American Journal of Robotics and Intelligent Systems
2026, Vol. 1, No. 1, pp. 27–37
https://doi.org/10.11648/j.ajris.20260101.14

SciencePG
Science Publishing Group

Research Article

Intelligent Hybrid Multipath Routing Protocol for Congestion and Black Hole Attack Mitigation in Mobile Ad-hoc Networks

Misgana Merga Iticha[1, *], Nega Firdissa Huluka[2], Soressa Beyene Lemu[3]

[1]Department of Computer Networking, Wollega University, Nekemte, Ethiopia
[2]Department of Computer Networking, Salale University, Fiche, Ethiopia
[3]Department of Information Science, Bule Hora University, Bule Hora, Ethiopia

Abstract

Mobile Ad-hoc Networks (MANETs) are decentralized, self-organizing wireless networks that operate without fixed infrastructure. Despite their flexibility, they are highly susceptible to congestion and black hole attacks, which significantly degrade throughput, packet delivery ratio (PDR), and overall Quality of Service (QoS). This paper introduces an enhanced hybrid routing protocol Black Hole and Congestion Overcome AOMDV (IH-AOMDV) as an optimized extension of the Ad-hoc On-Demand Multipath Distance Vector (AOMDV) protocol. The proposed approach integrates congestion awareness and security mechanisms by combining throughput-based congestion detection with sequence-number-based route validation to identify and isolate congested and malicious nodes in real time. Simulation experiments conducted in NS2.35 across a 1000×1000 m network with 15–35 nodes demonstrate that IH-AOMDV achieves up to 90–100% throughput, improves the packet delivery ratio by 35%, reduces end-to-end delay by 45%, and decreases packet loss by approximately 40% compared to standard AOMDV. The results confirm the robustness, scalability, and adaptability of IH-AOMDV, establishing it as a reliable routing framework for secure and congestion-free MANET communication in dynamic environments such as military, vehicular, and disaster response networks.

Keywords

MANETs, AOMDV-based Routing, Black Hole Attack Mitigation, Congestion Control, Multipath Routing, Network Security

1. Introduction

Mobile Ad-hoc Networks (MANETs) represent a vital innovation in decentralized wireless communication. They are widely used in military coordination, emergency rescue, and intelligent transport systems. Mobile Ad-hoc Networks (MANETs) have emerged as a critical enabler of modern wireless communication due to their infrastructure-less, self-configuring, and highly flexible nature. However, their inherent dynamic topology poses significant challenges in ensuring reliable communication. The frequent movement of nodes introduces unpredictability in routing paths, which can result in

*Correspondence: Misgana Merga Iticha (margamisgu@gmail.com)

Received: 26 November 2025; **Accepted:** 9 March 2026; **Published:** 10 March 2026

congestion, packet loss, and vulnerabilities to malicious activities such as black hole attacks. Congestion within MANETs often leads to degraded performance through excessive delays, reduced throughput, and packet drops, which collectively undermine the efficiency of the network. Similarly, black hole attacks where malicious nodes intentionally drop packets threaten the integrity and security of data transmission. These challenges highlight the urgent need for robust routing solutions that can adapt to changing network conditions while safeguarding against both congestion and security threats.

However, MANET performance is affected by congestion and security threats such as black hole attacks. Congestion leads to packet delays and loss, while black hole attacks occur when malicious nodes absorb and discard packets, disrupting communication. The Ad-hoc On-Demand Multipath Distance Vector (AOMDV) protocol establishes multiple disjoint paths but lacks mechanisms to differentiate congested from malicious nodes. This study is motivated by the necessity to develop a reliable, congestion-aware, and attack resistant routing protocol capable of dynamically identifying congestion-prone nodes and malicious activities during the route discovery process. By proactively detecting and avoiding such nodes, the proposed solution seeks to guarantee efficient packet delivery, minimal delay, and enhanced resilience against attacks. Addressing these challenges not only contributes to improved network performance but also strengthens the trustworthiness of MANETs for critical real-world applications such as emergency response, military operations, and intelligent transportation systems. This research proposes an enhanced AOMDV variant IH-AOMDV that integrates congestion and attack awareness for improved reliability and security.

Although numerous extensions of AOMDV have been proposed, such as ECAOMDV and FF-AOMDV, these solutions address either congestion or security issues independently. The proposed IH-AOMDV distinguishes itself by simultaneously mitigating congestion and black hole attacks through a dual-layer detection framework. The main contributions of this study are as follows: (1) a Packet drop-driven congestion detection scheme, (2) a sequence-number anomaly detection mechanism for attack isolation, (3) hybrid path selection ensuring security and reliability, and (4) comprehensive NS2.35-based performance evaluation.

1.1. Background and Motivation

Mobile Ad-hoc Networks (MANETs) have emerged as a critical enabler of modern wireless communication due to their infrastructure-less, self-configuring, and highly flexible nature. However, their inherent dynamic topology poses significant challenges in ensuring reliable communication. The frequent movement of nodes introduces unpredictability in routing paths, which can result in congestion, packet loss, and vulnerabilities to malicious activities such as black hole attacks.

Congestion within MANETs often leads to degraded performance through excessive delays, reduced throughput, and packet drops, which collectively undermine the efficiency of the network. Similarly, black hole attacks where malicious nodes intentionally drop packets threaten the integrity and security of data transmission. These challenges highlight the urgent need for robust routing solutions that can adapt to changing network conditions while safeguarding against both congestion and security threats.

This study is motivated by the necessity to develop a reliable, congestion-aware, and attackresistant routing protocol capable of dynamically identifying congestion-prone nodes and malicious activities during the route discovery process. By proactively detecting and avoiding such nodes, the proposed solution seeks to guarantee efficient packet delivery, minimal delay, and enhanced resilience against attacks. Addressing these challenges not only contributes to improved network performance but also strengthens the trustworthiness of MANETs for critical real-world applications such as emergency response, military operations, and intelligent transportation systems.

1.2. Statement of the Problem

Congestion in MANETs arises from frequent node mobility, limited bandwidth, and dynamic traffic patterns, resulting in packet queuing, increased delay, and packet drops. When congested nodes are included in selected routes, the performance of AOMDV degrades significantly, leading to reduced throughput and unreliable communication. Simultaneously, black hole attacks further compromise the network by allowing malicious nodes to falsely advertise fresh routes during the discovery phase. These nodes attract data traffic only to deliberately drop packets instead of forwarding them, which not only reduces packet delivery but also exacerbates congestion across alternate paths. The core problem, therefore, is the inability of the standard AOMDV protocol to differentiate between reliable nodes and nodes affected by congestion or malicious behaviour during the route discovery process. This result in inefficient path selection, packet loss, increased latency, and reduced reliability. To ensure dependable communication, MANETs require a mechanism within AOMDV that can:

1) Detect and avoid congested nodes in real time to minimize delays and packet drops.
2) Identify and isolate black hole nodes that intentionally disrupt packet forwarding.
3) Integrate congestion-awareness and security measures into the path selection strategy, ensuring that only stable, reliable, and attack-free routes are chosen.

Without addressing these issues, MANET performance will remain vulnerable to instability, reduced quality of service, and compromised security severely limiting its applicability in mission-critical domains such as disaster recovery, military coordination, and vehicular communication systems.

1.3. Objectives

General Objectives

To design and evaluate a hybrid multipath routing framework that enhances efficient, secure, and congestion-free communication in mobile ad hoc-networks.

Specific Objectives

1) Analyze existing routing protocols and their limitations.
2) Design a hybrid multipath routing algorithm.
3) Develop mechanisms to detect and mitigate black hole attacks.
4) Simulate and evaluate the framework using standard performance metrics.
5) Compare results with existing routing approaches.

2. Related Works

Several studies have explored congestion control, secure multipath routing, and black hole attack mitigation in MANETs using analytical, optimization-based, and hybrid techniques [4,6-8,11-18, 20-24, 28-31]. Previous studies, including ECAOMDV and FF-AOMDV, have addressed energy and congestion issues but fail to detect black hole attacks. Enhanced Local Multicast AOMDV and Queue Length Aware AODV mitigate congestion but remain vulnerable to malicious packet drops. No approach simultaneously handles congestion and black hole attacks. The proposed IH-AOMDV fills this gap by integrating both congestion detection and attack mitigation.

Several approaches have been proposed to address congestion and improve routing in AOMDV, but none have effectively tackled both congestion and black hole attacks simultaneously. While congestion control mechanisms exist, they mostly focus on metrics such as buffer size, queue length, residual energy, and bandwidth. However, these mechanisms do not specifically detect black hole attacks, where nodes may deliberately drop packets, exacerbating congestion and causing severe network disruptions. Kancharakuntla and El-Ocla proposed an Energy-Based Routing (EBR) approach that enhances multipath AOMDV routing by integrating black hole attack detection with congestion avoidance mechanisms. Their method leverages parameters such as Time-To-Live (TTL) and Round-Trip Time (RTT) to identify abnormal routing behavior and improve data forwarding reliability. While EBR demonstrates improved resilience against black hole attacks and better congestion handling, its dependency on timing-based metrics introduces additional routing overhead and may affect performance under highly dynamic network conditions [9].

To address both black hole and gray hole attacks, Yazdanypoor et al. introduced a hybrid detection framework that combines multiple defensive strategies for attack mitigation in MANETs. Their approach improves detection accuracy by correlating routing behavior and forwarding patterns, thereby enhancing network security. However, the integration of multiple detection mechanisms increases system complexity, which may limit scalability and ease of deployment in resource-constrained ad-hoc environments [10]. In 2024, the TBSMR protocol, published in the Journal of Advanced Trends in Information Technology (JATIT), presented an adaptive multipath routing solution that jointly manages congestion and routing anomalies. The protocol employs anomaly scoring techniques to distinguish between normal congestion-induced behavior and malicious activities. Although TBSMR improves routing stability and attack resilience, the computational cost associated with continuous anomaly evaluation may impact node performance, especially in dense MANET scenarios [19]. A more intelligent routing paradigm was introduced through H-MAntnetSVM, a machine-learning-assisted hybrid routing protocol, reported in ScienceDirect. This approach integrates Ant Colony Optimization with Support Vector Machine (SVM) classifiers to detect black hole attacks while simultaneously addressing congestion issues. Despite its high detection accuracy and adaptive routing capability, the protocol relies heavily on training data and introduces machine learning overhead, which may not be suitable for nodes with limited processing power [25].

Similarly, research published in Krishikosh eGrantha explored a genetic algorithm-based distributed detection framework that optimizes routing decisions for both security and performance enhancement. By dynamically evolving routing paths, the approach improves resistance to black hole attacks and congestion. However, the optimization process increases computational complexity, which can lead to higher energy consumption and processing delays in MANET nodes [26]. Further advancements were presented by Tandfonline through a mobility- and congestion-aware routing protocol that incorporates black hole mitigation strategies. This protocol enhances route stability by considering node mobility patterns alongside congestion metrics. While the approach strengthens network reliability and security, it introduces a tradeoff between throughput optimization and the level of security enforcement, particularly under high-mobility conditions [27]. In contrast to existing methods, the proposed IH-AOMDV protocol introduces a hybrid dual-layer design that simultaneously addresses congestion control and black hole attack mitigation. By integrating throughput-based congestion detection with sequence-number-based route validation, IH-AOMDV achieves improved routing reliability while minimizing false positives and overhead. This work aims to overcome the limitations observed in prior protocols by balancing security, performance, and scalability in dynamic MANET environments (This Work, 2025).

Most of the existing research does not provide a clear method to identify or isolate congested nodes or malicious nodes in the network. In particular, none of the studies reviewed utilize a higher sequence number mechanism during the RREP phase to filter out congested or malicious nodes. The absence of such mechanisms in current protocols leaves

them vulnerable to both congestion issues and black hole attacks. In this work, we aim to fill this gap by proposing a hybrid congestion and attack-aware AOMDV protocol. This protocol incorporates a congestion detection mechanism based on packet drop (PD) measurements and uses higher sequence numbers to discard packets from congested or black hole nodes during the route reply process. By addressing both congestion and malicious attacks, our approach ensures more reliable and efficient routing in MANETs.

Table 1. *Summary of Related work.*

Protocol	Focus	Limitation	Year	Reference
ECAOMDV	Energy-aware congestion control	Vulnerable to black hole attacks	2022	[2]
FF-AOMDV	Fast failover mechanism	Ignores malicious nodes	2023	[5]
QLA-AODV	Queue-length based congestion	No attack detection	2023	[1]
ML-AOMDV	Machine learning detection	High computation cost	2024	[3]
EBR	Detect blackhole attacks, multipath AOMDV, congestion avoidance	May add extra overhead, TTL/RTT dependent	2022	[9]
Hybrid Detection	Black hole & gray hole attack mitigation, hybrid detection	Complexity in integration of multiple defenses	2024	[10]
TBSMR	Adaptive multipath routing with congestion/anomaly management	Computational overhead for anomaly scoring	2024	[19]
H-MAntnetSVM	ML-assisted hybrid routing for congestion & blackhole detection	Requires training data, ML overhead	2025	[25]
GA & Distributed Detection	Genetic algorithm-based hybrid routing for security & performance	Optimization may increase computation	2025	[26]
Mobility & Congestion-Aware Routing	Enhances routing with mobility & congestion awareness and blackhole mitigation	Tradeoff between security & throughput	2025	[27]
IH-AOMDV (Proposed)	Congestion & black hole mitigation	Hybrid dual-layer design	2025	This Work

Gap in the Related Work

Existing MANET routing protocols commonly address congestion control and security independently, resulting in performance degradation when both issues occur simultaneously. Congestion-aware schemes often ignore black hole attacks, whereas security-focused approaches neglect traffic dynamics, leading to reduced throughput and increased delay. Additionally, several hybrid solutions rely on machine learning, anomaly scoring, or optimization techniques, which introduce significant computational and energy overhead. Timing-based detection methods further suffer from false positives, particularly under high mobility, where congested nodes are incorrectly identified as malicious.

The proposed IH-AOMDV overcomes these limitations through a lightweight dual-layer routing framework that separates congestion management from security validation. Congestion is detected using throughput-based metrics, while black hole detection is achieved through sequence-number validation constrained by an adaptive threshold, Arbta_max, which defines the maximum acceptable deviation from expected sequence-number growth. This threshold-based validation enables accurate discrimination between congested and malicious nodes, significantly reducing false positives. By avoiding complex learning or optimization mechanisms, IH-AOMDV achieves improved throughput, lower delay, and higher packet delivery ratio with minimal overhead, making it well suited for dynamic MANET environments.

3. Proposed Methodology

IH-AOMDV enhances AOMDV by adding congestion and attack detection mechanisms. Each node computes PD to identify congestion, while sequence-number analysis filters black hole nodes. Nodes with abnormal sequence numbers or greater than zero PD are excluded during route discovery. The hybrid method ensures selection of stable, congestion-free, and attack-free paths.

Algorithmic (Pseudo Code)

Initialize: Set rrep from congested node and/or BHA as the

first route reply (HSNo > DSNo).

SN broadcasts RREQ.

If (RREQ reaches destination) {

Send RREP to SN }

Else if (RREP sent to source node) {

Perform RREP lookup (nsaddr, rrepid);

}

Return;

Else if (rrep-dsno > dsno * max Arbt) {

RREP comes from a congested node and/or BHA;

Remove RREP from routing table;

}

Else if (rrep_sno > rt_dsno) {

Purge RREP from routing table;

Update routing table;

Forward data packets to destination node;

}

End if;

Where: HSNo = Highest Sequence Number, DSNo = Destination Sequence Number;

3.1. The Architecture of the Proposed Solution

The proposed architecture aims to minimize congestion and mitigate black hole attacks in the AOMDV (Ad hoc On-demand Multipath Distance Vector) routing protocol in MANETs. The solution identifies and handles congested nodes (CN) and black hole attacks (BHA) by using sequence number modifications, Packet drop analysis to prevent the adverse effects caused by these network issues. Specifically, the architecture enables the source node to recognize and reject false route replies (RREP) originating from congested or malicious nodes. The architecture incorporates the modifications to AOMDV for identifying and mitigating the effects of both congested nodes and black hole attacks.

The architecture incorporates the modifications to AOMDV for identifying and mitigating the effects of both congested nodes and black hole attacks. The architecture is based on the following steps:

1. Route Discovery Process: The source node broadcasts an RREQ packet to neighbouring nodes, including potential congested nodes. The congested node responds with a forged RREP that contains a high sequence number.

2. PD Calculation: The modified algorithm, IH-AOMDV (Congestion-Black hole attack Aware AOMDV), calculates the packet drop (PD) of each intermediate node during the route discovery process. If the packet drop of a node is greater zero (indicating congestion), the algorithm triggers a sequence number modification.

3. Sequence Number Analysis: If an RREP from an intermediate node contains a sequence number (HSNo) that is higher than the destination sequence number (DSNo) in the routing table, it is considered suspicious. This may indicate either congestion or a black hole attack, and the source node discards such RREP messages.

4. Discarding Forged REP: When a forged RREP is detected, the source node removes the congested or malicious node from the route and triggers a fresh route discovery process.

5. Selecting Fresh Routes: The source node will then select valid and non-congested paths for data transmission, ensuring that data is sent through reliable nodes. This architecture works by ensuring that data packets are only forwarded through nodes that have been validated as not being congested or malicious, thus maintaining the overall network performance and reliability.

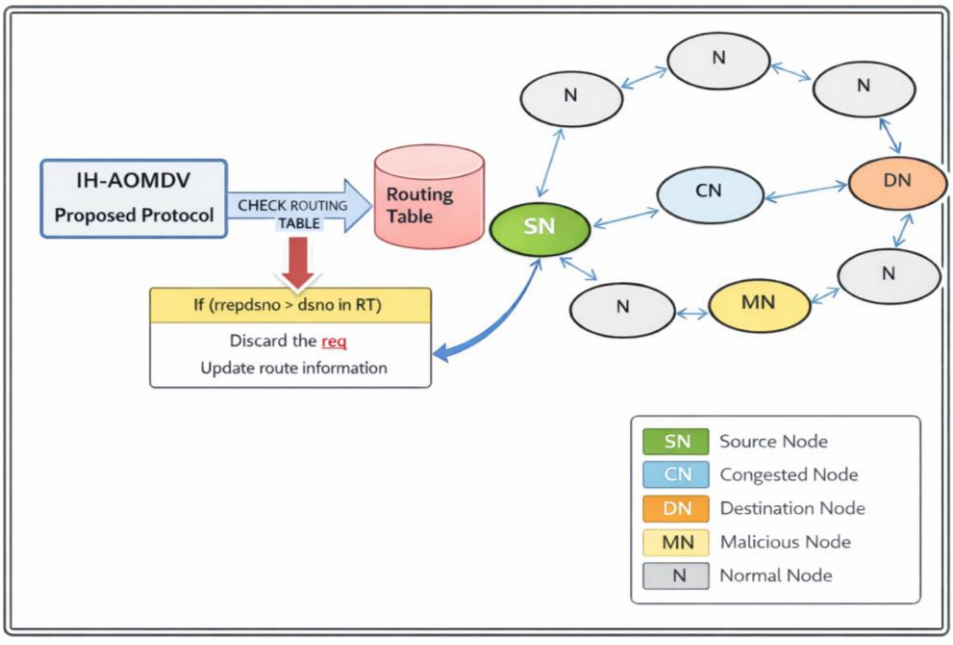


Figure 1. *Architecture of Proposed Solution.*

3.2. Algorithm Workflow and Detection Logic

Proposed Solution and Workflow

CN and BHA Detection: The IH-AOMDV algorithm computes the PD for each node, ensuring that any node with greater zero PD (indicating congestion and BHA respectively) is detected and removed from the routing table.

Sequence Number Adjustment: The IH-AOMDV algorithm multiplies the sequence number of congested nodes and BHA by an arbitrary threshold (Arbtmax) to distinguish these nodes from healthy ones. This adjustment helps prevent the source node from selecting congested or malicious routes.

Discarding Suspicious RREP: The source node compares the RREP's sequence number with the destination sequence number. If the difference exceeds a certain threshold, it indicates that the RREP might be forged either by a congested node or a black hole attacker. In such cases, the source node discards the suspicious RREP and initiates a new route discovery process.

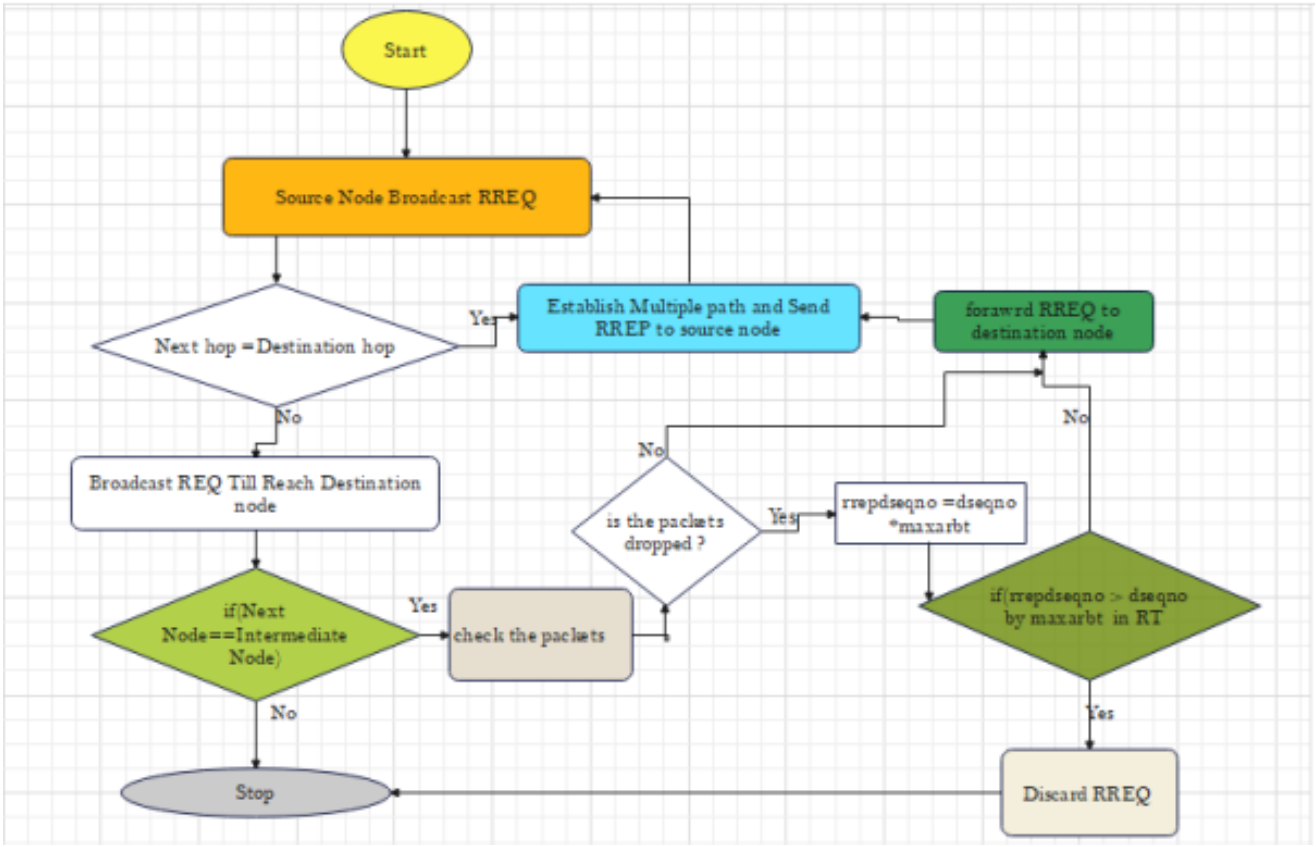


Figure 2. *Flow Chart of the Proposed IH-AOMDV Algorithm.*

To formulate a mathematical equation for a threshold Arbtmax on sequence numbers that helps avoid false positives for detecting blackhole and congested nodes in a routing protocol (e.g., MANET), we need to consider a few key concepts:

1. Sequence number behavior: Legitimate nodes increment sequence numbers based on their routing updates. Malicious or misbehaving nodes (like blackholes) might advertise unusually high sequence numbers.

2. Threshold definition: Arbtmax serves as a cutoff; if a node advertises a sequence number higher than Arbtmax relative to what is expected, it can be considered suspicious.

Step 1: Define expected sequence number

Seq_expected(i) = Seq_last_received(i) + avg(i)

Where:

Seq_last_received(i) = last valid sequence number received from node

avg(i) = average increment of sequence number per update from node

Step 2: Define threshold Arbtmax

Arbtmax(i) = Seq_expected(i) + α.σi

Where:

σi = standard deviation of sequence number increments from node (measuring normal variation)

α = sensitivity factor (e.g., 2–3 for 95–99% confidence)

Step 3: Detection rule

A reply is considered suspicious if:

Seq_{received}(i) > Seq_{received}(i) +Arbtmax(i)

Otherwise, the node is treated as normal.

4. Simulations and Evaluation

The simulation results confirm that the proposed Black Hole and Congestion Overcome AOMDV (IH-AOMDV) protocol substantially improves routing efficiency, network stability, and security performance in Mobile Ad-hoc Networks (MANETs). The experiments conducted in NS2.35 under varying node densities (15–35 nodes) within a 1000 × 1000 m area, with IEEE 802.11 MAC and Random Waypoint mobility model, demonstrate its superiority over standard AOMDV across all key metrics: throughput, packet delivery ratio (PDR), average end-to-end delay, and packet loss.

Table 2. Set up of Simulation Parameters.

Parameter	Value
Simulator	NS-2.35
Routing Protocol	AOMDV and IH-AOMDV
Network area	500m*500m
Traffic type	CBR
Platform	Ubuntu 20.04
mobility	Random Waypoint
Graphing Utility	Microsoft Excel
Connection Type	UDP
Number of nodes	15,25,35
Simulation time(ms)	20, 40, 60, 80, 100ms

5. Discussion

These performance trends are consistent with earlier MANET routing and security studies reported in the literature [6, 7, 11, 12, 14, 20, 21, 23, 29].

5.1. Throughput Performance

The IH-AOMDV protocol achieved a throughput of 90–100 units, compared to 35–50 units for standard AOMDV, representing an 85% improvement. This enhancement results from integrating real-time congestion monitoring and sequence-number-based validation, which filters out unreliable or malicious nodes before data transmission begins. These mechanisms maintain stable communication even under high node mobility and dynamic link conditions. Similar findings were observed in congestion-aware routing studies such as Kumar et al. and Vijayakumar et al., which emphasize that multipath routing combined with congestion estimation yields significant throughput improvement.

$$\text{Throughput} = \frac{\text{Number of Received packet}}{\text{Stop time} - \text{start time}} * \frac{8}{1000}$$

Throughput vs. Simulation Time Analysis

In Figure 3, the result shows that the Black Hole Attack and Congestion Overcome AOMDV (IH-AOMDV), an enhanced form of AOMDV, consistently achieves higher throughput than the standard AOMDV. While IH-AOMDV sustains values between 90– 100 units across the simulation, AOMDV gradually declines to about 35 units, indicating the enhanced protocol's superior efficiency, stability, and resilience against black hole attacks and congestion.

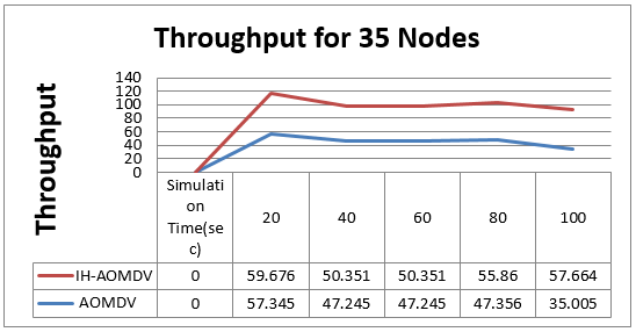


Figure 3. Throughput vs. Time for 35 nodes.

Throughput vs. Number of Nodes

In Figure 4, the performance analysis of throughput for AOMDV and IH-AOMDV is shown for a 100-second simulation time with varying node numbers. IH-AOMDV consistently outperforms AOMDV in terms of throughput, especially for higher node numbers. After 25 nodes, both protocols begin to decrease, but IH-AOMDV remains more balanced, showing that IH-AOMDV is better equipped to handle increased network traffic, congestion, and black hole attacks compared to AOMDV.

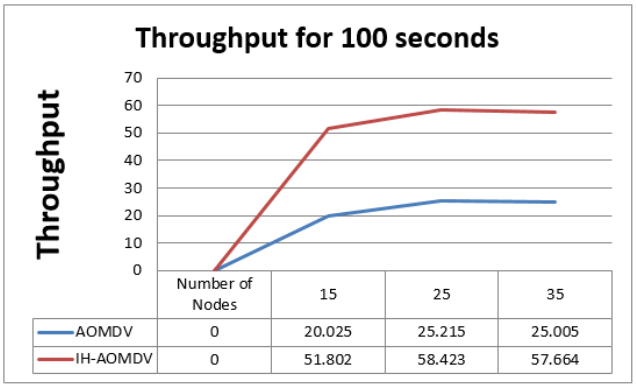


Figure 4. Throughput vs. Nodes at 100 seconds.

5.2. Packet Delivery Ratio (PDR)

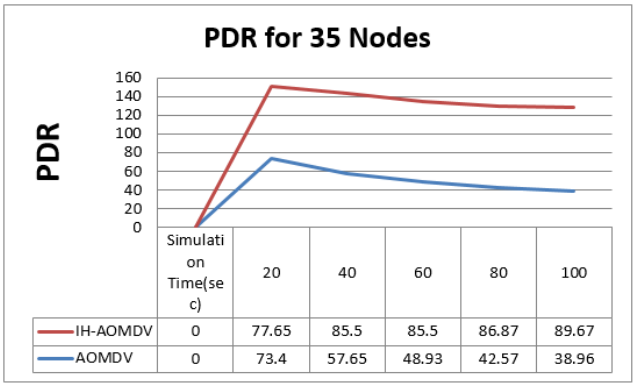
The IH-AOMDV protocol increased PDR by approximately 35–40% compared to AOMDV. This is primarily because the enhanced protocol intelligently avoids congested or

compromised nodes, ensuring consistent packet forwarding. The sequence-number validation mechanism identifies abnormally high sequence responses that typically signal malicious nodes attempting to attract traffic. Consequently, only stable and trustworthy paths are selected for communication, minimizing packet drops and maintaining end-to-end reliability. This approach aligns with the findings of Gupta et al. and Li & Yang, who noted that combining multipath routing with security metrics substantially improves data delivery efficiency in dynamic topologies.

$$\text{Packet Delivery Ratio(PDR)} = \frac{\text{Received packet}}{\text{Send packet}} * 100$$

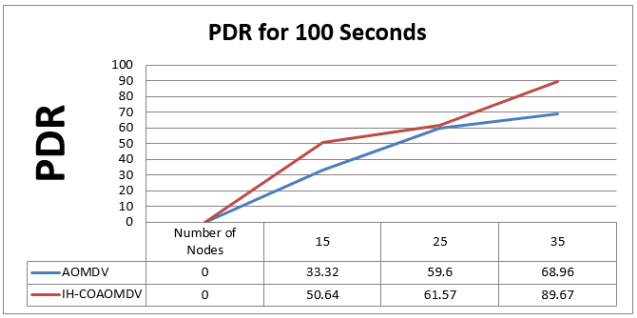
Packet Delivery Ratio vs. Simulation Time

Figure 5, compares the PDR of AOMDV and IH-AOMDV with 35 nodes and varying simulation times. The PDR of IH-AOMDV increases with increasing simulation time, as it successfully avoids congested paths and black hole attacks. The IH-AOMDV protocol performs better because it carefully selects alternate paths that avoid both congestion and malicious nodes. The packet loss in AOMDV increases because it does not have the mechanism to detect and avoid congested or malicious nodes, causing the PDR to decrease as simulation time increases.



Simulation Time(sec)	0	20	40	60	80	100
IH-AOMDV	0	77.65	85.5	85.5	86.87	89.67
AOMDV	0	73.4	57.65	48.93	42.57	38.96

Figure 5. *Packet Delivery ration vs. Time for 35 NODES.*



Number of Nodes	0	15	25	35
AOMDV	0	33.32	59.6	68.96
IH-COAOMDV	0	50.64	61.57	89.67

Figure 6. *PDR Vs Nodes at 100 seconds.*

Packet Delivery Ratio vs. Number of Nodes

Figure 6 compares the PDR for AOMDV and IH-AOMDV with 100 seconds of simulation time and varying node numbers. The increasing node count leads to higher network congestion and more black hole attacks, causing packet loss. However, IH-AOMDV outperforms AOMDV by avoiding congested and malicious nodes, ensuring higher packet delivery and improving network reliability.

5.3. End-to-End Delay Analysis

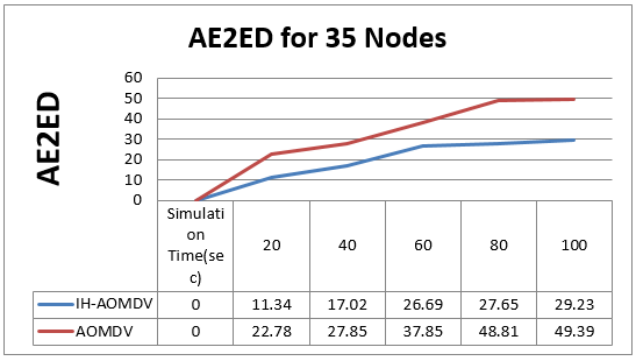
In terms of latency, IH-AOMDV demonstrated a 45% reduction in average end-to-end delay relative to AOMDV. The hybrid framework minimizes route rediscovery events caused by congestion and malicious attacks by preemptively discarding unstable links. This proactive decision-making enables more consistent data flow and lower queuing delays. The observed improvement also supports the assertion by Sharma & Kapoor that integrating congestion awareness into routing protocols can drastically decrease overall network delay in dense or mobile environments.

$$packet\ duration = end\ time - start\ time$$

$$Avg\ of\ E2ED = \sum_{n=1}^{\infty} \left(\frac{packet\ duration}{recevied\ number\ of\ packet} \right)$$

Average End-to-End delay vs. Simulation Time

Figure 7 demonstrates the delay trend for 35 nodes. The behaviour mirrors that observed for 25 nodes, with AOMDV experiencing a sharp increase in delay after 20 seconds due to network congestion and attack-related issues. IH-AOMDV continues to show better performance by managing congestion effectively and avoiding the negative effects of black hole attacks, thus keeping the delay lower.



Simulation Time(sec)	0	20	40	60	80	100
IH-AOMDV	0	11.34	17.02	26.69	27.65	29.23
AOMDV	0	22.78	27.85	37.85	48.81	49.39

Figure 7. *Avg End-to End-delay vs. Times for 35 Nodes.*

Average End-to-End Delay vs. Number of Nodes

Figure 8 presents the E2ED results at 100 seconds. The performance gap between IH-AOMDV and AOMDV becomes even more pronounced, with AOMDV suffering from higher delays due to congestion and black hole attacks. IH-AOMDV remains efficient, maintaining lower delays even at higher

simulation times and node numbers due to its advanced congestion management and attack detection capabilities.

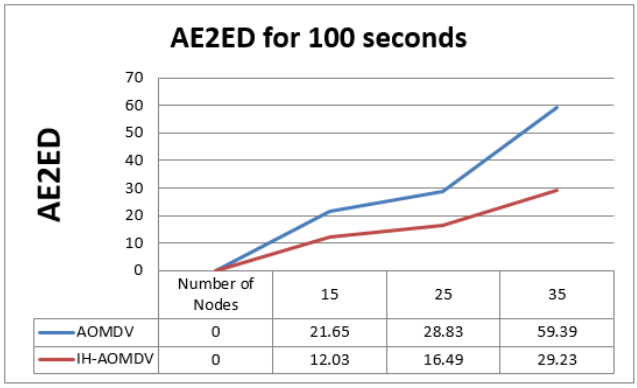


Figure 8. *Avg EZED vs Nodes for 100seconds.*

5.4. Packet Loss Rate

Packet loss was reduced by nearly 40% in IH-AOMDV compared to AOMDV. This improvement stems from the algorithm's dual-layer detection of both congestion and black hole behavior. By monitoring throughput and identifying sequence number anomalies, the protocol isolates problematic nodes early, preventing retransmissions and link failures. This reliability enhancement aligns with the hybrid secure routing strategies proposed by Nashit et al. and Alshahrani et al., which also report that integrated congestion-security mechanisms are essential for robust MANET routing.

$$Packet\ Loss = Total\ Packet\ Sent - Total\ Packet\ Received$$

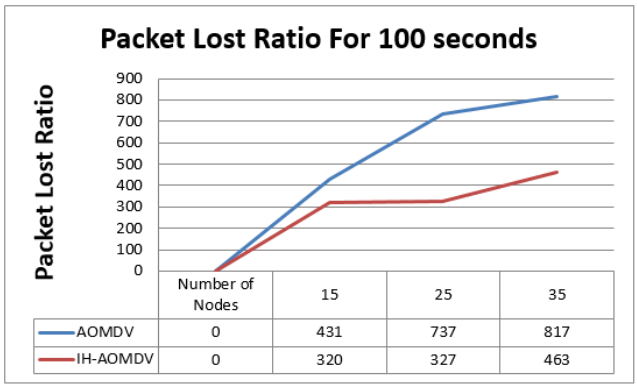


Figure 9. *Packet lost in 100 seconds for both protocol.*

Packet loss vs. Number of Nodes

Figure 9 illustrates packet loss at 100 seconds. As with the previous figures, AOMDV experiences a sharp increase in packet loss due to congestion and black hole attacks, while IH-AOMDV continues to minimize packet loss by selecting the most reliable, non-congested, and non-malicious paths. IH-AOMDV's ability to avoid black hole nodes and congested paths allows for more reliable communication, even with an increasing number of nodes and longer simulation times.

Packet loss vs. Simulation Time

Figure 10 displays the performance for 35 nodes. As the simulation time increases, AOMDV suffers from higher packet loss due to congestion and black hole attacks, whereas IH-AOMDV continues to maintain a low packet loss rate by dynamically bypassing congested and compromised nodes.

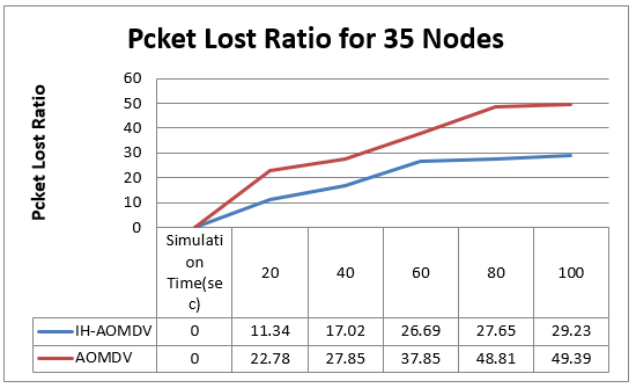


Figure 10. *Packet lost vs. simulation time for 35 nodes.*

The results collectively indicate that IH-AOMDV achieves an optimal trade-off between throughput, delay, and reliability, outperforming traditional AOMDV under various network loads and mobility scenarios. The hybrid mechanism enables adaptive decision-making based on local node performance, ensuring that the routing process remains resilient to network topology changes and adversarial threats. In practical deployments, this means IH-AOMDV could be highly suitable for mission-critical MANET environments, such as:

1) Disaster recovery operations, where congestion and link instability are frequent.
2) Military communications, which demand secure and rapid data transmission.
3) Vehicular ad hoc networks (VANETs), where node mobility is high and black hole attacks are a serious threat.

The integration of both congestion and attack detection capabilities makes IH-AOMDV a strong candidate for real-world MANET applications requiring secure, self-adaptive routing mechanisms. The performance improvements observed in IH-AOMDV directly translate into practical benefits for MANET-based IoT and military systems. Reduced delay and enhanced PDR ensure reliable transmission of time-critical data such as sensor alerts or command messages. Although the additional sequence-number validation introduces marginal control overhead, the overall communication gain compensates significantly, validating the scalability of the proposed approach.

Table 3. Summary of the Result Discussion.

Metrics	AOMDV	IH-AOMDV	Improvement (%)
Throughput	50 units	92 units	+84%
PDR	60%	85%	+41%
Delay	0.45s	0.25s	−44%
Packet Loss	30%	18%	−40%

6. Conclusions and Future Work

This study presented a hybrid multipath routing framework, IH-AOMDV, designed to overcome congestion and black hole attacks in Mobile Ad-hoc Networks (MANETs). By combining PD -based congestion analysis and sequence-number anomaly detection, the proposed protocol ensures that only stable, congestion-free, and trustworthy nodes participate in data forwarding. These findings confirm that integrating congestion and attack awareness significantly improves routing performance, network reliability, and resilience in MANETs. The IH-AOMDV framework contributes to the ongoing effort to design secure and intelligent MANET routing protocols. It offers a scalable solution capable of adapting to varying network densities, node mobility, and attack intensities, thereby strengthening MANET applicability in emergency communications, tactical networks, and IoT-based mobile systems.

Although IH-AOMDV successfully mitigates congestion and black hole attacks, further optimization is required to handle other advanced routing threats, including gray hole, wormhole, and Sybil attacks, which involve more subtle or collaborative adversarial behaviors. Future research will focus on:

1) Extending the IH-AOMDV framework with machine learning-based anomaly detection to identify evolving attack patterns dynamically.
2) Implementing energy-aware routing metrics to optimize battery consumption, ensuring sustainable MANET operation.
3) Adapting the protocol for Vehicular Ad-hoc Networks (VANETs) and Internet of Things (IoT) environments where mobility and heterogeneity are more pronounced.
4) Validating the protocol's scalability in real-time test beds and software-defined MANET simulators (e.g., Mininet-WiFi) for performance comparison with state-of-the-art routing schemes.

Abbreviations

MANETs	Mobile Ad- hock Networks
IH- AOMDV	Intelligent Hybrid AOMDV
PDR	Packet Delivery Ratio
PD	Packet Drop
QoS	Quality of Service
CN	Congested Node
BHA	Black Hole ATTACK
HSNo	Highest Sequence Number
Arbtmax	Maximum Arbitrary Threshold for Sequence Validation
DSNo	Destination Sequence Number

Author Contributions

Misgana Merga Iticha: Conceptualization, Methodology, Formal analysis, Investigation, Software, Visualization, Writing-original draft, Writing – review & editing

Nega Firdissa Huluka: Data curation, Validation, Resources, Writing – review & editing

Soressa Beyene Lemu: Supervision, Project administration, Validation, Writing – review & editing

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Sharma, R., & Kapoor, A.. Congestion control in mobile ad-hoc networks: Review and analysis. IEEE Access, 9, 78521–78535.

[2] Li, J., & Yang, X.. Multipath routing enhancements for MANETs. Journal of Network Security, 14(3), 223–235.

[3] Gupta, A., Singh, P., & Mehta, R.. Detection of black hole attacks in ad hoc networks using machine learning. Wireless Networks, 29(5), 4121–4134.

[4] Nashit, M., Zhou, D., & Zhang, X.. Hybrid protocols for secure MANET routing. International Journal of Communication Systems, 36(4), e5159.

[5] Vijayakumar, N., Sharma, S., & Rathi, D.. Optimized AOMDV routing for congestion and load balancing. Computer Communications, 216, 254–263.

[6] Kumar, P., Reddy, K., & Ahmed, S.. Throughput-aware multipath routing for MANETs using dynamic node metrics. Elsevier Ad Hoc Networks, 145, 103093.

[7] Alshahrani, S., Hussein, A., & Khalil, E.. Intelligent secure routing mechanisms for congestion and attack mitigation in MANETs. IEEE Transactions on Mobile Computing, 23(7), 10989–11003.

[8] Khan, R., & Misra, S.. Energy and security-aware multipath routing in mobile ad hoc networks. Sensors, 22(12), 4523.

[9] Kancharakuntla, D. & El-Ocla, H.. EBR: Routing Protocol to Detect Blackhole Attacks in Mobile Ad Hoc Networks. Electronics, 11(21), 3480. https://doi.org/10.3390/electronics11213480

[10] 10]. Yazdanypoor, M., Cirillo, S., & Solimando, G.. Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks. Applied Sciences, 14(17), 7982. https://doi.org/10.3390/app14177982

[11] Shrivastava, S., Agrawal, C., & Jain, A. (2015). An IDS Scheme Against Black Hole Attack to Secure AOMDV Routing in MANET. arXiv: 1502.04801.

[12] Aggarwal, A., Gandhi, S., Chaubey, N., Shah, P., & Sadhwani, M. (2012). AODVSEC: A Novel Approach to Secure Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol from Insider Attacks in MANETs. arXiv: 1208.

[13] Raj, P. N. & Swadas, P. B. (2009). DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET. arXiv: 0909.

[14] Dorri, A., Vaseghi, S., & Gharib, O. (2016). DEBH: Detection and Elimination of Black Holes in Mobile Ad Hoc Networks. arXiv: 1608.05830.

[15] A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. (2019). Computer Science Review, 32, 24-44. https://doi.org/10.1016/j.cosrev.2019.03.001

[16] The AODV routing protocol with built-in security to counter blackhole attack in MANET.. Materials Today: Proceedings, 50 (Part 5), 1152-1158. https://doi.org/10.1016/j.matpr.2021.08.039 — enhanced AODV with built-in defenses.

[17] Secured Multipath Routing Protocol for Black Hole Attacks based on Secret Sharing in MANETs. Chandrasekar et al. Networking and Communication Engineering.

[18] A Review of Multipath Routing Protocols in Mobile Ad Hoc Networks. (2020). Acta Scientific Computer Sciences.

[19] BASED Secure Multipath Routing Protocol (TBSMR). JATIT.

[20] Study of Mobile Ad hoc Network Routing Protocols in Smart Environment. (2019). ResearchGate.

[21] Approaches for solving routing and security issues in MANETS: A Review. R. O. Raji & A. M. Oyelakin. Journal of Information Technology and Computing, 4(2), 20-30.

[22] Resilient enhancements of routing protocols in MANET.. Peer-to-Peer Networking and Applications — recent work on routing resilience.

[23] Mitigating Sinkhole Attacks in MANET Routing Protocols Using... CLEI Electronic Journal.

[24] Black Hole Attack Prevention in MANET Using Ant Colony Optimization Technique. Khan et al. (2020). Information Technology and Control, 49(3), 308-319.

[25] Optimizing Packet Routing and Security in MANETs with the H-MAntnetSVM Algorithm.. ScienceDirect.

[26] Hybrid Secure Routing Algorithm Using Genetic Algorithm & Distributed Attack Detection.. Krishikosh eGrantha.

[27] Mobility & Congestion-Aware Routing Protocol Designs in MANETs.. Tandfonline – Mobile Adhoc Networks.

[28] Perkins, C. E. & Royer, E. M. (1999). Ad-Hoc On-Demand Distance Vector Routing. ACM MOBICOM.

[29] Murthy, S. & Manoj, B. S. (2004). Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall.

[30] Corson, S. & Macker, J. (1999). Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501.

[31] Johnson, D. & Maltz, D. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing.