The main effective parameters on wireless sensor network performance

Samar Fakher[*], Mona Shokair[**], M.I. Moawad [**], and Karam Sharshar[*]

[*] Radiation Eng. Department, in NCRRT, Atomic Energy, Egypt.
[**] Electronics and Electrical Communications dept. Faculty of Electronic Engineering, Menufia University, Menouf, Egypt.

Abstract- Wireless Sensor Network (WSN) consists of a large number of sensor nodes to detect some physical phenomena. To design a WSN it is necessary to identify the major issues or the main metric parameters of WSN, which are network lifetime, data gathering, and security. These parameters effect on the overall performance of WSN. To enhance the performance of that network in this paper, we present a survey study of the methods and proposed algorithms that were used to overcome those issues. A number of challenges and research issues emerging from this survey study have been reported for further investigations.

Index Terms- WSN- network lifetime- data gathering- security

I. Introduction

WSN has come forth as an important new field in wireless communication. Due to recent advances in Micro-Electronic-Mechanical System (MEMS) and wireless communication technologies, sensors are deployed in a physical environment and communication through wireless links and thus provide new opportunities for variety of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control [1]. Sensor nodes monitor physical parameters such as temperature, pressure, motion and vibration. The sensor node performs three primary functions which are sensing, communication and data processing [2]. Sensor node consists of microcontroller, small energy and limited battery capacity. Due to more traffic load on sensor node its energy will be depleted that is required to increase network lifetime. In WSN, the security of data is a great issue. Security and privacy issues must be seriously taken into account in order to exploit the full benefits of WSN. Security deal with the cryptographic technic that is used to secure communication channels by ensuring message integrity, confidentiality, and authentication. While privacy issue involves studying the trust and risk associated with collection, storing, and associated with personal data [3]. Data gathering is an important issue that is used for solving the overlap problem. In this paper, some routing protocols will be explained to gather/ route the data [4]. Fading and interference represent the main channel impairments that prevent transmitted message from arriving to transmitter correctly. Therefore, channel impairments, will be investigated. This paper is organized as follows: related works will be made in Section 2. Section 3 represents network lifetime. The security of data will be made in Section 4. Data gathering and some routing protocols will be investigated in Section 5. Finally, conclusions will be made in Section 6.

II. Related work

Solutions on privacy support for data centric sensor networks (PDCS). The proposed schemes offer different levels of location privacy and allow a tradeoff between privacy and query efficiency. PDCS also includes several query optimization techniques that are based on Euclidean Steiner Tree and Bloom Filter to minimize the query message overhead and increase the query privacy. Simulation results verified that the KBF scheme can significantly reduce the message overhead with the same level of query delay. More importantly, the KBF scheme can achieve these benefits without losing any query privacy in [5]. An overview on security moreover, reliability challenges for WSNs was described in details in [6]. and introduces a toolbox concept to support such a framework and classification of hierarchy routing protocols were discussed. Development for malicious nodes discovery in wireless sensor network security was discussed in [7,8]. Sensed data are continuously collected at all or some of the sensor nodes and forwarded through wireless communications to a central base station for further processing. This makes it different from other applications of WSNs as well as traditional sensor data collection using wired networks. A survey on recent advances in networked wireless sensor data collection was presented. Specifically, a feature of sensor data collection in WSNs, by comparing it with both wired sensor data collection networks and other applications using WSNs was discussed. Issues on using WSNs for sensor data collection, which in general can be broken into the deployment stage, the control message dissemination stage and the data delivery stage were obtained in [9]. The performance comparison of the routing protocols Destination-Sequenced Distance Vector (DSDV) routing protocol, Ad-hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) using NS-2 Simulator were described in [10]. The comparison of these routing protocols is based on the basis of Average End-to-End delay, Normalized Routing Load, and packet delivery fraction by varying number of nodes, pause time and maximum speed. Through the analysis and comparison of network simulation results, when number of nodes are varied, AODV delivers the highest Packet Delivery Ratio (PDR) and Normalized Routing Load (NRL) due to on-demand nature of this protocol, while Average End to- End delay is maximum for DSR due to caching mechanism of DSR. When pause time is varied, AODV delivers the highest PDR and NRL while average End-to-End delay is

maximum for DSR. When maximum speed is varied, AODV delivers the highest PDF and NRL and Average End-to-End delay is maximum for DSR. In all of the three cases, AODV has the highest PDF and NRL. And DSR has the highest Average End-to-End delay, while DSDV because of its proactive nature provides the minimum delay. In [11] presents a comprehensive review of the existing distributed mobile sink routing protocols was presented. The unique challenges associated with mobile sinks and the design requirements of a mobile sink routing protocol were discussed in detail to provide an insight into the motivations and the inherent mechanisms. An accurate classification of the protocols was given and the advantages and drawbacks of the protocols were individually determined with respect to the performance requirements. The determined classes of protocols have different benefits which may provide motivations for new solutions. The hierarchical approaches exploit a virtual structure which serves as a rendezvous region for the sink advertisement and data packets. The virtual structure reduces the overhead of the sink advertisement by confining it to a subset of the network; however, the high-tier nodes constituting the structure are susceptible to becoming hotspots since they are likely to carry and process more traffic.

III. Network Lifetime

Sensor nodes have limited energy battery. These are deployed in several areas. They are used for monitoring and transmitting their data to the sink node. The area around the sink node is known as bottleneck zone, and the nodes near to the sink node its energy will be wasted easily due to high traffic on it and more over load. That leads to decrease network lifetime and then that node will die. Network lifetime depends on number of survive node after a certain period of time . To increase network lifetime two proposed algorithms that were made will be investigated in the following,

a. Using Relay Nodes

Depends on using relay nodes to forward the received data that leads to decrease the traffic on the nodes that is near to the sink. That techniquedepends on using different number of relay nodes and makes the transmission power of relay nodes varied. It was found that when using relay nodes with different transmission powers to forward the data It will lead to increase network lifetime and decrease average end to end delay. Moreover average jitter will be decreased [12] .

b- Using Realistic Sensing and Traffic Generation Model

The system depends on using realistic sensing and radio model to increase network lifetime. That system depends on using Elfes sensing model and event generation model which are described in [14]. In Elfes sensing model the probability of an event occurs depending on distance (x) from the sensor node being sensed and can be expressed by the following equation

$$p(x) = e^{-\alpha x} \quad D_{max} \geq x \geq 0, \qquad = 0 \quad x > D_{max}. \tag{1}$$

Where α is a constant and depends upon the sensor node and D_{max} is the maximum range of the sensor node.

Discrete radio model was used to determine which link should be used between two nodes for transmission that depends on achieving the lowest cost and low power for transmission. Discrete radio model follows the some steps for calculating the Received Signal Strength Indicator (RSSI). Depending on the RSSI, it can choose the best link for transmission discrete number of bower level that is based on standard CC240. That power is used to calculate RSSI then it can choose the best link for transmission. That model was applied on single hope and multi hope network [13].

IV. Security and Privacy

WSNs are composed of wireless sensors which are often deployed in public or untrusted environment which prompts a number of security and privacy issues that must be studied. Many advanced researches have been made and reported on recent years.

In [14] the author based on using a secret key between transmitter and receiver. Authentication broadcast requires asymmetry key. Otherwise any compromised receiver could forge the message from the sender. Asymmetric cryptography requires a high computation and storage overhead, which makes their usage is impractical. Moreover, security requirements are achieved using Secure Network Encryption Protocol (SNEP) and Micro Version of Timed, Efficient, Streaming, Loss-tolerant Authentication protocol (µTESLA). SNEP provides data confidentiality, two parties data authentication, integrity and freshness. µTESLA provides authentication for data broadcasting [15]. Actually some spread spectrum technique for security at physical layer communication using frequency hopping spread spectrum and direct sequence spread spectrum (DSSS) were discussed in [16].

Using cryptography for encryption, there are two types of cryptography are used which are symmetry and asymmetric cryptography. At symmetric cryptography, the shared key between transmitter and receiver is the same. This is means that the decryption key is the same as encryption key. In Asymmetric key, cryptography encryption key is different from decryption key. The main idea of this is to convert plain text to cipher text based on the key which is known to the transmitter and receiver [17]. On the following, some parameters which are affected on the security will be discussed

4.1 Type of attackers

Data privacy related to preventing data from internal and external attacker. Type of security protocols depends on type of attacker. Therefore some type of attackers will be explained as follow:

a. Internal attack where anode in the network is reprogrammed to be used as attacker. That type of attacker can be overcome by end to end encryption.

b. Malicious attacker where attacker node attracts packet by inserting false routing protocol. Security in that case depends on using different shared keys between each node and base station.

Data privacy also related to time and location of sensor node. That depends on using fake packet that allow establishing different routing paths. Attacker cannot identify the original traffic. While steganography depends on modifying the carrier to hide the message and allow the data to be loaded on image, sound and videos [18].

4.2 Security on Collected and Aggregated Data

The system depends on using a number of aggregator nodes to aggregate the data to overcome the problem of energy consumption. The aggregator nodes not include the security key but the security depends on end to end encryption between sensor nodes and sink node. Encryption key depends on holomorphic encryption in which the system is known as concealed data aggregation security [19].

4.3 Multiple Security Levels

Multiple securities were concluded to provide uniform secure access at the network allowing using different security levels for different information. Two proposed algorithms were made for multiple security levels which will be explained in the following :

4.3.1 Multiple Level Security (MLS)

- In MLS algorithm, every group of nodes has symmetry shared key for encryption. Each node receives data decrypt it with the shared key used for encryption. Guard node was used when transmitted data from high security level to low security level of transmission.
- Guard node that contains information about nodes and also about the keys of different security levels.
- When transmitting the data from high security to low security level. First, the data was received by the guard node which decrypts the data with its transmission key then re- encrypt it with its required key for transmission to the other node at lower security level. That system depends on using collator and down grader. That depends on guard node to identify the source node and the destination node and allow identifying the key for encryption and decryption. That organizes the transmission level as collator allows transmission from low level security to high level security.
- Down grader allows transmission from high level security to low level security. The algorithm depends on using tiny key man algorithm for construction asymmetry key between each two node [20].

4.3.2 WSN Cluster Multilevel Security Model (WSN – CMLSM)

In which all sensor nodes and cluster heads have different security clearances. WSN is modeled as a tree, in which the base station is the root, and each cluster is the sub tree. In each cluster, the security clearances of all nodes are lower than the clearance of the cluster head, and the clearances of nodes are decreased from the root to leaf. That system depends on election to cluster head node. Each group of nodes belongs to one cluster head. That cluster head collects the data and transmits it to base station. That model aims to organize the security levels. The security clearance of cluster head must be higher than the sensor node. That model was organized only for transmission of data from low level communication to high level communication [21].

V. DATA GATHERING

WSN consists of sensor nodes which are capable of collecting information from the environment and communication with each other via transceiver. The collected data will be delivered to one or more sink. The sensor nodes are typically expected to operate with batteries and are often deployed to not easily accessible or hostile environment. Sometimes in large quantities, it can be difficult or impossible to replace the batteries of sensor nodes. The main goal is to aggregate the data with maximizing the network lifetime.

Data gathering represents one of the main issues in WSN, which means aggregation / collecting the data to be transmitted to base station. Many researches have been proposed routing solutions to enable such networks. That routing protocols are broken down into four groups are data centric, hierarchical, location based and quality of services (QOS) routing protocols.

3.1 Data Centric Routing Protocol

Data centric routing protocol requires attribute based on naming. That system is more interested in querying an attribute of the phenomenon, rather than querying an individual node. The Base Station (BS) sends queries to a certain area for information and waits for replying from the nodes of that particular region. Since data is requested through queries, attribute based naming is required to specify the properties of the data. Depending on the query, sensor collects a particular data from the area of interest and this particular information is only required to transmit to BS [22,23]. Some of those protocols are sensor protocols for information via negotiation (SPIN), direct diffusion and energy aware routing protocol which are explained in the following,

3.1.1 SPIN

That routing protocol based on two basic ideas which are first sensor nodes that operate more efficiently by sending the data that describes the sensor data instead of sending the whole data.

Second sensor nodes must monitor the change in their energy resources. SPIN has three types of messages (ADV, REQ and data). The sensor broadcasts an advertisement message contains a descriptor of data. If the sensor interested in the data, it sends a request message for the data, then it is sent. That process is repeated until finishing the process [24, 25].

3.1.2 Direct Diffusion

At direct diffusion routing protocol, the sink sends out interest which represents a task description to other sensor nodes based on diffusion. Each sensor node stores the interest in its cache. As the interest is propagated through the network, the gradient from the source back to the sink are setup When the

source has a data for the interest. It sends the data along the interest gradient path that achieves minimum energy [26]. As shown in Fig .1

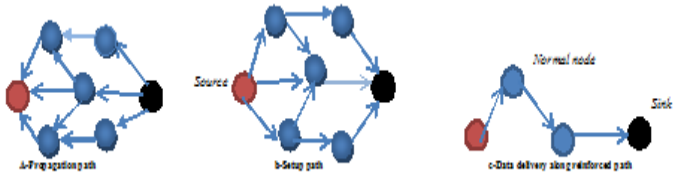

Fig. 1 Direct diffusion routing protocol .

5.1.3 Energy Aware Routing Protocol

The paths between the source and sink are determined by some of probability function. The aim is to increase network lifetime. The probability function in choosing the path is based on energy consumption of each path [27].

$$P_i(t) = \begin{cases} \dfrac{k}{N - k * (r \bmod N/k)} & C_i(t) \neq 0 \\ 0 & C_i(t) = 0 \end{cases} \quad (3)$$

Where:

K: is the expected number of cluster head.

N: is the total number of nodes in the network.

r: is the current round and the expected number of nodes that have not been a cluster head in the round r which is given by *(N-K*r).* When c_i *(t) =0*, the node will be chosen to be cluster head. In setup phase, once the nodes have elected themselves to be a cluster head. The cluster head nodes must tell all the other nodes in the network that they have chosen to be cluster head for current round. Cluster head broadcasts an advertisement message. Each non cluster head node determines to which it belongs by choosing the cluster head that requires the minimum communication energy based on received signal strength of the advertisement from each cluster head. . In steady state phase, the nodes send their data to the cluster head that was chosen by the nodes. The data is transmitted at frames using TDMA. Each node has slot to transmit data in it. Once cluster receives data, it can operate on the data and transmit it to BS [28]. As shown in Fig.2

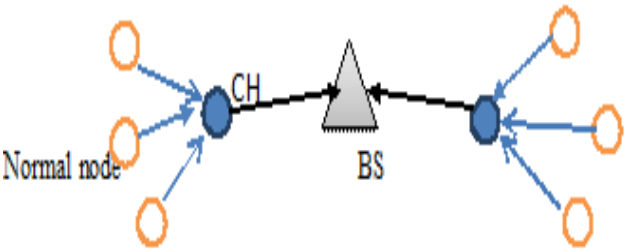

Fig. 2 LEACH routing protocol

5.2 Hierarchical Routing Protocol

Hierarchy protocols are proposed for energy consumption. Sensor nodes form clusters where the cluster heads aggregate the data to transmit it to sink node. The cluster head form another layer of clusters among themselves before reaching the sink. Some of hierarchy protocol were proposed for sensor network are LEACH, PEGASIS, TEEN and APTEEN [27].

5.2.1 Low Energy Adaptive Clustering Hierarchy (LEACH)

The operation of LEACH is divided into two phases which are setup phase and steady state phase. At setup phase, the node chosen them to be cluster head based on a random number when the random number is less than threshold, the sensor node is chosen to be cluster head as shown in equation(2) . The probability for each sensor node (i) to be a cluster head at time (t) is given by [28],

5.2.3 PEGASIS

- PEGASIS requires the nodes in the network to form chains. Each node at the chain aggregates the data and only one node through a chain is allowed to communicate with base station.
- PEGASIS stands for Power Efficient Gathering in Sensor Information System. This chain based protocol that provides improvement over LEACH algorithms. Therefore PEGASIS is an extension of the LEACH protocol. PEGASIS protocol requires information of chain which is achieved in two steps that are chain construction and gathering data.
- Chain construction that forms a chain from sensor nodes so that each chain transmits and receives from a neighbor and only one chain is elected to transmit to the base station. The chain construction is performed in a greedy way, starting from the node farthest to the sink. The nearest node to this node is put as the next node in the chain. A node can be in the chain at only one position. During each round, a leader node is randomly selected. The construction phase assumes that all the sensors have a global knowledge about the network. When a sensor fails or dies due to low battery power, the chain is constructed using the same greedy approach by passing the failed sensor.
- Gathering data where the data is aggregated and moves from node to node, and sent to base station. PEGASIS avoids cluster formation and uses only one a chain to transmit to its local neighbors in the data fusion phase instead of

sending directly to its cluster head as in the case of LEACH. As shown in Fig.3 node A passes its data to node B. node B aggregates data of node A with its own and then transmits to the leader. After node C passes the token to node E, node E transmits its data to node D. Node D aggregates the data of node E with its own data and the transmit to the leader C. Node C waits to receive data from both neighbors data. Finally, node C transmits one message to the base station [29].

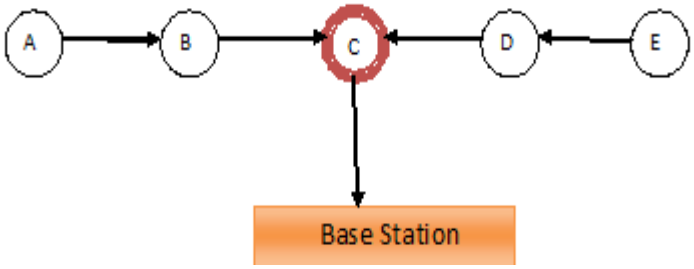

Fig. 3 Data gathering and chain construction in PEGASIS.

5.2.4 Hybrid Energy Efficient Distributed Clustering (HEED)

Excellent cluster based protocol. It elect cluster heads based on residual energy and node degree or density of nodes as a metric for cluster selection to achieve power balancing, which is a rational improvement compared with LEACH. Cluster heads are selected according to a combination of two clustering parameters. The primary parameter is a function of cluster density. The primary parameter is their residual energy of each sensor node and the secondary parameter is the intra – cluster communication cost as a function of cluster density. The primary parameter is used to probabilistically select an initial set of cluster heads while the secondary parameter is used for breaking ties. Sensor node sets the probability CH_{prob} of becoming a cluster head as obtained in (3)

$$CH_{prob} = C_{prob} * E_{residual} / E_{max} \quad (4)$$

Where $E_{residual}$ is the estimated current residual energy in this sensor node and E_{max} is the maximum energy corresponding to a fully charged battery, which is typically identical for homogeneous sensor nodes. The parameter C_{prob} is only used to limit the initial cluster head announcements and has on direct impact on the final cluster structure.

In HEED the clustering process at each sensor node require several rounds. Every round is long enough to receive messages from any neighbor within the cluster range. The CH_{prob} value must be greater than a minimum threshold. If a sensor node is selected to become a cluster head, it broadcasts an announcement message as a tentative cluster head or a final cluster head. A sensor node hearing the cluster head list selects the cluster head with the lowest cost from this set of cluster heads. A sensor hearing the cluster head list selects the cluster head with the lowest cost from this set of cluster heads [30,31].

5.2.5 Threshold sensitive Energy Efficient sensor Network (TEEN)

Is a hierarchical clustering protocol, which groups sensors into clusters with each led by cluster head. The sensors within a cluster report their sensed data to their cluster head. The cluster head sends aggregated data to higher level cluster head until the data reach the sink. The cluster head broadcasts to its member by the following:

- Hard threshold: This is a threshold value for the sensed attribute. It is the absolute value of the attribute beyond which, the node sensing this value must switch on its transmitter and report to its cluster head.
- Soft threshold: This is a small change in the value of the sensed attribute which triggers the node to switch on its transmitter and then transmit it.

The nodes sense their environment continuously, the first time parameter from the attribute set reach its hard threshold value, the node switch on its transmitter and send the sensed data.

The sensed value is stored in an internal variable in the node, called sensed value. The nodes will next transmit data in the current cluster period, only when both the following conditions are true:

a. The current value of the sensed attribute is greater than the hard threshold.
b. The current value of the sensed attribute differs from sensed value by an amount equal to or greater than soft threshold.

Whenever a node transmits data, sensed value is set equal to the current value of the sensed attribute. Thus, the hard threshold tries to reduce the number of transmission by allowing the nodes to transmit only when the sensed attribute is in the range of interest. The soft threshold further reduces the number of transmissions by eliminating all the transmissions which might have otherwise occurred when there is little or no change in the sensed attribute once the hard threshold. TTEN is not suitable for sensing applications where periodic reports are needed since the user may not get any data at all if the threshold is not reached [32].

As shown in Fig. 4

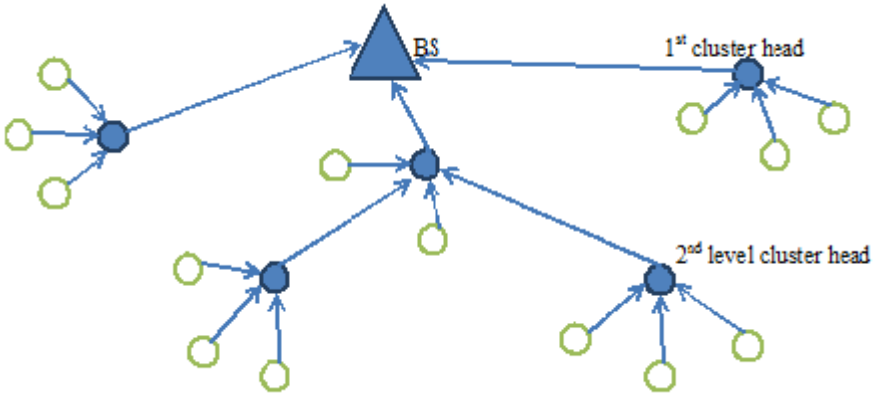

Fig. 4 TEEN routing protocol.

5.2.6 Adaptive Periodic Threshold sensitive Energy Sensor Network Protocol (APTEEN)

In APTEEN once the cluster heads are decided, in each cluster period, the cluster head first broadcasts the following parameters:

a. Attributes: This is a set of physical parameters which the user is interested in obtaining data about
b. Threshold: This parameter consists of a hard threshold and soft threshold. Hard threshold is a particular of an attribute beyond which a node can be triggered to transmit data. Soft threshold is a small change in the value of an attribute which can trigger a node to transmit data again.
c. Schedule: This is a TDMA schedule assigning a slot to each node.
d. Count time: It is the maximum time period between two successive reports sent by anode. It can be a multiple of the time division multiple access schedule length and it account for the proactive component.

The main features of APTEEN are by sending periodic data, it gives the user a complete picture of the network. Energy consumption can be controlled by the count time and the threshold value.

The main drawback of this scheme is the additional complexity required to implement the threshold functions and the count time [33].

5.3 Energy Efficient Clustering Scheme (EECS)

It is clustering based LEACH protocol that is operated in single hop mode between cluster head and base station. Sensor nodes compete for the ability to become cluster head for a given round. It involves sensor nodes into competition by broadcasting their residual energy to neighboring candidates. If a given node doesn't find anode with more residual energy, it becomes a cluster head. The main distinguishing features from LEACH are the dynamic sizing that is used in clustering in which cluster distance from base station is computed. In despite of these features EECS have some limitations as it uses single hop networks and can consume more energy for longer distance between cluster heads and base station, as all nodes compete for elevating to cluster head will add more complexity overhead. This overhead becomes due to more global knowledge about distance between base station and cluster heads.

5.4 Energy Efficient Protocol with Static Clustering (EEPSC)

It is also based on LEACH and comprise of three phases are setup phase, responsible node selection phase and steady state phase. It is based on dynamic clustering and taking temporary cluster heads in responsible node selection phase which are going to help in choosing the best cluster head within a cluster which will increase the network lifetime. It is hierarchical based on static routing protocol in which cluster formation is initially predetermined by base station thus removing the complexity overhead due to dynamic clustering. In setup phase, it is assumed that base station knows the locations of all the sensor nodes. In this scheme, the base station sends k-1 messages where k is the desired number of clusters set initially with different transmission powers. The sensor nodes who listen to the messages will respond by sending the join request message. The sensor nodes which are not joined to any cluster will set k as their cluster ID and will inform base station. It uses Carrier Sense Multiple Access (CSMA) for sending join request messages to base station in order to reduce collision so that energy can be reserved which will enhance network lifetime. base station selects one temporary cluster head randomly for each cluster and forward it to clusters in whole network. It is also send TDMA for all nodes in each cluster and allow nodes to transmit its data at its time slot. In next phase the round for selection cluster head begin all the nodes will send energy levels to the temporary cluster head, it then compare residual energy level of all the nodes and the node with highest energy level is selected as the cluster head during current round. The node with the lowest energy level is selected as temporary cluster head for next round. In steady state phase the nodes will send the data to cluster head at their allocated time slot. The cluster head will aggregate data and send it to base station. The major limitation of EEPSC is that the nodes located at the boundary of the cluster will consume more energy that lead to early dead nodes.

5.5 Enhanced energy Efficient Protocol with Static Clustering (EEEPSC)

It is based on existing scheme EEPSC by modifying it in order to remove the limitation of EEPSC. Cluster head is chosen not only on the basis of the highest residual energy as well as the relative location of the node in cluster. The objective of the scheme is to select the high residual node which is approximately central in the cluster. Base station compute the mean position of node distribution of every cluster. And distance from mean position to every node in every corresponding cluster. And node with highest residual energy and smallest mean distance will be selected as cluster head. The node with second highest residual energy is selected as temporary cluster head for next round in each cluster [34, 35 and 36].

5.5 Energy Efficient Data Gathering Mechanism Using Mobile Collector

M- Collector is responsible for gathering data from local sensors in the subarea. M collectors forwards the sensed data to one of the other nearby M- collector, and finally all the data are forward to the sink node. That protocol based on the following steps:

- first some of sensor nodes will be selected as polling point, these polling point will temporarily cache the data and upload them to the mobile collector when it arrives.
- The polling point can simply be a subset of sensors in the network or some other special devices such as storage nodes with a large memory and more battery power.
- Second, mobile collector has the freedom to move to any location. In the sensing field when the mobile collector arrives, it polls each polling point to request data then upload data to mobile collectors. Finally mobile collector handover the data to sink node then to base station [37].

Research issues and challenges

1- WSN used for many applications as military application, environmental monitoring. WSN consists of a number of sensor nodes that may be static or mobile sensor node. The following design issues of the sensor network must be taken into consideration.

2- To achieve security that is represent a great challenges as it is necessary to use an algorithm that not effect on energy resources as there is a tradeoff between security and network lifetime (sensor's energy). As sensor node has a limited energy, limited processing power and limited storage. So it is necessary to use security algorithm that secure the data with less energy consumption. Multiple security level must be applied on data aggregation system.

3- Privacy also represents an important issue that related to protection of private sphere bodily characteristics data as body temperature. Encryption key to protect data must be strong enough but with feasible computational to be used by sensor with limited energy.

4- Sensor nodes must be reliable as some sensor nodes may fail or be blocked due to lack of power or due to environmental interference. The failure of nodes shouldn't affect the overall performance of the network. This the reliability or fault tolerance issue of which is the ability to sustain sensor network functionalities without any interruption due to sensor node failure.

5- Scalability is one of the main issues in wireless sensor network as wireless sensor network consist of a large number of sensor nodes in order of hundreds or thousands and routing scheme must be scalable enough to respond to events.

6- Since the sensor network consists of a large number of sensor nodes. The cost of single node is very important to justify the overall cost of the networks so production costs must be taken into consideration.

7- Operating environment must be taken into consideration as sensor nodes are deployed in different area in the environment as in biologically or chemically contamination field or in a home or large building.

8- Network lifetime is related to power consumption as the transmission power is proportional to distance square. So multi hop routing protocol will consume less energy than direct communication. However, multi hop produce more routing overhead but direct communication would perform well if all nodes were close to each other.

9- Data delivery must be taken into consideration as it related to when the data was delivered. That depend on the application of the sensor network, the data delivery to the sink node can be divided in to continuous, event driven, query driven and hybrid. In the continuous delivery model, sensor node sends data periodically. In event driven the transmission of data triggered when an event occurs. In query driven when the query is generated by the sink by the sink, the sensor node transmits its data. A hybrid model uses a combination of continuous, event driven and query driven.

10- The routing protocol must have high quality of services which is related to long lifetime, energy efficiency, packet delivery ratio and throughput.

11- Overhead and data latency which are the most important factors that must be taken into consideration in designing wireless sensor network. As data aggregation and multi-hop relay cause data latency. Moreover, some routing protocols create excessive overhead to implement their algorithms, which are not suitable as it effects on energy of sensor nodes.

12- Provably secure routing: Routing is one of the most basic networking functions in multi-hop sensor networks. The presence of malicious nodes must be considered and precautions taken. Routing has two main functions: finding routes to the sink nodes, and forwarding data packets via these routes. Security approaches for routing protocols have mainly been analyzed by informal means only. What is needed is a mathematical framework in which security can be precisely defined.

VI. Conclusions

In this paper, we made an attempt to provide a survey on the issues and metric parameters that effect on the overall

performance of wireless sensor network. We have discussed several security problems, privacy issues, network lifetime increment, data gathering and channel impairments solutions. A number of existing standard solutions have been studied along with their mechanism. Also there are still interesting problems for future investigations, also traditional complex cryptography for security that require more processing and effects on the lifetime of network is not necessary to be used. Routing protocols must be investigated to identify the most one that have more network lifetime, less delay, less routing overhead. From the above it is necessary to design A WSN that has the following metric parameters that have studied above.

REFERENCES

[1] Ian F. Akyilidiz, Weilian Su, Yogesh sankara ubramaniam, and erdal caryirci " A survey On Sensor Network", IEEE communication magazine, Vol.38, PP393-422, 2002.

[2] Alkhatib and Gurvinder singh Baicher, " wireless Sensor Network Architecture", International Conference On Computer Network Architecture, International Conference On Computer Network and Communication Systems (CNCS), Vol.35,2012.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci " A surveyon sensor networks". IEEE Communications Magazine, PP102–114, August 2002.

[4] Q.wang and T. Zhang," Bottleneck Zone Analysis in Energy Constrained Wireless Sensor Network", Vol.13, No.6, PP423-42, June2009.

[5] Min Shao, Sencun Zhu, Wensheng Zhang and Guohong Cao, " PDCS, : Security and Privacy Support For Data Centric Sensor Networks", Vol.5, 2009.

[6] Dirk WESTHOFF, Joao GIRAO and Amardeo SARMA "Security Solutions for Wireless Sensor Networks", NEC Technical Journal, Vol 1, No.3, 2006.

[7] Rajaashree. V.Biradar, V.C. patil, Dr. S.R. Sawant and Dr. R.R. Mudholkar " Classification and Comparison of Routing Protocols in Wireless Sensor Networks. Ubicc Journal vol.4.

[8] Daniel –Ioan Curiac, Madalin Plastoi, Ovidiu Banias and Constantin Volosencu, " Software Development for Malicious Nodes Discovery in Wireless Sensor Network Security", Fourth International Conference on Sensor Technologies and Applications, IEEE Computer Society, 2010.

[9] Feng Wang, Student Member, IEEE, and Jiangchuan Liu, Senior Member, IEEE " Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches", IEEE Communications Surveys & Tutorials for possible publication, Vol.13, No.4, Fourth quarter 2011.

[10] Ginni Tonk, Indu Kashyap, and S.S. Tyagi " Performance Comparison of Ad-Hoc Network Routing Protocols Using NS-2", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN, Vol.1, PP 2278-3075, issue-1, June 2012.

[11] Can Tunca, Sinan Isik, M. Yunus Donmez, and Cem Ersoy, Senior Member, IEEE " Distributed Mobile Sink Routing for WirelessSensor Networks: A Survey", IEEE communications surveys & tutorials, 2013.

[12] Kavita Kumar, Manju, Ranjana Thalore, Vikas Raina and M.k. Jha " Enchancement of Life Time Using Relay Nodes in Wireless Sensor Networks, International Journal of Scientific&EngineeringResearch (IJSER), Vol.4, issue11, November2013

[13] Ayon chakraborty, Rashmi Ranjan Rout, Aveek chakrabarti and soumga K. Ghosh " On Network Lifetime Expectancy with Realistic Sensing and Traffic Generation Model in Wireless Sensor Networks. IEEE sensors journals, 2013.

[14] Daniel . Ioan Curiac, Madalin Plastoi, Ovidiu Banias and Constantin Volosencu " Software Development for Malicious Discovery in Wireless Sensor Network Security, IEEE Computer Society, 2010.

[15] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou "Sensor Network Security: A Survey", IEEE communications surveys & tutorials, Vol. 11, No. 2, second quarter 2009.

[16] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Commun. Surveys Tutorials, vol.8, PP 2–23, 2006.

[17] Orihashi, M, Nakagawa, Y, Murakami, Y, and Kobayashi, K" Channel Synthesized Modulation Employing Singular Vector for Secured Access on Physical Layer"IEEE GLOBECOM, Vol.3, PP1226-1230, December 2003.

[18] Dirk Westhoff Girao and Amar deo Sarma " security solutions for wireless sensor network", NEC Technical Journal, 2006.

[19] Kamral Islam, Weiming shen and Xianbin Wang " Security and Privacy Considerations for Wireless Sensor Networks in Smart Home Environments", IEEE, 2012.

[20] B. Carbunar, Y. Yu, L. Shi, M. Pearce, V. Vasudevan, " Query Privacy in Wireless Sensor Networks,", IEEE Communication Society Conference on Sensor, pp.203-212, 2007.

[21] Jangdeoglee, Sang H. Son and Mukesh Singhal " Desing of Architecture for multible security levels in wireless sensor network.

[22] Chaolee, Li. Hua Yin and Yun- chuan Guo " A multilevel security model for wireless sensor network.

[23] Rajaashree. V.Biradar, V.C. patil, Dr. S.R. Sawant and Dr. R.R. Mudholkar " classification and comparison of routing protocols in wireless sensor networks. Ubicc Journal vol.4.

[24] K.Karthikeyan , M.Kavitha " Comparative Analysis of Data Centric Routing Protocols for Wireless Sensor Networks ", International Journal of scientific and Research Publication, Vol. 3, PP1-6, January2013.

[25] Geetu , Sonia Juneja "Performance Analysis of SPIN and LEACH Routing Protocol in WSN" , International Journal of computational Engineering Research, Vol.2,pp. 1179-1185, September 2013.

[26] Zeenat Rehena, Sarbani Roy, Nadini Mukherjee, " Amodified SPIN for wireless sensor networks", IEEE, 2011.

[27] Kristoffer clyde Magsino, H. Srikanth Kamath ," Simulation of Routing Protocols of Wireless Sensor Networks", World Academy of Science , Engineering and Technology, Vol. 3, PP 192-194, February 2009.

[28] Chenmin Li, Guoping Tan, Jingyu wu, Zhen Zhang and Lizhong Xu " Analysis cluster head selection mechanisms and improving the LEACH", IEEE, 2011.

[29] S. Lindsey and C.S Raghavendra, " PEGASIS : power efficient gathering in sensor information system", proceedings IEEE Aerospace conference, Vol.3, May 2002.

[30] Ossama Younis and Sonia Fahmy " HEED: A Hybrid protocol for efficient, distributed clustering approach for ad- hoc networks" IEEE Transactions on mobile computing, Vol.3, PP 366-369, October- December 2004.

[31] Pratik R. Chavda and prof paresh kotak: " comparison of HEED and LEACH cluster based protocol for wireless sensor network, IOSR journal of computer engineering.

[32] A. Manjeshwar and D.P. Agrawal, " TEEN: A protocol for enhanced efficiency in wireless sensor networks", in the proceedings of the international workshop on parallel and distributed computing issues in wireless networks and mobile computing, April 2001.

[33] Arati Manjeeshwar and dhrama P. Agrawal "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks", proceeding of the international parallel and distributed processing symposium IEEE , 2002.

[34] Jahangeer Ali, Gulshan Kumar and Dr. mirtun jay Kumar rai: " Major energy efficient routing scheme in wireless sensor networks survey and ideas, international journal of computers and technology, Vol. 4, May-April 2013.

[35] konstantions kalpakis and shilang tang " collaborative data gathering in wireless sensor networks using measurement co-occurrence.

[36] Navdeep kour, Deepika sharma and prabhdeep singh " classification of hierarchical routing protocols in wireless sensor network: a survey, international journal of p2p network trends and technology, vol.3, issue1, 2013.

[37] K.Revanth Kumar Reddy, H.Usha Rani and K.Rubesh Kumar " Energy Efficient Data Gathering Mechanism In Wireless Sensor Networks Using Mobile Collector", International Journal Of Engineering And Computer Science, Vol.3, Issue1, pp 3789-3793, January 2014.

AUTHORS

First Author – Samar Fakher, Radiation Eng. Department, in NCRRT, Atomic Energy, Egypt, Email: samarfaker@yahoo.com
Second Author – Mona Shokair, Electronics and Electrical Communications dept. Faculty of Electronic Engineering, Menufia University, Menouf, Egypt, Email: mona.sabry@el-eng.menofia.edu.eg
Third Author – M.I. Moawad, Electronics and Electrical Communications dept. Faculty of Electronic Engineering, Menufia University, Menouf, Egypt
Fourth Author – Karam Sharshar, Radiation Eng. Department, in NCRRT, Atomic Energy, Egypt