
Purvi N. Jani¹
¹M.E. (I.T.)
¹Parul Institute of Engg & Technology, Vadodara, India

Abstract--- Wireless Sensor Networks are characterized as computational and energy resources & an ad hoc operational environment. Wireless Sensor Networks are used in many applications include the monitoring of sensitive information so security is prime issue. This paper examines the possible potential attacks on sensor network. Owing to the wireless communication’s broadcast nature, wireless sensor networks are vulnerable to denial of service attacks. This paper also provides the qualitative analysis of different types of attacks in DOS.

Keywords: Wireless Sensor Networks, Sensor Security, DOS, Attacks

I. INTRODUCTION
Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. Typical multi-hop wireless sensor network architecture is shown in figure 1. These networks will consist of thousands of self-organizing, low-power, low cost wireless nodes deployed to monitor and affect the environment. WSNs are quickly gaining popularity due to low cost solutions to a variety of real world challenges. Their low cost provides large sensor arrays in a variety of conditions capable of performing both the military and the civilian tasks. WSNs introduce resource constraints due to their lack of data storage and power capacity introduce major obstacles to the implementation of traditional computer security techniques in WSN. The unreliable communication channel and unattended operation makes the security defenses even more harder. There are many researchers who have started to address the challenges of increasing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. In this the WSNs are being examined involving secure and efficient routing. Traditional security issues that many general-purpose sensor network techniques predict that all nodes are cooperative and trustworthy. In real-world wireless sensor networking applications require a fix amount of trust in the application in order to maintain proper network functionality.

Researchers therefore started to focus on modeling a sensor trust model to solve the problems beyond the capability of cryptographic security [1]. Physical attacks to sensors play a very important role in the operation of WSNs. I am presenting a survey on the study of various aspects of WSNs security in this process. Wherever possible, classification of work is also completed. Issues need to be addressed in future research are also identified, which provide a vital information for future researchers.[2]

II. RELATED WORK

A. Security Requirements
A sensor network is a very special type of network. It shares some common functionality with a computer network, but also poses some unique requirements. The goal of security services in WSNs is to protect the information and resources from attackers and their misbehavior. The security requirements in WSNs include:

1) Availability: which ensures that the desired network services are available even in the presence of denial-of-service attacks
2) Authorization: which ensures that only authorized sensors can be involved in providing information to network services
3) Authentication: which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node
4) Confidentiality: which ensures that a given message cannot be understood by anyone other than the desired recipients
5) Integrity: which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
6) Nonrepudiation: which denotes that a node cannot deny sending a message it has previously sent
7) Freshness: Which implies that the data is recent and ensures that no adversary can replay old messages

Moreover, as new sensors are deployed and old sensors fail, forward and backward secrecy should also be considered:

1) Forward secrecy: Sensors should not be able to read any future messages after it leaves the network.
2) Backward secrecy: A joining sensor should not be able to read any previously transmitted message.

The security services in WSNs are usually centered around cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical for use. [3]
B. ATTACKS IN SENSOR NETWORKS

WSNs are vulnerable to various types of attacks. According to the security requirements in WSNs, these attacks can be categorized as [4]:

1) Attacks on secrecy and authentication: Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

2) Attacks on network availability: Attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

3) Stealthy attacks against service integrity: The goal of the attacker is to make the network accept a false data value. The attacker compromises a sensor node and injects a false data value through that sensor node.

C. DENIAL OF SERVICE AND DENIAL OF SERVICE ATTACK

We consider any type of intentional activity that can disrupt, subvert or even destroy the network as a Denial of Service (DoS) attack. In the context of WSN, DoS attacks that target the network resources are one of the most significant: the hardware of sensor nodes is usually very constrained, and attackers can try to overload them. Consider any kind of attempt of an adversary to disrupt, subvert, or destroy the network as a denial of service attack. In practicality, a DoS situation can occur due to any kind of incident that diminishes, eliminates, or hinders the normal activities of the network. Say for example, any kind of hardware failure, software bug, resource exhaustion, environmental condition, or any type of complicated interaction of these factors can create denial of service. It should be noted that the term 'DoS’ indicates that a particular situation in the Denial of Service in Wireless Sensor Networks: Issues and Challenges 3 network and when DoS situation occurs due to an intentional attempt of an adversary, it is called DoS attack. DoS attacks can mainly be categorized into three types:

1) Consumption of scarce, limited, or non-renewable resources

2) Destruction or alteration of configuration information

3) Physical destruction or alteration of network resources

D. PHYSICAL LAYER

The physical layer is responsible for the frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [4]. As with any radio-based medium, there exists the possibility of jamming in WSNs. In addition, nodes in WSNs may be deployed in hostile or insecure environments where an attacker has easy physical access. These two vulnerabilities are explored in this subsection.

Jamming: Jamming is the deliberate interference of the wireless communication channel. In fact, sensor nodes are very vulnerable against this type of physical attack [8]. Jamming is a type of attack which interferes with the radio frequencies that a network’s nodes. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network. Even with lesser-powered jamming sources, such as a small compromised subset of the network’s sensor nodes, an adversary has the potential to disrupt the entire network provided the jamming sources are randomly distributed in the network. Typical defenses against jamming include variations of spread-spectrum communication as frequency hopping and code spreading. In FHSS, 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. As the range of possible frequencies are 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, thus 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 [2].

Tampering: Tampering is another type of physical attack, which targets the actual hardware of the sensor nodes (e.g. sensitive chips, sensor hardware). While it is difficult to know whether any particular DoS situation is caused intentionally or unintentionally, there are some detection methods that help to thwart each type of DoS attack [9].

Another physical layer attack is tampering: Physical access is given to the node so in the network attacker can extract sensitive information like cryptographic keys. The node may also be altered or replaced to create a compromised node which the attacker controls. One defense to this attack involves tamper-proofing the node’s physical package. However, it is usually assumed that the sensor nodes are not tamper-proofed in WSNs due to the additional cost. This indicates that a security scheme must consider the situation in which sensor nodes are compromised [2].

E. LINK LAYER

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access, and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network. Attacks at the link layer include purposely introduced collisions, resource exhaustion, and unfairness. This subsection looks at each of these three link-layer attack categories.

Collisions: A collision occurs when two nodes attempt to transmit on same frequency simultaneously. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid. 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 in certain media access control (MAC) protocols. A typical defense against collisions is the use of error-correcting codes. Most codes work best with low levels of collisions, such as those caused by environmental or probabilistic errors. However, these codes also add additional processing and communication overhead. While it is possible to detect these malicious
collisions, no complete defenses against them are known at this time [2]. Exhaustion: Repeated collisions can also be used by an attacker to cause resource exhaustion. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets. Unless these hopeless retransmissions are discovered or prevented, the energy reserves of the transmitting node and those surrounding it will be quickly depleted. A possible solution is to apply rate limits to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions [2]. A second technique is to use time-division multiplexing (TDMA) where each node is allotted a time slot in which it can transmit [2]. This eliminates the need of arbitration for each frame and can solve the indefinite postponement problem in a back-off algorithm. However, it is still susceptible to collisions.

Unfairness: Unfairness can be considered a weak form of a DOS attack [2]. An attacker may cause unfairness in a network by intermittently using the above link-layer attacks. Instead of preventing access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline. The use of small frames lessens the effect of such attacks by reducing the amount of time an attacker can capture the communication channel. However, this technique often reduces efficiency and is susceptible to further unfairness, for example, when an attacker is trying to retransmit quickly instead of randomly delaying.

F. NETWORK AND ROUTING LAYER

The network and routing layer of sensor networks is usually designed according to the following principles [4]:

1) Power efficiency
2) Sensor networks are mostly data-centric.
3) An ideal sensor network has attribute-based addressing and location awareness.

The attacks in the network and the routing layer include the following.

Spoofed, Altered, or Replayed Routing Information: The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. A countermeasure against spoofing and alteration is to append a message authentication code (MAC) after the message. By adding a MAC to the message, the receivers can verify whether the messages have been spoofed or altered. To defend against replayed information, counters or timestamps can be included in the messages [7].

Selective Forwarding: A significant assumption made in multihop networks is that all nodes in the network will accurately forward received messages. An attacker may create malicious nodes which selectively forward only certain messages and simply drop others. A specific form of this attack is the black hole attack in which a node drops all messages it receives. One defense against selective forwarding attacks is using multiple paths to send data. A second defense is to detect the malicious node or assume it has failed and seek an alternative route. Multi-hop networks like WSNs rely on the assumption that all nodes in the network will faithfully forward the received messages to the base station. In these attacks, a malicious node in the routing path acts as a normal node by forwarding messages, but selectively drops sensitive packets – which is hard to detect by the system. This attack is independent from the Sinkhole/Blackhole attacks, although a malicious node can make use of them to increment its effect in the network. As possible solutions to detect this type of attack, some secure routing algorithms and IDSs using different techniques have been proposed in [10].

Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information. The end result is that surrounding nodes will choose the compromised node as the next 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 will flow through the adversary’s node [2]. In this attack, a malicious node acts as a blackhole to pull in all the traffic in the network. The attacker listens to the route requests and then replies to the target node informing that it has the shortest path to the base station. A victim node is enticed to select it as a forwarder for its packets. Once a malicious node puts itself between the base station and sensor node, it is able to do whatever it wants (drop all packets, change the content, etc) with the packets that pass through it. This type of attack can be very harmful for sensor nodes that are deployed considerably far from the base station [11].

Sybil: The Sybil attack is a case where one node presents more than one identity to the network. Protocols and algorithms which are easily affected include fault-tolerant schemes, distributed storage, and network-topology maintenance. For example, a distributed storage scheme may rely on there being three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while in reality it has not [13].

Wormholes: A wormhole is a low-latency link between two portions of the network over which an attacker replays network messages. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to the sinkhole attack, as an attacking node near the base station can provide a one hop link to that base station via the other attacking node in a distant part of the network [2]. In this attack, an attacker records the packets at one location in the network and tunnels those to another location with the help of a long-range wireless channel or an optical link. This attack can be launched even if the attacker has not compromised any node because the packets are broadcasted and can be overheard by anyone in network. Attackers offer less number of hops and less delay than other normal routing paths, thus sensor nodes are enticed to send data through them. There are...
various types of wormhole attacks. In fact, in a recent work, three types of wormhole attacks namely Energy Depleting Wormhole Attack (EDWA), Indirect Wormhole Attack (IBA), and Targeted Energy Depleting Wormhole Attack (TEDWA). There are also many wormhole detection techniques, which make use of connectivity information or even additional hardware mechanisms such as directional antennas [14].

Hello Flood Attacks: Many protocols which use HELLO packets make the naive assumption that receiving such a packet means the sender is within radio range and is therefore a neighbor. If the attacker falsely broadcasts a superior route to the base station, all of these nodes will attempt transmission to the attacking node, despite many being out of radio range in reality [2]. Many routing protocols need to broadcast HELLO packets in order to discover one-hop neighbors. This attack uses such packets as a weapon to attract sensor nodes. In particular, an attacker with a large radio range and enough processing power can send HELLO packets to a large number of sensor nodes by flooding an entire section of the network. A node which receives such a packet may assume that the attacker is within normal radio range. Hence, sensor nodes can be persuaded that the adversary is their neighbor. Possible solutions to detect this type of attacks could be the use of bidirectional verification of links, secure multipath routing, and use of multiple base stations [15].

Acknowledgment Spoofing: Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. An example of such false information is claiming that a node is alive when in fact it is dead [2].

Misdirection Attack: It is the most popular Denial of Service Attack. This attack can be performed in different ways. A malicious node could deny a valid route to a particular node thereby denying service to the destination. A. Types of Misdirection attack. It can be performed in two ways:

1) Packets forwarded to a node near to the destination: This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay, thus decreasing throughput of network (bit transfer per second).

2) Packets forwarded to a node far away from the destination: This kind of misdirection attack is very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination. Due to the attack the delay becomes infinite and further results in zero throughputs [4].

G. TRANSPORT LAYER

The transport layer is responsible for managing end-to-end connections. Two possible attacks in this layer, flooding and desynchronization, are discussed in this subsection [2].

Flooding: whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding. An attacker may be repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored. One proposed solution to this problem is to require that each connecting client demonstrate its commitment to the connection by solving a puzzle. The idea is that a connecting client will not needlessly waste its resources creating unnecessary connections. Given that an attacker does not likely have infinite resources, it will be impossible for him/her to create new connections fast enough to cause resource starvation on the serving node. While these puzzles do include processing overhead, this technique is more desirable than excessive communication [2].

Desynchronization: Desynchronization refers to the disruption of an existing connection. An attacker may, for example, repeatedly spoof messages to an end host, causing that host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data, thus causing them to instead waste energy by attempting to recover from errors which never really existed [2].

III. CONCLUSION AND FUTURE WORK

In this work, detailed study on different types of attacks is provided. Ignoring DoS vulnerabilities or it’s effects may lead to the unexpectedly easy compromise of network resources as in Adaptive Rate Control’s potential preference for malicious traffic. Without sufficient protection from DoS and other attacks, sensor networks may not be deployable in many areas & may result in loss of sensitive information. Only suitable to limited, controlled environments falling far short of their promise. In future a lot of research can be done on different attacks for better routing, packet forwarding, & secure data transfer.

ACKNOWLEDGMENT

With a sense of gratitude and respect, I would like to heartily thank Assistant Prof. Yask Patel without his support and encouragement this paper could not have been completed.

REFERENCES


