JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-21, No.-08, August (2026) pp 180-197 ISSN (Print) 0973-8975

AN ADAPTIVE HYBRID ANTNET WITH OPTIMIZED SVM FOR RELIABLE AND SCALABLE MANET ROUTING

G. Kalaiselvi[1], M. G. Kavitha[2]

[1]School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu, India-613401.

[2]University College of Engineering Pattukkottai, Rajamadam, Tamil Nadu, India-614701.

Email: [1]winmathy05@gmail.com, [2]mgkavi@gmail.com

Corresponding Author: **G. Kalaiselvi**

https://doi.org/10.26782/jmcms.2026.08.00011

(Received: May 16, 2026; Revised: July 29, 2026; Accepted: August 08, 2026)

Abstract

Mobile Ad hoc Networks (MANETs) are decentralized, infrastructure-less networks characterized by dynamic topology, making them highly vulnerable to security threats such as blackhole attacks and prone to performance degradation under increasing network scale. Most established routing protocols cannot simultaneously address adaptive routing efficiency and intrusion detection with low computational overhead. An enhanced routing framework, Adaptive Hybrid Antnet with Optimized Support Vector Machine (AH-MantnetOpSVM), presented in this paper, offers adaptive, scalable, and secure communication in MANETs. This approach combines adaptive parameter tuning into the Antnet routing mechanism for the dynamic regulation of pheromone updates based on the residual energy of the node and real-time congestion levels while incorporating an optimized SVM-based intrusion detection for identifying and isolating malicious nodes involved in blackhole attacks, with reduced computational overhead. There is a consistent and substantial improvement in packet delivery ratio, throughput, and network lifetime while reducing delay and false positive rate. Unlike conventional approaches that suffer performance degradation as node density increases, AH-MantnetOpSVM consistently maintains stable and reliable performance across varying network scales, thereby effectively enhancing both security and scalability in the MANET environment.

Keywords: Mobile Ad Hoc Networks, Ant Colony Optimization, Support Vector Machine, Intrusion Detection System, Blackhole Attack, Secure Routing.

I. Introduction

Mobile Ad Hoc Networks (MANETs) operate as self-organizing wireless systems where mobile nodes dynamically form communication links without the need for fixed infrastructure. Due to their flexibility and rapid deployment capabilities,

MANETs are widely applied in scenarios such as disaster management, military operations, and remote communication environments. However, the absence of centralized control and the highly dynamic topology introduce significant challenges in maintaining reliable communication and efficient routing [XVIII], [XVI].

One of the primary challenges in MANETs is the frequent topology variation caused by node mobility, which leads to unstable routing paths and increased packet loss. In addition, limited energy resources and increasing node density further complicate network scalability and performance. As the number of nodes grows, congestion and routing overhead increase, resulting in degradation of key performance metrics such as packet delivery ratio and throughput [XXVI], [I]. Therefore, designing adaptive and energy-efficient routing mechanisms remains a critical research issue.

Along with routing challenges, security threats pose a major concern in MANET environments. The open medium and lack of centralized monitoring make these networks highly vulnerable to various attacks, among which the blackhole attack is one of the most severe. In such attacks, malicious nodes falsely advertise optimal routes and subsequently drop data packets, causing significant disruption in communication [XI]. Traditional routing protocols such as AODV and DSR often suffer from increased routing overhead and reduced performance in highly dynamic environments and are not equipped with mechanisms to detect or mitigate such attacks, leading to severe performance degradation.

To address these issues, several research efforts have focused on integrating intelligent techniques into routing and security frameworks. Machine learning-based intrusion detection systems have been widely explored to enhance attack detection accuracy [V],[XXI]. Recent studies have demonstrated the effectiveness of deep learning and hybrid models in identifying anomalous behavior in MANETs [XIX], [XIII]. However, many of these approaches introduce additional computational complexity and are not tightly integrated with routing mechanisms.

Bio-inspired routing techniques, particularly those based on ant colony optimization, have shown promising results in improving routing efficiency and adaptability in dynamic networks. These approaches utilize pheromone-based path selection to identify optimal routes under varying network conditions [XXII],[XVII]. Although such methods enhance routing performance, they often lack integrated security mechanisms, making them susceptible to malicious attacks. Similarly, hybrid approaches combining routing and machine learning have been proposed, but they often fail to address scalability and parameter optimization effectively [XI], [XXV], [VII].

Despite significant advancements, there exists a critical need to develop a unified framework that simultaneously addresses adaptive routing, efficient intrusion detection, and scalability under varying network conditions. Most existing works either focus on routing optimization or security enhancement independently, without considering the combined impact of node density, energy efficiency, and dynamic network behavior. Furthermore, limited attention has been given to adaptive parameter tuning mechanisms that can improve system performance in real-time.

Earlier work introduced hybrid routing frameworks such as H-MAntnetSVM, which integrates AntNet routing with SVM-based intrusion detection to improve security and performance in MANETs. An enhanced version, H-MantnetOpSVM, further improved detection accuracy through SVM parameter optimization. However, these approaches do not incorporate adaptive parameter tuning within the routing process and show limitations in scalability under increasing network sizes [XI], [XIV].

To overcome these limitations, an Adaptive Hybrid Antnet with Optimized Support Vector Machine (AH-MantnetOpSVM) framework is proposed in this paper that integrates adaptive parameter tuning into the Antnet routing mechanism for dynamic pheromone regulation based on residual energy and congestion levels. Additionally, an optimized SVM-based intrusion detection model is incorporated to accurately identify and isolate malicious nodes involved in blackhole attacks while reducing computational overhead through feature optimization.

The main contributions of this work include the development of an adaptive bio-inspired routing mechanism, integrated with optimized machine learning-based intrusion detection, and comprehensive performance evaluation under varying node densities ranging from 50 to 200 nodes. The proposed model is evaluated using metrics such as packet delivery ratio, end-to-end delay, throughput, accuracy, false positive rate, and network lifetime to demonstrate its effectiveness.

The remainder of this paper is organized as follows: Section 2 presents the literature review of the existing routing and security detection approaches in MANETs. Section 3 describes the proposed methodology, the adaptive routing mechanism, parameter tuning strategy, and optimized SVM-based intrusion detection. Section 4 discusses the simulation setup along with the results and discussion, analysing the performance of the proposed method under varying network conditions. The last section concludes the paper and highlights the potential directions for future research.

II. Literature Survey

Mobile Ad Hoc Networks (MANETs) are highly dynamic and infrastructure-less networks, making routing and security significant challenges. The frequent topology changes and absence of centralized control expose MANETs to various routing attacks such as blackhole and flooding attacks. Therefore, designing an efficient and secure routing mechanism remains a critical research problem.

H-MAntnetSVM, proposed in [XI], integrates Antnet-based routing with SVM-based intrusion detection for secure communication in MANETs. However, its fixed SVM parameters limit scalability under higher node density, leading to increased computational overhead. To overcome the limitations of H-MAntnetSVM, H-MantnetOpSVM was developed by incorporating SVM hyperparameter optimization via a grid search, achieving improved detection accuracy [XIV].

An Adaptive Ensemble Tree Learning (AETL) based 2-stage intrusion detection, and Hybrid Dual Optimization of Machine Learning Model (HDOMLM) are introduced in [XIX] to improve energy efficiency and network lifetime through optimized clustering and leading agent selection. A hybrid Network Intrusion Detection System (NIDS) combining XGBoost, Random Forest, Graph Neural Networks (GNN), Long

Short-Term Memory (LSTM) networks, and Autoencoders is presented in [VI]. AI-driven intrusion detection systems (IDS) enhance MANET security by tackling the vulnerabilities caused by their decentralized dynamic characteristics, improving attack detection rates and minimizing false positives [XIII].

The application of deep learning methodologies in Intrusion Detection Systems (IDS) enhances the security of MANETs by detecting attacks such as black hole and gray hole attacks. [XXIII]. An adaptive clustering mechanism is presented to minimize energy utilization and improve network efficiency and robustness of the dynamic MANETs [XXVI]. An energy-efficient adaptive routing mechanism is proposed to address energy consumption and network performance while considering the dynamic nature and energy constraints of MANETs [XXVIII].

The review highlights that combining clustering algorithms and energy-efficient routing protocols addresses many issues in dynamic and energy-constrained MANETs [V]. Improved Grey Wolf Optimization Artificial Neural Networks (IGWO-ANN), a classification algorithm, is proposed to improve the detection of intruders by combining IGWO and ANN [XXIV]. MANET security is improved using Support Vector Machine (SVM) based anomaly detection to detect black hole attacks [II]. Artificial Neural Networks (ANNs) are explored for energy saving and routing in MANETs [XII]. The fuzzy-based inference system with ensemble classification offers a high degree of improvement in intrusion detection and classification to provide the trustworthiness of MANET services [VIII].

A machine learning approach with a trust-based system that is a combination of methods produces an improvement in detection while reducing its impact on network performance [XX]. A security approach is presented to address vulnerabilities of MANETs arising from their decentralized nature and exposure to various attacks [I]. A combination of security mechanisms and performance measures presented in [XXII] caters to specific issues encountered in MANETs, such as the ever-changing topology and the security issues faced. Adaptive techniques and multi-objective optimization are incorporated into ACO to overcome slow convergence and local optima, with improved heuristic functions and pheromone updates for effective routing. These issues are most significant in infrastructure-less networks where existing routing protocols can no longer perform well [XXV], [XVI].

A secure and effective routing mechanism to address the various attacks while considering node mobility and the lack of infrastructure is required [XXI]. A decision tree (DT) based intrusion detection approach achieved 98.9% accuracy, representing sophisticated detection mechanisms for network security [III]. A comparative analysis of bio-inspired algorithms, including AntNet, ARA, and AntHocNet, efficiently adapt the routing of a dynamic network [X]. HyphaNet, a bio-inspired routing algorithm that uses the self-organizing and adaptive characteristics of fungal networks to optimize routing based on attractiveness and resource availability, achieves improved performance over traditional algorithms [IX].

AOERP is an energy-aware protocol enhancing route reliability and extended network lifetime by selecting feasible paths by considering the limited energy of the nodes within the transmission range [IV]. An adaptive greedy strategy, GSACO, is

proposed to improve routing through enhanced network stabilization [XVII]. MAODV-ACO protocol achieves a 99.66% Packet Delivery Ratio (PDR) for 100 nodes, while reducing delay compared with CARP and AODV-BA-DST[VII]. Reactive routing protocols combined with ACO provide an improved, efficient, and secure routing in MANETs, through repetitive configuration of routes [XV].

Research Gap and Motivation

Despite several advances in MANET routing and security over the period, a few limitations still exist. Most existing studies focus either on route optimization or on intrusion detection using swarm intelligence methods, limiting the integration between routing and security functionalities. Some hybrid models such as H-MAntnetSVM and H-MantnetOpSVM improve performance but depend on fixed parameters and limited network size, restricting adaptability and scalability. Moreover, the optimized SVM detection adds processing load and is not closely linked with routing decisions.

These limitations highlight the need for an adaptive framework addressing routing efficiency, security, and scalability. Accordingly, the AH-MantnetOpSVM integrates adaptive Antnet routing with parameter tuning and an optimized SVM-based intrusion detection for efficient, secure, and scalable communication in dynamic MANET environments.

III. Methodology

Network Model

The Mobile Ad Hoc Network (MANET) is modelled as a dynamic graph G= (V, E), where V represents the set of nodes in the network, and E denotes the wireless connectivity between them. Each node in the network operates independently and participates in routing by forwarding packets for other nodes without relying on any centralized infrastructure. The mobility and limited transmission range of the nodes in the network result in frequent route disruptions, which are experienced in the network, making route discovery and maintenance more complex.

The links established between the nodes fall within each other's communication range, so a multi-hop transmission is achieved between nodes. Certain essential characteristics of MANETs, like the absence of centralized monitoring in the network along with inconsistent topology, make them vulnerable to several routing threats. Among all the types of attacks, blackhole attacks are significant ones that particularly disrupt the entire network, as malicious nodes advertise false optimal routes; once it receives the data packets from other nodes in the transmission range, they intentionally drop packets. Hence, an efficient routing strategy must be integrated with a reliable intrusion detection mechanism to ensure secure and consistent data transmission [XI].

System Architecture

The proposed energy efficient and security enhanced routing algorithm, which combines adaptive swarm intelligence based Antnet routing with an optimized Support Vector Machine (SVM) based intrusion detection system for Mobile Ad Hoc

Networks (MANETs), is illustrated in Fig.1. The system architecture consists of four major components: the Adaptive Hybrid Antnet routing module, parameter tuning module, feature extraction unit, and SVM based intrusion detection system.

During the route discovery process, the routing module explores multiple paths using swarm intelligence techniques, where optimal routes are selected based on pheromone values and heuristic information. The adaptive parameter tuning module dynamically adjusts routing parameters, such as the pheromone update rate, based on residual energy and congestion levels, thereby enhancing overall network performance.

The feature extraction unit collects node behavioral parameters, including packet forwarding ratio and delay variation, which are utilized by the SVM classifier to detect malicious nodes and classify them as either normal or malicious. Once blackhole nodes are identified, they are isolated from the network, and a secure path for data transmission is recomputed by the routing module. Thus, the proposed approach ensures both efficient routing and enhanced security in dynamic MANET environments.

Adaptive Hybrid Antnet Routing

An adaptive hybrid antnet algorithm is proposed to overcome the challenges arises in mobile ad hoc networks by providing an energy-efficient route discovery by considering the limited energy sources of the nodes. The method is inspired by swarm intelligence, utilizing artificial ants that reinforce high-quality routes by exploring multiple paths between the source and destination through pheromone updates.

Residual energy, congestion level, and node connectivity are the network state variables primary focussed in the proposed routing technique that need dynamic updates based on the network condition. Unlike conventional Antnet protocols that use fixed parameters, the proposed approach provides adaptive parameter tuning to improve route reliability and prevent excessive energy consumption under high-density networks.

The routing process is initiated by the source node with the generation and propagation of forward ants (FANTs) through neighboring nodes. Next-hop selection is done based on pheromone intensity and heuristic information. Using the probabilistic transition rule represented in Eq. (1), the probability of selecting the next hop during route discovery is determined,

$$P_{ij} = \frac{(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}}{\Sigma(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}} \quad (1)$$

where τ_{ij} represents the pheromone concentration on the link between nodes $i$and j, and the heuristic value reflecting node quality is denoted by η_{ij}. The parameters $\alpha$and βcontrol the influence of pheromone trails and heuristic information, respectively. This mechanism enables a balance between exploration of new paths and exploitation of previously successful routes.

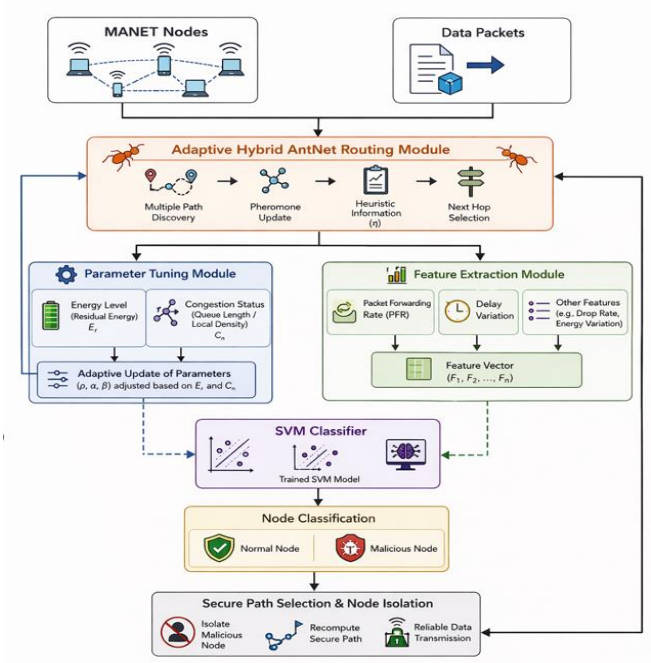

Fig. 1. Adaptive H-MantnetOpSVM Architecture

The heuristic value is defined based on node energy and distance as represented by eq (2), where node j's residual energy is E_j, and the distance between the nodes i and j is represented as D_{ij}. Higher energy and shorter distances between the nodes are the priorities of this formulation so that energy efficiency is improved and the transmission delay is reduced. To support adaptability, the pheromone update mechanism is modified as in eq (3). The pheromone evaporation factor is ρ, E_i is the residual energy of the node, and Q_i denotes the queue length representing congestion. γ and δ are the weighting parameters that regulate the influence of energy and congestion. τ_{ij}^{t+1} represents the updated pheromone value on the link between nodes i and j at iteration t+1. Thus, the routing performance is improved by the adaptive update strategy, which prioritizes energy-rich and less congested nodes, thereby enhancing network lifetime and scalability [XIV].

$$\eta_{ij} = \frac{E_j}{D_{ij}} \tag{2}$$

$$\tau_{ij}^{t+1} = (1-\rho)\tau_{ij}^{t} + \gamma E_i + \delta Q_i \tag{3}$$

The adaptive pheromone update incorporates residual energy and congestion conditions into route selection. The weighting parameters γ and δ regulate their contributions and control pheromone evaporation. Thus, the routing process adapts to changing network conditions and favors suitable routes. Additionally, simulation-based evaluation under changing network conditions demonstrates its effectiveness, while further theoretical analysis can provide insight into its stability.

Intrusion Detection Using Optimized Support Vector Machine

An optimized Support Vector Machine (SVM) based intrusion detection mechanism is integrated into the routing framework to identify normal and malicious nodes. Node behavior is assessed using the packet forwarding ratio, packet drop rate, route reply frequency, residual energy, and delay variation extracted from the network traffic, which help identify anomalies such as packet dropping or false route advertisement [XIX]. The SVM classifier constructs a decision boundary to separate normal and malicious nodes using the classification function as defined in eq (4). Here, x is the feature vector, $x_{i,}$is the support vector, y_i is the class label, α_i is the Lagrange multiplier, K is the kernel function, and b is the bias term. The kernel function is defined in eq (5).

$$\mathrm{f(x)} = \mathrm{sign}\Big(\sum_{i=1}^{n} \alpha_i y_i \, K(x_{i,} x) + \mathrm{b} \Big) \tag{4}$$

$$K\big(x_{i,} x\big) = \exp(-\gamma \|x_i - \, x\|^2) \tag{5}$$

Hyperparameter optimization is applied to the SVM classifier to improve classification performance. The penalty factor and kernel parameters are tuned to maximize detection accuracy while minimizing false positive rates. Optimized SVM models have been shown to significantly enhance detection capability in MANET environments [VI][XIV][XV].

Secure Route Construction

As soon as the classification process is completed, the nodes classified as malicious are excluded from the routing. The routing table is dynamically updated by the routing algorithm by removing these nodes, and alternative secure paths are recomputed using the adaptive Antnet mechanism. Backward ants (BANTs) reinforce the selected secure path by updating pheromone values along the route. This ensures that future route discoveries favor reliable and secure paths. The proposed approach effectively mitigates the impact of malicious nodes and enhances packet delivery performance by combining intrusion detection with routing.

Scalability Evaluation

The scalability of the proposed model is evaluated under varying network sizes from 50 to 200 nodes. Major challenges of mobile ad hoc networks such as routing overhead, congestion, and energy depletion become more significant when the size of the network increases. The adaptive parameter tuning mechanism enables the routing protocol to adjust dynamically to these changes, maintaining stable performance across different network densities. The performance of the proposed model is evaluated using standard metrics, including packet delivery ratio, throughput, end-to-end delay, network lifetime, detection accuracy, precision, recall, and false positive rate.

IV. Results and Discussion

Simulation Environment

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Simulation Area	800 × 800 to 1500 × 1500 m
Number of Nodes	50, 100, 150, 200
Mobility Model	Random Waypoint
Transmission Range	250 m
Traffic Type	CBR (UDP)
Packet Size	512 bytes
Simulation Time	100 s
Routing Protocols	AODV, Antet, H-MAntnetSVM, H-MantnetOpSVM, AH-MantnetOpSVM
Attack Type	Blackhole
Initial Energy	100 Joules

NS-2.35 is used to evaluate the performance of the proposed AH-MantnetOpSVM routing protocol under varying network conditions using the parameters in Table 1. Mobile nodes with densities ranging from 50 to 200 are deployed over the simulation area of 800 m × 800 m to 1500 m × 1500 m, with the Random Waypoint mobility model, and communication is established using Constant Bit Rate (CBR) traffic over UDP. Each node is initialized with a fixed energy, with a 100s simulation time and a 250 m transmission range establishing communication links between nodes. The performance of the proposed model is compared with AODV, Antnet, H-MAntnetSVM, and H-MantnetOpSVM under blackhole attacks.

The routing metrics, including packet delivery ratio, end-to-end delay, and throughput, are obtained from NS2 trace files. Features extracted from the simulation logs are provided to the SVM classifier to identify malicious nodes. Detected nodes are removed from the routing path, and the updated network conditions are used for data transmission, enabling a comprehensive evaluation of both routing efficiency and security performance.

Packet Delivery Ratio

Table 2 presents the packet delivery ratio (PDR) results, indicating that AH-MantnetOpSVM outperforms the existing protocols across all network sizes, as depicted in Fig.2. As the number of nodes increases from 50 to 200, the PDR of all protocols gradually decreases, mainly due to increased congestion and routing overhead.

Even under these conditions, the proposed model maintains a higher PDR, with about 97% at 50 nodes and 91% at 200 nodes. Its adaptive parameter tuning mechanism selects nodes with higher residual energy and lower congestion, while the optimized SVM-based intrusion detection isolates malicious nodes, thereby reducing packet drops caused by blackhole attacks and maintaining more reliable data transmission even as the network size increases.

Table 2: Packet Delivery Ratio Performance Comparison

Nodes	AODV	Antnet	H-MAntnetSVM	H-MantnetOpSVM	AH-MantnetOpSVM
50	88	90	92	94	97
100	85	88	90	92	95
150	82	85	88	90	93
200	78	82	85	88	91

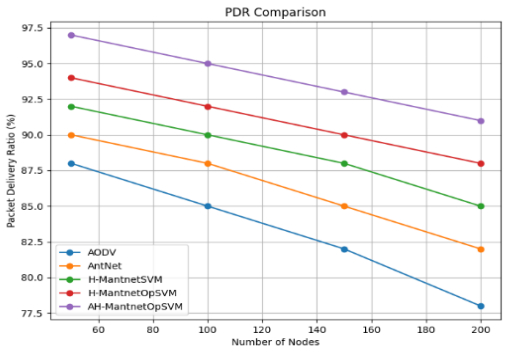

Fig. 2. Number of Nodes Vs Packet Delivery Ratio (PDR)

End-to-End Delay

The end-to-end delay results in Fig. 3, based on the values shown in Table 3, show that the AH-MantnetOpSVM achieves lower delay across all network sizes compared to AODV, Antnet, H-MAntnetSVM, and H-MantnetOpSVM. As the node density increases, delay rises for all protocols due to increased routing complexity and congestion. AODV records the highest delay due to frequent routing operations and the lack of optimization, whereas Antnet shows a moderate improvement because of probabilistic routing. The proposed algorithm maintains the lowest delay of 10 ms at 50 nodes and 18 ms at 200 nodes, thereby demonstrating reduced delay by integrating adaptive routing and intrusion detection.

Table 3: End-to-End Delay Performance Comparison

Nodes	AODV	Antnet	H-MAntnetSVM	H-MantnetOpSVM	AH-MantnetOpSVM
50	18	15	14	12	10
100	22	18	16	14	12
150	28	22	20	18	15
200	35	28	25	22	18

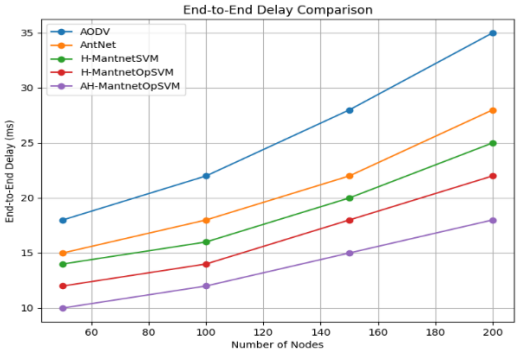

Fig. 3. Number of Nodes Vs End to End Delay

With adaptive pheromone-based route selection, which favors less congested and energy-efficient paths, the proposed methodology maintains lower delay in the network as node density increases. Additionally, the intrusion detection mechanism further reduces packet loss and retransmissions by isolating malicious nodes, and thereby ensuring faster and more reliable data delivery.

Throughput

The proposed protocol AH-MantnetOpSVM achieves a higher data transfer rate of 230 kbps at 50 nodes and maintains 185 kbps at 200 nodes compared to AODV, Antnet, H-MantnetSVM, and H-MantnetOpSVM across varying network sizes for a count of 1000 data packets for all protocols, as shown in Fig.4 and Table 4. As the number of nodes increases, throughput decreases for all protocols due to increased congestion and routing overhead, whereas the adaptive routing mechanism outperforms the existing methods that select the energy efficient paths on the network conditions. Also, isolation of malicious nodes by the SVM classifier ensures reliable packet forwarding and stable throughput even in dense MANET environments.

Table 4: Throughput Performance Comparison

Nodes	AODV	Antnet	H-MAntnetSVM	H-MantnetOpSVM	AH-MantnetOpSVM
50	180	190	200	210	230
100	160	175	185	195	215
150	140	160	170	180	200
200	120	145	155	165	185

Security Performance

AODV and Antnet protocols focus primarily on the routing operation and lack node classification capabilities. Accuracy, precision, recall, and F1-score are used to evaluate the routing protocols integrated with an intrusion detection mechanism. The security performance of H-MAntnetSVM, H-MantnetOpSVM, and AH-MantnetOpSVM is presented in Table 5. Fig.5 shows that H-MAntnetSVM and H-MantnetOpSVM exhibit lower results than AH-MantnetOpSVM across all evaluation metrics.

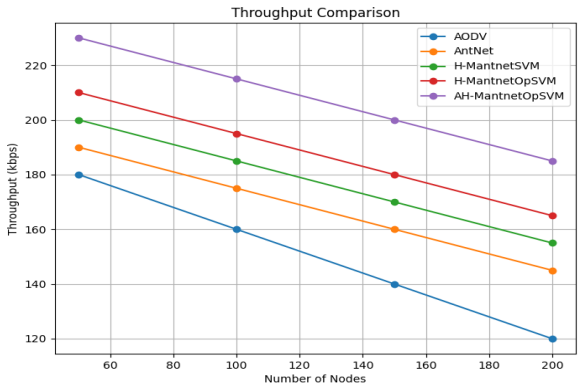

Fig. 4. Number of Nodes Vs Throughput

H-MAntnetSVM achieves an accuracy of 92%, with 91% precision and 90% recall, with fixed parameters and without optimization. H-MantnetOpSVM shows an increase of 94% in accuracy along with the corresponding increase in precision and recall, indicating better classification of normal nodes and malicious nodes through SVM optimization. The proposed framework further enhances the detection performance with 97% accuracy, 96% precision, 95% recall, and 95% F1-score through adaptive parameter tuning and SVM optimization, indicating an increased true positive rate and reduced false positive rate.

Table 5: Security Performance Comparison

Method	Accuracy	Precision	Recall	F1 Score
H-MAntnetSVM	92%	91%	90%	90%
H-MantnetOpSVM	94%	93%	92%	92%
AH-MantnetOpSVM	97%	96%	95%	95%

False Positive Rate (FPR)

The false positive rate analysis indicates that the proposed AH-MantnetOpSVM significantly reduces incorrect classification of normal nodes as malicious, as shown in Fig. 6. Table 6 shows a very low false positive rate of 3% for the proposed technique compared with 8% and 6% for other models. The network reliability is enhanced because of the optimization in parameters and the feature selection process.

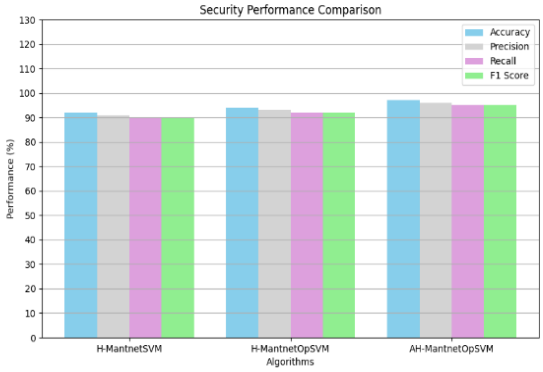

Fig. 5. Security Performance Comparison

Table 6: False Positive Rate Comparison

Method	FPR (%)
H-MantnetSVM	8
H-MantnetOpSVM	6
AH-MantnetOpSVM	3

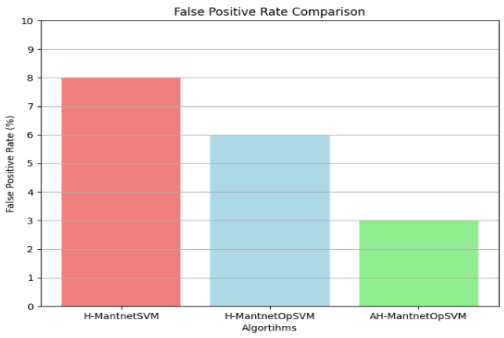

Fig. 6. False Positive Comparison

Network Lifetime (seconds or rounds)

A balance in the energy distribution among the nodes is achieved in AH-MantnetOpSVM due to the adaptive tuning of routing parameters that reduces the unnecessary routing activities in particular routes. Network lifetime represents the operational duration of the network measured in simulation time units based on the energy consumption patterns observed during the simulation process, as presented in Fig. 7 and Table 7., shows a maximum lifetime of 920 units measured in the proposed model, which outperforms both AODV and Antnet, that exhibits lower lifetimes, respectively, as well as H-MantnetOpSVM and H-MAntnetSVM. In addition, the early detection of malicious nodes also helps the protocol to avoid unnecessary energy depletion caused by retransmissions and failures in routes, thereby improving

overall network sustainability. This metric is evaluated for all routing protocols, as it is independent of intrusion detection and reflects overall energy efficiency.

Table 7: Network Lifetime Comparison

Method	Network Lifetime
AODV	620
Antnet	700
H-MAntnetSVM	780
H-MantnetOpSVM	850
AH-MantnetOpSVM	920

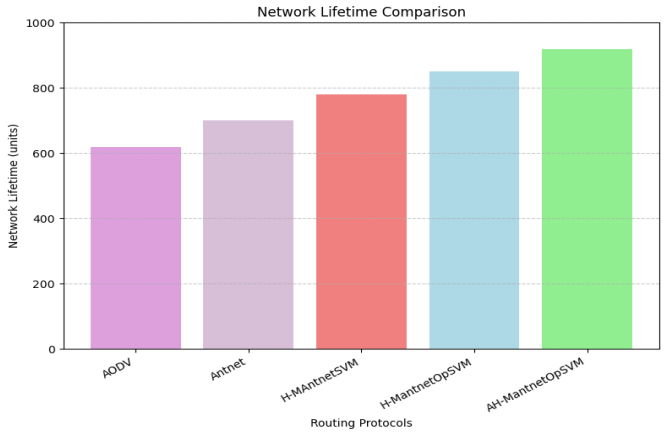

Fig. 7. Network Lifetime Comparison

V. Discussion

The proposed model shows clear improvements over existing protocols in the detection of blackhole attacks under the selected mobility model and simulation parameters. However, its performance under other routing attacks may vary. Therefore, evaluation under diverse attack scenarios and MANET conditions is considered for further investigation. In addition, formal analysis of routing-probability convergence and pheromone equilibrium can provide further insight into the stability of the adaptive pheromone mechanism. The adaptive Antnet component responds to network changes through effective pheromone updates to manage frequent link breaks, node movements, and variations in node energy, thereby improving the resilience and fault tolerance of the network. The efficiency of the proposed protocol is validated using performance metrics such as packet delivery ratio, delay, throughput, false positive rate, and network lifetime. Based on these improvements in routing and security, the proposed approach provides a reliable and scalable solution for MANET applications such as disaster recovery, military communication systems, and vehicular ad hoc networks.

VI. Conclusion

Mobile ad hoc networks face major challenges like energy efficiency and vulnerability to various security threats due to their changing network topology and

node mobility, despite their various applications. An adaptive and scalable routing framework based on AH-MantnetOpSVM has been developed to address the challenges of energy efficiency and security. Antnet routing mechanism enables dynamic adjustment of routing decisions with the integration of adaptive parameter tuning based on the network conditions, leading to improved route stability and efficient energy utilization. In addition, the incorporation of an optimized SVM-based intrusion detection system improves the classification of normal and malicious nodes effectively to mitigate the impact of blackhole attacks.

The proposed approach demonstrates superior performance compared to the traditional protocols and existing hybrid protocols in terms of packet delivery ratio, delay, throughput, false positive rate, and network lifetime, achieving up to 97% packet delivery ratio with improved reliability. Additionally, the model also maintains stable performance with the increase of network size up to 200 nodes. Future work can be focused on extending the proposed framework to handle multiple types of routing attacks and validating its performance in real-time environments. On the other hand, deep learning techniques can also be used to enhance intrusion detection accuracy and adaptability in highly dynamic MANET scenarios.

Conflict of Interest:

There was no relevant conflict of interest regarding this paper.

References

I. Abbood, Z. A., D. C. Atilla, and C. Aydin. “Intrusion Detection System through Deep Learning in Routing MANET Networks.” Intelligent Automation & Soft Computing. 2023;37(1). 10.32604/iasc.2023.035276.

II. Abdallah, A. A., M. S. Abdallah, H. Aslan, M. A. A. Abdallah, Y. I. Cho, and M. S.Abdallah. “Enhancing Mobile Ad Hoc Network Security: An Anomaly Detection Approach Using Support Vector Machine for Black-Hole Attack Detection.” International Journal of Safety & Security Engineering. 2024;14(4). 10.18280/ijsse.140401.

III. Abdan, M., and S. A. H. Seno. “Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET).” Wireless Communications and Mobile Computing. 2022;2022(1):2375702. 10.1155/2022/2375702.

IV. Abdullah, A. M., E. Ozen, and H. Bayramoglu. “Energy Efficient MANET Routing Protocol Based on Ant Colony Optimization.” Adhoc & Sensor Wireless Networks. 2020;47.

V. Adanigboa, O. O., S. Aina, A. I. Oluwaranti, and S. O. Oseni. "Advances in Energy Efficiency and Routing Optimization in Mobile Ad Hoc Networks: A Comprehensive Literature Review." Journal of Engineering, Technology, and Innovation. 2025;4(1):1–7.

VI. Almuhanna, R., and S. Dardouri. "A Deep Learning/Machine Learning Approach for Anomaly-Based Network Intrusion Detection." Frontiers in Artificial Intelligence. 2025;8:1625891. 10.3389/frai.2025.1625891.

VII. Anantapur, M., and V. C. Patil. "Ant Colony Optimization Based Modified AODV for Secure Routing in Mobile Ad Hoc Networks." International Journal of Intelligent Engineering and Systems. 2021;14(6):115–124. 10.22266/ijies2021.1231.11.

VIII. Arthi, A., A. Beno, S. Sharma, and B. Sangeetha. "Fuzzy Based Inference System with Ensemble Classification Based Intrusion Detection System in MANET." Journal of Intelligent & Fuzzy Systems. 2023;45(3):3567–3574. 10.3233/JIFS-230161.

IX. da Costa Bento, C. R., and E. C. G. Wille. "Bio-Inspired Routing Algorithm for MANETs Based on Fungi Networks." Ad Hoc Networks. 2020;107:102248. 10.1016/j.adhoc.2020.102248.

X. Dash, Y. "Nature Inspired Routing in Mobile Ad Hoc Network." 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). 2021:1299–1303. 10.1109/ICAC3N53548.2021.9725487.

XI. Gopalasamy, K., and K. G. Muthaiya. "Optimizing Packet Routing and Security in MANETs with the H-MAntnetSVM Algorithm for Energy Efficiency and Blackhole Detection." Sustainable Computing: Informatics and Systems. 2025;46:101123. 10.1016/j.suscom.2025.101123.

XII. Hande, J. Y., and R. Sadiwala. "Optimization of Energy Consumption and Routing in MANET Using Artificial Neural Network." Journal of Integrated Science and Technology. 2024;12(1):718–718. 10.62110/sc5m8x71.

XIII. Hemalatha, S., K. T. Reddy, T. Ramaswamy, and R. V. V. Krishna. "Enhancing MANET Security Using AI-Driven Intrusion Detection Systems." Journal of Communications. 2025;20(4):257–264. 10.12720/jcm.20.4.257-264.

XIV. G. Kalaiselvi and M. G. Kavitha. “Energy and Security Aware Routing in MANETs: A Hybrid Antnet with Optimized SVM Based Blackhole Attack Detection (H-MantnetOpSVM).” 2025 1st International Conference on Radio Frequency Communication and Networks (RFCoN). 2025:1–6. 10.1109/RFCoN65425.2025.11002026.

XV. Khan, D. M., T. Aslam, N. Akhtar, S. Qadri, I. M. Rabbani, and M. Aslam. “Black Hole Attack Prevention in Mobile Ad-Hoc Network (MANET) Using Ant Colony Optimization Technique.” Information Technology and Control. 2020;49(3):308–319. 10.5755/j01.itc.49.3.25288.

XVI. Khanpara, P., and S. Valiveti. “An Efficient Bio-Inspired Routing Scheme for Tactical Ad Hoc Networks.” Scalable Computing: Practice and Experience. 2023;24(1):45–54. 10.12694/scpe.v24i1.2186.

XVII. Li, W., L. Xia, Y. Huang, and S. Mahmoodi. “An Ant Colony Optimization Algorithm with Adaptive Greedy Strategy to Optimize Path Problems.” Journal of Ambient Intelligence and Humanized Computing. 2022;13(3):1557–1571. 10.1007/s12652-020-02531-1.

XVIII. Malyadri, N., R. M., R. Nandalike, P. Chavan, S. S., D. P., and R. S. “A Predictive Energy-Efficient Adaptive Routing Methodology for Mobile Ad Hoc Networks.” IET Networks. 2025;14(1):e70001. 10.1049/ntw2.70001.

XIX. Nirmala Bai, K. S., and D. M. Subramanyam. “Integrated Intrusion Detection Design with Discretion of Leading Agent Using Machine Learning for Efficient MANET System.” Scientific Reports. 2025;15(1):30849. 10.1038/s41598-025-14923-7.

XX. Prasad, M., S. Tripathi, and K. Dahal. “An Intelligent Intrusion Detection and Performance Reliability Evaluation Mechanism in Mobile Ad-Hoc Networks.” Engineering Applications of Artificial Intelligence. 2023;119:105760. 10.1016/j.engappai.2022.105760.

XXI. Prasanna, K. S., and B. Ramesh. “A Review: An Efficient and Reliable Secure Routing Mechanism with the Prevention of Attacks in Mobile Ad-Hoc Network (MANET).” Wireless Personal Communications. 2023;133(4):2541–2580. 10.1007/s11277-023-10556-0.

XXII. Rahman, M. T., M. Alauddin, U. K. Dey, and S. Sadi. “Adaptive, Secure and Efficient Routing Protocol to Enhance the Performance of Mobile Ad Hoc Network (MANET).” Applied Computer Science. 2023;19(3). 10.23743/acs-2023-21.

XXIII. Sardar, T. H., S. A. Dar, J. Jaiswal, G. Prasad, M. Mittal, and V. Kumar. "Enhancing Security in MANETs with Deep Learning-Based Intrusion Detection." Procedia Computer Science. 2025;259:120–129. 10.1016/j.procs.2025.01.316.

XXIV. Venketesh, R., and K. Sasikala. "The Design of an Intrusion Detection System in MANET Using the IGWO-ANN Classification Algorithm." International Journal of Networking and Virtual Organisations. 2024;31(1):22–42. 10.1504/IJNVO.2024.136007.

XXV. Wu, L., X. Huang, J. Cui, C. Liu, and W. Xiao. "Modified Adaptive Ant Colony Optimization Algorithm and Its Application for Solving Path Planning of Mobile Robot." Expert Systems with Applications. 2023;215:119410 . 10.1016/j.eswa.2022.119410.

XXVI. Yilmaz, K., R. Kara, and F. Katircioglu. "Energy-Efficient Hybrid Adaptive Clustering for Dynamic MANETs." IEEE Access. 2025. 10.1109/ACCESS.2025.3551234.