Analysis of Physical Attacks in WSNs

Kunal Kalra, Prakhar Purwar, Ranjit Kumar

1 Student, Information Technology, Galgotias College of Engineering and Technology, Greater Noida, U.P., India, kunal17kalra@gmail.com
2 Student, Information Technology, Galgotias College of Engineering and Technology, Greater Noida, U.P., India, prakharpurwar42@gmail.com
3 Assistant Professor, Information Technology, Galgotias College of Engineering and Technology, Greater Noida, U.P., India, ranj.kumar@galgotiacollege.edu

ABSTRACT

Wireless Sensor Networks (WSNs) are an emerging technology which are used in different applications, and thus become an interesting field of research. That is why security is a crucial issue and service in WSNs because wireless sensor nodes are typically deployed in unattended environments, leaving them open to possible hostile network attacks. As wireless sensor nodes have limited computing power, communication capabilities and data storage, there is a need to design user authentication protocols to efficiently operate in a resource constrained environment. The need for reliable security mechanisms for WSNs has increased to quite an extent. WSNs are required and beneficial in many fields, such as health monitoring, emergencies, environmental control, industries, military, and these networks are prone to malicious users' and physical attacks due to radio range of the network, untrusted transmissions, unattended nature and can get access easily. Security is a fundamental requirement for these networks. In this paper, we mostly focus on physical attacks and issues in WSNs and try to identify the capabilities and purpose of the attackers. Furthermore, we discuss well-known approaches of security detection mechanisms against physical attacks as well as simulate DOS attack. Our aim is to benefit researchers and manufacturers to find new research direction in WSN security.

Keywords:
WSNs, Compromised node, Attacks, Security, data confidentiality.

1. INTRODUCTION

The Research and advancement of Hardware Engineering approaches powerful software methods that would create a collection of several sensors which is called a wireless sensor network [1] [14] [27]. WSNs are created in terms of Groups with spatially discrete and dedicated sensors for observing and saving the bodily situations which would be able to manage the composed data at a mid-point. Sensors are quite active and small in size and also have medium processing and computational power [31] [19] [35], However, they are cheaper than most traditional sensors. WSNs measure the conditions of environment such as wind, temperature, sound, pollution levels and so on. WSNs research has now emerged in different domains, such as hardware and system designing, I-T systems, Networks, forensic Applications which are detailed in figure no.2, as a organization of data, different model of programming, security challenges and different factors [2] [25, 7]. WSNs are highly useful and essential in different application development systems such as in military and their surveillance [33] [28], utilize the purpose of natural disasters [5], tracking data of the patients [10] [20], and for exploration of hazardous environments for sensing purposes [30]. WSNs are connected to each other within a very short range of links, where they utilize a special type of infrastructure by forwarding the collected data to authorized entities over the base-station (BS) [2] [22, 24] [25]. According to recent research, sensors can observe temperature, pressure within the specific area, moisture, movement of objects, and other special properties [18].
In the case of intelligent nodes of sensors, which are very low power devices and are placed in one or more than one sensors, in the regard of a processor, memory, an acuter, a radio, etc. Generally speaking, WSN have no proper infrastructure because it is connected with thousands of sensors of nodes which work together for monitoring purposes and getting data about a particular environment. WSNs can categorized into two types of families. First one is structured and second is unstructured. In regard to structured, WSN nodes are deployed in the preplanned manner, they are very beneficial during the deployment with subordinate networks repair as well as managing cost. In unstructured, WSNs environment they are densely collected sensor nodes. Unstructured WSNs environment have more chances of failure of maintained and lack of connectivity between the participant nodes.

After the deployment phase, the network would be able to be left unattended to deliver, observe and report generation functions. In terms of security it’s a very important factor during the infrastructure phase of WSNs, nowadays many applications suffer because of unavailability of security within the networks and many researchers try to provide different kinds of authenticated schemes to WSNs. Security factor in WSNs has to be completed and a very basic requirement. These kinds of requirements are not enough to provide authenticity of sensitive information, but it could be explored if not bounded by resources in every sensor node, which can then maintain the sensor networks in the shape of life. Adversary attacks, susceptibilities, and chances that are two factored, which are able to provide the adversary chances to affect the WSNs. Sensor nodes would be able to expose the risk by capturing the active adversary. Therefore, it is possible to damage sensor node connectivity and lose of communication channel. Many key issues occur during the design of a proper channel for WSN environment, so it is necessary to support the WSN environments against these problems. WSNs need proper security in terms of authentication, integrity, and confidentiality for protection against the adversaries. Moreover, the characteristic boundaries in the communications channel and for calculation, deployment phase of WSNs creates a more susceptible in different attack issues. In the case of deployment nodes, system occupies large area and attackers have better chances to attacks on confidential data between the sensor nodes, figure no.1 shows the development of WSNs network. Adversaries are sharper as they can use special kinds of formula to track the sensing data between the sensor nodes. The adversary has some special targets such as, to detect the secret data, to hack the collected data within a special network and DoS and assured to potential threats in regard of privacy and security within the wireless sensor networks. During the capturing of the nodes by an adversary, result may occur in between the active and passive, as well as physical attacks can happen by an intellectual adversary. Moreover, during the initialization or creating of an attack by an adversary, it will still able to collect secret information by snooping to message interchanging, even by a single attack device or under a network with the support of a number of attacks devices occur in the development of the network. In such condition, if the message were not encrypted the attacker would be able to capture data about network working and there state. Although application of hardware and software development might point out this kind of security problems, development of new technologies in the recent century they face many security challenge issues in WSNs application during the hardware and software level approach.
Fig. 2 Application of WSNs

Structure of this paper follows as 1. We discuss the background study on WSNs. 2. Discuss about the architecture of WSNs and sensor components. 3. Classification of various attacks 4. Security solutions against WSNs 5. Conclusion of paper.

2. ARCHITECTURE OF WIRELESS SENSOR NODE

A sensor node depends on four basic components which are sensing component, processing component, radio transceiver component and power source component. These four components are detailed under figure.3. Sensor nodes also depend upon additional components. Sensing component depend on two sub-components called sensor and analogue, which direct to the digital converters. Sensors are able to create analogue signals, which can then be converted to digital signals, and then feed in the processing component. Generally speaking, processing components are connected with the storage components and they can organize the functions that create the node of sensors as a collaborator to the sensor nodes for assigning the sensing responsibilities. The duty of the transceiver component is to join nodes within the network environments. We analyze power component in a very important part of the WSNs environment because it would be able to be supported by the solar cell.

4. SECURITY ISSUES IN WSN

4.1 Availability: Availability in WSNs ensures that the network services are feasible even in the presence of denial of service attacks. The security protocols perform the availability of data in the network which fixate low energy and storage with reuse of code in the network [4]. In availability, a few approaches are chosen to adjust the code to reuse as much code as possible and make use of extra communication to achieve the same goal.

4.2 Self Organization: The WSN has many nodes for operations and are deployed in different locations and fields. In self-organization, the nodes are flexible to be self-organizing and self-healing in the network. The WSN is an Ad hoc network and all nodes are independent in network and without any infrastructure. This intrinsic characteristic brings a great challenge for WSN security.

4.3 Time Synchronization: The WSN applications rely on some type of synchronization. The nodes have two states in the network - on and sleep and radio may be turned on or in sleep mode for a period of time. The sensor calculates the end-to-end delay of the packet [5].
4.4 Secure Localization: WSNs use location based information for identifying the position of nodes in a network. Few attacks are related with the sensor location by investigation for attacks. The attackers search the header of packet and data for this purpose. The secure localization is an important factor during implementation of security in the network.

4.5 Confidentiality: The confidentiality is restricted data access to authorized personnel only. The data should not leak across adjacent sensor networks. When one node sends the highly sensitive data to its destination, it passes from many nodes in the network. For the provision of security of data, network protocols use encryption techniques with a secret key, the message is sent in encrypted form through the channel. Information should be encrypted to protect from traffic analysis attacks [6].

4.6 Authenticity: Authenticity is quite imperative in WSNs, because an adversary can easily inject messages. The receiver node needs to guarantee that any data used in any decision making process originates from a trusted source only. The data authenticity is to ensure the identities of communication nodes. It is required in various administrative tasks [4].

4.7 Flexibility: The WSN scenarios are different and dependent on different environmental conditions, hazards and missions because they are always changing [5]. The changing mission goals frequently need sensors to be reduced from sensor nodes in the network.

CHALLENGES IN SECURITY OF WIRELESS SENSOR NETWORKS

WSNs present a variety of unique challenges [2] which need be considered for the security concerns which may be present in sensor network applications.

Resource constraints
Security mechanisms, especially traditional mechanisms with high overheads are not suitable for resource-constrained WSNs.

Lack of central control
It is often not feasible to have a central point of control in sensor networks, for example, due to their large scale network size, network dynamics and resource constraints.

Remote location
The first line of any defense against the attacks is to provide only controlled physical access to a sensor node.

Error-prone communication
There are a variety of factor including routing failures, channel errors, and collisions that cause lost or corrupted packets.

6. SECURITY ATTACKS IN SENSOR NETWORKS

![Taxonomy of Attacks Diagram]

Fig 3: Taxonomy of attacks [5]
7. PHYSICAL ATTACKS

A WSN is designed in layers form and these layers protect the sensors from various attacks as shown in Figure 2. The sensor networks are power constrained with limited computational power, which causes the network to get exposed to the attackers. The physical attacks are based on different strategies and effects. Here we discuss physical attacks in detail.

7.1 Signal Jamming Attack: The radio or signal jamming attack transmits the radio signals emitted by the receiving antenna at the same transmitter. The attack techniques are constant, random, deceptive and reactive jamming in this attack. These attacks affect on radio interference and exhaust resources. The attack is based on modification of class and the availability and integrity is a main threat for WSN in this attack. It belongs to external and active threat model. The detection of this attack is possible by detecting background noise and misbehavior detection techniques. Another detection method is statistical information and channel utility degradation than the threshold. The WSN has various defensive approaches to protect from these attacks such as access restrictions encryption approach, reporting attacks to base station, buffering and through mapping protocols.

7.2 Tampering and Capturing Attack: Another physical attack is device-tampering attack on WSN in which the attacker captures the sensor node physically and replaces the node with malicious node. The effects of this attack are stopping the services or disturbing the network and may gain control over the captured node [33]. This attack belongs to intersection, fabrication and modification security class. The confidentiality, availability and integrity are attack threats in this class. The detection of this kind of attack is possible through node disconnection, node destruction and notice misbehavior of the node in network. The defense mechanism is optimizing and using crypto-processors and applying standard precautions in WSN. Furthermore, the physical protection of node and malicious node detection techniques are to protect the network from these attacks.

7.3 Path-Based DOS Attack: This attack is another type of physical attack and is mainly, a combination of jamming attacks. In this attack, the attacker sends a large number of packets to the BS (base station). The effects of this physical attack are to disturb the network availability and exhaust node batteries. This attack belongs to modification and fabrication class and authenticity and availability are the main threats for WSN network. Initially, the nodes along the path will rapidly become exhausted and after that the second set of nodes downstream from nodes along the main path which are then unable to communicate with base station. This is because of tree-structured topology and at last the path based DOS attacks can disable a much wider region than a single path.

7.4 Node Outage Attack: The node outage attack stops the functionality of WSN components and the attack applies physically or logically in the network. The effects of this attack are to stop the node services such as reading, gathering and launching of the functions. The attack belongs to modification model and authenticity and availability are main threats for this attack in the network.
7.5 Eavesdropping Attack: This attack is detection of contents of a communication by trying overhear attempts to data and apply through the WSN transmission medium. The eavesdropping is also called confidentiality attack and leads to wormhole or blackhole attacks in the network [34]. The effects of this attack are extracting sensitive information from the network and deleting the privacy and confidentiality of the nodes. This attack belongs to intersection model and confidentiality is the main threat in network for this attack and is based on external and passive threat models.

7.6 DOS (Denial of Services) Attack: The DOS attack is a general attack and applies on various layers such as data link layer, network layer, transport layer etc. In this attack, the attacker can inject fake broadcast packets to force sensor node to perform expensive signature verifications. The DOS attack affects these layers and their functions in the network. The DOS attack belongs to intersection and interruption security class and integrity, authenticity and availability are main threats for this attack [35].

8. Simulation of Denial of Service Attack

WSNs are concerned with a number of security issues. The constraint on the resources makes WSN more vulnerable to DoS attack because it more focuses on the energy protocols. [32] DoS attack prevents the system or the user to be termed as legitimate. It is mainly done by overloading the destination system with large number of requests. Due to this attack, efficiency and performance of the WSN would be greatly reduced. This particular type of attack in unfriendly environments and situations can be even more harmful. There are many kinds of DOS attacks. Amongst the various kinds of DOS Attacks, SYN flood is the most common kind of attack. SYN flood uses TCP three way handshake mechanism for communication amongst the nodes.

DoS Attack involves saturation of the performance of the target node with lots of unwanted communication requests which will generate fake traffic. [57] These kinds of attacks overload the entire server. Here, DOS attack is implemented by the use of UDP protocol and CBR application. Once the buffer is full, the target node can be seen dropping the packets which come from the malicious node as well as the source node. Figure 4.5 shows the simulation of the DoS attack. Node 42 is the source here and node 50 is the destination. The packets from the source are sent to the destination via the target node 54. After sometime, node 44 acts as a malicious node and starts sending large number of packets to the target node. Since the target node’s buffer size is limited, it can’t handle all the packets and therefore, at time 23 sec it will drop the packets coming from the malicious node 44 as well as the source node 42. This will lead to loss of data and will degrade the service of the entire network.

9. RESULTS

As a part for the proposed system, a graph is generated to monitor the network performance. It calculates the throughput of the WSN. Throughput indicates overall number of bytes received in the WSN. The Throughput can be affected by various number of factors. It plays a very important role in analyzing the network performance. The trace file which is
generated is passed as an input in order to generate a result graph. With the help of the graph, one can easily understand the simulation results of the WSN. The X Axis represents the time, and the Y Axis represents the throughput rate. When the transmission starts there is a huge amount of traffic in the system, so the throughput is high. Later it drops at one point when the attack occurs. Figure 5.4 shows the graph.

Fig 8: Graph for throughput

10. CONCLUSION
Provision of security in WSN is a vital requirement for a sufficient and stable network in communication technologies. It is a complex feature to deploy especially in wireless sensor network because due to the nature of network. Most physical security attacks disturb the WSN security dimensions like confidentiality, integrity, availability and authenticity. In this short paper, the security issues and physical attacks have been analyzed. We tried to focus more specific knowledge for the researchers. The approach followed is to first classify then compare the WSN’s physical attacks, their properties such as their effects and strategies and finally their associated defense and detection techniques against these kinds of attacks to handle them comprehensively and independently.

We also simulated DoS attack in NS2. On simulation, the performance and the efficiency of the network was analyzed. The behavior and the energy parameters can also be examined from the simulation. A mechanism for ensuring secure data transfer and preventing the attacks in a WSN is necessary and can be proposed by more thorough research. The parameters which determine the network performance can also be calculated from the simulation.

REFERENCES


802.11 wireless mesh networks, 2; 3 (2008).


