DoS Attacks on IEEE 802.11 Wireless Networks and Its Proposed Solutions

Abhishek Gupta[1], Manish Garg[2]

Department of Computer Science and Engineering

Punjab Engineering College, Chandigarh

[1]abhishekgupta10@yahoo.co.in, [2]manishgarg.pec@gmail.com

Abstract- In recent times, wireless Local Area Network (WLAN) became very popular in approximately all enterprises, organizations and universities. It motivates to provide more security in WLAN, so many high level security protocols for IEEE 802.11 has been developed. E.g. WEP, WPA, WPA2. These protocols are unable to protect our WLAN from the DoS (Denial of Service) attacks. This paper shows how these attacks are launches, how to create threats in security and what will be the effect of these attacks on the WLAN. Paper also shows that how easily to do attack on the WLAN while so difficult to prevent the same and some solutions to prevent them also proposed.

Key words: Wireless Network, DoS Attack, Security, management frame, MAC address, IEEE 802.11

1. Introduction

Cheap prices and flexibility [1] of the wireless network has gained more importance and seriousness in the field of security. Wireless network is preferred rather than wired network. Wireless LAN (Local Area Network) does not require any planning [1] for network establishments for any campus or office and provides more robustness [1]. Different security issues [12] are noticed for the secure working in WLAN. User authentication, data integrity and availability of the service are the major threats in IEEE 802.11 wireless network. The most secure protocol for WLAN is WPA2 (Wi-Fi protected access 2) [2-6] is also unable prevent these threats [14].

Management frames [2, 9] are the lose pole of the WLAN security which invites the DoS attack on the network. These frames are not protected by 802.11i (WPA2) protocol. Major DoS attacks are Deauthentication flooding (DeauthF), Authentication Request flooding (AuthRF) and Association Request flooding (assRF) [10, 11]. These DoS attacks [7, 8] make WLAN still vulnerable and make the network not accessible for the legitimate users.

This paper is organized in four sections. Section 2 provides the details of how to generate DoS attacks while using the most secure protocol. Section 3 proposes what can be the solutions to overcome these problems and section 4 discusses the conclusion.

2. DoS Attacks on management frames

In wireless networks, management frames are very important to provide connectivity. When client comes in the range of AP (access point) then it first send the association frame to the AP to ask to be associated then AP respond with an approval or denial of the request. Similarly authentication request frame and deauthentication frame also launches from the client and replied by the AP and for sending frame there is no restriction so intruder can also send the similar frame but thinking some wrong result and this way an attack is generated. Now these management frames became responsible for DoS attacks on WLAN.

Wireless security protocol uses various encryption algorithms but cannot have control on management frames so threats are still available. Strongest WLAN protocol WPA2 uses AES (Advance Encryption Standard) Algorithm [14]. AES is the most secure encryption algorithm but made the speed of process slow so this algorithm is implemented in hardware. Other WEP (wired equivalent access) and WPA uses RC4 algorithm [14].

Now we discuss about most common DoS attacks on IEEE 802.11 wireless network as DeathF, AuthRF, AssRF attacks.

2.1 *Deauthentication frames* [10, 11, 13] are continuously sent by intruder to its victim as shown in figure 1. These types of frames are the notification frames that have to be implemented its function and cannot be ignored by the receiver. But, this is not the single frame send by the intruder while continuously a large number of frames are sent which make full the victim's buffer with these type of request frames so it consumes victim's all the resources to process deauthF and waste time correspondingly to this, victim cannot process other requests or notifications coming from the other clients or AP because victim buffer is full with the intruder's deauthF so for this amount of time client is disconnected to the other devices.

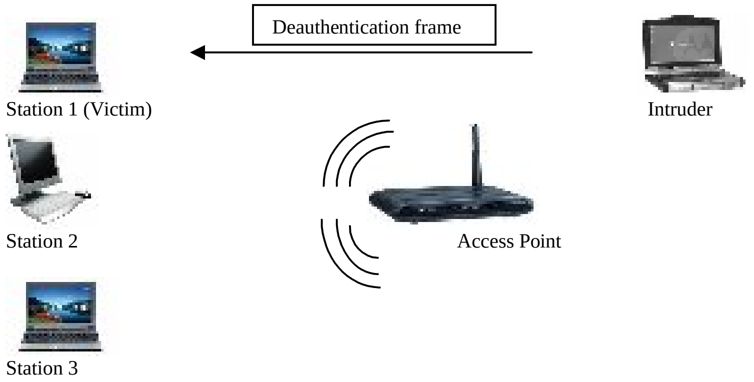

Figure 1: DeauthF Attack on Station 1

If intruder want to make this attack worse, then intruder will make attack on the access point (AP) because in this case all legitimate users will be disconnected from the whole networks which are already connected with the same AP.

2.2 *Authentication request frames* [10, 11, 13] are received by legitimate AP (as shown in figure 2) but with a faked source MAC address and correspondingly AP send the response but there is no receiver having the same MAC address so there will be no acknowledgement for that response. Thereafter AP will wait for the same till timeout and then will again send the same response. In this way AP keeps sending out many authentication response frames which result resources became busy to send response only and consume major time to wait for time out and this process. These results the communication become poor or may be disconnecting from the network.

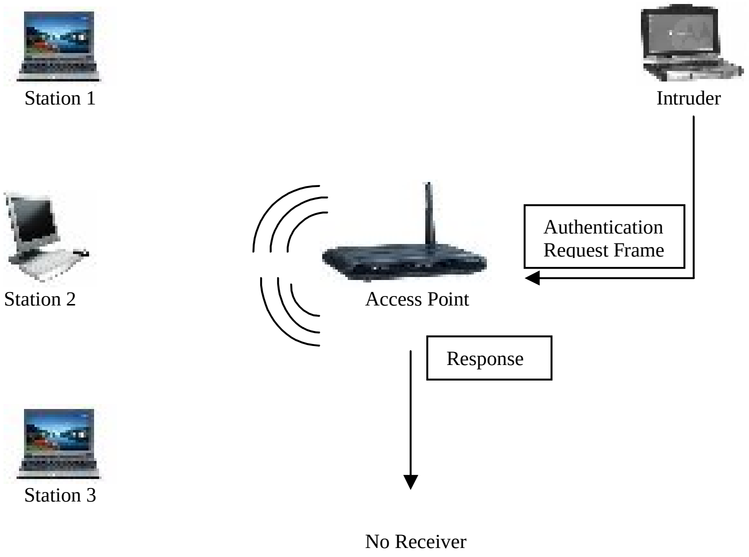

Figure 2: AuthRF Attack on Access Point

2.3 *Association request frames* [10, 11, 13] are also received by AP with a faked source MAC address. This is a request when any station want to associate with AP then sends so in this case intruder send this to the AP as shown in figure 3. AP checks its buffer but does not find sender as the legitimate wireless client in authenticated stable table. But AP cannot ignore this request frame and has to be response corresponding to it but as it is a faked MAC address so there is no receiver and acknowledgement will not be receive by AP. Similarly as the AuthRF, AP will wait till time out and keep sending out many responses. AP resources will consume all the time to search this faked source MAC address and sending response and throughput of the network will drops and can also stop the communication.

3. Prevention of DoS Attacks

As it is known that management frame cannot be protected but any how some techniques may be possible that can prevent these DoS attacks to some limit. In this paper we are discussing some techniques of them.

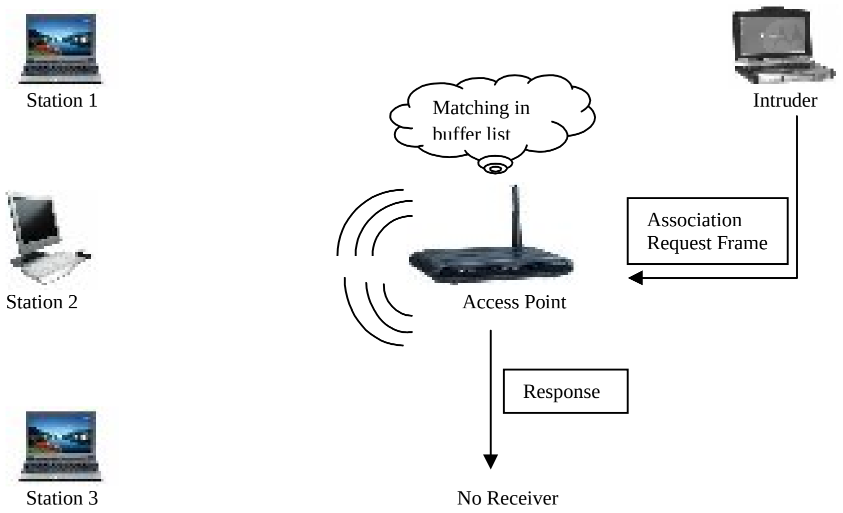

Figure 3: AssRF Attack on Access Point

3.1 *Maintaining MAC address Table*- Access point maintains a table consisting of the MAC address of the legitimate users. When any user send a management frame then the MAC address of the sender is search in the AP’s table if it matches then the frame will be proceed otherwise AP will drop that management frame.

But this way is not so much effective because an intruder can easily sniff and fake address of legitimate wireless users. So this technique is not much uses but can be more effective by combining this in another authentication method and used to prevent DoS attacks. Other problem arises about the poor scalability of the AP. Difficulty comes to add every MAC address in the table and to maintain that table for any enterprises. It also can be impractical if any user of wireless network enterprise is dynamic and moving one AP to another.

3.2 *Traffic filtering*- It is another method to prevent DoS attacks to define a limit for the AP to process the management frames in per second. AP will count the number of management frames per second receiving from any particular MAC address and if that are exceed from a already decided limit then next all frames will be ignored at that second for that particular MAC address. Actually this method consumes the limited resources for that particular MAC address. This way we also reduce the consuming time only a resource in per sec.

Solutions	Method	Dependency	Problems	Effectiveness
Maintain MAC	Stores All MAC	MAC Address	Sniffing and	Less

Address Table	Address	Table	Scalability	
Traffic Filtering	Processing Limit Per Second	MAC Address of Sender	Variable MAC Address	More

Table 1: Comparisons of DoS Attack Solutions

A problem can occurs only in a case if an intruder is sending continuously management frames by changing the MAC address for every frame per second then AP will process all the frames understanding that a large number of clients want to associated simultaneously. Table 1 also compare both Solutions.

4. Conclusion

IEEE 802.11 wireless network is still vulnerable after developing many more secure protocols. After all many techniques are proposed to provide security but some lose pole also be there in these methods. However at any limit it can be secure by combining more than a method or using for a special condition. Still research is going on for protecting these management frame so that DoS attacks can be prevent or reduces to make wireless network more significant at every time.

5. References

[1] Jochen Schiller, “Mobile Communication”, Pearson Education, second Edition, page No. 221-223

[2] IEEE Standard 802.11i .2004.Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements.

[3] 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

[4] Walker J. 2005.IEEE 802.11i Standard Improves Wireless LAN Security.

[5] Sithirasenan1 E., and Muthukkumarasamy. 2005. Detecting Security Threats in Wireless LANs Using Timing and Behavioural Anomalies.

[6] Arana P. 2006. Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2).

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

[8] 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.

[9] 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

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

[11] 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.

[12] 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.

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

[14] William Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall Third Edition, page No. 158-161 and Page No. 210-212