Chapter 5

CHAPTER 5

DISTINCT ATTACK IDENTIFICATION

5.1 INTRODUCTION

MANET lacks a centralized structure to regulate its operation because it is so autonomous and self-configuring. Because mobile devices, also known as nodes, are free to move around inside the network's coverage area, their ties to the various other devices will regularly alter. The nodes are free to join or exit the network whenever they choose. Therefore, the nature of the network architecture is such that it is dynamic. The mobile nodes do not rely on any underlying fixed infrastructure like as base stations or access points in order to function properly. Mobile nodes are dependent on one another to maintain the connectivity of the network. Every one of the mobile nodes serves as a host as well as a router. Only with the assistance of nodes the data transmission in the network is actually accomplished. In a MANET, each and every node is required to participate in the routing process in order to ensure that the network does not lose connectivity. The nodes not only find the routes, but they also keep them in good working order to ensure effective data transmission throughout the network. Since the communication in a MANET takes place in free space, it is vulnerable to many attacks from nodes that are trying to do harm. The most significant danger to communication comes in the form of attacks [59].

When a centralized control structure is impossible to implement, such as in inaccessible regions or during times of emergency, the role of MANET becomes significantly more important. Since the MANET uses wireless communication between the nodes, it is susceptible to a wide variety of different kinds of malicious attacks. To be isolated, for there to be any chance of a secure data transmission. Even if there are several methods in MANET that can enable encrypted transmissions, there is still an opportunity for improvement in MANET's security [52].

The performance of the network is influenced by a wide range of additional parameters in addition to black holes and gray holes. Additionally, it is vulnerable to a variety of attacks, including route fabrication, sinkholes, and heated holes. When an intruder compromises a network node and then utilizes that node to launch an attack, it's referred to as a sinkhole attack. Depending on the routing metric that the routing protocol employs, the targeted node will then attempt to draw in all of the traffic from the nearby nodes. Once it has done so successfully, it will launch an attack. Due to its communication architecture, which consists of many-to-one communication between nodes and each node providing data to the base station, this wireless sensor network is vulnerable to a sinkhole attack. A common wormhole attack involves the attacker receiving packets at one location in the network, forwarding them using a wired or wireless link that has lower latency than the network links, and then relaying those packets to a different location in the network [53]. A distributed wormhole identification method for wireless sensor networks is presented in this article. The algorithm is built to interface with these networks and recognizes wormholes based on the distortions they introduce. The approach reconstructs local maps for each node using a hop counting technique as a probe, then employs a "diameter" characteristic to find anomalies caused by wormholes. Hop counting is used by the program as a probe operation because wormhole attacks are passive in nature.

This research study focuses on recognizing different kinds of attacks and developing a protocol called Secure Intelligent Informer with Distinct Attack Identification

(SIIDAI) to protect MANET from those attacks. The proposed method can identify numerous attacks at the same time, which is a significant advantage. This protocol will choose the Secure Intelligent Informer node (SII) and once it has done so, it will create the SAP Number. This number will then be appended to the packet that will be transmitted by the origin node. The magnitude of the SAP number has the potential to have an effect on the packet drop. Multiple pathways are uncovered by the SII. A common method to detect attacks that are either bogus or modified is to use the acknowledgement number from the SAP system to spot the phony 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.

5.2 MOTIVATION

WSN and MANET have generated an incredible number of opportunities and popularity over the past few years. A number of problems, both in terms of network performance and security, are brought on by the highly customizable characteristics of the MANET. The MANET framework is put at risk in a number of different ways due to several flaws in its security. MANET attacks come in a variety of flavors, such as grey hole, black hole, sink hole, and others. These malicious attacks, regardless of the circumstances, have the effect of dramatically degrading the functioning of the network as a whole. In addition to that, assaults such as wormhole attacks, jellyfish attacks, route fabrication, and other similar attacks have an effect on the longevity of a network as well as the efficiency with which data is transmitted.

5.3 OBJECTIVE OF THIS CHAPTER

- The main objective of this work is to detect the various attacks that exploit vulnerabilities in secure route maintenance.
- To identify the attacks using secure intelligent informer techniques on any specific nodes.
- To utilize the SAP method which enable specific identification of the attacks.

5.4 METHODOLOGY

The SIIDAI protocol is explained briefly in this section. MANET nodes typically use enough energy to establish a data transmission link. Consider the various types of suspected nodes that exist in the network. The suspected nodes regularly send out beacon messages, resulting in a large amount of redundant traffic and increasing routing overhead. As a result, such nodes must be mitigated in order to reduce the additional routing cost. This protocol is used in the network to identify different types of suspect nodes to protect them and reduce routing costs. Other than grey and black holes, various factors influenced network performance. It is also vulnerable to various attacks such as warm hole, sink hole and route fabrication among others. SIIDAI, a new protocol, has been developed to address this issue (Secure Intelligent Informer with Distinct Attack Identification).

5.4.1 Existing Algorithms

- **Secure Route Discovery-Ad hoc on-Demand Distance Vector (SRD-AODV)**

The SRD-AODV routing protocol [24] was employed. This procedure is broken down into its component parts. At the beginning, the MECDH algorithm is used to verify the authenticity of each mobile node. After authentication has been completed, the

SRD-AODV routing protocol is used to protect neighbor discovery and the route from being tampered with by malicious nodes. After that, you should create a list of trust nodes in order to save the secure node and route. At this point, all of the malicious nodes have been eliminated from the network.

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

After the node was secured, it was broken up into a number of smaller subgroups. This node CDS, which stands for "Connected Dominated Set." SRMAD-AODV [25] is a protocol that is used by every mobile node in order to estimate energy and trust. The CDS approach is applied for deciding which node inside the Attack Discovery System (ADS) has the highest level of energy and confidence. The selected ADS node will then transmit a packet to the network region in question in order to check the status of that region. A blacklist of suspected black hole or grey-hole nodes is compiled by ADS nodes after conducting an analysis of the gathered behavioral data. The blacklist is then sent back to the node that initiated the process in order to verify that the nodes included on the list are susceptible to attack. After verifying the legitimacy of the blacklist, the origin node sends a block message to all of the other nodes in the network and then removes any suspect nodes from the routing path. This helps to ensure that data packets are not lost while being transferred. During the stage of the protocol known as "data transfer," the SRMAD-AODV Protocol was developed to identify and protect against assaults known as "black hole" and "grey hole." If a node does not discard any of its packets, then the attack is referred to as a grey-hole attack; otherwise, it is referred to as a black hole attack.

5.4.2 Proposed Algorithm

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

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 the attack 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 significance 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 phony 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.

The Secure Intelligent Informer (SII) is the name given to the particular node that was selected from the protected and trusted node list. A packet is transmitted along the SII from the origin node to the destination node. It offers multiple possible routes. SII is responsible for generating SAP Numbers; SAP Numbers are determined by node size, acknowledgment and path. After receiving the data packet from the node of origin, SII then forwards it together with the SAP number to all of the other possible destinations. SII maintains a record of all of the network's adjacent nodes. Whether it was affected by a packet drop, alteration, fake response, route fabrication and so on and so forth. The attacks were categorized in a variety of different ways.

- **Packet Drop**

The SAP Number is utilized in order to determine whether the packet has been dropped or not. It was determined that a packet drop occurred when the size of the node was reduced. When a packet is dropped in its whole, this is known as a black hole attack. In that case, a gray hole attack will take place.

- **Fake Reply**

A fake response will be acknowledged with a SAP number proving its authenticity. This type of attack is referred to as Bogus attack.

- **Modification**

The acknowledgement, in addition to the size of its packets, will serve as confirmation that the modification has taken place. A modification attack is the name given to this particular kind of attack.

- **Route Fabrication**

The node receiving the route fabrication instruction was sent down the wrong path. It is able to determine whether the path value in the SAP number has been modified or not. The process that is being described here is called "route fabrication." There is occasionally some commotion as a result of it. Flooding attacks are another term for this.

Algorithm 5.1. SIIDAI Protocol with SAP

```
Input: $N$ number of mobile nodes

Output: 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 node;

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 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:  $\boldsymbol{elseif}(n\boldsymbol{ode\ transmits\ the\ fake\ replie}s)$
        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:  End
```

5.5 RESULTS AND DISCUSSION

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 (PDR) and throughput are the metrics that are used in this investigation. The simulation parameters are presented in Table 5.1.

Table 5.1 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

5.5.1 End-to-end Delay (EED)

It is the amount of time that passes from the point at which the first packet is transmitted from the source to the point at which the first packet has successfully reached the target.

$$Delay = Accepted\ time - Forwarded\ packet\ time \qquad \text{(Eq.5.1)}$$

Table 5.2 Comparison Results based on End-to-End Delay

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

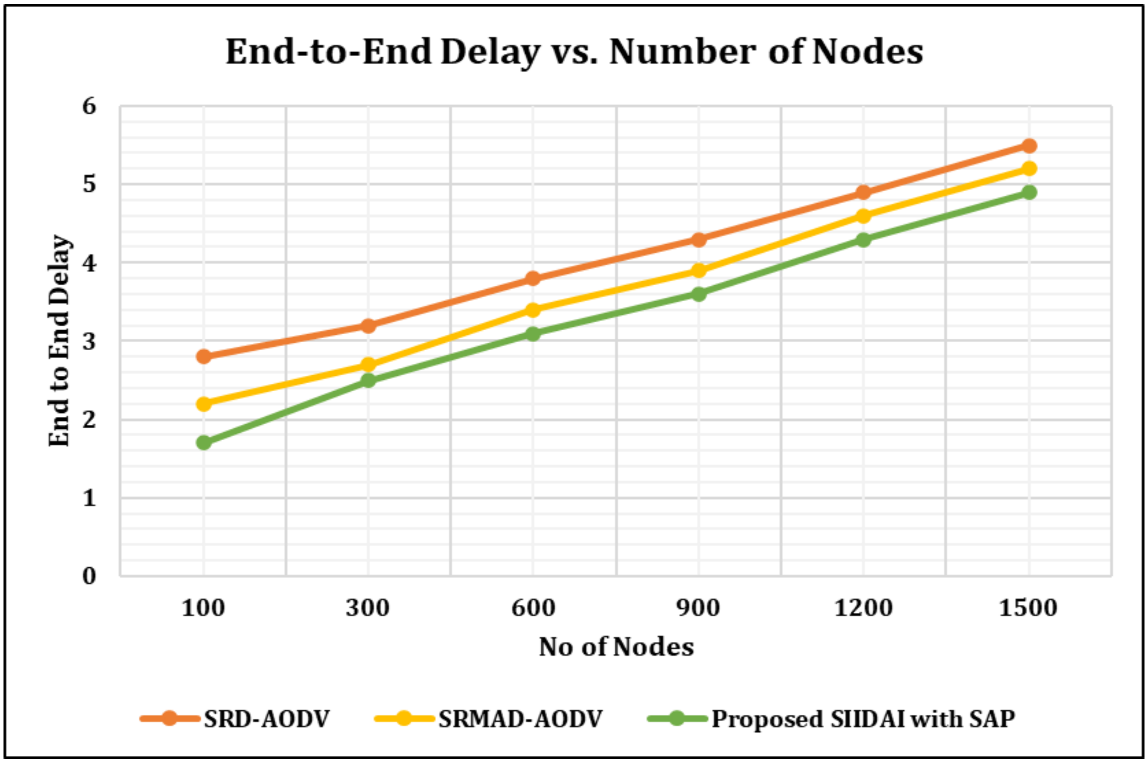

Figure 5.2 End-to-End Delay vs. Number of Nodes

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 5.1. 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.

5.5.2 Packet Delivery Ratio (PDR)

It is the ratio of the total quantity of packets supplied by the source to the total quantity of packets that have been efficiently acknowledged by the target.

$$PDR = \frac{Overall\ amount\ of\ packets\ accepted\ by\ target}{Overall\ amount\ of\ packets\ forwarded\ from\ origin} \quad \text{(Eq.5.2)}$$

Table 5.3 Packet Delivery Ratio

No. of Node	SRD-AODV	SRMAD-AODV	Proposed SIIDAI with SAP
100	95.4	96.2	97.1
300	94.1	95	95.5
600	92	92.8	93.4
900	90.3	91	91.6
1200	87.9	88.6	89
1500	85.2	86	86.7

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.

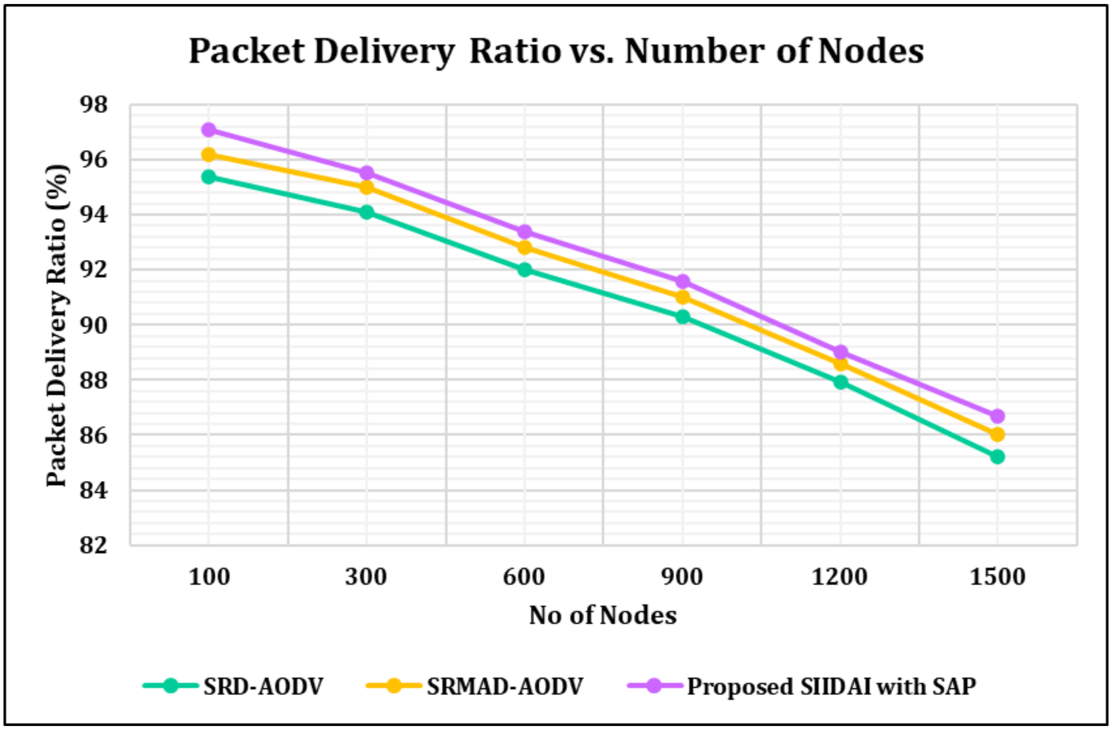

Figure 5.2 Packet Delivery Ratio vs. Number of Nodes

5.5.3 Throughput

It is the sum of all packets that have been forwarded in a specific amount of time and is computed as follows:

$$Throughput = \frac{Total\ amount\ of\ forwarded\ packets}{Time} \quad \text{(Eq.5.3)}$$

Table 5.4 Throughput

No. of Node	SRD-AODV	SRMAD-AODV	Proposed SIIDAI with SAP
100	77	78.1	79.5
300	78.5	80.2	81.5
600	81.2	82.6	84
900	83.4	85	86.5
1200	86	87.7	89.2
1500	88.9	90	93.4

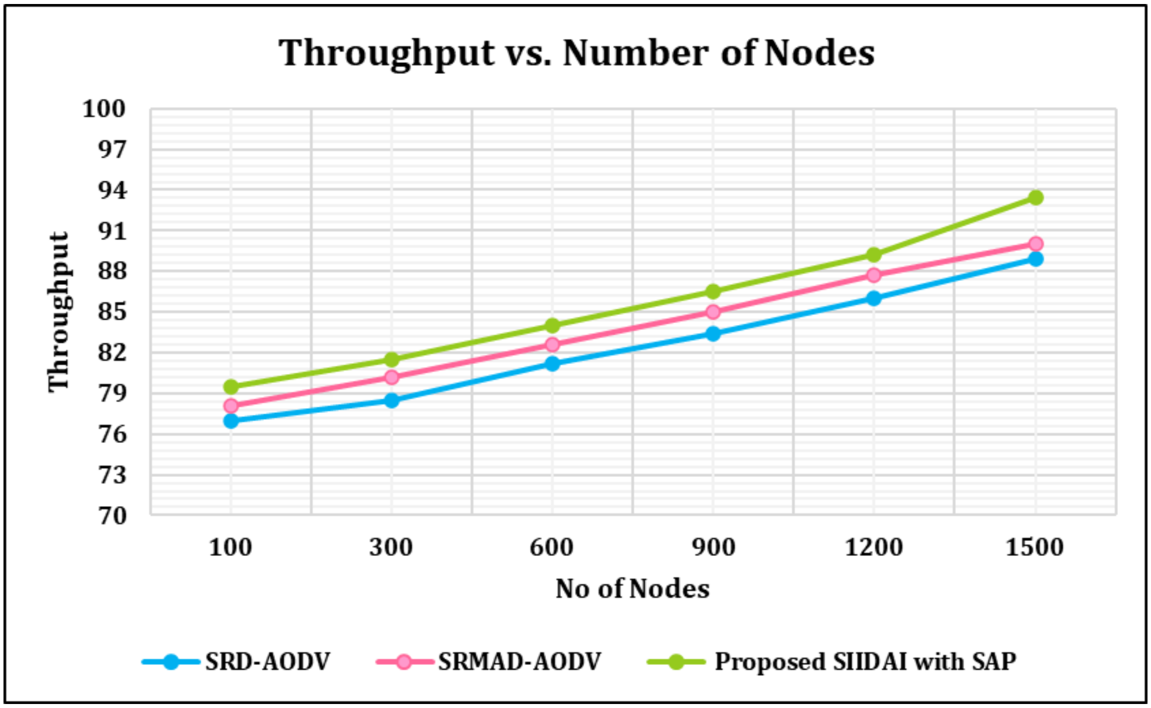

Figure 5.3 Throughput vs. Number of Nodes

Table 5.4 and Figure 5.3 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 SAP realizes the maximum throughput when compared to the other protocols used to identify the particular attacks in the network.

5.6 SUMMARY

In this chapter, the SIIDAI with SAP 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. In conclusion, the results of the simulation showed that the proposed SIIDAI protocol has an average end-to-end delay of 4.9 seconds, a packet delivery ratio (PDR) of 86.7% and the throughput of 93.4 kbps. This is in comparison to other existing routing protocols, which have a PDR of less than 90%.