ISSN 2319 - 6629

Volume 2, No.1, December 2012 – January 2013

International Journal of Wireless Communications and Networking Technologies

Available Online at http://warse.org/pdfs/2013/ijwcnt01212013.pdf

Security algorithms to prevent Denial of Service (DoS) attacks in WLAN

L. Arockiam[1], B. Vani[2]

[1]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

This paper proposes security algorithms which are used to mitigate the Media Access Control (MAC) layer Denial of Service (DoS) attacks in WLAN infrastructure networks. This work is aimed to attend the DoS attacks due to the susceptibility of the MAC layer's management frames. The management frames are sent unencrypted; this makes the intruder easily spoof the MAC address of the client or Access Point (AP) and stops their communication. There are two algorithms proposed in this paper namely, the Intruder Detector and Manager (IDM) and Letter Envelop Protocol with Traffic pattern filtering (LEPT). The Intruder Detector and Manager (IDM) algorithm detects and prevents the intruder entering into the network by maintaining tables in order to avoid the masquerading DoS attacks. When this procedure is followed, IDM increases the throughput by preventing intruders and maintains the history of intruders. This reduces the computational time of the AP and maintains the throughput and bandwidth. The LEPT algorithm is proposed to avoid the resource flooding DoS attacks. The experimental results prove that these algorithms effectively maintain the throughput and increase the performance of WLAN.

Key words : Denial of Service (DoS), Deauthentication, Disassociation, Throughput etc.

1. INTRODUCTION

In WLAN infrastructure network, the clients are connected with one or more Access Points (AP). The DoS attacks disable the WLAN by making the resources unavailable to the legitimated users. Physical layer DoS attacks are called the jamming attacks which prevent a station from transmitting or receiving frames from higher layers. There are three types of frames, namely, management, control and data frames used in the IEEE 802.11 networks [1]. Data frames carry higher-level protocol data in the frame body. Control frames are used to deliver the data frames by area clearing operations, channel acquisition and carrier – sensing maintenance functions. Management frames act as supervisory functions by joining and leaving the wireless networks and move association from one AP to other AP [2].

The MAC layer DoS attacks are more common due to the susceptibility of management frames [3]. The management frames are sent unencrypted and are used for network management and access control. This makes the intruders to spoof the MAC address of the client or the AP and uses up all of the network resources and forces it to shut down [4]. This adds significant overhead on the network and takes away bandwidth from authenticated clients. Several defense mechanisms have been proposed in the past to secure WLAN with Wired Equivalent Privacy (WEP) and WPA2 protocols which are proposed by WLAN 802.11 standards [5] [6]. But these techniques do not address the DoS attacks made by the unprotected management and control frames [7]. These include deauthentication, disassociation, Request to Send (RTS), Clear to Send (CTS) and Acknowledgement (ACK), and Power-Save Poll (PS-Poll) message based attacks [8]. The scope of the research is focused on management frames only since they are mostly exploited by DoS attacks.

1.1 Types of 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 [1]. 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 as shown in the Figure 1. The following sections discuss the MAC layer DoS attacks and their sub types.

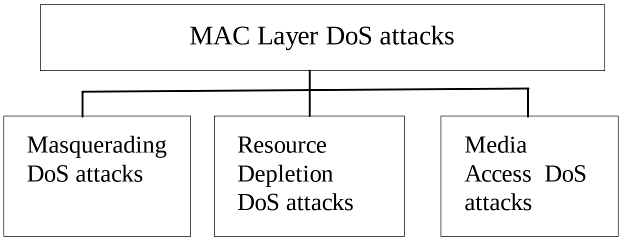

Figure 1: Types of MAC layer DoS attacks

1.1.1 Masquerading DoS attacks

In masquerading DoS attacks, the intruder spoofs the MAC address of the authenticated client or the AP [9]. 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. Deauthentication, disassociation and power saving attacks are based on the masquerading attack types [10].

- Deauthentication attacks

The client and AP mutually request deauthentication by sending a request message [11]. But these messages are not authenticated itself by any keying procedures. 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 [12].

- Disassociation

IEEE 802.11 standard allows the clients to associate to a single AP at a time, after authentication [13]. The client or AP sends an explicit disassociation message to each other. Like the deauthentication message, the disassociation management frames are also unauthenticated [14]. This makes the intruders to exploit the authenticated user and disconnect them from the 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 [15].

- Power Saving attacks

The IEEE 802.11 allows the clients enter into a sleep mode when there is no transmission in order to conserve power. During sleep mode, the clients do not send or receive messages. The AP buffers all the clients data until they polls it for data [8]. The intruder spoofs the polling message on behalf of the client and makes the AP to discard the client's packet. They also spoof the TIM to convince the client that there is no pending data present in the AP. One more vulnerability arises from power saving mechanism is that the client node fall out of synchronization and fails to wake up at appropriate times due to the nature of unauthenticated management frames.

1.1.2 Resource Flooding DoS attacks

The most important DoS vulnerability is flooding attacks which are named as Resource depletion or flooding DoS attacks which targets the shared resources such as AP and uses all its memory and processing so that it cannot continue services to its legitimated clients. The resource depletion attacks are categorized as probe request flood, association request flood, authentication request flood and deauthentication/disassociation request flood [16]. These attacks are briefly discussed in the following subsections.

- Probe request flood

Clients in a WLAN use probe request to scan the wireless environment for existing wireless networks. The APs respond to these requests by providing information about the wireless network. This makes the clients associate with AP network. The intruder transmits continuous probe requests with spoofed MAC addresses to simulate the existence of more number of clients seeking access to the network. This prevents the AP from responding to legitimate clients' request by consuming all of the memory and processing resources of an AP.

- Authentication request flood

An attacker sends authentication request frames with spoofed MAC addresses in order to authenticate to the AP. The intruder floods the AP with huge amount of authentication request frames and consumes the memory and processing resources. The AP does not allow legitimate clients since it has to allocate memory for each fake authentication request.

- Association request flood

An AP keep record of all association requests in a table called association table. The size of the table varies with different models. By randomly generated MAC addresses, an attacker sends a flood of associate requests in order to overload the association table. It is observed that many APs respond to association request in their initial state itself.

1.1.3 Media Access Attacks

The unauthenticated management and control frames contain a duration field which is used by the virtual carrier sense mechanism that is used for solving the hidden terminal problems. The media access attacks are caused by affecting the legitimate transmission by asserting a large duration field to ensure the value of Network Allocation Vector (NAV) value for each node is greater than zero.

This paper is organized as follows: Section 2 lists down the existing works on MAC layer DoS attacks. The proposed algorithm called Intrusion Detector and Manager (IDM) which is used to mitigate masquerading DoS attacks is explained in section 3. Section 4 elaborates the second algorithm called Letter Envelop Protocol enabled with Traffic Pattern Filtering (LEPT) proposed to minimize the resource flooding DoS attacks. Section 5 presents the results and discussion of both these algorithms validated by NS2 tool. Section 6 discusses the conclusion and future works to prevent MAC layer DoS attacks.

2. RELATED WORKS

Ping Ding, JoAnne Hollida and Aslihan Celik [17] proposed an efficient mechanism to avoid DoS attacks for WLAN using Central Manager (CM). CM acts as a back end server which maintains three tables and a timer to detect DoS attacks. CM reduces the effect from login DoS attacks and improve the performance of WLANs with the help of the three tables T1, T2, T3 and timer, CM either allows login or block it.

The mechanism proposed by Thuc Nguyen, Bao. N. Tran and Duc H. M. Nguyen [18] is an addition on current 802.11 based protocols. To prevent the disassociation attack, the authors used Letter-Envelop Protocol to authenticate management frames in association process.

Chibiao liu and James Yu [19] proposes a solution to detect and resolve Authentication Request Flooding (AuthRF) and Association Request Flooding (AssRF) attacks based on an experimental framework. It quantifies both the attacks against TCP and wireless voice over IP communication. The two solutions MAC Addressing Filtering (MAF) and Traffic Pattern Filtering (TPF) are used against both the attacks.

A sequence number based solution is suggested for disassociation DoS, which is one of the major attacks. The authors Baber Aslam, M Hasan Islam and Shoab A. Khan [20] 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 sequence number.

3. INTRUSION DETECTOR AND MANAGER (IDM)

Intrusion Detector and Manager (IDM) which can also be called as Integrated Central Manager (ICM), manages all the activities of client and AP to detect and block an attacker from entering into WLAN. IDM is intended to prevent the DoS attacks in an infrastructure network by maintaining five tables and a timer.

The tables are named as account (T1), intruder (T2), authenticated client (T3), unauthenticated client (T4) and client table (T5). The descriptions of the tables are as follows: T1 is for checking the client identity based on their Medium Access Control (MAC) address. T2 contains the MAC address of all the intruders which was detected and spoofed by IDM. T3 consists of MAC addresses of (working) clients who are in the communication process, login time of the client and logout time. Table T4 records the MAC address, login and logout time of wireless clients who are not in communication with the AP. Table T5, the client table, consists of MAC address and login time of all the clients.

In this section, the proposed algorithm called the Intruder Detector and Manager (IDM) is explained. The sequence of the steps to be followed when the AP receives a start frame or login request from a client is given in the following algorithm 1.

Algorithm: 1- IDM

```
Start
   Event_type  (login, logout)
   If (event_Request = login) then
      int_mac_a = get_Mac_Address()
      If (int_mac_a is in T2) then      /*Check Intruders' List*/
         (Ignore the request)
      else
          if ( int_mac_a is in T3) then    /*Check Authenticated Clients' List*/
            (Ignore login request) and
            (store int_mac_a in T2)
    else
             if ( int_mac_a is in T5) then /*Check Current Client's List*/
           (Ignore the request)
        else
      (Accept the login request) and
           (Start communication)
           end if
        end if
     end if
   end if
Stop
```

The masquerading DoS attacks are identified as the deauthentication, disassociation and power saving attacks. The deauthentication DoS attack is found to be the most dreadful attack since the intruder takes control of the AP or the client by spoofing the MAC address. The management frames carry MAC address of each client during communication. Since management frames are not encrypted, they are susceptible to these kinds of vulnerabilities.

4. LETTER ENVELOP PROTOCOL WITH TRAFFIC PATTERN FILTERING (LEPT)

According to the frame format, management frames are more vulnerable to DoS attacks since they are sent unencrypted. The proposed work is based on an algorithm called LEPT, which is used to prevent the resource flooding or resource depletion DoS attacks by protecting the management frames. This algorithm works on the combination of the Letter Envelop protocol (LEP) and the Traffic Pattern Filtering (TPF) techniques.

Algorithm 2: LEPT

```
Start
    Event-type (Login, Logout)
     integer :
    N1 be a semiprime from p1 and q1
    N2 be a semiprime from p2 and q2
    C1 be the client
    AP1 be the Access Point

    If (event_Request_C1 = login) then
    {
        compute N1 = p1 * q1; /*C1 generates and stores N1 value*/
       store N1 in C1;
       compute N2 = p2 * q2;  /*AP1 generates and stores N2 value*/
       store N2 in AP1;
  get_N1() value from C1 store into AP1;
       get_N2() value from AP1 and store into C1;
       start communication;
  If (event_Request_C1 = logout) then
           C1 sends logout request to AP1 with p1;
           logout_Req_C1+=1;

                If ((logout_Req_C1<=5) && (p1 corresponds to N1)) then
                 Accept the logout request;
        Else
                Reject the request assuming that it is from the intruder
                endif
       endif
       /*When AP1 wants to logout from the Network*/
       If (event_Request_AP1 = logout)
           AP1 sends p2 value to all clients;
           logout_Req_AP1+=1
   If ((logout_Req_AP1 >=5) && (p2 corresponds to N2)) then

/* C1 computes p2/N2 and verifies whether p2 corresponds to N2*/
          Accept the logout request
   else
       Reject the request assuming that it is from the intruder who attacks the AP1
           endif
         endif
      endif
   Stop
```

This algorithm is found to be effective in preventing request flooding attacks because, though the intruder spoofs the MAC address, the legitimated clients or the AP are not affected. The authentication is progressed based on envelop-protocol. The intruder generates prime numbers and communicates with AP. But the intruder cannot generate the same prime numbers as the client. So attacking the client or AP, spoofing the MAC address becomes difficult for the intruder. LEP is used to avoid slow request flooding attacks. When the intruder aims resource flooding DoS attacks, the pattern filtering methods are found to be comfortable when combined with LEP. The TPF method is employed in such a case to prevent continuous resource flooding requests from the intruder. To evaluate the performance of LEP and TPF, we have implemented LEPT in both real time and in simulation environment using NS-2. The solution is validated by measuring the throughput before and after implementing the LEPT algorithm.

5. RESULTS AND DISCUSSIONS

This section discusses the experimental results of both IDM and LEPT algorithms. The algorithms are implemented with the NS2 tool and also with a real time set up using Java coding.

5.1 Intruder Detector and Manager (IDM)

This section discusses the experimental results for the existing and proposed solutions which are carried out to prevent DoS attacks. From the experimental results, it is shown that the proposed IDM is better in preventing DoS attacks when compared with the existing Central Manager (CM) and Intruder Database (IDB) methods. The experimental setup consists of one AP, one target client and one attacker. A wireless client machine is considered as an AP. The solution is validated by measuring the throughput (the number of packets that can pass through in a fixed time) before and after implementing the IDM.

The attacks which have been taken for simulation are EAP logoff, EAPOL start frame targeted over AP and client. The simulations are built on Network Simulator NS-2. The simulation scenario is setup by taking AP as one node, client and attacker as the other two nodes. At the beginning of the simulation, AP and client are in communication with each other. At that time, intruder spoofs the MAC address of client and make masquerading DoS attack. During the DoS attack, the throughput is found to drop because the attacker permanently stops the communication.

The CM does not maintain the history of the intruders since it only detect and prevents them entering the WLAN. With IDB, a database is maintained which consists of 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; the 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 CM, the IDM is proposed which combines the concept of CM and IDB. It also maintains a duplicate IDM, which takes over the network, in case of IDM's failure. IDM updates the duplicate IDM often. When an intruder enters into the network with legitimate client's MAC address, the communication between client and AP is disconnected. So the throughput of the WLAN is dropped during the period of attack. The Figure 2 clearly shows the rapid fall of throughput during the attack.

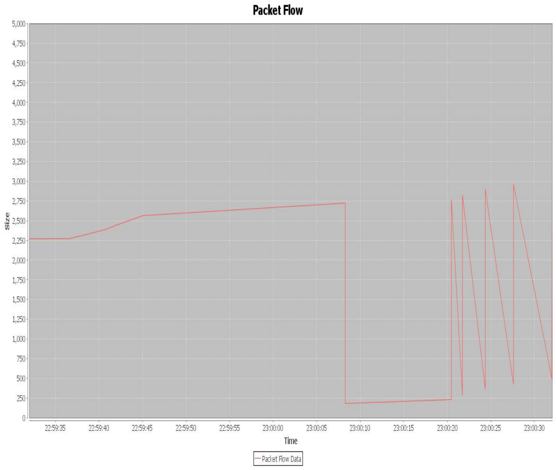

Figure 2: Throughput measurements during DoS attack

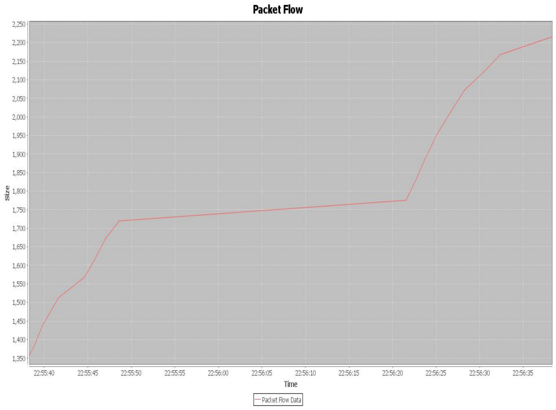

Figure 3: Throughput Measurements after implementing IDM

From the above Figure 3, after the IDM's installation, throughput does not decrease during the period of attack. The performance of the WLAN is increased by maintaining the throughput.

5.2 LEPT algorithm

LEP at association level prevents request flooding attacks. But the attacker can do his work or attack at the authentication level itself. Since the authentication process is carried out with "Open Shared" or "Pre Shared key" authentication, it cannot have a secure authentication. If the communication is stopped or hacked at the authentication level, the request flooding attacks are very easy to make. To overcome such disadvantage, LEPT is used at the authentication level itself. So, from the initial state itself, the LEPT starts functioning and the network is secured from flooding DoS attacks. When LEPT is sent along with authentication frame, the spoofing possibilities are minimized and it prevents vigorous resource flooding attacks.

When continuous flooding DoS attacks are experienced, the LEPT procedure is suitable for having a good throughput. The traffic pattern filtering method sets a threshold value of maximum five attempts to request for authentication or deauthentication. When the threshold value exceeds the limit, the request is ignored by the network. The envelop value generated by AP and client are mutually verified and the authentication and deauthentication processes are followed after that. AP stores the 'N' generated by clients and if the intruder tries to deauthenticate/disassociate legitimated clients after spoofing their MAC addresses, it becomes difficult due to the LEPT algorithm. So, when the intruder tries to deauthenticate, the intruder itself will be disconnected from the network. The client continues its original state.

The simulation scenario is set by taking AP and client as two nodes and intruder as another node. At the beginning of the simulation, AP and client are in communication. The intruder enters into the network by the spoofed MAC address. During the attack the throughput value is dropped. This is observed through the graph generated by NS2 by taking time/second in X axis and throughput along Y axis which is depicted in the Figure 5. After implementing the solution, the intruder finds difficulty in making the DoS attack because client authentication is based on the prime number generated by it. Hence LEPT algorithm identifies the intruder and drop level of throughput during the attack is prevented.

LEP at association level prevents request flooding attacks. But the attacker makes DoS attack at authentication level itself. Since the authentication process is carried 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. To overcome such disadvantage, LEPT is used at the authentication level itself. So, from the initial state itself, the LEPT starts functioning and the network is secured from flooding DoS attacks.

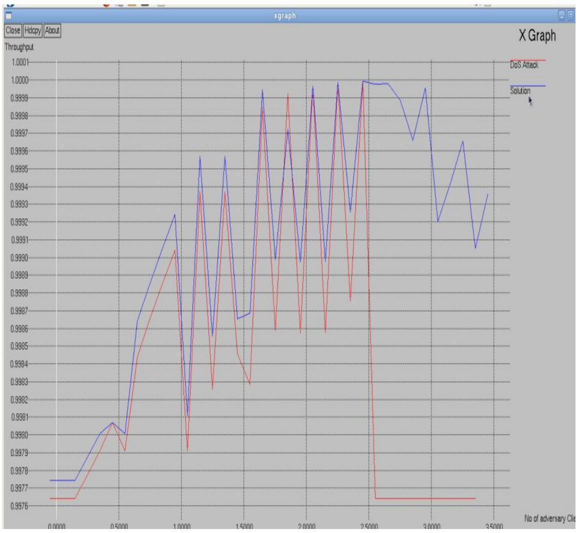

Figure 4: Throughput comparison before and after the solution.

The Figure 4 shows that the LEPT algorithm maintains the throughput value without rapid fall of throghput, when the network is under resource depletion attack. When LEPT algorithm is used, the continuos flooding attacks are prevented from affecting the network commnication.

6. CONCLUSION AND FUTURE WORKS

From the simulation results, the Intrusion Detector and Manager (IDM) has been improved the WLAN’s performance apart from preventing the masquerading DoS attacks. The added advantage in IDM was that it has been spoofed and stored the intruder’s MAC address. The throughput has been increased in IDM compared to CM. It was suggested that the usage of duplicate IDM to manage in case of failures. The maintenance of duplicate IDM will increase the traffic overhead. But, it prevents the WLAN from the total drop of throughput when compared with CM and IDB.

The second algorithm called LEPT was used to control the resource flooding DoS attacks. Letter Envelop Protocol is one effective method to prevent request flooding attacks. When the intruder starts the flooding attack at the authentication level, the network loses its control and becomes slow. The proposed algorithm LEPT has been used along with the authentication frame itself. Thus the intruder founds it difficult to disconnect the AP from the client and vice versa. There is a possibility of spoofing AP’s MAC address and sends the request as AP to client. But in LEP intruder cannot do the same. It is because the client stores ‘N’ value generated by the AP before it starts its communication. It has also been observed from the experiments, that LEP is effective in preventing resource flooding attacks when they are slow attacks. In the case of vigorous DoS attacks, LEPT is proved to be an effective method since it has traffic pattern filtering approach. With LEPT, the throughput becomes unaffected and the performance of WLAN is maintained.

The MAC layer DoS attacks are possible only when the MAC address of the client or the AP are spoofed by the intruder. With the help of free tools available, MAC address spoofing becomes easy as the management frames are sent unencrypted. The future work is focussed on detection and prevention of MAC spoofing totally and improving the performance and security of WLAN.

REFERENCES

1. Taimur Farooq, David Llewellyn-Jones, Madjid Merabti. **MAC Layer DoS Attacks in IEEE 802.11 Networks**, *PGNet* , 2010.
2. Chibiao Liu and James Yu. **Rogue Access Point Based DoS Attacks against 802.11 WLANs**, *The Fourth Advanced International Conference on Telecommunications, IEEE Xplore*, pp. 271-276, 2008.
3. 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, pp. 1-5, August 2008.
4. M. Bernaschi , F. Ferreri and L. Valcamonici. **Access points Vulnerabilities to DoS attacks in 802.11 networks**, *Springer Science+Business Media*, LLC, 2006.
5. 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, pp. 53-58, January 2004.
6. Baber Aslam, M Hasan Islam and Shoab A. Khan. **Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack**, *IEEE Xplore*, 2008.
7. Arash Habibi Lashkari Fcsit, Mir Mohammad Seyed and Danesh Behrang Samadi. **A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)**, *2nd IEEE International Conference of CS and IT, CSIT* 2009.

8. F. Ferreri, M. Bernaschi and L. Valcamonici, **Access points vulnerabilities to DoS attacks in 802.11 networks**, *Wireless Networks*, vol 14, pp. 159-169, 2008.
9. 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, pp. 1-5, August 2008.
10. Kemal Bicakci and Bulent Tavli. **Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks**, *Computer Standards & Interfaces*, pp. 931–940, 2009.
11. Radomir Prodanovi and Dejan Simi. **A survey of wireless security**, *Journal of Computing and Information Technology – CIT 15*, 3, pp – 237–255, 2007.
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. 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*, pp-214-223, 2008.
14. C. Liu and J. T. Yu. **Review and Analysis of Wireless LAN Security Attacks and Solutions,** *Journal of International Engineering Consortium*, vol. 59, 2006.
15. Mansoor Ahmed Khan and Aamir Hasan. **Pseudo Random Number Based Authentication To Counter Denial of Service Attacks on 802.11,** *WCON Conference*, Surabaya, Indonesia, IEEE Xplore, 2008.
16. Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa. **Emprical Analysis of Virtual Carrier Sense Flooding Attacks Over Wireless Local Area Network**, *Journal of Computer science 5(3),* pp. 214-220, 2009.
17. 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, pp. 35-44, January 2007.
18. Thuc N. Nguyen, Bao. N. Tran, Duc H. M. Nguyen. **A lightweight solution for wireless LAN: Letter-Envelop Protocol**, *Communication and Networking in China, Chinacom IEEE Xplore*, 2008.
19. Chibiao Liu and James Yu. **A Solution to Wireless LAN Authentication and Association DoS Attacks**, *IAENG International Journal of Computer Science,* August 2007.
20. Baber Aslam, M Hasan Islam and Shoab A. Khan. **Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack**, *IEEE Xplore*, 2008.

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 23 years of experience in teaching and 15 years of experience in research. He has published more than 129 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 twelve research papers in the International/National Conferences and Journals. Her other areas of interest include OOAD & UML, Software quality assurance and Testing and Computer Networks.