Indian Journal of Science and Technology, *Vol 10(25), DOI: 10.17485/ijst/2017/v10i25/110888, July 2017*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security Issues in Wireless Sensor Networks

Abdullah Alharbi*

Yanbu University College Badr, Yanbu Al Sinaiyah, Yanbu Al Bahr – 46455,
Saudi Arabia; albadrania@rcyci.edu.sa

Abstract

Objective: Wireless sensor networks are growing in popularity and in number of applications. They can be used in many areas such as health care, military, industrial processes, transportation, intelligent buildings, and many other applications. **Methods/Statistical Analysis:** Every WSN consists of very small nodes that act as data generators as well as network relays. Among other components, each node has one or more sensors which are designed and programmed to gather data from a physical phenomenon. Wireless sensor networks are, by nature, distributed systems. This means that every node in the deployment area has the ability to access the information shared in that area. **Findings:** Types of data transmitted through these networks are variants. Based on the type of data, different levels of security requirements are always needed. While looking for low-cost, diminished devices within a network is important, security must be taken in consideration as well. **Applications:** Due to the nature of deployment in Sensor networks being in public and hostile environment in many applications, the fact that these networks lack secure physical infrastructures compared to the traditional networks, and the nature of wireless communication between nodes, wireless sensor networks are highly vulnerable and more likely to be compromised when there is not enough security. This paper discusses the limitations in sensor networks and some other issues in wireless sensor networks, including the different security classes and the different kind of possible attacks.

Keywords: Network Attacks, Security, Wireless Sensor Networks, WSN

1. Introduction

A Wireless Sensor Network (WSN) usually has one or more base stations and a large number of small nodes that are low in cost and power. These nodes consist of sensors as well as microprocessors and radio transceivers. These components not only give them the ability to sense but also the ability to communicate and process data. Within a short distance, these nodes have the ability to communicate wirelessly and work together to complete a certain task. Sensor nodes in many WSN applications are deployed in an ad hoc way. These battery-powered nodes are supposed to operate without attendance for long periods of time and it is usually very challenging to replace them or recharge their batteries, especially when deployed in hostile environments such as battlefields. This makes them unreliable and vulnerable to both physical damage and different security threats.[7]

A sensor network can be looked at as a distributed database. Security of distributed databases requires that only authorized users can access the data (Confidentiality), the data should be real (Integrity), and the data should be always available for authorized users (Availability). In sensor networks case, these requirements are also required to secure the network. Because of their limitations in communication and computing and due to their deployment nature, sensor networks face many security challenges. Also, sensor networks can be deployed in very important applications such as, battlefield, measuring traffic flow, habitat monitoring, buildings, or bridges. Being deployed in applications where they have physical interactions with the environment, people, and other objects, sensor networks are more vulnerable to various security threats. The limitations in sensor networks are node limitations as well as network limitations. Moreover, Sensor networks are more vulnerable to attacks since they are always deployed in unattended environment. Attackers can capture the sensor nodes and have the network accept an evil node as a valid one. Then, attackers can apply variety of attacks when they are within the network.[5]

** Author for correspondence*

2. Limitations in Sensor Networks

There are some limitations in WSNs which can be classified into three types of limitations: node, network, and physical limitations. A typical sensor node has a processor of 4-8 MHz, 128 KB flash, 4KB of ram, and at best 916 MHz of radio frequency.[5] The reduction is size is needed in those nodes to reduce cost and have more applications. With size reduction comes energy reduction which also causes more limitations in storage and processing which then lead to more challenges in design.[12] Another limitation is the nature of sensor nodes being heterogeneous, which cause the impossibility to have one security solution. Moreover, sensor nodes are highly vulnerable to physical sabotage due to their deployment nature.[5] As well as node limitations, sensor networks have all the limitations of mobile ad hoc networks where they rely on insecure wireless media and lack physical infrastructure.[1] Sensor networks are highly vulnerable to capture and vandalism considering the nature of sensor networks deployment being in public and hostile environment in many applications. The security of physical materials increases the node's cost.[1] Techniques used to secure traditional wireless networks are not always easy to be implemented in wireless sensor networks. This is due to the energy restraints along with other limitations in WSNs such as the nature of deployment in which nodes communicate with no pre-existing infrastructure.[10]

3. Security in Sensor Networks

Security goals in sensor networks depend on the need to know what we are going to protect. In sensor networks, four security goals are determined: Confidentiality, Integrity, Authentication, and Availability (CIAA). Confidentiality is the ability to hide messages from unauthorized people, where the message transmitted on a sensor network stays confidential. Integrity is the ability to ensure that the received message is the same as the origin message that has been transmitted on the network, meaning that the message has not been tampered, altered, or modified. Authentication refers to the reliability of the message's origin, which means that the message is really from the node it claims to be from. Availability refers to the ability for a node to use the resources, and the ability for messages to move on the network.[4]

3.1 Security Classes

In computing systems the main assets are hardware, software, and data, while in sensor networks, the goal is to protect the network itself, including the sensor nodes and the communication between those nodes. Figure 1 shows the four threats that can exploit the weakness of security of the network.[1]

Interruption occurs when a link in a sensor network becomes lost or unavailable. Examples of this kind of threats are message corruption, node capture, addition of malicious code, etc. In the case of an interception, the network has been compromised by an enemy, meaning that an attacker has gained unauthorized access to a sensor node or to data on a sensor node. Example: Nodes capture attacks. In a modification threat, an attacker not only accesses the data but also tampers with it. An example of this kind of threat is when an attacker modifies the data packets that have been transmitted through the network causing a denial of service attack such as flooding the network with bogus data. Fabrication happens when an attacker adds false data and compromises the trustworthiness of information.[1]

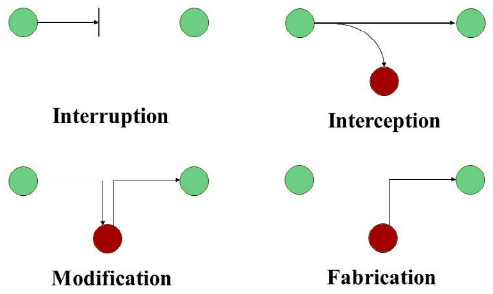

Figure 1. Network security threats.

3.2 Attacks on Sensor Networks

There are various possible security attacks in sensor networks. Some of these attacks are identified as following:[3]

3.2.1 Passive Information Gathering

A trespasser in this type of attacks has a strong receiver with an antenna to intercept the data being transmitted within a sensor network. The acquired data not only allow the intruder to access information on the sensors but also give them the ability to locate these sensors and destroy them.[8] In sensor networks, if information is not encrypted, an enemy with powerful resources may collect it.[11]

3.2.2 Node Subversion

A node's information can be revealed if a node is captured. This information includes cryptographic keys, which then will be disclosed. Disclosure of cryptographic keys cause of the compromising of the entire sensor networks.[4]

3.2.3 False Node

An adversary may inject malicious data through a malicious node. Addition to that, false node would be computationally strong to lure other node to send data to it.[3] It also prevents legitimate data from passing through the network. Destroying the network is possible by this attack, what is worse; however, is the fact that an adversary can be able to control the whole network[11].

3.2.4 Node Malfunction

Having a malfunctioning node among the network nodes will result in inaccurate data. This inaccurate data will affect the integrity of the network especially when that malfunctioning node is a node that collects data, such as a cluster leader.[3]

3.2.5 Node Outage

This happens when a node fails to function normally. When a cluster leader stops functioning, protocols of the sensor network have to be powerful enough to reduce and diminish the effects of node outages by finding alternate route.[1]

3.2.6 Message Corruption

The integrity of a message is compromised when an attacker modifies the contents of the message.[3]

3.2.7 Traffic Analysis

Even though the process of message transferring is encrypted in sensor networks, it still leaves the probability of analysis of communication patterns and sensor activities revealing enough information that an enemy may use to harm the sensor networks.[4]

3.2.8 Routing Loops

Attacks that occurs in the network layer are called routing attacks. Because WSNs are ad hoc routing networks, every node acts as a router and because they are mostly unprotected, they are vulnerable to routing attacks.[11] One of the routing attacks is routing loops attack, which can attack the information exchanged between nodes in sensor networks. When an attacker modifies and replays the routing information, false error messages are created. Routing loops repel the network traffic causing node-to-node latency.[3]

3.2.9 Selective Forwarding

Selective forwarding attacks is a way to affect the network traffic by believing that all the participating nodes in the network are reliable for forward the message. This attack is done when attack malicious nodes drop some messages instead of forwarding them. This process reduces the latency and; as a result, deceives the neighboring nodes that they are on a shorter route. How effect this attack is depends on two factors. First, the location of the malicious node, the closer the malicious node to the base station, the more traffic it attracts. Second, the percentage of messages the malicious node can drop. When the selective forwarder is able to drop more messages and forward less, it keeps its energy level, which keeps it powerful to keep deceiving the neighboring nodes.[3]

3.2.10 Sinkhole Attacks

In sinkhole attacks, adversary attracts the traffic to a compromised node. A sinkhole can be created simply by placing a malicious node where it can attract most of the traffic, or by placing a malicious node where it can deceive other nodes and make those nodes believe that this malicious node is a base station. One of the reasons attackers use sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. This kind of attacks is highly possible because of the nature of sensor networks where all traffic flows from nodes to one base station.[1]

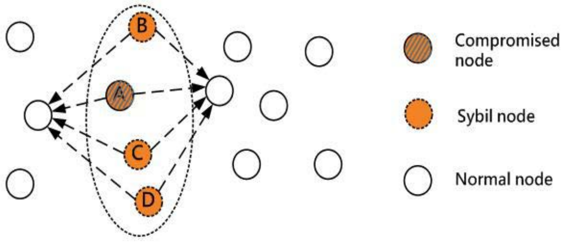

Figure 2. The model of sinkhole attacks.

3.2.11 Sybil Attacks

In Sybil attacks, a node creates multiple illegal identities by fabricating or stealing the identities of legal nodes. This kind of attacks can be used against topology maintenance and routing algorithms. Sybil attacks can reduce the effectiveness of fault tolerant schemes such as, dispersity and distributed storage. Moreover, a Sybil can appear in more than one place simultaneously (geographic routing).[1] The malicious node is capable of presenting a group of different nodes as itself in a WSN. This allows it to act and function as a distinct node and send false information about its position and signal strength. This malicious node can gain control over the whole WSN by this act of disguising[8].

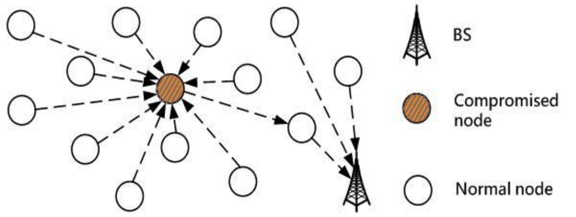

Figure 3. The model of Sybil attacks.

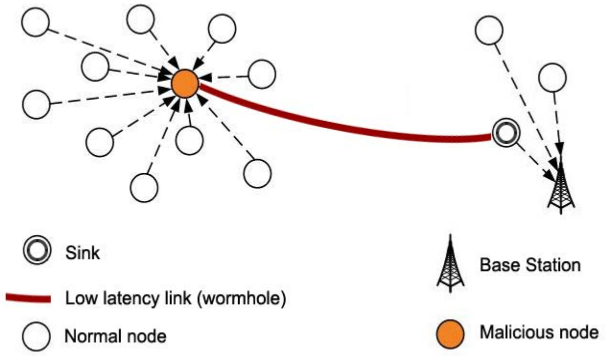

Figure 4. The model of wormhole attacks.

3.2.12 Hello Flood Attacks

In Hello Flood attacks, an attacker broadcast a message with stronger transmission power and pretending that the HELLO message is coming from the base station. The nodes that receive the message will assume that the HELLO message-sending node is the closest node and they will try to send their messages through this node, since it is closest node to the node as they assume. Thus, all nodes will be reply to HELLO floods and waste their energies. On the other hand, the real base station will also broadcast the similar messages but only few nodes will respond to it.[3]

3.2.13 Wormhole Attacks

In this kind of attacks, an adversary being positioned closer to the base station can totally disrupt the traffic by tunneling messages over a low latency link. In this case, an adversary deceives the nodes by making them believe that they are closer to the base station. This process also creates a sinkhole because the adversary on the other side of the sinkhole provides a better route to the base station.[3]

3.2.14 DoS Attacks

A denial of service attack occurs at physical level and causes battery exhaustion, radio jamming, interfering with network protocol, etc.[4] It makes a node unreachable by simultaneously sending large number of packets to it. This will cause a loss of genuine requests. This attack is designed to shutdown a victim node in the network. A defense mechanism is needed to detect and drop fake requests in order to prevent flooding attacks.[9]

4. Layering based Security Approach

The attacks and countermeasures in a layering model in sensor network are described in Table 1.

Table 1. Layering approach in sensor network attacks and countermeasures

Layer	Attack types	Countermeasures
Application	Subversion and Malicious Nodes	Malicious node detection and isolation
Network	Wormholes, Sinkholes, Sybil, Routing loops	key Management and secure routing
Data link	Jamming	encryption
Physical	DoS and node capture	Adaptive antennas and spread spectrum

4.1 Application Layer

It is important to ensure the reliability of data at the application layer since data is collected and managed at this layer. A flexible aggregation scheme has been presented by Wagner.[6] That scheme can be applied to a cluster-based network where a cluster leader works as an aggregator in sensor networks. This technique however, can be applied if the collecting node is in the range with all the source nodes and there is no intervening aggregator between source nodes and aggregator. Cluster leaders, to prove the validity of the aggregation, use cryptographic techniques.[1]

4.2 Network Layer

Messages routing from node to node, node to cluster leader, cluster leader to cluster leaders, cluster leaders to the base station and vice versa is the responsibility of the network layer. There are two types of routing protocols in sensor networks: ID-based protocols and data centric protocols. In ID-base protocols, packets are routed to the destination based on their IDs. In data centric protocols, packets have some attributes that specify the type of data that is provided.[3]

4.3 Data Link Layer

The error detection and correction, and encoding of data are done at data link layer. Data link layer is vulnerable to jamming and DoS attacks. A link layer encryption that depends on a key management scheme has been provided. However, an attacker with better energy efficiency may still do an attack. Some protocols such as, LMAC have good anti-jamming properties.[3]

4.4 Physical Layer

The physical layer focuses on the transmission media between nodes, strength of the signal, the data rate, and frequency types. FHSS frequency is used in sensor networks as it has a spread spectrum.[3]

5. Conclusion

Wireless Sensor networking has been one of the significant topics in computer networking as WSNs can be applied to many different applications. They have been increasingly used in military, health, commercial, and many other areas of applications. Since WSNs are different in deployment circumstances than many other traditional networks, security is concerned more. The nature of deployment, the limitation of nodes and the nature of wireless communication make difficult security challenges for sensor networks. In the lack of enough security, sensor networks are highly vulnerable to a various number of attacks. These attacks can occur in any network layer. Some techniques to protect WSNs have already been proposed. However, there is no single solution to protect all networks against all type of possible attacks. This paper tends to outline the limitation of sensor networks and some issues in wireless sensor networks including the different security classes and the different kind of possible attacks. It also aims to classify those attacks and briefly present some of the countermeasures that should be applied to protect WSNs against different type of attacks from physical layer to application layer.

6. References

1. Yang C, Tarng W, Hsieh K, Chen M. A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography. IEEE SMC – eNewsletter; 2010.
2. Fleeger CP. Security in computing. 3rd edition. Prentice-Hall Inc; NJ; 2003.
3. Undercoffer J, Avancha S, Joshi A, Pinkston J. Security for sensor networks. CADIP Research Symposium; 2002.
4. Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and Countermeasures. Elsevier's Ad Hoc Networks Journal. Special Issue on Sensor Network Applications and Protocols. 2003; 1(2-3):293–315.
5. Zhang H, Olariu S, Cao J, Johnson D. Mobile ad-hoc sensor networks. Third International Conference. Springer; Berlin, Germany; 2007. Crossref
6. Wagner D. Resilient aggregation in sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM Press; 2004. p. 78–87. Crossref
7. Zheng J, Jamalipour A. Wireless Sensor Networks: A Networking Perspective. John Wiley & Sons Publisher; Hoboken, NJ; 2009.
8. Hu C. International Journal of Future Generation Communication and Networking. 2016; 9(7).
9. Arunmozhi S, Venkataramani Y. International Journal of Computer Applications. 2011; 3(3).
10. Nunoo MH, Boateng K, Gadze J. International Journal of Network Security and its Applications. 2015; 109(11).
11. Padmavathi G, Shanmugapriya D. Journal of Computer Science and Information Security. 2009; 4(1&2).
12. Chelli K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. Proceedings of the World Congress on Engineering; London, UK; 2015 Jul 1-3.