International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Analysis of DoS attack in various layers of Wireless Sensor Network

Er. Himanshi Vashisht, Sanjay Bharadwaj, Sushma Sharma
[1]CSE, Haryana Engineering College, Jagadhri, Haryana, India
[2-3]Computer, DAV College for girls, Yamunanagar, Haryana, India

ABSTRACT

A wireless sensor networks (WSN) is a recent advancement of technology of computer networks and electronics. They have a wide variety of applications ranging from data gathering to data transmission through wireless media. Along with these applications, WSN also has some weakness due to which its sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is one of the most popular attack. This attack affects different layers of WSN and each layer has different type of DoS attack. Tackling this attack requires knowledge of all these types of DoS attacks. In this paper, WSN security requirements are studied. DoS attack on various layers of WSN and most common techniques to avoid these attacks are also analysed.

Keywords: Blackhole attack, DoS attack, Jamming, Physical layer

I. INTRODUCTION

Sensor Networks (WSN) are becoming popular these days due to its wide range of applications ranging from military appliactions to household applications [1]. Due to this wide application variety WSN is gathering a lot of researchers attention and consideration. These applications require some sensitive and critical data that is collected over by sensor nodes in WSN. This sensitive data is very critical to attacks. As a result, security of WSN is a well discussed area[2].

The sensor nodes deployed in a WSN are small, low cost devices with limited energy and transmission bandwidth. These weakness results in various attacks on WSN. One of such attack is Denial or Service (DoS) attack that may be present in various layers of WSN. In this paper, DoS Attack along with its various types has been presented.

II. SECURITY REQUIREMENTS OF WSN

Security in WSN has to be a fundamental requirement[3]. These can safeguard our sensitive data. The main security goal of security services in WSNs is to protect the data, information and resources from intruders, attacks and misbehaviour. The security requirements in WSNs include:

1. Confidentiality: In WSN the information is transmitted starting with one hub then onto the next hub, directing information through numerous hubs, and finally the information or data is passed to the base station. It is essential that any message steered through remote sensor network is private and not open to the unapproved client. Confidentiality ensures that a given message cannot be understood by anyone other than the desired recipients[4].
2. Authentication: An unapproved access by some pernicious hub may drop a few bundles from the system or may bring some false parcels into the system. Such undesirable impacts can be kept away if we intends to recognize the first sensor hubs. Authentication ensures that the

communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted sensor node[5].

3. Integrity: If some change is about in the information parcels by a malignant hub, it abuses the idea of honesty. Integrity intends to guarantee the rightness of the information and ensures that a message sent from one node to another is not modified by any malicious intermediate nodes. Recipient hub ought to get the same information as send by the sender hub[3].
4. Availability: A malignant hub may lead to a malignant base station, which may lead to the whole WSN system to get malignant. Sensor nodes and sink should be dependably be accessible to give administrations of WSN. Availability ensures that the desired network services are available even in the presence of denial-of-service (DoS) attacks[3].
5. Authorization: Authorization ensures that only an authorized sensor node can provide information to a WSN system[3].
6. Freshness: The data of each message should have freshness i.e. data should be recent. No old data should be replayed by malicious nodes[3].
7. Time Synchronization: Most of the Wireless sensor network uses time synchronization to calculate the delay between packets in a pair of two nodes.
8. Access control: Access control prevents unauthorized access to a resource. It prevents unauthorized participation in the network.

III. LAYERED ARCHITECTURE OF WSN

Wireless Security Networks have a layered architecture and they follow the most common OSI model architecture[6]. It contains five layers that are used by sensor nodes and the sink. These are-

1. Application layer- This layer does traffic management and provides software for various applications. These applications translate data in an understandable form or send queries to obtain some information. WSNs are deployed in various applications in many fields such as medical, military, environment, agriculture fields. Therefore this layer contains many protocols like NNTP, SIP, SSI, DNS, FTP, GOPHER, NFS, NTP, SMTP, SMPP, ANMP and TELNET.
2. Transport layer- This layer helps in avoiding congestion, and provides reliability. A lot of protocols are designed to serve this purpose. The major need of this layer is when a system is organized to access other network. It accepts data from above layers and split it into smaller parts and passes them to the network layer. It also ensures the delivery of all these pieces. It contains protocols like TCP, UDP, SCTP, DCCP, SPX.
3. Network layer- The major function of this layer is routing. Network layer faces a lot of challenges depending on the application its working on. However, the major challenges lies in the limited memory, power and buffers. Defining a reliable and redundant paths according to a certain metric that differs from protocol to protocol is the basic idea of the routing protocol in this layer. The routing protocols in his layer are divided into two categories. One is flat routing such as direct diffusion and the other one is hierarchal routing e.g., LEACH. It can also be divided into time driven, event driven and query driven.
4. Data link layer- The data link layer does error detection and correction. It is also accountable for the multiplexing of data frame detection, data streams, error control and medium access.
5. Physical layer- This layer provides an interface, to transmit a stream of bits over a physical medium. It is also responsible for generating carrier frequencies, frequency selection, signal detection, signals modulation and data encryption.

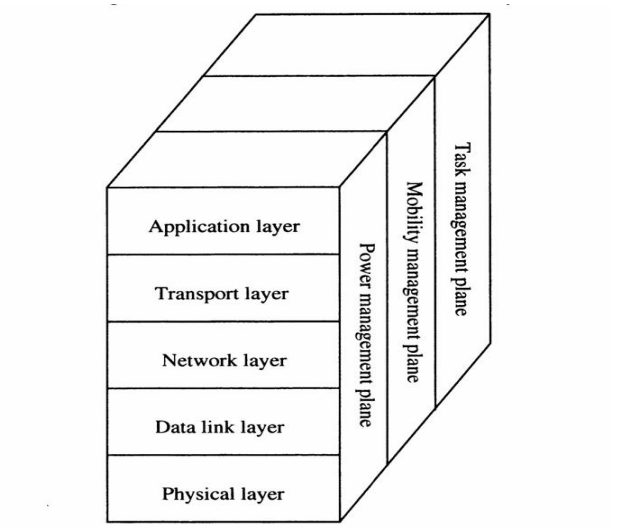

Fig 1 Layered Architecture of WSN

Other than these 5 layers there are three cross layers/planes[6].

1. Power management plane: It is responsible for managing the power level of sensor nodes for processing, sensing and communication.
2. Connection management plane: It is responsible for configuration and reconfiguration of sensor nodes in attempt to establish or maintain network connectivity.
3. Task management plane: It is responsible for distribution of tasks among sensor nodes to prolong network lifetime and improve energy efficiency

IV. DoS ATTACKS ON VARIOUS LAYERS OF WSN

Denial of Service or DoS are a type of active attacks[7], [8], [9]. It happens when there is an unintentional failure of sensor nodes caused by some malicious action. This makes them inaccessible to the user. Extra and unnecessary packets are sent to the victim node, preventing legitimate network users from accessing services and resources.

There are several types of DoS attacks in different layers that might be performed. At physical layer the DoS attacks could be jamming and tampering. In link layer, collision, exhaustion, unfairness can be some usual attacks. At network layer, neglect and greed, homing, misdirection, blackholes are carried out. In transport layer malicious flooding and desynchronization can occur.

These attacks are given in the table-

Layer	Attack	Defense
Transport Layer	Synchronization Flooding De-synchronization	Client puzzles Authentication
Network Layer	Black hole/Sinkhole Interception Homing Selective Forwarding	Authorization and Monitoring
Data link layer	Collision Exhaustion Unfairness Interrogation Denial-of-Sleep	Error-correction code Rate limitation Small frames
Physical layer	Jamming Attack Node Tempering	Spread spectrum Priority messages Region mapping

Table 1 Attacks on different layers in WSN

Physical Layer- Two types of attacks in physical layer are-

1. Jamming attacks[7], [8], [9] aim to interfere in RSN by emitting jamming signals thus, affecting the data transmission and reducing performance. The resources overutilization affects battery life, memory, etc. There are different types of jamming techniques that try to intentionally interfere with the communication between two nodes like Constant jammer that continually emits a radio signal. Deceptive jammer is another type of jammer. It constantly injects regular packets without any gap between transmissions rather than randomly sending bits. A Random jammer instead of continuously sending out a

radio signal, alternates between sleeping and jamming. after jamming for some time, it turns off its radio and enters into sleeping mode. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This model takes energy conservation into consideration. Reactive jammer transmits a radio signal as soon as it senses activity on the channel but, stays quiet when the channel is idle. One advantage of a reactive jammer is that it is harder to detect.

2. Node Tempering[7], [8], [9]- If an attacker gets access to physical layer, it can access all the sensitive information. He may also altered or replaced the node by a malicious node replaces to create a compromised node which the attacker controls.

Data Link Layer: There are 4 attacks that can occur in this layer[7], [8], [9]. These are-

1. Collisions: This attack occurs when two nodes attempt to transmit on the same frequency simultaneously at the same time. When these packets collide, it is obvious that a change will occur in the data. The packet will then become invalid. An attacker can strategically cause these collisions in specific packets.
2. Exhaustion: In this attack the WSN is exhausted due to repeated retransmission of data packets. Intruder targets a nearby nodes and sends a join-request or many acknowledgements to exhaust its neighbouring nodes batteries.
3. Unfairness: It is a weak form of DoS attack and can be performed by attacker in attempt to degrade the network performance instead of completely preventing access to a service. The amount of time is reduced due to use of small frames as it lessens the effect of such attacks. However, this technique often reduces efficiency and is susceptible to further unfairness such as an attacker trying to retransmit quickly instead of randomly delaying.
4. Interrogation: in this attack, the attacker makes use of the interaction between two nodes prior to data transmission. An attacker can exhaust a node's resources by repeatedly sending messages.

Network Layer: Two major types attacks in network layer are-

1. Blackhole attack[7], [8], [9]- Black-hole attacks also called packet drop attacks or sinkhole attacks, are one type of denial-of-service attack that is caused by an external element on a sensor nodes in a network. The adversary re-programs the nodes such that they do not transmit the data packets. These nodes called black hole nodes and the region which holds such nodes is known as the black hole region. As a result of this attack any information that enters in the blackhole region is captured and does not reach the base stations. The network performance parameters are affected due to this attack causing throughput to decrease significantly and increasing end-to-end delay.
2. Selective forwarding: In this attack[8], [9] an intruder drops some of the packets on its way to the sink. The intruder cannot be easily detected. Intruder should be somewhere near the sink; thus, the intruder can malfunction the entire WSN. Sensor nodes use a sequence numbers for each packet.

Transport Layer: There are two types of attacks that occurs in this layer[7], [8]. These are-

1. Synchronization Flooding- When a protocol is required to maintain a state it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. A very common form of DoS attacks involves sending a large number of common packets aimed at a single destination.

The most common packets used are: TCP, ICMP, and UDP. The huge traffic deluge caused by these packets leads the network to no longer be able to distinguish between legitimate and malicious traffic.

2. Desynchronization- In desynchronization an existing connection is disrupted. Attacker repeatedly spoofs messages causing the victim to request retransmission of missed frames. Attacker degrades or prevent a successful data exchange to instead waste energy attempting to recover from errors which never really existed. This will cause a considerable drainage of energy.

V. CONCLUSION AND FUTURE WORK

WSN due to its applicational variety is an emerging technology. It is vulnerable to various types of security attacks. Since there are many types of attacks, the most commonly attack type is Denial of Service (DoS) attack. In this paper, we have presented a brief survey of DoS attacks, and its types at various layers. Some common types of DoS attacks discussed are blackhole attack, desynchronization, exhaustion, flooding etc., WSN security requirements mainly focuses on data confidentiality and integrity.

In the future, it is planned to work on DoS attacks and propose a security mechanism to protect sensor network against these attacks.

VI. REFERENCES

[1]. D. P. Agarwal, 'Embeded systems' Springer 2017

[2]. R. Dubey, V. Jain, R S Thakur, S D Choubey, 'Attacks in WSN' International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March-2012 1 ISSN 2229-5518

[3]. N Alajmi, 'WSN attacks and solutions' International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014

[4]. Abhishek Jain, Kamal Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", to appear in IEEE ICACCT 2012.

[5]. Mayank Saraogi, "Security in Wireless Sensor Networks", University of Tennessee, Knoxville.

[6]. A Abed, A. Alkhatib, G. Singh,' Wireless Sensor Network architecture' International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014

[7]. E. ÜNSAL, Y ÇEBİ, 'Denial of service attacks in WSN'

[8]. D Buch, D. C. Jinwala, 'Denial os service attcaks in WSN' INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 09-11 DECEMBER, 2010

[9]. P Rolla, M Kaur,'Review of prevention technique for DoS attacks in WSN' NTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 07, JULY 2016