CHAPTER 1

INTRODUCTION

1.1 OVERVIEW MOBILE AD-HOC NETWORKS

The performance advancements recently happening in the computer and wireless communications technologies, have sprouted the expectation for the advanced mobile wireless computing to have a remarkably increased usage and application, more of which will have the Internet Protocol (IP) suite used. The objective of mobile ad-hoc networking is supporting reliable and effective functioning in mobile wireless networks by integrating the functionality of routing into mobile nodes. These networks are anticipated to possess dynamic, rapidly-varying sometimes, random, multihop topologies that are possibly consisting of considerably bandwidth-restrained wireless links.

In the Internet community, support for routing for the mobile hosts is currently being devised to be a "mobile IP" technology. This is basically a technology for supporting nomadic host "roaming", in which a roaming host might be attached to the Internet through different means except its popular fixed-address domain space. The host might be connected physically to the fixed network physically over a foreign subnet, or be attached by means of a wireless link, dial-up line, etc. Providing support to this kind of host mobility (or nomadicity) needs address management, protocol interoperability improvements and so on, though the core network functions like hop-by-hop routing are still depending on pre-available routing protocols that are functioning in the fixed network. On the contrary, the aim of mobile ad-hoc networking is about extending the mobility into the land of autonomous, mobile, wireless domains, in which a set of nodes that again might be some
combined routers and hosts from the network routing infrastructure functioning in an ad-hoc way.

A Mobile Ad-hoc Network is a group of autonomous mobile nodes which can communicate with one another through radio waves. The mobile nodes which are in radio range of one another can communicate directly, while the rest require the assistance of intermediate nodes for routing their packets. Every one of the nodes is equipped with a wireless interface for communicating with one another. These networks are distributed fully, and can operate at any place with no support of any pre-determined infrastructure in the form of access points. The important problem in constructing a MANET is fitting every device such as to constantly maintain the information necessary for routing the traffic properly, Zanjireh et al. (2013). These networks may function by themselves or might be attached to the larger Internet. They may have one or multiple and diverse transceivers between the nodes. This leads to a largely dynamic, independent topology.

MANETs are a type of wireless ad-hoc network which generally contains a routable networking environment over the top of a Link Layer ad-hoc network. MANETs comprises of a peer-to-peer, self-configuring, self-healing network. MANETs circa 2000-2015 generally communicate at the radio frequencies (30 MHz - 5 GHz). The evolution of laptops and 802.11/Wi-Fi wireless networking has elevated the MANETs to be a well-known research topic from the mid-1990s. Several academic research works assessed the protocols and their capabilities, supposing different levels of mobility in a bounded space, generally with all nodes that are lying within a few hops of one another. Several protocols are then assessed on the basis of the measures like the packet drop rate, the overhead brought in by the routing protocol, end-to-end packet delays, network throughput, capability for scaling, etc. The current
research work is associated with the research topic in MANET for providing an effective and secure routing for different MANET applications.

Figure 1.1 illustrates a simple ad-hoc network having 3 nodes. Node 1 and node 3 do not lie within the range of one another; but the node 2 could be utilized for forwarding the packets between node 1 and node 2. The node 2 will serve as a router and then these three nodes come together to form an ad-hoc network.

(Source: Gujral & Kapil 2011)

**Figure 1.1 Example of Mobile Ad-hoc Network**

### 1.2 MANETS CHARACTERISTICS

A MANET comprises of mobile platforms (e.g., a router having several hosts and wireless communications devices) simply called here as "nodes" that can independently move randomly. The nodes can be positioned in or on airplanes, ships, trucks, cars, besides even on people or tiny devices, and there might be many number of hosts per router. A MANET is an independent system of mobile nodes. The system may function in an isolated manner, or might have gateways for interfacing with a fixed network. In the operational
mode, it is generally assumed to function as a "stub" network that connects to a fixed internetwork. Stub networks transmit traffic that originates at and/or destined for the internal nodes, though do not allow exogenous traffic to make a "transit" through the stub network.

MANET nodes are fitted with wireless transmitters and receivers employing antennas that may be Omni-directional (broadcast), highly-directional (point-to-point), most likely steerable, or any combination. At a particular instant of time, based on the positions of the nodes along with their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity which is in the form of a random, multi-hop graph or "Ad-hoc" network is present between the nodes. This Ad-hoc topology can vary over time with the node movement or make an adjustment to their transmission and reception parameters. The features of MANET environment are tabulated as below:

1) **Distributed operation:** There exists no background network for the centralized control of the operations of the network; the network control is spread among the nodes. The nodes that are involved in a MANET must coordinate with one another and communicate among themselves and every node functions as a relay as necessary, for implementing particular functions like routing and security.

2) **Multi hop routing:** When a node attempts to transmit information to other nodes that are out of its range of communication, the packet must be forwarded through one or more intermediate nodes.

3) **Autonomous terminal:** In MANET, every mobile node is an autonomous node that could operate in the form of both a host and also a router.
4) **Dynamic topology:** Nodes move randomly with multiple speeds; therefore, the topology of the network might vary in a random manner and that too, unpredictably. The nodes present in the MANET establish the routing among themselves dynamically since they move around, creating their own network.

5) **Light-weight terminals:** In most of the cases, the nodes present in MANET are in movement with lesser CPU capacity, lesser power storage and smaller memory size.

6) **Shared Physical Medium:** The wireless communication medium can be accessed by any entity with the suitable equipment and sufficient resources. In accordance, the channel access cannot be restrained.

Although, above mentioned features render the MANET deployment to be a challenge. There are different MANET applications that are being deployed across the globe, making MANET to be a hot research topic. Few of the important applications of MANETs are explained below.

1.3 **MANETS APPLICATIONS**

With the increase in the number of lightweight devices in addition to the development in wireless communication, the technology of ad-hoc networking is achieving focus with the rising number of applications far and wide. Ad-hoc networking could be utilized anytime, anyplace with less or no communication infrastructure. The previous infrastructure is fanciful or irritating for use. The ad-hoc network architecture could be employed in real time business applications, corporate companies for increasing the productivity and also profit.
The ad-hoc networks can be divided based on their application since Mobile Ad-hoc Network (MANET) is a self-configuring infrastructure less network consisting of mobile devices communicating via wireless link. Vehicular Ad-hoc Network (VANET) exploits the moving cars in the form of nodes in a network to establish a mobile network. Wireless Sensor Network (WSN) comprises of independent sensors for controlling the environmental actions. The significance of ad-hoc network has been focused in several fields that are explained below:

1) Military battlefield: Ad-hoc networking allows the military to make the best use of commonplace network technology for maintaining an information network between the soldiers, vehicles, and military information head quarter, Bangnan et al. (2003).

2) Collaborative work: For few business scenarios, the necessity for collaborative computing may have more importance out of the office environments rather than the inside and places where people require having meetings outside to collaborate and exchange information over a given project.

3) Local level: Ad hoc networks can independently connect an instant and temporary multimedia network employing notebook computers for spreading and sharing the information among the participants in a conference or classroom. Another suitable local level application might exist in home networks in which devices can directly communicate for exchanging information.

4) Personal area network and blue tooth: A personal area network is actually a short range, localized network in which the nodes are generally associated with a particular person. Short-range MANET like Bluetooth can
make the inter communication between different mobile devices like a laptop, and a mobile phone simplified.

5) Commercial Sector: Ad-hoc can be utilized in emergency/rescue operations for efforts concerned with disaster relief, e.g. in fire, flood, or earthquake. Emergency rescue operations should be conducted in which the non-available or damaged communications infrastructure and quick deployment of a communication network is required.

1.4 ROUTING IN MANET

A routing protocol indicates the means in which the routers communicate with one another, distributing information which facilitates them to choose the routes between any two nodes over a computer network. Thus the routing algorithms decide the particular selection of route. Every router is rendered with a prior knowledge about the networks directly connected to it. A routing protocol partakes this information first among the next immediate neighbors, and thereafter through the entire network. By this means, routers come to know regarding the network topology.

An ad-hoc routing protocol is a standard, or a convention, which has the control on how the nodes determine by which way the packets are to be routed between the computing devices present in a mobile ad-hoc network. In the case of ad-hoc networks, nodes have no familiarity with their networks’ topology. Rather, they must find it: generally, a new node broadcasts its existence and then listens for the announcements which are broadcast by its neighbors. Every node learns regarding its neighbors and the means of reaching them, and might make an announcement that it can also reach them. In a wider sense, it is to be noted that, ad-hoc protocol can also be utilized literally, to refer to an implemented and frequently impromptu protocol which is created to serve a particular use. Ad-hoc network routing protocols are usually
categorized into three important classes; Proactive, reactive and hybrid protocols. In this work, Ad-hoc On Demand Distance Vector (AODV) protocol is employed against malicious attack.

AODV is one among the well-known on-demand routing protocol. In the case of AODV, the routes are maintained for the time duration as long as it is required. In AODV, each and every change happening in the network need not broadcasted to every node. At any particular point of the network, if there is any link breakage, it does not have any effect over the progressing transmission and in addition, global broadcasting is also not necessary, and just the impacted nodes are locally informed. The AODV protocol is the most extensively used and popular reactive routing protocol where the routes are established just when they are necessary. The mobile devices or nodes present in the network do the exchange of the routing packets between them when they desire to communicate with one another and thereafter maintain only these routes that are established. The AODV routing protocol is one that is adaptive to the DSDV (Destination-Sequenced Distance Vector) protocol for getting dynamic link conditions.

Every time that a node requires to transmit the data packet to another node, it does a check in its routing table. In case it contains a new route to the destination node, it makes use of that route for sending the data packet. When there is no route available or it is not a new route, then the node begins the process of route discovery. Hence, it does the broadcast of Route Request message (RREQ) to its neighbors. The intermediate nodes then checks if it is the destination node or else it has a new route to reach the destination node. In case of availability of a route, the intermediate node transmits back a Route Reply message (RREP) to the source node. Else, it just forwards the RREQ message to its peers by employing the flooding technique. This procedure continues till the destination node is discovered or the node which has a new
enough route for the destination is discovered. Once the route discovery
process is finished, the source node and the destination node can communicate
and transmit the packets back and forth. Therefore the AODV protocol is an
important protocol for providing secured routing in MANET. In the next
subsequent section the challenges in MANET are evaluated.

1.5 MANETS CHALLENGES

The ad-hoc networks are self-configuring, self-preserving, self-
healing architecture. The challenges faced are, unavailability of fixed access
point, dynamic network topology, hostile environment and inconsistent
connectivity. The Ad-hoc network establishes soon and adapts to the changes
and less amount of power. At last, Ad-hoc possess no trusted central authority.
Owing to the dynamically varying characteristic, the Ad-hoc is imposed with
few issues that are summarized in the coming sections.

1.5.1 Quality of Service (QOS)

The Ad-hoc network dynamically establishes the organization every
time the node desires to have communication with their neighboring node.
Because of the dynamically varying topology in ad-hoc network, offering QoS
is a hard task, Chakrabarti & Mishra (2001). QoS are necessary due to the
speedy evolution in mobile technology and real time applications such as
multimedia, voice. Provisioning QoS in ad-hoc network is required for
maintaining the best-effort-of service. The QoS metrics are namely bandwidth,
latency, jitter and guarantee of delivery. The bandwidth is utilized for
representing the data rate of transmission in the network.

Latency ensures the delay occurring from the origin to the
destination. Jitter represents the changes in delay. Reliability depicts the
percentage of refusal of access to the network service. Wireless channels are
changing in a rapid manner and it critically impacts the multi-hop flows. In the case of ad-hoc networks, the peer-to-peer channel quality might change fast. Hence, the quality of the link might impact the peer-to-peer QoS metrics in the multi-hop path, Wattenhofer et al. (2001). The QoS factors are explained below:

- Packets are tangle for the shared media over nearby links of a flow: Tangle between the packets present in the same stream at different nodes. Such a kind of tangle happens in the wireless channel shared by nodes present in the neighborhood.

- Intervention between the nodes negatively impacts the quality of transmission: In Ad-hoc network, QoS is adversely impacted by the interference from radio. Interference heavily develops in ad-hoc as the nodes are out of the transmission range. When the nodes are transmitting, the rest of the power is sufficient for interfering with transmission. Interference in the nodes in the non-neighborhood might lead to the packet to be dropped.

- Limited resources: Owing to the dynamic variations in the link flow, ad-hoc network renders changing resources.

- Sufficient admission control: The admission control makes the decision regarding if the bandwidth available will suffice for the link flow in the resources available. Ad-hoc networks offering a limited bandwidth capacity might impact the end quality of service.

- Highly dynamic: Ad-hoc network characteristics are of dynamically varying topology and this dynamic variation happens because of radio transmission and mobility.
Components of QoS

QoS model: The QoS model defines the complete architecture of ad-hoc network and in addition, helps in the services offered to the network. It does not give details regarding the protocols or its implementation. There are two kinds of QoS model available. The first one is the Integrated Service (Intserv) that has to maintain the virtual circuit connection oriented state information in each flow. The second one is the Differentiated Service (Diffserv) that does not provide any kind of state information.

QoS signalling: QoS signalling is employed for allocation and reallocation of the resources at the time of the network flow. The signalling process is in accordance with two categories. Firstly, QoS signalling is utilized between the routers. Secondly, the signalling can be correctly detected and utilized by the respective resources. The QoS signal can be categorized into in-band and out-band. In the case of in-band signalling, signal information is transmitted along with its packet. In the case of out-bound signalling, explicit packet is required for handling the signalling.

QoS routing: QoS routing is modelled to render the optimal path between end-to-end resources which satisfy QoS requirements like bandwidth, delay etc. The QoS can preserve the ad-hoc network by employing the admission control in order to check if the locally available bandwidth is larger than the necessary bandwidth. This way, the process may help in maintaining the quality of service in the ad-hoc network.

1.5.2 Scalability

The scalability issue arises in ad-hoc networks because of the characteristics of the multi-hop (Wattenhofer et al. 2001). The ad-hoc network scalability is dependent over the size of the network and the forwarded packet capacity in the network. In the recent times, several challenges have come up in
large-scale ad-hoc networks. The scalability is based upon the factors mentioned below:

- Equal node priority: Every node in the network has the same priority in sharing the physical resources. Hence, data rates of all the nodes are the same.

- Uniform distribution of destination: The packets are equally distributed from source to N-1 nodes, Chiafferini & Rao (2000).

- Spreading the node reliably: The transmission capacity of the node must be sufficiently large compared to their neighbor nodes in order to prevent interference.

- Shortest path: The packets which are transmitted from the source to the destination depends on the shortest path. The scalability can be maintained by partitioning the network area based on their geographical location. The entire network area can be partitioned into small virtual grid cells so that each node in every virtual grid cell can be in communication with the other nodes present in the same cell.

### 1.5.3 Security

Security is a critical issue in the standards of ad-hoc networking, Gagandeep et al. (2012). Data transformation in the case of ad-hoc network has to be carried out in a secured manner. The security challenges in ad-hoc network are dynamic topology, bandwidth, smaller device size and less battery life. Owing to the dynamic nature, it is hard to have secured transmission maintained in the network, Papadimitratos & Haas (2002). The ad-hoc network does not rely on any pre-available infrastructure such that the node can go out
and then join the network in a situation where the security may fail. Two kinds of attack happen in ad-hoc network, first one is passive attack, and this attack does not modify the transmitted information in the network. But, it can permit unauthenticated users to find the message. Second one is active attack, which is a severe one and disrupts the message flow between the nodes present in the network. It may permit the unauthenticated user to make modifications to the message. The adversary node can be recognized by means of dropped packets, drained battery, bandwidth consumption, unreliable packets, delay, connection failure and false routing.

### 1.5.4 Power Control

Power control is one among the chief elements in ad-hoc network since battery offers restricted capacity to the nodes. When the power failure happens in the node, it may impact itself and also the whole network architecture tends to fall apart. The cause for power control are the restricted capacity of nodes, non-static infrastructure, restraints on the battery sources, choice of remarkable transmission power and channel usage, Lorch and Smith, (1998). Ad-hoc power maintenance is dependent on:

- **Low capacity condition:** The low power mode facilitates the node to be active at the time of transmission of packet and it renders the node inactive while they are waiting for the receipt of the packet, Singh & Raghavendra (1998).

- **Transmission power control:** The transmission power control has to be dependent on the range of transmission, error rate and interference. This way, the stronger transmission power leads to an increase in the transmission range and minimizing the hop count to the destination, Ramanathan & Rosales-Hain (2000).
Power aware routing: The routing protocols are developed for finding the shortest hop from the source to the destination. By this way, the routing protocol helps in prolonging the network life time by minimizing the use of battery life time of the nodes (Wattenhofer et al. 2001).

In order to maintain power control by minimizing the active energy, the power down mode is used to minimize energy during inactive. The load balancing technique allows the network maximizing by reducing over usage of the node, Petrioli et al. (2001).

1.5.5 Cooperation Between Nodes

Cooperation between the nodes is necessary in the ad-hoc network. Every node in the network coordinates with other node for packet forwarding and routing. Owing to dynamic varying topology, the nodes in the network do not depend on other nodes. In the case of ad-hoc network, source node sends the data to destination through the intermediate node. Without the cooperation with the neighboring nodes, the source node cannot successfully transmit the data. Hence, frequent changes in the link may result in abrupt topology modifications and network disconnections. Then the non-cooperative nodes may be defined in two ways, the first one is the malicious nodes which refer to the set of the nodes which attacks the network or breaks the link. The selfish nodes make use of the network for their use without paying back for using the network. Both the nodes are treated to be misbehaving nodes, Buttyan & Hubaux (2003). In Ad-hoc, high level cooperation between the neighbor nodes yield more flexibility to the network. Low level cooperation among the nodes makes the network to be vulnerable. Techniques for node cooperation are as follows:
➢ Concentrating acquaintance: The node forwards or drops the packet on the basis of the behaviour of the neighbor node. This needs the node to pay attention in the abandoned mode for capturing the actions of its neighbor node.

➢ Conversation of node: Nodes are always in communication with one of closest neighbor node in the whole network. It has to recognize the misbehaving node and then isolate the respective node. In order to properly manage the cooperation between the nodes, there is a need to have the trade-off optimized while forwarding the packets for others and simultaneously saving their energy resources.

In this work, the QoS elements are employed for analyzing the scalability and security in the MANET routing performance and the challenges are examined. But still the vulnerabilities MANET are important challenges against the security and is discussed further.

1.6 MANET VULNERABILITIES

Vulnerability is basically a weakness in the security system. A certain system might be vulnerable to unauthenticated data manipulation as the system does not validate the identity of a user prior to permitting to access the data, Priyanka Goyal et al. (2011). MANET is more vulnerable to danger compared to wired network. Few of the vulnerabilities are as below:

1) Lack of centralized management: MANET doesn’t possess a central monitor server. The lack of management causes the attacks detection hard since it is not easy to have the traffic monitored in a hugely dynamic and a large scale ad-hoc network.
2) No predefined Boundary: In the case of mobile ad-hoc networks, a physical boundary of the network cannot be defined precisely. The nodes operate in a nomadic environment in which they are permitted to join and then leave the wireless network. Whenever a malicious node comes inside the radio range of a node, it can communicate with that particular node.

3) Cooperativeness: Routing algorithm for MANETs generally makes an assumption that nodes are cooperative and are non-dangerous. Consequently, a malicious attacker can become an essential routing agent easily and interrupt the network functioning.

4) Limited power supply: The nodes in the mobile ad-hoc network are required to take the limited power supply into consideration that will lead to multiple issues. A node in mobile ad-hoc network might behave selfishly when it finds that the power supply is limited.

5) Adversary inside the Network: The mobile nodes in the MANET are free to join and leave the network. The nodes inside the network might also behave in a malicious manner. This imposes difficulty in the detection when the node behaviour is malicious. Therefore this attack indicates more danger compared to the external attack.

The above said issues in MANET structure render the routing to be a huge challenge. Particularly, the dynamic characteristic of MANET is vulnerable to several attacks. Therefore, an effective security based routing protocol is necessary for MANET applications. The important reasons for vulnerabilities are evaluated and in order to surpass the issues mentioned above, the security goals are discussed in the coming section.
1.7 SECURITY GOALS

In MANET, all the networking functions like routing and packet forwarding, are carried out by nodes themselves in a self-organizing way. Due to this, providing security in a mobile ad-hoc network is a very challenging task. The points to be evaluated whether the mobile ad-hoc network is secure or not are as below:

1) Availability: Availability indicates that the assets are available to authenticated parties at suitable times. Availability is applicable to both data and services. It guarantees the network service survivability in spite of denial of service attack.

2) Confidentiality: Confidentiality assures that the computer-related assets are available only to authorized users. Information has to be preserved against any kind of disclosure attack such as eavesdropping- unauthenticated reading of message.

3) Integrity: Integrity specifies that the modifications to the assets can be done only by authorized users or only in authorized manner. Integrity ensures that a message which is being transmitted is not corrupted.

4) Authentication: Authentication is generally a guarantee that the participants in the communication are authorized and are not impersonators. The helps of network must be available only to the nodes that are authenticated.

5) Authorization: This characteristic allocates different access rights to various kinds of users. For instance, a network management can be carried out by network administrator only.
6) Resilience to attacks: It is needed so as to maintain the network operation while a section of nodes is endangered or destroyed.

7) Freshness: It assures that the malicious node does not do the retransmission of packets that are earlier captured.

In this work, the security against attacks is accomplished by means of AODV and DSR protocols are utilized.

1.8 CLASSIFICATION OF SECURITY ATTACKS

This section deals with the security attacks like black hole attack and grey hole attack that are explained below.

A black hole attack in AODV happens because of the presence of an adversary node that advertises itself to possess a shortest and a new route to the destination. This kind of malicious node is referred to as black hole node since it does not forward the data packet to its neighboring nodes; it just drops the packets which are originating from the source node. In the black hole attack, the malicious node eats up the packet sent by the source node or the intermediate node and then does not transfer it to the destination or the rest of the intermediate nodes. It interprets itself in the form of a normal node by transmitting a reply to the sender of the packet along with a higher sequence number. Seryvuth Tan et al. (2013) proposed a novel protocol SRDAODV (Secure Route Discovery for AODV-based MANET) for the detection of black hole nodes. Here, in this protocol, the authors specified three thresholds for the classification of the malicious and normal node in three diverse environments—small, medium and large environments. In this approach, the sequence number of every response gets checked with the threshold value. When it is greater, then that node is considered to be a black hole node else a normal node.
Watchdog and Pathrater techniques are utilized for detecting the black hole attacks. Watchdog facilitates the neighbor nodes in detecting the malicious nodes. Watchdog identifies the malicious nodes by discovering the nodes which are discarding packets repeatedly. Pathrater allocates a default value to every node and thereafter takes note of the transmission behaviour of every node. After sometime, in case the value for a node goes below a specific threshold, then the node will get added to the black hole nodes list. This technique is not capable of handling the cooperative attacks.

Grey hole attack is one in which a node reacts maliciously for some particular time period by letting out the packets though it might arrive at a balanced behaviour and then forwards the packets by means of packet ID to other nodes. A Grey hole might also be observed with a random behaviour in which it omits few the packets in random while forwarding to other packets. Hence its detection is more tedious compared to the black hole attack.

Grey hole is one among the attacks that are initiated in the ad-hoc network. This works as a slow toxin in the network. Therefore, any assumption cannot be made on how much amount data could be lost. In the case of grey hole Attack, a malicious node gets some packets just to drop them. The attacker drops the packets selectively that originate from a single IP address or a range of IP addresses and then forwards the rest of the packets. Grey hole nodes in MANETs are very intelligent. Each node maintains a routing table that keeps record of the next hop node information for routing a packet to the destination node. When the source node desires to route a packet to the destination node, it utilizes a specific route when there is availability of such a route in its routing table studied by Vishnu et al. (2010). Else, the nodes begin a route discovery process through the broadcast of a Route Request (RREQ) message to its neighbor nodes. After receiving the RREQ message, the intermediate node discovers the most recent path in their routing tables as a reverse route to the
source node. A RREP is transmitted back in the reverse direction of the source node, once the RREQ query is reached to either the destination node itself or any other intermediate node which possesses a fresh route to the destination.

The security attacks that are mentioned above are detected by making use of effective protocols studied in this research.

1.9 SECURE ROUTING IN MANETS

The working of secure routing has a significant role to play in MANETs security because of the lack of fixed infrastructure. The recent efforts towards the development of secure routing protocols are chiefly directed towards reactive (on-demand) routing protocols like DSR, Johnson and Maltaz, (1996), or AODV, Perkins & Royer (1999). On-demand routing protocols have been exploited for performing in a better manner with considerably lesser overhead compared to the proactive protocols in several scenarios, Pietro Michiardi & Refik Molva (2004). Few of the routing protocols which can help in security in the MANET are summarized as below:

- Secure On-Demand Routing Protocol – Ariadne
- Secure Ad-hoc On-demand Distance Vector routing protocol – SAODV
- Secure Efficient Distance Vector Routing – SEAD
- Securing the Destination Sequenced Distance Vector Routing Protocol – SDSDV
- Secure Routing Protocol – SRP
- Secure Link State Routing protocol – SLSP
- On-Demand Secure Routing Protocol Resilient to Byzantine Failures
Authenticated Routing for Ad-hoc Networks – ARAN

Secure Position Aided Ad-hoc Routing – SPAAR

Security Aware Routing Protocol – SAR

Few of the crucial security routing protocols are explained below.

**Secure Efficient Distance Vector Routing (SEAD) Protocol**

The Secure Efficient Ad-hoc Distance vector routing protocol (SEAD), which is a secure ad-hoc network routing protocol is developed on the basis of the Destination-Sequenced Distance-Vector routing protocol. For the purpose of supporting the usage with nodes having less CPU processing capability, and in order to safeguard against Denial-of-Service attacks where an attacker tries to make other nodes to eat up excess amount of network bandwidth or the processing time, use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs better over a range of scenarios that are tested, and is reliable against different uncoordinated attackers that create wrong routing state in other nodes, despite any active attackers or endangered nodes in the network. It is reliable against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network.

**Authenticated Routing for Ad-hoc Networks (ARAN)**

ARAN comprises of a preliminary certification process which is followed by a route instantiation process, guaranteeing end-to-end authentication. The protocol is simple in comparison with most of the non-secured ad-hoc routing protocols. ARAN employs cryptographic certificates for providing authentication, message-integrity and non-repudiation to the route discovery process. Therefore, ARAN needs the support of a trusted certificate server, the public key of which is known to every valid node. Nodes employ these certificates for authenticating themselves to other nodes at the
time of exchange of routing messages. ARAN, yields secure routing for the managed-open and open environments. ARAN renders authentication and non-repudiation services are utilizing cryptographic certificates which assure end-to-end authentication. ARAN restricts or avoids attacks which can discomfit the rest of the insecure protocols. ARAN is actually a simple protocol which does not need considerable extra work from the nodes present within the group.

Secure Ad-hoc On-demand Distance Vector routing protocol (SAODV)

The Secure Ad-hoc On-Demand Distance Vector (SAODV) Perkins et al. (2002) deals with the issue of providing security to a MANET network. SAODV extends the AODV routing protocol which can be utilized for protecting the route discovery technique rendering security features such as integrity, authentication and non-repudiation. SAODV supposes that every ad-hoc node contains a signature key pair from an appropriate asymmetric cryptosystem. Moreover, every ad-hoc node has the capability of doing a secure verification of the association between the address of a given ad-hoc node and the public key of that particular node. Accomplishing this is the task of the key management scheme.

In MANET, the security protocols mentioned above are employed for producing high level security against the number of attacks primarily.

1.10 PROBLEM SPECIFICATION

Even though several research proposals are available in literature dealing with secure data transmission and attack threats, MANET’s full potential has not been exploited so far. Hence there is a necessity of discovering the protocol which can deal with the security threats which might happen in the MANET environment during data transmission. The routing protocols must be capable of discovering the secured routing path with guaranteed QoS parameters and reliable environment. Inspired by the facts
above, this technical work yields a whole classification of different heterogeneous routing protocols and security mechanisms for MANET.

1.11 OBJECTIVE

The important goals of this work are

1. To evaluate the security threats imposed on MANET and the effects of active vulnerable attacks on the performance of MANET.

2. To design a security strategy against the active attack like DoS/DDoS and Black hole attack over MANET.

3. To enhance the network performance considerably in the scenarios of active attacks.

4. To assess the performance of the protocol proposed employing the NS-2 simulator. The performance is assessed with respect to throughput, Packet Delivery Ratio (PDR), end-to-end delay and network overhead.

5. To compare the performance of the new protocol with the available protocol in the environment vulnerable to active attacks like DoS and black hole attack.

1.12 RESEARCH CONTRIBUTION

The prime contribution of this work is focused over the security mechanism designed for network layer and it neglects the communication factors on the physical layer of the network. This research scope extends to

1. To get a stable and secured model of AODV protocol for improving the network performance against malicious node attack.
2. The available DSR routing protocol is transformed and used with trust based security measures for the detection and exclusion of selective black hole attack in MANET.

3. Black Hole Attack Detection in MANET employing Hybrid Swarm Optimization Algorithm

1.13 ORGANIZATION OF THESIS

Chapter 1 discusses about the overview on the Mobile Ad-hoc Network, features, applications and its security challenges. This paper chiefly focuses on the better routing mechanisms in MANET environment with due concern provided for QoS parameters and the security issues.

Chapter 2 overviews the short discussion of the relevant works on various routing protocols and security mechanisms for MANET.

Chapter 3 explains the modified DSR protocol working for the improvement in the network performance and the different trust measures.

Chapter 4 studies the description about the AODV protocol for improving the network performance against malicious attacks in detail.

Chapter 5 discusses about the hybrid swarm optimization methodology for the detection and prevention of the black hole attacks existing in the network,

Chapter 6 studies in detail regarding the result and the overall research work and evaluates the performance of the novel techniques.

Chapter 7 provides the conclusion and explains about the routing protocols of MANET environment for the improvement in the network
performance against security violations with a futuristic perspective over MANET routing.

1.14 SUMMARY

This Chapter 1 studies about the overview over the behaviour of Mobile Ad-hoc Networks along its variable characteristics. The application which uses the MANET environment also gets discussed with concern laid on various functioning procedures. The probability of the security challenges which could happen in the MANET environment is also explained. The variable routing mechanisms which can be employed in the MANET environment for achieving the secured routing is also studied. Different kinds of attacks and its classification with respect to their functionality is provided in detail.