Chapter 7

CHAPTER 7

RESULTS AND DISCUSSIONS

This chapter summarizes the research findings and the overall performance of the proposed framework for identification of plant leaf disease using heuristic algorithms. The proposed algorithms are SRD-AODV, SRMAD-AODV, SIIDAI Protocol with SAP and SIIDAI Protocol with DPI with significant parameters.

7.1 THE PROPOSED FRAMEWORK

The proposed framework for securing hybrid routing to thwart sequential attacks, protecting data packets and routing table information, secure route maintenance, detecting attacks and protecting the packets from various types of network attacks.

In the first phase, to secure node and discover the secure route using SRD-AODV (Secure Route Discovery-Ad hoc on-Demand Distance Vector) protocol we 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.

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. In data transmission, CDS node checks the neighbor node status whether the node

sending the packets 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 is useful 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 the existing protocols through simulation for detecting black and gray-hole attacks.

The third phase to identify various types of network attacks simultaneously with higher accuracy and defend them from the routing path during the data transmission. The Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) protocol is used to identify distinct attacks namely black hole, grey-hole, 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 proposed SIIDAI protocol offers protection against various types of malicious nodes in the network, resulting in reduced packet loss.

The fourth phase is to protect mobile ad-hoc network from various attacks using Secure Intelligent Informer with Distinct Attack Identification (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 and hence, 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.

7.2 RESEARCH FINDINGS OF PHASE 1 - SECURE ROUTE DISCOVERY

In this phase, the number of mobile users in the simulation is 150. The metrics of end-to-end delay, packet delivery ratio, average packet drop and throughput are measured. The results of pure AODV with limited features, EDRI-AODV and proposed SRD-AODV techniques are incorporated when the mobile users are 150.

7.2.1 Performance Analysis

- **End-to-End Delay**

In this research, we have used end to end delay which estimate 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 when compared to the AODV protocol.

- **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. However, SRD AODV has a PDR that is higher than AODV and EDRI AODV. This is because SRD-AODV avoids assaults in the network and ensures the routes work correctly, thereby preventing packet drops and failures in the connection.

7.3 RESEARCH FINDINGS OF PHASE 2 - ATTACK DISCOVERY BASED ON ENERGY AND TRUST

In this second phase the SRMAD-AODV protocol is emulated with the help of the network simulator (NS2.34). 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 EED, the PDR, and the throughput.

7.3.1 Performance Analysis

- **End-to-End Delay**

The end-to-end delay of the SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA and ITIM protocols for an increasing number of nodes has been discussed. The EED of SRMAD-AODV is 5.2% lower than the SRD-AODV, 5.5% lower than the ACIDS, 5.7% lower than the IAODV, 5.9% lower than the DPBHA and 6.4% lower than the ITIM protocols when 1500 nodes are presented in the network, so it can be concluded that the SRMAD-AODV has the least EED 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 EED of the network has decreased.

- **Packet Delivery Ratio**

The percentage of packet delivery ratio for the SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols when the number of nodes in the network is varied has been discussed 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 period of time. This makes the delivery of the data much more efficient.

- **Throughput**

The throughput (in kilobits per second) of the SRMAD-AODV, ACIDS, IAODV, DPBHA, and ITIM protocols is depicted in Figure 6 for a variety of different numbers of nodes. Because the throughput of the SRMAD-AODV protocol for 1500 nodes is 90% 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 ADS 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 ADS node will flag it as a suspicious node, and the other nodes will stop the transfer with that particular node.

7.4 RESEARCH FINDINGS OF PHASE 3 - DISTINCT ATTACK IDENTIFICATION

In this phase, the proposed SIIDAI with SAP protocol is simulated by the Network Simulator (NS2.34) in this part and its efficiency is compared to that of other protocols already in use. The end-to-end delay, packet delivery ratio and throughput are the metrics that are used in this investigation.

7.4.1 Performance Analysis

- **End-to-End Delay**

The end-to-end delay that was achieved for the SRD-AODV, SRMAD-AODV, and the proposed SIIDAI protocols while increasing the number of nodes has been analyzed and it is concluded that the suggested SIIDAI with SAP achieves the shortest end-to-end delay in comparison to the other protocols that are implemented in order to identify the specific attacks that are being made on the network.

- **Packet Delivery Ratio**

The PDR that can be accomplished using SRD-AODV, SRMAD-AODV and the proposed SIIDAI with SAP protocols is displayed in table 5.3 and figure 5.2, respectively, when the number of nodes in the network is increased. It suggests that the proposed SIIDAI is capable of achieving the highest PDR compared to the other protocols that are utilized to determine which specific attacks are occurring within the network.

- **Throughput**

The throughput (in kbps) achieved by SRD-AODV, SRMAD-AODV, and the proposed SIIDAI protocols while increasing the number of nodes has been analyzed which

indicates that the proposed SIIDAI with SAP realizes the maximum throughput when compared to the other protocols used to identify the particular attacks in the network.

7.5 RESEARCH FINDINGS OF PHASE 4 - PROTECTING MANET

In this phase, the proposed SIIDAI with DPI protocol is simulated by the Network Simulator (NS2.34), and its efficiency has been compared to that of other protocols already in use. The end-to-end delay, packet delivery ratio (PDR) and throughput are the metrics that are used in this investigation.

7.5.1 Performance Analysis

- **End-to-End Delay**

The proposed SIIDAI with DPI achieves the shortest 3.46 seconds end-to-end delay in comparison to the other protocols that are implemented in order to identify the specific attacks that are being made on the network.

- **Packet Delivery Ratio**

It suggests that the proposed SIIDAI with DPI is capable of achieving the highest 88% PDR compared to the other protocols that are utilized to determine which specific attacks are occurring within the network.

- **Throughput**

The throughput (in kbps) achieved by SRD-AODV, SRMAD-AODV, and the proposed SIIDAI protocols while increasing the number of nodes. This indicates that the proposed SIIDAI with DPI realizes the maximum throughput 95 kbps when compared to the other protocols used to identify the particular attacks in the network.

Table 7.1 Overall Comparison of Proposed Protocols

Nodes	Simulation Setup	SRD-AODV	SRMAD-AODV	SIIDAI WITH SAP	SIIDAI WITH DPI
100	End-to-End Delay	2.4	2.1	1.7	1.2
	Packet Delivery Ratio	95.2	96.7	97.1	97.5
	Throughput	76.3	78.2	79.5	80
300	End-to-End Delay	3.2	2.7	2.5	2.2
	Packet Delivery Ratio	94.1	95	95.5	96.2
	Throughput	78.5	80.2	81.5	83.3
600	End-to-End delay	3.8	3.4	3.1	2.4
	Packet Delivery Ratio	92	92.8	93.4	94
	Throughput	81.2	82.6	84	85.4
900	End-to-End delay	4.3	3.9	3.6	2.8
	Packet Delivery Ratio	90.3	91	91.6	92.4
	Throughput	83.4	85	86.5	88
1200	End-to-End delay	4.9	4.6	4.3	3.2
	Packet Delivery Ratio	87.9	88.6	89	90
	Throughput	86	87.7	89.2	90.2
1500	End-to-End delay	5.5	5.2	4.9	3.46
	Packet Delivery Ratio	85.2	86	86.7	88
	Throughput	88.9	90	93.4	95