Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 05 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

DETECTION AND PREVENTION DOS ATTACKS IN MANET USING INTRUSION DETECTION SYSTEM AND SUPPORT VECTOR MACHINE (SVM)

[1]Zulfiqar Ali Zardari, [2]Shahzad Nasim, [3]Munaf Rashid, [4]Manthar Ali, [5]Nasrullah Dahar*

[1,2]The Begum Nusrat Bhutto Women University Sukkur

[3]Ziauddin University, Karachi

[4]Shaheed Beanazir Bhutto University, Shaheed Benazirabad

[5]Shah Abdul Latif University, Khairpur

Corresponding Author: Shahzad Nasim (shahzad.nasim@bnbwu.edu.pk)

Article Info

Abstract

The Mobile Ad hoc Network (MANET) is a collection of moveable wireless nodes. These wireless nodes relate to wireless links i.e. radio waves. MANET nodes have full freedom such as open medium for communication, dynamic topology, and without any central control. MANET possesses popularity in various applications such as military, rescue, earthquake, and disaster operations. However, the mobility and freedom of Mobile nodes creates vulnerabilities to various routing and DoS attacks in MANET. Moreover, the nodes are prone to various attacks where a malicious node drops the data packets during communication and thus, reduces the network performance. To solve the above-mentioned concerns, a malicious node detection method is proposed using Support Vector Machine (SVM)-a supervised learning approach and intrusion detection system (IDS). In this paper, we proposed a hybridized technique (IDS-SVM) for identification of the malicious nodes. In the proposed technique, the IDS node searches the data items and retrieves closest neighbor nodes within the network range using Euclidean distance. IDS nodes are considered as query points and forwards the status packet periodically to judge the behavior of other nodes. IDS-SVM is implemented with the cluster approach to avoid beacon messages to route overhead in the network. Meanwhile, intermediate nodes are associated with the IDS nodes in a specific range. Simulation results indicate that IDS-SVM achieves consistent overhead routing and network delay. Our findings could also indicate that the proposed technique (IDS-SVM) has obtained a high accuracy rate in the detection of malicious nodes, thus it is fast and efficient from the perspective of MANETs.

Keywords:

MANET, Blackhole, Gray hole, Support vector machine algorithm, IDS nodes, clusters

1. Introduction

A MANET is a distributed network of wireless nodes, which connects nodes to wireless connections to communicate with each other[1]. MANETs are self-configuring networks that don't need centralized control or base stations. Specifically, it is designed for short-range, fast, and easy communication. Unlike the traditional infrastructure, it does not require cable wires, hubs, switches, and access points [2]. In MANET, if they are in the same contact range, nodes will communicate directly. Conversely, this communication relies on intermediate nodes when the distance is enough long. For instance, communication in battlefields, disaster rescue, and environmental monitoring relies on intermediate nodes, and wired infrastructure may not be possible as well. With the rapid change in topology, structureless network, and high mobility, nodes are always free to come to be the part of the routing process and leave out the network anytime [3]. However, every node has to cooperate and communicate during the war zone, disaster management, and military operations. Whereas, only specific protocols can deliver the data packets to a particular destination. Such routing protocols are used to communicate between nodes, i.e., proactive or in a reactive manner. Conversely, these protocols are also vulnerable to various kinds of attacks, i.e., Black hole attack, gray hole attack, flooding attack[4, 5].

1.1 Classification of (DoS) Attacks

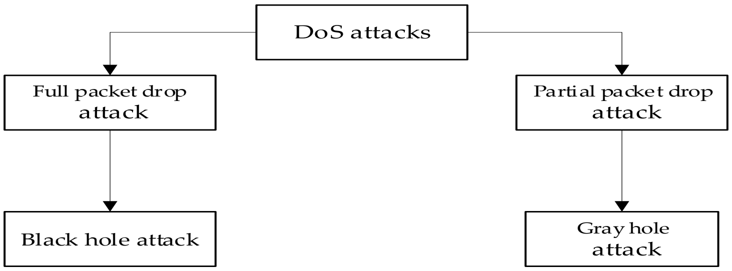

Figure.1 DoS Attacks

DoS assault is an event that decreases or eliminates the potential and intended operation of a network. DoS attacks are launched against network bandwidth or user resources to prevent authorized users from accessing their services. Figure 1 presents the classification of DoS attacks. The first assault is referred to as a full packet drop attack since the black hole drops entire packets. Gray hole attacks, on the other hand, cause certain packets to be dropped in the second attack. [7]. In this attack, a node is intelligent and assaulted by dropping infringements of the packets. During the route discovery phase, it behaves like a normal node. Suddenly, it's the behavior changed from normal to malicious and dropped selected data packets (i.e., smart gray hole node) after getting the path from the source node. Occasionally, the gray hole node possesses a valid path to the destination. However, it sends fake high sequence number routing information and intentionally drops the selective packets as an attack known as a sequence-based grey hole attack. [8, 9].

1.2 Black Hole Attack

It is a prominent attack because of the way it interferes with routing services. [10]. When the source node interacts with the target node, it sends a route request (RREQ) for route discovery. Normal nodes received the RREQ message that confirms a correct response. However, a black hole node responds rapidly without consulting the routing table to win the path from the source node. The black hole node sends an route reply (RREP) message to the source node with the highest sequence number and minimum hop count [11]. The sequence number provides the freshness of the route. Hop count indicates number of nodes between the corresponding and targeted node. The black hole node tries to inspire the source node to build the sequence number in the RREP message by creating a short path. [12]. The source node modifies its routing database after receiving this fake RREP message from the black hole node. Once the route is established, the source node transmits data packets to the black hole node, which discards all of the packets without transferring them to the destination node. [13, 14].

1.3 Gray Hole Attack

An active attack that works smartly during transmission is a gray hole attack [15]. It is challenging to recognize a gray hole node since it initially acts like a typical node before evolving into a malicious node. The two principal forms of gray hole attack are sequence-based gray hole and smart gray hole attack. The malicious node delivers a lengthy string of inaccurate routing information in the sequence-based method, with very few hops being recorded. As a result, attempts to attack the traffic. Periodically, it may have a valid route, and the path towards the target node may not be valid. Therefore, selective data packets are dropped.

Our proposed technique in this paper detects malicious nodes. Besides, intrusion detection system (IDS) and clusters (via support vector machine (SVM)) detect the malicious node's behavior by sending status packets periodically In MANET, when the nodes are free to move when the node moves away from the specified range and again join the network, this may be inflicted as the entry of malicious node. For this reason, the proposed technique uses clusters to manage the nodes. Many nodes are covered by a single cluster, and each cluster has a distinct range. The suggested IDS node was used to monitor each cluster and identify any malicious activity on the part of the other nodes. Periodically, IDS nodes broadcast the "status packet," which is made up of four inquiries pertaining to each node's state. To confirm the node's status, the packet is broadcast at a specific time interval. After receiving that packet from IDS node, genuine nodes normally replies without any ambiguity, whereas malicious node sends a fake reply. Consequently, IDS nodes can detect that malevolent (attacker) node. IDS node broadcast a blocked message when the node is marked as malicious in its cluster and information of malicious node is shared with remaining clusters.

1.4 Motivation and Contribution

The existing literature studies incorporate machine learning algorithms in combination with IDS in MANET were limited by our proposed technique (IDS-SVM). Specifically, the SVM algorithm and IDS in our proposed technique (IDS-SVM) stimulates network performances and recognizes nodes with malevolent behavior using a supervised learning algorithm in MANET. Besides, the proposed technique (IDS-SVM) is implemented using the clusters to avoid beacon messages and routing overhead. Additionally, the IDS node finds the data items and retrieves nearest neighbor nodes within the network range using Euclidean distance. IDS nodes are assumed as query points and allow forwarding the status packet intermittently to judge the behavior of other nodes. Simultaneously, intermediate nodes are related to IDS nodes in a specific range. Whereas, IDS finds the closest nodes with nearby distance and organized them into groups called clusters. Further, the proposed technique also identifies malevolent nodes by their behavior and sends the status packet in MANET. Our findings could entail high accuracy rate detection of malicious nodes by a single status packet even when there is a movement of nodes. In this paper, we present the following contributions:

- The proposed technique IDS-SVM.
- The proposed technique (IDS-SVM) detects a malicious node using supervised learning (SVM) and IDS.
- The proposed technique (IDS-SVM) identifies the malicious nodes and their behavior by sending the status packet in MANET.
- The proposed technique (IDS-SVM) prompted the clusters-based approach to avoid extra messages and to be routed in the network which causes high overhead.
- The proposed technique (IDS-SVM) gained high accuracy of rate detection, which proves that it is a fast and efficient technique as compared to other techniques in MANET.

The rest of the paper is arranged in five sections. The second section presents the existing solutions and limitations. The third section explains the proposed technique' methodology, deployment of IDS nodes, and status packet questions. The fourth section is about the network simulation environment in NS-2 along with results discussion. In the final section, concluding remarks of the paper is presented.

2. Background and Related Work

The primary objective of a safe wireless network is to keep data transmission safe and successful between two endpoints. A safety mechanism that can render the network resilient against multiple assaults, which is essential for the network to perform effectively. Usually, attacks exploited MANETs over the previous couple of years. To defend against such attacks, possible countermeasures with various vulnerabilities were suggested. Existing literature in this regard provide mechanisms, solutions, and algorithms for mitigation, detection, and isolation of various black hole attack version. In contrast, a discussion on current state-of-the-art mechanisms for detecting packet drop attack is presented, as follows:

2.1 Cryptography Based Scheme

Encryption is a highly secured approach against attacks on MANETs (E-HSAM) [16] involves the injection of dummy chunks in data to ensure integrity, while attack detection is done through watchdog encountered at every intermediate node [17]. Self-organized public key infrastructure PKI [18]prevents attack through authentication using some designated nodes to ensure the reliability of paths. Triangular encryption [19] uses symmetric key sharing through routing packets to ensure the authentication of routes, thus avoids attacks.

2.2 Threshold Based Schemes

Adaptive mechanism [20], cumulative sum (CUSUM) [21], mitigating black hole effects through detection and prevention MBDP-AODV[6], and cluster analysis method [22], are the schemes that monitor the difference between sequence numbers of two packets against the threshold. Bait Detection mechanism [23], CBDS [24], and detection of collaborative black hole attack (D-CBH) [25], which incorporates the DSR protocol and adjacent node as a bait location to detect as an attacking node and analyzes the RREP packet's intermediate nodes. Game-theoretic [26] mechanism uses the pay-off function for communication that could be minimized for its betterment. Moreover, it uses a threshold value when a node is found misbehaved, hence, it is marked as Blackhole. Localized secure architecture for MANET (LSAM). Neighborhood route monitoring table NRMT [27] uses special monitoring nodes for the detection of malicious nodes with their forwarding behavior. On the other hand, NRMT [28] monitors the time interval between RREQ and RREP packet, and the originator of the RREP packet is marked as a black hole when the time interval is found to be below a threshold. Dual security method [29] deploys promiscuous mode for identification of misbehaving nodes, while Enhanced Temporal Windowing (ETW) [30] manipulates same with cross layer collaboration monitoring RTS/CTS ratio against a threshold value.

2.3 Trust-Based Schemes

AMDMM[31] trust-based scheme involves an equation that increases the trust gradually as the behavior is good, and decreased the trust substantially in case of misbehavior. DATEA [32] performs future prediction of the trust-based scheme using current forwarding performance is experienced by a node for another node. FrAODV [33] mechanism uses the concept of a friend node whose presence in a path makes the route more trustable by a particular source. GTRTMS[34] employs a promiscuous facility through which attacking nodes are detected, followed by an update in trust value and its sharing among the neighborhood. Bedsides, OBTRP [35] nodes maintain a separate list for fair, Blackhole, and suspected nodes to monitor and update their trust values accordingly. Opinion based trust [36] uses suggestions from the other network nodes to check whether the node is malicious or not. However, schemes such as Re-TEAODV[37], trusted AODV [38], and TBDSR [39] update trust using PDR only, and their residual energy is also considered during route establishment. Trust-based detection (RTBD) [40] updates the trust via residual energy, size of the queue, and data packet count, as they follow the recommendations from other network nodes. Additionally, TRUCE[41] is a preventive measure in which threshold trust, friend index, reputation index, confidence index, and threshold TRUCE value have been reported for reliability in the route formation. trust-based QoS routing algorithm (TQR) [42] provides a path based scheme on different QoS [43]. For instance, trust and energy-based algorithms [44] uses PDR and residual energy for trust updates inflicting the detection process lightweight. Whereas, Trust-based Source Routing protocol (TSR), TSR [45] TeAOMDV [46] involves the fuzzy calculation of trust for accurate behavior representation.

2.4 Acknowledgment Based Scheme

A3ACK [47] employs three adaptive acknowledgment models depending upon the throughput of the network. It uses end-to-end acknowledgment, two/three-hop acknowledgment as per network requirements. On the other hand, EAACK[48] employs the detection of an attack and uses acknowledgment packets for assuring secure transmission. It uses MRA mode to identify whether a suspected node is malicious or not. NACK [49]uses a novel two-hop acknowledgment packet for ensuring integrated delivery of the packet.

2.5 Routing Based Scheme

AODV control packet [50] uses an additional packet along with cross-layer validation ensuring a secure path formation. CDSM [51] embeds a single byte with each data packet to be processed by a designated intermediate hop, and thus ensures the reliability of the route formed. the collaborative routing protocol (CRP) [52] is being utilized the cryptography both at hop-to-hop and end-to-end level. DEBH [53] have employed the use of a control packet for analysis of route reliability and in the detection of attack as well. Extended data routing information (EDRI) [54] makes the use of a random number for validation of the reliability of the path and detection of attacking nodes. improved extended data routing information (I-EDRI) [55] follows the strategy of a next-hop neighbor, which monitors the variation in the packet sent to the node and then packet forwarded by that node to identify the source of the attack. Similarly, modified AODV [56] adds a packet to standard AODV and verifies the respondent of the RREQ packet. MEDRI [57] considers a routing table involving additional fields for the detection of malicious nodes. NHBADI [58], co-operative mechanism[59], and DBA-DSR [60] make use of fake RREQ packet in route formation with a non-existing destination, and thus sender of RREP packet for that fake RREQ packet is marked as malicious. Receive reply method [61], and EMAODV [62] are pre-RREP signal to analyze the amount of the RREP packet sequence at the source node for detecting the attack.

2.6 Cross-Layer Collaboration Based Scheme

Multiclass IDS [63] performs detection through training, validation, and actual execution of the detection process incurring isolation of a node from the rest of the network followed by the collection of data through the MAC sublayer. HBDADCS [64] and CARRADS [65] also consider the data collected by MAC and the routing layer is matched against a threshold for detection of malicious behavior.

2.7 Miscellaneous Schemes

There are several detection and prevention schemes involved: 1) anomaly-based detection, 2) overhearing scheme, and 3) logical inference. For instance, a modular anomaly detector [66] performed an anomaly detection scheme at both local and global levels using DRI table if the PDR comes to a specific threshold level. Besides, local detection is used for finding malicious nodes that are not so far participating in routing actively. Aumann agreement theorem [67] employs an election procedure; whether to decide the node under suspicion is attacking or not. Bernoulli Bayesian model [68] performs a classification of nodes based on behavior and data collection using Markov's chain rule enabling accurate detection of the attacking node. Collaborative Bayesian Watchdog [69] applies Bayesian filters for analysis and inference of any variant of black hole attack through a notion of trust. CoCoWa [70], IBFWA[71], I-Watchdog [72] make use of overhearing with the previous hop for the analysis of forwarding activities and detection unless the forwarding is not done frequently. TRACEROUTE mechanism also deploys anomaly detection packets and interludes by Cooperation breaking; labeling one of the co-operation nodes [73] and detect the source of co-operative Blackhole attack as well.

2.8 Research Gaps

The following above mention several schemes related to various detection and mitigation for malicious nodes and its variants. Several research gaps have been identified and targeted to validate the attack mitigation process accurately and impactful. These research gaps are examined in this proposed works as follows:-

- The mechanisms of the gray hole attack fail to detect every form of selective packet drop for mitigation.
- Most of the mechanisms postulate high routing overheads and introduce packets are broadcasted globally, particularly for trust recommendation, thus decreases the overall performance of the network.
- Trust-based mechanism only makes use of packet delivery ratio for calculation of trust value, which creates room for selfish behavior of fair nodes rendering high trust value but low energy and high mobility.
- The mechanisms do not accurately perform the interlude of co-operation and detection of co-operative attacks which may involve three or more nodes.
- The detection procedure is complex that may sharply drain out the battery of the nodes.

3. Proposed Methodology

3.1 Intrusion Detection System (IDS)

The proposed methodology works in a step by step working mechanism of the intrusion detection system (IDS) as depicted in Figure 2. The entire IDS process is based on IDS nodes which provide a strong detection mechanism of malicious nodes. IDS nodes detect maliciously, when it sends status packets, it checks whether the node inside the cluster range is legitimate or malicious. A node is misbehaving such as dropping data packets, partial or drop limited data packets when communicating resulting IDS node transmits a block message, and notifies the malicious nodes. IDS's primary aim is to identify the attacker node, besides the nodes in a wireless network are communicating simultaneously, hence the identification of malicious node(s) is challenging.

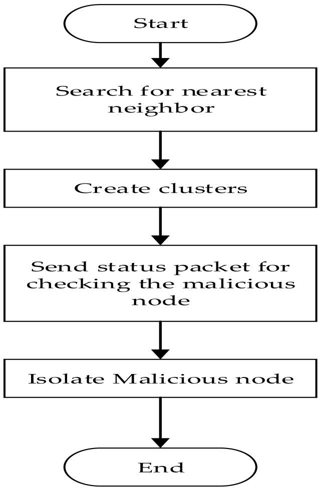
Start
Search for nearest neighbor
Create clusters
Send status packet for checking the malicious node
Isolate Malicious node
End

Figure.2 Flowchart of IDS Nodes

3.2 Euclidean Distance Using Nearest Neighbor Nodes

Occasionally, the source node near/far from form destination node requires the intermediate node to communicate as the nodes are scattered and moving randomly. Euclidean distance is used in the proposed technique to find the nearest neighboring nodes in the network, which may appear near the query point. A major concern is a distance from the query point to the intermediate nodes. By doing so, we calculate the distance between the query point and neighbor node using the Euclidean distance (x, y) function as follows:

$$\textbf{Euclidean Distance} = \sqrt{(x1 - x2)^2 + (y1 - y2)^2}$$

Where x and y are the nodes, x1, x2, and y1, y2 are coordinates of the given nodes. In MANET, it is necessary to minimize the traffic load due to the limited power and bandwidth of nodes. Periodic messages sent by the nodes in the whole network creates a huge amount of unnecessary traffic. Thus a suitable method is required to overcome this issue. The proposed technique uses a supervised learning approach and it has been used to search the k nearest neighbor node from the given query point. Additionally, IDS needs data items near to their locations in the proposed technique by using the SVM algorithm. To ease this process of finding out the distance of a node from a query point, this process can be fastened with the help of the Euclidean distance equation. When the distance is known to IDS nodes, it creates the clusters of normal nodes near to the query point. For instance, Figure 3 shows the nearest neighbor node using the SVM algorithm in MANET, wherein a node (army officer) acquires the items to its closest data (e.g., information about injured soldiers) from the current location in a battlefield situation. If the query node requested; it receives all the information objects from the entire network and there may be a great deal of unnecessary traffic. A user can search for nodes efficiently when they are arranged in a group. Therefore, effective searching of data items can reduce traffic and searching time. In the SVM algorithm, the query requested node defines its location, and it is essential for the query requested node to measure the distance of intermediate nodes from its query point within the cluster range. The advantage of using cluster is the broadcasted message will remain within-cluster range so that congested traffic can be avoided.

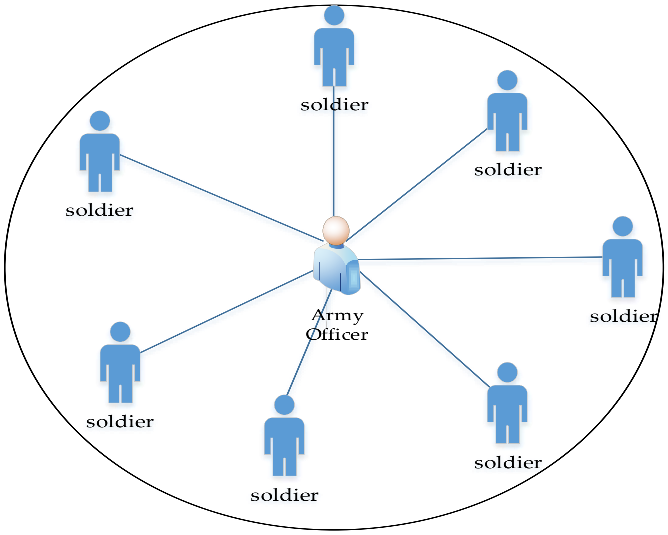

Figure.3 SVM and k-Nearest Neighbor in One Cluster

3.3 SVM and k-Nearest Neighbor

In our proposed technique, the k-nearest neighbor algorithm classifier is used in MANET to identify the attacker node. In any type of data set, it is highly useful in the prediction of changing behavior. Since SVM is also extremely helpful for anticipating assaults and vulnerabilities. With the use of an SVM classifier, the nodes cannot alter the behavior. When there is any change in the behavior, it will be notified instantly, and that node will leave the routing route. When status packet records are stored in the routing table of the corresponding nodes. KNN and SVM classify the data based on the behavior of the nodes i.e. the answers provide to by the nodes in the network.

3.4 Status Packet

To determine whether every node in the cluster is doing well when it comes to forwarding or dropping data packets during transmission, the cluster analyzes the nodes' performance. Communication is suspended when a malicious node is present between the source and the destination nodes, which is an undesired situation. To overcome this problem, IDS nodes broadcast the status packet often within their cluster range for a set period of time. The IDS node reviews the responses when they are received from a separate cluster node and makes a decision based on them. A gray hole node is very intelligent, demonstrates true performance in the routing process, and sends the right sequence number, while a black hole node sends a high sequence number and doesn't send data packets to the intermediate nodes. It drops partial or selective data packets during communication after receiving them from the source nodes. The IDS node indicates if a node is a black hole or gray hole node after verifying responses using responses from any node and then failing to respond to even one question.

Figure.4 demonstrates the architecture system flowchart of the proposed work. Initially, every node broadcasting the status packet periodically within the cluster range in the network area using IDS nodes. When the status packet receives legitimate information, all the nodes receive this packet and proceed genuinely. At the same time, the malicious node receives the status packet as abnormal behavior or provides fake routing information to the monitoring nodes of IDS. This kind of behavior is associated with the black hole node if a node sends a huge sequence, number, and drops all data packets. This kind of behavior is associated with the gray hole when a node provides an average non-high sequence number and selective data packets are dropped. The number of data packets received and discarded during communication is crucial in this case. It is evident from node behavior that malicious nodes give misleading information. The suggested technique addresses the assertion made by a rogue node that data packets are discarded because of traffic congestion or queue size. Generally speaking, each node in the network has the same traffic load in comparison to other nodes. Because each malicious node has the same traffic load, it is clear that the malicious node is a fabricator with the intention of dropping the data packets. All communication types from that specific node are rejected by the IDS node's block message, which is composed of the malicious node ID once the node has been confirmed to be malicious.

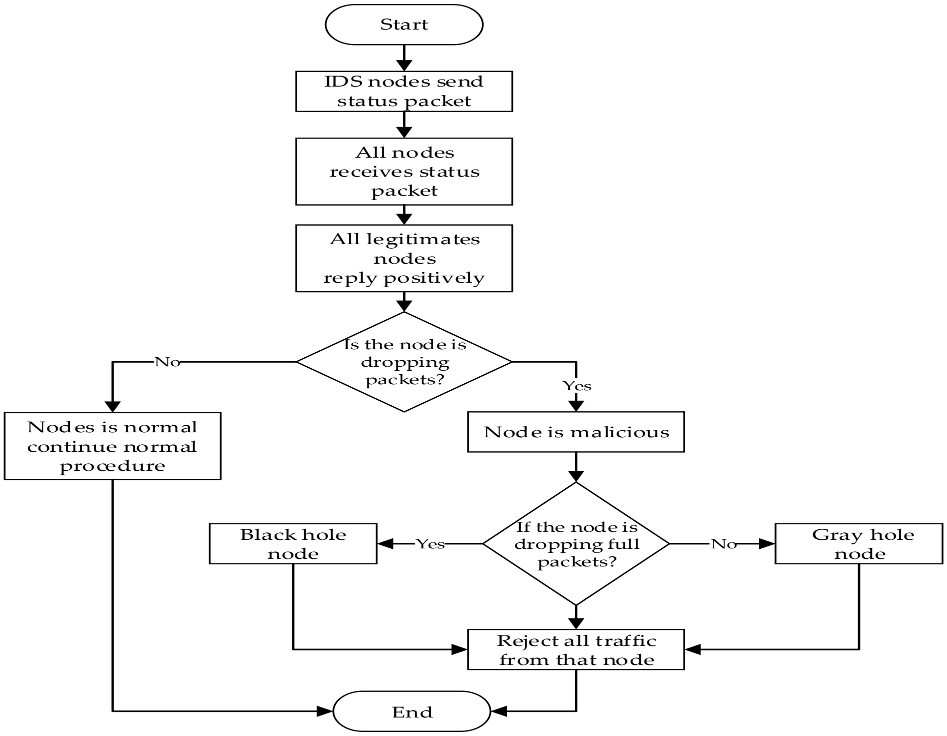
Start
IDS nodes send status packet
All nodes receives status packet
All legitimates nodes reply positively
Is the node is dropping packets?
No
Yes
Nodes is normal continue normal procedure
Node is malicious
If the node is dropping full packets?
Yes
No
Black hole node
Gray hole node
Reject all traffic from that node
End

Figure.4 Proposed Technique Flowchart

1. Experiment and Analysis

Results experiments in our proposed technique are simulated to evaluate network performance in the NS-2 open-source network simulator. In the simulation, IEEE 802.11b of the MAC layer is used. Network simulation contains several 09 IDS fixed nodes, and 100 normal nodes are deployed. The network size is 1000×1000 m, simulation time is 1000s.

Table 1. Simulation Parameters

Parameters	Value
Network Simulator	NS-2(ver.2.34)
Network area	1000× 1000 m
Normal nodes	50
IDS nodes	09
Protocol	AODV
Simulation time	1000s
Traffic type	CBR
Packet size	512bytes
Nodes mobility (varying)	5-35m/s
Range of the Transmission	250m
Pause time	5-20s

The source node sends a route request RREQ for route discovery to the destination node via intermediary nodes since it initially lacks a communication route. The malicious node uses this RREQ to determine whether the node is a gray hole or a black hole. Route reply RREP asserts that a route is legitimate.

4.1 Packet Delivery Ratio Under Dense Network

Figure 5 shows the result of the packet delivery ratio of the proposed technique and simple AODV with & without attack through the dense network, i.e., the number of nodes up to 200. Because the attacker node misses data packets during communication, the PDR of an AODV attack is extremely low. Because there isn't a hostile node in the network, the PDR of AODV without attack is extremely high. Furthermore, the suggested technique's PDR is lower than basic AODV and greater than AODV with assault. This demonstrates how the status packet's quick identification of a rogue node raises PDR. Nevertheless, PDR was reduced by either a rogue node or a link failure, where the malicious node is near the source node and transmits false information to it faster.

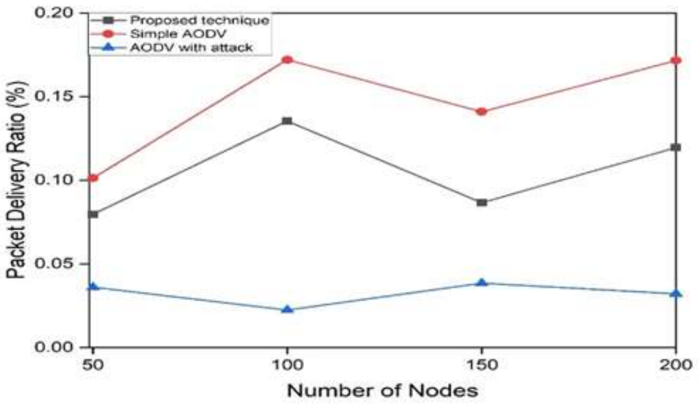

Figure.5 Packet Delivery Ratio Under Dense Network

4.2 Throughput Under Dense Network

Figure 6 shows the result of the throughput of the proposed technique and simple AODV with & without attack by using the dense network, i.e., the number of nodes is up to 200. When an attack occurs, a malicious node disrupts communication, resulting in a reduced throughput of AODV. On the other hand, since no malicious nodes are detected and nodes are free to communicate, the throughput of AODV without attack is great. In a similar vein, the suggested technique's throughput is lower than plain AODV and superior to AODV with attack. The suggested method's throughput is reduced, nevertheless, either when the malicious node drops data packets or when the link fails during communication.

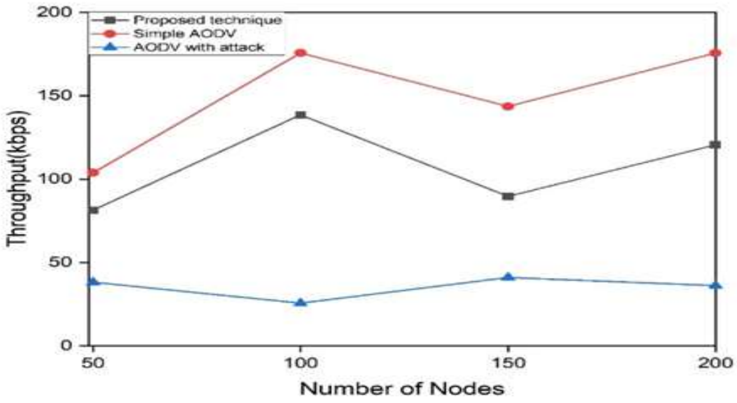

Figure.6 Throughput Under Dense Network

4.3 Average Delay Under Dense Network

Figure 7 displays the average delay of the suggested method and basic AODV with and without attack via the dense network, which has up to 200 nodes. AODV has a low latency when an attack happens. As a result, data packets cannot arrive at their destination node in a timely manner. Both the suggested method and simple AODV are outperformed by AODV without attack. While the suggested technique is less than the AODV under assault and better than simple AODV, the attacker node is not disturbed.

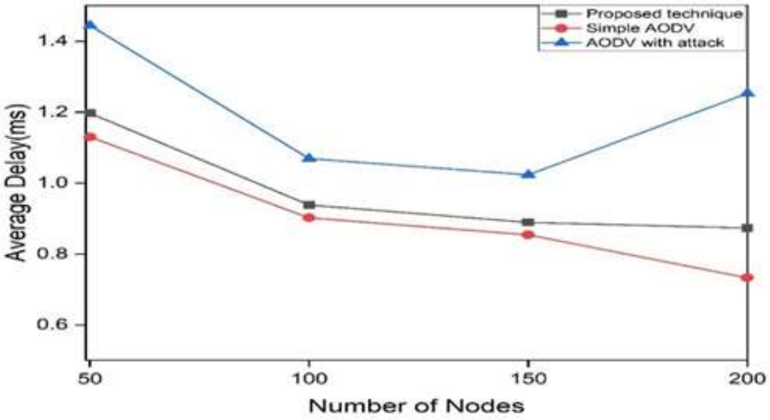

Figure. 7 Average Delay Under Dense Network

4.4 Packet Delivery Ratio (PDR) Under Malicious Nodes

Figure 8 shows the result of the PDR of the proposed technique and simple AODV with & without attack by using several malicious nodes. As the number of malicious nodes increases, the PDR of AODV under assault falls until it reaches zero. On the other hand, PDR is stable in the network since the malicious nodes have no effect on AODV. PDR is initially higher in the suggested technique, but it decreases as the number of nodes increases over time. This occurs when malicious nodes discard some packets when the query reaches the nodes at that moment. The suggested method can successfully identify the malicious nodes even while the malicious node drops data packets and PDR remains consistent.

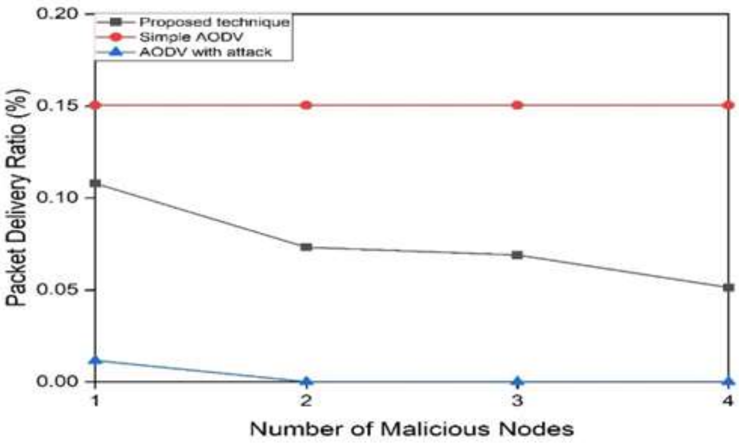

Figure.8 Packet Delivery Ratio Under Malicious Nodes

4.5 Throughput Under Malicious Nodes

Figure 9 shows the result of the throughput of the proposed technique and simple AODV with & without attack by using several malicious nodes. The PDR of the AODV under attack decreases until it hits zero as the number of malicious nodes rises. However, since the malicious nodes have no influence on AODV, PDR remains steady in the network. PDR is initially higher in the suggested technique, but it decreases as the number of nodes increases over time. This occurs when malicious nodes discard some packets when the query reaches the nodes at that moment. The suggested method can successfully identify the malicious nodes even while the malicious node drops data packets and PDR remains consistent.

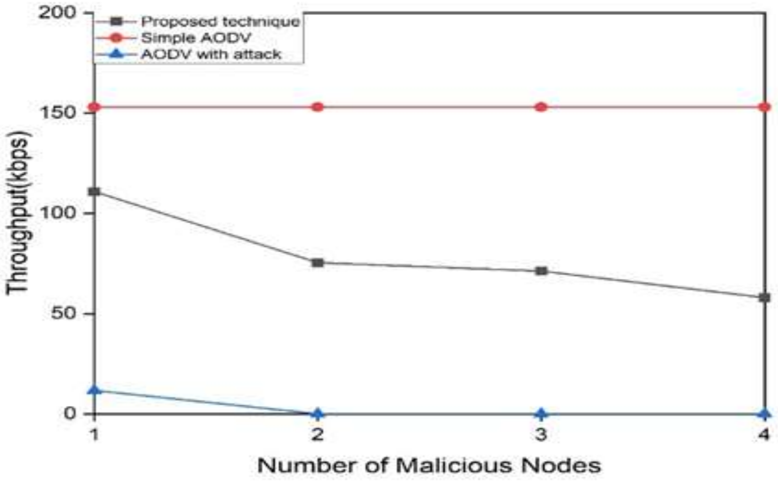

Figure. 9 Throughput Under Malicious Nodes

4.6 Average Delay Under Malicious Nodes

Figure 10 shows the result of the average delay of the proposed technique and simple AODV with & without an attack of malicious nodes. When hostile nodes infect the source and destination nodes, data packets are lost, resulting in a large latency in AODV attacks. Both the suggested method and simple AODV are outperformed by AODV without attack. This suggests that there are no malevolent nodes situated in between the network pathways. In contrast, the suggested method is less than AODV with an attack and superior to plain AODV. There aren't many hostile nodes on the route to the destination since the malicious nodes are good at detecting the status packet.

Figure. 10 Average Delay Under Malicious Nodes

5. Conclusion

To the best of our knowledge, we present the proposed technique (IDS-SVM), which investigates the malicious nodes based on IDS using a supervised learning approach via the SVM algorithm. Additionally, IDS obtains nearest neighbor nodes and forwards the status packet periodically to check the behavior of other nodes as well. The proposed technique (IDS-SVM) is implemented with the cluster approach to avoid beacon messages to route overhead. It is considered a key activity to avoid the failure of the network to identify and isolate any Dos attack in the network. Also, an intelligent detection and isolation technique is in the construction and development of any Dos attack which combats protocols and methods. The proposed techniques (IDS-VSM) uses a status packet query to enhance Dos attack detection ability while protecting the performance metrics. In prospects, we further strive to improve the proposed technique using PDR to reduce the average delay as well in the network.

Reference

1. Ali Zardari, Z., et al., A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs. Future Internet, 2019. 11(3): p. 61.

2. Pathan, M., et al., An efficient trust-based scheme for secure and quality of service routing in MANETs. Future Internet, 2018. 10(2): p. 16.

3. Pathan, M.S., et al., An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2019. 10(1): p. 243-251.

4. Gupta, P., et al. Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET. 2019. Singapore: Springer Singapore.

5. Yasin, A. and M. Abu Zant, Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018. 2018: p. 10.

6. Gurung, S. and S. Chauhan, A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks, 2018: p. 1-15.

7. Gurung, S. and S. Chauhan, A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 2018. 24(2): p. 565-579.

8. Gurung, S. and S. Chauhan, Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. Wireless Networks, 2019. 25(3): p. 975-988.

9. Gurung, S. and S. Chauhan, A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Networks, 2019. 25(4): p. 1685-1695.

10. Merlin, R.T. and R. Ravi, Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Personal Communications, 2019. 104(4): p. 1599-1636.

11. Hammamouche, A., et al., Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of information security and applications, 2018. 43: p. 12-20.

12. Khamayseh, Y.M., S.A. Aljawarneh, and A.E. Asaad, Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. Sustainable Computing: Informatics and Systems, 2018. 18: p. 90-100.

13. Satav, P.R., P.M. Jawandhiya, and V.M. Thakare. Secure Route Selection Mechanism in the Presence of Black Hole Attack with AOMDV Routing Algorithm. in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). 2018.

14. Tiruvakadu, D.S.K. and V. Pallapa, Honeypot Based Black-Hole Attack Confirmation in a MANET. International Journal of Wireless Information Networks, 2018. 25(4): p. 434-448.

15. Sharma, R., Gray-hole attack in mobile ad hoc networks: a survey. IJCSIT) International Journal of Computer Science and Information Technologies, 2016. 7(3): p. 1457-1460.

16. Obaidat, M.S., et al., A cryptography-based protocol against packet dropping and message tampering attacks on mobile ad hoc networks. Security and Communication Networks, 2014. 7(2): p. 376-384.

17. Khanna, N. and M. Sachdeva, A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 2019. 32: p. 24-44.

18. Mary Anita, E. and V. Vasudevan, Prevention of Black Hole Attack in Multicast Routing Protocols for Mobile Ad-Hoc Networks Using a Self-Organized Public Key Infrastructure. Information Security Journal: A Global Perspective, 2009. 18(5): p. 248-256.

19. Chatterjee, N. and J.K. Mandal, Detection of blackhole behaviour using triangular encryption in NS2. Procedia Technology, 2013. 10: p. 524-529.

20. Kumar, V. and R. Kumar, An adaptive approach for detection of blackhole attack in mobile ad hoc network. Procedia Computer Science, 2015. 48: p. 472-479.

21. Panos, C., et al., Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. Computer Networks, 2017. 113: p. 94-110.

22. Shim, W., G. Kim, and S. Kim, A distributed sinkhole detection method using cluster analysis. Expert Systems with Applications, 2010. 37(12): p. 8486-8491.

23. Jhaveri, R.H. and N.M. Patel, A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wireless Networks, 2015. 21(8): p. 2781-2798.

24. Chang, J.-M., et al., Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE systems journal, 2014. 9(1): p. 65-75.

25. Arathy, K. and C. Sminesh, A novel approach for detection of single and collaborative black hole attacks in MANET. Procedia Technology, 2016. 25: p. 264-271.

26. Das, D., K. Majumder, and A. Dasgupta, Selfish node detection and low cost data transmission in MANET using game theory. Procedia Computer Science, 2015. 54: p. 92-101.

27. Poongodi, T. and M. Karthikeyan, Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. Wireless Personal Communications, 2016. 90(2): p. 1039-1050.

28. Arunmozhi, S. and Y. Venkataramani, Black hole attack detection and performance improvement in mobile ad-hoc network. Information Security Journal: A Global Perspective, 2012. 21(3): p. 150-158.

29. Patel, A.D. and K. Chawda, Dual security against grayhole attack in MANETs, in Intelligent computing, communication and devices. 2015, Springer. p. 33-37.

30. Sánchez-Casado, L., et al., A model of data forwarding in MANETs for lightweight detection of malicious packet dropping. computer networks, 2015. 87: p. 44-58.

31. Vijayakumar, A. and K. Selvamani, Reputed packet delivery using efficient audit misbehaviour detection and monitoring method in mobile ad hoc networks. Procedia Computer Science, 2015. 48: p. 489-496.

32. Subramaniyan, S., W. Johnson, and K. Subramaniyan, A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. EURASIP Journal on Wireless Communications and Networking, 2014. 2014(1): p. 205.

33. PravinRenold, A. and R. Parthasarathy, Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks. ICACCI. 12: p. 3-5.

34. Movahedi, Z. and Z. Hosseini, A green trust-distortion resistant trust management scheme on mobile ad hoc networks. International Journal of Communication Systems, 2017. 30(16): p. e3331.

35. Garg, K. and M. Misra. Misbehaving nodes detection through opinion based trust evaluation model in MANETs. in Proceedings of the International Conference & Workshop on Emerging Trends in Technology. 2011. ACM.

36. Hinge, R. and J. Dubey. Opinion based trusted AODV routing protocol for MANET. in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. 2016. ACM.

37. Sethuraman, P. and N. Kannan, Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. Wireless Networks, 2017. 23(7): p. 2227-2237.

38. Zhao, D., Z. Ma, and D. Zhang. A distributed and adaptive trust evaluation algorithm for MANET. in Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks. 2016. ACM.

39. Mohanapriya, M. and I. Krishnamurthi, Trust based DSR routing protocol for mitigating cooperative black hole attacks in ad hoc networks. Arabian Journal for Science and Engineering, 2014. 39(3): p. 1825-1833.

40. Eissa, T., et al., Trust-based routing mechanism in MANET: Design and implementation. Mobile Networks and Applications, 2013. 18(5): p. 666-677.

41. Saminathan, R. and K. Selvakumar, TRUCE–An Adaptive Trust Management Algorithm Over MANET for Service-Based Mobile Computing Environments. Information Security Journal: A Global Perspective, 2011. 20(4-5): p. 173-184.

42. Wang, B., X. Chen, and W. Chang, A light-weight trust-based QoS routing algorithm for ad hoc networks. Pervasive and Mobile Computing, 2014. 13: p. 164-180.

43. Mandhare, V., V. Thool, and R. Manthalkar, A novel approach to improve quality of service in MANET using cache update scheme for on-demand protocol. International Journal of Communication Networks and Distributed Systems, 2017. 18(3-4): p. 353-370.

44. Venkanna, U., J.K. Agarwal, and R.L. Velusamy, A cooperative routing for MANET based on distributed trust and energy management. Wireless Personal Communications, 2015. 81(3): p. 961-979.

45. Xia, H., et al., Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Networks, 2013. 11(7): p. 2096-2114.

46. Xia, H., et al., Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks. Journal of Network and Computer Applications, 2016. 62: p. 112-127.

47. Basabaa, A., T. Sheltami, and E. Shakshuki, Implementation of A3ACKs intrusion detection system under various mobility speeds. Procedia Computer Science, 2014. 32: p. 571-578.

48. Shakshuki, E.M., N. Kang, and T.R. Sheltami, EAACK—a secure intrusion-detection system for MANETs. IEEE transactions on industrial electronics, 2012. 60(3): p. 1089-1098.

49. Sun, H.-M., C.-H. Chen, and Y.-F. Ku, A novel acknowledgment-based approach against collude attacks in MANET. Expert systems with Applications, 2012. 39(9): p. 7968-7975.

50. Dhaka, A., A. Nandal, and R.S. Dhaka, Gray and black hole attack identification using control packets in MANETs. Procedia Computer Science, 2015. 54: p. 83-91.

51. Ahmad, S.J., et al. Detection of black hole attack using code division security method. in Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. 2015. Springer.

52. Sun, H.-M., et al., A collaborative routing protocol against routing disruptions in MANETs. Personal and ubiquitous computing, 2013. 17(5): p. 865-874.

53. Dorri, A., S. Vaseghi, and O. Gharib, DEBH: detecting and eliminating black holes in mobile ad hoc network. Wireless Networks, 2018. 24(8): p. 2943-2955.

54. Dorri, A., An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Wireless Networks, 2017. 23(6): p. 1767-1778.

55. Patel, A.D., R.H. Jhaveri, and S.N. Shah, I-EDRI Scheme to Mitigate Grayhole Attack in MANETs, in Intelligent Computing, Communication and Devices. 2015, Springer. p. 39-43.

56. Chavan, A., D. Kurule, and P. Dere, Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack. Procedia Computer Science, 2016. 79: p. 835-844.

57. Hiremani, V.A. and M.M. Jadhao. Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. in 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE). 2013. IEEE.

58. Babu, M.R. and G. Usha, A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET. Wireless Personal Communications, 2016. 90(2): p. 831-845.

59. Kim, G., Y. Han, and S. Kim, A cooperative-sinkhole detection method for mobile ad hoc networks. AEU-International Journal of Electronics and Communications, 2010. 64(5): p. 390-397.

60. Woungang, I., et al., A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks. Security and Communication Networks, 2016. 9(5): p. 420-428.

61. Choudhury, D.R., L. Ragha, and N. Marathe, Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack. Procedia Computer Science, 2015. 45: p. 564-570.

62. Rana, A., V. Rana, and S. Gupta, EMAODV: technique to prevent collaborative attacks in MANETs. Procedia Computer Science, 2015. 70: p. 137-145.

63. Arthur, M.P. and K. Kannan, Cross-layer based multiclass intrusion detection system for secure multicast communication of MANET in military networks. Wireless Networks, 2016. 22(3): p. 1035-1059.

64. Usha, G., M.R. Babu, and S.S. Kumar, Dynamic anomaly detection using cross layer security in MANET. Computers & Electrical Engineering, 2017. 59: p. 231-241.

65. Joseph, J.F.C., et al., CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS. Computer Networks, 2010. 54(7): p. 1126-1141.

66. Sen, J., et al. A mechanism for detection of gray hole attack in mobile Ad Hoc networks. in 2007 6th International Conference on Information, Communications & Signal Processing. 2007. IEEE.

67. Poongodi, M. and S. Bose, Detection and Prevention system towards the truth of convergence on decision using Aumann agreement theorem. Procedia Computer Science, 2015. 50: p. 244-251.

68. Rmayti, M., et al., A stochastic approach for packet dropping attacks detection in mobile Ad hoc networks. Computer Networks, 2017. 121: p. 53-64.

69. Serrat-Olmos, M.D., et al. Accurate detection of black holes in MANETs using collaborative bayesian watchdogs. in 2012 IFIP Wireless Days. 2012. IEEE.

70. Hernández-Orallo, E., et al., CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes. IEEE Transactions on Mobile Computing, 2015. 14(6): p. 1162-1175.

71. Kollati, V.K., IBFWA: Integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET. Information Security Journal: A Global Perspective, 2017. 26(1): p. 49-60.

72. Lal, N., et al., Detection of malicious node behaviour via I-watchdog protocol in mobile Ad Hoc network with DSDV routing scheme. Procedia Computer Science, 2015. 49: p. 264-273.

73. Khanna, N., Mitigation of collaborative blackhole attack using TRACEROUTE mechanism with enhancement in AODV routing protocol. International Journal of Future Generation Communication and Networking, 2016. 9(1): p. 157-166.