SINKHOLE ATTACK: A SECURITY ISSUE IN WIRELESS SENSOR NETWORKS

Tejinderdeep Singh Kalsi*

Anand Nayyar**

Harpreet Kaur Arora*

ABSTRACT

Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article we discuss security issues in WSNs.

In a wireless sensor network, multiple nodes would send sensor readings to a base station for further processing. It is well-known that such a many-to-one communication is highly vulnerable to the sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and then performs selective forwarding or alters the data passing through it. A sinkhole attack forms a serious threat to sensor networks, particularly considering that such networks are often deployed in open areas and of weak computation and battery power. In this paper, we discuss SINKHOLE ATTACK as a major problem in wireless sensor networks. Later on an efficient algorithm will be designed to prevent the network from these type of attacks.

Keywords— WSN(Wireless Sensor Networks), BS(Base Station), SH(Sinkhole attacks), ADC(Analog to Digital Converter).

* CSE Department, SBBSIET, Padhiana (Jalandhar), M-Tech Scholar, Assistant Professor(CSE), SBBSIET, Padhiana, Jalandhar.

** Assistant Professor, Computer Applications and IT, KCLM&IT, Jalandhar.

INTRODUCTION

A WSN is usually composed of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS).

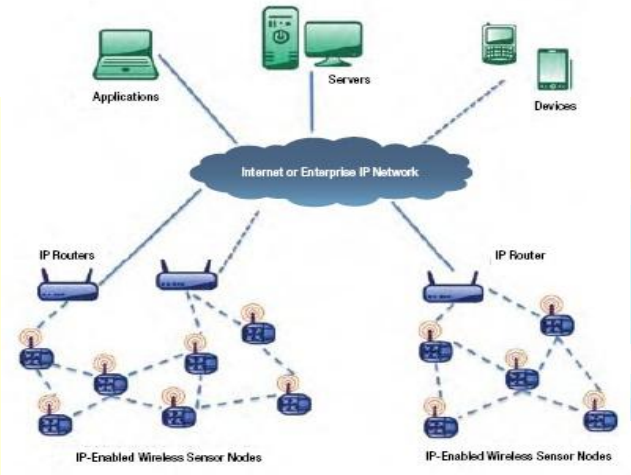

Figure 1. Wireless Sensor Networks

A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit. It may also have additional application- dependent components such as a location finding system, power generator, and mobilizer as shown in Figure 2. Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. A mobilizer needed to move the sensor node, depending on the application.

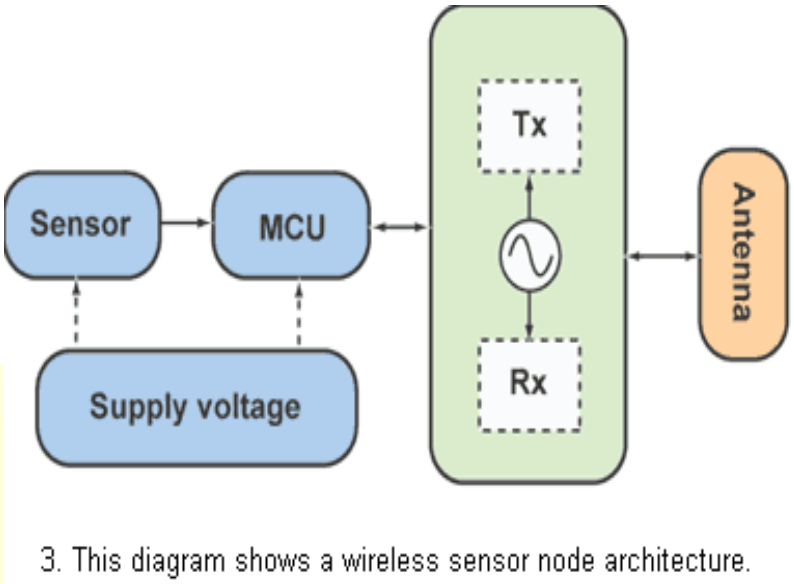

Figure 2. Components of Sensor Nodes

The protocol stack used in sensor nodes contains physical, data link, network, transport, and application layers defined as follows :

• Physical layer: responsible for frequency selection, carrier frequency generation, signal deflection, modulation, and data encryption

• Data link layer: responsible for the multiplexing of data streams, data frame detection, medium access, and error control; as well as ensuring reliable point-to-point and point-to-multipoint connections

• Network layer: responsible for specifying the assignment of addresses and how packets are forwarded

• Transport layer: responsible for specifying how the reliable transport of packets will take place

• Application layer: responsible for specifying how the data are requested and provided for both individual sensor nodes and interactions with the end user.[1]

II. REQUIREMENTS IN THE SECURITY

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

• Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks

• Authorization, which ensures that only authorized sensors can be involved in providing information to network services

• 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

• Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients

• Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes

• Nonrepudiation, which denotes that a node cannot deny sending a message it has previously sent

• 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, we suggest that forward and backward secrecy should also be considered:

• Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.

• Backward secrecy: a joining sensor should not be able to read any previously transmitted message.[2]

III TYPICAL SECURITY TREATS AND DEFENSE TECHNIQUES IN WIRELESS SENSOR NETWORKS

Communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of treats. A large-scale sensor network consists of huge number of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities. These small sensor nodes are pervious to several key types of treats.

For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Treats on sensor networks can be classified into attacks on physical, link (MAC), network, transportation, and application layers.

Treats can also be classified based on the capability of the possible attacker, such as sensor-level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger computation and communication capabilities than a sensor node. Treats can also be classified into outside and inside treats. An outside attacker has no access to most cryptographic materials in sensor networks, while an inside attacker may have partial key materials and the trust of other sensor nodes. Inside attacks are much harder to detect and defend against. Typical treats and adequate defense techniques in WSNs are summarized as in Table I.[6]

Table I. Typical treats in WSNs

Treat	Layer	Defense techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route infor. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

IV PROBLEM STATEMENT: SIKHOLE ATTACKS

A sinkhole attack prevents the base station from obtaining complete and correct sensing data, and thus forms a serious threat to higher-layer applications. It is particularly severe for wireless sensor networks given the ulnerability of wireless links, and that the sensors are often deployed in open areas and of weak computation and battery power. Although some secure or geographic based routing protocols resist to the sinkhole attacks in certain level, many current routing protocols in sensor networks are susceptible to the sinkhole attack.[6][7].

We consider a sensor network that consists of a base station (BS) and a collection of geographically distributed sensor nodes, each denoted by a unique identifier *IDv*. The sensor nodes continuously collect and send the sensed application data to the base station by forwarding packets hop-by-hop. As mentioned earlier, this commonly used many-to-one communication pattern is vulnerable to sinkhole attacks. In a sinkhole attack, an intruder usually attracts network traffic by advertising itself as having the shortest path to the base station. For example,an intruder using a wireless-enabled laptop will have much higher computation and communication power than a normal sensor node, and it could have a high-quality single-hop link to the base station (BS). It can then advertise imitated routing messages about the high quality route, thus spoofing the surrounding nodes to create a sinkhole (SH). A sinkhole can also be performed using a wormhole, which creates a metaphorical sinkhole with the intruder being at the center. An example, where an intruder creates a sinkhole by tunneling messages received in one part of the network and replays them in a different part using a wormhole. We assume the sensor nodes are either *good* or *malicious*. The center of a sinkhole attack is a malicious node compromised by the intruder. Note that, even if there is only one compromised node providing a high quality route to the base station, it can affect many surrounding sensors. Furthermore, this intruder may also cooperate with some other malicious nodes in the network to interfere detection algorithms. In an extreme case, all the malicious nodes are colluding with the intruder. They may collaboratively cheat the base station by claiming a good node as the intruder (the victim, SH'), and thus hide the real one.

V PROPOSED SOLUTION

The solution proposed for SINKHOLE attacks in WSN is done in three steps. Wireless Sensor Network is an open network as it has wireless nature. The security feature becomes less when we are working in a Wireless Sensor Networks. To avoid this problem, we will first find out the technique to detect and then we decide whether we want to remove or correct the Intruder Node. Then we define an algorithm to detail about the technique and in the last step we compare our results with our Base Protocol. The focus of our work is to effectively identify the real intruder in the sinkhole attack in presence of colluding nodes. We assume that the base station is physically protected or has tamper-robust hardware. Hence, it acts as a central trusted authority in our algorithm design. The base station also has a rough understanding on the location of nodes, which could be available after the node deployment stage or can be obtained by various localization mechanisms.

VI CONCLUSION AND FUTURE WORK

In this paper, we discuss the most important SINKHOLE ATTACK in WSN. An Important security issue for WSN or any other network and also a major problem because it drops the whole data of node or the network. As the Intruder , in wsn, directly attacks the source node causing whole data to be lost. Because by attacking our route, as in other attacks, we may prevent our data in whole or some of the data but if we miss our source we will be unable to prevent the data as the intruder node drops all the packets.

Future work is to detect the SINKHOLE attack in the network by providing a technique, and an efficient algorithm will be implemented to detect and correct this attack and the results will be compared with the previous generated algorithms.

REFERENCES

1) A Survey of Security analysis in WSN by young wang in CSE journals in 2006.

2) Wireless Sensor Network Technology, Protocols and Applications by Kazem Sohraby in 2007.

3) S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

4) Common security issues in WSN and WMN by Tahir Naeem in 2009.

5) Secure routing in wireless sensor networks: attacks and countermeasures by Chris Karlof David Wagner

6) On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks Edith C. H. Ngai,1 Jiangchuan Liu,2 and Michael R. Lyu1

7) Security Issues in Wireless Sensor Networks Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz

8) En.wikipedia.com