Ingénierie des Systèmes d'Information
Vol. 31, No. 5, May, 2026, pp. 1737-1746
Journal homepage: http://iieta.org/journals/isi

Black Hole Attack Detection and Prevention Using Stable Election Protocol-Based Clustering and Digital Signature Authentication in Mobile Ad Hoc Networks

Sunil Gupta[1], Kiran Napte[2], Kamal Sauja[1], Chander Prabha[1], Shikha Mittal[1], Snehal Bhosale[3*], Darshana Sankhe[4], Mrunal Rane[4]

[1] Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab 140401, India
[2] Department of E&TC, PCET's Pimpri Chinchwad College of Engineering and Research, Ravet, Pune 412101, India
[3] E&TC Department, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune Campus, Pune 412115, India
[4] Department of E&TC, D. J. Sanghvi College of Engineering, Mumbai 400056, India

Corresponding Author Email: snehal.bhosale@sitpune.edu.in

https://doi.org/10.18280/isi.310529

Received: 7 January 2026
Revised: 20 March 2026
Accepted: 20 April 2026
Available online: 31 May 2026

Keywords:
Mobile Ad Hoc Networks, black hole attack, secure routing, digital signature authentication, Stable Election Protocol, energy-efficient clustering, Ad hoc On-Demand Distance Vector

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are highly vulnerable to routing attacks because of their decentralized architecture, dynamic topology, and lack of centralized security mechanisms. Among these threats, black hole attacks represent a critical challenge, as malicious nodes can exploit the route discovery process of the Ad hoc On-Demand Distance Vector (AODV) protocol by advertising forged routing information and subsequently discarding intercepted packets. Existing countermeasures often focus either on routing authentication or energy-efficient communication, while limited attention has been given to integrating both security and network sustainability. This study proposes an energy-aware secure routing framework that combines digital signature authentication (DSA) with the Stable Election Protocol (SEP) to detect and mitigate black hole attacks in MANET environments. In the proposed approach, routing control packets are authenticated using digital signatures to prevent forged Route Reply (RREP) messages, while SEP-based clustering selects energy-efficient cluster heads to support localized verification and reduce routing overhead. The framework was evaluated through simulations involving 100 mobile nodes under black hole attack scenarios and compared with conventional AODV and AODV enhanced with digital signatures only. Experimental results demonstrate that the proposed AODV+DS+SEP framework achieves a packet delivery ratio of 96.67%, compared with 71.67% for AODV+DS and 64.17% for standard AODV. In addition, the proposed method improves residual energy utilization and extends network lifetime while maintaining reliable routing performance. These findings indicate that integrating energy-aware clustering with cryptographic authentication provides an effective and practical solution for secure and sustainable routing in MANETs.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are decentralised wireless communication systems where mobile nodes serve as both hosts and routers. A Mobile Ad Hoc Network (MANET) is different from ordinary wireless networks since its nodes may put themselves together on their own and in real time, rather than relying on existing infrastructure [1]. Cooperative forwarding is needed for communication to work over a shared wireless channel, which makes it harder to guarantee effective security. Any mobile node that is within range of transmission can intercept, inject, or alter packets. This makes it feasible for enormous multiplayer online network assaults like impersonation, route disruption, and denial of service to happen [2].

There are several hazards at the routing layer, but black hole assaults are the most hazardous [3]. An enemy node sends out an exaggerated destination sequence number to make other nodes think it has the fastest or most up-to-date path to the target. During route discovery, the attacker makes the initiating node assume that a bogus Route Reply (RREP) is real. When the rogue node is picked as the forwarding hop, it throws away all incoming data packets, which causes a substantial decline in performance and eventually makes the connection fail [4].

Figure 1 shows that the full process of route discovery in AODV involves a source node sending out Route Request (RREQ) packets. The packets then go through intermediate nodes until they reach their destination or another intermediate node that has a good path. When the source node gets an RREP, it starts sending data along the right path.

Because wireless media are naturally exposed, MANET communication is very easy to exploit. People who have a mobile device close by could be able to listen in on conversations and get onto the network without having to log in [5]. The danger is higher because there are hostile nodes in

the network that are involved in routing and can change, throw away, or misroute packets by using cooperative routing behavior. Prior studies [6] have underscored that MANETs rely solely on trust-based routing coordination, display quickly evolving topologies, and are devoid of centralized security procedures. These traits make networks more likely to be manipulated when routing, which makes them less reliable. To understand how black hole nodes take advantage of weaknesses, you need to look at the AODV routing design. AODV uses control messages like RREQ, RREP, and RERR to find and set up routes as needed. Flooding-based RREQ propagation speeds up the process of finding routes, but it also lets bad nodes send fake RREPs without checking the route first.

In the AODV route discovery process, node "A" usually sends out an RREQ when it needs a way to go to node "G." If the destination or an intermediate node doesn't react with an RREP, the nodes around it will rebroadcast the request. The built bidirectional path makes it easier to move data, as seen in Figure 2.

AODV additionally uses the Route Error (RERR) message to keep the route up to date. If a middle link goes down, the node that finds the problem will send an RERR signal to the source, cutting off the channel. If the link between nodes "D" and "E" goes down, node "E" will send an RERR message to the starting node "A," which will start a fresh route discovery. Figure 3 shows how this method works.

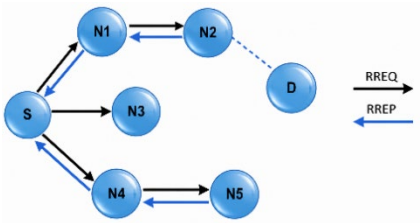

Figure 1. Ad hoc On-Demand Distance Vector (AODV) route discovery process showing Route Request propagation (black arrows) and Route Reply return path (blue arrows)

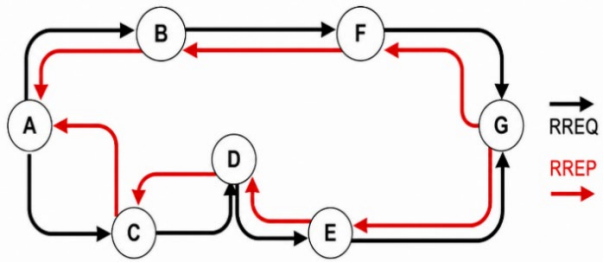

Figure 2. Normal Ad hoc On-Demand Distance Vector (AODV) route discovery and link establishment between source A and destination G

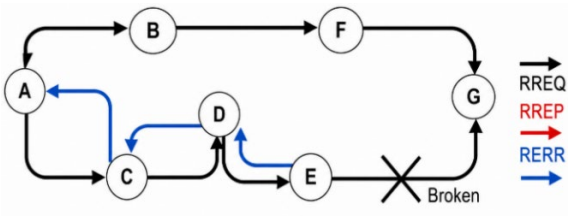

Figure 3. Ad hoc On-Demand Distance Vector (AODV) route maintenance process showing link break detection and Route Error propagation (blue arrows)

AODV is susceptible to black hole attacks due to its operational traits, such as reliance on cooperative algorithms, lack of centralized verification, and capacity to create routes on demand. These attacks involve putting fake RREPs with fake sequence numbers into the data stream to steal it. So, to make sure that data is sent safely in MANET systems, routing must be safe and verified.

1.1 Contributions

The main contributions of this work are summarized as follows:

- This study presents a novel integration of Stable Election Protocol (SEP)-based clustering with digital signature authentication (DSA) within the AODV routing protocol to mitigate black hole attacks in MANETs.
- A cluster-head-assisted verification mechanism is introduced, where selected cluster heads perform localized authentication of routing control packets, reducing global verification overhead.
- The proposed model enables energy-aware secure routing by combining residual energy-based cluster formation with cryptographic validation, thereby improving both network lifetime and security.
- A comprehensive evaluation is conducted comparing AODV, AODV+Digital Signature (DS), and AODV+DS+SEP in terms of packet delivery, energy efficiency, and overhead.
- Statistical validation using multiple simulation runs and confidence interval analysis is incorporated to ensure the robustness and reliability of results.

2. RELATED WORK

Routing security in MANETs has received significant attention due to the protocol vulnerabilities that arise from decentralized control and cooperative forwarding. Prior countermeasures fall broadly into the following categories: cryptographic authentication, trust and incentive schemes, intrusion and anomaly detection, protocol-level modifications, and WSN/energy-aware adaptations. Below we summarize representative contributions and highlight remaining gaps.

Cryptographic authentication and key-exchange. Public-key and symmetric cryptographic schemes have been employed to ensure the authenticity and integrity of routing control messages. Password based key exchange systems as studied by Asokan et al. [7] enabled session setup without centralised authorities. Threshold and certificate based strategies may be used to bind routing claims to credentials and to mitigate forgeries. Digital signatures have been proposed [8] to guarantee non-repudiation at the cost of higher processing requirements to prevent wormhole and other attacks. Cryptographic approaches are effective against basic spoofing. However, they can be costly for resource constrained nodes because of the heavy computational and communication overheads they impose [9].

Trust, reward and neighbour surveillance strategies Many research use incentive mechanism or trust evaluation to promote collaboration and detect misbehaviour. The credit and nuglet techniques encourage cooperation in packet forwarding; however, they may incur additional administrative overhead and protocol complexity [10, 11].

Neighbour data forwarding activity is monitored using methods such as watchdog and pathrater techniques, which prefer routes with reliable nodes [12]. In studies [13-15], legitimacy tables and neighbour promiscuous monitoring have been used to remove nodes that show unusual packet drop patterns. Trust-based methods can detect selfish or inappropriate behaviours of nodes gradually; nevertheless, they are susceptible to collusion and may take longer observation periods, which might hinder responsiveness in dynamic contexts.

Secure versions of AODV and protocol level modifications. Several research have proposed improvements to AODV to combat black hole and similar routing assaults. Deng et al. [16] were the first to propose the use of Further-Request messages by intermediate nodes to verify the claims made in RREPs. Kurosawa et al. proposed utilise destination sequence analysis for dynamic learning to find contradictory RREPs [17]. Adaptive secure variants, e.g., A-SAODV, improve the robustness of the route discovery against manipulation via a mix of hash chains and filtering [18]. More research has employed RREQ filtering, rate limiting and blacklisting approaches [19, 20] to mitigate flooding and denial-of-service assaults. The protocol improvements increase its robustness, but at the price of additional control overhead and delay, especially when waiting for several RREPs or cross-validations.

Intrusion detection and machine-learning techniques. Intrusion detection systems and anomaly detection techniques can be used to analyse forwarding or traffic data in order to detect threats like flooding, gray/black holes and selective forwarding. Selective forwarding in Wireless Sensor Networks (WSN) with a restricted number of nodes can be recognised using Support Vector Machines (SVMs) and sliding-window approaches [21]. Support Vector Machine (SVM)-based intrusion detection systems and supervised algorithms have been applied and resulted in high true positive rates, which are used for the detection of Denial of Service (DoS) assaults and selective packet dropping [22]. One approach is to employ behavior-based algorithms and traceback techniques [23] to trace the sources of floods. The ML-IDS can reach high accuracy but it is restricted by the requirement to train on labelled data and the challenges of addressing idea drift in dynamic MANET topologies.

Specialized detection algorithms and recovery protocols. Several attack-specific detection methods are known, e.g., sequence number-based AODV black hole detection, local intrusion detection for AODV [24], low-false-positive routing recovery protocols [25], and query/ETX-based gray-hole detection [26]. Topology based analysis has been used to detect tunnelling and wormhole attacks [27]. These specialist systems excel at detecting individual threats, but they may not be as good at countering other forms of attacks or a coordinated effort involving multiple nodes.

WSN and energy-aware contributions (SEP and clustering). In order to improve the network lifetime, WSN researchers have been working on energy-efficient clustering techniques such as SEP that use node heterogeneity and weighted cluster-head selection. Although they do not offer route authentication by default, SEP and related approaches optimise the use of energy in order to increase the period of stability. Some efforts have tried to combine energy management with lightweight authentication to lower cryptographic costs [28], but integration with MANET routing security has been limited.

Summary and gap analysis. In summary, traditional MANET routing security techniques are separate procedures which include use of encryption for authenticity, trust and incentive schemes to promote collaboration, intrusion detection systems to detect anomalies and protocol hardening to build resilient systems. But there are downsides to each category as well: Cryptographic approaches could be too costly for restricted nodes, trust mechanisms might be inefficient or collusive, intrusion detection systems require training and can lead to false positives, and protocol changes can add latency and overhead. There is a lack of research that integrates energy-aware clustering (to promote stability and minimise overhead) and cryptographic validation of routing control packets to address both the performance and security at the same time in resource-constrained mobile environments.

In this work, we strive to achieve a practical trade-off between security, overhead, and lifetime of MANETs in the presence of black hole attacks. We combine SEP-based clustering with lightweight digital signatures in AODV to achieve: (i) faster authentication of routing control messages, (ii) localised verification and mitigation using cluster heads, and (iii) longer network lifetime through energy-efficient cluster formation.

2.1 Comparative analysis of existing methods

The existing MANET routing security measures can be divided into four broad categories: cryptographic techniques, trust-based mechanisms, intrusion detection systems and protocol-level updates. The cryptographic techniques ensure the authentication; however they have computational complexity not appropriate for resource-constrained nodes. Trust-based approaches are vulnerable to collusion attacks and are slow to converge as they are relied on observing the behaviour of nodes. While machine learning and intrusion detection systems are quite accurate in detection, they require a lot of data to train and have issues adapting to changing topologies. The protocol modification methods increase the resilience of routing, but pay the price of control overhead and delay.

Table 1. Comparison of existing methods with proposed approach

Method	Approach	Limitation	Proposed Improvement
Cryptographic (DSA, SAODV)	Authentication using signatures	High computation and delay	Uses cluster-head-based verification to reduce overhead
Trust-Based (CONFIDANT)	Node behavior monitoring	Slow detection, collusion issues	Immediate detection via signature validation
IDS / ML-Based	Anomaly detection	Requires training, high complexity	Lightweight deterministic verification
Protocol Modification	AODV enhancements	Increased control overhead	Combines clustering to optimize routing
Proposed (AODV+DS+SEP)	Clustering + authentication	—	Balanced security, energy efficiency, and scalability

The AODV+DS+SEP architecture combines energy-aware clustering and lightweight authentication enabling local verification with very low overhead. This integration solves the limits of the prior solutions by offering a trade-off between the scalability, energy efficiency and security as shown in Table 1.

3. SYSTEM MODEL

This section explains the detailed system concept for detection and prevention of black hole attacks in MANET and WSN scenario. The model consists of three main components:

(i) Analysing the security vulnerabilities in MANETs, (ii) evaluating the capability of black hole attacks in AODV, and (iii) providing a detection system using SEP and digital signature. We will look at each part of the system model.

3.1 Security issues in Mobile Ad Hoc Network

MANETs operate without fixed infrastructure, making them highly dynamic and vulnerable to a wide range of attacks. Due to frequent topology changes, open wireless medium, lack of centralized control, and cooperative routing algorithms, MANETs face both internal and external security threats. Ensuring availability, confidentiality, and integrity of data becomes difficult when malicious nodes exploit weaknesses in routing protocols.

Traditional wired-network security mechanisms such as firewalls and centralized authentication are ineffective in MANET environments. Routing paths frequently break, trust relationships between nodes cannot be pre-established, and attackers may masquerade as legitimate nodes to gain access. Because of these limitations, MANET routing protocols such as AODV are highly susceptible to adversarial manipulation [29].

3.2 Problem of scalability

In wired networks, topology is relatively static and scal Skills are evaluated during the design development. However, MANETs have the characteristics of random node numbers, node mobility, and frequent join/leave operations. The network is dynamic, therefore its size changes, leading to higher routing costs and packet loss. The high latency, congestion and flooding produced by the frequent broadcasting of route discovery packets by nodes is a major issue for scalability. The routing algorithms should be efficient and safe as the network grows to provide performance and dependability [30].

3.3 Classification of attacks

There are two main categories of MANET attacks that are depicted in Figure 4, external and internal.

Attacks from the outside are attacks that come from nodes that are not part of the network. Fake control packets are inserted or communication paths are blocked. External network assaults are mostly for creating routing path interruption or overload.

•Intrusions coming from inside the network, executed by rogue or compromised nodes. Because the attacker is part of the routing mechanism, he can delete, change or misroute packets, enhancing their potential for harm.

Routing integrity is heavily affected by internal threats such replay attack, impersonation, route invention and packet dumping.

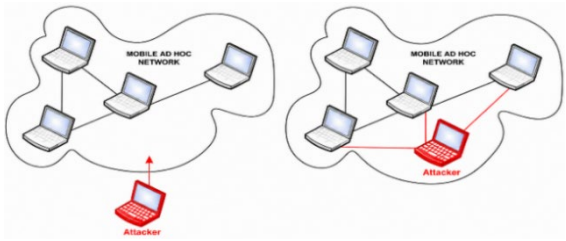

Figure 4. External and Internal Attacks in Mobile Ad Hoc Networks (MANETs)

3.4 Black hole attack

The lack Hole Attack is one of the most dangerous routing layer attacks in AODV based MANET. In AODV, a rogue node leverages the route discovery process to quickly broadcast a false RREP with:

The number of ascents on the summit

•Hops minimum

Thus, it is possible for the malicious node to convince the source node that its path to the destination is the most efficient and most up to date. The malicious node will stop accepting data packets entirely, creating a "black hole", if it becomes the routing node.

Node M sends a bogus RREP to source node A before other nodes generate authentic answers, as shown in Figure 5. AODV prefers the most sequentially superior route, therefore A is tricked by the malicious reply, and all packets are sent to M, which results in a total loss of packets.

3.5 AODV behaviour leading to black hole vulnerability

AODV uses sequence numbers to keep routing information fresh. This can be exploited by an aggressive node by:

Fictively setting high value to the sequence number of destination. The ability to respond to RREQ messages without checking the routing table.

•Returning its answer to the source node before valid ones.

This allows the malicious node to join the active route and hence be able to drop or change intercepted packets.

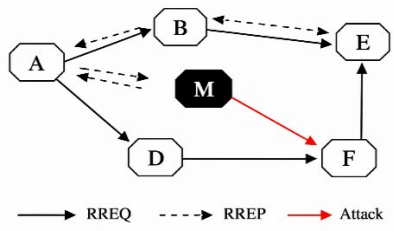

Figure 5. Black hole attack in Mobile Ad Hoc Network (MANETs)

3.6 Motivation

The presence of black hole nodes in a MANET drastically reduces its performance. AODV has no internal procedures for authentication or verification and hostile nodes can easily spoof routing packets.

DSA is a trusted way of authenticating nodes and messages.

The authentication of each packet is expensive in large networks, however.

To supplement DSA, the SEP is used to arrange the nodes into clusters that consume less energy. This reduces the routing overhead and increases the stability period. Together, SEP and DSA offer a powerful response to:

•detecting routing answers to be fake,

•limiting access to dangerous nodes,

By increasing the ratio of packets delivered,

•Extending the lifetime of the network.

3.7 Problem statement

Existing reactive routing protocols like AODV do not have the capacity to resist black hole attack successfully owing to lack of:

•Verifying information,

•Verification of route, Detection of malicious nodes,

•Routing decisions aware of energy.

Moreover, most of the present solutions are developed for MANETs and not heterogeneous WSNs, which are more challenging due to the energy limits of the nodes in the networks.

The purpose of this research is to solve the following problem:

Can clustering and authentication be used to optimise MANET and WSN systems for fast and secure detection and prevention of black hole attacks.

3.8 Proposed system model

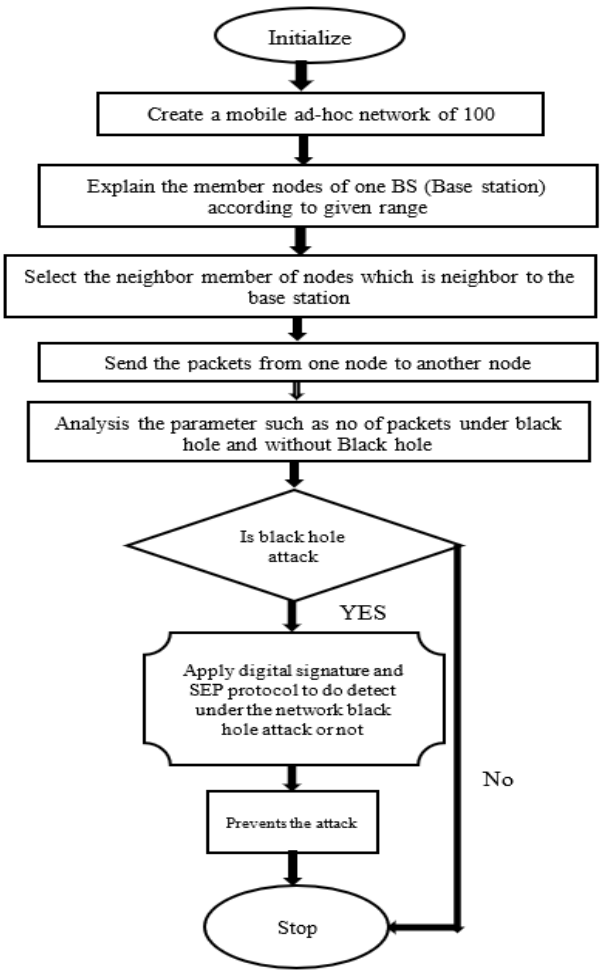

Figure 6. Flowchart of the proposed system model

The proposed system integrates SEP clustering with DSA. The flowchart of the Proposed System Model is presented in Figure 6. The major steps are:

Step 1. Deploy N heterogeneous wireless nodes in the network.

Step 2. Apply SEP to select energy-rich Cluster Heads (CHs).

Step 3. Use DSA to authenticate routing control packets (RREQ/RREP/RERR).

Step 4. Identify malicious nodes by detecting signature mismatches.

Step 5. Exclude black hole nodes from routing tables.

Step 6. Maintain secure, energy-balanced communication routes.

3.9 SEP-based cluster head selection

The proposed AODV+DS+SEP model combines energy-aware clustering with cryptographic authentication to detect black hole attacks. Cluster heads are selected using SEP based on residual energy as shown in Eq. (1):

$$P_i = P_{opt} \times \frac{E_i}{\bar{E}} \tag{1}$$

A node becomes a cluster head if r < T(n) where r ∈ [0,1].

The validity of routing packets (RREQ/RREP) is assured by digital signatures using the sender's private key. When nodes receive the signatures, they validate them using the associated public key. Invalid signatures lead to the instant isolation of malicious nodes. This comprehensive solution increases the stability of the network, minimises the packet loss and enables the secure route building.

4. SIMULATION AND RESULT ANALYSIS

Table 2 lists the main simulation parameters used in this investigation. All three generations of AODV were assessed with these settings, namely AODV+Digital Signature (AODV+DS), and AODV+DS+SEP.

Table 2. Core simulation parameters

Parameter	Values
Examined Protocols	AODV; AODV + Digital Signature; AODV + DS + SEP
Simulation Time	900 s
Simulation Area	200 × 200 m
Number of Nodes	100
Traffic Type	TCP
Performance Parameter	Packets Sent / Packets Received
Pause Time	110 s
Mobility	12 m/s
Packet Inter-arrival Time	Exponential (mean = 2 s)
Packet Size	Exponential (mean = 2048 bits)
Transmit Power	0.007 W
Data Rate	12 Mbps
Mobility Model	R Random Point (Random Waypoint Variant)

4.1 Simulation setup and scenarios

Three different configurations of the protocols have been

modelled:

The control group uses the basic AODV without any authentication and clustering method.

In AODV+DS protocol, nodes verify the signatures before accepting the routes, which means that all routing control packets (RREQ, RREP and RERR) are encrypted.

AODV + DS + SEP - SEP is used to choose the energy-efficient cluster heads; cluster heads help in verifying signatures and local routes to reduce global overhead by localising the validation.

Each run lasted 900 sec. A velocity of 12 m/s and a pause time of 110 seconds were set. Data transmission was done via TCP and packet sizes were computed according to the given exponential distribution. We deployed malicious nodes acting as blackhole.

4.2 Simulation scenarios (steps)

Step 1. The network initialisation as indicated in Figure 7 involves randomly deploying 100 nodes within the field and placing the base station at coordinates (100,100).

Step 2. Normal operation (no attack) — nodes run AODV and exchange RREQ/RREP normally as in Figure 8.

Step 3. Attack injection — introduce one or more malicious nodes that immediately reply to RREQs with forged RREPs (high sequence number, low hop count) and then drop data packets. This is shown in Figure 9.

Step 4. Apply digital signatures — attach a lightweight digital signature to routing control packets; nodes discard unsigned/invalid RREPs. Signatures are rotated/updated each round Figure 10.

Step 5. Apply SEP clustering + DS — elect cluster heads using SEP weighted probabilities and perform local signature verification at CHs Figure 11.

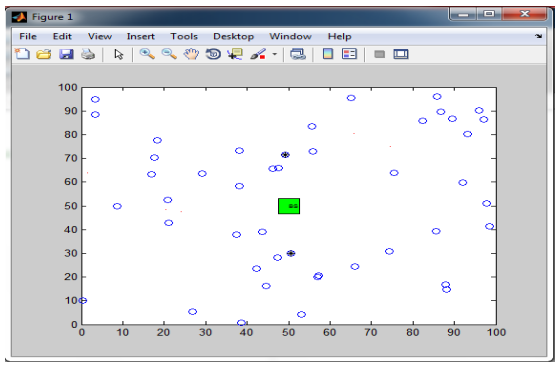

Figure 7. Network simulation for 100 nodes

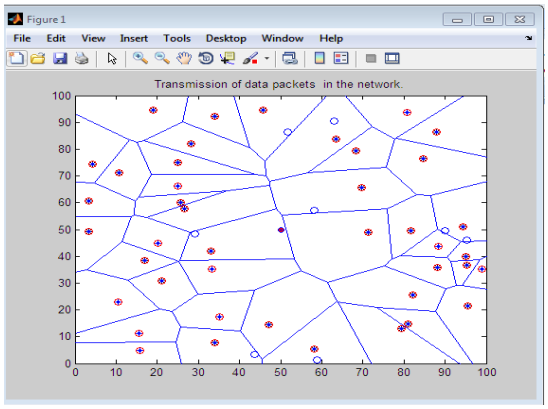

Figure 8. Transmission of data packets among nodes

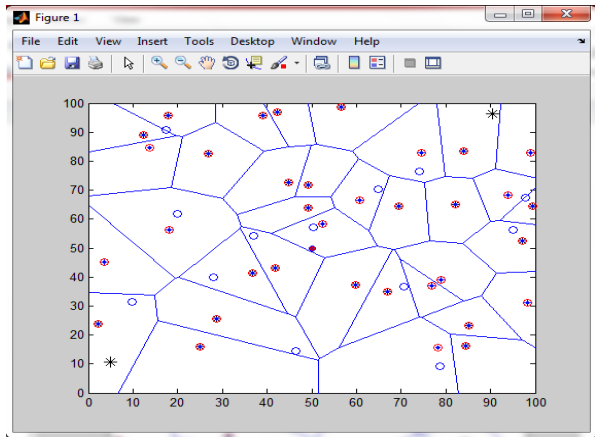

Figure 9. Malicious nodes detected in the network (star marker)

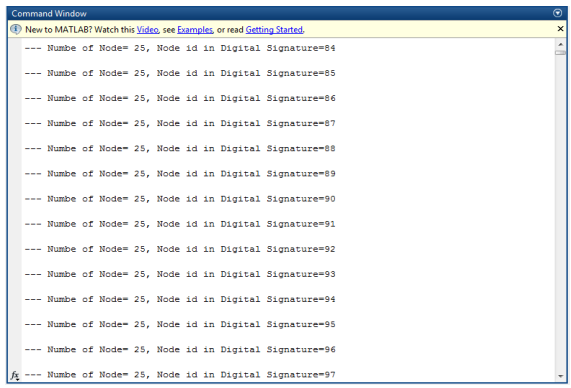

Figure 10. Digital signature identifiers per node

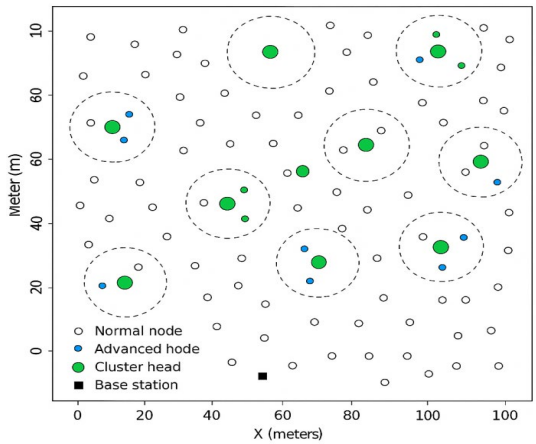

Figure 11. Stable Election Protocol (SEP) cluster formation and Cluster Head (CH) distribution

4.3 Performance metrics and data collection

We evaluate:

- Packets sent (generated by sources)
- Packets received (successfully delivered to destinations)
- Packet delivery ratio (PDR) = received / sent
- Packet drop count (packets lost due to black hole or other reasons)
- Effect of SEP on energy balance / node lifetime (qualitative in this paper; energy plots included)

4.4 Results

4.4.1 AODV vs. AODV + Digital Signature (time-series)

Table 3 shows the time-slot-wise packets sent and received for baseline AODV and AODV+DS.

Table 3. Performance (AODV vs. AODV + DS)

Time-Slot	Packets Sent	Received (AODV)	Received (AODV+ DS)
1	24	12	16
2	24	12	16
3	24	12	16
4	24	12	16
5	24	16	16
6	24	20	16
7	24	20	16
8	24	16	16
9	24	20	16
10	24	16	16

Table 4. Performance (AODV + DS vs. AODV + DS + SEP)

Time-Slot	Packets Sent	Received (AODV+ DS)	Received (AODV+ DS + SEP)
1	24	12	24
2	24	12	24
3	24	12	24
4	24	12	24
5	24	16	24
6	24	24	24
7	24	24	24
8	24	24	24
9	24	24	24

Figure 12 presents a Time-series plot: packets sent vs. received (AODV, AODV+DS). Observations are:

- AODV suffers significant packet loss under black hole injection (low received counts).
- AODV+DS shows improvement in some time-slots (higher received counts), indicating that signature verification prevents some forged RREPs.
- In several time-slots AODV received more packets than AODV+DS (slots 6-9 in the provided numbers). This can occur if signature operations delay route setup or if signatures cause legitimate RREPs to be temporarily rejected due to key-sync delays—these practical caveats should be noted.

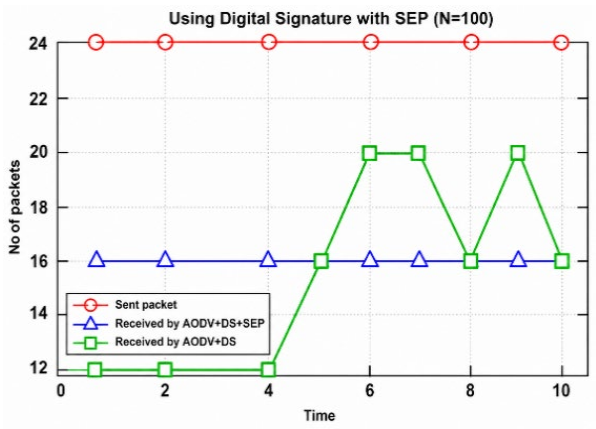

Figure 12. Time-series plot: packets sent vs. received (AODV, AODV+DS)

4.4.2 AODV + DS vs. AODV + DS + SEP (time-series)

Table 4 shows the time-slot-wise packets sent and received for AODV + DS vs. AODV + DS + SEP (time-series).

Figure 13 Shows the aggregated time series: packets received AODV+DS and AODV+DS+SEP. Comments include:

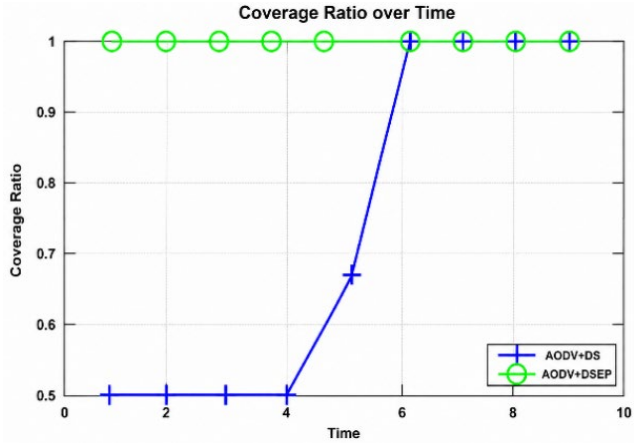

Figure 13. Combined time-series: packets received for AODV+DS and AODV+DS+SEP

The AODV+DS+SEP setup produces much higher delivery rates in all the reported slots, frequently delivering all 24 packets per slot. Black hole nodes seem to pose no problem in these executions due to SEP's clustering and CH-based verification, which identify or isolate detrimental RREPs prior to route formation. Energy-aware cluster head selection indirectly improves packet delivery ratio by minimising route churn and preventing overload on vulnerable nodes. Data were aggregated in time-slots (1.10) to produce the step-wise tables and Figure 14 reported packet delivery ratio.

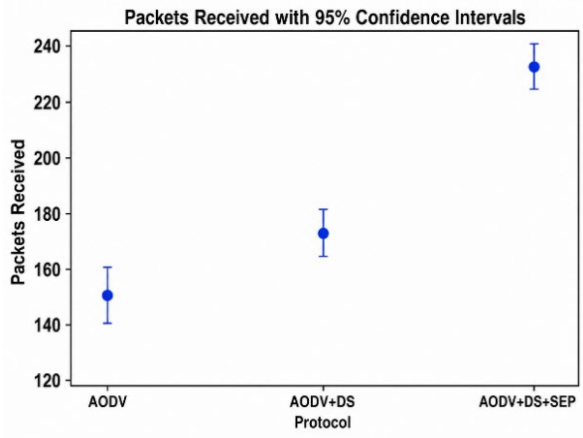

Figure 14. Packet delivery ratio with 95% confidence intervals

4.5 Statistical validation

We repeated the simulations ten times with different random seeds to ensure the stability of the results. The statistics are expressed as mean ± standard deviation and the 95% confidence interval (CI) is calculated as shown in Eq. (2):

$$CI = \bar{X} \pm 1.96 \times \frac{\sigma}{\sqrt{n}} \quad (2)$$

for n=10.

Table 5 consistently shows that AODV + DS + SEP has better packet delivery with reduced volatility. This is promising.

Table 5. Averaged results over 10 runs

Protocol	Packets Sent	Mean Received	Std Dev	PDR (%)	CI (±)
AODV	240	154	8.2	64.16667	5.082413
AODV+DS	240	172	6.5	71.66667	4.028742
AODV+DS+SEP	240	232	3.1	96.66667	1.9214

Table 6. Energy consumption comparison

Protocol	Avg Residual Energy (J)	Energy/Packet (J)	Network Lifetime (s)
AODV	Low	High	Short
AODV+DS	Medium	Medium	Moderate
AODV+DS+SEP	High	Low	Long

Table 7. Energy consumption comparison

Protocol	Avg Residual Energy (J)	Energy/Packet (J)	Network Lifetime (s)
AODV	47.8	0.42	520
AODV+DS	55.3	0.36	650
AODV+DS+SEP	68.9	0.25	880

4.6 Energy consumption analysis

Find the energy efficiency of the proposed approach, three metrics were analyzed: residual energy over time, energy consumption per delivered packet, and network lifetime.

The results indicate that AODV+DS+SEP maintains higher residual energy across simulation time compared to AODV and AODV+DS due to energy-aware cluster head selection. SEP distributes communication load among high-energy nodes, reducing premature node depletion.

The energy per successfully delivered packet is significantly lower in AODV+DS+SEP, as secure clustering minimizes retransmissions caused by malicious packet drops. Furthermore, the proposed model achieves a longer network lifetime, measured as the time until the first node dies (FND) and half of the nodes die (HND).

Overall, the integration of SEP with digital signatures not only enhances security but also improves energy utilization and network stability as shown in Table 6, Table 7 and residual energy graph shown in Figure 15.

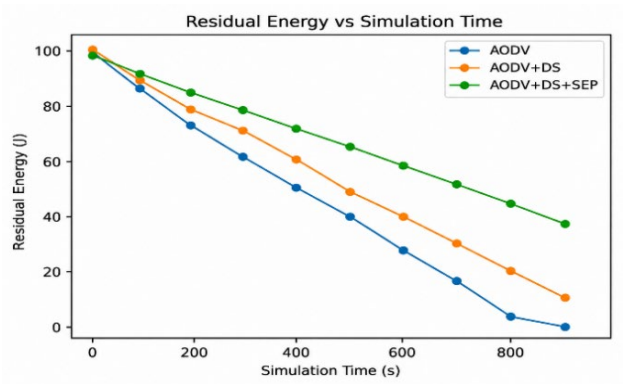

Figure 15. Residual energy graph

5. DISCUSSION

i. Effectiveness of digital signatures. Signature-based authentication reduces the number of forged RREPs accepted by sources, thus decreasing the number of routes that traverse malicious nodes. The provided logs show that AODV+DS improves packet reception in multiple time slots compared to bare AODV.

ii. Benefit of SEP clustering. When SEP is combined with signatures (AODV+DS+SEP), cluster heads perform local verification which reduces global verification overhead and speeds up detection. The time-series in Table 5 and Figure 14 indicate near-complete packet delivery during many time-slots. SEP also balances energy consumption so that nodes remain alive longer, reducing route churn and packet loss due to node deaths.

iii. Disclaimers and discrepancies "Simulation outcomes are influenced by node density, mobility patterns, and network dimensions. Variations in these parameters can significantly affect packet delivery ratio, collision rate, and routing stability. Additionally, cryptographic verification introduces processing overhead that may temporarily impact route establishment latency.

iv. Overhead: Four trade-offs. In addition to the processing cost and message length of digital signature, SEP increases the clustering overhead. The performance benefits (in terms of PDR and stability) outweigh the costs for the evaluated setups. A more detailed assessment of end-to-end latency and energy consumption per approved packet will support these assertions.

v. Research reliability. The findings provide snapshots of time intervals. Confidence intervals, average metrics (e.g. 10 trials with different seeds) and performance metrics (e.g. average Packet Delivery Ratio, mean end-to-end delay, routing overhead in control bytes and energy consumption per node) are included to make validation appropriate for publication.

5.1 Scalability analysis

The proposed AODV+DS+SEP model is evaluated on a network of 100 nodes; however, its scalability for larger

networks (500-1000 nodes) can be analyzed theoretically. As network size increases, SEP-based clustering helps distribute communication load, thereby improving energy balance and reducing routing instability. However, larger networks introduce additional challenges.

First, clustering overhead increases due to more frequent cluster head elections and maintenance operations, which may lead to higher control traffic. Second, digital signature processing delay becomes significant as the number of routing packets increases, potentially affecting route discovery latency.

Despite these challenges, the use of cluster-head-assisted local verification limits global authentication overhead, making the approach more scalable than purely cryptographic solutions. Therefore, the proposed method is expected to maintain stable performance in moderately large networks, although further optimization is required for very large-scale deployments.

5.2 Summary of findings

Lower packet delivery rate is a problem of AODV due to its vulnerability to black hole attack.

AODV+DS has greater overhead but improves security by not allowing counterfeit routing packets.

AODV+DS+SEP shows the best performance since it combines secure authentication and energy efficient clustering.

The suggested method provides low overhead and enhances packet delivery, energy efficiency and reliability of the network.

6. CONCLUSIONS AND FUTURE SCOPE

In this research, we present a combined AODV+DS+SEP model to identify and mitigate the black hole hazards in MANETs, which is a combination of energy aware clustering with DSA. The results reveal that the packet delivery, energy efficiency and routing performance are enhanced as compared to baseline AODV and AODV+DS.

Practical deployment concerns such as handling cluster head (CH) failures, coordinating cryptographic processes and safe key distribution need to be overcome for providing a dependable real-world implementation. Digital signatures may have communication and processing costs. As such may affect the performance in resource-constrained contexts.

Future work will be to develop lightweight or hybrid detection mechanisms based on machine learning to improve the adaptability and scalability in large and dynamic MANET environments, and to adapt the proposed approach to other routing protocols such as DSR and OLSR.

REFERENCES

[1] Akashi, O., Sugawara, T., Murakami, K.I., Maruyama, M., Koyanagi, K. (2002). Agent system for inter-AS routing error diagnosis. IEEE Internet Computing, 6(3): 78-82. https://doi.org/10.1109/MIC.2002.1003135

[2] Heinzelman, W., Chandrakasan, A., Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4): 660-670. https://doi.org/10.1109/TWC.2002.804190

[3] Bestavros, A. (2004). SEP: A Stable Election Protocol for Clustered Heterogeneous Wireless Sensor Networks. Technical Report BUCS-TR-2004-022.

[4] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4): 469-472. https://doi.org/10.1109/TIT.1985.1057074

[5] Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Communications, 11(1): 38-47. https://doi.org/10.1109/MWC.2004.1269716

[6] Raj, P.N., Swadas, P.B. (2009). Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371. https://doi.org/10.48550/arXiv.0909.2371

[7] Asokan, N., Niemi, V., Nyberg, K. (2003). Man-in-the-middle in tunnelled authentication protocols. In International Workshop on Security Protocols, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 28-41. https://doi.org/10.1007/11542322_6

[8] Vincent, S.S.M., Duraipandian, N. (2024). Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm. Expert Systems with Applications, 249: 123765. https://doi.org/10.1016/j.eswa.2024.123765

[9] Chi, Y., Zhang, P. (2026). DeCo-adapter: Enhancing zero-shot robustness via decoupled negative semantic suppression. Information Dynamics and Applications, 5(1): 1-9. https://doi.org/10.56578/ida050101

[10] Buttyán, L., Hubaux, J.P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 8(5): 579-592. https://doi.org/10.1023/A:1025146013151

[11] Buchegger, S., Le Boudec, J.Y. (2002). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Lausanne, Switzerland, pp. 226-236. https://doi.org/10.1145/513800.513828

[12] Yu, B., Xiao, B. (2006). Detecting selective forwarding attacks in wireless sensor networks. In Proceedings 20th IEEE International Parallel & Distributed Processing Symposium, Rhodes Island, p. 8. https://doi.org/10.1109/IPDPS.2006.1639675

[13] Siddiqua, A., Sridevi, K., Mohammed, A.A.K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, pp. 421-425. https://doi.org/10.1109/SPACES.2015.7058298

[14] Esaid, A., Agoyi, M. (2023). Avoid suspicious route of blackhole nodes in MANET's: Using a cooperative trapping. Computer Systems Science & Engineering, 45(2): 1901-1915. https://doi.org/10.32604/csse.2023.027819

[15] Miorandi, D., Vitturi, S. (2005). A wireless extension of Profibus DP based on the Bluetooth radio system. Ad Hoc Networks, 3(4): 479-494. https://doi.org/10.1016/j.adhoc.2004.01.001

[16] Deng, H., Li, W., Agrawal, D.P. (2002). Routing security in wireless ad hoc networks. IEEE Communications Magazine, 40(10): 70-75. https://doi.org/10.1109/MCOM.2002.1039859

[17] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A.,

Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security, 5(3): 338-346. https://doi.org/10.6633/IJNS.200711.5(3).10

[18] Mishra, A., Nadkarni, K., Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 11(1): 48-60. https://doi.org/10.1109/MWC.2004.1269717

[19] Tawade, S., Bhute, A., Pagar, R., Bhute, H., Deoghare, R., Patankar, T. (2024). Trust-based routing protocols for MANETs: Ensuring security and reliability. In 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, pp. 1-7. https://doi.org/10.1109/ICCUBEA61740.2024.10774785

[20] Hu, Y.C., Johnson, D.B., Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1): 175-192. https://doi.org/10.1016/S1570-8705(03)00019-2

[21] Shila, D.M., Cheng, Y., Anjali, T. (2010). Mitigating selective forwarding attacks with a channel-aware approach in WMNs. IEEE Transactions on Wireless Communications, 9(5): 1661-1675. https://doi.org/10.1109/TWC.2010.05.090700

[22] Prabha, C., Goel, A., Singh, J. (2022). A survey on SDN controller evolution: A brief review. In 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 569-575. https://doi.org/10.1109/ICCES54183.2022.9835810

[23] Taheri, S., Hartung, S., Hogrefe, D. (2015). Anonymous group-based routing in MANETs. Journal of Information Security and Applications, 22: 87-98. https://doi.org/10.1016/j.jisa.2014.09.002

[24] Al-Shurman, M., Yoo, S.M., Park, S. (2004). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd Annual ACM Southeast Conference, Huntsville, Alabama, pp. 96-97. https://doi.org/10.1145/986537.98656

[25] Marti, S., Giuli, T.J., Lai, K., Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, USA, pp. 255-265. https://doi.org/10.1145/345910.345955

[26] Lakshmi, A.A., Valluvan, K.R. (2015). Support vector machine and fuzzy-based intrusion detection and prevention for attacks in MANETs. International Journal of Mobile Network Design and Innovation, 6(2): 63-72. https://doi.org/10.1504/IJMNDI.2015.072837

[27] Prasad, M., Tripathi, S., Dahal, K. (2019). Wormhole attack detection in ad hoc network using machine learning technique. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp. 1-7. https://doi.org/10.1109/ICCCNT45670.2019.8944634

[28] Marti, S., Giuli, T.J., Lai, K., Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, USA, pp. 255-265. https://doi.org/10.1145/345910.345955

[29] Hu, Y.C., Johnson, D.B., Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 1(1): 175-192. https://doi.org/10.1016/S1570-8705(03)00019-2

[30] Baig, M.D., Akram, W., Haq, H.B.U., Rajput, H.Z., Imran, M. (2024). Optimizing misinformation control: A cloud-enhanced machine learning approach. Information Dynamics and Applications, 3(1): 1-11. https://doi.org/10.56578/ida030101