CHAPTER 2

RELATED WORKS

The various aspects of WSN routing protocols are analyzed in various aspects in attaining their goal of routing. The learning outcome of the review resulted in understanding the issues, challenges of the existing protocols and attacks in the Hierarchy routing protocol helped in deriving new methods for improving them in order to achieve the objective of designing routing protocols.

2.1 WSN ROUTING PROTOCOLS

WSN nodes communicate wirelessly and often organize themselves after being deployed in an adhoc fashion. Routing typically begins with neighbour discovery, nodes send messages and build a table. (John A. Stankovic 2006). Each table includes the minimum information of each neighbor’s ID and location. The nodes must know their geographic location prior to route discovery, residual energy, delay, signal strength and link quality. Once a table exists, WSN routing messages are directed from source location to the destination based on geographic co-ordinations.

In general, various energy efficient and energy awareness routing protocols, different methodologies and algorithms have been proposed. Cluster based routing protocols are widely used for energy efficiency in WSN.

Hierarchical routing technique has been used to enhance the energy efficiency, prolong network longevity, reservation based scheduling, collision
avoidance, data aggregation by the cluster head, uniform energy dissipation, low latency are characteristics of Hierarchical routing protocols. Low Energy Adaptive clustering hierarchy (LEACH) is Hierarchical routing protocols in WSN.

The Hierarchical routing LEACH protocol (Raed M Bani Hani et al. 2013; Shankar et al. 2012) includes distributed clustering and utilizes a randomized rotation of cluster heads for even distribution of the energy load in the network. It calculates the threshold value to elect the cluster head.

A simple energy-efficient routing scheme (Jinhua Zhu et al. 2005) is meant to improve the performance in mobility scenarios using Progressive Energy Efficient Routing (PEER) protocol. PEER first finds the energy efficient path progressively and maintains the route between the source and the destination, then adjusts the nodes whenever necessary to ensure energy efficiency of the path all the time. Performance evaluation of the PEER protocol achieves reduced routing overhead, shorter setup time, and great energy efficiency. The limitation of this protocol is spending more time to establish the shortest path. As the number of node increases, the setup time has also increases to discover and maintain the route for long distance.

The Best-effort Fault-Tolerant Routing (BFTR) system employs end-to-end ACKs (Yuan Xue et al. 2004; Khatawkar et al. 2011), has discussed the various systems that serve as an add-on technique to detect routing misbehaviour and to mitigate their adverse effect. But applying monitoring mechanism to each individual node and validating the node while communication brings more effect than other techniques. (Manjula & Chellappan 2011) propose a technique Randomized and Trust based watcher judgment strategy for duplication attack detection mechanisms in wireless sensor networks (RTRADP) with the trust factor.
In the LEACH (Alakesh Braman et al. 2014) routing protocols, communication between cluster heads and the base station requires more energy than the non-cluster nodes. This means increasing the number of clusters-heads can increase the energy consumption of the whole network and shorten the network longevity. Therefore, it is necessary to select the optimal number of cluster heads to make the energy consumption minimum. The original LEACH algorithm, selects the cluster heads at random with fixed round time for the selection. It considers the remnant power of the sensor nodes in order to balance network loads and changes the round time depending on the optimal cluster size.

In LEACH-C protocol (Petre-Cosmin Huruială et al. 2010; Raed M Bani Hani et al. 2013) each node transmits its information to the corresponding base station and the sink node makes the choice of selecting the cluster head and how to divide clusters. Then the cluster head sends this information to BS. In Hierarchy routing protocol a CH collects data from its cluster members, aggregates all data and forwards it to the BS that might be located far away from it. The CH is compromised and gets dropped. The compromised CH becomes ineffective, because the data aggregated by cluster head never reaches the base station. V-LEACH (Bani Yassein et al. 2009) protocol, besides having a CH in the cluster, also has a vice-CH that takes the role of the CH when dropped/compromised. The vice-cluster nodes forward data directly to the BS. Messy GAs solves (David Goldberg et al.1989) problems of coverage of local maxima with the optimal search. The choice of the best cluster head node, to minimize the energy consumption and latency by choosing the energy efficient nodes in the network.

Subhasis Bhattacharjee et. al. 2013 have proposed a novel mechanism for verifying the neighbor nodes and selecting a secured shortest path for transferring the data in a secure manner. (Jianguo Shan 2013)
represents the energy saving by LEACH protocol in various kinds of WSN topology. The necessity for safety in LEACH protocol has motivated many scholars to design protected versions of this protocol and to create its resilience against insider and outsider attackers. (Mohammad Masdari 2013) discussed about the current state-of-the-art secure LEACH schemes that are proposed in the literature. (Hiren Kumar Deva Sarma 2011) said a novel secure routing protocol is projected for wireless sensor networks in which sensor nodes as well as the base station or mobile. The protocol achieves security property through symmetric key cryptography and threshold key cryptography.

A different type of hierarchical routing protocol (Manimozhi et al. 2013) is discussed considering battery replacement or charging as not practical. As a result, routing protocols must be energy-efficient to prolong the network longevity (Raed M Bani Hani et al. 2013; Shankar et al. 2012). The Optimal set of protocols is proposed to show the performance optimization system for WSNs with the given application and relative QoS requirements. The performance of a WSN can be modelled into a linear formula in terms of a multiple of assigned weight vectors and the genetic algorithm metrics generated by simulations (Jin Fan et al. 2007).

WSN Cluster-based LEACH routing protocol has greater energy efficiency, residual energy and geometric distance between candidate nodes and the BS to elect CH nodes. It is clear that the CH node closer to the BS will consumes less energy than other nodes as communication of data consumes the most energy in WSNs residual energy of the CH nodes and exchange cluster-head roles after a specified duration to balance energy consumption among the nodes in the WSN (Nguyen Duy Tan et al. 2012). (Wu Xinhua & Wang Sheng 2010) enhanced the HCR protocol using GA,
which determines the clusters, CHs, Cluster-members and the schedules for transmission.

Trust-based LEACH protocol is (Fei Song et al. 2008) meant to provide secure routing, while preserving the essential functionalities of the original protocol. The decision-making of the scheme proposed in this work is based on the decision trust, evaluated separately and dynamically for different decisions by basic situational trust. The situational trust is maintained by a trust management module integrated with a trust-based routing module, having novel techniques in trust update model and cluster-head-assisted monitoring control. Basic classification of routing protocols in WSNs (Alakesh Braman 2014) has named LEACH as the most energy efficient protocol explaining its advantages and disadvantages.

2.2 SECURITY THREATS IN WSN

Eliana Stavrou et al. (2010), have discussed the need for security in sensitive WSN application has lead researchers to design secure multipath routing protocols from the beginning or design security extensions for existing protocols. This paper surveys the current state-of-the-art of secure multipath routing protocols in WSN. In the context of multipath routing, all the classical security requirements needed in single-path routing still applies, but multipath routing also contributes to the establishment of these requirements, and providing additional benefits and risks. The most important security requirements in critical WSNs applications the availability, reliability, resiliency, authentication, freshness, integrity, confidentiality and threats in multipath routing are network congestion, energy exhaustion, routing database divergence, network node partitioning etc. The attacks in the multipath routing are route discovery, data forwarding and route maintenance. The protocols have been categorized based on their security purpose and the security implementation approach. The results are
analyzed and comparison tables are listed based on the security requirement of the protocols, security attacks on both inside and outside adversaries, and energy efficiency, communication and storage overheads, reliability.

The approaches are based on the networking protocol level analysis (Xiangqian Chen et al. 2009) for recognizing the threats and susceptibilities of WSN’s. The security issues are divided into seven categories are cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. The authors analyze the advantages and disadvantages of current security schemes in each category and also discussed that the by choosing the appropriate cryptographic algorithms, parameters are used in WSN. The symmetric key is used in WSN in terms of speed and low energy and cost. Efficient and flexible key management scheme also need to be designed, attack detection and prevention, secure routing, secure location secured data fusion and also other security issues are also discussed.

The node misbehavior can be detected and controlled by different techniques such as Intrusion Detection System (IDS) (Isha V Hatware 2012; Weichang Li et al. 2011) Cooperative Intrusion Detection, Watch Dog (WD) and path rater. These are more efficient than other general techniques. In the existing algorithm, the identification of misbehaving nodes in adhoc networks is critically important to detect security attack in the network. The two types of misbehaving nodes detected and identified in the existing algorithm, namely, selfish and malicious nodes are taken into consideration.

Heena Chawla et al. (2016) have discussed the sensor networks face many challenges due to the use of wireless medium for communication which is prone to various types of attacks. There are various issues like energy exhaustion, memory and storage shortage, security attacks. In this paper discussed about the security goals, attacks in WSN, The Data Packet
Separation Slot Size Randomization (DSSSR) and Round Robin (RR) slot size assignments are the modifications to the sub layer to detect the malicious nodes in the static sensor network. Attack detection time, communication overhead, Energy consumed and computational power are reduced. Number of times the test packet is transmitted is reduced. throughput increases. Wastage of time slot in case the node doesn’t have data for transmission in the allotted slot. Each time the network is redeployed which is very frequent due to removal of faulty nodes and addition of new sensor nodes, the neighbour discovery phase.

Rupinder Singh et al (2016) have discussed various security issues, various security requirements for wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSN are playing a great role in the controlling and managing environments in different situations and has become important part of research area. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments.

2.3 SECURITY MECHANISMS FOR WSN ROUTING PROTOCOLS

A newfangled discovery mechanism, called CRSD (Cooperative RSS based Sybil detection), is projected for static wireless sensor networks, which precedes the usage of the received signal strength (RSS) to conclude the remoteness (Shaohelv et al. 2008) among two individualities and additional controls the positions relative to the thought-provoking by use of the RSS statistics from multiple neighbour nodes, e.g., via node assistance. To manage the intrusion, and protect the data, a secure Identity based routing
Protocol, can ensure that the nodes in the routing discovery process are trusted nodes (Weichang Li et al. 2011). Digital signatures based on ECC are in the protocol in this work, it has many virtues, such as less energy cost, more rapid calculation, shorter storage keys, etc. The attacks faced by WSNs were analyzed and the "Security Aware Ad-hoc Routing (SAR), (Sasikanth Avancha et al. 2003) was introduced. SAR characterizes and explicitly represents the trust values and relationships which associated with ad-hoc nodes and uses these values to make secure routing decisions. Security protocols in WSNs, dissimilar the traditional techniques, need extraordinary efforts and problems to be addressed.

Kejun Liu et al. (2007) have proposed the 2ACK system that helps as an add-on method for routing systems to sensor routing misbehaviour and to alleviate their opposing effect. The key impression of the 2ACK system is to send two-hop response packets in the reverse direction of the routing path. In order to avoid the routing overhead, only a portion of the received data packets are acknowledged in the 2ACK scheme. These schemes are divided into two categories, viz; credit based scheme and reputation based scheme. The basic idea of the credit-based scheme is to provide incentives for nodes to faithfully perform networking functions. For achieving this goal virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. In the reputation scheme network, nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network. In the TWOACK scheme, the receiving node in the 2ACK scheme only sends 2ACK packets for a fraction of receiving data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of receiving data
packets gives the 2ACK scheme a good performance with respect to routing overhead. The 2ACK scheme has an authentication mechanism to make sure that the 2ACK packets are genuine. TWOACK packet in the S-TWOACK (Selective-TWOACK) scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a subtle change, the 2ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK.

Chobe et al. (2013) have proposed a new scheme called 2ACK which is used where the 2ACK scheme is to send two-hop acknowledgment in the opposite direction of routing path. In 2ACK scheme, to reduce extra routing overhead, only a few of the received data packets are acknowledged. Ad-hoc Multipath On-Demand Distance Vector routing protocol as similar characteristic of AODV discover multiple paths between the source and the destination in every route discovery. AOMDV and AODV have several characteristics in common. Based on the distance vector concept and uses hop by hop routing approach. AOMDV also finds routes on demand using a route discovery procedure. Comparison between the 2ACK and AOMDV shows the best performance of AOMDV in terms of delay, throughput, PDR and overhead.

Janakiraman et al. (2009), have proposed an Intrusion Detection Systems for achieving maximum resiliency against attacks. A New Dynamic Intrusion Detection Protocol model (DIDN) has been designed based on data flow for High Error Rate Wireless Sensor Networks (WSNs). The Dynamic Intrusion Detection nodes (DIDN) are deployed here. These will act as forwarding nodes as well as Intrusion Monitoring Node with respect to the data flow through the sensor nodes. The Dynamic Intrusion Detection Nodes are selected from the one-hop or two hop neighbor’s non-forwarding node list
by using Secure Session Key Management approach without deploying separate Intrusion Monitoring Nodes. This makes the network more flexible and dynamic against various attacks and provides monitoring node’s availability to the maximum with better resiliency in high error rate. The monitoring nodes are dynamically changed in its behaviour within the session itself depends on mobility and based on proposed conditions. An attacker will create problem to identify and attack the DIDN Nodes within the limited session. By this protocol the attacks and compromised nodes can be effectively identified at runtime in high data rate static or dynamic Wireless Sensor Networks (WSNs). The drawback of this DIDN is that the single node acts as a monitoring node and also a forwarding node, the energy spent by the node is more and node always in active state.

Marti et al. (2007) have detected and eliminated the malicious node using the watchdog and the path rater tools. The watchdog methods detect the misbehaving node in the network. Implementing watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the locate presence of a match, the packet in the buffer is removed. A packet has remained in the buffer longer than a certain timeout, the watchdog increments a failure tally for the node responsible for the forwarding of the packet. In path rater each node maintains a rating for every other node, it knows about in the network. It calculates a path metric by averaging the node ratings in the path. This metric has been chosen as it gives a comparison of the overall reliability of different paths and allows path rater to emulate the shortest length path algorithm when no reliable information has been collected, if there are multiple paths to the same destination, has chosen the path with the highest metric.

Messy Genetic Algorithms solve (Goldberg et al. 1989) problems by combining relatively short, well-tested building blocks to form longer,
more complex strings that increasingly cover all features of a problem. Minimizing the energy consumption and latency of sensor node is done by choosing the best nodes to become cluster-heads. Minimization is realized with a multi-objective genetic algorithm executed on a central BS and the results are sent to the network nodes (Petre-Cosmin Huruiñă et al. 2010).

2.4 ALGORITHMS TO DETECT SYBIL ATTACKS

A Sybil attack (Prameet kaur & Sandeep Singh Kang 2013) is a solitary node which acquires multiple characteristics of other nodes in the network and is referred to as Sybil node. In Sybil attack, a node replicates another node’s identity. An adversary may present multiple identities. It may jam the network and foil participation of other nodes in the network and directly results in the data loss. Sybil attack (Pramod, AV et al. 2012) is more severe and created dynamically during data transmission. Much attention is needed, as it prevents other nodes from participating in the network, which degrading the performance of the entire network.

Jorge Hortelano et al. (2010), discuss the intrusion detection module watchdog, which aims to monitor the activity of the nodes in the network in order to detect misbehaviour node detection of selfish nodes and malicious attackers. When a node forwards a packet, the watchdog ensures that the next node in the path also forwards the packet. Watchdog checks the all nodes in the transmission within range level. Watchdog monitors the next node, forwards the packet in the transmission within the time period. If the node is not forwarded, that node is said to be a misbehaviour node. The drawback of the watchdog mechanism within the range limit only monitors the nodes, the watchdog is vulnerable to cooperative attacks and it is not accurate when mobility of the nodes is increased.
Shanshan Chen et al. (2010) have proposed the security mechanism based on LEACH routing protocol against Sybil. The problems of low energy consumption and high security of WSN are considered. The mechanism is set to start up Sybil attack detection policy based on RSSI (Received signal strength indicator) when the cluster-heads number in WSN is above a threshold. LEACH-Security mechanism was proposed to improve the security performance of LEACH protocol. When an attacker changes its Identity each time, this information is broadcast to neighbour nodes and claim it as a cluster head node. The cluster head is selected in each round with a time duration. The results conclude that it defends against the Sybil attack effectively and the energy consumption is comparatively low.

Kuo-Feng Ssu et al. (2009) have proposed to protect WSNs against Sybil attack, in which, the node identities are verified simply by analyzing the neighbouring node of the suspected information in order to determine whether these nodes share the information with the same neighbours are identified as the Sybil nodes. Each malicious node creates many fake identities and is exploited to develop a mechanism to protect from the Sybil attacks. When a malicious node discerns itself to be within the communication range of a normal node, it immediately forges multiple Sybil nodes. Since these Sybil nodes are all associated with the same physical node (i.e. The malicious node), they share information from the same set of neighbours. This characteristic of Sybil nodes can be exploited to detect the occurrence of a Sybil attack and to identify the Sybil nodes simply by comparing the neighbouring information collected from the neighbour of the victimized node. The set of nodes is classified into different sets like set of normal node, malicious node, normal neighbour’s node, and common neighbours of two nodes etc. is calculated based on the occurring time in the network. Each Sybil node has the same set of neighbours since they are created by the same
malicious node. The results are analyzed based on the node density, threshold value, malicious node and neighbour node position, number of Sybil nodes.

RenXiu –li & Yang Wei (2009) have proposed deployment of sensor nodes within the radio range in a network using Radio Signal Strength Indicator (RSSI) with two levels. In the first level Sybil node is apprehended and in the second level, it is confirmed as a Sybil node. Every node in the route should provide its neighbour node information within the range to the source node in order to discover the route. The nodes which share equal distance have to be found and grouped according to the distances. These nodes are referred to as the suslist1. The Sybil node occurrence is calculated from suslist1 to suslist2 and forms a Sybil list. Every line of the Sybil list is checked and if there are two or more same IDs present in one line are said to be Sybil nodes. The number of Sybil nodes is detected after different iterations. The main disadvantage of this approach is that it consumes a lot of time in checking the Sybil node from distance list and Sybil list and affects overall network quality and performance. Verification based only on the ID makes this approach less accurate.

Sybil node is a solitary node (Abirami & Shanthi 2013), which acquires the multiple characteristics, mainly the identification of the other nodes in the network. The Sybil attack is one of the primary attacks, which pave way for various other attacks to take place in the network. The Sybil nodes cannot be detected directly by checking only the ID or the node information.

Raghu Vamsi P et al (2016), proposes a method for detecting Sybil attack using sequential analysis. This method works in two stages. First, it collects the evidences by observing neighbouring node activities. Further, the collected evidences are consolidated to provide input to the second stage. In the second stage, collected evidences are validated using the sequential
probability ratio test to decide whether the neighbour node is Sybil or trusted node. Sequential Probability Ratio Test (SPRT) is modeled as a random walk with a lower and upper bound. In this random walk, the decision-making process will start at a point in the two bounds and move towards any of the two bounds depending on the input evidences. When the random walk reaches or exceeds the upper bound, SPRT rejects the null hypothesis and accepts the alternate hypothesis. On the other hand, if the random walk reaches or exceeds the lower bound, SPRT accepts the null hypothesis and rejects the alternate hypothesis. Sybil Attack Detection Using Sequential Analysis (SADSA) consist of two phases are evidence collection and evidence validation. Nodes collect the evidences to reach a decision on detecting malicious nodes. The collected evidences are consolidated and provided as input to the SPRT for validation.

Vinayaka AP & Nalinakshi B G (2016), The proposed algorithm is to maximize the security aspects of nodes in wireless network t by using the IP, MAC check process and RSSI value calculation to enable the extensive features of security. method to use signalprints to detect Sybil attacks in open ad hoc and delay-tolerant networks without requiring trust in any other node or authority. Using motion to defeat the signal print technique are detected by requiring low-latency retransmissions. First it relies on trusted external measurements, e.g., RSSIs from trusted access points, which are generally unavailable in open ad hoc networks. it restricts the attack model to stationary devices, even though attackers can easily use mobile devices.
<table>
<thead>
<tr>
<th>Author</th>
<th>Protocol/Methodology</th>
<th>Approach</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raed M Bani Hani et al. (2013); Shankar et al. (2012), Nguyen Duy Tan et al. (2012), Alakesh Braman et al. (2014), Jinhua Zhu et al (2005), Petre-Cosmin Huruială et al. (2010); Manimozhi et al. (2013)</td>
<td>LEACH, enhanced-LEACH (E-LEACH), LEACH-centralized (LEACH-C), multi-hop LEACH (M-LEACH), LEACH with fixed cluster (LEACH-F), PEGASIS, hierarchical PEGASIS (H-PEGASIS), Hybrid, Energy-Efficient Distributed Clustering (HEED), TEEN and APTEEN</td>
<td>In Set-up phase, when the sensor nodes are organized to form cluster either in a cluster-based / chain-based /optimal cluster/ manner In Steady phase data are routed from sensor nodes to the BS using distributed algorithm or centralized algorithm</td>
<td>Dynamic, distributed clustering mechanism, reduces communication, increases scalability, improved energy efficiency</td>
<td>IF all the nodes starts with the same initial energy Nodes are static in nature, failure of cluster head creates a problem</td>
</tr>
<tr>
<td>Isha V Hatware (2012), Weichang Li et al. (2011), Eliana Stavrou et al. (2010), Xiangqian Chen et al. (2009), Heena Chawla et al. (2016), Rupinder Singh et al (2016)</td>
<td>Cryptography, Key management, security requirements, Intrusion Detection methods, Fitness, Watchdog, Path Rater</td>
<td>To find the misbehaviour nodes, detect and prevent and control the attacks by different techniques for secure routing, secure location, secured data fusion</td>
<td>Attack detection time, communication overhead, Energy consumed and computational power are reduced.</td>
<td>Problems of selecting incorrect malicious nodes, limited power transfer, node conspiracy and impartial removal are tackled effectively. Malicious nodes are detected but are not isolated</td>
</tr>
<tr>
<td>Shaohelv et al. (2008), Weichang Li et al.(2011), Sasikanth Avancha et al. (2003), Kejun Liu et al. (2007), Chobe et al. (2013), Janakiraman et al. (2009), Marti et al. (2007), Petre-Cosmin Huruială et al. (2010), Raghu Vamsi et al. (2016), Vinayaka &amp; Nalinakshi (2016)</td>
<td>CSRD based RSS, RSSI, Digital Signature based ECC, 2ACK, DIDN, watchdog,pathrater, Multi-objective GA, Sequential analysis.</td>
<td>To find node positions by use of the RSS statistics from multiple neighbour nodes, response packet in two hops, DIDN act as a forwarding node as well as ID</td>
<td>Avoids routing overhead, reducing error rates by one or two hop response, minimize the delay and packet loss, increases the throughput, and utilize the network efficiently</td>
<td>Energy spent is more when signal node act as a forwarding node and monitoring node. Waiting time for acknowledgement is more. Path metric is maintained high for reliable data.</td>
</tr>
</tbody>
</table>
2.6 Research Gap

In the existing LEACH protocols, cluster based selection has only been focussed and not included security mechanisms. Most of the existing research works, for Sybil node detection metrics such as delay, packet loss, network performance are considered. In the proposed work, network and energy metrics such as energy, PDR, throughput and packet loss are also considered to analyze the performance periodically. The traditional cryptographic mechanisms such as DES, AES, ECC, DS have widely been used in LEACH protocol. In the proposed work, enhanced crypto mechanism like dynamic password comparison in RPC, secured location key pair in ULKP and digital signature and two fish algorithm in DSED are used. Further soft computing techniques such as genetic algorithm in LEACH-GA and efficient monitoring node in PD have been used in the proposed work.

2.6 LIMITATIONS OF THE EXISTING ALGORITHMS

The major issues and limitations of the existing algorithms are:

- Use of the RSSI ranging method, implies a lot of time wasted in calculating the distance and identifying the Sybil node

- PEER protocol requires a long time to establish the shortest path. As the number of node increases, the setup time also increases to discover and maintain the route for long distance

- Clustering algorithms based on metrics such as residual energy, uniformity of CH distribution, cluster size, location awareness, node mobility, delay, hop distance and cluster formation methodology etc.

- The nodes energy is drained when the data transmission occurs peer to peer
• Due to the node mobility, nodes compromise themselves and send false data to the neighbour nodes

• An Intrusion detection mechanism like watchdog and pathrather is used within the range of transmission and also vulnerable to attacks.