Chapter 6

CHAPTER 6

PROTECTING MANET

6.1 INTRODUCTION

As MANETs are devoid of pre-established base stations or communication infrastructure, a multi-hop path needs to be constructed for communication from the source to the destination by nodes themselves. This communication is to be carried by nodes functioning with constrained resources viz., memory, battery power, computational capacity, bandwidth capacity, etc. MANET routing protocols are designed assuming mutual trust and cooperation among participating nodes. These protocols assume that all network nodes trust each other and extend their full cooperation in carrying out network functionalities without maliciously disrupting the network operations by violating the protocol specifications. However, the possibility of malicious nodes cannot be disregarded in any system [40]. Unfortunately, mobile ad hoc networks have a high probability of getting attacked by such adversaries due to their open wireless nature.

The source node waits for an end-to-end acknowledgement from the destination node before attempting to transfer the packets to it. It will obtain the end-to-end acknowledgement packet from the destination node on the reverse path if there is no malicious node present in the network. As soon as the source node identifies any intruders along the path, it will begin transmitting a "Intruder check" (IC) packet along the path [39]. The destination node id is encrypted within the intruder check packet using the source's private key. When a neighbor node receives an intruder check packet, it will decrypt the packet using the neighbor node's public key. This will happen whenever the neighbor node

receives the packet. It will check to see that the packet is addressed to the correct location. In that case, it will encrypt the IC packet before sending it on to the node that is its neighbor. At the same moment, an acknowledgement will be sent to the node that was the source of the data [44]. All of the genuine nodes are able to decrypt the message and send an acknowledgement to the one that came before them. The intruder node does not have either a public key or a private key, therefore it is unable to decrypt the packet [43]. Concerning the unauthorized node, the message of alarm will be transmitted from the source node to each and every other node in the network.

To resolve this issue, the Secure Route Maintenance and Attack Detection (SRMAD-AODV) protocol is used. This method is used to detect black holes and other anomalies. During the data transfer stage, this method is used to detect black-hole and gray-hole attacks. Aside from that, wormhole attacks, jellyfish attacks, route fabrication, and other similar attacks have an impact on network lifetime and data transmission efficiency. The Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) protocol is used to resolve this. SIIDAI protocol is used to identify attacks and protect packets and routes by selecting a specific node known as Secure Intelligent Informer (SII). SAP (Size Acknowledgement Path) and DPI (Dynamic Packet ID) are generated by Secure Intelligent Informer. The SAP number is used by the Secure Intelligent Informer to identify distinct attacks. DPI is used for node and route protection. Finally, when compared to existing protocols, the SIIDAI with DPI protocol achieves high network and efficiency.

6.2 MOTIVATION

An insufficient dynamic structure of a MANET makes it particularly vulnerable to various routing attacks. it is necessary to authenticate the nodes during data transmission

since the gray-hole nodes broadcast an accurate Target Sequence Number (TSN) during the route discovery, whereas it becomes malicious and drops the packets during the data forwarding. In addition, different kinds of attacks such as black-hole, grey-hole and sink-hole, bogus, modification attacks, route fabrication attacks and etc. influence the network lifetime and data transmission efficiency. It is necessary to protect the packets using novel protocol.

6.3 OBJECTIVE OF THIS CHAPTER

- The main objective of this phase is to protect data packets and routing table information from consecutive attacks in a mobile ad-hoc network (MANET).
- To propose novel approach that able to increase data transmission efficiency which extending network lifetime.

6.4 METHODOLOGY

6.4.1 Proposed Algorithm

- **Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) with DPI**

MANET nodes often consume an amount of energy sufficient to set up a connection for the transfer of data. Taking into consideration the many distinct kinds of possible nodes that are found in the network a substantial quantity of unnecessary traffic is generated as a result of the suspicious nodes and consistent beacon message broadcasting, which also contributes to an increase in the routing overhead. As a consequence of this, such nodes need to have their impact minimized in order to cut down on the additional routing costs. This protocol is utilised in the network to identify the various questionable node types, safeguard those nodes, and cut down on the costs associated with routing. SIIDAI, which

stands for Secure Intelligent Informer with Distinct Attack Identification, is a brand-new protocol that has been developed specifically to address this problem. This procedure focuses on a pair of different actions.

i. Identifying distinct attacks

ii. Protecting MANET from distinct attacks

i. Identifying Distinct Attacks

The proposed approach can distinguish between six distinct forms of attack, which are referred to as black-hole, grey-hole and sink-hole assaults, as well as false attacks, modification attacks and route creation. The SIIDAI protocol selects a particular node from the list of protected and trustworthy ADS nodes. Attacks known as black holes, grey holes and sink holes are all included in the category of packet drop attacks. Because there are several entry points, it is possible that an assault will come from one of those. SII is responsible for generating the SAP Number that is appended to the packet that is being transmitted by the origin node. The magnitude of the SAP number has the potential to have an effect on the packet drop. The Secure Intelligent Informer (SII) can identify a number of different routes. One way to detect assaults that are either bogus or modified is to use the acknowledgement number from the SAP system to spot the phoney answer. The goal of the route fabrication attack is to determine, upon detecting a change in the path, which branch of the SAP number should be used to reroute the packet.

ii. Protecting MANET from Distinct Attacks

SII generates the Dynamic Packet ID (DPI) in order to defend the node against a total of six different types of attacks, which include black-hole, grey-hole and sink-hole

assaults, as well as fraudulent, modification and route fabrication attacks. A random integer is used to determine the value of the DPI setting. It is determined through application of the formula,

$$DPI = (xn) \quad \text{(Eq 6.1)}$$

where x is a fixed value, and n is a variable that can be anything you want it to be. After the DPI has been created, it will be appended to the packet that will be transmitted across the SII from the origin node to the destination node. When the packet reaches a new node, a new DPI is formed and attached to it for protection. This continues until the packet reaches its final destination. This approach has been shown to be highly secure on multiple occasions because of the fact that whenever a new node is reached, a new DPI is produced and attached to each packet. Because of the packets' ability to undergo dynamic changes, it is difficult for an attacker to keep track of them. Additionally, the DPI makes it even more difficult for an adversary to get the data by preventing data leaks. Because of this, it is one of the most secure techniques for transmitting data that is currently accessible.

Algorithm 5.1. SIIDAI Protocol with DPI

Input: N number of mobile nodes

Output: Protection Distinct types of attacks (suspected nodes)

Begin

Step 1: Construct the MANET comprising N number of nodes;

Step 2: Generate secure key to verify every nodes;

Step 3: Generate the sub group of nodes by performing the CDS technique;

Step 4: Determine each node's energy and trust values;

Step 5: Decide the node with the highest energy and trust values as the ADS;

Step 6: Transfer the packet from source to destination;

Step 7: Select the specific node is known as Secure Intelligent Informer (SII);

Step 8: Generate SAP number and DPI from SII;

Step 9: Origin node sends the packets via SII;

Step 10: SII receives the packet and forward the packet by attaching the SAP number to all nodes within the transmission region;

Step 11: SII monitor all nodes activities;

Step 12: Analyze each node's replies to the corresponding status packet, i.e., verify whether the node transmits fake replies, dropped packets etc;

Step 13: **If (node drops the packets)**

Step 13.1: Verify the node size in SAP number

Step 13.2: Observe the cause for packet dropping;

Step 13.3: Identify whether the node is black hole, gray hole or sinkhole attacked node;

Step 14: ***elseif*** (***node transmits the fake replies***)

Step 14.1: Verify the acknowledgment in SAP number

Step 14.2: Compare the replies (node characteristics) with the authentic node;

Step 14.3: Identify the attack known as bogus attacks or modification attacks;

Step 15: **elseif (**node transmit via false route)

Step 15.1: Verify the path in SAP number;

Step 15.2: Identify whether the attack is route fabrication or flooding attack;

Step 16: **endif**

Step 17: Create the blacklist and store comprising the identified distinct types of suspected nodes;

Step 18: Transfer the data packets between the SII node and the target node;

Step 19: **If (SAP number is legitimate)**

Step 19.1: SII is ready to send the packets to the nodes.

Step 19.2: SII generate DPI number and attaches with the packet;

Step 19.3: Transfer the packets via that routing path, which has no suspected nodes;

Step 19.4: Update the new routing table to all other nodes in the network;

Step 19.5: Enhance the network efficiency

Step 20: ***Endif***

Step 21: ***End***

6.5 RESULTS AND DISCUSSION

The proposed SIIDAI with DPI 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 (PDR) and throughput are the metrics that are used in this investigation. The simulation parameters are presented in Table 6.1.

Table 6.1 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
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

6.1.1 End -to- End Delay (EED)

Table 6.2 End-to-End Delay vs. No. of Nodes

No. of Node	SRD-AODV	SRMAD-AODV	Proposed SIIDAI with SAP	Proposed SIIDAI with DPI
100	2.4	2.1	1.7	1.2
300	3.2	2.7	2.5	2.2
600	3.8	3.4	3.1	2.4
900	4.3	3.9	3.6	2.8
1200	4.9	4.6	4.3	3.2
1500	5.5	5.2	4.9	3.46

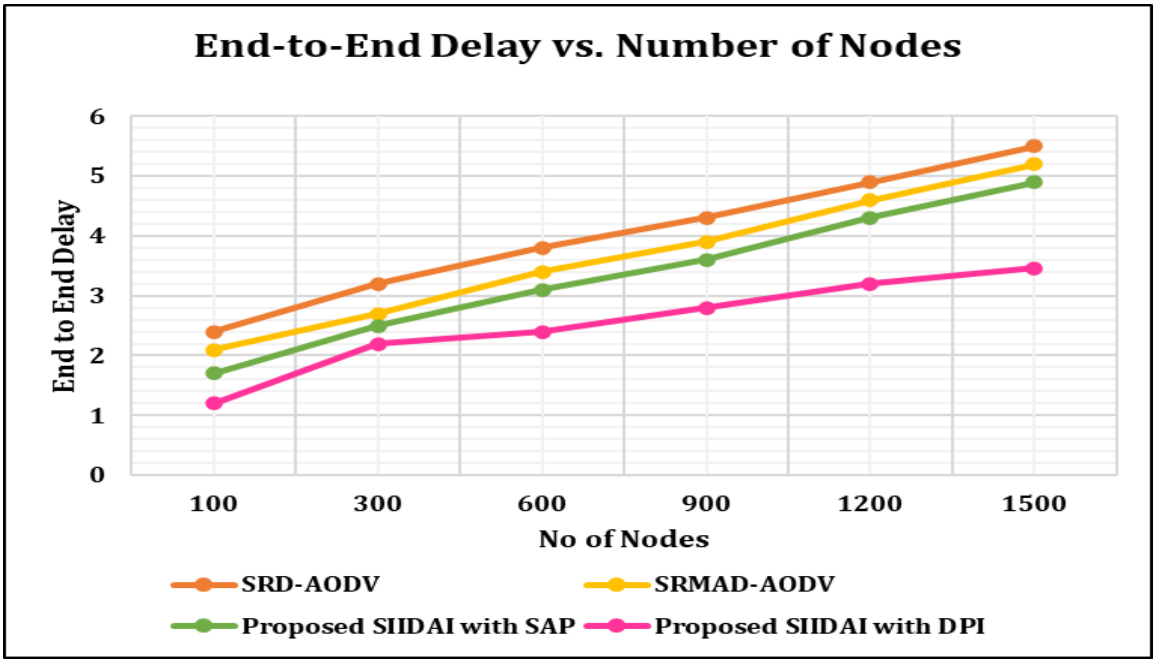

Figure 6.1 End-to-end Delay vs. Number of Nodes

The end-to-end delay (in seconds) that was achieved for the SRD-AODV, SRMAD-AODV and the proposed SIIDAI protocols while increasing the number of nodes is depicted in Figure 6.1. It is concluded that the suggested SIIDAI with DPI 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.

6.1.2 Packet Delivery Ratio (PDR)

The PDR that can be accomplished using SRD-AODV, SRMAD-AODV and the proposed SIIDAI with SAP protocols is displayed in table 6.3 and figure 6.2, 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.

Table 6.3 Packet Delivery Ratio

No. of Node	SRD-AODV	SRMAD-AODV	Proposed SIIDAI with SAP	Proposed SIIDAI with DPI
100	95.2	96	97.1	97.5
300	94.1	95	95.5	96.2
600	92	92.8	93.4	94
900	90.3	91	91.6	92.4
1200	87.9	88.6	89	90
1500	85.2	86	86.7	88

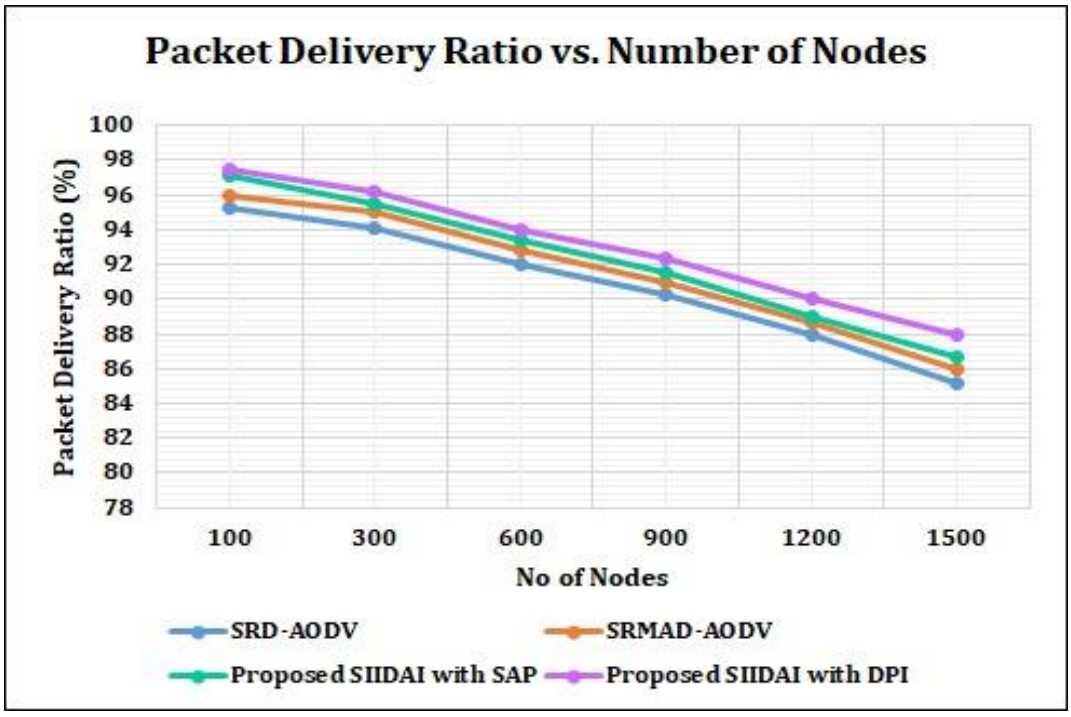

Figure 6.2 Packet Delivery Ratio vs. Number of Nodes

6.1.3 Throughput

Table 6.4 and Figure 6.3 both depict 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 when compared to the other protocols used to identify the particular attacks in the network.

Table 6.4 Throughput

No. of Node	SRD-AODV	SRMAD-AODV	Proposed SIIDAI with SAP	Proposed SIIDAI with DPI
100	76.3	78.2	79.5	80
300	78.5	80.2	81.5	83.3
600	81.2	82.6	84	85.4
900	83.4	85	86.5	88
1200	86	87.7	89.2	90.2
1500	88.9	90	93.4	95

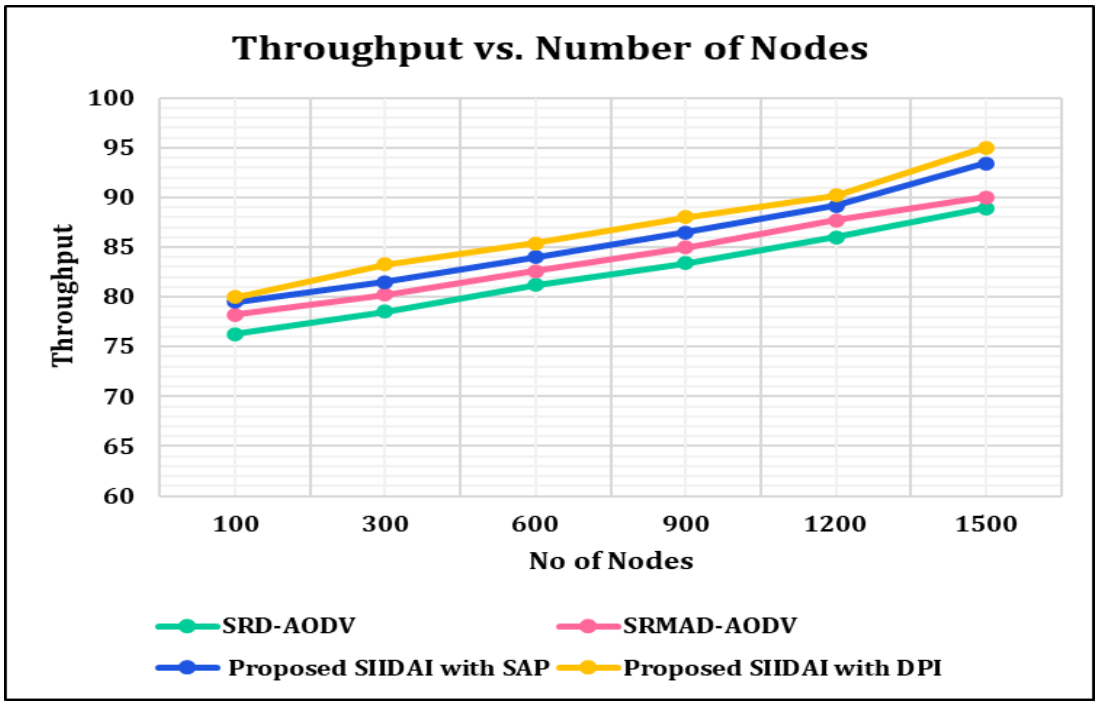

Figure 6.3 Throughput vs. Number of Nodes

6.6 SUMMARY

In this chapter, the Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) with Dynamic Packet ID (DPI) protocol was designed in order to recognize various types of attacks based on the SAP number associated with each attack. As a consequence of this, various kinds of malicious nodes have been discovered. DPI is used for node and route protection. Finally, when compared to existing protocols, the SIIDAI with DPI protocol achieves high network and efficiency. In conclusion, the results of the simulation showed that the proposed SIIDAI with DPI protocol has an average end-to-end delay of 3.46 seconds, a packet delivery ratio (PDR) of 88%, and a throughput of 95 kbps. This is in comparison to other existing routing protocols, which have a PDR of less than 90%.