Wireless Sensor Network: An Overview

Usha Soni[1], Anjali Namdev[2]

[1]M. Tech. student,Somany Institute of Tech. and Mgt., Rewari
[2]HOD(CSE Deptt.), Somany Institute of Tech. and Mgt., Rewari

Abstract: **Wireless sensor network is emerging field due to its lots of applications. It is wireless which consists of wireless nodes with sensing capabilities. They are made of four basic components of sensing, power, computation, and communication. It has potential use in applications like Military, Environmental, Health (Scanning), Space Exploration, Vehicular Movement, Mechanical stress levels on attached objects, disaster management, combat field reconnaissance etc. Due to various design issues a lot of protocols for power saving and routing are proposed. But there are various constraints like limited energy, communication capability; storage and bandwidth with sensor nodes network. Various characteristics of sensor networks like flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment make many new and exciting application areas for remote sensing. This paper is based on various aspects of routing protocols in wireless sensor networks. We give an overview of wireless sensor networks and their application domains including the challenges that should be deal with for the development of this technology further.**

Keywords: **WSN, Sensor nodes, Routing, Ad hoc networks**

I. INTRODUCTION

In the architecture SNs are grouped into clusters controlled by a single command node. Sensors are only capable of radio-based short-haul communication and are responsible for probing the environment to detect a target/event. Every cluster has a gateway node that manages sensors in the cluster. Clusters can be formed based on many criteria such as communication range, number and type of sensors and geographical location. Sensors receive commands from and send readings to its gateway node, which processes these readings. Gateways can track events or targets using readings from sensors in any clusters as deemed by the command node. However, sensors that belong to a particular cluster are only accessible via the gateway of that cluster. Therefore, a gateway should be able to route sensor data to other gateways. Gateway nodes interface the command node with the sensor network via long haul communication links. The gateway node sends to the command node reports generated through fusion of sensor readings, e.g. tracks of detected targets. The command node presents these reports to the user and performs system-level fusion of the collected reports for overall situation awareness.[1]

A SN also called mote is a node in WSN that is capable of performing some processing, gathering sensory information and communicating with other connected nodes. Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. The sensing electronics measure ambient condition related to the environment surrounding the sensor and transforms them into an electric signal [4]. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. A large number of these disposable sensors can be networked in many applications that require unattended operations. A WSN contains hundreds or thousands of these SNs. the command node reports generated through fusion of sensor readings, e.g. tracks of detected targets .These sensors have the ability to communicate either among each other or directly to an external Base-Station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy. Each individual node is comprised of one or more sensing devices, a processor, a communication unit, and a power supply [3, 4].It shows the communication architecture of a WSN. SNs are usually scattered in a sensor field, which is an area where the SNs are deployed. SNs coordinate among themselves to produce high-quality information about the physical environment. Each SN bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources. Each of these scattered SNs has the capability to collect and route data either to other sensors or back to an external BS. A BS may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data [6,7].

II. CHARACTERISTICS OF WSN

Due to a lack of infrastructure, SNs need to cooperate with each other so as to maintain life and secure information. Each SN not only acts as a host, but also as a router for data forwarding. Each SN has limited power, memory storage, data processing capacity and radio transmission range [4,5]. Generally, a WSN has the following characteristics:

Ad hoc Deployment SNs are spread randomly and hence they do not fit into any regular topology. Once distributed, they usually do not require any human intervention. Hence, the setup and maintenance of the network should be entirely independent and the network should be self-reconfigurable.

Dynamic Network Topology SNs may run out because of limited power or new nodes may be added to the network. Hence, the network connectivity changes with time, resulting in dynamically changing network topology.

Energy Constrained Operation An important bottleneck in the operation of SNs is the available energy. Sensors usually rely on their battery for power, which in many cases cannot be recharged or replaced. Hence, the available energy at the nodes should be considered as a major constraint while designing protocols as well as computational complexity and storage. For instance, it is desirable to give the user an option to trade off network lifetime for fault tolerance or accuracy of results.

Unattended Operation WSNs are usually spread in a hostile environment, and operating in an unattended mode. SNs are spread randomly and hence they do not fit into any regular topology. Once distributed, they usually do not require any human intervention. Hence, the setup and maintenance of the network should be entirely independent and the network should be self-reconfigurable.

Infrastructure-less WSNs are primarily infrastructure-less. There is no central authority to monitor SNs. Therefore, all routing and maintenance algorithms need to be distributed. Sometimes this property becomes main drawback in operation of SN. Due to these property SNs needs to be self-organizing and self-maintaining.

Shared Bandwidth The radio channel in a WSN is broadcast in nature and is shared by all the nodes within its direct transmission range. So, a malicious node could easily obtain access to the data being transmitted in the network.

Large Scale of Deployment A WSN is a large-scale network, in which thousands of sensors are arbitrarily spread to track surrounding environment or monitor a particular object.

III. APPLICATION OF WSN

WSN applications can be classified into two categories: monitoring and tracking. Monitoring applications include indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans, and vehicles. While there are many different applications, below we describe a few example applications that have been deployed and tested in the real environment. In all of applications, it is mandatory to maintain the integrity and the correct operation of the deployed network. Therefore, the security in WSNs becomes an important and a challenging design task.

- Area Monitoring
- Greenhouse Monitoring
- Air Pollution Monitoring
- Forest Fires Detection
- Machine Health Monitoring
- Landslide Detection[3]
- Water/Waste-Water Monitoring
- Health Applications
- Agriculture
- Structural Monitoring

IV. CHALLENGES IN WSN

A sensor node, also known as a mote is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. Sensor nodes are small in size, low power, low cost. Despite plethora of applications of WSN, these networks have several restrictions e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSN is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. In order to design an efficient routing protocol, several challenging factors should be addressed meticulously. The following factors are discussed below:

Node deployment: Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. Hence, random deployment raises several issues as coverage, optimal clustering etc. which need to be addressed.

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. In a multi hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Node/Link Heterogeneity: Some applications of sensor networks might require a diverse mixture of sensor nodes with different types and capabilities to be deployed. Data from different sensors, can be generated at different rates, network can follow different data reporting models and can be subjected to different quality of service constraints. Such a heterogeneous environment makes routing more complex.

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 routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

Scalability: The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols 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.

Network Dynamics: Most of the network architectures assume that sensor nodes are stationary. How-ever, mobility of both BS‘s and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, besides energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

Transmission Media: In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. As the transmission energy varies directly with the square of distance therefore a multi-hop network is suitable for conserving energy. But a multi-hop network raises several issues regarding topology management and media access control. One approach of MAC design for sensor networks is to use CSMA-CA based protocols of IEEE 802.15.4 that conserve more energy compared to contention based protocols like CSMA (e.g. IEEE 802.11).

Coverage: The coverage of a WSN node means either sensing coverage or communication coverage. Typically with radio communications, the communication coverage is significantly larger than sensing coverage. For applications, the sensing coverage defines how to reliably guarantee that an event can be detected. The coverage of a network is either sparse, if only parts of the area of interest are covered or dense when the area is almost completely covered. In case of a redundant coverage, multiple sensor nodes are in the same area.

Data Aggregation: Sensor nodes usually generate significant redundant data. So, to reduce the number of transmission, similar packets from multiple nodes can be aggregated. Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. It is incorporated in routing protocols to reduce the amount of data coming from various sources and thus to achieve energy efficiency. But it adds to the complexity and makes the incorporation of security techniques in the protocol nearly impossible.

Data Reporting Model: Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. In wireless sensor networks data reporting can be continuous, query-driven or event-driven. The data-delivery model affects the design of network layer, e.g., continuous data reporting generates a huge amount of data therefore, the routing protocol should be aware of data-aggregation .

Quality of Service: In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

Routing: Multi hop routing is a critical service required for WSN. Because of this, there has been a large amount of work on this topic. Internet and MANET routing techniques do not perform well in WSN. Internet routing assumes highly reliable wired connections so packet errors are rare; this is not true in WSN. Many MANET routing solutions depend on symmetric links (i.e., if node A can reliably reach node B, then B can reach A) between neighbors; this is too often not true for WSN. These differences have necessitated the invention and deployment of new solutions. For WSN, which are often deployed in an ad hoc fashion, routing typically begins with neighbor discovery. Nodes send rounds of messages (packets) and build local neighbor tables. These tables include the minimum information of each neighbor's ID and location. This means that nodes must know their geographic location prior to neighbor discovery. Other typical information in these tables include nodes' remaining energy, delay via that node, and an estimate of link quality.

Security: Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.[7]

V. CLASSIFICATION OF WIRELESS SENSOR NETWORK

A simple classification of Wireless sensor networks based on their mode of functioning and the type of target application is given below.

Proactive Networks The nodes in this sort of network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Hence, they collect the data for the relevant parameters at regular intervals. They are well suited for applications requiring periodic data monitoring. Some known instances or protocols of this kind are the LEACH (Low Energy Adaptive Clustering Hierarchy) protocol [9], some improvements on LEACH such as [6] and PEGASIS (Power-efficient gathering in sensor information systems)[11].

Reactive Networks The nodes of the networks according to this scheme react immediately to sudden and drastic changes in the value of a sensed attribute. They are well suited for time critical applications. Typical instances of this sort of networks are [8,10].

Hybrid Networks The nodes in such a network not only react to time-critical situations, but also give an overall picture of the network at periodic intervals in a very energy efficient manner. Such a network enables the user to request past, present and future data from the network in the form of historical, one-time and persistent queries respectively. Such kind of network takes advantages of Proactive and Reactive networks. Some instances of this kind of networks are [11, 12, 13].

VI. CONCLUSION

Wireless Sensor Network is a wide field of study. A lot of scope exist in the advancement and study of wireless sensor network since the various issues like energy saving, congestion, data loss and routing issues are not solved completely till now. Congestion cause a lot of packet loss in the network and hence failing the protocol which otherwise is very energy efficient. Many techniques which includes machine learning algorithm have been introduced in recent years but still there is a gap for improvement in packet delivery and energy consumption in WSN.

VII. REFERENCES

[1]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, August 2002.

[2]. Marcos August M. Vieira, Claudionor N. Coelho Jr., DigenesCecilio da Silva Junior, and Jose M. da Mata, "Survey on Wireless Sensor Network Devices",in proceedings of the ETFA '03 IEEE Conference on Emerging Technologies and Factory Automation, vol. 1, pp. 537 – 544, September 2003.

[3]. S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Labelled data collection for anomaly detection in wireless sensor networks," in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Sixth International Conference on, pp. 269 –274, December. 2010.

[4]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", Computer Networks, vol. 38, no. 4, pp. 393-422, March 2002.

[5]. T. Kavitha, A. Chandra, "Wireless networks: a comparison and classification based on outlier detection methods "in CSEA 2012, vol. 4, special issue 1; 2013.

[6]. Ihsan A. , Saghar K. , Fatima T. "Analysis of LEACH protocol(s) using formal verification" Applied Sciences and Technology (IBCAST), 254 – 262, 13-17 Jan. 2015

[7]. Ioan Raicu ,"Routing Algorithms for Wireless Sensor Networks", IEEE Wireless Communications, vol.46, pp.110-119,Sept.2002.

[8]. Leonardo B. Oliveira, Adrian Ferreira , Marco A. Vilaça , Hao Chi Wong , Marshall Bern , Ricardo Dahab , Antonio A.F. Loureiro "SecLEACH—On the security of clustered sensor networks" ELEVIER Volume 87, Issue 12, Pages 2882–2895 December 2007

[9]. Sudhanshu Tyagi , Neeraj Kumar "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks" Journal of Network and Computer Applications Volume 36, Issue 2, Pages 623–645, March 2013

[10]. Do-Seong Kim , Yeong-Jee Chung "Self-Organization Routing Protocol Supporting Mobile Nodes for Wireless Sensor Network" Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on Volume:2 , 622 – 626, 20-24 June 2006.

[11]. S.d. Muruganathan, D.C.F. Ma, A. Fapojuwo "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks" IEEE Radio Communications,s8-s13, March 2005

[12]. Arati Manjeshwar , Dharma P. Agrawal "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks (2001) " IPDPS Workshops,2001

[13]. Nitin Mittal, Davinder Pal Singh, Amanjeet Panghal, R.S. Chauhan "improved leach communication protocol for wsn" National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010

[14]. Jamal N Al-Karaki , Ahmed E Kamal "Routing techniques in wireless sensor networks: a survey" IEEE Wireless communications volume11, pages6-28,2004