SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I4P109

Volume 11 Issue 4, 80-88, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Detecting Intruder and Black Hole Attackers in Mobile Adhoc Network

S. Hemalatha[1], Maddala Janakidevi[2], Pullela SVVSR Kumar[3], M.S. Arunkumar[4], Sanjeevkumar Angadi[5], T. Murugananthам[6], R. Hamsalekha[7], T. Vijay Muni[8]

[1]*Department of Computer Science and Business Systems, Panimalar Engineering College, Tamil Nadu, India.*
[2]*Department of Computer Science and Engineering, SRKR Engineering College, Andhra Pradesh, India.*
[3]*Department of Computer Science and Engineering, Aditya College of Engineering, Andhra Pradesh, India.*
[4]*Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India.*
[5]*Department of Computer Science and Engineering, Nutan College of Engineering and Research, Pune, Maharastra, India.*
[6]*Department of Electronics and Communication Engineering, K. Ramakrishnan College of Engineering, Tamil Nadu, India.*
[7]*Department of Electronics and Communication Engineering, New Horizon College of Engineering, Karnataka, India.*
[8]*Department of Electrical and Electronics Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India.*

[1]*Corresponding Author : pithemalatha@gmail.com*

Received: 10 February 2024 Revised: 09 March 2024 Accepted: 08 April 2024 Published: 30 April 2024

***Abstract** - Making the packet transfer communication among the wireless nodes in Mobile Adhoc Network is a tedious task due to the nature of the communication nodes and the suspicious nodes' activities like intruders and attackers. Much research work was concentrated on thwarting the packet delay node and dropping the node in the transmission with the support of modern techniques and internal node parameter monitoring that are supplementary work to the node's communication and reduce the performance of the nodes. This paper anticipated a new algorithm named classification algorithm with a simple forward time of the node parameter to predict the intruder node as well as the black hole attacker in the communication. The proposed effort was called a Classification algorithm-based intruder as well as a Black Hole Attack AODV, and it was tested with the simulator. The outcome was compared with the normal AODV method. The simulation results showed that the proposed CAIBHA-AODV worked better packet delivery, less delay and attack detection time and constant attack rate compared with the normal AODV.*

***Keywords** - MANET, Intruder, Black Hole Attackers, Suspicious node, Classification algorithm, Forward time.*

1. Introduction

Packet sending from node to node in a Wireless network like MANET is a cumbersome task owing to the occurrence of malicious nodes [1]. Thiagarajan et al. [2] conducted research on malicious node isolation using a secure, optimized approach. Gurung and Chauhan [3] discussed challenges and surveyed black hole attack techniques in MANETs. One of the roles of the malicious nodes is packet delaying or dropping the packets, called intruders as well as Blackhole attackers [3].

Khanna and Sachdeva [4] employed taxonomy techniques for black hole attacker detection, and Borkarn and Mahajan [5] discussed various articles supporting secure data communication to prevent attacks in MANETs. Figure 1 depicts the normal packet flow beginning in the node to another node; Figure 2 shows the holding of the packet for a period of time called delay in forwarding, which is done by the intruder node. Figure 3 shows that the nodes dropping the packet rather than forward to the next hop, which is called a black hole attacker. The purpose of the article is to detect intruder nodes and black hole nodes in MANETs during communication. The number of study works was conceded for the identification of intruder nodes as well as attacker nodes with the aid of routing protocols, secure approaches, modern techniques, and algorithms. Nagaraj et al. [6] developed a clustering routing approach to identify intruders and routing misbehavior nodes.

Kumari et al. [7] devised a method for creating black hole attacks in the AODV routing protocol. Shankar [8] proposed secured data transmission using the ZRP protocol to enhance Quality of Service (QoS) amidst gray hole attacks, and Suma et al. [9] proposed location-aided routing techniques to combat attackers in MANETs. Veeraiah and Krishna [10] proposed an optimal routing algorithm to secure communication routes and prevent intruder interference. Veeraiah et al. [11] proposed an HRMA for intruder detection to ensure trustworthy transmission between nodes. Authors in [12] proposed a routing algorithm aimed at preventing internal and external attacks in node communication.

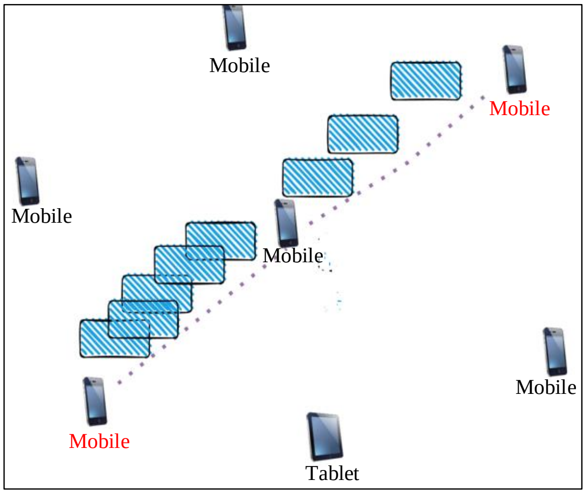

Fig. 1 Normal packet flow

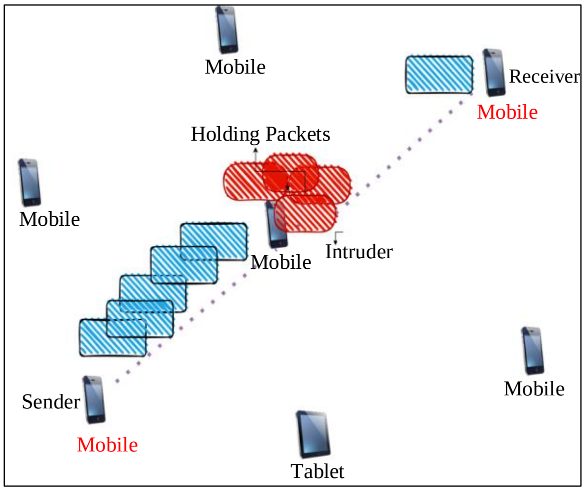

Fig. 2 Packet delay in forwarding

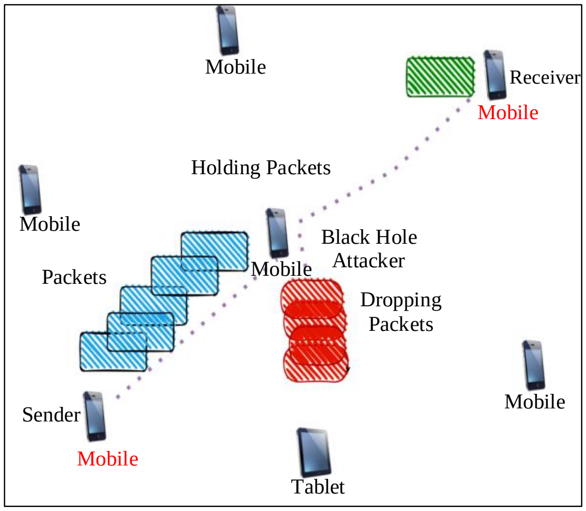

Fig. 3 Packet dropping rather than forwarding

The purpose of the article is to detect intruder nodes and black hole nodes in MANETs during communication. The number of study works was conceded for the identification of intruder nodes as well as attacker nodes with the aid of routing protocols, secure approaches, modern techniques and algorithms.

Nagaraj et al. [6] developed a clustering routing approach to identify intruders and routing misbehavior nodes. Kumari et al. [7] devised a method for creating black hole attacks in the AODV routing protocol. Shankar [8] proposed secured data transmission using the ZRP protocol to enhance Quality of Service (QoS) amidst gray hole attacks, and Suma et al. [9] proposed location-aided routing techniques to combat attackers in MANETs.

Veeraiah and Krishna [10] proposed an optimal routing algorithm to secure communication routes and prevent intruder interference. Veeraiah et al. [11] proposed an HRMA for intruder detection to ensure trustworthy transmission between nodes. Authors in [12] proposed a routing algorithm aimed at preventing internal and external attacks in node communication.

Rani et al. [13] proposed AI with a Swarm algorithm for detecting black hole and gray hole attackers. Khan et al. [14] explored the ant colony approach to prevent black hole attackers in MANETs. Teli et al. [1] utilized mitigating techniques to recognize black hole and gray hole attackers, and Goswami et al. [15] proposed trust-based techniques for black hole detection in MANETs.

Hassan et al. [16] incorporated AI techniques into MANETs to predict black hole attackers to ensure secure communication. Hussain et al. [17] introduced an AI-enabled routing protocol for secure communication, Sultan [18] used a deep learning-based Artificial Neural Network (ANN) technique for IDS detection, performed black hole detection using machine learning algorithms [19] and AI-based techniques were invented to discover the black and gray hole attacker [13], wormhole attacks [1], employed AI-based techniques [20] for wormhole attack recognition, Numerous research endeavors have been dedicated to the finding and anticipation of intruders and attackers in MANET, employing innovative techniques such as AI, ML, DL algorithms, data analytics methods, and fuzzy logic.

Despite these efforts, the effectiveness of intruder detection and protection against attacks in MANETs remains an ongoing challenge. This research objective could be accomplished by monitoring the forwarding time of each packet across every participating node involved in communication. The organization of this article is delineated as follows: Section 2 encompasses a survey pertaining to connected research endeavors, Section 3 delves into algorithmic and classification techniques, Section 4 presents the simulation work for the proposed research, and Section 5 offers concluding remarks.

2. Literature Survey

This section elaborates on the details survey carried out to the attacker as well as intruder detection on MANET. Table 1 discusses the different methods and types of attacks with merits and demerits. From the literature survey, numerous authors have conducted research on identifying intruders and black hole attackers in MANET using various parameters, algorithms, novel techniques, and methods for MANET nodes. However, existing methods often impose additional computational overhead on the nodes' operations. In contrast, this article proposes an algorithm that does not require additional computation and can effectively predict intruder nodes and attacker nodes in the transmission. This is achieved by coordinating the forward time of every node to identify potential attackers and intruders in the transmission.

Table 1. Literature survey

S.No.	Authors	Methods	Types of Attack	Merit	Demerit
1	Sivanesan and Rajesh [21]	Machine Learning Categorization Model	DoS attacks, Gray holes, black holes, flood attacks.	96.75% enhancement in accuracy.	Classification takes more time.
2	Murali and Sathya [22]	Black Hole Resistance Method	Black hole attack	Produced energy efficient and better latency and packer delivery.	The shortest round-trip time among nodes remains a challenge.
3	Shaik Shafi et al. [23]	Machine Learning And Trust-Based	Identify trust nodes	Improved throughput	Method relies on an excessive number of parameters for route determination.
4	Vijayalakshmi et al. [24]	Intrusion Detection System with Game Theory	Defect or cooperate nodes	Packet delivery ratio of 42%.	Limited to single attacks
5	Sampada and Shobha [25]	Smart & Secure Aodv	Black hole / gray hole	Better output performance	Used more parameters (RSSI), power, and battery.
6	Edwin Singh and Maria [26]	Fuzzy-Based PCA-FELM	Intruders	Higher accuracy of 99.08%	Required more logical comparison.
7	Haik Shafi et al. [23]	ML-AODV Method	Flood and black hole attacks	Throughput reliability, routing overhead, and packet loss ratio improvements.	Training the data set takes more time.
8	Olanrewaju et al. [27]	Enhanced On-Demand Distance Vector	Thwarting black hole attackers	Better throughput	This approach entails encrypting packets using Diffie-Hellman and Message Digest 5 limitation of this work lies in its reliance on packet acknowledgement provided by the recipient.
9	Jayant Kumar & Manjunath [28]	Kangaroo-Based IDS	Malicious nodes	Enhances data transmission security.	More parameters are used.
10	Jyoti Dhanke et al. [29]	Destination Sequence Number	Black hole attackers	98.15% Packet Delivery Ratio.	DSN Limitation
11	Aurelle Tchagna Kouanou [30]	Secure Communication Approach	Wormhole and black hole attacks	A 99% accuracy rate was achieved.	Need adoption of deep learning methodologies to monitor the expanding dataset effectively.
12	Abdelhamid et al. [31]	Lightweight Detection Technique	Black hole attackers	Transmission power	Conducting simulations with a limited number of systems.

3. Research Methods

The Literature survey reveals that many techniques were proposed for detecting and preventing the intruder node as well as black hole attackers with the hold of the many internal parameters. However, those parameters were able to find the values after the packet processing was done.

This article finds a new solution to the MAENT nodes to prevent and detect intruders and attackers while the packet flows from one node to another node with the support of the packet forward time. This parameter is a live executable parameter which does not take additional cost and overloads the MANET nodes to detect and prevent the intruder.

Let us take the MANET nodes as N1, N2, N3...Nn where n is the maximum number of nodes and the route path from the source to destination are S, IM1, IM2,...D where IM are intermediate nodes from the source to the destination. The source node is responsible for finding the path to the destination using the RREQ (route request). The RREQ floated to all the nodes in the MANET so as to reach the destination. The destination node sends RREP (Route Reply) to the source to get the path from the source to the destination.

Once the reliable path is selected, the source initiates the packet transmitting in a sequence number. All the packets have the details of the packet, like packet received time and forwarding time. This packet received and forwarding time values help to find out the intruder who is making the delay in forwarding or the black hole attacker who does not forward the packet to the next hop. Calculation of Node forwarded time is done using the equation (1).

$$\text{Forward Time } F_t = \sum ttP_i \qquad (1)$$

Where transmission time is tt.

Every node has an internal buffer to hold the received packet and forward the packet. If the buffer is full, then packet dropping is done that is not the attacker node; when the buffer is empty, if packet dropping is done, then it is an attacker node. So, research work is needed to determine the time for holding the packet in the buffer based on the value names as threshold values.

Determining the threshold value is based on the time of flight defined as the packet flow time from the source to reach the destination. When a forward time is less than the threshold values, then the node is a normal node; otherwise, it is an intruder and also a black hole attacker. To determine the threshold, the nodes follow the algorithm I. Two variations of the Threshold value are determined based on the congestion and buffer overflow using Equations (2) and (3).

$$\text{Threshold} = \text{Time of flight / Hop count} \qquad (2)$$

$$\text{Threshold Value} = (\text{TF} + \text{BS})/\ \text{HC}) \qquad (3)$$

Where TF is the Time of flight, BF is Buffer Size, and HC is the Hop count.

```
Algorithm 1
1.  Source node initiates the route to the destination node
2.  Every node determines the threshold value
    If there is no congestion or the buffer full
    Then, the threshold value is = time of Flight / Hop count.
    Otherwise threshold value = (time of Flight + buffer size) / hop count
3.  Each node cross-verifies the received packet Forward time.
4.  If variation in forward time value, initiate the classification algorithm to classify whether it is an intruder or a black hole attacker.
5.  If the classification algorithm returns the intruder or attacker node, alert the MANET nodes.
```

Classification Algorithm (Suspicious Node S)

```
{
//Classification of suspicious node is an Intruder or Black hole attacker

If (monitor the forward time of the suspicious node > threshold Value)
{
Monitor the all the packet forwarding time of the suspicious node
    If (forward time varies on selective packet and buffer is not full)
        Conclude the Node is an Intruder and return
        Else if (not find the forward time of the selective and is varies not occur for few packets)

            Node is a black hole attacker

    Else is a normal node
}
Return S
}
```

Figure 4 shows the overall working of the classification algorithm. The source node initiates the route recovery process by sending the RREQ and getting the RREP. The source node starts sending the packets, and all the intermediate packets are responsible for checking the intruder as well as the black hole attacker present in the route by having the simply received value of forward time from the previous hop node.

Calculate the threshold value based on the congestion and buffer overflow if forward time varies and the node checks any congestion or buffer overflow in the network. If it varies, then call the classification technique to determine whether the suspicious node is an intruder or a black hole attacker node.

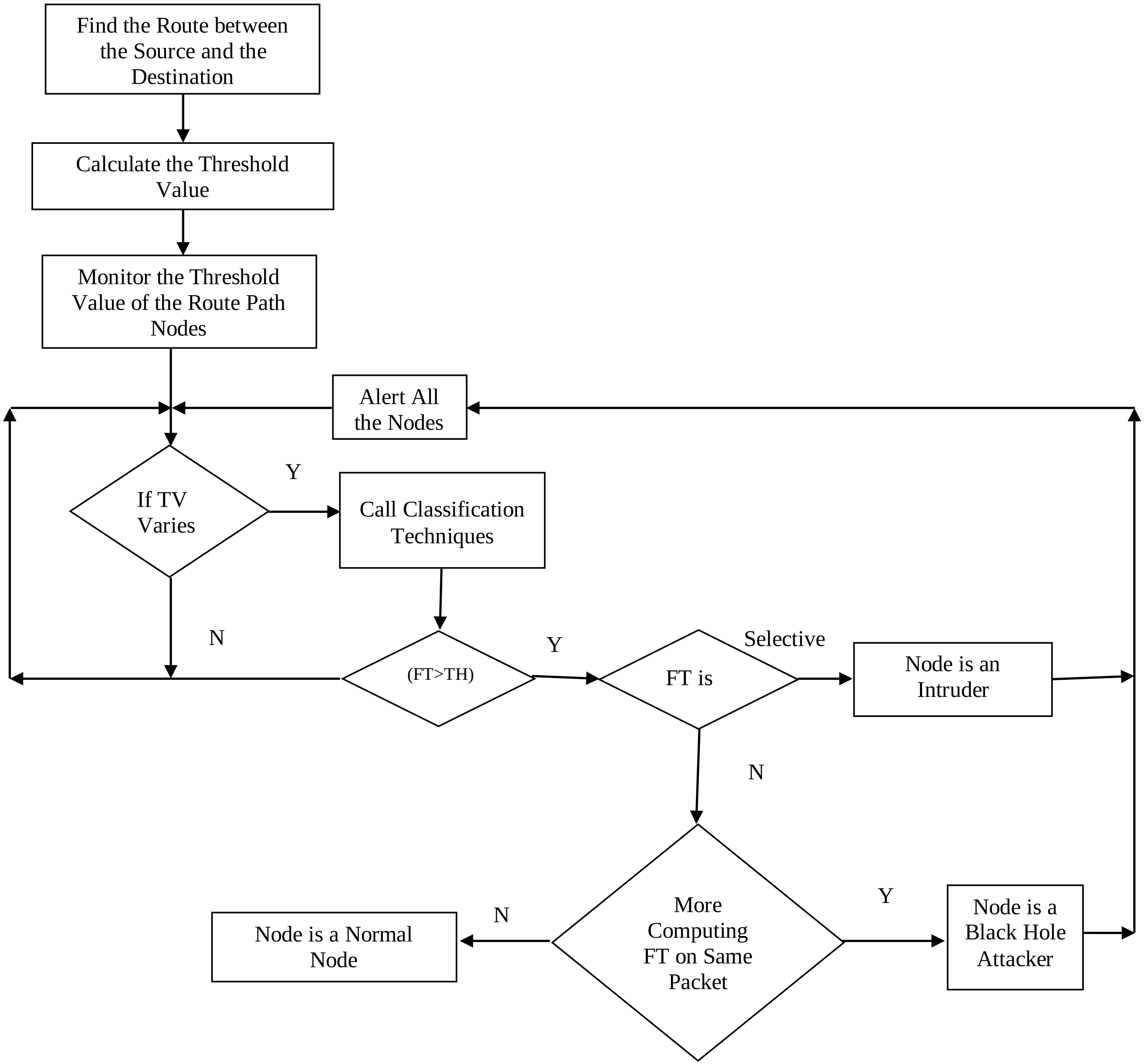
Find the Route between the Source and the Destination
Calculate the Threshold Value
Monitor the Threshold Value of the Route Path Nodes
Alert All the Nodes
If TV Varies
Y
Call Classification Techniques
N
(FT>TH)
Y
FT is
Selective
Node is an Intruder
N
More Computing FT on Same Packet
N
Y
Node is a Normal Node
Node is a Black Hole Attacker

Fig. 4 Classification algorithm

The classification algorithm checks the node delay in packets which is selective for all the packets, and there is no congestion and overflow in the buffer, then decides the node is an intruder. The classification algorithm checks whether the packets are drops but have no overflow in the network and then decides whether the suspicious node is a black hole attacker. Otherwise, the node is a normal node.

The proposed work of intruders, as well as black hole attacker detection techniques, was implemented using the network simulator 2.34 with a total number of nodes and other parameter setup given in Table 2. The On Demand AODV protocol was selected for the route path selection because of the protocol characteristics. Initially, 50 nodes were initiated in the 500*500 meter simulation network area, and the nodes count increased by 50 every 5 ns to reach the 200 nodes maximum; each node's mobility is random, and speed was 0 to 25ms, and the simulation study time was 200 sec, packet transmission of each nodes 10,15,20,25,30,35,40 packets to get the simulation graph values.

To analyse the trace packet values, two different scenarios were created; the first scenario was the AODV protocol without the classification technique, and the classification algorithm was added with the AODV protocol named Classification Algorithm based intruder as well as Black Hole

Attack AODV (CAIBHA-AODV). Two securities-related parameters like, attack rate and attack detection time, were taken for the performance comparison. Attack rate determines the attacks in the MANET, and the attack detection time shows the performance of the classification algorithm.

Two parameters related to the transmission of the packet were taken for the performance comparison: PDR and END. PDR used for reaching out the packet with put drop makes it possible to prove the black hole attacker and end-to-end delay for delay in the packet forwarding which is used for proving the intruder in the MANET communication. The network simulator generated values like Node ID, transmission time, forward time, data received, and buffer size are given to the classification algorithm for predicting the attacker nodes present in the communication.

Table 2. Metric value used for simulation

Metric	Value
Simulator	NS 2.34
Protocol	AODV
Nodes Count	50,100,150, 200
Time	200 sec
Mobility	Random
Speed	0-25 m/s
Network Dimension	500m*500 m
Sending Packet	10,15,20,2530,35,40
Traffic	Constant Bit Rate

3.1. Attack Packet Rate

The ratio of the total number of nodes currently detected as an intruder node and black hole attacker node with the nodes called attack rate. In the beginning, 50 nodes were defined and slowly increased to 100, 150 and 200 nodes, and the route path between the sources to the destination was selected; then one node was set as dropping the packet, and another node was set as delay in transmission. The proposed Classification Algorithm based intruder, as well as Black Hole Attack AODV (CAIBHA-AODV) compared with the existing AODV protocol simulation values, are shown in Table 3, and the comparison graph is depicted in Figure 5.

The result proved that when the nodes are 50nos, the attack rate is 95%; even if the nodes increase, the classification algorithm maintains the constant attack rate, whereas the existing work attack rate fluctuates from 90 to 83% even when the nodes count increases it find difficult to maintain the constant predicting attack rate. The simulation result shows that the proposed CAIBHA-AODV performs the 95% attack rate, where the existing variation varies from 83% to 90%.

Table 3. Attack rate

Nodes	CAIBHA-AODV	AODV
50	90	95
100	90	95
150	88	95
200	82.5	95

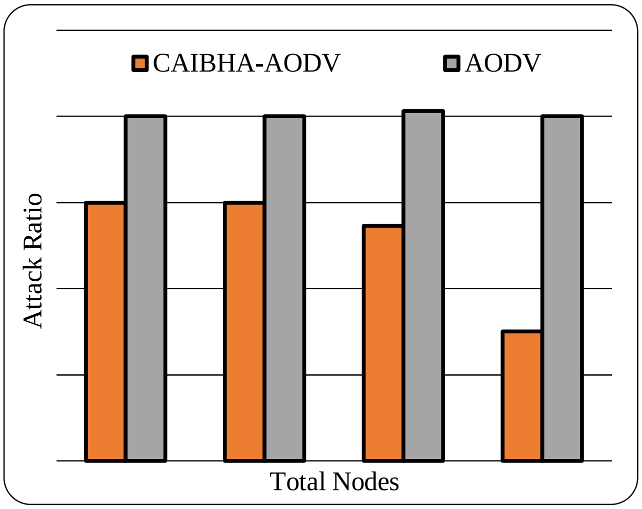

Fig. 5 Attack rate

3.2. Attack Detection Time

The time taken for detection of the first suspicious nodes, which could be the intruder or a black hole attacker called detection time. The simulation of the proposed Classification Algorithm based intruder, as well as Black Hole Attack AODV (CAIBHA-AODV) compared with the existing AODV protocol simulation values, are shown in Table 4, and the comparison graph is depicted in Figure 6. This shows that the proposed CAIBHA-AODV work has proven the attack detection time is less, between 10ms to 25ms, even if the nodes and attackers are increased, which maintains the gradual attack detection time. In contrast, the existing AODV attack detection takes more time, between 15ms to 40ms.

Table 4. Attack detection time

Nodes	CAIBHA-AODV	AODV
50	10	15
100	20	25
150	22	35
200	25	40

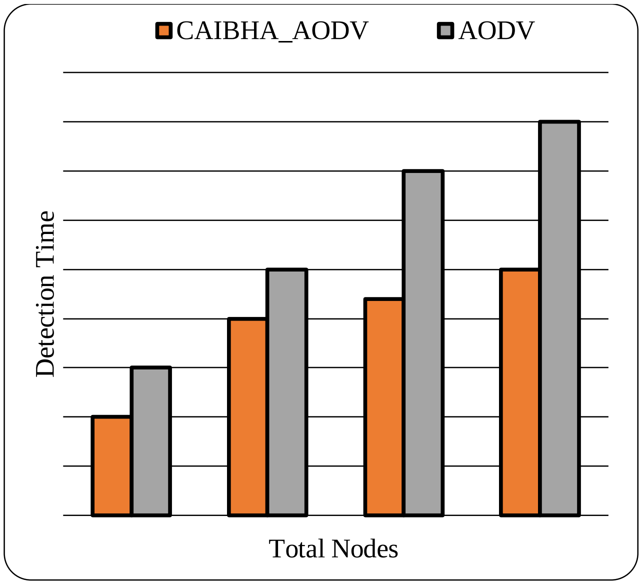

Fig. 6 Attack detection time

3.3. Packet Delivery Ratio

The ratio between the number of packets received by the receiver node and the number of packets sent from the sender node. Initially, the packets are started send set from 10, and slowly increasing by 15, 20,25,30,35, and 40. The defined to one node to delay in the packet and another node to drop the packet to compute the packet delivery ratio.

The simulation result values are shown in Table 5, and the comparison graph shown in Figure 7 which shows that the anticipated CAIBHA-AODV packet delivery ratio is between 90 to 92 %, which maintains even the packet count increased from 10 to 40 packets where, as the existing AODV packet delivery ratio was 55 to 70 %. The existing AODV could find it difficult to deliver the packet when the intruder or black hole attack is present.

Table 5. Packet Delivery Ratio

Packet	AODV	CAIBHA-AODV
10	70	92
15	73	94
20	65	80
25	63	80
30	60	90
35	58	85
40	55	90

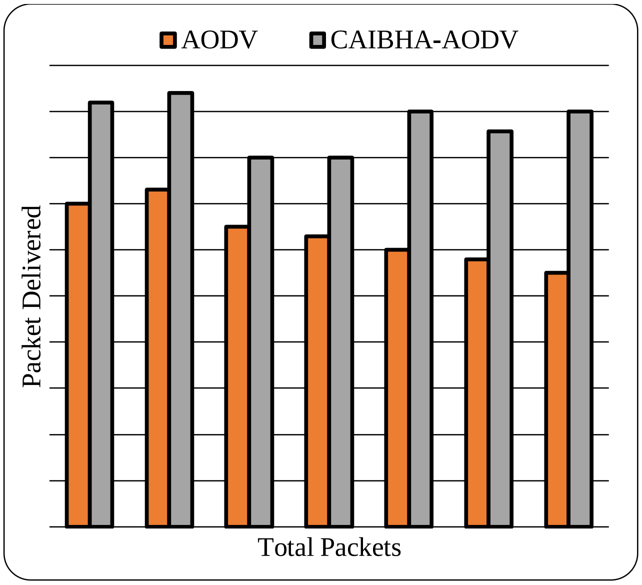

Fig. 7 Packet Delivery Ratio

3.4. End-to-End Delay

End-to-end delay was computed from the delivery packet time difference between the packet sent and the packet received. Initially, the packet sent is set from 10, and slowly increasing by 15, 20,25,30,35, and 40, the defined to one node to delay in the packet and another node to drop the packet to compute the End to End delay.

The simulation result value is shown in Table 6, and the comparison graph shown in Figure 8 shows that the proposed CAIBHA-AODV end-to-end delay is less from 6ms to 24ms even though the packet count increased, whereas the existing end-to-end delay was 8ms to 36ms when the nodes count the nodes delay gets increased proportionally.

Table 6. End-to-end delay

Total Packet	AODV	CAIBHA-AODV
10	8	6
15	3	1
20	18	12
25	14	12
30	20	17
35	31	24
40	36	24

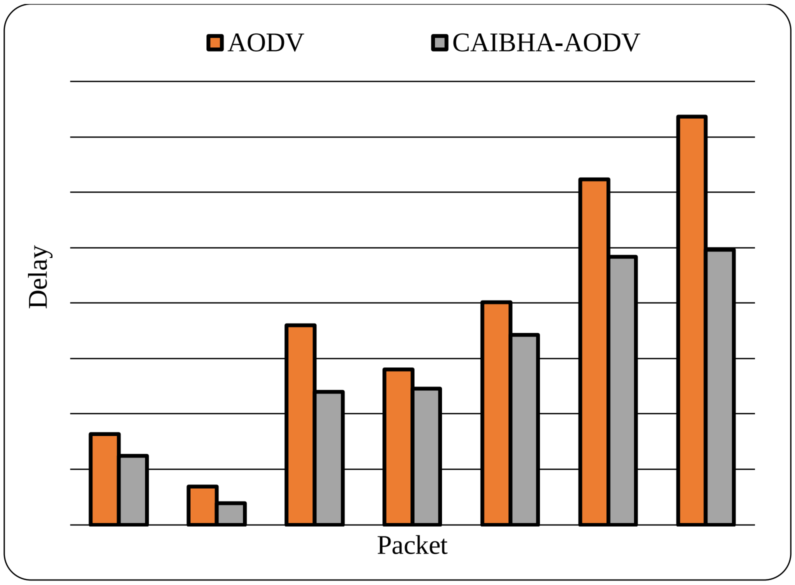

Fig. 8 End-to-end delay

4. Conclusion

This article finds out the simple algorithm to envisage the intruder node and black hole attacker node in the communication with the support of a simple MANET node forward time parameter and classification algorithm. The anticipated work was called Classification Algorithm Base Intruder as well as Black Hole Attack AODV, and it was simulated and outcomes were compared among the standard AODV protocol. The simulation results show that the proposed CAIBHA-AODV work packet delivery ratio is between 90 to 92 %, end-to-end delay is less from 6ms to 24ms, the attack detection time is less between 10ms to 25ms and the attack rate is constant 95%.

In contrast, the existing AODV packet delivery ratio was 55 to 70 %, the end-to-end delay was 8ms to 36ms, attack detection took more time between 15ms to 40ms, and attack rate fluctuated from 90 to 83%, respectively.

References

[1] Tawseef Ahmad Teli, Rameez Yousuf, and Dawood Ashraf Khan, “MANET Routing Protocols Attacks and Mitigation Techniques: A Review,” *International Journal of Mechanical Engineering*, vol. 7, no. 2, pp. 1468-1478, 2022. [Google Scholar] [Publisher Link]

[2] R. Thiagarajan et al., “Optimized with Secure Approach in Detecting and Isolation of Malicious Nodes in MANET,” *Wireless Personal Communications*, vol. 119, pp. 21-35, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Shashi Gurung, and Siddhartha Chauhan, “A Survey of Black-Hole Attack Mitigation Techniques in MANET: Merits, Drawbacks, and Suitability,” *Wireless Networks*, vol. 26, pp. 1981-2011, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Nitin Khanna, and Monika Sachdeva, “A Comprehensive Taxonomy of Schemes to Detect and Mitigate Blackhole Attack and Its Variants in MANETs,” *Computer Science Review*, vol. 32, pp. 24-44, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Gautam M. Borkar, and A.R. Mahajan, “A Review on Propagation of Secure Data, Prevention of Attacks and Routing in Mobile Ad-Hoc Networks,” *International Journal of Communication Networks and Distributed Systems*, vol. 24, no. 1, pp. 23-57, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Nagaraj Balakrishnan, Arunkumar Rajendran, and Ajay P., “Deep Embedded Median Clustering for Routing Misbehaviour and Attacks Detection in Ad-Hoc Networks,” *Ad Hoc Networks*, vol. 126, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Anshu Kumari, Madhvi Singhal, and Nishi Yadav, “Black Hole Attack Implementation and Its Performance Evaluation Using AODV Routing in MANET,” *Inventive Communication and Computational Technologies*, pp. 431-438, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Kollu Spurthi, and T.N. Shankar, “Hybrid Energy Efficient Secured Attribute Based ZRP Aiding Authentic Data Transmission,” *Journal of Scientific & Industrial Research*, vol. 81, no. 1, pp. 69-75, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] R. Suma, B.G. Premasudha, and V. Ravi Ram, “A Novel Machine Learning-Based Attacker Detection System to Secure Location Aided Routing in MANETs,” *International Journal of Networking and Virtual Organisations*, vol. 22, no. 1, pp. 17-41, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Neenavath Veeraiah, and B.T. Krishna, “An Approach for Optimal-Secure Multi-Path Routing and Intrusion Detection in MANET,” *Evolutionary Intelligence*, vol. 15, pp. 1313-1327, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Neenavath Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," *IEEE Access*, vol. 9, pp. 120996-121005, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Nitesh Ghodichor et al., "Secure Routing Protocol against Internal and External Attack in MANET," *Proceedings of the International Conference on Emerging Trends in Artificial Intelligence and Smart Systems*, pp. 1-8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Pooja Rani et al., "Mitigation of BH and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network," *IEEE Access*, vol. 8, pp. 121755-121764, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Dost Muhammad Khan et al., "Black Hole Attack Prevention in Mobile Ad-Hoc Network (MANET) Using Ant Colony Optimization Technique," *Information Technology and Control*, vol. 49, no. 3, pp. 308-319, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Mahuwa Goswami, Prashant Sharma, Ankita Bhargava, "Black Hole Attack Detection in MANETs Using Trust Based Technique," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 4, pp. 1446-1451, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Zohaib Hassan et al., "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," *IEEE Access*, vol. 8, pp. 199618-199628, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sadoon Hussain et al., "AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks," *Applied Computational Intelligence and Soft Computing*, vol. 2022, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohamad T. Sultan, Hesham El Sayed, and Manzoor Ahmed Khan, "An Intrusion Detection Mechanism for MANETs Based on Deep Learning Artificial Neural Networks (ANNs)," *International Journal of Computer Networks & Communications*, vol. 15, no. 1, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Shweta Pandey, and Varun Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India, pp. 797-802, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Maria Hanif et al., "AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks," *Electronics*, vol. 11, no. 15, pp. 1-28, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Sivanesan Narayanan, and A. Rajesh, "Mitigating Intruder Detection System in Mobile Adhoc Network (MANET) Using Optimizer Based ANN Model," *KeAi: Cyber Security & Applications*, pp. 1-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] S. Murali, and V. Sathya, "Reliability Assessment and Detection of Nodes Causing a Blackhole Attack in Portable Informal Networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 8s, pp. 173-185, 2024. [Google Scholar] [Publisher Link]

[23] Shaik Shafi, S. Mounika, and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," *Procedia Computer Science*, vol. 218, pp. 2309-2318, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] S. Vijayalakshmi et al., "Hybrid Defense Mechanism against Malicious Packet Dropping Attack for MANET Using Game Theory," *Cyber Security and Applications*, vol. 1, pp. 1-9, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Sampada H.K., and Shobha K.R., "Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On-Demand Distance Vector Routing Protocol in MANETs," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 11, no. 1, pp. 13-28, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] C. Edwin Singh, and S. Maria Celestin Vigila, "Fuzzy Based Intrusion Detection System in MANET," *Measurement: Sensors*, vol. 26, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[27] Oyenike Mary Olanrewaju, Abdulwasiu Adebayo Abdulhafeez Abdulwasiu, and Abdulhafiz Nuhu, "Enhanced On-Demand Distance Vector Routing Protocol to Prevent Blackhole Attack in MANET," *International Journal of Software Engineering and Computer Systems*, vol. 9, no. 1, pp. 68-75, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Jayantkumar A. Rathod, and Manjunath Kotari, "TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 11, no. 1, pp. 61-81, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Jyoti Dhanke et al., "An Efficient Approach for Prevention of Blackhole Attack in MANET," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 12s, pp. 743-752, 2024. [Google Scholar] [Publisher Link]

[30] Aurelle Tchagna Kouanou et al., "Machine Learning for Intrusion Detection in Ad-hoc Networks: Wormhole and Blackhole Attacks Case," *Cloud Computing and Data Science [Internet]*, vol. 5, no. 1, pp. 62-79, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] Ashraf Abdelhamid et al., "A Lightweight Anomaly Detection System for Black Hole Attack," *Electronics*, vol. 12, no. 6, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]