DENIAL OF SERVICE (DOS) ATTACKS

Pimal Khanpara[1], Param Khanpara[2]

[1]Assistant Professor,[2]B.Tech. Scholar, CSE Department, Institute of Technology, Nirma University,Ahmedabad, Gujarat, (India)

ABSTRACT

Wireless Local Area Network (WLAN) have become very popular in almost all organizations and universities. WPA, WPA2, WEP, etc. are some of the examples of these Our WLAN's are not protected from DoS attacks although it has many of these features. Interconnected systems, such as Webservers, database-servers, cloud-computing servers, etc. are under threats of network attackers.[1] Serious impact on computer system is caused by DoS attacks. Wireless solutions are quite important n various organizations, universities and many other places as there are no issues related to wired structured.[2] In wireless networks DoS attacks is of quite importance in present years. Demonstration show that Dos Attacks can be easily launched in MAC layer. The MAC addresses of wireless network devices is forged in most of the cases by the attackers to halt the operation of the wireless network. Such types of attack are easily available for attackers by many tools. Degradation of the network quality and loss of availability of the network within the organization is resulted by such attacks.[1] DDoS attack is a form of DoS attack in which attacker try to use the IP address of the legitimate user. It is an active category of attack among the two type of attack. The main aim of the attacker is to utilize all the resources so that user cannot use them. Large number of computers access is gained by them to set up attack armies (known as botnets) by exploiting their vulnerabilities. A large scale attack can be launched by these created army against the system. Several strategies could be used by the attacker to achieve this goal. The important and common among them is flooding the network with bogus requests. As multiple computer is used the attack is distributed to launch DoS attacks.[3] This paper reviews various denial of service attacks and there prevention/detection solutions. Paper shows how DoS attacks are created, some methods to prevent them and its types. We also identify the issues with existing countermeasure and provide future research directions.

Keyword: DoS Attack, Wireless Network, IEEE 802.11 Network

I. INTRODUCTİON

DENIAL-OF-SERVICE (DoS) attacks are one type of aggressive and menacing intrusive behaviour to online servers. Availability of a victim can be degraded by DoS attacks, which could be a host, a router, or network. By exploiting its system vulnerability or flooding it with huge amount of useless packets they impose intensive computation tasks to the victim. System or victim can be affected for few minutes to several days. Serious damages can be caused to the victim by this.[2] Therefore, for the online services DoS attacks should be taken care of. The main focus is on the development of network-based detection mechanisms.[4]

Wireless networks are preferred over wired networks due to their cost effectiveness and ease of use. New dimensions have been opened up because of Technological innovation in wireless networking. Denial of service is an attack which denies authorized user access to the service provider. Reports show that DoS attack is serious and expensive attack. DoS attack target different layers of OSI model:[6]

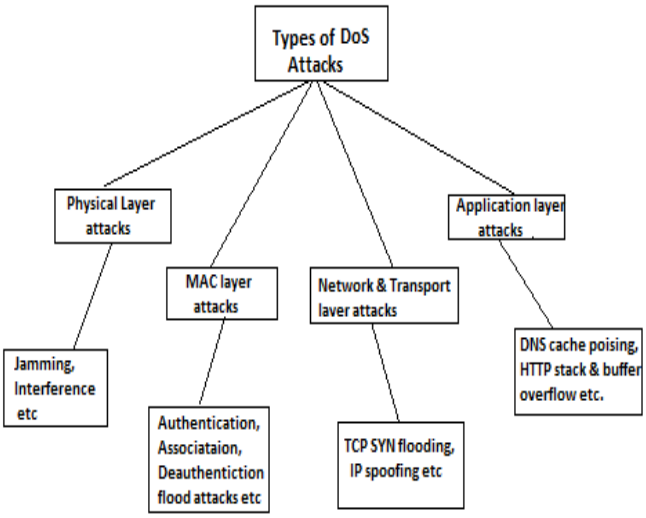
- **Physical layer**: by accidentally cutting a communication cable to take down network services.
- **Data link layer**: to disable the ability of hosts to access the local network.

- **Network layer**: by sending a large amount of IP data to a network.
- **Transport layer**: many TCP connection requests are sent to a host
- **Application layer**: by sending large amount of legitimate requests to an application.

DoS attacks at various layers are shown in the Table below.

Layers	**Attacks**
Routing	Blackhole, Wormhole, Greyhole, Jellyfish,Byzantine, Sybil, flooding
MAC	Unfairness, Selfish MAC, flooding
Physical	Jamming, Scrambling

The various kind of Dos attacks are 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.[5]



1.1 Denial of Service (DoS) Attack

A Denial of Service (DoS) attack aims to stop the service provided by a target. There are two forms to launch it. To exploit software vulnerabilities of a target would be the first form by sending malformed packets and crash the system.[4] The second form creates useless traffic so as to use the resources available to the legitimate users. First form of attack can be easily protected but the second form of attack is not that easy to protect. As the target are connected to public internet they are easily attacked. [7]

A DoS attack is a malicious attempt by a single person or a group of people to disrupt an online service. DoS attacks can be created against a web server and networks.

1.2 Types of DoS Attack

TCP Syn Flood Attack

UDP flood attack

Ping of death attack

Teardrop attack

1.3 Distributed Denial of Service (DDoS) Attacks

In the distributed form of DoS attacks (called DDoS), the attacker first takes control of a large number of vulnerable hosts on the internet, and then uses them to simultaneously send a huge flood of packets to the

victim, exhausting all of its resources. There are huge amount of system that are connected to the public internet and they do not have the security protection and so they could be easily affected by the attack and large amount of loss can be carried out.[8]

1.4 Types of DDoS Attack

IP Spoofed Attack

Distributed Reflector Attacks

Forged Source Attack[8]

II. PHYSICAL LAYER

Communications between wireless devices and launching of simple DoS attacks by scrambling and jamming against the wireless networks can be easily observed due to the shared nature of the wireless medium. In the Physical layers, such attacks through conventional security mechanisms cannot be addressed. Continues transmit in a wireless channel and disregard of the medium access protocol could be carried out by the attacker. When attackers carry out such task users are not allowed to use the legitimate MAC operations . [9]

WiMAX security is implemented in the security sub-layer above the physical layer. Due to this security layer is not secured and several attacks like jamming, scrambling or water torture attack can target the user or the system itself. As mobility is supported by WiMAX these attacks could be easily created as they do not stay at a single place due to this.[10]

2.1 Jamming Attacks

Jamming can be defined as an attack achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel. Jamming can be intentional or unintentional. As information and equipment are easily obtained, jamming attack can be performed easily.

As per Michel Barbeau, jamming attack can be prevented by increasing the power of signals or by increasing the bandwidth of signals using spreading techniques such as frequency spread spectrum (FHSS) or direct sequence spread spectrum (DSS).[10]

The conclusively detect the presence of a jammer of signal strength and carrier sensing time are unable. Packet delivery can be used to differentiate between jamming and congestion but cannot be used to decide the poor utility due to jamming or congestion. There are two protocols by which we can find that jamming occurred or not. One scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, and the other employs location information to serve as the consistency check.[9]

2.2 Scrambling Attacks

Scrambling is a kind of jamming attack that is provoked for a short intervals of time, targeted for a specific WiMAX frames and the parts of the frames that are at physical frame. Attackers in order to affect the normal operation of the network can scramble control or management information selectively. In order to retransmit the slots of data traffic block belonging to the targeted SSs, they can be scrambled selectively. Jamming attacks are more easier to perform than the scrambling attacks as the need, by the attacker, to interpret control information and to send noise during specific intervals. Scrambling is difficult than jamming as it s only for a short time. By monitoring the performance we can introduce the Scrambling attacks.[10]

III. MAC LAYER

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. Using a spoofed source MAC address of an access point an attacker can transmit the packets. The recipient, doesn't know that they are spoofed or not and thus handle the request.[11] Two main MAC layer are follow:

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

3.1 Authentication (Association) Flood Attack

- An attacker uses spoofed source MAC addresses during the authentication/association flood attack, that tries to authenticate and associate to target access point. Resources have been used up by the attacker by making continues false request and thus wasting the memory.

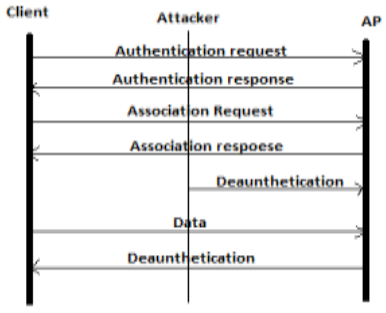
3.2 De-Authentication (Disassociation) flood Attacks

- These are also known as Identity Vulnerabilities. During de-authentication Client first authenticate itself to AP as shown in figure, one part of the authentication framework is a message that allows clients and access points to explicitly request DE authentication from one another. Encryption is not done in the message. So either by pretending to be client or the access point message can be spoofed by the attacker. Disassociation frames are used when client have multiple access point. 802.11 Since a client can be authenticated from multiple access points in order to decide which access point can be used on behalf of client's access point. Like DE authentication de-association frames can be sending by the attacker[12].

3.3 Techniques Used for the Detection of DoS Attacks Are

MAC address spoof detection:

- Spoofing can be detected using sequence number field, whose value is incremented by one for each non-fragmented frame. If the sequence number on the wireless card can't be changed the attacker can not create an attack. 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.[13]



Protection through Cryptography

- The new extension will be able to provide protection to some of theDoS attacks created in this layer but not to all of them [13]. The cryptographic solution can work against different types of attacks but especially public key cryptography is expensive and can easily be a DoS target for itself. For not creating anymore attacks the new protocol has its own importance.

Maintaining MAC address Table:

Access point maintains a table consisting of the MAC address of the legitimate users. 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 it is not that important as the attacker can easily spoof the address of the user. So this technique alone is not that useful but can be used if combined with other type of techniques. Poor scalability of the AP is the another problem. 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[14].

IV. NETWORK LAYER

DoS attacks in network layer can be carried out in wireless as well as wired network. Any client associated with the wireless network is vulnerable to the DoS attack. DoS attack in network layer can be created by sending a huge amount of data. The wireless network infrastructure can be targeted of the victim by these type of attack. ICMP flood is the good example of this attack[15].ICMP flooding is carried out by sending the large amount of ICMP echo-request to the server and using the resources. The attacker can use whole of the resource by spoofing the address of the source and sending the false request. If the attacker makes use of thousands of systems to perform this attack, the target wireless system may be brought down. The attack will quickly consume all available bandwidth, resulting in legitimate users being unable to access wireless services.

DoS attacks in the network layer mainly focus on exploiting routing and forwarding protocols in wireless networks. Ad hoc and sensor network can be easily affected by these attacks. Network layer DoS attacks are different from all other types carried out in the internet. DoS attacks in network layer in wireless system can be easily created as routers support the backhand of the system for such attacks . In addition, DoS defence techniques in the Internet that demand the cooperation of routers are no longer valid.

4.1 Routing Attacks and Defences

Researchers have shown that attackers can manipulate ad hoc network routing protocols to break valid routes and connections. For example, the user is not able to access the destination if the attacker changes the ip address of the destination without the knowledge of the user and so user can't send the packets to the original destination. Thus to avoid the DoS attacks the security of the protocols used for routing is of quite importance. In order to prevent attackers from exploiting the security flaws in routing protocols, several secure routing protocols have been proposed to protect the routing messages and thus prevent DoS attacks. For example, Hu *et al.* (2002) proposed to use TESLA, which is a symmetric broadcast authentication protocol, in routing discovery to secure routing protocols. A route request sent by the source is checked against its own TESLA to prevent attackers from forging or modifying the request.

4.2 Forwarding Attacks and Defences

Similar to routing attacks, attackers can also exploit forwarding behaviour. Typical attacking approaches include injecting junk packets, dropping packets, and disorder packets in legitimate packets. Attackers can use spoofed packets to disguise their attacking behaviour, or find partners to deceive defenders. In order to not permit the access to the service the aim is to utilize the bandwidth or to exhaust it by false request. Hop-by-hop source authentication is needed to prevent attackers from spoofing and flooding packets in wireless networks so that every node participates in the protection of the network. Ye *et al.* (2004) proposed a statistic filtering scheme

that allows en route nodes to filter out false data packets with some probability. This approach will not filter packets that do not carry keys that the en route nodes have, but will discard them at the destination. Zhu *et al.* (2004) proposed an interleaved hop-by-hop authentication scheme that guarantees that false data packets will be detected and dropped within a certain number of hops, although the scheme does not tolerate the change of routers. There is another hop-by-hop source authentication approach with a higher overhead to ensure that a packet can be verified when a route is changed due to unreliability in wireless networks. In this approach, the new route that emerges from the old route takes the responsibility to authenticate the packet. The routing nodes in the new route can then verify the packets based on the new authentication information.

Various DoS attacks at Network Layer can be listed as:

4.3 Wormhole attack

In this attack, the attacker sends the packet received from one place to another place by tunnelling them so that none of them could be lost[16]. This type of process of tunnelling is referred to as Wormhole Attack. It can be established either in wired network between the two end users or in the wireless network where user are connected with no wired structure. As there is an broadcast of packets of radio channel the attacker can also create an attack for the packets that are actually not meant for itself. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. Most of the existing route protocols seems to fail if no extra care is taken for the attacks created by the wormhole and thus special care should be taken of that.

4.4 Blackhole Attack

In this attack, a malicious node falsely advertises good paths (*e.g.*, shortest path or most stable path) to the destination node during the path-finding process (in on-demand routing protocols) or in the route update messages (in table-driven routing protocols). The main intension of these type of attacks is to hinder the path or to convey the false path so that all the data can be exposed to the attacker and the resources are no more available.

4.5 Byzantine Attack

In this type of attacks the attacker writes such an algorithm or the attack in such a way that there quest or the packet of data loops in that is it goes inside an infinite loop[17]. Its very difficult to detect the Byzantine. When the network is being attacked by such attacks it seems to be normal even though its been attacked y such type of attacks and continues its normal operation.

4.6 Information Disclosure

Here the private information of the user may be disclosed by the attacker by establishing such type of attacks. Network topology, geographic location of nodes, or optimal routes to authorized nodes in the network, etc. type of information may be disclosed by such attacks.

4.7 Resource Consumption Attack

In this type of attack the node in the network tries to utilize all of the resources of the other node present in the network. Battery power, bandwidth, and computational power type of resources which are available in limited quantity are targeted in ad hoc wireless networks. The attacks can be in the form of unnecessary requests of the

routes, beacon packets that are generated frequently, stale packets that are forwarded to nodes. Sleep deprivation attack is an attack in which a node remains always busy using the battery power of another node by pumping packets of that node.

4.8 Routing Attacks

There are large number of attacks whose basic aim is to interrupt the network and use the resource (i.e. the bandwidth of the network). Various types of attacks that fall into these category are mentioned below.

Routing Table Overflow: The advisory nodes present in the network advertise in these type of attack to the non-advisory node or the authorized nodes present in the network about the attacks. By such types of attacks the routing tables are being overflowed which is the main aim of attack, so no new node can be added up as there is no space for the entry of new node. These attacks affect more to the proactive protocols as compared to the routing based protocols.

Routing Table Poisoning: In these types of attacks the attacker node either changes the original packets sent to the other nodes or they sent the false request to the other nodes present in the network. The results of these would be the congestion in part of the network, may lead to suboptimal routing or can make part of the network not work properly.

Packet replication: Here the attacker node replicates the original packets. The result of these would be the consumption of the bandwidth, consumption of the power and the destination node might also be confused among such large amount of replicated packets.

Route cache poisoning: In these type of attacks every nodes keep the track and information of the other node across which this node have came in the past and maintains a table of it. Now the attacker node can attack these cache tables and can affect the whole network.

Rushing attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack [19]. An adversary node which receives a*RouteRequest* packet from the source node floods the packet quickly among the whole network before the reaction of the other node that receive the same request. Nodes that receive original request assumes it to be the duplicate or replicated and thus ignores the original one over that sent by the attacker node. Among all the possible path between the source and the destination there would be an intermediate node present in between. Thus all the paths between the source and the destination are not secure as the attacker node is always present. Because of these such attacks are very difficult to be detected usually in wireless network.

REFERENCES

[1] V. Paxson, “Bro: A System for Detecting Network Intruders in Real-Time,” Computer Networks, vol. 31, pp. 2435-2463, 1999.

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, “Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges,” Computers and Security, vol. 28, pp. 18-28, 2009.

[3] Jochen Schiller, “Mobile Communication”, Pearson Education, second Edition, page No. 221-223

[4] 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.

[5] Yao Chen, Shantanu Da, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak Detecting and Preventing IP-spoofed Distributed DoS Attacks International Journal of Network Security,Vol.7, No.1,, pages 70 - 81, July 2008.

[6] Tao Peng, Defending Against Distributed Denial of Service Attacks IEEE 2002.

[7] Xia Wang∗, Johnny S. Wong, Fred Stanley and Samik Basu, *"Cross Layer Based Anomaly Detection in Wireless Mesh Networks"* in Ninth Annual International Symposium on Applications and the Internet, 2009

[8] Shafiullah Khan, Kok Keong Loo, Zia Ud Din, *"Cross layer design for routing and security in multi-hop wireless networks"* in Journal of Information Assurance and Security 4 (2009) pp.170- 173.

[9] Qijun Gu and Peng Liu Texas State University – San Marcos San Marcos, TX, 78666, Pennsylvania State University University Park, PA, 16802.

[10] A survey of wimax security threats, Trung Nguyen**.**

[11] 802.11 Denial of Service Attacks and Mitigation‖ Stuart Compton SANS Institute.

[12] 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.

[13] Kemal Bicakci, Bulent Tavli, ―Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks‖, Computer Standards & Interfaces 31 (2009) 931–941.

[14] Abhishek Gupta, Manish Garg :‖ DoS Attacks on IEEE 802.11 Wireless Networks and Its Proposed Solutions‖.

[15] ICMP Flood Attacks - http://www.securityfocus.com/infocus/1853

[16] Y. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedings of IEEE INFOCOM 2003, vol. 3, pp. 1976-1986, April 2003.

[17] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proceedings of the ACM Workshop on Wireless Security 2002, pp. 21-30, September 2002.

[18] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, February 1999.

[19] Y. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security 2003, pp. 30-40, September 2003.