International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 5 Issue 5, May-2016

A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks

Ms. Snehleta[1], Mr. Ashish[2]

[1]M. Tech Scholar, RIEM, Rohtak, Haryana
[2]AP, ECE Dept., Rohtak Institute of engg. & mgmt., Rohtak, Haryana

ABSTRACT

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 [2]. It is hardwired or hardcoded 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.[3]

Keywords: Denial of services, Media Access layer, Access Point, Access control list, Frequency- hopping spread spectrum

1. 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 traditionalDoS 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.[4]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. DoS attacks are perpetrated at various levels of the network defined in the OSI seven-layer network model. [5] 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.

2. 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.

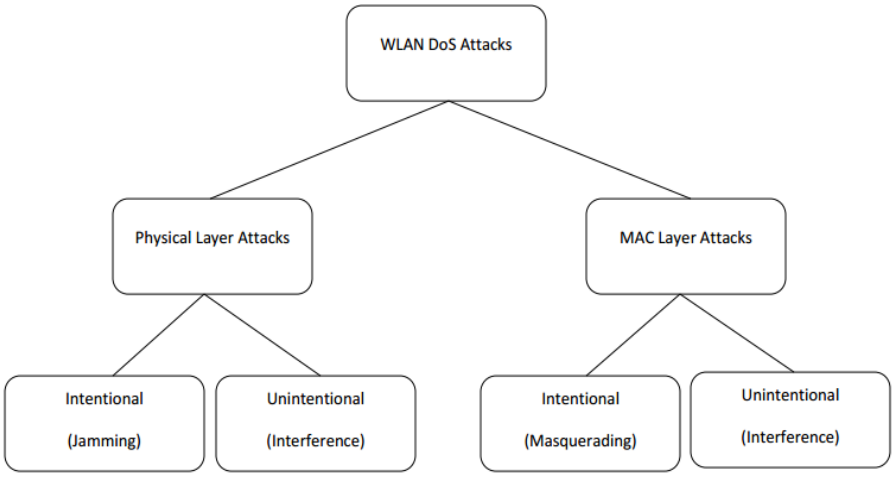

Fig.1 Tree classification of Denial of Service attacks in wireless data networks

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 [5]. 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.

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 5 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.

3. JAMMING TECHNIQUES:-

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.[4] 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 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).[4] 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.

4. INTENTIONAL DOS AT THE MEDIA ACCESS CONTROL (MAC) LAYER:-

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; deauthentication flooding, de-association flooding and resource exhaustion attacks; proberequest 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.[5] 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.

B) 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 MAC layer DoS Intentional Unintentional Masquerading Resource Exhaustion Probe request flooding Deauthentication flooding DeAssociation flooding Authentication flooding Association flooding 9 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.

C) 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 11 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.

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..

REFERENCES

[1]. Stuart Compton : GAWN Gold Certification Author, stuartcompton@hotmail.com, “802.11 Denial of Service Attacks and Mitigation” - Sans Institute Reading , May 2007
[2]. Konstantinos Pelechrinis, MariosIliofotou and Srikanth V. Krishnamurthy, University of California, Riverside, “Denial of Service Attacks in Wireless Networks: The case of Jammers” - IEEE March, 2011.

[3]. 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
[4]. Vikram Gupta, Srikanth Krishnamurthy and MichalisFaloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks" – IEEE, Oct 2002
[5]. 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
[6]. Taimur Farooq, David Llewellyn-Jones, Madjid Merabti , "MAC Layer DoS Attacks in IEEE 802.11 Networks" - 2007 G. Dazhi Chen, Jing Deng, and Pramod
[7]. Varshney, EECS Dept., Syracuse University, Syracuse, "Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming" - 2003
[8]. 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
[9]. Rupinder Cheema, Divya Bansal, Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks" - International Journal of Computer Applications, June 2011