Chapter 1

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION TO AD-HOC NETWORKS

Ad-hoc Network (AN) belongs to a class of peer-to-peer wireless communication network in which direct communication takes place between wireless devices without the assistance of any Access Point's (AP). As and when the need of communication arises, the WN is established spontaneously subject to the condition that the participating nodes should be in close proximity of each other. In case the two devices are not in close range, multi-hop communication comes in to play. However, as the size and number of devices increase the connection quality and the communication speed deteriorates. On the contrary the self-supporting nature of AN's is quite handy in dealing with the situations such as natural calamity, emergency situations, military operations and other scenarios where a prompt response for data communication is required. Nevertheless, in spite of being easy to deploy and quick response, there are few practical limitations of AN's especially in terms of security and reliability [42].

1.1.1 Categories of Ad-hoc Networks

Ad-hoc networks can be categorized as follows [56]:

- Mobile Ad-Hoc Networks (MANET): It consist a pool of nodes, which are mobile and self-sustaining. MANET has introduced a new category of network establishment that is best suitable for an environment where instant and cost-effective communication solution is required.

- Wireless Mesh Networks (WMN): It is an Intranet of various clients viz: laptops, wireless nodes etc. structured and connected in the form of mesh topology. The data generated in WMN is shared within the mesh network and is not transmitted to the outer world.

- Wireless Sensor Networks (WSN): It consist of numerous sensor-based nodes and is deployed sense and observe physical or environmental data such as temperature, pressure, sound etc. The application of WSN's is widespread and cover areas such smart city, vehicle detection, weather monitoring and so on.

1.2 MOBILE AD-HOC NETWORKS

A network of mobile nodes is known as MANET that are moving between different locations. In a general wireless network, the whole geographic region has some base stations each of them has fixed coverage in the geographic area. The mobile transmit whatever the signals nodes can hear the base station. Any mobile node will always be coming to some base station and the base stations deliver whatever the signal or data. This environment is a generic view of wireless networks. The MANET nodes, in contrast, participate in cooperative packet transmission, with every mobile node participating for both transmission and reception, with the goal of transmitting the packet to a different node [4]. A customized routing operation does not require to be carried out through the wireless router. To transmit the packet to the intended node, each mobile node can execute routing and route selection.

Mobile ad-hoc networks require cooperative transmission of packets. The reason behind the cooperative communication is, unlike other types of the wireless network here is no base station to coordinate the routing process and to transfer the packet to the

destination. In addition, the nodes of the network are always moving towards any direction that makes the topology as unfixed one. The mobile ad-hoc network is a topology less network; the packet forwarding requires cooperative transmission [50]. Figure 1.1 shows a general mobile ad-hoc network.

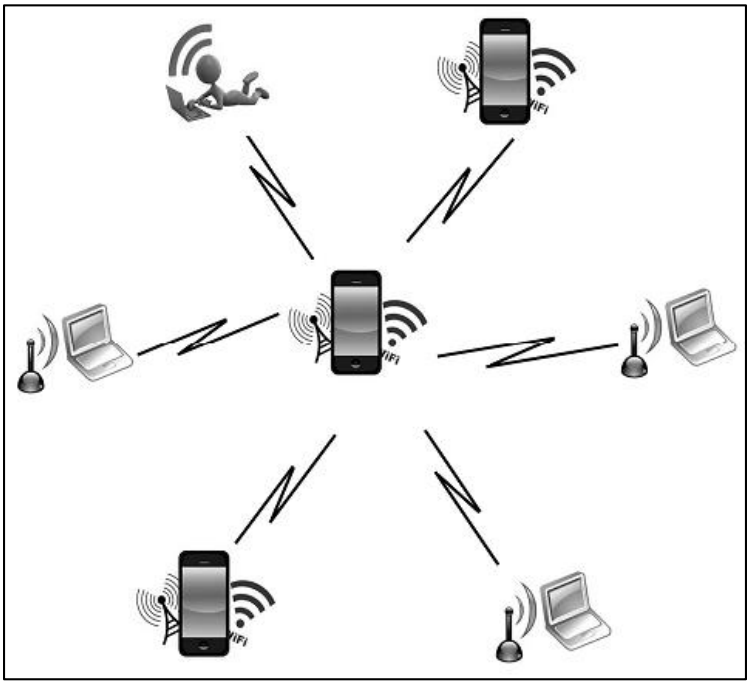

Figure 1.1 Mobile Ad-hoc Network

Similar to topology, there are other constraints to notice on mobile nodes in this kind of network. The most important one is the nodes come up with a single radio that has fixed transmission range. The transmission range of the radio decides how far the signal transmitted by the mobile node could be heard. In addition, each node has some constant power in Watts, which is required to activate the radio for the transmission and reception of signals. Whatever the process is doing, whether transmission or reception of the signal, the node loses some energy, and the lifetime of the node is only up to the energy it has.

The mobile node has other properties like mobility speed; the node can move at any speed and any direction. This property changes the topology of the network in a more frequent manner that affects the transmission of packets highly. The factors that influence the functioning of the mobile ad-hoc network and routing are discussed in detail in this section.

1.2.1 Main Advantages of MANETs

Several benefits distinguish MANET from traditional wireless networks [18, 19]. Here are listed few of them:

- MANET's decentralized design offers it additional resilience against centralized methods' single points of failure, such as base station or access points
- MANET can be used in situations where setting up and maintaining a wired network would be nearly impossible (e.g., a disaster area or a battlefield)
- A distributed wireless network with no fixed infrastructure is known as a MANET. This implies that the state of the clients can be maintained without a centralized server
- Multi-hop networks with autonomous terminals and changeable topology are known as MANET
- MANET is a viable option for the temporary network
- Very low cost is estimated

1.2.2 MANET Applications

The Mobile ad-hoc networks have different challenging and exciting areas of application in various ranges like from classrooms to war fields.

- Battlefield: In a battlefield, the power of the defense will be added through the use of an AD network, where the nodes that can detect and communicate will be established rapidly and without delay. Ad-hoc nodes' perceive and communicate capabilities aid inside the transmitting of messages through one unit to the next with the purpose of receiving assistance, sending control messages, or relaying pertinent information regarding the status of the force
- Rescue Operation: When there is a fire accident, the ambulance and fire service are required, and they must be called in quickly. In these circumstances, the wireless network may be set up quickly, allowing the communication amongst the rescuers
- Event Coverage: This feature facilitates information sharing across criteria that are identical. For instance, in a media conference, multiple reporters can transmit relatively similar information via wireless gadgets such as laptops
- Classroom: The teacher may set up an ad-hoc network so that laptops can be used to transfer files between participants
- Collaborative work: In a small number of corporate settings, the need for interactive computing could be more critical outside of the office than inside, in locations where workers must gather outside in order to collaborate and exchange information regarding a certain project

- Local level: Ad-hoc networks can establish a temporary, transient multimedia network using laptops in dispersing as well as distributing information between attendees of a conference or class independently. Home networks, where devices can interact directly to exchange information, may be another potential local level use
- Personal Area Networks (PAN) and Bluetooth: PAN is a confined, short-range network where each node is typically linked to a specific person. A laptop and a mobile phone can communicate with one another more easily thanks to short-range MANETs like Bluetooth
- Commercial Sector: Ad-hoc can be employed in crisis operations during disaster relief efforts, such as in fire, flood, or earthquake situations. When a data transmission must be quickly deployed due to a destroyed or unavailable communications infrastructure, immediate recovery efforts must be carried out [41]

1.3 ROUTING IN MANET

A routing protocol describes various channels through which routers share and communicate information, making it easier for them to select the paths between any two nodes within a computer network. As a result, the routing algorithms choose specific path. Each router is built with intelligence of the networks that are immediately correlated to it. This information is shared by a routing protocol first among the next closest neighbors, then throughout the overall infrastructure. Routers learn about the network structure in this way [8].

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 [9].

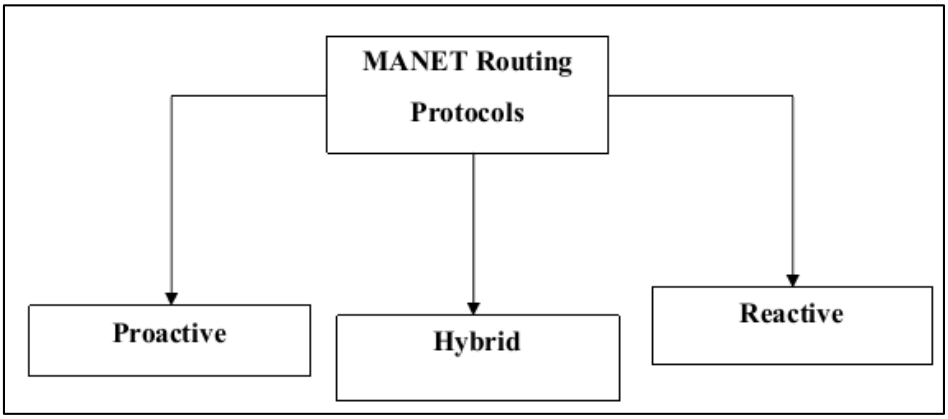

Figure 1.2 Classification of MANET Routing Protocols

1.3.1 Proactive Routing Protocol

This kind of routing protocol employs a table to keep track of various routes that can be used to connect to each node in the network. Frequently, the table will be modified through broadcasting an update message to all of its neighbors and network nodes. In a wired network, routing protocols like Routing Internet Protocol (RIP) are replaced by them.

The next hop on the chosen route to the destination must be chosen from the routing table by the node attempting to transmit a packet [13].

In this type of routing protocol, the nodes follow the chosen path of transmission to forward the data packets. The problem with this kind of routing protocol is, if there exist any traffic and the source node will not know packet drop at some point of the route then it. It keeps sending the packet through the selected route and degrades the Quality of Service (QoS) by increased packet drop.

1.3.2 Reactive Routing Protocols

In reactive approach, the nodes start routing without having any prior knowledge, and it learns the network topology by identifying the network topology and the nodes present in the network. The routes available to reach other nodes are computed using a variety of control packets that starts forwarding the packet. In this type of routing, the forwarding phase is performed by monitoring the traffic present in other nodes of the selected route. Each node performs monitoring the traffic and selection of the new route according to the situation.

In contrast to proactive methods, reactive direction-finding algorithms only locate a path to a destination when it becomes essential. The phases one and two of the reactive framework are path discovery and maintenance. If there is no route in its route table during the path discovery phase, the node that must transmit a packet launches a sighting instrument. When a positive flag is sent from the route's opposing side, it is recognized that the route is present. The route tracking method maintains the routing table and examines for node failure.

1.3.3 Hybrid Routing Protocol

The hybrid approach aims at combining the best features of both proactive and reactive routing protocols. It was proposed to eliminate the disadvantages of the reactive and proactive approaches such as high control overhead in proactive routing protocols and high delay associated with the route discovery in reactive routing protocols.

1.4 MANET CHALLENGES

- **Limited Wireless Transmission Range:** The wireless networks include radio band, that's why they are much cheaper than the prices available on the wireless networks. The protocols used for routing wireless networks should therefore always use bandwidth to keep overhead as low as possible.
- **Overhead Routing**: Nodes also change the position of their networking for Ad-hoc wireless networking. In the routing table, some bad routes result in unnecessary overhead routing.
- **Battery Restrictions**: This is an ad-hoc network's limited resources and constitutes a significant restriction to the nodes. The power supplies used in such networks are energy supplies that restrict system weight, size, and portability. Through power and speed, the nodes are voluminous and less compact. Therefore, this resource must be used only for MANET nodes [42].
- **Asymmetric Connections**: The bulk of the wired networks are always enabled by the symmetrical links. Nevertheless, Ad-hoc networks are not mobile because the nodes change their location continuously within the network.

- **Packet Losses caused by Mis-transmission**: Factors such as high BERs (high bit error rates), increased collisions due to unseen terminal presence, interference presence, contending at the location, unidirectional connections node, standard node mobility path disruption and inherent fading properties are causing substantially greater losses in ad-hoc wireless networks.
- **Self-governing**: No centralized management firm is available to handle the various mobile nodes' operations.
- **Dynamic Topologies**: Mobile nodes can be connected and connected dynamically at random. The connections to the network vary in time and depend on one node to the next.
- **Discovery Device**: A dynamic update must provide the information and identify appropriate newly moved nodes to allow for the optimal automated selection of a path.
- **Optimize Bandwidth**: Wireless connections are much more efficient than wired communications. The bandwidth is always optimally used in wireless networks by routing the Protocol, while maintaining the overhead as low as possible.
- **Limited Resources:** Mobile nodes depend on a scarce resource, battery power. Capacity and strength are severely restricted as well.
- **Scalability**: Network's scalability can be precisely defined such that even with existence of large no. of nodes service level is sufficient.
- **Physical Security Limited:** Availability means greater risk protection for both legitimate and malicious network users, such as peer-to-peer network systems and

the wireless intermediaries. Eavesdropping, spoofing & denial of service should be measured for infringement.

- **Self-operated and less infrastructure**: Self-healing function requires MANET to refine to cover every node moving out of their control. Self-healing needs to be done.
- **Poor Quality of Transmission**: This is an important problem of wireless communication, resulting in loss of received signal by multiple error sources.
- **Ad-hoc Approach**: problems to be incorporated into a traditional approach framework.
- **Security**: Security is a critical issue in the standards of ad-hoc networking: Ad-hoc networks need that data transformation be done in a secured environment. Ad-hoc network security challenges include changeable topology, bandwidth, constrained device size, and limited battery life [42].

1.5 MANET SECURITY

In a MANET, nodes perform essential networking tasks, such as packet forwarding and routing, in a self-organizing manner. Due to this, providing security in a mobile ad -hoc network is a very challenging task [46]. The following criteria must be met in order to determine whether a mobile ad-hoc network is secure:

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:** It states that only authorized users or just in an allowed method may modify the resources. Integrity guarantees that an information being transferred is not interfered with.

4) **Authentication:** Generally, authenticating a communication ensures that the parties involved are legitimate and not imposters. Only authenticated nodes should have access to the network's resources.

5) **Authorization:** This characteristic allocates different access rights to various kinds of users. For instance, network administrator can carry out a network management only.

6) **Resilience to Attacks:** It is needed to maintain the network operation while a section of nodes is endangered or destroyed.

7) **Freshness:** This ensures that the malicious node does not repeat packets that have already been intercepted.

1.6 ATTACKS IN MANET

There are two main categories of attacks. They are:

- Active attacks
- Passive attacks

1.6.1 Active Attacks

In this attack, the malicious node publicizes false information for confusing the framework topology. Active assault refers to attempts to compromise the system in computing security. An active assault involves the introduction of data into the system and the potential modification of data already present [47]. These dynamic attacks can either center at the routing framework or endeavor to surge the framework systems. The different sorts of dynamic attacks are as follows:

- Sinkhole attack
- Replay attack
- Flooding attack
- Location Discovery attack
- Black Hole attack
- Wormhole attack
- Blackmail attack
- Denial of Service attack
- Rushing Attack

- **Sinkhole Attack**

A node attempts to gather data from each neighboring node toward itself in a sinkhole attack. A rogue node creates false routing information in this attack and appears as regular nodes. The sinkhole nodes try to handle all framework development on their

own, change the data packets, shorten the lifespan of the framework, and create a disorganized system topology that would ultimately destroy the framework [72].

- **Replay Attack:** Playback attack is another name for replay attack. Here, a challenger or initiator intentionally forwards the packet or delays legitimate data transmission by rerouting the data and retransmitting it through IP packet transmission [81].

- **Flooding Attack:** To prevent the targeted client from being able to use the framework assets for proper communication, a rogue node may also introduce bogus packets as part of this attack. Most on-demand direction tables, including Source Routing Protocol (SRP), Secure Ad-hoc on Demand distance vector (SAODV), etc., allow for the flooding attack [82].

- **Location Discovery Attack:** Attacks aimed at an ad-hoc network's security requirements include location discovery. An attacker is capable of learning the location of a node or even the structure of the entire framework using action examination techniques or more explicit testing and observing approaches.

- **Black Hole Attack:** In a black hole attack, the malicious node uses the routing protocol to assert that it is the only node that can reach the target node in the quickest amount of time, but it discards the routing packets and fails to pass them on to its neighbors. In MANETs, a single black hole assault is very common.

- **Wormhole Attack:** The wormhole attack is one of the most significant attacks among those mentioned here since it involves two hostile nodes that share the framework. Think about two attackers who are working together and have a high-speed link between them as an example. Due to the high-speed link, every route request that passes

through the colluding nodes A1 and A2 will appear to cross the shortest path [77]. As a result, source will deliver all messages to the destination over the insecure links A1 and A2. The two attackers have complete control over the network of nodes that have established a route through the wormhole relationship.

- **Black Mail Attack:** A malicious node behaves like a blackmailer in this attack by discarding all data packets passing through it and dissipating energy. The network is basically split into two unconnected nodes if the attacking node is a connecting node.
- **Denial of Service (DoS) Attack:** In recent times this type of attack has gain much attention from the hacker's community. There are various ways to implement this type of attack but the most prominent is when the attacker decipher itself to be a service provider and in the event of any request from other nodes, the attacker drops the packets. The most critical aspect of this attack is that the affected node remains unaware about being attacked.
- **Rushing Attack:** The packets will be forwarded swiftly in a rushing attack in order to join the forwarding group. If an attacker is present when a node sends a route request packet to a neighboring node in a wireless network, the attacker will accept the packet and send it to the neighbor with a higher transmission speed than other nodes in the wireless network. The attacker will initially use a high transmission speed to get the packet to the target node. The destination node will accept this route request packet, and any later route request packets will be ignored [32]. The receiver as being reliable recognized this route, and it was used for continued transmission. Attacker will be able to intercept the sender and receiver's communication in this approach.

1.6.2 Passive Attacks

In a passive attack, the attacker merely tries to gather vast amounts of information by listening to the routing activity without interfering with the operation of routing protocols. The attacker does nothing more than observe and watch the transmission; no attempt is made to alter or edit the data packets. Passive attacks come in two different flavors [31]. As follows:

- Traffic analysis
- Eavesdropping

- **Traffic Analysis:** In this attack, attacker watches the transmission of information to gather basic information, like, frequency and length of messages.
- **Eavesdropping:** In Eavesdropping, attacker obtains arranged information of keys like, private key, public key and password that was kept secret during transmission.

1.7 MOTIVATION

In the recent trends, wireless networks and MANET have yielded tremendous opportunity and popularity. This opportunity and popularity insisted on many kinds of research to focus on it. This highly flexible nature of the MANET also creates many network performance-related and security related issues. Various security vulnerabilities threaten the process in MANET in various ways. Sequence number attacks such as grey hole and black hole attacks are such dangerous attacks that significantly weaken the functioning and performance of the network in different situations.

The most of the existing protocols have been developed to identify either black-hole or gray-hole attacks during the route discovery stage. There are only a few unified

protocols to identify both types of attacks. In addition, the attacks during data transmission can degrade the transmission efficiency by dropping data packets, which affects the network throughput. Therefore, it is necessary to identify the attacks during the data transmission stage.

An insufficient dynamic structure of a MANET makes it particularly vulnerable to various routing attacks. Black-hole attacks are suspected nodes that emerge in the system and surreptitiously reject data transmitted or received. The discovery and avoidance of this attack are made more difficult by the constant denial of information during the exchange. The block-hole node is a node that joins the AODV protocol by declaring itself as a legitimate route for the target. It builds a new route to the target node via the source node and rejects packets from any other nodes, preventing valuable data from being exchanged. Gray-hole nodes forward data in the same way as regular nodes do. However, it may reject packets selectively without confidence and realize suspected behaviors based on rejecting or broadcasting packets from other nodes. Sequence number assaults are another name for black-hole and gray-hole attacks.

1.8 OBJECTIVES

The main objective of this research is to secure hybrid routing to thwart sequential attacks in mobile ad-hoc networks.

- To protect the data packets and routing table information from consecutive attacks in a MANET
- To enhance the security by reducing routing overhead to improve the energy efficiency and optimizing data delivery

- To ensure route maintenance security by implementing the robust attack detection mechanisms which helps to identify and defend the black and grey hole attacks during the data transfer stage
- To detect the various attacks that exploit vulnerabilities in secure route maintenance using the Secure Intelligent Informer technique to identify the attacks on any specific nodes
- To protect the packets from various types of network attacks simultaneously with higher accuracy from the routing path during the data transmission stage
- To propose novel approach that able to increases data transmission efficiency while extending network life

1.9 CONTRIBUTIONS

The main aim of the first phase is to secure node and discover the secure route using SRD-AODV (Secure Route Discovery Ad-hoc on-Demand Distance Vector) protocol developed a hybrid framework with secure neighbor discovery, node authentication using Modified Elliptic-curve Diffie–Hellman (MECDH) and malicious node detection and isolation process. The hybrid framework is incorporated with the AODV protocol and developed as SRD-AODV. This protocol prevents the malicious nodes from routing by isolating them from the network with many restrictions. Hence, the secure nodes and routes are discovered using proposed SRD-AODV protocol. Performance evaluation of this protocol is conducted using metrics such as packet delivery ratio and delay. The SRD-AODV protocol also compares with AODV and other existing protocols.

In the second phase, the proposed Secure Route Maintenance and Attack Detection based AODV (SRMAD-AODV) protocol is used to estimate node energy and trust, recognize black-hole and gray-hole attacks, and defend against them throughout the data transfer. The secure nodes are grouped together called Connected Dominating Set (CDS). Initially, an Attack Discovery System (ADS) node is decided from the CDS method based on energy and confidence score. The nodes consume adequate energy to create a path for data transmission. In data transmission, check the responses of the node to the status packet that is whether the node sends counterfeit responses or drops the packet. If node drops entire packet, it is considered as black hole attack and the part of the packet drops considered as grey-hole attack. The suspected nodes transmit beacon messages regularly, resulting in a large amount of redundant traffic to increase the routing overhead. Hence, such nodes must be mitigated to minimize the additional routing overhead. For this purpose, this proposed protocol can integrate CDS and ADS methods to identify the suspected nodes (i.e., black and gray-hole nodes) and to minimize the routing overhead. To evaluate the effectiveness of the proposed protocol, it is compared to existing protocols through simulation for detecting black and gray-hole attacks. The evaluation is performed based on several performance metrics including End-To-End Delay (EED), Packet Delivery Ratio (PDR) and throughput.

In third phase is to identify various types of network attacks simultaneously with higher accuracy and defend them from the routing path during the data transmission. Different kinds of attacks such as wormhole attacks, jelly fish attacks, etc., influence the network lifetime and data transmission efficiency. Hence, Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) protocol is used to identify distinct attacks namely

black hole, grey-hole, and sinkhole, bogus, modification attacks, and route fabrication depending on their Size Acknowledgement Path (SAP) number. SIIDAI protocol chooses a specific node from the secured trusted ADS node list. The black-hole, grey-hole, and sink-hole attacks are considered as packet drop attacks. There is a possibility that attacks will enter through the multiple paths. Secure Intelligent Informer (SII) generates the SAP Number, which is attached to the packet sent by the origin node. The size of the SAP number can influence the packet drop. The SII detects multiple paths. Bogus or modification attacks is to identify the fake response using the acknowledgement of the SAP number. Route fabrication attack is to identify when a change in the path is detected, the path of the SAP number redirects the packet. The proposed SIIDAI protocol offers protection against various types of malicious nodes in the network, resulting in reduced packet loss. In comparison to SRD-AODV and SRMAD-AODV protocols, the SIIDAI protocol is evaluated based on end-to-end delay, Packet Delivery Ratio (PDR), and throughput. As a result of the evaluation, it was found that the SIIDAI protocol outperforms the SRD-AODV and SRMAD-AODV protocols in terms of end-to-end delay, PDR and throughput, while providing better protection against malicious nodes.

The primary objective of the final phase is to protect mobile ad-hoc network from various attacks using SIIDAI protocol based on Dynamic Packet ID (DPI). Secure Intelligent Informer creates the DPI in order to protect the node from six different attacks namely black hole, grey-hole, sinkhole, bogus, modification attacks and route fabrication attacks. DPI is a constant number that is chosen at random. After creating the DPI, it is attached to the packet that is sent from the origin node to the destination node via SII. When the packet reaches a new node, a new DPI is generated and attached to it for protection.

The use of dynamic DPI generation and attachment to each packet upon reaching a new node has proven to be highly secure. Attackers face difficulties in tracking the packets due to their constantly changing nature, the inclusion of DPI creates additional challenges for attackers attempting to gain access to the data. Hence, this method is considered one of the most secure means of data transmission. The performance of this approach is evaluated based on end-to-end delay, PDR, and throughput.

1.10 ORGANIZATION OF THE THESIS

Chapter 1: This chapter discussed the overview of ad-hoc networks, Categories, Mobile Ad-Hoc Networks, routing in MANET, challenges, security and several attacks in MANET.

Chapter 2: The purpose of this chapter was to conduct a literature review on the many different techniques that are targeted at Secure Route Discovery. Attack Discovery based on Energy and Trust were examined. Previous works of distinct attack identification were investigated. Various techniques of the protection of MANET were discussed.

Chapter 3: This chapter discussed about secure route discovery. The proposed method was developed a hybrid framework with secure neighbor discovery, implementing the node authentication using Modified Elliptic Curve Diffie-Hellman (MECDHA) enables the identification and subsequent isolation of malicious nodes within the network area. The hybrid framework is incorporated with the AODV protocol and proposed as SRD-AODV protocol. This proposed methodology achieves the good attack detection rated and improves the packet delivery.

Chapter 4: This chapter introduces the Secure Route Maintenance and Attack Detection routing protocol (SRMAD- AODV) helps to provide the attack discovery system based on energy and trust. The black hole and grey hole attacks are identified and minimized energy consumption. Hence, the data packet dropping was mitigated and the routing overhead was reduced.

Chapter 5: This chapter describes the methodologies for distinct attack identification. The SIIDAI protocol is proposed to identify the various types of attacks based on their SAP number. The SIIDAI protocol based on SAP number used to identify six different sequential attacks namely black-hole attack, grey-hole attack, sink-hole attack, bogus, modification attack, and route fabrication attack.

Chapter 6: This chapter explores the collaborative approach of the preceding proposals and to protect the packets and routing table information from sequential attacks based on their DPI number. The proposed approach increases data transmission efficiency while extending network life

Chapter 7: This chapter pictures the performance evaluation of the existing and proposed schemes in secure route discovery, black hole and grey hole attack discovery based on energy and trust, distinct attack identification based on SAP number, and protection based on DPI number

Chapter 8: This chapter summarizes the conclusions of the presented chapters. The future directions for this research work are also discussed.