Conference on Recent Research in Science and Technology
همایش پژوهش های نوین در علوم و فناوری

# An Experimental Framework for Vulnerability Analysis of 802.11 Wireless Networks

**Mina Malekzadeh**
*Computer Dept. of Electrical and Computer Engineering Faculty, Hakim Sabzevari University, Sabzevar 9617976487, Iran*
*m.malekzadeh@hsu.ac.ir*

## Abstract

In recent years, wireless LAN (WLAN) has gained popularity in a variety of locations. This has led to development of high level security protocols for WLAN. The newest protocol IEEE 802.11i ratified to provide strong data encryption but it cannot prevent Denial of Service (DoS) attacks on WLAN. This work in a Linux-based testbed, conducts an experimental framework to implement and quantify common types of DoS attacks against WLAN throughput. The results from implementation of the experiments in the framework show that how easily DoS attacks can be performed on WLAN which causes to reduce throughput of communication considerably to make inaccessible wireless connection for its authorized members.

**Keywords:** DoS attack, wireless network, network security, management frame, IEEE 802.11

## 1. Introduction

Cheap price of wireless devices and being easy to install, make wireless networks more popular and widely deployed. Different security protocols were proposed and implemented over WLAN to make it more reliable [1]. The latest protocol, IEEE 802.11i (WPA2) [5, 6, 8, 9, 12, 13, 14], provides strong data encryption by using advanced encryption standard (AES) [11] algorithm. It also provides a high level data integrity by using IEEE 802.1x [10] protocol. Therefore, IEEE 802.11i can address most issues on data security over WLAN however this protocol does not protect WLAN against DoS attacks [١٣ ,٧ ,٤ ,٢ ,١].

Major DoS attacks on WLAN arise from management frames vulnerabilities which are not protected by 802.11i protocol [2, 7]. Hence these frames can be used by any attacker to launch different types of DoS attacks. Major DoS attacks on WLANs include authentication request flooding (AuthRF), association request flooding (AssRF), deauthentication flooding (DeauthF) and disassociation flooding [1, 4, 13]. These DoS attacks cause the WLAN or some of its wireless nodes out of services.

In this paper we implement a variety of common DoS attacks in a tested WLAN, which is using IEEE 802.11i security protocol to demonstrate existing vulnerability of the protocol. Then by an experimental framework we quantify the effect of DoS attacks on WLAN throughput.

The remaining sections of this work are organized as follows. Section 2 details the most common DoS attacks over the WLANs. In section 3 we present our experimental design to implement the DoS attacks over WLAN along the performance metrics. Section 4 discusses the results of the experiments. Conclusions are provided at section 5.

## 2. Related works

Some management frames exchanges between Access Point (AP) and stations to make a physical connection [1]. These frames are not protected by any of the current wireless security protocols. Therefore, an attacker by using these frames can start a variety of DoS attacks. In this paper we investigate the most common DoS attacks over wireless network as DeauthF, AuthRF, and AssRF attacks. In DeauthF attack [3], intruder sends continually forgery deauthentication frames to its victim to make it unavailable for the other legal clients of the WLAN. Since deauthentication is a notification, the victim can not ignore it and it has to implement its function and be disconnected from the network. This attack can be done even worse when the attacker chooses the AP as its victim. In this case all legal clients are disconnected and the whole network becomes unavailable.

In AuthRF attack [3], when the legitimate AP receives the authentication request with a faked source MAC address, it sends out an authentication response to the faked wireless client. Since the faked wireless client does not exist, the AP cannot receive the acknowledgement frame for the transmitted authentication response frame. The AP keeps sending out several authentication response frames which overload the WLAN since to process these authentication requests consumes a great deal of the AP's resources. As a result, the AP has little resource to serve the other clients, and these wireless clients may either suffer poor communications or lose the communication completely.

In AssRF attack [3], when the AP receives an association request with a faked source MAC address, it checks its buffer and finds that the faked wireless client does not exist in its authenticated state table. It then sends out the deauthentication frame to the faked wireless client. Since there is no acknowledgement from the faked wireless client, it keeps sending out several deauthentication frames. For AssRF DoS attacks, the victim AP always keeps checking buffers and sending multiple response messages for each received association request. It has no time or resources to serve other wireless clients. This forces the associated wireless clients to slow down or even stop their data communications.

## 3. Experimental Test Setup

We implemented our experiment in presence of all current security protocols such as WEP, WPA, and WPA2. The results of our experiment show that none of these protocols can prevent the mentioned DoS attacks. To quantify the impact of DoS attacks on wireless network throughput, we choose the strongest security protocol of 802.11i (WPA2) to protect the tested WLAN in our experiment. The tested WLAN includes a Linksys wireless router *WRT54G* as a base station. Three legal stations *sta1, sta2,* and *sta3* are equipped with IEEE 802.11 g Intel chipset wireless adapter and they are running on *Windows XP* with *service pack2*. A station is used as a sniffer to capture all frames transferred over the tested WLAN. A traffic analyzer is installed on this sniffer station to analyze the captured frames. It uses *Wireshark* application as a sniffing tool to trace attacker path. Both sniffer client and attacker client are equipped with IEEE 802.11 g *Atheros* chipset *AR5212* wireless adapter and they are running on *Ubuntu gusty 7.10*. The attacker client is using *aircrack-ng* application as DoS attacking tool. All the clients and wireless router support 802.1x user authentication. To conduct our research, we consider

three common types of attacks on wireless networks as DeauthF, AuthRF, and AssRF. By implementing three experiments, we quantify the throughput of the tested WLAN to evaluate the impact of these attacks on wireless networks.

### 3.1 Performance Metrics

When an attacker launches his desired DoS attacks in different possible forms, he tries to flood the wireless network by illegitimate traffics. Hence other legitimate users at a low rate of speed can transmit their valid information if it is not impossible. In this case throughput considerably decreases for these legal users since throughput is total bytes received at receiver per second. Therefore, to show the impact of the tested attacks, this research considers investigating wireless network throughput in two states:

- Throughput measuring before the attacks
- Throughput measuring during the attacks

We use these two metrics to compare wireless network throughput in case of the attacks. In the entire of this paper, we consider throughput as total byte receive at receiver side per time.

## 4. Experimental Results

This section illustrates operation of throughput measurement for the three mentioned DoS attacks. In all attacks, the metric is considered as total bytes received at receiver per second. In our experiment we consider the attacker chooses *sta1* as its victim. The sniffer computer keeps tracks of the any attacks to obtain the results of the experiments.

### 4.1 Throughput Measuring for DeauthF Attack

We conducted this experiment to demonstrate the impact of DeauthF attack on throughput of the tested WLAN. In this experiment the attacker client continually floods the victim (*sta1*) with the 100 forgery deauthentication frames per seconds to keep Sta1 disconnected from the WLAN. We keep the track of these forgery frames by our sniffer client to investigate any difference in throughput of either the victim or other legal clients (*sta2, sta3*) in the WLAN. The sniffer shows that immediately after reception of the first forgery deauthentication frame in 62 seconds, the victim is disconnected from the WLAN and cannot transmit any information until the end of the attack in 100 seconds. Attack duration in this experiment is about 38 seconds which brings the network throughput to zero for the victim.

This experiment measures number of packets transmitted by either legitimate client of the tested WLAN or the attacker before and during DeauthF attack along the corresponding times. The results of the experiment are shown in Table 1.

Table 1: Results of DeauthF Attack over the Tested WLAN

| | Total No of Packets | Total Experiment Duration (s) | Avg. Load (bytes/s) | Bytes | Before Attack | | | During Attack | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | No of Data Packets | Bytes | Time (s) | No of Data Packets | Bytes | Time (s) |
| Network | 39478 | 147.460 | 45479.977 | 6706490 | 1077 | 789835 | 63.075 | 0 | 0 | 37.988 |
| Attacker | 3638 | 37.988 | 16280.255 | 618460 | 0 | 0 | 63.075 | 3638 | 618460 | 37.988 |

Therefore, from the above table we conclude that:
Throughput measuring before the attack=789835/63.075=12522.15616 B/s
Throughput measuring during the attack=0/37.988=0 B/s
The results of throughput performance are shown in Figure 1 in three states: before, during, and after DeauthF attack over the tested WLAN.

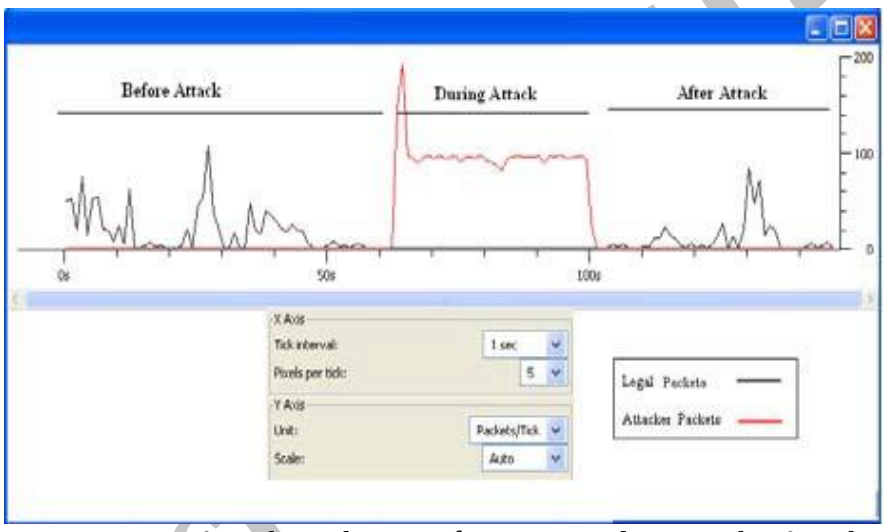

Figure 1: WLAN Throughput Performance under DeauthF Attack

As the above figure shows, before and after attack the victim exchanges information as normal. Attacker starts his attack in 62nd second and keeps doing his attack for about 38 seconds until 100th second. During these 38 seconds, there is no any data transmission by the victim because it has been disconnected from the WLAN by the attacker therefore the throughput for the victim is zero. The graph shows that the only transmitter is the attacker device which occupies the whole of WLAN bandwidth with his forgery deauthentication frames and does not let the victim uses its legal bandwidth.

4.2 Throughput Measuring for AuthRF Attack

In this experiment we demonstrate the impact of AuthRF attack on throughput of the tested WLAN. The attacker device continually sends out the authentication request frames to the victim (sta1). The attacker after sending these types of forgery frames expects to receive authentication response frames from the wireless router which means successful authentication to the sta1. Our sniffer device traces these forgery frames. This experiment measures number of packets transmitted by either legitimate clients of the tested WLAN or the attacker before and during AuthRF attack along the corresponding times. The results of the experiment are shown in Table 2.

Table 2: Results of AuthRF Attack over the Tested WLAN

| | Total No of Packets | Total Experiment Duration (s) | Avg. Load (bytes/s) | Bytes | Before Attack | | | During Attack | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | No of Data Packets | Bytes | Time (s) | No of Data Packets | Bytes | Time (s) |
| Network | 126444 | 190.554 | 129306.123 | 15717886 | 2380 | 2191940 | 115.302 | 76 | 12768 | 39.319 |
| Attacker | 15927 | 39.319 | 76303.766 | 2771298 | 0 | 0 | 0 | 15927 | 618480 | 36.319 |

Therefore, from the above table we conclude that:
Throughput measuring before the attack=2191940/66.302=33059.9 B/s
Throughput measuring during the attack=12768/36.319=351.55 B/s
The results of throughput performance are shown in Figure 2 in three states: before, during, and after AuthRF attack over the tested WLAN.

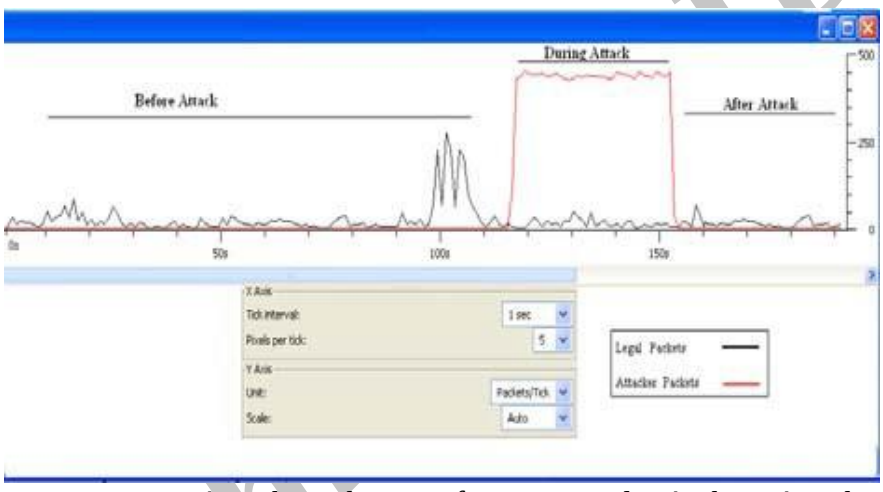

Figure 2: WLAN Throughput Performance under AuthRF Attack

As the above figure shows, before and after attack the wireless network is as normal. In the attack duration which started from about 115th seconds until 154th seconds, there are a few number of legal packet transmissions against the huge amount of the forgery packets of the attacker. The victim has a very small throughput during these 39 seconds attack. This is because the attacker consumes the most resources of the wireless router and the router is completely busy to response to the attacker forgery frames. Therefore, during the attack, the network is very slow for either the victim or the other legal members.

4.3 Throughput Measuring for AssRF Attack

We conducted this experiment to demonstrate the impact of AssRF attack on throughput of the tested WLAN. In this experiment the attacker client continually floods the victim (sta1) with the forgery association request frames to keep the wireless router busy to response to these forgery frames which means bandwidth consuming. In this experiment our sniffer keeps track of the huge number of the transmitted deauthentication frames form the wireless router to the attacker client. This experiment measures number of packets transmitted by either legitimate clients of the tested WLAN or the attacker before and during AssRF attack along the corresponding times. The results of the experiment are shown in Table 3.

Table 3: Results of AssRF Attack over the Tested WLAN

| | Total No of Packets | Total Experiment Duration (s) | Avg. Load (bytes/s) | Bytes | Before Attack | | | During Attack | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | No of Data Packets | Bytes | Time (s) | No of Data Packets | Bytes | Time (s) |
| Network | 132038 | 58.851 | 2374539.433 | 13974812 | 283 | 219393 | 16.029 | 7 | 5293.5 | 9.477 |
| Attacker | 500 | 9.477 | 41785.8 | 103500 | 0 | 0 | 0 | 500 | 103500 | 2.477 |

Therefore, from the above table we conclude that:
Throughput measuring before the attack=219393/22.029=9959.28 B/s
Throughput measuring during the attack=5293.5/2.477=2136.45 B/s
The results of throughput performance are shown in Figure 3 in three states: before, during, and after AssRF attack.

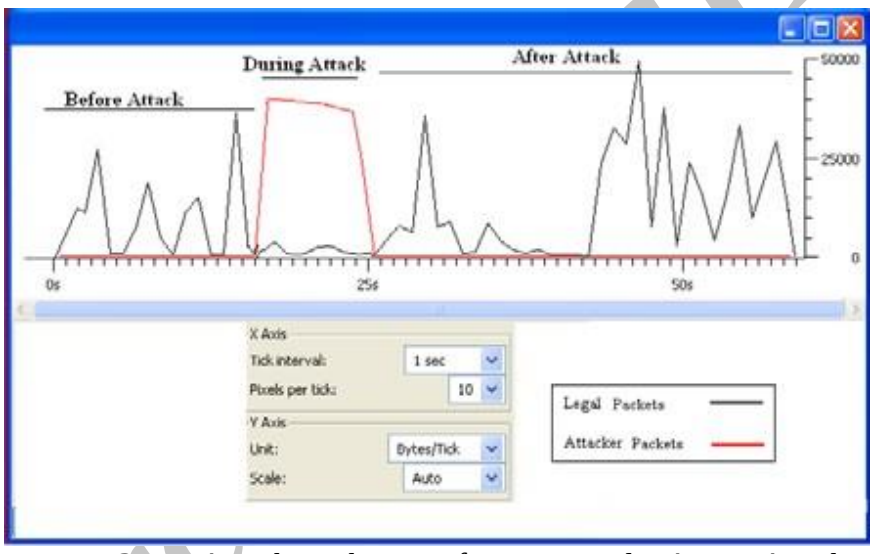

Figure 3: WLAN Throughput Performance under AssRF Attack

As the above figure shows, the wireless network is acting normal before and after attack. Unlike DeauthF attack we have a small numbers of legal packets during the AssRF attack which shows the legal user is not completely disconnected but has a very small throughput because of the huge amount of forgery packets of the attacker. The attacker starts his attack in 16th seconds and ends it in 25th second. During the 9 seconds attack duration, the attacker consumes the network bandwidth with forgery association request so that communication is very slow for the clients of the WLAN.

Figure 4 summarizes and compares the amount of throughput for all the implemented DeauthF, AuthRF, and AssRF attacks.

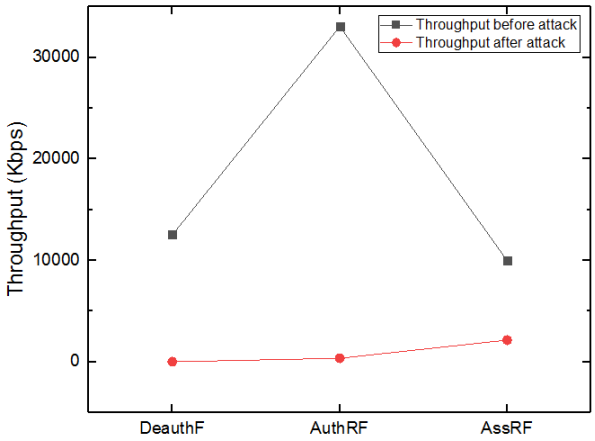

Figure 4: Compare the Throughput for the Tested DoS Attacks

Form the above figure we can see that DeauthF attack is the most serious attack against wireless network throughput than the AuthRF and AssRF. This is because DeauthF attack can completely break down the wireless network to make a zero throughput for the victim so that legal users cannot use the network at all. Regarding to the above graph, during AuthRF and AssRF attacks unlike DeauthF attack, users can access to network but very slowly and bandwidth decreases so that legal transmission is a painful process. The graph shows that AuthRF has more impact on the wireless network than AssRF attack. In AuthRF attack duration, the throughput is lower than AssRF attack and this is because the victim needs to exchange more frames to start over its communication.

## 5. Conclusion

IEEE 802.11i security protocol was ratified to make wireless networks more secure. But even in presence of this protocol, wireless networks still vulnerable to DoS attacks. Attackers can easily use unprotected management frames to implement different types of attacks as all the above graphs, and tables show this vulnerability. In this work, we implement three common DoS attacks against IEEE 802.11 WLANs. We demonstrate the impact of DeauthF, AuthRF, and AssRF DoS attacks on throughput of a tested WLAN in presence of 802.11i protocol. From the outcomes of the experiments it is concluded that DoS attacks are serious security problem over the wireless networks throughput. The results show that these DoS attacks can consume the wireless network resources so that the remainder of the throughput (zero for DeauthF and very small for AuthRF and AssRF) is not enough to continue legal communication for the network members at all.

References

[1] IEEE Computer Society LAN MAN Standards Committee. 1999. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications in IEEE Std 802.11.

[2] Malekzadeh M. et al. 2007. Security Improvement for Management Frames in IEEE 802.11 Wireless Networks. International Journal of Computer Science and Network Security, VOL.7 No.6.

[3] Bellardo J. and Savage S. 2003. 802.11 Denials-of- Service Attacks: Real Vulnerabilities and Practical Solutions. Proceedings of the USENIX Security Symposium.

[4] Liu C. 2005. 802.11 Disassociation Denial of Service (DoS) attacks. School of CTI DePaul University.

[5] IEEE Standard 802. 11i.2004.Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements.

[6] Sithirasenan E., Muthukkumarasamy V., and Powell D. 2005. IEEE 802.11i WLAN Security Protocol - A Software Engineer's Model. Proceedings of the 4th Asia Pacific Information Technology Security Conference. pp. 39–50.
[7] He C. and Mitchell J. C. 2005. Security Analysis and Improvements for IEEE 802.11i. Proceedings of the 12th Annual Network and Distributed System Security Symposium.
[8] IEEE 802.11i. 2004. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
[9] Edney J., Arbaugh W. 2003. Real 802.11 Security: Wi- Fi Protected Access and 802.1li.
[10] IEEE Standard 802.1X.2001. IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control.
[11] Announcing the advanced encryption standard (AES). 2001. Federal Information Processing Standards Publication.
[12] Walker J. 2005.IEEE 802.11i Standard Improves Wireless LAN Security.
[13] Sithirasenan1 E., and Muthukkumarasamy. 2005. Detecting Security Threats in Wireless LANs Using Timing and Behavioral Anomalies.
[14] Arana P. 2006. Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2).