FRAMEWORK TO DETECT AND PREVENT MEDIUM ACCESS CONTROL LAYER DENIAL OF SERVICE ATTACKS IN WLAN

L. Arockiam[1]
Associate Prof., Dept. of Computer Science,
St. Joseph's College, TN, India,
larockiam@yahoo.co.in.

B. Vani[2],
Assistant Prof., Dept. of Computer Science,
Srimad Andavan Arts and Science College, TN, India,
balasundaramvani@yahoo.co.in

***Abstract*— Wireless Local Area Networks are susceptible to Denial of Service (DoS) attacks due to the broadcasting media of wireless networks. Management frames that carry the MAC address of the source are vulnerable to DoS attacks since they are sent without encryption. Among the different kinds of MAC layer DoS attacks, deauthentication/disassociation are found to be dreadful since they disconnect the user from the network. This paper focuses on the detection and prevention of different types of MAC layer DoS attacks. A framework with three proposed MAC layer security algorithms is designed to prevent the MAC layer DoS attacks. The various features of the proposed algorithms are compared with the existing mechanisms and the results are validated with a network simulator. All the proposed algorithms increase the throughput value to a greater extent. The recovery time and packet resend rates are proved to be minimized with the proposed algorithms. The proposed framework is a cost effective one and need no firmware upgradation when deployed in the WLAN infrastructure networks.**

Keywords: Denial of Service (DoS), Deauthentication, Disassociation, MAC Spoofing, Management frames etc.

I. INTRODUCTION

IEEE 802.11 has proposed many security extensions to secure wireless networks from malicious attacks that are possible due to the broadcast nature of wireless access. But these extensions deal only with vulnerabilities related to unauthorized access and confidentiality issues [1]. It is important to consider the issue of availability which is one of the security requirements [2]. Denial of Service (DoS) attacks is attacks against availability which attempts to prevent the legitimate users from accessing the network [3]. There are more number of recent research works focused on the security protocols and authentication mechanisms [4]. But IEEE 802.11network is still vulnerable to DoS because, these attacks take place before the security protocols are evoked [5]. WLAN infrastructure networks are connected through a central device called Access Points (AP). DoS attacks may target different layers of the Open System Interconnection (OSI) model. They are Application layer, Transport layer, Network layer, Media Access Control layer and Physical layer [6]. IEEE 802.11 Medium Access Control (MAC) layer communicates through the three types of messages namely, management, data and control frames. The management frames are sent unencrypted and they are susceptible to DoS attacks more frequently [7]. In order to secure these management frames, IEEE is in the process of standardizing IEEE 802.11w standard. The control frames are also susceptible to DoS attacks as discussed by the authors Sushma Myneni et al. [8]. Most of the research works investigate on how these DoS attacks are carried out rather than providing solutions to this problem.

IEEE 802.11i ratified that security of the wireless network has been improved by using Cipher Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP uses Advanced Encryption Standard (AES) as opposed to the RC4 cipher found in the implementations of Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol (TKIP). But this protection offered by 802.11i applies to data frames only and does not provide any protection to the management frames [9]. These management frames are insecure and are susceptible to DoS attacks [10]. An adversary can easily forge the management frames that are sent in clear by spoofing the MAC address with the help of the tools such as Airjack and WLAN-jack. All the WLAN users could be disconnected by broadcasting the deauthentication/disassociation frames by setting the destination address as FF:FF:FF:FF:FF:FF instead of directing them to one target which means that all the supplicants are disconnected by just sending one deauthentication frame [11].

This paper is organized as follows: Section 2 describes the related works on MAC layer DoS attacks and their proposed solutions. Section 3 expands the security framework proposed for WLAN infrastructure networks. The three proposed algorithms namely, IDM DoS, LEPT DoS and MAC SDP DoS are explained in the following subsections. . Section 4 elaborates the findings and interpretations of the proposed framework with three security algorithms compared with the existing methods. Section 5 discusses the conclusion and future works.

II. RELATED WORKS

Some recent research works have analyzed this vulnerability and proposed few protective measures to them. Bellardo et al. [12] suggested a mechanism which delays the

execution of deauthentication/ disassociation requests to 5 – 10 seconds to see whether any data message is coming after that. The other methods suggest authentication of these two management frames namely, deauthentication and disassociation [13] [14].

A usage of dynamic MAC address is proposed to prevent MAC spoofing DoS attacks [15]. Li Wang et al. [16] proposed a 3-way handshake mechanism to prevent memory DoS attacks by generating nonce.

Rango et al. [17] proposed an extended resource aware variant approach to get a tradeoff between memory and CPU exhaustion. But none of them provide a preventive mechanism to the MAC layer deauthentication/disassociation attacks. Table 1 lists down the various types of DoS attacks and their proposed solutions as discussed by the authors Taimur Farooq et al. [18].

Table 1. Types of Dos Attacks and Countermeasures

Attacks	Target	Existing Countermeasures
Probe Request Attack	Access Point(AP)	Signal Print
Authentication Request Attack	AP	Signal Print, Client Puzzle
Deauthentication Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Association Request Flood	AP	Signal Print
Disassociation Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Virtual Carrier Sense Attacks	Medium Access	Explainability of Collision, Spatial Retreats
Sleeping Node Attack	Station and AP	Limiting Duration Field Value, Signal Print, MAC Spoof Detection

Based on the existing research works on MAC layer DoS attacks, the proposed work focuses on the detection and prevention of deauthentication/disassociation and MAC spoofing DoS attacks. Since the deauthentication is found to be the most dreadful attack, there is an immediate requirement for a complete algorithm to detect and prevent the MAC layer DoS attacks [19]. This paper develops a framework which comprises of three proposed algorithms to detect and prevent the MAC layer DoS attacks in WLAN.

II. FRAMEWORK TO SECURE WLAN USERS FROM MAC LAYER DOS ATTACKS

There are many types of wireless DoS attacks that an attacker can carry out against an organization's wireless network. DoS attack targets different layers of the Open System Interconnection (OSI) model. They are Application layer -7, Transport layer -4, Network layer -3, Media Access Control layer -2 and Physical layer -1. The wireless clients as well as the AP become the target for DoS attacks [20]. The following sections describe briefly about the DoS attacks launched at different layers:

- Application Layer (7) DoS attacks

The application layer DoS attacks are carried out on a wired or a wireless network. The intruders launch these attacks by sending large amount of legitimate requests to an application. A Hyper Text Transfer Protocol (HTTP) flood attack makes thousands of page requests to a web server which exhausts all of the server's processing capability. In this attack, intruder sends a SYN packet, and the target system responds with SYN ACK which stands for synchronization acknowledgement. The three way handshake with an ACK packet is completed by the attacker and then issues an HTTP GET request for a common page on the target system. This process causes a very high computational load on the target system and may result in the degradation of the wireless network to a complete loss of availability of application. Examples of these sorts of attacks are MyDoom worm that targeted thousands of sites by sending 64 requests every second from every infected system [21].

- Transport layer (4) attacks

Transport layer DoS attacks are launched by sending too many connection requests to a target host. This attack is based on the Internet Protocol (IP) spoofing techniques and is targeted on the operating system of victim. The TCP SYN flood is the example for this kind of attack. During the TCP connection, the client sends a SYN packet from a specific port to a server. The server sends back a SYN ACK and waits for an ACK acknowledgement before the connection is established. Whenever the SYN flood attack made, attackers send huge amounts of SYN packets

to the target system [22]. The target system attempts to complete the session by sending back SYN ACK packets which will never be acknowledged or reset. The target system attempts to make a connection and this attempted connection are removed from the queue after the connection establishment timer expires. The three way handshake is never completed and the victim station does not clear the queue before receiving new SYN requests. This may result in the degradation of the wireless network.

- Network layer (3) attacks

Network layer DoS attack is achieved by sending a large amount of data to a wireless network. This attack targets the wireless infrastructure network of the victim. If the intruder spoofs source IP address, all the available bandwidth is consumed and the legitimate users being unable to access wireless services [23].

- Media Access Control (MAC) layer (2) DoS attacks

In MAC layer DoS attacks, intruder spoofs the MAC address of AP or the client. The recipient of these spoofed frames processes them unknowingly whether they are legitimate or illegitimate requests. The different types of MAC layer attacks are masquerading, resource flooding and media access DoS attacks [24].

From the various layers of DoS attacks as discussed above, this research work is focused on the MAC layer DoS attacks specifically. The MAC layer DoS attacks are possible due to the unencrypted transmission of management frames that carries MAC address of the source. With the help of available tools, intruder simply makes MAC layer DoS attacks either on the client or AP. MAC layer DoS attacks are categorized into masquerading, resource flooding and media access attacks. In order to detect and prevent the various kinds of MAC layer DoS attacks in a WLAN infrastructure environment, this research work proposes three enhanced security algorithms namely, IDM DoS, LEPT DoS and MAC SDP DoS. In an infrastructure network, all the clients are connected with one or more APs. Both the client and AP are susceptible to MAC layer DoS attacks due to the unencrypted management frames that carry the MAC address of the sources.

First, Intrusion Detector and Manager for DoS, IDM DoS algorithm is proposed to detect and prevent the masquerading DoS attacks. The deauthentication, disassociation and power saving attacks come under the masquerading DoS attacks.

Second, Letter Envelop Protocol with Traffic pattern filtering for DoS, LEPT DoS algorithm is proposed for preventing the resource flooding DoS attacks which includes probe request flooding, authentication/deauthentication request flooding and association/disassociation flooding attacks.

Third, MAC SDP DoS algorithm is proposed to detect and prevent deauthentication/disassociation and MAC spoofing DoS attacks.

A framework is proposed by integrating these three algorithms which are used to detect and prevent MAC layer DoS attacks. The proposed framework is depicted in Figure 1.

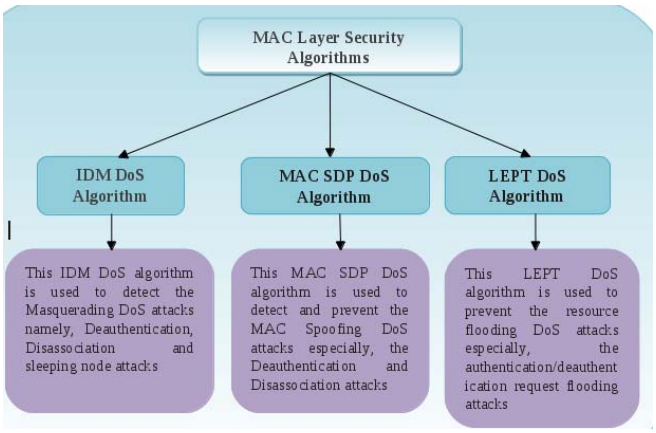

Figure 1. Framework with Security Algorithms

This framework could be deployed in the AP which acts as a central device through which all the other clients are communicated with one another. MAC layer DoS attacks are launched whenever the MAC spoofing attacks are made. These attacks are possible by spoofing the MAC address that is carried by the management frames which are sent unencrypted. This framework is activated whenever login and logout requests are made by the users in the particular WLAN environment. Depending on the type of requests received, the algorithms are activated to detect and prevent MAC layer DoS attacks.

V. FINDINGS AND INTERPRETATIONS

The three proposed algorithms namely, IDM DoS, LEPT DoS and MAC SDP DoS are implemented in a simulation environment with the NS2 tool. NS2 is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. The experimental results are compared with the existing mechanisms. Experimental results of each algorithm compared with the existing mechanisms are listed below:

A. IDM DoS algorithm

IDM DoS algorithm is proposed to detect and prevent the masquerading DoS attacks. With the existing central manager method, it is observed that the DoS attack is reduced [25]. This method does not maintain the history of the intruders since it only detects them. Whenever authentication/ deauthentication requests are made, the MAC address is verified and this method takes more computation and time. In the case of existing Intruder Data Base (IDB) method, it maintains a database which contains all the MAC addresses of authenticated clients and intruders. The Probability of Denied Service (PDS) is

decreased after implementing IDB. The authentication process is based on an open shared key authentication, since the key is open to all; intruder easily finds the key. IDB does not prevent the DoS attacks when the intruder enters with a MAC address which is not yet installed in the database.

To overcome the drawback of these existing methods, the IDM DoS algorithm is proposed and validated with NS2, a network simulator tool and with a Java procedure. After implementing the proposed algorithm, intruder finds difficulty in making the DoS attacks, because the client authentication is based on the tables maintained by IDM DoS algorithm. Hence, IDM DoS easily identifies the intruders and prevents them from entering into the network. The throughput, which is the measure of number of packets transferred per unit time, is increased as compared to the existing methods. The packet flow rates are proved to be increased while using this algorithm.

B. LEPT DoS Algorithm

Second, LEPT DoS algorithm is proposed to prevent resource flooding DoS attacks by generating prime numbers that are exchanged between the user and the AP along with Traffic Pattern Filtering (TPF). The existing algorithm LEP at association level can prevent request flooding attacks. But attacker launches the attack at the authentication level itself. Since the authentication process is carried out with "Open Shared" or "Pre Shared key" authentication, it has no secure authentication. If the communication is stopped or hacked at the authentication level, the request flooding attacks are very easy to make. The existing algorithm is effective against farewell attacks, but works only with specific platforms like Atheros chipset running on Linux and needs hardware upgradation as described by the authors [26]. To overcome such disadvantage, LEPT is used at the authentication level itself along with TPF and needs no hardware upgradation. So, from the initial state itself, the LEPT starts functioning and the network is secured from flooding DoS attacks. The throughput is increased with LEPT DoS algorithm which is validated by NS2 tool.

C. MAC SDP DoS Algorithm

Third, MAC SDP DoS algorithm is proposed to detect and prevent the MAC spoofing DoS attacks. This algorithm is validated with NS2 simulator. The bandwidth and throughput values reach zero during the deauthentication/disassociation DoS attacks as discussed in the existing algorithms [27]. The existing algorithms only detect deauthentication/disassociation and MAC address spoofing. The existing works do not provide any preventive measures for these DoS attacks. The proposed algorithm MAC SDP for DoS not only used to detect but also used to prevent deauthentication/disassociation and MAC spoofing DoS attacks with an exchange of passkey values. This algorithm prevents deauthentication/disassociation and MAC spoofing DoS attacks from entering into the WLAN infrastructure environment with an authentication mechanism.

The procedure of MAC SDP DoS algorithm is explained below:

[1] First, the connectivity is initialized and the passkey is sent to the receiver. The passkey is an 8 bit key, generated in random using the current timestamp as the seed value. The passkey is stored by both the sender and the receiver.

[2] When an attack occurs, this passkey helps in faster connection establishment, hence reduces the need for redundant retransmissions.

[3] Threshold limits for deauthentication and flooding attacks are set by the user. This value determines when the system is to be intimated as being under attack. Setting these threshold limits to an optimal value is mandatory for proper functioning of a system. Setting it to a high value might lead to longer attacks before detection and blocking, while setting it to a low value might lead to frequent blockages, which has the probability of interrupting smooth transmissions.

[4] Deauthentication attack occurrences and flooding attack occurrences are maintained in each system. When every attack is detected, these counters are incremented and if the values of these counters go beyond the specified threshold value, then the user is given a warning about the deauthentication attack and the countermeasures for facing the attack are performed.

[5] The beginning time of transmission is recorded and the network is monitored for packets. The network packets are monitored at specified time intervals and checked for signs of attack. If a packet arrives, its frame type and subtype are checked. If the value of type is 0 and sub type comes out to be 12 then the frame would be identified as the deauthentication frame. If a deauthentication frame is encountered, then the counters are incremented accordingly.

[6] The time difference Δ is calculated. Δ is the difference between the current time and the value of timer stored earlier (time of beginning the transmission). The number of deauthentication frames per unit time is calculated. The deauthentication count that was maintained is divided by Δ and this value gives the number of deauthentication frames per unit time. If this value is found to be greater than the flooding threshold specified by the user, an attack occurrence is registered.

[7] If the value of counter for attack occurrences is greater than the threshold specified for the attack then it has been notified as the detection of the deauthentication attack. This process is periodically performed to ensure that all attacks get recorded in the system and no

flooding attack is missed. If the counter value reaches the threshold, then it is assumed that the particular source is launching a DoS attack on the system. So the source is blocked.

[8] After this process, the system checks for data frames from the same source. If data frames arrive, then harvest the MAC address and check for the authenticity of the client. If this comes out to be of legitimate client, then the attack is considered to have been launched by spoofing MAC.

[9] A spoofing attack in general affects both the original sender and the receiver. The receiver usually blocks all legitimate messages from the sender suspecting an attack. This leads to the need for a complete handshake mechanism for proving the legitimacy of the sender. This becomes quite time consuming. The proposed MAC SDP DoS algorithm provides a way to solve this issue with passkeys.

[10] Once a spoofing attack has been detected, the receiver requests for the passkey from the sender. The received passkey is cross verified with the available passkey. After verifying the received passkey's authenticity, the receiver sends the last found legitimate packet's sequence number. The receiving system sends the packets starting from that sequence number.

[11] MAC SDP DoS algorithm has been found to be reducing the need for unnecessary packet re-transmission by providing the sequence number. Hence, there is no need for transmitting packets that had been received by the system. These packets are usually discarded in the receiving side. This leads to unnecessary power consumption. Further, with a single passkey for authenticity verification, it reduces the need for a complete handshake mechanism. Hence, MAC SDP DoS algorithm reduces unnecessary retransmissions and improves WLAN performance.

With this algorithm, the packet drop rate is decreased and the performance of the WLAN is increased by improving the throughput value. The packet resend rate is also reduced to zero compared to the existing methods. Secondly, the recovery time is reduced as compared to the existing MAC spoof detection algorithm and the packet resend rates are found to be vanished. The recovery time is called the time taken to resume the communication after preventing the DoS attack. This validation show that the MAC SDP DoS algorithm works well in preventing the MAC layer DoS attacks that are launched by spoofing the MAC address of the adversaries. The packet resend rates, which is the measure of number of redundant packets to be sent after the communication is resumed from MAC spoofing DoS attacks.

Thus, the three proposed algorithms namely IDM DoS, LEPT DoS and MAC SDP DoS are validated and their results are compared with the existing methods and are listed in Table 1.

Existing Methods	Proposed Framework
1.CM and IDB	**1.IDM DoS Algorithm**
Existing central manager is proposed to detect MAC layer DoS attacks.	IDM DoS is proposed to detect and prevent MAC layer DoS attacks.
MAC address is verified during each and every request and intruder data is not recorded, which in turn increases the computational time.	IDM DoS algorithm records the intruders' MAC address and the computation and time is reduced.
The authentication process is based on an open shared key authentication, since the key is open to all; the intruder easily finds the key.	There are no keying procedures required.
IDB does not prevent the DoS attacks when the intruder enters with a MAC address which is not yet installed in the database.	IDM DoS prevents DoS attacks when the intruder enters with a MAC address which is already stored in intruder table and thereby reduces computational time.
2.LEP	**2. LEPT DoS Algorithm**
The existing algorithm is able to prevent slow DoS attacks used at association level.	When continuous flooding DoS attacks are experienced, the LEPT DoS algorithm is suitable for having a good throughput.
The intruder starts his entry during the authentication process itself. Since the authentication process is carried with "Open Shared" or "Pre Shared key" authentication, it cannot have a secure authentication.	LEPT DoS algorithm is used at the authentication level. So, authentication level DoS attacks are prevented.
If the communication is stopped or hacked at the authentication level, the request flooding attacks are very easy to make.	The Traffic Pattern Filtering (TPF) method sets a threshold value of maximum five times to make request for authentication or

	deauthentication.
This existing algorithm is effective against farewell attacks, but works only with specific platforms like Atheros Chipset running on Linux and needs hardware upgradation	LEPT DoS prevents vigorous resource flooding DoS attacks and does not require any firmware upgradation.
3. MAC Spoof Detection Algorithm	**3. MAC SDP DoS Algorithm**
The existing algorithms only detect deauthentication/disassociation attacks and MAC address spoofing attacks.	MAC SDP DoS algorithm is proposed not only to detect but also to prevent deauthentication/ disassociation and MAC spoofing DoS attacks.
The existing works do not provide any preventive measures for these DoS attacks.	The packet drop rate is decreased and the performance of the WLAN is increased by improving the throughput value.
Existing algorithm works on wireless mesh network	The packet resend rate is also reduced to zero compared to the existing methods.
This algorithm has reduced the generation of false positives.	The recovery time has been comparatively reduced with the existing algorithm

In summary, the following interpretations are arrived:

1. The framework with three proposed algorithms is used to detect and prevent various MAC layer DoS attacks from entering into the WLAN environment.
2. The throughput is increased in all the three proposed algorithms compared with the existing methods.
3. The recovery time is reduced with respect to the MAC SDP DoS algorithm compared with the existing spoof detection algorithm.
4. The packet resend rates are reduced to zero with respect to the MAC SDP DoS algorithm compared with the existing spoof detection algorithm.

The framework which comprises of the three proposed algorithms could be used to prevent the various types of MAC layer DoS attacks. These algorithms are selectively used to prevent the deauthentication/disassociation and MAC spoofing DoS attacks which are found to be dreadful compared to the other attacks. When the type of attacks, among the different layer DoS attacks are identified with the help of these algorithms, the prevention is made immediately. This enhances the performance of the WLAN communication by increasing throughput values. Thus, the security of WLAN infrastructure environment is improved with increased packet transfer rates. The WLAN user experiences a secured network access in wireless communication as compared with the wired access.

VI. CONCLUSION

The framework developed to detect and prevent MAC layer DoS attacks consists of the three security algorithms namely, IDM DoS, LEPT DoS and MAC SDP DoS. The three algorithms are compared with one another and the results are analyzed. These algorithms are selected based on the type of DoS attacks. DoS attacks can be made on the Physical, Media Access Control layer, Network, Transport and Application layers of the Open System Interconnection (OSI) model. This framework is meant for the DoS attacks made on the MAC layer due to the masquerading, resource flooding and media access attacks. The persistent MAC layer DoS attacks may lead to disconnection of the legitimate users from the WLAN access. When this framework is deployed in the WLAN setup, the MAC layer DoS attacks are easily identified and prevented. With the security framework, throughput has been increased in all the proposed algorithms. Recovery time has been reduced and packet resend rates were also found to be null with MAC SDP DoS algorithm. Thus the WLAN communication is made secure against the MAC layer DoS attacks.

REFERENCES

1. Maocai Wang,Guangming Dai, Hanping Hu and Lei Pen, “Security Analysis for IEEE 802.11”, IEEE Explore, 4th International Conference on Wireless Communication, Networking and Mobile Computing, 2008.
2. Radomir Prodanovi and Dejan Simi, “A survey of wireless security”, Journal of Computing and Information Technology, 2007, pp. 237–255.
3. Kemal Bicakci and Bulent Tavli, “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks”, Computer Standards & Interfaces, 2009, pp. 931–940.
4. Adam Stubblefield, John Ioannidis and Aviel D. Rubin, “A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)”, ACM Transactions on Information and System Security, 2004, pp. 319–332.

5. Arash Habibi Lashkari Fcsit, Mir Mohammad Seyed Danesh Behrang Samadi, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)", 2nd IEEE International Conference of CS and IT, 2009.
6. Borisov Nikita, Goldberg Ian and Wagner David, "Intercepting mobile communications: the insecurity of 802.11", International Conference on Mobile Computing and Networking, 2001, pp. 180-189.
7. J. Walker, "802.11 security series – part II: The Temporal Key Integrity Protocol (TKIP), Intel Corporation, 2002.
8. Sushma Myneni and Dijiang Huang, "IEEE 802.11 Wireless LAN Control Frame Protection", IEEE CCNC Proceedings, 2010.
9. M. León, R. Aldeco, and S. Merino, "Performance Analysis of the Confidentiality Security Service in the IEEE 802.11 using WEP, AES-CCM, and ECC", 2nd International Conference on Electrical and Electronics Engineering and XI Conference on Electrical Engineering, Mexico, 2005, pp. 52-55.
10. Maocai Wang,Guangming Dai, Hanping Hu and Lei Pen, "Security Analysis for IEEE 802.11", IEEE Explore, 4th International Conference on Wireless Communication, Networking and Mobile Computing, 2008.
11. Chibiao Liu and James Yu, "Rogue Access Point Based DoS Attacks against 802.11 WLANs", The Fourth Advanced International Conference on Telecommunications, IEEE Explore, 2008, pp. 271-276.
12. John Bellardo and Stefan Savage, "802.11 Denial-of Service attacks: real vulnerabilities and practical solutions", USENIX Security Symposium, Washington D.C, 2003.
13. Baber Aslam, M Hasan Islam and Shoab A. Khan, "Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack", in proceedings of the First Mobile Computing and Wireless Communication International Conference, Amman, 2006, pp. 215-220.
14. M.S. Bargh, R.J. Hulsebosch and E.H. Eertink, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs", Proceedings of the 2nd International Workshop on Wireless Mobile Application and Services on WLAN Hotspots, 2004, pp. 51- 60.
15. Kemal Bicakci and Yusuf Uzunay, "Pushing the Limits of Address Based Authentication: How to Avoid MAC Address Spoofing in Wireless LANs", World Academy of Science, Engineering and Technology, 2008, pp. 214-223.
16. Li Wang and Blasubramaniam Srinivasan, "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard", in Proceedings of Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE Computer Society, 2010, pp. 109-113.
17. F. D. Rango, D. C. Lentini, and S. Marano, "Static and dynamic 4- way handshake solutions to avoid Denial of Service attack in Wi-Fi Protected Access and IEEE 802.11i", EURASIP Journal on Wireless Communications and Networking, vol. 2, 2006, pp. 1-19.
18. Taimur Farooq, David Llewellyn-Jones and Madjid Merabti, "MAC Layer DoS Attacks in IEEE 802.11 Networks", PGNet , ISBN: 978-1-902560-24-3, 2010.
19. Nancy Cam-Winget, Russ Housley, David Wagner and Jesse Walker, "Security flaws in 802.11 data link Protocols", Communications of the ACM, Vol.46, No.5, 2003.
20. M. Bernaschi , F. Ferreri and L. Valcamonici, "Access points Vulnerabilities to DoS attacks in 802.11 networks", Springer Science+Business Media, LLC, 2006.
21. Stuart Compton, "802.11 Denial of Service and mitigation", SANS Institute, 2008.
22. Ondiwa Nashon Odhiambo, E. Beirmann and G. Noel, "An Integrated Security model for WLAN", Conference on Africa, IEEE Africon, 2009.
23. Mohd Nazri Ismail, "Analysis of Secure Real Time Transport Protocol on VoIP over Wireless LAN in Campus Environment", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, pp. 898-902.
24. Guenther Lackner, Udo Payer and Peter Teu, "Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods", International Journal of Network Security, Vol.9, No.2, 2009, pp.164-172.
25. Ping Ding, JoAnne Hollida and Aslihan Celik, "Central Manager: A Solution to Avoid Denial of Service Attacks for Wireless LANs", International Journal of Network Security, Vol.4, No.1, 2007, pp. 35-44.
26. Thuc N. Nguyen, Bao. N. Tran and Duc H. M. Nguyen, "A lightweight solution for wireless LAN: Letter-Envelop Protocol", Communication and Networking in China, IEEE Explore, 2008.
27. Rupinder Cheema, Dhivya Bansal and Dr. Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", International Journal of Computer Applications, Volume 23– No.7, 2011.

ACKNOWLEDGEMENTS

1 Dr. Arockiam. L is working as Associate Professor in the Department of Computer Science, St.Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has 24 years of experience in teaching and 17 years of experience in research. He has published more than 140 research articles in the International / National Conferences and Journals. He has also presented 2 research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. He has authored a book on "Success through Soft Skills". His research interests are: Software Measurement, Cognitive Aspects in Programming, Data Mining and Mobile Networks. He has been awarded "Best Research Publications in Science" for 2010, 2011, & 2012 and ASDF Global Awards for "Best Academic Researcher" from ASDF, Pondicherry for the academic year 2012-13.

2 Vani. B is working as Assistant Professor in the Department of Computer Science, Srimad Andavan Arts and Science College, Trichy, Tamil Nadu, India. She has 15 years of experience in teaching and 5 years in research. Her area of research is wireless network security. She is presently working on Denial of Service attack on wireless infrastructure network. She has published more than 13 research papers in the International/National Journals and Conferences. Her other areas of interest include OOAD & UML, Software Quality Assurance and Testing and Computer Networks.