Proc. of Int. Conf. on *Recent Trends in Information, Telecommunication and Computing, ITC*

Wireless Sensor Networks-A Survey

Pooja Chaturvedi[1] and A. K. Daniel [2],
[1] M. M. M. University of Technology, Gorakhpur, India
Email: chaturvedi.pooja03@gmail.com
[2] M. M. M. University of Technology, Gorakhpur, India
Email: danielak@rediffmail.com

***Abstract*— Wireless Sensor networks are dense networks, which consist of small low cost sensors having severely constrained computational and energy resources, which operate in an adhoc environment. Sensor network combines the aspects of distributed sensing, computing and communication. Despite the numerous applications of sensor networks in various fields there are various issues which need to be explored and resolved such as resource constraints, routing, coverage, security, information collection and gathering etc. In this paper we aim to provide the detailed overview of the wireless sensor technologies and issues related to them, such as advancement of sensor technology, architecture, applications, issues and the work done in the field of routing, coverage and security.**

***Index Terms*— Wireless sensor networks, routing, security, information collection**

I. INTRODUCTION

It is possible to deploy large scale wireless sensor networks due to the recent developments in semiconductor, networking and material science technologies. These advancements provide the facility to design sensor networks which can be manufactured and maintained at significantly low costs and efforts as compared to the earlier technologies. Sensor network is an infrastructure comprised of sensing (measuring), computing and communication elements that gives an administrator the ability to instrument, observe and react to events and phenomena in a specified environment [1]. The main aim of deploying these nodes is to sense or track the problem domain and gather and transmit that information to a limited number of base stations which are known as sinks. These sensor nodes and sink can be either stationary or mobile. The deployed sensor nodes posses some characteristics based on the initial distribution and the energy models adopted. Wireless sensor technology can be understood by examining the various aspects of sensor networks. In section 2 we will discuss the brief evolution of sensor networks. In section 3 we will describe the various design considerations for the sensor networks. In section 4 we will describe the work done so far regarding these issue and challenges. Section 5 describes the conclusion and future scope of the wireless sensor networks.

II. EVOLUTION OF SENSOR NETWORKS

Wireless sensor networks also find their roots in the military applications and industrial applications like many other technologies. The first sensor network called Sound Surveillance system was developed by the United States military to detect and track the Soviet submarines in 1950s. The system consists of acoustic sensors which were submerged in the Atlantic and Pacific oceans.
To develop the hardware for today's internet United States Defense Advanced Research P rojects Agency

DOI: 02.ITC.2014.5.533

(DARPA) further extended the concept of sensor network for the distributed applications known as Distributed Sensor Network. Following this the sensor networks were also begin to be used in various monitoring and tracking system such as air quality monitoring, forest fire detection, natural disaster management, weather forecasting and structural monitoring. After these improvisations many corporate giants such as IBM and Bell labs started to use this technology in the heavy weight industrial applications such as power distribution, waste water treatment and specialized factory automation [1].

Several initiatives have been taken to enable the light weight industrial and commercial applications, such as [2]:

UCLA wireless Integrated Network Sensors (1993).

2. University of California at Berkeley PicRadio Program (1999).
3. Micro adaptive multi domain Power aware sensor program at MIT (2000).
4. NASA sensor Webs (2001).
5. Zigbee Alliance (2002).
6. Center for Embedded Network Sensing (2002).

A. Semiconductor Technology Advancements

The hardware implementation of sensor networks was based on the bulky and power consuming discrete circuits and multi-chip solutions earlier. The evolution of semiconductor had simplified the hardware implementation of the networks by providing the facility of designing a whole system on a single chip. These multipurpose control units have system on chip devices which comprised of general purpose control unit and a radio frequency transceiver in a single chip. The system on chip devices contains the high performance peripherals and non volatile memory to handle the application processing and protocol stack and also provides the RF links to the network.

B. Types of Sensors

The processing capabilities of the sensor networks depends on the types of the sensor nodes deployed. The sensor nodes can be of three types [2]:

Micro Electro Mechanical Systems: Gyroscopes, Accelerometers, Magnetometers, Pressure Sensors, Pyroelectric Effect Sensors, Acoustic Sensors.

CMOS-based sensors: CMOS based sensors are used for Temperature, Humidity, Capacitive proximity, Chemical composition.

LED sensors: LED sensors are used for ambient light sensing, proximity sensing, chemical composition.

The various functions of sensor nodes are as follows: i) Signal conditioning and data acquisition for different sensors, ii) temporary storage of the acquired data, iii) data processing, iv) analysis of the processed data for diagnosis and potentially alert generation, v) Self-monitoring (voltage supply), vi) scheduling and acquisition of the measurement tasks, vii) management of the sensor node configuration, viii) reception, transmission and forwarding of data packets, ix) coordination and management of communication and networking [5].

C. Types of Sensor Networks

The sensor networks can be of two types on the basis of the organization:

Structured Wireless sensor networks: In structured sensor networks few sensor nodes are deployed at specific locations, so the network management and maintenance costs are lower.

Unstructured Wireless Sensor Networks: In unstructured networks nodes are deployed densely in an adhoc manner. In unstructured networks the nodes are left unattended to perform the tracking and monitoring functions. The network maintenance such as managing connections and detection of failures is difficult in these networks is difficult because of the dense deployment of nodes.

The sensor networks can be of five types depending on the operating environment [3]:

Terrestrial WSNs: In terrestrial networks the nodes are deployed by dropping them from a plane in a given area randomly.

Underground WSNs: In underground wireless sensor networks the nodes are deployed in the underground areas such as caves or mines.

Underwater WSNs: The underwater networks are deployed to monitor or track the submarines of opponent countries for defense purposes.

Multimedia WSNs: Multimedia sensor networks are used for multimedia transmission such as video, audio and imaging.

Mobile WSNs: The mobile wireless sensor networks are deployed in the sensitive areas such as military surveillance and disaster affected areas. These sensor networks provide better coverage and connectivity than the static sensor networks.

D. Topology

Wireless sensor networks topology can be of four types: one way, bidirectional, star and mesh as shown in figure1 [3].

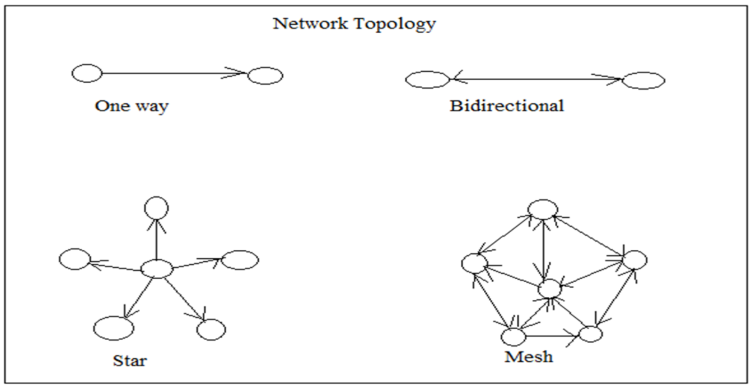

Figure1. Various topologies of sensor networks

E. System Architecture of sensor network

The sensor network consists of a number of sensor nodes, actuator, central unit, communication module and energy sources such as battery. The architecture of sensor network is shown in Figure2. Sensor node consists of a Sensor and Mote. Sensor is a device which is used to sense the information such as pressure, humidity, temperature, heartbeat etc. Sensor passes the sensed information to a small number of base stations known as sinks. For transmitting the information towards the base station sensors use the multi-hop mechanism. Mote is the processor unit of sensor network which consist of processor, memory, battery, an analog to digital converter to provide the connection to the sensor and a radio transmitter which is used to provide the adhoc connections. Sensor nodes have the self organizing capabilities to detect the presence of the sensor within the transmission range and connect them to form a network.

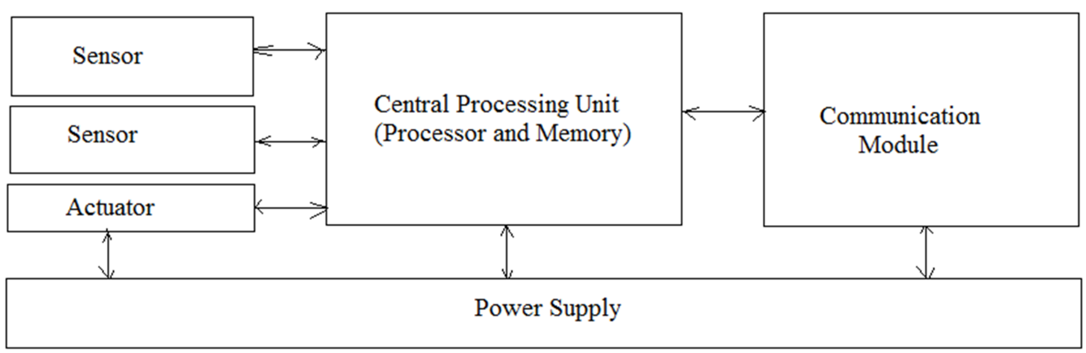

Figure2. System design of sensor network

F. Sensor Network Applications

WSN applications can be divided in two categories: Event Detection and Spatial Process Estimation. In the first case, the aim of deploying the sensor nodes is to detect and inform about an event to the sink nodes. The emphasis is on deploying the nodes with simple signal processing capabilities and to keep the number of sensor nodes to be sufficient to detect an event but they must avoid the false alarms. The examples of event detection applications are detection of fire in a forest or an earthquake. In spatial process estimation the main aim is to estimate a physical phenomenon which can be modeled as bi-dimensional random process. The entire behavior of the spatial process is estimated by receiving the samples from the sensor nodes which are deployed at the random locations.

WSN applications are divided into two categories as: Monitoring and Tracking. The various systems used for the purpose of monitoring and tracking are: PinPtr: an experimental counter-spiner system which is used to detect and locate the shooters, Macroscope of redwood: which is a case study of WSN that monitors and records the redwood trees in Sonoma, California, Semiconductor plant and oil tanker application: which is focused on preventive equipment maintenance using vibration signatures gathered by the sensors to detect the equipment failures, Underwater monitoring study developed a platform for underwater sensors to monitor the coral reefs and fisheries, MAX is a system which provides the facility for the people to search and locate the physical objects as per need, CenWits is a connection less sensor based tracking system which is worn by the people and offers them the facility to locate their current location, Cyclops is a camera device which bridges the gap between the computationally constrained sensor nodes and the complementary metal oxide semiconductor imagers, Volcanic monitoring WSNs can accelerate the process of deployment, installation and maintenance, various health monitoring systems such as Fireline: which is a wireless heart rate sensing system, Heart@Home system: which is a wireless heart rate monitoring and tracking system, LISTSENse enables the hearing impaired to be informed about the target audience, ZebraNet is a mobile wireless sensor network which is used to monitor and track the animal migrations [4].

Another application of sensor network is in the area of environmental monitoring. The environment monitoring tasks can be categorized in two types: indoor and outdoor applications. The communication standard used in wireless sensor networks is IEEE 802.15.4. The various implementations of the wireless sensor networks for the environment monitoring are: GreatDuckIsland: which was the first wireless sensor network developed to monitor the habitat in a particular region, Sonoma Dust is a WSN consisted of 120 Mica2 motes deployed to monitor the redwood trees in Sonoma, California, A WSN was deployed in central Ecuador, to monitor the volcanic eruptions at Tungurahua Volcano, Lofar agro project was deployed to monitor the microclimate in potato crops, SEACOAS project was developed at Scroby sands off the coast of Great Yarmouth to monitor the impact of the newly developed wind farm on coastal processes in the area. The paper also discusses about the challenges of the environment monitoring system, which are: power management, scalability, remote management, usability, standardization, mesh routing support, size and IP end to end connectivity [5].

Structural monitoring systems are of particular interest during forced vibration testing or natural excitation scenarios such as volcanic eruption, earthquakes, flooding etc.) The major advantage of structural monitoring system is that they reduce the complexity and cost of wired systems. In this paper the functional components of the structural monitoring systems are also presented which are: sensing interface: consist of analog to digital converter which converts the analog data into digital formats, Computing core: consist of microcontroller and memory, actuation interface: includes analog to digital converters to command active sensors and actuators with analog signals and wireless radio to transmit and receive data between other wireless sensors and data servers. The comparison of various hardware implementations of structural health monitoring systems are also discussed [6].

Structures such as bridge, dams, building and pipelines are designed to aid in the society's economic and industrial growth and progress. These structures are often prone to harsh loading conditions and severe environmental conditions which were not anticipated during the development. The earlier detection mechanism which can alarm of the deteriorating conditions can be of great significance in handling the disastrous situations efficiently. The wired setup can be very expensive and time consuming. The wireless sensor networks can be of great help for monitoring the condition of these structural entities [7].

III. Issues And Challenges

The various factors that affect the designing of WSN are as follows [3] [8] [9]:

1. Hardware and Operating System for WSN: The system design of sensor networks must emphasize on strategies to improve signal reception, design of low cost, less power sensors and processing units. The sensor nodes are designed such that the power consumption is optimized and simple modulation schemes must be kept simple. The operating system must provide memory management and resource management in a constrained environment.

2. Wireless Radio Communication Characteristics: The communication system designed for WSN must support low power consumption and adopt CMOS circuit optimized for sensor networks.

3. Medium Access Schemes: MAC mechanisms must be employed so as to reduce the collisions and power consumption.
4. Nodes Deployment: Node deployment strategies must consider the visibility and range of the sensor nodes. Antennas must be placed to detect the incorrect readings as soon as possible so as to reduce the latency and the congestion in the communication is reduced. Node deployment must also ensure the coverage of the problem domain in such a way such that there are no holes in the region. Holes are referred to as dark spots which witness the absence of sensor nodes. This problem usually occurs in the case of random deployment, in which some areas may be densely covered and some may be devoid of nodes.
5. Localization: Localization is another crucial issue and challenge in the field of wireless sensor networks. Localization refers to the process of determining the physical location of the sensor nodes after they have been deployed. Localization enables the development of energy efficient routing protocols. The localization algorithms must be precise and accurate enough to determine the node failures and losses as soon as possible. Localization is difficult in wireless sensor network because there is no global addressing mechanism.
6. Time synchronization: Time synchronization is necessary to achieve correct data collection at the sink after the process of data aggregation. The higher the accuracy between the transmission and reception, the more resources will be required. So we need to have trade-off between the synchronization accuracy and resource requirements according to the application. Various synchronization protocols are Reference Broadcast synchronization (RBS) and Delay measurement time synchronization protocol.
7. Calibration: Calibration is the process of transforming the collected sensor readings into the corrected values by comparing them to the previous stored values. It is difficult task in sensor networks due to the heterogeneity of sensor nodes as they are dependent on the application.
8. Network Layer: Network layer is concerned with the identification of the routes which provide energy efficient transmission. The routing protocols developed for communication must handle the heterogeneity of the nodes. The routing protocols must also address the data redundancy at the sink nodes so various aggregation mechanism must be incorporated.
9. Transport layer: Transport layer is basically responsible for the end to end transmission. End to end transmission is not possible for WSN as the position of the nodes is not predetermined. Pump Slowly, Fetch quickly is an example of transport layer protocol which is used in the wireless sensor network.
10. Data aggregation and Data Dissemination: Data aggregation is the technique applied at the sensor nodes to reduce the redundancy so as to provide energy efficient transmission. Data dissemination is the process through which the queries for the data are routed in the sensor network. It is a two step process: in the first phase nodes broadcasts the interest message regarding the data they need, to their neighbors. In the second step the nodes having the requested data sends the response to the source node. The objective of these mechanisms is to conserve the energy resources and to improve the latency and data accuracy, quality of service in terms of bandwidth utilization and end to end delay.
11. Privacy and Security: The wireless sensor network must be designed such that it may cope with the various kinds of attacks such as Gray hole, black hole and worm. Message integrity and user authentication is also a major challenge in wireless environment.

IV. Related Work

The basic aim of routing protocols is to determine the optimum path from source to the sink node. The optimum routing path is one which ensures the delivery of information to sink in cost and resource conserving manner. The aim of coverage maintenance is to deploy nodes in such a manner to ensure the desired coverage to every point in the target region. Security mechanisms are employed to fulfill the security requirements and overcome the various threats such as Dos attacks, black hole attacks etc. In this we aim to discuss the work done so far in the area of routing, sensor holes and wireless sensor network security.

A. Routing

Routing protocols can be broadly classified into two types: Network structure based and Protocol operation based. Network structure based protocols can be further classified as: Flat, Hierarchical and Location based routing. Various data centric protocols such as flooding and gossiping, SPIN Directed Diffusion has been proposed. The various hierarchical routing protocols have been developed which aim to minimize the energy consumption and hence increasing the network lifetime by using the clustering techniques. LEACH was the first hierarchical routing protocol. Various other hierarchical routing protocols have been proposed such as PEGASIS and hierarchical PEGASIS and so on [10].

In this survey we aim to discuss some energy aware routing protocols. A hierarchical energy aware protocol for routing and data aggregation (HEAP) is proposed which utilizes the subscribe and publish mechanism for forming a heap. The protocol consists of two parts: Hierarchical tree construction and restructuring the tree. The sink node broadcast an interest message to the neighboring node. These nodes further pass this interest message to their subsequent messages. Nodes which have the required data reply the sink following the optimal path and hence form a hierarchy. The node also maintains a parent list which is used in the case of the energy depletion or failure. In this the heap is restructured and hence the energy consumption is evenly distributed among the nodes. As the near-by nodes often tend to sense and transmit the redundant data an aggregation mechanism is also applied at the parent node. The aggregation is employed at the path closer to the sink so this mechanism reduces the number of control messages in the transmission. The efficiency of this algorithm is measured on the basis of following parameters as average dissipated energy, average delivery rate, lifetime of the network and average configuration time. On the basis of the simulation results authors have concluded that the HEAP algorithm outperforms the HPEQ protocol [11].

A regional energy efficient cluster heads based on maximum energy routing protocol for wireless sensor network (REECH- ME) uses static clustering by dividing the target region into a number of regions. It aims to improvise the localization and energy consumption compared to probabilistic LEACH. In this the target area is divided into 9 regions. Clusters in this protocol are formed on the basis of the received signal strength from the cluster head and its associate nodes. The node with the maximum energy is chosen as the cluster head for that particular round. The performance of this algorithm is compared with the LEACH on the basis of certain parameters such as confidence interval, network lifetime, throughput and the packet drop. The confidence interval refers to the deviation of the graphs from the mean value. From the simulation results it has been found that it outperforms the LEACH in terms of efficient energy utilization and the better coverage [12].

A modified version of energy aware routing protocol (EAP) is proposed as Low Loss Energy Aware Routing protocol (LLEAP) is proposed. EAP protocol consists of two phases; cluster formation phase and the CH tree construction phase. In the cluster formation phase nodes are assigned roles as candidate, plain or head. In the CHs tree construction phase the head nodes are assigned the responsibility for the formation of clusters. Although this algorithm is efficient in energy consumption as compared to the LEACH but it lacks the various QoS parameters such as packet loss, delay and throughput. A modified version of EAP is proposed as Low Loss energy aware routing protocol which considers these limitations. The limit on the balancing factor is proposed and a scheduling mechanism to mitigate the QoS requirements. The nodes follow a scheduling mechanism to determine when the nodes are awake or sleep. From the extensive simulation results the proposed LLEAP outperforms the LEACH and EAP in terms of end to end delay, packet loss and throughput [13].

A logical framework based routing protocol (LCR) eliminates the need of GPS for the localization of sensor node. In this approach several landmark nodes are selected and the position of all the sensor nodes is determined on the basis of those. Each node is assigned a logical coordinate vector. The landmark selection algorithm consists of three phases as: clustering, voting and landmark admission. In the clustering each node receives the self election beacon from the neighboring nodes. If the node does not receive a self-election message from other nodes then it sends the self-election message to all the other nodes. In the voting phase each node broadcast its hop count number according to which the node with the highest hop count number declares itself as landmark node. In the landmark admission the elected landmark nodes broadcast the other nodes about their hop count numbers. The performance of this algorithm is evaluated in terms of the packet delivery ratio, path optimality, protocol overhead and path length prediction. The results are compared with the GF and GPSR algorithm. On the basis of the comparison the LCR have been found more efficient than other protocols [14].

B. Sensor Hole

The occurrence of holes in the sensor networks is also a major problem, as it may degrade the network efficiency severely. Hole may be referred to as the communication void which act as an obstacle in the communication. Holes can be of four types: Routing Hole, Coverage Hole, Jamming Hole and Sink/Worm Hole. Routing hole occurs when the nodes present in the network cannot participate in the network operations, due to local minima problem as in Geographic forwarding routing. The coverage hole usually occurs in the case of the random deployment. In this there is not enough number of sensor nodes to cover the target region. In the jamming hole the target node may be equipped with the equipment which can jam the radio frequency signals. The sink hole occur when a malicious node deviate the nodes to transmit the data to the sink node. The worm hole occurs due to the malicious behavior of a node [15].

In this survey we aim to discuss the work in the field of coverage preservation and the coverage maintenance. Coverage can be defined from the information collection perspective. The field coverage is defined as how well a region of interest is monitored by sensors. In this authors have described a mobile sensor network architecture which consists of a number of sensor holes using the Gaussian-Markov Mobility and random walk approaches. In this paper the nodes deployment mechanism are used as grid distribution, random walk based distribution and the Gaussian Markov distribution of the nodes. The coverage is defined as the number of sensor nodes which come in the transmission range of the sink node over the time. The extensive simulations have been performed by varying the speed of the nodes and the transmission range between the sensor node and sink. The results demonstrate that the coverage is improved with the Gaussian-Markov mobility model [16].

There are two types of redundancies possible in the coverage determination as: sensing range and the communication range. It have proved that the communication range twice the sensing range is the sufficient condition and the tight lower bound to ensure that complete coverage preservation implies connectivity among active nodes if the original network topology is connected. The following assumptions are made in the network model: there may be a large number of sensor nodes in the network. However the number is always finite and two nodes are not at the same location. The authors have also extended the results for the k-coverage and k-connectivity. If every point in the target region is covered by atleast k sensor nodes then the region is said to be k-covered [17].

C. Security

Security is also a major challenge in the wireless environment. Various requirements for ensuring the security are confidentiality, authentication, message integrity and protection against eavesdropping. The performance of various cryptographic algorithms has been studied. Various block and stream ciphers energy consumption cost is computed by calculating the CPU cycles. On the basis of simulation results it has been found that light weight block cipher known as Byte- oriented substitution permutation network is more energy efficient than AES, RC4 and Sosemanuk and it also provides a good level of security [18].

A clean slate secure routing protocol is discussed. In this mechanism, the presence of the network authority is assumed which have a public and private key. All the nodes in the network are authenticated by the network with their id, network address and certificates. All the nodes are provided a network address by arranging them in a tree structure and assigning a network prefix based on their id. This protocol consists of two phases: in the first network is established by assigning the network address to each node and in the second phase the nodes are grouped according to their size. Smaller groups are merged and subsequently all the nodes belongs to a single group. The packets are forwarded by comparing each bit of network prefix. In this a mechanism based on grouping verification tree is used to authenticate the newly admitted node. To authenticate the root node the hash function of all the leaf nodes with the corresponding siblings are obtained. To authenticate the leaf nodes root performs the hash function of the node leading to the node to be authenticated [19].

A combined system is designed by using the two security mechanism of Kerberos and the Elliptical curve Menezes-Q-u-Vanstone (ECMQUV). The proposed system consists of three layers in which layer 1 are 1-hop that is node in the layer1 can communicate directly, layer2 uses 2-hop communication and layer3 is a 3-hop communication system. Layer 1 is considered as small network and light weight Kerberos is applied in this. Layer 2 and 3 are considered as large network and ECMQUV) is applied at these. The simulation results demonstrate the significance security achieved by using the combined system architecture [20].

V. CONCLUSION AND FUTURE SCOPE

In this survey we have discussed the wireless technology starting from its evolution, history, underlying technology considerations, various issue and challenges. We have also described the comprehensive work done so far in the field of WSN. Wireless sensor network is a hot area for researchers but there are still some challenges which need to be addressed and resolved. For example: there is still no mechanism to provide the global identification to the sensor nodes. Extensive research has been done so far with the assumptions that nodes are homogenous in terms of storage and communication capabilities. Further research may be done by deploying the heterogeneous nodes. Till now research has been carried out with single and stationary sink nodes. In future we can evaluate the performance of the network having multiple and mobile sink nodes.

Further research would be needed to address QoS of clustering routing, which mainly exists in real-time applications, such as battle-target tracking, emergent-event monitoring, and etc. Recently there is very little research focuses on handling QoS requirements in the resource-constrained WSN environment. Finally, with the increase of the network scale in WSNs, more redundant information is created and a certain degree of redundancy may be desirable for increasing reliability of the network. Thus, a trade-off between redundancy reduction and redundancy utilization is still an open question. In the hole problem various research have been done in the areas of detection, prevention and avoidance of holes, but very less work has been done in the area of repairing the holes. Logical and Semantic holes have been studied very less. Further research is needed to be done in the area of incorporating the security requirements which may facilitate the information collection. Various studies are needed to address the energy efficient MAC protocols. In the future, work can be carried out to integrate the wireless sensor networks with the internet. Extensive research is needed for the coverage preservation and connectivity maintenance in the field of heterogeneous sensor networks.

REFERENCES

[1] Kazem Sohraby, Daniel Minoli and Taieb Znati, "Wireless sensor networks- Technology, Protocols and applications", Wiley Interscience,A John Wiley & Sons Inc. Publications.

[2] "The evolution of sensor network", Silicon Inc. Rev 1.0.

[3] Gowrishankar .S, T. G. Basavaraju, Manjaiah D. H, Subir Kumar Sarkar, "Issues in Wireless Sensor Networks", Proceedings of the World Congress on the Engineering", 2008, Vol I,WCE 2008,July 2-8,2008,London, U.K.

[4] Jennifer Nick, Biswanath Mukherjee, Dipak Goshal, "Wireless Sensor Network Survey", Computer Network 52 (2008) 2292-2330.

[5] Chiara Buratti, Andrea Conti, Davide Dardari, Roberto Verdone,"An Overview of Wireless Sensor Networks Technology and Evolution", Sensors, ISSN 1424-8220.

[6] Luis M. L. Oliviera, Joel J. P. C. Rodrigues, "Wireless Sensor Networks: A survey on Environmental Monitoring", Journal of communications, Vol. 6, No. 2, April 2011.

[7] Jerome P. Lynch, Keneth J. Loh, "A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring", The Shock and Vibration Digest, Vol. 38, No. 2, March 2006, 91-128.

[8] I. F.Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A survey", Computer Networks 38 (2002), 393-422.

[9] Bhaskar Krishnamachari, "Wireless Sensor Networks", Tutorial presented at the Second International Conference on Intelligent Sensing and Processing (ICISP), Chennai, India, Jan 2005.

[10] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks".

[11] M. Moazeni, A. Vahdatpour, "HEAP: A hierarchical energy aware protocol for routing and aggregation in sensor networks", WICON Oct. 22-24, 2007, Austin, Texas, U. S. A.

[12] A. Haider, N. Javaid, N. Amjad, A. A. Awan, A. Khan, N. Khan, "REECH-ME: Regional Energy Efficient Cluster Heads based on Maximum Energy Routing Protocol For WSNs", arXiv:1307.7052v1 [cs.NI], 26 July 2013.

[13] Basma M. Mohammad El-Basioni, Sherine M. Abd El-Kader, Hussein S. Eissa, Mohammad M. Zahra, "An Optimized Energy Aware Routing Protocol for Wireless Sensor Networks", Egyptian Informatics Journal (2011) 12, 61-72.

[14] Q. Cao, T. Abdelzaher, "Scalable Logical Coordinates Framework for Routing in Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 2, No. 4, November 2006, Pages 557-593.

[15] Nadeem Ahmad, Salil S. Kanhere, Sanjay Jha, "The Hole Problem in Wireless Sensor Networks".

[16] Yueming Hu, Yueju Xue, Qing Li, Fangming Liu, Gabriel Y. Keung, Bo Li, "The Sink Node Placement and Performance Implication in Mobile Sensor Networks", Mobile Network Applications (2009) 14: 230-240.

[17] Di Tian, Nicolas D. Georganas, "Connectivity Maintenance and Coverage Preservation in Wireless Sensor Networks", Ad Hoc Networks 3 (2005) 744-761.

[18] Lingling Si, Zhigang Ji, Zhihui Wang, "The Application of Symmetric Key Cryptography Algorithms in Wireless Sensor Networks", 2012, International conference on Solid State Devices and Material Science, Physics, Procedia 25 (2012) 552-559.

[19] [19] Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig, "Secure Sensor Network Routing: A Clean Slate Approach", ACM 2006, 1-59593-456-1/06/2012.

[20] N. S. Fayed, E. M. Daydamoni, A. Atwan, "Efficient Combined Security System for Wireless Sensor Networks", Egyptian Informatics Journal (2012) 13, 185-190.