A Survey of Wireless Sensor Network Security

Monika Soni[1]*, Dr. Vaseem Naiyer[2]

[1] Research Scholar, Madhyanchal Professional University, Bhopal

E-mail - ms2194952@gmail.com

[2] Asst. Professor, Madhyanchal Professional University, Bhopal

Abstract - In the paper we have discussed about Wireless sensor network and its design and development aspects while keeping security of information into mind. From the primary information point-of-view we discussed about network and wireless sensor network, primary characteristics of WSN. Different network topologies are explained in this paper and need of network security while sending and receiving data is also explained. The art of hiding text in some scrambled text is also explained into this paper under the section cryptography.

Keywords- Wireless Sensor Network, Network Topologies, Network Security, Cryptography,

- X -

INTRODUCTION

Network is a specially organized arrangement of devices that are connected to share information collectively. A network may be of any nonliving devices or a living human that share some sort of information for a dedicated objective. The communication between devices takes place using Radio wave, Satellites, Infrared Beam, Telephonic Line and cables. The concept of networking stared from the very first research work in the field of networking named ARPANET which is the acronym for “Advance Research Projects Agency Network”. ARPANET uses TCP/IP protocol for communication between two computers. According to application networks are divided into various streams these are: Wireless Sensor Network (WSN), Body Sensor Network (BSN), Distributed Sensor Network (DSN), Local Area Network (LAN), Wide Area Network (WAN) etc. Each network is primarily defined and deployed for communication and data sharing purpose with each network has its own characteristics, limitations, and area of work. In recent years networking system has grown to a level that affects the human life. Each computer user directly or indirectly is a part of networking system which is known as Internet. Internet is the collection of computer systems that share hardware and software resources while keeping sharing of information as a primary objective. Similar concept was used in sensing war field during the cold war in United States which s Sound Surveillance System (SOSUS) that uses acoustic waves to detect submarines [1]. From the year 1949 the sensor network system has grown dramatically and now we are surrounded by various sensor networks. Each network has the same objective of sharing information and is affected by various attacks to steal information or scramble the data to reduce these attacks various security features developed and incorporated into networks. Few of them are: Firewall in internet blocks unauthorized access, Encryption changes the plain text into scrambled data, Authorization check is data sent by authorized device or not, and more security features added.

WIRELESS SENSOR NETWORK

A Wireless Sensor Network (WSN) is specially arranged group of sensors that communicate with each other to send data to the central hub. WSN has vast range of application including medical, military, automobile industry and etc. WSN are designed to check environmental conditions in any critical zones. A wireless sensor system builds around low powered microcontroller with some sensing elements that are used to detect environmental conditions [2]. A typical wireless sensor network block diagram is shown is figure 1. A WSN has three main components first is Host/Controller Node – this node is responsible for data centralization and controlling of complete network from base location. Second is Gateway Node – This node is responsible for host to end node communication a gateway node convert’s one protocol data to another protocol and vice versa in the network. Third Element in WSN is Sensor Node – It is the end node in Network which is responsible for sensing and controlling parameters if any [3]. Sensor node is loaded with various sensing elements, microcontroller, and communicating circuitry each has its own dedicated task to accomplish.

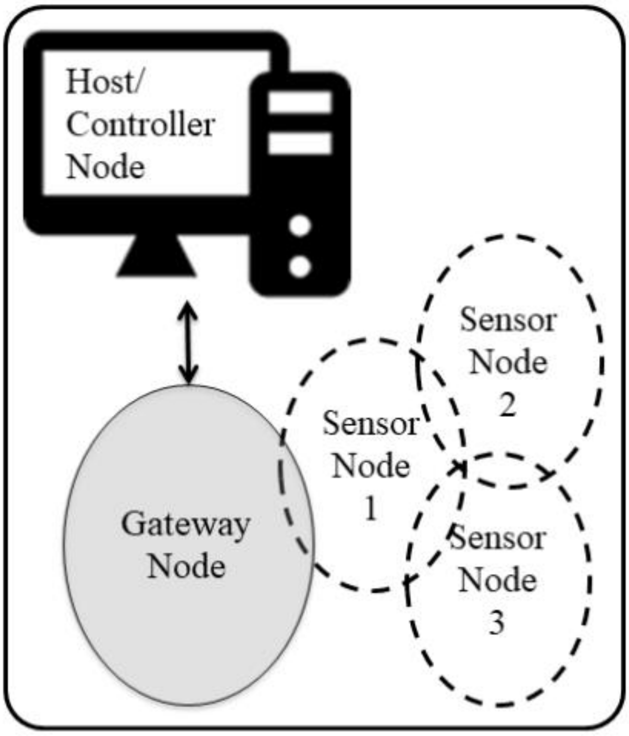


Figure 1 WSN Block Diagram

WSNs are usually are communicated through radio links to make the network wireless. A sensor network may have two or more than two sensor nodes that detects nearby environmental conditions and it to gateway or sink node. Some times WSN are deployed to detect parameters that are crucial from security point of view and are supposed to be more secure. From the military application point of view data confidentiality is more important as data may be misused by any unauthorized person [4] [8]. Attributes of a common WSN listed below.

Table 1 Attributes of WSN.

Attributes	Sub Attributes	Details
Sensor and Sensing entities of interest	Size	Small (e.g., MSME), Large (e.g., satellites, radars)
	Number	Small, Large
	Type	Passive (e.g., Acoustic, Seismic, Video), Active (e.g., Radar)
	Composition	Homogeneous (Same types of sensors), Heterogeneous (Different types of sensors)
	Spatial Coverage	Dense, sparse
	Deployment	Fixed (e.g., Factory Network), Ad-hoc(Air-dropped)
	Dynamics	Stationary (e.g., Seismic Sensors), Mobile (e.g., On Robotic Vehicle)
	Extent	Distributed (e.g., Environmental Monitoring), Localized (e.g., Target tracking)
	Nature	Cooperative (e.g., Air Traffic Control), Non-Cooperative (e.g., Military Targets)
	[illegible]	[illegible]
Operating Environment		Benign (Factory floor), Adverse (Battlefield)
Processing Architecture		Centralized (All data to central site), distributed (located at sensor or at other sites), Hybrid
Energy Availability		Constrained (e.g., in Small Sensors), Unconstrained (e.g., in Large Sensors)

NETWORK TOPOLOGIES

Network topologies are the layout of connections in any network it may be a physical or logical a physical layout represents the physical layout of the network and in logical which decides how data is actually moved in network. Some of network topologies are explained below [2]. Each type of network topology is shown in figure 2.

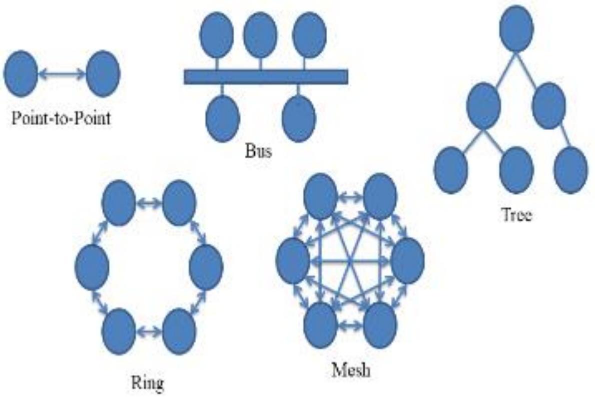


Figure 2 Different Types of Network Topologies

- **Point-to-Point**: Simplest topology in this type of topology two nodes are directly connected together.
- **Bus**: Each Node is connected to single cable to form a network.
- **Star**: In such kind of network each node is point-to-point connected to central hub.
- Ring: In this kind of network is formed circular in fashion each node is connected point-to-**point** and last node is connected to first node.
- Mesh: All nodes are point-to-point connected together and can share information in any **order**.
- **Tree**: It is a hierarchical type of network.

NETWORK SECURITY

It is an organizational strategy or a technology that with the objective of security within the network. It is also important to monitor and prevent unauthorized access or denial of service to computer/device network. For this some sort of policies are adopted by the network deploying authority which is known as security policies. Figure 2below shows the requirements in network [5] [:

- **Data Confidentiality:** The main objective of any security policy is to make data confidential.

- **Data Integrity:** A security policy should be capable of check data is unaltered or not.

- **Data Freshness:** Freshness of data is also as important as confidentiality and integrity is concern. If data received is not correct and on time it should be rejected by the security system of network.

- **Self Organization:** A network should be of self organization type so one can assure about its ad-hoc nature.

- **Time Synchronization:** System should be synchronized in time domain so data freshness maintained by the network.

- **Authentications:** Even after all methodologies an authentication method should also be maintained in the network policy which ensure about the entry and data communication is from authentic node.

There are various security tools that are used to enhance the performance in the system and are discussed below.

- **Access Control:** A sink node must not be connected to end sensor nodes it must be connected by some intermediate links with some access control procedures.

- **Network Segmentation:** A network must be segmented into parts that will help developer to rectify the bug in network.

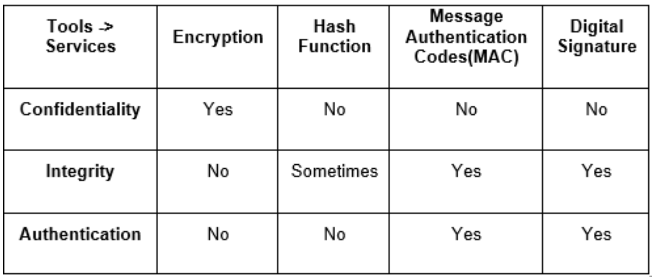
- **Firewalls:** A software or hardware firewall may be incorporated to restrict unauthorized access to the sink node.

- **Encryption:** To secure data from unauthorized access and misuse of data. Some sort of encryption system is used which scramble the data into unreadable text.

- **Application Security:** A system must have some application oriented software tool which ensures the data is used for the same application for which it is defined.

CRYPTOGRAPHY

Since the writing art has been developed by human society it is considered that the concept of cryptography has been developed. Root of cryptography found in Egyptian Roman Civilizations. The first cryptography technique is considered “hieroglyph”. In earlier Roman cryptography Caesar Shift Cipher Cryptography technique is used is this kind of cryptosystem each latter in the work has shifted by 2 (i.e. ‘A’ is replaced by ‘C’). The classical cryptography is considered to be applied on letters and digits directly, and in modern cryptography is applied on binary bit sequence [6]. Modern cryptography mathematical algorithms are applied using some sort of coding during processing of data which is secured by some secret key. The primary objective of cryptosystem is to make data confidentiality, Authentication, Data Integrity. There various cryptographic tools that are used to incorporate these features are discussed in table below.



Tools -> Services	Encryption	Hash Function	Message Authentication Codes(MAC)	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes

A basic chipper system is shown in figure 3. The plain text is the data that has to protect. Cipher Text is the scrambled data generated after applying some sort of encryption technique. Encryption and Decryption Algorithms are the mathematical process prior converts plain text into cipher text and later convert cipher text into plain text [7] [9]. Encryption Key and Decryption Key are some alphanumeric value that is known to sender and receiver and are used to encrypt and decrypt plain text to/from cipher text. If any attacker attacks the data it will receive encrypted version of text which is nothing without decrypting key and algorithm that guarantee about data confidentiality. There are two types of cryptosystems one is Symmetric Key Encryption in which encryption and decryption keys both are same. Whereas in Asymmetric Key Encryption, each communicating device has a pair of keys one is public key for encryption and private key for decryption [10].

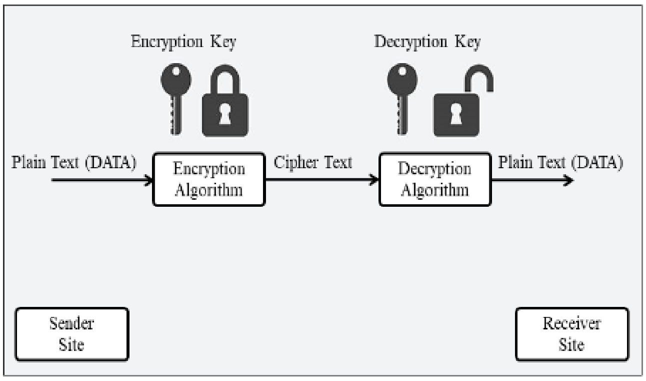


Figure 3 Basic Cryptosystem.

CONCLUSION

From the development phase of ARPANET the first network and from the first use of sensor network SOSUS security of information has been considered to be very important and has grown in drastic way, from single layer of security to multilayer security policy has been incorporated in network security. In this paper we have conclude about the need of information security and tools used for make data secure.

REFERENCES

[1] Chong, Chee-Yee, and Srikanta P. Kumar. "Sensor networks: evolution, opportunities, and challenges." Proceedings of the IEEE 91.8 (2003): 1247-1256.

[2] Groth, David (2005). Network Study Guide, Fourth Edition'. Sybex, Inc. ISBN 0-7821-4406-3

[3] Rathee, Pinki, and Sanjeev Indora. "An Object Tracking Mechanism in Wireless Sensor Networks." (2017).

[4] López, J. and Zhou, J. eds., 2008. Wireless sensor network security (Vol. 1). Ios Press.

[5] Walters, John Paul, et al. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367.

[6] William Stallings, “Cryptography and Network Security Principle and Practices, Fourth Edition”, ISBN0-14-187316-4

[7] R. Stockton Gaines, “Using Encryption for Authentication in Large Network of Computers”,

[8] “Wireless Sensor Networks Concepts, Application, Experimentation and Analysis”, Fahmy, H.M.A., 2016, ISBN: 978-981-10-0411-7,

[9] R. Stockton Gaines, “Communication of ACM”, December 178, Volume 21, Number 12, pp.993-998

[10] Simmons, Gustavus J. "Symmetric and asymmetric encryption." ACM Computing Surveys (CSUR) 11, no. 4 (1979): 305-330.

Corresponding Author

Monika Soni*

Research Scholar, Madhyanchal Professional University, Bhopal