Theoretical Framework of the Algorithm to Thwart MAC Spoofing DoS Attack in Wireless Local Area Infrastructure Network

M. Durairaj and A. Persia

Abstract A major threat in wireless local area infrastructure network is denial-of-service (DoS) attacks. It makes the resources unavailable for its anticipated user which can be accomplished through spoofing legitimate client/AP's medium access control (MAC) address. Less protection in MAC address led to get easy spoofing. Since the management frame is unencrypted, adversary sends the management frame to the victim using spoofed MAC address. This prerequisite goaded to offer an effective prevention mechanism for DoS attack. Even though several preventing mechanisms are available, no one provides complete solution in preventing MAC layer DoS attack. This paper proposes a theoretical framework of threshold value (ThreV) algorithm, which is based on setting up ThreV for the management frame, to effectively address this issue.

Keywords Denial of service · Medium access control · Spoofed MAC address · Threshold value algorithm · Wired equivalent protocol

1 Introduction

Security issues in wireless network increases as popularity increases. In wireless local area network (WLAN) infrastructure architecture, communication takes place with the help of access point (AP). In general, 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. This makes the intruders to easily enter into the network and do malicious harm to the network.

M. Durairaj · A. Persia (✉)
School of Computer Science, Engineering and Applications, Bharathidasan University, Tiruchirappalli, India
e-mail: persia_paradise@yahoo.co.in

M. Durairaj
e-mail: durairajum@gmail.com

L.P. Suresh et al. (eds.), *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Advances in Intelligent Systems and Computing 324,
DOI 10.1007/978-81-322-2126-5_12

There are number of attacks possible in infrastructure network [1]. Many people are not aware of the denial-of-service (DoS) attack [2] on their own network. Sending continuous stream of forgery frames by an attacker can easily slow down the network, which prevents the availability for authenticated clients. Several protocols were developed to protect wireless network. Everyone has security deficiencies. 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 802.1x 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 [3]. Currently, as literatures say there are no effective IEEE-approved ways to solve the security hole. This paper proposes a theoretical framework of ThreV algorithm to address the issues of preventing attacks in an infrastructure network.

In this paper, Sect. 2 presents the background review and related work, which are to understand the paper. Section 3 explains the architecture of the proposed technique and experimentations carried out. Section 4 presents the theoretical framework of ThreV algorithm which is to prevent attacks in an infrastructure network. Section 5 concludes the paper.

2 Related Work

To detect DoS attacks in its early stages before it reaches the victim using stateful and stateless signature, John Haggerty et al. propose Distributed DoS Detection Mechanism (DiDDeM). It provides a natural way of tracking the attack sources without requiring the use of any trace-back techniques. The DiDDeM offers a distributed and scalable approach to attack responses [4].

Samra et al. propose an algorithm to enhance the performance of the correlation of two wireless intrusion detection techniques (WIDTs) such as Received Signal Strength Detection Technique (RSSDT) and Round Trip Time Detection Technique (RTTDT) for detecting medium access control (MAC) spoofing DoS attacks. The experiments were demonstrated with the absence of false negatives and low number of false positives [5].

Ding 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 WLAN. This proposed solution is evaluated by five different DoS attacks such as large number of association requests (LASO), EAP failure, EAP start, EAPOL logoff, and MAC disassociation [6].

Sheng et al. propose Gaussian Mixture Modeling (GMM) for Received Signal Strength (RSS) profiling to detect spoofing attacks using multiple air monitors (AMs) which sniffs wireless traffic passively without the cooperation of APs and clients.

In this method, accurate detection of MAC spoof is obtained using GMM mechanism [7].

Saelim et al. provide a MAC spoofing detection algorithm in IEEE802.11 networks. To differentiate an attacker station from a genuine station, the proposed algorithm utilizes physical layer convergence protocol (PLCP) header of IEEE 802.11 frames. Experimental results provide cent percentage of MAC spoofing DoS detection when two monitoring stations are located at an appropriate location [8].

3 Proposed Solution to Prevent DoS Attack

Many security techniques were introduced to prevent DoS attacks; still, effective solution for DoS attack is needed. In this paper, multiple techniques are introduced to address the drawback of existing solutions.

Hybridization of multiple detection techniques is proposed to develop as an effective tool for preventing DoS attack in an infrastructure network. The detection technique called as computerized monitoring system (CMS) [9] is an integration of three algorithms which are ThreV, alternative numbering mechanism (ANM), and traffic pattern filtering and letter envelop protocol (TPatLetEn). The architectural frame work of the proposed model is illustrated in Fig. 1. Experimentation on the DoS attacks consists of two stages, i.e., *evaluation of attack* and the *preventive mechanism.* Effectiveness of the attacks is evaluated by measuring delay time, packet loss and throughput. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet delay time refers to the time taken for a packet to transmit across a network from source to destination. Throughput is the average rate of successful message delivery over a communication channel. It is usually measured in bits per seconds and sometimes in data packets per second. As a preventing mechanism, integration of threshold value (ThreV), ANM, and Traffic Pattern Filtering with (TPatLetEn) is used to detect and block DoS attack.

3.1 Computerized Monitoring System (CMS)

CMS integrates three detection techniques such as ThreV, ANM, and TPatLetEn. It maintains an intruder table (InT) contains MAC address of intruders, and basic identity check (BIC) table contains MAC addresses of WLAN users. When client sends a request to AP, it first checks in InT whether it has particular MAC address or not. If address is presented, the request is considered as spoofing attack. If not, the request goes to BIC for basic check. If the MAC address is not presented in the table, CMS blocks the user from further communication, whereas if the user's identity was found in BIC, the ThreV mechanism takes over this. After this process, the request goes to ANM and TPatLetEn. When above three conditions are satisfied,

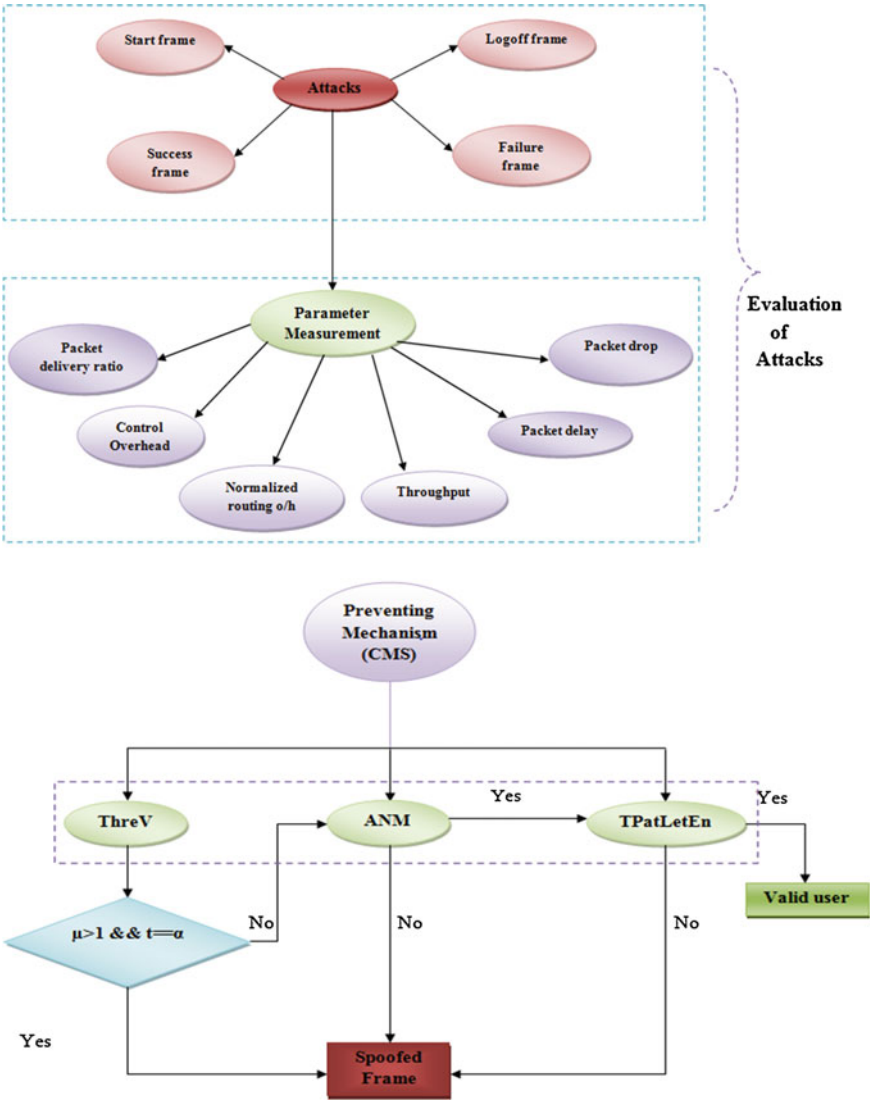

Fig. 1 Architecture of proposed model

CMS allows the AP/Client to start their communication. If any one of the prescribed solutions fails to satisfy, it can be considered as a spoofing attack. The operations of CMS are as illustrated in Fig. 2.

Basic Identity Check (**BIC**). BIC table contains MAC address of WLAN users who are all in the network. Once the request is processed, it checks in BIC whether the client/AP's MAC address presents or not. If not, it blocks the sender and stores

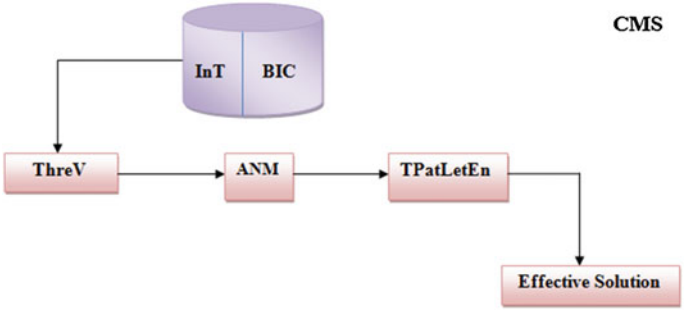

Fig. 2 Operation of CMS

its original MAC address in InT. If the MAC is presented, it redirected to ThreV algorithm to detect the MAC spoofing attack for effective detection of DoS.

Intruder Table (**InT**). Hackers are identified by the CMS, and it blocks the intruders, then find out the intruders MAC address, and stores its InT which stores the MAC address of the intruder.

Threshold Value (**ThreV**). By receiving login request from client, AP should respond by sending response message. Here, the threshold is assigned as 4 ms. AP should response to client at 4 ms. If AP receives more than one request within the certain ThreV, this request is considered as a spoofed frame (SF). In the case of AP, if client receives response message from AP before the threshold stage, it will be taken as a SF. There are some cases where AP cannot respond to client within threshold, and it may take more than 4 ms as a result of traffic overload. In this case, it cannot be assumed as an attacker. So the ANM detection technique will be used.

Alternative Numbering Mechanism (**ANM**). ANM is used instead of sequence number field. Odd number should be given for this such as 1, 3, 5, 7, 9, …, n. Sequence number can be easily tracked by hacker. If intruder randomly guesses the sequence number, attacks can be launched in a simple manner. Maintaining ANM, hackers cannot assume the exact sequence number which presents in the numbering field. It is difficult for an intruder to assume the apt ANM to make MAC spoofing attack. If it finds out the exact ANM of client/AP, it should be redirected to TPatLetEn.

Traffic Patter Filtering with Letter Envelop Protocol (**TPatLetEn**). The client randomly generates two prime numbers $p1$ and $q1$ and then computes $N1 = p1 * q1$. In the same way, AP generates $p2$, $q2$ and computes $N2$ [10].

- 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 the $p1$. The AP will compute $p1/N1$ and finds whether it corresponds with the $N1$ which was already stored.

- If it is correct, the client will be disconnected. Otherwise, the frame will be rejected assuming that it is from the hacker.

Similar procedure is followed for AP when it wants to disconnect from the 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 the combination of traffic pattern filtering (TPF) with LEP where AP uses TPF along with LEP. The TPF works as follows:

- If a request is received more than five times at a particular time from a client, it infers that the request is from the hacker and ignores it.
- Since the hacker continuously sends request, AP is unable to process the request from the legitimate clients.

4 Preventing DoS Attack Using ThreV

ThreV is a mechanism which thwarts DoS attack in an infrastructure network. This section describes that how the attacks are took place and the way ThreV prevents the intruders.

4.1 ThreV in EAP Start Frame Attack

Client sends a start frame request to AP. After AP received the request, CMS checks the client's identity using InT. If the client's MAC address is presented in InT, it reject and blocks the intruder. If not, BIC takes over this packet which stores all the WLAN user's MAC addresses. If the client's MAC is presented, then ThreV process the request. Here, ThreV is set to 4 ms, i.e., ThreV(α) = 4 ms. At the 4th ms, the transmitted packet (μ) will be calculated. After calculating μ, the requisite conditions will be checked.

If the μ is greater than one within the threshold time (α), then it considered as a SF. If μ is equal to 1 but it exceeds α, this will be redirected to second prevention algorithm which is called ANM. This is not a simple process considering SF, because heavy traffic may be a reason for delayed packet. If μ is equal to one at threshold time α, this will be redirected to ANM which provides additional security to defend against DoS attacks. After subjected to ANM and TPatLetEn (ANM and TPatLetEn is not covered in this paper), CMS will decide whether it responds back to the user with yes or no. If it replies with yes, the communication between AP and client gets starts. The user will be blocked when any of the mechanisms are not satisfy the conditions and spoofing the intruders' original MAC addresses and store it in InT.

4.2 ThreV in EAPOL Logoff Frame Attack

During the communication period, when AP receives logoff request from client, it sends logoff packet to client by asking whether client want to logoff or not. If a client replies to AP with α and continue logoff message, ANM and TPatLetEn take control over the packet. If μ is greater than one within α period, this is considered as SF, and CMS spoofs the attackers' original MAC address and stores it in InT.

4.3 ThreV in EAP Success Frame Attack

After a login request is evaluated by three algorithms and find that the request is from legitimate, then it proceed with yes or no message to AP for further communication. If success frame μ is greater than two within its α period, this is considered as spoofing attack then the attackers MAC address is spoofed and stored it in InT. If μ is equal to one, but it exceeds α, this will automatically redirected to ANM and then TPatLetEn. This delay may happen due to traffic overhead which is a reason for not blocking them. If μ is equal to one at α, this will also be redirected to next prevention algorithm which enhances the security by hybridizing multiple techniques.

4.4 ThreV in EAP Failure Frame Attack

In some cases, the AP responds to client with failure message which represents congestion overhead in an infrastructure network. By sending failure frame, If μ is greater than two within its α period, this will be considered as spoofing attack and then the attackers' MAC address is spoofed and stored it in InT. If μ is equal to two but exceeds α, this will be automatically redirected to ANM and then TPatLetEn. This delay may happen due to traffic overhead which is a reason for not blocking them. If μ is equal to two at α, the next prevention algorithm which enhances the security by using hybridizing multiple techniques will be exploited. Sample ThreV algorithm to detect Start frame attack target as client is as follows.

Algorithm: ThreV

1. *initialize α = 4 ms, μ = 1, t = 0*
2. *if μ ==1 && t < α then*
3. *Reject the packet, spoof and store it in Intruder Table*
4. *if μ ==1 && t > α then*
5. *redirect it to ANM*
6. *if μ > 1 && t == α then*
7. *Reject the packet, spoof and store it in intruder Table*

8. *if* μ ==1 && t == α *then*
9. *redirect it to ANM*

The above algorithm describes that by receiving login request from client, AP should respond back by sending response message. Here, the threshold is assigned as 4 ms. AP should response to client at 4 ms. If AP receives more than one request within the certain ThreV, this request is considered as a SF. In the case of AP, if client receives response message from AP before the threshold, it will also be taken as a SF. There are some cases where AP cannot respond to client within threshold. It may take more than 4 ms because of traffic overload. In this case, it cannot be assumed as an attacker. So the ANM detection techniques will be used.

5 Conclusion

WLAN offers increased wireless access to the client with the help of AP. Since the popularity of wireless increases, the security issues also increases as well. DoS is a great threat in wireless infrastructure network which is an immense challenge to defend against it. Theoretical framework of ThreV algorithm is proposed in this paper to detect MAC spoofing DoS attack. This framework would provide a better solution for preventing the intruder's attack on WLAN. As a future work, ThreV algorithm is to be deployed in NS2 [11] and the throughput, drop rate, control overhead, end-to-end delay, and jitter will be measured, and optimization of the parameters will be proved with the aid of results. This paper suggests CMS is an effective solution for detecting and preventing MAC spoof attack in wireless local area infrastructure network.

References

1. A. Celik, P. Ding, in *Improving the Security of Wireless LANs by Managing 802.1x Disassociation*. Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC04) (2004), 53–58
2. J. Haggerty, Q. Shi, M. Merabti, Early detection and prevention of denial-of- service attacks: a novel mechanism with propagated traced-back attack blocking. IEEE J. Sel. Areas Commun. **23**(10), 1994–2002 (2005)
3. A.A. samra, R. Abed, Enhancement of passive MAC spoofing detection techniques. Int. J. Adv. Comput. Sci. Appl. **1**(5) (2010)
4. P. Ding, A solution to avoid denial of service attacks for wireless LANs. Int. J. Netw. Secur. **4** (1), 35–44 (2007)
5. Y. Sheng, K. Tan, G. Chen, D. Kotz, A. Cambell, in *Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength*. The 27th Conference on Computer Communications IEEE (2008)
6. S. Sivagowry, A. Persia, B. Vani, L. Arockiam, in *A Solution to Prevent Resource Flooding Attacks in 802.11 WLAN*. Lecture Notes in Computer Science Communication in Computer and Information Science (CCIS 269) (2012), pp. 607–616

7. The ns Manual, the VINT Project (2009). http://www.scribd.com/doc/52291274/Network-Simulator-2-Manual
8. T. Saelim, P. Chumchu, C. Sriklauy, A new MAC address spoofing detection algorithm using PLCP header. IEEE ICOIN. 48–53 (2011)
9. A. Persia, S. Sivagowry, L. Arockiam, B. Vani, Inhibition of denial of service attack in WLAN using the integrated central manager. Int. J. Comput. Appl. **29**(8), 28–33 (2011)
10. A. Gupta, M. Garg, DoS Attacks on IEEE 802.11 Wireless Networks and its Proposed Solutions. Soc. Sci. Res. Netw. (2010)
11. A. Persia, S. Sivagowry, M. Durairaj, Study of thwarting DoS attacks by detecting MAC spoof in WLAN infrastructure network. IEEE Xplore 264–268 (2012)