ORIGINAL RESEARCH PAPER

Computer Science

SECURITY MECHANISM ISSUES IN WIRELESS SENSOR NETWORKS

KEY WORDS: Wireless Sensor Networks, Attacks, Security Mechanisms

Suman Asst. Professor in Computer Science, Govt. PG College for Women, Rohtak (Haryana).

Dr. Geeta Dalal Asst. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak (Haryana).

Seema Sangwan Asst. Professor in Computer Science, Pt. N.R.S. Govt. College, Rohtak (Haryana)

ABSTRACT

In this paper we have studied and reviewed, the security in wireless sensor networks is a very important issue. These networks may be exposed it different attacks. With this in mind, researchers propose in this area variety of security techniques for this purpose, and this article describes security in wireless sensor networks. Discussed threats and attacks of wireless sensor networks. The article also aims to provide the basic information related to determining essential requirements for the protection WSNs. We mention some security mechanisms against these threats and attacks in Wireless Sensor Network which is most important and mandatory for the entire wireless networks.

INTRODUCTION

A wireless sensor network is the most important emerging technology trend in the coming years because sensing technologies and processing power, and wireless communication make it beneficial for use in the soon future. Wireless sensor networks (WSNs) are used to collect data from the physical environment; wireless sensor networks can work in any environment other than conventional networks, especially if they are not wired connections in those environments.

Wireless sensor networks (WSNs) have recently gained a lot of attention by scientific community. Small and inexpensive devices with low energy consumption and limited computing resources are increasingly being adopted in different application scenarios including environmental monitoring, target tracking and biomedical health monitoring. In many such applications, node localization is inherently one of the system parameters. Localization process is necessary to report the origin of events, routing and to answer questions on the network coverage, assist group querying of sensors. In general, localization schemes are classified into two broad categories: range-based and range-free

The sensor nodes used in WSNs deploy efficiently more than the conventional wired sensor network; the sensor nodes consist of several components such as sensing, data processing, and wireless communication technology, which monitor the environment without connection with the wired network. Therefore, WSNs more advantages than the conventional wired sensor network.

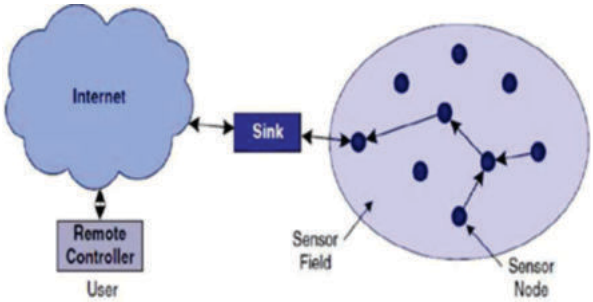

Fig-1: Wireless Sensor Networks

Security is quite a challenging issue in WSNs. It is used in many practical applications, in military applications, disaster management in remote areas, traffic monitoring, and monitoring intelligent houses and cities. The WSNs can be prone to different security threats and attacks or hackers to disrupt the entire network. From challenges and Issues face in WSN today is security.

Therefore, security for WSNs becomes most important. This paper's purpose and requirements security in WSNs then mention some of the security mechanisms used to handle those security issues in WSNs.

WIRELESS SENSOR NETWORKS (WSNS)

Wireless Sensor Networks are self-configured and infrastructure-free wireless networks that track physical or environmental conditions such as temperature, sound, vibration, friction, motion, or pollutants and cooperatively transfer their data through the network to a central position or sink where it can be viewed and analyzed. Sensing and computing instruments, radio transceivers, and control components are all used in a wireless sensor node. A wireless sensor network's individual node is resource restricted by design: they have minimal processing power, storage space, and connectivity bandwidth. The sensor nodes can operate in either a continuous or event-driven mode. The WSN uses a gateway known as a sink to connect a wired network and the distributed wireless sensors. The sensors collect the data sent to the gateway, which sends it to the user through a network or internet.

WSN can also be defined as a network comprising of possibly low-size and low-complexity devices termed as nodes which are capable of sensing the environment and communicating gathered information from the monitored area; the gathered data can be transmitted directly or through multi –hops to sink, which can then use it locally or is connected to other networks (e.g. internet) through gateway nodes

An internet of things (IoT) is a substantial regional configuration that is linked to the standard characteristics of a traditional system that may connect and exchange data. IoT also known as the "internet of everything, it is a new paradigm that connects the physical and digital worlds via a network of sensors, computers, the internet, radio frequency identification (RFID), embedded systems and communication technology. IoT architecture is shown in Figure 1. Any equipment, program, or sensors can be used in the system technique. Data and security management are provided through the Internet of things. IoT links people and things from all around the world. IoT may be used for a variety of purposes, including vehicle response, smart buildings, fast medical assistance, and smart cities. A big number of sensors may be replaced by a small number of sensors in current IoT systems, and IoT can be placed on one platform, consuming

power and energy. An efficient detection technology was created with IoT in mind. In the context, detection technology was created with IoT in mind. The sensing, data response, and control phases are the three main stages of the detection and control architecture. In most cases, a wireless sensor node is required to run the sensing unit wireless Sensor network (WSN). The WSN receiver module uses an ultra-low power radio frequency (RF) signal to achieve data synchronization. The control framework can benefit from the employment of an electronic power converter to deliver the created control to the network. The IoT-based WSN is a game-changing smart monitoring solution

One of the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. The topology control in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs. In the following, we summarize some of the challenges and design issues that affect the topology construction and maintenance in WSNs.

NODE DEPLOYMENT:

Node deployment in WSNs is application dependent and affects the performance of topology control algorithms. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

ENERGY CONSUMPTION WITHOUT LOSING ACCURACY:

Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy-conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime.

DATA REPORTING MODEL:

Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. Data reporting can 736 Preetkamal Singh, Dr. OP Gupta and Sita Saini be categorized as either time-driven (continuous), event-driven, query-driven, and hybrid. The time-driven delivery model is suitable for applications that require periodic data monitoring. As such, sensor nodes will periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest at constant periodic time intervals.

NODE/LINK HETEROGENEITY:

In many studies, all sensor nodes were assumed to be homogeneous, i.e., having equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different role or capability.

FAULT TOLERANCE:

Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and topology control algorithms must accommodate formation of new links and routes to the data collection base stations.

SCALABILITY:

The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any topology control scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing control algorithms should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

SECURITY:

In some applications, the communication among nodes is required to be secured enough so as to maintain the confidentiality. It is mostly required while dealing with the military applications like battlefield surveillance, military operations etc.

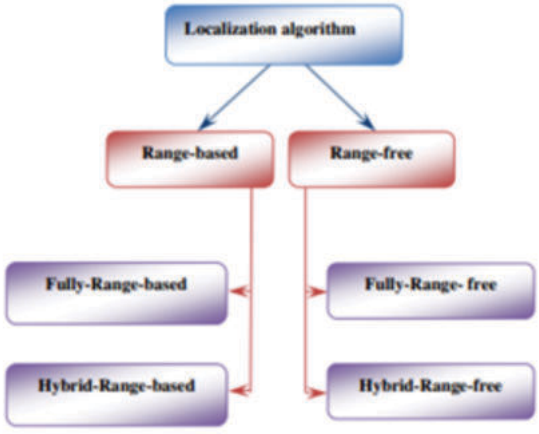

Fig-2: Localization of Sensor Networks Scheme

APPLICATIONS OF WSN

Wireless Sensor Networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, and acoustic and radar. They are able to monitor a wide variety of ambient conditions that include temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics such as speed, direction and size of an object. WSN application can be classified into following categories:

- Military applications:
- Environmental applications:
- Healthcare applications:
- Home applications:
- Traffic control:

CONCLUSION AND FUTURE SCOPE

The paper reviewed about the security features and best performance in WSN technology. When using WSNs, sensor nodes collect data from sensors and send it to other nodes, which in turn collect data from end tags. The end tags then send their data to routers, which in turn send the data to the cloud (Ethernet). The routers then provide services to multiple clients, including data display, and the data is stored in the base station. The client can visit the base station remotely via (website) Ethernet. The ZigBee standard is an important WSN and IoT communication in order to facilitate low-power, low-cost IoT applications and to handle numerous network topologies. It is well tailored to a broad variety of energy control and productivity applications in areas such as medical and health care, building engineering, manufacturing and home automation, as mentioned out in this study.

REFERENCES

1. Fatimah khalil aljwari, hajer abdullah alwadei and aseel abdullah alfaidi security in wireless sensor networks: comparative study international journal of computer science & information technology (ijcsit) vol 14, no 3, june 2022
2. I.f. Akyildiz, s. Weilian, y. Sankarasubramaniam, e. cayirci, "a survey on sensor networks", ieee communications magazine, vol. 40, issue (8), pp. 102-114, 2002.
3. a brief research study of wireless sensor network
4. Preetkamal singh1, dr. Op gupta2 and sita saini3

5. advances in computational sciences and technology issn 0973-6107 volume 10, number 5 (2017) pp. 733-739
6. Rghioui and a. Oumnad, "internet of things: surveys for measuring human activities from everywhere," international journal of electrical and computer engineering (ijece), vol. 7, no. 5, p. 2474, oct. 2017, doi: 10.11591/ijece.v7i5.pp2474-2482.
7. H. Bagdadee, m. Z. Hoque, and l. Zhang, "iot based wireless sensor network for power quality control in smart grid," procedia computer science, vol. 167, no. 2020, pp. 1148–1160, 2020, doi: 10.1016/j.procs.2020.03.417.
8. M. Manpreet, "simulation analysis of tree and mesh topologies in zigbee network," international journal of grid and distributed computing, vol. 8, no. 1, pp. 81–92, feb. 2015, doi: 10.14257/ijgdc.2015.8.1.08.
9. V. Kumar, a. Jain, and p. N. Barwal, "wireless sensor networks: security issues, challenges and solutions," int. J. Inf. Comput. Technol., vol. 4, no. 8, pp. 859–868, 2014, [online]. Available: http://www.irphouse.com.
10. Teymourzadeh, r. Vahed, s. Alibeygi, and n. Dastanpor, "security in wireless sensor networks: issues and challenges," arxiv, 2020, doi: 10.47277/ijcncs/1(7).