DOS Attacks on TCP/IP Layers in WSN

Isha¹, Arun Malik², Gaurav Raj³

¹²³Department of Computer Engg, LPU Jalandhar, India

ABSTRACT

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges on their security to researchers. These networks are likely to be composed of thousands of tiny sensor nodes, which are low-cost devices equipped with limited memory, processing, radio, and in many cases, without access to renewable energy resources. While the set of challenges in sensor networks are diverse, we focus on security of Wireless Sensor Network in this paper. First, we propose some of the security goal for Wireless Sensor Network. To perform any task in WSN, the goal is to ensure the best possible utilization of sensor resources so that the network could be kept functional as long as possible. In contrast to this crucial objective of sensor network management, a Denial of Service (DoS) attack targets to degrade the efficient use of network resources and disrupts the essential services in the network. DoS attack could be considered as one of the major threats against WSN security. Further, various DoS attacks on different layers of OSI are proposed.

Keywords: Wireless sensor networks, Security, Denial of Service (DoS), Availability, OSI model.

1 INTRODUCTION

A wireless sensor network is composed of thousands of small, spatially distributed devices called sensor nodes or motes, with each of them having sensing, communicating and computation capabilities to monitor the real world environment using radio. WSN can be used for many applications such as military implementations in the battlefield, environmental monitoring, in health sectors as well as emergency responses and various surveillances. Due to WSNs’ natures such as low-cost, low power, etc. they have become one part of our daily life and drawn great attentions to those people who are working in this area.

For the proper functioning of WSN, especially in malicious environments, security mechanisms become essential for all kinds of sensor networks. However, the resource constrains in the sensor nodes of a WSN and multi-hop communications in open wireless channel make the security of WSN even more heavy challenge. The nodes deployed in a network are relatively easy to be compromised, which is the case that the nodes are out of the system control and an adversary can easily get full access to those nodes. Hence, all the data could be modified and restored in those targeted nodes, including the cryptographic keys. The common attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the other legitimate sensor nodes. In this paper, the Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to wireless sensor networks. One of focuses of this paper is to give an overview of DoS attack of a WSN based on the Open System Interconnect (OSI) model.

2 SECURITY GOALS FOR SENSOR NETWORKS

A WSN is a different type of network from a typical computer network as it shares some commonalities with them, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes [1]. The following are the important security goals in WSN:

2.1 Data confidentiality

Confidentiality is the way to secure the message from passive attackers as it is communicated over the network. Only the intended receiver can
understand that message. This is the most important issue in network security. In a WSN, the issue of confidentiality should address the following requirements

- A sensor node should not reveal its data to the neighbours. For example, in a sensitive military application where an adversary has injected some malicious nodes into the network, confidentiality will preclude them from gaining access to information regarding other nodes.

- Establishing and maintaining confidentiality is extremely important where the public information like node identities and keys are being distributed to establish a secure communication channel among sensor nodes.

2.2 Data Integrity

The mechanism should ensure that no message can be altered by any entity as it traverses from the sender to the recipient. Data integrity can be lost even if confidentiality measures are in place due to following reasons:

- A malicious node present in the network injects fraudulent data.

- Disordered or uncontrolled conditions in wireless channel cause damage or loss of data.

2.3 Data Availability

This goal ensures that the services of a WSN should be always available even in presence of any internal or external attacks such as a denial of service attack (DoS). Different approaches have been proposed by researchers to achieve this goal. While some mechanisms make use of additional communication among nodes, others propose use of a central access control system to ensure successful delivery of every message to its recipient. However, failure of the base station or cluster leader’s availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

2.4 Authentication

Authentication ensures that message has come from the legitimate user. Attacks in WSN are not only due to alteration of packets, adversary can also inject fabricated packets in the network. So, data authentication verifies the identity of senders. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes will share secret keys to compute the message authentication code (MAC). A number of methods have been developed by the researchers for secret keys, but the energy and computational limitations of sensor nodes makes it impractical to deploy complex cryptographic techniques.

2.5 Data Freshness

Data freshness means that the data is recent, and it ensures that no old messages have been replayed by the adversary. To solve this problem, a nonce or time-specific counter may be added to each packet to check the freshness of the packet.

3 DENIAL OF SERVICE ATTACK IN WSN

Denial of Service attack is an incident that reduces, eliminates, or hinders the normal activities of the network. In a DoS attack a legitimate user is deprived of the services of a resource he would normally expect to have. As a result, it makes the system or service unavailable for the user. Internal DoS situations can occur due to any kind of hardware failure, software bug, resource exhaustion, environmental condition, or any type of complicated interaction of these factors. External DoS situation occurs due to an intentional attempt of an adversary, and it is called as a DoS attack.

The basic types of DoS attacks are:

- Consumption of scarce, limited, or non-renewable resources like bandwidth or processor time

- Destruction or alteration of configuration information between two machines

- Disruption of service to a specific system or person

- Disruption of routing information.

- Disruption of physical components

Among these three types of DoS attacks, the first one is the most significant for wireless sensor networks as the sensors in the network suffer from the lack of enough resources.
4 DOS ATTACKS AT VARIOUS OSI LAYERS

Sensor networks are usually divided into layers, and this layered architecture makes WSNs vulnerable to DoS attacks as they may occur in any layer of a sensor network. Layer wise categorization of DoS attacks was first proposed by Wood and Stankovic [2]. Later, Raymond and Midkiff [3] enhanced the survey with some updated information. In this paper, the denial of service attacks at each layer and their possible countermeasures are given.

4.1 Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [4]. Nodes in WSNs may be deployed in hostile or insecure environments where an attacker has the physical access. Two types of attacks are present at physical layer:

4.1.1 Jamming

In this Denial of Service Attack, the adversary attempts to hinder the operation of the network broadcasting a high-energy signal. Even with less powerful jamming sources, an adversary can potentially disrupt communication in the entire network by distributing the jamming sources. Jamming attacks can further be classified as:

- Constant, which corrupts packets as they are transmitted
- Deceptive, that sends a constant stream of bytes into the network to make it look like legitimate traffic
- Random, which randomly alternates between sleep and jamming to save energy
- Reactive, transmits a jam signal when it senses traffic.

Counter measures for jamming involve variations on spread-spectrum communication such as frequency hopping and code spreading. Frequency-hopping spread spectrum (FHSS) [5] is a method of transmitting signals by rapidly switching a carrier among many frequency channels using a pseudo random sequence known to both transmitter and receiver. Without being able to follow the frequency selection sequence an attacker is unable to jam the frequency being used at a given moment in time. However, as the range of possible frequencies is limited, an attacker may instead jam a wide section of the frequency band. Code spreading is another technique used to defend against jamming attacks and is common in mobile networks. However, this technique requires greater design complexity and energy restricting its use in WSNs. In general, to maintain low cost and low power requirements, sensor devices are limited to single-frequency use and are therefore highly susceptible to jamming attacks.

4.1.2 Tampering

Sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks [6]. The physical attacks may cause irreversible damage to the nodes. The adversary can extract cryptographic keys from the captured node, tamper with its circuitry, modify the program codes or even replace it with a malicious sensor [7].

Counter measures for tempering involves tamper-proofing the node’s physical package which include:

- Self-Destruction (tamper-proofing packages) – whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information.
- Fault Tolerant Protocols – the protocols designed for a WSN should be resilient to this type of attacks.

4.2 Data Link Layer

4.2.1 Collision

A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [8]. When packets collide, they are discarded and need to re-transmit. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions.

Counter measures for collision is the use of error correcting codes.
4.2.2 Exhaustion

A malicious node disrupts the Media Access Control protocol, by continuously requesting or transmitting over the channel. This eventually leads a starvation for other nodes in the network with respect to channel access.

**Counter measures** for exhaustion are:

- Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions.
- Use of time division multiplexing where each node is allotted a time slot in which it can transmit.

4.2.3 Information gathering

In this the attacker makes use of the interaction between two nodes prior to data transmission. For example, wireless LANs (IEEE 802.11) use Request to Send (RTS) and Clear to Send (CTS). An attacker can exhaust a node’s resources by repeatedly sending RTS messages to elicit CTS responses from a targeted neighbour node.

**Counter measures** for information gathering is to put a check against such type of attacks a node can limit itself in accepting connections from same identity or use anti replay protection and strong link-layer authentication.

4.3 Network Layer

4.3.1 Spoofed routing information

The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

**Counter measures** for spoofed routing is to append a MAC (Message Authentication Code) after the message so that the receiver can verify whether the messages have been spoofed or altered. To defend against replayed information, counters or timestamps can be included in the messages.

4.3.2 Selective forwarding

In a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others.

**Counter measures** for selective forwarding attacks are:

- Use multiple paths to send data.
- Detect the malicious node or assume it has failed and seek an alternative route.
- Use implicit acknowledgments, which ensure that packets are forwarded as they were sent.

4.3.3 Sinkhole

In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbours by forging the routing information [9]. The result is that the neighbour nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

**Counter measures** for Sinkhole attack is to make use of Geo-routing protocols as one of the routing protocol groups because they are resistant to sinkhole attacks, as their topology is built using only localized information, and traffic is naturally routed based on the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

4.3.4 Sybile attack

It is an attack where one node presents more than one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks [10]. Newsome et al describe this attack from the perspective of a WSN. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting.

**Counter measures** for Sybil attack is to use identity certificates. During initialization, before
deploying the sensor nodes, unique information is assigned to them by the server. Server then creates a certificate for each node which binds node’s identity with the unique information. To prove its identity node has to present its certificate.

4.4  Transport Layer

Two attacks are possible at transport layer:

4.4.1  Flooding

In this a protocol which is maintaining state information at both the ends during communication, becomes vulnerable to exhaustion of memory resources. This is due to the number of fake requests are made by an attacker, so that legitimate user cannot access the resources.

Counter measures for flooding at transport layer is either give a puzzle to every new node that joins a network, so a node can join network only if it solves the puzzle. This will also put a limit on number of connections that a node can maintain at a time, or use a mechanism to trace back everything but this is difficult in sensor networks due to limitation of resources, sudden unavailability of some nodes due to their failure.

4.4.2  De-synchronisation

In this an adversary repeatedly spoofs messages to end nodes and eventually that nodes will request the retransimion of missed frames. So, an adversary can waste the energy of legitimate end nodes which keep on attempting to recover from errors that actually don’t exist.

Counter measures for this attack is authentication of packets before they are delivered to end nodes whether they belong to legitimate user or not

4.5  Application Layer

4.5.1  Path based DoS

In this a adversary injects replayed packets to flood the end to end communication between two nodes every node in the path towards the base station forwards the packet, but if large number of fake packets are sent all of these will become busy. So, this attack consumes network bandwidth and energy of the nodes [11].

4.5.2  Reprogramming attack

Reprogram mean to again program the nodes in network may be due to version updating, changing the old program or for other network management purpose [12]. If this process of reprogramming is not secure, the attacker can have hold on large portion of network.

Counter measures for attacks at application layer is to choose a best authentication method or anti replay protection

DoS attack at various layers and its possible counter measures are given in table 1 below.

<table>
<thead>
<tr>
<th>LAYERS</th>
<th>ATTACKS</th>
<th>CONTERMEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHYSICAL LAYER</td>
<td>JAMMING</td>
<td>Spread spectrum, priority messages, region mapping</td>
</tr>
<tr>
<td></td>
<td>TAMPERING</td>
<td>Tamper-proofing packages, or use fault tolerant protocols</td>
</tr>
<tr>
<td>DATA LINK LAYER</td>
<td>Collision</td>
<td>Error correcting codes</td>
</tr>
<tr>
<td></td>
<td>Exhaustion</td>
<td>Rate limitation</td>
</tr>
<tr>
<td></td>
<td>Information gathering</td>
<td>use anti replay protection and strong link-layer authentication</td>
</tr>
<tr>
<td>NETWORK LAYER</td>
<td>Spoofed routing information</td>
<td>Authentication, anti-replay</td>
</tr>
<tr>
<td></td>
<td>Selective forwarding</td>
<td>Use multiple paths, acknowledgments</td>
</tr>
<tr>
<td></td>
<td>Sinkhole</td>
<td>Redundancy checking</td>
</tr>
<tr>
<td></td>
<td>Sybil attack</td>
<td>Authentication, monitoring, redundancy</td>
</tr>
<tr>
<td>TRANSPORT LAYER</td>
<td>Flooding</td>
<td>Client puzzles</td>
</tr>
<tr>
<td></td>
<td>De-synchronisation</td>
<td>Authentication</td>
</tr>
<tr>
<td>APPLICATION LAYER</td>
<td>Path based DoS</td>
<td>Authentication and antireplay protection</td>
</tr>
<tr>
<td></td>
<td>Reprogramming attacks</td>
<td></td>
</tr>
</tbody>
</table>
5 CONCLUSION

Security plays a crucial role in the proper functioning of wireless sensor networks. In this paper, we have classified attacks on wireless sensor network at all the layers of TCP/IP. Along with the attacks, countermeasures are also given so that wireless sensor network is not venerable to such kind of attacks as prevention is better than cure. Sensor networks are more vulnerable to DoS attacks at physical layer than all other layers. In all the layers except physical, it is very difficult to identify that attack is intentional or not. At last, DoS attacks are effective at all the layers, so a special attention is required for their detection as well as prevention.

6 REFERENCES