Chapter-II

Literature Review
A thorough review of literature is a mandate before the design of any novel algorithm for WSNs. A survey of the routing protocols is presented by classification of the protocols on the basis of secure routing, power management, cryptographic and non-cryptographic algorithms. The secure routing algorithms are further detailed into hierarchical, multipath and geographical routing. Power management schemes are classified into device and network level approaches. Cryptographic and non-cryptographic algorithms include protocols that are listed under flat and hierarchical routing protocols. Figure 2.1 shows the routing protocol categories investigated for WSNs in this survey.

Figure 2.1 Categories of WSN routing techniques
2.1 SECURE ROUTING ALGORITHMS

Most of the routing protocols for WSN do not support the security and they are mainly concerned only about the data transfer (Mahgoub & Ilyas, 2016). The secure routing protocols for sensor networks are broadly classified into three types.

1. Secure hierarchical routing protocol
2. Secure multipath routing protocol
3. Secure geographical routing protocol

2.1.1 Secure hierarchical routing protocol

Hierarchical Secure Routing protocol against Black Hole attacks (HSRBH) were designed for WSN. A black hole attack is a severe attack that can be easily employed against routing in sensor networks (Yin & Madria, 2006). In a black hole attack, a malicious node spuriously announces a short route to the sink node to attract additional traffic to the malicious node and then drops them. The hierarchical secure routing protocol detects and defends against black hole attacks and uses only symmetric key cryptography to discover a safe route against black hole attacks.

Two Tier Secure Routing (TTSR) protocol for heterogeneous sensor networks has two heterogeneous network models (Du et al, 2007). They are High-end Sensor (H-Sensor) and Low-end Sensor (L-Sensor). H-Sensors are tamper resistance which cannot be easily compromised. TTSR has two tier routing scheme called intra-cluster routing and inter-cluster routing. Intra-
cluster routing is the routing executed within the cluster and inter-cluster routing is the routing across the cluster. In intra-cluster routing, the packets are sent to the Cluster Head (CH) by constructing the minimum spanning tree or shortest path. For inter-cluster routing, the CH eliminates the redundant data and forwards the data to the Base Station (BS) after verifying the key and location information. This protocol eliminates the Sybil attack with the help of authentication among the nodes to guarantee that one node cannot pretend to be another node. Moreover, this protocol defends against sink hole and wormhole attacks. Data are transferred to BS with the help of H-Sensor and relay cells. Hence, the attacker cannot modify the route in TTSR. It prevents the flood attack, as the L-Sensor utilizes the two-way handshake protocol to initiate the neighbour relationship.

A key management scheme based on random key pre-distribution for Heterogeneous Sensor Network (HSN) suffers from high communication overhead, computation overhead, and/or high storage requirements (Kausar et al, 2008). In a key pre-distribution phase, all the keys of the key pool are assigned to H-sensors and only one key of that pool is assigned to L-sensor, which significantly reduces the storage requirements while providing full network connectivity. Message Authentication Code is calculated among the nodes with the help of a shared pair wise key. Sink hole and worm hole attacks are not possible because attacker node cannot route the packet in relay cells among H-Sensor and BS. Since H-Sensors are tamper resistant, they enjoy safeguard from the node compromise attack, but L-Sensors can be
compromised. To overcome this issue, the packet is included with the unique ID and compromised node ID is also attached. The attacker node cannot receive the data.

Secure Routing protocol against Wormhole Attacks (SeRWA) protocol in sensor networks avoids the use of any special hardware such as the directional antenna and the precise synchronized clock to detect a wormhole. Moreover, it provides a real secure route against the wormhole attack (Madria & Yin, 2009). SeRWA protocol only has very small false positives for wormhole detection during the neighbour discovery process. The average energy usage at each node for SeRWA protocol during the neighbour discovery and route discovery is below 25 mJ, which is much lower than the available energy at each node. The cost analysis shows that SeRWA protocol only needs small memory usage at each node, which is suitable for the sensor network.

Secure alternate path Routing IN Sensor (SeRINS) networks detect and isolate the compromised nodes, which try to inject inconsistent routing information, from the network by neighbour report system (Lee & Choi, 2006). In neighbour report system, a node’s route advertisement is verified by its surrounding neighbour nodes so that the suspect node is reported to the BS and is excluded from the network. SeRINS is resilient in the presence of several compromised nodes which launch selective forwarding attacks and robust by excluding the compromised nodes which inject inconsistent routing information from the network.
Secure routing protocol for sensor networks safeguards sensor networks against different types of attacks (Yin & Madria, 2006). This protocol uses symmetric cryptography to secure messages, and uses a small cache in sensor nodes to record the partial routing path to the destination. It guarantees that the destination will be able to identify and discard the tampered messages and ensure that the messages received are not tampered.

Random pair-key for Low Energy Adaptive Clustering Hierarchy (RLEACH) protocol for sensor network is an extension of Low Energy adaptive Clustering Hierarchy (LEACH) protocol (Zhang et al, 2008). LEACH protocol suffers severe attacks and they are not secure. RLEACH is introduced, which uses the Random Pairwise Key (RPK) for security. RPH that manages the key pool comprises L different key chains. The key chain is established with the help of hash function by public seed and key. It prevents the network from network layer attacks like selective forwarding attack. This protocol uses the node-to-node authenticating. Hence, Sybil attack and hello flood attacks are not possible in this protocol.

An authentication framework uses certificates for authentication (Bohge & Trappe, 2003). The use of message authentication code in the framework protects all data against malicious modification and information forgery. It present an authentication framework for an application driven hierarchical ad hoc sensor network and deals with compromised nodes (Sadananda et al,
2013). It cannot prevent intruders from entering, sending packets and cannot protect against eavesdropping in the network.

Secure Routing Protocol for Sensor Networks (SRPSN) was an energy-efficient level-based hierarchical routing technique (Tubaishat et al, 2004). They have designed a secure routing protocol for WSNs to safeguard from different attacks by building a secure route from the source to sink node (Perrig et al, 2002). They used the symmetric key cryptography and designed a group key management scheme for secure communication, which contains group communication policies; algorithm and a group membership requirement for generating a distributed group key. One drawback associated with this protocol was that there was no authentication mechanism. SRPSN fails against some attacks like spoofing, altering and replaying.

Securing heterogeneous hierarchical WSNs with an arbitrary number of levels uses the symmetric key scheme and has following assumption: an adversary to compromise the group key takes a certain time or temper with a node in the communication network (Oliveira et al, 2005). It prevents intruders (outsider attacker) from taking to activity, tempering with or injecting the message into the networks and prevents eavesdropping on communication between legitimate nodes (Karlof & Wagner, 2003). Authentication and confidentiality are maintained by shared pairwise key. It deals with orphan node problem.
Efficient Security Model of Routing (ESMR) protocol uses only public key cryptography technique (Chen et al, 2008). ESMR’s performance is not better in an environment where there are no attackers, but it becomes useful when the number of attacker node increases inside the communication network. This protocol only deals with outsider attack and computation burden is high due to the use of public key cryptography (Rabin, 1989).

The objective of Secure Routing Protocol Cluster Gene Based (SRPBCG) for WSNs was to manage trust and reputation locally and to authenticate an identity of a node with minimal overhead and time delay (Zhou & Li, 2009). Biological authentication mechanism has been used, biological “gene” as the encryption key is very secure and efficient key distribution scheme, which require only few memory and communication overhead. This method deals only with the adversary’s attack and compromised nodes.

Secure Hierarchical Energy Efficient Routing (SHEER) protocol provides secure communication at the network layer (Ibriq & Mahgoub, 2006). It uses the three-level hierarchical clustering architecture and the probabilistic broadcast mechanism to improve the network energy performance and increase its lifetime. To secure the routing, SHEER protocol developed asymmetric key cryptography technique and a secure key transmission protocol.

Novel Hierarchical Routing Protocol Algorithm (NHRPA) is a routing protocol which adopts suitable routing technology for the nodes according to the distance of the node to BS, density of the nodes distributed and residual
energy of the nodes (Cheng et al, 2008). It was compared with Directed Diffusion (DD) regarding the energy usage, packet latency and security in the presence of node compromised attacks (Fang et al, 2005). This routing protocol does not use any cryptography technique and so the overhead is small. But only node compromise attack is prevented in it.

Authentication Confidentiality cluster based secure routing protocol uses both public key (in digital signature) and private key cryptography (Srinath et al, 2007). This protocol deals with the interior adversary or compromised node. Because of the high computational requirement (use of public key cryptography), it is not efficient for the WSNs.

2.1.2 Secure multipath routing protocol

Secure-Sensor Protocol for Information via Negotiation (S-SPIN) protocol does not include any security algorithms for data transfer. It is vulnerable to many attacks (Tang & Li, 2009). S-SPIN protocol is a three stage protocol where the node uses three categories of messages: 1.advertise, 2.request and 3.data message. When a sensor node receives a new data, it sends an advertise message to its neighbour nodes. The interested nodes forwards the request messages to retrieve the data. Advertise and request messages are protected though use of a MAC. It ensures secure data transfer among the sensor nodes. S-SPIN protocol works more efficiently and consumes lesser energy and bandwidth. It forwards the metadata to the neighbours before forwarding the original data.
Intrusion Tolerant Secure Routing Protocol (ITSRP) integrates the authenticated key exchange and energy factor into the secure routing algorithm and tolerates damage caused by salient intruders who has compromised deployed sensor nodes and is intent on injecting, modifying or blocking packets (Zhou et al, 2008). The security mechanism incorporated provides defence against wormhole attacks, sinkhole attacks and sybil attacks. ITSRP has three phases: Phas1. path discovery, Phas2 route establishment and Phas3 secure data transfer. When a source node needs to forward a message to destination, it has neither shared session key nor route path. The source node transmits packets with a unique tag and set the ancestor value as ‘0’. It broadcasts the message to the entire network within the range. The nodes accept the message and verify the destination address. When the node is not the given destination, then it updates the routing table and sends the packet. If it is recognized as the destination, it recovers the packet with the distributed key and updates the routing table. In the last phase, the node transfer the data using session key.

A secure routing and aggregation protocol with low energy cost for sensor networks was designed which utilized a one-way hash chain and multi-path mechanism to achieve security of WSNs and develop a network expanding model to control communication cost incurred by multi-path routing (Gui et al, 2009). This protocol is composed of three phases: 1.initialization phase, 2.data transfer and 3.filtering and source authentication sink. During the initialization phase, the destination node broadcast the hello message to the sensor nodes. During data transfer and filtering, the source node forwards the
data to its parent node and then transfers the data to the destination node using hop by hop fashion. In the last phase, the protocol authenticates the source node identity and data integrity.

Curve Based Greedy Routing (CBGR) generates a curve for data transmission. All the sensor nodes broadcast the packet with Time To Live (TTL), the position of the node and sequence number (Cheng et al, 2006). On receiving this message, the protocol generates the neighbour table and each sensor has the sharing key with its direct neighbour node. The flooding method is used by the destination to broadcast the position and required data. The destination node uses the master key to estimate the length of the key and encrypts the message and then broadcast it. This protocol creates B-Spline curve to transfer the data as it needs lesser computation complexity which consumes less energy. This protocol is resilient against selective forwarding attack. Moreover, CBGR does not manage all the connections between sources to destination, hence it prevents the network from hello flooding attack.

Secure routing protocol with malicious node detection and diagnosis for WSNs uses the µ-Timed Efficient Stream Loss-tolerant Authentication (Jiang & Zhao, 2007). Most of the secure routing approaches consider the flat network. But this approach uses the cluster network and uses the simplest way to identify the malicious nodes. A node ‘m’ forwards the data and saves the data in the buffer and wait for receiving the acknowledgment. If the
acknowledgment message is not received, then it is recognized as the malicious node. This process gets repeated until the data reaches the destination node.

In segment Transmission Secure Routing Protocol, the source node identifies the neighbour nodes and decides some of the sensors as relay nodes (Wen et al, 2006). The source node splits the data into small segments on the basis of the code type and length, the number of relay nodes and provides a unique identification number for each segment. The source encrypts the message with the help of shared key and appends the code which verifies the data automatically. The source node appends the message header for all the segmented data. The header includes message ID, sensor ID, number of segments and index. This protocol uses the light weighted cryptography for encryption. This protocol consumes lesser energy for data transmission.

2.1.3 Secure geographical routing protocol

The trust technology and node’s location information are employed in the process of routing (Yao & Zheng, 2008). At the same time, for prolonging the life of the network, the residual energy is still regarded as an important factor to make routing decision. Based on the method of weighted sum of square in the multi-objective optimization technology, a secure routing scheme is put forward, in which the routing decision is made by the residual energy, trust value and the hops to destination sink. This routing scheme can achieve secure routing and prolong the life of the network simultaneously. This protocol has three main phases: initialization phase, routing discovery phase
and acknowledgement phase. Initialization phase is divided into online and offline. During the online phase, every node estimates its hops to every destination and formulates its neighbour list based on their distance. If the distance between the cell centre and the centre of its one neighbour cell is greater, then it is recognized as the malicious node and moved into the blacklist. If the source node accepts the acknowledgment message from the neighbour node, then the packet can be forwarded successfully.

Secure Routing on the Diameter (SRD) provides efficient and scalable data delivery from source to destination node (Yin et al, 2003). It uses the token strategy for providing to a huge sensor network. Hence, the energy taken for computation is lesser for calculation. Ticket server is used to establish the route in diameter with the help of pre-loaded token. The server encrypts the data with the help of its private key. During data transmission, the nodes authenticate each other with the help of the private key.

Geographical Energy Aware Routing (GEAR) was an energy-efficient routing protocol for routing queries to target regions in a sensor field (Yu et al, 2001). In GEAR, the sensors are supposed to have localization hardware equipped, for example, a Global Positioning System (GPS)unit or a localization system so that they know their current positions (Bulusu et al, 2000). Furthermore, the sensors are aware of their residual energy as well as the locations and residual energy of each of their neighbours inside the network. GEAR uses energy aware heuristics that are based on geographical information
to select sensors to route a packet toward its destination region. GEAR uses a recursive geographic forwarding algorithm to disseminate the packet inside the target region.

2.2 POWER MANAGEMENT ALGORITHMS

The main source of energy is usually battery power. Sensors are often intended for deployment in areas such as a battlefield or radiation plants; once deployed, it is impossible to recharge or replace the batteries of sensors. But long system life time is needed for any monitoring application. Important challenge to the design of a WSN is the energy efficiency problem. Static power saving techniques maintains the same characteristics throughout the network lifetime (Nayyar, 2013). On the other hand, dynamic techniques adapt to changes in the network, allowing enhanced power saving mechanisms for attaining prolonged network lifetime. To save energy, both approaches apply the partial or total turn off of some or all node units.

Energy Aware Routing (EAR) protocol is a reactive protocol that aims at increasing the lifetime of the network (Sendra et al, 2011). This protocol seeks to maintain a set of paths instead of maintaining or enforcing one optimal path at higher rates, although the behaviour of this protocol is similar to directed diffusion protocols. These routes are selected and maintained by a probability factor. The value of this probability depends on the lowest level of energy achieved in each path. The energy of a path cannot be determined easily as the system has several alternatives to establish a route. Network survivability
is the main metric of this protocol, which assumes the addressable feature of each node through a class-based addressing scheme which includes the location and the type of nodes.

Initially, there is a process of flooding, which is used for discovering all the routes between various source/destination pairs and their costs. This will allow the creation of routing tables, where high-cost paths are discarded (Shah & Rabaey, 2002). Data is sent to its destination using these tables with a probability that is inversely proportional to the cost of the node. The destination node performs a localized flooding in order to maintain the paths that are still operative. However, having to collect location information, and the establishment of the steering mechanism for nodes, complicates the path settings.

An extra energy saving is possible in the system by using Dynamic Power Management (DPM), which shuts down the sensor node when there is no event. The basic idea is to shut down sensor devices when not needed and wake them up when really necessary so as to perform the sensor network tasks (Sinha & Chandrakasan, 2001). However, it is not easy to decide which node should sleep and which should be active at any given time, because these decisions strongly depend on the application running on the top of the network. It is not desirable to keep nodes inactive for too long, because it can impact the QoS. Depending on the approach that is used, DPM policies are classified as predictive or stochastic policies. Predictive schemes attempt to predict a
device’s usage behaviour in the future usually based on the past history of usage patterns and decide to change power states of the device accordingly. A widely used predictive technique consists of turning OFF the system components if the idle time being greater than or equal to a timeout threshold value T. This approach is based on the assumption that, if the idle time is greater than the threshold T, the system is likely to remain idle for a long time to save energy. Prediction based dynamic power management can be categorized into two groups: 1. adaptive and 2. non-adaptive. Non-adaptive strategies set the idleness threshold for the algorithm once and for all and do not alter them based on observed input patterns. On the other hand, adaptive strategies use the history of idle periods to guide their decisions of the algorithm for future idle periods. Stochastic approaches make probabilistic assumptions about usage patterns and exploit the nature of probability distribution to formulate an optimization problem, the solution to which drives the DPM strategy. Reduction in the power dissipation in the various operations can be accomplished from two different scopes: device-level, and network-level.

2.2.1 Device Level Approaches

This section presents the approaches for reducing the power consumed in Measurement Nodes (MNs) excluding networking operations. It comprises of hardware component selection and their configuration to achieve minimum energy consumption. Based on this concept, many techniques have been proposed.
Dynamic Voltage Scaling (DVS) has become a promising way for WSNs to exploit multiple voltage and frequency levels and prolong the sensor node’s life. However, pure DVS for embedded systems did not perform well without considering the feature of WSNs’ workloads (Tuming et al, 2010). A task-driven feedback dynamic voltage scaling algorithm was designed based on the multi-hop routing and topology changed easily could scale the working frequency and voltage levels dynamically according to the workloads of sensor node, fix the errors through feedback scheme and reduce the node’s power consumption at the premise of real-time tasks.

Dynamic Modulation Scaling (DMS) optimizes transmission energy with respect to number of packets that need to be transmitted at that particular time intervals (Joshi et al, 2007). DMS trades off transmission energy against transmission delays. Multilevel modulation is the key aspect for dynamic modulation scaling. Dynamic variations in the constellation size $b$ (number of bits per symbol) with respect to number of packets that need to be transmitted helps in optimizing transmission power. In this scenario it is very important to decide minimum and maximum bounds on constellation size (scale of modulation) otherwise it may result in performance degradation. Various factors affecting minimum and maximum limit of $b$ are discussed and it is shown that the individual node can decide minimum limit on $b$ but for deciding maximum limit it needs to consider network aspects such as network topology, node density, location of particular node etc. Appropriate selection of these
limits alone can provide optimized power consumption with satisfactory performance. Otherwise trying to save energy without satisfying performance parameters will require retransmission and the energy cost for that will be much higher than what was saved earlier.

Radio power consumption strongly depends on the packet size. Therefore, removing redundancy existing in the data is essential to find a more compact representation. Compression may be lossy or lossless according to the compression algorithm. There are different algorithms for data compression in WSNs such as wavelet transform and low-complexity video compression (Kimura & Latifi, 2005).

Cognitive agents capable of making proactive decisions based on learning, reasoning and information sharing when interspersed in sensor networks may help achieve end-to-end goals of the network, even in the presence of multiple constraints and optimization objectives. Cognitive radio at the physical layer of such agents would have the ability to enable the opportunistic use of the heterogeneous environment in which the sensor network is deployed (Vijay et al, 2010). Providing a comparative study of the different cognitive techniques applied to sensor network applications in recent times and evaluating their effectiveness in achieving the network’s end-to-end goals is considered as the main contribution.

Cognitive radio at the physical layer may enable the opportunistic use of the heterogeneous wireless environment. However, research efforts have been
Discrete and cognitive techniques have focused on improving specific aspects of the network or benefiting specific applications. The main contribution is the provision of the vision and advantage of a holistic approach to cognition in sensor networks, which can be achieved by incorporating learning and reasoning in the upper layers and opportunistic spectrum access at the physical layer (Vijay et al., 2010). Rather than providing an ostensive survey of cognitive architectures applicable to sensor networks, this concept provides the reader with a framework based on knowledge and cognition that can help achieve end-to-end goals of application-specific sensor networks.

Data acquisition controls the sensing power especially in cases of “energy-hungry” sensors such as gas and GPS sensors. For instance, adaptive sampling techniques reduce the number of samples by exploiting spatiotemporal correlations between sensed data (Alippi et al., 2007).

2.2.2 Network Level Approaches

A collection of power saving techniques which involve optimization of communication techniques and networking protocols is presented in this section.

The techniques meant for mobility are based on employment of n mobile sinks or mobile relay nodes in order to reduce the number of multi-hops and thereby minimizing the transmission cost (Dong & Dargie, 2013). These mobile nodes are often attached to mobile entities in the environment such as vehicles, animals or dedicated robots. In data-driven approach, distributed processing is
made throughout the entire network in order to prolong the WSN lifetime. For instance, Compressive Sensing (CS) is a distributed compression technique in which the data is processed to remove redundancy by exploiting spatial correlation (Balouchestani et al, 2011). CS depends on reconstructing the sparse WSN’s data from a small number of random-linear readings. A prediction based data reduction algorithm based on the Least Mean Square (LMS) algorithm was implemented on a FPGA to reduce the communication between the sensor nodes and the BS.

Data prediction is a technique in which identical predictors, implanted in the source and sinks nodes, are utilized in order to minimize the number of transmitted packets (Debono & Borg, 2008). Many prediction algorithms are utilized in WSNs including time series forecasting, stochastic and algorithmic approaches. WSN spawns a surge of unforeseen applications. The diversity of these emerging applications represents the great success of this technology. A fundamental performance benchmark of such applications is topology control, which characterizes how well a sensing field is monitored and how well each pair of sensors is mutually connected in WSNs (Li & Yang, 2006). Existing topology control techniques are classified into two categories: 1. network coverage and 2. network connectivity. For each category, a surge of existing protocols and techniques are presented with the focus on blanket coverage, barrier coverage, sweep coverage, power management and power control that attract significant research attention in recent years.
Transceivers consume a major portion of the available energy. Therefore, switching the transceiver into the sleep mode helps prolonging the network lifetime. Selecting the node that has to go to sleep can be based either on aggregation techniques, redundancy control or on MAC protocols. In the first approach, data is aggregated either through event driven, periodic sampling or store and forward strategies. The second approach exploits network redundancy to extend the network longevity by switching a number of redundant MNs into sleep mode. In the meantime, active MNs can also be switched into sleep mode according to the workload to further save energy (Baronti et al, 2007). Choosing the active MNs can be accomplished in two ways: 1. a location-based approach and 2. connectivity-based approach. In the former procedure, the sensing field is divided into cells. In each cell, only one MN is activated while the others are switched to sleep mode.

MAC protocols have the responsibility for the coordination between neighbours. Optimizing MAC protocols leads to significant reduction in power consumption. For instance, Time Division Multiple Access (TDMA) is a well-known MAC protocol. Data collision is avoided by dividing the time frame into slots. Time frames are divided into slots where each node is assigned two fixed time slots for transmitting and receiving packets (Czapski, 2006). As a result, MNs are active during their assigned slots and inactive during other slots. Advantages of the TDMA protocol comprise elimination of data collision and conserving significant amount of energy. However, this technique
requires a precise synchronization among the various nodes which may be
difficult in many situations.

Routing is the process of delivering information to the destination
through a short path. Many optimization techniques have been proposed for the
improvement of the performance of this task in terms of energy consumption
(Cirstea, 2011). A classification of routing protocols for WSNs focuses on the
following categories:

2.2.2.1 Multipath based protocols

MNs determine the k-shortest paths to the sink node. MNs divide their
load evenly among these paths. Sensordisjoint multipath and braided multipath
protocols are based on this concept.

2.2.2.2 Data centric protocols

Protocols in this category, MNs send their information to the sink node
via neighbouring nodes. These intermediate nodes aggregate the readings and
perform different processing in order to reduce the traffic. Examples of this
approach include Sensor Protocols for Information via Negotiation (SPIN) and
Energy Aware Data-centric (EAD) routing.

2.2.2.3 Heterogeneity based protocols

The core idea of protocols in this category is to utilize special nodes
with unlimited energy sources for assisting the battery-powered sensors in
aggregating information. Examples of protocols include Information Driven Sensor Query (IDSQ) and Cluster Head Relay (CHR) routing.

### 2.2.2.4 QoS based protocols

Many paths are formed between the sink and the sensor nodes. Then, a path is selected which optimizes energy consumption and other QoS parameters such as availability, reliability or latency. Examples are Sequential Assignment Routing (SAR) and energy-aware QoS routing.

### 2.2.2.5 Hierarchical clustering based protocols

Hierarchical protocols are suitable for continuous transmission due to the presence of redundant data. Specifically, this approach of using hierarchical protocols is based on splitting the network into groups called clusters. One node from each cluster, is elected as a CH. It aggregates the packets from its cluster members. Optimizing the collected information could be accomplished by the CH in order to decrease energy and traffic. Examples of hierarchical clustering include LEACH, Power Efficient Gathering in Sensor Information Systems (PEGASIS) and Adaptive Periodic Threshold sensitive Energy Efficient sensor Network (APTEEN) protocol.

LEACH, a hierarchical routing protocol is a TDMA based MAC protocol which is integrated with the clustering and a simple routing protocol in WSN (Pal et al, 2010). The goal of LEACH is to economize energy consumption required for creation and maintenance of clusters in for improving the lifetime of a WSN. In LEACH protocol, BS is fixed and located far away
from sensors and all sensor nodes are same in nature. LEACH randomly selects CH for energy balancing purpose. So, all sensors consume the same battery power. BS is a high energy node while the leaf node is low energy node. In this, most nodes transmit to CHs and CHs aggregate and compress the data and forward it to the BS. LEACH performs in rounds, it has two phases: Setup Phase and Steady phase. In setup phase, clusters are created and CH is selected randomly for each cluster, whereas in steady phase leaf node sends data to CH within certain time period using TDMA.

Threshold sensitive Energy Efficient sensor Network (TEEN) is a cluster based routing protocol which is based on LEACH (Manjeshwar & Agrawal, 2001). This protocol transfers the data less frequently and senses the medium continuously. The network consists of simple nodes, first level CHs and second level CHs. LEACH strategy is used in this protocol for cluster formation. First level CHs are formed away from the BS and second level CHs are formed near the BS. It is targeted at reactive networks and is the first protocol developed for reactive networks. The main drawback of this scheme is that, if the thresholds are not reached, the nodes will never communicate and the user will not get any data from the network and will not come to know even if all the nodes die. This protocol is not well suited for applications where the user needs to get data on a regular basis.

APTEEN is the improved version of the TEEN which enables reliable monitoring and analysis of the environment (Manjeshwar& Agrawal, 2002).
decision is taken on, in the CHs in each cluster period, the CH first broadcasts the following parameters: attributes, thresholds, schedule and count time. If a node does not send data for a time period equal to the count time, it is forced to sense and retransmit the data, thereby maintaining energy consumption. Since it is a hybrid protocol, it can emulate a proactive network or a reactive network depending on the count time and threshold value. One of the limitations of this protocol is that in order to implement the threshold function and count time additional complexity is required.

In PEGASIS, each node communicates only with a close neighbour and takes turns transmitting to the BS, thus reducing the amount of energy spent per round (Lindsey & Raghavendra, 2002). This approach will distribute the energy load evenly among the sensor nodes in the network. Nodes will be organized to form a chain, which can either be accomplished by the sensor nodes themselves using a greedy algorithm starting from some node. Alternatively, the BS can compute this chain and broadcast it to all the sensor nodes. For gathering data in each round, each node receives data from one neighbour, fuses with its own data and transmits to the other neighbour on the chain. PEGASIS performs data fusion at every node except the end nodes in the chain. Each node will use its neighbour’s data with its own to generate a single packet of the same length and then transmit that to its other neighbour. Thus, each node in PEGASIS receive and transmits one packet in each round and be the leader once every 100 rounds.
Group based Sensor Network (GSEN) can be divided into two phases: 1. Group formation phase and 2. Transmission phase (Tabassum et al, 2006). GSEN prefers reconstruction of groups after every $R$ number of rounds. Therefore, once the groups are formed they remain fixed for the next $(R-1)$ number of rounds but the responsibility of the group leader keeps on changing randomly among the other member nodes of the group at every round (Song, 2005). Each group in GSEN covers a particular geographical region, and each group leader acts as a representative of that region. Each leader accumulates data from the member nodes within its group, at the beginning of the data collection and transmission phase.

There arise some typical hierarchical routings, which are variants of cluster-base routing and present special hierarchical architecture, including chain-based, tree-based, grid-based and area-based routing (Liu, 2015). Hierarchical routing of these types are similar to the traditional cluster based routing, but are different in hierarchy division and communication.

- **Chain Based Routing**

  In chain-based topology, one or more chains are constructed for the connection of the deployed sensor nodes for data transmission. In a chain, a leader is selected to perform the task of data collection, like a sink. Data is delivered along the chain and ultimately to the leader node. Data aggregation is performed during the process of transmission. For chain based routing, it has a simple topology compared with traditional cluster-based routing, because such
a topology is easy to implement and maintain. In chain based routing, a node only sends data to its next node, which is very close to it. So, a part of energy is saved by local communication compared to intra-cluster communication in cluster-based topology. The entire network is organized to one or multiple chains in chain-based topology and generally a chain is very long with large number of hops from one end to the other in the chain. Thus, data transmission needs large delay with large number of hops.

- **Tree Based Routing**

  In tree based routing, a logical tree is constructed by all sensor nodes. Data is delivered from leaf nodes to their parent ones. In turn, the parent nodes send the received data to their parent nodes towards the root nodes. Data aggregation is possibly performed in each node. Tree topology is simpler than cluster-based routing includes a relatively complex process of cluster formation. Energy consumption is decreased compared to flat routing in WSNs, because flooding is not necessary for data transmission. Data transmission is performed between neighbour nodes and therefore can save much energy consumption.

- **Grid Based Routing**

  In a grid based topology, the network is divided into various grids using the geography approach. Thus, grid-based routing generally belongs to location-aware routing. The distinct characteristic of this type of routing is that the routing operation is performed without any routing table. Once the position
of the destination is achieved by the source, all routing operations are locally performed. In grid-based networks, grids are regularly constructed by geographic locations and CH competition and Ordinary Nodes (ONs) selection can be left out. So the hierarchical structure is simple compared with cluster-based routing. It can provide efficient data delivery in WSNs, since each node only maintains a simple forwarder candidate to transmit data.

- **Area Based Routing**

  Area-based topology is an up-to-date structure, where in some sensor nodes are designated in a specific area and act as high-tier nodes. Generally, such nodes perform the task of data collection from ONs and data transmission to the sink. The size of the area can be adjusted on the basis of the load balancing requirements. Such topology is always used in mobile WSNs. Only a specific area requires determination and it is easy to locate the nodes that act as high-tier tasks. Therefore, the structure of area-topology is also simpler than that of cluster-based routing which includes a relatively complex process of cluster establishment. There is reduction in energy consumption is decreased compared with other clustering routing schemes in WSNs, because data exchange is performed in the local regions. This can avoid long-distance communication and decrease large energy dissipation.

### 2.3 CRYPTOGRAPHIC ALGORITHMS

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process
Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit (Akkaya & Younis, 2005). However, in today’s computer-centric world, cryptography is most often associated with scrambling plaintext into ciphertext, then back again. Individuals who practice this field are known as cryptographers.

- **Secure sensor protocol for information via negotiation**
  
  SPIN is a data dissemination protocol that disseminates its information to all the nodes in its vicinity (Xiao et al, 2006). Secure SPIN is the secure extension for the SPIN protocol which is divided into three phases and uses some cryptographic functions that require small memory and processing power to create an efficient and practical protocol (Heinzelman et al, 1999). This protocol increases the security of data communication in WSNs. SPIN is classified in different classes like SPIN-Point to Point, SPIN-Broadcast, SPIN-Reliable and SPIN-Energy Centric and is used depending upon the application.

- **Directed diffusion**
  
  DD is a flat network protocol that works on the principle of flooding (Sohrabi et al, 2000). The sink node floods the interest signal in the network through the neighbors. On receipt of a request, every node maintains an interesting cache. This is maintained till the gradient is not formed. The gradient is a reply link through which a request was received. Gradient contains all the information about the path (i.e.) data rate, duration, etc. among all the
paths formed from sink to source the best path is selected through the reinforcement process.

- **Gradient-based routing**

  Gradient Based Routing (GBR) techniques such as the GBR-Generic and the GBR-Competing have been previously proven to be energy efficient in single sink WSNs (Migabo et al, 2015). Enhanced GBR-G and GBR-C routing approaches consider the definition of a gradient model to maximize network lifetime. The generic energy balancing-GBR and competing for energy Balancing-GBR techniques not only consider the selection of the highest gradient link but also the link that avoids the most overloaded sensor nodes when forwarding packets.

- **Sequential assignment routing**

  Sequential Assignment Routing is based on the association of a priority level to each packet (Al-Karaki & Kamal, 2004). Additionally, the links and the routes are related to a metric that characterizes the potential provision of QoS. This metric is based on delay and the energy cost. Then, the algorithm creates trees rooted at one-hop neighbours of the sink. Parameters including packet priority, the energy resources, and the QoS metrics are taken into consideration for this approach. This protocol must periodically recalculate the routes to be prepared in case of failure of one of the active nodes.
• **Minimum cost forwarding algorithm**

Minimum Cost Forwarding Algorithm exploits the fact of the knowledge of the direction of routing that is, towards the external BS. Hence, a sensor node need not have a unique ID nor maintain a routing table (Ye et al, 2001). Instead, each node maintains the least cost estimate from itself to the BS. Each message to be forwarded by the sensor node is broadcast to its neighbours. When a node receives the message, it checks if it is on the least cost path between the source sensor node and the BS. If this is the case, it re-broadcasts the message to its neighbours. This process is repeated until the BS is reached. In MCFA, each node should know the least cost path estimate from itself to the BS.

• **Little energy adaptive clustering hierarchy**

LEACH is a TDMA based MAC protocol which is integrated with clustering (Yadav & Sunitha, 2014). The goal of LEACH is to lower the energy consumption required to create and maintain clusters to improve the lifetime of a WSN. All nodes that are not CHs only communicate with the CH in TDMA, according to the schedule created by the CH. LEACH also uses Code Division Multiple Access (CDMA) so that each cluster uses a different set of CDMA codes, to minimize interference between clusters.

• **Two Level-LEACH**

Two Level-LEACH was an extension of the LEACH algorithm (Loscri et al, 2005). It utilizes two levels of CHs in addition to the other simple sensing
nodes. In this algorithm, the primary CH in each cluster communicates with the secondaries, and the corresponding secondaries communicate with the nodes in their sub-cluster. Data-fusion can also be performed as in LEACH. Also, communication within a cluster is still scheduled using TDMA time slots. The organization of around will consist of first selecting the primary and secondary CHs using the same mechanism as LEACH, with the a priori probability of being elevated to a primary CH less than that of a secondary node.

- **Specification-based secure LEACH**

  Specification-based Secure LEACH is a protocol based on LEACH protocol, considering routing security and network lifetime (Wu et al, 2008). Improving the method of electing CHs, the SS-LEACH protocol forms dynamic stochastic multipath CHs chains using nodes self-location technology and key pre-distribution strategy. So the SS-LEACH protocol strongly improves the energy efficiency and hence prolongs the lifetime of the network (Lee et al, 2009). The SS-LEACH protocol can prevent compromised node and preserve the secrecy of the packet. It also can avoid sybil attack, selective forwarding and hello flooding.

- **Authenticated Key Management**

  Authenticated Key Management (AKM) for hierarchical networks is based on the random key pre-distribution (Kausar et al, 2008). Security is provided using two kinds of keys, a pair-wise shared key between nodes, and a network key. AKM scheme uses an existing Ring structure Energy-efficient
Clustering Architecture for dividing nodes into cluster. Using more than one encryption key, AKM provides multiple levels of encryption, secure cluster formation algorithm and avoid node captures (Zhong et al., 2010). AKM provides confidentiality, global and continuous authentication of nodes in the network by periodically refreshing the network key. AKM scheme can be applied for different energy-efficient data dissemination techniques for sensors networks.

- **Energy-efficient cluster based key management**

  Energy-Efficient Cluster Based Key Management is the cluster based technique for key management in WSNs (Lalitha & Umarani, 2011). The Exclusion Basis System key set contains pairwise keys for intra-cluster and inter-cluster communication. These keys are distributed to the nodes by the CH before communication (Ekici et al, 2008). However, the problem of this protocol is that it works well in the environment with the low density of sensors, but is exposed to many kinds of active attack.

- **Improved key distribution mechanism**

  Improved Key Distribution Mechanism (IKDM) is based on hierarchical network architecture and bivariate polynomial key pre-distribution mechanism (Cheng & Agrawal, 2007). In IKDM, each sensor has a unique id in the network. An offline Key Distribution Server (KDS) first initializes sensors before deployment by giving each sensor node a polynomial share. They exchange their node ids first for the purpose of setting up a pair wise key
between two sensors. The nodes then evaluate their stored polynomial. Since, sensors nodes can obtain the same value from the two distinct calculations, which can be used as their pair-wise communication key. In IKDM, two communicating parties can establish a unique pair-wise key between them. IKDM can achieve better network resilience against node capture attack, hence can provide efficient security and is not affected by the number of compromised sensors. IKDM scheme provides improved scalability, network throughput, fixed key storage overhead, full network connectivity and is suitable for large-scale WSNs. IKDM scheme is more energy efficient due to the lower communication overhead for sensor nodes during the pair-wise key establishment process.

2.4 NON-CRYPTOGRAPHIC ALGORITHMS

The protocols that do not cryptography are called non-cryptographic protocols. The non-cryptographic scheme assumes that all players have unlimited computational power. It frustrates the use of cryptography for protection. Thus, if there is a non-cryptographic solution, it means that adversary not only unable to compute anything about data of good players in some reasonable time, but it cannot compute it at all.

- Reliable energy aware routing

Reliable Energy Aware Routing (REAR) uses three types of nodes: a network sink, target source and intermediate nodes (Hassanein & Luo, 2006). REAR algorithm works on network structured as two layers: one layer for which it provides the aware energy path using the energy reservation
mechanism and one transport layer which provides reliability. Service path discovery, backup path discovery, reliable transmission and reserved energy release are considered to be parts of REAR components.

- **Rumor routing**

  Rumor Routing (RR) protocol looks at routing queries to the nodes which have observed a particular event (Braginsky & Estrin, 2002). RR algorithm uses a set of long-lived agents which create paths that are directed towards the events they encounter. Whenever an agent crosses path with a path leading to an agent that has not encountered, it adapts its behavior to the new situation thus creating a path state which leads to both the events. Any node generating a query will transmit the query if it has the route to the event else it will transmit it in a random direction (Messina et al., 2007). If the node gets to know that the query did not reach the destination, then it will flood the network. The lesser the number of questions which flood, the lower the energy consumed.

- **Active query forwarding in sensor networks**

  In active query forwarding in sensor networks, the sink node sends a query, which is then forwarded by each node receiving the query (Sadagopan et al., 2003). During this process, each node tries to respond to the query partially by using its pre-cached information and then forwards it to another sensor node. If the pre-cached information is not up-to-date, the nodes gather
information from their neighbors within a look ahead of $d$ hops. ACQUIRE behaves similarly to flooding; however the query has to travel.

- **Link quality estimation based routing**

  Link Quality Estimation based Routing takes the decision on data forwarding by a dynamic window that stores the history of transmission success over the link (Chen et al., 2008). This protocol considers the minimum Hop Count (HC) value for selection on next hop. Using flooding mechanisms in which the sink starts advertising the HC sets minimum HC field. Initially, all the nodes have maximum HC set. When a node receives any HC lesser than it has already recorded, it replaces the stored HC with the new one. By doing this, it gets the shortest path.

- **Cougar approach to in-network query processing**

  The Cougar approach was introduced to task sensor networks through declarative queries (Yao & Gehrke, 2002). Given a user query, a query optimizer generates an efficient query plan for in-network query processing, which can vastly reduce resource usage and thus extend the lifetime of a sensor network. Also, since queries are asked in a declarative language, the user is shielded from the physical characteristics of the network.

- **Constrained anisotropic diffusion routing**

  Constrained Anisotropic Diffusion Routing has a major role in energy efficient data querying and routing in ad-hoc sensor networks for a range of collaborative signal processing tasks (Chu et al., 2002). The key idea is to
introduce an information utility measure to select the sensors to query and to guide data routing dynamically. This allows maximizing information gain while minimizing detection latency and bandwidth consumption for tasks such as localization and tracking (Mazinani & Safari, 2015). The information is driven querying, and routing techniques are more energy efficient, have lower detection latency, and provide algorithms anytime to mitigate risks of link/node failures.

- **A stateless protocol for real-time communication in sensor networks**

  The stateless protocol provides three types of real-time communication services, namely, real-time unicast, real-time area-multicast and real-time area-anycast (He et al., 2003). The stateless protocol is specifically tailored to be a stateless, localized algorithm with minimal control overhead. End-to-end soft real-time communication is achieved by maintaining a desired delivery speed across the sensor network through a novel combination of feedback control and non-deterministic geographic forwarding. The stateless protocol is a highly efficient and scalable protocol for sensor networks where the resources of each node are scarce.

- **Directed query dissemination**

  Directed Query (DirQ) dissemination routes query the appropriate source nodes based on both constant and dynamic-valued attributes such as sensor types and sensor values (Chatterjea et al., 2006). Information relating to location is not essential for the operation of DirQ. DirQ uses only the locally
available information to route queries accurately and to enable autonomous adaptation to changes in network topology (Arisar & Kemp, 2009). This is due to certain cross-layer features that allow it to exchange information with the underlying MAC protocol. However, if the sink does not receive any message from a particular node, then it assumes that this node has a measured value that has not changed. All network nodes should have the capability of storing information which can be considered a disadvantage depending on the amount of information stored in the topology and the number of nodes. This is for allowing a precise delivery of applications DirQ is a protocol suitable for situations where the number of requests is high and times of transmission of requests are known.

• **Minimum energy communication network**

  Minimum Energy Communication Network (MECN) sets up and maintains a minimum energy network for wireless networks by utilizing low power GPS (Rodoplu & Meng, 1999). Although the protocol assumes a mobile network, it is best applicable to sensor networks, which are not mobile. A minimum power topology for stationary nodes including a master node is found. MECN assumes a master site as the information sink, which is always the case for sensor networks. MECN is self-reconfiguring and thus can dynamically adapt to node's failure or the deployment of new sensors. Between two successive wake ups of the nodes, each node can execute the first phase of the algorithm while the minimum cost links are updated by considering departure or joining new nodes.
• **Small minimum energy communication network**

Small Minimum Energy Communication Network (SMECN) is an extension to MECN (Li & Halpern, 2001). In SMECN possible obstacles between any pair of nodes are considered. However, the network is still assumed to be fully connected as in the case of MECN. The sub-network constructed by SMECN for minimum energy relaying is provably smaller than the one constructed in MECN if broadcasts can reach to all nodes in a circular region around the broadcaster. As a result there is decrease in the number of hops for transmissions. SMECN uses less energy than MECN and maintenance cost of the links is less. However, finding a sub-network with the smaller number of edges introduces more overhead in the algorithm.

• **Geographic adaptive fidelity**

Geographic Adaptive Fidelity (GAF) is energy aware location based routing algorithm designed primarily for networks (Xu et al., 2001). GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. It forms a virtual grid for the covered area. Each node uses its GPS indicated location for associating itself with a point in the virtual grid. Nodes relating to the same point on the grid are considered equivalent regarding the cost of packet routing (Zhang et al., 2006). Such equivalence is exploited in keeping some nodes located in a particular grid area in sleeping state to save energy. Thus, GAF can substantially increase the network lifetime as the number of nodes increases (Bao & Liang, 2011).
- **Energy-aware greedy routing**

  In Energy Aware Greedy Routing (EAGR), all nodes have the same energy level, and a threshold energy level is set (Sharma et al., 2008). Nodes having less than the energy level are considered dead. All the nodes having energy level greater than their threshold value get information about their neighbor and create a table of their locations. For forwarding data, the algorithm selects the nodes having the distance equal to or less to this average distance value and having maximum energy level amongst the neighbors. In EAGR, packets only get dropped when the destination is dead, or there is no further neighbor alive to forward data.

- **Hierarchical power aware routing**

  Hierarchical power aware routing is a power aware routing protocol that divides the network into a group of sensors called zones (Li et al., 2001). Each zone is a group of geographically close sensor nodes and is treated as an entity. Thus, the first step in this protocol is the formatting of the clustered zones. The next step is the function of the routing scheme to decide how a message is routed across other zones hierarchically so as to enable maximization of battery life of nodes in the system is maximized. This can be done with a message that is routed along a path with a maximum power over all minimum remaining powers. This path is called max-min path. The main idea of making such a decision relates to the possibility of a path with high residual power known for more energy consumption than the minimum energy consumption path. This scheme presents an approximation algorithm called max-min ZPmin algorithm.
The algorithm first finds a path with less power consumption by applying the Dijkstra algorithm. It then finds a second path that maximizes the minimal residual power in the network. The protocol then tries to optimize both solution criteria. The discovery of the power estimation may consult on the overhead to the network.

- **Multicast listener discovery authentication**
  
  Multicast Listener Discovery Authentication (MLDA) is a multicast listener discovery extension intended for use with an authentication, authorization and accounting server (Hayashi et al., 2004). MLDA is also based on Challenge/Response and response forwarding.

- **Self-organizing protocol**
  
  In Self-Organizing Protocol, router nodes are stationary and form the backbone for communication (Bandyopadhyay & Coyle, 2003). Collected data are forwarded through the routers to the most powerful BS nodes. Each sensing node should have the ability to reach a router to be part of the network. Sensing nodes are identifiable through the address of the router node to which they are connected. Further, this algorithm incurs a small cost for maintaining routing tables and keeping a balanced routing hierarchy. Formation of a hierarchy is considered to be another issue (Doumit & Agrawal., 2002).

- **Virtual grid architecture routing**
  
  Virtual Grid Architecture (VGA) routing is a GPS free technique to split the network topology into logically symmetrical side by side, equal and
overlapping frames (Al-Karaki & Kamal, 2004). The transmission occurs grid by a grid (Chiu & Hwang, 2006). VGA provides the capability to aggregate the data and in network, processing to increase the lifespan of the network. Data aggregation is done in two steps (i.e.) first at a local level and then globally. The nodes responsible for aggregate data locally are local heads, and the nodes have to aggregate data received from local heads. After the formation of logical grids, an election is started in each grid to decide for the local head of the grid based on a node the energy and how many times it has been selected as a local head. And then the global heads are also selected randomly from the selected local heads.

- **Hybrid energy efficient distributed**

  Hybrid Energy Efficient Distributed (HEED) clustering periodically selects CHs according to a hybrid of the node residual energy and a secondary parameter, such as node proximity to its neighbors or node degree (Younis & Fahmy, 2004). HEED terminates in O(1) iterations, incurs low message overhead and achieves relatively uniform CH distribution across the network. HEED can asymptotically guarantee the connectivity of clustered networks with proper bounds on node density and intra-cluster and inter-cluster transmission ranges.

- **A Grid Clustering Routing Protocol**

  The Grid Clustering Routing algorithm is a grid-based clustering algorithm where in one of the sinks dynamically, and randomly builds the
cluster grid (Yu et al., 2006). The CHs are arranged in a grid-like manner. Forwarding of data queries from the sink to source node is propagated from the Grid Seed (GS) to its CHs, and so on. The GS is a node within a given radius from the primary sink. Regarding CH selection, on a given round the primary sink selects a GS based on residual energy. Energy conservation is achieved due to the lower transmission distance for upstream data.

- **An energy efficient coordination algorithm**

  Span, a power saving technique for multi-hop ad-hoc wireless networks reduces energy consumption without any significant diminution in the capacity or connectivity of the network (Chen et al., 2002). Span builds on the observation that when a region of a shared channel wireless network has a sufficient density of nodes, only a small number of them need be on at any time to forward traffic for active connections. Span is a distributed, randomized algorithm where nodes make local decisions on whether to sleep or to join a forwarding backbone as a coordinator. Each node bases its decision on an estimate of how many of its neighbors will benefit from it being awake and the amount of energy available to it. Improvement in system lifetime due to span increases as the ratio of idle to sleep energy consumption increases.

- **Energy efficient clustering scheme**

  Energy Efficient Clustering Scheme (EECS) is a clustering algorithm in which CH candidates compete for the ability to get elevated to CH for a given round (Ye et al., 2005). This competition involves candidates broadcasting
their residual energy to neighboring candidates. If a given node does not find a node with more residual energy, it becomes a CH. EECS extends this algorithm by dynamic sizing of clusters based on cluster distance from the BS. The result is an algorithm that addresses the problem that clusters at a greater range from the BS requires more energy for transmission than those that are closer. This improves the distribution of energy throughout the network, resulting in better resource usage and extended network lifetime.

2.5 SUMMARY

This overview presents various techniques that enable reduction in both communication and sensing energy in WSNs. Traditionally, communication energy has been a major part of a node’s energy consumption. But, with the necessity of implementing high-consuming sensors in WSNs, sensing unit has to be driven carefully. Real life implementations of these WSNs require autonomy of several years, with battery power supply. Thus, energy resources should be managed judiciously with reduction in energy consumption on the sensor level, node level and network level.