ISBN 978-93-84468-20-0
Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015)
Singapore, March 29-30, 2015, pp. 224-228

Wireless Sensor Network: Challenges, Issues and Research

Anjali Potnis[1], and C S Rajeshwari[2]

[1, 2] Electrical & Electronics Engineering, NITTTR, Bhopal, M.P. India

Abstract**:** *Wireless Sensor Network (WSN) being one of the emerging dominant technology trends in the coming decades has posed numerous unique challenges to researchers. The sensing technology combining with processing capability with ultra low power consumption and wireless communication makes it lucrative for being exploited in abundance in future. WSN is gaining popularity in the every field of modern society like healthcare, traffic management, military, remote applications, inventory management, environment monitoring, data collection on land, air and submarine etc. It provides multifold solution for transferring the information from one point to the other point located anywhere on the globe. As data is moving on the wireless channel it faces many challenges in terms of safety and efficient delivery of the data. Distance involved for the data transfer limits the speed of data transfer and also the reliability. Power requirements of sensor nodes, computational capabilities, ambient environmental conditions, periodicity of data sampling and practical parameters related to wireless channel are the major challenges for the proper and efficient working of WSN. This paper discusses the challenges and issues related to wireless sensor networks in general and at the same time encouraging the new researchers to work in this upcoming research field which will be the need of modern society.*

Keywords: *WSN, ultra low power electronic circuit, sensor nodes, security, real time*

1. Introduction

Wireless Sensor Network basically consist of numerous sensors nodes and the wireless channel to connect the nodes and each node mainly consists of transreceiver section, ultra-low power digital signal processor or microcontroller/microprocessor, external memory , various interfaces for data collection and power section as shown in fig.1. Number of nodes in any network varies from hundreds to thousands which makes it different than other wireless networks and therefore WSN is complex and challenging to control and maintain on continuous basis.

As data is moving from various sensor nodes in the network the issues related to sensor data collection, data formatting, data transfer, data speed, data security and privacy, power optimization and power management, memory space and computational limitations, time delay and synchronization of the complete process and other related aspects opens new fields of research.

Wireless Sensor Network works in environment conditions especially where wired connections are not possible. Wireless sensor nodes consists of different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of physical and environmental conditions.

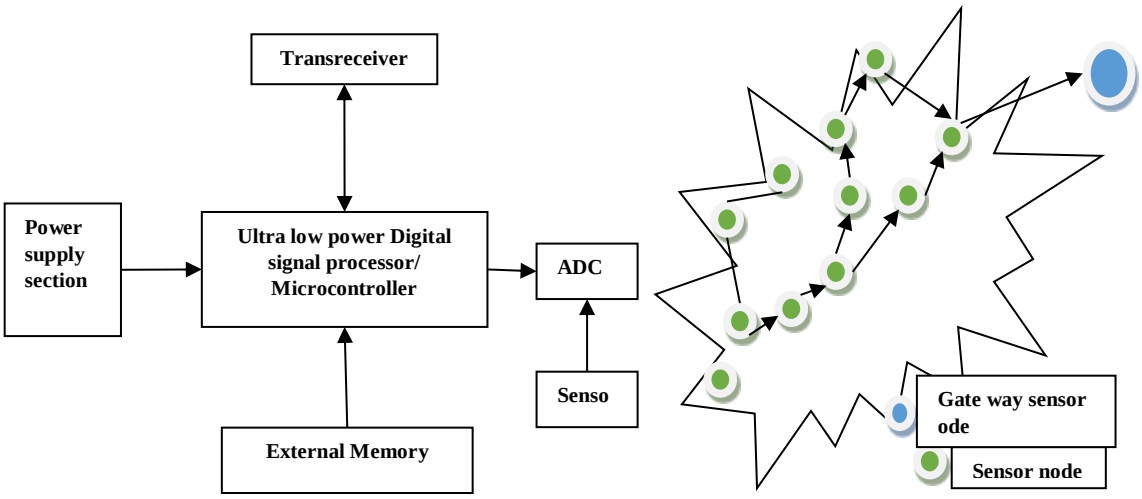

Fig. 1: Basic Block diagram of sensor node and sensor network

Wireless sensor nodes contain array of sensors in case of multiple data collection. The sensor node can be put for continuous or selective sensing, location sensing, motion sensing and event detection etc. A base station links the sensor network to sense, process and disseminate information of targeted physical environments.

2. Major Challenges:

2.1 Security and privacy

The sensors are deployed either in a controlled environment where monitoring and surveillance are critical or in an uncontrolled environment where security for sensor networks becomes extremely important. As the transfer of data is on wireless channel the privacy and security is the prime concern of these networks. Due to limited computational capacity, memory and power available, reliable data transfer becomes challenging in the wireless environment. Malicious attacks and noisy wireless channel requires special care for the faithful data transfer. Due to the limited computational capacity and power limitation on various nodes WSN require different approaches to tackle these problem compare to other wired or wireless networks. WSN are susceptible to various attacks like Denial of Service (DoS), Wormhole attack, Hello flood Attack, Sinkhole Attacks, Sybil Attack etc. [1],[2] which can be attended by various strategies depending on service types, data type and computational capacity of the nodes.

2.2 Power requirement of wireless Sensor Networks

As data collection is continues process in most of the applications the power requirement of the sensor nodes and system becomes challenging and optimization of power utilized is another important and essential research issue. For the sensor node's faithful operation Ultra low power electronic circuits and dynamic power optimization algorithms are gaining attention of researchers to come up with new solutions.

2.3 Challenges in real time

WSN deal with real time data for applications like military and health services. In many applications sensor data must be delivered within time constraints so that appropriate decision can be made or actions taken in time for the corrective measure is crucial. Most protocols either ignore real-time or simply attempt to process as fast as possible and hope that this speed is sufficient to meet deadlines [3]. Some initial results exist for real-time routing but. It is important not only to develop real-time protocols for WSN, but associated analysis techniques must also be developed for the reliable and robust operation of WSM. Other functions must also meet real-time constraints including: data fusion, data transmission, target and event detection and classification, query processing, and security.

3. Issues

The major issues that affect the design and performance of WSN are as follows: Hardware and operating systems, wireless channel characteristics, medium access schemes, localization, synchronization, calibration, transport layer, data aggregation and data dissemination, data centric and querying, architecture, programming models for sensor networks, quality of service, network layer and security [4]. Only layer issues and security issues are considered in this paper.

3.1 Wireless Network Layer Issues

The data transfer from wireless sensor network are also based on standard layered architecture where each layer have issues as follows:

3.1.1 Physical Layer

Types of sensors, distance between sensor nodes, path loss, reflection, absorption and scattering loss, interference i.e., co-channel and inter-channel interferences, modulation techniques, signal quality and strength are the major issues related to the physical layer data transfer.

3.1.2 Data link layer

Data link layer's major responsibility is to ensure interoperability amongst communication between nodes. This layer deals error detection and correction, flow control, multiplexing for WSN. Moreover, to create secure key during network deployment and maintenance, some scientist suggested the probable use of public key cryptography, and secure code distribution [2].

3.1.3 Network layer

Optimized path selection for the packet routing is the major responsibility of network layer. Network layer works for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa .Identification number based protocols and data centric protocols are used by WSN for routing mechanism. Due to the broadcast nature of transmission for WSN, secure routing protocol is an essential requirement. Separate encryption and decryption techniques are utilized for secure routing.

3.1.4 Transport Layer

As external sensor network connected to the internet can use the same Transport layer set up for the data transfer, however it is the main difficult issue in wireless sensor networks.

3.1.5 Application Layer

Application layer is used to display ultimate yield by guarantee reliable data flow to lower layers. This layer is in charge of data collection, management and processing of the data by using the application software to obtain reliable data transmission.

3.2 Security Issues

The security issues are classified as primary and secondary. The primary issues are known as Standard security requirement such as Confidentiality, Integrity, Authentication and Availability (CIAA).The secondary issues are Data Freshness, Self Organization, Time Synchronization and secure localization.

3.2.1 Primary Issues

Data Confidentiality:-This is the most important issue in network security. A sensor node should not reveal its data to the neighboring nodes .WSN should be able to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential.

Data Authentication:-Authentication ensures the reliability of the message by identifying its origin.

Data Integrity:-Data integrity in sensor networks is needed to ensure the reliability of data and refers to the ability to confirm that the message has not been tempered with, altered or changed. Although the network has confidentiality measures there is still a possibility of the data integrity compromising. The integrity of the network will be in trouble when either a malicious node present in the network injects false data or unstable conditions due to wireless channel cause damage or loss of data [5].

Data Availability:-Data Availability is of primary importance for maintaining an operational network. This determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network.

3.2.3 Secondary Issues

Data Freshness: - In spite of the fact that data confidentiality and data integrity are assured, it is required to ensure the freshness of each message. Data freshness suggest that the data is recent and it ensures that no old messages have been replayed. To solve this problem time related counter can be added into the packet to ensure data freshness.

Self organization:-If self organization is lacking in a WSN then the damage resulting from an attack or even the risky environment may be devasting. A WSN typically is an ad-hock network requiring every sensor node to be independent and flexible enough to be self organizing and self healing according to different situations as there is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security.

Time Synchronization:- A more collaborative sensor network may require group synchronization for tracking applications. Most sensor network applications require some or other form of time synchronization.

Secure localization:-A sensor network designed to locate faults will need accurate location information in order to point out the location of a fault. An attacker can easily manipulate non-secured location in information by reporting false signal strengths, replaying signals.

4. Research Areas

The design of a WSN depends on the specific application, considering the factors such as environment, application's design objective functions, cost, hardware, and system capabilities. Dimensions of sensors, cost of sensor nodes and power requirement are the major tradeoff for the WSN solutions. Data types and sensors are the starting point for the new protocol development area. Special Real time data transfer protocols is the need of WNS. Smart sensors and smart antenna concept integration for further enhancement of applications and services opens new research areas for WSN. Optimization of number of nodes and hybrid topology will be the future WSN needs and will lead to new dimension for research in WSN.

5. Conclusion

Wireless Sensor Networks are bit different than just a specific form of ad hoc networks. Recent advances in ultra-low power hardware technologies has resulted in more energy efficient sensors as well as reduction in dimension up to few millimeters volume. The major challenge is still energy constraints. As wireless sensor networks are still at its nascent stage of research, much activity is still ongoing to solve many open basic Issues related to hardware problems, especially with respect to the energy supply and miniaturization, are not yet completely solved, Wireless Sensor Networks are having certain short comings, which are to be solved. In spite of the present shortcomings WSN is emerging as a very important tool for making modern life style more comfortable and safe. Yet, there is enormous scope for improving this WSN technology.

6. References

[1] Y. Wang, G. Attebury, Byrav Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials • 2nd Quarter 2006*.

[2] Mayur Dhaye, Himangi Pande "Security in Wireless Sensor Networks: Issues and Challenges" *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, ISSN 2348 – 4853,Volume 1, Issue 12, December 2014,pp.59-65.

[3] Indu, Sunita Dixit, "Wireless Sensor Networks: Issues & Challenges," *International Journal of Computer Science and Mobile Computing(IJCSMC)*,ISSN 2320–088X, Vol. 3, Issue. 6, June 2014, pp.681-685**.**

[4] Gowrishankar. S, T. G.Basavaraju, , Manjaiah D.H, Subir Kumar Sarkar , "Issues in Wireless Sensor Networks," in *Proceedings of the World Congress on Engineering 2008(WCE 2008)* , Vol. I, July 2 - 4, 2008, London, U.K.

[5] Vikash Kumar, Anshu Jain, P. N. Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions," *International Journal of Information & Computation Technology (IJICT)*, ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868.