Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Protecting Manet From Different Attacks Using Siidai Protocol

Dr. K.R.Kanchana , Dr. J.Viji Gripsy[2]

[1]Assistant Professor ,Department of Computer Science Government Arts College, Udhagsmandalam.. kanchumsc@gmail.com
[2]Associate Professor, Department of Computer Science PSGR Krishnammal College for women, Coimbatore. vijigripsy@gmail.com.

In recent years, wireless sensor networks and Mobile Ad-hoc networks (MANET) have created tremendous opportunity and popularity. The highly adaptable nature of the MANET causes a number of network performance and security issues. Various security defects endanger the MANET framework in a variety of ways.MANET attacks include grey hole, black hole, sink hole, and other types. In all situations, these dangerous attacks significantly weaken the network's functions and overall performance.Aside from that, wormhole attacks, jellyfish attacks, route fabrication, and other similar attacks have an impact on network lifetime and data transmission efficiency.To overcome this difficulty,Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) protocol is proposed which is used to identify attacks and protect packets and routes by selecting a specific node known as Secure Intelligent Informer (SII). Size Acknowledgement Path (SAP) and Dynamic Packet ID (DPI) are generated by SII.

Keywords: MANET; Secure Intelligent Informer; Size Acknowledgement Path; Dynamic Packet ID; Secure Intelligent Informer with Distinct Attack Identification Protocol

1. Introduction

MANET is very independent and self-configuring that it does not have any centralized system to control its working. The mobile devices or nodes can travel anywhere in the area of network and will therefore change its links to other devices frequently. The nodes can join or leave the network anytime. So, the topology of the network is dynamic in nature.The mobile nodes do not depend on any underlying fixed infrastructure likebase station/access points. Mobile nodesrely on each other to keep thenetwork connected. All the mobile nodes act as both host and router. The datatransmission in the network is done only with the help of nodes. In MANET,all the nodes have to get involved in routing process in order to maintainconnectivity in the network. The nodes discover the routes and also maintainthem for efficient data transmission in the network. The communication inMANET takes place in free space and so there are prone to several attacks bymalicious nodes. Attacks are the major threat to communication.

The role of MANET is significant in remote areas and inemergency situations where the centralized control structure is difficult todeploy. The nodes communicate in the wireless

medium and so the MANETis vulnerable to many types of malicious attacks. To provide a secure datatransmission, the attacks should be detected and the malicious nodes causingthe attacks should be isolated. Even though there are some techniques toprovide secured transmission in MANET, still there is a scope for enhancingthe security in MANET.

This research work deals with identifying various attacks and protecting MANET from these attacks using proposed Secure Intelligent Informer with Distinct Attack Identification (SIIDAI) protocol. The proposed protocol is used to detect multiple attacks at the same time. This protocol selects the Secure Intelligent Informer node (SII). Two numbers are generated by this node. SAP and DPI are the numbers. The proposed SIIDAI protocol is used to identify various attacks based on SAP number, and SIIDAI protocol is used to protect data and route it away from various attacks based on DIP number. This protocol will help to identify various types of network attacks while also protecting the packet and route from sequential attacks.

2. Literature Survey

Doss et al. [14] developed precise mitigation and identification of Jelly Fish AIS (JFAIS) based on the ensemble legitimate routing-based strategy to identify attacks. The Support Vector Machine (SVM) was applied to learn the efficiency of packet transfer and identify the suspected nodes. Also, the legitimate nodes were selected to transfer data according to the hierarchical trust estimate property of nodes. However, it was not effective to identify more types of attacks in the network.

Rajendran et al. [15] developed a Cross Centric AIS (CCAIS) to enable secure routing over black hole attacks in the MANET. It depends on the route source choice, priority bit allocation and AIS attack minimization. The secure routing by PIHNSPRA routing scheme was used by the route source choice and the route from end-to-end nodes was chosen securely to mitigate the black hole attack. Also, the priority bit allocation was applied to handle the node location and network forecasting by the previous interaction history. Moreover, a secure AIS transfer efficiency was obtained to establish an effective routing path. However, the throughput was not high, which indicates that this system was not suitable to detect various attacks.

Tahboush&Agoyi [16] designed a Hybrid Wormhole AIS (HWAIS) to identify in-band and out-of-band wormholes in MANET. The in-band wormholes were identified by executing Round Trip Time (RTT) depending on its hop count and Packet Delivery Ratio (PDR). Also, K-means clustering was used to obtain the optimum centroid, which was considered as the PDR threshold in in-band identification. The out-band wormholes were identified by the communication range between successive nodes in a highly optimistic way. However, its flexibility and identification efficiency were not effective in a large topological region.

Prem Kumar &Manikandan [17] developed a Distributed Hybrid Sybil AIS (DHSAIS) to detect static and dynamic Sybil attacks in ad-hoc networks. First, a specified group of nodes was chosen as monitoring nodes depending on the neighbor density of the nodes. If the node was static, the Sybil attack was identified by using the Received Signal Strength Indicator (RSSI) and Angle of Arrival (AoA) rate of any identical position claims. If the node was

traveling and if the mobility distance at successive timeslots were varied, it was termed as Sybil attack. However, it has a high computational overhead while concurrently identifying various types of attacks.

Dhanaraj et al. [18] developed a hybrid identification model for attacks by using a Proportional Coinciding Score (PCS) and an MK-means algorithm to detect the black hole and sinkhole attacks. Initially, the number of collected training data attributes was minimized by the data pre-processing in the PCS. Then, the chosen attributes were fed to the MK-means algorithm to learn the data and identify specific attack decision measures. Though, the records considered for the simulation were limited and so it was not apt for multiple attacks identification.

3. PROPOSED 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, 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). This protocol focuses on two activities.

1. Identifying distinct attacks
2. Protecting MANET from distinct attacks

3.1 Identifying Distinct Attacks

The proposed methodology is used to identify six different attacks namely black-hole, grey-hole, and sink-hole, bogus, modification attacks, and route fabrication. 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. SII generates the SAP Number which is attached to the packet sent by the origin node. The size of the SAP number can influence the packet drop. The SII (Secure Intelligent Informer) detects multiple paths. Bogus or modification attacks is to identify the fake response using the acknowledgement of the SAP number. Route fabrication attack is to identify when a change in the path is detected, the path of the SAP number redirects the packet.

3.2Protecting MANET from Distinct Attacks

SII creates the DPI (Dynamic Packet ID) in order to protect the node from six different attacks namely black-hole, grey-hole, and sink-hole, bogus, modification attacks, and route fabrication attacks. DPI is a constant number that is chosen at random. It is calculated using the formula,

$$DPI = (xn)$$

where x is a constant number and n is an arbitrary number. 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. Since a new DPI is generated and attached to each packet when a new node is reached, this method has been proven to be extremely secure. It is difficult for an attacker to track the packets as they are dynamically changing. Additionally, the DPI makes it even more difficult for an attacker to gain access to the data. This makes it one of the most secure methods of data transmission available.

Algorithm 3.2. SIIDAI Protocol

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**(n**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: **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**

4.Simulation Results

In this section, the SIIDAI protocol is simulated by the Network Simulator (NS2.34) and its efficiency is compared with the existing protocols. This analysis is conducted according to the end-to-end delay, PDR and throughput. Table 4.1 lists the simulation parameters.

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
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

4.1 End-to-end Delay

It is the interval between the initial packet forwarded from the source and the first packet effectively reached the target.

$$\text{Delay} = \text{Accepted time} - \text{Forwarded packet time} \quad \text{(Eq.4.1)}$$

Table 4.1 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

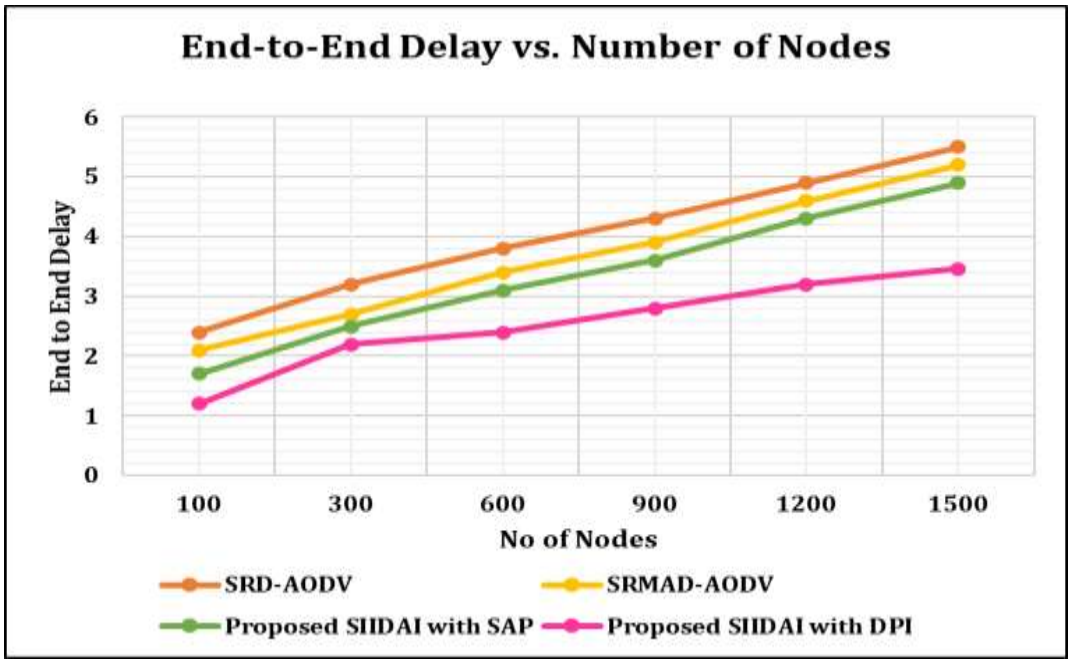

Figure 4.1 End-to-end Delay vs. Number of Nodes

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 4.1. 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.

.

4.2 PDR

It is the rate of sum quantity of packets effectively accepted by the target to the sum quantity of packets sent by the source.

$$\text{PDR} = \frac{\text{Overall amount of packets accepted by target}}{\text{Overall amount of packets forwarded from origin}} \quad \text{(Eq.4.2)}$$

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 4.2 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

z

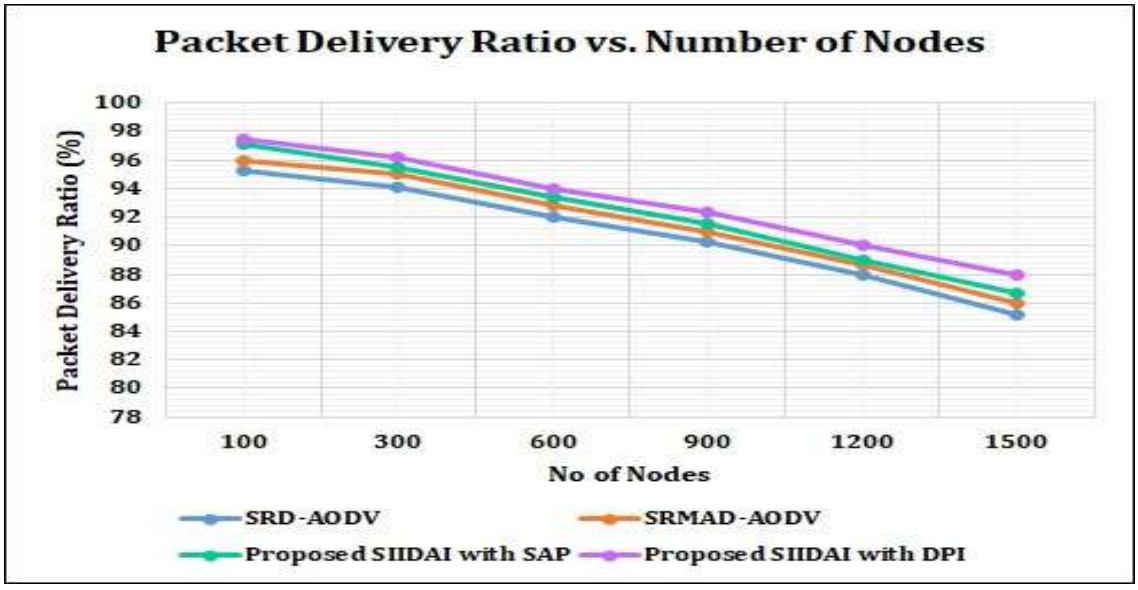

fig 4.2 Packet Delivery Ratio vs. Number of Nodes

4.3 Throughput

It is the total amount of forwarded packets within a given time and calculated as:

$$\text{Throughput} = \frac{\text{Total amount of forwarded packets}}{\text{Time}} \quad \text{(Eq.4.3)}$$

Table 4.3 and Figure 4.3 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 4.3 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

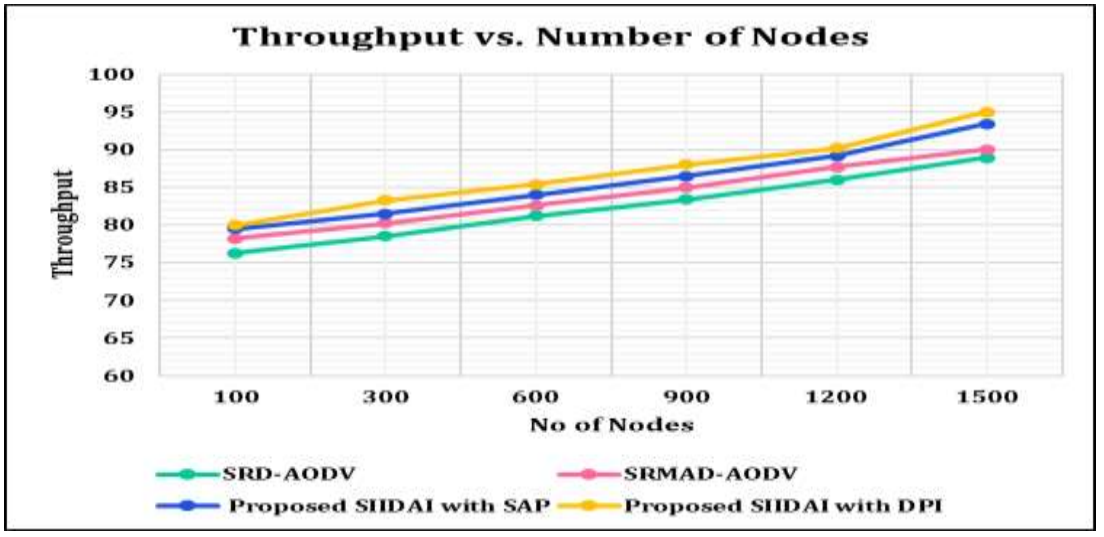

Figure 4.3 Throughput vs. Number of Nodes

5. Conclusion

In this article, the SIIDAI protocol was developed to identify various attack types based on their SAP number and to protect packets from sequential attacks based on their DPI number. The proposed SIIDAI protocol is used to detect various types of attacks and protect MANET. As a result, different types of malicious nodes are identified, and packets and routing are protected. Finally, when compared to other existing routing protocols, the simulation results showed that the proposed SIIDAI protocol has an average end-to-end delay of 3.46 seconds, a PDR of 91.98%, and a throughput of 87.84 kbps.

REFERENCES

[1] Aldana, J. A. A., Maag, S., & Zaidi, F. (2018). MANETs interoperability: current trends and open research. In 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 481-487.

[2] Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., & Yaacob, M. (2018). A survey on MANETs: architecture, evolution, applications, security issues and solutions. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 832-842.

[3] Saudi, N. A. M., Arshad, M. A., Buja, A. G., Fadzil, A. F. A., &Saidi, R. M. (2019). Mobile ad-hoc network (MANET) routing protocols: a performance assessment. In Proceedings of the Third International Conference on Computing, Mathematics and Statistics, Springer, Singapore, pp. 53-59.

[4] Bai, Y., Mai, Y., & Wang, N. (2017). Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs. In IEEE Wireless Telecommunications Symposium, pp. 1-5.

[5] Syed, S. A. (2021). A systematic comparison of mobile ad-hoc network security attacks. Materials Today: Proceedings, 1-6.

[6] Nabou, A., Laanaoui, M. D., &Ouzzif, M. (2018). Evaluation of MANET routing protocols under black hole attack using AODV and OLSR in NS3. In 6th IEEE International Conference on Wireless Networks and Mobile Communications, pp. 1-6.

[7] Khanna, N., & Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 32, 24-44.

[8] Vinayagam, J., Balaswamy, C. H., &Soundararajan, K. (2019). Certain investigation on MANET security with routing and blackhole attacks detection. Procedia Computer Science, 165, 196-208.

[9] Gurung, S., & Chauhan, S. (2020). A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. Wireless Networks, 26(3), 1981-2011.

[10] Khan, A. U., Puree, R., Mohanta, B. K., &Chedup, S. (2021). Detection and prevention of blackhole attack in AODV of MANET. In IEEE International IOT, Electronics and Mechatronics Conference, pp. 1-7.

[11] Gurung, S., & Chauhan, S. (2019). Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wireless Networks, 25(3), 975-988.

[12] Gripsy, J. V., & Kanchana, K. R. (2020). Secure hybrid routing to thwart sequential attacks in mobile ad-hoc networks. Journal of Advanced Research in Dynamical & Control Systems, 12(4), 451-459.

[13] Gripsy, J. V., & Kanchana, K. R. (2022). Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System.

[14] Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: Accurate prevention and detection of jelly fish attack in MANET. IEEE Access, 6, 56954-56965.

[15] Rajendran, N., Jawahar, P. K., & Priyadarshini, R. (2019). Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. Computer Communications, 148, 129-135.

[16] Tahboush, M., &Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access, 9, 11872-11883.

[17] PremKumar, R., & Manikandan, R. (2021). Distributed hybrid sybil attack detection framework for mobile ad hoc networks. Materials Today: Proceedings, 1-4.

[18] Dhanaraj, R. K., Krishnasamy, L., Geman, O., &Izdrui, D. R. (2021). Black hole and sink hole attack detection in wireless body area networks. Computers, Materials & Continua, 68(2), 1949-1965