CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO MOBILE AD HOC NETWORKS

The development in the field of wireless communication and the widespread use of hand held devices change information access from “anytime anywhere” to “all the time, everywhere”. A multihop wireless network plays a major role in achieving this goal. Mobile Ad hoc Networks (MANETs), which drive under the multihop network are rapidly deployable, self-organizing, self-healing and infrastructure-less network of independent devices. Each device in a MANET is free to move independently in an arbitrary direction and will be therefore found establishing links with a different set of neighbours forming a dynamic topology. An ad hoc network is a peer-to-peer multihop wireless network, where the packets are transmitted in a store and forward manner through intermediate nodes. Some types of MANETs are restricted to form an infrastructure less local area network of wireless devices, while others may be connected to the Internet. For example, a Vehicular Ad Hoc Network (VANET) is a type of MANET that allows vehicles to communicate with roadside equipment. The vehicles may not have a direct Internet connection but the wireless roadside equipment may be connected to the Internet, allowing data from vehicles to be sent over the Internet.
1.2 EVOLUTION OF MANET

Basically, MANETs can be categorized as first, second and third
generations. The first generation came up with Packet Radio Networks
(PRNET) sponsored by Defense Advanced Research Projects Agency
(DARPA) in the early 1970’s. The PRNET employed a combination of
ALOHA and Carrier Sense Multiple Access (CSMA) approaches for
accessing the shared radio channel. The most admirable features of PRNET
are rapid deployment and self-organizing of nodes. It has evolved to be a
robust, reliable and an experimental network.

In the second generation, Survivable Adaptive Radio Networks
(SURAN), an extension of PRNET was evolved in early 1980’s with
significant improvement on ad hoc networking with small, non-expensive,
power-thrift devices, with improved routing and scalability of the network.
This serves as a packet-switched network to the mobile battlefield in an
infrastructure less environment. SURAN turned out to be beneficial in
improving the radio’s performance by making them smaller, cheaper and
resilient to electronic attacks. SURAN employed Code Division Multiple
Access (CDMA) and Time Division Multiple Access (TDMA) techniques to
support many users to share the allocated spectrum. At the same time, United
States Department of Defence (USDoD) funded Global Mobile (GloMo)
Information Systems. The goal of GloMo was to offer an Ethernet-type
environment to establish a multimedia connectivity “anytime anywhere”, in
handheld devices. GloMo makes use of CSMA/CA (Collusion Avoidance)
and TDMA techniques to provide an improved self-organizing and self-
healing network, i.e., Asynchronous Transfer Mode (ATM) over wireless,
satellite communication network.

The growing interest in the field of computer communication and
the realization of the necessity of open standards in the area of
communication, paved way to various other great developments in the third generation (1990’s). The functioning group within Internet Engineering Task Force (IETF) formed the MANET working group, to standardize the routing protocols and they categorized them as reactive and pro-active protocols. The motto of IETF is to bring a standardized routing functionality to help nodes in ad hoc networks to self-organize them. It is described as a commercial network as it connects various mobile devices like PDA’s, palmtops, notebooks, etc. When the concept of making use of radio signals to connect various devices was introduced, the Institute of Electrical and Electronics Engineers (IEEE) established the standards for wireless technology (802.11). The various standards are 802.11a, 802.11b and 802.11g. Among these, Wi-Fi (802.11b) technology became ubiquitous and vendor neutral. Wi-Fi works at 2.4 GHz Industrial Scientific and Medical (ISM) band; the data rate can peak from 2 Mbps to 54 Mbps. Later WiMAX (802.16) was introduced and it is a super set of Wi-Fi. WiMAX assures a higher data rate of 30 Mbps + and is particularly designed for wide area networking.

1.3 CHARACTERISTICS OF MANET

The mobile ad hoc network does not have the defined cell boundary. Therefore the nodes in the network stay dynamic in the infrastructure less environment. A number of challenges are faced to retain the network. Some of them are listed below

Mobility: The nodes in the network move in a random direction with variable speed (Random Way Point), where the location and topology maintenance is a challenging issue.

Bandwidth constraint: Since the nodes in the broadcast region share the channel, the bandwidth available for any link depends on the number of nodes
and the traffic it handles. Therefore, the total bandwidth available for any node in the network will be lower.

**Energy management:** Ad hoc networks do not have any power source to provide the backup. As the nodes are involved in forwarding the data packets of other nodes, there is a higher probability of decrease in the energy level. Therefore to extend the lifetime of the nodes in the network, several power optimization methods are required.

**Induced traffic:** Ad hoc wireless is a multi-hop radio relaying network. A link-level transmission affects not only the sender and the receiver but also the neighbouring nodes of both sender and receiver due to the traffic from neighbouring links.

**Lack of central co-ordination:** Unlike the cellular networks, MANETs does not have any central authority to coordinate the nodes’ communication. This further hinders the Quality of Service (QoS) and security provisioning in ad hoc networks.

**Hidden terminal:** The hidden terminal problem arises when more than two senders which are not in the direct range, start sending packets to a common receiver. This causes collision, leading the sender to retransmit the packets. It will not be acceptable for the flow that has stringent QoS requirement. Busy Tone Multiple Access (BTMA) and Dynamic Time Division Multiple Access (DTMA) provide solutions to the hidden terminal problem to a certain extent.

**Insecure medium:** The communication among nodes is carried in the shared wireless channel without any central controller, leading to higher risk in the security aspects. Especially, in the environment where the packets should be sent more securely like, military and tactical applications.
Multihop network: Nodes in the network act as a transceiver. During communication, nodes which fall on the direct range, openly communicate with each other. In the case of communicating nodes which are not in the range, the packets are transmitted with the support of two or more intermediate nodes by taking multiple hops. The performance of the network depends on the behaviour of the nodes.

1.4 ROUTING

Communication in a network is facilitated by forwarding the packets through multiple nodes. The process of transferring the packets from source to destination is often termed as routing. It has a set of functional components like building and choosing routes, administering network topology, disseminating the network information for the route construction, locating end points of the session and transmitting along the selected routes. If routing is to be done to only one destination, it is called unicast routing. When multiple destinations are involved, it is termed as multicast routing. In order to enable effective and reliable communication in the network, several routing protocols are designed. An ad hoc routing protocol decides how the packets should be routed between nodes in the network. In mobile ad hoc network, routing protocols are divided into proactive routing, reactive routing and hybrid routing as given in Murthy & Manoj (2007).

1.4.1 Proactive or Table Driven Routing Protocol

A proactive routing protocol is table driven protocol which continuously evaluates the routes of all reachable nodes in the network and maintains the same in an updated manner. In this type of routing protocol, each node must maintain at least one table to store the routing information. In the case of network topology changes, the node is expected to propagate the route update messages throughout the network so that a stable network view
is maintained. The various well known proactive protocols are Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Optimized Link State Routing (OLSR), Cluster-head Gateway Switch Routing (CGSR) protocol, Fisheye State Routing (FSR) and Source Tree Adaptive Routing (STAR).

DSDV, works based on the Bellman–Ford algorithm which was developed by Perkins & Bhagwat (1994). The main role of the algorithm was to give solution to the routing loop problem. Each node maintains a routing table with a route entry for each destination based on the number of hops. It has routes to all the destinations from every node. The tables are exchanged between neighbours periodically to maintain the current status of the network. The tables are updated with the destination sequence number to prevent loops.

WRP was introduced by Murthy & Garcia Luna-Aceves (1996), where each node maintains a set of four tables, namely distance table, routing table, link cost table and Message Retransmission List (MRL) table. Distance table contains the distance and penultimate node to reach the destination. Routing table contains the predecessor and successor nodes in the routing path. Link cost table contains the cost of forwarding through each link. MRL is used to store the nodes that have not acknowledged a route update. The WRP is classified as one of the path finding algorithms, where the count to infinity problem has been avoided by making each node to check the consistency of the predecessor information reported by its neighbours. Here, each node learns about its neighbours from the acknowledgements and other messages it receives. Each node sends a periodic update message to its neighbours to ensure that the routing information is accurate. The update message indicates the destination ID, distance to destination, predecessor to destination and a list of all nodes that acknowledge the receipt of update message.
OLSR was proposed by Jacquet et al. (2001), which is an extension of the link state protocol which minimizes the flooding of control traffic packets broadcasting by means of selected nodes, called multipoint relays. OLSR employs an efficient link state packet mechanism called MultiPoint Relaying (MPR). When a node wants to send topology updates, it selects a group of neighbouring nodes (MPR) to retransmit the packet from the source node. If the node receives a topology update packet from a node for which it is not a multipoint relay, it will update the topology with the information in the packet and not by rebroadcasting the packets. The goal of the multipoint relay was to achieve controlled flooding.

In CGSR, given by Chiang et al. (1997), the mobile nodes are grouped into clusters and a leader is appointed. All nodes that are in the transmission range of the leader belong to one cluster. A node within the transmission range of two or more leader serves as a gateway node. Leader scheme can cause performance degradation in a dynamic network due to frequent leader elections. Thus CGSR uses the Least Cluster Change (LCC) algorithm. In LCC, if a change in network causes two cluster-heads to come into a single cluster, a leader change occurs. It also occurs when one of the node moves out of the range of all the leaders. In this protocol, the source node forwards the data packet to its leader. The leader then sends the packet to the gateway node and then it is forwarded to the intermediate cluster leader till the leader of the destination is reached. The destination’s leader then forwards the packet to the destination.

STAR was given by Garcia Luna-Aceves & Spohn (1999). Each node maintains a source routing tree which consists of preferred paths that the node takes to each destination in the network. Each node broadcasts its source tree to its neighbours through an update message. A node can form a partial topology graph by aggregating the neighbours information. When a node A
has to send data packets to a node B for which no path exists in its source tree, node A broadcasts an update message to all its neighbours. This update message again triggers another update message from a neighbour which has path to node B. After receiving source tree update from neighbours node A update its source tree and finds path to all the nodes in the network. Node A retransmits the update message with increasing intervals till it receives path to destination B. STAR does not work well for high mobility patterns.

FSR is a hierarchical routing given by Iwata et al. (1999). It uses the “Fish eye” technology given by Pei et al. (2000). The fish eye captures the high detail information about the pixels near to the focal point as the distance increases from the focal point the information detail decreases. The functionality of FSR is similar to LSR. Unlike LSR, the update information is flooded only to the local neighbours. FSR works well even when the network becomes larger.

1.4.2 Reactive or On-Demand Routing

Reactive routing is an on-demand routing where routing paths are established only when required. Here, the node mobility causes a higher overhead on route maintenance and the source node suffers delays in route discovery. Dynamic Source Routing (DSR), Ad hoc On-demand Distance Vector Routing (AODV), Temporally Ordered Routing algorithm (TORA) and Ant colony based routing algorithm are some of the examples of reactive routing. Hybrid routing combines the merits of both, reactive and proactive routing. Zone Routing Protocol (ZRP) is an example of Hybrid Routing Protocol.

DSR was developed by Johnson & Maltz (1996). In DSR the source node maintains the set of nodes that need to be traversed to reach the destination, which is based on source routing concept. It has two major
phases, which are route discovery and route maintenance. The route discovery packets are used for caching the path information. The routed packets have the address of all the nodes traversed. Route reply would be generated, only if the message has reached the intended destination node. When a data packet is sent, the node checks its route cache to find an unexpired route to the destination. In case of route breakage, the failed nodes are removed from the route cache and route establishment process is again initiated. The DSR protocol is a beacon less protocol and no periodic hello packets are required for route maintenance.

AODV was described by Perkins & Royer (1999). When a node wishes to send a data packet Route Request (RREQ), messages are flooded in the network. The flooding of RREQ packets provides higher reliability of data delivery, since numerous routes are discovered to reach the destination. Each node maintains a table, which contains the list of next hops to reach the destination and sequence number of destination. The nodes also store the precursor nodes for route maintenance. On establishing the route, an Route Reply (RREP) message is sent. Any intermediate node can also send the RREP message if the destination sequence number of the path known is more recent. Upon data transmission, each node receives the data packets, checks for the validity of route and forwards to the next hop neighbour. When a link fails, an Route Error (RERR) message is passed back to a transmitting node, and the process repeats. If any route becomes stale, it is either discarded or the lifetime of the route is updated. The advantage of AODV is that it does not craft extra traffic for communication along existing links. Also, distance vector routing is simple, and does not require much memory or calculation. However, it requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.
TORA is a highly adaptive loop-free distributed routing algorithm proposed by Park & Corson (1997). It limits the control message propagation in the mobile network and provides multiple routes to the source and destination pair. The nodes in the network maintain the routing information about adjacent nodes. It has three phases route creation, route maintenance and route erasure. Creating the route from a node (source) to the destination requires establishment of sequence of directed links leading from source to destination, created only when there is no directed route available from the source to destination. Thus creating routes includes assigning direction to the undirected network and builds a Directed Acyclic Graph (DAG) rooted at the destination. Upon detection of the network partition all links (in the portion of the network that has partitioned from the destination) must be marked as undirected to erase all invalid routes. TORA performs three functions by the use three control packets Query (QRY), Update (UPD), and Clear (CLR). QRY packets are used to create routes, UDP is for both creating and maintaining routes and CLR is for erasing route.

The basic concept of ARA, given by Gunes et al. (2002), is based on swarm intelligence and on the ant colony based meta heuristics. It works as the food searching behavior of ants. When ants search for foods, they have to start from the nest and move towards the food. When it reaches the intersection point, it decides the branch to the next take based on the concentration of pheromone (while walking they deposit a substance called pheromone). It indicates the frequent usage of a path or the shortest path in use. This matches with the dynamic property of ad hoc network. It works based on the local information; here no information has to be shared with other nodes in the network. Link quality is mapped to the computation of pheromone concentration. This will improve the decision process of each node in the path selection.
1.4.3 Hybrid Protocol

The protocol which belongs to this category combines the advantages of both the reactive and proactive routing protocol. The topology of the network is divided into several zones. Zone Routing Protocol (ZRP) and Zone–based Hierarchical Link State (ZHLS) routing protocol are two protocols which fall under this category.

ZRP routing is given by Haas (1997) combines the advantages of both table-driven and on-demand routing protocols. This protocol was especially designed to increase the speed of data delivery. Each node has a defined routing zone separately, and the zones of neighbouring nodes overlap. The number of nodes in the routing zone can be controlled by regulating the transmission power of nodes. Each node in a zone maintains the route information to reach its neighbouring nodes within its routing zone by the periodic exchange of update packets. Hence larger the zone, higher the update control traffic. If the destination of the packets generated is in the same zone as the origin, the proactive protocol is used. If the route of the destination outspreads the packets originating zone then the reactive protocol is used, which verifies each successive zone to find whether, the destination node is present inside that zone. Thus, ZRP reduces the control overhead for longer routes by using two different protocols.

Joa-Ng & Lu (1999) proposed ZHLS an additional version of ZRP routing protocol. It holds two levels of topologies, namely node level and zone level. The physical connectivity between nodes within a zone is given by node level topology. If at least one node of a zone is physically connected to the node of another zone, then, a virtual link will exist between them. This is referred as zone level topology. Each node contains complete knowledge about the nodes in its zone and also the connectivity information about other zones in the network. When the zone ID and the node ID of a destination are
known, the data packets are effortlessly routed to the destination. This protocol overcomes the overlapping zone problem of ZRP but additional traffic is produced by the creation and maintaining zone-level topology.

1.5 ATTACKS IN MANET

Due to unique characteristics of MANET, it is prone to many security threats. During the transmission of data and control signals, the security requirements such as integrity, reliability, availability, authentication, non-repudiation, access control and confidentiality should be focused. The network should be protected from various kinds of attacks by the defense mechanism. Security attacks are broadly classified into two types, namely internal and external attacks.

1.5.1 Internal Attacks

Internal attacks disturb the network by means of compromised nodes present in the network. The nodes in the network may become selfish and modify the routing information, which is difficult to identify. These attacks may broadcast wrong routing information to the neighbouring nodes. Internal attacks are difficult to handle as most of them occur when a legitimate node turns to a selfish node. A compromised node can generate a valid signature using its private key since the insider knows the valuable, secret information and possesses privileged access rights. Hu & Perrig (2004) have conducted a wide survey on internal attacks.

1.5.2 External Attacks

External attacks are caused by the nodes that do not belong to the network. Unauthenticated attackers can inject any form of disruption to the network. In case of an external attack the attacker tries to interfere with the
operation of the protocol. It may prevent the dissemination of correct routing information in the network. It affects the network performance by causing various passive and active attacks.

In passive attacks, the attacker snoops the data exchanged without altering the information. These attacks are hidden and they trap the communication lines to eavesdrop the data. Passive attacks can be grouped into eavesdropping and traffic analysis. The pattern of the network traffic is more important for the adversaries. In a clustered topology, the cluster head has more responsibility than the other nodes. It is easy for the adversaries to know the network information through the snooping cluster head.

In active attacks, the attacker alters the message exchanged between the nodes in the network. These attacks may disrupt the normal functioning of the MANET. Sometimes the attacker node acts legitimately to gain unauthorized access to the system resources. This active attack is further grouped into four types, namely physical, message modification, Denial of Service (DoS) and misbehaving attacks. Physical attacks are one of the security attacks which fall in the domain of fault tolerance. Physical attacks over the hardware are the major issues, mainly in the tactical communications and sensor networks. When nodes are unattended, they are physically attacked by means of many tampering techniques like micro-probing, laser cutting, focused ion beam manipulation, glitch attacks and power analysis. Electro Magnetic Pulse (EMP) is one of the most common threats listed within the physical security attacks. An EMP is the burst for short duration of high intensity electromagnetic energy that produces voltage surges and damages the electronic devices.

In message modification attack, a node called masquerade node which acts as a legitimate node to collect the data and modifies the content
before being replaying. Masquerading, message replay and content modification indulge the integrity of messages or services of the network.

The availability of the network services are mainly targeted by the DoS attacks. DoS attack can be classified based on three properties, malicious, disruptive and asymmetric. Malicious behaviour is caused due to the malfunction of any node in the network. Disruption is an attack in which attacker nodes do not re-broadcast route request packets and prevent route discovery for the overall network to degrade the QoS offered according to Ocakoglu et al. (2015).

In wormhole attack, the attacker node receives the packets and tunnels them to another attacker node which is closer to it. In black hole attack, the attacker node acts as a legitimate node to show that it has the shortest route to reach the destination for the source request, the attacker node consumes all the data packets arrived from source node. Grey hole is similar to the black hole attack but it selectively forwards and drops the packet. In Sybil attack, the attacker uses multiple identities of the network to gain the reputation; these attackers can be identified by passive monitoring.

Rushing attack makes an immediate route reply with the lowest sequence number when it gets the route request from a source node, which later isolates the legitimate node from participating in the route discovery process.

Sinkhole is a type of intrusion attack. The attacker falsely advertises that it has the optimum route to reach the destination and receives the data packets from source and tampers the network.

Jelly fish is a kind of rushing attack which acts in the transport layer. The attackers get full access of the network and increases the packet
end to end time delay and delay jitter. Stealthy attacks are a combination of misrouting, power control, colluding collision and identity delegation attacks. This attack steals the data packets at the intermediate node without reaching the target node and makes the legitimate node to come under a suspicious check for the misbehaving activity. Misrouting attack relays the packets to the wrong hop. Power control makes the transmission to exclude next hop. Colluding collision makes the simultaneous transmission to create a collision at the intermediate node, and stops the packet from reaching the destination. In case of identity delegation attack, the malicious nodes relay their identities to some other compromised node in the network as to make the packet which it receives to be delivered to a wrong next hop by making use of that delegated identity.

Nodes in the network act selfishly to reserve the resources. If many nodes in the network act to be selfish, these nodes give an impact which is similar to other attacks. In order to motivate the nodes to exhibit the truthful behaviour, many credit-based systems are designed by Pari et al. (2013). Nodes compete to gain the incentive. If a seamless credit approach is not designed that may lead the nodes may turn to be selfish in order to gain the incentive, by disturbing the normal functioning of the network. In sleep deprivation attack, an attacker attempts to consume more energy of other resources, by sending data to many route discovery packets or, by forwarding unnecessary data in the network.

These attacks could be overcome by efficient techniques designed to prevent malicious nodes from participating in the network activities. The misbehaving nodes are encouraged to exhibit the legitimate behaviour to cooperate with the other nodes in the network. This cooperation can be accomplished with any parameters like incentives, energy and virtual
currency. This is the motivation for the present research in the field of ad hoc network.

1.6 MOTIVATION

MANETs are rapidly deployable, self-organizing, self-healing and infrastructure less network of independent devices. Each device in a MANET is free to move independently in an arbitrary direction and will therefore be found to establish links with different sets of neighbours forming a dynamic topology. An ad hoc network is a peer-to-peer multi-hop wireless network where packets are transmitted in a store and forward manner through intermediate nodes.

MANETs are dynamic in nature due to the flexibility of the network. In recent days, they play a vital role in wireless communication. They have a wide application in military, emergency rescues, vehicular network, and conferences to share information. The node pair, which is not in the direct communication range, should travel in a multi hop path in a wireless medium to reach the destination, which increases the security risk. Moreover, the routing schemes proposed are mainly focused on choosing an efficient routing path for packet transmission and allocation of resources to the shared medium. The concentration paid over security while designing the routing algorithm is comparatively less. The security mechanisms, provided in the wireless local area network like, key exchange, and authentication may be provided to ad hoc networks. However the wider distribution of the nodes in the open medium makes MANET more vulnerable to attacks. Thus the security services provided to the wireless network cannot be adapted as such for ad hoc networks. In order to have the secure communication, cooperation between heterogeneous nodes is essential. A legitimate node at any point of time can turn into a malicious node or selfish node. Most of the existing approaches decrease the performance of the network by utilizing most of the
bandwidth for the exchange of control information rather than forwarding data packets and thereby reducing the lifespan of the nodes in the network. Various intrusion detection techniques and security protocols are evolved to evaluate the behavior of the nodes in the network. Many mechanisms are still in the stage of development as the area of research is vast.

1.7 CONTRIBUTION OF KNOWLEDGE

This thesis brings the idea of how the mobile ad hoc remains scalable and secured under different attacks. It summarizes the attacks on wireless links and detects possible attacks and isolates the same. To monitor the behavior of nodes in the communicating path reliance metric is built. A cluster based network topology is adapted to improve scalability and manage the mobile nodes. The trust metric developed in this thesis will be useful for the network to maintain the privacy and to monitor the traffic of their communication without violating the privacy rules.

1.8 OBJECTIVES

i. To design a recommendation based reliance model to encourage the nodes to exhibit cooperation by means of reputation and to revoke the certificate of malicious nodes in the network to improve the system performance.

ii. To design a mechanism based leader election model to elect a stable and optimal cluster head by means of voting and motivate the nodes to exhibit the truthfulness by means of paying incentives to serve other nodes in the cluster.
iii. To develop a local monitoring system aided with overhearing, that mitigates the stealthy attacks by electing guard nodes, in an optimized manner.

iv. To build an intrusion detection system analogous to the human immune system to detect the misbehaving nodes in the network by discriminating the normal and abnormal on enhanced negative selection algorithm.

1.9 LITERATURE SURVEY

Mohammed et al. (2011) proposed the leader election mechanism in the presence of selfish and malicious nodes. In order to balance the resource consumption, the node leaves out with higher energy and battery resources are chosen as the leader node to prolong the life time of the MANET. Without incentive for serving others, the node becomes seriously selfish and lies about its remaining resources. Here the nodes are paid with the incentives to circumvent the selfish behaviour of the node. They also address the global optimal way of electing the leader with low cost. This mechanism failed in demonstrating the leader election process in the cluster independent mobile ad hoc environment.

Shakshuki et al. (2013) introduced an Enhanced Adaptive ACKnowledgment (EAACK) model for secure communication amongst mobile nodes. The EAACK serves as an intrusion detection system wherein an end-to-end acknowledgement is propagated back to the sender by the receiver. If the sender fails to receive the acknowledgement within the time-out, the sender switches to Secure ACKnowledgement (S-ACK) mode to identify misbehaved nodes in the route. A Misbehavior Report Authentication (MRA) with digital signatures are generated to reroute the dropped packets. This forces the source node to find another path to destination to transmit
dropped packets. EAACK is designed to tackle three weaknesses of watchdog scheme: false misbehavior, limited transmission power and receiver collision. However when the forged acknowledgement is sent, there is a possibility of loss of packets.

Dong & Liu (2009) presented a solution for harmless cluster members. The cluster members elect the same leader as long as they are connected with that leader and malicious attacks cannot make any attempt to spam the leader election, make a harmful node as the leader. In cluster dependent leader election, the leader is elected periodically. It includes three phases, initialization, anti-spoofing announcement and distributed decision making. The nodes are provided with a unique ID and two one-way key chains for authentication process. In each round of election, the nodes are authenticated to either join in YES chain to act as the leader or NO chain to act as a cluster member. In each round the nodes in YES chain are allowed to compete with the leader election. The main purpose of the leader election is to facilitate the network integration. The cluster leader is elected by means of mechanism design, where leader is elected by the presence of remaining energy. But this type of periodic election is not suitable in a hostile environment.

Garcia-Teodoro et al. (2009) conducted a survey on an intrusion detection technique, to detect the anomalies in the network called Anomaly-based Network Intrusion Detection System (A-NIDS). This system protects the target system from the dangerous security threats. A-NIDS is classified into three categories, statistical-based, knowledge-based and machine learning-based. Various models are used to find the prior knowledge of malicious nodes and the pros and cons of various intrusion techniques are discussed.
Raychoudhury et al. (2013) illustrated the top k-weighted leaders. The nodes having the highest weight among their hop neighbours are chosen as red nodes to act as a coordinator by a voting mechanism, while the other nodes are marked as white nodes. The red node starts the diffusing computation procedure asynchronously and individual diffusion trees are built. The proposed algorithm is scalable, reliable and message-efficient; it can handle dynamic topology changes in a well sustained manner. Thus all the red nodes coordinate among themselves to pick the final leader. This model minimizes the number of computations and hence reduces the resources. The complete weight information of all nodes is stored in the highest weighted red node. The main problem which should be corrected is, the safety of nodes, its life time and mutual exclusion between nodes.

Khalil et al. (2009) introduced the framework called Unmask. In this frame work, guard nodes are elected to overhear information from an authenticated one hop neighbour, to detect different forms of attack like wormhole, sybil and rushing attacks. Guard nodes are elected based on Khalil & Bagchi (2011). Lightweight Secure Routing (LSR) protocol is used for securing the multiple node-disjoint paths. This framework works well in the static environment.

Janzadeh et al. (2009) proposed a Reliable Clearance Center (RCC). It utilizes the hash chain function on messages to defend against cheating by the nodes. RCC issues a digitally signed certificate to each node which intends to join the network. RCC decides whether to involve the node in the packet transmission or not, based on the credit it holds.

Sabat & Kadam (2014) explained the leader election, based on the reputation and energy based mechanism. The adaptive energy based scheme, adjusts the range of the transmission between the distances among the nodes. This work deals with the adjustment of the transmission range, considering
the maximum distance between the nodes. Here the energy of the nodes is conserved, compared to the fixed range transmission. Thus the leader can serve the cluster for long duration, by increasing the life time of nodes and conserving the energy of nodes. Most of the energy is spent in electing an optimal leader, where dealing with other network activities is given least preference.

A consensus algorithm which applies a local decision attained by an Adaptive Quickest Detection (AQD) detects the malicious nodes, is stated by Avallone et al. (2011). The AQD computes local likelihood ratio by comparing with the threshold. Later a source probability is estimated and used in an adaptive Sequential Probability Ratio Test (SPRT) to reduce False Alarms (FA). The values are forwarded to the fusion center where it merges the nodes opinion by Maximum Cardinality (MC) to find the honest nodes and punish the malicious nodes.

Anchal et al. (2014) proposed permission-cum-cluster-based distributed mutual exclusion algorithm, for mobile ad hoc networks. A node in a cluster sends request for accessing Critical Section (CS) to its respective cluster leader by specifying its request message ID, cluster leader ID and timestamp, if its respective cluster leader does not have the CS, it enqueues the node’s request and further forwards it to the other cluster leader present in its information set. After receiving request from cluster leader, the other cluster leader sends leader reply message, otherwise it enqueues request of cluster leader. Cluster leader allow the member node to enter the CS after receiving leader reply message from the other cluster leader. This approach fails to handle the faulty node’s performance, which will degrade when the cluster heads are not in one hop range.

Saxena et al. (2014) designed an energy efficient clustering algorithm to prolong the life time of MANET. In every cluster, there will be a
cluster head. The cluster head is elected based on its energy level and the highest energy node will become the root of the max_heap. The clusters have a stable end-to-end communication without the support of gateway nodes. This algorithm concentrates only on energy saving. Even a bogus node which has a higher energy can act as a cluster head where it ruins the communication.

Laxmi et al. (2014) analyzed the behavior and influence of Jelly Fish (JF) attack over TCP-based MANET. The three variants of Jelly Fish attacks JF-reorder, JF-delay and JF-drop are evaluated. Node $X$ calculates $T_{\text{forward}}^f$, the time required to forward $\rho$ number of packets by the node $A$ in the route. If the transmission is successful, $X$ associates two timers to determine the trustworthiness of node $A$. The accuracy of the detection algorithm depends on timer value. Owing to the dynamic channel condition, moving average is considered as the weighing parameter in calculating timer value. The obtained value is compared with the threshold, if the value is less than the threshold the monitoring node detects node $A$ as a JF attacker. Node $X$ blacklists the node $A$ with a timer value $t$. Once the timer value $t$ expires node $A$ is given another chance in order to avoid the false positive. Again if the node $A$ is blacklisted it is permanently revoked from the network activities. The work concentrated only on direct monitoring. The mobility of nodes affects the throughput highly.

Dhurandher et al. (2011) devised a routing scheme which uses a reputation value, to discriminate among nodes to select the optimal path. Initially, challenge is exchanged among all neighbour nodes to compute the initial reputation. Authenticated lists, unauthenticated lists and question mark lists are maintained for nodes which are trustable, not trustable and questionable trust, respectively. A global reputation is calculated by weighted average of net rating, friend rating and observed rating. Friend-based Ad hoc
routing using Challenges to Establish Security (FACES) assumes transitive property of nodes, that is, if \( A \) is the friend of \( B \) and \( B \) is the friend of \( C \), then \( C \) is the friend of \( A \). Mobility of nodes effects the associative property and does not allow to hold the property. It also makes nodes to store more information.

Defrawy & Tsudik (2011) introduced a Privacy-friendly Routing In Suspicious MANETs (PRISM) protocol. It is a privacy-friendly, anonymous, location-centric on-demand routing protocol based on AODV and secure group signature scheme. PRISM makes use of session identifiers or location-based identifiers instead of using long term identifiers, which makes the nodes easily trackable. If the sender wants to communicate a node, the target is searched within a radius \( r \) from the sender, and when the node is found it is authenticated. Else, the source node increases its radius and continues its search. Intermediate nodes do not cache the routing path, and no insider knows about the exact location of the destination node. PRISM protocol finds great use in military application, where the location of a node is kept as a secret.

Shen & Li (2015) proposed a hierarchical Account-aided Reputation Management (ARM) system to efficiently provide incentives and to deter the selfish behavior in MANETS. ARM builds a hierarchical locality-aware Distributed Hash Table (DHT) infrastructure to globally collect all the reputation information of the nodes by maintaining Hamiltonian cycle. The collected information is used to calculate more accurate reputation and to detect any abnormal reputation information, thus enabling higher-reputed nodes to pay less for their received services.

Anantvalee & Wu (2007) developed an encouragement scheme to build cooperation among nodes. A Reputation Management System (RMS) is
an extension to source routing protocols for detecting and punishing selfish nodes in networks. RMS comprises four main components which are the monitoring module, the reputation manager, the response module and the communication module. It not only detects selfish nodes but also responds in terms of reputation. This motivates the selfish nodes to be cooperative. The nodes are categorized as cooperative, selfish and suspicious nodes. A state model is introduced to decide the response towards the nodes in each category. Cooperative nodes and selfish nodes are rewarded and punished respectively. Whereas, suspicious nodes are further investigated and if they tend to behave selfishly, actions are taken against them.

1.9.1 Clustering

Energy efficiency and QoS are major issues in MANETs. Since a centralized controller is not practical, scalability of the network is also unpredictable. According to Lin & Gerla (1997) the partitioning of the network into clusters improves the scalability and gives better network co-ordination in the network.

Lin et al. (2009) presented a clustering technology algorithm where the node with lowest ID among its neighbours is chosen as a cluster head and other nodes become cluster members. The relay node, which is in the transmission range of more than one cluster, chains in the cluster communications. Clustering helps in maintaining the connectivity and increasing efficiency by the controlled traffic.

In leach clustering algorithm, proposed by Heinzelman et al. (2000), there is a possibility that the same node is chosen as a cluster leader again and again. Younis & Fahmy (2004) proposed a Hybrid Energy Efficient Distributed clustering (HEED) in which the residual and the reference energy relationship is used in the cluster head selection. Wang & Li (2003) proposed
a standardized cluster-based approach for the local coordination. A stochastic method of choosing a cluster leader by modifying the probability of each node to become leader head is proposed by Zytoune et al. (2009).

1.9.2 Intrusion Detection System

Intrusion Detection System (IDS) is a security technology applied to identify an unauthorized user entry into a system, or to detect the misuse of any privilege, in order to perform malfunction in the network. Intrusion detection gives the second wall of protection and it is important for high-survivability network. According to Zhang & Lee (2000), the measures such as authentication and encryption can be employed in MANETs to decrease the intrusions, but they cannot be eliminated. To guarantee a high secure environment, intrusion detection technique can be used along with the above said measures. The ID technique, which is designed for an infrastructure less network, should be a light weighted ID.

Anderson (1980) designed IDS to wired networks in initial days. Later various security threats pose a challenge in developing perfect IDS to wireless networks. This makes IDS designing an emerging area for research. Kachirski & Guha (2002) proposed IDS based on mobile agent technology, the aim of the algorithm is to track and detect the intruders. A routing misbehavior can occur in the network due to traffic overload, link failure, misbehavior or selfish nodes in the network. The pathrater and watch dog are designed to monitor the routing information.

Different techniques are used in designing IDS like the statistical algorithm, which employs four classes of measures to track activities like categorical, continuous, intensity and event distribution and to describe the misbehaving events. An expert system, which contains a set of rules, is designed, where the system will trigger for certain events which satisfy the
rules, as proposed by Porras & Valdes (1997). Kumar & Spafford (1994) proposed misuse intrusion detection based on the coloured petrinet to match the input event with the pattern representing audit data to detect the anomalies.

1.9.3 An Anomaly-Based Intrusion Detection System

The misbehaving event is detected by examining the deviation from the normal to expected behaviour of the system. If the deviation is detected, IDS sets the flag and generates an alarm. The main challenge in anomaly detection is increase in high false rate because of the comprehensive nature of expected behaviour. Invoking neural network in IDS involves three steps, feeding the normal pattern as input, training the neural network to identify the misbehaving nodes, and matching the output to detect the intruders.

Different authors have proposed various approaches for measuring the trust worthiness of a node. Trust is the contribution of the node to the network. Some approaches are proposed to measure the contribution made by serving node, given by Buragohain et al. (2003); Wang & Li (2003). According to Papaioannou & Stamoulis et al. (2005) trust is based on the quality of service offered by the serving node. Marti & Garcia-Molina (2004) discussed the approaches of measuring the trust. It is the ratio of the resources received by the resource provided to a node. According to Satsiou (2010), trust is calculation of the ratio of the sum of resources availed, to the resource requested for a certain transaction.

Kamvar et al. (2003) suggested that power trust uses Bayesian theorem to compute local reputation, and eigen trust (the sum of both negative and positive ratings) to calculate global reputation. Zhao et al. (2010) suggested that peer trust normalizes the rating on each transaction held during
the packet transmission. Liang & Shi (2005) differentiate transactions based on sensitiveness, hit ratio, effectiveness and applicability. It assigns different weight to each type while computing the average trust of a node. Tao et al. (2005) explained trust as the ratio of successful transaction to the total transaction. Banerjee et al. (2005) suggested that, different reputations are calculated for various resources and the resources are not given equal priority. Song et al. (2005) proposed Fuzzy-trust, to find the trust of a node $X$. The fuzzy interference is applied on parameters of $X$ by node $Y$ to calculate the local trust and then node $Y$ aggregates the trust values established from the neighbours by assigning weights. Selcuk et al. (2004) states that, neighbour node holds a binary vector of $m$ bits. For every successful and unsuccessful transmission 1 and 0 are added respectively to the vector by right shifting the bits. Zhou & Hwang (2007) proposed a power trust algorithm in which the high energy nodes are considered to be the highly reputed nodes. The cluster head calculates the trust of cluster members and maintains the global reputation. Yu & Fujita (2012) designed a mechanism by which the node renders its service to network, should be given higher reputation than the newly arrived node. In most of the existing approaches the reputation of a node is considered as global. But a node does not behave uniformly with all the peers. This is not due to the node being selfish, this may happen due to many other network factors. It leads to a false accusation.

### 1.10 ORGANIZATION OF THE THESIS

Chapter 1 discusses in detail about the evolution and importance of MANET. The characteristics and challenges of MANET are also explained. Due to the lack of infrastructure, MANET is more vulnerable to attacks. Various attacks and the routing protocols are specified. In MANET, nodes are self-directed; it may prevent them from co-operating with the other nodes in the network or become selfish. Hence the nodes are motivated with some kind
of incentive, to be cooperative with each other. To provide an incentive and to monitor the behaviour of nodes, a monitoring system acts as an intrusion detector. A number of schemes for IDS are discussed in the literature.

Chapter 2 describes a certificate revocation technique to provide riskless communication in the network. A reliant is a factor associated with every node to represent the goodness. The goodness of a node depends on two factors, reward and punishment. This scheme has the inspiration of voting and non-voting method. The direct and recommendation trust factors, are considered for the calculation of goodness. The certificate of the malicious node is revoked by the certificate authority with the interruption of cluster head.

Chapter 3 deals with portrays the mechanism to avoid selfish node in the networks. A hierarchical clustering is formed by the co-operation of the nodes in the network. The nodes with lowest cost are elected as a cluster head to serve as an IDS. The nodes in the network are motivated to say the truth by means of paying incentives. A cost function is calculated with the private information gathered by the elected cluster head. The node which acts selfish without revealing the private information are not paid with an incentive. If it prolongs to be selfish, it will lose all its reputation and become an invalid node.

Chapter 4 demonstrates the local monitoring system for MANETs. Guard nodes are selected from the list of common neighbours between the communicating nodes. Guard nodes which serve as an intrusion detector co-ordinate among themselves to avoid the stealthy attacks. Stealthy attacks which disturb the network by mitigating the packets from reaching the destination are due to the misbehaviour of nodes. The guard nodes are elected based on the trust value computed.
Chapter 5 discusses an artificial immune system analogous to the human immune system to provide appropriate IDS. It also explains about the discrimination of self/non-self patterns by means of detector generation using Enhanced Negative Selection Algorithm (ENSA). ENSA optimizes the detector generation process and performs a precise classification of the network traffic.

Chapter 6 consolidates the performance evaluated with the proposed mechanisms to mitigate the vulnerabilities in MANET and gives a roadmap for future work.