ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Techno Research Publishers, Bhopal, India.**
www.computerscijournal.org

ISSN: 0974-6471
April 2015,
Vol. 8, No. (1):
Pgs. 59-64

Comprehensive Review on Wireless Sensor Networks

RUPAM SHARMA and NIDHI TRIPATHI

Gwalior Institute of Technical Studies, Gwalior, India.

(Received: March 16, 2015; Accepted: April 20, 2015)

ABSTRACT

Wireless Sensor Networks (WSNs) consists of low power, low-cost smart devices which have limited computing resources. A lot of real world applications have been already deployed and many of them will be based on wireless sensor networks. These applications include geographical monitoring, medical care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring, and surveillance systems. In this paper, we present a snapshot of the wireless sensor network architecture, security requirements and obstacles of sensor security.

Key words: Wireless Sensor Networks; Basic Architecture; Security Requirements; Attacks on WSNs**.**

INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technology in the past decades. It has received tremendous attention from all over the world [1]. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computational capabilities. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task. They are finding their usages in habitat monitoring, manufacturing and logistics, environmental observation and forecast systems, military applications, health, home and office applications and a variety of intelligent and smart systems.

Such a sensor network is typically composed of hundreds, and sometimes thousands of nodes. These nodes are capable of receiving, processing and transmitting information, as based on the assigned tasks. Information flowing through WSN may be susceptible to eaves dropping, retransmit previous packets, injection of redundant or causeless bits in packets and many other threats of diverse nature. To ensure that the data being received and transmitted across these networks is secure and protected, information security plays a vital role. Therefore the article comprises elementary knowledge on Wireless sensor networks (WSNs).

WSN Architecture

In this section, we are presenting here basic architecture of WSN and it consists of four network components as shown in figure 1 namely;

Field devices, Gateway, Network manager and Security manager [2].

Field devices

Field device is also known as Sensor motes and the devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.

Gateway or Access points

A Gateway enables communication between Host application and field devices. Therefore it is called as Access points.

Network manager

A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

Security manager

The Security Manager is responsible for the generation, storage, and management of keys.

Security Requirements in WSN

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks [3]. Here we are included common requirements on the basis of its applications.

Data Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality means keeping information secret from unauthorized parties. The confidentiality relates to the following:

a) 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.

b) 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.

c) Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. Data integrity ensures the receiver that the received data is not altered in transit by an adversary. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

Data Authentication

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 (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. 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 secret key to compute the message authentication code (MAC) of all communicated data.

Data Freshness

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives. Assuming nodes devote only a small fraction of their RAM for this neighbor table, an adversary replaying broadcast messages from many different senders can fill up the table. At this point, the recipient has one of two options: ignore any messages from senders not in its neighbor table, or purge entries from the table. Neither is acceptable; the first creates a DoS attack and the second permits replay attacks. In the authors contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets.

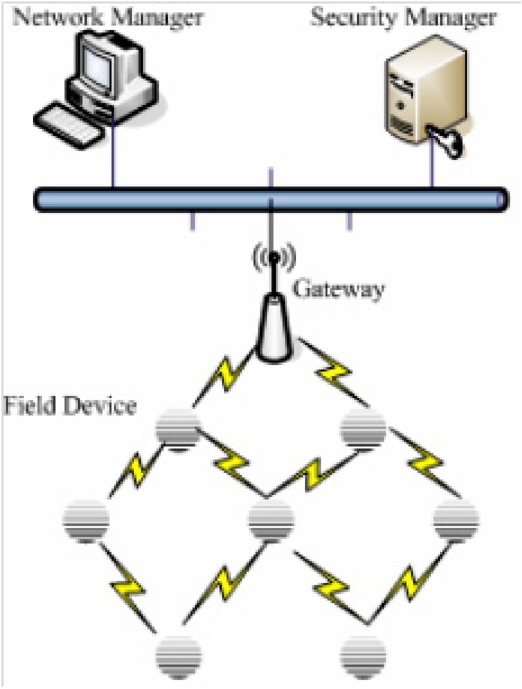

Fig. 1: Basic Architecture of Wireless Sensor Network

Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

a) Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.

b) Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.

c) A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals. This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

Obstacles of Sensor Security

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack [4]. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [3].

Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor. The major parameters are:

Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. With such a limitation, the software built for the sensor must also be quite small.

Power Limitation

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network.

Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol,

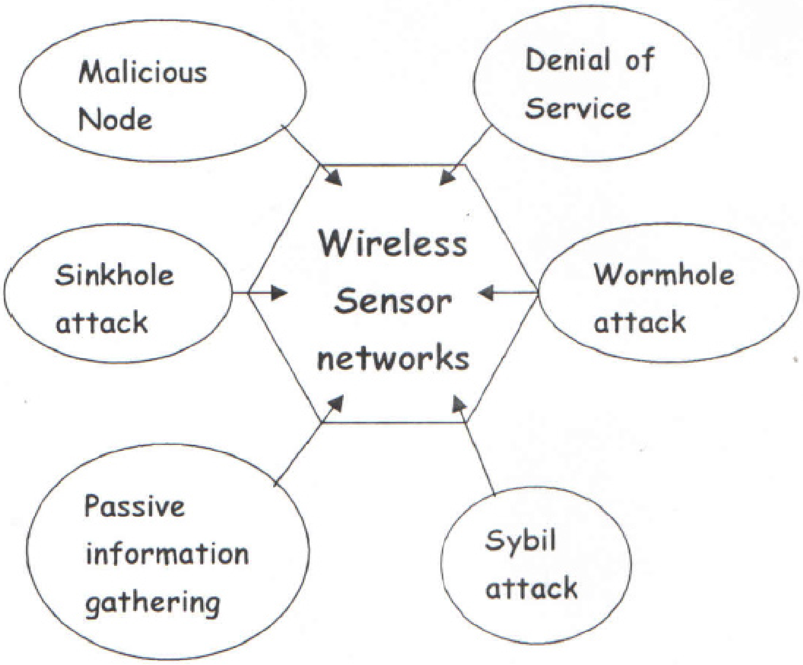

Fig. 2: Security attacks on wireless sensor networks

which in turn depends on communication. The major parameters are:

Unreliable Transfer

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets.

Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem. More details about the effect of wireless communication can be found.

Latency

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

Unattended Operations

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes:

Exposure to Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network [3].

Managed Remotely

Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

No Central Management Point

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

Attacks on WSN

Wireless sensor networks are power constraint networks, having limited computational and energy resources. This makes them vulnerable enough to be attacked by any adversary deploying more resources than any individual node or base station, which may not be a tedious task for the attacker. As described earlier, a typical sensor network may be composed of potentially hundreds of nodes which may use broadcast or multicast transmission. This mode of transmission results in a large volume wireless network with many potential receivers of the transmitted information. This makes a number of attacks such as packet alteration or new packet insertion, capturing of node, reply attacks, denial of service and traffic analysis possible to be performed on any sensor network [5]. Figure 2 is showing major attacks of WSN.

WSN can be cooperatively attacked by colluding in which the adversary makes use of illegitimate nodes with the same capabilities as of network nodes. Deployed malicious nodes can work together to take control of any network node, which can be used further to make damages to the network or to amplify the scope of the attack. The opponent may have highly capable communication links available to carry out any malicious activity, thus making the countermeasure an expensive task. This is a limitation to the security of WSN as we constantly need inexpensive and small devices as nodes in sensor networks.

Deployment of many nodes of WSN in open and harsh environment poses them another major threat. This compromises their physical security, and if the nodes are not temper-resistant, they can be mishandled and tempered with. Attacks on the physical security of the nodes can cause the node to give away the data stored on it, which may enable the attacker to gain access to critical information such as source code, key and other data which may be crucial for security protocol of the entire wireless network. Making these nodes temper resistant may be able to reduce the effects of side-channel attacks and to enhance the physical security of the network devices, but this may not be the feasible solution as the cost per node increases dramatically if we consider such defenses.

WSN are continuously being used in many critical and sensitive applications. WSN are popular because of their ability to incorporate in numerous applications in diverse fields. Health care, security, logistics and military applications are some of the areas of deployment of these wireless networks. It is evident that if the capabilities or functionalities of the sensor network are reduced or endangered, it may cause huge losses in terms of money, resources and may even result in human injuries or fatalities.

CONCLUSION

Wireless Sensor Networks, are self organizing, self healing networks of small “nodes” have huge potential across industrial, military and many other sectors. This article serves as a text for researchers especially the beginners, and enables them to get an overview of this ever increasing area of research, wireless sensor networks. The article gives a brief yet extensive insight into intriguing world of the sensors with elementary idea.

REFERENCES

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. A survey on sensor networks. *IEEE Communications Magazine*, **40**(8):102–114 (2002).
2. Karl, H., Willig, A. Protocols and Architectures for Wireless Sensor Networks, ISBN 0-470-09511-3 ; 1 – 526 (2006).
3. Murugaboopathi, G., Geta, V., Sujathabai, V., Rathish babu, T.K.S., Hariharasitaraman, S. An Analysis of Threat’s in Wireless Sensor Networks, *IJARCSSE*, **2** (10) (2012).
4. Kumar, P., Cho, S., Lee, D.S., Lee, Y.D., Lee, H. J. TriSec: A secure data framework for wireless sensors networks using authenticated encryption. *Int. J. Marit. Inf. Commun. Sci* 129-135 (2010).
5. David R., Scott, R., Midkiff, F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing*, **7**(1): 74-81 (2008).