An Overview of Wireless Sensor Network

Piyush Raja[1], Dr. M. M. Rahman[2], Dr. Md. Safdar[3]

[1]Research Scholar, A.N. College, Patna, Bihar, India
[2]Associate Professor, PG Deptt. of Mathematics, A.N. College, Patna, Bihar, India
[3]Lecturer, Deptt of Computer Science, IGNOU, New Delhi

Abstract

Wireless Sensor Networks (WSNs) can be defined as a self-configured and organization less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed. A wireless sensor network (WSN) is a network of distributed sensors grouped together to monitor physical or environmental conditions, like temperature, pressure, sound etc. and to pass their sensed values through the network to a main location (sink) cooperatively. Every node in sensor network consist of three subsystem, first sensor subsystem which sense environment, second processing subsystem which perform local computation on sensed data and third communication subsystem which is responsible for message exchange. A variety of Studies in this field utilize that mobile sink node is used to collect environmental explanation such as weather forecasting data from sensor nodes.A sink or base station acts like an interface between users and the network. One can retrieve required information from the network by injecting queries and gathering results from the sink. Typically a wireless sensor network contains hundreds of thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. A wireless sensor node is equipped with sensing and computing devices, radio transceivers and power components. They have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them.

Keywords*: Characteristics of WSNs, Applications, Security, Protocols*

Introduction:

A wireless sensor network (WSN) are structurally distributed self-directed sensors to monitor environmental or physical conditions such as sound, temperature, pressure, military work etc. and to cooperatively transfer their data through the network to a main location. Its simplest form makes it a

network of (possibly low-size and low-complex) devices denoted as nodes that can sense the atmosphere and communicate the information collected from the monitored field through wireless links; the data is forwarded, possibly by multiple hops transmitting, to a sink that can use it locally, or is connected to other networks (e.g. Internet) through a gateway [1]. A sensor node or mote is a node in a sensor network that is proficient of performing some processing [2], collecting sensory information and communicating with other associated nodes in the network. Gateways allow the scientists/system executives to interface Motes to personal computers (PCs), personal digital assistants (PDAs), Internet and surviving networks and protocols. In a shell, gateways act as a proxy for the sensor network on the Internet [3]. Application Manager connects to the gateways via some media like Internet or satellite link. Task Managers consist of data service and client data browsing and processing [3]. Sink interconnects the user through internet or satellite communication. It is positioned near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop arrangement less architecture through the sink

2. Characteristics of Wireless Sensor Network

- ✓ Scalability
- ✓ Wide range of densities
- ✓ Re-programmability
- ✓ Maintainability
- ✓ Ability to face node failures
- ✓ Mobility of nodes
- ✓ Dynamic network topology

3. Applications of Wireless Sensor Network [4] [5] [6]:

- ✓ Environmental sensing
- ✓ Condition monitoring
- ✓ Process automation

4. Security issues in WSN

4.1 Data Integrity: It ensures that data packets received by destination is exactly the same with transmitted by the sender. [7][8].

4.2 Data Confidentiality: Confidentiality is to shield data during communication in a network to be understood other than intended recipient. [7][8].

4.3 Data Availability: Availability ensures that the services are always presented in the network even under the attack such as Denial of Service attack (Dos). [7][8].

4.4 Data Authentication: Data authentication is attained through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys [7] [8].

4.5 Data Freshness: It is achieved by using mechanisms like nonce or timestamp should add to each data packet [7].

5. Secured Protocols in Wireless Sensor Networks

There are following Secured Protocols in Wireless Sensor Network-

5.1 SPINS: Security Protocols for Sensor Networks: Adrian Perrig et al. [9] proposed "SPINS" a suite of security protocols optimized for sensor networks. SPINS has two secure building blocks: SNEP and µTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments.

5.2 TINYSEC: Karlof et al. designed the replacement for the unfinished SNEP, known as TinySec[10]. Inherently it provides similar services, including authentication, message integrity, confidentiality and replay protection.

5.3 MINISEC: MiniSec [11] is a secure network layer protocol that claims to have lower energy consumption than TinySec while achieving a level of security which matches that of Zigbee.

5.4 LEAP: Sencun Zhu et. al.[12] proposed LEAP Protocol, which is a key management protocol for sensor networks. LEAP is designed to support secure communications in sensor networks; therefore, it provides the basic security services such as confidentiality and authentication.

5.5 ZIGBEE: Zigbee[13] Coordinator acts as "Trust Manager", which allows other devices to join the network and also distributes the keys. It plays the three roles as follows:

a) Trust manager, whereby authentication of devices requesting to join the network is done,
b) Network manager, maintaining and distributing network keys, and
c) Configuration manager, enabling end-to-end security between devices.

5.6 LiSP: Lightweight security mechanism is based on efficient rekeying technique. It can be used for key management of small and large networks as well. The main features of LiSP includes efficient key broadcast without retransmission/ACK, ability to detect and recover lost keys, key refreshment without disrupting ongoing data encryption/decryption [13].

5.7 LEDS: It provides end-to-end authentication, security and enroots filtering. It provides location aware key management. LEDS can be used in both small and large networks [14]. However, number of keys increases with cell size. In addition, LEDS does not support dynamic topology. It divides the network in cell regions. If an event happens within a region, the event should be sensed by T nodes.

5.8 Energy Efficient Link-Layer securities Protocol (LLSP): It ensures message authentication, access control, message confidentiality, and replay protection. It follows the same idea follows in Tinysec. However, it uses different packet format and crypto structure.

6. Conclusion:

Wireless Sensor Network technology has an incredible potential to improve quality of life in all aspects and is likely to be widely used in the medium-term future. In this paper, the basic parts of sensor nodes, the technology used with the wireless sensor network have been explained. We have followed by the characteristics, applications and secured protocols challenges of wireless sensor network. An overview of the wireless sensor networks, their design issues, network services and developments that have recently taken place. The use of wireless sensor technology has seen proliferation in a large number of applications and this paper is towards that effort to develop a system for a specific application.

REFERENCE

[1] Abu Shohel Ahmed, 27 April 2009 “An Evaluation of Security Protocols on Wireless Sensor Network”, pp 2-5

[2] Akkaya, K. and Younis, 2005 “A survey of Routing Protocols in Wireless Sensor Networks”, Elsevier Ad Hoc Network Journal, pp 4

[3] Sangeeta , Mr. Rajesh Parihar, May-2015 “A comprehensive study of Medium Access Control Protocols in Wireless Sensor Network ” International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 4 Issue 5, pp 82.

[4] D. Puccinelli and M. Haenggi, Aug. 2005 “Wireless Sensor Networks-Applications and Challenges of Ubiquitous Sensing,” IEEE Circuits and Systems Magazine, pp 19-31.

[5] Marco Zennaro, ICTP Trieste-Italy, “Introduction to Wireless Sensor Networks”, February 2012, pp 3, 7,14,20,24.

[6] Kazem sohraby, daniel minoli, taieb znati, 2007“Wireless Sensor Networks Technology, Protocols, and Applications”,pp 10-11.

[7] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, 2009 “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol. 4, pp 1-2

[8] Himani Chawla, July 2014 “Some issues and challenges of Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, pp-237-238

[9] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. In Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001), July 2001.

[10] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, 162 – 175

[11] M. Luk, G. Mezzour, A. Perrig, and V.Gligor, "MiniSec: A Secure Sensor Network Communication Architecture," in IEEE International Conference on Information Processing in Sensor Networks (IPSN'07), Cambridge, Massachusetts, USA, 2007.

[12] S. Zhu, S. Setia, and S. Jajodia. “Leap: efficient security mechanisms for largescale distributed sensor networks”, In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, New York, USA, 2003, 62–72

[13] ZigBee Specification v1.0: ZigBee Specification (2005), San Ramon, CA, USA: ZigBee Alliance. http://www.zigbee.org/en/spec_download/download_request. asp

[14] Abu Shohel Ahmed, 27 April 2009 “An Evaluation of Security Protocols on Wireless Sensor Network”, pp 2-5