A Review on Wireless Sensor Network

R. Krithika, S. Nidhi, V. Sandhiya
Department of Computer Science, 2nd B.SC Computer Tecnology,
Sri Krishna Adhiya College of Arts and Science, Kovaiputhur Pirivu, Coimbatore, Tamil Nadu, India

ABSTRACT

If sensor networks are to attain their potential, security is one of the most important aspects to be taken care of. The need for security in military applications is obvious, but even more benign uses, such as home health monitoring, habitat monitoring and sub-surface exploration require confidentiality. WSNs are perfect for detecting environmental, biological, or chemical threats over large scale areas, but maliciously induced false alarms could completely negate value of the system. , habitat monitoring, and traffic control are presented. Technical challenges in sensor network development include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. The paper concludes by presenting some recent research results in sensor network algorithms, including localized algorithms and directed diffusion, distributed tracking in wireless ad hoc networks, and distributed classification using local agents.

Key words: *Wireless Sensor Networks, Security Protocols, Network Threats, querying and tasking, sensor networks, tracking and classification, wireless network.*

INTRODUCTION

Networked micro sensors technology is a key technology for the future. In September 1999, Business Week heralded it as one of the 21 most important technologies for the 21st century. Cheap, smart devices with multiple onboard sensors, networked through wireless links and the Internet and deployed in large numbers, provide unprecedented opportunities for instrumenting and controlling homes, cities, and the environment. In addition, networked micro sensors provide the technology for a broad spectrum of systems in the defense arena,

generating new capabilities for reconnaissance and surveillance as well as other tactical applications. Typical applications of sensors include emergency response information, energy management, medical monitoring, inventory control, and battlefield management. If sensor networks are to attain their potential, secure communication techniques must be developed in order to protect the system and its users.

1. HISTORY OF RESEARCH ABOUT SENSOR NETWORK:

To understand the tradeoffs in today's WSNs, it is helpful to briefly examine their history. Like many advanced technologies, the origin of WSNs can be seen in military and heavy industrial applications, far removed from the light industrial and consumer WSN applications that are prevalent today. The first wireless network that bore any real resemblance to a modern WSN is the Sound Surveillance System (SOSUS), developed by the United States Military in the 1950s to detect and track Soviet submarines. This network used submerged acoustic sensors – hydrophones – distributed in the Atlantic and Pacific oceans. This sensing technology is still in service today, albeit serving more peaceful functions of monitoring undersea wildlife and volcanic activity. Echoing the investments made in the 1960s and 1970s to develop the hardware for today's Internet, the United States Defense Advanced Research Projects Agency (DARPA) started the Distributed Sensor Network (DSN) program in 1980 to formally explore the challenges in implementing distributed/wireless sensor networks. With the birth of DSN and its progression into academia through partnering universities such as Carnegie Mellon University and the Massachusetts Institute of Technology Lincoln Labs, WSN technology soon found a home in

academia and civilian scientific research. Governments and universities eventually began using WSNs in applications such as air quality monitoring, forest fire detection, natural disaster prevention, weather stations and structural monitoring. Then as engineering students made their way into the corporate world of technology giants of the day, such as IBM and Bell Labs, they began promoting the use of WSNs in heavy industrial applications such as power distribution, waste-water treatment and specialized factory automation. While the market demand for WSNs was strong, moving beyond these limited applications proved to be a challenge. The military, science/technology and heavy industrial applications of previous decades were all based on bulky, expensive sensors and proprietary networking protocols. These WSNs placed a premium on functionality and performance, while other factors such as hardware and deployment costs, networking standards, power consumption and scalability fell to the wayside. The combination of high cost and low volume prevented the widespread adoption and deployment of WSNs into a broader range of applications.

TYPE OF WSN:
According to formerly research paintings completed five forms of WSN are feasible relying upon wherein and how sensors are installed up to monitor info. According to these properties of sensor deployment we are able to classify WSNs into five primary sorts namely; underground WSN, Ground (terrestrial) WSN, aquatic (underwater) WSN, and mobility WSNs.

A. Ground (Terrestrial) WSNs:
Usually include hundreds to thousands of cheap WSN deployed randomly in a given sensing region. Sensor nodes can be dropped from a randomly and plane located into the target region in ad hoc diffuse. In a ground (terrestrial) WSN, reliable communiqué in a dense atmosphere is very vital. Ground sensor nodes must be able to efficiently communicate info return to the BS. While battery power is constrained resource aid and its important constraint on network performance and its able to not be rechargeable or replaceable again, ground sensor nodes however can be well found with a secondary power source e.g. battery or solar cell. So due to this it is always important for sensor nodes to conserve energy.

B. Underground WSNs
Underground WSNs are sequence of few of the sensor nodes located inside the earth crust or in a cave or in a mine and they may be utilized to monitor underground activities together with volcanic situations and many others. Extra sink or BS nodes are positioned above crust of earth to transmit info from the sensor nodes to the BS .These kind of WSN are a entire. More high priced than a ground (terrestrial) WSN in phases of equipment, maintenance and deployment.

Underground sensor nodes are extra high priced because vital device parts ought to be decided on to ensure reliable communiqué thru soil, water, rocks, and other contents residing internal crust. The inside circumstances atmosphere create wirelessly communiqué a challenge because of highest levels of signal losses and attenuation.

C. Aquatic (Underwater) WSNs :
Aquatic WSNs comprise of few of sensor nodes and vehicles diffuse under water. As opposite to ground WSNs, aquatic sensor nodes are more high-priced and lesser sensor nodes are diffuse in sensing area. Self-directed aquatic vehicles are utilized for collecting or exploration data from sensor nodes. As in evaluation to a dense diffuse of sensor nodes in a ground WSN, a sparse diffuse of sensor nodes is located at sea level. Typical aquatic (underwater) wirelessly communications are implemented through transmission of acoustic waves.

D. Multi-media WSNs:
Multi-media WSNs are mixture of a no. of lowest price sensor nodes well-appointed with microphones and cameras. These sensor nodes interconnected with every different over a wirelessly connection for data sensing, records processing, statistics correlation, and records compression. Multi-media WSNs are utilized to allow monitoring of events inside the shape of multimedia programs.

E. Mobile WSNs:
Mobility WSNs are a no. of transferring sensor with their interplay with sensing atmosphere. Moving sensor nodes have the potential to compute, like non-moving nodes. Mobility WSNs are utilized in military and other industrial applications].

SENSOR LOCATION AWARE SERVICES:

1. Smart Home/Smart Office :

Smart home environments can provide custom behaviors for a given individual. Considerable amount of research has been devoted to this topic. The research on smart homes is now starting to make its way into the market. It takes a considerable amount of work and planning to create a smart home. There are many examples of products currently on the market which can perform individual functions that are considered to be part of a smart home. Several useful applications which take advantage of information collected by WSN are presented by Hussain et al. (2009).

2. Lilitary:

New and emerging technologies, such as networks, support military operations by delivering critical information rapidly and dependably to the right individual or organization at the right time. This improves the efficiency of combat operations. The new technologies must be integrated quickly into a comprehensive architecture to meet the requirements of present time. Improvement in situation awareness (Chien Chung Shen, 2001) is must requirement. Doumit and Agrawal (2002) described some other important application is detection of enemy units' movements on land/sea, sensing intruders on bases, chemical/biological threats and offering logistics in urban warfare. Command, control, communications, computing, intelligence, surveillance, reconnaissance, and targeting systems are well described by Akyildiz (2002).

3. Industrial & Commercial:

Since the long time wireless transmission of data is being done in industrial applications, but recently it has gained importance. Successful use of wireless sensors in systems such as supervisory control and data acquisition has proved that these devices could effectively address the needs of industrial applications. The critical process applications of WSNs in industry are monitoring temperature, flow level, and pressure parameters. With the rapidly increasing technological advances in wireless technology and its subsequently decreasing prices, numerous wireless applications are being developed in industry. WSN in manufacturing industries can monitor and optimize quality control.

4. Traffic Management and Monitoring:

Every big city is suffering from traffic congestion around the world. A sincere effort is being made to solve the traffic congestion. Congestion can be alleviated by planning managing traffic. A real time automatic traffic data collection must be employed for efficient management of rush hour traffic. Research on this topic is considered as part of the Intelligent Transport System (ITS) research community. Chinrungrueng (2006) explained ITS to be the application of the computers, communications, and sensor technology to surface transportation. The vehicle tracking application is to locate a specific vehicle or moving object and monitor its movement. This work also describes design of WSN for vehicular monitoring. As the power source (battery) is limited, it is important that a design of sensor node is power efficient.

5. Structural Healthcare:

Structures are inspected at regular time intervals, and repairing or replacing based on the time of use, rather than on their working conditions. Tiwari et al. (2004) has explained that sensors embedded into structures enable condition based maintenance of these assets. Wireless sensing will allow assets to be inspected when the sensors indicate that there may be a problem. This will reduce the cost of maintenance and preventing harmful failure. These applications include sensors mounted on heavy duty bridges, within concrete and composite materials (Arms et al. 2001), and big buildings.

6. Agriculture:

Wang and Wang (2006) stated that agriculture can also be benefited by the deployment of WSN to get the information regarding soil degradation and water scarcity. With help of WSNs we can check the clean water consumed in irrigation and manage it.

1.2. Topology and Coverage Control:

Topology control is one of the fundamental problems in WSNs. It has great importance for prolong lifetime, reducing radio interference, increasing the efficiency of media access control protocols and routing protocols. It also ensures the quality of connectivity & coverage and increase in the network service as well. A significant progress in research can be seen in WSNs topology control. Many topology control algorithms have been developed till date, but problems such as lack of definite and practical algorithm, lack of efficient measurement of network performance and idealness of mathematical model still exist. Several graph models used in topology control, the present hot spots and the future trends on the research of topology control are presented by Jardosh and Ranjan (2008).

1.3. Quality of Service (QoS) Provision:

QoS support is challenging due to severe energy and computational resource constrains of wireless sensors. Various service properties such as the delay, reliability, network lifetime, and quality of data may conflict; for example, multipath routing can improve the reliability; however it can increase the energy consumption and delay due to duplicate transmissions. Modeling such relationships, measuring the provided quality, and providing means to control the balance is essential for QoS support. There are various research opportunities in enhancing the QoS of WSNs. One of the researches is the project described by Abidin (2009) that analyzes and enhances the performance of a WSN by deploying a simple max min fairness bandwidth allocation technique.

1.4. Mobility management:

Mobility is one of the most important issues in next generation networks. As WSNs are becoming the next elements of the future Internet, it is crucial to study new models that also support mobility of these nodes. WSNs are applicable in variety of cases that make it difficult to produce a standard mobility scenario. Following are some cases where the mobile support is necessary presented in Camilo (2008). Intra WSN device movement is probably the most common scenario in WSNs architectures, where each sensor node has the ability to change from its local position at run time without losing the connectivity with the sensor router (SR). In the case of inter WSN device movement, sensor nodes move between different sensor networks, each one with its SR responsible to configure and manage all the aggregated devices. A research project of IETF working group NEMO, an example of WSN movement is described in RFC3963 by Devarapalli (2005). Sensor network deployed in a moving bus is a real scenario of this type. It is possible to have a scenario where a sensor network can use another sensor network in order to be connected through Internet. MANEMO (Wakikawa et al., 2007) project is also an example.

1.5. Security and Privacy Concern:

The field that paid less attention is the privacy concern on information being collected, transmitted, and analyzed in a WSN. Such private information of concern may include payload data collected by sensors and transmitted through the network to a centralized data processing server. The location of a sensor initiating data communication, and other such context information, may also be the focus of privacy concerns. In real world applications of WSNs, effective countermeasures against the disclosure of both data and context oriented private information are indispensable prerequisites. Privacy protection in various fields related to WSNs, such as wired and wireless networking, databases and data mining, has been extensively studied by Li and Das (2009). Effective privacy preserving techniques are needed for the unique challenges of WSN security.

1.6. Biomedical/Medical:

The uses of WSNs in biomedical and medical are in growing phase. Biomedical wireless sensor networks (BWSNs) show the future opportunities for supporting mobility while monitoring vital body functions in hospital and home care.

REFERENCE:

1. N. M. Nair, J. S. Terence, "Survey On Distributed Data Storage Schemes In Wireless Sensor Networks", Indian Journal of Computer Science and Engineering (IJCSE), Vol.4, No.6, pp.1-6, 2014.

2. Communication Engineering, Vol.4, Issue.4, pp.289-295, 2015.

3. Jaydip Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security, Vol.1, No.2, pp.1-16, 2009.

4. Xiaoliang Menga, Xiaochuan Shia, Zi Wangb, Shuang Wua, Chenglin Lia, "A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters", Elsevier, Vol.51, NO.11, pp.47–61, 2016.

5. Hacene fouchal, javier biesa, elena romero, alvaro araujo, octavio nieto taladrez, "a security scheme for wireless sensor networks", 2016 IEEE Global Communications Conference (GLOBECOM), Washington, pp.1-5,2016.

6. Gagandeep Kaur, Deepali, Rekha Kalra, "Improvement and analys security of WSN from passive attack", 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, pp.420-425, 2016.