A Brief Research Study of Wireless Sensor Network

Abstract

Wireless Sensor Networks (WSNs) play a major role in revolutionizing the world by its sensing technology. WSNs has emerged as that powerful technology which has multiple applications such as such as military operations, surveillance system, Intelligent Transport Systems (ITS) etc. WSNs comprises of various sensor nodes, which captures the data from the surrounding alongside monitoring the external environment. Much of the research work is focused on making the sensor network operating with minimum consumption of energy, so that it can survive for longer duration. The primary concern in the direction of saving energy has been due to the discharging of those batteries on which sensor nodes are operated. In addition to that, WSNs are also exploited for its security aspects so that it can be used in some confidential sectors like military battlefield. This paper, introduces the WSN in different aspects like applications, routing and data collection, security aspects and also briefs about simulation platform that can be used in WSNs. This paper contributes in a fashion about introducing the WSNs in different sectors of its operation and reflecting its significance.

Keywords: Introduction to WSN, Routing, Simulation platform in WSN, security aspects in WSN, applications of WSN.

1. INTRODUCTION TO WSN

Advancement in wireless communication has made possible the development of wireless sensor networks comprising of devices called sensor nodes. Sensor nodes are

low power, small size & cheap devices, capable of sensing, wireless communication and computation. As soon as the sensors are deployed in the network they configure themselves and connect with each other for data collection and thereby forwarding the data to the Base Station.

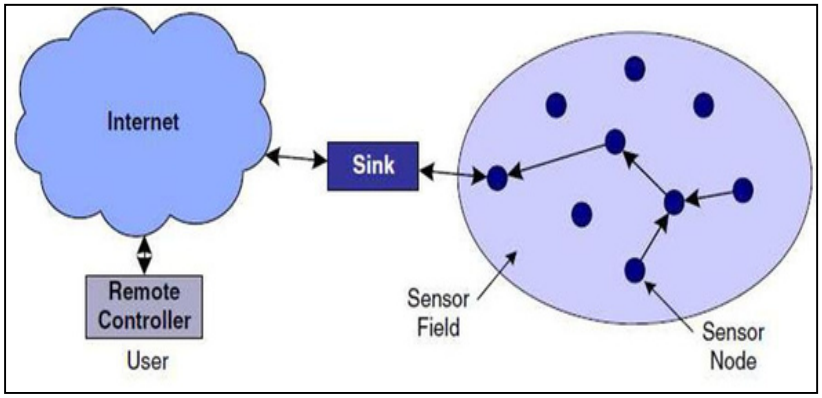

Fig.1 Architecture of a typical WSN [1]

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 [1].

The main components of sensor node consist of a sensing unit, a processing unit, a transceiver and a power unit as shown in the Figure 2. Sensing unit senses the physical quantity which is then transformed into digital one through ADC i.e. Analog to Digital converter. Thereafter processor is used for further computations and transceiver is used to transmit and receive data from the other nodes or from the Base Station. Power unit is the most prominent unit in any sensor node. Once the battery is exhausted, it can't be replaced for unattended applications. Other units are application dependent unit like Mobilizer, Power Generator and Location Finding System.

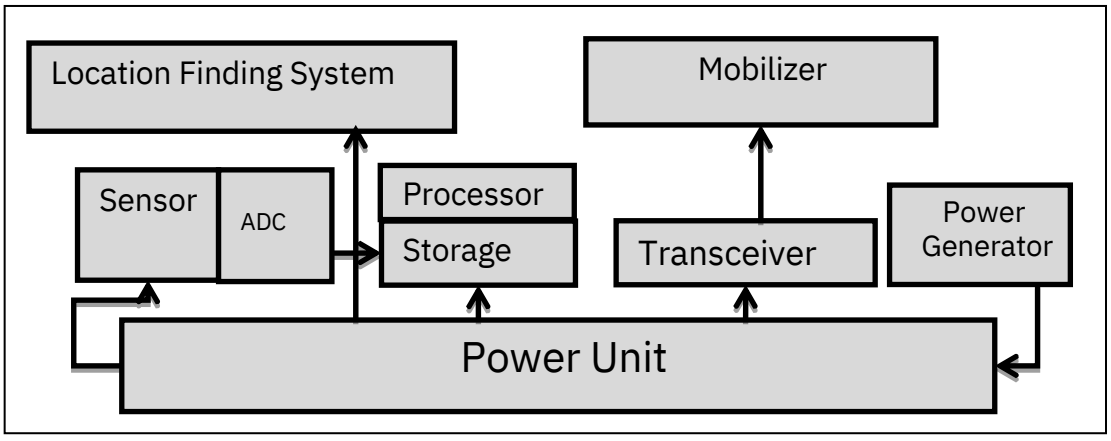

Fig. 2 Components of a sensor node

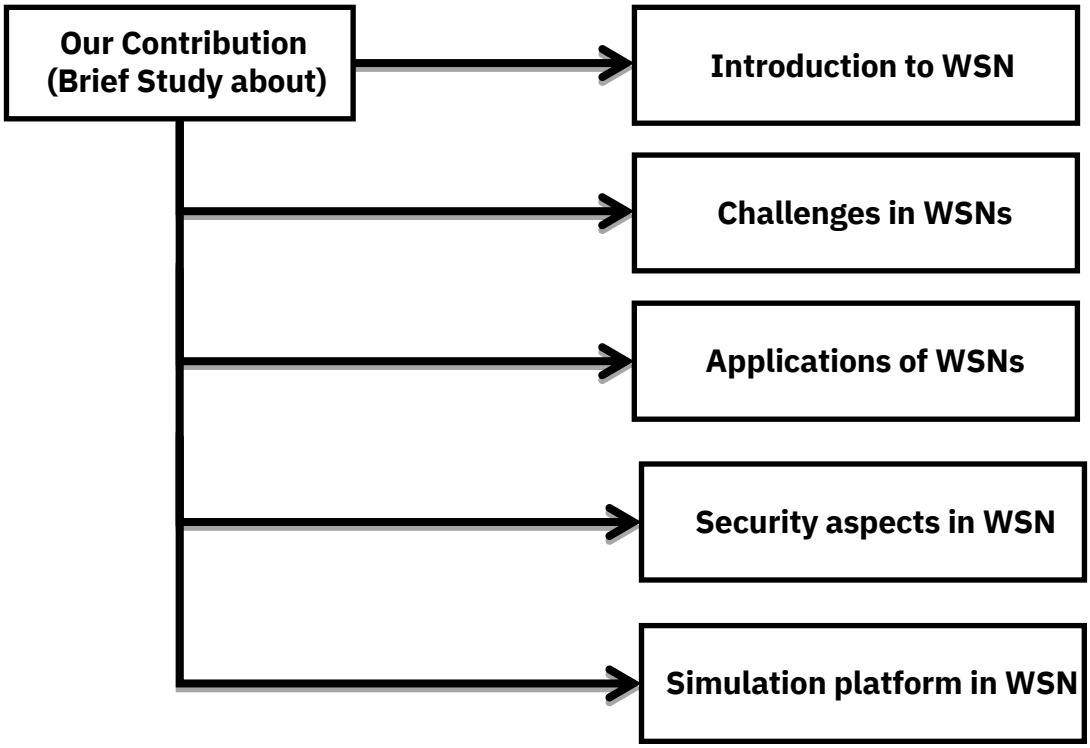

Fig.3 Contribution demonstration

2. CHALLENGES IN WSNs

Oneof the main design goals of WSNs is to carry out data communication while trying to prolong the lifetime ofthe 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 beovercome before efficient communication can be achieved in WSNs. In the following, we summarize someof the challenges and design issues that affect the topology construction and maintenance in WSNs [2].

a. 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.

b. 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.

c. 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

 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, and then switch off to conserve energy.

d. 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.

e. 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.

f. 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.

g. 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.

3. APPLICATIONS OF WSN

Wireless Sensor Networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, 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:

a. Military applications:
b. Environmental applications:
c. Healthcare applications:
d. Home applications:
e. Traffic control:

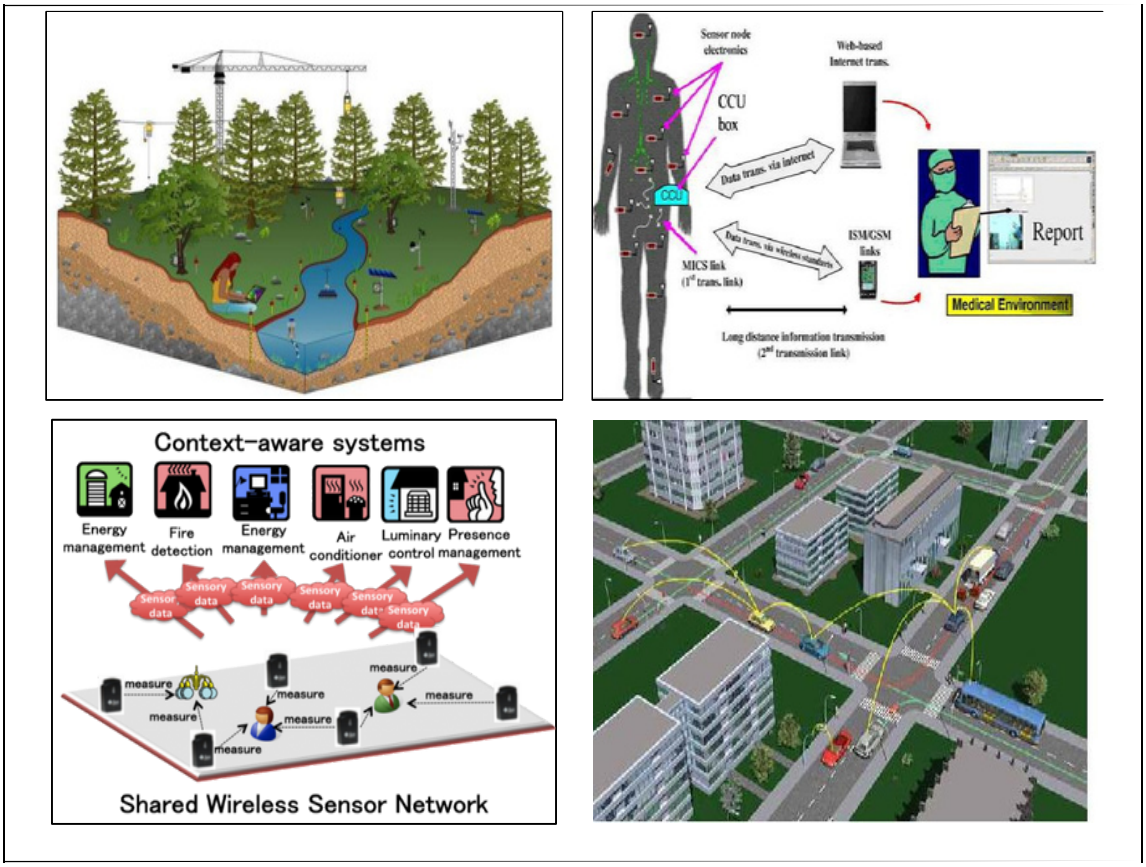

Fig. 4 Applications of WSN [3]

4. SECURITY ASPECTS OF WSN

The popularity of WSN has been tremendously on a peak with respect to different applications like climate change, environmental monitoring, traffic monitoring and home automation. Therefore keeping the WSN has always been a challenging task. Cryptography provides security through symmetric key techniques, asymmetric key techniques and hash function. Since WSN are very constrained in terms of computing, communication and battery power, it requires a light weight cryptographic algorithm. Due to constraints of sensor nodes, the selection of cryptographic technique is vital in WSN. Cryptography in WSN can be explained in the following three aspects: symmetric, asymmetric and hash function [4].

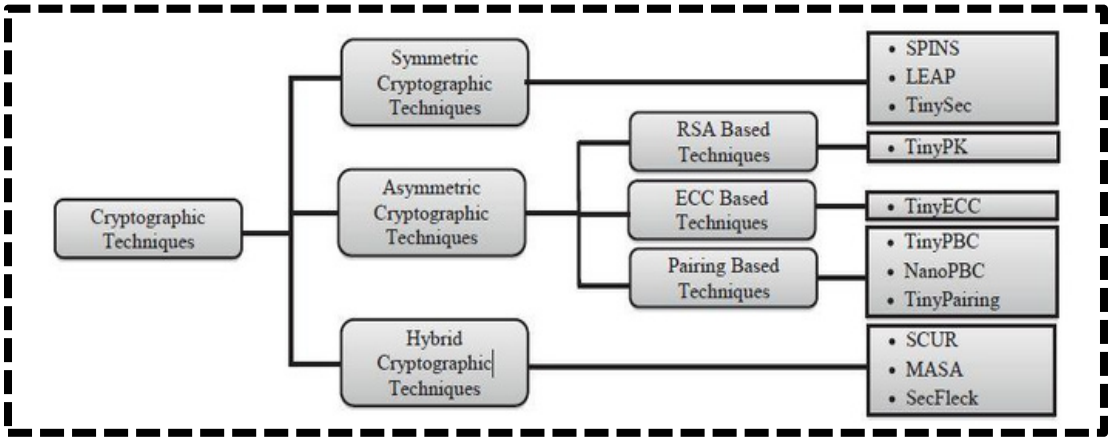

Fig.5 Security in WSN [4]

5. SIMULATION PLATFORM IN WSN

In WSNs, simulation is one of the most predominant evaluation methodologies for the development of new communication architectures, and network protocols as well as to test and validate the existing one in various scenarios. Simulation helps researchers to get significant information on feasibility and practicability crucial to the implementation of the system prior to investing significant time and money. In WSNs, simulation based testing and validation has many advantages, such as: ease of implementation, lower cost, flexibility and possibility of testing large-scale networks. The availability of a large number of simulation tools and specific requirement (e.g. energy-constraints, large-scale deployment) of WSNs makes it difficult for a user to choose a suitable tool for his evaluation. To address this issue, we have presented [] some of the most widely-used and state-of-the-art simulation tools for WSNs. The aim is to help researchers in the selection of an appropriate simulation tool to evaluate their work, and to acquire reliable results for large-scale WSNs [5].

Table 1: Comparison table of the reviewed simulation tools

Tools Features	Interface	Accessibility & User Support	Availability of WSNs Modules	Scalability
NS-2	C++/OTcl with limited visual support	Open source with Good user support	Excellent	Limited
OMNeT++	C++/NED with good GUI and debugging support	Free for academic use, licence for commercial use with Good user support	Excellent	Large-scale
GloMoSim	Parsec (C-Based) with limited visual support	Open source with Poor user support	Good	Large-scale

OPNET	C or C++/Java with Excellent GUI and debugging support	Free for academic use, licence for commercial use with Excellent user support	Excellent	Moderate
SENSE	C++ with good GUI support	Open source with Poor user support	Excellent	Large-scale
TOSSIM	C++/Python with good GUI support	Open source (BSD) with Excellent user support	Good	Large-scale
GTSNetS	C++ with good user interface & visual support	Open source with good user support	Excellent	Very Large-scale

6. CONCLUSION WSNs have been profoundly used in various sectors of human life. The sensing technology has made it possible for any sensor node to communicate and respond to the different attributes. This paper has briefed about various aspects in WSN. With the brief introduction to the WSN, the special issues have been discussed. Applications have been highlighted along with the security aspects in WSN. Thereafter the tabular comparison of different simulation software's has been given. It can be concluded from the study done in this paper, that WSN has revolutionized almost every sector of modern era. It has huge scope of research in handling different aspects of human life.

REFERENCES

[1] 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.

[2] Samira Kalantary, Sara Taghipour, " A Survey on architectures, protocols, applications and management in wireless Sensor Networks", Journal of Advanced Computer Science & Technoloy, pp. 1-11, 2014.

[3] KazemSohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks", Wiley Publications, Second Edition.

[4] Gaurav Sharma, SumanBala, Anil K. Verma, "Security Frameworks for Wireless Sensor Networks-Review," 2nd International Conference on Communication, Computing & Security [ICCCS-2012] , No. 6, pp. 978 – 987, 2012.

[5] Muhammad Zahid Khan et al. , "Limitations of Simulation Tools for Large-Scale Wireless Sensor Networks," Workshops of International Conference on Advanced Information Networking and Applications, pp. 820-825, 2011.