BUSINESS NEED FOR SECURITY

Denial of Service Attacks in Wireless Networks

By

Mallikarjun Hangargi

Graduate Student

Master of Science in Information Assurance

Northeastern University

Table of Contents

Table of Illustrations

BACKGROUND

Wireless network is a data communication network that uses radio frequency band for transmission by obviating wires for connection, transmission and reception. Wireless LAN is a computer network that connects computing nodes over the wireless medium.

A Denial of Service (DoS) attack is a type of attack that is aimed at bringing down system resources. A hacker attempts to make systems resources unavailable to legitimate users.

Physical layer is the lowest layer of OSI 7 layer network model. It deals with transmission and reception of data between devices at the bit-level.

Media Access Control (MAC) layer is the sub layer of Data Link layer, which is the second layer of OSI 7 layer network model.

An Access Point (AP) is a data communication device that connects wireless computer/devices to a wired network. AP acts as the central node for transmission and reception of signals.

An access control list (ACL) is a list of access control entries. Each in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee.

A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it

Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. It is utilized as a multiple access method in the frequency hopping.

I. Introduction

Wired networks for data communication were considered to be faster than wireless networks. However technological advancements in wireless networks have disapproved the claims made by the proponents of wired networks. Wireless data networks use radio waves for data communication between devices. By the very nature, the medium for wireless communication is intangible. Wireless networking has changed the fabric of data communication by unbinding users from the shackles of wires and chords. The promise of anytime and anywhere connectivity can only be fulfilled by wireless networks.

Wireless data networks are the need of the hour for every emerging business. It's equally essential for an established business to incorporate wireless networks in their IT infrastructure to gain a technological edge over its peers. The reason is that, wireless data networks add a great deal of mobility, flexibility and expandability in the business. Besides, there is considerable cost saving when compared to traditional wired networks. However, organizations should be well prepared to face the problems that come with wireless networks. DoS attacks are a commonplace in data networks. Guarding against DoS attacks should be a critical component of a security system in the current modern day era. Threats like virus, worm, and malware are old school when compared to Denial of Service (DoS) attacks because Denial of Service attacks in wireless data networks have a potential to undermine the advantages that come with wireless networks. It's because of the shared medium of transmission that WLANs are very much vulnerable to DoS attacks. While traditional DoS attack involve overwhelming a host with service requests, in wireless networks limited bandwidth and routing functionality associated with nodes open up new avenues for launching DoS attacks. The aftermath of DoS attacks range from crippling the network performance to completely bringing it down. So for an organization that has critical operations like point of sales, security cameras over wireless network, surveillance systems etc., any hiccups in the network can cause severe impact on their business. It only makes sense for organizations that have wireless networks deployed, that they be prepared for DoS attacks. For traditional wired networks DoS have been extensively studied but there has been a lack of research study to prevent such attacks on wireless data networks. DoS attacks are perpetrated at various levels of the network defined in the OSI seven-layer network model. This paper covers the attacks carried out at the first two layers wiz Physical layer and MAC layer - a sub layer of Data Link layer. At the physical layer, DoS attack is perpetrated by signal jamming also known as intentional interference. There is another form of unintentional interference that is induced by signals from other devices. The two main protocol

attacks that are carried out at the MAC layer are masquerading attacks and resource exhaustion attacks. This paper also discusses the solution methods available for mitigating the DoS attacks discussed here.

II. Jamming(intentional interference) and unintentional interference at the Physical layer

Wireless data communication happens over a shared medium where information is broadcasted as data frames via radio waves. Although shared medium is the biggest advantage of wireless networks, it's the same-shared medium that makes wireless networks more vulnerable to DoS attacks. WLANs use 2.4 GHz spectrum, which is free and non-regulated. These frequency bands are unlicensed and can be used by any radio devices for data communication; all of which have the same right to use a band.

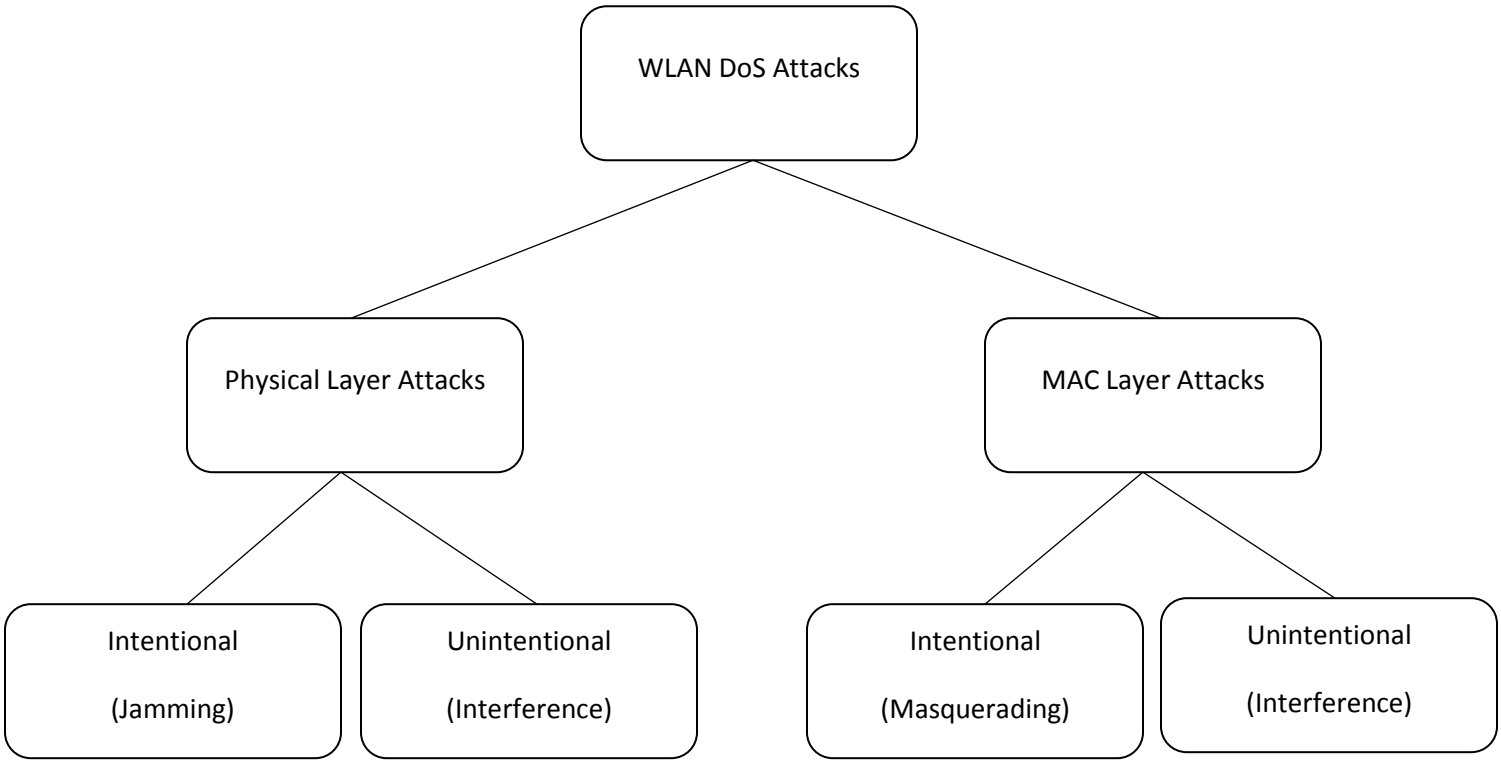

Fig.1 Tree classification of Denial of Service attacks in wireless data networks

Source: This illustration has been adopted from, "PREVENTING WIRELESS LAN DENIAL OF SERVICE ATTACKS, a guide to combating WLANs DoS vulnerabilities" – A white paper by Motorola solutions

Therefore, Denial of Service attacks at the physical layer could be unintentional like interference from other signals within the spectrum range or intentional interference like jamming by malicious nodes.

Interference is one of the prime reasons for sluggishness and instability in wireless data networks. Since radio transmission for data communications in wireless networks are broadcast type, any receiver within the range of a transmitter can listen to the transmissions. Operating several Access points (AP) closely within a single WLAN also results in interference due to the collision of signals. Likewise, when several of the clients connected to a single AP are in close proximity, interference occurs. Signal interference could arise from neighboring WLANs as well. Interference faced by a WLAN is often assumed to have been induced by a neighboring WLAN or by devices within the WLAN. However interference is also caused by non-WLAN traffic for e.g. devices like television remotes, blue-tooth devices, cell phones, microwave ovens etc. Devices such as microwave ovens simply belch out energy in the 2.4 GHz band when they are powered up. Devices such as wireless video cams also use a continuous wave modulation scheme wherein they always emit energy on a given RF channel in the 2.4 GHz band. Of late, there has been a proliferation of wireless devices like cell phones which operate in the 2.4 GHz band. If many of these devices operate in the vicinity of a WLAN, they can cause significant disturbance in the medium.

Monitoring the spectrum and accordingly adjusting the transmission power of Access Points in WLAN helps to deal with physical layer DoS attacks. Radio resource management also known as RF spectrum management tools usually addresses interference in WLAN traffic. Many vendors have started to incorporate these tools in enterprise class WLAN systems. Just like network equipment in the upper layer of network offers ways to manage the layer, these tools offer ways to manage the physical layer of wireless data networks. They offer important functions like adjustment of transmission power, automatic setting of channel assignments and re-configuration of network parameters. Network conditions change for a WLAN when it comes under interference; therefore reconfiguration of network parameters is necessary. These tools help reduce interference by simply adjusting the transmission power of APs and selecting channels to switch to, and transmit the signals. Radio frequency spectrum Management tools function with the help of a device called Spectrum analyzer, which is ubiquitous in the current day WLAN systems. The radio devices used in WLAN APs can only detect WLAN noise; they are not very effective in diagnosing interference from non-WLAN devices. That is why, even though these tools are useful, there is a need for more sophisticated implementation. Thanks to the

progress in the field of VLSI, to the progress in spectrum analyzer architecture and associated software, more evolved tools for WLAN security have emerged. These tools are known as Spectral Assurance tools and are particularly designed for WLAN Applications. A countermeasure for interference arising from other than nearby WLAN is to use 5 GHz band. Devices like microwave ovens, Bluetooth, cordless phones, radio equipment operate in 2.4 GHz bands. Operating WLAN in 5 GHz band segregates it from the devices operating in 2.4 GHz band; therefore devices in the 5 GHz WLAN will not hear signals from non-WLAN devices. Devices designed as per wireless technology standard IEEE 802.11b and 802.11g still operate in the unprotected 2.4 GHz frequency band. The IEEE 802.11a technology standard devices operate in the 5GHz frequency band. This band is slightly bigger and less vulnerable to interference. Reports suggest that 5 GHz band has so far been underutilized because of the apprehensions that the operating range is less when compared to 2.4 GHz band. Studies have proved that the range of these two bands is more or less the same when operated at maximum throughput. The IEEE 802.11a standard, an amendment of the original standard IEEE 802.11 was ratified in the year 1990. Since then, this new standard has been widely implemented across the world, particularly in corporate IT infrastructure. Another wireless transmission standard, IEEE 802.11ac was ratified in January 2014. This standard supports operation of wireless devices over 5 GHz band with lesser interference from other wireless devices. Beam forming is an amazing characteristic of this new generation wireless standard. A wireless node instead of radiating omnidirectional signal can concentrate the transmission such that most of the signals sent out reach the targeted devices. Sometimes organizations deploy several APs within a small area to provide connectivity to the users in a dense working environment. This results in interference due to collision of signals from different APs as they are closely deployed. This problem has been addressed in the IEEE 802.11ac wireless standard. This standard supports an increased number of clients per AP. More number of clients can be served with relatively fewer APs deployed, hence with reduced interference. There are additional advantages of migrating over to this wireless standard. It offers over 12 non-overlapping channels to accommodate a large number of users and a very high throughput. It has also incorporated co-existence mechanism for IEEE 802.11a and IEEE 802.11n devices.

The second form of physical layer DoS attack in wireless data networks discussed in this paper is the case of jamming. Jamming falls under the category of intentional interference. The attack is perpetrated using a broadband jammer device that essentially consumes the supposed bandwidth with Gaussian white noise or similar signals having relatively high amplitude. Such

devices come as cheap off-the-shelf equipment and are otherwise very easy to build. A jamming device or a compromised node relentlessly transmits radio signals with the intention of blocking legitimate access to the medium and/or to interfere with reception at receiving nodes. This is called jamming and the malicious nodes/devices are called jammers. The intention of the attacker is to cause disruption in the data communion resulting in excessive power consumption and long waiting times. Jamming techniques vary from simple ones like continuously transmitting interference signals, to more sophisticated attacks that are aimed at exploiting vulnerabilities in the underlying protocols.

There are several jamming techniques employed by jammers. The first one is constant jamming wherein radio signals are emitted continuously with intervals. This type of jamming causes two things: (a) The signals from the jammers keep the medium busy and therefore transmissions are deferred at the transmitting node, and/or (b) At the receiving node reception is interfered with due to the signals transmitted by the jammers. The other method is deceptive jamming wherein the radio signals are continuously transmitted with regular intervals. This is relatively tougher to detect because it deceives a sender node by giving an impression of a legitimate traffic over the channel. As a result a sender node that wants to transmit data remains in the listening mode after sensing the channel as busy.

Counter jamming measures have to be employed not only to ensure smooth operation of WLANs but also for optimal performance. There are three approaches of counter-jamming in wireless networks: avoidance, detection and mitigation. The most effective way of dealing with jamming is to avoid it completely by switching over to a wired medium or moving the AP and/or devices away from the range of jamming devices. However, practically it's not possible to completely avoid jamming because replacing a wireless network with a wired medium on the onset of a DoS attack is not a feasible option. Also moving APs away from the reach of jamming devices is not possible by any means. Besides the operational infeasibility, switching to wired networks essentially means not using a wireless network at all and doing so defeats the very purpose of deploying wireless networks which is mobility.

The first line of defense against jamming should be to have a mechanism to identify its presence so that the impact of disruption is minimized. This could be achieved through a continuous monitoring mechanism to detect any potential malicious activity by a jammer. The mechanism consists of a subset of nodes within a WLAN, which acts as network monitors and a detection algorithm at each monitoring node. A quantity is observed at each monitoring node

to detect the presence of jamming. Probability of collision is one such metric that could be used. It is the percentage of erroneous packets received at a node. A period of normal network functioning under the absence of jammer is considered for training. During this training period, the probability of collision is carefully studied as a long-term average of the ratio of number of slots in which there was collision over the total number of slots in training period. During the real-time operation of WLAN, the probability of collision observed is compared with the learned long-term average from the training period. When a wireless data network is under attack, changes will occur in the signal behavior. Any increase in the probability of collision when compared to the learned average or any temporary increase in the probability of collision compared to the average during normal network operation may be the result of an ongoing attack. Detection algorithm takes sample values from the monitoring nodes to decide whether it is an attack or not. Once detected, measures can be taken to shun the attack. Therefore early detection using such mechanisms is crucial in a way to prevent it and reduce the implications of an attack.

The techniques for mitigating jamming are employed at the signal level. Spread spectrum signal transmission is often used to minimize jamming in wireless networks. Out of the two modulation techniques of spread spectrum signal transmission, frequency hopping has been studied rigorously to prevent jamming. Frequency hopping refers to the changing of frequencies during a radio transmission. This is also known as Frequency-Hopping Code Division Multiple Access (FHCDMA). This enables radio signal to be transmitted over a wider band. This band is wider than the minimum bandwidth required for information signal. Instead of concentrating the transmission energy in the narrowband, it is spread across a number of frequency band channels. A transmitter switches between available frequencies based on random or preplanned decisions. For this, it is necessary that the transmitter and receiver operate in sync with each other. This essentially means that a receiver remains tuned to the same center frequency as the transmitter. To start with, a quick burst of data is transmitted on a narrow band. Then, the transmitter switches to another frequency and transmits again on that new frequency. The receiver is capable of switching its frequency over a given bandwidth several times in accordance to transmitter because as they are synchronized with each other. However, this switching technique requires a much wider bandwidth than what is needed to transmit the same information when using a single carrier frequency.

III. INTENTIONAL DOS AT THE MEDIA ACCESS CONTROL(MAC) LAYER LIKE MASQUERADING ATTACKS and RESOURCE EXHAUSTION ATTACK

WLAN also comes under Denial of Service (DoS) attacks at Media Access Control (MAC) layer, which is one of the two sub layers of the Data Link layer of the OSI seven-layered network model. Just like in the physical layer, at the MAC layer also, wireless networks are susceptible to unintentional-interference. When two or more co-located WLANs operate on the same channel, there is interference that results in loss of frames. This usually leads to increase in the transmission latency and decrease in the network throughput. This paper primarily focuses on masquerading attack and resource exhaustion attack, which are intentional interference attacks. In the section it was mentioned that a shared medium is the reason why wireless networks are more prone to DoS attacks. To add to this, the open medium of wireless networks makes the task easy for an attacker to sniff traffic to find devices on the network. The identities of the devices after they are known are spoofed to carry out masquerading attacks; de-authentication flooding, de-association flooding and resource exhaustion attacks; probe-request flooding, authentication-request flooding, association-request flooding.

A. Lack of management and control frame protection

Data at the MAC layer is transmitted in the form of frames. Frames at the MAC Layer are of three major types. They are: data frames, control frames and management frames. Data frames carry data from the higher-level protocol in their frame body. Control frames do not carry any higher protocol data but they assist in delivery of data frames. They address channel acquisition, carrier sensing and other MAC layer reliability functions. Management frames are used to perform overseeing functions. These frames assist in joining, leaving a network and associating a client with an AP, moving from network of one AP to another etc. MAC layer DoS attacks are perpetrated by spoofing messages exchanged between a client and Access Point. There are vulnerabilities in the protocols at the MAC layer. Although protection for data frames is addressed through encryption, there is lack of protection methodologies implemented for control and management frames. There is no cryptographic mechanism to determine if a frame is sent by a genuine client or AP. Therefore, various Control frames and Management frames are subject to manipulation by an intruder making it feasible for him to carry out DoS attacks.

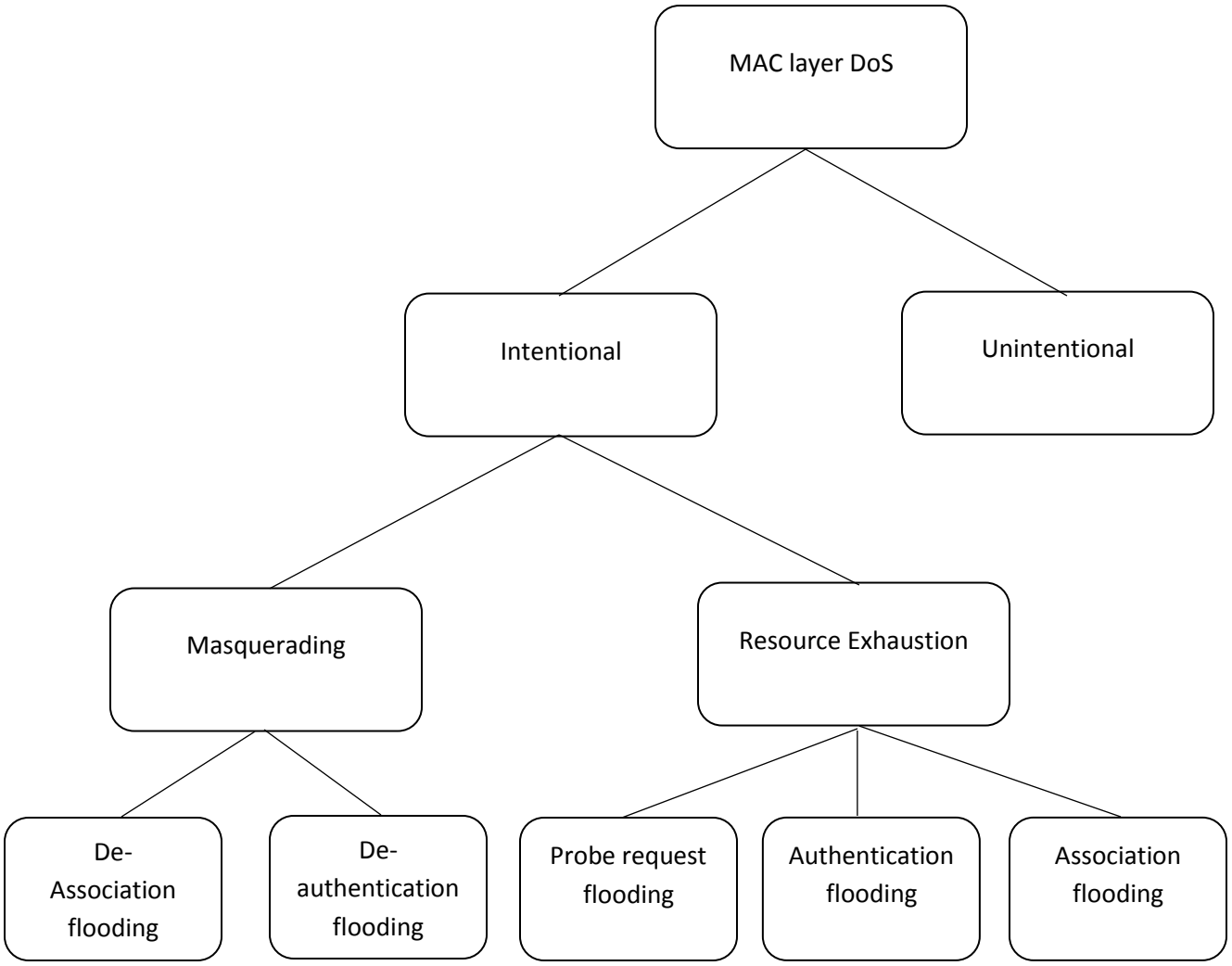

Fig 2: Tree classification of MAC layer DoS attacks discussed in this paper

Source: This illustration has been adopted from, “PREVENTING WIRELESS LAN DENIAL OF SERVICE ATTACKS, a guide to combating WLANs DoS vulnerabilities”- from - A white paper by Motorola

i. Resource Exhaustion attack

Resource Exhaustion attack is aimed at consuming system resources, memory and processor. When resource exhaustion attacks are launched they result in legitimate clients being denied of the services originally intended for them. MAC layer DoS attacks

perpetrated with the intention of resource exhaustion are Probe request flood, authentication request flood and association request flood. A wireless client regularly scans the wireless environment around to find out the presence of APs in the vicinity by broadcasting probe requests. On receiving a probe request from a client, APs respond to probe requests by sending out information about their wireless network to facilitate the client to authenticate and then associate with them. An attacker targets APs by sending out large volumes of probe requests by faking MAC address in each request. This is called probe-request flooding. This tricks APs to believe that they have been receiving probe requests from several wireless clients. APs are therefore, forced to respond to these requests which in turn increases processor and memory utilization. During the course when legitimate clients send probe requests, response to such request is delayed. Eventually when all the memory and processing resources are consumed, requests from legitimate clients are no longer served.

Likewise an attacker can inundate APs with authentication requests by sending bursts of request frames, each holding a spoofed MAC address. Each such frame tries to authenticate a client to an AP. When encountered with torrential authentication requests, AP commits its processor to serve the requests, allocates memory to maintain state table. State tables contain information about clients, which have been authenticated. So when under authentication flooding attack, APs fail to respond to authentication requests coming from legitimate clients. APs also maintain an association table. It contains an entry for each client that has associated with it. If an attacker has cracked the network password and/or SSID, several of non–existent clients can be associated with an AP by spoofing authentication request followed by an association request. This results in over flooding of association table because there is a limit on the count of client associations an AP can have. This is relatively tougher to carry out for an attacker because, as said earlier the password and/or SSID of the network must be cracked first. Even without the knowledge of network password, authentication flooding can be carried out but APs more or less remain unperturbed. A failed authentication request will not result in overflowing of Association table or State table; it only takes up the processor speed for pre – processing of requests.

Carrying out authentication and association flooding attacks can be made difficult for an attacker by having an Access Control List (ACL) in place. Every AP should be updated with ACL to filter MAC addresses, only those clients registered with the WLAN administrator and/or those previously associated with the AP should be allowed to authenticate itself to the APs. This however brings in a little administrative overhead. Network administrators should maintain a database holding clients' MAC addresses; perhaps an out of band client registration with the network administrator is required, for e.g. client first shares it's MAC address with the administrator via email. Network Administrator should then periodically update the ACL on the APs to add newly registered clients' MAC and to purge out MAC address of clients, which should no longer be authenticated. This method should work well enough for an enterprise level WLAN system. Most of the corporate IT infrastructure setups across the globe have MAC binding implemented for the wired LAN, therefore ACL based MAC filtering shouldn't be difficult to incorporate. However this is not feasible for a public WLAN. It is difficult to maintain a list of clients and update the ACL on APs because the list of clients keeps changing every day, perhaps every hour. Strong authentication methods also go a long way in preventing authentication and association flood attacks. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi-Protected Access 2 (WPA2) are standards used to authenticate users so that only authorized clients can access the network. WEP is the initial standard rolled out for wireless network security to provide similar protection to that provided by physical security measures in wired networks. WEP is now considered to be a weak authentication method- this was proved by a research group from University of Berkeley, California. With current day systems' computation power and widely available software tools, password used in WEP standard can be easily cracked. Surprisingly older wireless network devices still continue to use WEP standard, which was superseded long back by WPA in 2004. The latest standard is WPA2 that uses a 256-bit key for encryption, therefore it is highly recommended to use WPA or WPA2.

ii. De-authentication Flooding attack

Even before communication between a client and an AP starts, the client has to authenticate itself with the AP. De-authentication message is part of the whole authentication process through which client and APs can request to de-authenticate from each other. There is no secure authentication method employed for this. Therefore an attacker can easily spoof a de-authentication message. An attacker sends a spoofed de-authenticate messages to an AP with the MAC address of its clients. On

receiving this message an AP de-authenticates and then de-associates the client whose MAC address is specified in the de-authentication message. The above scenario is a typical example of how a de-authentication message is spoofed when identity of clients is known through sniffing. Similarly, de-authentication message from AP to client(s), which essentially means that AP is terminating the connection, is also spoofed. In order to carry this out, an attacker must first spoof the MAC address or the BSSID of the AP. The former is used to target a particular client while the latter is used to target multiple clients. A sustained attack can prevents client(s) from connecting to an AP, which can result in loss of productivity from employees and sometimes there is even a potential for loss of revenue, business. Even worse, de-authentication flooding attack is used as the first stage of a multi-level attack.

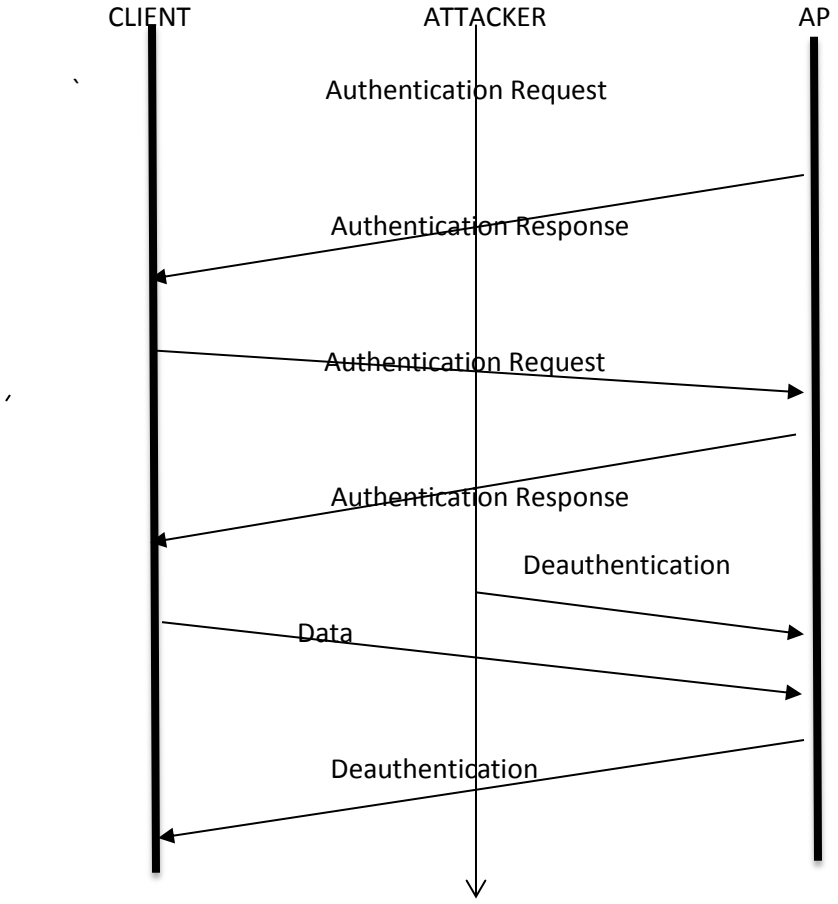

Fig 3. A graphical depiction of de-authentication attack

Source : This illustration has been adopted from "De-authentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks" - International Journal of Computer Applications, June 2011 Edition

This attack is carried out for many reasons.

1) To capture hidden SSID because sometimes SSID are cloaked and not broadcasted.
2) To capture authentication handshaking between client(s) and AP.
3) To generate ARP frames for carrying out WEP replay attack.
4) To trick clients into connecting to a rogue AP or honey point AP.

These attacks are carried out at the higher layers of network protocol. These attacks are beyond the scope of this paper therefore they have not been discussed in details.

iii. Dis-association Flooding attack

There exists vulnerability in the association protocol just like in authentication. Soon after authentication, an association message is exchanged between a client and AP to associate client to AP. A dis-association message when sent or exchanged dis-associates a client from AP. There is no authentication in place for exchanging these messages. This vulnerability is exploited in a similar fashion to that in the authentication protocol. An attacker sends a spoofed message to an AP, on receiving the message; AP dis-associates the client whose MAC address is mentioned in the message. Although dis-association attack works similar to de-authentication attack, the latter is more severe. De-authentication attack forces a victim client to do more work than dis-association attack. When a client is de-authenticated it takes more time to get connected back to AP because it first has to authenticate and then associate with the AP.

The DoS attacks at the MAC layer discussed above are very much prevalent in the IEEE 802.11 standard networks. As mentioned earlier there is no authentication method whatsoever for management and control frames. On encountering a management and control frame, APs cannot determine whether a genuine client has sent a frame. Cryptographically protecting management and control frames to bridge the vulnerability is a possible solution to mitigate these attacks. IEEE ratified an amendment to the original standard IEEE 802.11 and came up with a new standard 802.11w. IEEE 802.11w extended security to manage frames by including security mechanism to provide data confidentiality, integrity and data origin authenticity of management frames. This standard could provide protection against some of the MAC layer DoS attacks but was not a solution for all DoS attacks. None of the current standards address cryptographic protection schemes for control frames at the MAC layer. Therefore 802.11w WLAN are still vulnerable to DoS attacks like resource exhaustion attacks that are perpetrated

by spoofing control frames. The de-authentication vulnerability in particular can be fixed by authenticating control frames explicitly. It also requires dropping invalid authentication/de-authentication requests.

MAC layer DoS attacks, de-authentication flooding in particular can be mitigated by delaying the effect of requests. Request delay method has been studied to be an effective approach. The effects of a de-authentication and disassociation request should be delayed by queuing the request for a few seconds. This gives an AP ample time to study the subsequent requests coming from a client. In the next few seconds, if a data packet is received from a client, de-authentication request previously queued should be dropped. The decision to drop de-authentication requests should be taken on the condition that there is a de-authentication request in the queue. A legitimate user would never send data packets after it has requested to de-authenticate from the APs. Similarly if multiple de-authentication requests are received from a client when already a request is in the queue, the freshly received requests from client must be dropped. A legitimate client would never send bursts of de-authentication requests; it would do so only once. The same method can be employed in reverse order to reduce spoofed de-authentication messages sent to client(s) on behalf of an AP. There is an added advantage in this approach; it can be implemented with only a simple firmware changes to existing Network Interface Cards and APs, without requiring a completely new management structure. However, the standardization of such capabilities is still some ways off and legacy MAC implementations do not have sufficient processing capacity to implement this functionality in the form of a software upgrade. Therefore, system level defenses like MAC address spoof detection offers significant value in dealing with DoS attacks at MAC layer.

MAC address spoofing is based on sequence number field. A sequence number field should be included in frames and the value should be incremented by one for each non-fragmented frame. An attacker cannot change firmware functionality of wireless cards; hence an attacker wouldn't be able to alter the value in the sequence number field. Detection systems should be used to analyze the sequence number in the frames sent by clients, maintaining a state of sequence number from clients. Any random or out of sequence number in the filed should trigger the alarm of spoofed messages. Studies have showed that this is a false proof mechanism for to detect MAC address spoofing as long as an attacker doesn't attempt with reverse-engineered attack cards.

IV. CONCLUSION

In this paper we have discussed Denial of Service (DoS) attacks in wireless networks launched at the Physical Layer and Media Access Control (MAC) layer – sub layer of Data Link Layer. Open and shared medium of wireless network makes it all the more vulnerable to DoS attacks. At the first layer wiz physical layer WLANs face jamming and unintentional interference whereas at the MAC layer, DoS attacks are perpetrated by spoofing management, control frames. The attacks are Resource Exhaustion attacks and Masquerading attacks. We also discussed that the IEEE 802.11 is extremely vulnerable to DoS attacks. Ratification of 802.11w has helped to some extent by protecting management frames at MAC layer. However they are still vulnerable to attacks launched by spoofing control frames. DoS attacks can be very detrimental. A sustained attacker can completely bring down a network. Such an incident would be the most undesirable one for an organization that has critical operations dependent on the WLAN deployed. Therefore organization needs to secure its WLAN to ensure smooth business operations and to avoid any downtime occurring from DoS attacks.

According to recent studies, there is an increase in the number, size and complexity of Denial of Service (DoS) attacks. Besides, the attack vectors have also been emerging. An organization without protection against DoS attacks is deemed as a soft target for attackers. It is necessary for an organization to take proactive measures against DoS attacks. The organizations with technical controls in place for DoS prevention, in addition to mitigation as part of incident response plan will fare much better in the event of DoS attacks. The impact of DoS attacks is not limited only to IT. DoS attacks can lead to disruption and delay in normal operations of an organization. This impacts customer satisfaction, customer services, employee productivity, stock prices, investor confidence, sales revenue and profitability, ranks and reputations. There is an immediate need for new standards that address the protection of control frames at MAC layer through cryptographic protection schemes. There is also a pressing need to evolve the technology for detection and prevention of jamming.

V. REFERENCE

A. Stuart Compton : GAWN Gold Certification Author, stuartcompton@hotmail.com, “802.11 Denial of Service Attacks and Mitigation” - Sans Institute Reading , May 2007

B. Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, University of California, Riverside, “Denial of Service Attacks in Wireless Networks: The case of Jammers” - IEEE March, 2011

C. Taimur Farooq, David Llewellyn-Jones, Madjid Merabti, School of Computing and Mathematical Sciences, Liverpool John Moores University, UK, “MAC Layer DoS Attacks in IEEE 802.11 Networks” – IEEE, Oct 2002

D. Vikram Gupta, Srikanth Krishnamurthy and Michalis Faloutsos, “Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks” – IEEE, Oct 2002

E. Nisha Sharma, Paras Nath Barwal, “Study of DoS Attacks on IEEE 802.11 WLAN and its Prevention/Detection Techniques” - International Journal of Engineering Science and Innovative Technology (IJESIT) , May 2014

F. Taimur Farooq, David Llewellyn-Jones, Madjid Merabti , “MAC Layer DoS Attacks in IEEE 802.11 Networks” - 2007

G. Dazhi Chen, Jing Deng, and Pramod K. Varshney, EECS Dept., Syracuse University, Syracuse, “Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming” - 2003

H. Deepthi N. Ratnayake, Hassan B. Kazemian, Syed A. Yusuf, Azween B. Abdullah, “An Intelligent Approach to Detect Probe Request Attacks in IEEE 802.11 Networks” - 12th INNS EANN-SIG International Conference, Sep 2011

I. Rupinder Cheema, Divya Bansal, Sanjeev Sofat, “Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks” - International Journal of Computer Applications, June 2011

J. Yihong Zhou, Dept. of Electrical and Computer Engineering, The University of Texas at Austin, “Analyzing and Preventing MAC-Layer Denial of Service Attacks for Stock 802.11 Systems”

K. A white paper by Motorola Solutions, “Can Wireless LAN Denial of Service Attacks Be Prevented? Understanding WLAN DoS Vulnerabilities and Practical Countermeasures” – http://www.motorolasolutions.com –(accessed November 15, 2014)

L. A white paper by Motorola, “PREVENTING WIRELESS LAN DENIAL OF SERVICE ATTACKS, a guide to combating WLANs DoS vulnerabilities”, Published May 2010 - http://www.motorolasolutions.com - (accessed November 15, 2014)
M. Far Point group Technical Note – “Evaluating Interference in Wireless LANs : Recommended Practice”, Published April 2010 , http://www.cisco.com - (accessed November 15, 2014)
N. Far Point Group White Paper – “The Invisible Threat: Interference and Wireless LANs”, Published May 2010, http://www.cisco.com – (accessed November 15, 2014)
O. Chibiao Liu, and James Yu, Member, IEEE, “A Solution to WLAN Authentication and Association DoS Attacks”- International Journal of Computer Science , Aug 2007
P. Arockiam. L, Vani. B, “A Survey of Denial of Service Attacks and it’s Countermeasures on Wireless Network” - International Journal on Computer Science and Engineering, May 2010
Q. Fluke Networks Solutions , “WLAN ANALYSIS” , http://www.flukenetworks.com - (accessed November 15, 2014)
R. Frequency-hopping spread spectrum , http://www.princeton.edu/ - (accessed November 15, 2014)
S. http://www.academia.edu/3292210/Wireless_DoS_Attacks_Deauthentication-Disassociation_Flood_Attack – (accessed November 15, 2014)