International Journal of Safety and Security Engineering
Vol. 16, No. 1, January, 2026, pp. 1-15
Journal homepage: http://iieta.org/journals/ijsse

Trust-Aware Five-Class Multinomial Logistic Regression for Packet-Dropping Mitigation in Mobile Ad Hoc Networks

Arshad Ahmad Khan Mohammad[1], Kumar Babu Batta[1], Mohammed Abdul Bari[2], Masood Ahmad Mahammad[3], Mohammad Khaja Nizamuddin[1*], Arif Mohammad Abdul[1], Prathyusha Annapragada[1]

[1] Department of Computer Science and Systems Engineering, School of Computer Science and Engineering, GITAM Deemed to be University, Hyderabad 502329, India
[2] Department of Computer Science and Engineering, ISL Engineering College & Technology, Hyderabad 500005, India
[3] Department of Electrical, Electronics and Communication Engineering, School of Core Engineering, GITAM Deemed to be University, Hyderabad 502329, India

Corresponding Author Email: kmohamme@gitam.edu

https://doi.org/10.18280/ijsse.160101

Received: 2 August 2025
Revised: 23 October 2025
Accepted: 24 November 2025
Available online: 31 January 2026

Keywords:
Mobile Ad Hoc Networks, multinomial logistic regression, dynamic trust scoring, trust-based routing, packet drop attack, trust, machine learning, packet drops mitigation

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are highly vulnerable to packet-dropping attacks because of their dynamic, infrastructure-less topology. Existing binary classification and trust-based approaches often fail to distinguish malicious behaviours, such as black hole and gray hole attacks, from non-malicious packet losses caused by buffer overflow and energy depletion, thereby leading to false positives and inefficient routing decisions. This study proposes a trust-aware framework that combines multinomial logistic regression (MLR) for five-class node behaviour classification with a dynamic reputation-based trust model. Features extracted from NS-2 simulations are used to classify node behaviours, and the classification results are incorporated into real-time trust updates for secure Ad hoc On-Demand Distance Vector (AODV) routing. Experimental results show that the proposed method achieves a classification accuracy of 95.7%, with precision and recall ranging from 0.93 to 0.98 across all classes and an area under the curve (AUC) greater than 0.90. In routing evaluation, the framework attains a 95% packet delivery fraction (PDF), representing an 80% improvement over the baseline reactive protocol under misbehaviour and a 31% gain over multifactor mitigation, while maintaining low delay (0.20 s) and low energy consumption (93.27 J). These findings indicate that the proposed approach can reduce false positives, improve packet delivery, and enhance routing reliability in resource-constrained MANET environments.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a collection of mobile devices that autonomously establish a communication network without centralized control or pre-existing infrastructure [1]. Without relying on fixed infrastructure, it enables decentralized, self-organizing wireless communication among mobile nodes, such as smartphones, sensors, or vehicles [2]. This dynamism makes MANETs ideal for dynamic environments such as disaster recovery, military actions, and also Vehicular Ad Hoc Networks (VANETs), and Internet of Things (IoT)-based smart city applications [3]. MANETs take advantage of node mobility and peer-to-peer routing to produce ad-hoc, short-lived self-forming topologies for quick operations in deprived infrastructure and low resource situations, unlike traditional wired or infrastructure-based wireless networks that use a well-planned topology [4]. But their open wireless environment, dynamic topology, and the absence of centralized authority, controlled transmission power, and restricted computation all make them highly vulnerable to malicious attacks [5]. One such malicious attack at the network layer is packet dropping attacks, such as black hole [6] and gray hole [7] attacks, which break the communication by deliberately discarding packets.

Moreover, packets are also dropped accidentally due to resource limitations and network characteristics such as buffer overflow and/or energy depletion [8]. These dropped packets will further diminish the network performance. This degeneration complicates the separation between malicious and unintentional packet dropping actions in the network [9]. Drop packets in MANET have a significant detrimental impact on vital performance parameters. It decreases the packet delivery ratio (PDRatio) and limits the network's capability to deliver data. The overall data transfer rate is further lowered due to the reduced throughput. Furthermore, dropping packets will add latency to communication. These kinds of problems undermine the dependability of mission-critical applications [10].

These types (black hole and gray hole) of attacks exploit the properties of the MANET routing protocol's vulnerabilities [11]. The routing protocols, such as reactive, proactive, hybrid, and resource-aware, assume that other nodes cooperate for

forwarding packets, but the packet dropping nodes exploit it. With a black hole attack, all the packets are dropped by nodes in a malicious manner to prevent network conversation from taking place [12]. Gray hole attack is the selective packet dropping in which detection is difficult to service [13].

At the same time, some non-malicious nodes in the network inadvertently drop packets due to reasons such as buffering and energy exhaustion [14]. These drops can be interpreted as malicious packet-dropping activity, such as a black or gray hole. Thus, existing packet-dropping detection systems are prone to producing false positives, as they misidentify non-malicious packet drops as malicious packet drops. Ultimately, the performance of the network degrades.

The available packet drops mitigation mechanisms in MANETs, such as credit-based [15], reputation-based [16], and acknowledgment-based, suffer several problems. Adoption of credit-based platforms requires the use of hard-to-deploy tamper-resistant hardware measures. Reputation-based approaches often can't differentiate malicious and non-malicious packet drops accurately, which leads to frequent false positives. At the same time, the protocols that use acknowledgment, like CACK [17], add excessive messages to confirm packet delivery. This increases overhead and still can't accurately detect the packets that drop due to system faults (unintentional drops) like energy or buffer issues [18]. Machine learning (ML) based intrusion detection systems (IDS), such as those using support vector machines (SVM) and random forests (RF), cannot classify different types of packet drops accurately, especially if the dataset is dominated by diverse drop patterns [19]. Although cryptographic frameworks enhance network security, they require high computational power, which is impractical for resource-constrained MANETs [20]. Collectively, these drawbacks of these existing solutions indicate the need for enhanced security strategies for MANETs.

To overcome the issues of existing systems, this study comes with a trust-based lightweight ML system to detect and prevent the malicious and non-malicious packet drops in MANETs. The proposed framework uses multinomial logistic regression (MLR) [21] to categorize the node behaviour into different packet dropping categories like black hole, gray hole, buffer overflow, and energy depletion. This classification helps to identify exact packet dropping behaviours of nodes, i.e., either malicious or non-malicious. The framework studies from NS-2 [22] trace files and extract network characteristics, packet-related information, and network performance, like packet delivery, queue utilization, and residual energy. Extracted information contributed to computing the trust value, and it is dynamic. Further, this trust value is used for route computation; this leads to increasing reliability by avoiding malicious nodes. Therefore, the proposed framework extends the network performance by packet delivery improvement, decreasing false positives, and increasing efficiency in decentralized MANETs.

The contributions in the study include 1. A five-class multiple linear regression classifier for the detection of dropped packets 2. Dynamic trust-based scoring 3. Integrating classification and trust into the Ad hoc On-Demand Distance Vector (AODV) protocol for secure routing.

The paper is organized as follows: Section 2 provides background, Section 3 reviews related work, Section 4 defines the problem, Section 5 details the proposed framework, Section 6 presents performance evaluation and discusses findings, and Section 7 concludes with future directions.

2. BACKGROUND KNOWLEDGE

MANETs are a type of self-organizing network where they communicate without a central network (decentralized networks) with autonomous mobile nodes like sensors, vehicles, or smartphones, in which each node acts like a sender/receiver and host. MANETs allow nodes in their network to enter or leave at any time, which leads to changing network structures frequently. This type of dynamic behaviour makes security and routing more challenging. MANETs make reactive, proactive, or hybrid-based routing decisions to minimize overhead in routing, but still, networks remain suspicious of malicious packet-dropping nodes.

Packet dropping in MANETs reduces PDRatio, throughput, and increases latency with malicious attacks like black hole or gray hole dropping packets intentionally. The unintentional drops in the network occur mostly due to network issues, system faults, or lack of resources as commonly the packets are dropped due to collisions, energy depletion, or buffer overflow. So, differentiating between these malicious and non-malicious nodes is very important to avoid false positives; otherwise, these false positives will disrupt network connectivity and further performance.

By monitoring nodes' packet operation behaviour, a trust-based framework assigns a trust score to each node [23]. The nodes with higher scores are preferred for routing, but static trust scores struggle to adapt to network changes or correctly differentiate malicious and non-malicious nodes. MLR helps characterize node behaviours by modelling nonlinear correlations between parameters, including packet delivery, queue utilization, and residual energy. To work in resource-limited MANETs and enable applications in tactical, vehicular, and IoT networks, ML models need to be lightweight so they can be scaled up and run in real time.

3. RELATED WORK

The security of MANETs against packet-dropping attacks has been researched extensively, with trust-based detection mechanisms, ML-based IDS, secure routing protocols, and hybrid frameworks.

3.1 Trust-based detection mechanisms

A trust-based mechanism tracks node behaviour rapidly and estimates the nodes' reliability against packet-dropping attacks. Existing works, such as CONFIDANT [24] and CORE [25], leverage positive and negative reputation scores computed on direct and indirect observables to mitigate forwarding nodes for malicious activities. Alerts are used in CONFIDANT to disseminate the reports of misbehaviour, whereas in CORE services, they are not provided to uncooperative nodes. However, the static scoring strategies cannot differentiate between unintentional and malicious drops and may cause false positives on dynamic MANETs. More advanced trust models use multi-metric evaluations considering packet forwarding rate, end-to-end delay, and residual energy [18]. A reputation-based scheme to defend against packet dropping attacks, but it cannot adapt quickly to changing topologies and is not temporally adaptive. Credit-based approach Termi-nodes project [26] encourages cooperation with a virtual currency, yet they necessitate tamper-resistant hardware, which adds to the complexity of the

deployment. These methodologies underline the demand for dynamic, lightweight trust systems that would be resilient to the resource limitations and diverse behaviours of MANETs.

3.2 Machine learning approaches

Various ML methods have been widely used to detect black and gray hole attacks in MANETs using behaviour pattern analysis. The training algorithms, such as SVM, RF, and k-nearest neighbours (k-NN), use properties of nodes like packet delivery fraction (PDF), routing overhead, and node characteristics to label the nodes as non-malicious or malicious. To illustrate, in the survey by Hassan et al. [19], ensemble classifiers have been shown to perform with great accuracy when tested with NS-2 simulation data to detect malicious nodes. More recently, deeper learning techniques such as networks have been used to effectively process data sequences, capture temporal correlations between the behaviour of nodes, and expose complex attacks. Federated learning (FL) is an advanced version of these techniques, which allows decentralized training of the model, keeping data privacy and enhancing the detection accuracy in the distributed MANET scenarios.

However, MANET constrains resources, making ML-based IDS less effective in MANET. Models used for fishing out attackers, like RF and SVM, do not have enough granularity to distinguish intentional packet dropping from adversaries versus unintentional due to resource limitations, thus they incur high false positive rates (FPR) [19]. The problem is further confounded and made worse by the unbalanced nature of the dataset, where the benign traffic overwhelms the findings of malicious activities, resulting in biases toward the majority class and undermining detection accuracy. Additionally, models such as Long Short-Term Memory(LSTM) are computationally expensive and require large amounts of training data, making them less suited for energy-constrained MANET nodes and real-time applications. Thus, scalable and adaptive ML models are essential to handle dynamic topologies and evolving security threats in MANETs.

3.3 Secure routing protocols

Secure routing schemes are proposed to embed the security mechanisms into the routing operations to defend against packet-dropping attacks. Security extensions of AODV [27, 28] used cryptographic authentication or trust-based path selection. A digital signature is embedded into AODV to authenticate route discovery by the source. Further, enhanced AODV to choose reliable paths according to the trust scores, assuming trusted certificate authorities (CAs), but it is not applicable in decentralized MANETs. It highlights the importance of incorporating security mechanisms into the routing protocols, as cited by Desai and Jhaveri [29], to ensure data confidentiality, integrity, and availability in MANET.

However, these methods face problems with non-centralized and resource-limited MANETs. Although cryptographic methods are promising, they are inefficient regarding low battery life and bandwidth, and cause network partitioning and low data throughput. Furthermore, trust-based protocols such as Trust-AODV and conditions need to have trusted CAs, which do not apply to completely decentralized environments. Also, these schemes have difficulty distinguishing packets lost by malicious attack and packet drops occurring naturally due to resource limitations, and thus, selective drops in gray hole attacks cannot be detected. Solutions to these challenges will require innovative approaches in network design, security, power management, and resource management that will increase the efficiency of such small-scale MANETs.

3.4 Hybrid and emerging approaches

Hybrid approaches for securing communication in infrastructure-less networks integrate trust evaluation, ML, and routing mechanisms. Work by Shafi et al. [30], a trust model that combines ML and trust-based methods, aims to mitigate black hole and Flooding attacks in MANETs, as reviewed by Hemalatha et al. [31], who concluded that the method relies on excessive parameters for route determination. However, its binary decision cannot distinctly discriminate between the malicious and dignified packet-dropping nodes. Another hybrid scheme [32] employs clustering and trust-based routing but still faces a high computational cost, which limits scalability. Clustering algorithms combined with trust-based routing introduce significant overhead due to maintaining cluster structures, evaluating trust metrics, and exchanging information between nodes.

Utilizing multi-objective particle swarm optimization (PSO) combined with adaptive acknowledgement and predictive trust evaluations offers a comprehensive solution for the security issues in MANETs. It makes theoretical research and practical countermeasures introduced against MANET security problems, such as black hole and gray hole attacks, feasible in real-world deployments [19]. Work by Kavitha et al. [32] implements Intruder Detection and Isolation based on PSO for feature optimization and Neural Networks for classification; in which trust feature computation is developed in the trust framework, which would help the misleading intruder nodes performing malicious acts to be identified effectively. Another work by Thanuja and Umamakeswari [33] suggested a mixed method utilizing PSO and trust-based routing to improve path selection and find the malicious nodes operating as black hole and grey hole attacks to make the MANET routing protocols more reliable. Nevertheless, these methods are subject to a resource-constrained MANET.

Although PSO and Neural Network-based methods are tailored for better computational complexity, they still put a lot of pressure on the nodes with the constraints on battery life and bandwidth, which may cause network split and decreased data throughput. Furthermore, these approaches face difficulty in identifying malicious packet drops and unintentional losses caused by resource limitations, leading to false positives, especially in recognizing the selective packet-dropping behaviours of gray hole attacks. The datasets are mostly imbalanced, so these imbalances lead to biased detection boundaries, causing IDS classifiers to fail to capture low-frequency attack behaviours, resulting in affecting their reliability in MANETs.

Recent studies in MANET security have focused highly on the importance of adaptive, lightweight algorithms that do not compromise routing protocols to enhance the security of network parameters like Throughput, PDR, and Latency. A survey by Hassan et al. [19] explains that many existing solutions lack the multi-class differentiation, like types of packet drops, including gray and black hole attacks vs drops due to system faults. The survey noted that systems operate independently of the routing protocols, resulting in the absence

of real-time integration, which prevents systems from reacting immediately to routing changes. It pointed out binary classifiers, such as SVM and RF, for a lack of granularity, which often misclassify unintentional and intentional drops, classifying unintentional drops as attacks. The survey also explains that when ML detection operates independently, it cannot provide instant feedback to routing protocols. This type of independence introduces latency, but high complexity ML methods cannot be implemented in resource-less environments like MANETs.

These methodologies show that security solutions for MANET networks should be lightweight, multi-class detection. They should also integrate easily with routing protocols. The proposed framework uses the lightweight MLR for classifying the nodes into 5 categories: normal, black hole, gray hole, buffer overflow, and energy depletion, providing high accuracy in classification and low computational cost on ARM Cortex-M-based device platforms. Simulation parameters considered in this work are carefully constrained in terms of energy, memory, processing latency, and queue length so that the simulation emulates an ARM Cortex-M-based device platform.

3.5 Research gap

Existing solutions exhibit several limitations: 1) Most systems majorly focus only on malicious drops or trust management, but ignore drops due to system faults like energy depletion or buffer overflow. 2) Several binary classifiers used by several ML models are insufficient for classifying the reasons for packet drops. 3)Cryptographic protocols and neural networks are computationally expensive, making them unsuitable for resource-limited MANET networks. 4) Static values cannot adapt to changing network conditions. 5) ML detection runs separately from routing protocols, causing delays in reacting to malicious behaviour in the network. In this paper, MLR is extended with dynamic trust scores and secure adaptive routing to resolve these voids. The proposed solution achieves scalability, low overhead, and high detection accuracy for MANET security.

4. PROBLEM STATEMENT

MANETS have a decentralized architecture and security model with no central authority, so they are prone to packet dropping. Malicious attacks, such as black and gray hole misuse, impact reactive, proactive, and hybrid routing protocols, resulting in low PDRatio, throughput, and network reliability. Non-malicious packet drops caused by system faults complicate the detection, as these accidental drops look like malicious attacks. Such challenges are especially critical in tactical, vehicular, and IoT networks with no resources, where constant connectivity is essential.

Existing solutions for handling packet drops, including trust-based systems, ML-based intrusion detection, and secure routing protocols, have various limitations. Trust-based models, including CONFIDANT and CORE, struggle to separate malicious from non-malicious drops, which apparently leads to high false positives, causing unnecessary isolation and reducing the PDRatio. Binary ML classifiers like SVM and RF are restricted to detecting nodes as malicious or not, but they can't detect diverse packet drops leading to false positives. Secure routing protocols like SAODV and AODV-SEC are unsuitable for resource-constrained nodes, as they do not address unmalicious drops. Moreover, static trust-based values fail to adapt under rapidly changing network conditions and security systems with no integration to routing react too slowly to threats. MANETs require a scalable, lightweight framework that distinguishes malicious and non-malicious packet drops with integration of real-time routing decisions.

5. TRUST-INTEGRATED MACHINE LEARNING FRAMEWORK FOR PACKET DROP MITIGATION IN MOBILE AD HOC NETWORKS

This section describes a methodology that combines trust with ML to detect and reduce packet drop behaviour in MANETs. Further, the proposed methodology addresses both malicious and non-malicious drops, ensuring secure routing even in dynamic, resource-constrained network conditions. It combines three main components: a five-class MLR classifier, a dynamic, reputation-based trust model, and the AODV routing protocol. The system produces accurate detection results, adapts to real-time, and is efficient.

5.1 System architecture

The framework has four layers that are linked to each other, as shown in Figure 1. Each layer addresses an essential part of reducing packet drops in MANETs. These layers collect data, find features, classify behaviours, calculate trust, and guide routing decisions.

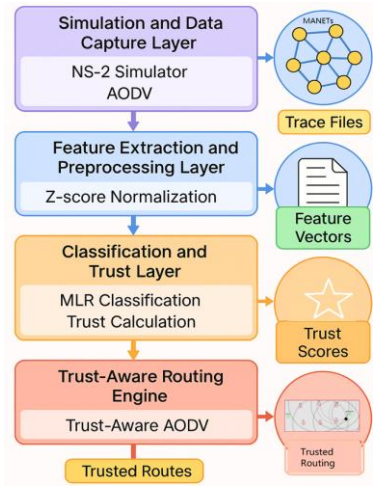

Figure 1. Architecture trust integrated machine learning (ML) framework

5.1.1 Simulation and data capture layer

This layer leverages the NS-2 simulator to model MANET scenarios. It uses input from a controlled environment to generate realistic packet transmission logs under black hole and gray hole attacks, as well as resource-limited conditions. The simulated network includes 30 to 100 nodes in a 1000 m × 1000 m area, following the Random Waypoint mobility model; nodes travel at velocities between 0 and 20 m/s. This model represents node mobility patterns and generates frequent topology changes, forcing distributed routing and security to adapt. The reactive routing protocol over User Datagram Protocol (UDP) is used for Constant Bit Rate (CBR) traffic because of its reactivity and low overhead. Nodes

between the source and destination overhear packets within their radio range and document them in trace files (.tr) for later analysis.

Table 1. Behavioural thresholds for node classification

Behavior	Threshold
Black hole	Drop Rate > 90% and PDRatio ≈ 0
Gray hole	Drop rate 30–60%
Buffer overflow	Queue utilization > 85%
Energy depletion	Residual energy < 25%
Normal	Otherwise

Note: packet delivery ratio (PDRatio).

The documented trace file contains detailed packet-level details like timestamps, node, rem_energy, and also event types like sent, received, or dropped. Python scripts analyse these trace files to derive features of nodes like queue occupancy, energy occupancy, PDR, and classify them into normal, black hole, gray hole, buffer overflow, and energy depletion using heuristic thresholds, as shown in Table 1. Each simulation runs for 100 seconds to ensure simulations are run for 100 seconds, and outcomes are averaged over several runs to ensure there is enough data for robust analysis to ensure accountability of node mobility and traffic patterns.

5.1.2 Feature extraction and pre-processing layer

This layer reads raw simulation and converts it to derive a set of features. These features help in identifying whether packet dropping is malicious or non-malicious. These are ten specific features that can describe how nodes perform; they include packet drop rate (PDR), packet delivery ratio (PDRatio), packet forwarding rate, queue utilization, residual energy, energy per packet, traffic intensity, hop count, routing overhead, and packet arrival/departure rates. These attributes capture not only the performance features (PDR and delay) but also the resource limitations (queue utilization and residual energy), leading to better behavioural analysis. Normalisation of the features to z-score to maintain equilibrium amongst the numerical and fair contribution from each feature (e.g., PDR percentage vs. joules for energy).

$$Z = \frac{x - \mu}{\sigma} \tag{1}$$

In Eq. (1), x is the value for a feature, μ is the mean, and σ isthe standard deviation across all nodes of that feature. All thesefeatures are standardized by the normalization standard scale. (zero-mean, unit variance), which guarantees MLR Classification stability. Simulation statistic thresholds are used for behaviour classification, which distinguishes between normal and malicious behaviour.

5.1.3 Classification and trust layer

Each node i in the network is assigned with reputation score by the model, i.e., reputation $scoreR_i(t) \in [0,1]$. This score indicates the node's reliability (less chance of failure) based on observed behaviour. Trust values are dynamically updated based on node behaviour and network dynamics. Two different trust score updating mechanisms are incorporated: one for active nodes and another for inactive nodes in the network. These two distinct approaches ensure reliable nodes get a higher trust value, balancing encouragement while mitigating inactivity or unreliability.

For active nodes, the dynamic trust model computes reputation scores using reinforcement based on their packet forwarding performance, which is computed using Eq. (2).

$$R_i(t+1) = R_i(t) + \alpha(S_i(t) - R_i(t)) \tag{2}$$

In Eq. (2), $R_i(t)$ is current reputation score and $S_i(t) \in [0,1]$ is the behaviour score derived from the MLR classifier's output, reflecting metrics like PDR and queue utilization, and $\alpha \in [0,1]$ is a learning rate (set to 0.1 in simulations). If a node successfully forwards packets ($S_i(t) > R_i(t)$), its trust score increases, incentivizing cooperation.

For inactive nodes, trust exponentially decays to avoid old reputation from affecting routing. Inactive nodes that are not actively forwarding packets require a mechanism to prevent stale trust scores, as prolonged inactivity indicates either constrained resources or potential malicious intent. For inactive nodes, the trust score is updated by Eq. (3).

$$R_i(t+1) = R_i(t)e^{-\lambda \Delta t} \tag{3}$$

In Eq. (3), where, $\lambda > 0$ controls the decay rate (set to 0.05 in simulations), and Δt measures elapsed time since the last activity. It is designed to reduce the trust score of nodes that are not forwarding packets (inactive nodes), capturing a potential reduction in reliability. Eqs. (2) and (3) combining work to update trust dynamically, rewarding active forwarding and decaying inactive nodes to match the rapidly shifting structure of MANETs.

Nodes are categorized based on trust thresholds: malicious ($R_i(t) < 0.3$), uncertain ($0.3 \leq R_i(t) < 0.5$), or benign ($R_i(t) \geq 0.5$). Such a trust mechanism, which changes over time and is tolerant to the ever-changing network topology as well as the nodes' behaviors of MANET. These empirically set thresholds balance sensitivity to misbehaviour against tolerance of transient resource shortfalls (the threshold values are chosen to minimize false positives).

5.1.4 Trust-aware routing engine

The trust scores are combined into the AODV routing protocol to compute secure and trustworthy routing. The cost of a path is minimized on the routing measure.

$$Cost(P) = \sum_{i \in P} \big(1 - R_i(t)\big) \tag{4}$$

In Eq. (4), subject to $R_i(t) \geq 0.5$, ensures only reputed nodes participate in routing, where nodes with a trust level lower than the threshold are not eligible to participate in forwarding data packets. It distinguishes between malicious or non-malicious packet drop nodes to improve the network reliability and packet delivery.

5.2 Design assumptions

The proposed work makes the following assumptions, which allow for practical deployment in MANETs:

1. Dynamicity of the Environment: MANETs are characterized by a high rate of topology changes because nodes are allowed to move in and out of shared range, which requires an adaptive security regime.
2. Variability in the Behaviour: Every node can misbehave, e.g., black hole, gray hole, or drop packets unintentionally caused by being out of energy and full buffer, at any time, so the detection should be reliable

alternatively.
3. Local Resource Monitoring: Each node maintains a local status of energy (in joules) and buffer usage. This results in low overhead feature extraction with no central control.
4. Implementation of IDS: The scenario placing the IDS node is implemented, which retrieves traffic distribution faithfully and according to IP-based protocols.
5. Sustainable Attacker: Attackers act sustainably during training, but the system must cope with dynamism at run-time, accounting for natural variability.

These assumptions also satisfy the nature of many MANETs, which are decentralized and lack energy resources; feasibility can be proved in different cases.

5.3 Design considerations

To handle these challenges of MANET, the framework has the following focus:

1. Efficient Computation: Algorithms leverage linear-time feature extraction and constant-time trust updates designed with low-power processors such as ARM Cortex-M in mind. Classification and trust calculations require less than 10 ms per node, making resource usage minimal.
2. Liveness: Trust scores and node classifications are updated continuously, enabling rapid routing decisions. This is very important for dynamic topologies in which node behaviour and network status change rapidly.
3. Flexibility: Exponential trust decay (Eq. (3)) adapts to new behaviour of nodes and does not base routing on stale trust evaluations, which would influence the routing decision.
4. Scalable: The modularity of the design means that it can go from 30 to over a hundred nodes, and this could be extended to hundreds or thousands of nodes for more challenging MANETs, as in IoT or tactical scenarios.

These reasons make the framework feasible in the resource-constrained and dynamic MANETs while maintaining high performance.

5.4 Key goals

The proposed work aims to achieve the following key objectives:

1. Behaviour Characterization: Identify malicious and unintentional behaviours accurately. This will avoid false positives while sustaining network reachability.
2. Dynamic Trust Assessment: Compute and dynamically update trust values for each node by considering current performance and historical trust values.
3. Secure Route Selection: Use trust scores to direct AODV so that paths must be selected via high-trust intermediary nodes.

These objectives address significant deficiencies in existing MANET security techniques that must be applied to transmit mission-critical information while at the same time achieving good performance.

5.5 Improvements over existing techniques

The framework provides significant advantages compared with existing approaches.

1. Multi-class Classification: Unlike standard AODV, resource-aware routing (RAR), and binary classification (malicious versus normal), this scheme makes use of MLR for live-class classification. It can detect more packet-dropping behaviours and minimize false positives by identifying unintentional loss from malicious behaviour.
2. Real-Time Trust: Real-time updating of trust scores differs from those derived by static models like CONFIDANT and CORE, allowing for more responsive trust assessments.
3. Closest Routing Integration: Unlike other stand-alone ML-based detection systems, in this architecture, classification is merged with AODV routing. This makes trust scores instantly enforceable with such approaches on the route selection, unlike secure key agreement (SKA)protocols that are overhead-heavy.
4. Low-cost Complexity: The lightweight nature of the system contrasts with heavy-duty cryptographic protocols and could be applied on IoT-grade devices.

These enhancements lead to better resilience and efficiency, and can easily be used for variable MANETs.

5.6 Dataset creation

The dataset was generated by NS-2 simulation in 1000 m x 1000 m networks containing from 30 to 100 nodes. It uses the random waypoint mobility model to simulate real node movement. Routing is managed according to the AODV protocol, and CBR traffic is transmitted over UDP so that it imitates active MANET communication behaviour. The scenarios consist of both misbehaviours, such as black hole and gray hole, and failure reasons like buffer overflow and energy depletion, to consider different causes of packet loss. Every case is simulated for100 seconds to provide sufficient data for evaluation. Intermediate nodes running in promiscuous mode receive all the traffic in their radio range. This produces trace files (.tr) that log packet-level details. These files, however, are processed by custom Python scripts to obtain node-dependent metrics such as PDRatio, queue usage, and energy. They also attach behavioural labels using heuristic thresholds (Table 1). Such an approach generates a stable, annotated data set to train and test the MLR classifier in dynamic environments reflecting malicious as well as non-malicious activities.

5.7 Feature engineering and preprocessing

Feature engineering is important to identify the behaviour pattern that separates different causes for dropping packets. The features available in the system are at most 10 node-specific attributes:

5.7.1 Packet drop rate

In Eq. (5), packet loss ratio is computed to detect black hole (nearly all lost, PDR > 90%) and gray hole (selective drop, PDR 30 to 60%).

$$PDR = \frac{Packet\ Dropped}{Packet\ Received} \tag{5}$$

5.7.2 Packet delivery ratio

In Eq. (6), Packet Delivery is measured, showing that packets are successfully delivered with the comparison of cooperative (high PDRatio) and non-cooperative nodes (low

PDRatio).

$$PDRatio = \frac{Packet\ Delivered}{Packet\ Sent} \tag{6}$$

5.7.3 Residual energy level

Eq. (7) detects inadvertent drops caused by energy depletion (REL< 25%) by normalizing current energy against initial capacity.

$$REL = \frac{Current\ Energy}{Initial\ Energy} \tag{7}$$

5.7.4 Other features

Additional context for behaviour analysis is provided by packet forwarding rate, queue utilization (which identifies buffer overflow at >85%), energy per packet, traffic intensity, hop count, routing overhead, and packet arrival/departure rates. Z-score standardization (Eq. (1)) is used to normalize features to guarantee uniform scaling and avoid biases in MLR classification caused by different units (e.g., percentages vs. joules). To reduce misclassification and guarantee strong behaviour differentiation, behavioural labels are assigned using empirical thresholds (Table 1) that are obtained from simulation analysis.

5.8 Classification via multinomial logistic regression

The MLR model uses the softmax function to classify nodes into five classes (normal, black hole, gray hole, buffer overflow, energy depletion).

$$P(y = k|X) = \frac{exp(w_K^T X)}{\sum_{j=1}^{K} exp\left(w_j^T X\right)} \tag{8}$$

In Eq. (8), W_k represents weight vector for class k, x represent feature vector, and $K = 5$. This equation produces class-wise probabilities and sums them to 1, ensuring multi-class classification. The model minimizes regular cross-entropy loss.

$$L = -\sum_{i=1}^{N}\sum_{k=1}^{K} y_{ik} \log\left(P(y = k|X_i)\right) + \lambda \sum_{k=1}^{K} ||W_k||_2^2 \tag{9}$$

In Eq. (9), $y_{ik} = 1$, if node i belongs to class k, else 0, and $\lambda = 0.01$ controls $L2$ regularization to prevent overfitting. The first term addresses the errors in classification, while the second enhances generalization of the model by constraining weight magnitudes.

Stochastic gradient descent (SGD) is used for performing optimization as seen in Eq. (10).

$$W_k \leftarrow W_k \leftarrow \eta \nabla L \tag{10}$$

With a decaying learning rate η = 0.01. This iterative update converges with optimal weights, which enable efficient and accurate classification in resource-constrained environments.

MLR has been selected because it aligns with the technical and practical requirements of MANET. In contrast to binary classifiers (SVM, RF…) that cannot calculate the non-hypothesis probability of a label directly, MLRs can be used as a multi-class classifier (5 different behaviours are separated: normal, black hole, gray hole, buffer overflow, and energy depletion). This also gives us precisely the granularity we needed; it can reduce the number of false positives by accurately detecting unintentional dropouts and thus prevents isolating (good) nodes. And keep connected to the network. MLR has a linear computational complexity in the feature dimension that makes it suitable for real-time operation on resource-constrained devices, such as ARM Cortex-M processors, unlike neural networks that require big computational resources. Class-specific weight vectors of the models will easily integrate with trust-based routing since classification probabilities directly inform behaviour scores $S_i(t)$ in Eq. (2). MLR's transparency via interpretable weights and probabilities also allows for easier debugging and decision-making in dynamic environments. In this paper, MLR balances accuracy, efficiency, and adaptability to assure robust performance under MANET conditions, enabling applications in tactical, vehicular, and IoT networks.

5.9 Algorithmic framework

Implementation is carried out through four algorithms, each addressing a specific function. Each algorithm is shown below as pseudocode along with its purpose, impact, and relationship to equations.

Algorithm 1 processes raw trace files to extract 10 features to capture comprehensive network and resource dynamics in MANETs. Only PDR, PDRatio, queue utilization, and REL are used for heuristic labelling based on thresholds (Table 1). All features are normalized and included in the feature vectors for the MLR classifier.

Algorithm 1: Feature Extraction and Labelling

Require: Trace file (.tr)

Ensure: Labelled feature vectors

1. for each node i do
2. Extract features: PDR, PDRatio, Queue Utilization, REL, Queue Utilization, Energy per Packet, Traffic Intensity, Hop Count, Routing Overhead, and Packet Arrival/Departure Rates.
3. Normalize features $z = \frac{x-\mu}{\sigma}$
4. if PDR > 90% and PDRatio ≈ 0 then
5. Label node i as Black Hole
6. else if PDR ∈ [30%, 60%] then
7. Label node i as Gray Hole
8. else if Queue Utilization ≥ 85% then
9. Label node i as Buffer Overflow
10. else if REL < 25% then
11. Label node i as Energy Depletion
12. else
13. Label node i as Normal
14. end if
15. Store feature vector (normalized PDR, PDRatio, REL, Queue Utilization, Energy per Packet, Traffic Intensity, Hop Count, Routing Overhead, Packet Arrival/Departure Rates) with label.
16. end for
17. return labelled feature vectors

Algorithm 2 computes dynamic trust scores, reflecting node reliability in real-time. Eq. (2) balances historical and current behavior, ensuring stability and responsiveness, while Eq. (3) decays trust for inactive nodes, preventing outdated reputations from affecting routing. This algorithm mitigates

risks from malicious or unreliable nodes, supporting secure routing decisions.

Algorithm 2: Trust Score Update

Require: Node i, behavior score $S_i(t)$, time t, α = 0.1, λ = 0.1

Ensure: Trust score $R_i(t)$

1. if node i is active then
2. $R_i(t) = \alpha R_i(t-1) + (1-\alpha)S_i(t)$
3. Else
4. $R_i(t) = R_i(t-1)e^{-\lambda \Delta t}$
5. end if
6. if $R_i(t) < 0.3$ then
7. Categorize node i as Malicious
8. else if $0.3 \leq R_i(t) < 0.5$ then
9. Categorize node i as Uncertain
10. Else
11. Categorize node i as Benign
12. end if
13. return $R_i(t)$

Algorithm 3 enhances AODV by integrating trust scores into route discovery and selection. It filters out low-trust nodes ($R_i(t) < 0.5$) and selects paths minimizing Eq. (4), ensuring secure and reliable routing. This tight integration improves responsiveness compared to stand-alone detection systems.

Algorithm 3: Trust-Aware Routing

Require: Source s, destination d, trust threshold τ = 0.5

Ensure: Trusted path P

1. Source s broadcasts RREQ with trust scores
2. for each node i receiving RREQ do
3. $if R_i(t) < \tau$ then
   Drop RREQ
4. else
   Append $R_i(t)$ and forward RREQ
5. Endif
6. End for
7. Destination d sends RREP if all nodes in path $R_i(t) \geq \tau$
8. Source s selects path P minimizing $Cost(P) = \sum_{i=P}(1 - R_i(t))$
9. return path P

Algorithm 4: Real-Time Node Classification

Require: Feature vector x, trained MLR model

Ensure: Node behavior class

1. for each class $k \in$ {Normal, Black Hole, Gray Hole, Buffer Overflow, Energy Depletion} do
2. Compute $P(y = k|X) = \frac{exp(w_K^T X)}{\sum_{j=1}^{K} exp(w_j^T X)}$
3. end for
4. Assign class k with highest $P(y = k|X)$
5. if class is Black Hole or Gray Hole, then
6. Flag node as malicious
7. end if
8. return assigned class

Algorithm 4 classifies node behavior in real-time using MLR, leveraging Eq. (10) for probabilistic multi-class prediction. It informs trust score updates (Algorithm 2) and routing decisions (Algorithm 3), ensuring context-aware security.

5.10 Routing integration

The MANET is mathematically represented as Graph G = (V, E), where V represents nodes and E represents communication links, shown in Figure 2. The routing objective minimizes the path cost, $Cost(P) = \sum_{i=P}(1 - R_i(t))$ subject to $R_i(t) < 0.5$. The cost function favours the nodes with high trust for routing, making sure forwarding is trustworthy. $Cost(P)$ maintains network performance in dynamic topologies by balancing path efficiency and trustworthiness by aggregating trust deficits.

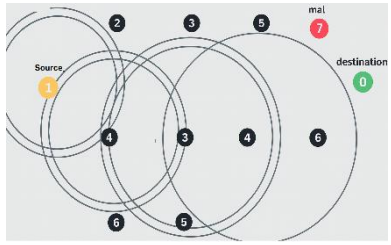

Figure 2. Mobile Ad Hoc Network (MANET) scenario with nodes and communication (depiction of simulation)

5.10.1 Integration with Ad hoc On-Demand Distance Vector routing protocol

The AODV protocol is extended to make it trust-aware, guaranteeing secure routing.

1. Route Request (RREQ): The source node broadcasts an RREQ packet to which every intermediate node appends its trust score $R_i(t)$. Every node with $R_i(t) < 0.5$ discards the RREQ packet so that untrusted nodes cannot participate in route discovery.
2. Route Reply (RREP): The destination node sends back the RREP if and only if all nodes in the proposed path satisfy $R_i(t) \geq 0.5$. This condition guarantees path reliability.
3. Routing Decision: Among the multiple RREPs, the source node chooses the path that gives the minimum value to Eq. (4). This is the path that provides a good balance between trust and efficiency.
4. Dynamic Trust-Based Routing: When the trust of a node goes below 0.5, the routes are invalidated, and rediscovery takes place in order to exclude unreliable nodes.
5. Route Maintenance: After route failures due to mobility or changes in trust, new route discovery is conducted by excluding low-trust nodes to maintain network security. The integration here ensures routing decisions based on current trust assessment values for more security and reliability in dynamic MANETs.

5.10.2 Routing process

The trust-based routing algorithm enhances the performance of AODV by incorporating trust scores and classification of MLR in every phase of route discovery, selection, and maintenance. It ensures that only the trustworthy nodes involved in routing effectively reduce the influence of malicious (black hole, gray hole), and the undesired (buffer overflow, energy starvation) packet drops. The approach is proactive, and it provides a lightweight (by leveraging Algorithms 2-4) and dynamic (i.e., adaptive and reactive to the dynamic MANET topology) solution against power attacks. The next part will detail the routing process,

with an emphasis on technical details, logic, and real-world implications.

5.10.3 Route discovery (Route Request)

1. Route Discovery: When a source node $'s'$ wants to communicate with a destination node $'d'$, it initiates route discovery by flooding the network with an RREQ packet. In conventional AODV, the RREQ packet includes a hop count and sequence number to differentiate between new routes. Proposed work includes trust scores $R_i(t)$ from Algorithm 2 into the RREQ packet header. Each intermediate node i which receives the RREQ, performs the following activities:
2. The trust value (R_i) on a node, either active or inactive, is verified by using Eq. (2) and Eq. (3), respectively. If $R_i(t) < \tau = 0.5$, this is an untrustworthy (malicious or uncertain node) and it discards the RREQ, preventing itself from participating in that route. It makes explicit use of Algorithm 3 to ensure that unreliable nodes are filtered out as soon as possible in the discovery process.
3. Trust Score Propagation: If $R_i(t) \geq 0.5$, the node inserts its reputation value in the RREQ packet and broadcasts it to neighbour nodes (from Algorithm 3). By performing this, it ensures the destination will receive a list of trust scores for all nodes over each path that is possible.
4. Dynamic Update: Trust scores are real-time updated via Algorithm 2, which is based on MLR classification of the sensor nodes by Algorithm 4. The MLR model is by using Eq. (10), which classify the behaviour of nodes according to, say, PDR to give trust scores that reflect up-to-date behavioural states; hence, a node turning into a node of gray hole attack commands reduced having $R_i(t)$ and therefore low $S_i(t)$ protocol (IP protocol traffic). This ensures that only nodes classified as benign-that is, $R_i(t) \geq 0.5$-participate in route discovery and minimize the chances of malicious nodes advertising false routes, such as black hole nodes advertising optimal paths. Inclusion of trust scores at RREQ packets creates hardly any extra overhead because each of them is a single floating-point value, thereby making this approach suitable for resource-constrained MANETs.

5.10.4 Route Reply

The destination node $'d'$, on receiving an RREQ, checks the trust value of the proposed path.

1. Path Trust Validation: The destination extracts the trust scores of all nodes in the path from the RREQ packet. It checks that all nodes satisfy $R_i(t) \geq 0.5$. If any node has $R_i(t) < 0.5$, the RREQ is discarded, ensuring that the path excludes malicious or uncertain nodes.
2. RREP Generation: If the path is a valid one, it generates the RREP packet at the destination node containing a list of node IDs along with their trust value. The reverse path RREP is returned back towards the source node $'s'$. Intermediate nodes transmitting the RREP will have to recheck their trust score so that it is above the threshold in their specificcase (taking into consideration potential changes in its behaviour from the moment of sending RREQ until forwarding a received RREP).
3. Handling Multiple Paths: In a dynamic MANET network, the destination often receives several RREQ packets from various paths. It creates an RREP for all valid paths (with $R_i(t) \geq 0.5$ on every node) such that the source can select the preferred path.

This step guarantees that only reliable paths are taken into account, taking advantage of the MLR classifier to classify abnormal behaviors (black hole and gray hole) from unintended drop actions while avoiding false positive decisions that might discard legitimate nodes.

5.10.5 Routing decision

Multiple RREPs describing a valid path to the destination are sent to the source node $'s'$. The process of selecting it can rely on other requirements like efficiency and trust.

1. Calculating Path Cost: Eq. (4) is used by the source to calculate the cost for each path P, i.e., $Cost(P) = \sum_{i=P}(1 - R_i(t))$ .This cost isa sum of trust deficit affecting the nodes in the path, lower value is better (Trustworthy path, i.e., having higher $R_i(t)$). For example, a path with nodes having trust scores $[0.9, 0.8, 0.95]$ has a cost of $(1 - 0.9) + (1 - 0.8) + (1 - 0.95) = 0.35$, while a path with scores $[0.6, 0.5, 0.7]$ has a cost of 1.2, favouring the former, shown in Figure 3.

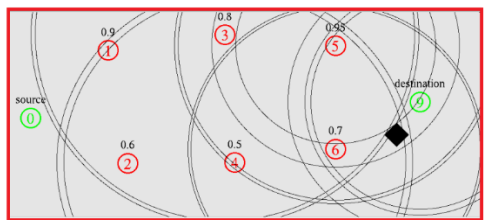

Figure 3. Mobile Ad Hoc Network (MANET) scenario path with nodes having trust scores

2. Best Path Selection: Source selects the path P with minimum cost. Hop count (calculated from RREP) metrics are used to differentiate costs andminimize latency in the case of equal cost alternatives.
3. Adaptive Decision Making: The classification with MLR through Algorithm 4 steers the continuous adaptive trust scores using Algorithm 2. A route is discarded, and the source is forced to consider other alternatives if any node has a trust score lower than 0.5 through its path selection (due to new gray hole behavior as identified by Eq. (10)).
4. This decision-making process has been designed to provide the optimum compromise between trustworthiness and efficiency, guaranteeing reliable packet transmission in the face of malicious or resource-limited nodes.

5.10.6 Dynamic trust-based routing

Routing flexibility is ensured through ongoing trust monitoring in the framework:

1. Trust Score Monitoring: After selecting a path, trust scores are updated periodically using Eq. (2) for active nodes and Eq. (3) for inactive nodes. The MLR classifier runs in real-time, analyzing features like PDR and REL to update behavior scores $S_i(t)$. For example, a node initially classified as normal may be reclassified as energy-depleted if its REL drops below 25%, reducing its trust score.
2. Invalid Route: If the value of $R_i(t)$ gets below 50% at

a node on the active path, the route is invalidated. This rapidly removes malicious or unreliable nodes by re-executing route discovery.

3. Low Overhead: Real-time adaptation is possible in resource-constrained MANETs because trust updates and MLR classifications are lightweight, finishing in less than 10 ms/node on ARM Cortex-M devices.
4. In MANETs, where topology and node reliability change quickly, this dynamic approach guarantees that routing decisions take into account the most recent node behaviors.

5.10.7 Route maintenance

Failures brought on by mobility, shifts in trust, or interruptions in the link are addressed by route maintenance:

1. Failure Detection: A node becomes malicious and sends a Route Error (RERR) packet to the source node if it detects a link failure because of mobility or a trust score drop below 0.5.
2. New Route Discovery: Using Algorithm 3, the source starts a new RREQ in accordance with the trust-aware procedure. The new path is reliable because nodes with $R_i(t)< 0.5$ are eliminated.
3. Proactive Monitoring: To identify behavioral shifts, IDS nodes feed data to the MLR classifier while continuously monitoring traffic in promiscuous mode. A gray hole node that selectively drops packets, which lowers its trust score and starts a route discovery.

By adjusting to behavioral (trust) and physical (mobility) changes with minimal overhead, this maintenance procedure guarantees network resilience.

6. PERFORMANCE EVALUATION

The framework is evaluated in a 1000×1000 m^2 network using NS-2 with 30 to 100 benign and attacker nodes under random waypoint mobility. Simulations ran for 100 seconds with CBR traffic over UDP. Ten runs per scenario were averaged, maintaining a 95% confidence interval. Varying network size from sparse to dense ensures scalability testing. The random waypoint mobility model enables node movement in MANETs in an unpredictable way with 1-20 m/s speeds. Other parameters of simulation, such as area (1000×1000 m^2), simulation time (100s), CBR traffic over UDP, are selected based on standard MANET benchmarks to enable fair comparisons with prior works [18, 33], while keeping a 95% confidence interval across 10 runs per scenario.

This analysis presents the performance evaluation of the proposed trust-integrated ML framework for mitigating packet-dropping behaviors in MANETs. The proposed framework integrates MLR for five-class node classification, namely, normal, black hole, gray hole, buffer overflow, and energy depletion, along with a dynamic reputation-based trust model that extends the traditional reactive routing protocol. The performance evaluation is based on NS-2 simulation results over the following performance parameters: node classification accuracy, routing performance, scalability, attack mitigation, and computation efficiency of the proposed approach, along with comparisons against standard AODV and RAR. Performance metrics include PDF, end-to-end delay, energy efficiency, routing overhead, and other node classification metrics such as precision, recall, F1-score, and Matthews Correlation Coefficient (MCC).

6.1 Classification results

High performance is achieved with cross-validation accuracy of 95.9% and test accuracy of 95.7% (Table 2) through the MLR model, trained with L2 regularized (C= 0.01), 5-fold cross-validation, 5% label noise, and label smoothing. Some misclassifications in classification are seen in the confusion matrix, especially between buffer overflow and energy depletion, and between normal flow and other classes. These misclassifications are due to resource-related symptoms that overlap with transitional node behaviour, like excessive queue usage and moderate drop rates. For all classes, receiver operating characteristic (ROC) curves reported an area under the curve (AUC) > 0.90 for all classes, indicating excellent separability. Featured importance analysis using regression coefficients and SHapley Additive exPlanations (SHAP) inspired evaluation highlights most influential features like PDF, queue utilization, residual energy, packet forwarding rate, and routing overhead, which match the behavioural thresholds used for classification.

Table 2. Classification results for node behavior types

Behavior	Precision	Recall	F1-Score	MCC
Black hole	0.97	0.97	0.97	0.93
Buffer overflow	0.98	0.91	0.95	0.93
Energy depletion	0.95	0.95	0.95	0.93
Gray hole	0.93	0.98	0.95	0.96
Normal flow	0.96	0.98	0.97	0.96
Macro average	0.96	0.96	0.96	0.94
Weighted average	0.96	0.96	0.96	0.94

Note: Matthews Correlation Coefficient (MCC).

In Table 2, the high precision of all classes (0.93–0.98) suggests a low rate of false positives, which is important in preventing the false isolation of legitimate nodes. High recall in all the classes (0.91–0.98) demonstrates the model is able to identify true samples for all behaviours. The F1-scores for all classes are around 0.95–0.97 and show robust performance in terms of precision and recall. The MCC (0.93–0.96) indicates that the classification quality is high when considering the class distribution of the data. The macro and weighted averages are 0.94, indicating the average F1 score across the classes. The model is very accurate for all behaviours, and its constant scores on the features suggest a tiny effect of feature overlap.

Nevertheless, the feature and the buffer overflow accuracy (0.93) are only slightly compromised for the proposed architecture in terms of the feature overlapping with gray hole behaviours (i.e., for the moderate PDF (40-70%) and high queue utilization > 85%). This coincidence represents a fundamental difficulty in discriminating between the two behaviours as they share common network performance properties in some cases. This is much smaller than that in a black hole (0.91), which is caused by the fact that the patterns for black holes and gray holes are similar occasionally. It can be observed that the MCC for buffer overflow (0.93) is less in comparison to normal flow and gray hole (0.96) because it is hard to separate buffer overflow and gray hole, as both have the same PDF and queue utilization. Even though it does not, it still has high precision and recall for other behaviours, which proves its quality. The proposed model is designed with this very overlap and the complexity of distinction in mind, so it performs well and is flexible even in real-world environments where the network topology and nodes change over time.

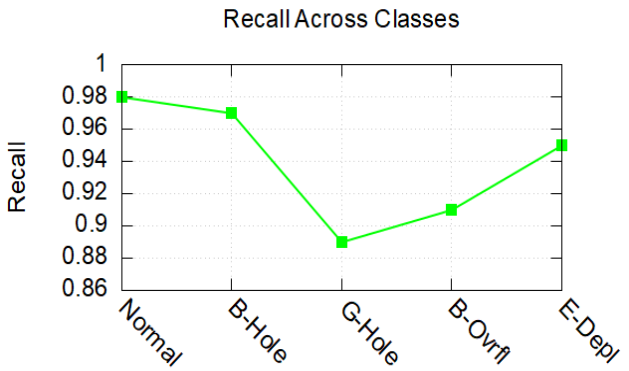

Figure 4. The recall scores across different node behavior classes

Figure 4 shows exceptionally high recall for normal and black hole behaviours, suggesting that the model strongly detects those behaviours. A minor drop in recall from the normal and black hole behaviours to both gray hole and buffer overflow behaviours likely results from the intersection of behaviours expressed in both classes. The model's performance on energy depletion shows recovery, suggesting better differentiation for energy-based node degradation.

The model depicted in Figure 5 has high precision for most behaviours, and the highest precision rate occurs on Buffer Overflow behaviour (0.98). A significant valley also appears in the gray hole class (0.93), possibly reflecting third-party overlap, i.e., they can drop packets selectively or according to energy or buffering. Overall performance is still high; the model consistently achieves precision above 0.93 for every class, minimizing false positives and enabling accurate routing decisions.

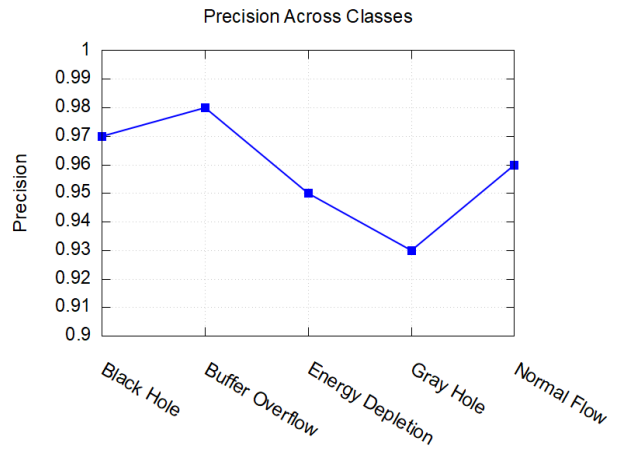

Figure 5. Precision scores across different node behaviour classes

6.1.1 Receiver operating characteristic curves

Figure 6 shows the ROC curves that depict strong separability between behaviours, with an AUC > 0.90 for every class. When compared to binary classifiers like SVM and RF, which typically report AUCs of 0.85–0.90 for malicious detection only, the proposed framework achieves high AUCs by effectively separating malicious (black hole, grey hole) and unintentional (buffer overflow, energy depletion) drops, thereby reducing false positives.

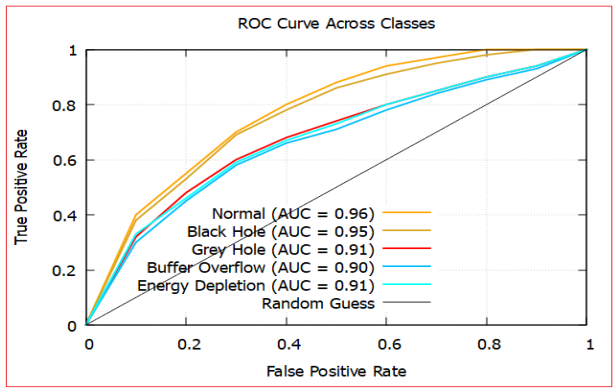

Figure 6. Receiver operating characteristic (ROC) curves for node behaviour classification

The ROC examines how true positive rates vary against false rates at various thresholds for every behavior category. Strong separability is indicated by the AUC exceeding 0.90 for every class.

6.1.2 Confusion matrix

A confusion matrix for the classification task (Figure 7) shows diagonal dominance, a sign of high classification accuracy for each node behavior class. The majority of predictions fall on the identity line, indicating that the model is able to accurately recognize, say, Black Hole (55/59), Gray Hole (56/57), and Energy Depletion (55/58) with high precision and recall (≥ 0.95). Relatively small confusions are observed among Buffer Overflow (confusion with Energy Depletion and Normal Flow).

By comparison, Gray Hole obtains the highest recall of 98% with a somewhat lower precision (93%), testifying to the model's superiority in capturing all the gray hole instances at the expense of some false positives.

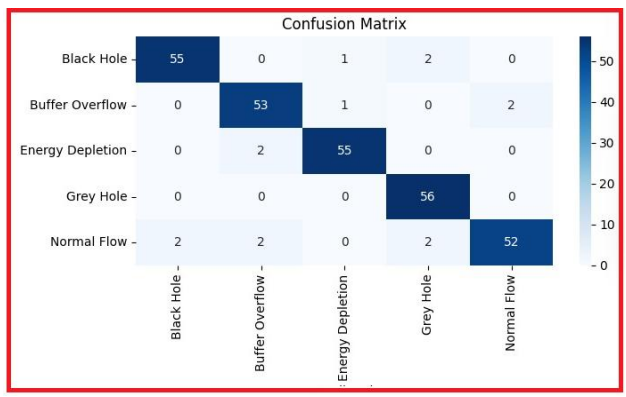

Figure 7. Confusion matrix for node behaviour classification

6.2 Routing performance

The framework's trust-aware AODV routing (TMLR) compared with standard AODV with no misbehaving nodes and standard AODV with misbehaving nodes and multifactor misbehaving mitigation [18] and Acknowledge (ACK) based misbehaving node mitigation [17] across key metrics (Table 3), evaluated in a network of 30 to 100 nodes.

Table 3 shows that the proposed framework achieves a 95% PDF, significantly outperforming AODV under misbehaviour (15%) and Multifactor (64%) conditions, nearing AODV's ideal 99% PDF. It improves PDF by 80% over AODV under

misbehaviour and 31% over Multifactor, surpassing the ACK-based method's 57% PDF by 38%. The trust-aware routing mechanism (Algorithm 3) minimizes path cost by excluding malicious and unreliable nodes. The MLR model ensures precise identification of packet-dropping behaviours for reliable path selection.

Table 3. Routing performance comparison

Metric	AODV No Misbehave [33]	AODV Under Misbehave	Multi Factor [20]	ACK	Proposed (TMLR)
End-to-end delay (s)	0.19	0.19	0.20	0.21	0.20
Routing delay (s)	0.25	1.53	0.58	0.43	0.28
Throughput (M bits)	0.23	0.03	0.17	0.13	0.35
Packet delivery (%)	99	15	64	57	95
Remaining energy (J)	89.05	72.16	79.4	55.39	93.27

Note: Ad hoc On-Demand Distance Vector (AODV); trust-integrated multinomial logistic regression (TMLR).

The proposed framework achieves an end-to-end delay of 0.20 seconds, closely matching AODV's ideal condition delay of 0.1986 seconds and outperforming AODV under misbehaviour (0.1902 s, skewed by packet loss), Multifactor (0.20534 s), and ACK (0.21 s). MLR classifications and real-time trust evaluation select reliable routes by avoiding malicious and resource-limited nodes. This type of approach results in low latency even in dynamic MANET environments, even under malicious or system faults. When compared to multifactor and ACK, this adaptive framework minimizes significant delays.

Compared to AODV, the framework records a remaining energy of 93.27 Joules even under ideal conditions (89.05 J) and misbehaving conditions (72.16 J), Multifactor (79.4 J), and ACK-based approaches (55.39 J). The energy consumption is reduced through efficiency, low-complexity computations as implemented in Algorithm 4. Energy loss is seen in AODV due to unmitigated malicious and system faults, while multifactor partially checks for these issues, and ACK introduces a high acknowledgment overhead. The dynamic trust-based filtering in the framework improves network lifetime in resource-limited MANETs.

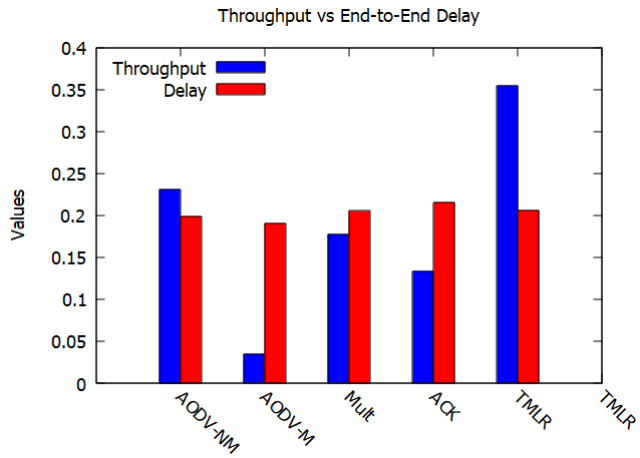

Figure 8. Routing performance comparison in terms of throughput and delay

This approach concludes low latency in a dynamic MANET environment under malicious behavior or system faults. The trust integrated ML framework, when compared to AODV, outperforms under misbehavior and multi-factor based techniques, which results in improving packet delivery. As per Figures 8 and 9, the framework performs better than AODV, Multifactor, and ACK-based methods, and also while simultaneously maintaining low delay, robust throughput, high energy efficiency, and PDF. Its lightweight, adaptable design guarantees scalability and reliability in dynamic MANETs, and it successfully reduces malicious and system fault drops. According to the results, the framework shows constant high performance and delivery rate throughout the scenarios tested. These outcomes conclude that the framework is not only efficient for detecting attack types but also for maintaining resilient routing performance under adversarial conditions.

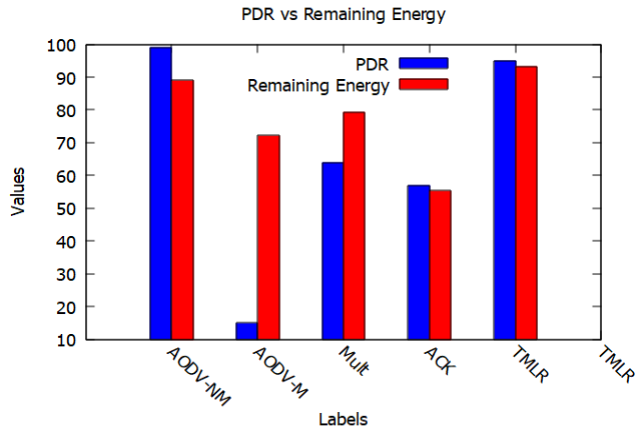

Figure 9. Routing performance comparison in terms of packet delivery fraction (PDF) and remaining energy

6.3 Attack impact

The framework mitigated attack impacts (Table 4). More than 90% PDF with high precision/recall ensures the proposed work to detect and mitigate the packet-dropping nodes accurately. Thus, the superior PDF performance across different attack scenarios makes it more effective than the Multifactor approach in mitigating packet dropping issues in MANETs.

Table 4. Impact of attacks on packet delivery fraction (PDF)

Scenario	PDF (Multifactor)	PDF (Proposed)
Black hole	64%	95%
Gray hole	64%	92%
Buffer overflow	70%	93%
Energy depletion	79%	91%

6.4 Scalability

Tests with 30–100 nodes yielded classification accuracy >90%, inference time <10 ms/node, and PDF degradation <2%, all demonstrating clarity of proficiency and scalability. Table 5 confirms that the classification model is robust and scalable. The classification accuracy was relatively invariant to the different density levels, and the original classification performance was maintained up to the maximum density used in this study.

Table 5. Classification accuracy by network size

Network Size	Average Accuracy	Lowest to Highest Accuracy	Unusual Results
30 Nodes	91.7%	88.0% to 94.0%	94.5%
50 Nodes	91.1%	87.5% to 93.5%	93.8%,94.2%
100 Nodes	90.0%	86.0% to 93.0%	93.5%, 94.0%, 86.5%

Table 6. Inference time (ms/node) by network size

Network Size	Average Time (ms)	Shortest to Longest Time (ms)	Unusual Longer Times (ms)
30 Nodes	3 ms	2 ms to 4 ms	None
50 Nodes	5 ms	4 ms to 6 ms	None
100 Nodes	8 ms	6 ms to 9 ms	≥10 ms

The relatively low inference times (remaining consistently below 10 ms/node) shown in Table 6, which show the overall real-time capability of the system, especially when using low-power hardware platforms such as ARM Cortex-M devices. These findings further ensure the suitability of the framework for deployment in resource-limited and delay-sensitive scenarios.

6.5 Discussion

By distinguishing between intentional (black hole, gray hole) and unintentional (buffer overflow, energy depletion) packet drops, the framework reduces false positives when compared with binary classifiers. The introduction of trust-aware routing improves other mitigation techniques with low overhead and energy efficiency, making the proposed framework more suitable for tactical, vehicular, and IoT MANETs. The system effectively handles packet drop behaviour from both malicious and unintentional packet drops.

The confusion matrix shown in Figure 7 indicates gray hole and buffer overflow behaviors have some misclassification, mainly due to features like moderate PDF (40–70%) and high queue utilization (>85%), as gray hole intentionally imitates a resource constraint environment to avoid detection in MANETs. Using regression coefficients and SHAP-inspired evaluation, the features are analyzed, which confirmed some key predictors like PDF, queue utilization, residual energy, packet forwarding rate, and routing overhead, which align with empirical thresholds in Table 1. A 7% misclassification rate is caused by these overlaps, which in turn leads to an increase in false positives. To reduce these errors, integrating temporal features like time series analysis of drop patterns (bursty vs. consistent drops) or a hybrid reinforcement learning model to adapt thresholds dynamically is useful, and also reduces classification error, ensuring reliability in MANETs with resource-constrained environments.

7. CONCLUSIONS

The paper concludes a new trust-integrated multinomial logistic regression (TMLR) framework, which focuses on reducing packet dropping behaviour in MANETs. This study uses an MLR classifier, which classifies black hole, Normal, gray hole, buffer overflow, and energy depletion, combined with trust-aware AODV routing and a dynamic reputation-driven trust mechanism; this integration ensures that the malicious and non-malicious packet drops are distinguished accurately. The results of the simulation are obtained using NS-2. It achieves 95.7% classification accuracy; in turn, PDF is improved by 31% over multifactor-based misbehaving mitigation, and maintains a low cost of processing. The proposed framework's high precision (0.93–0.98) and recall (0.91–0.98) reduce false positives compared to binary classifiers, ensuring network connectivity by avoiding the isolation of legitimate nodes. The model's scalable performance across dynamically changing network sizes and its lightweight design make it well-suited for MANETs, which have limited resources. Future work, which includes integrating time-series analysis (using LSTM variants optimized for low overhead), includes capturing sequential drops and distinguishing between gray hole and buffer overflow patterns. This type of framework is used to reduce limitations in black hole recall (0.91) and gray hole precision (0.93). Moreover, future work plans real-world deployment on testbeds like Raspberry Pi-based MANETs to validate performance under actual hardware constraints.

REFERENCES

[1] D., P.K., Sandhya, E., Sk, K.S., Mantena, S.V., Desanamukula, V.S., Koteswararao, C., Vemula, S.R., Vemula, M. (2025). Enhancing security and efficiency in mobile ad hoc networks using a hybrid deep learning model for flooding attack detection. Scientific Reports, 15: 818. https://doi.org/10.1038/s41598-024-84421-0

[2] Razouqi, Q., Boushehri, A., Gaballa, M., Alsaleh, L., Abbod, M. (2024). Extended comparison and performance analysis for Mobile Ad-Hoc Networks routing protocols based on different traffic load patterns and performance metrics. Electronics, 13(14): 2877. https://doi.org/10.3390/electronics13142877

[3] Baird, I., Wadhaj, I., Ghaleb, B., Thomson, C. (2024). Impact analysis of security attacks on mobile ad hoc networks (MANETs). Electronics, 13(16): 3314. https://doi.org/10.3390/electronics13163314

[4] Saranya, P., Nithya, A. (2023). Reputation-based opportunistic routing protocol using Q-Learning for manet attacked by malicious nodes: A survey. Tuijin Jishu/Journal of Propulsion Technology, 44(4): 5195-5204. https://doi.org/10.52783/tjjpt.v44.i4.1874

[5] Wang, N., Zhang, S.C., Zhang, Z., Qiao, J.W., et al. (2023). Lightweight and secure data transmission scheme against malicious nodes in heterogeneous wireless sensor networks. IEEE Transactions on Information Forensics and Security, 18: 4652-4667. https://doi.org/10.1109/tifs.2023.3297904

[6] Shu, T., Krunz, M. (2015). Privacy-preserving and truthful detection of packet dropping attacks in Wireless Ad Hoc Networks. IEEE Transactions on Mobile Computing, 14(4): 813-828. https://doi.org/10.1109/tmc.2014.2330818

[7] Malik, A., Khan, M.Z., Qaisar, S.M., Faisal, M., Mehmood, G. (2023). An efficient approach for the detection and prevention of gray-hole attacks in VANETs. IEEE Access, 11: 46691-46706.https://doi.org/10.1109/ACCESS.2023.3274650

[8] Shyam, D.N.M., Hussain, M.A. (2023). A naive bayes-driven mechanism for mitigating packet-dropping attacks in autonomous wireless networks. Ingénierie des Systèmes d'Information, 28(4): 1019-1027.

https://doi.org/10.18280/isi.280422
[9] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S. (2019). Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3): 239-267. https://doi.org/10.1504/IJHI.2019.103580
[10] Djahel, S., Nait-abdesselam, F., Zhang, Z.H. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. IEEE Communications Surveys & Tutorials, 13(4): 658-672. https://doi.org/10.1109/SURV.2011.072210.00026
[11] Shakshuki, E.M., Kang, N., Sheltami, T.R. (2013). EAACK—A secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics, 60(3): 1089-1098.https://doi.org/10.1109/TIE.2012.2196010
[12] Ahmed, A.A., Fadhil, S.A., Najim, A.H., Alheeti, K.M.A., Satar, N.S.M., Hashim, A.H.A. (2024). Assessing the effects of blackhole attacks on MANET reliability and security. In 2024 International Conference on Decision Aid Sciences and Applications (DASA), Manama, Bahrain, pp. 1-6. https://doi.org/10.1109/DASA63652.2024.10836645
[13] Gurung, S., Mankotia, V. (2024). ABGF-AODV protocol to prevent black-hole, gray-hole and flooding attacks in MANET. Telecommunication Systems, 86: 811-827. https://doi.org/10.1007/s11235-024-01154-1
[14] Banerjee, S. (2008). Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In Proceedings of the World Congress on Engineering and Computer Science 2008WCECS 2008, San Francisco, USA. https://www.iaeng.org/publication/WCECS2008/WCECS2008_pp337-342.pdf.
[15] Saetang, W., Charoenpanyasak, S. (2012). CAODV free blackhole attack in ad hoc networks. In 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012), pp. 63-68. https://scispace.com/pdf/caodv-free-bl-ackhole-attack-in-ad-hoc-networks-2u6oozzoz6.pdf.
[16] Kshirsagar, D., Patil, A. (2013). Blackhole attack detection and prevention by real time monitoring. In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, pp. 1-5. https://doi.org/10.1109/ICCCNT.2013.6726597
[17] Atheeq, C., Rabbani, M.M.A. (2021). CACK—A counter based authenticated ACK to mitigate misbehaving nodes from MANETs. Recent Advances in Computer Science and Communications, 14(3): 837-847. https://doi.org/10.2174/2213275912666190809104054
[18] 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
[19] Hassan, S.M., Mohamad, M.M., Muchtar, F.B. (2024). Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks. IEEE Access, 12: 150046-150090. https://doi.org/10.1109/ACCESS.2024.3457682
[20] Bulla, S., Chaparala, P.,Mekala, S. (2021). A comprehensive survey on cryptography evaluation in mobile (MANETs). Turkish Journal of Computer and Mathematics Education, 12(2): 3406-3416. https://doi.org/10.17762/turcomat.v12i2.2402
[21] Bayaga, A. (2010). Multinomial logistic regression: Usage and application in risk analysis. Journal of Applied Quantitative Methods, 5: 288-297. https://jaqm.ro/issues/volume-5%2Cissue-2/9_bayaga.php.
[22] Rehmani, M.H., Saleem, Y. (2015). Network simulator NS-2. Encyclopedia of Information Science and Technology, Third Edition. IGI Global Scientific Publishing, pp. 6249-6258. https://doi.org/10.4018/978-1-4666-5888-2.ch615
[23] Nadeem, A., Howarth, M.P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE Communications Surveys & Tutorials, 15(4): 2027-2045. https://doi.org/10.1109/SURV.2013.030713.00201
[24] 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
[25] Michiardi, P., Molva, R. (2002). Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security. IFIP — The International Federation for Information Processing, pp. 107-121 https://doi.org/10.1007/978-0-387-35612-9_9
[26] Hubaux, J.P., Gross, T., Le Boudec, J.Y., Vetterli, M.(2001). Toward self-organized mobile ad hoc networks: The terminodes project. IEEE Communications Magazine, 39(1): 118-124. https://doi.org/10.1109/35.894385
[27] Zapata, M.G. (2002). Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3): 106-107. https://doi.org/10.1145/581291.581312
[28] Atheeq, C., Rabbani, M.M.A. (2016). Secure data transmission in integrated internet MANETs based on effective trusted knowledge algorithm. Indian Journal of Science and Technology, 9(47): 1-7. https://doi.org/10.17485/ijst/2016/v9i47/98497
[29] Desai, A.M., Jhaveri, R.H. (2019). Secure routing in mobile ad hoc networks: A predictive approach. International Journal of Information Technology, 11: 345-356. https://doi.org/10.1007/s41870-018-0188-y
[30] Shafi, S., Mounika, S., Velliangiri, S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. Procedia Computer Science, 218: 2309-2318. https://doi.org/10.1016/j.procs.2023.01.206
[31] Hemalatha, S., Janakidevi, M., Kumar, P.S., Arunkumar, M.S., Angadi, S., Murugananthan, T., Hamsalekha, R., Vijay Muni, T. (2024). Detecting intruder and black hole attackers in mobile ad hoc network. International Journal of Electronics and Communication Engineering, 11(4): 80-88. https://doi.org/10.14445/23488549/IJECE-V11I4P109
[32] Kavitha, T., Geetha, K., Muthaiah, R. (2019). India: Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach. Journal of Medical Systems,43:

179. https://doi.org/10.1007/s10916-019-1309-2
[33] Thanuja, R., Umamakeswari, A. (2019). Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. Cluster Computing, 22: 3131-3143. https://doi.org/10.1007/s10586-018-2006-5