Chapter 4

CHAPTER 4

ATTACK DISCOVERY BASED ON ENERGY AND TRUST

4.1 INTRODUCTION

The majority of the time, MANETs are dynamic, self-organizing platforms without a centralized controller or connecting resources. The other nodes are chosen to operate as intermediary nodes for information transfer between those nodes if the mobile node is outside of the other's service region. Additionally, each node moves independently and uses fluctuating networks for coordination. Rapid changes in network structure might thereby affect routing protocol robustness and tolerance to efficiency loss, among other issues. Proactive and reactive routing protocols [27] are the two basic categories into which routing protocols are split. Regardless of whether the routes are being used or not, proactive protocols allow nodes to send packets on a regular basis and to constantly choose the best paths between any network nodes.

This has to do with the capability that diffuses a lot of resources, including power and throughput, which isn't the best thing for MANET. Reactive protocols, such as AODV routing protocols, on the other hand, do not need to transmit data continuously and only discover the route when two nodes are communicating. Contrarily, working with the system's suspected nodes has an impact on the routing protocols. MANETs with insufficient dynamic structures are particularly vulnerable to various routing attacks, such as black-hole and other types of holes. Black-hole attacks are believed to be nodes that have appeared in the system and that surreptitiously reject data that has been accepted or sent without informing the origin node. The frequent rejection of data during transmission,

or the nodes dropping the data rather than forwarding it to the next node, makes it difficult to identify and mitigate this assault.

The suspicious node will hang around and wait for other nodes in the neighborhood to initiate the route request (RREQ) packet. Even if the suspicious node does receive the RREQ packet, it immediately sends the faked route reply (RREP) packet, which contains the highest possible sequence numbers. Therefore, the origin node develops a new route to transfer the data towards the target node via the suspected node and rejects the RREP packets from any other nodes that are present in the network. In addition to this, the suspicious node prevents packets from being transferred to the target node. The block-hole node often participates in the AODV protocol by designating itself as a genuine route for the target. This allows the block-hole node to begin accepting packets from other genuine nodes while simultaneously rejecting packets that contain valuable data [28].

In a similar way, the gray-hole node also transmits the data in the same manner as the usual nodes. However, it is possible that it will reject certain packets without changing their confidence score. The behaviors that were suspected were realized based on the fact that the packets from other nodes were either rejected or broadcasted at predetermined intervals. Both the black-hole and gray-hole assaults are also referred to as sequence number attacks. A great number of strategies, both developed and proposed, have been developed and proposed in order to identify and mitigate various types of assaults in MANETs. Despite the fact that these strategies reduce the impact of malicious actions, the efficiency of routing security remains unchanged.

The extension of the AODV protocol to retain the pathways using sequence numbers was suggested as a predictive technique to address the security issues in MANET.

To calculate the route freshness, they used the TSN. The suspected node altered the RREP packet to have a lower hop count and a higher sequence number in order to construct the fake path. After that, the suspected node arbitrarily discontinued packet forwarding for a certain target or set period. As a result, the linear regression that takes into account past knowledge was used to estimate the TSN of the acceptable RREP. The actual TSN accepted by the RREP was then compared to the estimated projected TSN. The node transmitting that RREP was identified as a suspicious node if the RREP TSN was higher than the predicted value. The suspected node was also eliminated from the routing path. Otherwise, standard protocol actions were carried out, and a data structure was created to contain the interval of RREP acceptance together with the TSN value [29]. The regular RREP was then forwarded to the origin node via the alternate route. However, it must incorporate the newest secure routing methods to increase efficiency.

As a consequence of this, a successful authentication method based on the Modified Elliptic Curve Diffie-Hellman Algorithm (MECDHA) was utilized in the development of an SRD-AODV protocol. This protocol's goal is to ensure that the maximum amount of network security is achieved by securing the packets as well as the routing table. In SRD-AODV, only legitimate nodes are allowed to participate, and access control is accomplished through the sharing of authentication keys prior to the beginning of the routing process. On the other hand, it only verifies the nodes during the path discovery step; however, during the data transmission stage, there is no verification of the nodes. Because gray-hole broadcasts the accurate TSN during the path discovery phase but then becomes suspicious and drops packets during the data transfer phase, the authentication of nodes during data transmission is crucial. Because of this circumstance, the performance of the network as a whole is negatively impacted.

4.2 MOTIVATION

The majority of the currently used protocols were designed to identify black-hole or gray-hole attacks during the stage of route discovery. There are just a small number of unified protocols that can detect both kinds of attacks. In addition, attacks that occur while data is being transmitted might reduce the efficiency of the transmission by causing the discarding of data packets, which in turn lowers the throughput of the network. Therefore, it is vital to recognize the attacks while the data is in the process of transmission. When seen from this angle, the primary focus of this research is on the detection and prevention of black-hole and gray-hole attacks during the stage of data transmission. Additionally, it reduces the EED while simultaneously raising both the PDR and the throughput for more efficient data transfer.

4.3 OBJECTIVE OF THIS CHAPTER

- The main objective of this phase is to enhance security while reducing routing overhead by improving the energy efficiency and optimizing data delivery.
- To ensure route maintenance security by implementing the robust attack detection mechanism which identify and defend the black and gray-hole attacks during the data transfer stage.

4.4 METHODOLOGY

During this phase, an SRMAD-AODV protocol will be built in order to identify and defend against black-hole and gray-hole attacks that occur while data is being sent. The following is a list of the key contributions that this study has made:

- First, an ADS node is chosen by the CDS method, which determines each node's energy and confidence score. The chosen ADS nodes with the greatest energy and confidence score forward a status packet within the size of the dominating set to retrieve the entire behavioral data.
- Then, ADS nodes examine the gathered behavioral data to recognize nodes as black or gray-hole attackers and add them to the blacklist.
- Once the blacklist is created, ADS sends this blacklist to the origin node, which transmits a data packet to the target node and waits for an acknowledgement (ACK) to confirm that the data has been delivered without being dropped by any malicious nodes in the route.
- By receiving the ACK, the origin node verifies whether the received ACK packet is legitimately forwarded by the target or a counterfeit ACK packet received from the black/gray-hole node.
- If the black or gray-hole nodes are identified in the routing path, then the origin node updates the routing table and alerts each node in the path to eliminate misbehaving nodes.

Thus, both black-hole and gray-hole attackers are effectively identified and prevented during the data transmission phase.

4.4.1 Existing Algorithms

- **Indirect Trust and Indirect Mutual (ITIM)**

In MANETs, the detection of black-hole is considered to be one of the most important goals of this work [88]. The detection process is carried out depending on the

condition of sensor nodes organized into clusters. Because of the presence of blackhole nodes in the network, the rate at which packets are lost in the network is likely to increase, which in turn has a negative impact on the quality of MANETs as a whole due to the decreased throughput. The malicious sensor nodes cause an even greater increase in the occupancy of the available bandwidth and the excessive use of available resources between the sensor nodes. The blackhole attack is caused by the dropping of data packets, the dropping of route request packets, and a change in the route request. The relationship of direct, indirect, or mutual trust that exists between any two sensor nodes, regardless of how that trust was established. Other trust metrics, such as social trust, service trust, and quality of service trust, have been recommended for the present research.

- **4.4.1.2 Accurate and Cognitive Intrusion Detection System (ACIDS)**

The malicious node acts as an intermediate node during the MANET route discovery process, luring the data packet to be routed through the path where it is present by faking the RREP packet and giving it a high sequence number. The ACIDS [87] method assesses the difference between the DSN in the nodes' routing tables and flags it as suspicious in cases where the resultant value is out of the ordinary. The newly established RREP ID field of the routing table stores the relevant RREP IP address of the suspicious nodes. When an IP address is listed more than once, the RREP IDs are compared to all other IP addresses in the relevant field, and the value of an ID is increased. The node is fixed as malicious when the incremented value exceeds the fixed threshold limit, and any further RREP from that node will be deleted throughout the route discovery process. By removing the RREP of the malicious nodes and protecting the route discovery process, this will improve the AODV overall and increase the packet delivery ratio.

- **Indirect Trust Mechanism for AODV (ITAODV)**

Direct trust is the term used to describe the type of trust that can be calculated by a node using only its own observations [85]. If the node has a significant number of observations about all of the other nodes that are taking part in the network, then the direct trust will be of more benefit. On the other hand, this is difficult to accomplish in a large network since there are many nodes that are not in direct communication with each other. Because of this, it is preferable to obtain recommendations for the target node from other nodes. In order to determine the cumulative trust value, these recommendations are typically blended with the author's own observations. The term "indirect trust" refers to this type of trust value. In the work that has been proposed, indirect trust in a node is expressed in terms of the level of reliability and trustworthiness that is provided by the node in the process of packet routing. Every node keeps an eye on its neighbor for a set of events that have to do with the dependability of the packet forwarding abilities of the nodes.

- **Detection and Presentation of a Black Hole Attack (DPBHA)**

The DPBHA [89] takes advantage of the two primary characteristics that make a BHA harmful. First, the RREP of the node that is attempting to attack contains a higher sequence number and a lower minimum hop count value. This is because the attacker node is pretending to have a new route to the destination. Second, the attacker node will always answer first to any RREQ without going to its routing table to check it out. In order to detect and avoid BHAs in VANETs, the default operations of the AODV routing protocol have had fair adjustments made to them in order to take advantage of the two qualities mentioned above. During the connectivity phase, the network that is being considered is launched, the topology is set up, and it appears that communication between the cars

(nodes) has begun. In the second step, the potentially malicious node that has a tendency to be a black hole (with a probability of fifty percent) is discovered. In the third step, it was completely established that the node that had been suspected of being hostile was in fact a black hole node, and it was recommended that this node be removed from the network.

4.4.1 Proposed Algorithm

- **Secure Route Maintenance and Attack Detection AODV (SRMAD-AODV)**

This section provides a concise overview of the SRMAD-AODV routing protocol that is used in MANET. In a typical configuration, the MANET nodes consume a suitable amount of energy in order to establish a conduit for the transmission of data. A huge quantity of unnecessary traffic is generated as a result of the suspicious nodes' consistent transmission of beacon messages, which results in an increase in the routing overhead. Therefore, measures need to be taken to mitigate such nodes in order to reduce the additional routing overhead. In order to achieve this goal, the proposed protocol can merge CDS and ADS approaches in order to decrease the routing cost and identify the suspected nodes (also known as black-hole nodes and gray-hole nodes). The modeling diagram for the suggested architecture can be found in Figure 4.1.

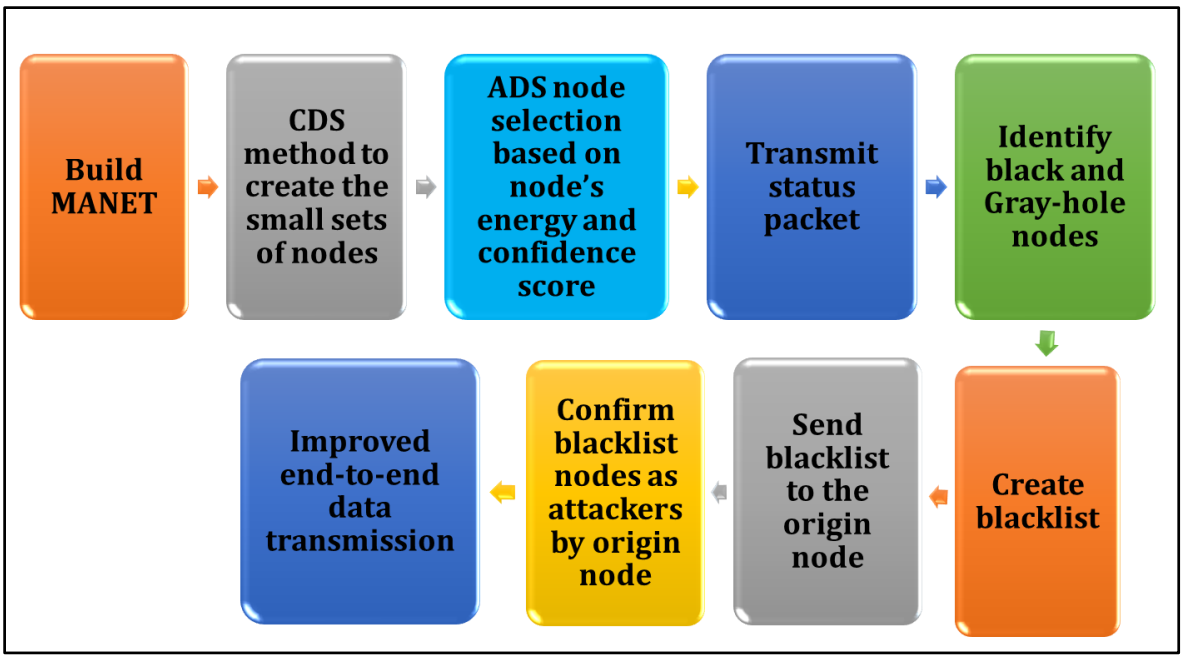

Figure 4.1 Proposed SRMAD-AODV Architecture Modelling Diagram

The major contributions to this SRMAD-AODV routing protocol are the following:

- The Connected Dominating Set (CDS) method is applied to create small sets of dominating nodes and choose the nodes with adequate energy and confidence scores as the Attack Discovery System (ADS) set.
- The status packets are transmitted from the ADS-set nodes to each other node in the network to identify the suspected nodes and create the blacklist.
- The blacklist is sent to the origin node for confirmation of the suspected nodes and mitigating them from the routing path during data transmission.

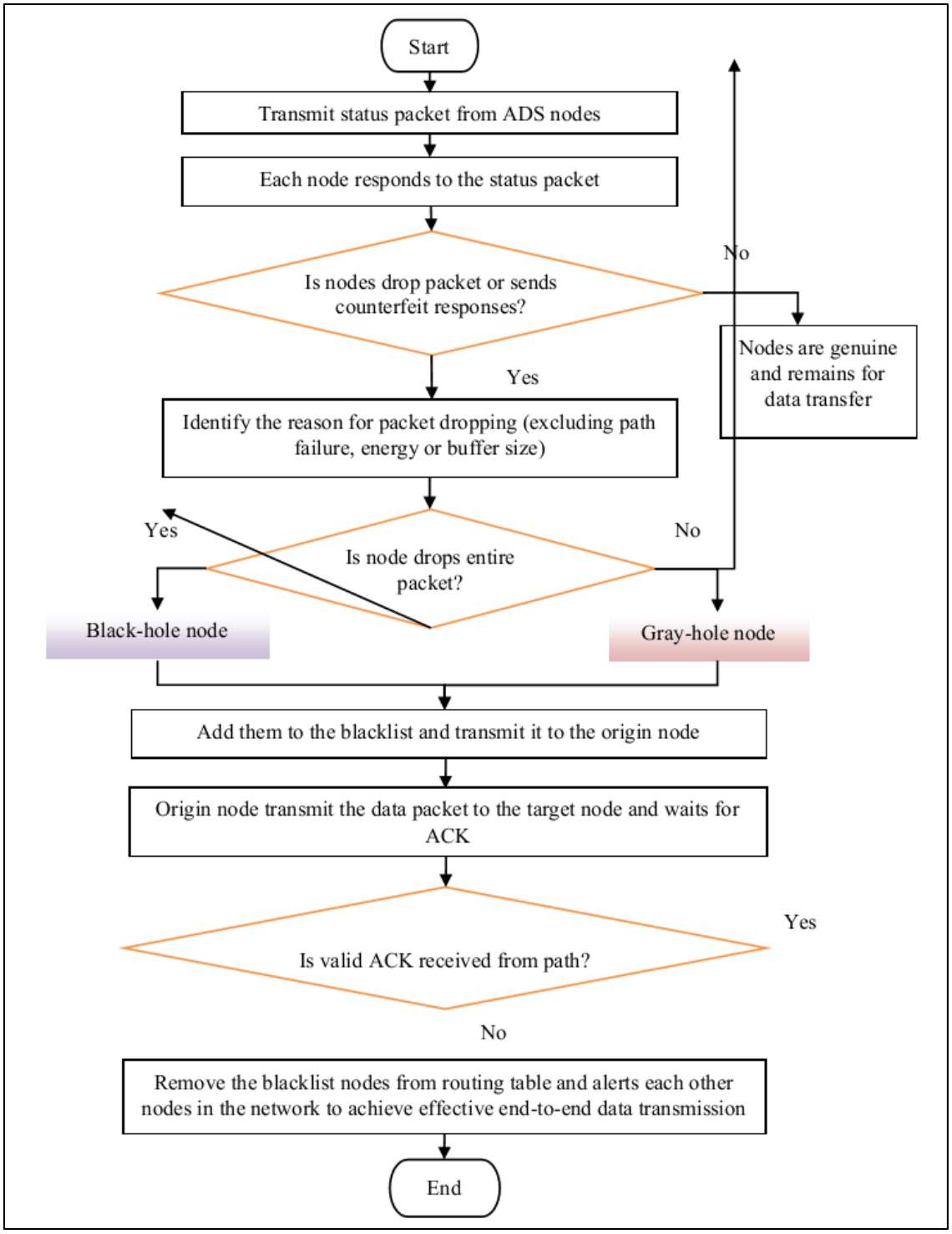

Figure 4.2 Flow diagram of SRMAD-AODV routing protocol

- **CDS and ADS Node Selection**

The network's dominant collection of subgroup nodes is called CDS. Although there are not necessarily any links between each node in that subgroup of the network, at least one node must belong to it. The CDS, or dominant set, needs to be linked. The CDS is made up of the fewest coupled nodes necessary to completely encapsulate the network's maximum range. The ADS set is a theory of the network's subgroup in a manner similar to that. It is used to put nodes together according to their level of energy and confidence across the entire network. Additionally, the ADS set is used to reduce routing overhead and traffic load.

The ADS node for query processing is chosen to be a secure node with sufficient energy. The ADS set's nodes are all connected to one another by links. They are interconnected in order to ensure full network coverage. By selecting the ADS query issuing node from the ADS set, the CDS technique is improved. This technique checks the node's energy and confidence score before selecting it. Each node in the ADS set must recognize its neighboring node in promiscuous mode for it to become confidential. Each node in the ADS set maintains records of the neighboring node's activities in relation to the lost packet, and this data is accumulated in each node's knowledge table.

- **Adversary Model**

Consider that there are black-hole and gray-hole nodes in the MANET. The suspicious nodes attempt to disrupt network transmission without revealing their identities. In black-hole attacks, the suspect node transmits fake data to the source node by tricking it into believing it has a new and authentic path to the target. During gray-hole assaults, the suspect node discards particular packets during the data forwarding phase.

Due to their dissimilar behaviors, identifying these suspect locations is a challenging endeavor. Therefore, an adversary model is incorporated into this SRMAD-AODV protocol to account for the varying effects of the adversary's diverse activities on this protocol.

- **Identify Suspected Attackers by ADS Nodes**

The primary objective of the ADS query node is to develop a robust security strategy against black and gray-hole nodes in MANETs. To accomplish this, every ADS query node must contain an acceptable amount of energy and a confidence score. The energy value of a node N to be selected as an ADS query node is given in the table below.

$$\left(1 - \frac{E_C\,(N)}{E_B\,(N)}\right) \times 100 > \Gamma \; or \; \frac{E_C\,(N)}{E_T\,(N)} \times 100 < \theta \qquad \text{(Eq 4.1)}$$

In Eq. (1), N is a node, $E_C\,(N)$ is the node's current energy, $E_B\,(N)$ is the node's initial energy, $E_T\,(N)$ is the node's overall energy while it is completely charged, Γ is the highest % of $E_B\,(N)$ for the ADS query node and θ is the least % of $E_T\,(N)$ should be conserved. The values of Γ and θ are depending on the mean energy of the nodes. In the same way, the node's confidence score is determined using both direct and indirect confidence scores. Considering the data transfer between node i to node j, the Direct Confidence (DC) score is computed as:

$$DC = \frac{\sum Totalpkt_i - (\sum Succpkt_j - \sum Droppkt_j)}{\sum Totalpkt_i} \qquad \text{(Eq 4.2)}$$

In Eq. (2), $\sum Totalpkt_i$ is the overall quantity of packets sent by i, $\sum Succpkt_j$ is the overall quantity of effective packets sent by j and $\sum Droppkt_j$ is the overall quantity of dropped packets by j. Also, the Indirect Confidence Score (IDC) is computed as:

$$IDC = \frac{\sum Trust\ value\ from\ adjecent\ about_j}{Total\ amount\ of\ Nodes} \quad \text{(Eq 4.3)}$$

So, the overall confidence score value of j is estimated as:

$$Confidence\ Score = \frac{DC+\omega.IDC}{2} \quad \text{(Eq 4.4)}$$

$$\omega = \begin{cases} 1, \\ \frac{N_{Trust}}{N_{Untrust}} \end{cases}$$

$$N_{untrust} = 0\ or\ else$$

In Eq. (4.4), N_{Trust} is the number of dishonest nodes and $N_{Untrust}$ is the number of honest nodes.

- **Status Packet**

When the ADS set has been acquired, the nodes in question will begin periodically transmitting status packets in order to investigate the throughput, latency, routing overhead, and PDR of each and every node in the network. The following queries coming from authentic nodes are included in the status packet:

- The ADS node requests the genuine node: What is the sequence number?
- The ADS node requests the genuine node: How many packets have been accepted?
- The ADS node requests: How many packets have been transferred?
- The ADS node requests: How many packets have been dropped and why?

Each query contained in the status packet is answered by all of the nodes after they have received it. After that, these responses from each node are sent to the ADS query node

for processing. In this way, the ADS query node verifies the node's packet transfer actions on a regular basis in order to distinguish between authentic and suspicious nodes.

There are potentially two criteria that might be applied to nodes that are under suspicion: (i) the node either sends fake data to the ADS node in an effort to conceal its individuality or (ii) the node does not provide any response to the ADS node and instead drops the status packet. Since it is believed that the node in question is a fabricator node, it is the one that sends the fake response to the ADS node and never reveals its true identity to it. The ADS node, once it has accepted responses from all of the nodes, investigates which nodes are not reacting adequately and determines why.

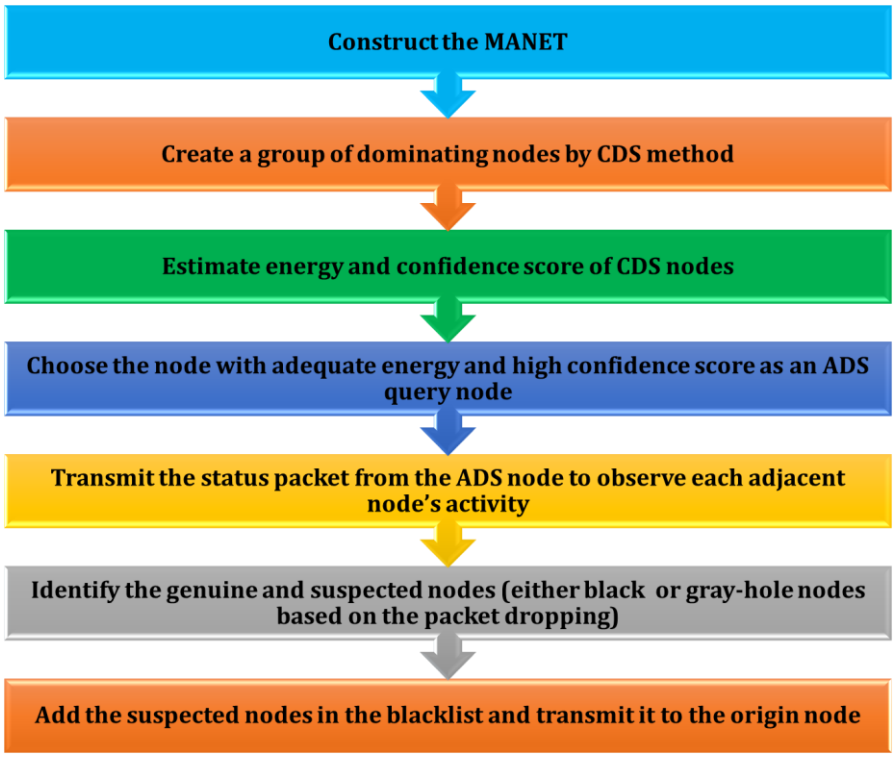

Figure 4.3 ADS node selection and suspected node identification processes

If any node is not answering the queries or broadcasting counterfeit responses and failing to satisfy the predefined questions without any justification for the path failure,

energy, or buffer size, then the ADS node will proclaim that node as a suspected node. This occurs when the ADS node fails to fulfill the predefined inquiries. In addition to this, the ADS node will add any questionable nodes to the blacklist before sending them to the origin node so that they can be used in authenticating the end-to-end data transmission. The entirety of the ADS node's functioning can be seen in Figure 4.2.

Confirm Suspected Attackers by Origin Node

The origin node sends a data packet to the target node after it has been given the blacklist. The origin node then waits for an ACK from the target node to verify that the data have been accepted and that there is not a suspicious node anywhere along the route. The origin node checks to see if the ACK it has received is a real one that was transmitted by the target or a counterfeit one that was transmitted by the node that is suspected. It does this by receiving the ACK. A nonce is added to the ACK in the event that it is determined that the ACK was fake or that it did not arrive at all. Because this sequence number is utilized in ACK's nonce determination, which is performed to assert that it is a valid ACK, the origin node transfers the initial packet with a random sequence number so that any adversary (blacklist nodes) cannot recognize it as the initial packet. This is done to prevent the adversary from identifying it as the initial packet.

While the target node accepts the initial packet, it determines nonce N_1 with the preferred Initial Random Prime (IRP) number and the initial packet's random sequence number X as:

$$N_1 = X + IRP \qquad \text{(Eq 4.5)}$$

Then, it transmits ACK_1 with N_1 to the origin node. If the initial packet's ACK is entered at the origin node, then the variance value PN is computed as:

$$PN = N_1 - X \quad \text{(Eq 4.6)}$$

When the PN is a prime number, the timer is turned off; or else, it is a counterfeit ACK, which is rejected instantly and declared as it is coming from the blacklist nodes. Succeeding nonce N_k is computed using the next prime number (NPN) and X as:

$$N_k = X + NPN \quad \text{(Eq 4.7)}$$

Algorithm: SRMAD-AODV Protocol

Input: N number of nodes

Output: Black and gray-hole nodes

Step 1: Build the MANET using N nodes;

Step 2: Apply the CDS method to create the sets of dominating nodes;

Step 3: Estimate the energy and confidence score of each node using Eqns. (1)-(5);

Step 4: Choose the dominating nodes having adequate energy and confidence score as ADS set;

Step 5: Transfer status packet from ADS nodes to other nodes within the network range;

Step 6: Check the node's responses to the status packet, i.e., whether the node sends counterfeit responses or drops the packet;

Step 7: ***if (node drops packet)***

Step 8: Find the reason for the packet dropping apart from path failure, energy, or buffer size;

Step 9: ***if(node drops entire packet)***

Step 10: Declare that node as a black-hole node;

Step 11: ***elseif(node drops part)***

Step 12: Declare that node as a gray-hole node;

Step 13: ***endif***

Step 14: Add the black & gray-hole nodes to the blacklist;

Step 15: Transmit blacklist to the origin node from the ADS set;

Step 16: Origin node transfers the data packet to the target node and waits for an ACK;

Step 17: Compute nonce N_1 for initial packet's acceptance using Eq. (6);

Step 18: Determine the variance prime number and succeeding nonce N_k via Eqns. (7) & (8);

Step 19: Identify genuine and counterfeit ACK to verify that the data has been transmitted via the path without the nodes in the blacklist;

Step 20: Discard the blacklist nodes from the routing table and notifies each other nodes regarding the updated routing table;

Step 21: ***else***

Step 22: Node is genuine and continues the data transmission;

Step 23: ***end if***

The authentication of succeeding nonce N_k at the origin node is carried out by verifying whether the variance of received N_k and X is similar to the NPN; otherwise, it is counterfeit ACK, which is also declared as it is coming from the blacklist nodes and rejected instantly. Thus, the origin node authenticates all blacklist nodes in the routing path during data transmission and notifies all other nodes in the network about the blacklist nodes to prevent the packet from dropping. Fig. 3 depicts an entire flow of SRMAD-AODV protocol.

4.5 RESULTS AND DISCUSSION

The SRMAD-AODV protocol is emulated with the help of the network simulator (NS2.34) in this section. Additionally, its effectiveness is evaluated in comparison to that of previously established protocols by simulating them in the context of the detection of black and gray-hole attacks. These protocols include SRD-AODV, ITIM, ACIDS, ITAODV, and DPBHA. This investigation is carried out in accordance with the End-to-End Delay, the PDR, and the throughput. The simulation parameters are presented in Table 4.1.

Table 4.1. Simulation Parameters

Parameters	Range
Simulation area	1000×1000 m^2
Number of nodes	1500
Number of suspected nodes	35
Channel type	Wireless channel
Antenna type	Omni-directional antenna
Radio propagation model	Two-ray ground

Parameters	Range
Interface queue type	Drop tail
MAC type	MAC 802.11
Routing protocol	AODV
Mobility model	Random waypoint
Mobility speed	50m/sec
Traffic type	Constant bit rate
Packet size	512 bytes/packet
Simulation time	300 sec

4.5.1 End-To-End Delay (EED)

It is the amount of time that passes between when the first packet is forwarded from its original location and when the first packet actually reaches its intended destination. The end-to-end delay (in seconds) of the SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols for an increasing number of nodes is depicted in Figure 4.4. It can be concluded that the SRMAD-AODV has the least end-to-end delay of all the other protocols. Because the SRMAD-AODV eliminates the possibility of data packets being lost by removing the nodes that are under suspicion from the network, it is not necessary to retransfer data packets to the node that will serve as the target. Because of this, the end-to-end delay of the network has decreased.

Table 4.2 End-to-End Delay

No. of Node	IITM	DPBHA	IAODV	ACIDS	SRD-AODV	SRMAD-AODV
100	3.8	3.6	3.2	3	2.4	2.1
300	4.9	4.7	3.9	3.7	3.2	2.7
600	5.2	5	4.5	4.3	3.8	3.4
900	5.6	5.4	5	4.7	4.3	3.9
1200	6.1	5.9	5.7	5.3	4.9	4.6
1500	6.8	6.4	5.9	5.7	5.5	5.2

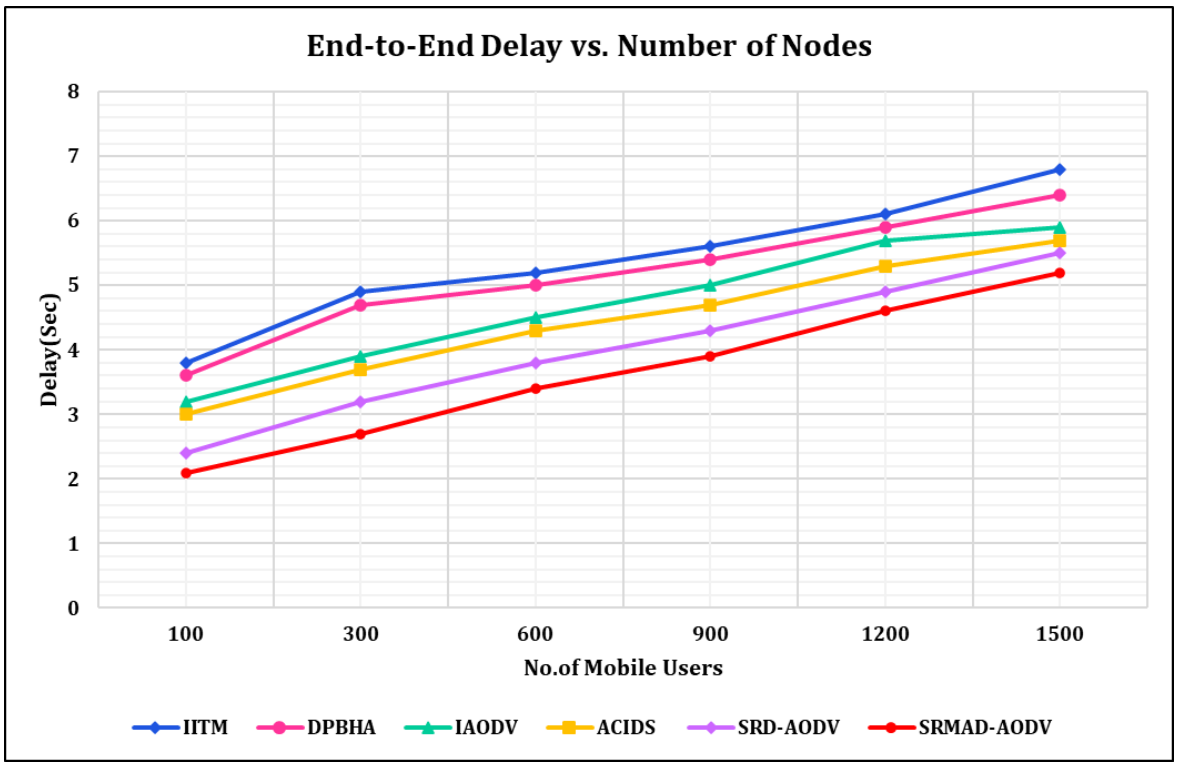

Figure 4.4 Comparison of End-to-End Delay

4.5.2 Packet Delivery Ratio (PDR)

It is the ratio of the total number of packets transmitted by the origin to the total number of packets successfully accepted by the target. Figure 4.5 depicts the percentage of packet delivery failures for the SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols when the number of nodes in the network is varied. It can be concluded that the SRMAD-AODV has the maximum PDR as compared to the other protocols. This is due to the fact that, following the identification of black- and gray-hole nodes with the use of status packet inquiries, the data packets may be easily and rapidly delivered to the target node by adding them to the blacklist in a short amount of time. This makes the delivery of the data much more efficient.

Table 4.3 Packet Delivery Ratio

No. of Node	IITM	DPBHA	IAODV	ACIDS	SRD-AODV	SRMAD-AODV
100	87	89	90	94.2	95.2	96.7
300	86	88	92	93	94.1	95
600	85.9	87.4	90	91.3	92	92.8
900	85.1	86.8	88.5	89	90.3	91
1200	83	84.3	85.2	86.3	87.9	88.6
1500	80	82.8	83.2	84.5	85.2	86

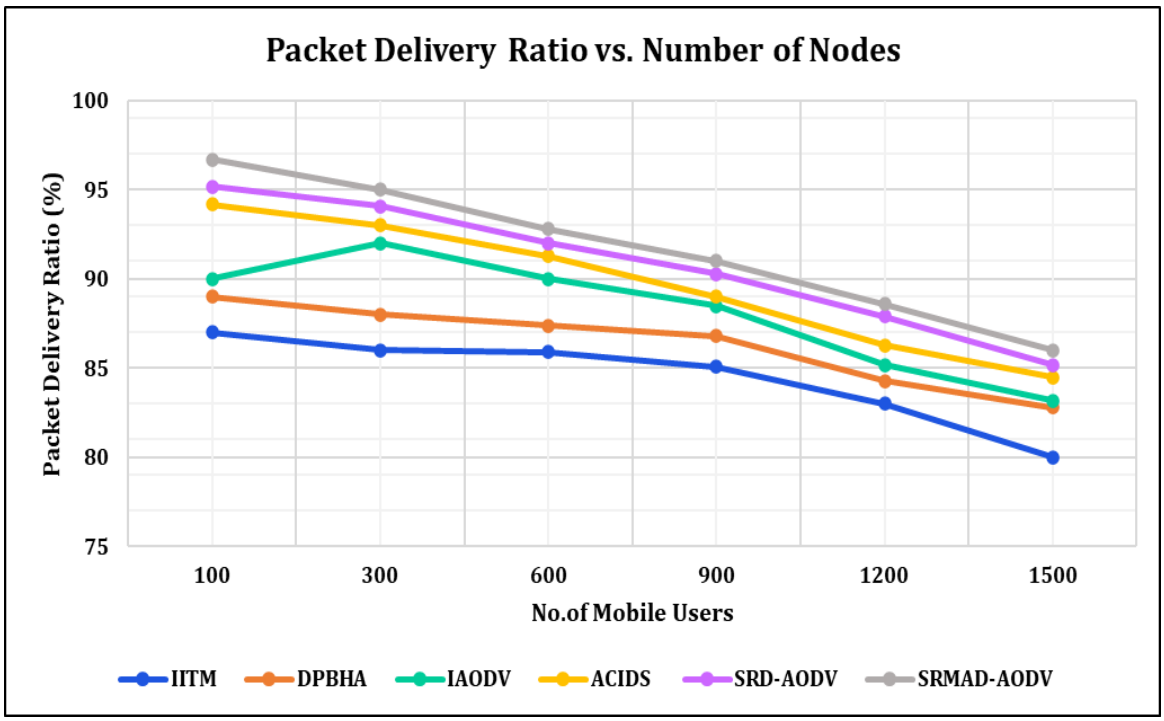

Figure 4.5 Comparison of Packet Delivery Ratio

4.5.3 Throughput

It refers to the total number of packets that have been forwarded in a specific amount of time. The throughput (in kilobits per second) of the SRMAD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols is depicted in Figure 4.6 for a variety of different numbers of nodes. One can deduce that the SRMAD-AODV protocol has the highest throughput of all the other protocols. This is due to the fact that under SRMAD-AODV, each CDS node is required to send out status messages, to which all other nodes must respond positively. If there is a node that does not meet the pre-defined requirements, the CDS node will flag it as a suspicious node, and the other nodes will stop the transfer with that particular node

Table 4.4 Throughput

No. of Node	IITM	DPBHA	IAODV	ACIDS	SRD-AODV	SRMAD-AODV
100	73.9	74.6	75	76	76.3	78.2
300	74.7	75.4	76.9	77.8	78.5	80.2
600	75.5	76.9	77.2	79	81.2	82.6
900	76	77.4	78.1	80.3	83.4	85
1200	77.7	78.9	79.2	81.8	86	87.7
1500	79.8	80.2	81.3	82.9	88.9	90

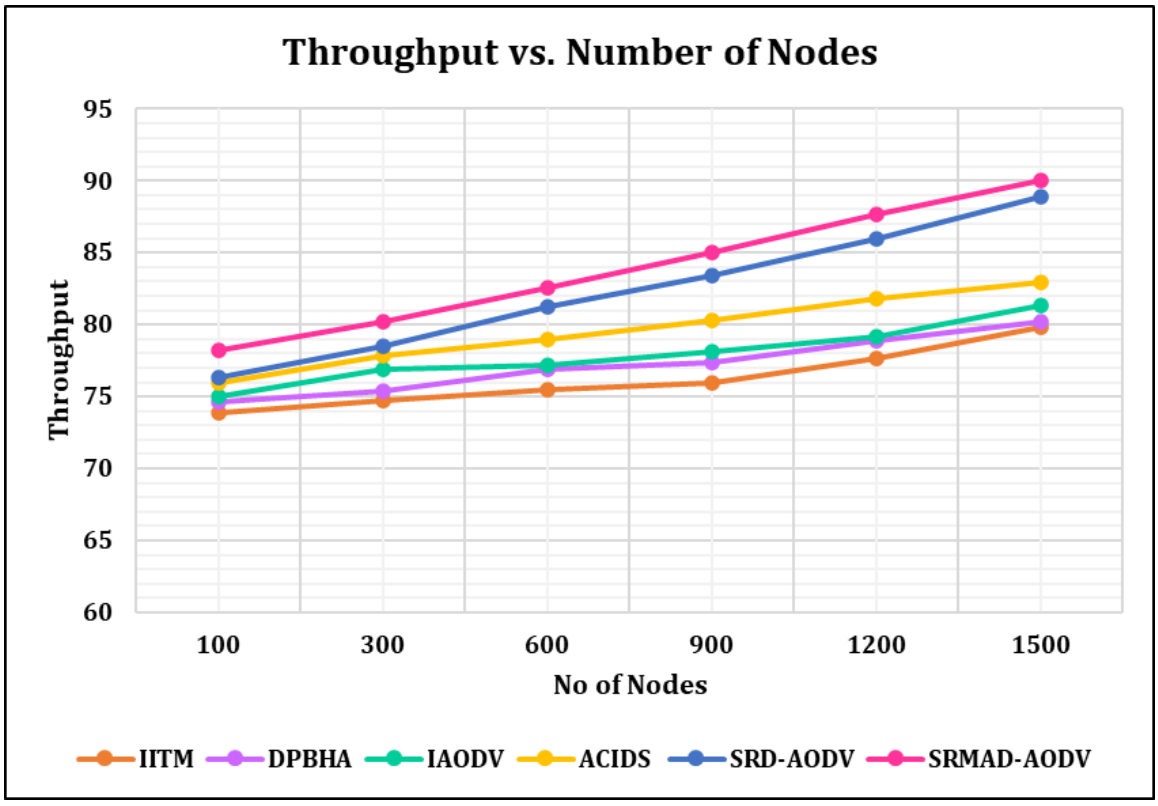

Figure 4.6 Comparison of Throughput

According to the findings presented here, the SRMAD-AODV protocol improves the efficiency of the network in terms of EED, PDR, and throughput when compared to

other protocols already in use, such as the SRD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols. This is due to the fact that all of the currently used protocols are only able to avoid black-hole and gray-hole attacks during the phase of route discovery. On the other hand, the SRMAD-AODV protocol that was developed can prevent black-hole and gray-hole attacks throughout the phase of data transmission, which leads to a lower rate of packet drop and a higher PDR.

4.6 SUMMARY

The SRMAD-AODV protocol described in this article was created to identify and counteract black-hole and gray-hole attacks during the data transfer phase. The CDS approach was initially used to build up compact collections of dominant nodes. The nodes selected for the ADS set have sufficient energy and confidence scores. The chosen ADS set has the ability to send a status packet to every other node in the network, allowing for the identification of nearby node activity during transmission. The ADS nodes can identify the genuine and suspicious nodes in the network based on their responses to the status packet. The suspected nodes were put on the blacklist, and the origin node received a record of this. Additionally, the origin node sends the data to the target along a path devoid of blacklist nodes and waits for an ACK to confirm the data has been received by the target. The origin node flagged the node as questionable and removed it from the routing database if the ACK was not returned. To ensure successful end-to-end data transfer, the changed routing table was also communicated to every other node in the network. As a result, the routing overhead was decreased and data packet loss was minimized. Finally, the simulation results demonstrated that the SRMAD-AODV protocol outperforms the

SRD-AODV, ACIDS, IAODV, DPBHA, and ITIM routing protocols with EEDs of 5.2 seconds, PDRs of 86%, and throughputs of 90 kbps. This protocol may be expanded in the future to recognize and counteract a variety of assaults that may be launched against the MANET. A few real-time MANET situations will also use this protocol.