International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 09, September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A Comprehensive Study on Wireless Sensor Networks

Madhu K P

Assistant Professor, Department of Computer Science and Engineering, Government Engineering College Idukki, Kerala, India - 685603

ABSTRACT

Wireless Sensor Network (WSN), is a major communication technology that has wide applications in domains like military, disaster management, transportation, agriculture, health, home and industry. Most of these applications usually have a hostile environment. The WSN is designed to serve these requirements in an effective manner. Sensors are a major component of WSN. They share wireless communication channels, adopt multi-hop routing, have untrusted transmission mediums, deployed in hostile and unattended environments and utilize limited resources. WSNs are prone to both active and passive type of attacks. This paper deals with overview of WSNs and various security challenges on WSNs.

Keywords: Wireless Sensor Networks, security

1. INTRODUCTION

Wireless Sensor Networks (WSN) [1] is a cheap solution to many real time applications. It is attributed by the developments in sensor design, wireless communication technologies, embedded systems and energy efficient communication protocols. These networks are deployed in various applications such as environmental monitoring, health observing, habitat watching, disaster detection and management, industrial quality control and protection, transportation, law and order enforcement, agriculture, smart buildings and traffic monitoring [2] [3]. Most of these applications which deploy WSN are critical in security and privacy. Hence, an apt security scheme in WSN is acute due to its characteristics viz. sharing of communication channels, multi-hop communication, untrusted transmissions, deployment in hostile environments, and limited resource availability [4]. The WSN is vulnerable to various security attacks. An attacker can attack on any layer of the protocol stack of WSN. The attacks are grouped as active/passive attack, External/Internal attacks, Mote-class/Laptop-class attacks and attacks on Secrecy, Availability, and Stealthy [2]. These attacks may reduce the performance of WSN and the life of a sensor node. Most of the security mechanisms available for the traditional networks will not suite for WSN because of the constraints of sensor nodes such as limited energy, memory, computing and communication capabilities and their deployment in restricted environments.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The paper is organized as follows. Section 2 gives a brief overview of WSN. Section 3 discusses about the need for security, security goals and the challenges faced in providing security in WSN.

2. OVERVIEW OF WSN

A. Architecture of WSN

WSNs are a distinct type of ad-hoc networks, comprising a large number of heterogeneous sensor nodes and designed to operate in hostile and conditions to sense environmental data such as temperature, humidity, pressure, light, sound etc. The sensor nodes sense the data, process it and transmit it to a sink node through wireless links. The architecture of WSN [1] is shown in Fig. 1.

The major components of a WSN are:

- Sensor Nodes
- Sink
- Task Manager Node

The sensor network comprises different types of sensors deployed to constitute a sensor field. Each sensor node has the capability to collect data and send it to the sink/gateway node through a transmitter. Data are transmitted to the task manager node by the sink node either through wired or wireless channel. In most of the applications the sink may communicate with the task manager/end-user via Wi-Fi, Bluetooth, WiMAX or Serial communication through Ethernet cable [1].

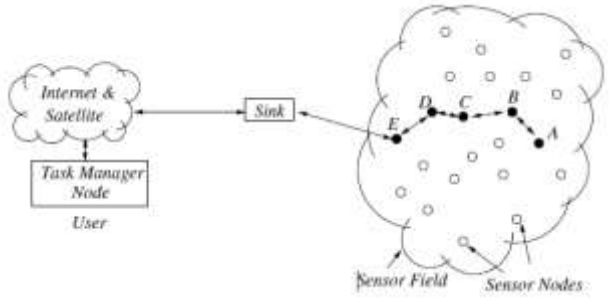

Fig.1: Architecture of WSN [1]

A sensor node (or a mote) is a hardware circuit which can contain multiple sensors to read or detect environmental changes. A sensor node contains a microcontroller, transceiver, external/ internal memory and a battery. The sensor nodes store sensed data in memory, process it with the help of microcontroller and transmits this information with the help of transceivers. The structure of a sensor node is shown in Fig. 2. Sensors are hardware devices usually small in size and battery powered that measure change in a physical conditions. Most sensors creates an analog signal which is changed over to a digital signal by an Analog to Digital Converter (ADC) and sent it to a microcontroller for further processing.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

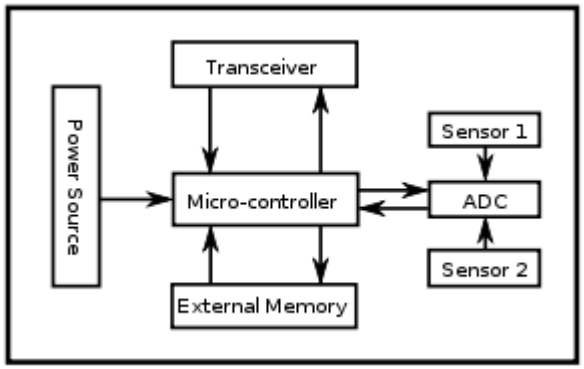

Fig.2: Structure of a Sensor Node

Various sensors are available in the market like Temperature sensor, Humidity sensor, Pressure sensor, Ultrasonic sensor, Gas sensor, Acceleration sensor, PIR Motion Sensor, Displacement sensor, Light sensor etc. The microcontroller is a programmable device that collect data from sensors and process it and also controls other components in the sensor mote like memory and transceivers. The microcontroller is energy efficient than a microprocessor. The Transceiver collects data from microcontroller registers and transmits it after modulation. Also it performs the operation of receiving data from other nodes. Most of the WSN applications rely on radio frequency based communication. Significant amount of energy is consumed while transmitting and receiving data. The external memory includes a program memory, RAM and EPROM. Memory requirements depends on WSN applications and is high for security critical applications. All the components of a sensor mote are battery powered: both rechargeable and non-rechargeable batteries are available.

B. Protocol stack of WSN

The protocol stack of WSN [1] is shown in Fig. 3. The protocol stack consists of five layers and a group of management planes. The physical layer is primarily in charge of frequency selection, data encryption and signal modulation. The Data Link Layer is in charge of overseeing channel access utilizing MAC (Medium Access Control) protocols and guaranteeing dependable communication through low-complexity error control mechanisms. The Network Layer performs directing of information supplied by the Transport Layer with the assistance of multi-hop wireless routing protocols. The Transport Layer protocols have the functionalities like Reliability and Congestion control for the flow of data. The Application Layer contains diverse application software and management functionalities depending upon the sensing tasks. The Mobility, Power, and Task management planes performs node movement observation, energy efficiency checking and task distribution among the sensor nodes. The Topology, Synchronization and Localization planes handle connectivity and coverage issues, time synchronization and localization of the events [1].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

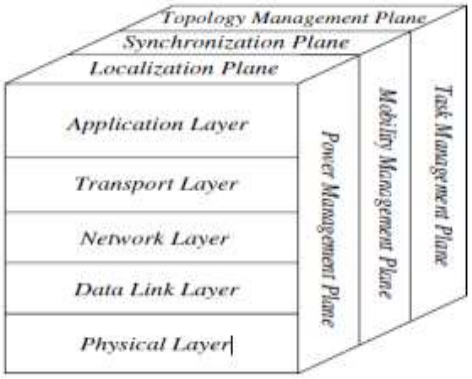

Fig.3: Protocol stack of WSN

C. Characteristics of WSN [3]

- **Lack of a Central Node:** There is no central coordinator node in a wireless sensor networks. All the nodes performs two functions: gathering information and forwarding messages to neighboring nodes thus forming a distributed environment. This lack of central coordination improves scalability and fault tolerance.
- **Self-Organization:** The sensor nodes are independent and self-organizing based on the contexts like frequent path breaks, security attacks and power losses. All the processing in a WSN is done in a distributed way. Self-organization is an important task and its absence causes WSN vulnerable to various attacks.
- **Scalability:** WSNs usually comprises a large number of sensor nodes arranged in different environments. This provides redundancy and thus it improves the reliability and stability of the system.
- **Dynamic Network Topology:** In a wireless sensor network, the network topology changes dynamically due to various reasons such as mobility of nodes, failure of nodes and the remaining battery power of nodes. In a large scale WSN, frequent topological changes results in more communication overhead to exchange the topological information and thus reducing the energy efficiency of sensors.
- **Multi-hop Routing:** Remote sensor networks use multi-hop data forwarding mechanism in which all the nodes forwards data for other nodes. The sensor nodes which are not in direct range of sink has to send the data to its intermediate nodes. Implementation of multi-hop routing requires the development of energy aware routing protocols.

D. Applications of WSN

WSNs have an extensive variety of applications. The different applications of Wireless sensor network include:

- Military applications

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

- Environmental monitoring
- Health monitoring of patients
- Disaster management
- Industrial safety
- Agriculture
- Law and order enforcement
- Transportation
- Traffic monitoring

3. SECURITY OF WSN

Security of WSNs is really significant as most of these networks are deployed in hostile environments and are vulnerable to attacks.

A. Need for Security

Since the wireless sensor network is used for many security critical applications, the secrecy and privacy of data being transmitted through the wireless medium has to be preserved. As an ad-hoc network with limitations on resources, the WSN faces multiple constraints which makes it more complicated. Multiple constraints that should be considered while considering a security mechanism for WSN are summarized below.

- **Wireless and Shared nature of Communication Channel:** The broadcasting nature of WSN make it vulnerable to multiple types of security attacks. The interception, analysis and alteration of the messages transmitted via the wireless channel can be done easily by an attacker. The attacker can easily inject false data into the network that can affect the integrity of data. A jamming or Denial of Service (DoS) attack can be executed by an attacker from inside or outside the network. The attacker can obtain the details of a legitimate node and replace that node with a malicious node. Security of data transmitted through a wireless communication channel and the security of WSN nodes itself is a great challenge.
- **Multi-hop communication:** Wireless Sensor Networks rely on multi-hop communication and thus the intermediate sensor nodes may modify or destroy the data send by other nodes. Sometimes the intermediate nodes drops the packets selectively which is very difficult to identify.
- **Untrusted transmissions:** An attacker can easily capture and modify the data send by a node if the data is not properly encrypted. All the encryption schemes used in traditional networks cannot be used in WSN due to its resource constraints.
- **Loopholes in communication protocols:** Most of the protocols developed for wireless sensor networks does not provide a full-fledged security mechanism. Since the code of these protocols are publicly available, an attacker can easily find a loophole [5].

- **Deployment in hostile and unattended environments:** Most of the wireless sensor applications uses a massive deployment of sensor nodes in harsh and hostile environments such as forest, sea etc. These sensor nodes are kept untouched or unattended for a long period of time. An attacker can physically access the node to get information, ruin the sensor node or change the sensor node by a malicious node. Also an attacker may intercept the signals from sensors, extract important information or modify the information.
- **Limited resources:** The resource constrained WSN nodes are a barrier to provide a strong security mechanism for WSN. The two major constraints are on memory and battery power. When strong security mechanisms have to be implemented, the memory and battery power requirement also increases. This makes it difficult to implement powerful cryptographic algorithms developed for traditional networks in WSN.
- **Immense Scale:** While implementing a strong security mechanism in WSN, the scale of the network plays a crucial part. The network performance in terms of computation, communication and energy efficiency has to be preserved while scaling the network by maintaining the same security features. The resource constraints are a barrier for scaling the network beyond a limit.

B. Security Goals

The primary goals of WSN security techniques are to ensure data confidentiality, data integrity and data availability.

- **Confidentiality:** Confidentiality is related to data security, secure channel and security of sensor information like keys and sensor identities. Encryption is the standard approach used to achieve data confidentiality.
- **Integrity:** Guarantees that a message is not altered or modified while transmitting through wireless medium by an adversary. This safeguards the WSN from false data injection or the modification of messages.
- **Availability:** The network is available for the nodes to communicate and resources are available for communication. Adding security to WSN should not affect the availability.

The secondary goals of security are given below.

- **Freshness:** Data freshness indicates that the stream of data coming from sensor nodes are recent. That is, a sensor node is not sending or replaying any old data. The data freshness can be weak and is acceptable for sensor readings, but a strong one is required for time synchronising data [4].
- **Self-Organization:** The sensor nodes are independent and self-organizing based on the situations like frequent path breaks, security attacks and power losses. All the processing shall be distributed. Self-organization is a great challenge and its absence makes the wireless sensor network vulnerable to various attacks [4].
- **Time Synchronization:** Time synchronization is important for multi-hop networks to synchronize the local clocks of sensor nodes. Some applications demand synchronization between groups of nodes.

- **Secure Localization:** Localization enables to locate the faults with accurate location information. The location information sent by a node through the wireless medium may be easily manipulated. Thus localization schemes must be designed with security in mind [4].
- **Access Control:** Access control is provided to prevent malicious nodes joining a WSN. This gives to the legitimate participants a means to detect the messages coming from external sources of the network [6].

4. CONCLUSION

This comprehensive study on WSNs explains the architecture, characteristics and various security challenges on WSNs.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"A survey on sensor networks", IEEE Communication Magazine, Aug 2002.

[2] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy,"A comparison of physical attacks on wsn", International Journal of Peer to Peer Networks, April 2011.

[3] David Culler, Deborah Estrin,"Overview of sensor networks", IEEE Computer Society, 2004.

[4] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudharyi,"Wireless sensor network security: A survey", Security in Distributed, Grid, and Pervasive Computing, 2006.

[5] Yun Zhou, Yuguang Fang, Yanchao Zhangf,"Securing wireless sensor networks: A survey", IEEE Communications Surveys and Tutorials, 2008.

[6] Sahabul Alam 'and Debashis De,"Analysis of security threats in wireless sensor networks", International Journal of Wireless and Mobile Networks, April 2014.

[7] Abdul Wahid, Pavan Kumar, "A survey on attacks, challenges and security mechanisms in wireless sensor network", International Journal for Innovative Research in Science and Technology, January 2015.

[8] Dr. G. Padmavathi, Mrs. D. Shanmugapriya,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol 4, No 1 and 2, 2009.

[9] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks", Communications of the ACM, vol. 47, no. 6, pp. 5357, 2004.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[10] Madhumita Panda,"Security Threats at Each Layer of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[11] Abhishek Pandey, R.C. Tripathi,"A Survey on Wireless Sensor Networks Security", International Journal of Computer Applications, Volume 3, No.2, June 2010.

[12] Yang Xiao et. al, "A Survey of Key Management Schemes in Wireless Sensor Networks", Computer Communications, Special Issue on Security on Wireless Adhoc and Sensor networks, 2007.

[13] Nusrat Fatema, Remus Brad,"Attacks and Counteattacks on Wireless Sensor networks", International Journal of Ad hoc, Sensor and Ubiquitous Computing, Vol.4, No.6, December 2013.

[14] Mohamed Lamine Messai,"Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application, April 2014.