A Study on Power Saving and Secure WSN

Anil Kumar (1), Preeti gulia (2), Shikha Sharma(3),
Department of computer science (1)
Asst. Prof. in Dept. of DCSA(2), Assistant Professor in SDDIET,(3)
Maharishi Dayanand University, Rohtak (HRY)(1,2), Barwala Panchkula , Haryana, India,(3)

Abstract: - wireless sensor network has a good future in many daily usage of a society system. WSN application is countless. Main benefit of this application is that we can implement in most of daily usage work. Security and power are major issues and challenges of any WSN's .Because these are the primary aspect of any WSN's system, some limitation and behaviour of WSN pose security challenges. In WSN area researchers are trying to find out best solution for battery efficiency improvement and reliable security improvable of WSN. In this review paper we have analysed applications, issues and challenges of WSN..

***Keywords*— wireless sensor network's (WSN) Introduction**

Introduction of WSN: - Wireless Sensor Network is an ad hoc network that consists of a number of resource constrained devices spread across some geographical area to monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants detection and for the surveillance in the military applications. A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability may contain multiple types of memory have an RF transceiver, have a power source (e.g., batteries and solar cells), and accommodate various sensors. WSN are network's that consists of sensors which are distributed in an ad hoc manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. WSN consists of protocols and algorithms with self-organizing capabilities Highly distributed networks of small, lightweight wireless nodes, Deployed in large numbers, Monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity, Node sensing , processing and communication.

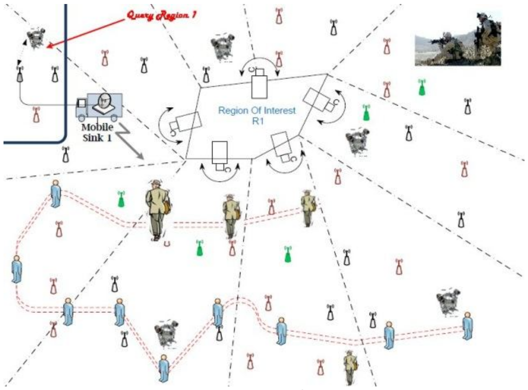

Fig.1 [ref. 62]

Inventory tracking: - Controls our inventory system, provide up to date position of our inventory while shipping, provide info about any problem in storage room.
Medical monitoring: - sensors in medical care and public health can work for a long time and provide better results. These instruments embed for use in clinics, homes, hospitals. Doctors monitor physiological and physical health condition which is critical to detect, diagnosis and treatment without these sensor. Medical sensor combines different transducers where patient can be monitor through electrical, chemical, thermal and optical signal. In fact modern medicine would not be effective without using of sensor i.e. thermometer (for temperature measurement), electrocardiography (EKG), blood pressure monitor, and other image sensors. In the same way location and proximity sensor can be used for finding the present location for improving the delivery of patient care as well as security. With the help of WSN Hospital staff and patients should be track and monitor and Drug administration in hospitals.

Application of WSN: -

*Environmental/Habitat monitorin***g**: - Habitat and environmental monitoring can enable_long-term data collection at scales and resolutions that are difficult, or even impossible, to obtain. Integration of local processing and storage allows sensor nodes to perform complex filtering and triggering functions, as well as to apply application-specific or sensor-specific data compression algorithms. Ability to communicate allows information and control to be communicated across the network of nodes; nodes cooperate in performing more complex tasks. Increased power efficiency application driven approach Separates actual problems from potential ones, relevant issues from irrelevant ones; helps to differentiate problems with simple, concrete solutions from open research areas. However, general solutions should seek from this. Collaboration with scientists in other fields helps to define a broader application space.

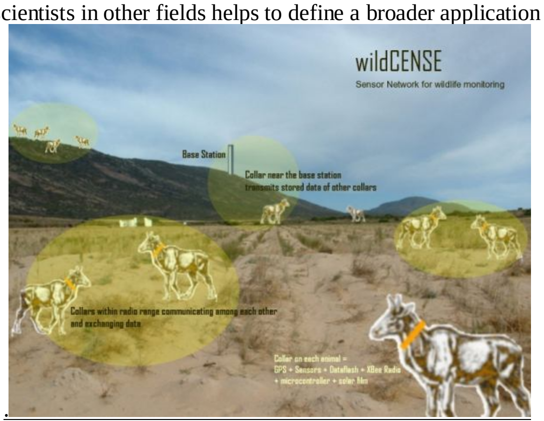
wildCENSE
Sensor Network for wildlife monitoring
Base Station
Collar near the base station transmits stored data of other collars
Collars within radio range communicating among each other and exchanging data
Collar on each animal = GPS + Sensors + Dataflash + XBee Radio + microcontroller + solar film

fig.4 [ref.62]

Military surveillance: - helpful in boarder area to identify activities of enemies and there operation.
Inventory tracking: - Controls our inventory system, provide up to date position of our inventory while shipping, provide info about any problem in storage room.
Medical monitoring:- sensors in medical care and public health can work for a long time and provide better results. These instruments embed for use in clinics, homes, hospitals. Doctors monitor

physiological and physical health condition which is critical to detect, diagnosis and treatment without these sensor. Medical sensor combines different transducers where patient can be monitor through electrical, chemical, thermal and optical signal. In fact modern medicine would not be effective without using of sensor i.e. thermometer (for temperature measurement), electrocardiography (EKG), blood pressure monitor, and other image sensors. In the same way location and proximity sensor can be used for finding the present location for improving the delivery of patient care as well as security. With the help of WSN Hospital staff and patients should be track and monitor and Drug administration in hospitals.

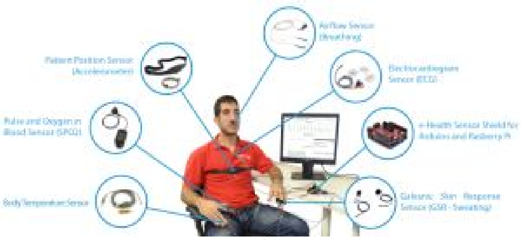

Fig.3 [ref...62]

Environment applications: -

- Monitoring the behavior of organisms,
- Forest fire detection,
- Flood detection,
- Mapping of the environment,
- Precision Agriculture
- Earth quake detection and analyses
- Soil makeup
- Temperature
- Weather analyses

Industrial & Commercial: -

- WSN is also helpful in numerous industrial and commercial applications like Agricultural Crop Conditions,
- Automated Problem Reporting, RFID –
- Theft Deterrent and Customer Tracing,
- Plant Equipment and Maintenance Monitoring.
- Chemical level and pressure measuring
- Load and strain

Traffic Management & Monitoring: - WSN also plays a very important role in traffic management & monitoring of vehicle. It provides up to date information of speed, distance and route updates, near and far vehicles so as to prevent us from accidents and save our time from traffic jams.

Smart home: - also control our home appliances like bulb, ac, TV window, geezers, and refrigerator.

Challenges in WSN:-

1.1. *WSN design challenges*

Many applications of WSN have several restrictions, such as limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. Some of the design challenges are summarized below:

*Node deployment***:** Node deployment in WSNs 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. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation. Inter-sensor communication is normally within short transmission ranges due to energy and bandwidth limitations. Therefore, it is most likely that a route will consist of multiple wireless hops.

*Network Dynamics***:** Most of the network architectures assume that sensor nodes are stationary. However, 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, in addition to 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.

*Energy Efficiency***:** Once the WSN is functional it becomes difficult to replace or recharge the battery of sensor nodes. This further poses the challenge to maintain sensors in hostile and harsh environment and scaling of sensor network to hundreds or thousands of nodes. Therefore, an energy-efficient mechanism is required to save energy and prolong the network lifetime.

*Data Aggregation***:** Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. This technique is used to achieve energy efficiency and data transfer optimization in a number of routing protocols. Signal processing methods can also be used for data aggregation. Data dissemination is a technique to spread the data throughout the network. It is used to propagate the query, routing information, time synchronization etc. in the network.

*Node/Link Heterogeneity***:** In many studies, all sensor nodes were assumed to be homogeneous, i.e., having equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different role or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing. These special sensors can be either deployed independently or the different functionalities can be included in the same sensor nodes. Even data reading and reporting can be generated from these sensors at different rates, subject to diverse quality of service constraints, and can follow multiple data reporting models. For example, hierarchical protocols designate a cluster-head (CH) node different from the normal sensors. These cluster heads can be chosen from the deployed sensors or can be more powerful than other sensor nodes in terms of energy, bandwidth, and memory. Hence, the burden of transmission to the BS is handled by the set of cluster-heads.

Fault tolerance and reliability: For many WSN applications, data must be delivered reliably over the noisy, error-prone, and time-varying wireless channel. In such cases, data verification and correction on each layer of the network are critical to provide accurate results. Additionally, sensor nodes are expected to perform self-testing, self-calibrating, self-repair and self-recovery procedures during their lifetime.

*Security requirements and possible attacks***:** The goal of security services in WSNs is to protect the information and resources from attacks and misbehaviour.

a) *Security requirements in WSNs***:** Security requirements in WSNs are as follows

Availability: Which ensure that the desired network services are available even in the presence of denial of service attacks?

Authentication: Which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node

Confidentiality: Which ensure that a given message cannot be understood by anyone other than the desired recipient.

Integrity: Which ensure that a message sent from one node to another is not modified by intermediate malicious node?

*b) Attacks in WSNs***:** WSNs are vulnerable to various types of attacks. According to the security requirements in WSNs, these attacks can be categorized as [7].

*Selective forwarding***:** Selective forwarding is a way to influence the network traffic by believing that all the participating nodes in network are reliable to forward the message [9]. In selective forwarding attack malicious nodes simply drop certain messages instead of forwarding every message. Once a malicious node cherry picks on the messages, it reduces the latency and deceives the neighbouring nodes that they are on a shorter route. Effectiveness of this attack depends on two factors. First the location of the malicious node, the closer it is to the base stations the more traffic it will attract. Second is the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighbouring nodes.

*Sinkhole attack***:** In sinkhole attacks, adversary attracts the traffic to a compromised node [9]. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible.

*Sybil attack***:** A type of attacks where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes [9, 10]. Sybil attacks can be used against routing algorithms and topology maintenance; it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

*Wormholes attack***:** In wormhole attacks an adversary positioned closer to the base station can completely disrupt the traffic by tunnelling messages over a low latency link. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station [9, 11]. This creates a sinkhole because adversary on the other side of the sinkhole provides a better route to the base station.

*Hello flood attack***:** Broadcasting a message with stronger transmission power and pretending that the HELLO message is coming from the base station [9]. Message receiving nodes assume that the HELLO message sending node is the closest one and they try to send all their messages through this node. In this type of attacks all nodes will be responding to HELLO floods and wasting the energies. The real base station will also be broadcasting the similar messages but will have only few nodes responding to it.

DoS attack: Denial of service attacks occur at physical level causing radio jamming, interfering with the network protocol, battery exhaustion etc.

Life Time: - critical to any wireless sensor network deployment is the expected lifetime. The primary factor for the lifetime of sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. Main goal of WSN is to have nodes placed out in the field, unattended, for month or year.

Coverage: - it is a primary evaluation metric for wireless networks and is advantageous to have the ability to deploy a network over a larger physical area. Keep in mind that coverage of the network is not equal to the range of the wireless communication links being used.

Cost and ease of deployment: - for system deployments to be successful, the wireless sensor network must configure itself. A key advantage of wireless sensor network is their ease of deployment. It is possible for nodes to be placed throughout the environment by an untrained person and have the system simply work. The total cost of ownership for a system may have more to do with the maintenance cost than the initial deployment cost.

Response time: - system response time is critical performance metric and an alarm signaled immediately when an intrusion is detected. Response time is also critical when environmental monitoring is used to control factory machines and equipment's. Response time can be improved by including nodes that are powered all the time.

Temporal accuracy: - to achieve temporal accuracy, a network must be capable of constructing and maintaining a global time base that can be used to chronologically order samples and events in distributed clock. Time synchronization information must be continually communicated between nodes.

Security: - Security means to provide the protection against the danger, loss and criminals but in the networks it is the Protection of information from theft, corruption or natural disaster while allowing the information to be accessible by the intended users.keeping the information secure is extremely important. WSN must be capable of keeping the information they are collecting private from eavesdropping. Data security becomes more significant. Not only the system must maintain privacy, it must also be able to authenticate data communication.

Power: - WSN has main issue of power because without power backup we can't assume any node in the network. If any protocols have a good battery backup then that node can survive for long term in the network. The long term battery backup also reduces cost effectiveness of the network.

Performance: - the performance of WSN on ground level is poor. It can cover only 10 meter distance (like Bluetooth).

Self-configuration:- whenever WSN should be reconfigure or self-configured itself System should resynchronize automatically without losing their original process.

Dynamic WSN: - WSN should be dynamic with changing of environment conditions and system should adopt changing connectivity and their system environment

Power saving and security issue aspects :- security is a major issue of WSN because when WSN deployed in hostile environment then it is necessary to encrypt the exchange data between sender and receiver. In wireless network, most security nodes are work on asymmetric cryptography, such as RSA or Elliptic Curve Cryptography (ECC) but these are not applied, due to high computational complexity. In WSN due lack of infrastructure support trusted server based key distribution protocol are not suitable for WSN.

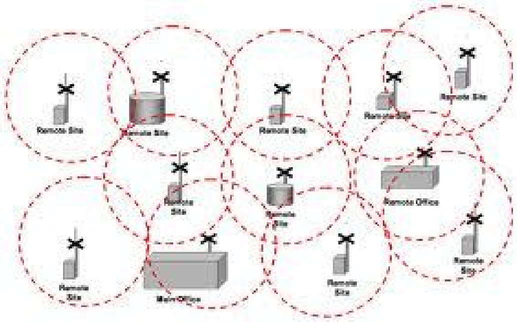

Fig.2 ref...62

But some researcher put an idea of preloading some secret key in SNs before deploying to the network. So that after deployment they discover shared key for secure communication. For preloading secret keys various techniques are in use. Some of the key management techniques are (single network-wide key establishment), (pair-wise key management), (dynamic key management), (public key schemes)

Time synchronization: - some of network work is synchronization to avoid losing power sensor radio may be turned off for period of time. Some authors propose a set of secure synchronization protocols for sender and receiver and group synchronization.

Data confidentiality: - this is an important issue of n/w security. It is extremely important to build a secure channel in WSN.

Data integrity: - sender should confidentiality satisfy that while on sending or receiving information no third party (attacker) can steal the data. Before transferring data sender has to ensure that either receiver is actual or not.

*Data freshne*ss: - after confidentiality and integration we also need to ensure freshness of each message. This shows that data is recent and this can be done with help of shared key.

LITERATURE SURVEY

3.1. Energy efficient routing protocols in WSNs

Routing protocols have a large scope of research work when implemented in WSNs, because the functioning of these protocols depends upon the type of network structure designed for the application or the network operations carried out using these protocols for a specific application model.

According to [16] the battery energy of a node is depleted by: (i) computational processing and, (ii) transmission and reception of data. The network layer controls both of these factors.

3.1.1. Flat routing protocols in WSNs

In flat networks, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. Early works on data centric routing, viz., Sensor Protocols for Information via Negotiation (SPIN) [16] and Directed Diffusion [17] has minimizes the energy issue through data negotiation and elimination of redundant data. Rumour routing [18] is a variation of directed diffusion and is mainly intended for applications where the geographic routing is not feasible.

3.1.2. Hierarchical routing protocols in WSNs

Hierarchical or cluster-based routing, are well known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy-efficient routing in WSNs. In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. Some of routing protocols in this group are: Power-Efficient Gathering in Sensor Information System (PEGASIS) [6], Threshold-Sensitive Energy Efficient TEEN [20] and Adaptive Threshold-Sensitive Energy Efficient (APTEEN) [21].

In [22], authors introduce Cluster Head Election mechanism using Fuzzy (CHEF) logic. They apply the fuzzy if-then rule to the CH election mechanism. By using fuzzy logic, the computational overhead is reduced and the network lifetime is extended. In addition, the operation of this mechanism is localized. The BS does not collect and elect CHs. The sensor nodes only elect CHs among themselves using the fuzzy logic. The routing algorithm proposed in [23] based on dynamic clustering protocol which grants a large lifetime for the network. The key idea of this protocol is to reduce transmission in intra-clusters when the objective is to collect the maximum or minimum data values in a region (like temperature, humidity, etc.).

A number of different strategies for multi-hop routing, including minimum distance and minimum-hop routing have been presented in [24]. In [25], authors have proposed efficient integer linear program formulations for assigning sensor nodes to clusters in a two-tired network where the higher powered relay nodes are used as CHs. The relay nodes can use a single hop model or multi-hop model to send the data to the BS. The objectives in both cases are to maximize the lifetime of the network.

The authors in [26] take a unique look at the CH election problem, specifically concentrating on applications where the maintenance of full network coverage is the main requirement. The approach for cluster-based network organization is based on a set of coverage-aware cost metrics that favour nodes deployed in densely populated network areas as better candidates for CH nodes for active sensor nodes and routers. Compared with using traditional energy based selection methods, using coverage-aware selection of CH nodes, active sensor nodes and routers in clustered WSN increases the time during which full coverage of the monitored area can be maintained depending on the application scenario.

In [27], authors analysing the advantages and disadvantages of conventional hierarchical communication protocols using MATLAB, they have developed Distance-Based Segmentation (DBS), a cluster-based protocol that significantly decreases the energy imbalance in the network by integrating the distance of the sensor nodes from the BS into clustering policies. Furthermore, a Media Access Control (MAC) protocol that eliminates redundant delays in the cluster formation period of conventional protocols is utilized as media access scheme.

The sensor nodes closet to the BS tend to deplete their energy faster than other sensor nodes [28, 29], which is known as an energy hole around the BS. No more data can be delivered to the BS after energy hole appears. Therefore, a lot of energy is wastes and the network lifetime ends prematurely.

In [30], authors have proposed a non-uniform node distribution strategy to achieve the sub-balanced energy depletion. The authors state that if the number of nodes in coronas increases then the network can achieve sub-balanced energy depletion.

In [31], authors have presented an important corona model to maximize the network lifetime by using adjustable transmission range. They have divided the maximal transmission range of sensors into several levels. The sensors nodes belong to the same corona have the same range of transmission, whereas different coronas have different transmission ranges. The authors concluded that transmission ranges to all coronas is the effective approach to extend the network lifetime.

In [32], authors have presented a short survey on the main techniques used for energy conservation in WSNs. The main focus is primarily on duty cycle scheme which represent the most suitable technique for energy saving. In [33], authors reviewed the existing definitions of network lifetime as propose in the literature. They discussed about the merits and demerits of the existing definitions, and summarized additional requirements. They have also introduced a number of new performance metrics that have found to be useful in the context of sensor network applications.

The authors in [34] have presented a systematic survey and comprehensive taxonomy of the energy saving schemes. They have also introduced mobility as a new energy saving paradigm with the purpose of maximizing the network lifetime. In [35], authors have proposed a new genetic algorithm (GA), for scheduling the data gathering of relay nodes, which significantly extends the network lifetime of a relay node network. For smaller networks, GA based approach is always finds the optimal solution. This algorithm can easily handle large networks as compared to traditional routing schemes.

The authors have presented a novel CH election problem in [24], specifically designed for applications where the maintenance of full network coverage is the main requirement. This approach is based on a set of coverage-aware cost metrics that favour nodes deployed in densely populated network areas as better candidates for CH nodes, active sensor nodes and routers. Compared with traditional energy-based selection methods, the coverage-aware selection of CH nodes increases the network lifetime depending on the application scenario.

In [36], authors have proposed and evaluated an Unequal Cluster based Routing (UCR) protocol for mitigating the hot spot problem in WSNs. It is designed for long-lived, source-driven sensor network applications, such as periodical environmental information reporting.

In [37], authors have studied a generic strategy of radioactivity minimization wherein each node maintains the radio switched on just in the expected packet arrival intervals and guarantees low communication latency. They define a probabilistic model that allows the evaluation of the packet loss probability that results from the reduced radioactivity. This model can be used to optimally choose the radioactivity intervals that achieve a certain probability of successful packet delivery for a specific radioactivity strategy. They also define a cost model that estimates the energy consumption of the proposed strategies, under specific settings.

3.1.2.1. Heterogeneous routing protocols for WSNs

WSNs attracted lots of researchers because of its potential wide applications and special challenges. For past few years, WSNs mainly focused on technologies based on the homogeneous WSN in which all nodes have same system resource but recently heterogeneous WSN is becoming more and more popular and the results of researches [38, 39] show that heterogeneous nodes can prolong network lifetime and improve network reliability without significantly increasing the cost.

A heterogeneous node is more expensive, and is capable to provide data filtering, fusion and transport. It may possess one or more type of heterogeneous nodes, e.g., enhanced energy capacity or communication capability. They may be line powered, or their batteries may be replaced easily. Compared with the normal nodes, they may be configured with more powerful microprocessor and more memory. They also may communicate with the BS node via high-bandwidth, long-distance network, such as Ethernet. The presence of heterogeneous nodes in a WSN can increase network reliability and lifetime. The main basic and important deployment problem is to decide how many and where heterogeneous nodes should be deployed in the network.

In an application for habitat monitoring [40], authors proposed a tiered system architecture in which data collected at numerous, inexpensive sensor nodes is filtered by local processing on its way through larger, more capable and more expensive nodes. The necessity of heterogeneity and the mechanisms of packet forwarding and processing are demonstrated in [41, 42]. However, how to use heterogeneous nodes effectively has not been studied comprehensively.

PEGASIS [6] discusses how to extend the lifetime of sensor networks. It is a near optimal chain-based protocol, not a clustering scheme. In PEGASIS, each node communicates only with an adjacent neighbour and takes turns transmitting to the BS. A number of issues are discussed, viz., reducing the amount of energy spent per processing round, minimizing overall distance between non-leader nodes of the system, and minimizing the number of data transmission to the BS. However, in PEGASIS, nodes die in random locations since the CHs have been chosen without any concern on an overall lifetime of each node.

To prolong the network lifetime by distributing energy consumption, HEED (Hybrid Energy-Efficient Distributed Clustering) [7] is a standalone distributed clustering approach in which each node considers two factors: remaining energy and communication cost before making a decision to join one cluster or the other. In HEED, once selected a CH is maintained for a fixed number of iterations. This is in contrast to some other approaches where the CHs are newly selected in every step. This is to reduce the unnecessary high setup cost associated with the CH selection process.

In [43], authors have studied the impact of heterogeneity of sensor nodes, in terms of their energy and have proposed a heterogeneous – aware protocol to prolong the time interval before the death of the first node, which is crucial for many applications where the feedback from the sensor network must be reliable. In [44], authors have proposed a new distributed energy efficient clustering scheme for heterogeneous WSNs, which are called DEEC. In DEEC, the CHs are elected by a probability based on the ratio between residual energy of each node and the average energy of the network.

The sensor nodes with high initial and residual energy will have more chances to become CHs than the nodes with low energy.

In [45], authors address the deployment problem of heterogeneous WSNs and is supported by an algorithm to decide how many and where heterogeneous nodes should be deployed in the WSN. The core algorithm is based on the locations of all sensor nodes, can optimize placement of heterogeneous nodes in an arbitrary WSN to increase the network lifetime and reliability. In [46], authors propose a distributed election clustering protocol to prolong the stable region of heterogeneous WSNs, which is based on remaining energy and communication cost to elect suitable CH nodes. Compared with classical clustering protocol, it can maintain load balancing of networks, and extremely prolong the stable region and the network lifetime.

In [47], authors have presented an Energy-Efficient Protocol with Static Clustering (EEPSC) which partitions the network into static clusters and utilizes CHs to distribute the energy load among high power sensor nodes for extending the network lifetime. But the authors have not investigated the effect of heterogeneity in the network system.

Energy-Efficient Hierarchical Clustering Algorithm (EEHCA) scheme [48] improves the performance of LEACH and HEED (Hybrid Energy-Efficient Distributed clustering), in terms of network lifetime. EEHCA adopts a new method for CH election, which can avoid the frequent election of CH. In order to improve the performance of the sensor network new concept of backup CHs is introduced. Therefore, when nodes finished the communication within their own clusters and the CHs have finished the data aggregation, the head clusters will transmit aggregated data to the BS.

3.1.3. Location based routing protocols

In location-based routing, all the sensor nodes are addressed by using their locations. Depending upon the strength of the incoming signals, it is possible to calculate the nearest neighbouring node’s distance. Due to obstacles in the network often the signal strength becomes weaker and nodes are unable to find the nearest neighbour nodes. There are many location-based schemes of which Geographic and Energy aware Routing (GEAR) [49] and Geographic Adaptive Fidelity (GAF) [50] are two important schemes.

3.2. Data aggregation and dissemination schemes for WSNs

The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime can be enhanced. Data gathering is defined as the systematic collection of sensed data from multiple sensors to be eventually transmitted to the BS for processing. Since sensor nodes are energy constrained, it is inefficient for all the sensors to transmit the data directly to the BS. Data generated from neighbouring sensors is often redundant and highly correlated. In addition, the amount of data generated in large sensor networks is usually enormous for the BS to process. Hence, we need methods for combining data into high quality information at the sensors or intermediate nodes which can reduce the number of packets transmitted to the BS resulting in conservation of energy and bandwidth. This can be accomplished by data aggregation. It may be defined as the process of aggregating the data from multiple sensor nodes to eliminate redundant transmission and provide fused information to the BS and it usually involves the data fusion at intermediate nodes and transmits the aggregated data to the BS.

Data aggregation attempts to collect the most critical data from the sensors and make it available to the BS in an energy efficient manner with minimum data latency. Data latency is important in many applications such as environment monitoring where the freshness of data is also an important factor. It is critical to develop energy efficient data aggregation algorithms so that network lifetime can be enhanced. There are several factors which determine the energy efficiency of a sensor network such as network architecture, the data aggregation mechanism and the routing protocol. The architecture of the sensor network plays a vital role in the performance of different data aggregation protocols.

3.2.1. In-network aggregation

In a typical sensor network scenario, different node collect data from the environment and then send it to some central node or BS which analyses and process the data and then send it to the application. But in many cases, data produced by different sensor nodes can be jointly processed while being forwarded to the BS node. In-network aggregation deals with this distributed processing of data within the network.

Data aggregation techniques explore how the data is to be routed in the network and the processing method that are applied on the packets received by a node. They have a great impact on the energy consumption of nodes and thus on network efficiency by reducing number of transmission or length of packet. In [51], authors define in-network aggregation process “In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime”.

There are two approaches for in-network aggregation: with size reduction and without size reduction. In-network aggregation with size reduction refers to the process of combining and compressing the data packets received by a node from its neighbours in order to reduce the packet length to be transmitted or forwarded towards BS. As an example, consider the situation when a node receives two packets which have a spatial correlated data. In this case it is worthless to send both packets. Instead of that one should apply any function like Average (AVG), Maximum (MAX), and Minimum (MIN) to send a single packet. This approach considerably reduces the amount of bits transmitted in the network and thus saving a lot of energy but on the other hand, it also reduces the precision of data value received. In-network aggregation without size reduction refers to the process of merging data packets received from different neighbours into a single data packet but without processing the value of data. As an example, two packets may contain different physical quantities (i.e., temperature and humidity) and they can be merged into a single packet by keeping both values intact but keeping a single header. This approach preserves the value of data and transmit more bits in the network but still reduce the overhead by keeping single header.

These two approaches depend on many factors like the type of application, data arrival rate and network characteristics. There is also a trade-off between energy consumption and precision of data for the two approaches.

Most of the work available in literature on in-network aggregation mainly deals with problem of forwarding packets from source to BS, to facilitate aggregation therein. Actually the main idea behind were to enhance existing routing protocols such that they can efficiently aggregate data. Most of the data aggregation techniques fall under three categories - tree-based approaches, multi-path approaches, and cluster-based approaches. There are also some hybrid approaches that combine any of these three techniques. These approaches are described in the coming sections with giving details of some of the main techniques by different authors.

3.2.2. Tree based approach

The simplest way to aggregate data is to organize the nodes in a hierarchical manner and then select some nodes as the aggregation point or aggregators. The tree-based approach perform aggregation by constructing an aggregation tree, which could be a minimum spanning tree, rooted at BS and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaf nodes up to the BS and therein the aggregation done by parent nodes. The way this approach operates has some drawbacks. In case of packet loss at any level of tree, the data will be lost not only for a single level but for the whole related sub-tree as well. In spite of high cost for maintaining tree structure in dynamic networks and scarce robustness of the system, this approach is suitable for designing optimal energy efficient aggregation technique.

A data-centric protocol is based on aggregation tress, known as Tiny Aggregation (TAG) approach [52]. TAG works in two phases: distribution phase and collection phase. In distribution phase, TAG organizes nodes into a routing tree rooted at BS. The tree formation starts with broadcasting a message from BS specify level or distance from root. When a node receive this message it sets its own level to be the level of message plus one and elect parent as node from which it receives the message. After that, node rebroadcast this message with its own level. This process continues till all the sensor nodes elect their parents. After tree formation, BS sends queries along structure to all nodes in the network. TAG uses database Structured Query Language (SQL) for selection and aggregation functions. In collection phase, data is forwarded and aggregated from leaf nodes to root. A parent node has to wait for data from its entire child node before it can send its aggregate up the tree.

3.2.3 Directed Diffusion

In [53], authors proposed a reactive data-centric protocol for applications where BS ask some specific information by flooding, known as directed diffusion paradigm as shown in Figure 3.1. The main idea behind directed diffusion paradigm is to combine data coming from different sources and en-route them by eliminating redundancy, minimizing the number of data transmission, thus maximizing network lifetime. Directed diffusion consists of several elements: interests, data messages, gradients, and reinforcements.

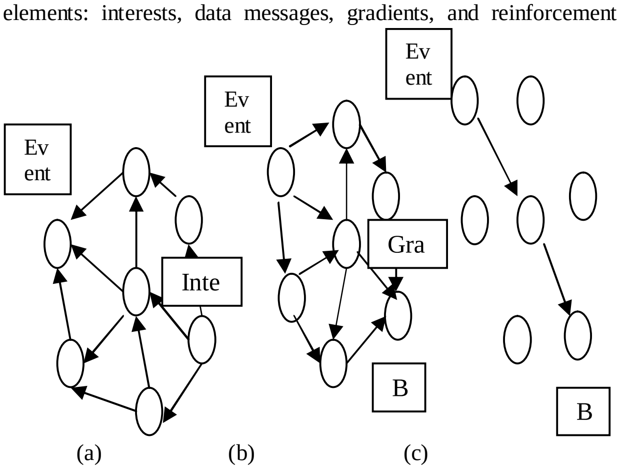

Figure 3.1 Simplified schematic for directed diffusion: (a) Interest propagation, (b) Initial gradients setup, (c) Data delivery along reinforced path.

The BS requests data by broadcasting an interest message which contains a description of a sensing task. This interest message propagates through the network hop-by-hop and each node also broadcast interest message to its neighbour. As interest message propagates throughout the network, gradients are setup by every node within the network. The gradient direction is set toward the neighbouring node from which the interest is received. This process continues till gradients are setup from source node to BS. Loops are not checked at this stage but removed at later stage. After these paths of information flow are formed, then best path are reinforced to prevent further flooding according to a local rule. Data aggregation took place on the way of different paths from different sources to BS. The BS periodically refreshes and resends the interest message and it starts to receive data from sources to provide reliability. The problem with directed diffusion is that it may not be applied to applications (e.g. environmental monitoring) that require continuous data delivery to BS. This is because query driven on demand data model may not help in this regard.

Also matching data to queries might require some extra overhead at the sensor nodes. Mobility of BS nodes can also degrade the performance as path from sources to BS cannot be updated until next interest message is flooded throughout the network. To cope up with above issue if introduce frequent flooding then also too much overhead of bandwidth and battery power will be introduced. Furthermore, exploratory data follow all possible paths in the network following gradients which lead to unnecessary communications overhead.

3.2.3. Multi-path approach

One of the main drawbacks of tree-based approach is the scarce robustness of the system. To overcome this drawback, many approaches are available in the literature. The theme behind these approaches is that instead of sending partially aggregated data to a single parent node in aggregation tree, a node sends data over multiple paths. In this scheme each node sends data to its possibly multiple neighbours by exploiting the wireless medium characteristic. Thus, data will flow from sources to BS along multiple paths and aggregation can be performed by each intermediate node. Clearly, schemes using this approach will make the system robust but with some extra overhead. One of the aggregation structures that fit well with this approach is ring topology, where network is divided into concentric circles with defining levels according to the hop distance from BS.

In [54], authors have presented a data aggregation technique using multi-path approach, known as synopsis diffusion. Synopsis diffusion works in two phases: distribution of queries and data retrieval phase. During distribution of queries phase, a node sends a query in the network. The network nodes then form a set of rings around the querying node. The node which is *i* hop away from querying node is considered as ring R_i. In the second phase, aggregation starts from outermost ring and propagate level by level towards the BS. Here, a source node may have multiple paths towards BS.

In [55], authors describe a new strategy for data gathering in WSN which considers both issues: energy efficiency and robustness. Authors first say that single path to connect each node to the BS is simple and energy-saving approach but expose a high risk of disconnection due to node/link failures. But multi-path approach would require more nodes to participate with consequent waste of energy. Authors present a clever use of multi-path only when there is loss of packet which is implemented by smart caching of data at sensor nodes. Authors also argue that in many practical situation data may be gathered only from a particular region, so they use a different approach that relies on a spanning tree and provides alternative paths only when a malfunctioning is detected. Algorithm adopts a tree-based approach for forwarding packets through the network. In the ideal situation when no failures occur, this is certainly the best choice, as the minimum numbers of nodes are engaged in the transmission phase. In the presence of link or node failures, the algorithm discovers an alternative path which ensures the delivery of as many packets as possible within the time constraints. The problem with this approach is that it may cause the arising of hot spots and nodes along preferred paths will consume their energy resources quickly, possibly causing disconnection in the network.

3.2.4. Cluster based approach

We have discussed about hierarchical organization of the network in tree-based approach. Another important technique to organize the network in hierarchical manner is cluster-based approach. In cluster-based approach, whole network is divided into several clusters. Each cluster has a CH which is selected among cluster members. CHs do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to BS. The advantages and disadvantages of the cluster-based approaches are similar to tree-based approaches.

A Maximum Lifetime Data Aggregation (MLDA) algorithm which finds data gathering schedule provided location of sensors and BS, data packet size, and energy of each sensor has presented in [56]. A data gathering schedule specifies how data packet are collected from sensors and transmitted to the BS for each round. In [57], authors present a Two-Phase Clustering (TPC) scheme. Phase I of this scheme creates clusters with a CH and each node within that cluster form a direct link with CH. Phase I of this scheme is similar to various scheme used for clustering. The CH rotation is localized and is done based on the remaining energy level of the sensor nodes which minimizes time variance of sensors and this leads to energy saving from unnecessary CH rotation. In phase II, each node within the cluster searches for a neighbor closer than CH which is called data relay point and setup up a data relay link. Now the sensor nodes within a cluster either use direct link or data relay link to send their data to CH which is an energy efficient scheme. The data relay point aggregates data at forwarding time to another data relay point or CH. In case of high network density, TPC phase II setups unnecessary data relay link between neighbor’s as closely deployed sensors will sense same data and this lead to a waste of energy.

An energy efficient and secure pattern based data aggregation protocol is designed for clustered environment which is presented in [58]. In conventional method data is aggregated at CH and CH eliminate redundancy by checking the content of data. This protocol says that instead of sending raw data to CH, the cluster members send corresponding pattern codes to CH for data aggregation. If multiple nodes send the same pattern code then only one of them is finally selected for sending actual data to CH. For pattern matching, authors present a pattern comparison algorithm.

3.3 Secure routing Protocol in WSNs

Due to the inherent limitations in sensor networks, routing is a challenging and difficult problem. Most of the routing protocols used in sensor networks are vulnerable to attacks because they were designed to optimize the limited resources rather than focusing on security. After discussing the following five routing protocols, security algorithms in sensor network routing will be examined.

In [59], authors provide a survey of key management schemes in wireless sensor networks. Wireless sensor networks have many applications, vary in size, and are deployed in a wide variety of areas. They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these networks. Sensor nodes used to form these networks are resource-constrained, which make security applications a challenging problem. Efficient key distribution and management mechanisms are needed besides lightweight ciphers. Authors provide many key establishment techniques that have been designed to address the tradeoff between limited memory and security, but which scheme is the most effective is still debatable. It is noticed that no key distribution technique is ideal to all the scenarios where sensor networks are used; therefore the techniques employed must depend upon the requirements of target applications and resources of each individual sensor network.

In [60], authors provide a secure energy-efficient routing protocol (SERP) for densely deployed wireless sensor networks which aims to achieve robust security for transmitted sensor readings with an energy-efficient network backbone. When the sensors with limited energy budgets are deployed in hazardous environment, ensuring energy efficiency and security of the sensor readings becomes a crucial task. Here, they address how to deal with such a deployment scenario. Their protocol ensures secure transmission of data from the source sensors to the base station in a way that it can best utilize the available amount of energy in the network. They use one-way hash chain and pre-stored shared secret keys for ensuring data transmission security. In SERP, first, a sink rooted tree structure is created as the backbone of the network. This energy-efficient network structure is used for authenticated and encrypted data delivery from the source sensors to the base station. To introduce data freshness, SERP includes an optional key refreshment mechanism which could be applied depending on the application at hand.SERP provides a good level of confidentiality and authenticity of data that are transmitted from the sensors to the base station. It also helps for energy-efficient structuring of the network so that the maximum lifetime of the network could be achieved.

In [61], SOAR, a secure route for the false data injection attack model is presented. As the WSN multi-media applications go deep into the military, monitor and other data-sensitive areas, stream data have become the main data processing objects instead of scalar data in WMSN. Because of the difference between the application environments and data features of stream data and scalar data, traditional secure routing for scalar data is not fit for stream data SOAR works in the stream data transfer mode and randomly detects the false data injection attacks.

*Future work***: -** WSN has a bright future. It is used in almost all areas of the daily life which reduce the man power and everything that work according to our requirement. It has potential to revolutionize human-computer interactions. Availability of sensors will lead to new and exciting applications. A lot of research has to be done on WSN’s to improve battery power and reliable security on wireless sensor network so that we can send or receive our data without any miscellaneous attack or losing confidential information.

*Conclusion***: -** by reviewing above all literature of WSN’s we finally realize that WSN’s have become an essential part of our life due to technological advancement in various domains. But due to some limitation like power backup and security issues people hesitate to use this and some time we are not sure about life of sensor which is cost effective.

REFERENCES:-

1. K. Akkaya, M. Younis, “A Survey of Routing Protocols in Wireless Sensor Networks,” Elsevier, Ad Hoc Network Journal, 3 (3): 325-349, 2005.
2. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications Magazine, 40(8): 102-114, 2002.
3. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks, 38(4): 393-422, 2002.
4. C.Y. Chong, S.P. Kumar, B.A. Hamilton “Sensor Networks: Evolution, Opportunities, and Challenges,” Proceedings of IEEE, 91(8):1247-1256, 2003.

5. W. Du, R. Wang, and P. Ning, “An Efficient Scheme for Authenticating Public KeysSensor Networks,” MobiHoc ’05 Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net. and Comp., New York: ACM Press, pp. 58–67, 2005.

6. C.P. Fleeger, Security in computing, 3rd edition, Prentice-Hall Inc. NJ. 2003.

7. A. Perrig et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks, vol. 8, no. 5, pp. 521–34, Sept. 2002.

8. K. Dasgupta, K. Kalpakis, and P. Namjoshi. "An Efficient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks". Wireless Communications and Networking (WCNC 2003). IEEE, Volume: 3, pp.16-20, March 2003.

9. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications, , pp. 113–27, May 2003.

10. J. Newsome et al., “The Sybil Attack in Sensor Networks: Analysis and Defenses,” IPSN '04: Proc. IEEE Int'l. Conf. Info. Processing in Sensor Networks, Apr. 2004.

11. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks,” Proc. IEEE INFOCOM 2003, Apr. 2003.

12. D. K. Goldenberg, J. Lin, A. S. Morse, B. E. Rosen, and Y. R. Yang. Towards mobility as a network control primitive. In *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2004*, Roppongi Hills, Tokyo, Japan, May 24–26, 2004, pp. 163–174.

13. G. Wang, G. Cao, and T. F. La Porta. Movement-assisted sensor deployment. In *Pro- ceedings of IEEE INFOCOM 2004*, Vol. 4, Hong Kong, March 7–11, 2004, pp. 2469–2479.

14. G. Wang, G. Cao, and T. F. La Porta. Proxy-based sensor deployment for mobile sensor networks. In *Proceedings of the First IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2004*, Fort Lauderdale, FL, October 25–27, 2004, pp. 493–502.

15. K. Akkaya, M. Younis and M. Bangad. Sink repositioning for enhanced performance in wireless sensor networks. *Computer Networks*, 49(1):512–534, 2005.

16. J. Kulik, W.R. Heinzelman, H. Balakrishnan, “Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks,” in Proceedings of Wireless Networks, 2002, 8(2/3): 169-185.

17. C. Intanagonwiwat, R. Govindan, D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensors Networks,” in Proceedings of 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 2000, 56-67.

18. D. Braginsky, D. Estrin, “Rumor Routing Algorithm for Sensor Networks,” in Proceedings of First ACM International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA, 2002, 22-31.

19. W. Heinzelman, A. Chandrakasan, H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Micro Wireless Sensor Networks,” in Proceedings of 33rd Hawaii International Conference on System Sciences, Maui, HI, USA, Piscataway, NJ, USA, 2000, 3005-3014.

20. A. Manjeshwar, D.P. Agrawal, “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks,” in Proceedings of 15th International Parallel and Distributed Processing Symposium (IPDPS'01) Workshops, San Francisco, California, USA, 2001, 3, 30189a.

21. A. Manjeshwar and D.P. Agrawal, “APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks,” in Proceedings of International Parallel and Distributed Processing Symposium 2002, 195-202.

22. J.M. Kim, S.H. Park, Y.J. Han, T.M. Chung, “CHEF: CH Election Mechanism Using Fuzzy Logic In Wireless Sensor Networks,” in Proceedings of 10th International Conference on Advanced Communication Technology (ICACT), 2008, 1: 654-659.

23. O. Zytoune, M. Aroussi, M. Rziza, D. Aboutajdine, **“**Stochastic Low Energy Adaptive Clustering Hierarchy,” Journal of Computer Networks and Internet Research ICGST- CNIR, 8(1):47-51, 2008.

24. **S. Stanislava, W.B. Heinzelman,** “Cluster Head Election Techniques for Coverage Preservation in Wireless Sensor Networks,” Elsevier, Ad Hoc Networks Journal, 7(5): 955-972, 2009.

25. G. Gupta, M. Younis, “Load-Balanced Clustering of Wireless Sensor Networks,” in Proceedings of IEEE International Conference on Communication,” 2003, 3:1848-1852.

26. A. Bari, A. Jaekel, S. Bandyopadhyay, “Clustering Strategies for Improving the Lifetime of Two-Tiered Sensor Networks,” Elsevier, Computer Communication Journal, 31(14): 3451-3459, September 2008.

27. N. Amini, M. Fazeli, S. G. Miremadi, M. T. Manzuri, “Distance-Based Segmentation: An Energy-Efficient Clustering Hierarchy for Wireless MicroWSNs,” in Proceedings of 5th Annual Conference on Communication Networks and Services Research, 2007, 18-25.

28. S. Olariu, I. Stojmenovic, “Design Guidelines for Maximizing Lifetime and Avoiding Energy Holes in Sensor Networks with Uniform Distribution and Uniform Reporting,” in Proceedings of 25th IEEE International Conference on Computer Communications, Barcelona, Spain, April 2006, 1-12.

29. J. Lian, K. Naik, G. Agnew, “Data Capacity Improvement of Wireless Sensor Networks Using Non-Uniform Sensor Distribution,” International Journal of Distributed Sensor Networks, 2(2): 121-145, 2006.

30. W. Xiaobing, G. Chen, S.K. Das, “Avoiding Energy Holes in Wireless Sensor Networks with Non-Uniform node Distribution,” IEEE Transactions on Parallel and Distributed System, 19(5):710-720, 2008.

31. C. Song, M. Liu, J. Cao, Y. Zheng et, al , “ Maximizing Network Lifetime Based on Transmission Range Adjustment in Wireless Sensor Networks,” Elsevier, Computer Communication Journal, 32(11): 1316-1325, July 2009.

32. H.Y. Shiue, J.X Lieo-hong, S. Horijuchi, “Energy Saving in Wireless Sensor Networks,” Journal of Communication and Computing, 6(5): 20-28, May 2009.

33. I. Dietrich, F. Dressler, “On the Lifetime of Wireless Sensor Networks,” ACM Transactions on Sensor Networks, 5(1): 5:1-5:39, February 2009.

34. G. Anatasi, M. Conti, M.D. Francesco, A. Passarella, “Energy Conservation in Wireless Sensor Networks,” Elsevier, Ad Hoc networks, 7(3):537-568, May 2009.

35. A. Bari, S. Wazed, A. Jacked, S. Bandyopadhyay, “A Genetic Algorithm based Approach for Energy Efficient Routing in Two-Tired Sensor Networks,” Elsevier, Ad Hoc Networks Journal, 7 (4): 665-676, June 2009.

36. G. Chen, C. Li, M. Ye, J. Wu, “An Unequal Cluster-based Routing Protocol in Wireless Sensor Networks,” Wireless Networks Journal, Springer, 15(2):193-207, February 2009.

37. G. Amato, A. Caruso, S. Chessa, “Application driven Energy Efficient Communication in Wireless Sensor Networks,” Elsevier, Computer Communication, 32(5): 896-906, March 2009.

38. R. Kumar, V. Tsiatsis, M.B. Srivastava, “Computation Hierarchy for in-Network Processing,” in Proceedings of 2nd ACM International Workshop on Wireless Networks and Applications, San Diego, CA, September 2003 , 68-77.

39. S. Rhee, D. Seetharam, S. Liu, “Techniques for Minimizing Power Consumption in Low Data-Rate WSNs,” in Proceeding of IEEE Wireless Communications and Networking Conference, Atlanta, GA, 2004, 3: 1727-1731.

40. A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, J. Zhao, “Habitat Monitoring: Application Driver for Wireless Communications Technology,” in Proceedings of ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, Costa Rica, April 2001, 20-41.

41. A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, “Wireless Sensor Networks for Habitat Monitoring,” in Proceedings of International Workshop on Wireless Sensor Networks and Applications, Atlanta, Georgia, USA, September 2002, 88-97.

42. H. Wang, D. Estrin, L. Girod, "Preprocessing in a Tiered WSN for Habitat Monitoring," EURASIP: Journal of Applied Signal Processing, January 2003, 392-401.

43. G. Smaragdakis, I. Matta, A. Bestavros, "SEP: A Stable Election Protocol for Clustered Heterogeneous Wireless Sensor Networks," in Proceedings of 2nd International Workshop on Sensor and Actor Network Protocols and Applications (SANPA 2004), Boston, MA, August 2004, 251-261.

44. L. Qing, Q. Zhu, M. Wang, "Design of a Distributed Energy-Efficient Clustering algorithm for Heterogeneous Wireless Sensor Networks," Elsevier, Computer Communication Journal, 29(12): 2230-2237, August 2006.

45. Y. Liyang, W. Neng, Z. Wei, Z. Chunlei, "Deploying a Heterogeneous Wireless Sensor Network," in Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), 21-25 September 2007, 2588-2591.

46. X. Wang, G. Zhang, "DECP: A Distributed Election Clustering Protocol for Heterogeneous Wireless Sensor Network," in Proceedings of 7th International Conference on Computational Science (ICCS), Part III, LNCS, 2007, 489: 105-108.

47. A. S. Zahmati, B. Abolhassani, A.A.B. Shirazi, A. S. Bakhtiari, "An Energy-Efficient Protocol with Static Clustering for Wireless Sensor Networks," International Journal of Electronics, Circuits and Systems, 3(2): 35-138, 2007.

48. G. Xin, W.H. Yang, D. De-Gang, "EEHCA: An Energy-Efficient clustering Algorithm for Wireless Sensor Networks," Information Technology Journal, 7(2): 245-252, 2008.

49. B. Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in Proceedings of 6th annual international conference on Mobile Computing and Networking, Boston, Massachusetts, United States, 2000, 243 – 254.

50. M. Stemm, R. H. Katz, "Measuring and Reducing Energy Consumption of Network Interfaces in Hand-Held Devices," IEICE Transactions on Communications, Special Issue on Mobile Computing, 1997, E80-B (8): 1125-1131.

51. E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, "In-network Aggregation Techniques for Wireless Sensor Networks: A Survey," IEEE Wireless Communication, 14(2): 70-87, 2007.

52. S. Madden M.J. Franklin, J.M. Hellerstein, W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," in Proceeding of 5th Symposium on Operating Systems Design and Implementation (OSDI), Boston, MA, 36 December 2002, 131-146.

53. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, "Directed Diffusion for Wireless Sensor Networking," IEEE/ACM Transactions on Networking, 11(1): 2-16, February 2003.

54. S. Nath, P.B. Gibbons, S. Seshan, Z.P. Anderson, "Synopsis Diffusion for Robust Aggregation in Sensor Networks," in Proceeding of 2nd International Conference on Embedded Networks Sensor System, Baltimore, MD, November 2004, 250-262.

55. L. Gatani, G.L. Re, M. Ortolani, "Robust and Efficient Data Gathering for Wireless Sensor Networks," in Proceeding of 39th Annual Hawaii International Conference on System Sciences, 4-7 January 2006, 9: 235.1.

56. K. Kalpakis, K. Dasgupta, P. Namjoshi, "Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks," in Proceeding of IEEE International Conference Networking, August 2002, 685-696.

57. W. Choi, P. Shah, S.K. Das, "A Framework for Energy-Saving Data Gathering Using Two-Phase Clustering in Wireless Sensor Networks," in Proceedings of International Conference on Mobile and Ubiquitous Systems: Networking and Services , Boston, 2004, 203-212.

58. H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, "ESPDA: Energy-Efficient and Secure Pattern-based Data Aggregation for Wireless Sensor Networks," in Proceedings of Second IEEE Conference on Sensors, Toronto, Canada, 22-24 October 2003, 732-736.

59. Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway"A Survey of Key Management Schemes in Wireless Sensor Networks"; Computer Communications, Special Issue On Security On Wireless Ad Hoc and Sensor Networks

60. AI-Sakib Khan Pathan and Choong Seon Hong,"Secure energy-efficient routing protocol for densely deployed wireless sensor network"Ann. Telecommun.(2008)63:529-541 DOI 10.1007/s12243-008-0042-5

61. Md. Abdul Hamid and Choong Seon Hong,"Energy conserving security mechanisms for wireless sensor networks,Annals of Telecommunications(2009)Volume 64,Numbers 11-12,723-734,DOI: 10.1007/978-0-387-33112-6-15

62. https://www.google.co.in/search?tbm=isch&hl=en-IN&source=hp&q=wireless+sensor+networks&gbv=2&oq=wireless+se&gs_l=img.1.0.0l10.2723.14879.0.17072.11.8.0.3.3.0.359.2113.0j1j5j2.8.0....0...1ac.1.34.img..1.10.1926._M9XOxDQC40