1.1 INTRODUCTION

Wireless Sensor Network (WSN) is quickly gaining popularity due to the low cost to a diversity of real world challenges (Akyildiz et al. 2002). WSN consist of a large collection of nodes organized into a cooperative network with limited power supply and computation capability (Marjan Radi et al. 2014). Each node consists of micro controllers, Central Processing Units (CPUs), Memory, Radio Frequency transceiver and a power resource (batteries, solar cells), and accommodates various sensors and actuators. WSN consist of self adaptive and self organizing nodes, which consist of limited communicated range, with sensor nodes of a high density. Packet forwarding through sensor networks is performed through multi-hop/multipath data transmission. Multipath transmission in WSN, poses many challenges and issues which stimulate research effort. Applications of sensor networks are seen in Environmental monitoring, Military, Healthcare, Home, commercial, child education, surveillance, micro-surgery and agriculture, etc. A collection of sensor nodes named as hosts communicate with each other via various wireless communication media with or without other nodes as routers. Distances between the sensor nodes vary dynamically due to their mobility (Jinhua Zhu et al. 2005). This natural behaviour and routing through multi-hop is insecure and vulnerable to threats.
1.1.1 Challenges and Issues in WSN

Major issues affected in the wireless sensor networks are limited resources, unreliable communication, and characteristic of the network (John Paul Walters et al. 2006; LIU Yong-Min et al. 2009).

- Very Limited Resources
  - Memory

  Sensor nodes are tiny devices which have limited memory. Typical sensor node processor is of 4-8 MHz, having 4 KB of Random Access Memory (RAM), 128 KB flash and ideally 916 MHz of radio frequency. The heterogeneous nature of sensor nodes is an additional limitation.

  - Storage Space

  Sensor nodes have limited processing and storage capability and limited computation functionality (Sangeetha vharkar et al. 2014). Sensor nodes use a small amount of memory and storage space for the code. The main challenges in the software development are hardware constraints are storage space, memory space, the size of the node, program space, consumption of battery power and limited bandwidth.

  - Energy

  All the sensor nodes are battery powered and capable of limited energy capacity. Energy constraint is the biggest challenge in the sensor networks. Sensor nodes require energy for each operation. Energy must be drained in continuous monitoring of the networks, neighbour node verification, data transmission, changing its localization, node position, capabilities. When the sensor nodes are deployed in a network, they cannot be
easily replaced or recharged. Energy consumption of the sensor nodes conserves the life of the individual node and the entire sensor network. When the security functions (Encryption, decryption, verifying the signature, authentication of data, etc) are implemented within a sensor node, the impact of the energy is considered in the security code and the battery life of the sensor nodes.

- **Unreliable Communication**
  - Unreliable environment network characteristics

  In sensor networks, sensor nodes deployed in dynamic and unreliable environment, create a threat to sensor security. The characteristics of the sensor networks are the topology of a network, routing path, dynamic in nature, communication link between the sensors, addition and deletion of sensor nodes, node failure and damage, energy depletion etc, which create a noisy, error prone, or missing packets.

  - Latency

  In the multi-hop routing, network congestion and node processing lead to latency, making achievements of synchronization among sensor nodes difficult

1.1.2 **Characteristics of WSN**

WSN has numerous characteristics such as mobility, switching characters and the limited capability of the battery power. Compared to these wireless networks, WSN has also some distinctive properties. The characteristics of WSN are:
Computing and Communication Capability

The Computing limitations are cost, node size and battery power consumption, program space and memory space of the sensors and the Communication bandwidth is narrow and distance is limited to 100mts.

Dynamic

Sensor nodes get disconnected from the network when the battery is very low (LIU Yong-Min et al. 2009). Addition or deletion of sensor nodes is based on the requirement of the network. This brings about changes in the WSN topology. Any node failure topology has the function of dynamic, self organization, into a communication network reconfiguring the connection.

No Central management, self organization

The deployment of wireless sensor nodes does not need any predefined network infrastructure. Sensor network should be a distributed network without a central management. This increases the longevity of the network (John Paul Walters et al. 2006). Sensor network once deployed, organizes sensor nodes are autonomously into independent network.

Multi-hop communication

Communication of sensor nodes with others is beyond the coverage range. Sensor nodes transmit data through intermediate nodes via multi-hop fashion.

Application relevance

WSN route is centralized, data gathering, multi-hop communication and many-to-one traffic.
1.1.3 WSN Architecture

The architecture diagram of a wireless sensing node is provided in Figure 1.1 (Martin et al. 2012; Jamal N Al-Karaki et al. 2004). When sensor nodes are deployed in the network communication is through the neighbour nodes or directly to the sink to the Internet. This allows use of different sensors with wireless sensing node.

![Figure 1.1 WSN Architecture](image)

1.2 ROUTING PROTOCOLS IN WSN

Routing protocols play a vital role in WSN (Yang Yu et al 2006). They are classified in different ways based on the network structure are flat based, hierarchical based, location based routing protocols. All the nodes have equal functionality and roles in flat based routing. In hierarchical based routing, nodes play different roles in the network. Location based routing protocol position of node (Jamal N Al karaka et al. 2004). Routing techniques are classified as Multipath based, Query based, negotiation based, QoS based on the basis of this routing protocol. Routing protocols are classified in three categories are shown in Figure 1.2
1.2.1 **Flat Based Routing**

Flat based routing protocols are multi hop flat routing protocols. All the nodes play an equal role and collaborate with each other in sensing. Global identification is not possible due to the presence of a large number of nodes. Flat routing is the data-centric routing where the source node sends a request to BS, while the intermediate node in the WSN can perform the aggregation from multiple source nodes and send the aggregated data to the BS. (Shio Kumar Singh et al. 2010). This data centric process results in energy saving due to smaller transmission required for sending the data from the source node to the BS.

### 1.2.1.1 Senor protocols for information via negotiation (SPIN)

Heinzeiman et al. (1999) have proposed Sensor Protocols for Information via Negotiation is an adaptive protocol that disseminate all the information at each node to every node in the network are likely base stations. This protocol queries any node and gets the required data immediately (Jamal N Al-Karaki et al. 2004). The SPIN protocol is based on two key mechanisms, namely, negotiation and resource adaptation (Shio Kumar Singh et al. 2010). SPIN protocol uses the metadata that the sensor node wants to
disseminate. The SPIN protocol uses the three types of messages, viz: Advertise new data (ADV), Request of data (REQ), data message contains actual sensor data (DATA). When a neighbour node is requested the data, it sends a REQ message to the neighbour node.

This protocol is classified into two types, viz: SPIN1 and SPIN2. SPIN1 uses the negotiation mechanism while SPIN 2 uses the resource aware mechanism for energy saving. The other family of the SPIN protocol are SPIN-BC, SPIN-PP, SPIN-EC are designed for broadcast channels.

**SPIN 1:** This protocol uses the three stage handshake protocol with which the sensors can disseminate their data. Spin protocol uses the point-to-point communication (SPIN-PP). SPIN- BC shows the better performance than the SPIN-PP by using the one-to-many communication.

**SPIN2:** Energy constraint. The energy-conservative heuristic used in the SPIN1 protocol. A node initiates a three stage protocol, only when it has enough energy for completion. A node when the energy is below threshold level can still receive messages, cannot send/receive DATA messages.

### 1.2.1.2 Directed diffusion

Directed diffusion protocol is a data-centric routing. In DD the entire data is gathered by the sensor nodes are called attribute-value pairs. Directed diffusion has key elements, including data naming, interests and gradients, data propagation, and reinforcement (Intanagonwiwat et al. 2000; 2003). At the beginning of the directed diffusion process, the sink specifies a data rate lower than the sink can reinforce by retransmitting the original message with a high data rate.
1.2.1.3 Rumor routing

Rumor routing is a flat based routing protocol using query flooding and event flooding (Braginsky et al. 2002). RR protocol uses agents which are a long-lived packet that traverses a network sending information to each sensor. An agent passes one or more hops through the network and then dies. Sensor and agent maintain the event list, the event-distance pairs, number of hops, visited, node, etc. The agent synchronizes the event list with all sensors on its path and finds its shortest path in the network.

1.2.3 Hierarchical Routing protocol

Hierarchical routing protocol, or cluster based routing (Neetika & Simarpreet Kaur 2012) is used for scalability and energy efficient communication. Higher energy nodes are used in cluster based routing for aggregation and send the information to BS. Low energy nodes are used to sense the media. The main tasks of the clustering protocols are the creation of cluster nodes and election of the cluster heads. Cluster head plays an important role to improve the network longevity and scalability. Hierarchical routing can reduce energy consumption within a cluster and perform data aggregation and send such data to the BS.

1.2.2.1 Low energy adaptive clustering hierarchy

Heinzelman et al. (2000) have proposed a Low Energy Adaptive clustering Hierarchy (LEACH) routing protocol for WSN to reduce energy consumption of the sensor nodes. LEACH randomly elects the cluster heads (CHs) at each round based on the energy threshold. Cluster head aggregates the data from the cluster member in the network, compresses it and forwards the data to the BS in order to reduce the load (Jamal N Al-Karaki et al. 2004).
LEACH protocol (Jia Xu Ning Jin et al. 2013; Alakesh Braman et al. 2014, Meena Malik 2013) is a routing protocol that plays a vital role in the conventional routing protocol. It is a Clustering based protocol which helps in improving the longevity of wireless sensor network. A clustering based protocol minimizes energy dissipation in sensor networks. LEACH protocol groups the nodes into small cluster groups and chooses one of them as the cluster-head. The node first checks its target and then sends the related data to its cluster-head. LEACH provides balancing of energy usage through random rotation of cluster heads. Then the high energy node is called CH aggregates and compresses the data received from all the nodes and sends it to the Base Station (BS). LEACH protocol, which form clusters where the data is needed. The remaining nodes are cluster members of this protocol divided into rounds, each round consisting of two phases, viz: cluster constructing setup phase and steady phase.

In the first phase, the cluster head, broadcasts its information to all nodes around it using the same amount of power. Based on the strength of receiving the signal, the node decides which cluster to join in and sends the message back to the corresponding cluster head. The cluster head allocates the communication time slot for each member node in the cluster based on TDMA (Time Division Multiple Access). In the steady working phase, member nodes of the cluster send data to the cluster head in the communication slot by using minimum-power, and the nodes are inactive to conserve power while out of this time slot. After receiving all the data, the cluster head congregates them and sends them to the sink. The time of steady phase is far greater than the setup phase for minimizing power consumption. Every node selects a number between 0 and 1 randomly. If the value is less than the threshold value $T(n)$, the node becomes the cluster head. $T(n)$ is shown as Equation (1.1).
\[ T(n) = \begin{cases} \frac{P}{1 - P} \cdot \lfloor r \text{ mod } (1/P) \rfloor & \forall n \in G \\ 0 & \text{otherwise} \end{cases} \] (1.1)

where \( P \) is the percentage of cluster heads to all nodes, and \( r \) is the selected rounds number, \( r \text{ mod } (1/P) \) stands for the number of selected cluster head nodes before this round, and \( G \) is the group of nodes which have not been elected as cluster head nodes earlier. When \( r = 0 \), the possibility of each node becoming the cluster head is \( P \). It can be no longer re-elected. After \( 1/P \) rounds, all nodes have a possibility of \( P \) to be a cluster head once again, over and over again. Data transmission begins at the steady state phase. Nodes send their data during their allocated time slot to the CH. The non-Cluster Head node can be a sleep mode until a TDMA slot is allocated to the nodes, thus minimizing energy dissipation in these nodes. When the entire data has been received, the CH aggregates this data and sends it to the BS. LEACH protocol collect the data from each cluster to reduce the size of data is transmitted to the base station.

The advantages of the LEACH protocol (Alakesh Braman et al. 2014)

- LEACH protocol is dynamic, distributed clustering mechanism is used.
- LEACH does not need any control information, from the base station and the sensor nodes do not require knowledge of the global network.
- LEACH reduces communication, energy increases as compared to direct transmission and minimum transmission-energy routing.
- LEACH protocol improves the scalability of the network by forming different clusters.
• Cluster Heads aggregate the data from the cluster nodes and compress them for transmitting to BS. It reduces the traffic load within the network and improves the energy efficient platform.

• The transmission between the cluster node and cluster head takes place in single hop to reduce the energy dissipation.

The disadvantage of the LEACH protocol

One of the significant limitations of LEACH protocol is its assumption by providing some energy to all the nodes. (Nguyen Duy Tan et al. 2012). The cluster heads are elected randomly, so that only the optimal number of cluster heads only selected. LEACH takes additional time to select a better node. This leads to vulnerability to attacks. The cluster heads communicate with the base station in a single-hop mode, which means LEACH cannot be used in large-scale wireless sensor networks for the limit effective communication range of the sensor nodes.

LEACH protocol types

Various types of protocols have been proposed (Bani Yassein 2009, Alakesh Braman et al. 2014) are LEACH-Advanced, LEACH-Balanced, LEACH-Centralized, LEACH Energy, LEACH-Two Level, LEACH-Mobile, LEACH-Vice etc. to enhance the LEACH protocol.

• LEACH-Centralized (LEACH-C)

LEACH does not guarantee location placement or number of cluster heads. Hence, LEACH-C (Heena Dawan & Seep Waraich 2014), an enhancement over the LEACH protocol has been proposed. LEACH-C protocol distributes the cluster heads throughout the network to improve the performance of the network. This protocol sends information and current
energy level of the sink. The sink computes the average node energy, and removes the low energy node from the network. The cluster heads and its members are found, the sink gets an ID of the cluster head. The steady-state phase of LEACH-C is same the LEACH protocol.

- **LEACH-Energy (LEACH-E)**

  In LEACH-Energy protocol, all nodes have the same energy initially and the same probability of becoming the cluster head. Each node energy level change at the end of the first round. The amount of each node’s residual energy is calculated. The nodes which have highest residual energy are elected as cluster heads. The cluster head changes at each round based on the energy level. Among the cluster heads, the node that has the highest residual energy aggregates the data from the remaining cluster heads and forwards it to the BS. LEACH -E improves the network longevity by balancing the energy load among all nodes in the network (Ahmad Jan et al. 2013; Usha et al. 2014). LEACH-E preserves residual energy more when compared to other LEACH hierarchical types. Each round cluster head selection and improvement of the energy level of a node is higher than other LEACH types in a hierarchical protocol (Bani Yassein et al. 2009).

- **LEACH-Fixed (LEACH-F)**

  In LEACH-F (Shio Kumar Singh et al. 2010; Neekita et al. 2012) clusters are formed at the beginning of the network setup and get fixed after that. The cluster head position rotates among the nodes within the cluster, is the same as LEACH. The advantage of this process compared to LEACH is the absence of any setup overhead at the beginning of each round F or cluster formation. LEACH -F uses a centralized cluster formation algorithm that is the same as LEACH -C. The disadvantage of this protocol is that the fixed clusters in LEACH -F do not allow new nodes to be added to the network and
do not make any adjustment in their behaviour when any node dies in the network

- **LEACH-Energy Balanced (LEACH-L)**

LEACH - L (Divya Prabha & Vishal Kumar Arora, 2014), is an advanced multi-hop routing protocol. It is suitable for large area covered WSNs. The cluster heads are able to communicate directly to the sink node when these sensor nodes are located close to the sink node. When sensor nodes are located too far from the sink, they can communicate in the process of multi-hop way. In LEACH-L, the sensor nodes are allowed to use different frequencies to communicate to the sink node. The clusters would reestablish in every round of transmission of information in the network which consists of both a setup phase and a steady state phase. In every round new CHs would elect for every cluster and the network load would be distributed among every node and thus balanced among the nodes would remain perfect in the network (Gnanambigai et al. 2012; Amit Bhattacharjee et al. 2013; Sandeep Verma et al. 2013).

- **LEACH-Mobile (LEACH-M)**

LEACH -M is being proposed to overcome the mobility issue which is important in LEACH protocol. During the setup and steady state phase, LEACH-M provides mobility for the non-CH nodes along with CH. In LEACH -M the nodes’ location assumed to be gained by the GPS process along with the characteristics of the nodes assumed to be homogeneous. The CHs are being chosen on the basis of minimum mobility of the node and the lowest attenuation mode of the node.
After this process, the status of the CHs is being broadcast within its transmission range. (Gnanambigai et al. 2012; Amit Bhattacharjee et al. 2013; Sandeep Verma et al. 2013; Neetilka et al. 2012).

1.2.2.2 Power Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS is a hierarchical protocol where sensor nodes form a chain for transmission and receipt of the data from the neighbour’s node and select one node from the chain, and select node aggregate data from the remaining nodes to forward data to the BS. Clustering head formation is not used in PEGASIS routing like LEACH. Selection of the node from the chain is based on a greedy approach (Shio Kumar Singh et al. 2010). Any one of the nodes dies due to of low energy, and the chain is constructed on greedy approach.

1.2.2.3 Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN)

Manjeshwar et al. (2001); Lou et al. (2005) is a hierarchical clustering protocol, forming a group, each group node being led by a CH. The node within a group sends its sensed data to its CH, which sends the aggregated data to the next higher level CH until the data reaches the sink. TEEN is mainly useful for critical sensing applications. TEEN protocol consumes more energy during the transmission phase than the sensing phase.

1.2.3 Location Based Protocol

1.2.3.1 Geographical and Energy-Aware Routing (GEAR)

Jitender Grover et al. (2014) GEAR is an energy-efficient routing protocol, where sensors are supposed to have localization and aware of their
residual energy. GEAR uses an energy aware mechanism that is based on geographical information to select sensors to send a packet to the destination. GEAR then uses a recursive geographic forwarding algorithm to disseminate the packet inside the target region.

1.2.3.2 Minimum Energy Communication Network (MECN)

Jitender Grover et al. (2014) is a location-based protocol for achieving minimum energy by deploying the nodes randomly. This protocol preserves a minimum energy network with mobile sensors. MECN uses the minimum power, which contains only the minimum power path from each sensor to the sink. It is based on the positions of the sensors on the plane and consists of two main phases, namely, enclosure graph construction and cost distribution. For a stationary network, in the first phase (enclosure graph construction), MECN constructs a sparse graph. A graph is a directed graph that includes all the sensors as its vertex set with edge set as the union of all edges between the sensors does the neighbours located in their enclosure regions. This graph has a directed path from each sensor to the sink and consumes the least total power among all graphs having directed paths from each sensor to the sink. Each sensor broadcasts its cost to its neighbors, where the cost of a node is the minimum power required for this sensor to establish a directed path to the sink.

MECN does not take the available energy into consideration at each sensor, and hence the optimal cost links are static. In other words, a sensor always uses the same neighbor for transmitting or forwarding sensed data to the sink. For this reason, this neighbor may die very quickly, the network thereby getting disconnected.
1.3 VARIOUS TYPES OF ATTACKS

In general, wireless networks are prone to various attacks. Cluster based routing protocols are widely used for energy efficiency. Particularly in WSN they are highly vulnerable to all types of attacks. The major types of attacks commonly affecting WSN are listed below (Venkatraman et al. 2014; Yudhvir Singh et al. 2012)

• Selective Forwarding

When data is transmitted in multipath, the attacker node takes the data and sends it through some other path and drop the packet, which spoils the path selection and the data does not reach the destination correctly.

• Sinkhole Attacks

A node in the network receives all the information in the path and does not pass it to the next hop. The intermediate node acts as the sink node. It can be any node on the route where the data is transmitted from source to destination.

• Black-hole Attack

In the black-hole attack, a malicious node advertises the wrong paths as good paths to the source node during the path finding process as in reactive routing protocols or in the route updating messages as in proactive routing protocols. Good path means the shortest path from the source node to the destination node or the most suitable path through the sensor network.

• Sybil Attack

Sybil attack (Kuo-Feng Ssu et al. 2009; Chitwan Bedi 2014) is a solitary node grants multiple characteristics of the other nodes in the network.
Fundamentally the sinkhole node baits approximately do all the transportation from one area to the other area of a compromised node, look attractive to surrounding nodes with respect to a routing algorithm. The network attackers are divided into two major types as inside attacker and outside attacker and into passive attackers and active attackers. These are then divided into collusion attackers and independent attackers. This is done by having a malicious node present multiple identities to the network.

- **Wormholes**

  In these attacks the adversary sends messages through tunnels over a low latency link, while where the messages are then replayed into the other part. The simplest occurrence of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes attract the distant nodes and nodes are neighbours, leading the quick drain of their energy resources. When this attack which is coupled with selective forwarding and the Sybil attack it is very difficult to detect.

- **Flooding**

  Client puzzles are a way of reducing the severity of flooding attacks by asking all client nodes to demonstrate their commitment to the resources they require. The server distributes a puzzle with each connection request that the client is required to solve in order to get a connection. The attacker now has to expend more energy to flood the network. The disadvantage is that legitimate nodes now have to expend extra resources to get connected.
Hello flood attacks

An attacking node broadcast the hello messages to announce their presence to their neighbours node. A node receiving such a message can assume that the node that sent the message is within its range. Nodes at a large distance from the attacker will be sending their messages into oblivion, leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole.

Sybil attack is one of the crucial attacks (Abirami K Shanthi 2013) more than all other attacks (Chitwan Bedi 2014) in the WSN network. Sybil attack jams the network, create a different identifier, and isolates the one to one mapping in the network and also disrupts the network services.

Table 1.1 Security Attacks on Protocol Stacks (Isha et al. 2013)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Layer</td>
<td>Path based DoS, Reprogramming and Reliability attacks</td>
</tr>
<tr>
<td>Transport Layer</td>
<td>Flooding, Desynchronization</td>
</tr>
<tr>
<td>Network Layer</td>
<td>Sinkhole, Selective forwarding, Spoofing, Sybil attack, Blackhole</td>
</tr>
<tr>
<td>Data Link Layer</td>
<td>Collision, Exhaustion, Information gathering, Fairness</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Jamming, Tampering</td>
</tr>
</tbody>
</table>

1.4 APPLICATIONS OF WIRELESS SENSOR NETWORK

In spite of the various design constraints, WSN offers numerous applications (Mauri Kuorilehto et al. 2005, Rajashree V Biradar et al. 2009).
Table 1.2 WSN Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Possible Scenarios and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental Monitoring</td>
<td>• Data archiving&lt;br&gt;• Digital Images&lt;br&gt;• Collaborative processing&lt;br&gt;• Minimal network traffic&lt;br&gt; • Automated battlefields</td>
</tr>
<tr>
<td>Emergency services</td>
<td>• Search and rescue operations&lt;br&gt;• Disaster recovery and management&lt;br&gt;• Fire and water detectors&lt;br&gt;• Detection of chemical hazards</td>
</tr>
<tr>
<td>Health</td>
<td>• Image Identification&lt;br&gt;• Complex processing&lt;br&gt;• Data security&lt;br&gt;• Communication Intensive</td>
</tr>
<tr>
<td>Home</td>
<td>• Person location awareness&lt;br&gt;• Home appliances</td>
</tr>
<tr>
<td>Education</td>
<td>• Location awareness&lt;br&gt;• Context security&lt;br&gt;• Data exchange</td>
</tr>
<tr>
<td>Industry</td>
<td>• Factory process control&lt;br&gt;• Industrial automation&lt;br&gt;• Monitoring and control of Industrial equipments</td>
</tr>
<tr>
<td>Military</td>
<td>• Battlefield surveillance&lt;br&gt;• Target Identification&lt;br&gt;• Collaborative processing&lt;br&gt;• Detection of enemy unit movements&lt;br&gt; • Data aggregation</td>
</tr>
<tr>
<td>Automotive</td>
<td>• Tire pressure monitoring&lt;br&gt;• Vehicle tracking</td>
</tr>
</tbody>
</table>

1.5 SCOPE OF THE RESEARCH WORK

Sybil attacks are highly vulnerable and highly possible in LEACH protocol (Raed Bani Hani et al. 2013; Sharmila & Umamaheswari 2012). Cluster based routing protocol is used in WSN for improving node energy. Cluster based routing protocols are being implemented to conserve the node
energy during transmission. Different schemes are proposed in this research work for detection and prevention of Sybil attacks.

1.6 PROBLEM STATEMENT

In general, more energy efficient and energy awareness routing protocols, different methodologies and algorithms have been proposed in WSN. In order to reduce energy dissipation, nodes are arranged based on signal strength to form a small group called clusters. Cluster based routing protocols are widely used for energy efficiency in WSN. Energy constraint protocols try to find the efficient path to transmit the data packet. Due to the energy constraint, different types of attacks are possible in WSN such as Sybil, sinkhole, black hole, wormhole, flooding etc.

1.7 RESEARCH OBJECTIVES

A mechanism is needed to detect and prevent Sybil attacks for cluster based routing protocol to improve the QoS parameters such as throughput, PDR ratio, delay and energy. The objectives are:

- To detect and prevent the Sybil node in the initial stage of data transmission for improving the network longevity by preserving the node energy and maintaining the network free from attacks
- To increase the energy conservation of each sensor node through clustering mechanism for avoiding the energy dissipation during transmission
- To establish a trustworthy energy efficient node between the source and the destination for preventing the Sybil attack
- To establish an efficient monitoring node for controlling the network from both internally and externally
To control the node behavior using a genetic algorithm

To provide secure communication through trustable nodes

In order to achieve the objectives mentioned above, five major contributory algorithmic solutions are proposed in this research work:

- Detection and Prevention of Sybil Attack using Random Password Comparison Method
- A Location-Key pair based Security for Wireless Sensor Network
- Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH protocol
- Digital Signature enabled Dydog node (DSED) algorithm to prevent Sybil attack
- An Efficient Monitoring node for secure communication for LEACH protocol.

1.7 ORGANIZATION OF THE THESIS

The rest of this dissertation is organized as follows. Chapter 2 gives an overview of related works and the limitations of wireless network routing protocols. Following this, the objectives of the thesis are presented from the implication of the literature survey. Chapter 3 describes the proposed work Random Password Comparison method (RPC) developed based on distance and the energy level of the node to prevent a Sybil attack based on dynamic password. Chapter 4 depicts Unique Location-Key pair based Security for Wireless Sensor Network developed based on node location is the key parameter to prevent the Sybil attack. Chapter 5 explains the Genetic algorithm enabled Prevention of Sybil Attacks for LEACH is used for monitoring and control of the node behaviour to prevent the attacks. QoS
parameters are improved through the use of genetic algorithm. Chapter 6 deals with DSED mechanisms developed for preventing the Sybil attack from the network and using the Dydog to monitor the network using this mechanism throughput and PDR ratio are increased and secure communication take place. Chapter 7 describes an Efficient Monitoring node (Petdog) as a new mechanism used for monitoring the network to detect and prevent the network attacks. The performance of the all the mechanism the Petdog (PD) shows better performance than all others. Chapter 8 includes the details of the contribution of the research work. Chapter 9 reports valuable conclusions that are observed from the research work and provide suggestions for future enhancements.