A Survey of Denial of Service Attacks and it's Countermeasures on Wireless Network

Arockiam. L
Associate Professor,
Department of Computer Science,
St. Joseph's College,
Trichy -2.

Vani. B
Lecturer
Department of Computer Science & Engg.,
Bharathidasan University,
Trichy – 23.

***Abstract* - Wireless networks are popular among the Laptop user community today because of the mobility and ease of use. People working through wireless connection must be aware of the surroundings due to the various types of attacks made by the intruders. One of the major attacks in wireless 802.11 WLANs is Denial of Service attack (DoS). Even though the users protect their systems with Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security protocols, DoS attack is still prevalent. This paper makes a survey on different types of DoS attacks and their countermeasures on the infrastructure networks which are based on the Access Points (AP). In this paper, the main attacks called Deauthentication and Disassociation Flooding DoS attacks are studied through experiments and the possible solutions are recommended. This paper also studies the vulnerabilities due to rogue access point, null data frames and Access Points. The various solutions suggested for this problem like Pseudo randomized sequence number based solution to 802.11 disassociation, Pseudo random number based authentication to counter DoS, Dual authentication for fast handoff in IEEE 802.11 and Letter Envelop Protocol as a light weight solution are studied and reported.**

Key Words - Access Points, DoS, Wireless Security, 802.11, Disassociation, Deauthentication, Flooding attacks.

I. INTRODUCTION

Wireless Local Area Networks (WLAN) have gained popularity as compared to the wired network due to the flexibility, low cost and easy deployment layouts. WLAN are widely used by laptop users on the corporate and educational environments. However, some fundamental weaknesses of the wireless access medium make wireless networks more vulnerable to attacks [1].

The IEEE 802.11 is the adopted standard for WLANs. The standard was approved in 1999 and reasserted in 2003. WLAN used Wired Equivalent Privacy (WEP) as the security protocol to achieve Confidentiality, Authentication and Integrity services. WEP offered two authentication schemes – Open system authentication and shared key authentication. It uses Rivest Cipher 4 (RC4) for confidentiality and for integrity Cyclic Redundancy Check 32 (CRC 32) is used [2]. But the architecture did not provide solutions to already discovered security weaknesses [3].

Since WEP did not provide the adequate level of security, IEEE proposed Wi-Fi Protected Access (WPA) and 802.11i [4] as the security standards for WLANs. WPA was designed as an intermediate security protocol to improve upon the level of security offered by WEP, until the final security protocol in shape of 802.11i could be ratified by IEEE Task Group i.

The 802.11i standard (ratified in 2004) offers a choice to use either 802.1x or Pre Shared Key for Authentication and Key Management (AKM) [5]. It employs Advanced Encryption Standard (AES) as the cipher in a newly designed protocol, namely Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP), as the default protocol for Confidentiality and Integrity. The use of 802.1x / Pre Shared Key (PSK) authentication, together with AES CCMP, forms a Robust Security Network Association (RSNA). The other option is to use Temporal Key Integrity Protocol (TKIP) for Confidentiality and Message Integrity Code (MIC) for Integrity [6]. Though TKIP does offer a much better security level than WEP, CCMP is the default and recommended protocol in 802.11i [7] due to its arguably uncompromised confidentiality and Integrity services. It is important to note that even 802.11i has not been designed to address potential threats to availability. The management and control frames of 802.11 based WLANs are still unprotected/ unauthenticated [8]. Consequently, WLANs, even with the deployment of 802.11i, are susceptible to Denial of Service (DoS) attacks.

A Denial of Service (DoS) attack is an attack that can disable a WLAN. All companies that are deploying WLAN should consider this DoS attack. One form of DoS attack is the "brute force" method. This attack has two forms: either a huge flood of packets that uses up all of the network's resources and forces it to shut down, or a very strong radio signal that totally dominates the airwaves and renders access points and radio cards useless. A hacker can make a packet-based brute force DoS attack by using other computers on the network to send the useless packets to the server. This adds significant overhead on the network and takes away useable bandwidth from legitimate users.

In the past, several defense techniques have been proposed to build DoS resistant 802.11 WLANs [9]. However, none of these address the complete range of attacks that can be launched based on the unprotected management and control frames. These include deauthentication, disassociation, Request to Send (RTS)/ Clear to Send (CTS) and Acknowledgment (ACK), and Power-Save Poll (PS-Poll) message based attacks.

The organization of the paper is as follows: Section II deals with the background and related works on DoS attacks and countermeasures. Section III presents the WLAN threats and vulnerabilities. Section IV studies the types of Denial of Service attacks in detail. This section deals with the Rogue access point based DoS attacks and Null data frames vulnerabilities against 802.11 WLANs. Section V describes an experimental study on access point vulnerabilities to DoS attacks in 802.11 networks and discusses the results collected for each network configuration. Section VI presents a summary of possible solutions to various DoS attacks like Pseudo random number based authentication, Pseudo Randomized Sequence Number based solution to Disassociation DoS attacks. It also discusses the Dual authentication methods, Letter Envelop Protocol and Secure WLAN (SWLAN) methods as countermeasures to DoS attacks. Section VII presents the discussion based on the results of various DoS attacks and the suggested solutions.

II. BACKGROUND

"A Survey of Wireless Security**"** [1] presents a summary of security improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection. Comparative analysis shows the advantages of the new 802.11i standard in comparison to the previous security solutions.

M.Bernaschi et al. [10] reports the access point vulnerabilities to DoS attacks in 802.11 networks with experiments on various network configurations. The experiments showed that the extent of vulnerability to DoS attacks strongly depends on the firmware used by the Access Points.

Baber Aslam et al. [12] suggests a Pseudo Randomized sequence Number based solution to 802.11 Disassociation DoS attack. He suggests that the solution does not require any additional hardware and can be implemented in both wireless clients and Access Point via firmware upgrade.

Masoor Ahmed Khan et al. [13] suggests a Pseudo Random Number based Authentication to counter DoS attacks on 802.11. He presented a mechanism which can be easily deployed as a comprehensive solution to all the discussed DoS attacks without any additional hardware or infrastructure requirements.

III. WLAN THREATS AND VULNERABILITIES

Before analyzing the DoS attacks, it is important to categorize the likely capabilities of the attacker. WLAN traffic consists of data frames, management frames and control frames. An attacker can manipulate these frames which affect the data integrity, confidentiality, authentication and availability. This is called as threat. The following sections describe the various types of threats and vulnerabilities [14].

A. *Eaves dropping/ Traffic analysis*

This type of attack includes sniffing, war driving, war walking, active eaves dropping, passive eaves droppings and traffic analysis. This attack takes advantage of the weak encryption and always compromise the data confidentiality.

B. Message modification

All the attacks aimed at modification of data such as network injection falls in this message modification category. These attacks compromise the integrity of information and data.

C. Rogue devices

This include rogue AP, rouge applications, soft Ps, Accidental associations, unauthorized Ad hoc networks. These devices may lead to compromise of the data and information confidentiality, integrity loss or questionable authenticity or non-repudiation. Rogue devices can launch replay attacks and malicious association.

D. Session Hijacking

The attacker planning this attack waits for a valid session to be initiated between a valid node and an AP. The attacker then acts as a valid node to the AP and valid AP to the node. The attacker sends a dissociation message to the node and continues acting as a valid node, completely taking over the session from the legitimate node who believes the session was terminated by the AP. The attacker can now mine for more information such as SSID and password.

E. Man-in-the Middle attacks

Some malicious AP between the client and the AP may act as legitimate AP or client may fool the user. Once both the AP and the client is fooled into this association, the man-in-the middle attack can intercept communication, read unencrypted information, can get passwords and even compromise the system further by denied legitimate users access to the resources. After a successful MAC spoofing, an attacker can ensure that each fake management frame from his device has a unique fake MAC address. This helps the attacker to simulate a network scenario where many stations send requests to AP. In this scenario the attacker is capable of launching the following Denial of Service attacks.

IV. DENIAL OF SERVICE ATTACKS

The use of 802.11 wireless networks is increasing despite of the security problems related to authentication, privacy and confidentiality issues. The wireless medium is more susceptible to Denial of Service attacks than the wired networks [15]. This is due to the undefined physical

boundaries of the wireless networks. A malicious station can appear in the range of such a network and launch an attack in order to stop any legitimate communication. The different types of DoS attacks are discussed in the following sections A to E.

A. Security attacks on WLANs

Crypto attacks and DoS attacks are the two main security attacks on WLANs [16]. Crypto attacks are related to the weaknesses of authentication and encryption procedures. This sort of attacks can be resolved with cryptographic solutions with strong authentications, encryptions and data integrity. DoS attacks can be launched against either Wireless Access Points (AP) or wireless clients. Authentication request flooding, Association request flooding, deauthentication flooding, disassociation flooding and distributed denial of service attacks are the different types of DoS attacks. The authors focused on three types of attacks: deauthentication and disassociation attacks rely on the repeated injection of fake deauthentication or disassociation frames (both from the AP to STAs and from a STA to the AP) in order to cause legitimate clients to be disconnected from the AP in use [10]. A third kind of attack is based on a malicious manipulation of the Network Allocation Vector (NAV) information contained in 802.11 frames, in order to prevent legitimate stations from gaining access to the medium.

Actually, deauthentication and disassociation attacks were already known in the developer's community, and proved to be really effective. The virtual carrier-sense attack (i.e., the malicious manipulation of the NAV) is more original and, in principle, harder to defend against in practice. The authors tested the NAV attack both by means of simulations (based on *ns*-2) and in real test-bed networks. The authors commented that although the attacks proved to be effective in the simulation environment, they didn't lead to relevant results when applied to real-world networks.

B. The 802.11 Operation

Before analyzing the DoS attack, it is important to understand the 802.11 operation. The basic 802.11 operation is illustrated in Figure. 1[17]

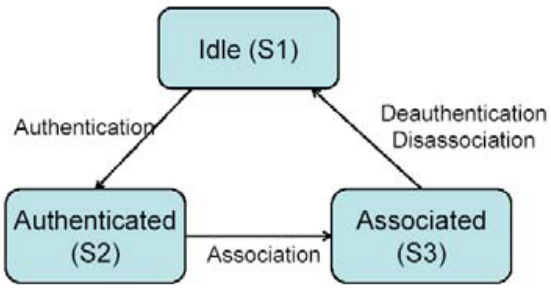

Figure 1. 802.11 Operation states

A wireless client follows the authentication and association procedures to establish a connection to an AP. At any time, the AP could send a disassociation or deauthentication frame to terminate the connection. According to the 802.11 standard, deauthenticaton and disassociation are *notification and cannot be rejected*. As a result, it is relatively easy for a hacker to send a faked deauthentication or disassociation frame to a client and terminate its wireless connection to the AP. The solution proposed is based on the results from simulation and theoretical analysis by applying Markov chain model.

C. Security Vulnerabilities of Null data frames

Null data frames are a special and important type of frames in 802.11 WLANs. They are special because their *Frame Body* fields are empty, and they are the only type of frame whose usage is not explicitly specified in the IEEE 802.11 standard. There are two types of attacks namely functionality based DoS attacks and implementation based fingerprinting attack. In this paper, the author studies the functionality *based* Denial-of-Service attacks [18]. In these attacks, the attacker spoofs the identity of the victim station, and sends fake null data frames to mess up with the intended functionalities of null data frames. Second, they study the *implementation based fingerprinting attack*. In this attack, the attacker takes advantage of implementation variations of null data frames, and correlates the frames sent from seemingly different stations by the unique behaviors in using null data frames. The IEEE 802.11 data frame format is given in the figure. 2 [18]

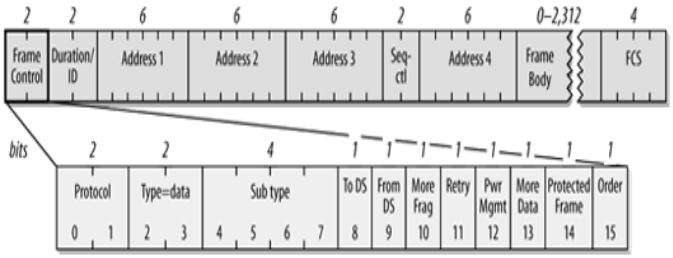

Figure 2. IEEE 802.11 data frame format

Although IEEE 802.11 standard does not explicitly specify the usage of null data frames, they are in fact widely used in reality. The main functionalities of null data frames are state switching in power management and channel scanning, and association keeping alive during idle period. When null data frames are used for state switching, an attacker can spoof the identity of a station in sleeping state or scanning in another channel, and generate fake null data frames to fetch the buffered frames of the victim station [19].

D. Disassociation DoS

A station sends a disassociation notification to another station if it wishes to terminate the association. Disassociation frame

can either be sent by a wireless client to an AP or by an AP to one or all wireless clients. On receiving a disassociation frame an AP or a client clears relevant states and keys from its memory. Disassociation happens when a mobile station has established authentication/association with another AP and wants to terminate its association with previous AP [20]. An AP can also broadcast a disassociation to terminate its connection with all currently associated stations.

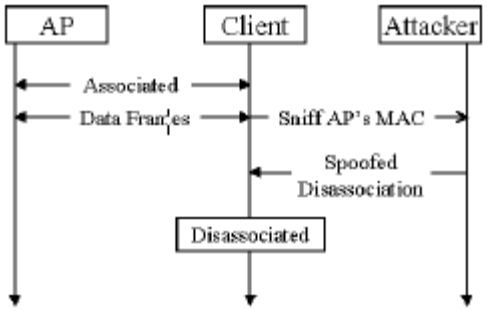

Figure 3. Disassociation DoS attack [20]

A disassociated station can neither send nor receive data; it has to restart communication setup process. DoS can take place if spoofed disassociation notifications are sent repeatedly. J. Bellardo et al. has shown the practicability of this attack in figure 3 [20], further many DoS attack tools such as Airjack [21], KisMAC, VoidlI etc can be successfully used to launch this attack.

E. Deauthentication message attack

When a supplicant discovers an AP via a beacon frame or a probe response to a probe request, it proceeds to authenticate itself to the AP. This is achieved via authentication mechanisms. The authentication mechanism under 802.11 also allows authenticated client or AP to deauthenticate itself with the other entity. The deficiency in this framework is that deauthentication message is neither cryptographically protected nor authenticated. As a result, any attacker may forge this message by either impersonating as the supplicant or the AP [22]. Consequently, the other entity egresses from the authenticated state and discards all subsequent communication, until the two get reauthenticated. Repeated transmission of these forged messages may deny service to the impersonated entity.

V. EXPERIMENTS ON DoS

Following a study of various types of DoS attacks, there are various experiments made to identify the type of attack. Once the type of the attack is identified, the countermeasures can be proposed accordingly. The following sections present the experimental reports of various types of DoS attacks.

A. Experimental results of Access Point Vulnerabilities

To study the access point vulnerabilities to DoS attacks on 802.11 networks, experiments are done on different network configurations like Enterasys RoamAbout R2 managed network, Netgear ME102 managed network, 3com access point 8000 managed network, Host AP, PC based managed network, D-Link DWL -1000AP, Linksys WRT54g, Netgear WG602, Cisco AP 350 and Compaq/HP WL520. The following figures 4 and 5 present the Packet loss and response times respectively [10].

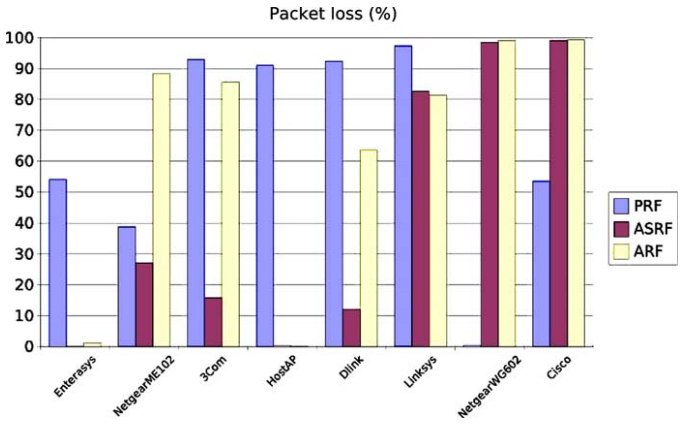

Fig 4. Packet loss (%): compares the results of all APs

Figure 4 compares the packet loss experienced by all the APs tested under the three different attack techniques namely Probe Request Flood (PRF), Authentication Request Flood (ARF) and Association Request Flood (ASRF). It is apparent how no AP is fully immune although some APs are much more vulnerable than others [23].

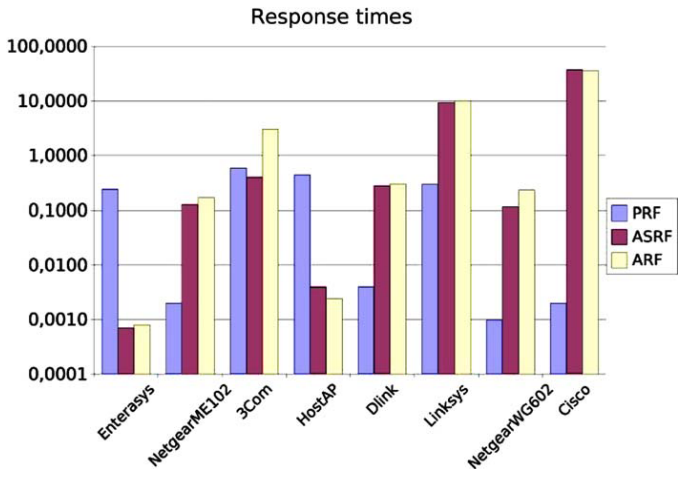

Figure 5. Response time's comparison

Figure 5 shows a similar comparison for the response times of the APs under attack. PRF, ARF and ASRF flooding attacks

can be executed by any malicious station in the area of a wireless infrastructure network, without being neither associated nor authenticated to the access point; – the minimum frame injection rate required to cause a DoS depends on the AP in use [24]. AP's main vulnerability to these flooding attacks seems to reside in unacknowledged frame retransmission, which causes memory buffers exhaustion and freezes AP functionalities; – weak implementations of the 802.11 protocol in the access points can determine further vulnerabilities, which allow malicious stations to crash an AP, or to prevent other legitimate stations from associating to the AP. From the above experiment the authors prove that any attacker with simple software and hardware can make a DoS attack with minimum effort.

B. *Rogue Access Point based DoS attacks*

To study the Rogue access points based DoS attacks against 802.11 WLANs, another experiment with simulation is made by the authors Chibiao Liu and James Yu [17]. The experimental set up is depicted in the figure 6. The author suggests the experimental set up which is illustrated in Figure 6. The DoS attacking tool of void11 is installed on a Red Hat (kernel 2.4.29) Linux machine (Rogue AP), which is used to launch layer-2 flooding DoS attacks. The TCP (Transmission Control Protocol) traffic generator of wsttcp [25] and the traffic analyzer of Ethereal are installed on workstations of the Wireless STA and Test STA. The traffic generator and analyzer are used to measure TCP performances over WLANs.

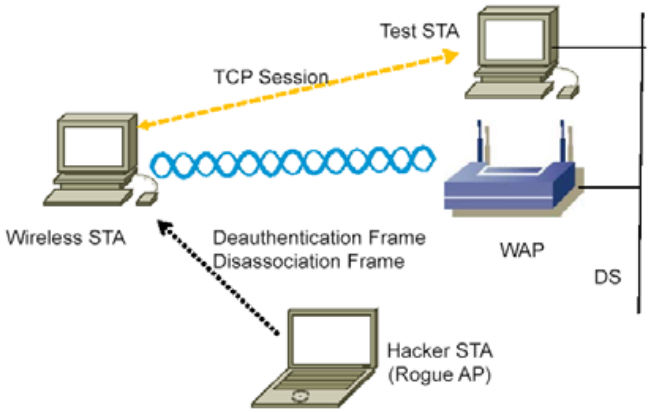

Figure 6. Experiments of DoS attacks [17]

During the experiment, a TCP session (with max data transmission rate) is maintained. When the rogue AP launches an attack, both the throughput data and the individual 802.11 frames for the packet flow analysis are collected which is illustrated in Figure 7 [17].

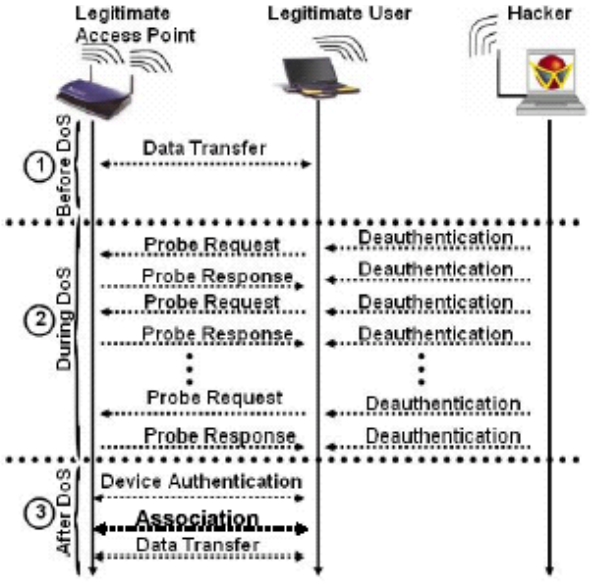

Figure 7. Flow analysis of Deauthentication attacks

From the above experiment the author shows that a hacker can easily terminate the data communication by sending faked deauthentication frames (or disassociation frames) [26] at a rate as low as one frame/sec. When the client tries to reestablish a new connection with the probe request, another deauthentication frame from the hacker would stop the new connection immediately. During the attack, the throughput immediately drops to zero.

C. *Security Vulnerabilities of Null Data Frames*

Null data frames are important type of frames in IEEE 802.11 based WLAN. They are widely used for power management, channel scanning and association keeping alive. These frames are lightweight and flexible to implement [27]. Such features can be taken advantage of the malicious attackers to launch a variety of attacks. In order to determine the feasibility of the above attack and its effectiveness, an extensive experiment is conducted by the authors Wenjun GU et al [19]. In this paper, the author studies two types of attack namely functionality based DoS attacks and implementation based fingerprinting attacks. The *attacker* conducts the DoS attack on the two victim *stations*, and the *logger* passively logs all wireless communications for later analysis. The experiment uses the Iperf as traffic generator and performance measurement tool. The server is installed with Iperf to generate TCP/UDP traffic, while the stations are installed with Iperf to receive traffic and measure throughput. Each test lasts for 300 seconds. Initially, there is no attack in place. The attack is enabled at the 60*th* second, lasts for 60 seconds, and is disabled at the 120*th* second. Again, the attack is enabled at the 180*th* second, lasts for 60 seconds, and is disabled at the 240*th* second.

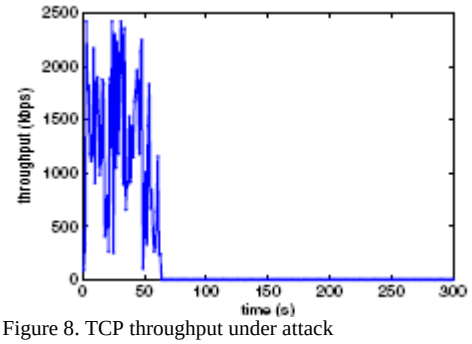

Figure 8. TCP throughput under attack

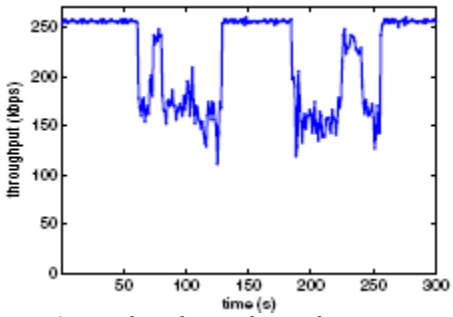

Figure 9. UDP throughput under attack

In Figs. 8 and 9 [27], TCP and UDP traffic are tested on Intel NIC with power saving mode enabled and MADWiFi access point respectively. From the fig. 8, the TCP throughput decreases to 0 immediately after attack comes at the 60*th* second. This is because the attacker keeps deleting the data from the access point. Even worse, the TCP connection is disconnected during the attack, and the throughput remains 0 after attack is disabled at the 120*th* second. This shows that consistent frame loss caused by the attack could cause TCP disconnection. Fig. 9 shows that UDP throughput degrades significantly during the time the attack is enabled. This is also because of the attacker deleting frames from the access point. However, UDP traffic is able to resume its normal throughput when the attack is disabled due to the connectionless nature of UDP. In summary, the author finds that the state switching based DoS attack has significant impact on both TCP and UDP traffic. TCP traffic is disconnected, while UDP traffic suffers from throughput degradation under attack.

So far, the experiments conducted from various situations were reported. From the results, the DoS attacks on WLAN 802.11 networks are ensured. The serious effect it causes to the security of the wireless network is emphasized through these experiments.

VI. SOLUTIONS TO DoS

The impact of DoS attacks are studied through different experiments in the previous sections. It is necessary to learn the possible and proposed solutions suggested by various research works to overcome DoS attacks in order to secure the wireless networking environment from malicious attackers. The following sections deal with the solutions proposed by different experiments conducted by various authors so far to mitigate DoS attacks.

A. Pseudo Randomized Sequence Number Based Solution to DoS

A sequence number based solution is suggested for disassociation DoS, which is one of the major attacks [29]. The authors Baber Aslam et al, suggests this solution as a robust one to overcome disassociation DoS attack [12]. The basic idea is to use a pseudo random sequence number (based on PTK) for a disassociation notification instead of a sequential sequence number [28]. The receiving side will confirm authenticity of notification by checking whether the pseudo randomized sequence number is within the range of acceptable sequence numbers or not. If not, the frame will be discarded, else processed. Since the attacker node will not have the keying material, he will not be able to calculate the sequence number. The incorrect sequence numbers will fail the attackers' attempt to spoof the disassociation frames. The solution will need a firmware upgrade. The percent success probability of novice attacker vs. expert attacker (who sniffs sequence numbers and generates frames with appropriate sequence numbers) against different sequence based solutions (using 5 frames gap) is given in figure 10 [12].

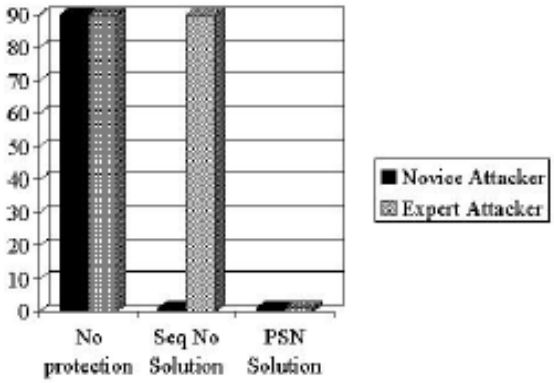

Figure 10. Percent Success Probability

B. Pseudo Random Number based Authentication to Counter DoS attacks

The proposed solution by the authors Mansoor Aahmed Khan et al is based on a modified Pseudo Random Number authentication mechanism that can be employed to counter all discussed DoS attacks on 802.11 based WLANs [13]. The Frame Control and Frame Check Sequence (FCS) are the only common fields present amongst all the management and control frames. The frame control field contains fundamental information in its subfields and does not contain sufficient

number of unused bits that can be utilized. This leaves only the FCS field which contains the IEEE 32-bit Cyclic Redundancy Code (CRC) [29]. The FCS field is the only feasible common field which may be utilized for incorporating the Pseudo random number based authentication mechanism for all management and control messages. The replacement of CRC32 with CRC16 would leave 16 bits in the FCS field which will be utilized for inserting the pseudo random number. It is suggested by the author that this solution could be an effective technique to resist deauthentication, disassociation and PS-Poll message based attacks.

C. *Letter envelop Protocol- Light weight solution to WLAN DoS attacks*

The solution proposed in this paper is an addition on current 802.11-based protocol. To prevent the disassociation attack, the authors, Thuc Nguyen et al, uses letter-envelop protocol to authenticate management frames in association process [30]. After authentication process between wireless station and access point, the association process takes place. Similar to attacking on the original 802.11protocol, they do the same flooding and dis'ing attack on proposed implementation system. The system can prevent these attack types. Table 1 and 2 [26] describe results of testing given by the authors.

Table 1. Result of AP overloads attack (Flooding)

Size of N (bits)	Defending against flooding attack
128	Stable
256	Stable
512	Stable

Table 2. Result of Dis'ing attack

Size of N (bits)	Defending against Dis'ing attack	
	AP	Wireless client
128	Stable	Stable
256	Stable	Stable
512	Stable	Stable

The above research suggests that the deployment is easy and only an addition to 802.11 based protocol. The association request/response message is modified to gain defending WLAN against DoS attack. This requires wireless systems update their firmware.

There are other proposed solutions to DoS attacks based on different situations like Rogue access point based DoS attacks and EAP based signaling Protocol for IEEE 802.11 WLANs [31]. When the Access Point vulnerabilities are controlled based on the various types of DoS attacks, the 802.11 WLAN can be secured against these attacks and provides a maximum secure environment to the user's community.

D. *DoS and Countermeasures*

The various DoS attacks and their countermeasures are tabulated in the table 3.

Table 3. DoS and countermeasures

Type of DoS attacks	Proposed Solutions
Deauthentication, disassociation and PS-Poll message based attacks.	Pseudo random number based authentication
Disassociation DoS	Pseudo randomized sequence number based solution
Disassociation DoS	Letter Envelop Protocol – light weight solution

There are certain proposed solutions to deauthentication and disassociation DoS attacks which are discussed by various authors. But there are no proposed solutions to DoS attacks such as probe request flooding, authentication request flooding, association request flooding, Network Allocation Vector (NAV) attacks, Null data frames and rogue access point based DoS attacks. The network Allocation Vector based attacks have some proposed countermeasures with ns-2 simulator, but it does not practically works well as stated by the author [10].

VII. CONCLUSION

The importance of overcoming DoS attacks on 802.11 WLAN environment is discussed in this paper. The various experiments to ensure DoS attacks are reported. The impact of DoS attacks may cause serious problems to the users since they are unaware of the attacker's intention. Once the type of DoS attack is identified, the defense mechanisms can be deployed on the network. Very recently new serious flaws in 802.11 equipment of major vendors have been reported. Although these vulnerabilities are due to problems in the management of packets at upper layers (arp requests and fragmented UDP packets), they confirm that much work remains to be done before wireless networks can be safely employed in locations (e.g., hospitals) where denial of service attacks could cause severe damage.

For Disassociation DoS attacks, there are few solutions proposed like a Pseudo Randomized Sequence number based solution and Letter Envelop Protocol solution. A robust solution based on pseudo random sequence number does not require any additional hardware and can be implemented in both wireless clients and AP via firmware upgrade.

The major attack called deauthentication can be overcome by the Pseudo Random Number based Authentication to counter DoS and Dual authentication can be adopted for fast handoff methods.

To resolve the problem due to Null data frames which are widely used in IEEE 802.11, some preliminary defense mechanisms are suggested. Similar attacks persist on the wireless networks that are yet to be mitigated.

REFERENCES

[1] Radomir Prodanovi and Dejan Simi, "A survey of wireless security", Journal of Computing and Information Technology - CIT 15, 2007, 3, pp – 237–255.

[2] Hani Ragab Hassan, Yacine Challal, "Enhanced WEP: An efficient solution to WEP threats", Wireless and Optical Communication Networks (WOCON), IEEE 2005, pp 594-599.

[3] Stanley Wong, **"**The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards**",** GSEC Practical v1.4b, 2007.

[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 2008*, Australia, January 21-23, 2008.

[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, CSIT 2009.

[6] J. Walker, "802.11 security series – part II: The Temporal Key Integrity Protocol (TKIP), Intel Corporation, 2002.

[7] Ezedin S. Barka, Emad Eldin Mohamed and Khadhim Hayawi, "End-To- End Security solutions for WLAN: A Performance Analysis for the underlying Encryption Algorithms in the Lightweight Devices", International Conference on Communication and Mobile Computing (*IWCMC'06)*, Vancouver, British Columbia, Canada, July 3–6, 2006.

[8] Aaron Sawyer, "A Brief Guide to Securing Wireless Networks: Closing the Back Door", Infosecwriters forum, 2008.

[9] 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.

[10] M. Bernaschi , F. Ferreri , L. Valcamonici, "Access points Vulnerabilities to DoS attacks in 802.11 networks, Springer Science+Business Media, LLC,2006.

[11] Daemen. J, Rijmen. V, " Rijndael: The Advanced Encryption Standard", Dr. Dobb's journal, March 2001, PP. 137-139

[12] Baber Aslam, M Hasan Islam, Shoab A. Khan, "Pseudo Randomized Sequence Number Based Solution to 802.11 Disassociation Denial of Service Attack", IEEE Xplore, 2008.

[13] Mansoor Ahmed Khan, Aamir Hasan, "Pseudo Random Number Based Authentication To Counter Denial of Service Attacks on 802.11 ", WCON Conference, Surabaya, Indonesia, IEEE Xplore, 2008.

[14] Ondiwa Nashon Odhiambo, E. Beirmann and G. Noel, " An Integrated Security model for WLAN", Conference on Africa, IEEE Africon, 2009.

[15] M. Zubair Shafiq and Muddassar Farooq, "Defence Against 802.11 DoS Attacks Using Artificial Immune System", Springer-Verlag Berlin Heidelberg , pp. 95–106, 2007.

[16] Anand balachandran **,** Geoffrey m. Voelker, Paramvir bahl, " Wireless hotspots: current challenges and future directions", Springer Science + Business Media, Mobile Networks and Applications 10, pp - 265–274, 2005.

[17] Chibiao Liu and James Yu, "Rogue Access Point Based DoS Attacks against 802.11 WLANs", The Fourth Advanced International Conference on Telecommunications, IEEE Xplore, 2008, pp-271-276.

[18] Wenjun Gu, ZhiminYang, Can Que, "On Security Vulnerabilities of Null Data Frames in IEEE 802.11 based WLANs", The 28th International Conference on Distributed Computing Systems (ICDCS), IEEE Xplore, June 2008, pp-28-35..

[19] Yasir Zahur and T. Andrew Yang, "Wireless Lan Security And Laboratory Designs", Consortium for Computing Sciences in Colleges (CCSC), 2004, pp-44-60.

[20] Bo Yan · Guanling Chen · JieWang · Hongda Yin, "Robust Detection of Unauthorized Wireless Access Points", Springer Science + Business Media, pp-508-528, LLC 2008

[21] Jihwang Yeo, Moustafa Youssef, Ashok Agrawala, "A Framework for Wireless LAN Monitoring and Its Applications", Workshop on Wireless Security, ACM, 2004, pp-70-79.

[22] Rupinder Gill, Jason Smith and Andrew Clark, "Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks", Proceedings of the 2006 australian Workshop on Grid computing and e-Resources, Australian Computer Society, 2006, pp-221-230.

[23] Chris Wullems, Kevin Tham, Jason Smith and Mark Looi, "A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs", 3rd IEEE Wireless Telecommunication Symposium(WTS) May 2004.

[24] SeongWoo Kim and SeungWoo Seo, "Dual Authentications for Fast Handoff in IEEE 802.11 WLANs: A Reactive Approach", IEEE Wireless VITAE'09, Aalborg, Denmark, May 2009.

[25] Artur Hecker, Houda Labiod, "A new EAP based signaling protocol for IEEE 802.11Wireless LANs", IEEE Xplore, 2004.

[26] 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.

[27] Maocai Wang,Guangming Dai, Hanping Hu, Lei Pen, "Security Analysis for IEEE802.11", IEEE Xplore, 4th International Conference on Wireless Communication, Networking and Mobile Computing, Wicom 2008,.

[28] Wuzheng Tan, Maojiang Yang, Feng Ye, Wei Ren, "A Security framework for Wireless Network based on Public Key Infrastructure", 2009 ISECS International Colloquium on Computing, Communication, Control and Management, IEEE, CCCM 2009, pp – 567-570.

[29] M.S. Bargh, R.J. Hulsebosch, 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, *WMASH'04, pp-51-60*

[30] Pascal Urien, Guy Pujolle, "Security and privacy for the next wireless generation", International Journal of Network Management, Vol. 18, Issue 2, pp -129–145, 2008

[31] Stuart Shanken, David Hughes, San Diego, "Secure Wlreless Local Area Network (SWLAN)", MILCOM 2004 - Military Communications Conference. IEEE, 2004, Vol. 2, pp- 886-891.

A. 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 22 years of experience in teaching and 13 years of experience in research. He has published 49 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.

B. 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. Other areas of interest include OOAD & UML, Software quality and Testing and Computer Networks.