A Solution to WLAN Authentication and Association DoS Attacks

Chibiao Liu, and James Yu, *Member, IEEE*

***Abstract*--The growing popularity of the 802.11-based Wireless LAN (WLAN) also increases its risk of security attacks. The new WLAN security standard, 802.11i, addresses most issues on user authentication and data encryption; however, it does not protect WLANs against Denial of Service (DoS) attacks. This paper presents a solution to detect and resolve authentication request flooding (AuthRF) and association request flooding (AssRF). We developed an experimental framework to demonstrate and quantify AuthRF and AssRF attacks against TCP and wireless Voice over IP (WVoIP) communications. Our study shows that such attacks can be easily launched, and cause service disruption. We then implement a solution based on traffic pattern analysis and filtering to resolve and prevent AuthRF and AssRF attacks. This solution is validated by empirical data.**

Index Terms: 802.11i, 802.11w, DoS, VoIP.

I. INTRODUCTION

Since the standardization of 802.11 in 1999, the WLAN becomes more and more popular and is widely deployed at home, Small Office/Home Office (SOHO), enterprise networks and hot spots due to its flexibility, ease of installation and configuration, high performance, relatively low cost and potential applications of WLAN VoIP. The popularity of WLANs encounters a continual increase in security attacks against WLANs, and the 2005 survey from Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) shows that WLAN abuses (i.e., security attacks) is the only "growing" threat of computer crimes [1]. We classify WLAN security attacks into two categories: *crypto* attacks and DoS attacks. Crypto attacks include unauthorized access, man-in-the-middle, masquerading, eavesdropping, replay, tampering and session hijack. In general, security solutions of VPN and 802.11i [2, 3] provide an effective mechanism to address crypto attacks. Unfortunately, these solutions do not protect WLANs against DoS attacks.

Chibiao Liu, PhD student, School of Computer Science, Telecommunications, and Information Systems, DePaul University, Chicago, IL 60604 USA (email: cliu1@cs.depaul.edu).

James Yu, Assistant professor, School of Computer Science, Telecommunications, and Information Systems, DePaul University, Chicago, IL 60604 USA (corresponding author, phone: 312-362-5938, email: jyu@cs.depaul.edu).

Major DoS attacks on WLANs include authentication request flooding (AuthRF), association request flooding (AssRF), deauthentication flooding and disassociation flooding [4, 5]. These DoS attacks cause the WLAN or some of its wireless nodes out of services. As DoS attacks against WLANs become more and more common, we see increased interests and publications on the issues and solutions of such DoS attacks [6-13]. Those publications raise the awareness of DoS attacks and provide wireless users and network managers with helpful practices to protect their WLANs. However, there are no studies to address solutions to resolve AuthRF and AssRF DoS attacks. In addition, there are no experimental studies of the effects of these DoS attacks on data integrity, network performance and user experience of time sensitive applications.

Meanwhile, to prevent DoS attacks on WLANs, 802.11w task group is working to protect management frames and action frames [14]. The mechanisms or protocols to protect management and action frames are very similar to the protection of data frame using the keys derived for TKIP or CCMP. However, there are some limitations in the draft version of 802.11w. First, all management frames sent or received by a station before keys are derived are unprotected. Secondly, 802.11w does not mention how to protect authentication request frame and association request frame, and it does not address how to prevent AuthRF and AssRF DoS attacks either.

The purpose of this paper is to provide comprehensive studies of AuthRF and AssRF DoS attacks against WLANs and their potential solutions, along with an experimental framework to study and quantify the effect of DoS attacks. The remaining sections of this paper are organized as follows. The second section presents the experimental design to study AuthRF and AssRF DoS attacks over WLANs. Demonstrations and detail analyses of AuthRF and AssRF DoS attacks on WLANs are presented in Section 3. Solutions to resolve AuthRF and AssRF DoS attacks are discussed in Section 4. Conclusions are provided at the end of this paper.

II. EXPERIMENTAL DESIGN OF WVOIP

An experimental environment is illustrated in Fig. 1, where Cisco Catalyst 2950 Ethernet switch (SW-1) is used to connect workstations, the Remote Authentication Dial In User

Service (RADIUS) server, Session Initiation Protocol (SIP) server and the 802.11 wireless access point (Linksys WAP-54G). Workstations (SIP-1, SIP-2, SIP-3 and SIP-4) are running Windows XP SP2 with installation of Xlite SIP v2 VoIP phone [15] which supports G.711 voice codec with a data rate of 64 kbps. For the tested soft VoIP phone, the sampling rate is set at 20 ms for each Real-Time Transport Protocol (RTP) packet. In our experiments, the RTP payload size is 160 bytes. Adding the RTP header size of 12 bytes, the UDP header size of 8 bytes, the IP header size of 20 bytes, and the layer-2 frame header of 14 bytes, then the total size for each voice frame is 214 bytes. The captured layer-2 throughput is 171.2 kbps (85.6 × 2) for both ways. Meanwhile, the TCP (Transmission Control Protocol) traffic generator of wsttcp [16], and the traffic analyzer of Ethereal is installed on workstations of SIP-1, SIP-2, SIP-3 and SIP-4. The traffic generator and analyzer are used to measure TCP performances over WLANs.

In this paper, we study the effects of 802.11 DoS attacks of AuthRF and AssRF. These DoS attacks are directly related with the processing mechanisms of the 802.11 management frames. They have nothing to do with the bandwidth requirements and the choice of vocoder. We assume that our studies using G. 711 are applicable to other vocoders such as G. 729A and G. 723.1 as well. In our experiment, we observe that the security schemes such as Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) cannot prevent any of these DoS attacks, and there is no need to report each one of them under different DoS attacks. To prevent crypto attacks, we choose the strongest security approach of 802.11i-AES to protect the tested WLAN in our experiment.

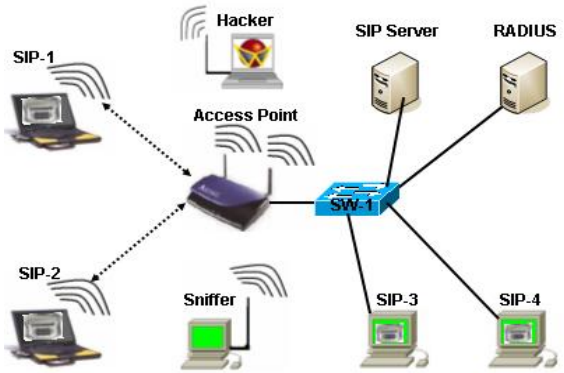

Fig. 1: Test Design for WVoIP Studies.

SIP-1 and SIP-2 are equipped with Linksys 802.11 b/g wireless adapters which support 802.1X user authentication, data encryption and integrity with TKIP and AES. SIP-1 and SIP-2 represent the wireless VoIP phones. SIP-3 and SIP-4 represent the wired VoIP phones. The RADIUS server for 802.1X user authentication is a Linux based freeRadius server (version 1.02), which is running on Red Hat 9.0 (Linux kernel of 2.4.29). SIP server of Asterisk is running on Fedora Core 2 with Linux kernel of 2.65-1.358. The DoS attacking tool of void11 [12] is installed on a Red Hat (kernel 2.4.29) Linux machine (Hacker), which is used to launch layer-2 flooding DoS attacks. For authentication request and association request flooding DoS attacks, the average speed is 250 frames per second. The physical bandwidth requirement for these 802.11 DoS attacks is below 0.11 Mbps, which is only 1.0% of the available physical bandwidth from 802.11b.

The sniffer is a Window XP machine installed with the sniffing software of LinkFerret [17], which runs on the Agere Orinoco 802.11b PCI (Peripheral Component Interconnect) adapter. This sniffer is used to capture frames transferred over the wireless medium. The captured frames include 802.1X authentication frames, 802.11 management frames, 802.11 control frames and data frames. The traffic analyzer of Ethereal is installed on workstations of SIP-1 to SIP-4. Ethereal is used to measure VoIP call performances over wired and wireless networks. In our experiments, Ethereal is used to analyze RTP traffic and report the throughput, the packet loss, and jitters. We calculate the delay based on the timestamp of the captured packets of Internet Control Message Protocol (ICMP) echo request and ICMP echo replay. Voice quality is measured by packet loss, delay and jitter, and these measurements are translated into Mean Opinion Score (MOS) (Table 1) based on Eq. (1) and Eq. (2) [18]. MOS provides a numerical assessment of VoIP quality, and MOS ranking and user satisfactions in Table 1 are from the published data [19, 22].

$$\mathbf{R = 94.2 - Id - Ie} \quad \mathbf{(1)}$$

$$\mathbf{MOS = 1 + 0.035 * R + 7 * 10^{-6} * R\,(R-60)*(100-R)} \quad \mathbf{(2)}$$

Table 1: MOS ranking and the user satisfaction.

MOS ranking	User Satisfaction
4.3 to 5	Very Satisfied
4.0 to 4.3	Satisfied
3.6 to 4.0	Some Users Dissatisfied
3.1 to 3.6	Many Users Dissatisfied
2.6 to 3.1	Nearly All Users Dissatisfied
Below 2.6	Not recommended

In Eq (1), Id is related to one-way delay and Ie is related to packet loss. And both of them are also related to the type of vocoder. For a typical WVoIP call from SIP-1 to SIP-4 (Fig. 1), the calculated MOS is 4.40, which is close to the reported value of 4.5 [19]. Based on the MOS ranking and the user satisfaction (Table 1), WVoIP call quality under the controlled test environment is *very satisfied*.

III. DOS ATTACKS ON WLAN COMMUNICATION

The convergence of voice and data networks has becoming one of the most popular technologies in the telecommunication industry. There is a growing demand and deployment of VoIP in the enterprise environment and as a standard service by major carriers. Attracted by the advantages of both WLANs and VoIP, WVoIP was proposed and implemented over WLANs [20]. We also see a trend and growing demand of dual-mode mobile devices with WVoIP and 3G capabilities. Meanwhile, the security threat becomes

an important issue for the success of VoIP. VoIP is a real-time service and very susceptible to DoS attacks that affect audio transmission. AuthRF and AssRF DoS attacks can be easily launched and could cause serious problems [12]. These attacks post a high risk for an enterprise to deploy VoIP successfully. DoS against VoIP can take various forms, but it generally prevents users from effectively using the VoIP service. In this section, we study and quantify the effects of DoS attacks against WVoIP and regular TCP data communications.

A. AuthRF and AssRF DoS attacks on WVoIP

AP authentication buffers are used to hold information during the authentication process. When the buffer is full, the AP would not be able to accept new call requests. A hacker could continuously flood the AP with authentication requests, making the AP incapable of accepting new WVoIP calls or serving those active WVoIP calls. We conducted experiments to demonstrate the AuthRF DoS attack on WVoIP. In Fig. 1, SIP-1 and SIP-4 have an active WVoIP call. After the hacker starts flooding authentication requests to the AP at the time of the 45th second (Fig. 1), the WVoIP call stops (no traffic) immediately. The DoS attack stops at the time of the 55th second, and it takes about 20 seconds to resume normal voice communications. The reason for taking so long to resume voice communication is that the AP itself is attacked and overflowed, and it needs a long time to return back to normal operations.

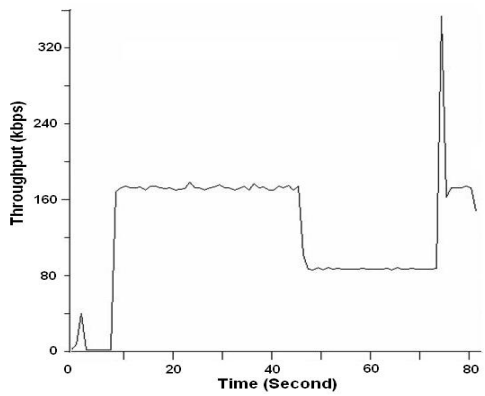

Fig. 2: WVoIP throughput under AuthRF.

Fig. 2 shows that there is still one way voice traffic captured at SIP-1 during the DoS attack. This is because AuthRF targets the AP, and SIP-1 still keeps sending voice data to the AP. However, the AP has no resource to receive and process the voice traffic from SIP-1. The sharp peak in Fig. 2 is due to the quick sending of the buffered data at the AP. Meanwhile, no new WVoIP calls can be accepted under the AuthRF attack. Table 2 gives the voice characteristics before and during the AuthRF DoS attack. During the attacking period, the voice packet loss rate is 35.0%. The average jitter is 25.63 ms. The MOS is 1.58, and this voice quality is unacceptable (Table 1). Under the AuthRF attack, there is no ICMP echo reply received for the outgoing ICMP echo request. We assume that the one way delay is bigger than 500 ms. Meanwhile, the average throughput is 111.3 kbps, which is calculated from the packet loss and the normal throughput of 171.2 kbps.

Table 2: Voice characteristics vs. AuthRF.

Parameter	**No AuthRF**	**Under AuthRF**
Throughput (kbps)	171.2	111.3
Packet loss (%)	0	35.0
Delay (ms)	0.73	>500
Jitter (ms)	2.69	25.63
MOS	4.40	1.58

For the AssRF DoS attack, a hacker could continuously flood the AP with association request frames to make the AP deny new WVoIP calls and stop serving active WVoIP calls. We conducted experiments to demonstrate the AssRF DoS attack on WVoIP. Effects of AssRF on WVoIP are similar to those of AuthRF.

B. AuthRF and AssRF on TCP communication

We conducted experiments to demonstrate AuthRF and AssRF DoS attacks on TCP data communication. In Fig. 1, SIP-1 and SIP-3 start a TCP session. After that, the hacker starts flooding authentication or association requests to the AP. During this DoS attack, the SIP-1/SIP-3 TCP session throughput drops immediately (Fig. 3). Effects of AuthRF on TCP data communication are similar to those of AssRF.

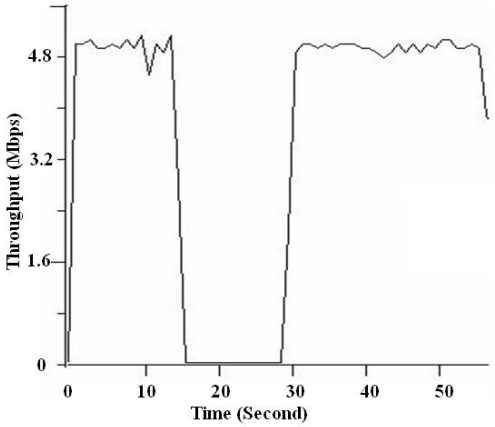

Fig. 3: TCP throughput under AssRF attack.

C. AuthRF and AssRF attacking mechanisms

When the legitimate AP receives the authentication request with a faked source MAC address, it reserves buffers for the authentication request and sends out an authentication response to the faked wireless client. Since the faked wireless client does not exist, the AP cannot receive the ACK (**ACK**nowledgement) for the transmitted authentication response frame. The AP keeps sending out several authentication response messages. For AuthRF, the victim AP always keeps reserving buffers and/or sending multiple response messages for each received authentication request. To process these authentication requests consumes a great deal of the AP's resources. As a result, the AP has little

resource to serve those already associated wireless clients (WVoIP phones), and these wireless clients may either suffer poor voice communications or lose the communication completely.

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 layer-2 ACK 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 those already associated wireless clients. This forces the associated wireless clients to slow down or even stop their data communications.

To prevent AuthRF and AssRF DoS attacks, the AP needs to have the capability to distinguish valid requests and hacking requests. Unfortunately, the current 802.11 (or 802.11i) standard does not support authentication of such requests.

IV. SOLUTIONS TO AUTHRF AND ASSRF

Currently, there are no published solutions to prevent DoS attacks of AuthRF and AssRF. In this paper, we demonstrate solutions to resolve AuthRF and AssRF DoS attacks through modification of source codes of a Linux based HostAP [21]. In this section, we discuss two approaches to resolve AuthRF and AssRF DoS attacks. One method is MAC address filtering, and the other method is traffic pattern filtering.

A. MAC addressing filtering(MAF)

Originally, MAC address filtering is an approach to control access to the wireless network based on the ap_control table such as Table 3. When MAC access filtering is enabled, the AP compares the source MAC address of the received authentication request frame with those in the ap_control table. If the received MAC address matches one of those in the ap_control table, it will further process the received authentication request or grant access to the wireless station. Otherwise, it will drop the received authentication request. However, MAC address filtering is not an effective way for access control because a hacker can easily sniff and fake MAC addresses of legitimate wireless users. Therefore, 802.11i-PSK (Pre-shared key) or 802.11i-802.1X/RADIUS is recommended for user authentication and access control. MAC address filtering alone is rarely used for access control to wireless network.

Table 3: Example of the ap_control table.

Name	**Content**
MAC policy	allow
MAC entries	3
MAC list	00:13:10:37:48:3d 00:50:8b:d0:ef:34 00:50:8b:d0:ee:b5

Although MAC address filtering is not an effective approach for access control, its combination with other authentication methods could be used to effectively prevent AuthRF and AssRF DoS attacks. For AuthRF and AssRF, hackers floods the AP with thousands authentication request and/or association request frames with different faked source addresses. The AP is forced to allocate resources and process these faked authentication/association request frames. Thus, it consumes significant resources to process faked requests and cannot serve the legally associated wireless clients. MAC address filtering can help the AP drop faked requests and save wireless resources to serve legitimate wireless users. To effectively prevent AuthRF and AssRF DoS attacks, MAC address filtering should be used as early as possible.

One advantage of MAC address filtering is its simplicity and effectiveness. The disadvantage is its poor scalability. It can be used for SOHO environment. However, it is difficult to use MAC address filtering to protect an enterprise environment with many wireless clients. This is because users of an enterprise wireless network are dynamic and often moving from one access point to another. It is impractical and difficult to add every MAC address to every AP in an enterprise environment.

B. Traffic pattern filtering (TPF)

Traffic pattern filtering is another method to prevent AuthRF and AssRF DoS attacks. In this paper, traffic pattern filtering means that the AP will stop processing authentication and or association request frames if it receives more than a certain number of frames per second. Under normal wireless environment, the wireless traffic is small and sporadic. And it is normal for one access point to receive and process around *five* 802.11 frames per second. Under AuthRF and AssRF DoS attacks, the wireless traffic would follow a different pattern. For each faked authentication request frame, the hacker sends it five times, and the AP responds with 5 802.11 ACK frames. Furthermore, the AP might receive and process up to hundreds authentication or association request frames per second.

To prevent AuthRF DoS attack, we implement traffic pattern filtering rule after the AP retrieving the header information from the received authentication requests. In this phase, we not only have enough information from the sender to implement traffic pattern filtering, but also avoid wasting AP resources to process faked authentication request frames. On the other hand, for the AssRF DoS attack, we implement traffic pattern filtering after checking the authentication state of the sender of the received association request frame. If the sender is already authenticated, the association request will be further processed. Otherwise, the traffic pattern of association request frames will be checked, and filtering rule will be applied. For both AuthRF and AssRF DoS attacks, we have similar filtering rules. If the number of authentication or association request frames received per second is greater than 5, the received frames will be dropped; otherwise, they will be processed.

C. Validation of MAF and TPF solutions

We implemented the solutions of MAC address filtering and traffic pattern filtering, and our experiments show that they both can prevent AuthRF and AssRF DoS attacks effectively and efficiently. In this paper, we report the results of traffic pattern filtering to prevent AssRF DoS attack.

For the WVoIP call using a Linux-based AP, the AssRF DoS attack could cause a high packet loss or call disconnection (Fig. 4 and Table 4). Under the attack, MOS becomes 2.20, which is unacceptable for all WVoIP users. Then, we modify the Linux based AP to use traffic pattern filtering to process the received association requests. After implementing traffic pattern filtering in the AP, when restarting the AssRF DoS attack, it has no effect on the tested WVoIP call quality (Fig. 5).

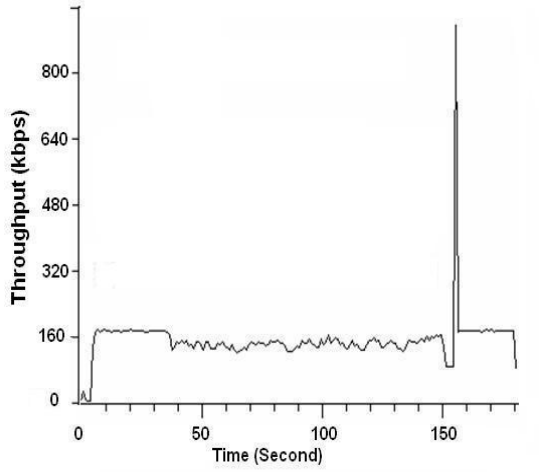

Fig. 4: WVoIP throughput under BM-AssRF.

Meanwhile, Table 4 shows that there is no voice data loss under the AssRF DoS attack. The jitter is small and similar to that without being attacked. Meanwhile, after modification, the calculated MOS for WVoIP calls is 4.40, and it does not change under the AssRF DoS attack. Thus, modification of association request processing mechanisms is successful, which prevents the AssRF DoS attack and guarantees a high WVoIP call quality.

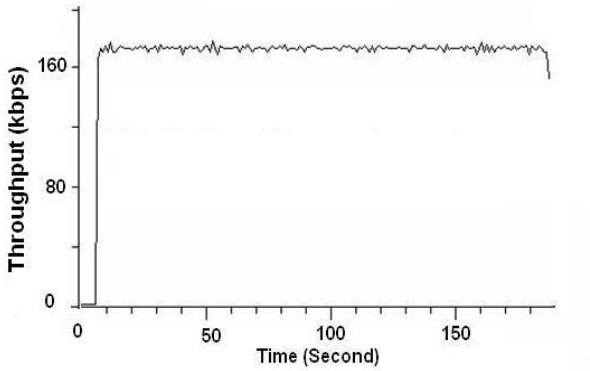

Fig. 5: WVoIP throughput under AM-AssRF.

Table4: Voice characteristics vs. modifications.

Parameter	BMN-AssRF	BM-AssRF	AMN-AssRF	AM-AssRF
Throughput (kbps)	171.2	134.2	171.2	171.2
Packet loss (%)	0	21.6	0	0
Delay (ms)	0.68	>500	0.69	0.70
Jitter (ms)	3.02	13	2.90	2.80
MOS	4.40	2.20	4.40	4.40

BMN-AssRF: Before modification without AssRF
BM-AssRF: Before modification under AssRF
AMN-AssRF: After modification without AssRF
AM-AssRF: After modification under AssRF

Meanwhile, experiments show that TPF can also effectively prevent AuthRF DoS attacks on the TCP data communication. Without TPF, the TCP throughput decreases by more than 99% under the AuthRF attack (Fig. 3). With TPF implementation on the AP, the effects of AuthRF on TCP performance reduce significantly (Fig. 6), where the TCP throughput decreases by 5% only. Meanwhile, effects of MAF solutions are similar to that of TPF. Without implementation of MAF, under the AuthRF attack, the TCP throughput decreases more than 99%. After implementing MAF, the effects of AuthRF on TCP performance reduce dramatically, and the TCP throughput decreases by 5% only.

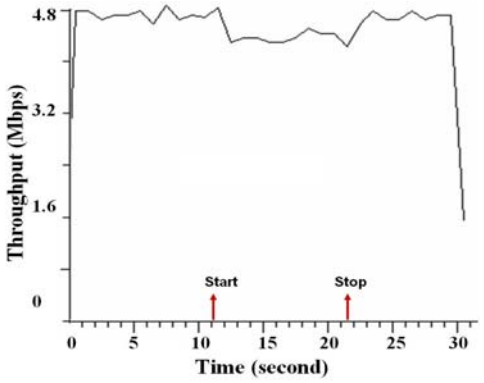

Fig. 6 TCP performances under AuthRF-TPF.

Above studies show that MAF and TPF solutions are effective and efficient to improve WVoIP and TCP performance under DoS attacks.

V. CONCLUSIONS

In this paper, we analyze two DoS attacks against 802.11 WLANs. We demonstrate AuthRF and AssRF DoS attacks on applications of regular TCP sessions and time sensitive WVoIP UDP traffic. It shows that these DoS attacks can cause serious problems for wireless communications. We also present a detailed study of the attacking mechanisms of AuthRF and AssRF DoS attacks. One major contribution of this paper is the implementation of a solution based on traffic pattern filtering to resolve AuthRF and AssRF DoS attacks against WLANs. Our solution is theoretically sound and cost-effective with no performance degradation to TCP or UDP traffic. Another contribution of this study is an empirical

framework to emulate AuthRF and AssRF DoS attacks and analyze performance impacts under different attacking scenarios.

MAC address filtering is not scalable, and difficult to use against AuthRF and AssRF attacks on enterprise WLANs. Traffic pattern filtering can resolve vigorous DoS attacks; however, it cannot eliminate slow flooding rate DoS attacks. In the future, we will further study AuthRF and AssRF DoS attacks using the queuing network model, which will assist us to develop more effective and efficient solutions.

Queuing network models have been used to study wireless data communication. In our future research, we will characterize the data processing functionalities of an AP with a queuing network model. The queues under study will be AP Receiver (APR), 802.11-ACK (ACK), AP Processor (APP), and AP Sender (APS). The APR queue mainly receives and stores 802.11 data. The ACK queue performs MAC layer acknowledgements to received wireless frames. Meanwhile, the APP queue mainly provides computation resource to process received data and prepare response messages. Finally, the APS queue takes care of the transmission and retransmission of response messages. Using a queuing network model, we would study properties of normal WLANs and the WLANs under DoS attacks. The queuing network model will help find the problem causes of AuthRF and AssRF. Based on analyses of the queuing models, we will develop better solutions to resolve AuthRF and AssRF DoS attacks.

REFERENCES

[1] L. A. Gordon, M. P. Loeb, W. Lucyshyn, R. Richardson, "CSI/FBI computer crime and security survey", http://www.usdoj.gov/criminal/cybercrime /FBI2005.pdf.

[2] C. Liu, J. T. Yu, "Protecting Enterprise Wireless LANs Using an Integrated Security Approach of VPN over 802.11i", *3rd International Conference on Cyber Information Technology and System Applications (CITSA)*, Orlando Florida, pp. 278-283, 2006.

[3] 802.11i, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, July, 2004.

[4] C. Liu, J. T. Yu, "Review and Analysis of Wireless LAN Security Attacks and Solutions," *Journal of International Engineering Consortium*, vol. 59, 2006.

[5] C. Liu, J. T. Yu, "An Analysis of DoS Attacks on Wireless LAN," *IASTED International Conferences on Wireless Networks and Emerging Technologies (WNET2006)*, Banff, Canada, 2006.

[6] J. Bellardo, S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", *Proceedings of the USENIX Security Symposium*, 2003, pp. 15-27.

[7] P. Ding, J. Holliday, A. Celik, "Improving the Security of Wireless LANs by Managing 802.1X Disassociation", *Proceedings of the IEEE Consumer Communications and Networking Conference*, Las Vegas, NV, 2004, pp. 53-58.

[8] S. Grech, J. Nikkanen, "A Security Analysis of Wi-Fi Protected Access", *The 9th Nordic Workshop on Secure IT-systems, Helsinki University of Technology, Finland*, November 2004.

[9] W. Ge, S. Sampalli, "A Novel Scheme For Prevention of Management Frame Attacks on Wireless LANs", March 29, 2005.

[10] D. Chen, J. Deng, P. K. Varshney, "Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming", *ACM MobiCom '03, Poster*, San Diego, CA, USA, September 14-19, 2003.

[11] V. Gupta, S. Krishnamurthy, M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", *Proceedings of 2002 MILCOM Conference*, vol. 2, 2002, pp.1118- 1123.

[12] A. A. Vladimirov, K. V. Gavrilenko, A. A. Mikhailovsky, *Wi-Foo: The Secrets of Wireless Hacking*, Pearson/Addison Wesley, June 2004, pp. 159-195.

[13] A. Mishra, W. A. Arbaugh , "An Initial Security Analysis of the 802.1X Standard", *University of Maryland, CS-TR-4328, UMIACS-TR-2002-10*, Feb., 2002.

[14] J. Walker, "Status of Project IEEE 802.11 Task Group w, Protected Management Frames", http://grouper.ieee.org/groups/802 /11/Reports/tgw_update.htm, 2007.

[15] CounterPath Solutions, www.xten.com/index.php.

[16] Wsttcp, "Benchmarking tool measures TCP and UDP performance", www.winsite.com/ bin/Info?5896.

[17] Tuca Software, "LinkFerret Wireless Packet Sniffer", http://www.linkferret.ws/wireless/wireless.htm.

[18] W. Jiang, H. Schulzrinne, "Comparisons of FEC and Codec Robustness on VoIP Quality and Bandwidth Efficiency", *IEEE International Conference on Networks (ICN)*, Atlanta, Georgia, August 2002, pp. 1-12.

[19] W. Jiang, H. Schulzrinne, "Comparison and Optimization of Packet Loss Repair Methods on VoIP Perceived Quality under Bursty Loss", *NOSSDAV'02*, Miami Beach, Florida, USA, May, 2002, pp. 73-81.

[20] M. Zibull, A. Riedel, D. Hogrefe, "Voice over wireless LAN: a fine-scalable channel-adaptive speech coding scheme", *WMASH'05*, Cologne, Germany, Sept., 2005, pp.111-114.

[21] S. Shin, A. G. Forte, A. S. Rawat, H. Schulzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs", *MobiWac'04*, October 1, 2004, Philadelphia, Pennsylvania, USA, pp. 19-26.

[22] A.P. Markopoulou, F.A. Tobagi, M.J. Karam, "Assessment of VoIP quality over Internet backbones", *INFOCOM 2002, Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, 2002, vol. 1, pp. 150-159.