ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)

Volume 1, Issue 11, February 2015

Evaluation on Safety Issues in Wireless Sensor Networks

Dr. Raman Chadha
Professor, Computer Science & Engg. Deptt.
Chandigarh Group of Colleges,
Jhanjeri, Mohali.
dr.ramanchdha@gmail.com

Mr. Ajay Kumar Prasad
B.Tech -III year Student,
Chandigarh Group of Colleges,
Jhanjeri, Mohali.
ajayprasad886@gmail.com

ABSTRACT

Wireless Sensor Network (WSN) is a rising technology that shows vast growth for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in abundance in future. The key features of Wireless sensor networks are low power, low-memory, low-energy and having bulky scaled nodes. The objective of this paper is to overview the various security attacks in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks.

Keywords: wireless sensor network, security, attack, threats.

I. INTRODUCTION

Wireless Sensor Network(WSN) are a most challenging and emerging technology for the research due to their low processing sensor network is a group of self- organized, low priced sensor nodes and creates network in spontaneous manner. The WSN combines sensing, computation and communication in a single small device, called Sensor Node. It mainly contains battery, radio, microcontroller and power devices. The sensors in a node provides the facility to get the data like temperature, pressure, light, motion, sound etc and capable of doing data processing. The main goal of the applications is achieved by the cooperation of all sensor nodes in Security networks .There are many sensor network applications like security monitoring, environmental data collection, medical science, military, tracking etc. Security becomes extremely important factor when sensor networks are randomly deployed in a hostile environment. Even through wireless sensor network is an advanced technology of network, it is extremely different from traditional wireless networks. This is, due to the unique characteristics of sensor nodes in WSN. So existing security mechanisms of traditional wireless networks are not directly applied in WSN. Sensor networks are closely interacting with physical environment. So sensor nodes are also deployed in all areas even physical accessible attacks and broadcasting sensed data in network. These reasons give a scope to new security mechanism rather than applying existing traditional security mechanisms in WSN. The major challenge is to deploy the above encryption techniques or their counterparts in a sensor network which is characterized with constrained memory, power supply and processing capability [1].

II. SECURITY GOAL FOR SENSOR NETWORKS

A sensor network is a special type of Ad hoc network. So it shares some common property as computer network. There are usually several security requirements to protect a network. These requirements should be considered during design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. The security requirements, of a wireless sensor network can be classified as follows:

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following: A sensor network should not leak sensor readings to its neighbors'. Especially in a military application, the data stored in the sensor node may be highly sensitive. In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

B. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when

- A malicious node present in the network injects false data

- Unstable conditions due to wireless channel cause damage or loss of data.

C. Data Authentication

Authentication ensures the reliability of the message by identifying its origin. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision- making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

III. ATTACKS IN WIRELESS NETWORKS

A. Denial of service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic[2].

B. Sybil attack

Sybil attack is a network threat introduced by one or more malicious nodes to declare numerous illegal identifies to confuse or even collapse the network applications. A new detection mechanism, called CRSD, is proposed for static wireless sensor networks, which takes use of the received signal strength (RSS) to infer the distance between two identities and further determines the positions relation of the interesting identities by use of the RSS information from multiple neighbor nodes, e.g., via node cooperation. A Sybil attack is detected when two or more different identities have almost the same position. The analysis and simulation results show that, first, Sybil attack deteriorates the system performance significantly and second, CRSD can detect such attack in most cases, thus protecting the overall performance effectively[3].The concept of Sybil (or multiple-identity) attacks was first proposed by Douceur in P2P networks, and it is defined as a single node has multiple identities to disrupt the accordance between entities and physical devices in the networks. A method was proposed using the trusted certification center to verify the physical identity for preventing multiple-identity attacks. The multiple-identity attacks usually use a single malicious node to confuse neighbor nodes, causing chaos among them, and finally the entire network is interfered and thus cannot function properly [4].

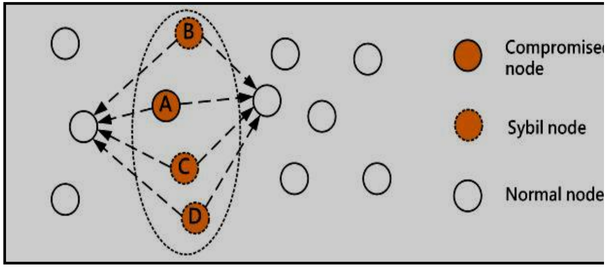

Figure 1[4] The model of Sybil attacks

C. Attacks on Information in transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission[2].

D. Blackhole / Sinkhole Attack

The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to announce itself as having a accurate route to a destination node, even though the route is counterfeit, with the intention of intercepting packets[5] In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations[2].Figure2 shows the conceptual view of a blackhole/sinkhole attack.

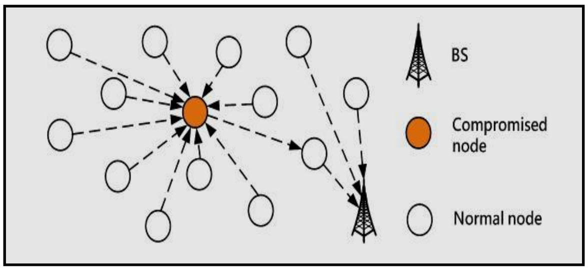

Figure2[4] conceptual view of a blackhole/sinkhole

E. Wormhole Attack

A typical wormhole attack requires two or more attackers - malicious nodes - who have better communication resources than regular sensor nodes. The attacker creates a low-latency link (i.e. high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes adopt these tunnels into their communication paths, rendering their data under the scrutiny of the adversaries. Once the tunnel is established, the attacker collect data packets on one end of the tunnel, send them using the tunnel (wired or wireless link) and replays them at the other end. Wormhole attacks may result in serious damages in WSNs by interrupting or altering the information flow towards the base station. In addition, if the attackers do not modify or fabricate data packets, cryptographic solutions alone cannot detect wormhole attacks[6]. A typical wormhole attack is shown in Figure3

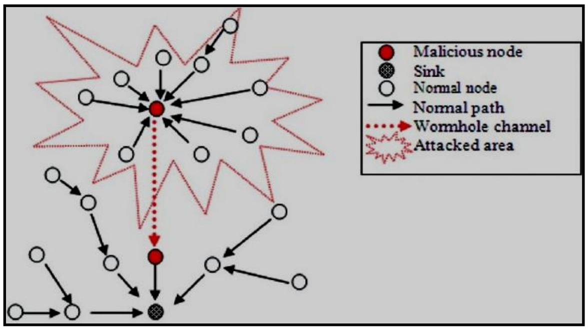

Figure3[6] conceptual view of a wormhole

F. Hello Flood Attack

Hello Flood Attack is introduced in this attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attack[2]. A typical hello flood attack is shown in Figure4.

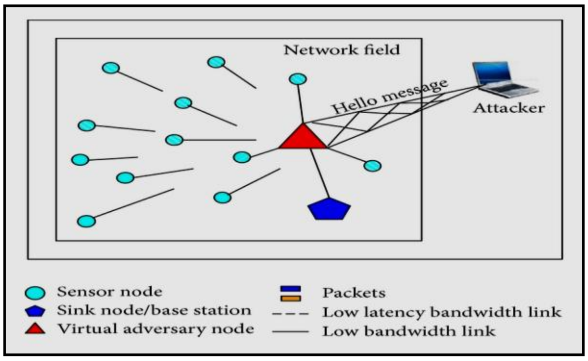

Figure4[7] conceptual view of a wormhole

G. Replay Attack

The attackers intercept encrypted packets with signatures and resend them without making any changes, so the receivers consider them as original packets. Using outdated information and the authentication of legitimate identity, the attackers can obtain secret data or useful information. To prevent such attacks, a time stamp or a sequence number can be added to check if the packet has been resent or not [4] A typical hello flood attack is shown in Figure5

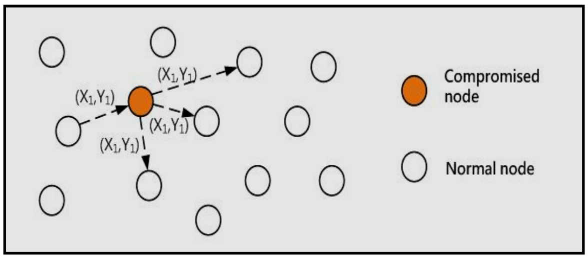

Figure5[4] The model of replay attacks

H. Selective Forwarding

After receiving a packet, the attackers selectively forward or not to forward the packet, or just send the packet containing the routing information to prevent it from reaching the destination. In that case, the packet needs to be re-transmitted and the network traffic and power consumption will increase, and thus the lifetime of the entire network is reduced[4].

IV. SECURITY THREATS AND ISSUES IN WIRELESS SENSOR NETWORKS

Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eaves dropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. These issues are well-enumerated in some past researches , and also a number of security schemes are already been proposed to fight against them. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. While ad hoc networks are self organizing, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the

centralized entity is absent ; the wireless sensor networks could have a command node or a base station (centralized entity, sometimes termed as sink).The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Nevertheless, the major challenge is induced by the constraint of resources of the tiny sensors. In many cases, sensors are expected to be deployed arbitrarily in the enemy territory (especially in military reconnaissance scenario) or over dangerous or hazardous areas. Therefore, even if the base station (sink) resides in the friendly or safe area, the sensor nodes need to be protected from being compromised [2].

V. CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks and also gives general overview of various security threats.

REFERENCE

[1]. Vinayak gupta, Brijesh kumar singh, parmeshwar lal bhanwariya "An Introduction to security issues in wireless sensor networks" Journalofenvironmentalscience,computer scienceandengineeringand technology(JECET) ;November 2013;vol.2 No.4,pp.1276-1285.

[2]. Al-Sakib Khan Pathan, Hyung-Woo Lee ,Choong Seon Hong "Security in wireless sensor networks:issues and challenges". The International conference on advanced computing and technologies (ICACT); 2006; february 20-22; pp.1043-1048.

[3]. Shaohe lv,xiaodong wang, xin zhav, xingming zhou, "Dtecting the Sybil attack cooperatively in wireless sensor network".computational intelligence and security,2008CIS '08'International conference vol.1;13-17 dec 2008;pp.442-446.

[4].Cheng-Lung Yang, Wernhuar Tarng, Kuen-Rong Hsieh, Mingteh Chen "A security mechanism for clustered wireless sensor network based on elliptic curve cryptography".Intelligent internet systems IEEE dec 2010 .

[5] Amol A bhosle, Tushar P.thosar, Snehal mehatre "Black hole and wormhole attack in routing protocol AODV in MANET". International journal of computer science , engineering and applications(IJCSEA) vol.2 no.1 feb. 2012; pp: 45-54.

[6] Majid megh dadi, Suat ozdemir , Inan guler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks" IETE technical review vol.28 , 17th march 2011
Pp: 89-102.

[7] Figure 9 (d) International journal of distributed sensor networks(IJDSN) ,2013; www.hindawi.com.