Jestr

Journal of Engineering Science and Technology Review 15 (6) (2022) 107 - 114

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Mitigating the Effect of Blackhole Attacks in MANAT

Ahmad Abadleh*, Alaa Btoush, Anas Ali Alkasasbeh, Alaa Mahadeen, Eshraq Al-Hawari, Aya Tareef and Maram M. Al-Mjali

Department of Computer Science, Mutah University, Karak, Jordan

Received 28 September 2022; Accepted 7 December 2022

Abstract

This paper mitigates the effect of blackhole attacks in mobile ad hoc networks according to the traffic of the Ad-hoc On-demand Distance Vector (AODV) routing protocol. The algorithm consists of two parts: In part one, machine learning algorithms are used to detect whether the network suffers from a blackhole attack or not. Part two will be activated if there is a blackhole attack. To block the compromised node, the proposed algorithm in stage two removes the highest sequence number in the route reply as the blackhole node increases the sequence number in the route reply. According to the simulation results, machine learning algorithms used in blackhole detection show an average accuracy of 97.8% for the Random Forest classifier. Throughput, delay, and packet delivery ratio (PDR) are enhanced in part two of the proposed approach.

Keywords: MANET, AODV, Blackhole, machine learning, recovery.

1. Introduction

Wireless communication technology is expanding and advancing rapidly. People want to use their network terminals (laptops, PDAs, etc.) anywhere and anytime. Mobility is made possible by wireless connectivity. Different wireless networks differ in how their nodes interconnect. They can be divided into two types: networks with fixed infrastructure and ad hoc wireless networks [1]. A mobile ad hoc network (MANET) can be used in a wide variety of applications.

MANET comprises a dynamic set of self-organizing mobile devices or nodes that directly communicate with each other without any fixed infrastructure (There is no central management system, unlike traditional networks). Thus, nodes in MANET perform the tasks of both hosts and routers to forward packets toward their destinations based on the employed routing protocol [2]. Using MANET, host devices can communicate between themselves in a constantly changing environment. It is a continuous challenge for packets to be delivered optimally in these networks due to the absence of a fixed infrastructure. For example, as the number of nodes increases in an area, interference between them increases significantly as well. Additionally, MANETs have low stability in areas with fast-moving nodes which leads to their reduced longevity [2].

Since any node can be out of reach at any time, every node can function as a router in a MANET. Data might be transmitted, saved, and forwarded. Additionally, the destination node's location may change frequently. Reactive and proactive routing protocols are usually used in MANETs. A proactive routing protocol is one in which the route formation decision is made based on the properties of the nodes already stored in the routing table, referred to as a table-driven routing protocol. A reactive route is formed on demand in contrast to a proactive route [3].

The Ad-hoc On-Demand Distance Vector (AODV) uses demand-based table-driven routing to make routing decisions. If there is a need to send some packets to a particular node (Destination Node) within the network, the nodes present in an AODV-based network look for routes to that node when needed. Routing tables are also available in AODV. Based on the packet transmission records of previous nodes in the network, every node has a routing table that keeps track of routes to those nodes. Whenever a route becomes inactive during the expiry period, it is considered invalid. Routes are maintained in the table with a lifetime, which is set up beforehand [2].

The source node sends RREQ first when sending a message without routing to the target node. After receiving the RREQ with the source and target addresses, the adjacent node checked whether it matched the target node's address. If it was, sent RREP to the source node, otherwise, check the routings in the routing table that could reach the target node, then send RREP to the source node, or continue to flood send RREQ. AODV protocol can maintain routing nodes by broadcasting hello messages regularly. If one link break, it sent an ERROR message to nodes, meanwhile deleting broken records or repairing the routing [4].

The important feature of AODV is that it is a time-based working protocol. AODV gives demand and destination sequence numbers based on the latest information for the route to the destination. The connection is set up more quickly with AODV. The advantages of AODV have made it popular in recent years. Discovery and maintenance of paths are the two steps of the process. In the path discovery phase, a connection is established between the source and destination nodes using Route Request (RREQ) and Route Reply (RREP) packets [5].

The Blackhole attack consists of the attacker node claiming that it has the shortest route to any desired node in the network, even if it does not have a route there; therefore, all packets will pass through it, enabling it to forward or discard packets during data transmission. Nodes that broadcast requests are trusting any reply they receive, and

*E-mail address: ahmad_a@mutah.edu.jo
ISSN: 1791-2377
doi:10.25103/jestr.156.13

the blackhole node takes advantage of this by claiming that it has the shortest path to the desired node. In normal circumstances, nodes discover a path to their destination during the discovery phase. Nodes receiving this request check whether they have a fresh path to the destination node. A request is broadcast from the source node to the destination node. As soon as the blackhole node receives this request, it responds to the broadcaster by claiming that it has the shortest and freshest path to the destination. Since there is no way to verify whether the request comes from a normal or blackhole node, the source node believes it received that reply. Nodes forward packets to blackholes hoping they will be delivered to the destination nodes, but instead blackholes drop them [2].

This paper proposes an algorithm for detecting and tackling networks from blackhole attacks. The algorithm consists of two parts: In part one, machine learning algorithms are used to detect whether the network suffers from a blackhole attack or not. Part two will be activated if there is a blackhole attack. To block the compromised node, the proposed algorithm in stage two removes the highest sequence number in the route reply as the blackhole node increases the sequence number in the route reply.

This paper makes the following contributions:

- Analyzing the effect of blackhole attacks on network performance.
- Presenting a machine-learning algorithm to detect blackhole attacks.
- Blocking the compromised node by removing the highest sequence number from route replies.

2. Related Work

Mai Mustafa Jaber and Marianne A. The simulation setup used in OPNET to use the following metrics to evaluate network performance in normal mode and in the presence of an attack: packet drop ratio, over routing, throughput, and packet delivery ratio [1].

Pooja Rani and others determined a blackhole node and routed it through a secure node based on modified AODV routing protocols. Based on a node's position, data transmission delays, and power consumption, it can be classified as a blackhole. According to the experiments, the proposed AODV with FFA and ANN method had a 98.19% PDR, a 92.13 kbps throughput, and a 0.042 MS delay on average [2].

Sijan Shrestha and colleagues propose an algorithm based on altering the sequence number present in control packets, particularly Route Reply Packets (RREP), to identify blackhole nodes and lower data loss by eliminating the path through them. Based on simulation results, the proposed algorithm is superior to the old intrusion detection system (IDS) for AODV [3].

Swapnil S. Bhalsagar et al. discussed how trust-based schemes would help to overcome the negative effects due to the presence of malignant nodes. Several types of malicious attacks are discussed, such as blackholes, gray holes, jellyfish attacks, and wormholes. With trust-based schemes, malicious nodes are prevented from being added to the path by assigning them a trust value. Moreover, a comparative analysis was carried out between the trust-based preventive protocols that ensure a high level of security and reduce the effects of malicious attacks. The DSR protocol is implemented under a blackhole attack, and its performance is evaluated by calculating the packet delivery ratio, throughput, and the number of received packets [6].

Md Ibrahim Talukdar and others implements denial-of-service attacks like blackhole attacks for general-purpose ad hoc distance vectors (AODV). they observe that blackholes adversely affect the performance of networks using three approaches: normal AODV, blackhole AODV (BH_AODV), and detected blackhole AODV (D_BH_AODV). Two techniques have been used to detect blackhole attacks within networks: intrusion detection systems (IDS) and encryption techniques (digital signatures). The packet delivery ratio (PDR), delay, and throughput parameters for the AODV and BHa AODV protocols are examined. The findings of this study demonstrate that blackhole attacks reduce network performance, but D BH AODV improves QoS performance by identifying blackhole nodes and avoiding them when establishing connections between nodes [7].

Ehsani Rad St and others. The K-near-neighborhood (KNN) technique for fuzzy clustering and inference for cluster head selection was proposed in the study as a new algorithm in MANETs for blackhole attack detection. Determine the confidence of each node using the beta distribution and Gusang's reasoning. Fuzzy heuristics choose the block header based on reputation and remaining energy. Then the trust server checks the target node. If permitted, it alerts the head of the block; If not, it recognizes the node as a malicious node in the blackhole attack for each group.) When compared with current blackhole detection techniques, simulation results show that the proposed method has improved parameters of packet loss rate, throughput, packet delivery ratio, total latency for the network and load normal routing [8]. Machine learning algorithms have been widely applied in different fields. For instance, in the security field, they are employed to find biometric keys [9–11]. Additionally, in the network, researchers utilize machine learning for network traffic analysis and indoor localization [12–23]. P Rani et al. [24] enhanced the AODV's resistance to black hole attack by merging the Firefly Algorithm with an Artificial Neural Network by training the ANN to the optimized node's attributes through FFA routes for both normal and abnormal nodes.

El-Semary at al. [25], enhanced an BP-AODV protocol by advancing the capabilities of the AODV and incorporating chaotic map features. The evaluation was computed during the execution time of 200s for 25 nodes. The average throughput reaches 2500 Kbps, with an end-to-end delay of about 5 ms and an average PDR of about 90%.

JM Chang at al. [26], The source node picks a nearby node at random to work with in order to use its address as the bait destination address to persuade hostile nodes to send a reply RREP message. Malicious nodes are consequently found and excluded from the routing activity by using a reverse tracing technique. In this configuration, it is assumed that anytime there is a significant drop in the packet delivery ratio, an alarm will be sent from the destination node back to the source node to restart the detection process.

In general, our method of identifying the attack and resolving it differs from previous work. We use machine learning to recognize attacks with high accuracy, and afterward, we employ our recovery algorithm to mitigate their impact.

3. Methodology

This paper proposes a new approach to tackle the issue of blackhole attacks in MANET utilizing machine learning. Fig. 1 illustrates the overall proposed approach.

As shown in Fig.1, the proposed approach consists of three stages. In stage one, a route is created via the AODV protocol for nodes (both normal and malicious). The protocol is modified by exploiting a blackhole node's fake information to generate a malicious node with fewer hops and the highest sequence number. Then, several network performance metrics are computed and analyzed to determine whether the network is compromised or not. Stage two involves detecting blackhole attacks using machine learning algorithms. Several network performance metrics are used in machine learning algorithms, including throughput, delay, and packet drop rate. Some simulations were conducted in stage one to generate the training data. As soon as a blackhole attack occurs in stage two, the recovery algorithm will be activated. This algorithm solves this issue by ignoring packets with the highest sequence number and the lowest hop count.

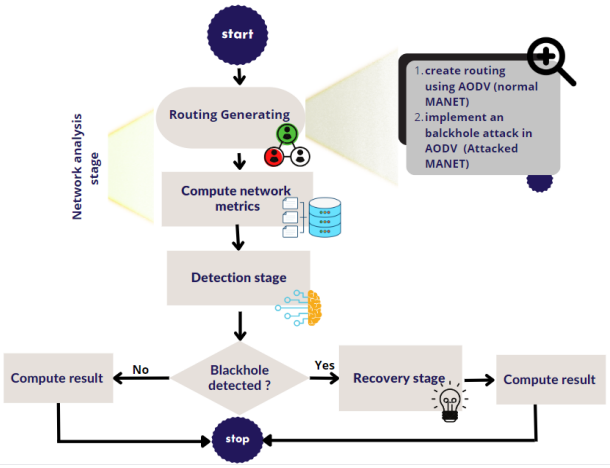

Fig. 1. System architecture.

The proposed approach consists of three stages as follows:

3.1 Network analysis stage:

The first part of the network analysis stage is the routing protocol. To do so, the network scenarios were implemented through the NS-3 simulator. The simulator is used to build many network topologies with the AODV routing protocol, which makes the route based on demand and minimizes the number of broadcasts needed.

For better explanation, Fig. 2 illustrates an example of an implemented scenario. Whenever source node 'A' wants to connect with destination node 'F', it broadcasts the RREQ to its neighbors B, C, and E.

In case that no blackhole nodes exist, neighbors B, C, and E received the RREQ and updated the route information related to the destination. Since it is not the destination, no RREP is generated.

It will keep repeating until the destination 'F' receives the RREQ packet. The connection is made through A,B,F once the RREP has returned to A. Source A will choose an RREP with the largest destination sequence number.

However, the RREP with the lowest hop count value will be used if the destination number is equal.

In the case that E is a blackhole node, node E generates fake information RREP, posing as the destination node, in response to receiving the RREQ from A.

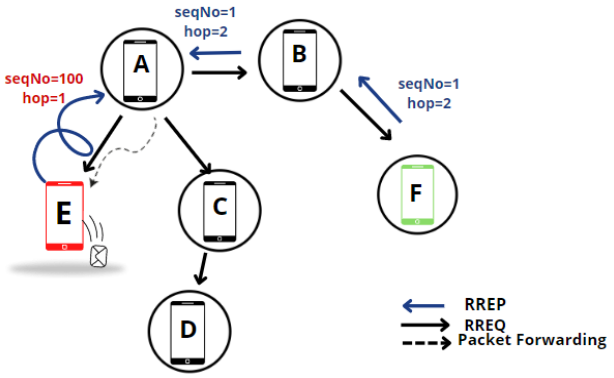

Fig. 2. Routing example with a blackhole attack.

The source node A will choose the shortest path with a higher sequence number and fewer hops, and then it will forward packets to E. The fake destination node E will drop these forwarded packets.

The second part of the network analysis stage is computing the network performance metrics. For this purpose, several simulation scenarios were constructed utilizing various network configurations.

The performance metrics are calculated and studied as network properties, including throughput, delay, packet loss, and packet delivery ratio (PDR). This process is repeated for various MANET topologies. This stage produces a dataset containing the calculated performance metrics and the status of the network as compromised or not.

3.2 Detection stage

Machine learning (ML) aims to detect unknown attacks, and algorithms such as decision trees, random forest classifiers, K nearest neighbors (KNNs), and artificial neural networks (ANNs) can be used to train a network prediction model and classify networks traffic. To create the best network model, ML classifiers are trained using Orange Workflow. It is trained using datasets generated from several network simulations that have been executed. Our main goal in creating the ML-based detection module is to classify the network and determine whether the blackhole affects it or not, which is expected to enhance the detection accuracy. Algorithm 1 illustrates how to detect blackhole attacks. The first step determines the features and the class to build the dataset. Then, the best model is produced using different machine learning classifiers. Finally, the algorithm returns "Yes" if the network is compromised by a blackhole attack or not.

Algorithm 1: Detection algorithm

Features[i]=network performance metrics i=1,2,3, … no of metrics.
Class={Yes, No} // compromised or not
Dataset = results of network simulations
Model = Machine_learning[dataset, features, class]
Return Class

3.3 Recovery stage:

Usually, a malicious node sends a fake RREP packet with a maximum sequence number (e.g., greater than 50) and fewer hops than the RREQ packets received from the rest of the network. The proposed approach employs these fake properties before evaluating them once the network is detected as having a blackhole by the detection stage.

Algorithm 2 illustrates how to solve blackhole attacks. When the detection stage detects that the network is compromised, the proposed approach ignores the RREP packet with the highest sequence number and lowest hop count. Then, it broadcasts RREQ again.

Algorithm 2: Recovery algorithm

```
isCompromised = DetectionAlgorithm()
if (isCompromised)
  ignore the least hop count
  remove the highest sequence number
  Broadcast RREQ.
```

4. Evaluation

4.1.Simulation environment

The proposed approach was evaluated using different MANET scenarios, including AODV routing protocol without attack, single blackhole attack, and multiple blackhole attack. The NS-3 (ver-3.24.1) simulator, Ubuntu 18.08, and the netanim-3.108 application were used to run the simulation. Figs 3 and 4 show the implemented scenarios. Moreover, Orange application used to create machine learning classifiers.

Scenario 1:

As presented in Fig. 3, we examined the impact of one blackhole by varying the data rate. We employed five nodes in two scenarios: one without a blackhole and one with a blackhole attack. We varied the data rate from 200 to 700 and recorded the results.

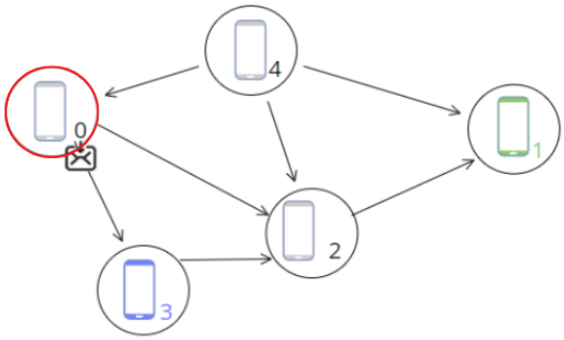

Fig. 3. Scenario one.

Scenario 2:

According to Fig.4, we implemented and examined a scenario with ten nodes in two ways: one without a blackhole attack and one with several. The scenario begins without an attack and gradually increases the number of malicious nodes until reaching four malicious nodes.

Several network performance metrics are calculated, including throughput, delay, and packet delivery ratio. Table 1 presents the simulation parameters.

Table 1. Simulations parameters

parameter	Value
Number of nodes	4 to 10
Max Packet Size	1040 bytes
Traffic Model	CBR
Link Data Rate	200 to 700 Kbps
Routing Protocol	AODV
Simulation Time	100 s
Mac Layer	802.11
Number of Malicious Nodes	1 to 4

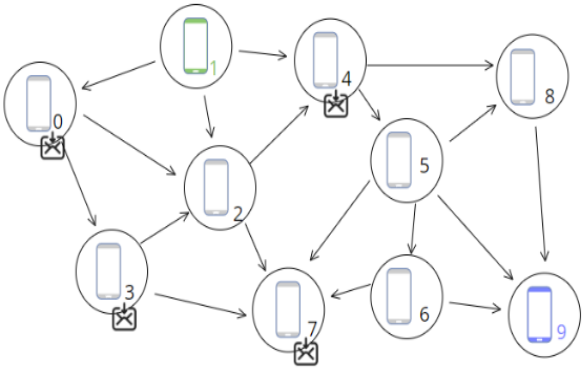

Fig. 4. Scenario two.

4.2 Simulation results

4.2.1. The effect of blackhole attack in MANET.

A. Throughput result

Fig. 5 demonstrates that, in the normal case for MANET, throughput increases to its maximum value, whereas, in the case of a blackhole attack, throughput value begins with a lower value and rises to a specific value with an increase in data rate. It is, nevertheless, lower than average, and the throughput is unstable because of the blackhole node.

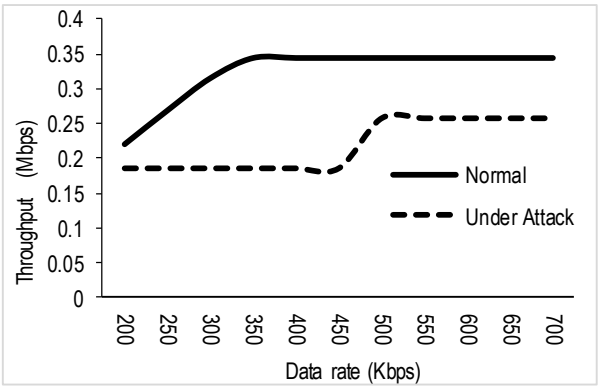

Fig. 5. Scenario 1 throughput result with different data rates.

Fig. 6 demonstrates how performance falls as the number of malicious nodes increases. When it comes to routing without blackholes, the AODV routing protocol performs better and more steadily. When there are many compromised nodes, the entire network goes down as the malicious nodes increase.

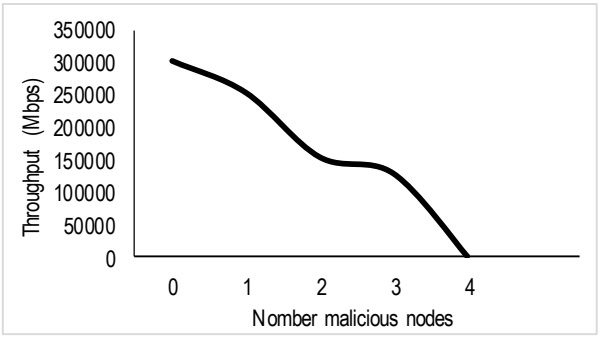

Fig. 6. Scenario 2 throughput result with different malicious nodes.

B. Delay result

The delay result for scenario one in the event of an attack is high, as illustrated in Fig. 7. The lower the packet delay, the better the network performance because the average end-to-end delay is short. Data rate hikes are causing the delay value to rise. In most cases, the effect appears worse than it is normal networks.

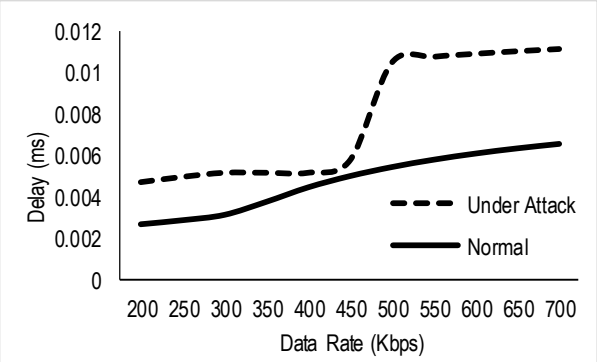

Fig. 7. Scenario 1 delay result with different data rates.

As the quantity of received packets declines, as seen in Fig. 8, the average latency reduces. Many packets are lost as we keep adding attackers. Fewer packets are sent and received at the destination as a result of the routing. As a result, because there are more compromised nodes, the needed amount of delay gets smaller as fewer packets are received.

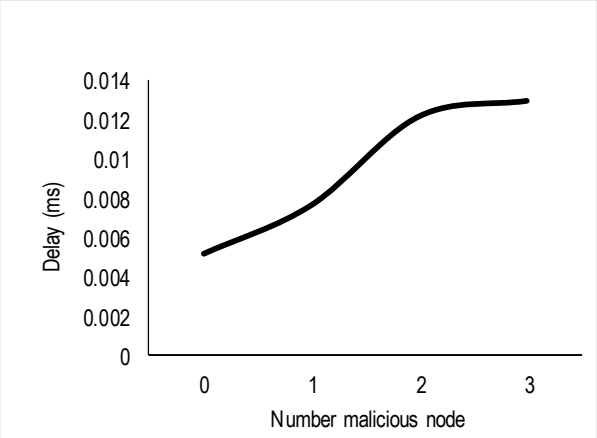

Fig. 8. Scenario 2 delay result with different malicious nodes.

C. Packet Delivery Ratio result (PDR)

Fig. 9 shows the results of PDR when the network is under attack and when it is normal. The result shows how the attack severely impacts PDR results. During an attack, PDR decreases by about 60%. All packets passing through the blackhole are absorbed and dropped, increasing packet retransmissions and packet drops during connection.

In Fig.10, the result of the PDR is shown when the network is under attack and under normal conditions. The figure shows how the attack strongly affects the results of the PDR. During an attack, the PDR decreases by about 20% and then doubles to 40% until it reaches 0%. Blackholes notice and drop all packets that pass through them, which increases the retransmission and dropping of packets.

4.2.2 The classification results

The dataset was collected from over ninety simulations and was used as training data for different classifiers to evaluate the best one. As shown in Fig.11, the classification accuracy plotted for each classifier was KNN (95.4%), ANN(95.8%),Naïve Base (94.4%),decision tree(96.6%), and random forest (97.8%). The result shows that a Random Forest classifier has the highest accuracy of 97.8%.

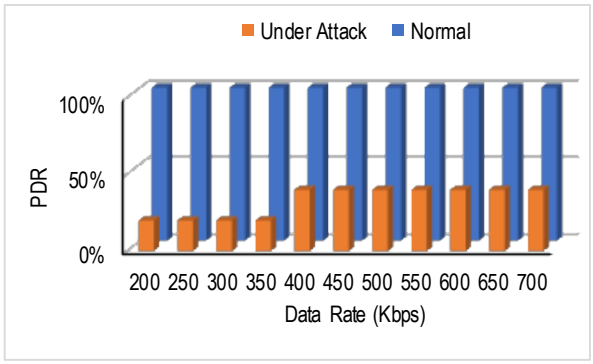

Fig. 9. Scenario 1 PDR result.

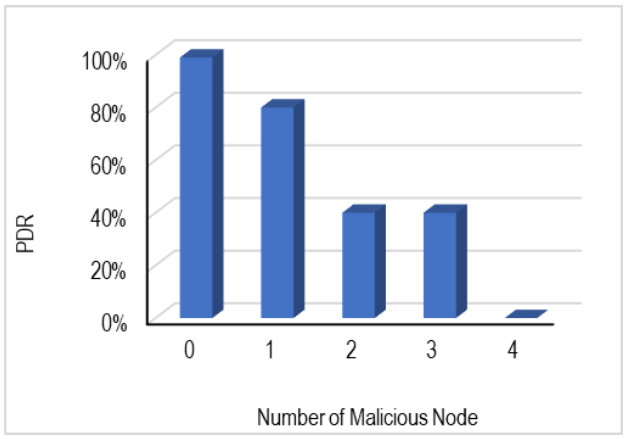

Fig. 10. Scenario 2 PDR result.

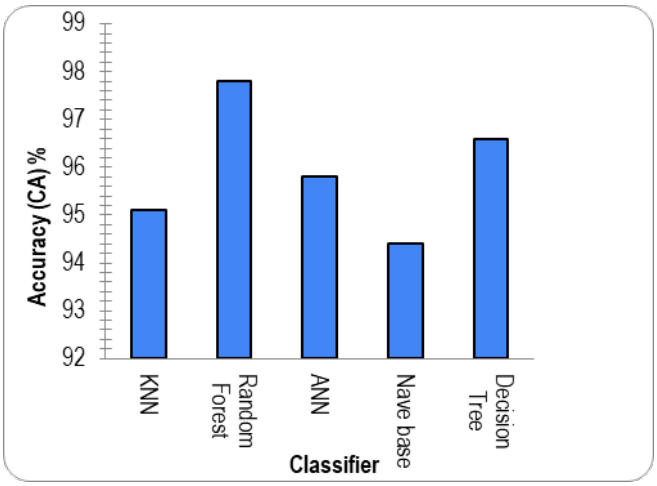

Fig. 11. comparison of ML accuracy.

4.3 The impact of recovery on detected attacked MANET.

To identify the performance of the recovery stage and its efficacy, the discovered attacked networks that were detected using a random forest classifier are fed into a recovery stage.

A. Throughput result

Fig. 12 shows the network's throughput performance for the detected networks and recovery stage when the data rate is changed from 200 to 700 Kbps with a single malicious node.

as the rate approaches its maximum, the number of bits transmitted each second increases (500 kbps). The throughput is lower when the networks are under attack. The outcomes appear better when recovery steps are carried out. Low rates of blackhole node detection were made, and the throughput was immediately increased by the applied recovery.

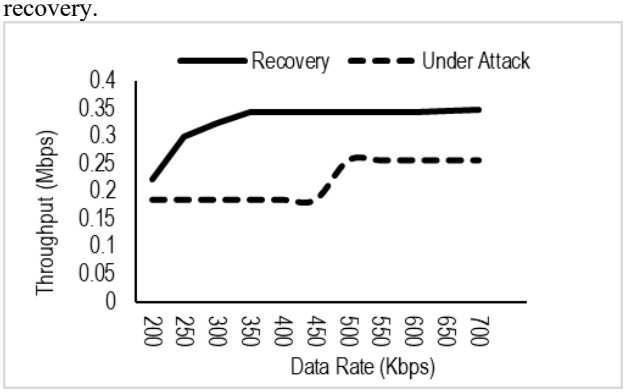

Fig. 12. Scenario 1 throughput results with different data rates.

Fig. 13 shows how a detected network's performance degrades as the number of malicious nodes rises. The network collapses when the number of attacker nodes rises. When compared to the other cases, the throughput at each point has improved significantly during the recovery stage. Due to early detection and blocking of fake pathways with malicious nodes.

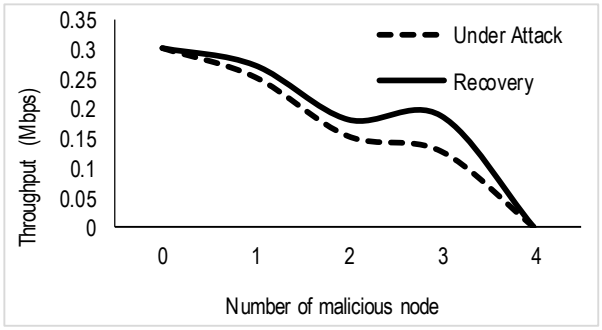

Fig. 13. Scenario 2 throughput with different malicious nodes.

B. Delay result

As shown in Figs 14 and 15, the proposed recovery algorithm reduces the delay when the network is attacked. The delay result continues to increase, as shown in Fig. 14 since so few packets are being quickly discarded by the blackhole at the start of the simulation. As the recovery algorithm starts, the delay decreases as the malicious node is blocked.

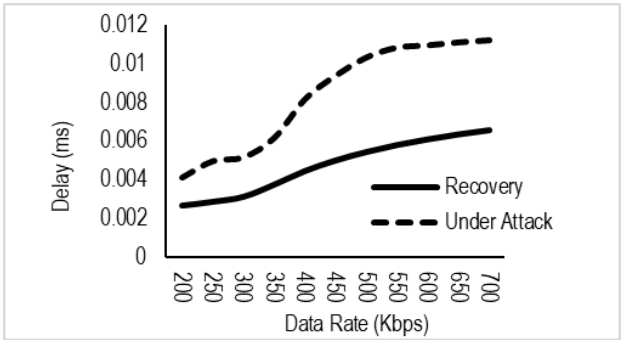

Fig. 14. Scenario 1 delay result with different data rates.

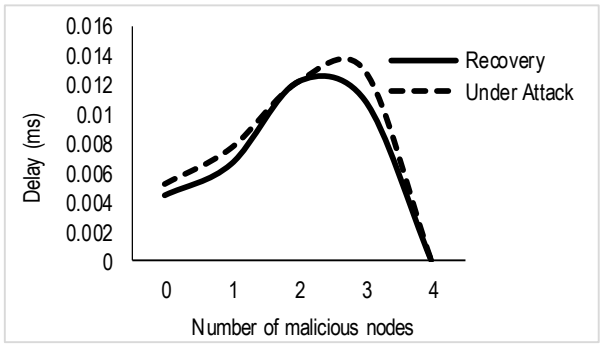

Fig. 15. Scenario 2 delay result with different malicious nodes.

C. Packet Delivery Ratio result (PDR)

Fig. 16 illustrates how the attack has a negative influence on both the network's detection and the recovery stage. PDR drops by around 60% during an attack. The blackhole absorbs and drops every packet it encounters, leading to increased packet retransmissions and packet loss during connections. In the following stage, the network is recovered, leading to decreasing in the dropped packets, improving the PDR result to 20% loss rather than 40% loss.

Fig. 17 depicts the outcome of the PDR during an assault on the network and during the implementation of recovery. The attack has a significant impact on the PDR's outcomes. All packets that pass through blackholes are noticed and dropped, which causes more packets to be retransmitted and dropped.

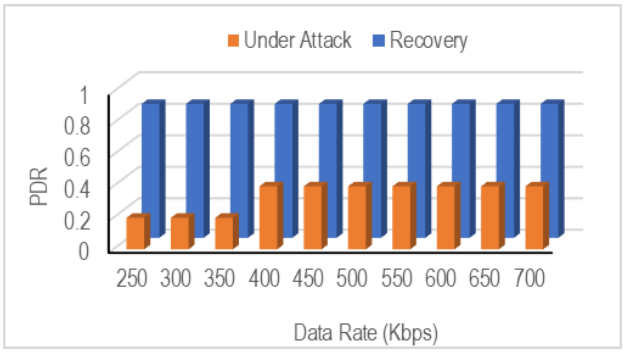

Fig. 16. Scenario 1 PDR with different data rates.

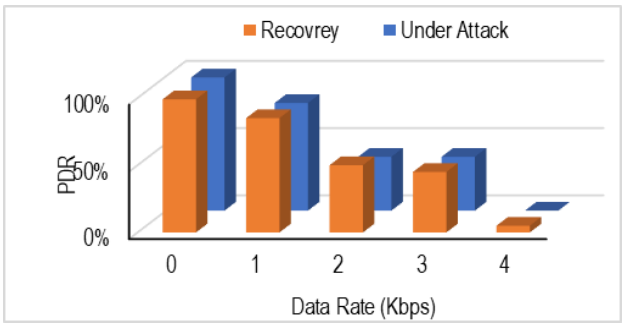

Fig. 17. Scenario 2 PDR result with different malicious nodes.

5. Comparative analysis

The proposed approach is compared with Shrestha et al. [27] and Patel et al. [28] to show how effective it is. The main method, throughput (Kbps), delay (MS), PDR, and other number of malicious nodes are used as the basis for comparison. Table II shows the overall comparison of the proposed approach with some of existing approaches.

Table 2. Compasion with existing approaches

Approach	Method	AVG Delay (ms)	AVG Throughput (kbps)	AVG PDR	# of MN
Proposed	Seq.no & ML	Decreased about 0.007 ms	Increase 28.4	46%	1-4
Shrestha et al.[27]	Modified Seq.no	---	Increased about 14.75	23.25 %	1-4
Patel et al. [28]	Intrusion detection and prevention mechanism IDS	Decreased about 35.9 ms	Increased about 11.93	10.31 %	1-4

6. Conclusion

This paper analyzes the traffic of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to reduce the impact of blackhole attacks in mobile ad hoc networks. The algorithm is divided into two sections: In the first section, machine learning methods are employed to determine whether the network has been subjected to a blackhole assault. If a blackhole assault occurs, part two will be initiated. As the blackhole node increases the sequence number in the route reply, the proposed algorithm in stage two eliminates the highest sequence number in the route reply to block the compromised node. The simulation outcomes reveal that the Random Forest classifier has an average accuracy of 97.8% when utilized in machine learning methods for blackhole identification. Moreover, using the recovery algorithm, the throughput, delay, and PDR have been improved, which enhances the network performance. As a future work, we decide to extend our work to apply it to vehicle networks where mobility is occurring more quickly. Furthermore, we are going to modify our approach to be more efficient by considering the time needed for the route reply packet.

References

1. Maurya, P. K., Sharma, G., Sahu, V., Roberts, A., Srivastava, M., & Scholar, M. T., "An overview of AODV routing protocol." *International Journal of Modern Engineering Research (IJMER)*, *2*(3), 2012, pp. 728-732.
2. Bamhdi, A. M., "Efficient dynamic-power AODV routing protocol based on node density", *Computer Standards & Interfaces*, 70 (1), 2020, pp.1-8.
3. Sen, B., Meitei, M. G., Sharma, K., Ghose, M. K., & Sinha, S., "A trust-based intrusion detection system for mitigating blackhole attacks in MANET", *Advanced Computational and Communication Paradigms*, 2018, pp. 765-775.
4. Kumar, S., Dhull, K., Arora, P., & Luhach, A. K., "Performance of energy conservation models, generic, micaz and micamotes, using AODV routing protocol on a wireless sensor network", *Scalable Computing: Practice and Experience*, 20(4), 2019, pp. 631-639.
5. Liu, Sheng, Yang Yang, and Weixing Wang. "Research of AODV routing protocol for ad hoc networks1." *AASRI Procedia* 5(1), 2013, pp.21-31.
6. Hassan, Marwan Hamid, et al. "Integrating African Buffalo optimization algorithm in AODV routing protocol for improving the QoS of MANET", *Journal of Southwest Jiaotong University*, 54(3), 2019, pp.1-12.
7. Manoranjini, J., Chandrasekar, A., & Jothi, S., "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework." *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, 60(3), 2019, pp.274-284
8. Yasin, A., & Abu Zant, M., "Detecting and isolating black-hole attacks in MANET using timer based baited technique", *Wireless Communications and Mobile Computing*, 2018(1), 2018, pp.1-10.
9. E. Hamadaqa , A. Abadleh , A. Mars and W. Adi , "Highly Secured Implantable Medical Devices", In: *International Conference on Innovations in Information Technology* (IIT), 2018, pp. 7-12.
10. S. Mulhem , A. Abadleh and W. Adi , "Accelerometer-Based Joint User-Device Clone-Resistant Identity", In: *Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4),* 2018, pp. 230-237.
11. A. Mars, A. Abadleh and W. Adi, "Operator and Manufacturer Independent D2D Private Link for Future 5G Networks*,"* In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* 2019, pp. 1-6.
12. Alabadleh A, Aljaafreh S, Aljaafreh A, Alawasa K., "A RSS-based localization method using HMM-based error correction*." J Loc Based Serv* 12(3–4), 2018, pp. 273–285.
13. Aljaafreh, A., Alawasa, K., Aljaafreh, S., & Abadleh, A., "Fuzzy inference system for speed bumps detection using smart phone accelerometer sensor." *J. Telecommun. Electron. Comput. Eng.,* 9(2–7), 2017, pp. 133–136.
14. Abadleh, A., Al-Hawari, E., Alkafaween, E., Al-Sawalqah, H., "Step detection algorithm for accurate distance estimation using dynamic step length," In: 2017 *18th IEEE International Conference on Mobile Data Management (MDM),* 2017, pp. 324–327.
15. Abadleh, Ahmad, et al. "Noise segmentation for step detection and distance estimation using smartphone sensor data." *Wireless Networks* 27(4), 2021, pp.2337-2346.
16. Alnabhan, Mohammad, et al. "Enhanced D2D Communication Model in 5G Networks." *International Journal of Computing and Digital Systems* 10(1), 2021, pp.217-223.
17. Alnabhan, Mohammad, et al. "Efficient Handover Approach in 5G Mobile Networks." *Int. J. Adv. Sci. Eng. Inform. Techn*ol 10(1), 2020, pp.1417-1422.
18. Abadleh, Ahmad. "Wi-Fi RSS-based approach for locating the position of indoor Wi-Fi access point", *Communications-Scientific letters of the University of Zilina,* 21(4), 2019, pp. 69-7.
19. Altarawneh, G. A., Hassanat, A. B., Tarawneh, A. S., Abadleh, A., Alrashidi, M., & Alghamdi, M, "Stock Price Forecasting for Jordan Insurance Companies Amid the COVID-19 Pandemic Utilizing Off-the-Shelf Technical Analysis Methods." *Economies*, 10(2), 2022, pp.43-50.
20. Al-Tarawneh, Nagham A., Ahmad H. Abadleh, and Zaid T. Alhalhouli. "Direction Estimation using Patterns of User Movement." *Journal of Engineering Science & Technology Review* 12 (4), 2019, pp. 195-201.
21. Abadleh, Ahmad, Et Al., "Covid-19 Disease Recognition Using Distributed Data Mining and Deep Learning." *Journal of Theoretical And Applied Information Technology* 100(2), 2022, pp.469-479.
22. Abbadi, M., et al. "Machine Learning-Based Approach for Detecting Driver Behavior Using Smartphone Sensors." *International Journal of Scientific and Technology reserach* 8(12), 2019, pp.1057-1060.
23. Abadleh, Ahmad, et al. "Comparative Analysis of TCP Congestion Control Methods", In: *13th International Conference on Information and Communication Systems (ICICS). IEEE*, 2022, pp.474-478.
24. Rani, P., Verma, S., Rawat, D. B., & Dash, S., "Mitigation of black hole attacks using firefly and artificial neural network". *Neural Computing and Applications*, 34(1), 2022, pp. 15101-15111.

25. El-Semary, A. M., & Diab, H. "BP-AODV:Blackhole protected AODV routing protocol for MANETs based on chaotic map." *IEEE Access*, 7 (1), 2019, pp.95197-95211.
26. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F., "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." *IEEE systems journal*, 9(1), 2014, pp. 65-75.
27. Shrestha, Sijan, et al. "Securing blackhole attacks in MANETs using modified sequence number in AODV routing protocol." 2020 *8th International Electrical Engineering Congress (iEECON). IEEE*, 2020, pp.1-4
28. Patel, Neelam Janak Kumar. "Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network." *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE),* 5(3), 2018, pp.2320- 2394