**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Securing AODV Against Black Hole Attack For Wireless Mesh Network

Vanlalhruaia[1*], Ajoy Kumar Khan[2], Amit Kumar Roy[3]

[1]Department of Computer Engineering, School of Engineering and Technology, Mizoram University, Aizawl, 796004, Mizoram, India; hruai_a56@yahoo.com
[2]Department of Computer Engineering, School of Engineering and Technology, Mizoram University, Aizawl, 796004, Mizoram, India; ajoyiitg@gmail.com
[3]Department of Computer Science and Engineering, Indian Institute of Information Technology Kottayam, Kottayam, 686635, Kerala, India; amit@iiitkottayam.ac.in

*__Correspondence__: Vanlalhruaia
Email: hruai_a56@yahoo.com

**ARTICLE INFO**

Received: 22 Dec 2024

Revised: 14 Feb 2025

Accepted: 26 Feb 2025

**ABSTRACT**

Wireless Mesh Networks (WMNs) offer flexible and scalable communication solutions but are vulnerable to various security threats, including black hole attacks. These attacks exploit the reactive nature of routing protocols like the Ad hoc On-Demand Distance Vector (AODV), which is commonly used in WMNs. Black hole attacks disrupt network operations by falsely advertising optimal paths, leading to data packet losses. To address this, we propose a detection mechanism for identifying malicious nodes in AODV-based WMNs. Our approach utilizes destination sequence number comparison and hop count verification to identify inconsistencies caused by black hole nodes. Through simulation and analysis, we demonstrate the effectiveness and efficiency of the proposed method, showing its ability to significantly mitigate the impact of black hole attacks on WMNs.

**Keywords**: Wireless Mesh Network, AODV, Black hole, Sequence number, Hop count, Routing

## 1.Introduction

The technology that provides global wireless internet access, called Wireless Mesh Networks (WMNs), is regarded as one of the greatest internet technologies because it offers high-quality data transmission [1]. Users can access high-bandwidth wireless networks for ubiquitous services anytime and anywhere, thanks to the emergence of ubiquitous computing and the recent rapid development of wireless network technology. Due to their wide signal coverage, low deployment costs, and high transmission rates, WMNs have gradually replaced wired networks.

A typical Wireless Mesh Network (WMN) is hierarchically structured, consisting of Mesh Routers (MRs), Mesh Clients (MCs), and Internet Gateways (IGWs), as illustrated in Fig. 1.The IGWs, which connect to the wired network, form the top tier of this hierarchy. MRs, functioning at layer 2, act as stationary access points (APs) interconnected via wireless links. These MRs facilitate the routing of traffic from MCs to IGWs using multi-hop methods. MCs, operating at layer 3, connect to the nearest available MR either directly or through multiple hops[2]. Their self-configuring and self-organizing capabilities are beneficial for establishing and maintaining community connectivity. Each node in a WMN can function as either an MC or an MR[3].

An MC is essentially a user device and typically acts as the endpoint for network data transmissions. MRs form a wireless backbone that connects the MCs. The MGs function as the connection points between the WMN and a wired network, usually the Internet. Consequently, when a network request originates from an MC, it is transmitted to the wireless backbone via the connected MR. The request may pass through several hops before reaching an MG, and from there, it is routed to the Internet (and vice versa)[4]. A gateway is the target of the majority of WMN traffic [5].

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

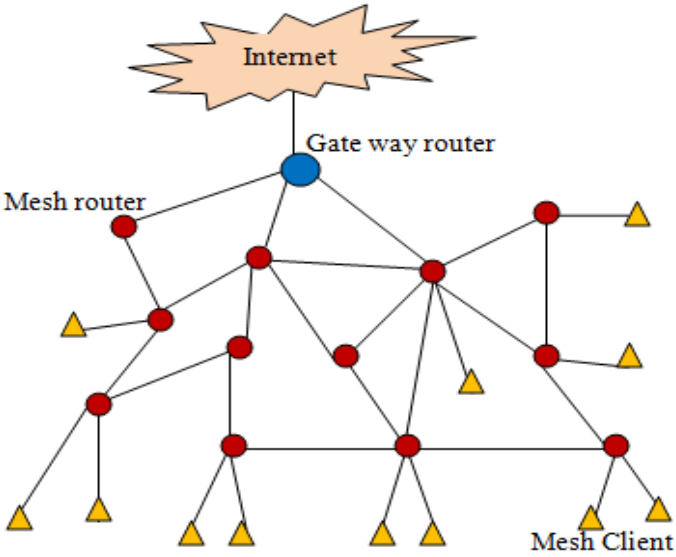


**Fig 1: Wireless Mesh Network**

Because of its quick implementation and low cost, Wireless Mesh Networks (WMNs) are becoming a popular new communication paradigm. Applications for wireless mesh networks (WMNs) include disaster recovery, intelligent transportation systems, transitory networks in convention centers, and wireless broadband Internet access.

Since Wireless Mesh Networks (WMNs) share similar traits with wireless ad hoc networks, routing protocols developed for MANETs can also be applied to WMNs[6]. The three main routing protocols recommended for mobile ad hoc networks (MANETs) are Ad hoc On-Demand Distance Vector (AODV)[7], Dynamic Source Routing (DSR)[8], and Destination-Sequenced Distance Vector (DSDV)[9][10]. DSR and AODV are examples of on-demand routing protocols, while DSDV follows a table-driven approach. This paper focuses on AODV, though the proposed solution can be adapted for use with other on-demand protocols with minimal adjustments.

AODV is the most commonly used on-demand routing protocol among all available options. However, since security was not a primary focus during its development, malicious nodes can exploit vulnerabilities in the protocol to carry out various attacks. Additionally, due to the inherent nature of MANETs, they are vulnerable to numerous threats, including DoS attacks such as Wormhole, Sinkhole, Gray hole, and Black hole, as well as spoofing, flooding, eavesdropping, and packet modification[11].

One benefit of AODV routing is that it eliminates the need for source routing[12], which reduces packet transfer overhead. The messages cannot be sent if the path becomes inoperable and the connection is lost. If a node detects the link disruption, the route error (RERR) message is transmitted. The unreachable location is shown in the RERR message. Nodes that receive such messages deactivate the route. Even in scenarios where nodes are moving constantly. In order to do wireless network routing, AODV routing is dependable, loop-free, and does not require a centralized network system. Because AODV routing is self-starting and loop-free, it eliminates the need for setting and releasing connections to determine the destination and last route[13].

A specific kind of attack known as a "Black Hole" attack jeopardies the security of the AODV protocol [14].In order to intercept packets, a malicious node in this attack presents itself as the one with the quickest path to the target node.In a black hole attack, a malicious node falsely advertises itself as having the shortest path to the destination node, thereby attracting all the traffic and then dropping it, preventing the legitimate communication from occurring.

During the route discovery phase of AODV, when a source node broadcasts a Route Request (RREQ) to find a route to the destination, the malicious node responds with a Route Reply (RREP) that claims it has a fresh route to the destination.The malicious node sets a high sequence number in the RREP, indicating that its route is fresher than any other routes that might be discovered.The source node, trusting this information, updates its routing table to direct traffic to the malicious node, believing it to be the quickest and most reliable path.Once the malicious node successfully inserts itself into the routing path, it intercepts all data packets intended for the destination. Instead of forwarding these packets, the malicious node discards them, effectively creating a "black hole" where data enters but does not emerge from the other side. When a single malicious node attacks the network, it is called single black hole attack

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

but when multiple black hole node work together it become cooperating black hole attack. This kind of attack greatly reduce network performance.

## 2.Related works

Several numbers of protocols have been proposed to counter black hole attack in MANET, but relatively few researches have been done on WMNs even though the two networks share many similar characteristic and routing protocols, they are slightly different in some characteristics like node mobility, infrastructure etc. In this section we briefly discuss some of the existing protocols which are related to our proposed protocol.

Sashi Gurung and Siddarth Chauhan[15] conducted an extensive review of techniques for mitigating black hole attacks. They categorized these methods based on various approaches, including cryptography, overhearing, sequence number threshold, acknowledgment, clustering, cross-layer collaboration, cross-checking, trust, intrusion detection systems, hybrid techniques, and others. In this classification, the proposed model falls under the cross-checking approach, where nodes maintain a Data Routing Information (DRI) table. A drawback of these methods is the increase in average end-to-end delay, mainly due to frequent path breaks caused by node mobility. However, this is less of an issue in WMNs, as the nodes (MRs) are stationary, and the proposed protocol addresses the delay caused by the cross-checking process performed by the source node.

In [16] the authorsProposed black hole protected AODV(BP-AODV) protocol based on chaotic map, in this protocol the source node insert challenge value, this value is response by the destination node using logistic chaotic map. The route discovery process composed of three steps: route request, route reply and route confirm. In route request the intermediate node is allowed to process up to three route requestsfrom different forwarding node. When the route request finally reaches the destination node it sends out route reply with response value, the response value is not fixed and depends on source and destination pair along with other parameter in each route request, this makes the protocol secure and resilient against black hole attack. The experimental result show good performance in this protocol, but there is significant delay in route discovery process as the destination node need to reply to each route request that need to be addressed.

In [17] the authors proposed detection of smart black hole node based on sequence number threshold, it is considered that the smart black hole node have intelligence to predict the sequence number of the destination node. The proposed protocol added two field in AODV route reply packet such as shared sequence numberand creation time of the RREP packet (timestamp). Analyzing the increasing timestamp and the sequence number the destination sequence number threshold value is set. Setting the safety margin value is a crucial part in this technique setting too high can increase false detection rate and too low can cause increase in undetected black hole node. It is likely that threshold value of a node that involve in data transmission in discrete time interval is difficult to predict.

In the DPS (Detection and Prevention System) network[18] suggested deploying some nodes with unique capability that continuously monitor the RREQs that are advertised by all other nodes in the network. DPS nodes seek to fulfill predetermined goals, one of which is to identify misbehaving nodes by observing their nearby neighbors' actions. When a node exhibits unusual behavior, as determined by experimental data, the DPS node labels that specific suspicious node as a black hole node by sending a threat message to every other node in the network. This protocol uses an AODV routing protocol clustering technique to detect and prevent the black hole attack. As a result, empirical analysis demonstrates that the black hole node is isolated from the rest of the system, forbidden from receiving data from any other node, and is not permitted to receive data at all.

In [19], the authorProposedtrust-based weighing method for detecting black hole node by considering three parameter such as node energy, buffer size and packet drop. the average of these parameters is collected from all nodes in the network, if energy and buffer size is smaller and packet drop is higher than average for particular node it is consider as suspicious black hole node, then the whole weight of suspected node is estimated with normalized value. if the trust weight is smaller than average trust weight of all nodes in the network it is consider as black hole node. This trust-based technique is efficient for improving the performanceand security.

In [20] the authors proposed detection technique by sending forge route request, the black hole node reply with high destination sequence number even if the destination does not exist in the network. When actual route request is broadcast, the route reply received are analyzed and the abnormally high sequence number in the route reply is consider to be coming from black hole node.

The authors of [21] Proposed fake route request technique, in the proposed method the route request packet contain source node own address and sequence number, the route reply received with higher

Journal of Information Systems Engineering and Management
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

sequence number can be considered to be coming from black hole node, then the source node send alarm packet to inform other nodes about the identity of black hole node.
The authors of[22] Proposed Anti Black hole, Grey hole and Flooding AODV, in this protocol the source node collect three route reply, from these the average and standard deviations of the destination sequence number is calculated, if the threshold value exceed the average then the presence of malicious node is confirmed and ALERT packet is transmitted in the network. This protocol can handle three different type of attack which is the great advantage.

## 3.Proposed Protocol

One of the advantages of AODV routing protocol is the ability of an intermediate node send route reply if it has a valid route, this greatly reduce route discovery time if the network size is large. But this open opportunity for an attacker to send fake route reply to disguise the source node in order to attract data traffic. This paper aim to reduce route discovery time and detect black hole node. In order to achieve these the following assumptions are made:
The source node and the destination node are not black hole node.
Even if the cooperating black hole nodes exist, the black hole node who receive route request always send route reply instead of forwarding to another black hole node.
Black hole node does not have intelligence to calculate destination sequence number or hop count.
Black hole node does not changes behavior.
Other types of attack are not considered in the proposed protocol.

In the proposed protocol each node maintains a list of trusted nodes, If a particular node send data packet to the destination successfully this indicate that there is no black hole node, so every nodes along the path including source and destination add one another in their trusted list. This can be achieved by adding ID by each node along the path in first data packet, then the destination node can send back along with acknowledgement and each node on the path can copy this list of trusted nodes.The proposed protocol consists of three steps:
*(i)Route request*
*(ii) Route reply and route verification*
*(iii) Route confirmation.*
When the source node wants to send data, it broadcast RREQ, an intermediate node who does not have valid route rebroadcast RREQ ultimately when RREQ reach the destination then the destination sends back RREP, then the route is valid and data packet can be sent. An intermediate node who have valid route(or claim to have valid route in case black hole node) perform the following:
(i)Check whether the source node is trusted node.
*(a)*if so send RREP, upon receiving RREP the source node checks its own trusted list and found that the intermediate node is trusted node then data packet can be sent.
*(b)*If the source node is not trusted node, send RREP to source and send route verification message towards the destination. the route verification message has the following fields {*source ID, destination ID, destination sequence number, intermediate node ID, Hop count* for each node along the destination}

<table>
<tr><td colspan="5">Source ID</td></tr>
<tr><td colspan="5">Destination ID</td></tr>
<tr><td colspan="5">Destination sequence number</td></tr>
<tr><td>Intermediate node ID</td><td>Next node ID</td><td>...</td><td>....</td><td>...</td></tr>
<tr><td>hop count</td><td>hop count=previous hopcount -1</td><td>....</td><td>....</td><td>....</td></tr>
</table>

**Fig 2: Route verification message**

Upon receiving route verification message, a node performs the following:
(ii)Check whether it have route to destination, whether the destination sequence number are same, if its hop counts equal to previous hop count-1. If any check is failed, declare all the nodes(*forth field*) in route verification message as black hole nodes.
If all check is pass, check whether the source is trusted node, if so send route confirmation message otherwise insert its own ID and hop count and forward to the next node.
The route verification message keeps forwarding until trusted node or destination node is found.

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

## 4.Simulation and result discussion

Simulation is performed in NS3 with 30 mesh routers the performance of each router is examined, the performance of proposed protocol is compared with AODV and AODV with Black hole nodes, the simulation parameter in table 1, the performance of each node is shown in table 2.

**Table 1: Simulation parameter**

| Parameter | Value |
|---|---|
| Area | 500m × 500m |
| Data rate | 5 pks/s |
| Packet Size | 64 bytes |
| Traffic | CBR |
| Transmission Range | 250m |

### 4.1 Throughput

It defines the total number of data packet sent/received per unit time. Figure 3(a), Figure 3(b) and Figure 3(c) Show the throughput for AODV without Black hole, AODV with Black Hole node and Proposed protocol respectively. From the simulation result the average throughput for proposed protocol is 21.48Mbps which is better than other two.

**Table 2: Throughput, Packet Delivery Ratio, End to End Delay Comparison andblack hole detection rate**

| Routers | Throughput(Mbps) | | | Packet Delivery Ratio(%) | | | End to End Delay(ms) | | | Black Hole Detection rate (%) |
|---|---|---|---|---|---|---|---|---|---|---|
| | AODV with black hole | AODV without Black Hole | Proposed | AODV with black hole | AODV without Black Hole | Proposed | AODV with black hole | AODV without Black Hole | Proposed | Proposed |
| 1 | 9.88 | 15.03 | 15.62 | 76.81 | 87.85 | 86.97 | 290.25 | 245.73 | 23.85 | 75.86 |
| 2 | 12.08 | 14.74 | 15.8 | 82.27 | 83.71 | 88.62 | 448.03 | 184.86 | 147.64 | 83.64 |
| 3 | 13.18 | 14.1 | 21.97 | 77.14 | 80.64 | 92.75 | 415.81 | 274.19 | 119.78 | 76 |
| 4 | 10.0 | 14.04 | 21.97 | 83. | 85.73 | 94.59 | 298. | 102.6 | 34.43 | 84.57 |

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 4 | | | 09 | | | 03 | 5 | | |
| 5 | 7.13 | 16.41 | 22.93 | 83.34 | 86.79 | 96.51 | 373.81 | 281.11 | 174.54 | 82.07 |
| 6 | 7.08 | 13.41 | 25.18 | 77.39 | 86.12 | 84.86 | 445.36 | 133.42 | 174.57 | 81 |
| 7 | 12.07 | 12.31 | 22.85 | 82.6 | 81.98 | 92.94 | 110.25 | 297.27 | 38.45 | 83.86 |
| 8 | 14.18 | 18.44 | 22.47 | 75.08 | 85.64 | 88.26 | 149.14 | 132.65 | 148.88 | 93.43 |
| 9 | 15.04 | 14.97 | 24.82 | 81.27 | 83.71 | 84.5 | 140.25 | 139.57 | 148.52 | 92.29 |
| 10 | 14.05 | 11.62 | 20.86 | 75.66 | 86.98 | 93.67 | 104.69 | 258.8 | 128.77 | 86.79 |
| 11 | 5.91 | 14.22 | 20.72 | 79.29 | 84.48 | 86.33 | 158.03 | 258.8 | 198.84 | 86.64 |
| 12 | 6.13 | 13.52 | 17.8 | 81.85 | 83.81 | 91.65 | 358.03 | 100.34 | 89.88 | 79.43 |
| 13 | 11.19 | 17.74 | 21.61 | 74.99 | 82.46 | 85.69 | 398.58 | 223.42 | 137.98 | 80.57 |
| 14 | 9.13 | 15.32 | 19.08 | 81.44 | 82.37 | 94.4 | 199.25 | 287.27 | 173.86 | 71.86 |
| 15 | 15.1 | 13.64 | 23.65 | 76.48 | 87.94 | 88.72 | 162.14 | 64.19 | 36.88 | 92 |
| 16 | 9.08 | 17.45 | 19.04 | 78.05 | 82.56 | 90.46 | 269.95 | 153.42 | 76.97 | 80 |
| 17 | 12.02 | 13.12 | 21.58 | 79.62 | 79.77 | 87.25 | 249.81 | 279.57 | 179.86 | 76.57 |
| 18 | 15.14 | 19.59 | 23.72 | 80.53 | 79.48 | 95.96 | 232.47 | 159.57 | 49.88 | 78.5 |
| 19 | 10.07 | 15.37 | 24.39 | 79.46 | 78.91 | 93.3 | 363.58 | 64.96 | 155.73 | 85.71 |
| 20 | 13.13 | 10.63 | 15.8 | 77.14 | 81.21 | 89.36 | 183.58 | 100.34 | 161.34 | 79.14 |

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 21 | 13.93 | 17.05 | 23.72 | 80.37 | 79.77 | 90.37 | 382.69 | 138.8 | 136.88 | 76.86 |
| 22 | 9.14 | 10.98 | 16.48 | 83.26 | 84.87 | 91.56 | 148.14 | 50.34 | 86.85 | 88.43 |
| 23 | 14.87 | 19.02 | 24.86 | 79.13 | 80.73 | 92.75 | 205.81 | 58.04 | 151.84 | 82.64 |
| 24 | 6.83 | 14.62 | 24.22 | 78.55 | 84.1 | 88.17 | 385.81 | 287.27 | 129.73 | 74.36 |
| 25 | 13.13 | 12.48 | 24.14 | 83.09 | 85.35 | 97.16 | 106.92 | 201.11 | 99.87 | 76.14 |
| 26 | 6.14 | 13.35 | 20.29 | 79.04 | 83.33 | 90.28 | 133.81 | 291.88 | 127.64 | 76.36 |
| 27 | 12.01 | 18.38 | 19.33 | 84.83 | 83.33 | 90.64 | 309.45 | 100.34 | 99.61 | 82.5 |
| 28 | 13.03 | 15.84 | 24.22 | 79.46 | 78.42 | 95.69 | 355.03 | 227.27 | 176.04 | 91 |
| 29 | 11.06 | 16.18 | 23.32 | 75.24 | 84.48 | 88.99 | 310.85 | 168.8 | 150.64 | 95 |
| 30 | 15.93 | 20 | 21.93 | 84.99 | 81.21 | 96.51 | 409.14 | 278.04 | 33.8 | 89.79 |
| **Avg** | **11.26** | **15.11** | **21.48** | **79.72** | **83.26** | **90.96** | **269.96** | **184.80** | **119.78** | **82.76** |

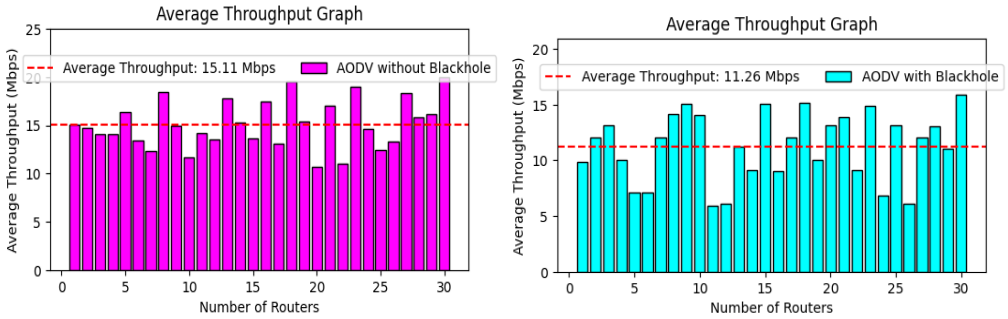


**Fig 3: (a) Throughput for AODV without Black Hole. (b)Throughput for AODV with Black Hole.**

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

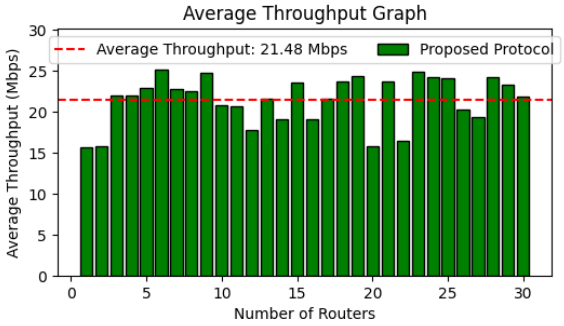


**Fig 3. (c) Throughput for Proposed Protocol.**

### 4.2 Packet Delivery Ratio

It represents the ration of total data packet received by total data packet sent. Figure 4(a), Figure 4(b) and Figure 4(c) Show thePacket delivery ratio for AODV without Black hole, AODV with Black Hole node and Proposed protocol respectively. From the simulation result the packet delivery ratio for proposed protocol is 90.96% which is better than other two.

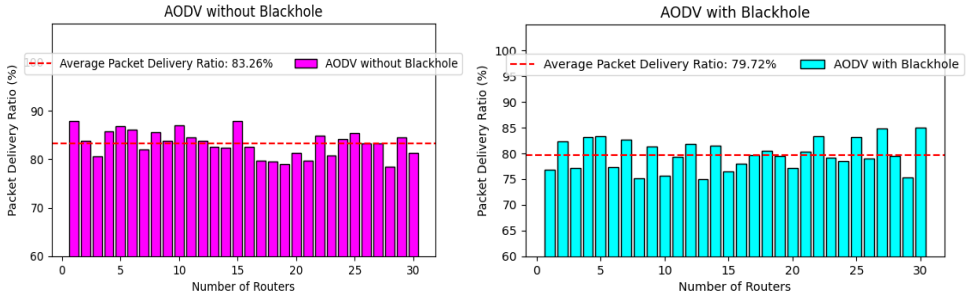


**Fig4. (a) Packet delivery ratio for AODV without Black Hole.(b) Packet delivery ratio for AODV with Black Hole**

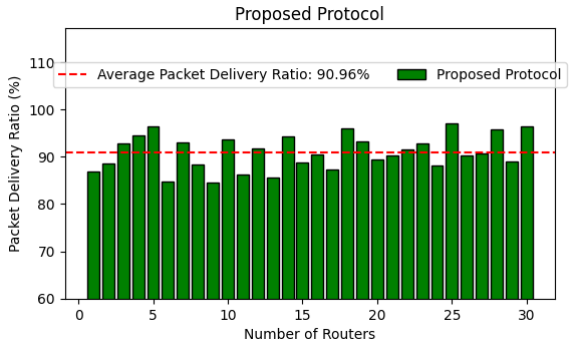


**Fig4(c): Packet delivery ratio for Proposed Protocol**

### 4.3 End to End delay

It refers to the time taken by data packet to travel from source to destination. Figure 5(a), Figure 5(b) and Figure 5(c) Show the end to end delayfor AODV without Black hole, AODV with Black Hole node and Proposed protocol respectively. From the simulation result end to end delay proposed protocol 119.78ms which is better than other two.

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

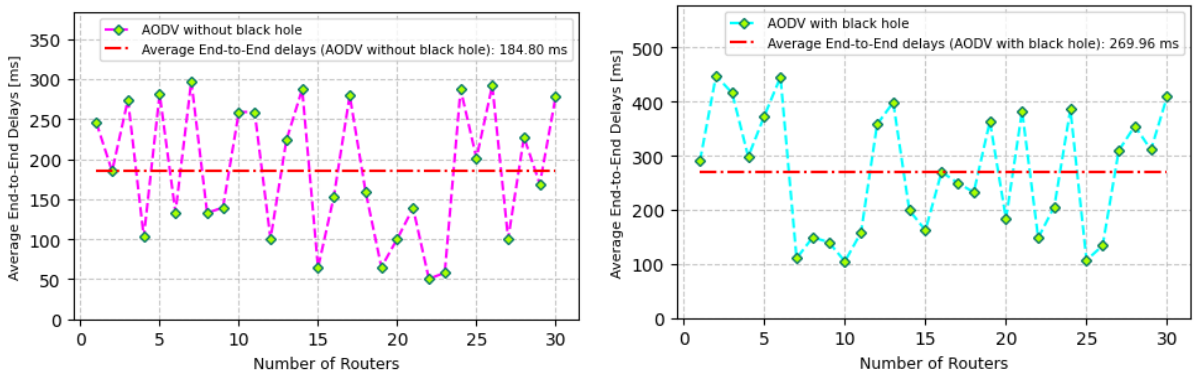


**Fig 5. (a) End to End delay for AODV without black Hole.(b) End to End delay for AODV with black Hole**

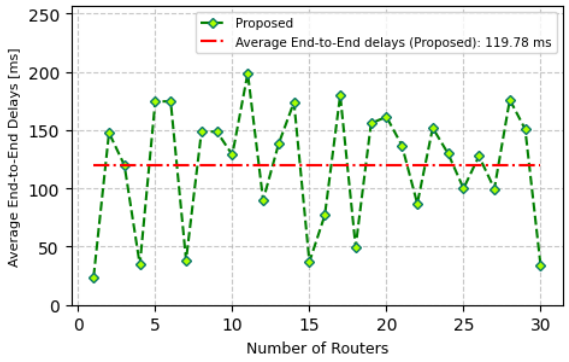


**Fig 5. (c) End to End delay for Proposed Protocol**

### 4.4 Black Hole detection rate

It represents percentage of black hole detected by each node, the number of black holes in the network is 10, a node that initiate route request detect black hole node. Black hole node detection rate is shown in Fig 6.

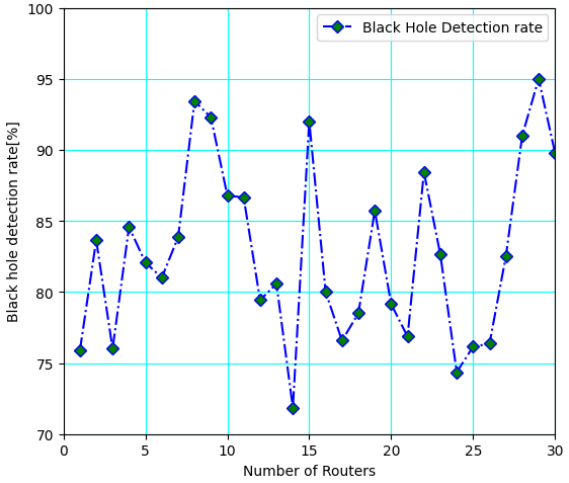


**Fig 6: Black Hole detection rate**

## 5.Conclusion

The proposed protocol detects black hole node with the help of trusted node, instead of detecting black hole node by source all the trusted node cooperating in detection of black Hole node, the proposed protocol reduces data traffic for detection of black hole node as it does not send route verification message to the source node. This also reduce bandwidth consumption. The nodes with higher number of

trusted nodes perform faster in detection/route confirmation, the node highly involve in data transfer have higher number of trusted nodes. The performance of the proposed protocol in throughput, end to end delay and packet delivery ratio is better in comparison with AODV and AODV with black hole node.

## References

[1] PK. Sharma, R. Mahajan, Surender. "A security architecture for attacks detection and authentication in wireless mesh networks", *Cluster Computing,* 20, pp. 2323-2332, 2017. doi: 10.1007/s10586-017-0970-9

[2] A, Prathapani, L. Santhanam, DP. Agrawal. "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents", *The Journal of Supercomputing,* 64,pp. 777-804, 2013. doi: 10.1007/s11227-010-0547-3

[3] SK. Dhurandher, et al. "A distributed adaptive admission control scheme for multimedia wireless mesh networks", *IEEE Systems Journal,* 9(2), pp. 595-604, 2014. doi: 10.1109/JSYST.2013.2296336

[4] S. Karunaratne, H. Gacanin. "An overview of machine learning approaches in wireless mesh networks", *IEEE Communications Magazine,* 57(4), pp. 102-108, 2019, doi: 10.1109/MCOM.2019.1800434

[5] AN. Le, et al. "Directional AODV routing protocol for wireless mesh networks", In *18th International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, pp. 1-5, 2007.doi: 10.1109/PIMRC.2007.4394647

[6] O. Shree, M. Talib. "Using merkle tree to mitigate cooperative black-hole attack in Wireless Mesh Networks",*International Journal of Advanced Computer Science and Applications,* 2(5), pp. 1-6,2011.doi: 10.14569/IJACSA.2011.020501

[7] CE. Perkins, EM. Royer. "Ad hoc on-demand distance vector (AODV) routing", In *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 2003. doi: 10.1109/MCSA.1999.749281

[8] DB. Johnson, DA. Maltz. "Dynamic source routing in ad hoc wireless networks." *Mobile computing,* 353, pp. 153-181, 1996. doi: 10.1007/978-0-585-29603-6_5

[9] CE. Perkins, P. Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." *ACM SIGCOMM computer communication review,* 24(4), pp. 234-244, 1994. doi: 10.1145/190314.190336

[10] EM. Royer, CK. Toh. "A review of current routing protocols for ad hoc mobile wireless networks." *IEEE personal communications,* 6(2), pp. 46-55, 1999. doi: 10.1109/98.760423

[11] N. Mistry, DC. Jinwala, M. Zaveri. "Improving AODV protocol against blackhole attacks." *International multiconference of engineers and computer scientists*, 2(6), 2010.

[12]S. Rani, et al. "An optimized framework for WSN routing in the context of industry 4.0." *Sensors,* 21(19),pp. 6474, 2021.doi: 10.3390/s21196474

[13] A. Bhatia, et al. "Networked control system with MANET communication and AODV routing." *Heliyon,* 8(11), 2022.doi: 10.1016/j.heliyon.2022.e11678

[14] H. Deng, W. Li, DP. Agrawal. "Routing security in wireless ad hoc networks." *IEEE Communications magazine,* 40(10), pp. 70-75, 2002. doi: 10.1109/MCOM.2002.1039859

[15] S. Gurung, S. Chauhan. "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability." *Wireless Networks,* 26, pp. 1981-2011, 2020. doi: 10.1007/s11276-019-01966-z

[16]El-Semary, M. Aly, H. Diab. "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map." *IEEE Access* 7, pp. 95197-95211, 2019. doi: 10.1109/ACCESS.2019.2928804

[17]T. Terai, et al. "Blackhole attack cooperative prevention method in manets." In *Eighth International Symposium on Computing and Networking Workshops (CANDARW)*. Pp. 60-66, 2020.doi: 10.1109/CANDARW51189.2020.00024

[18] IA. Shah, N. Kapoor. "To Detect and Prevent Black Hole Attack in Mobile Ad Hoc Network." In *2nd Global Conference for Advancement in Technology (GCAT)*,pp. 1-4, 2021.doi: 10.1109/GCAT52182.2021.9587471

**Journal of Information Systems Engineering and Management**
2025, 10(37s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

[19] V. Dani. "iBADS: An improved Black-hole Attack Detection System using Trust based Weighted Method." *Journal of Information Assurance & Security,* 17(3), pp. 91, 2022.
[20]Kheeramani, S. Thakur. "Detection and removal of multiple black hole attacks through sending forged packet in MANETs."*International Research Journal of Engineering and Technology*,9(5), pp. 140-144, 2022.
[21]Moumen, Idriss, et al. "AODV-based Defense Mechanism for Mitigating Blackhole Attacks in MANET." In*International Conference on Innovation in Modern Applied Science, Environment, Energy and Earth Studies 3S Web of Conferences*, pp. 11, 2023.doi: 10.1051/e3sconf/202341201094
[22] S. Gurung, V.Mankotia. "ABGF-AODV protocol to prevent black-hole, gray-hole and flooding attacks in MANET." *Telecommunication Systems,* 86, pp. 811-827, 2024. doi:10.1007/s11235-024-01154-1