV routing protocol is used in the simulation environment to establish and maintain the route between the users.

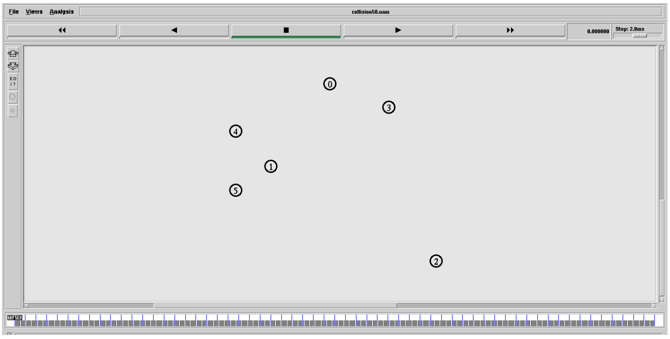

Figure 1: Simulation topology environment

3.2 Testbed Architecture

To achieve the same behavior and a level of control comparable to our simulation, we setup a wireless testbed with the exact same topology as our simulation environment. The network observation duration in the testbed, like the simulation, is 60 seconds. In our testbed, like the simulation, the node0 (which is also switched with a wireless access point during our experiments) is considered as the target of the attacker.

In order to start collision attacks, some preparations in terms of software and hardware are required. The list of software and hardware used in our testbed to conduct the collision attacks are described in Table 1.

3.3 Experiments Setting

The effectiveness of the collision attacks depends on different parameters. Thus, to determine how varying these parameters can influence the success rate of the attack, we take into account the following parameters.

- Legitimate traffics in the simulation experiments: this parameter describes the communication patterns in the target network. In our simulation, the legitimate traffics are created by a CBR UDP agent that continuously sends 500 bytes packets at regular 0.02s intervals. .

- Attack traffics in the simulation experiments: we can also call this feature as attack density or attack frequency. It describes the attributes of the malicious packets arriving at the victim. The goal is to determine the corresponding possible effects on the victim machines involved in the attack. In our simulation, the attack traffics are generated by a CBR agent that pulses three different packet sizes 50B, 100B, and 500B, at three different intervals, 0.05s, 0.02s, and 0.01s.

- Legitimate traffics in the testbed experiments: to achieve a fair comparison with the simulation envi-

Table 1: Preparations for the testbed

Tools	Name	Description
Software	Kali Linux with Builtin Metasploit framework and Nmap	Penetration tool that we use for packet crafting which is prerequisite for launching the collision attacks.
	Wireshark	Network analyzer to examine the network state before, during, and after the collision attacks.
	Operating system	Ubuntu Linux and Windows 7 with default security configurations are used as the OS of the nodes in the target network to examine if the type of OS has any role on survivability of the networks under the collision attacks.
Hardware	Wireless router	Linksys, Asus
	Wireless NIC	Netgear, Atheros chipsets
	CPU	Netgear, Intel; i7, dual core
	RAM	2GB, 4GB

ronment, the packets with the exact characteristics (500 bytes at 0.02s intervals) are transmitted into the testbed.

- Attack traffics in testbed experiments: to achieve the same behavior, the attacks are conducted in our testbed with the same specifications as our simulation. Therefore, three different packet sizes (50B, 100B, 500B), at three different packet intervals (0.05s, 0.02s, 0.01s) are generated and injected to the victim in our testbed.

Considering the combination of the above parameters, this research will generate different attack scenarios based on the following three key variables.

- Type of targets: two factors are aimed to select the victim of the collision attacks in our testbed to test their possible resilience to the attacks. These factors include OS of the target (either Windows or Linux) and role of the target machine (either a computer or access point).

- Security level of the targets: in the real world, different level of protection is provided for the systems and machines in the networks. Considering this fact, we implement the collision attacks in our testbed against the target with a pre-installed antivirus (brand remains unmentioned). Furthermore, we do these attack experiments against Windows-based machines with and without Windows Firewall (WF) configuration respectively. The experiments without WF validate the effectiveness of the collision attacks against this OS, and those with WF investigate the effectiveness of WF to provide a level of protection against these attacks.

- Attack rate: due to the attackers malicious intentions, they typically desire to remain anonymous. Therefore, the attackers generally conduct their attack in a low rate which has two advantages: (1) making it difficult to be detected and (2) consuming less resource of the attackers wireless equipments. Therefore, this work focuses on low rate collision attacks which are achieved by small attack packets size and rate. For this reason, we have set these parameters relatively low as mentioned above in the attack traffics features.

Finally, metrics including throughput, delay, and data lost rate are measured to show divergence during the collision attacks from the baseline case. Therefore, this research generates six distinct experiments as the attack scenarios based on the above parameters, key variables, and metrics. A description of each experiment for the simulation and testbed is summarized in Table 2 and Table 3 respectively.

Table 2: Simulation experiments designed to conduct collision attacks

Parameter	Description
Experiment numbers	Experiment 1 (Attack interval=0.05s)
	Experiment 3 (Attack interval=0.02s)
	Experiment 5 (Attack interval=0.01s)
Attack packet size	50,100,500B

Table 3: Testbed experiments designed to conduct collision attacks

Parameter	Description
Experiment numbers	Experiment 2 (Attack interval=0.05s)
	Experiment 4 (Attack interval=0.02s)
	Experiment 6 (Attack interval=0.01s)
Attack packet size	50,100,500B
Target OS	Windows 7 and Ubuntu 11
Target machine	PC and Access Point
Level of Security	with antivirus and with/without WF

4 Results and Analysis

In this section we present the simulation results and testbed results obtained from implementation of the six experiments.

4.1 Experiment-1

In this experiment, the COL-MOD module runs the collision attacks against the target wireless network in our simulation environment. The normal 500 bytes data enters the wireless network during the entire simulation time i.e. since the beginning of the simulation (0s) until the end (60s). Meanwhile, at the 20th second, the COL-MOD starts the collision attacks using 50,100,500 bytes as the Attack Packet Size (APS) at 0.05s intervals. The attack lasts for 20 seconds (20-39s). The time 40-60s represents the network state after the termination of the attacks. The simulation results of this experiment in terms of throughput, delay, and packet lost are presented in Figure 2.

As the above simulation results show, the consequence of the attack with very low rate (0.05s) is insignificant even with larger attack packets (500B). Comparing the effect of the three sizes of the attack packets on throughput imply relatively similar impact for the smaller packets (50 and 100B). In these cases, the attack does not have noticeable impact on the throughput but delay increases

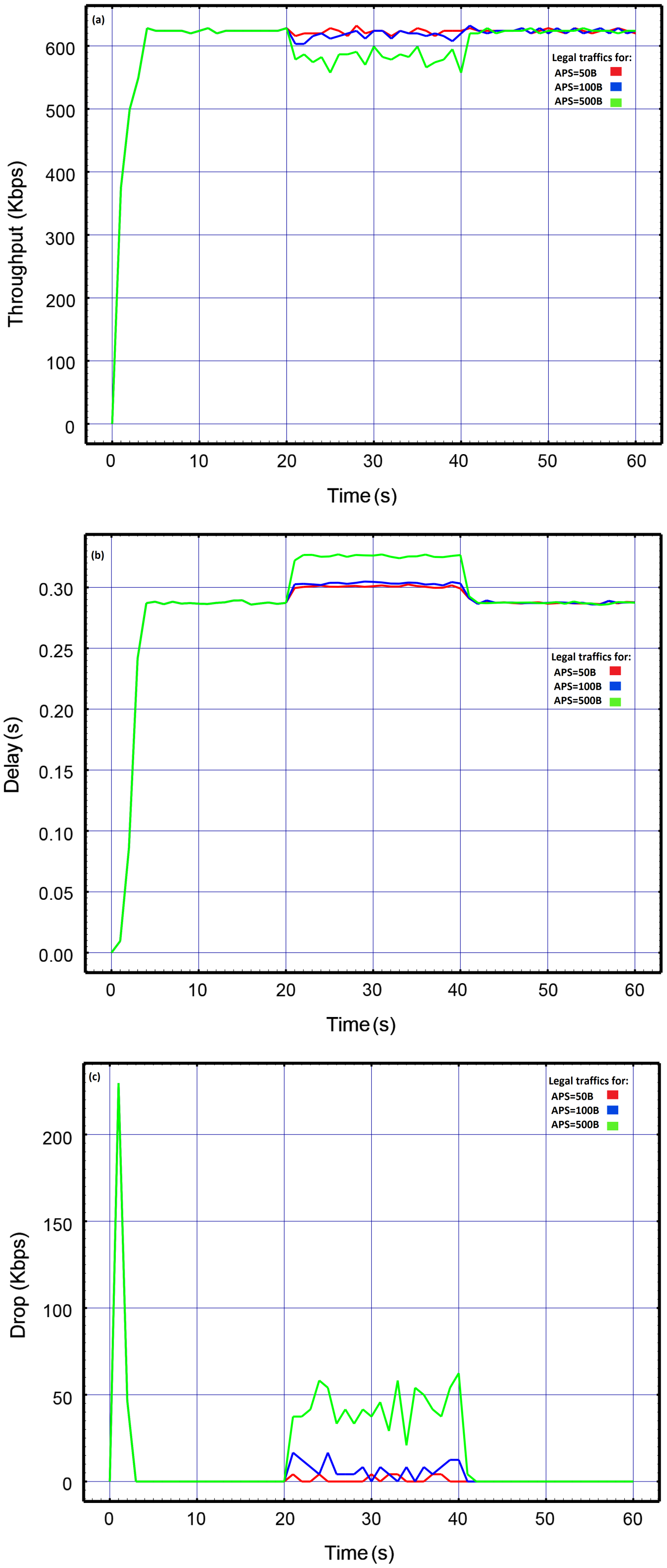

Figure 2: Simulation results: throughput, delay, packet lost

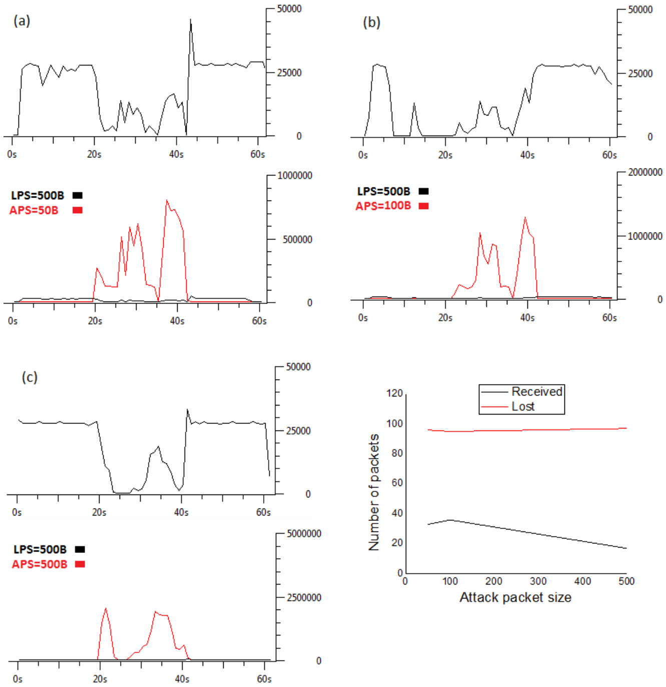

Figure 3: Testbed results on Windows target: throughput, packet lost

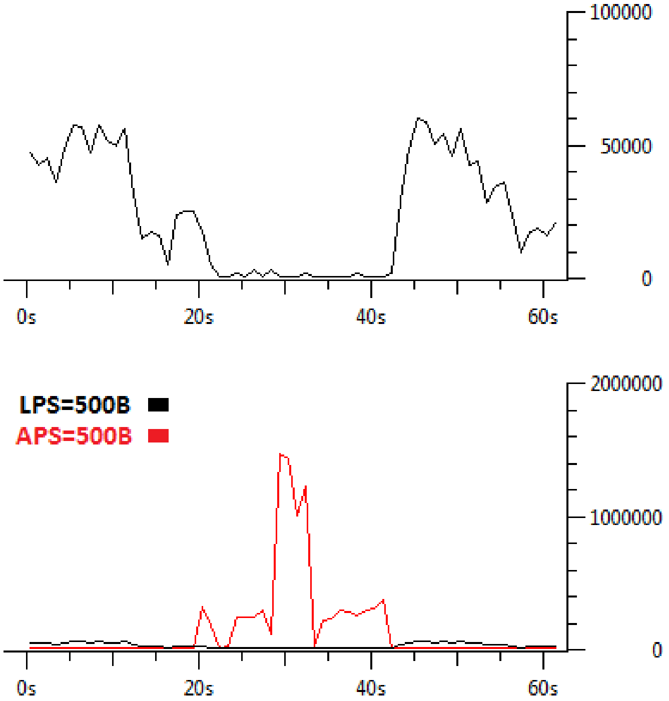

Figure 4: Testbed throughput with WF off

slightly. The sudden high peak in the lost packets graph is related to the transmission of the routing control packets by the DSDV protocol at the beginning of the route establishment. As it is depicted, the attack with 500B packets causes higher rate of the dropped packets than the smaller packets.

4.2 Experiment-2

In this experiment, the collision attacks run against the target wireless network in our testbed. The purpose is to measure the impact of the attacks in the real world to be compared against the simulation results obtained by COL-MOD from the Experiment1. The throughput results on the Windows-based victim machine with an installed and updated antivirus while the WF is enabled are provided in Figure 3.

The above results prove significant impact of the attack in the real world. Before the attack, normal data is transmitted steadily over the target network. However, as the attacks start at the 20th second, the attack packets collide with the normal traffics and the throughput fluctuates highly particularly by the 500 bytes attack packets. Although the network is highly affected by the attack, but after the attack (40-60s), the network is able to quickly recover from the attacks.

To determine whether the WF in active mode can provide any level of protection to prevent the collision attack in compare to when it is disabled, we repeat the above experiment with 500B attack packets and disabled WF. The results are provided in Figure 4.

After we disabled the WF, the results confirm vulnerability of the Winodws7-based machines to collision attacks regardless of presence or absence of the WF. In both cases the attack is completely destructive while when the WF is disabled there is a higher performance reduction. The results prove that even with small attack interval (0.05s), the attack packets collide with the legitimate packets and force them to drop. The null throughput during the attack signifies the great disturbance compelled by the attack to the wireless network to fully shut it down.

In order to investigate the impact of the same attacks on Linux-based machines, we conduct the above attacks over the target Ubuntu machine in our testbed. The throughput and packet lost results are provided in Figure 5.

The above results signify the high impact of the collision attack on Linux-based target even at a very low rate. As the results suggest, there is slight difference in term of the attack influence between the three sizes of the attack packets. Therefore, when targeting the Linux-based machines, the attackers even with very small 50B packets can interfere with the normal network transmissions and force them to drop. Comparing the above results with the results from targeting the Windows-based machines proves that without presence of the WF both OSs have comparable vulnerability to the collision attacks. However, enabling the WF makes the Windows-based machines to a small extent more resilience to the attacks with attributes tested in this experiment.

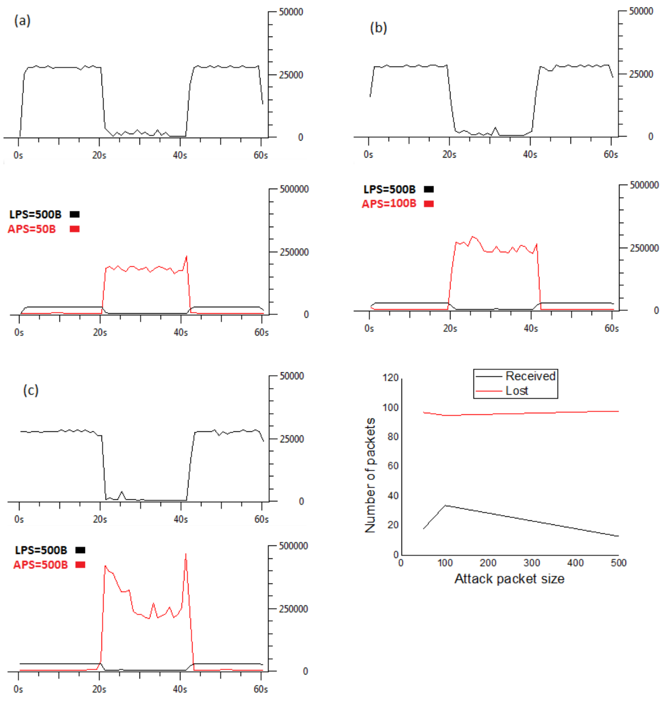

Figure 5: Testbed results on Linux target: throughput, packet lost

4.3 Experiment-3

In this experiment the COL-MOD runs the collision attack, with the corresponding details listed in Table2, against the target wireless network in our simulation environment. The simulation results in terms of throughput, delay, and packet lost rate are presented in Figure 6.

In the above simulation results, throughput falls from 610Kbps down to 490Kbps while the legitimate packets experience higher delay during the entire attack time. As mentioned, the steep rise at the beginning of the simulation in the packet lost graph is corresponding to the DSDV control packets to establish the route. The number of lost packets fluctuates significantly from zero before the attack to about 130Kbps during the attack which points out the effectiveness of the attack.

4.4 Experiment-4

Based on the corresponding attributes listed in Table3, this experiment makes an attempt to run the collision attacks against the target wireless network in our testbed. The throughput and packet lost results on Windows-based target machine with an installed and updated antivirus while the WF is enabled are provided in Figure 7.

The above outcomes prove the collision attacks can substantially disrupt the normal operation of the targets. The reason is related to vulnerabilities in TCP/IP processing. Therefore, even though victims are protected with high level of security, the attacks impact is significant. We observed that the attacks slow down the legiti-

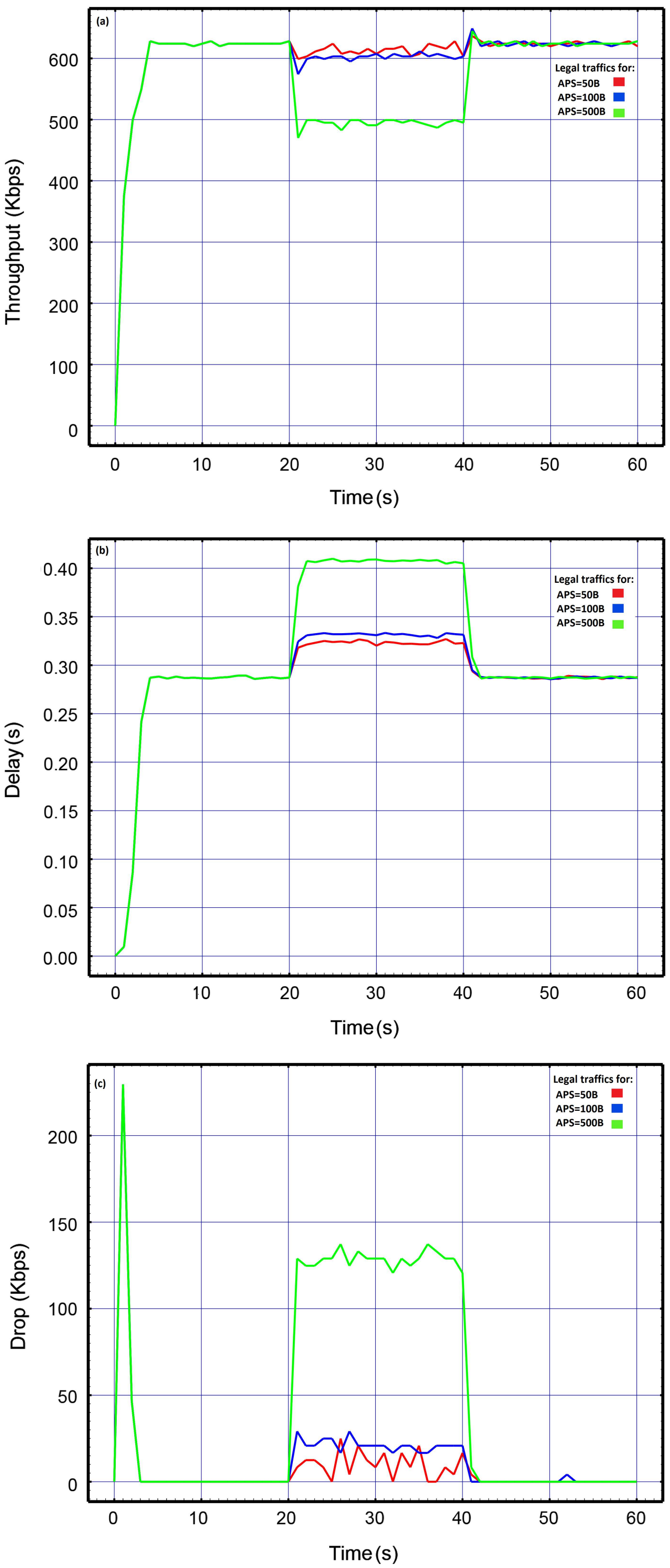

Figure 6: Simulation results: throughput, delay, packet lost

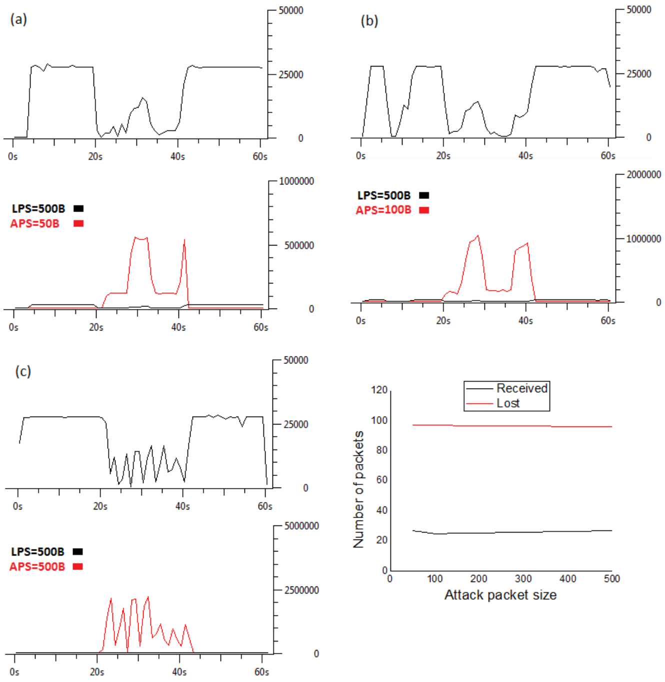

Figure 7: Testbed results on Windows target: throughput, packet lost

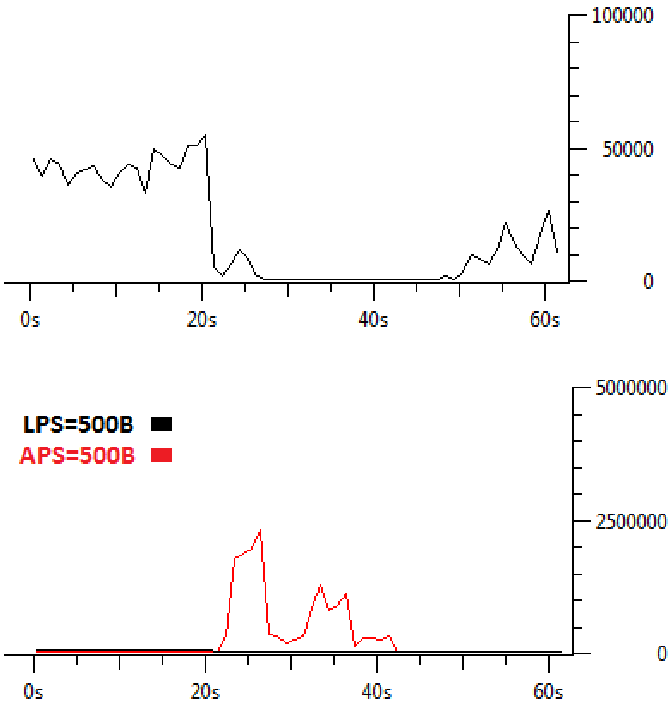

Figure 8: Testbed throughput with WF off

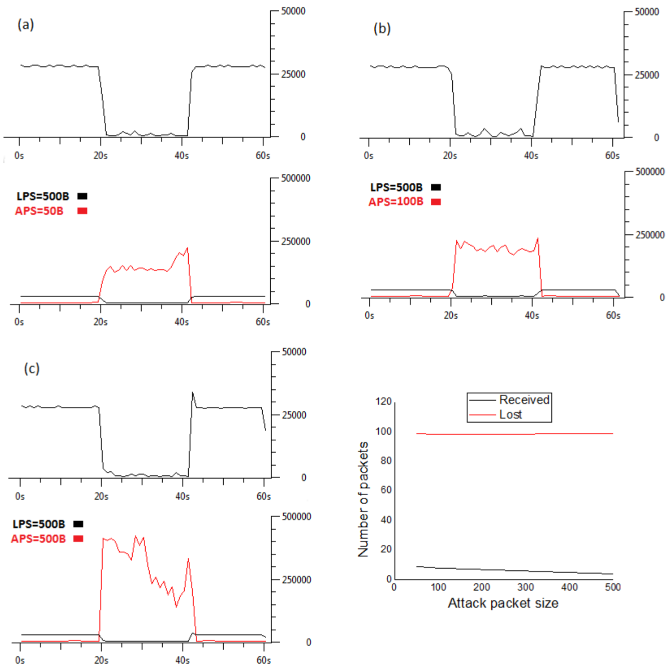

Figure 9: Testbed results on Linux target: throughput, packet lost

mate transmission rate so that even doing a simple task, for instance opening a webpage, was not possible. However, the target network was able to accomplish a fast recovery after the attacks.

In order to determine whether the WF had any effect on these results, we turned the WF off and repeated the above experiment for 500B attack packets. The results are presented in Figure 8.

The above results imply that disabling the WF can thoroughly open the network for penetration of the intruders. The null throughput during the attack reveals the significance of the attack. Using WF does not necessarily nullify the attack, but it has slight effect to reduce the impact.

Severely reduction of the throughput during the attack against the Windows-based machines motives our intention to test the same attack against the Linux-based target. The results of the attack against the Ubuntu target machine are presented in Figure 9.

The above outcomes provide evidence that the attack is quite successful against the target. We observed that, although the Ubuntu machine was not completely disconnected from the network, it was extremely slow to a level that from a practical point of view it was quite inaccessible for the intended users.

4.5 Experiment-5

In this experiment, the COL-MOD runs the collision attacks against the target wireless network in our simulation environment. The rate of the attack rises to a higher value (0.01s) than the previous experiments to examine any possible effects on the targets. The simulation results of this experiment in terms of throughput, delay, and packet lost rate are presented in Figure 10.

The above outcomes illustrate that in the simulation environment there is a direct relation between the attack rate and size of the attack packets on the impact of the attacks. As the attack rate grows to 0.01s, the network performance degrades severely in terms of lower throughput and higher delay and packet lost. Based on the results, the target suffers from a remarkable poor activity when the 500B attack packets are headed toward it.

4.6 Experiment-6

We run this experiment against the target in our testbed to determine the impact of 0.01s intervals between the attack packets on the performance of the target. The throughput and packet lost results on the Windows-based target with an installed and updated antivirus while the WF is enabled are provided in Figure 11.

The above results also confirm the significant impact of the collision attack on degrading the performance of the wireless networks even when protected by firewall and high level of security. At the beginning of the attack, the windows-based target can manage the collisions and the corresponding retransmissions. However, eventually the large numbers of retransmission of the legitimate packets that collide with the forgery packets consume the limited resources of the target which result in a remarkable performance reduction.

In order to see how disabling the WF varies the effect of the attack, we repeated the above attack against the Windows target machine with WF off in our testbed. The results for 500B attack packets are presented in Figure 12.

As we expected from our previous testbed experiments, disabling the WF exposes the network to the attackers. Null throughput during this experiment represents a 100% success rate for the attack.

The above experiment is repeated in order to determine the impact of the attack on Linux-based machines. The throughput and packet lost results are provided in Figure 13.

The above findings also reveal that the Ubuntu machine is fully vulnerable to the attack regardless of the size of the attack packets.

In order to complete our work, we repeated all the above testbed experiments against the wireless access point as the target to see whether it causes any changes on the impact of the attacks. The attacks results on the testbed reveal the same destructive impact on the overall performance of the wireless network.

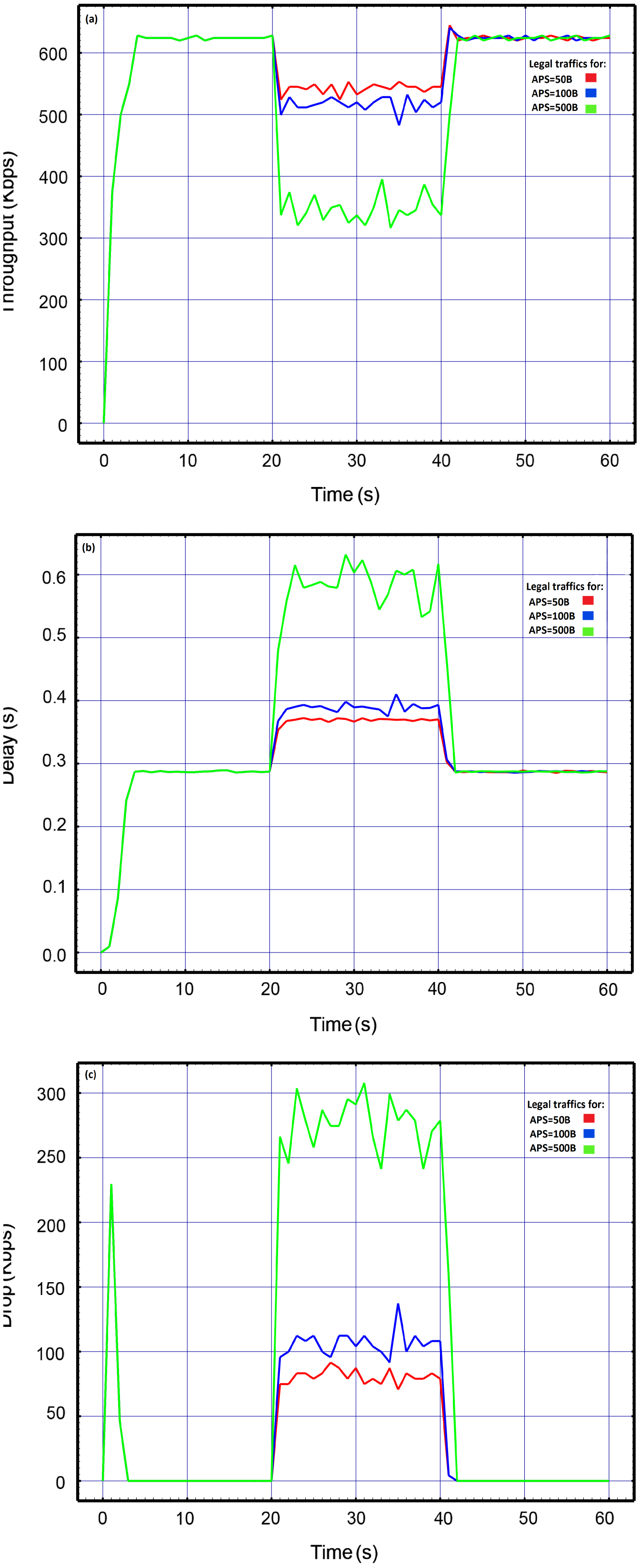

Figure 10: Simulation results: throughput, delay, packet lost

5 Conclusions

By comparing the testbed and COL-MOD results against each other we can find some differences for the collision at-

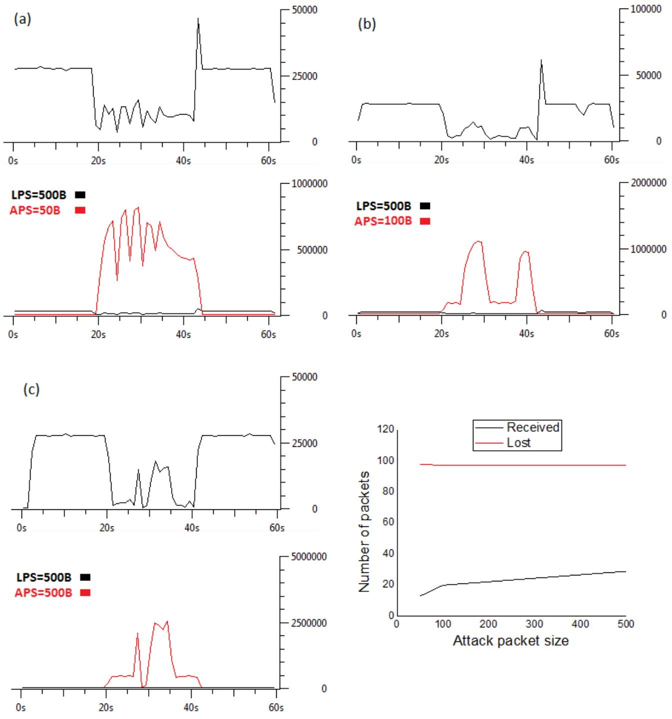

Figure 11: Testbed results on Windows target: throughput, packet lost

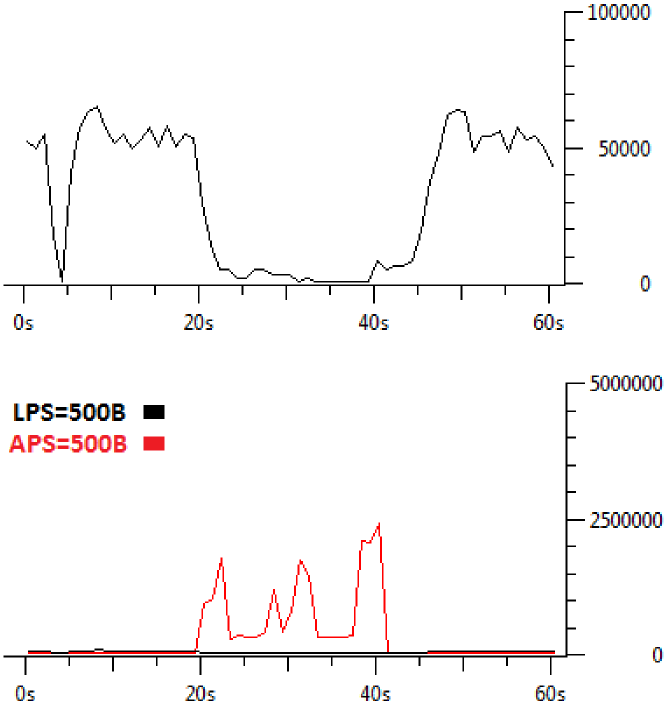

Figure 12: Testbed throughput with WF off

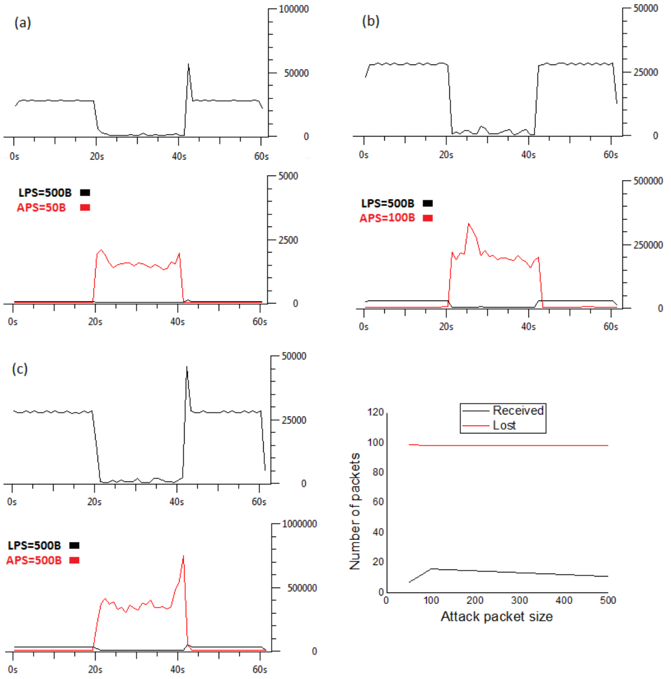

Figure 13: Testbed results on Linux target: throughput, packet lost

tacks. The testbed results show that all the attacks with attributes specified in this work are successful. Based on these results, all the attacks in the real world cause great disturbance and slow down or stop the normal operation of the target network. The collision attacks against the Windows-based machines with enabled WF cause to dramatically slow down the network. Moreover, the collision attacks against either the Linux-based machines or Windows-based machines with disabled WF were fully capable of rendering the targets shut down. The network behavior was relatively the same for all the attacks against the testbed.

In contrast, the COL-MOD module simulation results of the same attacks under the exact same conditions show a different behavior in some scenarios. For example, growing the attacks rate or size has a direct impact on significance of the attacks. We believe this difference between the testbed and simulation results is because the impact of a given attack on a real target network further depends on various network characteristics including its traffic and resources which are not precisely taken into account by the simulation tools.

References

[1] M. R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor network," *International Journal of World Academy Of Science, Engineering And Technology*, vol. 6, no. 2, pp. 427–430, 2012.

[2] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 68–72, 2016.

[3] H. C. Chaudhari and L. U. Kadam, "Wireless sensor networks: Security, attacks and challenges," *International Journal of Networking*, vol. 1, no. 1, pp. 4–16, 2011.

[4] J. Han, "Fingerprint authentication schemesfor mobile devices," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 3, pp. 579–585, 2015.

[5] S. Hemalatha, P. C. S. Mahesh, P. Rodrigues, and M. Raveendiran, "Analysing cross layer performance based on sinking and collision behaviour attack in manet," in *International Conference on Radar, Communication and Computing*, pp. 77–82, 2012.

[6] M. Kumar and N. Kumar, "Detection and prevention of ddos attack in manets using disable ip broadcast technique," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 7, pp. 29–36, 2013.

[7] P. H. Latha and R. Vasantha, "Mds-wlan: Maximal data security in wlan for resisting potential threats," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 4, pp. 859–868, 2015.

[8] N. Mohd, S. Annapurna, and H. S. Bhadauria, "Taxonomy on security attacks on self configurable networks," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 44–52, 2015.

[9] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[10] P. Reindl, K. Nygard, and X. Du, "Defending malicious collision attacks in wireless sensor networks," in *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, pp. 771–776, 2010.

[11] D. Subhadrabandhu, S. Sarkar, and F. Anjum, "Efficacy of misuse detection in adhoc networks," in *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON'04)*, pp. 1–11, 2004.

[12] M. N. Sudha and M. L. Valarmathi, "Minimization of collision in energy constrained wireless sensor network," *International Journal of Wireless Sensor Network*, vol. 1, pp. 350–357, 2009.

[13] W. West and E. Agu, "Experimental evaluation of energy-based denial-of service attacks in wireless networks," *International Journal of Computer Science and Network Security*, vol. 7, no. 6, pp. 222–236, 2007.

[14] A. D. Wood and J. A. Stankovic, *A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks, Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press LLC, 2005.

[15] O. Xi and X. Yang, "A novel framework of defense system against dos attacks in wireless sensor networks," in *IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'11)*, pp. 1–5, 2011.

Biography

Mina Malekzadeh is an assistant professor and lecturer in the department of computer science at Hakim Sabzevari University. Her research interests include communication networks, network security, VoIP, and system development programming. She holds a Doctoral degree in computer security from UPM, MSc in software engineering from UPM, BSc in computer engineering from SBU.

Moghis Ashrostaghi received the B.S. degree in Computer Science from Golestan University. He is currently a master student. His research interests are Computer Networks and wireless security.