Research Journal of Applied Sciences, Engineering and Technology 7(19): 4162-4170, 2014
DOI:10.19026/rjaset.7.782
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 28, 2013 Accepted: January 10, 2014 Published: May 15, 2014

Research Article

Comparison of ICM with TPF-LEP to Prevent MAC Spoof DoS Attack in Wireless Local Area Infrastructure Network

M. Durairaj and A. Persia
School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli-23, Tamilnadu, India

Abstract: A Comparison of Integrated Central Manager (ICM) and Traffic Pattern Filtering with Letter Envelop Protocol (TPF-LEP) is done. Denial of Service (DoS) attack is a biggest peril in wireless local area infrastructure network. It makes the resources unavailable for intended users which transpired through spoofing legitimate Client/AP's Medium Access Control (MAC) address. MAC address are easily caricatured by the adversary clients, subsequently they are not encrypted. Since, the adversary sends the management frame, which is unencrypted, to the victim using spoofed MAC address. This study compares the performance of Integrated Central Manager (ICM) and Traffic Pattern Filtering with Letter Envelop Protocol (TPF-LEP) and evaluated the result using NS2. The attack scenario is simulated and effectiveness of the solutions is validated after the instigation of solutions in the attack consequences. Throughput, Packet Delivery Ratio and Packet Loss are measured and taken to endorse the performance of ICM and TPF-LEP.

Keywords: Access point, dos attack, ICM, infrastructure network, MAC spoof, TPF-LEP

INTRODUCTION

Wireless Local Area Networks (WLAN) are popular due to easy installation and it offers augmented wireless access to the client with the help of Access Point (AP). Security issues in wireless network increases as popularity increases. Wireless Local Area Network (WLAN) architecture is divided into three types. They are Infrastructure architecture, ad-hoc architecture and mixed mode architecture. In infrastructure architecture, communication takes place with the help of Access Points (APs) where as each host communicate with each other in ad-hoc architecture. Mixed mode architecture is a type of network which is the mixture of infrastructure and ad-hoc architecture. This study discusses the security issues prevalent in infrastructure network and proposes an effective solution for this.

Infrastructure network does not have firewall to defend the entire network. Physical protection of wired medium such as firewalls and shields cannot be applied to wireless networks. So intruders can easily enters into the network and damage the network. As a result more number of attacks in infrastructure network. Many people are not aware of the DoS attack when it takes place in their network. Sending continuous stream of forgery frames by an attacker can easily slow down the network; hence the network would not be available for its authenticated clients. Several protocols were developed to protect wireless network. Every protocol has its own security deficiencies (Durairaj *et al*., 2013). Wired Equivalent Protocol (WEP) is a basic part of IEEE 802.11 standard for the protection of wireless network which uses RC4 algorithm. There are several safety deficiencies like two messages encrypted by the same key stream. To overcome these deficiencies Wi-Fi Protected Access (WPA) and 802.1 x were developed. The 802.1x is a security protocol based on the frame structure of 802.11. It attempts to provide strong authentication, access control and WEP key management for Wireless LANs. Unfortunately, 802.1x misses its goals in access control DoS attacks. Currently, there is scarcity of IEEE approved ways to resolve the security hole.

MATERIALS

Ping (2007) describes an efficient solution to avoid DoS attacks in WLAN using Central Manager (CM). CM acts as a back end server which maintains three tables and timer to detect DoS attacks. Apart from preventing DoS attack, this mechanism can be used to improve the performance of Wireless Local Area Network (WLAN). The solution suggested is evaluated by five different DoS attacks such as Large number of Association requests (LASO), EAP failure, EAP start, EAPOL logoff and MAC disassociation

Corresponding Author: A. Persia, School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli-23, Tamilnadu, India

Salem *et al*. (2007) proposed an Intruder Database (IDB) technique in order to prevent the intruders to bring down the network by DoS attack.

Persia *et al*. (2011) proposed a solution which combines existing CM and IDB, called it as an Integrated Central Manager (ICM). This acts as an authentication server which manages Client and AP's communication with the help of five tables and a timer. Duplicate ICM was proposed to overcome the overall drop of the throughput.

Nguyen *et al*. (2008) developed a light weight solution to defend against attacks on Management Frames. This is based on the factorization problem.

Shamala *et al*. (2009) developed an experimental framework to measure the possible attacks using unprotected EAP frames against wireless communication.

Sivagowry *et al*. (2012), suggested Letter Envelop Protocol (LEP) which is ensued to be the most effective solution in preventing Resource Flooding Attacks (RFA). But, in case of vigorous attacks, the employment of multiple techniques is required. In such a case, combined mechanism of Traffic Patter Filtering (TPF) with LEP was employed to prevent the legitimate users from adversary clients.

Attacks in WLAN: Higher numbers of attacks are probable in Wireless Local Area Network. They are categorized as passive attack, active attack, distributed attack, insider attack, close-in-attack, phishing attack and spoof attack, hijack attack, buffer overflow and exploit attack and password attack. This study dealt with Denial of Service (DoS) attack which comes under the category of active attack. It is one of the dreadful attacks in WLAN. It is a kind of attack set up by the intruders in a WLAN environment. Denial of Service attack is an attempt to make computer resources unavailable to its legitimate user. Intruders can easily access the network by pretending themselves as authenticated users. Numerous researches have been carried out to avoid DoS attacks and different security protocols were proposed and implemented over WLAN such as 802.11i (Jalil *et al*., 2008), Wired Equivalent Privacy (WEP) (Radomir and Dejan, 2007), Wi-Fi Protected Access (WPA) (Stanley, 2003), 802.11 (Bellardo and Savage, 2003; Bicakci and Tavli, 2009), 802.11b (Ferreri *et al*., 2008), 802.1x and 802.1w (Lashkari *et al*., 2009; Cam-Winget *et al*., 2003). None of them performs to be an effective solution to avoid DoS attacks.

Denial of service attack: There are different types of attacks comes under DoS attack such as Large number of Association Requests (LASO), EAP failure, EAP start, EAP success frame, EAPOL logoff and MAC disassociation. EAP messages are encapsulated in 802.1x messages and referred to as EAPOL. The attacks considered for the study are EAP start, EAPOL logoff, EAP failure and EAP success. Among the above four different types of attacks, EAPOL logoff is a most

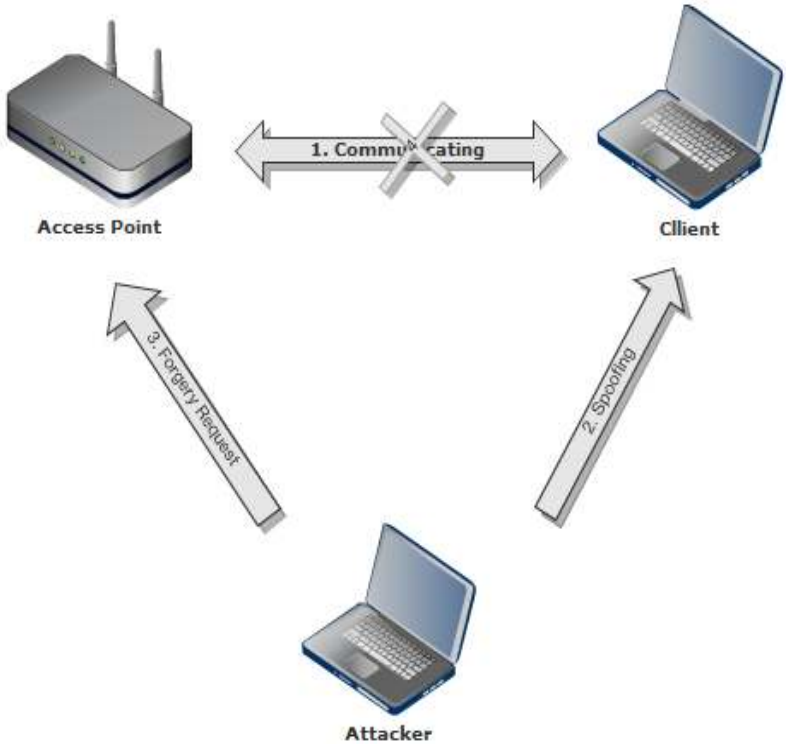

Fig. 1: DoS in WLAN

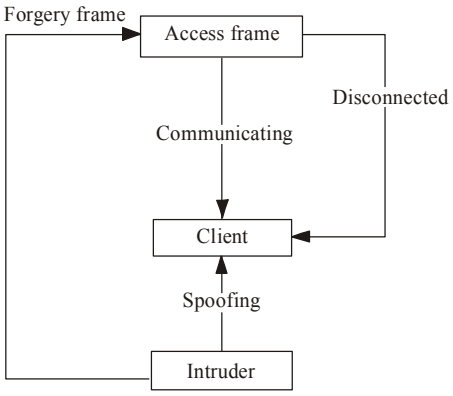

Fig. 2: Logical development of DoS attack

awful attack in which an AP or client disconnected from the entire network. After EAPOL attack takes place, user need to re-authenticate and re-associate to particular Access Point/Client.

Operation of DoS attacks are illustrated in Fig. 1. It denotes that while access point and client are in the process of communication, attacker spoofs the user identity and makes the Denial of Service attack. This resulted in the disconnection of legitimate clients from access points.

EAPOL start frame: Wireless client gain access to the network after sending an EAPOL start frame to the AP. Communication between AP and client starts after AP accepts the clients request by checking the user identity. When clients communicate with AP, attacker sends a forgery EAPOL start frame to AP and spoof the legitimate clients MAC address which makes AP is busy with attacker and inept to handle legitimate traffic. Therefore the communication between client and AP is rejected. This is known as EAPOL start frame over AP. The same vice versa is followed in the EAPOL start frame attack over the client.

EAPOL logoff frame: When a client wishes to leave from WLAN, it sends EAPOL logoff frame to access point to end its authenticated session. By using this chance, attacker spoofs the client MAC address and sends EAPOL logoff frame to the target access point. This causes the AP to believe that the legitimate station has concluded its session. The legitimate station will not be aware that its session has been ended until it attempts to transmit data. After that AP disassociates the original client from the transmission which is called as EAPOL logoff frame over AP. In the same way the hackers steals the working AP's MAC address and blocks the client from legal traffic, commonly known as EAPOL logoff frame over client.

The overall framework of attack is as depicted in Fig. 2. While AP and client are communicating with each other, intruder sends forgery frame to the AP after spoofing the MAC of the client. When the AP receives the forgery frame from the intruder, the connection between the AP and the client gets disconnected.

METHODS TO PREVENT DOS ATTACKS

This section discusses the working of Integrated Central Manager (ICM) (Persia *et al*., 2011) and Traffic Pattern Filtering with Letter Envelop Protocol (TPF-LEP) (Sivagowry *et al*., 2012) in details. The description of the solution is as follows.

ICM in DoS attacks: Integrated Central Manager (ICM) acts as an authentication server and takes responsibilities of AP to manage the AP and client communication. It detects and blocks the intruders in a WLAN using five tables and a timer. The tables are such as Accounts (T1), Intruder (T2), Authenticated Client (T3), Unauthenticated Client (T4) and Client table (T5). The contents and role of the tables are as follows: Account table is for checking the client identity based on their Medium Access Control (MAC) address. Intruder table contains the MAC address of all the intruders detected and spoofed by ICM. Authenticated table consists of MAC addresses of working clients, who are in the communication process and their login as well as logout time. Unauthenticated client table records the MAC address, login and logout time of wireless clients who are not in communication with AP. Client table contains the MAC addresses and login time of all the clients.

EAPOL start frame over the AP: Attacker send EAPOL start frame to AP by spoofing authenticated client's MAC address otherwise send request to AP by using client's own MAC address. When attacker sends an EAPOL start frame to AP, ICM checks T2 for address. If the address is found in T2, the request will be ignored by the ICM. Otherwise it goes to T3. If a particular MAC address is already in T3, ICM infers that the request is from an attacker and spoofs the forgery client's MAC address and stores it in T2. If it is not in T3, it checks in T5. If it does not match, ICM spoofs and records the MAC in T2.

EAPOL start frame over client: Hacker send EAPOL start frame to the client by spoofing MAC address of AP. When it sends login request to the client, the request automatically redirected to the ICM. After receiving the request, ICM tends to check table T2. If the MAC address is found, it will ignore the request. Otherwise it checks in T3. If the MAC address is already present in T3, it will ignore the request and also it spoofs the attacker's MAC address and stores it in the table T2.

EAPOL logoff frame over AP: Attacker send logoff request message to AP by using legitimate client's MAC address. ICM sends an encrypted message to the client whether to logoff or not. If the client accepts and responds with logoff continue message, it proceeds to logoff. If the client not responds to AP, ICM spoofs and stores the attacker's MAC address in T2.

EAPOL logoff frame over client: Attacker send logoff request message to client by using AP's MAC address. ICM sends an encrypted message to AP whether to logoff or not. If the AP accepts and responds with logoff continue message, it proceeds to logoff. If the AP does not respond to client, ICM spoofs and stores the attacker's MAC address in T2.

TPF-LEP in DoS attack: Management Frames are sent unauthenticated during the data transfer in WLAN. So they are easily susceptible to attacks. The main focus in the solution is to protect the Management Frames (MF). Letter Envelop Protocol (LEP) (Nguyen *et al*., 2008) is proposed to prevent Resource Flooding attacks. It works based on the factorization problem. The Letter Envelop protocol works as follows:

- The client randomly generates two prime numbers p1 and q1. It then computes N1 = p1*q1. In the same way, AP generates p2, q2 and computes N2.
- During the authentication, the client sends an "envelop" containing N1 to the AP. The AP stores it and sends N2 to the client. The N2 sent by AP is common for all clients.
- When the client wants to disconnect, it sends the de-authentication frame to the AP, along with p1. The AP computes p1/N1 and finds whether it matches with the N1 which was already stored.
- If it is correct, the client tends to be disconnected. Otherwise, the frame gets rejected assuming that it is from the hacker.
- Similar procedure is followed for AP when it wants to disconnect from the client.

This solution is found to be effective in preventing Resource Flooding attacks because even though the hacker could able to spoof the MAC address, nothing will happen to the legitimate client. The authentication is progressed based on the LEP. The hacker can generate prime numbers and communicate with AP but cannot generate the same prime numbers as the client. It takes extended time to generate the same number as the legitimate client. When the attack is vigorous, this protocol is not enough to save the client from the attackers.

In the case of vigorous attacks, we propose a prevention mechanism which is a combination of Traffic Pattern Filtering (TPF) with LEP. AP uses TPF along with LEP (Jalil *et al*., 2008). The TPF works as follows:

- If a request is received more than 5 times at a particular time from a client, it infers that the request is from the hacker and ignores it (Jalil *et al*., 2008).
- Since the hacker continuously sends request, AP is unable to process the request from the legitimate clients.

TPF is employed to prevent continuous Resource Flooding request from the attacker.

Performance evaluation on NS2: For the experimentation, in an average of 233 CBR packets were taken to evaluate during the attack and after applying the solutions. The performance of ICM and TPF-LEP is validated using NS2 simulator (The ns Manual (Formerly ns Notes and Documentation), 2009). Attacks discussed in the previous section were simulated and evaluated by measuring throughput, packet delivery ratio and packet loss. Start frame and Logoff frame attacks were simulated for experiment and the relevant parameters were measured during the attacks and after applying the solution. The experiments carried out on the logoff attack are discussed below.

Evaluation of throughput: Throughput of ICM and TPF-LEP were evaluated to measure the effectiveness of the proposed mechanism and compared with each other. Throughput is the average rate of successful message delivery over a communication channel. Throughput decreases in the attack scenario where as it increases at a maximum level after apply the ICM mechanism. The usage of TPF-LEP increases the throughput than the attack scenario, but it is not effective when compared to ICM. The throughput during attack and after applying the ICM is illustrated in Table 1. It shows that the throughput of ICM is increased when a packet rate is increased.

The comparison of throughput observed before and after applying the solution ICM indicates that throughput of the network increases with the increased number of packets. It clearly shows that ICM successfully detects and prevents the MAC spoof DoS attack in an effective manner.

In Table 2, the throughput during attack and after applying TPF-LEP is illustrated. It is observed that the throughput decreases in the attack scenario and increases in TPF-LEP employment. When comparing performance of ICM with TPF-LEP, the ICM outperforms in throughput measure.

Evaluation of packet delivery ratio: Ratio of the data packets delivered to the destination is called packet delivery ratio. By simulating ICM and TPF-LEP in NS2, the packet delivery ratios were measured during

Table 1: Throughput during attack and after applying the ICM

During attack		After applying ICM	
No. of packets	Throughput	No. of packets	Throughput
203	509302	211	948839
216	629940	223	955726
228	441109	236	961825
241	643169	261	970802

Table 2: Throughput during attack and after applying TPF-LEP

During attack		After applying TPF-LEP	
No. of packets	Throughput	No. of packets	Throughput
201	636080	211	889146
226	568257	221	900704
238	542180	237	909950
263	469948	264	921508

Table 3: Packet delivery ratio during attack and after applying ICM

During attack		After applying ICM	
No. of packets	Packet delivery ratio (%)	No. of packets	Packet delivery ratio (%)
203	68.0	211	95
216	81.0	223	95
228	58.8	236	96
241	80.0	261	96

Table 4: Packet delivery ratio during attack and after applying TPF-LEP

During attack		After applying TPF-LEP	
No. of packets	Packet delivery ratio (%)	No. of packets	Packet delivery ratio (%)
201	69.6	211	86.20
226	61.5	221	84.60
238	58.0	237	80.59
263	50.0	264	74.24

Table 5: Packet drop during attack and after applying ICM

During attack		After applying ICM	
No. of packets	Packet drop	No. of packets	Packet drop
203	64	211	10
216	41	223	10
228	44	236	10
241	47	261	10

Table 6: Packet drop during attack and after applying TPF-LEP

During attack		After applying TPF-LEP	
No. of packets	Packet drop	No. of packets	Packet drop
201	61	211	29
226	87	221	34
238	99	237	46
263	131	264	68

the attack and after deploying the solution. The better performance is achieved when the ratio is higher.

The packet delivery ratios measured during the attack and after applying ICM is as shown in Table 3. It shows that there are fluctuations in the packet delivery ratio whereas Table 4 shows that the packet delivery ratio upsurges in peak even when the number of packets increases.

Evaluation of packet drop: The ICM performance overcomes TPF-LEP in case of packet drop. The lower the number of packets drop, the higher the performance. The Table 5 and 6 explain the packets drop rate in attack scenario and after applying the solution.

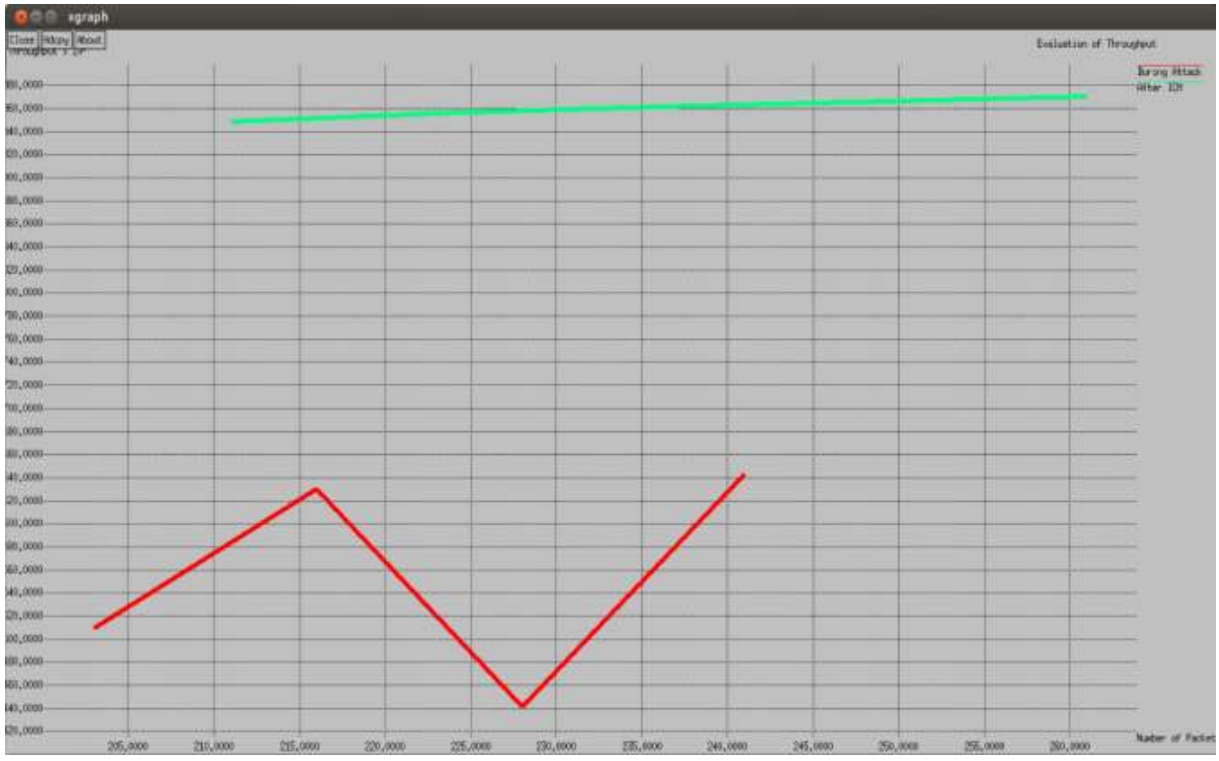

Fig. 3: Throughput during attack and after ICM

RESULTS AND DISCUSSION

This section discusses and compares the experimental result of ICM and TPF-LEP. From the experimental result, it is observed that ICM is an effective solution to defend against DoS attack than TPF-LEP.

Integrated central manager: The DoS attacks were simulated using NS2 for experiments. An average number of 233 packets were subjected for experimentation. The experimental results demonstrate that the performance of ICM is much better in detecting and preventing DoS attack. In order to validate the ICM performance, the Throughput, Packet Delivery Ratio and Packet Drop were measured. In Fig. 3 and 4, the graphs show that throughput and packet delivery ratio increases in a high rate and in the Fig. 5, the graph shows that the packet drop decreases. This shows the effectiveness of the proposed algorithm.

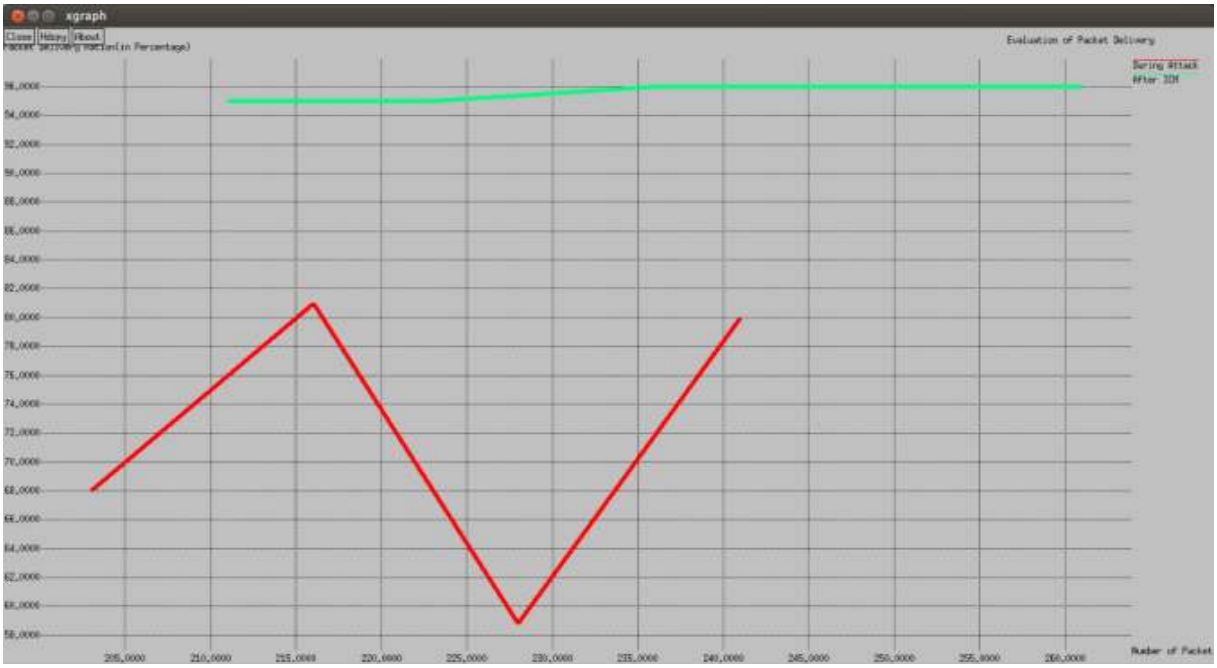

Fig. 4: Packet delivery during attack and after ICM

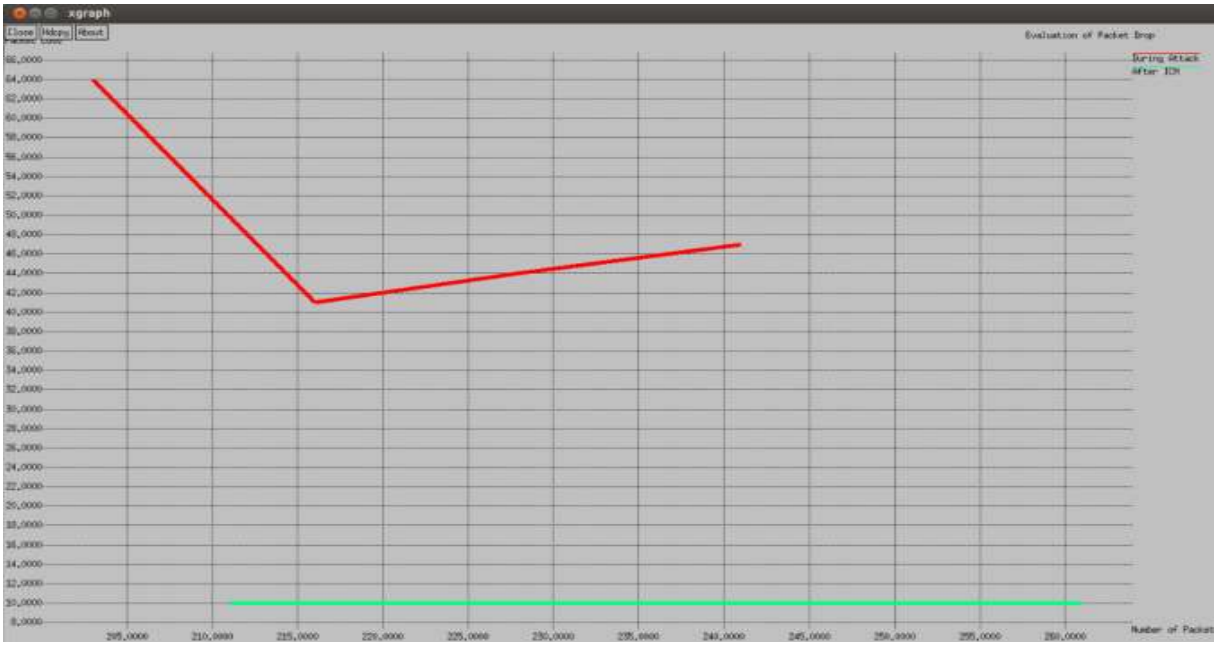

Fig. 5: Packet drop during attack and after ICM

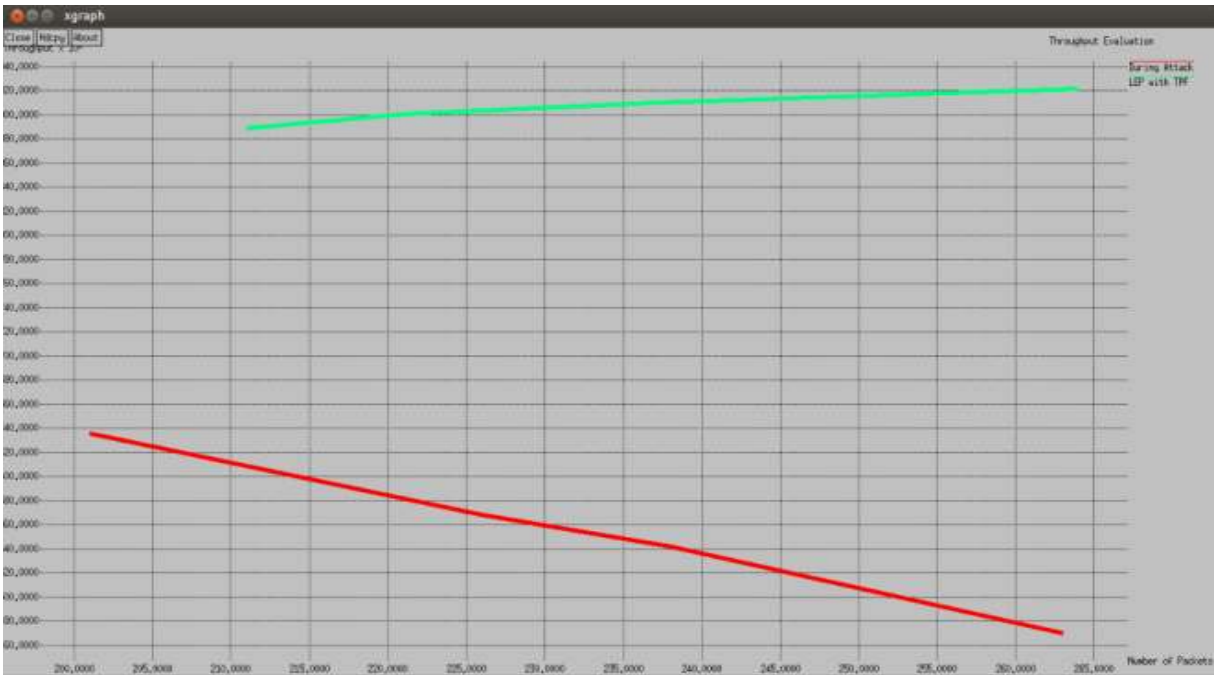

Fig. 6: Throughput during attack and after TPF-LEP

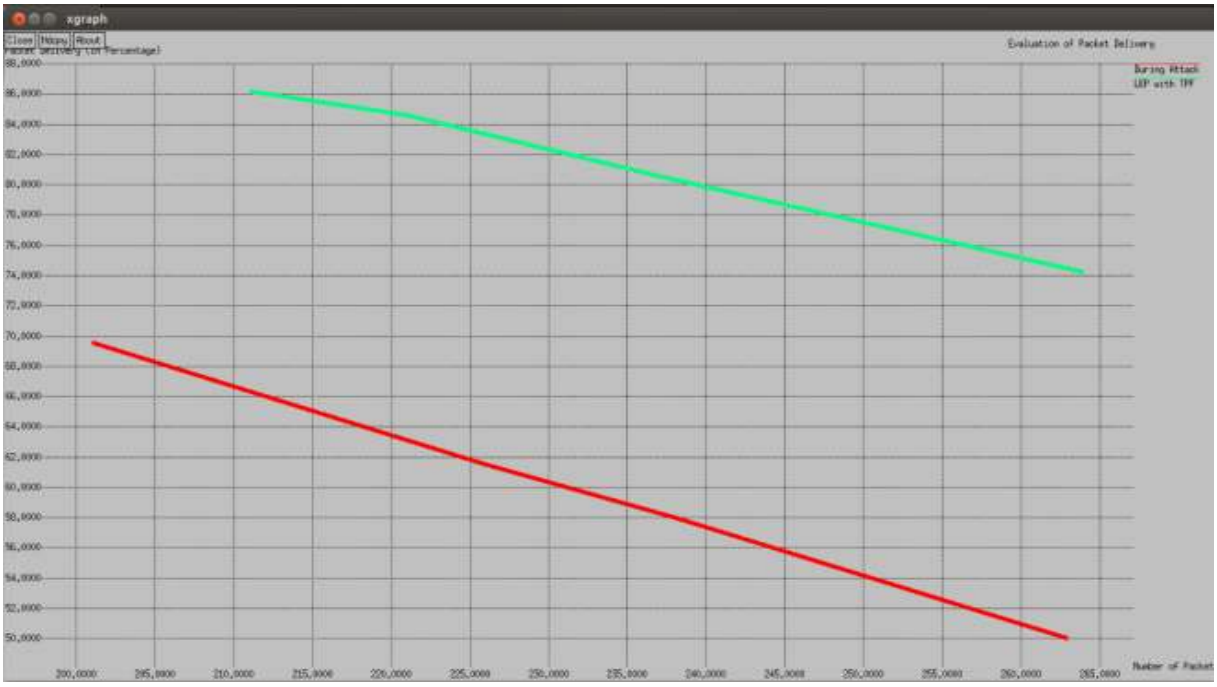

Fig. 7: Packet delivery during attack and after TPF-LEP

Traffic pattern filtering with letter envelop protocol: Throughput, Packet delivery ratio and Packet drop were measured in NS2 to evaluate the performance of TPF-LEP. The results show that TPF-LEP provides better solution but lesser than ICM. It provides reasonably considerable result when compared with attack scenario. Figure 6 and 7 show that the throughput and packet delivery ratio were increased when it is compared with attack scenario. In Fig. 8, the graph shows that the packet drop is reduced in a decent rate after applying the solution. During the attack, there is higher rate of packet drop whereas it decreased after applying the solution.

Performance comparison of ICM and TPF-LEP: The performance of ICM and TPF-LEP is evaluated

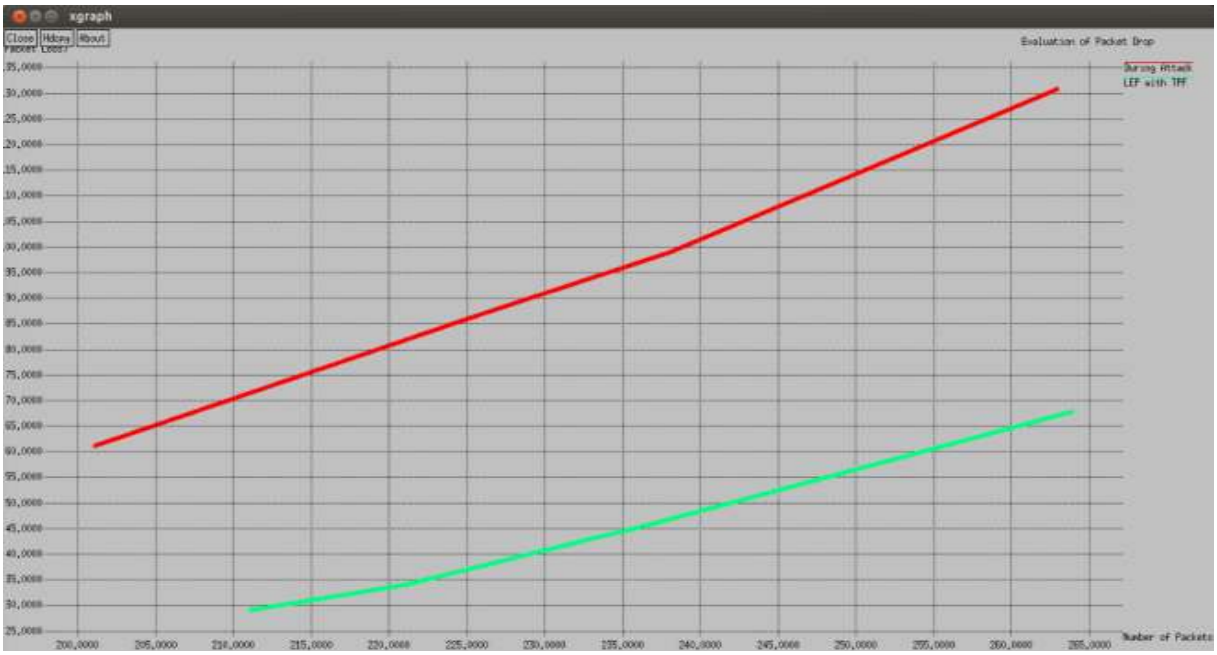

Fig. 8: Packet drop during attack and after TPF-LEP

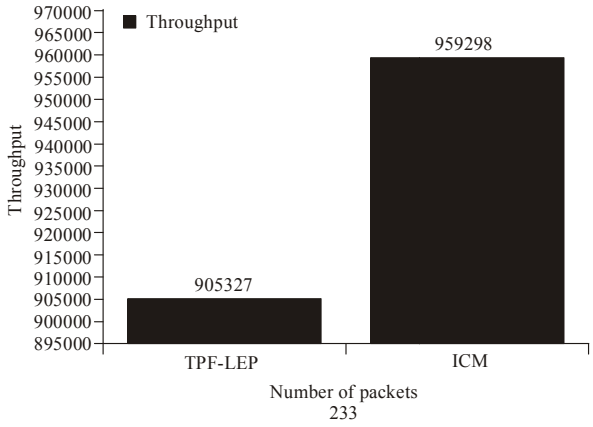

Fig. 9: Throughput comparison: ICM and TPF-LEP

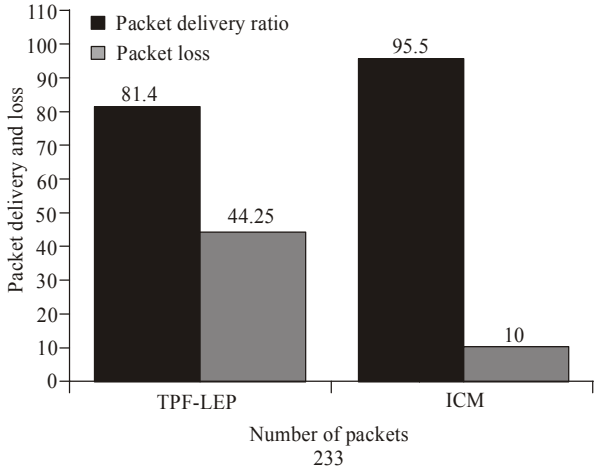

Fig. 10: Packet delivery and packet drop: ICM and TPF-LEP

here. To compare these two techniques, three parameters were taken for consideration such as throughput, packet delivery ratio and packet loss. ICM plays a better role in detecting and preventing DoS attack than TPF-LEP. TPF-LEP also detects and prevents the attacks in a reasonable manner but not effective like ICM. In Fig. 9, the graph shows that the throughput of ICM and TPF-LEP. X-axis represents the number of packets. Y-axis represents the throughput of the packet. By comparing these two mechanisms, performance of ICM is better in some extent. Figure 10 shows that Packet Delivery Ratio and Packet Drop. As expected, the ICM offers an effective solution than TPF-LEP.

CONCLUSION

Denial of Service attack is a dreadful attack which denies the legitimate user access from the network. The Integrated Central Manager (ICM) and Traffic Pattern Filtering with Letter Envelop Protocol (TPF-LEP) is one of the leading solutions to defend against start frame and logoff frame attack over AP and Client. These two solutions are proposed by us and are compared with each other to validate the performance. By comparing both the techniques, ICM is found to be an effective solution to prevent DoS in considerable extent. Consumption of bandwidth increased in ICM as a result of maintaining number of tables. To overcome the increased bandwidth consumption and to enhance the security mechanism of ICM, hybridization of multiple techniques has to be carried out for future study.

REFERENCES

Bellardo, J. and S. Savage, 2003. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. Proceedings of the USENIX Security Symposium. Washington, D.C.

Bicakci, K. and B. Tavli, 2009. Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks. Comput. Stand. Inter., 31: 931-941.

Cam-Winget, N., R. Housley, D. Wagner and J. Walker, 2003. Security flaws in 802.11 data link protocols. Commun. ACM, 46(5).

Durairaj, M., A. Persia and S. Sivagowry, 2013. A study of the existing solutions to prevent DoS attacks in wireless local area infrastructure networks. Int. J. Comput. Networks Secur., pp: 1123-1126.

Ferreri, F., M. Bernaschi and L. Valcamonici, 2008. Access points vulnerabilities to DoS attacks in 802.11 networks. Wirel. Netw., 14: 159-169.

Jalil, D., M. Mina, A. Abdul, G. Abdul and S. Shamala, 2008. An experimental evaluation of DoS attack and its impact on throughput of IEEE 802.11 wireless networks. Int. J. Comput. Sci. Network Secur., 8(8): 1-5.

Lashkari, A.H., M.M.S. Danesh and B. Samadi, 2009. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT). Beijing, China, pp: 48-52.

Nguyen, T.D., D Nguyen, B.N. Tran and H. Vu, 2008. A lightweight solution for defending against Deauthentication/disassociation attaks on 802.11 networks. Proceeding of 17th International Conference on Computer Communications and Networks (ICCCN '08), pp: 1-6.

Persia, A., S. Sivagowry, B. Vani and L. Arockiam, 2011. Inhibition of denial of service attacks in WLAN using the integrated central manager. Int. J. Comput. Appl., 29(8): 28-33.

Ping, D., 2007. Central manager: A solution to avoid denial of service attacks for wireless LANs. Int. J. Network Secur., 4(1): 35-44.

Radomir, P. and S. Dejan, 2007. A survey of wireless security. J. Comput. Inform. Technol., 15(3): 237-255.

Salem, M., A. Sarhan and M. Abu-Bakr, 2007. A DOS attack intrusion detection and inhibition technique for wireless computer networks. Proceeding of the International Congress for Global Science and Technology-CSIR, 7(1): 17-24.

Shamala, S., M. Mina, A. Abdul, G. Abdul and D. Jalil, 2009. Vulnerability analysis of Extensible Authentication Protocol (EAP) DoS attack over wireless networks. ICGST Int. J. Comput. Network Internet Res. CNIR, 9(1): 39-46.

Sivagowry, S., A. Persia, B. Vani and L. Arockiam, 2012. A Solution to prevent resource flooding attacks in 802.11 WLAN. Proceedings of the International Conference on Recent Trends in Computing, Communication and Information Technologies, pp: 607-616.

Stanley, W., 2003. The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards. GSEC Practical v1.4b.

The ns Manual (formerly ns Notes and Documentation), 2009. The VINT Project a Collaboration between researchers at UC Berkeley, LBL, USC/ISI and Xerox PARC. Kevin Fall hkfall@ee.lbl.govi, Editor Kannan Varadhan hkannan@catarina.usc. edui, Editor, May 9, 2010, pp: 73.