International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Wireless Sensor Networks : Security Issues and Challenges

Manvee Bansal[1], Prabhjot Kaur[1], Raghbir Kaur[1], C. K. Raina[2]
[1]Department of Computer Science, Adesh Institute of Technology, Gharuan, Chandigarh, Kharar, Punjab, India
[2]HOD of Computer Science Department, Adesh Institute of Technology, Chandigarh, Kharar, Punjab, India

ABSTRACT

Wireless Sensor Networks (WSNs) are formed by deploying as large number of sensor nodes in an area for the surveillance of generally remote locations. A typical sensor node is made up of different components to perform the task of sensing, processing and transmitting data. WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment. The basic requirement of every application is to use the secured network. Providing security to the sensor network is a very challenging issue along with saving its energy. Many security threats may affect the functioning of these networks. WSNs must be secured to keep an attacker from hindering the delivery of sensor information and from forging sensor information as these networks are build for remote surveillance and unauthorized changes in the sensed data may lead to wrong information to the decision makers. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks.

Keywords :- WSN, Sensor, Security, Attack, Challenge.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSNs usually measure environmental conditions like temperature, sound, pressure, pollution levels, humidity,wind speed and direction, etc. and plays a great role in controlling the environment. The challenges of security in WSN are totally different from traditional network security due to inherent resource and computing constraints. Sensor nodes are often deployed in large accessible areas that present the added risk of physical attack. Sensor networks also poses new security problems as they interact closely with their physical environments and with people. Most of the early proposed network techniques in the past assumed that all nodes are cooperative and trustworthy. However, this is not the case for many sensor network applications today, that require a certain amount of trust in the application. This is required in order to maintain proper network functionality. Consequently, the existing security mechanisms are inadequate resulting in new research directions and new ideas for properly addressing sensor network security. The security issues in wireless sensor network is due to the struggle of how much resources can be expended for security in proportion to the sensor application. The current security perspective for WSNs is on a per-attack basis, which creates an inflexible model resulting in poor efficiency and scalability. Creating a security framework offering high flexibility, good scalability and a redundancy-free security layer for the WSN protocol stack and is based on a resource perspective when deciding security solutions, where solutions are designed to secure each resource in the WSN environment, rather than defend against attacks.

II. WIRELESS SENSOR NETWORK SECURITY ISSUES

In this section of the paper we discuss various issues concern with the security of WSNs including limitations, unreliability, etc.

A. Sensor networks: The limitations:-

A distributed sensor network (usually heterogeneous) consists of hundreds to thousands of low-cost and lowpower small sensors that are interconnected through a communication network. The sensors are embedded devices that are networked via wireless media, usually integrated with a physical environment, and are capable of acquiring and processing the signals along with communicating and performing simple computational tasks. Common functions of WSNs are broadcasting, multicasting, routing, forwarding, and route maintenance. The vast applications of sensor networks highlight a vision in which a large number of tiny sensor nodes will be embedded in almost every aspect of human everyday life. However, the widespread deployment of sensor nodes and their overall success is directly related to their security strength. Though WSNs are capable of collecting large amount of information, recognizing significant events and responding appropriately, the need for security is obvious in WSNs.

1) Limited memory and storage

The memory of tiny sensor nodes usually ranges from 2 KB to 256 KB while the storage ranges from 32 KB to 2 GB. Table 1 provides the commonly available sensor nodes with memory and storage. Such hardware constraints of sensor nodes necessitate extremely efficient security algorithms in terms of computational complexity, bandwidth, and memory. The limitation of memory and storage makes it very difficult to implement highly efficient security mechanisms requiring more memory.

2) Limited Power

Energy (power) is the biggest constraint in wireless sensor capabilities. It is one of the main reason that nodes are subject to failures because of depletion of batteries, or more general, it is due to environmental changes. Sensor nodes need to operate autonomously for prolonged periods of time after deployment and it is not possible to easily replace or recharge the battery. Therefore, the energy consumption must be minimized for long life; this necessitates both the power efficiency of the hardware along with the efficiency of security and other routing protocols.

B. Unreliability of Communication

One of the major threats to sensor security is the very nature of the wireless communication medium, which is inherently insecure. The wireless medium is open and accessible to anyone unlike wired networks, where a device has to be physically connected to the medium. Due to this any transmission can easily be intercepted, altered, or replayed by an adversary. Intruder can easily intercept valid packets and inject malicious ones due to open access nature of wireless communication medium. Such weakness can be easily exploited by an intruder having a strong transmitter, and can easily produce interference (like jamming).

C. Operation Unattended

The hostile environment in another challenging factor is which sensor nodes function. Nodes may be left unattended for long periods of time depending on the application which exposes them to physical attacks. Sensor nodes face the possibility of destruction or capture and compromise by attackers. Nodes are compromised when an attacker gains control of a node after deployment in the network. A compromised node may be physically damaged or forced to non-functional, even sensor nodes characteristics/mechanisms may be altered to send out data readings of intruders choice. After gaining control, the attacker can alter the node in order to listen to information in the network and input malicious data or perform a variety of attacks. Intruder may also disassemble the node in order to extract information vital to the network's security including routing tables, data, and cryptographic keys.

III. WSNs SECURITY REQUIREMENTS

Sensor networks are a type of distributed networks and share some commonalities with a typical computer network, at the same time pose unique requirements and constraints. Therefore, security goals for WSN encompass both the typical network requirements and the special unique requirements suited for WSNs. The security requirement of WSN must include attributes such as confidentiality, integrity, data freshness, availability, and authentication.

A. Confidentiality of Data

Data confidentiality is the ability to conceal network traffic from an attacker so that any communication via the sensor network remains secret and is the most important issue concern with network security. In many applications (like key distribution) nodes communicate secret and highly sensitive data. The approach commonly used for keeping sensitive data secret is to encrypt it with a secret key that only intended receivers possess, therefore achieving confidentiality.

B. Authentication & Integrity of Data

False messages can be easily inject in a sensor network by an attacker, therefore the receiver needs to insure that the data to be used in any decision- making process is valid. Data integrity and authentication is therefore necessary to enable sensor nodes for detecting modified, injected, or replayed packets. Not only authentication of safety-critical applications is required, it is still needed for rest of applications otherwise the user of the sensor network may get the wrong information of the sensed world thus making decisions inappropriate. Symmetric or asymmetric mechanisms are used for achieving data authentication is in case sending and receiving nodes share secret keys. It is extremely challenging to ensure authentication due to the wireless and unattended nature of sensor networks that may cause data loss or damage.

C. Availability of Data

Availability is concern with the ability of a sensor node to use the resources and whether the sensor network is available for the communication of messages. A sensor network has to be robust against various security attacks, and impact should be minimized of a succeeded attack. However, it is extremely difficult to ensuring network availability due to limited ability of individual sensor nodes to detect between threats and failures.

IV. Basic Security Schemes in Wireless Sensor Networks

Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known.

A. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks.

1. Symmetric Cryptography in WSNs

The idea of the symmetric cryptography is to load secret information in the sensor nodes before their deployment in the network. This secret information may be the secret key itself or auxiliary information that helps the sensor nodes to derive the real secret key. With this secret key, nodes can securely communicate. The main disadvantage of this solution is that compromising one node (access to the preloaded key) might lead to compromise the entire network. To overcome this limitation, several researchers propose schemes that establish pairwise keys rather than a unique global key.

2. Asymmetric Cryptography in WSNs

The public key cryptography or asymmetric cryptography came up with a radical change of paradigms. According to Stallings public key algorithms are based on mathematical functions, instead of permutation and substitution. Besides the single most important thing is that the public key cryptography is asymmetric, involving the use of two different keys, in contrast to the conventional symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution and authentication. The main distinguishing feature of asymmetric encryption is that it allows the establishment of a secure communication between individuals, without the requirement of the previous share a single cryptographic key.

B. Steganography

While cryptography aims at hiding the content of a message, steganography aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.). The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources of the sensors is difficult and an open research issue.

C. Physical Layer Secure Access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used with a little expense of memory, processing and energy resources. Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and for employing this both the sender and receiver should maintain a synchronized clock. A scheme as proposed in could also be utilized which introduces secure physical layer access employing the singular vectors with the channel synthesized modulation.

V. CONCLUSION

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. In the paper we tried to discuss various issues concern with the security of WSNs along with WSNs requirements and research challenges. In the future work, various attacks on WSNs will be studied along the various countermeasures proposed in the literature to tackle with these attacks. Novel techniques will be proposed in the future for countermeasure to various attacks in order to make WSNs more secure and reliable fosr their extensions in other fields.

VI. WEB REFERENCES

[1]. https://en.wikipedia.org/wiki/Wireless_sensor_network

[2]. http://ieeexplore.ieee.org/document/7578876/

[3]. https://www.researchgate.net/publication/4239084_Security_in_wireless_sensor_networks_issues_and_challenges

[4]. https://bioinfopublication.org/files/articles/1_1_2_IJN.pdf

[5]. http://www.iaeng.org/publication/WCE2015/WCE2015_pp519-524.pdf