I. J. Computer Network and Information Security, 2026, 3, 221-239
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.03.12

Adaptive Trust Node Routing via Energy-Aware and Steerable Network with Stochastic Optimization for Augmented Intrusion Detection in MANET Infrastructures

Mehaboob Mujawar*
Department of Artificial Intelligence and Data Science, Bearys Institute of Technology, Mangalore, India
E-mail: mehaboob311134@gmail.com
ORCID iD: https://orcid.org/0000-0002-8260-7062
*Corresponding author

R. Mohandas
Department of ECE, Chennai Institute of Technology, Chennai, Tamil Nadu, India
E-mail: mohandasbe@gmail.com
ORCID iD: https://orcid.org/0000-0002-6669-9075

R. Giri Prasad
Department of Petroleum Technology, Aditya University, Surampalem, Kakinada, Andhra Pradesh, India
E-mail: geogiriprasad@gmail.com
ORCID iD: https://orcid.org/0000-0002-3961-2229

K. Narasimha Raju
Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering (Autonomous), Visakhapatnam, India
E-mail: rj.vizagg@gmail.com
ORCID iD: https://orcid.org/0000-0002-5789-9614

Received: November 5, 2024; Revised: June 6, 2025; Accepted: August 3, 2025; Published: June 8, 2026

Abstract**:** Mobile Ad-Hoc Networks (MANETs) are self-organizing networks without any fixed infrastructure, which are decentralized and, thus, find applications in a dynamic and infrastructure-less environment. Nevertheless, these networks face significant challenges, including excessive energy consumption, malfunctioning routing, and security risks posed by malicious nodes. Such issues tend to cause higher communication overhead and a shorter network lifetime, particularly in highly mobile environments. To overcome these challenges, this paper proposes a dynamic, energy-saving routing architecture that could improve the network's security and reliability. The suggested solution assesses the reliability of network nodes through energy performance and communication reliability, and continuously analyzes network traffic to identify malicious activity in real time. Data delivery is guaranteed through secure route selection and smart intrusion detection, allowing the framework to reduce superfluous energy consumption. The obtained simulation outcomes show that the suggested approach achieves 92.8% and 96.5% in the packet delivery ratio and intrusion detection, respectively, which is a strong indication of an impervious defense against attacks. Moreover, the method is highly energy-efficient, has a longer network lifetime, and is thus a good fit for the practice of MANET use, such as emergency response, military communications, and mobile IoT networks.

Index Terms: Trust Node Evaluation, Intrusion Detection, MANET, Energy-Driven Collaborative Routing, Manifold-Aware Point-wise Steerable Network, Stochastic Emperor Penguin Optimization.

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

1. Introduction

MANETs have become an important technology in the recent past due to their characteristics such as decentralized structure and connectivity [12]. Nevertheless, the presence of MANETs causes some vital security problems, especially in routing and node credibility due to a self-organization system [1]. To overcome these difficulties, Secure Intrusion Detection Routing Protocols [13] alongside trust node evaluation mechanisms [3] must be developed that will provide a comprehensive and reliable approach towards boosting network security [2].

The aspect that needs significant attention is the design of security routing protocols for MANETs, as the network is very dynamic and can be vulnerable to different types of attack [4]. The goal is to provide security solutions for routing protocols so that malicious activities can be detected through trust management mechanisms and hence improve the safety of transmitted data [5]. Trust Node Evaluation is another component of this framework which aids in the evaluation of nodes of the network with respect to their trustworthiness, which enhances their network stability [10]. These protocols encompass trust-based mechanisms that constantly analyse and assess the activity of every node in the network [6]. Trust computation frameworks play a significant role in dynamically calculating the trust value of nodes according to their activities and transactions on the network [7]. These dynamic trust mechanisms therefore make it possible to detect various types of routing attacks such as blackhole and grayhole attacks as well as Sybil attacks [8]. In addition, these protocols are less likely to have false positives since the intelligent trust models that can be complemented with machine learning are applied during the detection of malicious nodes [14].

Thus the intrusion detection routing protocols with trust node evaluation offer enhanced security architecture defence against both internal and external threats [9], enabling MANETs to function safely in hostile military environments without interruption in network functionality [11]. They also account for not only identifying hostile actions but also repeatedly authenticating nodes' internal integrity and reliability [15], improving upon security as well as network fluidity.

1.1. Contributions

- The study presents Energy-Driven Collaborative Routing (EnerCR) that identifies trusted data transfer points with regard to node energy in MANETs.
- It employs Manifold-Aware Point-wise Steerable Network (MaP-WiSNet) to assist the detection of intrusions by recognizing the topology of the network and directing the data stream.
- The study adopts the Stochastic Emperor Penguin Optimization (SEmPO) that resolves the issue in routing decisions and increases the chances of identifying security threats.
- Thus, our research integrates all these methods to establish a comprehensive framework that effectively not only addresses routing issues but also enhances network defence against invasions to make MANET infrastructures secure and power efficient.

The remainder of this paper is organized as Section 2: Literature review, Section 3: Proposed methodology, Section 4: Results and Discussion, Section 5: Conclusion.

2. Literature Survey

In 2022, Sivanesh, S. et al. [16], presented Analytical termination of malicious nodes (ATOM): intrusion detector system to identify black hole attack in cellular mobile ad hoc networks. This paper proposed the application of a host-based intrusion detection system (HIDS) known as Analytical Termination of Malicious nodes (ATOM) to recognize black hole attacks in MANETs. The security of AODV is enhanced drastically by accurately sensing the existence of malicious activity by ATOM which monitors the real level of RREP and packet drops within each node.

In 2024, Selvaraj, S. et al. [17], suggested an Effective security and efficiency in MANETs: clustering based solution with CGRUN and AGTO clustering optimization towards intrusion detection and path finding. The study suggests a clustering-based remedy to intensify the security and performance of MANETs by utilizing the suggested CGRUN model to accomplish precise classification of sequential data. CGRUN is better at intrusion detection and AGTO is better at weight reduction optimization by using fewer resources to achieve improved network performance due to the integration of CNNs and RNNs.

In 2023, Shafi, S. et al. [18], introduced a New Energy Aware MPR Selection to secure OLSR Routing Scheme under Black Hole Attack A machine learning method. The proposed DBN-OLSR methodology in this paper would enhance the security and energy efficiency of OLSR routing in case of black hole attacks. Concerning hop-count and excess energy, Multipoint Relay (MPR) nodes are selected and redundant beacon transmissions are eliminated. A Deep Belief Network (DBN) and Naive Bayes classifier are applied to prevent black hole attacks, making sure that the safety of data that are transmitted is guaranteed. The performance of DBN-OLSR protocol is measured against conventional OLSR and AODV routing protocols.

In 2023, Luong, N.T. et al. [19], offered BAPRP: Blackhole attacks prevention routing protocol is an Ad Hoc network machine learning algorithm. In this paper, a Blackhole Attack Prevention Routing Protocol (BAPRP) is

proposed through incorporation of Black Hole Attack Detection Algorithm (BADA) which is a machine learning-based solution. With regards to the malicious node detection in BADA, the algorithm used is the k-Nearest Neighbours algorithm and is based on the analysis of the past request and response behaviour of the route. BAPROP uses this mechanism of detection as an adapted AODV protocol to enhance black hole protection.

In 2023, Krishnasamy, B., et al. [20], proposed optimal DIWGAN based on Namib Beetle Optimization Algorithm to detect intrusion in mobile ad hoc networks. This study focuses on the Namib Beetle Optimization Algorithm-optimized Dual Interactive Wasserstein Generative Adversarial Network (DIWGAN) to detect intrusion in Mobile Ad hoc Networks (MANETs). Through the application of the one-way hash chain operation, the mobile users are registered with the Trusted Authority through submitting their finger vein biometrics, user ID and geographical coordinates (latitude and longitude) to be authenticated. Intrusion detection system has four phases: packet analysis, feature extraction, preprocessing, and feature classification so that it can be able to identify various attacks.

In 2024, Devi, V.A., et al. [21], suggested an Energy Efficient Routing Establishment (EERE) mechanism of MANET-IoT security. This paper suggests an Energy Efficient Routing Establishment (EERE) scheme to MANET-IoT security, which is a hybrid scheme combining Whale Positioning scheme with Flower Pollination Algorithm (WP-FPA) as the best routing algorithm, depending on the energy content of the node. In an attempt to add to the Security, the Aggregated Packet Control Trust Protocol (APCTP) evaluates the trustworthiness of individual nodes, countering the presence of compromised nodes on the route. The average residual energy, packet delivery ratio (PDR), packet delay and network lifetime are the metrics used to measure the performance of the proposed mechanism.

In 2024, Kaushik, S., et al. [22], recommended the use of K-AOMDV routing protocol to improve reliability of mobile ad hoc networks (MANETs) to overcome black hole attacks. This paper presents the K-AOMDV routing protocol, which is a variant of the AOMDV protocol that helps to reduce black hole attacks in MANETs. K-AOMDV detects and removes routing misbehavior by combining K-means clustering and route optimization by minimizing the number of packet hops. The estimation of the best pathways of the protocol considering assaults and delays is done using supervised machine learning. Based on the use of various routes and dynamism of route discovery, K-AOMDV increases the reliability of delivering data in a malicious node environment.

The summary of the existing methods is presented in Table 1 as below,

Table 1. Overview of the current procedures.

Reference Number	Methods	Highlights	Challenges
[16]	ATOM	- Efficient black hole attack detection - Improves AODV protocol performance	- High computational overhead - Limited scalability
[17]	CGRUN-AGTO	- Combines CNNs and RNNs for robust classification - AGTO optimizes resource usage	- Complex model requires extensive training - Potential overfitting with small datasets
[18]	DBN-OLSR	- Energy-efficient multipoint relay node selection - ML-based prevention of black hole attacks	- Increased routing complexity - Requires large training data for DBN
[19]	BAPRP	- k-NN effectively detects malicious node - Enhances AODV protocol security	- Relies heavily on historical data - High computational cost in large networks
[20]	DIWGAN	- Detects intrusion using GAN optimized with Namib Beetle - Biometric-based authentication adds Security	- Computationally expensive GAN training - Biometric data management may face privacy issues
[21]	EERE	- Optimizes path selection using WP-FPA - APCTP enhances network security	- Trust evaluation can add latency - High computational load for large-scale networks
[22]	K-AOMDV	- K-means clustering prevents routing misbehaviour - Multi-path routing ensures data delivery reliability	- High complexity due to clustering and ML components - Increased overhead in route discovery

2.1. Problem Statement

MANETs are autonomous networks that are highly mobile and are very much challenged in the area of security and reliable data communication. MANETs are especially vulnerable to various security threats because they operate on an open wireless medium with no fixed physical structure and infrastructure, thus common threats include malicious node attacks, eavesdropping, and routing misbehaviour. An important issue associated with MANETs and not solved effectively by traditional security measures and routing protocols is the inability to differentiate between friendly and hostile nodes. This gives rise to the need for a Secure Intrusion Detection Routing Protocol with Trust Node Evaluation which has the capability of detecting intrusion and at the same time will only route data through trustworthy nodes thus reducing the effects of malicious behaviour.

2.2. Motivation behind the work

The motivation for this work is the growing utilization of MANETs in important applications such as combat or emergency management, and smart homes and buildings. Since these networks are usually implemented in insecure and dynamic environments, the confidentiality and authenticity of the message must be safeguarded. Current security structures and routing protocols are an insufficient safeguard against internal threats and do not include methods for dynamic evaluation of node behaviour. Therefore, the inclusion of Trust Node Evaluation in the current work has

sought to improve the concurrent infrastructure of MANETs — the Secure IDRP, in order to provide a more robust solution that is capable of combating internal and external attacks, and also optimise the efficiency of the routing protocol in order to promote the establishment of the right social environment for secure communication. Apart from providing assistance in detecting malicious nodes, the establishment of the trust-based security framework is an essential improvement in increasing the reliability and performance of the MANET, making it essential to have improvements for MANET security advancements.

3. Proposed Methodology

The proposed methodology for adaptive trust node routing and intrusion detection in MANETs is geared towards problems arising due to the dynamic nature of MANETs, the decentralized nature of the nodes, their limited energy supply, and susceptibility to security threats. Figure 1 demonstrates the architecture of the MANET for Secure Intrusion Detection Routing Protocol.

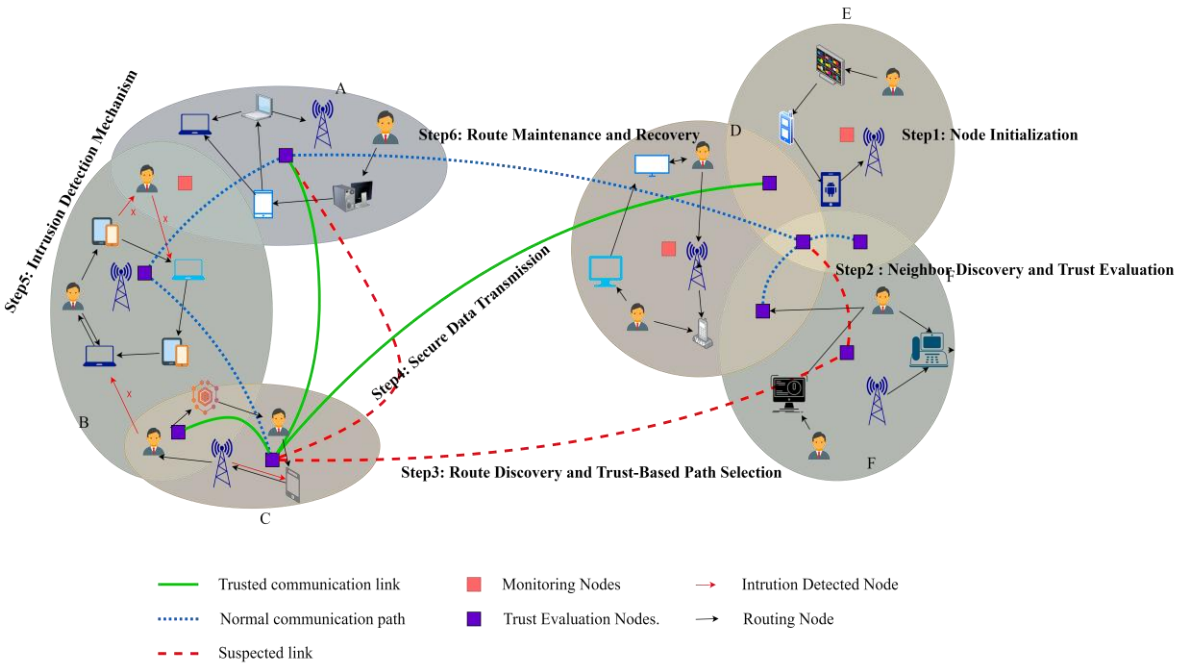


Fig. 1. Architecture of Intrusion Detection Routing Protocol for MANET.

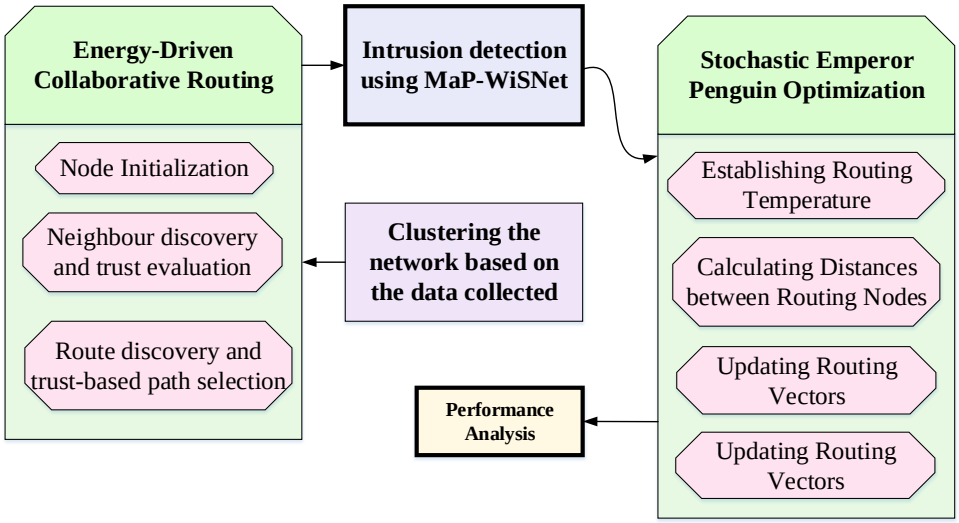


Fig. 2. Workflow of the proposed methodology.

All the nodes in the network go through Energy-Driven Collaborative Routing analysis. In this way the only trusted nodes are included and this improves the overall Security of the network. When the trust nodes are determined,

the method integrates an intrusion detection component which uses the Manifold-Aware Point-wise Steerable Network that is optimized utilizing Stochastic Emperor Penguin Optimization that investigates the network traffic flow and node behaviour. Abnormalities are captured in real-time, while the malicious node is isolated so that it cannot send undesirable data. After identifying the best routes, data is transferred through the chosen secure nodes in a secure and efficient manner.

Figure 2 explains the overall workflow of the proposed methodology.

3.1. Data Collection

In a MANET, the network topology is divided into clusters depending on the data usage and transmission rates. The information gathered in each cluster is used for determining the level of trust between nodes and this aspect is crucial for enhancing Security and reliable communication. This evaluation is done through the means of Energy-Driven Collaborative Routing, which helps the network in selecting and forwarding data through trusted nodes in the network.

3.2. Energy-Driven Collaborative Routing

The collected data within each cluster is then used for trust node evaluation through the Energy-Driven Collaborative Routing (EnerCR) [23] that directs and secures energy-efficient communication in the particular network.

Node Initialization: The node initialization is performed after each mobile node and sink node is deployed in the cluster. Every sink node with ordinary mobile nodes estimates its position as well as distance to neighbour nodes and sinks by RSSI method. Once the distance calculations have been made, all the mobile nodes along with all the sink nodes broadcast a DISCOVERY message in the network. Data transmission starts from the sink nodes, and the first available time slot is reserved for these nodes in the TDMA protocol. This message contains node ID, distances to neighbours, the destination node ID, source node current energy which is the sum of harvested energy and the residual energy, the location of the node, and the transmitted signal power.

Upon receiving the DISCOVERY message, each mobile node strips off the address of the sending node and calculates the path loss between that node and the current node.

The path loss between the receiving node m and the transmitting node n is given by (1),

$$path-loss_{m,n}(dB) = Q_x(dBM) - Q_{y,m,n}(dBm) \tag{1}$$

where $Q_{y,m,n}$ is the power of the received POWER signal at node m and Q_x is the transmitted power.

By this process, both the mobile nodes as well as the sink nodes obtain the information about the neighbouring nodes or the formations of nodes and distances between them and also all the possible routes towards the sink nodes. All the nodes, including the sink nodes, save this information in the local memory to use it later in the EnerCR protocol.

Neighbour discovery and trust evaluation: After the initialization phase, the Neighbour Discovery and Trust Evaluation process is implemented with the information gathered in the previous phase. In every evaluation round, one node that satisfies the predetermined criteria on trust and energy in every clique is chosen for trust evaluation in that clique.

This means that the nodes chosen for neighbour discovery should be placed in areas that have less interference in terms of communication. Furthermore, these nodes should possess the highest obtainable total energy, including both the residual/current energy as well as the harvested energy; the nodes should also route data with minimal energy expense for the entire network. The actual process of trust evaluation and neighbour discovery remains dynamic and is described in the next subsections.

Route discovery and trust-based path selection: For route discovery in MANET using Energy-Driven Collaborative Routing (EnerCR), the sink node, upon receiving REPLY messages from all participating nodes, performs the following computations: it calculates the number of active and inactive nodes in the network, the total current energy $En_{tot-urr}(n)$ of all active nodes, and the transmission power (TxnP) required for nodes to send data to the sink. With these metrics, the sink node determines the Cost Factor for each node as described in (2),

$$CostFactor = \frac{En_{tot-loss}(n)}{En_{tot-curr}(n)} \times TxnP \tag{2}$$

The node with the lowest CF value is selected as the optimal route node for the next routing round. This selection process prioritizes nodes with minimal total network energy loss $En_{tot-loss}(n)$ and maximal total current energy $En_{tot-curr}(n)$. Consequently, the chosen route node is anticipated to execute data transmission and reception with minimal energy depletion, enhancing the overall efficiency of the routing process within the MANET.

Data is transmitted if either of the following conditions is satisfied; otherwise, it is deemed redundant and discarded:

Data Differentiation: That data is said to be transmitted to the trusted route node only if it is not equal to the sensed data stored during the last sensing round.

Critical Data: This data is regarded as valuable, and if it is above or below the target, then it goes to the sink directly.

Definition of Variables and Parameters: Let n denote a mobile node and mmm denote a receiving node in the MANET. Q_x represents the transmitted signal power of node n (in dBm), and $Q_{y,m,n}$ denotes the received signal power at node mmm (in dBm). The path loss between nodes n and m is computed as $path-loss_{m,n}(dB)$.

$E_{res}(n)$ denotes the residual energy of node n, $E_{har}(n)$ represents the harvested energy, and the total current energy is defined as $En_{tot-curr}(n) = E_{res}(n) + E_{har}(n)$.

$En_{tot-curr}(n)$ indicates the total network energy loss associated with node n, while $TxnP$ denotes the transmission power required for node n to forward data to the sink.

The Cost Factor $CF(n)$is a scalar value computed for each node and is used to rank candidate route nodes during path selection.

Algorithm Execution Clarification: During node initialization, all nodes compute neighbour distances using RSSI and store the received DISCOVERY information locally. In the neighbour discovery phase, trust evaluation is performed dynamically at each routing round by selecting nodes that satisfy minimum interference and maximum energy constraints. During route discovery, the sink evaluates all replying nodes by computing $CF(n)$; the node with the minimum Cost Factor is deterministically selected as the trusted routing node for the current transmission round.

Below is the algorithm for the trust node evaluation using Energy-Driven Collaborative Routing (EnerCR)

Algorithm 1. Trust Node Evaluation using EnerCR

Input: Set of mobile nodes N, sink node S, RSSI measurements, initial energy values
Output: Selected trusted routing node

1. Deploy all mobile nodes and sink nodes in the MANET environment.
2. For each node $n \in N$:
   a. Measure RSSI to neighboring nodes and sink.
   b. Compute distances and path loss using Equation (1).
   c. Broadcast a DISCOVERY message containing node ID, neighbor distances, residual energy, harvested energy, location, and transmission power.
3. Upon receiving DISCOVERY messages, each node stores neighbor information in local memory.
4. For each routing round:
   a. Evaluate trust eligibility based on minimal interference, maximal total energy, and energy-efficient routing capability.
   b. Compute the Cost Factor for each node using Equation (2).
5. Select the node with the minimum Cost Factor as the trusted routing node.
6. Forward non-redundant and critical data through the selected trusted node; discard redundant data.

End Algorithm

Through the evaluated trust nodes, the data is transmitted, and the intrusion is detected using the Manifold-Aware Point-wise Steerable Network.

3.3. Manifold-Aware Point-wise Steerable Network

After the trust node is evaluated, the data is transmitted by the use of routing protocol. The intrusion in the network is then detected with the help of the Manifold-Aware Point-wise Steerable Network (MaP-WiSNet) [25-26].

Steerable Convolutional Network: Steerable Convolutional Networks offer a versatile framework for constructing convolutions that are equivariant to a group of transformations in $\Re^m$, denoted as $(\Re^m,+) \circ H \subseteq E(m)$. These groups can be decomposed as a semi-direct product of the translation group $(\Re^m,+)$ and an origin-preserving compact group $H \subseteq E(m)$, where $E(m)$ represents the group of mmm-dimensional rotations and reflections. Since translation equivariance is inherently guaranteed by the convolution operator itself, it is sufficient to ensure equivariance to H.

For intrusion detection, feature spaces are characterized by collections of feature fields. A feature field of type β is a feature map $g: \Re^m \to \Re^m$ equipped with a group representation $\beta: H \to \Re^{e \times e}$ that describes how an element $h \in H$ transforms the feature as (3),

$$[h \cdot g](y) := \beta(h) g(h^{-1} \cdot y) \tag{3}$$

Moreover, each convolutional layer functions as a mapping between feature fields. For this map to be equivariant, it must maintain the transformation properties of its input and output feature fields. Practically, this imposes the following constraint on the space of convolution kernels as (4),

$$\tilde{m}(h \cdot y) = \beta_{out}(h) \tilde{m}(y) \beta_{in}(h)^{-1} \tag{4}$$

where $\tilde{m} : \Re^m \to \Re^{f_{out} \times f_{in}}$ and $\beta_{in} : H \to \Re^{f_{in} \times f_{in}}$ and $\beta_{out} : H \to \Re^{f_{out} \times f_{out}}$ are the respective representations for input and output feature fields, and h represent the group element and y is input coordinate or point in the input space where the feature map is evaluated.

Point-wise Steerable Convolutional Network: For a given group H, the Point-wise Steerable Convolutional Network is structured as (5),

$$\psi = \psi_m \circ \tau_{m-1} \circ \psi_{m-1} \circ \ldots \circ \tau_1 \circ \psi_0 \tag{5}$$

where ψ_m are arbitrary H-representations, $\tau_m : \varpi_m \to \varpi_m$ are non-affine H-equivariant functions and hence $\psi_m \in Aff(\varpi_m, \varpi_{m+1})$.

An activation $\tau : \varpi_m \to \varpi_m$ is point-wise if there exists a basis $B_m = \{u_1, .., u_m\}$ of ϖ_m and a function $\tau' : \Re \to \Re$ expressed as (6),

$$\tau(a_1 u_1 + \ldots + a_m u_m) = \tau'(a_1) u_1 + \ldots + \tau'(a_m) u_m \tag{6}$$

for each $a_1, \ldots, a_m \in \Re$.

For intrusion detection in MANETs using the Manifold-Aware Point-wise Steerable Network, the loss function $Loss$ is defined as (7),

$$Loss(y, \hat{y}) = \frac{1}{M} \sum_{j=1}^{M} loss(y_j, \hat{y}_j) + \lambda \cdot regualization(\Theta) \tag{7}$$

where y_j is the true label for the j-th data instance whereas $\hat{y}_j$ is the predicted label for the j-th data instance. M is the total number of instances and the term $regualization(\Theta)$ penalizes the complexity of the model parameters and λ is a regularization parameter that balances the trade-off between minimizing the loss and controlling the model complexity through regularization.

Explicit Definition of Variables and Network Components: Let H denote a compact symmetry group acting on the input space, where each element $h \in H$ represents a rotation or reflection transformation. The input feature map is defined as $g : \Re^m \to \Re^m$, where m is the spatial dimension and n is the number of feature channels. The group representation $\beta : H \to \Re^{e \times e}$ encodes how feature channels transform under group actions.

In Eq. (3), $y \in \Re^m$ denotes an input coordinate, and the term $g(h^{-1} \cdot y)$ represents the inverse group action applied to the spatial domain. In Eq. (4), $\tilde{m}(\cdot)$ denotes the steerable convolution kernel constrained to satisfy equivariance, while β_{in} and β_{out} represent the group representations associated with the input and output feature fields, respectively.

For the point-wise steerable network, ψ_m denotes the feature field at layer mmm, and $\tau : \varpi_m \to \varpi_m$ represents a non-linear point-wise activation function that preserves group equivariance. The basis $B_m = \{u_1, .., u_m\}$ spans the feature space ϖ_m, and the scalar activation function $\tau'(\cdot)$ is applied independently to each basis coefficient as shown in Eq. (6).

In the loss formulation of Eq. (7), y_j denote the ground-truth and predicted labels of the j th sample, respectively, M is the total number of training samples, and λ controls the regularization strength to prevent overfitting.

Below is the algorithm for the intrusion detection using Manifold-Aware Point-wise Steerable Network

Algorithm 2. Intrusion detection using MaP-WiSNet

Input: Network traffic feature vectors X , labels Y
Output: Intrusion classification result

1. Initialize symmetry group H and define group representations β_{in} , β_{out}
2. Initialize steerable convolution layers with equivariant kernels satisfying Eq. (4)
3. For each training epoch:
   a. For each input sample $x \in X$:
      i. Apply steerable convolution to extract equivariant features
      ii. Apply point-wise activation τ as per Eq. (6)
      iii. Compute predicted output $\hat{y}$
   b. Compute loss using Eq. (7)
   c. Update network parameters using gradient-based optimization
4. During testing, classify each input instance based on the trained network output
5. Label the instance as intrusion or normal

End Algorithm

Fig. 3 shows the inner workings of the suggested Manifold-Aware Point-wise Steerable Network (MaP-WiSNet). The architecture commences with the input traffic and routing feature vectors gathered at the trusted nodes, which are initially mapped into structured feature fields. These feature fields are then processed by a series of steerable convolutional layers that are equivariant to the transformation group H. Each layer extracts the transformation-consistent spatial features and the constraints of group symmetry are maintained. Each feature field is then subjected to point-wise steerable activation functions to enable non-linear modeling without breaking equivariance. The extracted invariant representations are then sent to the classification layer, which decides whether the observed traffic behavior is normal or an intrusion.

After detecting an intrusion, routing decisions are updated and optimized using the Stochastic Emperor Penguin Optimization thus optimizing the network's loss function to improve network security.

3.4. Stochastic Emperor Penguin Optimization

Based on the detected intrusions, routing decisions are adjusted to enhance network security and performance. These adjustments are further optimized using the Stochastic Emperor Penguin Optimization (SEmPO) [24] algorithm, which refines routing paths to avoid compromised areas and improve overall network resilience and efficiency.

The routing boundary is influenced by network traffic patterns and signal strength, which form the basis for the boundary formulation. This boundary can be mathematically expressed using (8),

$$v = s\Delta \tag{8}$$

where v represents the gradient of network signal strength, and Δ refers to the direction of traffic flow influenced by intrusions. A complex potential is created by integrating the signal strength vector c with Δ, as shown in (9),

$$k = \Delta + ic \tag{9}$$

where i denotes the imaginary constant used in the representation of the polygonal boundary in the network plane. From iteration optimization it has been found that the most effective route nodes occur at the centre of the polygon boundary. These nodes adaptively optimize their routing tables to the optimal node depending on the prevailing circumstances within the MANET.

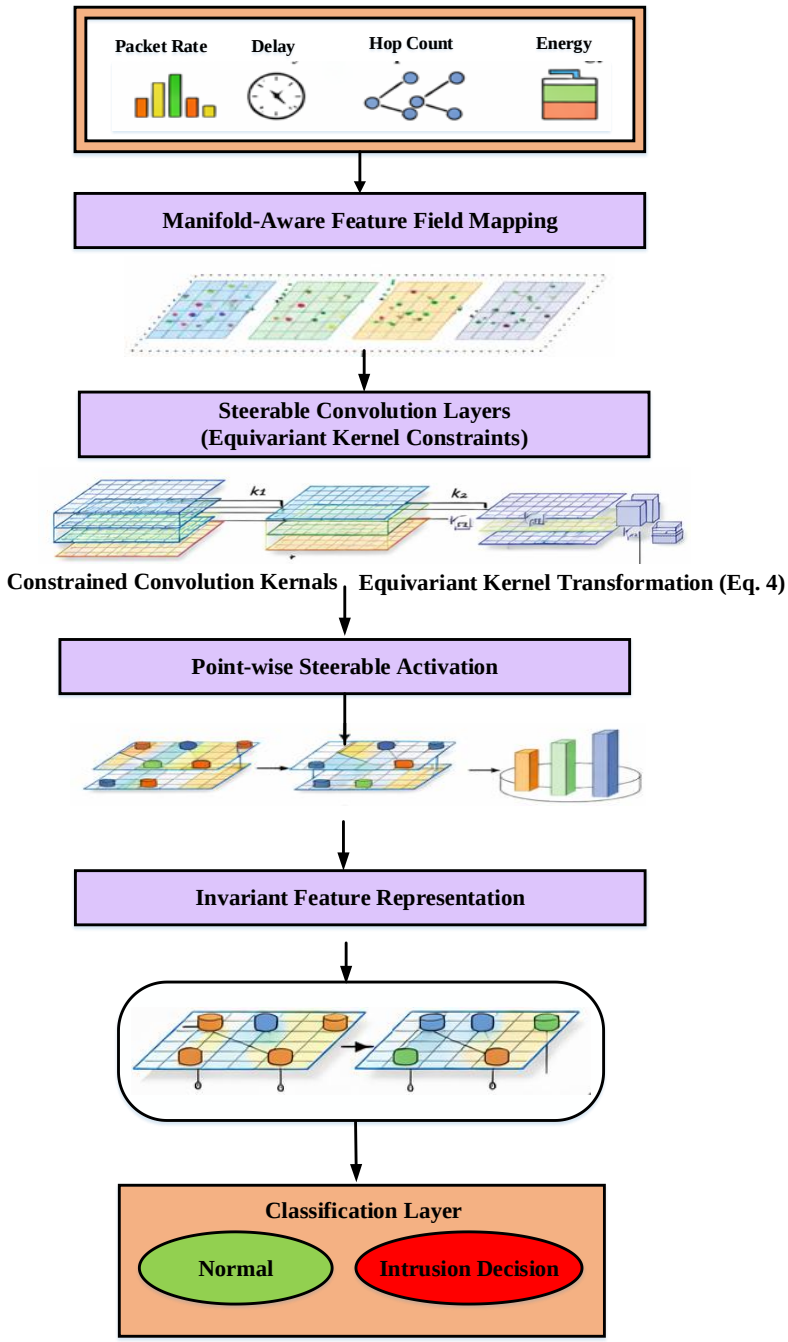


Fig. 3. Internal architecture and data flow of the proposed Manifold-Aware Point-wise Steerable Network (MaP-WiSNet) for intrusion detection in MANETs.

Fitness Function: The fitness function describes how effectively the nodes are routing the traffic while at the same time, preventing intrusion from attacking the network based on aspects such as energy consumed, PDR, and the ability to avoid congested or compromised paths. The objective is to reduce the loss function of the convolutional network. The fitness function can be represented as (10),

$$Fitness(P_{ep}) = \min(Loss) \tag{10}$$

where P_{ep} is the emperor penguin or search agent.

Step 1: Establishing Routing Temperature

In SEmPO applied to MANETs, the radius Q of the coverage area is a key determinant of the routing temperature U . The temperature controls the balance between exploration (seeking new routes) and exploitation (optimizing known routes) after intrusion detection. The routing temperature can be expressed by (11) and (12),

$$U = \begin{cases} 0 & if \quad Q > 1 \\ 1 & if \quad Q < 1 \end{cases} \tag{11}$$

$$U' = U \frac{J_{\max} - Z}{J_{\max}} \tag{12}$$

where $J_{\max}$ represents the maximum number of routing updates (iterations), U is the current temperature variable controlling the network exploration and exploitation, and U' is the updated routing temperature.

Step 2: Calculating Distances between Routing Nodes

After the boundary has been drawn following the intrusion, the distance from a node to the optimal node is then determined. It aims to change the routing decision to reduce the losses (for example, packet loss and energy loss) and make the communication system more efficient. The equation for the distance calculation in MANETs is represented in (13),

$$D_{route} = \left| T(B) - N(y) - D(N_{best}) \right| \tag{13}$$

where D_{route} is the distance between a node and the current best (optimal) solution, $T(B)$ represents the influence of other nodes' traffic (social forces) in making routing decisions, and $N(y)$ and $D(N_{best})$ are vectors that represent the positions of the nodes and their distance from the best node, ensuring that they avoid collisions or interference.

Step 3: Updating Routing Vectors

The vectors B and D that control the routing decisions and avoid network interference (i.e., packet collisions, channel interference) are calculated using (14) and (15),

$$B = \left(L \times \left(U' + N_{grid}(Accuracy) \right) \times D \right) \times U' \tag{14}$$

$$N_{grid}(Accuracy) = \left| N - N_{best} \right| \tag{15}$$

where L is a constant, typically set to 2, and $N_{grid}(Accuracy)$ represents the difference between the current routing position and the optimal node's position within the network. $D = Rand()$ is a random number generator that introduces a degree of randomness to avoid deterministic routing decisions, which could be exploited by intrusions.

Step 4: Updating Node Positions and Routes

The updated positions of the nodes in the MANET, after all iterations, can be calculated using (16),

$$N_{route}(y+1) = N(y) - B \cdot D_{route} \tag{16}$$

At iteration y , $N_{route}(y+1)$ represents the next position of the routing node, updated based on the results of the optimization. This ensures that after each routing update, the network's nodes move closer to the optimal routing configuration, avoiding any intrusion-related disturbances.

Figure 4 details the step-by-step procedure of the Stochastic Emperor Penguin Optimization.

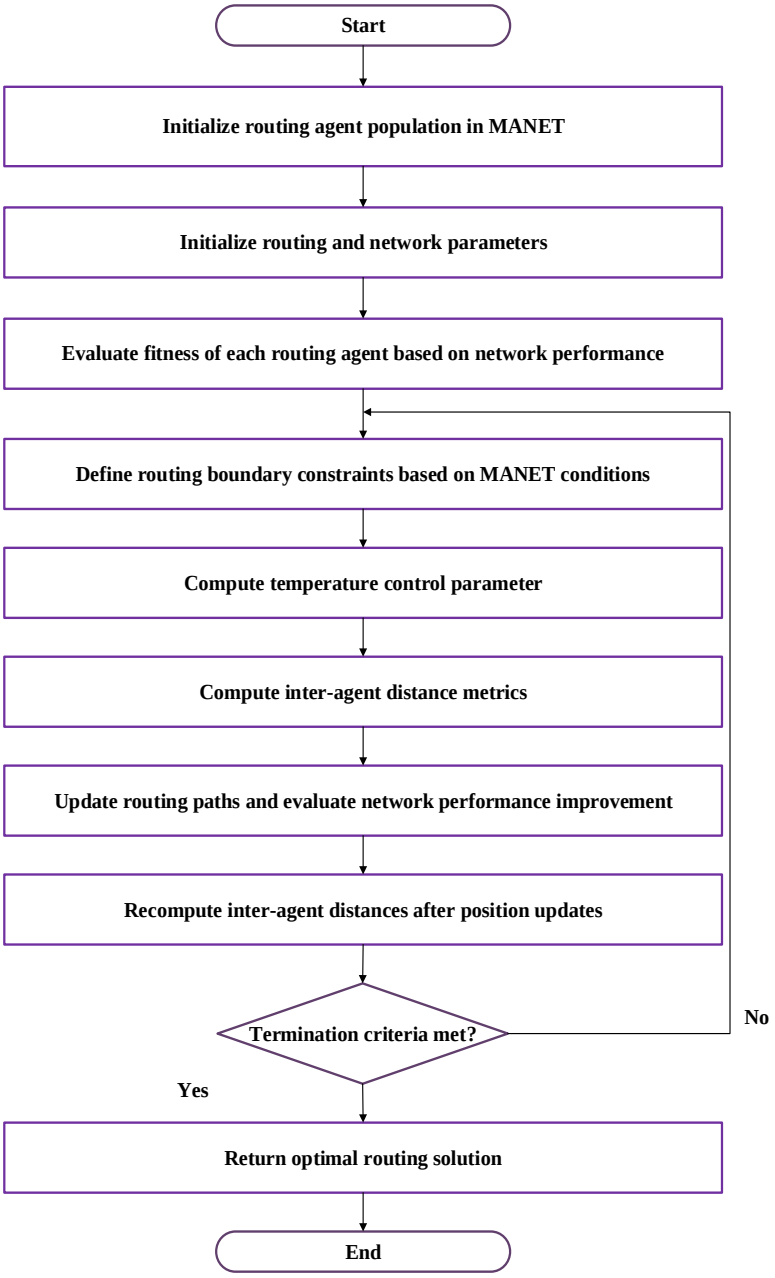


Fig. 4. Step-by-step internal optimization process of the SEmPO algorithm for secure and energy-efficient routing.

Fig. 4 presents a step-by-step procedure for the Stochastic Emperor Penguin Optimization (SEmPO) algorithm when used for optimizing secure routing in MANETs. After intrusion detection, the emperor penguin agent candidate routing nodes are initialized into a dynamically constructed polygonal routing boundary. The algorithm repeatedly recalculates routing temperatures, inter-node distances, and movement vectors to balance exploration and exploitation. Fitness is evaluated at every iteration, taking into account energy consumption, packet delivery efficiency, and intrusion-avoidance capability. Routing positions are adjusted to the global best solution until convergence, at which point an optimal, intrusion-resistant routing path is selected.

Thus the proposed methodology integrates the routing algorithm with intrusion detection network and optimization to enhance the Secure Intrusion Detection Routing Protocol for MANET with Trust Node Evaluation.

4. Results and Discussion

This section provides a detailed analysis of the results and the suggested approach. The method's performance was assessed on the Ubuntu 14.04 platform, proving that it worked there. The NS-3.26 simulator was used to validate it.

The analysis highlights the performance and effectiveness of the proposed method within these testing conditions. Some of the implementation parameters are mentioned in Table 2:

Table 2. Implementation Parameters.

Parameters	Description
No. of user nodes	100
Simulation area	3x3 m^2
No. of packets	~1550
Network Simulator	NS-3.26
Packet Size	512 KB
Simulation Time	10000 sec
OS	Ubuntu 14.04 LTS

Table 2 depicts the basic setup for a network simulation experiment. It involves 100 user nodes (devices) that are spread across a small area of 3x3 m^2. During the simulation, about 1550 packets of data will be sent, with each packet being 512 kilobytes in size. The simulation will run for 10,000 seconds using NS-3.26, a network simulator often used to study and model network behaviour. The operating system running the simulation is Ubuntu 14.04 LTS, a version of the Linux operating system.

4.1. Simulation Setup, Dataset Description, and Reproducibility

The entire experiment described in this paper was conducted using the NS-3.26 network simulator running on an Ubuntu 14.04 LTS environment. The simulator was used to synthetically generate MANET scenarios by setting node density, mobility, traffic load, and attack behaviors based on the implementation parameters shown in Table 2. Traces of network traffic were observed and recorded after simulation runs and used to derive datasets for intrusion detection and routing.

The datasets include node-level and flow-level data, such as packet transmission statistics, route selection, remaining energy, packet delivery results, and intrusion labels. The same features were directly extracted from simulation trace files to ensure compatibility between network behavior and the inputs to learning. All comparative experiments held the same simulation settings and parameter values to ensure fair evaluation.

The entire source code is not publicly available due to institutional and policy limitations. The simulation scripts, configuration files, and data generation procedures may, however, be provided upon reasonable request to verify academic validity and non-commercial research. This makes it transparent and allows independent reproduction of the reported results.

4.2. Performance Analysis

Evaluation parameters play a crucial role in the evaluation of the Adaptive Trust Node Routing via Energy-Aware and Steerable Network with Stochastic Optimization for Augmented Intrusion Detection in MANET Infrastructures. The following metrics provide a detailed insight into the working of the system with respect to secure intrusion detection routing and better performance than other methods.

Table 3. Performance metrics and equation.

Performance metrics	Equation
Accuracy	$A_{cc} = \frac{G_N + H_N}{G_N + H_N + G_A + H_A}$
Recall	$R_{ecall} = \frac{G_N}{G_N + H_A}$
Specificity	$S_{pecificity} = \frac{H_N}{H_N + G_A}$
Precision	$P_{recision} = \frac{G_N}{G_N + G_A}$
F1-Score	$F_{Score} = 2 \times \frac{P_{recision} \times R_{ecall}}{P_{recision} + R_{ecall}}$

4.2.1. Performance metrics

The efficiency of the proposed scheme, Adaptive Trust Node Routing via Energy-Aware and Steerable Network with Stochastic Optimization for Augmented ID in MANET Infrastructures is evaluated with the help of the following performance parameters, which are relevant to the efficiency of the routing scheme and its secure intrusion detection ability. Measurable parameters can encompass the network lifetime, the overall packet delivery ratio, and the resistance

to attacks. Table 3 shows the Performance metrics and equation. These metrics offer a comprehensive analysis of how effective and secure the proposed method is compared to ATOM [16], CGRUN-AGTO [17], DBN-OLSR [18], BAPRP [19], DIWGAN [20], EERE [21] and K-AOMDV [22]. The following is the formulation of performance metrics equations:

- **True Positive: Normal correctly classified as normal.**
- **False Positive: Normal misclassified as abnormal.**
- **False Negative: Abnormal wrongly classified as normal.**
- **True Negative: Abnormal correctly classified as abnormal.**

4.2.1.1. Packet Delivery Ratio (PDR)

The ratio of the number of data packets received at the destination to the number of transmitted packets can be described as PDR. It can be defined as the number of packets that are received over the number of packets sent.

$$PDR = \frac{Total\ \ no.\ of\ \ successful\ \ packet\ \ received}{Total\ \ no.\ of\ \ transmitted\ \ packet}$$

4.2.1.2. Collision Ratio (CR)

Packet Loss Ratio or Collision Ratio (CR) may be defined as the number of MAC collisions or lost packets in the transmission of data to the number of broadcast packets.

$$CR = \frac{Total\ \ packet\ \ transmitted - delivered}{Total\ \ no.\ of\ \ transmitted\ \ packet}$$

4.2.1.3. Average end-to-end delay

Average End to End Delay (EED) is a measure of the average time that the information packets take to travel through the network to the destination. It gives the time spent by the packets that were sent and delivered. One would therefore like to minimize the delay to improve the network performance.

$$Avg\ EED = \frac{Average\ \ time\ \ taken\ \ to\ \ deliver\ \ packet}{Total\ \ no.\ of\ \ delivered\ \ packet}$$

4.2.1.4. Overhead transmission

The connectivity density is characterized by Overhead Transmission (OH). It is the percentage of routing packets in relation to the amount of packets provided in MANET. When the value of OH increases, then this implies a low status of the network and the value of OH decreases showing a high status of the network.

$$OH = \frac{Total\ \ no.\ of\ \ overhead\ \ messages}{Total\ \ no.\ of\ \ transmitted\ \ data\ \ packet}$$

Table 4 presents the performance analysis of the proposed method.

Table 4. Performance Analysis of the proposed method.

Metrics Methods	Routing Overhead (%)	Network Lifetime (%)	Throughput (%)	Transmission Speed (%)	Packet Transmission (%)	Energy Consumption (%)
ATOM [16]	65.2	81.80	70.96	84.35	85.21	78.52
CGRUN- AGTO [17]	69.36	84.23	76.31	86.37	86.39	78.94
DBN-OLSR [18]	75.21	73.57	84.37	89.41	87.16	87.39
BAPRP [19]	78.14	78.05	88.81	94.39	89.97	84.29
DIWGAN [20]	86.87	81.37	89.97	93.08	92.47	91.57
EERE [21]	89.75	85.45	93.27	95.61	95.61	93.6
K-AOMDV [22]	91.54	90.65	65.61	96.66	96.48	94.8
Proposed	94	93.2	96.74	97.86	97.23	95.19

Table 4 compares several methods used in network simulations based on key performance metrics such as Routing Overhead, Network Lifetime, Throughput, Transmission Speed, Packet Transmission, and Energy Consumption. Among the methods, our proposed approach stands out as the best performer across all categories. It has a Routing Overhead of 94%, meaning it manages network resources efficiently, and the highest Network Lifetime at 93.2%, ensuring the network operates longer. Additionally, it achieves the best data transfer rate (Throughput) at 96.74% and offers the fastest Transmission Speed at 97.86%. In terms of Packet Transmission, the proposed scheme successfully transmits 97.23% of packets, outperforming all others. Lastly, its energy efficiency is 95.19%. These results clearly show that the proposed technique provides superior performance and efficiency compared to the other methods.

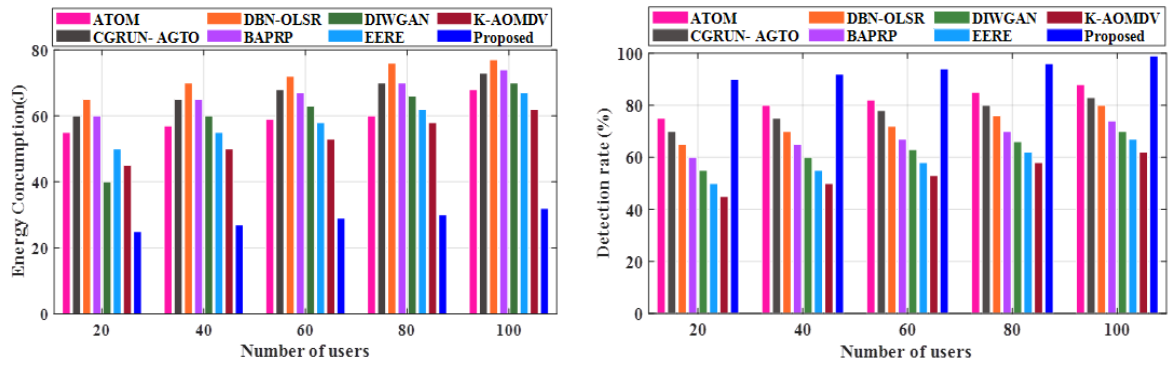


Fig. 4. Analysis of (a) Energy Consumption and (b) Detection rate.

Figure 4 compares different systems based on energy consumption and detection rate for various user counts. In the analysis of energy consumption, our proposed method achieves 95.19% energy efficiency and maintains a high detection rate of 96.5% across all user numbers. Other systems show lower values, especially as the number of users increases. This makes the proposed system the best choice for energy efficiency and detection rate, ensuring optimal performance under varying conditions.

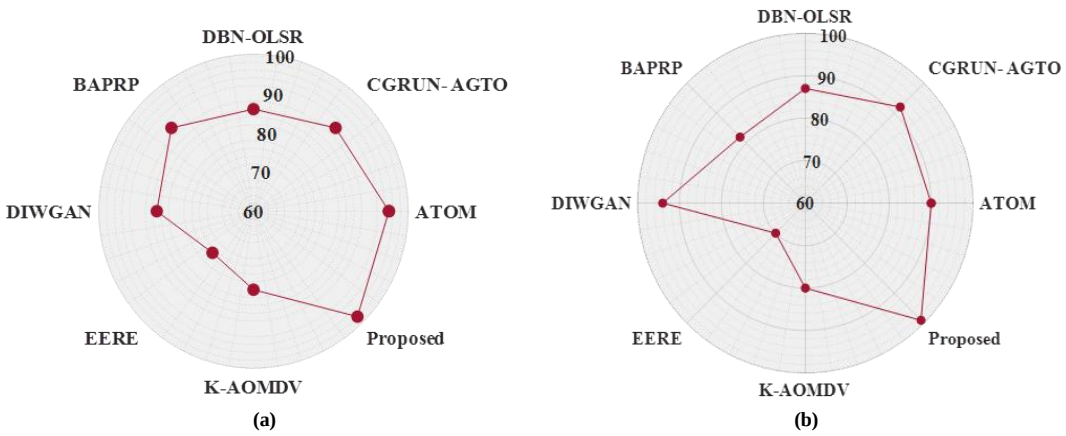


Fig. 5. Evaluation of (a) Packet Transmission and (b) Throughput.

The figure 5 evaluates the performance of different algorithms in terms of packet transmission (a) and throughput (b). In the packet transmission graph (a), the proposed method achieves approximately 97%. In the throughput graph (b), compared with other existing methods, our research accomplishes the best score of 96.74%, surpassing ATOM and K-AOMDV, which are close to 70 and 60, respectively. Through the evaluation of packet transmission and the throughput, we can conclude that our proposed method performs best when compared to other methods.

Figure 6 shows the performance of different algorithms in terms of network lifetime (a) and transmission speed (b). For network lifetime, the proposed system achieves the highest score of 93.2%. Other algorithms like CGRUN-AGTO and ATOM perform moderately, scoring near 80. In transmission speed, our method scores around 97.86%, surpassing all other methods, showing the superiority of the proposed method in comparison to other existing methods.

Figure 7 shows the evaluation of PDR (a) and intrusion detection (b). Figure 7(a) tracks how well various protocols deliver data over time. Our method has a PDR of 92.8%. Figure 7(b) compares a regular security system (Normal IDS) with a new, proposed system. The proposed system performs better in detecting attacks and other important factors like

accuracy, showing an improvement over the normal system. This proves that our proposed method is more efficient than all other methods.

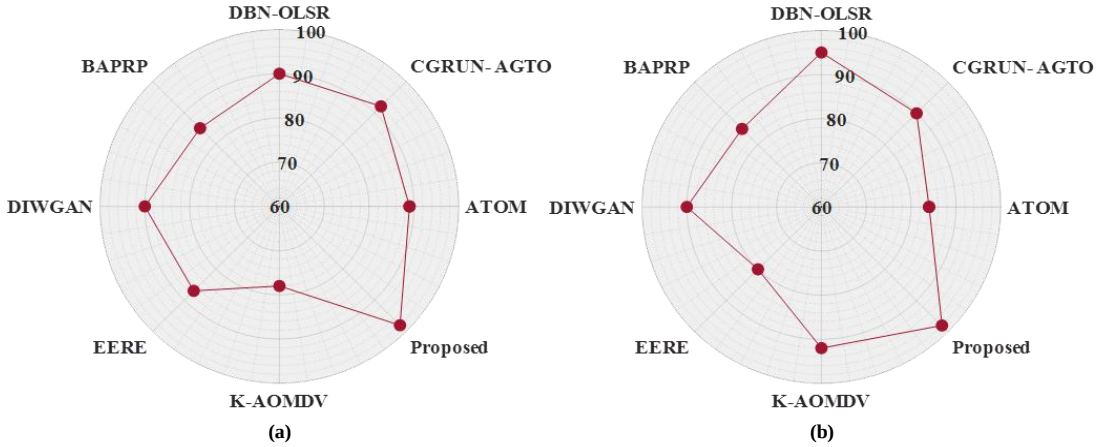


Fig. 6. Evaluation of (a) Network Lifetime and (b) Transmission Speed.

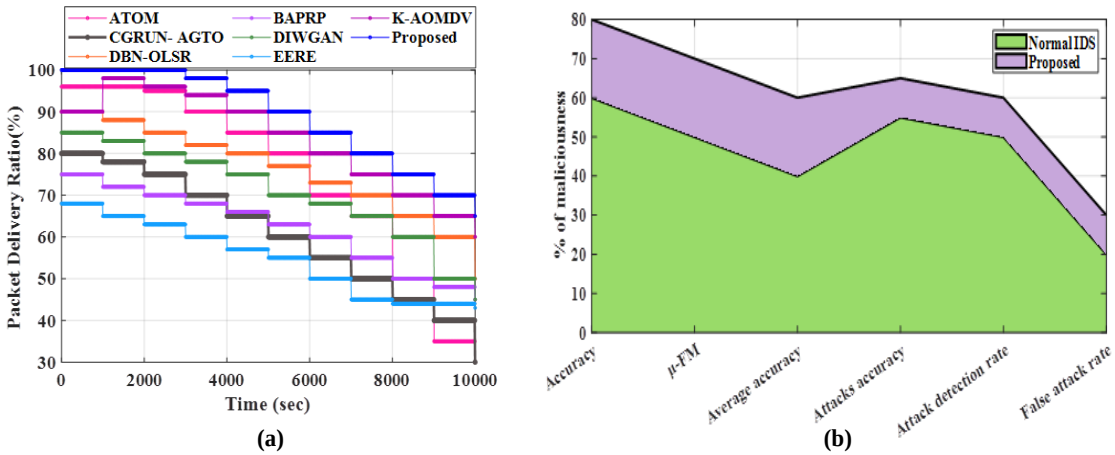


Fig. 7. Analysis of (a) PDR and (b) Intrusion detection**.**

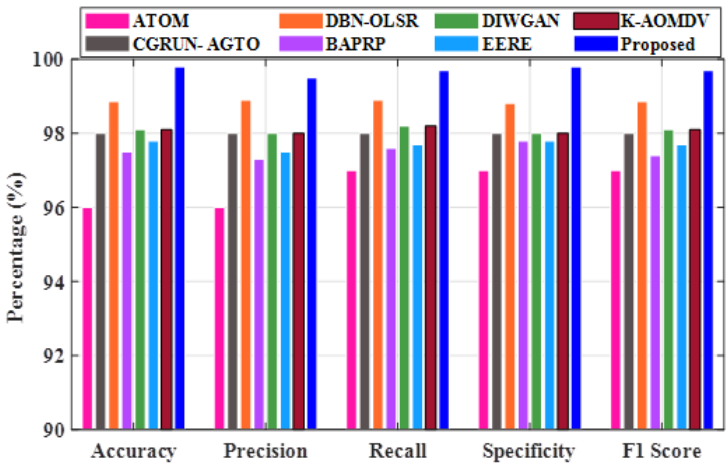


Fig. 8. Performance comparison with existing methods.

Figure 8 compares various systems across metrics. The proposed system outperforms all others, with values consistently above 95%. It achieves 96.5% accuracy, 95.5% precision, 96.8% recall, 95.7% specificity, and 96.2% F1

score. Other protocols fall below these values, making the proposed method the best-performing one across all metrics, showing the highest effectiveness in each category.

Table 5. Comparison with Recent AI-Based and Blockchain-Integrated MANET Intrusion Detection Protocols.

Method	Core Technique	Blockchain Integration	Detection Accuracy (%)	PDR (%)	Energy Efficiency (%)
ATOM [16]	Trust-based routing	No	88.21	86.75	87.10
CGRUN-AGTO [17]	Deep RNN + Optimization	No	89.64	88.92	89.03
DBN-OLSR [18]	Deep Belief Network	No	90.12	89.45	90.26
BAPRP [19]	Blockchain-assisted routing	Yes	91.08	90.73	91.11
DIWGAN [20]	GAN-based IDS	No	91.96	91.64	92.03
EERE [21]	Energy-aware DL routing	No	92.14	92.01	92.48
K-AOMDV [22]	AI-enhanced multipath routing	No	92.36	92.21	92.74
Proposed Method	MaP-WiSNet + EnerCR + SEmPO	Implicit trust (no ledger overhead)	96.50	92.80	95.19

Table 5 shows the comparative performance results. The suggested solution offers consistently high detection accuracy, energy efficiency, and reliable packet delivery. In contrast to approaches based on blockchain that might incur additional communication and computation costs, the given framework combines trust assessment, intrusion detection, and optimization through a closely interrelated architecture, enabling effective security enforcement without overloading resources. In addition, manifold-aware equivariant feature learning combined with stochastic optimization enables the model to generalize effectively in settings with high node mobility and adversarial conditions.

Table 6. Statistical significance comparison of proposed method with existing approaches.

Method	Accuracy (%) Mean ± SD	PDR (%) Mean ± SD	Energy Efficiency (%) Mean ± SD	p-value vs Proposed	Significance
ATOM [16]	88.21 ±1.34	86.75 ±1.51	87.10 ±1.29	< 0.001	Significant
CGRUN-AGTO [17]	89.64 ±1.21	88.92 ±1.36	89.03 ±1.18	< 0.001	Significant
DBN-OLSR [18]	90.12 ±1.17	89.45 ±1.28	90.26 ±1.14	< 0.001	Significant
BAPRP [19]	91.08 ±1.09	90.73 ±1.22	91.11 ±1.06	< 0.001	Significant
DIWGAN [20]	91.96 ±1.02	91.64 ±1.18	92.03 ±1.01	0.002	Significant
EERE [21]	92.14 ±0.97	92.01 ±1.05	92.48 ±0.95	0.004	Significant
K-AOMDV [22]	92.36 ±0.93	92.21 ±1.02	92.74 ±0.91	0.006	Significant
Proposed Method	96.50 ±0.61	92.80 ±0.74	95.19 ±0.58	–	–

To statistically demonstrate the performance enhancements, a paired two-tailed Student t-test was performed between the proposed method and each baseline method, using the metric values obtained under the same simulation parameters across 10 independent simulation runs. The null hypothesis is that there exists no statistically significant difference between the compared methods. The level of significance is 0.05 (alpha = 0.05). Table 6 indicates that the p-values for all baseline methods are less than 0.05, which shows that the advantages offered by the proposed method in accuracy, packet delivery ratio, and energy consumption are not due to random chance. The given standard deviations indicate the variation across independent simulation runs.

Table 7. Ablation study.

Performance metrics Methods	IDS Efficiency (%)	Routing Success Rate (%)	Routing Latency (sec)
Steerable Convolution Network	93.12	92.78	2.35
MaP-WiSNet with SEmPO	95.58	95.22	1.04
MaP-WiSNet-SEmPO with EnerCR	96.5	97.8	0.6

Table 7 compares the performance of three methods in terms of IDS efficiency, routing success rate, and routing latency. The Steerable Convolution Network shows good performance with 93.12% IDS efficiency and a 92.78% success rate, but its latency is relatively high at 2.35 seconds. The MaP-WiSNet with SEmPO improves these metrics, achieving 95.58% efficiency, a 95.22% success rate, and reducing latency to 1.04 seconds. The best performance comes from MaP-WiSNet-SEmPO with EnerCR, with 96.5% efficiency, a 97.8% success rate, and the lowest latency of 0.6 seconds. In all performance metrics, our proposed method consistently outperforms existing techniques, demonstrating superior accuracy, efficiency, and robustness. The protocol demonstrates superior detection accuracy, effectively identifying malicious nodes with minimal false positives. Additionally, it ensures enhanced network stability and reliability through trust-based evaluations, significantly reducing packet loss and delay. Compared to conventional routing protocols, our solution offers improved Security and robustness against various attack vectors. Overall, it provides a comprehensive and efficient defense mechanism for mobile ad hoc networks.

5. Conclusion

The proposed adaptive routing framework for MANETs demonstrated significant improvements in both security and energy efficiency through extensive simulation using NS-3.26. The use of a trust-based evaluation mechanism within the network has helped in minimizing the intrusions while maintaining the quality of network performance. The use of the dynamic node steering network and optimization techniques facilitated the development of efficient IDS for intrusion detection in the resource-constrained environment and the ability to maintain the network node life cycle while achieving a high detection rate of the malicious activities. Simulation results demonstrated an increase in the accuracy of detection, energy savings, and efficient routing, which proved the effectiveness of the proposed solution. The stability of the framework was also checked under different network conditions and proved to be useful for real-life settings in MANET infrastructures.

Further studies will be devoted to considering the generalization of the framework for more complicated attack scenarios and studying its effectiveness in the heterogeneous MANETs with different mobility characteristics. Moreover, the real-world application and validation in larger-scale networks will be carried out.

All the Declarations and Statements

Author Contributions Statement

Mehaboob Mujawar – Conceptualization, Methodology, and Supervision: Proposed research ideas, Constructed the overall framework, and supervised project execution.
R. Mohandas – Data Curation and Software Implementation: Handled data acquisition, dataset preprocessing, and implementing the research model.
R. Giri Prasad – Model Training, Validation, and Performance Evaluation: Led the model training process, validated results using standard metrics, and benchmarked performance against existing methods.
K. Narasimha Raju – Formal Analysis, Visualization, and Statistical Analysis: Performed in-depth analysis of experimental results, prepared performance charts, and ensured the statistical robustness of the evaluation.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research was supported by the grant “Project Number” “Project Full Name”.

Data Availability Statement

This study analyzed datasets generated from simulation traces. The simulation scripts, configuration files, and derived datasets may be provided upon reasonable request to verify academic validity.

Ethical Declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

AI tools were used only for minor grammar checking and language refinement. All methodological development, analysis, and technical content were entirely carried out by the authors without AI assistance.

Abbreviations

The following abbreviations are used in this manuscript:

ATOM - Analytical termination of malicious nodes
EERE - Energy Efficient Routing Establishment
EnerCR Energy-Driven Collaborative Routing
GAN - Generative Adversarial Network
MANETs - Mobile Ad-Hoc Networks

MaP-WiSNet - Manifold-Aware Point-wise Steerable Network
PDR - Packet Delivery Ratio
SEmPO - Stochastic Emperor Penguin Optimization
TxnP - Transmission Power
WP-FPA - Whale Positioning scheme with Flower Pollination Algorithm

Appendix

None.

References

[1] S.S.M. Vincent, and N. Duraipandian, Detection and prevention of sinkhole attacks in MANETS based routing protocol using hybrid AdaBoost-Random forest algorithm. *Expert Systems with Applications*, 249, p.123765, 2024.

[2] P. Aruchamy, S. Gnanaselvi, D. Sowndarya, and P. Naveenkumar, An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 35(23), p.e7818, 2023.

[3] B. Sharma, and D. Saxena, Design and Analysis of Energy Efficient Service Discovery Routing Protocol in MANETs. *SN Computer Science*, 4(5), p.495, 2023.

[4] S. Shafi, S. Mounika, and S.J.P.C.S. Velliangiri, Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. *Procedia Computer Science*, 218, pp.2309-2318, 2023.

[5] R. Sathiya, and N. Yuvaraj, Swarm Optimized Differential Evolution and Probabilistic Extreme Learning based Intrusion Detection in MANET. *Computers & Security*, p.103970, 2024.

[6] R. Prasad, Secure intrusion detection system routing protocol for mobile ad-hoc network. *Global Transitions Proceedings*, 3(2), pp.399-411, 2022.

[7] N. Ilakkiya, and A. Rajaram, Blockchain-enabled lightweight intrusion detection system for secure MANETs. *Journal of Electrical Engineering & Technology*, 19(4), pp.2667-2681, 2024.

[8] S.M. Hassan, M.M. Mohamad, and F.B. Muchtar, Advanced Intrusion Detection in MANETs: A Survey of Machine Learning and Optimization Techniques for Mitigating Black/Gray Hole Attacks. *IEEE Access*. 2024.

[9] A.A. Alyoubi, Enhancing Data Security in Mobile Ad-hoc Network (MANETs) Using Trust-Based Approach with RSSI and Fuzzy Logic. *Mobile Networks and Applications*, pp.1-17, 2024.

[10] M.S. Gowtham, M. Vigenesh, and M. Ramkumar, An artificial immune system-based algorithm for selfish node detection in Mobile Ad Hoc Networks (MANETs). *Transactions on Emerging Telecommunications Technologies*, 35(2), p.e4938, 2024.

[11] R. Chakravorty, J. Prakash, and A. Srivastava, An efficacious neural network and DNA cryptography-based algorithm for preventing black hole attacks in MANET. *Soft Computing*, 28(5), pp.4667-4679, 2024.

[12] M. Deivakani, M.S. Sheela, K. Priyadarsini, and Y. Farhaoui, An intelligent security mechanism in mobile Ad-Hoc networks using precision probability genetic algorithms (PPGA) and deep learning technique (Stacked LSTM). *Sustainable Computing: Informatics and Systems*, 43, p.101021, 2024.

[13] J. Ryu, and S. Kim, Trust system-and multiple verification technique-based method for detecting wormhole attacks in MANETs. *IEEE Access*, 2024.

[14] I. Baird, I. Wadhaj, B. Ghaleb, and C. Thomson, Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs). *Electronics*, 13(16), p.3314, 2024.

[15] S. Rajasoundaran, S.S. Kumar, M. Selvi, K. Thangaramya, and K. Arputharaj, Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. *Wireless Networks*, 30(1), pp.209-231, 2024.

[16] S. Sivanesh, and V.R. Sarma Dhulipala, Analytical termination of malicious nodes (ATOM): an intrusion detection system for detecting black hole attack in mobile ad hoc networks. *Wireless Personal Communications*, pp.1-14, 2022.

[17] S. Selvaraj, and M. Chakkaravarthy, Enhancing Security and efficiency in MANETs: a clustering-based approach with CGRUN and AGTO optimization for intrusion detection and path establishment. *International Journal of Information Technology*, pp.1-11, 2024.

[18] S. Shafi, and D. Venkata Ratnam, New Energy Aware MPR Selection for Securing OLSR Routing Scheme Under Black Hole Attack: A Machine Learning Approach. *Wireless Personal Communications*, 132(3), pp.1917-1931, 2023.

[19] N.T. Luong, and D. Hoang, BAPRP: a machine learning approach to blackhole attacks prevention routing protocol in vehicular Ad Hoc networks. *International Journal of Information Security*, 22(6), pp.1547-1566, 2023.

[20] B. Krishnasamy, L. Muthaiah, J.E. Kamali Pushparaj, and P.S. Pandey, DIWGAN optimized with Namib Beetle Optimization Algorithm for intrusion detection in mobile ad hoc networks. *IETE Journal of Research*, pp.1-20, 2023.

[21] V.A. Devi, V. Ganesan, and V.S.A. Padmini, An Energy Efficient Routing Establishment (EERE) Mechanism for MANET-IoT Security. *Franklin Open*, p.100150, 2024.

[22] S. Kaushik, K. Tripathi, R. Gupta, and P. Mahajan, Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks. *SN Computer Science*, 5(2), p.263, 2024.

[23] H.L. Gururaj, R. Natarajan, N.A. Almujally, F. Flammini, S. Krishna, and S.K. Gupta, Collaborative energy-efficient routing protocol for sustainable communication in 5G/6G wireless sensor networks. *IEEE Open Journal of the Communications Society*. 2023.

[24] O.W. Khalid, N.A.M. Isa, and H.A.M. Sakim, Emperor penguin optimizer: A comprehensive review based on state-of-the-art meta-heuristic algorithms. *Alexandria Engineering Journal*, 63, pp.487-526, 2023.

[25] L. Veefkind, and G. Cesa, A Probabilistic Approach to Learning the Degree of Equivariance in Steerable CNNs. *arXiv preprint arXiv*:2406.03946. 2024.
[26] L.K. Singh, M. Khanna, H. Garg, and R. Singh, Emperor penguin optimization algorithm-and bacterial foraging optimization algorithm-based novel feature selection approach for glaucoma classification from fundus images. *Soft Computing*, 28(3), pp.2431-2467, 2024.

Authors' Profiles



Mehaboob Mujawar is currently working as an Associate Professor and Head of the Department in the Department of Artificial intelligence and Data Science at Bearys Institute of Technology, Mangalore, Mangaluru, Karnataka 574199, India. He haspublised many research papers. His area of interst is Data Analysis, Artificial intelligence techniques and Data secutity.



R. Mohandas currently working as a Professor in the Department of ECE, at Chennai Institute of Technology, Chennai, Tamil Nadu, India. He has been worked as a system admin at eDeveloper HR Sciences from 3008 to 2024. His research are includes telecommunication technologies, Machine learning and artificial intelligence techques.



R. Giri Prasad received B.Tech Degree in Mining from GATE College of Engineering, Kodhada affiliated to JNTU, Hyderabad. M.Tech Degree in Mining Engineering from KITS Ramachandrapuram affiliated to JNTU, Kakinda. M.Tech Degree in Petroleum Exploration from Andhra University. Ph.D Earth Science from SV University Tirupathi. Present working as Associate Professor in Petroleum Technology Dept. and Associate Dean Admissions, Aditya University, Surampalem. Kakinada District, Andhra Pradesh, INDIA. His research interests include Data Communication Networking, Application of AI in Mining and Petroleum Industry.



K. Narasimha Raju received B.Tech degree in CSE from MVGR college of Engineering, Vizianagaram affiliated to JNTU, Hyderabad, Andhra Pradesh in 2004 and M.Tech Degree in Computer Science and systems engineering from Andhra University, Visakhapatnam, Andhra Pradesh in 2010. He received Ph.D. degree at the Department of Computer Science and systems engineering, Andhra University, Andhra Pradesh, India. His research interests include soft computing, Artificial Intelligence and Computer Networks.

How to cite this paper:

Mehaboob Mujawar, R. Mohandas, R. Giri Prasad, K. Narasimha Raju, "Adaptive Trust Node Routing via Energy-Aware and Steerable Network with Stochastic Optimization for Augmented Intrusion Detection in MANET Infrastructures", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.3, pp. 221-239, 2026. DOI:10.5815/ijcnis.2026.03.12