Inhibition of Denial of Service Attack in WLAN using the Integrated Central Manager

B. Vani
Lecturer
Dept of Comp.Sci & Engg
Bharathidasan University
Trichirappalli, TN, India.

L. Arockiam
Associate Proffessor,
Dept. of Computer Science
St. Joseph's College
Trichirappalli, TN, India.

A. Persia
Research Scholar,
Dept of comp. sci & engg, Bharathidasan university, Trichirappalli, TN, India.

S. Sivagowry
Research scholar
Dept. of comp. sci & engg.Bharathidasan university, Trichirappalli, TN, India.

ABSTRACT
Denial of Service (DoS) attack is a major problem prevalent in Wireless Local Area Network (WLAN). Many security techniques were introduced to prevent the DoS attacks in WLAN. However, there are still many weaknesses which provide interest and way for hackers to do such attacks. This research mainly deals with the two types of DoS attacks, namely EAPOL (Extensible Authentication Protocol over LAN) start and EAPOL logoff frame over Access Point (AP) and wireless client. The experimental test bed is taken and the solutions are simulated using NS-2, a Linux based simulator, to analyze how far it prevents the DoS attacks in WLAN. The Central Manager (CM) along with Intruder Database (IDB) is proposed to defend the two different types of attacks targeted on Access Point and Client. The CM and IDB can be combined together and called as Integrated Central Manager (ICM). It acts as an Authenticated Server (AS) which manages the communication between the client and the Access Point. The proposed solution increases the throughput. When there is a chance of the failure of the ICM, maintaining a duplicate ICM is proposed which secure the client and Access Point from the attacks.

Keywords
WLAN Security, Denial of Service, MAC Spoofing, Central Manager, Intruder Database.

1. INTRODUCTION
Wireless Local Area Networks (WLAN) are popular due to easy installation and it offers increased wireless access to the client with the help of Access Points (AP). Providing a better communication for data transferring in a wireless medium without hindrance is a challenging task. Intruders can easily access the network by pretending themselves as authenticated users. Denial of Service (DoS) attack is one kind of attack which is made by the intruders in a WLAN environment. In an infrastructure WLAN environment, all the nodes are connected through a central device called an Access Point (AP).

The AP does not have any firewall to protect WLAN against vulnerabilities. So it makes the DoS attack more serious. There are number of attacks possible in WLAN [1, 2]. But many people are not aware of the Denial of Service (DoS) attacks. Number of studies have been taken to avoid DoS attacks [3,4] and different security protocols were also proposed and implemented over WLAN such as 802.11i [5], Wired Equivalent Privacy (WEP) [1,6], Wi-Fi Protected Access (WPA) [2], 802.11 [7,8], 802.11b [9], 802.1x and 802.1w [10,11]. None of them provide specific solution to avoid DoS attacks [12, 13]. This paper proposes an improved solution called the Integrated Central Manager (ICM) which is found to be an effective method for preventing Denial of Service (DoS) attacks in WLAN.

In this paper, section III describes the four types of DoS attacks. Section IV describes how the ICM avoid DoS attacks in Wireless Local Area Network (WLAN). Section V analyzes the performance of ICM in the real time environment and simulation. In Section VI, the results of the ICM in WLAN are discussed based on throughput with a graphical representation.

2. RELATED WORK
Ping Ding [14] describes an efficient solution to avoid DoS attacks for WLAN using Central Manager (CM). CM acts as a back end server which maintains three tables and timer to detect DoS attacks.

Mina Malekzade et al., [15] developed an experimental framework to measure the possible attacks using unprotected Extensible Authentication Protocol (EAP) frames against wireless communication.

Mofreh Salem et al., [16] proposed an Intruder Database (IDB) technique which prevents the intruders to bring down the network by DoS attack.

Abdul Azim Abdul Ghani et al., [12] developed an extension module for wireless DoS attacks using object modular network test bed in a C^{++} ($OMNeT^{++}$). $OMNeT^{++}$ is an open source C^{++} environment with a Graphical User Interface (GUI) support.

3. DENIAL OF SERVICE ATTACKS (DoS) IN WLAN

WLAN are subject to different types of vulnerabilities. DoS attacks are the most challenging issue on the WLAN. It causes to reduce throughput of wireless communication for its authorized clients [5]. The attacks taken under the study are EAPOL start frame and EAPOL logoff Frame targeted to Access Point and Client [15].

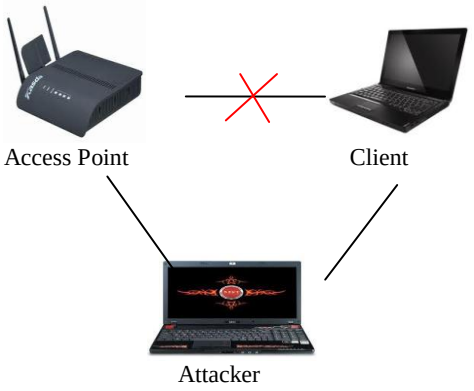

Fig 1: DoS in WLAN

Fig 1 describes how the DoS attack takes place in WLAN. It shows that the attacker attempts to make computer resources unavailable to its legitimate users by sending forgery EAP frames targeted to AP or client.

3.1 EAPOL start frame over the AP

Wireless clients gain access to the network after sending an EAPOL start frame to the AP. Communication between AP and client will start after AP accepts the client's request by checking the user's identity. This is depicted in the figure 2. When clients are communicating with AP, an attacker sends a forgery EAPOL start frame to AP by spoofing the legitimate client's MAC address to make AP busy with an attacker and unable to handle legitimate traffic. So the client and AP's communication is discarded [17].

3.2 EAPOL start frame over the client

In this type of attack, an attacker sends a forgery EAPOL start frame to the client in the mid of normal transmission by spoofing AP's MAC address. The below Fig 2. describes how the EAPOL start frame attack takes place in WLAN.

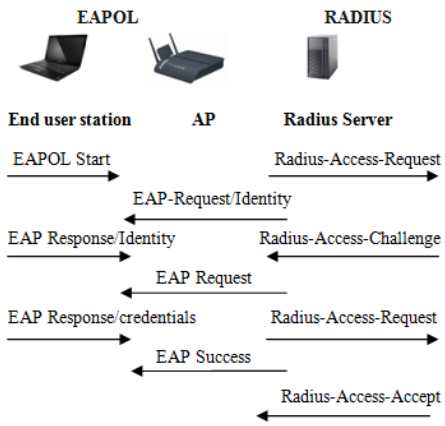

Fig 2: EAPOL start frame

3.3 EAPOL logoff frame over AP

When a client wishes to leave from WLAN, it sends EAPOL logoff frame to AP. By using this chance, an attacker spoofs the client's MAC address and sends EAPOL logoff frame to AP. In this case, AP considers this request is from one of the client and proceeds with logoff message to legal client. Then it disassociates the client from the transmission.

3.4 EAPOL logoff frame over client

An attacker sends an EAPOL logoff frame to the targeted client by spoofing AP's MAC address. The client thinks that the legitimate AP wants to logoff because of heavy traffic and accepts the logoff request.

4. INTEGRATED CENTRAL MANAGER

To prevent the DoS attacks discussed above, there is a need to follow a new mechanism which identifies the intruder and prevent him entering the network. Central Manager (CM) and Intruder Database (IDB) are clubbed together and formed an Integrated Central Manager (ICM). It manages all the activities of client and AP to detect and block an attacker from entering into WLAN. ICM is intended to prevent the Denial of Service attacks in an infrastructure network by maintaining five tables and a timer.

4.1 Tables maintained by ICM

The tables can be named as Accounts (T1), Intruder (T2), Authenticated Client (T3), Unauthenticated Client (T4) and Client table (T5). The descriptions of the tables are as follows: Account table is for checking the client identity based on their Medium Access Control (MAC) address. Intruder table contains the MAC address of all the intruders which was detected and spoofed by ICM. Authenticated table consists of MAC addresses of (working) clients who are in the communication process and their login and logout time. Unauthenticated client table records the MAC address, login and logout time of wireless clients who are not in communication with AP. Client table contains MAC address and login time of all the clients. The sample table is shown in Table 1.

Table 1. Authenticated Client table (T3)

MAC address	Login time	Logout time
70-71-BC-31-C3-8E	2:52:43 PM	2:56:16 PM
70-71-BC-31-C3-8E	2:53:29 PM	2:59:11 PM
F0-4D-A2-BF-C4-75	2:55:58 PM	2:57:08 PM
70-71-BC-31-C3-8E	2:58:14 PM	2:59:16 PM

4.2 ICM in DoS Attacks

It acts as an authentication server and takes responsibilities of AP to manage the AP and client communication, detect and block the intruders in a WLAN.

4.2.1 EAPOL start frame over the AP

An attacker sends EAPOL start frame to AP by spoofing authenticated client's MAC address else send request to AP by using his own MAC address. When an attacker sends an EAPOL start frame to AP, ICM will check in T2. If the address is found in T2, the request will be ignored by the

ICM. Otherwise it goes to T3. If the particular MAC address is already in T3, ICM infers that the request is from an attacker and will spoof the forgery client's MAC address and stores it in T2. If it is not in T3, it checks in T5. If it does not match, ICM spoof and records the MAC in T2.

4.2.2 EAPOL start frame over Client

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

4.2.3 EAPOL logoff frame over AP

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

4.2.4 EAPOL logoff frame over Client

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

5. PERFORMANCE EVALUATION

To evaluate the performance of ICM, It is implemented in both real time and in simulation environment. The solution is validated by measuring the throughput before and after implementing the ICM.

5.1 Test Bed for Real Time Environment

The experimental setup consists of one AP, one target client and one attacker. Configuration requirements are as follows:

- One PC (CPU: Intel i3, RAM 2 GB, HDD 80GB) as Wireless Client.
- One PC (CPU: Intel i5, RAM 2 GB, HDD 80GB) as Attacker.

Initially, the client and AP are allowed to communicate. When the client sends EAPOL start frame request to AP, ICM checks its MAC address in T2. After checking in T2, it accepts the request, if the MAC address of the client is not in T2. After acceptance, AP and the client will communicate. The attacker will both spoof the MAC address of the AP or client and send EAPOL start frame or log off request. The request will be automatically sent to the ICM. It checks in T2, if the MAC address is not in T2, it checks in T3 since T3 contains the address of the authenticated clients. While checking in T3, it identifies that the request is from hacker. To confirm that, it sends encrypted message to either the client or AP, depending on the attacks. After confirmation, it infers the request is from the hacker and it automatically spoofs the hacker's MAC address and stores it in T3.

5.2 Simulation in NS-2

We set up a simulation environment to show the performance of ICM. 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 [18, 19]. The description is given in Sec VI.

6. RESULTS AND DISCUSSIONS

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 ICM is better in preventing DoS attacks when compared with the existing Central Manager (CM) and Intruder Database (IDB).

6.1 Central Manager (CM)

The simulations are built on Network Simulator NS-2 and uses Case-Based Reasoning (CBR) applications as traffic generators. The CM's performance is evaluated by simulation, based on throughput and delay time. The attacks are simulated in two parts, login part (EAP start and 802.11 Association) and logout part (EAP failure, EAPOL logoff, MAC disassociation) [14].

From the following Figures 3 and 4, it is found that the throughput with CM is much better than throughput without CM. The same result is observed for delay time in WLAN. Simulation result for logout attack is same as for login attack. With CM, the WLAN's efficiency and performance is improved [14].

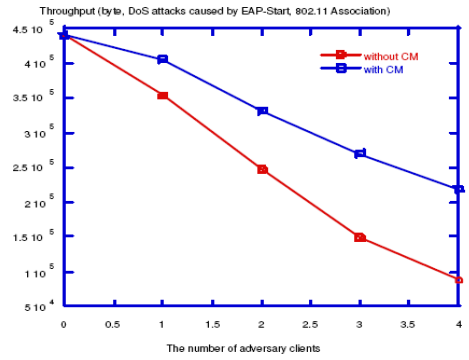

Fig 3: Throughput (Login DoS Attack) [14]

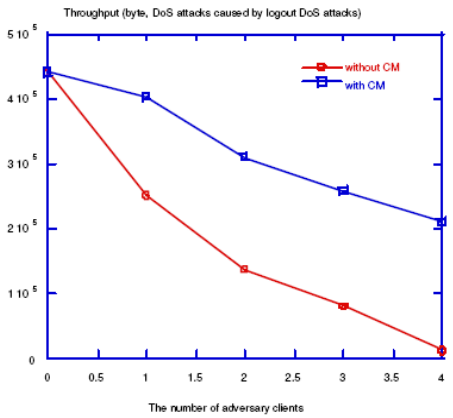

Fig 4: Throughput (Logout DoS Attack) [14]

6.2 Intruder's Database (IDB)

IDB creates and modifies the database when an intruder is detected. This database prevents the intruders from bringing down the network by DoS attacks. The simulation results of this technique measures the probability of denied service with respect to the number of attacks and the maximum number of connections that the AP allows. The simulation result shows that the Probability of Denied Service (PDS) is decreased at different attack rates and increases the number of connections that the AP allows after using the IDB [16].

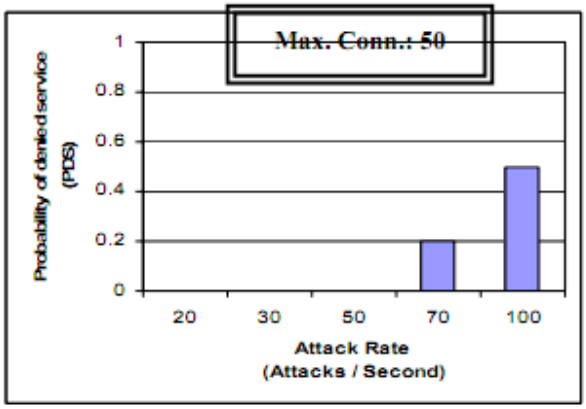

Fig 5: Attack rate in 50 connections [16]

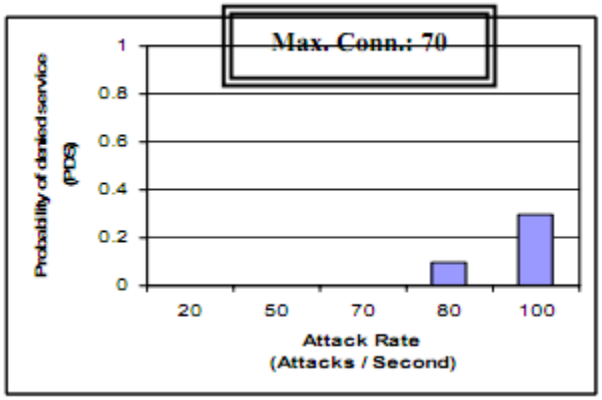

Fig 6: Attack rate in 70 connections [16]

The above figures 5 and 6 show that, as the attack rate increase, the PDS increases. However, when the maximum number of connections increases, the technique was able to defeat attacks at higher rates (at 50 and 70 connections) [16].

6.3 Integrated Central Manager (ICM)

By using CM, it is observed that the DoS attack is reduced. It uses 802.11 MAC protocol to show the effects of DoS attacks. Apart from preventing the attack, it also improves the performance of WLAN. But, in the case of failure of CM, the whole transmission is collapsed, as the attacker can easily make DoS attacks. In the case of IDB, 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, the hacker can easily get the key. IDB does not prevent the DoS attacks when the hacker enters by using a MAC address which is not yet installed in the database. To overcome the drawback of CM we propose ICM which clubs the concept of CM and IDB. It also maintains a duplicate ICM, which will take over the network, in case of failure of ICM. ICM will update the duplicate ICM often.

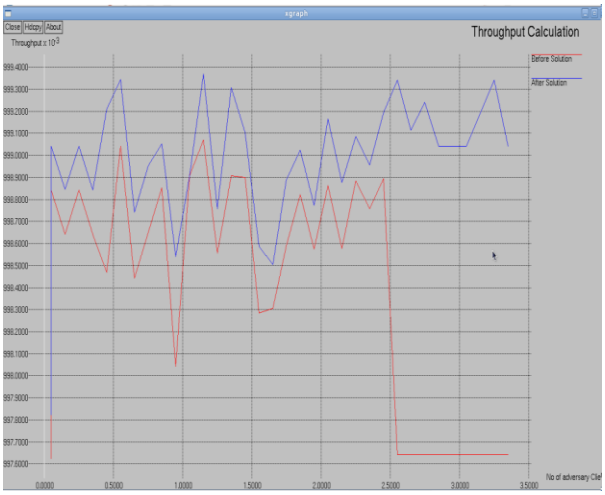

Fig 7: Results using the Existing and Proposed Solutions

The simulation scenario is set by taking AP as one node, client as other node and attacker as another node. At the beginning of the simulation, AP and client are in communication. At that time attacker will hack the MAC address of client and start the attack. During the attack the throughput is found to drop because the attacker will permanently stop the communication. This is observed through the graph generated by NS2 by taking time/second in X axis and throughput along Y axis. After implementing the solution the attacker cannot do the attack because the client authentication is based on the tables maintained by ICM. Hence ICM can easily identify the intruder and block him. Hence the throughput won't drop as shown in the figure7. The performance of the CM, IDB and ICM are compared based on the throughput. The result observed is represented in Figure 8.

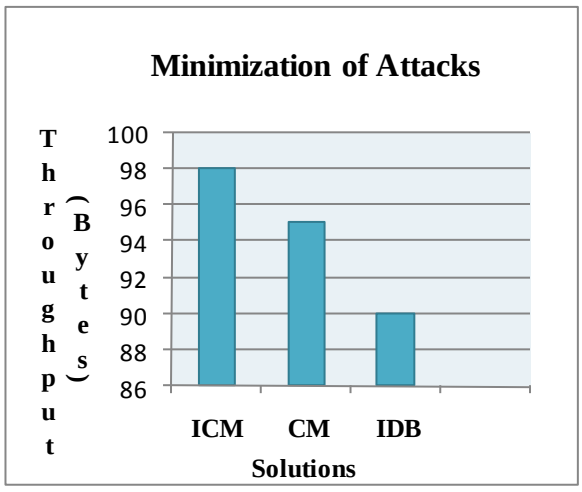

Fig 8: Comparison between Existing and Proposed Solutions

7. CONCLUSION

From the simulation results the Integrated Central Manager (ICM) improves the WLAN's performance apart from preventing the attacks. The added advantage in ICM is that it spoofs and stores the intruder's MAC address without the knowledge of the intruder. The throughput is increased in ICM compared to CM. The DoS attack can be easily prevented by checking the intruder table which is maintained by ICM. The proposed solution prevents the DoS attack completely whereas Central Manager (CM) and Intruder database (IDB) only minimizes the attacks. But the maintenance of duplicate ICM will increase the traffic over head. But it prevents the network from the total drop of throughput when compared with CM and IDB.

8. REFERENCES

[1] Abhishek Gupta and Manish Garg, "DoS Attacks on IEEE 802.11 Wireless Networks and its Proposed Solutions", http://ssrn.com/abstract, April 2010.

[2] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, Behrang Samadi, "A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i)", *2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT),Beijing, China*, pp. 48-52, August 8-11,2009.

[3] Arockiam .L. and Vani .B, "A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network", *International Journal on Computer Science and Engineering*, Vol.02, No. 05, pp. 1563-1571, 2010.

[4] Arockiam. L and Vani .B "A Comparative Study of the available Solutions to Minimize Denial of Service Attacks in WLAN", *International Journal of Computer Technology and Application*, Vol 2 (3), pp. 619-625, 2011.

[5] 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.

[6] Radomir Prodanovic and Dejan Simic, "A Survey of Wireless Security", *Journal of Computing and Information Technology*, CIT 15, 3, pp. 237-255, 2007.

[7] John Bellardo and Stefan Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions", *USENIX Security Symposium*, Washington D.C., 2003.

[8] Kemal Bicakci and Bulent Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", *Computer Standards & Interfaces*, pp. 931–941, 2009.

[9] F. Ferreri and M. Bernaschi, L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks",Wireless Networks, vol 14, pp. 159-169, 2008.

[10] Nancy Cam-Winget, Russ Housley, David Wagner and Jesse Walker, "Security flaws in 802.11 data link protocols", Communications of the ACM, Vol.46, Issue. 5, May 2003.

[11] Stanley Wong, "The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards", GSEC Practical v1.4b, May 2003.

[12] Mina Malekzadeh, Abdul Azim Abdul Ghani, Shamala Subramaniam, and Jalil Desa, "Validating Reliability of OMNeT^{++} Wireless Networks DoS Attacks: Simulations vs. Testbed", *International Journal of Network Security*, Vol-13, No. 1, pp. 13-21, 2011.

[13] 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.

[14] Ping Ding, "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.

[15] Shamala Subramaniam, Mina Malekzadeh, Abdul Azim Abdul Ghani and Jalil Desa "Vulnerability Analysis of extensible Authentication Protocol (EAP) DoS Attack over Wireless Networks*", The International Journal on Computer Network and Internet Research, CNIR*, Vol 9, Iss. 1, pp. 39-46, July 2009.

[16] Mofreh Salem, Amany Sarhan and Mostafa Abu-Bakr "A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks", *The International Congress for global Science and Technology-CSIR*, Volume (7), Issue (1),pp. 17-24 , July 2007.

[17] 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 , pp. 53-58, January 2004.

[18] http://www.scribd.com/doc/52291274/Network-Simulator-2-Manual. The ns Manual, *the VINT Project*, January 6, 2009.

[19] Baber Aslam, Monis Akhlaq and Shoad A. Khan, **"**802.11 disassociation DoS attack simulation using Verilog", *World Scientific and Engineering Academy and Society*, Vol 7, pp. 198-206, March 2008.

[20] Tutorial for the Network Simulator "ns", available at http://www.isi.edu/nsnam/ns/tutorial/

9. AUTHORS PROFILE

1. Vani. B is working as Lecturer in the Department of Computer Science & Engg., Bharathidasan University, Trichy, Tamil Nadu, India. She has 12 years of experience in teaching and 2 years in research. Her area of research is Wireless network security. She is presently working on Denial of Service attack on wireless network. She has published about ten papers in National/International conferences. Her other areas of interest include OOAD & UML, Software quality and Testing and Computer Networks.

2. Arockiam. L is working as Associate Professor in the Department of Computer Science, St. Joseph's College (Autonomous), Trichirappalli, Tamil Nadu, India. He has 23 years of experience in teaching and 15 years of experience in research. He has published 80 research articles in the International/ Journals and National Conferences. 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.

3. Persia. A is a Research Scholar in the Department of Computer Science & Engg., Bharathidasan University, Trichy, Tamil Nadu, India. She is presently working on wireless network security. She has also presented 2 papers in National Conferences.

4. Sivagowry. S is a Research Scholar from Department of Computer Science & Engg., Bharathidasan University, Trichy, Tamil Nadu, India. Her area of research is to study the security attacks on wireless network and presented a paper in National Conference.