MEDIUM ACCESS CONTROL SPOOF DETECTION AND PREVENTION ALGORITHM (MAC SDP DoS) FOR SPOOFING ATTACKS IN WLAN

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

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

***Abstract*— Wireless Local Area Network (WLAN) is widely used today because of its mobility and ease of deployment. Providing complete security to the WLAN users is a challenge due to the open nature and undefined boundaries of the wireless networks. This paper is intended to protect the 802.11 WLAN environments from Medium Access Control (MAC) layer Denial of Service (DoS) attacks especially, the deauthentication and disassociation attacks. This paper proposes an algorithm to detect and prevent deauthentication/ disassociation DoS attacks. These attacks are launched due to the vulnerability of the management frames which carries the MAC address of the client or Access Points (AP) that are not encrypted. So, there is an urgent requirement for a security mechanism to prevent MAC layer DoS attacks which does not require any change in the hardware or protocols. In this paper, an algorithm is proposed to detect and prevent MAC spoofing DoS attacks with an exchange of passkey values. The proposed algorithm, MAC Spoof Detection and Prevention (MAC SDP DoS) is compared with the existing algorithm which is used for MAC spoof detection. This algorithm is validated by NS2, a network simulator tool. The proposed algorithm improves the performance of WLAN by increasing the throughput and reduces the packet resend rates to a greater extend. The recovery time has also been reduced compared with the existing method.**

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

I. INTRODUCTION

The IEEE 802.11i uses WPA2 protocol which provides lower price of wireless devices and strong encryption with Advanced Encryption Standard (AES) algorithm. However, this protocol does not secure the WLAN from DoS attacks [1]. Wireless communication are made through three types of frames namely, data, control and management frames. The management frames are not protected by the IEEE 802.11 standards [2]. This makes them more vulnerable to DoS attacks. The users of a wireless network have the flexibility to join and leave the network any time [3]. The WPA and 802.11i were used to solve most of the problems related to authentication, confidentiality and integrity aspects with authentication mechanisms. They are Extensible Authentication Protocol (EAP), Message Integrity Check functions (MIC, Michael) and confidentiality solutions like Temporal Key Integrity Code and Advanced Encryption Standard (TKIP and AES) [4].

The third aspect of security is called availability, which provides legitimate users to access computer resources [5]. Resources access denial attacks are called Denial of Service (DoS). It involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable [6]. Such attacks usually lead to a server overload [7]. In general terms, DoS attacks are implemented by either forcing the target computer(s) to reset, or consuming its resources. So that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim [8].

DoS attack takes place on the Physical, Medium Access Control, Network, Transport and Application layers of the Open System Interconnection (OSI) model. The scope of this research paper is focused on the MAC layer DoS attacks and their mitigation. Figure 1 shows the WLAN infrastructure environment with Access Points (AP). The different types of MAC layer DoS attacks are discussed in the following subsections.

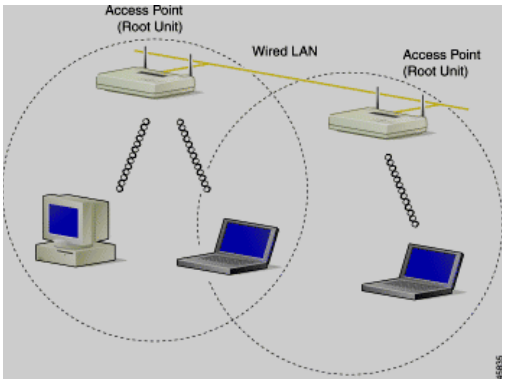

Figure 1. WLAN Infrastructure Environment

A. MAC Layer DoS attacks

MAC layer DoS attacks are launched due to the unencrypted management frames and they disrupt the network access selectively or completely [9]. The selective DoS attacks are made on the individual stations not on the whole network. The MAC layer DoS attacks are classified into three types namely masquerading, resource flooding and media access DoS attacks. MAC layer DoS attacks are commonly launched by MAC address spoofing techniques [10].

In masquerading DoS attacks, the intruder spoofs the MAC address of the authenticated client or AP [11]. With the help of free tools using the identities of the client or AP, the intruder traces the MAC address and brings the network under control [12]. Deauthentication, disassociation and power saving attacks are based on the masquerading attack types [13]. This paper is focused on the deauthentication and disassociation DoS attacks which come under the masquerading attacks that are found to be the dreadful attacks [14].

- Deauthentication attacks

The client and AP mutually request deauthentication by sending a request message. But these messages are not authenticated itself by any keying procedures [14]. This vulnerability makes the intruder to exploit the client or AP and launch the deauthentication attack. In response to the attack, the client or AP refuses to access the packets until they reauthenticate [15].

- Disassociation

IEEE 802.11 standard allows the clients to associate to a single AP at a time, after authentication [16]. The client or AP sends an explicit disassociation message to each other. Like the deauthentication message, disassociation management frames are also unauthenticated [17]. This makes the intruders to exploit the authenticated user and disconnect them from network. But the deauthentication DoS attacks are more severe than the disassociation DoS attacks since it takes long time for the user to resume connection.

This paper is organized as follows: Section 2 describes the existing works on MAC layer DoS attacks and their proposed solutions. The proposed algorithm MAC Spoof Detection and Prevention (MAC SDP DoS), which is used to detect and prevent deauthentication and disassociation DoS attacks, is explained in section 3. Section 4 elaborates the simulation results of the proposed algorithm compared with the existing algorithm. Section 5 discusses the findings and interpretations of MAC SDP DoS algorithm. The algorithm is validated with NS2, a simulator tool. Section 6 discusses the conclusion and future works.

II. RELATED WORKS

John Bellardo et al. [18] made an experiment on 802.11 DoS attacks and explored the identity vulnerabilities and media access vulnerabilities.

A sequence number based solution is suggested for disassociation DoS, which is one of the major attacks. The authors Baber Aslam et al. [19] suggest this solution as a robust one to overcome disassociation DoS attack. The basic idea is to use a pseudo random sequence number (based on PTK) for a disassociation notification instead of a sequential number.

One of the most applied authentication techniques is the address based authentication which assumes that the source could be identified by the network address from which the packets arrive. This address could be either the layer 3 Internet Protocol (IP) address or the layer 2 MAC address. Kemal Bickaki et al. [20] suggested a methodology which uses dynamic MAC addresses.

During the DoS attacks, the network is overwhelmed with large amount of illegitimate data and disconnecting legitimate clients from accessing the resources. DoS attacks are generally made by a person to prevent legitimate services from functioning efficiently, temporarily or indefinitely. The websites like Amazon, CNN, Yahoo and eBay had history of blocked instances due to DoS attacks. Rupinder Cheema et al. [21] implemented DoS attacks on the real wireless mesh test bed and analyzed their impact on the network performance and proposed a security algorithm for detecting these attacks. The authors considered two parameters such as throughput and bandwidth for analyzing the performance of their wireless mesh test bed before and after the launch of the attack. They emphasized the need for preventive measures to be taken to control the MAC layer DoS attacks.

III. MEDIUM ACCESS CONTROL SPOOF DETECTION AND PREVENTION ALGORITHM FOR DOS (MAC SDP DOS)

The identity vulnerabilities cause three types of attacks namely; deauthentication, disassociation and beacon spoofing attack [22]. Since the management frames are sent unprotected, the MAC address of the client or AP is spoofed by the intruders and deauthentication or disassociation attacks are launched on the legitimate clients. As the deauthentication requests are notifications, they cannot be ignored and the AP responds instantly to these requests [23]. The intruders monitor all the channels and send this spoofed message to all clients thus halting the connection. The deauthentication attacks are more dreadful compared to the other DoS attacks since they completely disconnect the legitimate users from the network [24]. There is an urgent requirement for preventing these deauthentication/ disassociation DoS attacks [25].

The detection algorithms are useful in identifying or classifying the type of DoS attacks and are not protecting the WLAN environment from MAC spoofing attacks. This

proposal provides one of the efficient ways in detecting and preventing deauthentication/disassociation DoS attack that are entering into the system by spoofing the MAC addresses of the victim stations. In our proposed MAC SDP algorithm, every authentication and association requests or response is passed on with a passkey value which is valid for a certain amount of time. Initially, the interface is monitored for packets. Counters for deauthentication and disassociation messages are maintained. Threshold values are assigned, which act as the trigger values for flooding detection. The frame types and sub types are checked. If the value of frame type is 0 and sub type comes out to be 12 then the frame would be identified as the deauthentication frame. If the number of deauthentication/disassociation packets received per unit time exceeds the threshold value, DoS attack has been detected. The passkey value is used along with the authentication/deauthentication requests/responses instead of the regular authentication request and response messages. The algorithm called Medium Access Control Spoof Detection and Prevention for DoS (MAC SDP DoS) is given below:

Algorithm 3.1 – MAC SDP DoS

1. Initialize connectivity
2. Initially, send a passkey to the receiver.
   The passkey is a random key generated using the current timestamp
3. Initialize the variables such as the Cdeauth, Cattack occurrences counter for recording the number of attack occurrences and set these to zero value.
4. Record the value of starting time.
5. Start sniffing the interface for monitoring packets.
6. Initialize variables for specifying the values of thresholds specified for deauth flooding as Thresh flood.
7. Value of the analyzed time interval is stored in Valueinit and the value of threshold for notifying attack is stored in variable Threshattack
8. Check frame type and subtype and if the value of type is 0 and sub type comes out to be 12 then the frame would be identified as deauthentication frame.
9. Calculate Δ that is the difference between current time timecur and the value of timer stored earlier.
10. If delta is greater than Valueinit and (Cdeauth /Δ) comes out to be greater than the threshold specified for the deauthentication flooding detection Threshflood,
    - Increment the value of the counter for recording the number of attack occurrences Cattack ocuurences.
    - If the value of counter for attack occurrences Cattack ocuurences is greater than the threshold specified for the attack Threshattack, then it has been notified as the detection of deauthentication attack.
11. Check for other frames from the same source. If it arrives,
    - Harvest MAC address and this comes out to be of legitimate client as the attack has been launched after spoofing MAC.
    - Request the node for passkey
    - After receiving the passkey, check if it is a legitimate one
    - After successful verification of the passkey, send the last transferred sequence number
    - The receiving system sends packets from that sequence number

This MAC SDP-DoS algorithm detects the MAC spoofing attacks and prevents the intruders from entering into WLAN environment.

IV. SIMULATION RESULTS

This section discusses the experimental results of MAC SDP DoS algorithm. This algorithm is implemented with the NS2 tool and results are compared with the existing algorithm. The MAC layer DoS attacks are common among the 802.11 WLAN user community. In the WLAN infrastructure networks, every user is connected through an AP. User and AP communicates each other by sending authentication/ deauthentication and association/ disassociation requests. These requests are considered as notifications and they are not supposed to be rejected. Existing algorithms only detect the deauthentication/disassociation attack launch.

The proposed algorithm MAC SDP DoS is used to detect and prevent the deauthentication /disassociation DoS attacks that are launched by spoofing the MAC address of either the client or AP. This algorithm is implemented on a WLAN setup which consists of four nodes including the intruder node. The NS2 tool is used to validate this algorithm. The existing deauthentication/ disassociation detection and MAC spoof detection algorithms are implemented on the WLAN setup and the interface is monitored for DoS attacks. The existing algorithm proposed by Rupinder Cheema et al. [21] is implemented on the same setup with four nodes. The NS2 set up is given in Figure 2.

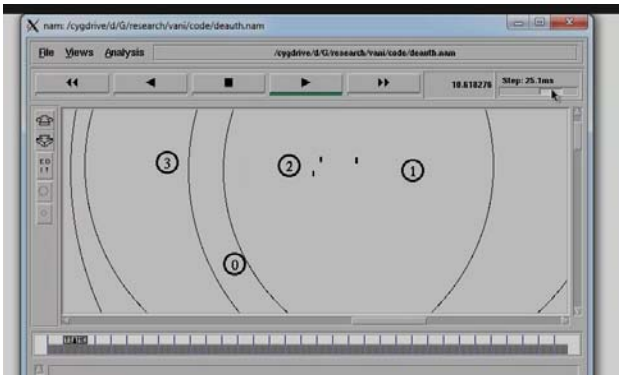

Figure 2. WLAN Setup with Four Nodes

A. *Deauthentication/Disassociation attack launch*

Deauthentication/disassociation attacks are launched with the existing algorithm. Connection between the AP and client is established by the exchange of various frames. The exchange of series of authentication and association request frames takes place. AP responds by sending the authentication/association response frames. The traffic and throughput rates are monitored. Now, the deauthentication attack is launched with the algorithm. Since the management frames are not protected and sent in clear, they are spoofed by the intruder. The MAC address of client or AP is spoofed by the intruder with unprotected management frames. Then the intruder sends deauthentication requests with the client or AP's MAC address as source. AP responds by sending deauthentication response to the client and the communication is halted. Since deauthentication requests are notifications, they could not be ignored and AP responds immediately to these requests. Network connection could be terminated with these spoofed messages that are sent by the intruders. The intruders scan all the channels periodically to send these messages.

The deauthentication/ disassociation algorithm is tested and traffic is monitored before and after the attack launch. The packets are dropped in transit during the attack. The bandwidth and throughput values reach zero during the deauthentication/disassociation DoS attacks as discussed in the existing algorithms. The existing algorithms only detect deauthentication/disassociation and MAC address spoofing DoS attacks. The existing works do not provide any preventive measures for these DoS attacks. In order to overcome this problem, MAC SDP DoS algorithm is proposed to detect and prevent the MAC spoofing DoS attacks and the results are discussed in the following sections.

B. *Results of MAC SDP DoS*

The proposed algorithm MAC SDP DoS is implemented in the same experimental set up. Figure 3 depicts the traffic flow between the nodes and exchange of passkey values in a simulation environment with the help of NS2 tool, nam animator.

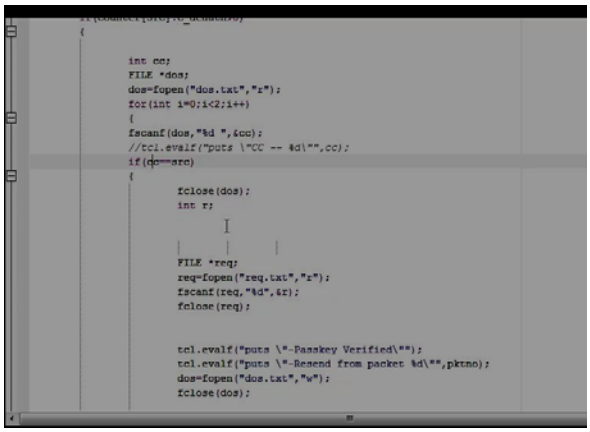

Figure 3. Exchange of Passkey Values

The packet size and the maximum packets to be transferred are fixed. When deauthentication attack is made, the packets are dropped. During deauthentication attack launch, MAC address of the legitimate client is spoofed by the intruder. Then the intruder sends one deauthentication request to AP in the name of legitimate client. AP responds to the deauthentication request immediately, since the request is considered as a notification that could not be ignored. The packet drop rate is increased during the deauthentication attack launch. The communication between the legitimate client and the AP is stopped during this attack launch. The legitimate client waits for the connection to be established again.

Thus, deauthentication DoS attack is proved to be the most dreadful attack since it disconnects legitimate users from the network connection. The proposed algorithm MAC SDP DoS is intended to prevent this by incorporating the authentication mechanism by exchanging the passkey values. When connection between the nodes established, traffic is monitored by setting timestamps. A random key is used as the passkey value and is sent along with each authentication and deauthentication requests. AP verifies the passkey and responds correspondingly. The timestamp is followed and threshold values are set for monitoring the number of requests that are sent continuously.

The existing MAC spoof detection algorithm is compared with the proposed MAC SDP DoS algorithm. Existing algorithm detects the deauthentication/disassociation attacks when the MAC address of the legitimate client or AP is spoofed by the intruder. In the name of legitimate user's MAC address, intruder sends the deauthentication requests and the connection between the user and AP is stopped.

Packet flow rates are monitored before and after the usage of the proposed algorithm MAC SDP DoS. Within the fixed timestamp, the recovery time is compared between the existing and proposed works. Packets are dropped

during transit when the spoofing attacks are made. These packets have to be resent after recovering from the MAC spoofing attacks. Thus the packet resend rates are compared between the existing and proposed algorithms. The findings are discussed in the following sections.

V. FINDINGS AND INTERPRETATIONS

The proposed MAC SDP DoS algorithm is implemented in NS2 setup and compared with the existing algorithm which is used to detect the MAC spoofing attacks. The proposed MAC SDP DoS algorithm uses an authentication method for each deauthentication requests and response. A random key is generated and used as a passkey value which is exchanged between the legitimate client and AP. Since this passkey is generated randomly by maintaining timestamps, this could not be easily predicted by the intruders. Though the MAC address of the legitimate user is spoofed by the intruder, it is impossible to impersonate the user. Whenever the intruder makes a deauthentication request, it is asked for the passkey value to be exchanged. The attempt to launch MAC spoofing attack becomes impossible for the intruder because of the passkey value. The existing and proposed algorithms are compared in terms of three metrics namely, packet flow rates, recovery time and packet resend rates. These three parameters are compared before and after the MAC SDP DoS algorithm deployment and the findings are depicted through graphs.

The number of packets sent per unit time is called throughput. This throughput value is compared before and after the usage of the proposed MAC SDP DoS algorithm. The packet drop rate is decreased and the performance of the WLAN is increased by improving the throughput value. This is depicted in the Figure 4.

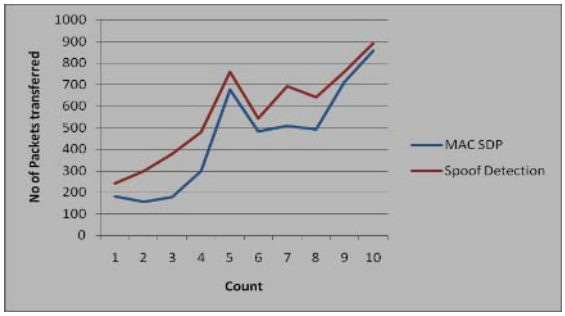

Figure 4 Packet Flow Rates

From Figure 4, packet flow rates or the throughput is maintained as same during the MAC spoofing attacks. The number of deauthentication attack launched is taken as count in X axis. In both the existing and the proposed algorithms, packet rate is found to be increased. In the MAC SDP DoS algorithm, the passkey authentication is an additional procedure to be followed by the network. This shows that MAC SDP DoS algorithm performs well without making reduction of packet flow rates.

The second parameter to validate the proposed algorithm is recovery time. The recovery time is the time taken to resume the connection after the attack is made. During the attack, packets are dropped. In the proposed MAC SDP algorithm, the recovery time is found to be reduced as shown in the Figure 5.

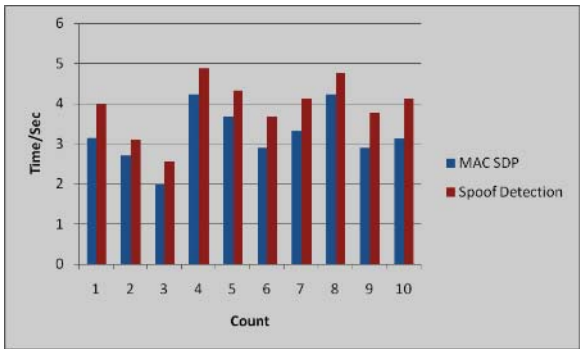

Figure 5 Recovery Time

From Figure 5, the recovery time for the proposed algorithm MAC SDP DoS is reduced compared with the existing spoof detection algorithm. Since there is no fall of packet rates in the proposed algorithm, recovery time is reduced approximately 3 to 5%. Since, recovery time is reduced, traffic becomes faster for the legitimate users and their corresponding APs. The existing work is implemented on wireless mesh testbed. In this research work, both the existing and the proposed algorithms are tested on the WLAN setup.

The third validation is with respect to the packet resend rates measurement between the existing and the proposed algorithms. The packets are dropped to a greater extent whenever the MAC spoofing and deauthentication/disassociation DoS attacks are made. The dropped packets have to be sent again when the network recovers from the attacks. There is an additional computation involved for the network to identify dropped packet sequences and resend them to the destinations. These packet resend rates are compared between the existing and proposed algorithms and depicted in the Figure 6.

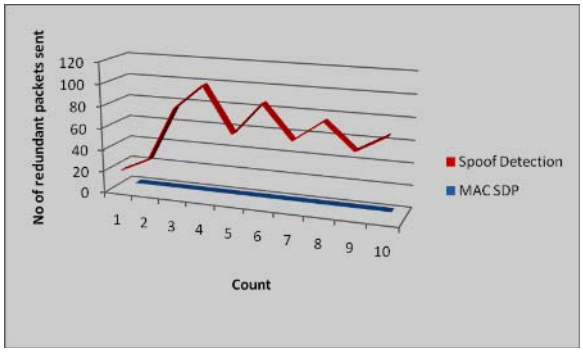

Figure 6 Packet Resend Rate (No. of Redundant Packets Sent)

From Figure 6, the packet resend rates have been completely vanished as they reach zero value when compared to the existing detection algorithm. In the existing algorithm, which is used to detect the MAC spoofing DoS attacks, the packets are dropped in transit. They have to be sent again to the corresponding destinations after the legitimate users recover from the attacks. This packet resend rates were found to be greater in the existing algorithm. But, in MAC SDP DoS algorithm, the packet resend rates are found to be null. From this, it is inferred that, there is no packet loss during transit. This is due to the prevention of the MAC spoofing DoS attacks by following the exchange of passkey values among the legitimate users and APs. The experimental results proved to be successful in increasing the throughput values.

VI. CONCLUSION

The MAC layer DoS attacks are made due to the open nature of management frames. These management frames carry the source MAC address and are susceptible to deauthentication and disassociation DoS attacks. The existing methods provide detection of deauthentication and disassociation attacks and are not providing any preventive measures without disturbing the firmware or protocol change. The proposed MAC SDP DoS algorithm was proved to be successful in detection and prevention of the MAC layer DoS attacks. The proposed algorithm MAC SDP DoS, with the passkey exchange between the user and AP with a timestamp is validated to be a successful one for preventing MAC spoofing DoS attacks and deauthentication/disassociation DoS attacks. Packets that are dropped in transit have to be sent again to the client or AP. The packet resend rate has been reduced to zero as shown in the results. Existing algorithms do not provide any preventive measures for the packet loss during communication. The proposed MAC SDP DoS algorithm has the following features compared to the existing algorithms. Number of packets transferred is increased without any fall; the time requirement for resuming communication after detecting the attack entry is reduced compared with the existing algorithms; the packet resend rates have been completely reduced to zero which implies the number of redundant packets sent is zero in MAC SDP DoS. The experimental focus is limited to a single AP, thus the future research may involve with more number of APs.

REFERENCES

1. 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.
2. Daemen. J and Rijmen. V, "Rijndael: The Advanced Encryption Standard", Dr. Dobb's journal, 2001, pp. 137-139.
3. 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, May 2003.
4. Halil Ibrahim Bulbul, Ihsan Batmaz and Mesut Ozel, "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols", Proceedings of the I International Conference on Forensic Application and Techniques in Telecommunication, Information and Multimedia Workshop, e- Forensics, Australia, 2008.
5. Pascal Urien and Guy Pujolle, "Security and privacy for the next wireless generation", International Journal of Network Management, Vol. 18, Issue 2, 2008, pp.129–145.
6. Radomir Prodanovi and Dejan Simi, "A survey of wireless security", Journal of Computing and Information Technology, 2007, pp. 237–255.
7. Bo Yan, Guanling Chen, JieWang and Hongda Yin, "Robust Detection of Unauthorized Wireless Access Points", Springer Science + Business Media, LLC 2008, pp. 508-528.
8. Payal Pahwa, Gaurav Tiwari and Rashmi Chhabra, "Spoofing Media Access Control (MAC) and its Counter Measures", International Journal of Advanced Engineering & Application, 2010, pp. 186-192.
9. 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.
10. M. Bernaschi , F. Ferreri and L. Valcamonici, "Access Points Vulnerabilities to DoS attacks in 802.11 networks, Springer Science+Business Media, LLC,2006.
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. Li Wang and Blasubramaniam Srinivasan, "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard", Proceedings of Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE Computer Society, 2010, pp. 109-113.
13. Kemal Bicakci and Bulent Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", Computer Standards & Interfaces, 2009, pp. 931–940.
14. Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, "An Experimental of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks", International Journal of

Computer Science and Network Security, Vol. No. 8, August 2008, pp. 1-5.
15. 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.
16. Aslihan Celik and Ping Ding, "Improving The Security of Wireless LANs By Managing 802.1x Disassociation", Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC04), Las Vegas, NV, January 2004, pp. 53-58.
17. Jalil Desa, Mina Malekzadeh, Abdul Azim Abdul Ghani and Shamala Subramaniam, "An Experimental Evaluation of DoS Attack and Its Impact on Throughput of IEEE 802.11 Wireless Networks", International Journal of Computer Science and Network Security, Vol. 8, No. 8, August 2008, pp. 1-5.
18. John Bellardo and Stefan Savage, "802.11 Denial-of Service attacks: real vulnerabilities and practical solutions", USENIX Security Symposium, Washington D.C, 2003.
19. Baber Aslam, M Hasan Islam,Shoab and A. Khan, "Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack", IEEE Explore, 2008.
20. 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.
21. 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.
22. 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.
23. Qing Li and Wade Trappe, "Reducing Delay and Enhancing DoS Resistance in Multicast Authentication Through Multigrade Security", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, June 2006, pp. 190-2004.
24. Rupinder Gill, Jason Smith and Andrew Clark, "Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks", Proceedings of the Australian Workshop on Grid computing and e-Resources, Australian Computer Society, 2006, pp. 221-230.
25. Anand balachandran**,** Geoffrey M. Voelker and Paramvir Bahl, "Wireless hotspots: current challenges and future directions", Springer Science + Business Media, Mobile Networks and Applications, 2005, pp. 265–274.

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.