Chapter 3

CHAPTER 3

SECURE ROUTE DISCOVERY

3.1 INTRODUCTION

Many different applications take advantage of the wireless network. The MANET's inherent characteristics, such as its dynamic infrastructure and immediate topology, have allowed for this wonderful expansion. The network generation can be flexible and set up whenever and wherever it is needed. This great degree of adaptability causes numerous performance and security problems for networks. The procedure in MANET is threatened by a number of security issues in different ways [19]. Grey hole and black hole attacks, which are examples of critical sequence number attacks, significantly limit the network's ability to function and execute in a variety of situations. By deploying false routes and modifying the routing information, sequence number attacks and black hole attacks destroy and discard a specific number of data packets [5]. Numerous academics have already proposed various methods for identifying sequence number attacks. To proactively identify those threats in MANET, a novel approach and routing protocol are developed in this study. Additionally, by doing this, the network's fake nodes that are susceptible to misbehaviors are removed.

The SRD-AODV (Secure Route Discovery Ad hoc On-Demand Distance Vector) protocol that has been proposed includes secure neighbour node discovery for secure route discovery by selecting trusted node detection, hybrid cryptographic methods to secure the data packets and routing table information, and finally incursion detection and prevention from sequential attacks in MANET. All of these features are included in the protocol.

The secure routing protocol that has been proposed discovers valid nodes and offers hybrid cryptography as a means of providing a cryptographic shield to data packets. This protocol is also able to detect attacks that are carried out by suspicious nodes and prevent these unhealthy nodes from routing by isolating them from the network and placing various limits on their access to it. Simulations are carried out with the help of the well-known open-source Network Simulator. The SRD-AODV protocol is also compared to attacked AODV as well as other MANET protocols that are already in use. The SRD-AODV routing protocol that has been suggested can ensure that data packets pass across the network with the highest possible level of security. In challenging circumstances, it is able to fulfil all of the essential requirements for security, including authentication, non-repudiation, confidentiality, and integrity. This SRD-AODV protocol ensures that only valid nodes can participate and also achieves access control over the participants by distributing authentication keys prior to the beginning of the routing process. In addition, this protocol ensures that only legitimate nodes can participate.

3.1.1 Routing Architecture in MANET

A MANET is a self-configuring network, meaning that its structure and topology do not depend on being predefined. Therefore, the process of routing is determined by demand. The two most common protocols used in MANET are AODV and AOMDV. In a MANET, the source node is the one that generates the route request (RREQ) packet, which is then sent to the destination node after passing via a series of intermediary nodes. In order for all of the neighbour to obtain the path, the RREQ packet will be broadcast. When it has finished receiving the packets, the neighbouring node will begin broadcasting once more until it locates the destination [58]. The route reply (RREP) packet is what the destination

node will use to communicate its response to the route request. The RREP will typically include a sequence number that can be used to determine how recently the route was travelled. The design of the MANET route is depicted in Figure 1, which shows the source node S1 broadcasting RREQ to all neighbour nodes 2, 5, and waiting for the RREP from the destination node D11. The destination D11 will generate RREP and transmit using the path with the fewest available hops, which is 9→6→2.

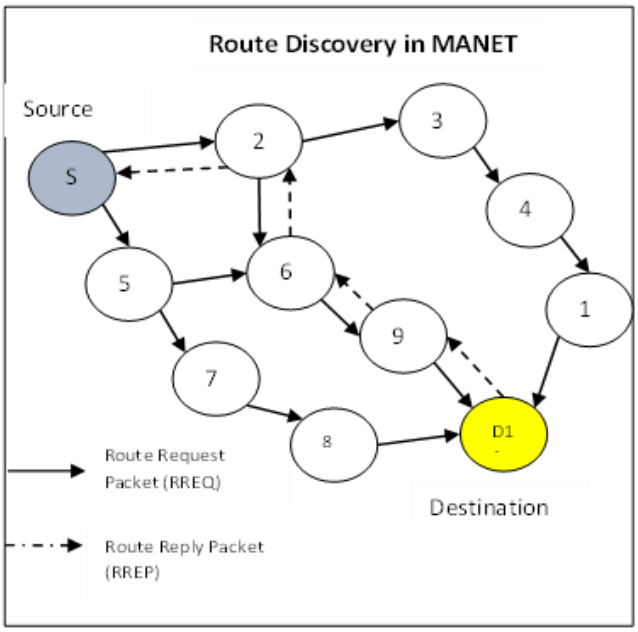

Figure 3.1 Route Establishment in MANET

The path is chosen and utilized in this manner for the transfer of data. As a result of the nature of route discovery, a great number of intermediary nodes produce fake RREP in order to carry out a variety of attacks [68].

3.1.2 Sequence Number Attacks

A type of denial-of-service (DoS) attack known as a sequence number attack is one that can be carried out in a variety of contexts. In this type of attack, the attacker, who

is in reality an authorized internal node, violates the availability issue by inventing or changing the packets in order to behave inappropriately. This is done in order to carry out the attack. The majority of the time, attacks of this kind are carried out via reactive routing protocols like AODV and Dynamic Source Routing (DSR). During an attack, the malicious node in the network that draws the packets by erroneously stating that it has the shortest and most up-to-date route to reach the destination would then drop the packets after having attacked them. These sequence number attacker nodes are capable of committing a variety of malicious actions on the network, including the following: the node occasionally fabricates the control packets; the node acts as a source node by fabricating or falsifying the Route Request packet; the node acts as a destination node by falsifying the Route Reply packet; the node can reduce and change the number of hops count at the time of Route Request packet broadcasting.

The functionality of the network is the primary target of these attacks, which are designed to disrupt it. The attacker node will make an attempt to join the network and become a part of the route when the attack first starts. In order for the attacker to accomplish this goal, they must first transmit a faked RREP and then announce that the node has the more recent route to transfer the data. This is accomplished by the malicious node by means of the transmission of an RREP packet that contains a fabricated destination sequence number and indicates a high level of route authenticity. The message that is generated may attract the attention of the source node, which may then cause it to select the erroneous path to get to the destination. As a direct consequence of this, the node that is responsible for the attack will start to discard packets after it has completed the path between the source and the destination [58].

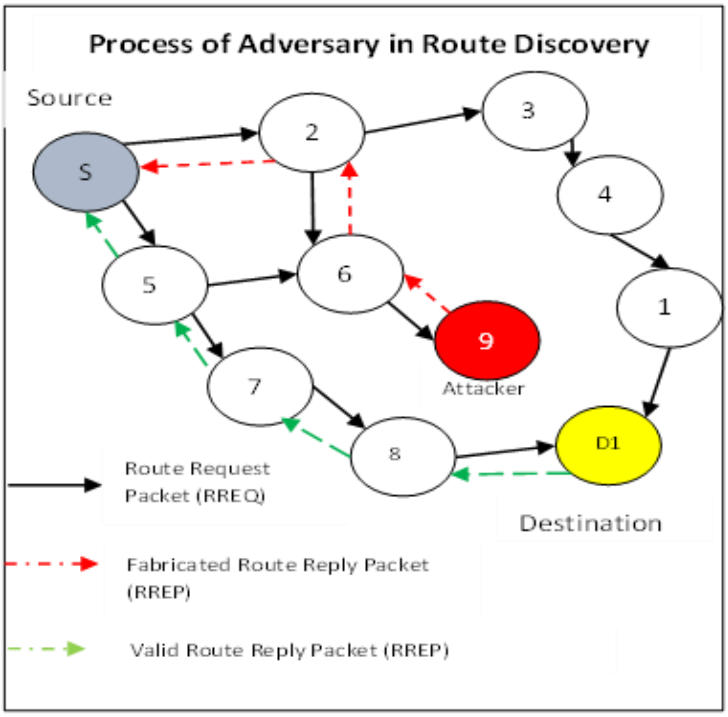

Figure 3.2 Process of Adversary in Route Discovery

3.2 MOTIVATION

The most recent developments in MANET have resulted in an enormous amount of opportunity and popularity, both of which have required numerous types of research to concentrate on the topic. This very flexible structure of the MANET also generates various challenges related to the performance of the network as well as issues related to the security of the network. The process in MANET may be at risk in a number of different ways due to a variety of security issues. Sequence number attacks, which include the grey hole attack and the black hole attack, are extremely dangerous attacks that greatly affect the functioning and performance of the network in a variety of contexts. The primary objective of this phase is to produce a fusion outline that is compatible with the AODV routing protocol in order to mitigate the effects of these attacks.

3.3 OBJECTIVE OF THIS CHAPTER

- 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 provide both proactive and reactive solutions by deploying effective authentication using the Modified Elliptic Curve Diffie-Hellman algorithm (MECDHA) methods.

3.4 METHODOLOGY

A high-security routing strategy that enables the detection and prevention of malicious nodes that are undertaking sequential attacks has been presented as a means of providing MANET with high-security network communications. The research that is being proposed can identify the attacker from routing, which is the source of many different types of attacks and has a high probability of doing so. The proposed methodology recommends modifying the AODV routing protocol in order to protect against these kinds of assaults. SRD-AODV is the term given to a protocol that has been updated and renamed. This protocol includes secure route discovery for the purpose of secure route discovery by selecting trusted node detection, hybrid cryptographic methods to protect the data packets and routing table information, and lastly, incursion detection and prevention from sequential attacks in MANET as a final component.

The secure routing protocol that has been proposed discovers valid nodes and offers hybrid cryptography as a means of providing a cryptographic shield to data packets.

This protocol is also able to detect attacks that are carried out by hostile nodes and stops these unhealthy nodes from routing by isolating them from the network and establishing various limits on their access to it. The effective discovery of neighbour nodes, the protection of data packets and routing tables through the use of hybrid cryptography, and, as a last step, the exclusion of misbehaving nodes from the network are the essential components of the proposed secure routing protocols.

3.4.1 Existing Algorithms

AODV Protocol

AODV is a reactive strategy-based routing protocol that will set up a path at the start of communication between two communicating nodes and employ it until the path breaks; after that, AODV will commence the setup of a new path. AODV is founded on the idea that routing should be reactive rather than proactive. It does this by going through two stages: (a) discovering the route between the originating node and the receiving node, and (b) repairing the route between communicating nodes [21]. The Routing Protocol uses Error of Path (RERR) message to repair the path in the event that there is a break in the path between communication nodes. Request of Path (RREQ) and Reply of Path are used to determine the best feasible route between the node that is sending the data and the node that is receiving the data. It uses a distinct technique for the management of routing information and makes use of routing tables with one entry for each destination that is part of MANET.

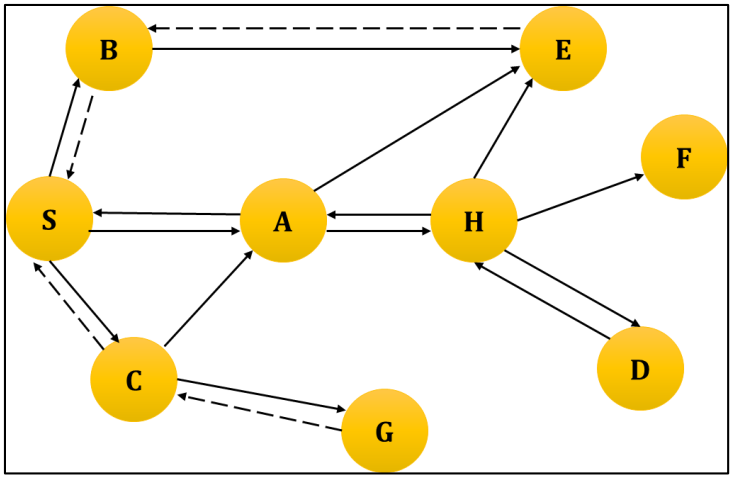

Figure 3.3 Path Discovery in AODV

AODV took advantage of the entries in the routing table to transmit the reply of route (RREP) back to the originating node. The originating node, in turn, sends data packets to the receiving node. AODV ensures that the path is always new by using sequence numbers that are generated by the destination in order to prevent routing loops. After a predetermined amount of time, determined by the value of the timer, an entry in the routing table related to the destination will become invalid. A collection of nodes, also known as neighbouring nodes, is kept for each item in the routing table. When the link between the current hop and the next hop becomes unavailable, these neighbouring nodes are notified of a route error, abbreviated as RERR. Each neighbouring node is responsible for removing all of the pathways that contain the broken connection [63]. The AODV path discovery method is depicted in Figure 3.3. This mechanism makes use of the RREQ and RREP messages. As can be seen in Figure 3.3, the source node S first transmits a request for route RREQ message in order to identify a path to the receiver D, and then it receives a RREP message in order to locate a path between the originating node and the receiver.

Extended Data Routing Information (EDRI)

The proposed solution addresses both the black hole and the grey hole attacks by maintaining an Extended Data Routing Information (EDRI) [12] table in each node in addition to the routing table that is used by the AODV protocol. This provides an additional layer of redundancy to the network. The DRI table is applied at each node in order to diagnose black holes. It basically stores the records for other nodes in the network that are considered to be going to or coming from it via different other nodes. However, in a situation in which nodes can take on a new grey personality, this cannot be considered satisfactory. Even though the DRI protocol uses trust as a parameter, once a node has been verified as dependable, it is not subject to further suspicion. This could be a gap in the system that allows grey nodes to visit secret locations.

The specific EDRI table is beneficial to the grey behaviour connected with nodes simultaneously. However, the concept also keeps a record of the previous harmful instances of the nodes that are recognized as black holes. This ensures that a larger comprehension of the node can be created, and the node is typically offered its impending opportunity as a result. Although the concept provides future opportunities for the nodes that are recognized as black holes, it also maintains a record of those past harmful instances. The counter keeps track of the number of times a new node has been captured, and the cost associated with this counter is typically proportionate to the amount of time that must pass before that node is provided with another opportunity. When a node is repeatedly caught engaging in malicious behavior, that node will eventually no longer have the opportunity to engage in such behavior. In addition to the already present RREQ and RREP, the following packets are also used: the refresh packet, the BHID packet, the further request packet, and the further response packet.

The refresh packet is typically sent out from the source along the troublesome path anytime the concept detects (with the assistance of NACK) that the dangerous node could be active on that path. Each node that receives its instruction to delete the problematic path coming from it and to update its DRI data does so after receiving its instruction. A table of routes. The identification of the potentially dangerous node, as assessed by the criteria, is included in the BHID packet. This particular packet is typically delivered in order to ensure that each of the nodes can quickly bring their records for the malicious node up to date. The particular further request and further response packets function similarly to the ways that are used for solving problems involving black holes, but they also include some additional information to back up the grey behavior.

3.4.2 Proposed Algorithm

In order to protect against sequential attacks in MANET, a brand-new hybrid framework has been developed. A newly developed and improved protocol known as the SRD-AODV protocol, which guards against sequential assaults by establishing a secure route beginning with secure node discovery. This protocol was given the acronym SRD-AODV [24]. The network is capable of configuring itself, and it provides security for nodes during the process of discovering routes and neighbours. A Secure Neighbor and route Discovery approach that uses the "Modified Elliptic-curve Diffie-Hellman (MECDH) algorithm" for secure key generation and sharing is proposed for use in MANET in a hybrid setting. This method can detect and prevent malicious nodes from communicating with one another. The protocol is well suited for use in networks with high levels of mobility. The authentication, route, and neighbour discovery processes that have been proposed have been implemented in AODV and compared with AODV and other

protocols that are already in use. Secure Neighbour and Route Discovery (SNRD), cryptography, and the Incursion Detection Process (IDP) are the three components that will allow you to accomplish maximal authentication against sequential attacks. Figure 3.4 outlines the primary security components that are utilized in the process of enhancing the operational efficacy of a secure routing protocol.

Several different methods and components are presented in order to ensure the security of data transfer within MANET against sequential attacks. At the time of the node's initialization, the node's authentication was accomplished using a set of private and public keys. Following the completion of the node initialization process, the secure neighbour will be determined when the route request is made. Only the neighbour who has successfully completed the network's authentication process will have their RREQ request satisfied. Following is a full explanation of the procedure for each individual component.

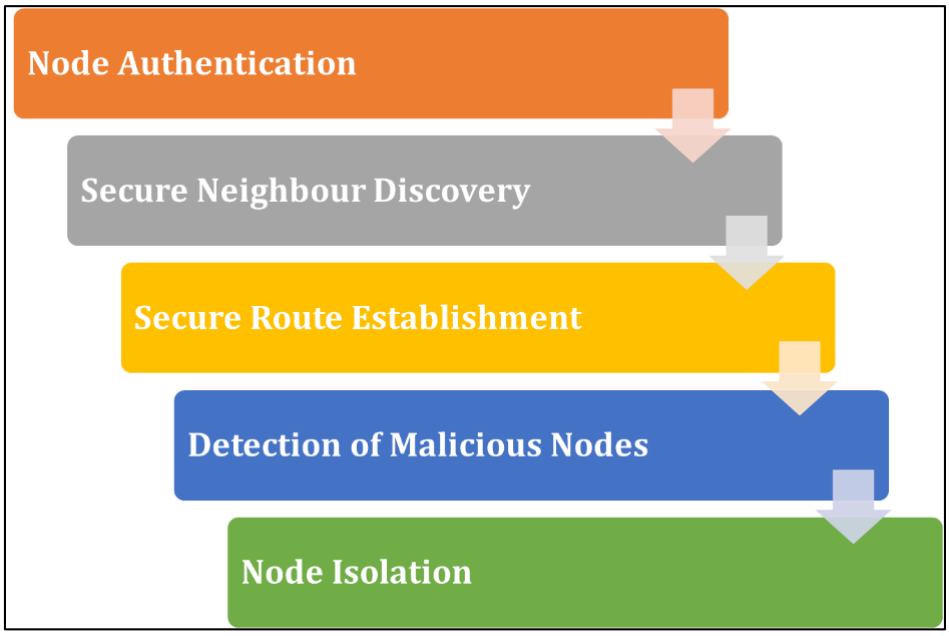

Figure 3.4 Security components of the proposed work

- **Node Authentication**

The process of authenticating mobile nodes, after which each node will be verified individually for secure transmission. This verifies the nodes using information about their identities. It is essential to find a reliable way for authenticating nodes in a MANET due to the restricted network resources available in this type of network. Authentication of nodes is carried out in a demand scenario by the SRD-AODV that has been proposed. The MECDH algorithm is utilized in order to generate and exchange keys in a secure manner. The MECDHA algorithm offers a more secure method for exchanging keys and generating keys over MANET than any other technique. MECDHA requires significantly less computational power than RSA does, making it an ideal choice for use in highly dynamic mobile apps. Private and public key pairs serve as the foundation for MECDHA.

Secure Neighbour Discovery and the Establishment of Routes during the secure node discovery procedure, the best neighbour node is chosen. This node has the lowest probability of being a malicious node in the network. The route is then established. Therefore, at the beginning, five steps are carried out in order to identify a secure neighbour.

1. Using MECDH, which is an unidentified key agreement protocol which permits two nodes, each having an elliptic-curve public-private key pair. By means of this node is recognized and a mutual secret over an insecure channel. Here for each node in the transaction region a pair of a public key and private key generated. The key generation process is done with the following equation 1.

$$k_i = \sum_{i=0}^{n} \binom{n}{k} keygen(Pri^k + Pub^k) \quad \text{(Eq 3.1)}$$

Here, ki is the key generation process for each node. I, n is the total number of active nodes in the region; Pri^k is the private key; Pub^k is the public key. From the private and public key pairs, the anonymous key is generated.

2. After generating an anonymous key pair for each node, then a packet request is broadcast by the source node, which is called a handshaking process. The initial Hello packet is sent to its neighbour along with its public key. Here, the ECDH also provides an anonymous key exchange in the handshaking process.

$$S = \sum_{i=0}^{n} \binom{n}{k} Broadcast(k_i + Pub^k) \quad \text{(Eq 3.2)}$$

Here, S is the source node, which broadcasts the request packet to all neighbors with the anonymous key k_i and its public key Pub^k.

3. After receiving the request packet from S, it verifies the key and adds that node as a neighbour with its public key along with its time value. Equation 3 shows the verification process done at receiver side R. Here, T is the time value.

$$R = \ Verify(k_i, Pub^k, T) \quad \text{(Eq 3.3)}$$

4. In the selected region, every mobile node sends a reply to the handshaking message along with the ID. From this, a trust node list is generated.

$$Receiver \rightarrow Reply\ (k_i, Pub^k, T) \rightarrow S \quad \text{(Eq 3.4)}$$

5. If the received packet contains a timestamp value, then it will send RREQ to that. The responses are valid for a particular time window. After that, the source node self-authenticates with each of its first-hop neighbours by fetching the reply that it received from them and adding them to the expected trusted neighbour list.

$$ND = validate\big(Reply(n_i)\big) \rightarrow add\ to\ (TNL) \quad \text{(Eq 3.5)}$$

Here ND is the neighbour node discovery process, which validates and adds to the replies received from every node. The secure anonymous key is hidden in the reply packet. If the validation is successful, then the node is anonymous.

After completion of the secure neighbor discovery phase, the route is discovered by adding the link between nodes. For example, from the network, the path will be this process is proactive; if the valid node acts as a vulnerable part, then our reactive incursion detection system helps to find and eliminate the node in the network for a particular period of time. Figure 2 indicates the overall flow of the proposed hybrid framework for secure neighbour and route discovery against sequential attacks.

- **Node Isolation System**

The design of the intrusion detection system in the suggested work can detect malicious activity, particularly sequential attacks, and isolate the misbehaving node for a specified period. There are different ways that have been utilized in the research to detect and destroy a malicious node. However, the proposed strategy provides a distinct score-based isolation process to facilitate network transactions.

Here, the frequent, infrequent, and uncommon maliciously behaving nodes are all identified using the anonymous key. The remaining nodes can easily learn more about their surrounding nodes. Malicious or legitimate nodes can be identified after malicious nodes and their activities have been detected. The protocol can choose the best route from the RREP and the value over it by adding this outcome category to the data packet at the time

of the RREP. Although with a MANET, proactive procedures ought to be possible, they are not always achievable. The secure routing system needs to include a proactive approach.

Hence, the system that has been proposed operates in both a proactive and reactive manner. The pre-path security requirement of the SRD-AODV protocol is satisfied in this manner. The SRD-AODV routing protocol gives users peace of mind that a malicious node will not be able to join the network and cause problems for other nodes or routes.

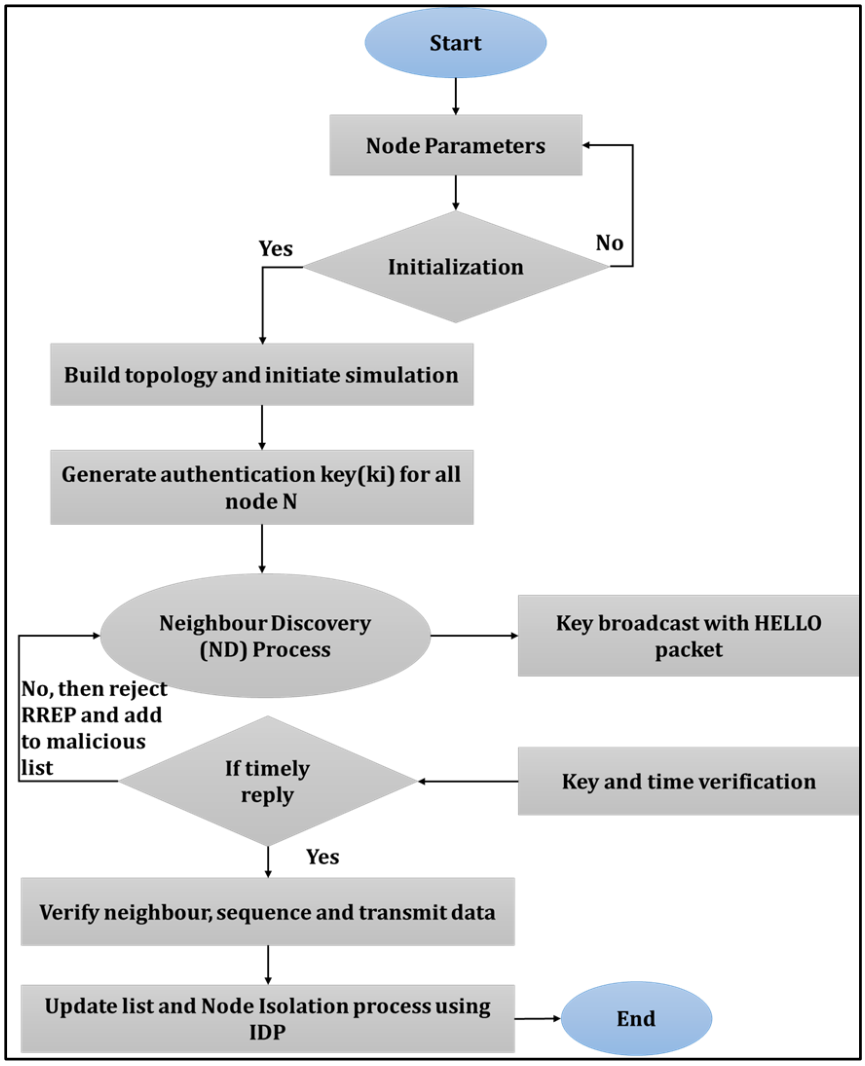

Figure 3.5. Secure Route and Neighbor Discovery Using Hybrid Framework

3.5 RESULTS AND DISCUSSION

In the simulation and experiments, the NS-2 simulator is used. Ns-2 is a widely used network simulator, and results are obtained from that for comparison. To prove that the SRD-AODV protocol gives improved performance when compared to the AODV and other EDRI-based approaches, we compare the performance of those approaches with different QoS (Quality of Service) metrics. For the experimental process, different stimulation parameters were used for a total of 300 seconds of simulation. The simulation area topography is generated at 1000 m×1000 m. The performance of the SRD-AODV protocol is done with the simple AODV protocol and improved AODV with EDRI. The different parameter-based performance comparisons of various techniques are explained. This includes packet delivery ratio, throughput, delay, and energy consumption. The detailed simulation parameters are shown in **Table 3.1**.

Table 3.1 Simulation Parameters

Parameters	Values
Simulator	NS 2.35
Routing protocols	AODV, EDRI-AODV, SRD-AODV
Coverage area	1000m x 1000 m
Mobility model	Random Way Point
Simulation	Time 300s
Number of Nodes	1500
Maximum mobility (varying)	5m to 25 m/s
Pause time (varying)	5-30s
Type of traffic	Constant bit rate
No. of Connections (varying)	2 to 12
Transmission Rate (varying)	5 to 25 Packets per second

The number of mobile users in the simulation is 1500. The metrics of end-to-end delay, packet delivery ratio, average packet drop and throughput are measured. The following figures show the results of pure AODV with limited features, EDRI-AODV, and proposed SRD-AODV techniques when the mobile users are 1500.

3.5.1 End-to-End Delay

Delay is calculated by taking the difference between the time when the first packet was transmitted by the source and the time when the first packet successfully reached the destination.

$$Delay = Received\ Packet\ Time - Send\ Packet\ Time \quad \text{(Eq 3.6)}$$

To calculate end-to-end delay, we take the time of packet generation and the time when a packet is received at its destination, and then we take the difference. Figure 3 shows the performance comparison of existing AODV, EDRI-AODV and proposed SRD-AODV protocols in terms of total end-to-end delay value. Here, the delay value is calculated for each protocol and compared with the proposed system.

Table 3.2 End to End Delay for Varying Mobile Users

No. of Nodes	AODV	EDRI-AODV	SRD-AODV
100	3	3.5	2.4
300	4.5	3.9	3.2
600	6	4	3.8
900	8	6	4.3
1200	10	8	4.9
1500	12	10	5.5

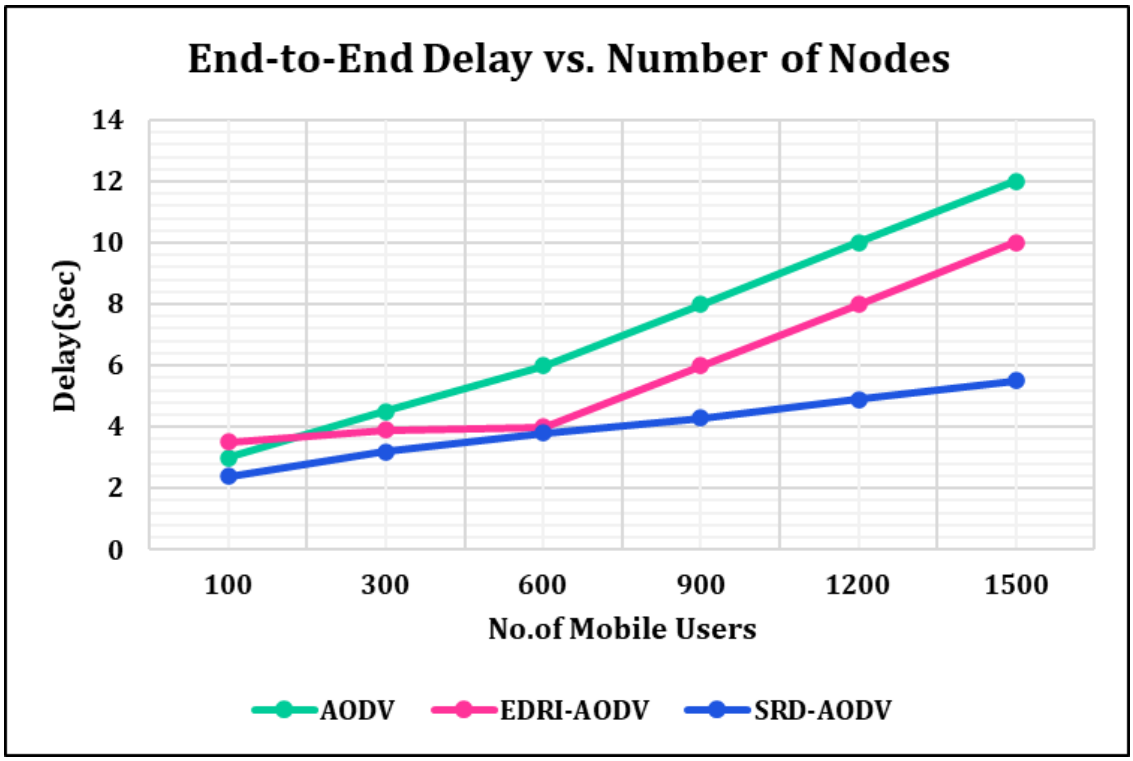

Figure 3.6 Comparison of End-to-End Delay

Figure 3.6 shows the end-to-end delay for all the techniques compared with the proposed system. It represents the total time taken to transmit the data from the source to the destination after successful attack verification using the modified protocol. When the number of mobile nodes is above 100, overhead occurs, leading to an increase in delay. The use of MECDH and region-based verification in SRD-AODV reduces the delay by 85% when compared to the AODV protocol.

3.5.2 Packet Delivery Ratio

It is calculated by dividing the total number of successfully captured packets by the number of packets sent by CBR sources.

$$Packet\ Delivery\ Ratio = Total\ Packets\ Received / Total\ Packets\ Sent \quad \text{(Eq 3.7)}$$

Table 3.3 Packet Delivery Ratio

No. of Nodes	AODV	EDRI-AODV	SRD-AODV
100	89	93	95.2
300	88	92	94.1
600	87	90.5	92
900	85	87	90.3
1200	84.5	86	87.9
1500	84	84.5	85.2

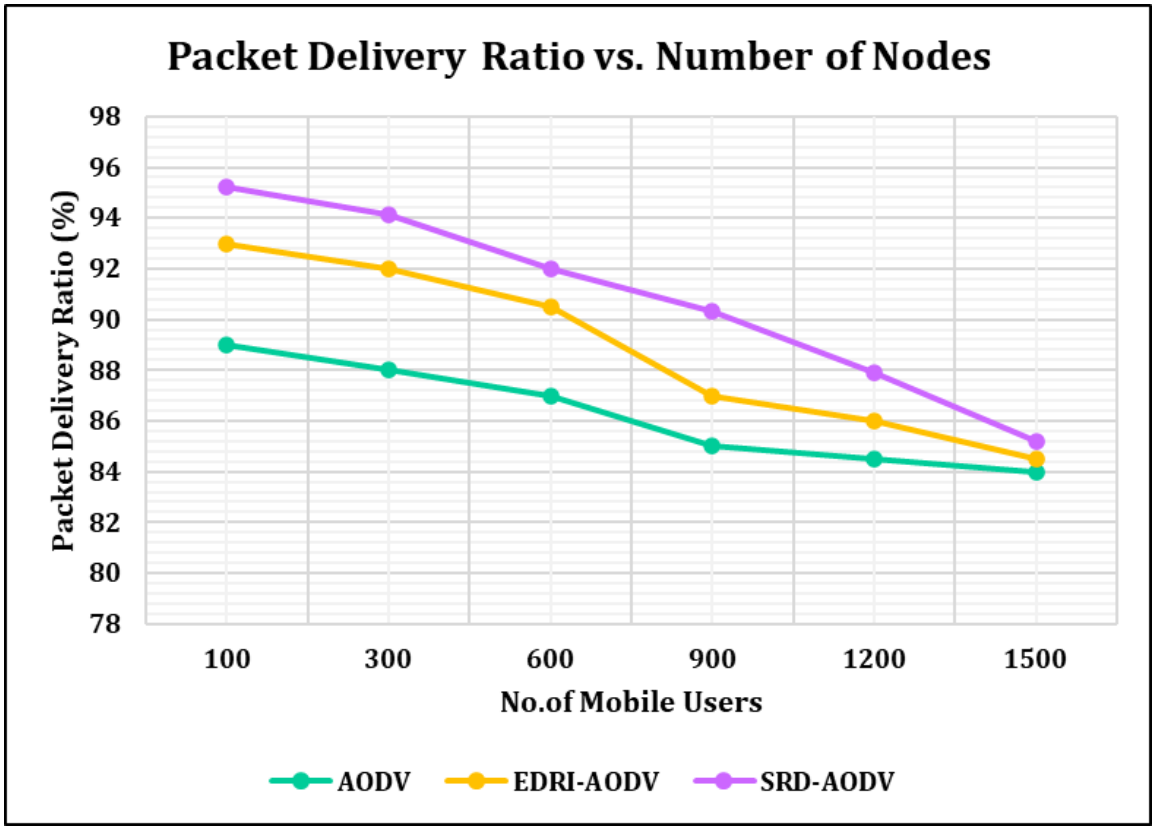

Figure 3.7 Comparison of a Packet Delivery Ratio

Packet Delivery Ratio (PDR) will decrease as a result of an increase in the number of mobile users due to the fact that the source discovered an increased number of alternative routes, as shown in Figure 3.7. However, SRD AODV has a PDR that is 85.2% higher than AODV and EDRI AODV. This is because SRD-AODV avoids assaults in the network and ensures that routes work correctly, thereby preventing packet drops and failures in the connection.

3.6 SUMMARY

Wireless technologies have grown in popularity because of their simplicity of deployment, high mobility, and dynamic infrastructure. Numerous security issues are occurring on this network under various circumstances. This problem makes security for data packet routing a very challenging problem that calls for a range of solutions. The proposed approach established a hybrid framework with secure neighbour discovery, node authentication using MECDHA and intrusion detection and isolation mechanisms in order to provide high security over MANET routing and security against sequential attacks. The AODV protocol is integrated with the hybrid framework and named SRD-AODV. Security is offered at two levels in the SRD-AODV routing protocol, including security for routes and security for data. First-stage evaluations of route and neighbour security include secure neighbour discovery, which can distinguish between real and fraudulent nodes. Non-legitimate nodes are prevented in this case by the SRD-AODV protocol before the routing procedure even starts. In AODV, rogue nodes can be recognized and such links avoided by employing the best authentication system and a secure neighbour discovery method. The proposed work enhances packet delivery and obtains good attack detection ratings.