Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.9, No.5, 2018

A Survey of Different Dos Attacks on Wireless Network

Manish Tyagi*
PG Scholar, CSE Dept., RITS, Bhopal, INDIA

Seema Narvare
Asst. Prof., CSE Dept., RITS, Bhopal, INDIA

Chetan Agrawal
Asst. Prof., CSE Dept., RITS, Bhopal, INDIA

Abstract
Wireless technologies like Wireless LAN (WLAN) 802.11 picking up ubiquity in all associations, undertakings and colleges because of its profitability, cost sparing when contrasted with wired system and usability by enabling the system clients to move physically while keeping up an association with the wireless system. Wireless systems are main stream among the Laptop client group today in light of the portability and usability. Individuals working through remote association must know about the surroundings because of the different sorts of assaults made by the interlopers. Remote systems are extremely defenseless against (Denial of Service) DoS attacks. DoS attacks are an endeavor to make a machine or system asset inaccessible to its clients. It can happen in numerous layers of OSI demonstrate and can happen in different frame Network clients can ensure their frameworks with Wi-Fi Protected Access (WPA) security conventions and Wired Equivalent Privacy (WEP), however DoS attack still can't be averted utilizing these conventions. These attacks bring about debasement of the system quality or finish loss of accessibility of the system inside the association. This survey paper makes a review on various kinds of DoS attacks and their countermeasures on the framework systems which depend on the Access Points (AP). The fundamental assaults called Deauthentication and Disassociation Flooding. DoS assaults are considered there avoidance/discovery arrangements.
Keywords- Access Points, DoS, Wireless Security, 802.11, Disassociation, Deauthentication, Flooding attacks

1. 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.

Denial of service is an attack which denies authorized user access to the service provider. The recent report shows that the most expensive computer crime over the past year was due to denial of service.

DoS attack target different layers of OSI model [2]:

- Physical layer: by accidentally cutting a communication cable to take down network services.
- Data link layer: to disable the ability of hosts to access the local network.
- Network layer: by sending a large amount of IP data to a network.
- Transport layer: by sending many TCP connection requests to a host
- Application layer: by sending large amount of legitimate requests to an application.

The various kind of Dos attacks are[3] ARP Poisoning, MAC Spoofing, Web Spoofing, ICMP Flooding, CPU and Memory attacks, Window Multiplication, Airwaves Jamming, Disassociation attack, Distributed Denial of Service (DDoS) attack, De-authentication message attack etc. WLAN used Wired Equivalent Privacy (WEP) security protocol [1] to achieve Authentication Integrity and Confidentiality services. Since WEP did not provide the required level of security, IEEE proposed two another security protocols as Wi-Fi Protected Access (WPA) and 802.11i as the security standards for WLANs. WPA was an intermediate security protocol to improve the level of security offered by WEP, until the final security protocol in shape of 802.11i. The management and control frames of 802.11 based WLANs are still unprotected. Consequently, WLANs, even with the deployment of 802.11i, are susceptible to Denial of Service (DoS) attacks.

Rest of the paper is organized as following: in section 2 we describe literature survey of work previously did in the domain of DoS attacks on WLAN, in section 3 we explained briefly the DoS attacks and its types, in section 4 detection and prevention of Dos Attacks are explained, in section 5 we conclude our paper with future research directions.

2. Related Work

Wireless DoS can be performed at physical as well as MAC layer. At the physical layer jammers are utilized to disrupt or prevent communication between stations. At the MAC layer media access vulnerabilities and the openness of the management and control frames are exploited to launch DoS attacks. Some of the solutions proposed in the literature to tackle the de-authentication DoS attack are listed below.

"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.

Bellardo et.al. [26] suggests modifying the authentication framework and authenticating all management frames. This approach can help prevent the de-authentication DoS attack but requires firmware upgrades on both the client and the AP. Adding authentication to each management frame would incur additional cost on both client as well as AP. Since authentication is an expensive process, authenticating every management message would in-turn quickly drain the batteries of handheld devices like smart-phones, PDAs etc. Bellardo also suggests another approach in which he proposes delaying the effect of management frames. If a de-authentication frame is received from a victim STA and subsequently a data frame is received from the same victim STA the previous de-authentication frame(s) is not honored. However delaying the effect of all management frames may create association troubles for roaming clients and may reason handoff issues.

Edgar Cardenas et. al. [27] proposes the utilization of Reverse Address Resolution Protocol (RARP) to detect spoofed frames. However an intelligent assaulter can manipulate the IP address of the client to circumvent the RARP technique. Also in the case when multiple IP address are assigned to same NIC the solution fails.

Upgrading to 802.11w standard - This standard [28] authenticates the de-authentication and dis-association frames. The authentication prevents spoofing and hence can prevent the de-authentication DoS attack. However 802.11w is a very recent standard released in 2009. Upgrading all millions of Wi-Fi devices to support the

802.11w is a difficult task.

Nguyen et al. [29] have proposed a Letter-envelop protocol to prevent the de-authentication DoS attack. In their approach the client and AP share a secret key which is used for authenticating the de-authentication frame and Disassociation frames. This helps in alleviating the assault and does not incur too much load on either the client or the AP. However this method also engages firmware upgrades on both client and AP and hence proves to be costly.

A centralized framework like 802.1x can help prevent a variety of assaults including de-authentication DoS attack, however such centralized solutions suffer from single point of failure [14]. If the authentication server is compromised all the clients belonging to the network can be compromised.

To summarize the drawbacks of the current approaches to detect or prevent the de-authentication DoS attack are listed as follows:

- Expensive Deployment.
- Requires modification in 802.11 protocols to support Authentication and Encryption of frames which are currently non-authenticated.
- Patching client software.
- Requires proprietary hardware.
- Up gradation to newer standards.

From the above summary it is clear that a scheme to detect the de-authentication DoS attack is required having the following features.

- No modification of 802.11 protocols.
- Easy deployment to legacy as well as new networks
- Hardware costs should not be exorbitant.
- Should not require patching of underlying operating system or installation of new software.
- Should be able to recover victim STA from the assault swiftly.

3. DoS ATTACKS

DOS attack occurs when any of system resource is not available to network users. A DOS attack floods the remote system with so much traffic that it cannot handle normal, valid requests made from others network systems[2].DOS attacks are not easily detectable, as the remote computer cannot easily distinguish requests and traffic sent from the DOS-attacking machines and that sent by valid means. DOS can also occur because of high legitimate demand. DoS attacks can be roughly classified according to the OSI model [4, 5]:

- Application layer DoS attacks.
- Inter-Network and transport layer attacks.
- Media access layer DoS.
- Physical layer DoS.

Application layer attacks: Here the attacker attempts to exploit a weakness of an application protocol like DNS (cache poisoning), HTTP (stack and buffer overflow) [5]. It is achieved by sending large amounts of legitimate requests to an application. For example, [4] an HTTP flood attack can make hundreds of thousands of page requests to a web server which can exhaust all of the server‘s processing capability.

Inter-Network and transport layer attacks: A transport layer DoS attack involves sending many connection requests to a host. It is very effective and extremely difficult to trace back to the attacker because of IP spoofing techniques used. A network layer DoS attack [4] is achieved by sending a large amount of data to a wireless network.

Media access layer attacks: Protocol layer attacks take place on media access layer. Wireless networks are particularly vulnerable to MAC level attacks due to the use a shared medium. [4] An attacker can transmit packets using a spoofed source MAC address of an access point. The recipient of these spoofed frames has no way of telling if they are legitimate or illegitimate requests and will process them. Two main MAC layer are follow:

- Authentication/Association flood attack.
- Deauthentication/Disassociation flood attacks.

Physical layer attacks: Main two attacks are jamming and interference. Jamming a wireless network with noise signals may reduce the throughput of the network. Interference with other radio transmitters is another possibility to thrash the performance of a wireless network. Fig 2.

3.1. Types of DoS attacks

The various DoS attacks are explained as follow:

WLAN management frame attacks: 802.11 devices use management frames for the discovery, authentication and association of WLAN clients to an access point .Many of these management frame types are not authenticated

and thus vulnerable to DoS attacks [5]. For example an attacker could send Deauthentication frames with forged source MAC addresses to the access point thus rendering the client device inaccessible.

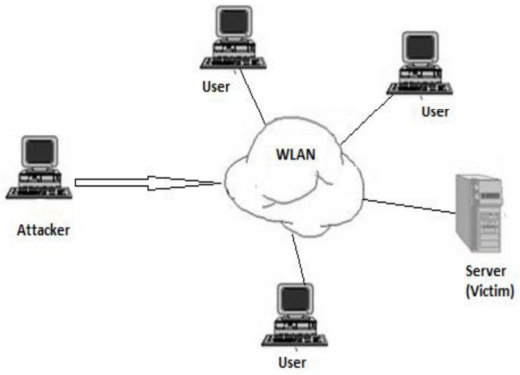

Fig 1: DoS Attack

Teardrop Attack: Teardrop attack [14] exploits the network by sending IP fragment packets that are difficult to reassemble. A fragment packet first identifies an offset that can be used to assemble the entire packet so that the receiving system can reassemble them. In this attack, the attacker's IP puts an offset value in the subsequent fragments that confuses the receiving system thus making the system unable to handle that situation in turn leading to system crash.

Distributed Flooding DoS: This kind of attack is launched by first compromising large number of innocent nodes in the wireless network termed as Zombies [7], which are programmed by highly skilled programmer. These zombies send data to selected attack targets such that the aggregate traffic congests the network. In most of the cases, the DDoS is impossible to prevent.

Power save Exploits: At client‘s sleep state, WLAN is disabled to conserve battery life; the traffic destined for the client is subsequently discarded. An attacker can send a spoofed power save poll message, while the client is still sleeping, causing the AP to transmit and discard any buffered traffic [8]. Also buffered frames at the AP are advertised in a Traffic Indication Map (TIM). An attacker can spoof a TIM to show the client that there is no buffered traffic, causing the client to go back to the sleep state and resulting in the frames for the client eventually getting dropped.

WPA 802.1i attack: WPA and 802.11i which are aimed at securing a WLAN network may be used to launch an attack [5]. As a protection measure if a WLAN AP or station receives more than 1 message with an invalid MIC checksum the session is to be shut down for 1 minute and then a new session key has to be generated, this behavior can be misused to launch a DoS attack virtually disabling the wireless service by repeatedly sending messages with forged MIC checksums.

Authentication/Association flood attack: During the authentication/association flood attack, an attacker uses spoofed source MAC addresses that attempt to authenticate and associate to a target access point. The attacker repeatedly makes authentication/association requests, eventually exhausting the memory and processing capacity of the access point leaving clients with little or no connection to the wireless network.

Deauthentication/Disassociation flood attacks: these are also known as Identity Vulnerabilities [16]. During Deauthentication Client first authenticate itself to AP as shown in figure 2, one part of the authentication framework is a message that allows clients and access points to explicitly request Deauthentication from one another. This message is not encrypted. So the attacker can easily spoof this message, either pretending to be the access point or the client. Disassociation frames are used when client have multiple access point. 802.11 Since a client can be authenticated from multiple access points to 802.11 provides a association message to allow the client and access point to agree which access point shall have responsibility for forwarding packets on the client‘s behalf. Like Deauthentication deassociation frames can be sending by the attacker similarly described above in figure.3 [16].

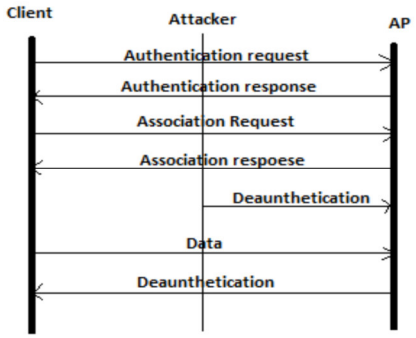

Fig.2: Deauthentication Client authentication to AP

3.2 Deauthentication Attack:

The connection between the Mesh clients and Mesh APs has been be established by the exchange of various frames as shown in Fig 3. The communication between the mesh client and the mesh AP has been established after probing the available wireless APs. After that the exchange of the series of management frames like authentication and association request frame takes place [2] . Then the mesh AP responds by sending authentication response and association response via the authentication server (Radius server) [17].

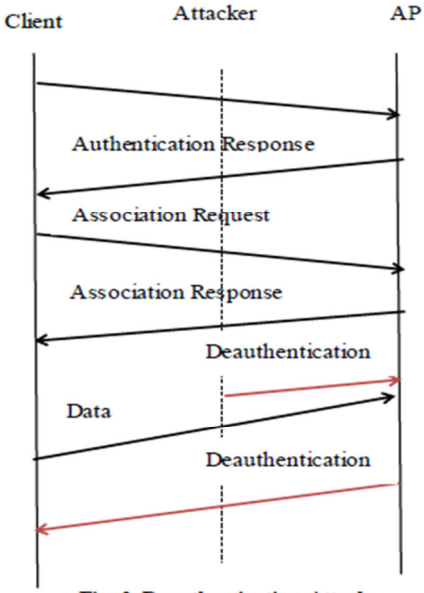

Fig. 3 Deauthentication Attack

As these frames are unprotected and sent in clear. So these frames have been spoofed by the attacker [4]. The attacker then sends Deauthentication requests with the client's address set as the source. Then the mesh AP responds by sending the Deauthentication response to the client. Thus the communication between the client and the AP has been halted [13]. As Deauthentication requests are notifications, so cannot be ignored and the AP responds instantly to these requests [2]. The attacker can periodically scan all the channels and send these spoofed messages to valid clients thus terminating their connection [19].

3.3 Disassociation Attack:

A client can be authenticated to more than one Mesh APs, but has been associated to only one AP at once [6]. Fig 4 shows the frames exchanged between the client and the AP for the launch of the disassociation attack. The client sends association request to the selected AP and this communication too may be spoofed by the attacker. Then the client sends disassociation request to the AP with source address set to client's address, as these too are notifications and cannot be ignored. So the Mesh AP instantly responds by sending the disassociation response frame Thus halting the communication between the Mesh AP and the client, but the client has been still authenticated to the previously associated network. The client may reassociate after the attack by sending solely the reassociation request. As reconnection requires less time in this case, so this attack is less severe than the Deauthentication attack [2].

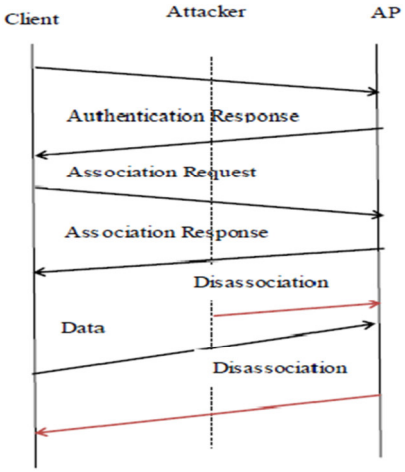

Fig. 4 Disassociation Attack

Authorization flooding on backbone devices: a Probe request frames is used by IEEE 802.11 to discover a wireless network [6], if a wireless network exist then the AP respond with Probe response frame. The clients select that AP which provides the strongest signal. The attacker can spoof a flood of probe request frames presenting a lot of nodes searching for wireless network; can overload the AP or wireless mesh router. If the load exceeds the threshold value will cause the AP or wireless mesh router to stop responding and may create service unavailability.

Web Spoofing: In Web spoofing, the attacker convinces the victim that he is visiting a legitimate web site, when the web pages are created by the attacker to steal information such as passwords and credit card numbers [3]. The attacker can achieve this by compromising the intranet server of any company and redirecting some links to his web server.

MAC Spoofing: The attacker would change the manufacturer-assigned MAC address of a wireless adapter to the MAC address he wants to spoof. An attacker can learn the MAC address of the valid user by capturing wireless packets. On successful MAC spoofing the IP address assigned to the attacker‘s computer will be identical to the IP address of the victim computer, whose MAC address was being spoofed [3]. In order to access the wireless network, the attacker had to perform DoS attack to disconnect the target computer from its wireless connection.

ICMP Flooding: It is used to report the delivery of Internet Protocol (IP) echo packets, troubleshooting purposes to show when a particular end station is not responding, when an IP network is not reachable, when a node is overloaded or when an error occurs in the IP header information etc. Typical DoS attack using ICMP is known as ICMP flooding [3]. It involves flooding the buffer of the target computer with unwanted ICMP packets and finally lack of response or system failure. Other DoS attacks are Rogue and selfish backbone devices, ARP Poisoning, Something-of-death attack, Node deprivation attack etc.

The SYN Flooding Attack: One of the most common DoS attacks is the SYN Flooding Attack [17]. TCP implementations are designed with a small limit on the maximum number of half-open connections per port that are possible at any given time. In Figure 4, an attacker initiates a SYN flooding attack by sending many connection requests with spoofed source addresses to the victim machine. As a result victim allocates resources. When the limit of half open connections is reached, all successive connection establishment attempts are refused, whether they are legitimate or not. If the attacker wants the denial of service condition to last longer than the timeout period, he needs to continuously keep requesting the victim for new connections. The amount of CPU and network bandwidth required by an attacker for a sustained attack is negligible [17].

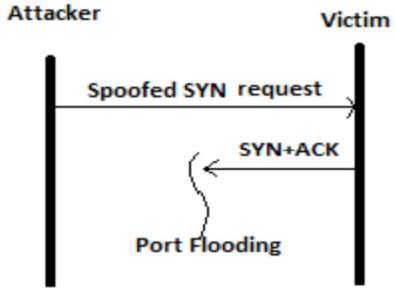

Fig 4. SYN flooding attack

4. DETECTION AND PREVENTION OF DOS ATTACKS

Application layer Dos attack detection: Some techniques used for used for application layer DoS detection are [13]:

- Client Puzzle Protocol.
- Intrusion Detection Systems.
- Ingerss Filtering.
- Threshold Values.

The idea of Client Puzzle Protocol is to correctly solve a mathematical puzzle before establishing a connection, after solving the puzzle, the client would return the solution to the server, which the server would quickly confirm or reject. The puzzle requires a minimal amount of computation on the client side. The malicious user will not be able to simultaneously establish a large numbers of connections due to time delay in solving puzzle. Intrusion detection is the process of monitoring events occurring on the network and analyzing them for signs of probable incidents, malicious threats etc. IDS is a software tool that automates the intrusion detection process. Ingress filtering is a technique used to make sure that incoming packets don‘t have spoofed source IP addresses in their headers. Threshold value is defined as a predetermined percentage of the maximum number of requests that a server can handle. The two novel approaches for application DoS/DDoS attack detection are Signature based attack detection and Anomaly based attack detection.

Detecting/Preventing Dos at MAC layer: Some techniques used for used for MAC layer DoS detection are:

MAC address spoof detection: Spoofing can be detected using sequence number field, whose value is incremented by one for each non-fragmented frame [9]. An attacker does not have the ability to alter the value of sequence number if he cannot control the firmware functionality of his wireless card. Through the analysis of the sequence number pattern of the captured wireless traffic, detection systems were shown to be capable of detecting MAC address spoofing to identify de-authentication/de-association attacks.

Cryptographically protecting management and control frames: IEEE started to work on a proposal at the 802.11 Task Group ‘w‘to extend security to the management traffic. The new extension will be able to provide protection against some of the MAC layer DoS attacks (e.g. Deauthentication attacks), but will not surely be a solution for all DoS attacks. The final specification of protocol is yet to be publicized; however, it is known that mitigating DoS attacks is not the actual goal of the working group [9]. The cryptographic solution can work against different types of attacks but especially public key cryptography is expensive and can easily be a DoS target itself. For the sake of not opening a new DoS hole, the efficiency of the new protocol has utmost importance. Similar to 802.11i, we expect 802.11w to be comprehensively reviewed in detail after it is announced.

Maintaining MAC address Table: Access point maintains a table consisting of the MAC address of the legitimate users [10]. When any user send a management frame then the MAC address of the sender is search in the AP‘s table if it matches then the frame will be proceed otherwise AP will drop that management frame. But this way is not so much effective because an intruder can easily sniff and fake address of legitimate wireless users. So this technique is not much uses but can be more effective by combining this in another authentication method and used to prevent DoS attacks. Other problem arises about the poor scalability of the AP. Difficulty comes to add every MAC address in the table and to maintain that table for any enterprises. It also can be impractical if any user of wireless network enterprise is dynamic and moving one AP to another.

Detecting/Preventing DoS at Physical layer: Jamming attack is a type of DoS attack at physical layer [9]. Low throughput, low packet delivery ratio (PDR) and high packet latency are indicators of a jamming attack. But, these indicators can also be present, at network congestion. Thus, better way should be used to differentiate it from other network conditions.

Two types of jamming detection approaches are:

- Signal strength consistency.
- Location consistency.

In signal strength consistency approach, a station is suspected to be a victim of a jammer station, if the measured average signal strength of incoming signals is high and PDR is low. Signal strength level is an indicator of a high quality channel.

In Location consistency, if the PDR of a data flow between a sender and a receiver is extraordinarily low despite the fact that these stations are physically close enough, then a jammer station is suspected to be present in the surrounding area. If the existence of an active jammer is detected or suspected then the legitimate users in the network should take actions to counter the intended actions of the jammer .Another solution can be if there are multiple spatially dispersed APs around then a mobile station can move away to a position where it can associate with another AP provided that the jammer station's power is not high enough to jam the new link.

DDoS prevention and Detection techniques: The mechanisms can be categorized mainly in two categories as:

- Source based mechanisms.
- Destination based mechanisms.

Source based mechanisms are deployed near the source of attack to prevent generating DDoS attacks. Various source based mechanisms are[12] Ingress/Egress filtering mechanisms (used to detect and filter packets with spoofed IP addresses at the source‘s edge routers based on the valid IP address range internal to the network), D-WARD(detect DDOS flooding attack traffic by monitoring both inbound and outbound traffic of a source network and comparing the network traffic information with predefined normal flow models), Multi-Level Tree for Online Packet Statistics (MULTOPS, Normally the rate of traffic in one direction is proportional to the opposite direction. So, a significant difference between the rates of traffic going to and coming from a host can indicate that the network prefix is either the source or the destination of an attack. MULTOPS detects and filters DDoS flooding attacks based on this mechanism).

In Destination-based mechanisms detection and response is mostly done at the destination of the attack. Various Destination-based mechanisms are[12] IP Trace back mechanisms(It is a process of tracing back the forged IP packets to their true sources rather than the spoofed IP addresses that was used in the attack is called trace back), Management Information Base (MIB, its data is comprised of parameters that indicate various packet and routing statistics. Continuously analyzing MIB can help victims to identify when a DDoS attack is occurring), Packet marking and filtering mechanisms (aim to mark legitimate packets at each router along their path to the destination so that victims‘edge routers can filter the attack traffic), Packet dropping based on the level of congestion (drop suspicious packets when the network links are congested to a certain level).

We can also avoid these attacks by installing the updated security patches from software vendors [3]. Install antivirus software with up-to-date signatures on all mail servers to keep email worms that could be DoS tools. Firewalls and routers can provide a great degree of protection through ingress (inbound) and egress (outbound) filtering Use Egress filter in the network firewall and/or router and make sure whatever comes out of the network only has source addresses that belong to the network and use Ingress filter to confirm that packets coming to the network have source addresses that are not on the inside network.

The various other available solutions to avoid or detect DoS attacks are explained as follow:

Packet Marking: It inscribes some path information into the header of the packets themselves [15]. The marking can be deterministic or probabilistic. In deterministic marking, every router marks all packets. The drawback of the deterministic packet marking is that the packet header grows as the number of hops increases and overhead will be imposed on routers to mark every packet. The probabilistic packet marking (PPM) encodes the path information into a small fraction of the packets. The assumption is that during a flooding attack, a huge amount of traffic travels towards the victim. Therefore, there is a great chance that many of these packets will be marked at routers throughout their journey from the source to the victim. It is likely that the marked packets will give enough information to trace the network path from the victim to the source of the attack.

Traffic filtering- It is another method to prevent DoS attacks to define a limit for the AP to process the management frames in per second. AP will count the number of management frames per second receiving from any particular MAC address and if that are exceed from an already decided limit then next all frames will be ignored at that second for that particular MAC address. A problem can occurs only in a case if an intruder is sending continuously management frames by changing the MAC address for every frame per second then AP will process all the frames understanding that a large number of clients want to associated simultaneously.

Letter envelop Protocol: To prevent the disassociation attack, we can uses letter-envelop protocol [1] to authenticate management frames in association process .After authentication process between wireless station and access point, the association process takes place.

ICMP Trace back: In this approach every router samples the forwarded packets with a very low probability [15] and sends an ICMP trace back message to the destination. An ICMP trace back message contains the previous and next hop addresses of the router, timestamp, portion of the traced packet, and authentication information. The drawback of this approach is that the attacker can send many false ICMP Trace back messages to confuse the victim.

Location tracking: Once a DoS attack is detected, it is paramount to determine the physical location of the source or attacker [8]. For example, by generating an alarm in real-time and pin-pointing the location of the attacker.

Large Number of Association Request (LASO): In this attack, the attacker continuously uses random MAC address for making association with an Access Point (AP). By using this, the attacker makes the AP busy in working with the attacker‘s request. It prevents any other clients to join with AP. Pre-Check and Pre-Association processes [11] work together to avoid LASO attacks

Against Spoofing: ARP poisoning or ARP spoofing [3] can be avoided couple of solutions. Use network switches that have MAC binding features that store the first MAC address that appears on a port and do not allow this mapping to be altered without authentication. Making ARP request unicast can save lot of congestion. Adding authentication to know the identity of the sender or against packet tampering makes it secure. ARP

request packets can be sent to a central server which has the IP-MAC address mapping and the server can sent the ARP response with a strong digital signature using a collision free one way hash function to the requested host. This can protect against tampering or injection of new forged ARP packets. Web spoofing depends mainly upon social engineering tricks and it is thus important to educate users and to be generally aware of the address window in a browser that displays the web address that they are directed to. That can help if some suspicious web site address comes up. DNS spoofing can be prevented by securing the DNS servers and by implementing anti-IP address spoofing measures.

Against flooding attack : TCP SYN flooding on devices behind a firewall from hosts with random IP addresses is easy, since access list can block such IP addresses or blocks of it. But on web or mail server with public internet access, there is no way to check whether the incoming IP addresses are hostile or non-hostile. Some options available in such as case are [3]: increase the connection SYN ACK queue, decrease the time-out waiting for 3 ways handshake and employ vendor software patches. A combination of Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS) can greatly help especially against all flooding attacks. Signature detection scheme would be good at detecting any known attacks. Alerts arising from any suspicious activity can be intimated to the administrator immediately. Firewalls are an excellent form of protection; however, they must leave some ports open to allow the operation of the web, mail, ftp, and other Internet based services, and which are the paths exploited by most of the vulnerabilities.

5. CONCLUSIONS

DoS attacks are significantly simpler to transmit on wireless systems than on wired systems commonly because of the idea of wireless correspondence as a packet wildly travel around noticeable all around. In the wake of creating numerous safe principles IEEE 802.11 wireless system is as yet helpless against assaults. DoS attacks could formulate difficult issues the genuine clients. DoS could be started at physical layer, data link layer, network layer, application layer and so on through numerous ways. In future more consideration must be paid to DoS issues as accessible arrangements are not ready to stop DoS attacks completely. What's more, ensured insusceptibility against DoS attacks could never be conceivable because of the transparency of the channel. This survey paper thoroughly clarified diverse DoS attacks and there accessible arrangements. The significance of beating DoS attacks on 802.11 WLAN condition is talked about in this paper. The different analyses to guarantee DoS attacks are accounted for. The effect of DoS attacks might formulate significant issues the clients since they are unconscious of the assailant's aim. Once the sort of DoS attack is recognized, the guard components could be conveyed on the system. Recently new genuine imperfections in 802.11 supplies of real merchants have been accounted for. Despite the fact that these vulnerabilities are because of issues in the administration of bundles at upper layers (ARP asks for and divided UDP parcels), they affirm that much work stays to be done before remote systems can be securely utilized in areas (e.g., healing centers) where dissent of administration assaults could cause serious harm.

REFERENCES

[1.] Arockiam. L Vani. B ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network‖ IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1563-1571.
[2.] Mofreh Salem, Amany Sarha, Mostafa Abu-Bakr ―A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks‖ ICGST- CNIR, Volume (7), Issue (I), July 2007.
[3.] Lawan A. Mohammed and Biju Issac ―Detailed DoS Attacks in Wireless Networks and Countermeasures‖ Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 1, 2006.
[4.] 802.11 Denial of Service Attacks and Mitigation‖ Stuart Compton SANS Institute.
[5.] Peter Egli, Product Manager Wireless & Networking Technologies ―Susceptibility of wireless devices to denial of service attacks ―.
[6.] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem,‖Denial of Service Attacks and Challenges in Broadband Wireless Networks‖ IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008.
[7.] G.A Marin ―Network security basics,‖ In IEEE Security and Privacy, Vol.3, p 68-72, November 2005.
[8.] Understanding WLAN DoS Vulnerabilities & Practical Countermeasures‖ Part number WP-WLAN-DENIAL. Printed in USA 01/10. MOTOROLA.
[9.] Kemal Bicakci, Bulent Tavli, ―Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks‖, Computer Standards & Interfaces 31 (2009) 931–941.
[10.] Abhishek Gupta, Manish Garg :‖ DoS Attacks on IEEE 802.11 Wireless Networks and Its Proposed Solutions‖.
[11.] Arockiam .L , Vani .B ― A Comparative Study of the Available Solutions to Minimize Denial of Service Attacks in Wireless LAN‖ Int. J. Comp. Tech. Appl., Vol 2 (3), 619-625.

[12.] Saman Taghavi Zargar, James Joshi, David Tipper, ―A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks‖ IEEE communications surveys & tutorials, vol. 15, no. 4, fourth quarter 2013.
[13.] Veronika Durcekova, Ladislav Schwartz and Nahid Shahmehri ―Sophisticated Denial of Service Attacks aimed at Application Layer‖ IEEE 2012.
[14.] Arshey.M, Mr.C.Balakrishnan ―Prevention Strategies and Network Intrusion Prevention Techniques for Dos Attacks―International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2013.
[15.] Ahsan Habib, Mohamed M. Hefeeda, and Bharat K. Bhargava. ―Detecting Service Violations and DoS Attacks‖.
[16.] John Bellardo and Stefan Savage‖ Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions‖ Department of Computer Science and Engineering University of California at San Diego.
[17.] A. B. M. Alim AI Islam, Tishna Sabrina ―Detection of various Denial of Service and Distributed Denial of Service Attacks using RNN Ensemble‖ .Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December, 2009, Dhaka, Bangladesh.
[18.] Wenjun Gu, ZhiminYang, Can Que, "On Security Vulnerabilities of Null Data Frames in IEEE 802.11 based WLANs", The 28thInternational 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.] Bellardo, John, and Stefan Savage. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions." In USENIX security, pp. 15-28. 2003.
[27.] Edgar D Cardenas - MAC Spoofing – An Introduction. [Online].Available: http://www.giac.org/paper/gsec/3199/mac-spoofing-anintroduction/105315
[28.] IEEE 802.11 Working Group. "IEEE standard for information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments." IEEE Std 802, no. 11 (2010).
[29.] Nguyen, Thuc D., Duc HM Nguyen, Bao N. Tran, Hai Vu, and Neeraj Mittal. "A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks." In Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on, pp. 1-6. IEEE, 2008.
[30.] J. S. Park and D. Dicoi, "WLAN security: current and future," IEEE Internet Computing, vol. 7, no. 5, pp. 60–65, 2003.