Received: July 8, 2022. Revised: August 25, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System

Vijigripsy Jebaseelan[1] **Kanchana Kavartty Raju[1]***

[1]*Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, India*
* Corresponding author's Email: *kanchuphd22@gmail.com*

Abstract: In mobile ad-hoc network (MANET), identification and mitigation of black and gray-hole attacks is a challenging task compared to the detection of other attacks. To solve this issue, a secure route discovery ad-hoc on-demand distance vector (SRD-AODV) protocol has been suggested, which verifies the nodes only during the path discovery. But, 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. Hence in this article, a secure route maintenance and attack detection AODV (SRMAD-AODV) protocol is proposed for identifying and defending the black and gray-hole attacks in the data transfer stage. Initially, an attack discovery system (ADS) node is decided from the connected dominating set (CDS) method based on energy and confidence score. The CDS is a robust, distinct and localized method to identify nearby linked dominating sets of nodes in a limited range in MANETs. The selected ADS nodes forward a status packet within the size of the dominating set to retrieve the entire behavioral data. ADS nodes examine gathered behavioral data and create a blacklist in which the suspected black and gray-hole nodes are added. Then, the blacklist is forwarded to the origin node to confirm the susceptibility of nodes present in the blacklist. Once the origin node authenticates the blacklist, it broadcasts a block message to all other nodes in a path for discarding blacklist nodes from the routing path. Further, this SRMAD-AODV protocol is simulated and the findings exhibit that it realizes 5.2sec of end-to-end delay (EED) and 86 % of packet delivery ratio (PDR) in contrast to the SRD-AODV protocol.

Keywords: MANET, Routing, Black-hole, Gray-hole, SRD-AODV, Connected dominated set, Attack discovery system, Status packet.

1. Introduction

MANETs are usually dynamic self-organizing platforms, with no centralized controller or resources for connectivity. If the mobile node is not under the other's coverage area, then each other nodes are decided to act as intermediate nodes for information transfer between those nodes. Also, each node travels individually and coordinates via fluctuating networks [1]. Thus, rapid fluctuations in network structure may cause many problems in routing protocol including robustness and tolerance to efficiency loss. The routing protocols are mainly split into two major types such as proactive and reactive protocols. Proactive protocols enable nodes to send packets periodically and to constantly decide the routes between any network nodes, independent of whether the routes are being used or not [2-4]. This relates to the capability that diffuses a huge amount of resources including power and throughput which is not ideal in MANET. In contrast, reactive protocols like AODV routing protocols need not require constant data transmission and only realize the route while two nodes are interacting [5].

Conversely, the routing protocols are influenced via collaborating with the suspected nodes in the system. An inadequate dynamic structure of MANET is highly susceptible to the different routing attacks [6] including black-hole, gray-hole, etc. Black-hole attacks are suspected nodes that appeared in the system in which the data forwarded or accepted are secretly rejected without notifying

the origin node. Identification and mitigation of this attack are mostly complicated due to the frequent rejection of data during transfer i.e., the nodes drop the data rather than forward it to the next node [7]. The suspected node waits for nearby nodes for initiating the route request (RREQ) packet. While the RREQ packet is accepted by the suspected node, it directly forwards the forged route reply (RREP) packet with the maximum sequence numbers. So, the origin node creates a new route to forward the data towards the target node via the suspected node and rejects the RREP packets from any other nodes. Besides, the suspected node blocks the transfer of packets to the target node. Typically, the block-hole node enters in AODV protocol by defining itself as a genuine route for the target to initiate the acceptance of packets from the genuine nodes and rejects the packets having the valued data [8-9].

Likewise, the gray-hole node forwards the data comparable to the typical nodes. But, it may selectively reject the packets without affecting their confidence score. The suspected behaviors were realized based on rejecting or broadcasting the packets from other nodes at specified intervals [10]. The black- and gray-hole attacks are also known as sequence number attacks. Many approaches have been designed and suggested to identify and mitigate these kinds of attacks in MANETs [11]. Though these approaches mitigate malicious activities, still the routing security has less efficiency.

From the perspective of security challenges in MANET, a predictive approach [12] was recommended via extending the AODV protocol to maintain the paths with the aid of sequence numbers. They used the TSN to compute the path freshness. The RREP packet was forged with a higher sequence number and lesser hop count by the suspected node for creating the bogus path. After, the packet forwarding from a certain target or specified interval was dropped randomly by the suspected node. So, the TSN of the accepted RREP was estimated via the linear regression which encounters the prior knowledge. Afterward, the estimated predicted TSN was evaluated to the actual TSN accepted from the RREP. If the RREP TSN was greater than the estimated value, then the node forwarding that RREP was denoted as a suspected node. Also, the recognized suspected node was rejected from the routing path. Or else, typical protocol operations were conducted and the interval of RREP acceptance with the TSN value was stored in a data structure. Then, the normal RREP was forwarded on the opposite route to the origin node. However, it needs to enhance efficiency by integrating the new secure routing solutions.

As a result, an SRD-AODV protocol [13] was developed via an effective authentication by the elliptic curve diffie-hellman algorithm (ECDHA). This protocol has the objective of protecting the packets and routing table to ensure maximum network security. In SRD-AODV, only the genuine nodes can participate and achieve access control via sharing the authentication keys before the routing starts. But, it authenticates the nodes only during path discovery whereas the nodes are not verified in the data transfer stage. The authentication of nodes during data transmission is essential because gray-hole broadcasts the accurate TSN during the path discovery phase, but it becomes suspected and drops the packets in the data transfer. Due to this condition, the overall network performance is decreased.

So in this article, an SRMAD-AODV protocol is designed for identifying and defending the black and gray-hole attacks during data transmission. The major contributions of this study are the following:

1. First, an ADS node is chosen by the CDS method that 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.
2. Then, ADS nodes examine the gathered behavioral data to recognize nodes as the black or gray-hole attackers and add them to the blacklist.
3. 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 have been delivered without being dropped by any malicious nodes in the route.
4. By receiving the ACK, the origin node verifies whether the received ACK packet is a legitimate forwarded by the target or a counterfeit ACK packet received from the black/gray-hole node.
5. 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 misbehavior nodes.

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

The remaining sections of this manuscript are organized as follows: Section 2 discusses the studies

related to this work. Section 3 describes the SRMAD-AODV protocol briefly and section 4 exhibits its performance. Section 5 concludes the entire study and provides further improvement.

2. Literature survey

An improved trust identification method (ITIM) [14] was proposed to maximize the likelihood of identification and mitigation of black-hole nodes in MANETs. In this method, the activities of every node were observed using different trust metrics including the relationship between the sensor nodes, social and service attribute trust and quality-of-service (QoS) metric trusts. Based on the observed activities, the suspected nodes were recognized and omitted from the routing path. But, the false alarm rate was still high.

Gray wolf trust accumulation (GWTA) method [15] has been developed to preserve and improve confidentiality in routing. First, based on the nature of gray wolf optimization (GWO), the black and gray-hole attacks were detected. Then, the route stability for information sharing was preserved by the trust schematic procedure, which forecasts every node and enhances the route stability. However, the detection rate was not high since GWO's searching ability and convergence speed were poor.

A trust-based model [16] model was developed to create a network resilient to malevolent nodes. Trust was determined by the RREQ and RREP counter for identifying the malevolent nodes. But, it needs other metrics to increase the detection rate. A novel secured and reliable technique [17] was developed to hinder the black hole attacks in MANETs using a correlation coefficient. But, its detection rate was still not effective.

The black-hole attacks detection method was implemented [18] based on the AODV protocol and recognized the black-hole attacks in the MANET based on the anomaly recognition technique and digital sign-based cryptography. However, its scalability was not effective for real-time purposes because of using a limited number of nodes and packets for analysis.

Accurate and cognitive intrusion detection system (ACIDS) [19] was designed to recognize black-hole attacks. The attributes like destination sequence number (DSN) and RREP were considered to recognize the invaders via detecting the variance of these attributes from the regular activity. However, throughput was less and packet drop was still high.

A new trust-based routing protocol called indirect trust-AODV (ITAODV) [20] was developed, which measures the node's reliability during data transfer for detecting and isolating malicious nodes from the routing path. But, its efficiency was influenced while increasing the node mobility speed.

Detection and prevention of a black hole attack (DPBHA) [21] were designed to protect and enhance the total confidentiality of the system by recognizing the blackhole attacks at an early phase of the path-finding task. It was depending on the determination of an adaptive threshold and the creation of the fake RREQ packet. But, it needs to identify and mitigate gray-hole attacks to further increase the network performance.

A reliable and secure algorithm (RSA) [22] was designed for gray-hole attack detection and prevention according to the probabilistic threshold. Initially, the validity of the nodes of a path was measured to choose a valid path. After that, the malevolent nodes in the path were identified and discarded from the network. But, the mean EED was still high.

2.1 Problem definition and research objective

From the literature survey, it is addressed that most of the existing protocols have been developed to identify either black-hole or gray-hole attacks during the route discovery stage. There are only a few unified protocols to identify both types of attacks. Also, the attacks during data transmission can degrade the transmission efficiency by dropping data packets, which affects the network throughput. So, it is necessary to identify the attacks during the data transmission stage. From this viewpoint, this study focuses on detecting and preventing black and gray-hole attacks during the data transmission stage. Also, it reduces the EED, as well as, increases the PDR and throughput for effective data transfer.

3. Proposed methodology

3.1 CDS and ADS node selection

CDS is a dominating set of subgroup nodes in the network. Each node is not essentially linked within that subgroup; yet, a minimum of one node must be a member of that subgroup of the network. The dominating set should be linked known as the CDS. The CDS consists of the minimum number of linked nodes to enclose the maximum range of the network. Similarly, the ADS set is a theory of the subgroup of the network. It is utilized to create a group of nodes depending on the node's adequate energy and confidence score within the whole network. As well, the ADS set is executed to

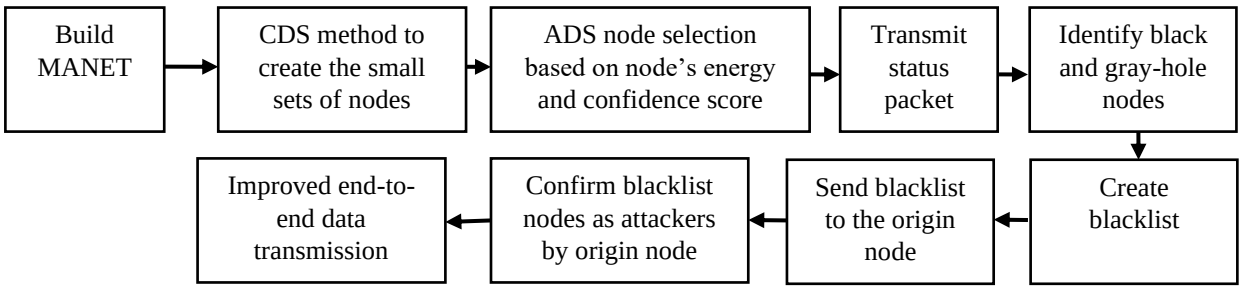

Figure. 1 Proposed architecture modelling diagram

minimize the traffic load and the routing overhead.

A confidential node with adequate energy is chosen as the ADS node for query processing. Each node under the ADS set is linked with every other. They are linked in such a manner to guarantee complete network coverage.

The CDS method is enhanced by choosing the ADS query issuing node from the ADS set. Before choosing this node, this protocol verifies the node's energy and confidence score. For a node to become confidential, each node in the ADS set should recognize its adjacent node in promiscuous mode. All nodes in the ADS set observe the activity of the adjacent node about the packet lost and this information is accumulated in their knowledge table.

3.2 Overview of SRAD -AODV routing protocol

This part explains the SRMAD-AODV routing protocol in MANET briefly. Normally, the MANET nodes consume adequate energy to create a path for data transmission. The suspected nodes transmit beacon messages regularly, resulting in a large amount of redundant traffic to increase the routing overhead. So, such nodes must be mitigated to minimize the additional routing overhead. For this purpose, this proposed protocol can integrate CDS and ADS methods to identify the suspected nodes (i.e., black and gray-hole nodes) and to minimize the routing overhead.

3.3 Scientific contribution of SRAD -AODV routing protocol

Fig. 1 shows the proposed architecture modeling diagram. The major contributions in this SRMAD-AODV routing protocol are the following:

- The CDS method is applied to create the small sets of dominating nodes and choose the nodes having adequate energy and confidence score as 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 confirming the suspected nodes and mitigating them from the routing path during data transmission.

3.4 Adversary model

Consider that black and gray-hole nodes exist in the MANET. The suspected nodes try to interrupt the network during transmission without representing their individualities. In the black-hole attacks, the suspected node transmits counterfeit data to the origin node by deceiving it into believing that it has a genuine and new path to the target. During the gray-hole attacks, the suspected node drops specified packets during the data forwarding stage. The identification of these suspected nodes is a difficult process due to their dissimilar activities. So, an adversary model is incorporated in this SRMAD-AODV protocol to recognize the different impacts of varied activities conducted by the adversary on this protocol.

3.5 Identify suspected attackers by ADS nodes

ADS query node's main objective is to create a robust security strategy against black and gray-hole nodes in MANETs. To achieve this, each ADS query node should contain acceptable energy and a confidence score. The energy value of a node N to be chosen as an ADS query node is given below:

$$\left(1-\frac{E_C(N)}{E_B(N)}\right)\times 100 > \Gamma \text{or} \left(\frac{E_C(N)}{E_T(N)}\right)\times 100 < \theta \quad (1)$$

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:

$$DC = \frac{\sum TotalPkt_i - (\sum SuccPkt_j - \sum DropPkt_j)}{\sum TotalPkt_i} \quad (2)$$

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:

$$IDC = \frac{\sum Trust\ value\ from\ adjacent\ about\ j}{Total\ amount\ of\ nodes} \quad (3)$$

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

$$Confidence\ Score\ = \frac{DC + \omega \cdot IDC}{2} \quad (4)$$

$$\text{Where } \omega = \begin{cases} 1, & N_{Untrust} = 0 \\ \frac{N_{Trust}}{N_{Untrust}} & Or\ else \end{cases} \quad (5)$$

In Eq. (5), $N_{Untrust}$ is the number of dishonest nodes and N_{Trust} is the number of honest nodes.

3.6 Status packet

Once the ADS set is obtained, such nodes transmit status packets regularly to examine the throughput, delay, routing overhead and PDR of all nodes in the network. The status packet comprises the below queries from genuine nodes:

1. The ADS node requests the genuine node: What is the sequence number?
2. The ADS node requests the genuine node: How many packets have been accepted?
3. The ADS node requests: How many packets have gone transferred?
4. The ADS node requests: How many packets have been dropped and why?

All nodes receive the status packet and respond to each query in that packet. Then, such responses from each node are transmitted to the ADS query node. In this manner, the ADS query node confirms the node's packet transfer activities regularly to differentiate the genuine and suspected nodes.

For the suspected nodes, there may be 2 criteria: (i) it either transmits counterfeit data to the ADS node to conceal its individuality, or (ii) it does not transmit any response to the ADS node and drops the status packet. As the suspected node is a fabricator node, it transmits the fabricated response and never displays its actual individuality to the ADS node. After accepting responses from each node, the ADS node verifies which node is not replying appropriately and why.

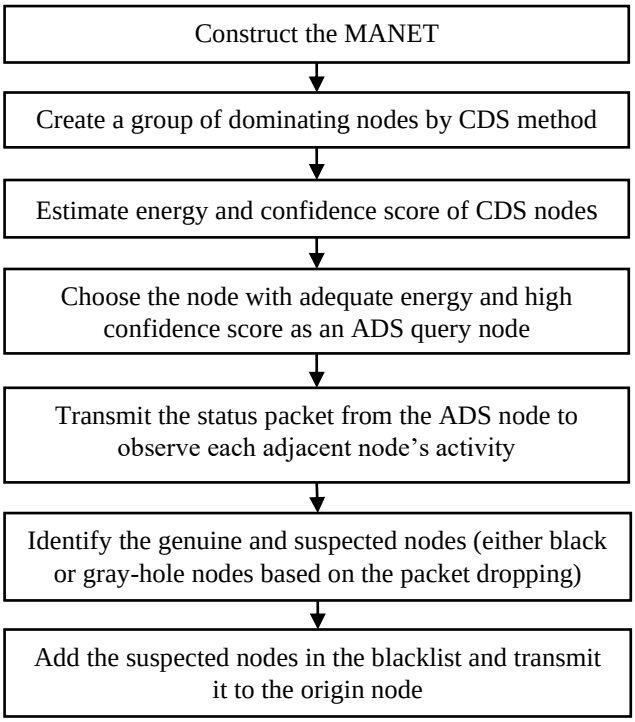

Figure. 2 ADS node selection and suspected node identification processes

When any node is not answering the queries or transmitting counterfeit responses and failing to satisfy the predefined queries without any reason for the path failure, energy or buffer size, then the ADS node announces that node as a suspected node. As well, the ADS node adds such suspected nodes to the blacklist and transmits them to the origin node for authenticating the end-to-end data transmission. Fig. 2 portrays the ADS node's complete operations.

3.7 Confirm suspected attackers by origin node

After receiving the blacklist, the origin node transmits a data packet to the target node and waits for an ACK to authenticate that the data have been accepted and there is no suspected node along the route. By receiving the ACK, the origin node verifies whether the received ACK is a valid one transmitted by the target or a counterfeit one transmitted by the suspected node. When there is an arrival of counterfeit ACK or no ACK, a nonce is combined with the ACK. The origin node transfers

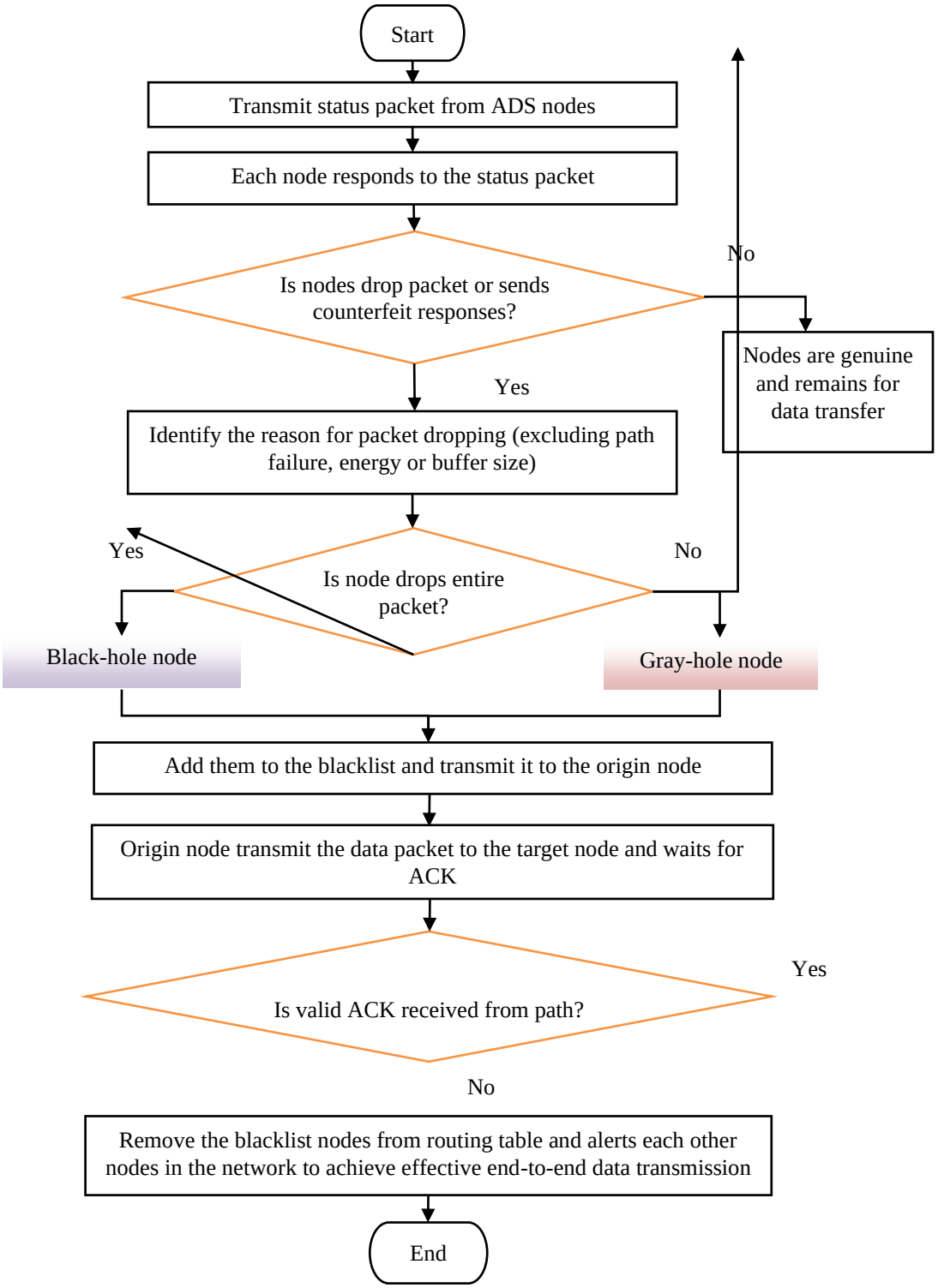

Figure. 3 Flow diagram of SRMAD-AODV routing protocol

the initial packet with a random sequence number so that any adversary (blacklist nodes) cannot detect it as the initial packet because this sequence number is utilized in ACK's nonce determination, which is applied to claim that it is a valid ACK.

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:

$$N_1 = X + IRP \tag{6}$$

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:

$$PN = N_1 - X \quad (7)$$

When the PN is a prime number, the timer is turned off; or else, it is 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:

$$N_k = X + NPN \quad (8)$$

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.

Algorithm: SRMAD-AODV protocol

Input: N number of nodes

Output: Black and gray-hole nodes

Build the MANET using N nodes;

Apply the CDS method to create the sets of dominating nodes;

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

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

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

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

if $(node\ drops\ packets)$

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

if $(node\ drops\ entire\ packet)$

Declare that node as a black-hole node;

elseif $(node\ drops\ part\ of\ the\ packet)$

Declare that node as a gray-hole node;

end if

Add the black & gray-hole nodes to the blacklist;

Transmit blacklist to the origin node from the ADS set;

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

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

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

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

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

else

Node is genuine and continues the data transmission;

end if

4. Simulation results

In this section, the SRMAD-AODV protocol is simulated using network simulator (NS2.34). Also, its efficiency is compared to the existing protocols by simulating them for black and gray-hole attacks detection: SRD-AODV [13], ITIM [14], ACIDS [19], ITAODV [20] and DPBHA [21]. This analysis is conducted according to the EED, PDR and throughput. Table 1 lists the simulation parameters.

4.1 EED

It is the interval between the initial packet forwarded from the origin and the first packet effectively reaching the target.

In Fig. 4, the EED (in sec) of SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA and ITIM protocols for an increasing amount of nodes are portrayed. The EED of SRMAD-AODV is 5.45 % decreased than the SRD-AODV, 10.34 % decreased than the ACIDS, 13.33 % decreased than the IAODV, 17.46 % decreased than the DPBHA and 21.21 % less than the ITIM protocols when 500 nodes are presented in the network so that it concludes that the SRMAD-AODV has the least

Table 1. Simulation parameters

Parameters	Range
Simulation area	1000×1000 m^2
Number of nodes	500
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

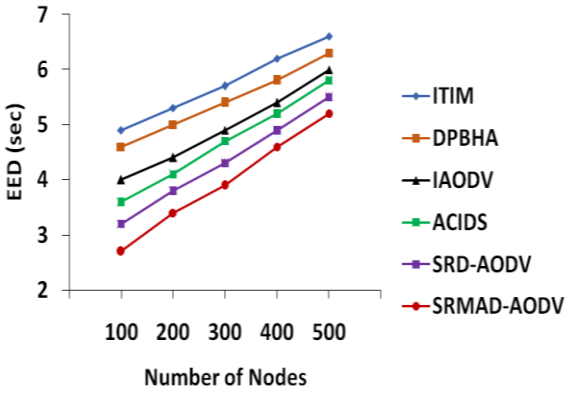

Figure. 4 EED vs. No. of nodes

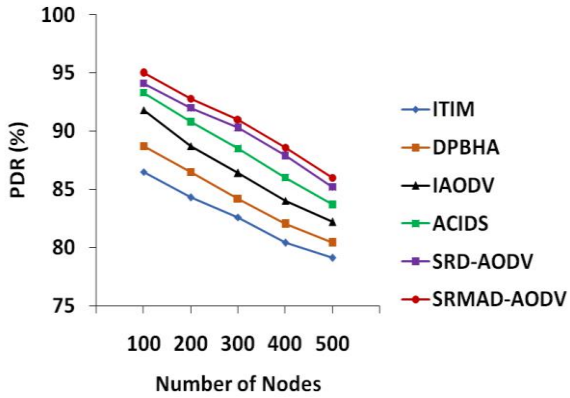

Figure. 5 PDR vs. No. of nodes

EED than the all other protocols. This is because the SRMAD-AODV reduces the packet dropping by removing the suspected nodes from the network and so there is no need of retransferring data packets to the target node. This reduces the EED of the network.

4.2 PDR

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

Fig. 5 exhibits the PDR (%) of SRMAD-AODV, SRD-AODV, ACIDS, IAODV, DPBHA and ITIM protocols under a varying number of nodes. The PDR of SRMAD-AODV is 0.94 % increased than the SRD-AODV, 2.75 % increased than the ACIDS, 4.62 % increased than the IAODV, 6.97 % increased than the DPBHA and 8.72 % increased than the ITIM protocols when considering 500 nodes so that it concludes that the SRMAD-AODV has the maximum PDR as compared to the all other protocols. This is because, after identifying the black- and gray-hole nodes with status packet queries, the data packets are easily delivered more quickly to the target node by adding them to the blacklist in a short amount of time.

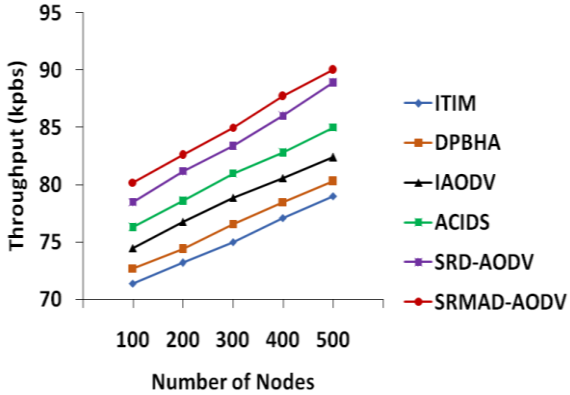

Figure. 6 Throughput vs. No. of nodes

4.3 Throughput

It is the total amount of forwarded packets within a given time.

Fig. 6 portrays the throughput (kbps) of SRMAD-AODV, ACIDS, IAODV, DPBHA and ITIM protocols for a varying number of nodes. For 500 nodes, the throughput of SRMAD-AODV is 1.24 % higher than the SRD-AODV, 5.88 % higher than the ACIDS, 9.22 % higher than the IAODV, 12.08 % higher than the DPBHA and 13.92 % higher than the ITIM protocols so that it concludes that the SRMAD-AODV has the highest throughput than the all other protocols. This is because, in SRMAD-AODV, each ADS node transmits status packets to which each node replies positively. If any node does not satisfy the pre-defined criteria, then the ADS node marks it as a suspected node and the other nodes terminate the transfer with that specific node.

According to these findings, the SRMAD-AODV protocol enhances the network efficiency in terms of EED, PDR and throughput compared to all existing protocols like SRD-AODV, ACIDS, IAODV, DPBHA and ITIM protocols. This is because all the existing protocols can prevent black and gray-hole attacks only during the route discovery phase; whereas, this proposed SRMAD-AODV protocol can mitigate black and gray-hole attacks during the data transmission phase, which results in less packet drop and high PDR.

5. Conclusion

In this article, the SRMAD-AODV protocol was designed to find and defend the black and gray-hole attacks in the data transfer stage. Originally, the CDS method was applied to create small sets of dominating nodes. The nodes having an adequate

energy and confidence score were chosen as the ADS set. The selected ADS set can transmit the status packet to each other node in the network to recognize the adjacent node activities during transmission. Based on the responses to the status packet, the ADS nodes can find the suspected node and genuine node in the network. The suspected nodes were added to the blacklist and this blacklist record was sent to the origin node. Further, the origin node transmits the data to the target and waits for an ACK to verify the data has been received by the target along the path without any blacklist nodes. If the ACK was not received, then the origin node declared that node as suspected and removed from the routing table. Moreover, the modified routing table was notified to each other node in the network to achieve end-to-end data transmission without failure. So, the data packet dropping was mitigated and the routing overhead was reduced. At last, the simulation results proved that the SRMAD-AODV protocol achieves an EED of 5.2sec, a PDR of 86 % and a throughput of 90kbps which are higher than the SRD-AODV, ACIDS, IAODV, DPBHA and ITIM routing protocols. In the future, this protocol can extend to identify and mitigate several types of attacks that exist in the MANET. Also, this protocol will implement in a few real-time MANET scenarios.

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

Conceptualization, Vijigripsy; Methodology, Kanchana; Software, Simulation, Kanchana; Writing—Original draft preparation, Kanchana; Visualization, Investigation, Supervision, Vijigripsy; Reviewing and Editing, Vijigripsy.

References

[1] J. A. A. Aldana, S. Maag, and F. Zaidi, "MANETs Interoperability: Current Trends and Open Research", In: *Proc. of 32nd IEEE International Conf. On Advanced Information Networking and Applications Workshops*, Krakow, Poland, pp. 481-87, 2018.

[2] K. Pandey and A. Swaroop, "A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid Manets Routing Protocols", *International Journal of Computer Science Issues*, Vol. 8, No. 3, pp. 432-441, 2011.

[3] M. T. Sultan and S. M. Zaki, "Evaluation of Energy Consumption of Reactive and Proactive Routing Protocols in MANET", *International Journal of Computer Networks & Communications*, Vol. 9, No. 2, pp. 29-38, 2017.

[4] N. A. M. Saudi, M. A. Arshad, A. G. Buja, A. F. M. Fadzil, and R. M. Saidi, "Mobile Ad-Hoc Network (MANET) Routing Protocols: A Performance Assessment", In: *Proc. of the Third International Conf. On Computing, Mathematics and Statistics*, Springer, Singapore, pp. 53-59, 2019.

[5] Y. Bai, Y. Mai, and N. Wang, "Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs", In: *Proc. of IEEE Wireless Telecommunications Symposium*, Chicago, IL, USA, pp. 1-5, 2017.

[6] S. K. Aluvala, R. Sekhar, and D. Vodnala, "An Empirical Study of Routing Attacks in Mobile Ad-Hoc Networks", *Procedia Computer Science*, Vol. 92, pp. 554-561, 2016.

[7] N. W. Lo and F. L. Liu "A Securing Protocol to Prevent Cooperative Black Hole Attack in MANET", *Intelligent Technologies and Engineering Systems*, Springer, New York, pp. 59-65, 2013.

[8] P. Golchha and H. Kumar, "A Survey on Black Hole Attack in MANET using AODV", In: *Proc. of IEEE International Conf. on Advances in Computing, Communication Control and Networking*, Greater Noida, India, pp. 361-365, 2018.

[9] V. K. Amatchi and R. Mukesh, "Securing Data from Black Hole Attack using AODV Routing for Mobile Ad Hoc Networks", *Advances in Computing and Information Technology*, Springer, Berlin, Heidelberg, pp. 365-373, 2013.

[10] S. U. Patil, "Gray Hole Attack Detection in MANETs", In: *Proc. of 2nd IEEE International Conf. for Convergence in Technology*, Mumbai, India, pp. 20-26, 2017.

[11] S. Dixit, K. K. Joshi, and N. Joshi, "A Review: Black Hole & Gray Hole Attack in MANET", *International Journal of Future Generation Communication and Networking*, Vol. 8, No. 4, pp. 287-294, 2015.

[12] A. M. Desai and R. H. Jhaveri, "Secure Routing in Mobile Ad Hoc Networks: A Predictive Approach", *International Journal of Information Technology*, Vol. 11, No. 2, pp. 345-356, 2019.

[13] J. V. Gripsy and K. R. Kanchana, "Secure Hybrid Routing to Thwart Sequential Attacks in Mobile Ad-Hoc Networks", *Journal of Advanced Research in Dynamical & Control Systems*, Vol. 12, No. 4, pp. 451-459, 2020.

[14] J. Manoranjini, A. Chandrasekar, and S. Jothi,

"Improved QoS and Avoidance of Black Hole Attacks in MANET using Trust Detection Framework", *Automatika*, Vol. 60, No. 3, pp. 274-284, 2019.

[15] R. Vatambeti, K. S. Supriya, and S. Sanshi, "Identifying and Detecting Black Hole and Gray Hole Attack in MANET using Gray Wolf Optimization", *International Journal of Communication Systems*, Vol. 33, No. 18, pp. 1-16, 2020.

[16] G. K. Wadhwani, S. K. Khatri, and S. K. Mutto, "Trust Framework for Attack Resilience in MANET using AODV", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 23, No. 1, pp. 209-220, 2020.

[17] M. Thebiga and R. SujiPramila, "A New Mathematical and Correlation Coefficient based Approach to Recognize and to Obstruct the Black Hole Attacks in MANETs using DSR Routing", *Wireless Personal Communications*, Vol. 114, No. 2, pp. 975-993, 2020.

[18] M. I. Talukdar, R. Hassan, M. S. Hossen, K. Ahmad, F. Qamar, and A. S. Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection using IDS and Digital Signature", *Wireless Communications and Mobile Computing*, Vol. 2021, pp. 1-13, 2021.

[19] S. Sivanesh and V. R. Dhulipala, "Accurate and Cognitive Intrusion Detection System (ACIDS): A Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks", *Mobile Networks and Applications*, Vol. 26, No. 4, pp. 1696-1704, 2021.

[20] H. Jari, A. Alzahrani, and N. Thomas, "A Novel Indirect Trust Mechanism for Addressing Black Hole Attacks in MANET", In: *Proc. of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 27-34, 2021.

[21] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J. T. Seo, "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs", *Sensors*, Vol. 22, No. 5, pp. 1-27, 2022.

[22] Y. Ebazadeh, and R. Fotohi, "A Reliable and Secure Method for Network-Layer Attack Discovery and Elimination in Mobile Ad-Hoc Networks based on a Probabilistic Threshold", *Security and Privacy*, Vol. 5, No. 1, pp. 1-18, 2022.