Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.151 – 159

A REVIEW ON DENIAL OF SERVICE ATTACKS IN WIRELESS MESH NETWORK

Swati Singla[1], Deepika Dhingra[2]

Student[1], Assistant Professor[2]

Department of Computer Science and Engineering, Om Group of Institutions

singla.swati1993@gmail.com [1]

dhingra.deepika17711@gmail.com [2]

Abstract: Wireless Mesh Networks (WMN) being multi-hop wireless networks are prostrate to most of the prevention attacks on multi-hop wireless networks. Wireless Mesh Networking is an advance technology in order to provide a possibility to build a network that can acquire in term of coverage to offer service access (i.e. internet access) for a large number of people with different need.

In this chapter discuss about the security owing in multi-hop wireless networks that are related to WMN. The attacks in WMN and the possible solution mechanism to prevent and relieve these attacks. At present, near field wireless communication technology had been used to widely, especially for Bluetooth, wireless local area network (WLAN), infrared, etc. After that we would study of Existing Security loop holes within wireless mesh based distributed network environment [1]. Main objective is to boost outer layer security by enhancing packet filter mechanism. The purpose of this article was to examine security & privacy issues within some new & emerging types of wireless networks, & attempt to identify directions for future research.

Introduction:

A mesh network is outline of peer wireless access nodes that allow for Promote connections to a network infrastructure, including reorganized around blocked paths, by "hopping" from node to node. The term “Mesh Network” is frequently put upon similar with “Wireless Ad-hoc Network”. However, ad-hoc networking typically refers to an arbitrary topology of client nodes and associated hosts, where a mesh network generally refer to a network of attach wireless access nodes that use provide multi-hopping backhaul service between client node and the Internet[1]. For mesh security, this case become significant – while most of the underlying technologies are indistinguishable there are inexplicit trust acceptation pretended in a mesh network (e.g., the nodes belong to the same administrative and security domain) conflict assumed random and arbitrary collection of nodes in an ad-hoc network[1].

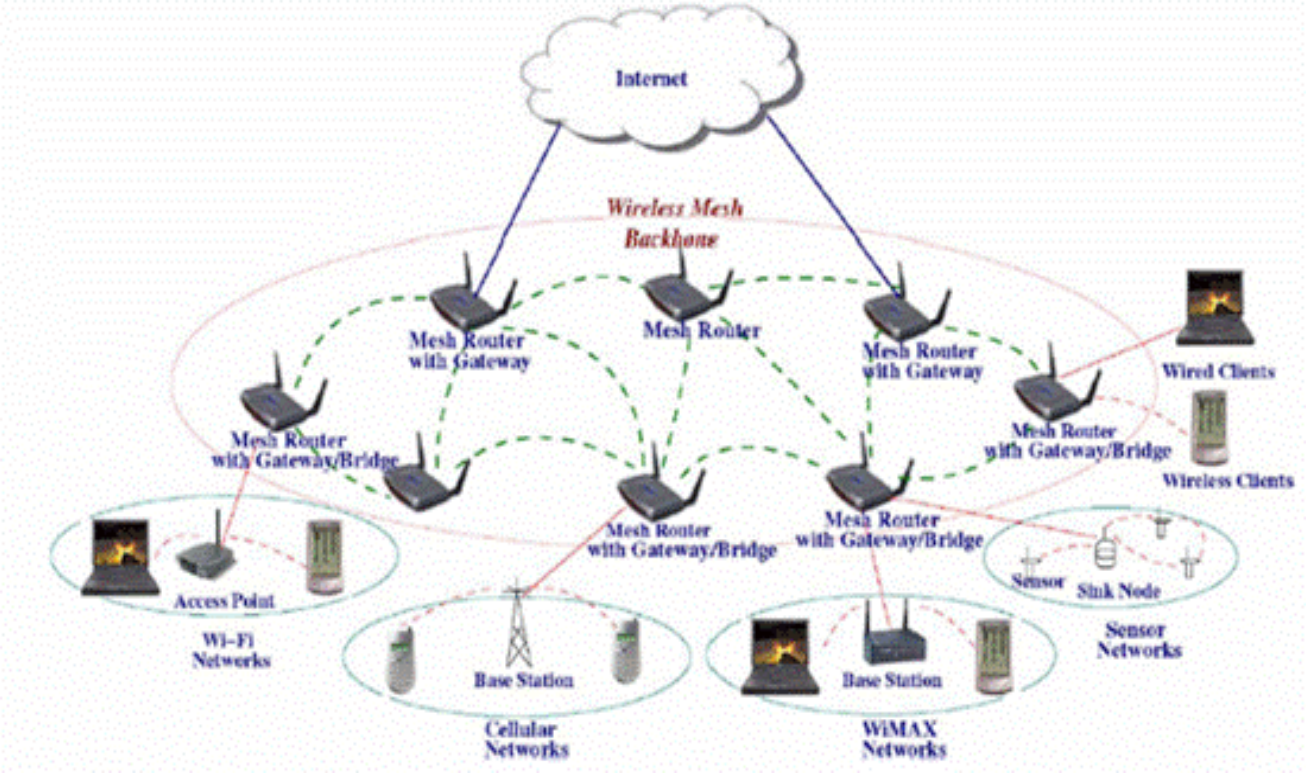

Figure 1: Wireless mesh network

In wireless mesh networks (WMN) wireless mesh routers form thickly interconnected multi-hop topologies [4]. For local communication and routing to a wired access network the routers

automatically configure a wireless broadband backbone. Three variety of wireless mesh network rear be identified:

1) In infrastructure WMNs [3] (Figure 1) mesh routers form a network offering connectivity to clients. The network is meant to be self-configuring and self

Healing and to offered gateway functionality for connections to wired network.

2) Client WMNs are ad-hoc networks formed by clients among them self. None of the dedicated routers or infrastructure exists, so that the clients have to be self configured and act as routers for the traffic in the client WMN (if mobility is there Client WMNs are very similar to MANET). In this type of architecture, client nodes make the actual network to perform routing and configuration functionalities as well as provided end-user applications to customers.[1]

3) Hybrid WMN aggregate the advantage of the two other WMNs. mesh client can approach the network through mesh routers as well as directly meshing with other clients [5]. The infrastructure provide connectivity with other network such as the Wi-Fi, Internet, cellular, and sensor networks and inside WMN the routing capabilities of client provide improved connectivity and reporting.

DENIAL OF SERVICE ATTACK (DoS):

A Denial of Service (DoS) attack is that effort to prevent the victim from being able to use all or part of his network connection. Denial of service attacks may hold out to all layer of the protocol stack[2]. They target service availability access to a service provider. They have numerous form and they are hard to prevent. For instance, an attacker may send an unreasonable amount of request to a server that had to test their legitimacy. These test require an amount of CPU and memory capacity[2]. Due to the excessive number of request the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired network, DoS attacks in MANETs may not only add damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be congested due to the limited bandwidth available as compared to fixed networks. Denial of service attacks may extend to all layers of the protocol stack.[12] They target service authorized users access to a service provider. They have numerous form and they are hard to prevent. For instance, an attacker may send an excessive amount of request to a server that has to test their legitimacy. This test requires an amount of CPU and memory capacity[3]. Due to the

excessive number of request, the server will be busy in testing illegal request and will be unavailable for legal users. In comparison with wired networks,[11] DoS attacks in MANETs may not only bring damage to the victim node, but may also degrade the performance of the whole network because nodes have limited battery power and the network can easily be engorged due to the limited bandwidth available as compared to fixed networks. Physical Layer: DoS attack can be launched against physical layer by using radio jamming device by source of strong noise to interfere the physical channel and may compromise the service availability. For jamming attack in WMN, the attacker can launch the attack from anywhere. Due to the huge coverage area and thick deployment of wireless mesh router in WMN, it is more than vulnerable to physical layer DoS attacks. Different types of jamming attacks [5] are:

- Trivial Jamming Attack: In which an attacker constantly transmits noise.
- Periodic Jamming Attack: In which an attacker transmit a short signal periodically[6]. This transmission can be scheduled often enough to disrupt all other communications, for example, with a period less than the AIFS. It is also called scrambling.
- Reactive Jamming Attack: In which an attacker transmit a signal whenever it observe that another node has suggest a transmission, causing a collision during the second portion of the message.

Detection and Prevention of DoS Attack:

The extreme point diversity of DoS attack has produced likewise various protection proposal from the network security research community[11]. In most cases complete protection architecture should include the following elements:

- **Detection** of the existence of an attack. The detection can be either anomaly-based or signature based or a hybrid of these two. In anomaly-based detection, the system recognize a difference from the standard behavior of its client while in signature-based it trie to identify the characteristics of known attack types.
- **Classification** is the incoming packet into valid (normal packet) and invalid (DoS packets). As in detection, one can choose between anomaly-based and signature-based classification techniques[12].
- **Response.** isn the most general sense, the protection system either drop the attacking packet in a timely fashion or renders them harmless by redirecting them into a trap for further evaluation and analysis. Detection and Classification usually overlap, since the method used to detect the existence of an attack often provide the necessary information to start responding towards probable normal and probable DoS traffic. Also, all three

element of protection may benefit by the use of an additional secondary element, which is the *trace back* of the real source of the traffic[13].

In 2016 DoS detection and prevention by using Server modules

To detect the DoS attack this mechanism is used. In this enable the connection between two systems using LAN cable taking one as Client side and another one as Server side. Confirming the connection using PING command.[17] Check for the proper file sharing. Set the maximum number of request to 10 and blocking time for 10 minutes at server side. At the beginning open the ORACLE Data Base and run the query to check data is present or not; now user tries to login and sends request to the server using User Name and Password, by clicking on LOGIN button which hits the requests to the server[17]. Check the Data Base to ensure Number of hits, IP Address, Timing and Status (BLOCKED OR UNBLOCKED). If the Number of hits is greater than the set value the user is blocked automatically by providing the error message.[17]

In 2015 DoS attacks prevention on Collaborative Detection of DoS Attacks

Collaborative Detection of DoS Attacks over Multiple Network Domains Present a new distributed approach to detecting DoS (distributed denial of services) flooding attacks at the traffic flow level. The new defense mechanism system is suitable for efficient implementation over the core network operated by Internet service providers (ISP)[18]. At the early stage of a DoS attack, some traffic fluctuation is detectable at Internet routers of edge networks. We accquire a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The idea is to detect abrupt traffic change across multiple network domain at the earliest time. Early detection of DoS attacks minimize the flooding damage to the victim system service by the provider. The system is built over attack-transit routers, which work together cooperatively. Each ISP domain has a CAT server to aggregate the flooding alert reported by the routers. CAT domain servers collaborate among themselves to make the final decision. To resolve policy conflict at different ISP domain, a new secure infrastructure protocol (SIP) is developed to establish the mutual trust or consensus.[18]

In 2014 DoS attacks prevention on mitigation system & ACL Detection of DoS Attacks

The Intelligent DDoS Mitigation Systems (IDMSs) and ACL are the most effective mechanism and commonly used mitigation mechanism (Arbor, 2014). It is also believed that IDMSs provide more intelligent, surgical capabilities for DoS attack mitigation. Firewall usage is at the third place after IDMS and ACL[17]. Other possible DoS attack mitigation technique include SYN proxy, connection limiting, aggressive ageing, source rate limiting, dynamic filtering, active verification, anomaly recognition, granular rate limiting, white list-black list, and dark address prevention.

Countermeasures of Denial of Service attacks

1. Cookies Cookie-based approaches change in the TCP signaling behavior by using one-way hash functions to verify the authenticity of connection requests. Bernstein and Bona suggested a stateless cookie approach. When a client sends a SYN packet, the server calculates a one-way hash of the sender's sequence number, ports, the server's secret key, and a counter that changes every minute [2]. The server sends the result of the one-way hash to the client, and the connection is not established. When the client replies with an ACK packet, the server recalculates the same hash function and throws away the packet if it fails to authenticate with the server. Otherwise, set up the Transmission Control Block, if it doesn't already exist .

2. Stateless protocols Aura and Nikander described weaknesses of stateful protocols, and methods to change stateful protocols into stateless ones. Stateful protocols have an upper limit on number of simultaneous connections, because there is a limited space available for storing connection state information[13]. When this limited space is exhausted, new connections are refused. To remedy this, the state information is stored on the client rather than on the server . To ensure integrity and confidentiality of state data and connection, the data stored on a client can be encrypted with the server's key.

3. Client-Puzzle protocols To prevent junk mail, Dwork and Naor proposed requiring a sender to compute a moderately hard pricing function or cryptographic puzzle for each message; the cost to compute the pricing function is negligible for normal users, but high for mass mailers. Juels and Brainard extended the idea so that if a server suspects it is under a DOS attack, small cryptographic puzzles are sent to clients making requests. To complete its requests, a client must solve its puzzle correctly.

4. Cryptography

Cryptography has been process of altering plaintext (ordinary text, just as letter) using process encryption into cipher text using procedure decryption[3]. This procedure has been used for secure communication btw two parties within occurrence of third party.[8] There are four goals for Modern cryptography:

- Confidentiality: It identifies that only participants (Sender & Receiver) should be able to access message.
- Integrity: Content of message should not be changed. If this has been altered, then this has been called type of modification attack.

- Non-repudiation: There has been situation where sender converts content of message & after that he refuses that he had not sent message[8].
- Authentication: Both sender & receiver has to prove credentials to each other.

In current times cryptography has been basic requirement of computer expert for security purpose so that two parties could send data to each other without any modification & confidently. So both sender & receiver could validate to each other for secure communication so that material could be safely send to each other.

5. Intrusion Detection Limitation

Intrusion detection has become an executable mean of spotting threats against wireless networks. Since the 802.11 medium accesses control technology is susceptible to denial-of-service attacks, as well as the possibility of spoofing legitimate access points, wireless intrusion detection systems have offered some defending team through detection of wireless network attack[3]. However wide-area wireless mesh networks fix wireless intrusion detection much harder due to the dispersion geographic distribution of wireless nodes. For example any 802.11 MAC management vulnerabilities are mainly addressed by detection, rather than prevention[9]. Wireless intrusion detection sensor are often used in enterprise wireless networks to detect common 802.11 attacks including MAC management attacks as well as "rogue AP" attacks.

 Open authentication will imply limits on network authentication. Wireless intrusion detection sensor is most effectively deployed indoor in a bounded physical local, where wireless IDS models to wide-area outdoor deployment extended is not feasible.

 Integrated threat detection. Mesh access point that provide integrated detection and prevention controls for wireless threats will best address the security threats. This may include security features that observe MAC management attacks (e.g. de-authentication or MAC association flooding, etc.) or report unauthorized mesh AP evils-twins broadcasting within the deployment area.

6. **Digital Signatures:** If the nodes can produce digital signature and check them; then the solution is straight forward. While one node can verify the other node signature using public key cryptography, both nodes will establish a common secret key, using imprinting techniques, and will be able to accept messages protected by secret key.

7. **Pair-Wise Key Sharing**: In WMNs, symmetric cryptography is possible as it requires less computation than asymmetric cryptographic techniques[8]. Or a better solution would be using the Diffie-Hellman (D-H) key exchange9. Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish shared keys over an insecure communications channel. This key can then be used to encrypt subsequent communication using a Symmetric key cipher.

8. **Secure Routing:** To attain accessibility of routing protocol should be robust in front of dynamically changing topology and malicious attacks. There are two sources of threats to Routing protocols. The first comes from external attackers. The second and the most important kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. To protect from such attacks we can effort certain properties of WMN to reach assure routing.[3]

The basic idea is to transmit redundant information through additional routes for error detection and correction. Even if certain routes are compromised the receiver may still be able to validate messages.

Conclusion

In this we have discussed the main security issues and challenges in Wireless Mesh Networks. We resolve that security attacks at different layers while most attacks are much harder to counter because the challenger is aware of the network secrets and protocols. DoS attacks can compromise the two main characteristics of secure wireless networks i.e. data integrity and service availability. WMN is more vulnerable to different types of DoS attacks are compared to IEEE 802.11 and IEEE802.16 due to multi-hop architecture, vast coverage area, and ad-hoc end-users connectivity. In future more attention must be paid to DoS issues as available solutions are not able to stop Dos attacks fully. And guaranteed immunity against DoS attacks can never be possible due to the openness of the channel.

REFERENCES

1. Radomir Prodanovi and Dejan Simi, "A survey of wireless security", Journal of Computing and Information Technology
2. Kemal Bicakci and BulentTavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks", Computer Standards & Interfaces
3. L.Arockiam and B. Vani, "framework to detect and prevent medium access control layer denial of service attacks in wlan",Computer science
4. Ian F.Akyildiz,Xudong Wang and Weilin Wang, "wireless mesh networks: a survey," Computer Networks, vol. 47, pp. 445- 487,
5. W. Zhang, Z. Wang, S. K. Das, and M. Hassan, "Security Issues in Wireless Mesh Networks," In Book Wireless Mesh Networks: Architectures and protocols. New York: Springer
6. A. Patcha and A. Mishra," Collaborative security architecture for black hole attack prevention in mobile ad hoc networks","*Radio and Wireless Conference,*
7. Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks," In Book Ad Hoc Networks Technologies and Protocols, Springer,
8. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT,
9. M.Imani Bing He, S M.E.RajabiM.Naderi "Vulnerabilities in network layer at Wireless Mesh Networks (WMNs) ".International Conference on Educational and Network Technology
10. C. Meadows, "A Formal Framework and Evaluation Method for Network Denial of service
11. Sahil Seth,Anil Gankotiya "Denial of Service attacks and Detection Methods in Wireless Mesh Networks " In 2010 International Conference on Recent Trends in Information, Telecommunication and computing.
12. paper.ijcsns.org/07_book/200605/200605C01.pdf
13. IEEE 802.11 Wireless LAN Security Overview by Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, Department of Electrical & Computer Engineering – Sultan Qaboos University, Oman. IJCSNS International Journal of Computer Science & Network Security, VOL.6 No.5B, May 2006
14. Attacks within Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, & David B. Johnson, Member, IEEE, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006
15. Lightweight Hidden Services by Andriy Panchenko, Otto Spanioly, Andre Egnersy, & Thomas Engel Computer Science department, RWTH Aachen University, Germany within June 2011
16. In 2011 PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks 36th Annual IEEE Conference on Local Computer Networks, 978-1-61284-927-0/10/$26.00 ©2011 IEEE
17. International Journal of Advanced Research in Computer Science and Software Engineering, Detection and Prevention of DoS Attack
18. A survey on distributed denial of service attack and defence international journal of engineering sciences & research technology.

