FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

STAGNet-COpt: A Spatio-Temporal Attention Graph Network with Cluster-based Optimized Trust Routing for MANET Security

Manbir Kaur Brar[1,3*], Sukhpreet Singh[2], and Sajjan Singh[3]

[1]*ECE Department, Chandigarh University, Mohali, Punjab, India; manbirbrar90@gmail.com*
[2]*ECE Department, Chandigarh University, Mohali, Punjab, India; sukhpreet.ece@cumail.in*
[3]*ECE Department, Chandigarh Engineering College, Chandigarh Group of Colleges Jhanjeri-140307, Mohali, Punjab, India; sajjantech@gmail.com*

***Correspondence:** *Manbir Kaur Brar; manbirbrar90@gmail.com*

ABSTRACT- Mobile Ad Hoc Networks are highly dynamic and infrastructure-less environments that are inherently vulnerable to a range of routing-based attacks. To address the limitations of traditional defense mechanisms, this paper proposes STAGNet-COpt, a novel spatio-temporal trust-aware defense framework that integrates deep learning-based attack detection, fuzzy clustering, and hybrid meta-heuristic routing optimization. The detection component, STAGNet, leverages Graph Attention Networks in combination with Long Short-Term Memory networks to capture both the topological dependencies and temporal behavior of nodes for accurate intrusion detection. To enhance routing security and efficiency, TrustFuzz employs fuzzy logic for trust-aware clustering, while WOACO-R, a hybrid of Whale Optimization Algorithm and Ant Colony Optimization, is utilized for adaptive and trustworthy route selection. The framework is evaluated using NS-2 simulations under diverse attack scenarios, including blackhole, wormhole, grayhole, denial-of-service, and integrated attacks, across varying node densities. Results show that STAGNet-COpt achieves an average Packet Delivery Ratio of 94.05%, packet loss of 5.45%, throughput of 119.5 kbps, end-to-end delay of 3.63 ms, and routing overhead of 325.25, significantly outperforming existing benchmarks. The proposed model demonstrates high scalability, detection accuracy, and resilience, establishing a robust and intelligent solution for secure MANET communication.

Keywords: MANETs, Security, Integrated Attacks, Deep Learning, Optimization, Trust.

ARTICLE INFORMATION

Author(s): Manbir Kaur Brar, Sukhpreet Singh, and Sajjan Singh;
Received: 08/11/2025; **Accepted**: 02/03/2026; **Published**: 30/03/2026;
E- ISSN: 2347-470X;
Paper Id: IJEER0811A04
Citation: 10.37391/ijeer.140124
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-14/ijeer-140124.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Digitalization is empowering the modern world by connecting people, devices, systems, etc. and transforming information sharing, decision making, and many other services. Mobile Adhoc Networks (MANETs) are the heart of these transformations and provide flexible and infrastructure-independent communication [1]. The use of MANET, also called a self-configuring network of mobile nodes, is rapidly growing owing to the dynamic environment. These networks have shown their relevance in mission-critical applications, including military, disaster recovery, automobiles, and healthcare. The decentralized network architecture of MANET offers rapid deployment, scalability, flexibility, etc. However, there are some significant challenges, such as limited bandwidth, energy, topology changes, and security threats, because of which sometimes failures happen [2]. Therefore, MANET still demanded intelligent and adaptive solutions for such problems in order to improve the performance of the network.

Security in MANETs is a crucial problem owing to the decentralized and dynamic nature of the network. Unlike traditional networks, MANETs operate in an open and hostile environment and are highly vulnerable to various threats [3]. The network faces difficulty in ensuring confidentiality, authentication, integration, etc., as nodes frequently join and leave the network and also rely on neighbor nodes for data transmission. Limited computational resources and the absence of centralized control also make it a tough task for implementing robust security or cryptography algorithms across different network nodes [4]. This additionally creates opportunities for intruders such as blackhole, wormholes, etc. to severely disrupt the network traffic, compromise sensitive data, and degrade its overall performance.

Researchers have proposed several security solutions for MANETs that include cryptography algorithms, routing protocols, and trust-based frameworks [5] [6]. Cryptography methods such as encryption and digital signatures ensure data authentication and confidentiality, whereas security protocols protect transfer routes from manipulation. Trust-based approaches have also been adopted in the past few years, which evaluate the nodes' behaviour and mitigate various threats. Despite these solutions, MANET is highly struggling for security owing to its highly dynamic nature, limited resource constraints, overhead, etc. Recently, Artificial intelligence (AI)

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

and Machine learning (ML) have emerged as promising solutions that enable the detection and classification of attacks such as blackhole, wormhole, etc. These methods analyze node behaviour and network patterns to identify the potential threats and anomalies [7]. However, the challenges related to the dataset, noise, complexity, etc., make the security system difficult to improve network performance in some cases. To overcome these challenges, there is a growing need for adaptive, lightweight, and context-aware AI models specifically designed for the highly dynamic and decentralized nature of MANETs.

With the aim of enhancing the level of security in MANETs, this research study proposes a novel STAGNet-COpt, A Spatio-Temporal Attention Graph Network with Cluster-based Optimized Trust Routing, which provides overall security by implementing both detection and prevention systems. In terms of this, the contribution of this paper is as follows:

- STAGNet: A new spatio-temporal graph attention network that combines the graph attention networks (GAT) with long-short-term-memory (LSTM) networks in order to enhance the performance of the detection and classification system.
- TrustFuzz: A fuzzy-based trust-aware clustering approach for distributing MANET nodes into dynamic clusters.
- WOACO-R: An energy and security aware routing protocol in MANET based on hybrid whale optimization (WOA) and ant colony optimization (ACO) algorithms.
- Self-generated dataset: A large-scale dataset based on simulations under different network scenarios, such as varying nodes, attackers, etc., is created and then labeled manually with respect to their respective attack.
- Evaluations and Comparisons: The proposed architecture is evaluated using a self-generated dataset and compared with different existing state-of-the-art (SOTA) approaches.

The rest of the paper is organized as follows. *Section 2* detailed review of existing security approaches and highlights the key challenges. *Section 3* introduces the proposed methodology for both the detection and prevention systems. *Section 4* covers all the experimentation and results-related aspects. *Section 5* concludes the work and outlines potential directions for future research.

2. RELATED WORK

Over the past decade, a significant security solution has been proposed for enhancing MANETs' security, including cryptography, trust-based, secure routing, and AI-based approaches. This section presents a comprehensive review of existing solutions, highlighting their strengths and limitations.

2.1.Route Selection and Data Encryption based security Methods

A distributed blockchain-based method recently assisted the MANETs' communication over zones. In this study, a neuro-fuzzy inference approach was first implemented to form secure network clusters and elliptic curve cryptography (ECC) was used for authentication and data encryption [8]. This proposed method, though, secures the network for data transmission. However, a blockchain requires significant computational resources, and combining it with multi-step encryption, blockchain verification, etc., may increase the latency. An improved Elephant Herd Optimization (IEHO) with blockchain introduces a security level in MANETs' communication. The computational overhead and risk of premature convergence may affect the performance of the network [8]. The blockchain integration with homomorphic encryption also improves the packet delivery rate (PDR) of the MANETs in the presence of attacks [9]. This integration increases cumulative resource demands and can also raise scalability issues. The zone-based clustering with reinforcement learning based cluster head selection improves the cluster formation in order to enhance security. Additionally, quantum-resistant cryptography, deep learning-based trustworthiness, and lightweight encryption enhance security and improve the PDR. A hybrid genetic algorithm (GA) and particle swarm optimization (PSO) was designed to reduce energy consumption while maintaining security in this study [10]. An optimization-based trust approach was introduced in [11] integrates cat-swarm and sparrow search optimization. This integration potentially led to unstable convergence and can deteriorate the overall performance of the network.

The density-based adaptive soft clustering with Elk-herd optimization (EHO) for cluster head formation, multi-attributed trust computation, and adaptive snow geese optimization (ASGO) for route optimization together form a secure communication in the dynamic environments of MANETs [12]. A Hierarchical Manta Ray Foraging Optimization Algorithm (HMRFOA) was also used for selecting a trust-aware path in order to secure the data transmission [13]. The Red Panda Optimization (RPO) and Lyrebird Optimization Algorithm (LOA) algorithms were designed to select the cluster heads and optimize routing based on delay, distance, link quality, and energy to make the network trustworthy [14]. The Hybrid Swallow Swarm Optimisation-Memetic Algorithm also performs better than existing route optimization algorithms [15]. A Coot chimp optimization algorithm (CCOA) was designed with parameters energy, distance, neighborhood quality, link quality, and trust in order to enhance network communication [16]. A Hybrid Tasmanian Gazelle Optimization (HTGO) with a fuzzy-based trust evaluation approach was designed to enhance the attacker node detection in MANETs [17]. With graph clustering, an artificial rabbit optimization (ARO) prioritizes secure and energy-efficient routing that enhances the overall performance of network communication [18].

A cryptography algorithm, AES, is enhanced with adaptive chaotic grey wolf optimization, and route selection based on fuzzy butterfly optimization enhances and secures the data during network communication [19]. Federated Learning Long Short-Term Memory (LSTM) Trust-aware Location-aided Routing approach was designed for trust prediction and routing decisions in MANETs [20]. Clustering, a hybrid routing

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

protocol, and hybrid cryptography guarantee the appropriate, secure, and accurate delivery of packets. However, it increases the network overhead due to high computational requirements [21]. Several different optimization approaches, such as hybrid Osprey and Fire Hawk Optimization [22], Refined Adaptive Harris Hawks Optimization Algorithm (RAHHO) [23], Artificial Gorilla Troops Optimizer [24], Hybrid ACO and whale optimization [25], Philippine eagle (PE) optimization [26], Guided WOA [27] and many other optimizations are incorporated in MANET routing with different parameters such as security, trust, energy, etc. and enhance the overall data transmission between nodes. However, their effectiveness largely depends on the dynamic nature of the network, node mobility, energy constraints, and the adaptability of the algorithm to frequent topology changes, which can lead to increased routing overhead or degraded performance if not properly addressed. *Table 1* summarizes these approaches and also discusses their limitations.

Table 1. Existing Route Selection and Data Encryption-based Security Methods

Ref.	Approach	Techniques	Benefits	Limitations
[8]	Blockchain-based MANET (zone-wise)	Neuro-fuzzy inference, ECC	Secure cluster formation & encrypted communication	High computation; latency due to multi-step encryption & blockchain verification
	IEHO with blockchain	Improved Elephant Herd Optimization	Adds security to MANET communication	Computational overhead; risk of premature convergence
[9]	Blockchain + homomorphic encryption	Homomorphic encryption, blockchain	Higher PDR under attacks	High resource demand; scalability issues
	Zone-based clustering with RL CH selection	RL-based CH selection, quantum-resistant crypto, deep learning trust, lightweight encryption	Strong security & improved PDR	
[10]	Hybrid GA–PSO	Genetic Algorithm + Particle Swarm Optimization	Lower energy consumption with security	Tuning complexity
[11]	Trust optimization	Cat-swarm + Sparrow search	Better trust-based routing	Unstable convergence; performance drop
[12]	Secure MANET via clustering & routing	Soft clustering, EHO (CH), multi-attribute trust, ASGO (routing)	Secure comm. in dynamic MANETs	High computation; scalability issues
[13]	Trust-aware routing	HMRFOA	Secures data transmission	Processing delays due to complexity
[14]	CH & routing optimization	RPO, LOA	Trustworthy routing via multi-metrics	Overhead; slower convergence
[15]	Route optimization	Hybrid Swallow Swarm–Memetic	Better than existing routing methods	Higher memory & CPU demand
[16]	Routing with trust metrics	CCOA (energy, distance, link quality, trust)	Improved network comm.	Resource-intensive; not ideal for low-power nodes
[17]	Attacker detection	HTGO + fuzzy trust evaluation	Better malicious node detection	Complex tuning; frequent updates needed
[18]	Secure energy-efficient routing	Graph clustering + ARO	Efficient & secure routing	Overhead; less effective in highly dynamic topologies
[19]	Secure routing with enhanced AES	AES + adaptive chaotic GWO; fuzzy butterfly optimization for routing	Strong encryption & secure data transmission	High computational cost; complex parameter tuning
[20]	Trust-aware routing	Federated Learning LSTM + Location-aided Routing	Accurate trust prediction & improved routing	FL communication overhead; higher latency
[21]	Secure packet delivery	Clustering + hybrid routing + hybrid cryptography	Reliable, secure, and accurate delivery	High processing & network overhead
[22]	Routing optimization	Hybrid Osprey–Fire Hawk Optimization	Multi-criteria routing improvement	Complexity may impact scalability
[23]	Routing optimization	Refined Adaptive Harris Hawks Optimization (RAHHO)	Enhanced routing & security	Possible slower convergence in dynamic networks
[24]	Routing optimization	Artificial Gorilla Troops Optimizer	Better routing decisions	Parameter sensitivity; resource use
[25]	Routing optimization	Hybrid ACO–Whale Optimization	Secure & energy-aware routing	Integration complexity; increased computation
[26]	Routing optimization	Philippine Eagle Optimization	Improved routing efficiency	Limited testing in large-scale scenarios
[27]	Routing optimization	Guided Whale Optimization	Higher PDR & secure transmission	Risk of local optima; may require tuning

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

2.2. AI-based Attack Detection Methods

Deep learning approaches, including cascading backpropagation networks, feedforward networks, and convolution networks, were integrated to design a robust security system for detecting attacks from the MANETs [28]. This integration not only increases the complexity but can also lead to overfitting and high resource consumption. A multi-scale superpixel guided weighted graph convolutional network (MSWGCN) detects selfish nodes [13]. Gated recurrent unit (GRU) with Giant Armadillo optimization (GAO) improves the intrusion detection capabilities of the networks [29]. Deep Q-Networks-based architecture was designed for blackhole attack detection, and its weight updation is enhanced with CCOA optimization [16]. A recurrent neural network (RNN) architecture was used to prevent MANETs from different attackers [30]. A convolutional GRU classifies the attacker nodes based on both spatial and temporal information. However, high computational demands make its accessibility limited [24].

The LSTM and federated learning enhance attack detection accuracy, specifically in the detection of blackhole and grayhole attacks [31]. Machine learning algorithms such as K-nearest neighbors (KNN) and support vector machine (SVM) were used for blackhole attack detection in MANETs [32]. Deep learning approaches such as convolutional neural networks (CNN), LSTM, and GRU were integrated and showed a significant improvement in the attack detection architecture for flooding attacks in MANET [33]. Deep RNN with Gannet Optimization Algorithm enhances the detection capabilities for detecting network layer attackers in MANET [34]. Bidirectional LSTM with Coati optimization improves the classification of DDoS attacks, MitM attacks, and normal traffic [35]. Multi-head self-attention with graph convolutional neural networks (GCN) achieved higher precision and accuracy compared to other existing methods [36]. Deep neural networks [37], hybrid SVM and artificial neural networks [38], graph neural networks (GNN) [39] [40], dual graph convolutional neural networks (DGCN) [41], graph convolution attention (GCAT) [42], etc., are some of the recently designed deep learning approaches that aim to detect different types of intruders in MANETs. *Table 2* summarizes these approaches and also highlights their advantages and limitations.

Table 2. Existing AI-based Attack Detection Methods

Ref.	Approach	Techniques	Benefits	Limitations
[28]	Attack detection	Cascading backpropagation, feedforward, CNN	Robust multi-model security system	High complexity; risk of overfitting; high resource consumption
[13]	Selfish node detection	MSWGCN (multi-scale superpixel guided weighted GCN)	Accurate detection of selfish nodes	Graph processing overhead; scalability limits
[29]	Intrusion detection	GRU + Giant Armadillo Optimization (GAO)	Enhanced detection capabilities	Optimization adds processing overhead
[16]	Blackhole attack detection	Deep Q-Network + CCOA optimization	Improved detection & optimized weight update	High computation; tuning complexity
[30]	Multi-attack prevention	RNN	Effective against multiple attack types	Possible vanishing gradient; training time
[24]	Attacker classification	Convolutional GRU (spatial + temporal features)	High accuracy in attacker classification	High computational demand; limited suitability for low-power nodes
[31]	Blackhole & grayhole attack detection	LSTM + Federated Learning	High detection accuracy for specific attacks	FL communication overhead; high computation
[32]	Blackhole attack detection	KNN, SVM	Simple, interpretable models	Lower accuracy for complex patterns; feature sensitivity
[33]	Flooding attack detection	CNN + LSTM + GRU	Improved detection performance	High training cost; risk of overfitting
[34]	Network layer attacker detection	Deep RNN + Gannet Optimization	Enhanced detection capabilities	Optimization adds processing delay
[35]	DDoS & MitM attack classification	Bi-LSTM + Coati Optimization	Better classification accuracy & traffic differentiation	Complex tuning; higher resource usage
[36]	General intrusion detection	Multi-head self-attention + GCN	Higher precision & accuracy	Graph computation overhead; scalability concerns
[37]	Intrusion detection	Deep Neural Networks (DNN)	Good generalization	Requires large datasets; high training cost
[38]	Intrusion detection	Hybrid SVM + ANN	Combines interpretability with learning capability	Parameter tuning complexity
[39], [40]	Intrusion detection	Graph Neural Networks (GNN)	Captures structural relationships	High memory and computation demand
[41]	Intrusion detection	Dual Graph Convolutional Networks (DGCN)	Better relational feature extraction	Graph processing overhead
[42]	Intrusion detection	Graph Convolution Attention (GCAT)	Improves detection accuracy via attention	Increased complexity; longer training time

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

Although deep learning architectures claim better detection capabilities, they still have some limitations, such as failure in capturing dynamic spatio-temporal dependencies, a lack of labeled datasets, and a lack of contextual awareness. These challenges highlight the need for more flexible, adaptive, and interpretable solutions. With this aim, this research work proposes a novel STAGNet-COpt architecture and also uses the large-scale self-generated datasets.

3. METHODOLOGY

This section shown the experimental result of our novel ANN-FLC-Nanofluid-Lyapunov A framework -Nanofluid-Lyapunov A framework is employed for a 400 kVA, 33/0.38 kV, ONAN transformer at the Nasiriyah Electrical Research Laboratory. All verifications were carried out under harsh operating conditions: 40°C ambient, 140% overload, 5.2% THD, and +15°C step fluctuation.

3.1. Dataset Structure and Time-Scale Separation

The primary aim of this research work is to enhance the security level in MANETs by adding both attack detection and prevention capabilities in a single system. With this aim, this study proposes a STAGNet-COpt, a spatio-temporal attention graph network with cluster-based optimized trust routing to detect and prevent the network from various types of attacks, including blackhole, wormhole, grayhole, DoS, and integrated attacks. The MANET communication architecture, as shown in *figure 1*, presents that this proposed approach designs three novel modules, including STAGNet, TrustFuzz, and WOACO, and embeds them in the network architecture in order to enhance the performance effectiveness. TrustFuzz divides the network nodes into clusters, WOACO-R optimizes the path selection, and STAGNet focuses on detecting attacker nodes, respectively. A suspicious list has been formed during simulation, which maintains the record of attacker nodes and passes the information to WOACO-R to avoid suspicious nodes' participation in communication. These modules have dynamic capabilities that sustain their performance throughout transmission and any communication. The details of the proposed modules are provided in the following subsections.

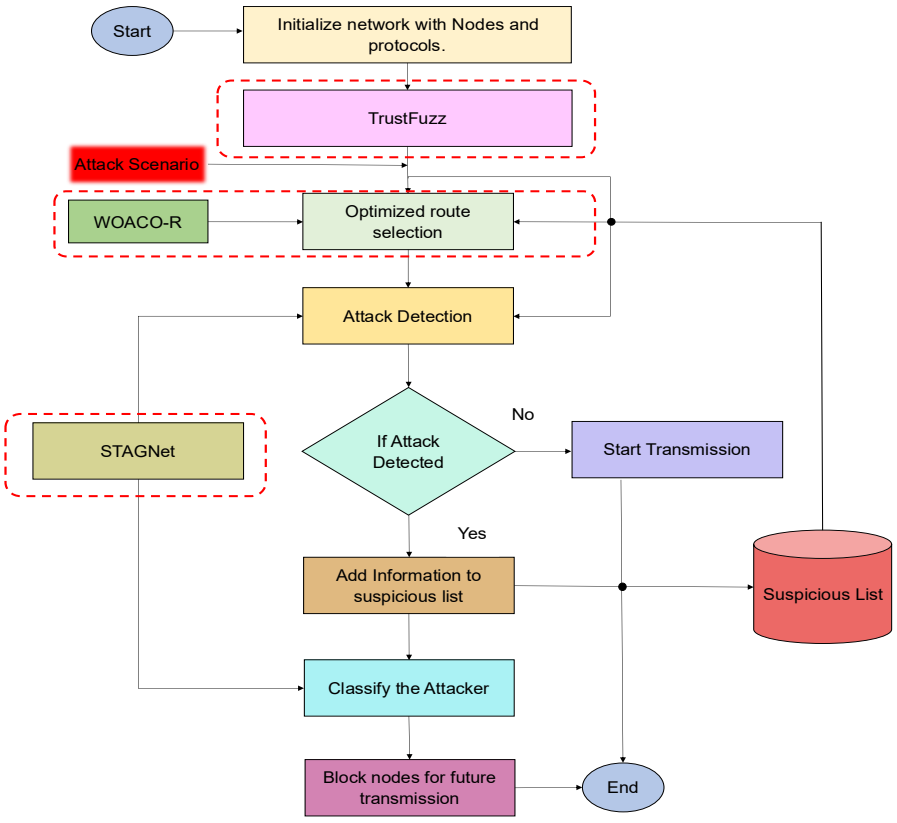

Figure 1. Real-time φ(t) trajectory *vs* hotspot suppression system

3.1. Spatio-Temporal Attention Graph Network (STAGNet)

The proposed STAGNet integrates graph attention networks (GATs) with long short-term memory (LSTM) networks to learn both spatial and temporal patterns from the network traffic data. *Figure 2* represents the process of how a proposed STAGNet is implemented on the network nodes' traces and is discussed in the following subsections.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

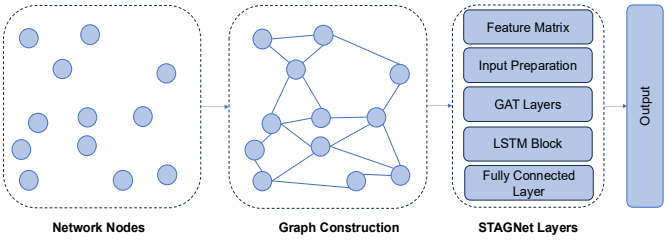

Figure 2. Sequence of operations from network nodes to graph construction and then proposed STAGNet layers for attack detection

- ***Graph Construction:*** A MANET network consists of *n* self-configuring nodes that communicate with the help of neighbor nodes. At a given time *t*, network nodes are modeled as graph $G_t = (V_t, E_t)$, where V_t are the set of nodes and E_t represents links between nodes. Each node in the network $v_i \in V_t$ is associated with a feature vector $x_i^{(t)} \in \mathbb{R}^F$, including different features of network nodes. Since MANET has dynamic topology and it also changes node behaviour over time, so it is modeled as *'k'* sequence of graphs $\{G_1, G_2, \dots, G_k\}$.

- ***Spatial Modeling with GATs:*** This step involved to learn spatial relationships between nodes and enhancing this process using an attention mechanism over the neighborhood of each node. Unlike graph neural and convolutional networks that use fixed weights, GAT dynamically assigns an attention score to the neighboring nodes. In this, the feature matrix of each node is linearly projected into higher higher-dimensional space as given in *eq. (1)* below:

$$z_i = Wx_i, \quad W \in \mathbb{R}^{H \times F} \tag{1}$$

Here, F is the number of input features and H is the dimensionality of the space. Then the importance means the attention score of the i^{th} node features *(j)* is computed using *eq. (2)*:

$$e_{ij} = LReLU\left(a^T[z_i \parallel z_j]\right) \tag{2}$$

Here, *LReLU* is a leaky rectified linear unit activation function that ensures even negative values of the concatenated feature vector $[z_i \parallel z_j]$ contribute to the attention score, which improves the learning dynamics. a is here a learnable vector defined as $(a \in \mathbb{R}^{2H})$. Further, these scores are normalized using *eq. (3)*:

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum_{m \in \mathcal{M}_i} \exp(e_{im})} \tag{3}$$

Where $\mathcal{M}_i$ is the set of nodes directly connected to a node *i*.

Now the new representation of each node is computed based on the weighted sum of transformed features of its neighbors and is computed using *eq. (4)*:

$$h_i = \rho\left(\sum_{j \in \mathcal{M}_i} \alpha_{ij} z_j\right) \tag{4}$$

Here ρ is an exponential linear unit activation function.

Instead of relying on a single set of attention weights, multiple attention heads have been used with their own $W^{(k)}$ and are computed in *eq. (5)*.

$$h_i^{GAT} = \|_{k=1}^{K} \sigma\left(\sum_{j \in \mathcal{M}_i} \alpha_{ij}^{(k)} W^{(k)} x_j\right) \in \mathbb{R}^{K \cdot H} \tag{5}$$

- ***Temporal Modeling using LSTM:*** The information for each time stamp *(T)* is when passed through GAT, it obtains the following sequence as mentioned in *eq. (6)* for each node:

$$\mathcal{H}_i = \left[h_i^{(1)}, h_i^{(2)}, \dots\dots, h_i^{(T)}\right] \in \mathbb{R}^{T \times (K \cdot H)} \tag{6}$$

In LSTM, each cell maintains a hidden state $(h_t \in \mathbb{R}^d)$and cell state $(c_t \in \mathbb{R}^d)$ where hidden state represents the output at time *t*, the cell state stores the long-term memory. The process of LSTM is that each cell includes three gates: input, forget, and output, and an intermediate candidate state. The input gate controls how much of the new input $h_i^{(t)}$ from the GAT layer should influence the memory and be represented in the *eq. (7)*:

$$I_t = \sigma\left(W_I h_i^{(t)} + U_I h_{i-1}\right) \tag{7}$$

Here, h_{i-1} is the previous hidden state, W_i and U_i are the learnable weights, and σ is a sigmoid function. The forget gate then determines how much of the past information should be retained and is represented in *eq. (8)*:

$$\mathrm{F}_t = \sigma\left(W_\mathrm{F} h_i^{(t)} + U_\mathrm{F} h_{i-1}\right) \tag{8}$$

The control gate determines how much of the current memory $c_t$should be revealed to the next layer as computed in *eq. (9)*:

$$o_t = \sigma\left(W_o h_i^{(t)} + U_o h_{i-1}\right) \tag{9}$$

Based on this, the candidate state, i.e., a potential new memory, is generated and updated using *eq. (10):*

$$\tilde{c}_t = tanh\left(W_c h_i^{(t)} + U_c h_{i-1}\right) \tag{10}$$

The combined output is presented in *eq. (11)*:

$$c_t = \mathrm{F}_t \odot c_{t-1} + I_t \odot \tilde{c}_t \tag{11}$$

From all the above states, the output of the LSTM cell represents the temporally enriched embedding of the node at time *t* and is represented in *eq. (12)*:

$$h_T^{(i)} = o_t \odot tanh(c_t) \tag{12}$$

- ***Fully Connected Layer:*** The final output from the LSTM cell is passed through a fully connected layer for classifying the normal and malicious network traffic, along with the attack type, and is represented in *eq. (13)* and *eq. (14)*:

$$z_i = ReLU\left(W_1 \cdot h_T^{(i)} + b_1\right) \in \mathbb{R}^{64} \tag{13}$$

$$\hat{y}_i = Softmax(W_2 \cdot z_i + b_2) \in \mathbb{R}^C \tag{14}$$

Here $\hat{y}_i$ is the predicted probability distribution over *C* classes.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

3.2. Fuzzy-based Trust-aware Clustering (TrustFuzz)

Traditional clustering in MANETs does not ensure security due to static parameter information, such as node ID, distance, etc. However, the trustworthiness of the nodes is a crucial factor in MANETs to form secure and reliable zones. This research work proposes a TrustFuzz module for trust-aware clustering in MANETs that dynamically divides the network nodes into clusters based on behavioural and contextual factors. As the TrustFuzz proposes a trust-aware design, the trustworthiness of each network node is evaluated continuously using k different features (f_k): packet forwarding rate, frequency of route request replies, and rate of control packet generation. The trust value at the i^{th} node $T_i \in [0,1]$ is the weighted aggregation of normalized weights as given in *eq. (15)*:

$$T_i = \sum_{i=1}^{n} w_k \cdot f_k^{(i)} \quad (15)$$

TrustFuzz then employs a fuzzy inference system to effectively model the dynamicity and uncertainty of the MANETs, which takes the computed trust T_i, as an input and fuzzified it into {Low, Medium, High}. Additionally, it incorporates mobility of nodes, i.e., {Static, Moderate, High}. Based on these two input factors, different rules are formed to select a node as cluster head (CH) and output as {Reject, Member, CH candidate}. After initial fuzzification, the nodes are grouped using a modified fuzzy c-mean algorithm, which incorporates trust score in its distance metric. Therefore, a new distance formula that replaces traditional Euclidean distance methods is given in eq. (16):

$$D_{ij}^{trust} = \sqrt{\left\|x_i - x_j\right\|^2 + \lambda \cdot \left(T_i - T_j\right)^2} \quad (16)$$

Where λ is the trust sensitivity weight. Based on this new distance value, nodes with similar levels are grouped into one cluster, and malicious nodes drift away from the high-trust clusters. So, if a network has N nodes and forms C clusters, the membership degree of node i to cluster j is updated as given in *eq. (17)*:

$$\mu_{ij} = \frac{1}{\sum_{k=1}^{C}\left(\frac{D_{ij}^{trust}}{D_{ik}^{trust}}\right)^{2/(m-1)}} \quad (17)$$

And the cluster centers are updated as given in *eq. (18)*:

$$v_j = \frac{\sum_{i=1}^{N} {\mu_{ij}}^m \cdot x_i}{\sum_{i=1}^{N} {\mu_{ij}}^m} \quad (18)$$

Therefore, this proposed TrustFuzz transforms the traditional clustering into secure and reliable clustering in order to enhance both network resilience and routing robustness against insider and outsider threats.

3.3. Hybrid WOA and ACO-based Route Optimization (WOACO-R)

In MANETs, dynamic route selection through different existing protocols, such as AODV, DSR, etc., does not consider the additional factors, such as trust, energy, etc., which makes them unreliable and inefficient in current scenarios. In this research work, a hybrid WOA and ACO is proposed for route optimization. WOA uses spiral and encircling strategies that balance exploration and exploitation better than many newer algorithms. On the other hand, ACO is probabilistic and adaptive in nature, allowing it to refine routes over time based on pheromone feedback, which mimics real-time link quality learning. It maintains routing memory, improving path stability and reliability with each iteration compared to other optimization algorithms. WOA generates diverse, globally distributed path candidates early, and ACO then locally improves and reinforces the most promising ones. This combination avoids stagnation and provides both exploration and adaptive exploitation. Therefore, this combination is suggested here to enhance routing in the MANETs along with the other modules. This hybrid algorithm works in two phases, and the final route is selected based on these phases. It includes:

- ***Global Path Discovery:*** The WOA is inspired by the bubble-net feeding strategy of whales, here used as a route selection approach, and in this, each whale agent represents a candidate path from source to destination across trusted cluster heads. The first step in this is the path encoding as given in *eq. (19)*, where each whale $\vec{X}$ is a sequence of node IDs forming a path between source S and destination D:

$$\vec{X} = [v_1, v_2, \dots \dots, v_k], \text{here } v_1 = S \text{ and } v_k = D \quad (19)$$

Each path is evaluated based on fitness value computed based on Trust score *(T),* residual energy *(E),* and distance *(D),* as given in *eq. (20)*:

$$F(i) = \sum_{m,n \in i}\left[w_1 \cdot {}^1/_{T_n} + w_2 \cdot {}^1/_{E_n} + w_2 \cdot D_{mn}\right] \quad (20)$$

Here w_1, w_2, w_3, are weights with values {0.4,0.4,0.2}, respectively which is selected based on experimentations. Based on this, the lower the fitness, the better the route. During different iterations, WOA updates the position of each using encircling, attack, and exploration. The encircling of the best path is defined in *eq. (21)*:

$$\vec{X}(t+1) = \vec{X}^*(t) - \vec{A} \cdot \left|\vec{C} \cdot \vec{X}^*(t) - \vec{X}^*(t)\right| \quad (21)$$

The spiral bubble attack strategy computes the best path using *eq. (22)*:

$$\vec{X}(t+1) = \left|\vec{X}^*(t) - \vec{X}(t)\right| \cdot e^{bl} \cdot \cos(2\pi l) + \vec{X}^*(t) \quad (22)$$

Random search means exploration, compute the path as given in *eq. (23)*:

$$\vec{X}(t+1) = \vec{X}_{rand} - \vec{A} \cdot \left|\vec{C} \cdot \vec{X}_{rand} - \vec{X}(t)\right| \quad (23)$$

These movement updates help in generating the high-quality initial paths and are further fed to ACO for final route selection.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

- ***Local Route Refinement:*** The ACO works on the foraging behavior of ants, where pheromone trails are laid on favorable paths. In this, each ant probabilistically selects the next node *j* from the current node *i* using *eq. (24)*:

$$P_{i,j} = \frac{[\tau_{ij}]^{\alpha} \cdot [\eta_{ij}]^{\beta}}{\sum_{k \in N_i} [\tau_{ik}]^{\alpha} \cdot [\eta_{ik}]^{\beta}} \quad (24)$$

Here, α and β control the impact of trial and heuristic, τ_{ij} is the pheromone value on edge, $\eta_{ij} = \frac{T_j}{E_j \cdot D_j}$, the process repeats until a complete path between source and destination is not built.

After path formations, the pheromones are updated as given in *eq. (25)*:

$$\tau_{ij} \leftarrow (1 - \rho) \cdot \tau_{ij} + \sum_{a=1}^{N} \Delta\tau_{ij}^{(a)} \quad (25)$$

Where $\Delta\tau_{ij}^{(a)} = \begin{cases} \frac{Q}{cost_a}, & if\ (i,j) \in path_a \\ 0, & otherwise \end{cases}$, to ensure frequent, efficient and secure paths for MANETs' communication over time.

The final best path P_{opt} is selected from all candidate paths and then used for data transmission between clusters using *eq. (26)*:

$$P_{opt} = \arg\min_{a} cost_a \quad (26)$$

This hybrid optimization ensures that routing bypasses attacker nodes, reinforces trustworthy links, and minimizes retransmissions and delay. The pseudo code for the proposed WOACO-R is given as follows:

Algorithm 1: WOACO-R

Input:

- Clustered graph G (V, E)
- Trust score T, energy E, distance D for each link
- Source node S, Destination node D
- Parameters: MaxWOAIters, NumWhales, NumAnts, α, β, γ, ρ, Q

Output:

- Optimal path $\boldsymbol{P_{opt}}$

// ------ WOA Phase: Global Path Search ------
Initialize whale population: each whale $W_i \leftarrow$ *random path from S to D*
For iter = 1 to MaxWOAIters do
For each whale W_i *do*
Evaluate Fitness $(W_i) = \sum Cost_{ij}$ *over path*
Identify X_{best} *with minimum cost*
For each whale W_i *do*
Update position using either encircling, spiral, or random search
End For
End For
WOA_Paths $\leftarrow$ *final whale population paths*
// ------ ACO Phase: Local Refinement -------
Initialize pheromone matrix $\tau_{ij} \leftarrow$ *small constant*
For each ant a = 1 to NumAnts do
Initialize ant at node S
While current_node ≠ D do
Probabilistically select next node j using:

$$\boldsymbol{P_{ij} = \frac{[\tau_{ij}]^{\alpha} \cdot [\eta_{ij}]^{\beta}}{\sum_{k \in N_i} [\tau_{ik}]^{\alpha} \cdot [\eta_{ik}]^{\beta}}}$$

Append j to $path_a$
End While
Evaluate $cost_a = \sum cost_{ij}$ *over* $path_a$
End For
// Update Pheromones
For all edges (i, j):

$$\boldsymbol{\tau_{ij} \leftarrow (1 - \rho) \cdot \tau_{ij} + \sum_{a=1}^{N} \Delta\tau_{ij}^{(a)}}$$ *if (i, j)* $\in path_a$

$P_{opt} \leftarrow$ *path with minimum* $cost_a$
Return P_{opt}

3.4. Temporal Workflow

The proposed MANET architecture integrates STAGNet, TrustFuzz, and WOACO-R in a temporally coordinated manner to ensure secure and adaptive communication under dynamic network conditions. Since detection, trust computation, clustering, and routing are interdependent processes, a clear temporal workflow is necessary to maintain consistency and minimize the impact of malicious nodes. *Figure 3* presents the temporal workflow with an example of an attack and its detection.

- ***Trust Update Mechanism:*** The trust values are dynamically updated using a hybrid mechanism that combines periodic and event-triggered updates to balance responsiveness and computational overhead. The periodic update ensures behavioral consistency by updating values at a fixed interval of 5ms throughout the simulation, and event-driven updates are triggered when anomalous behavior is detected.

- ***Detection Latency Modeling:*** Detection latency is defined as the time difference between the initiation of malicious activity and its confirmation by STAGNet. In the proposed framework, it is bounded by a 5ms trust update interval and continuous behavioural monitoring. The maximum delay before trust recalculation is limited to one update cycle, which ensures rapid identification of malicious nodes.

- ***Routing Adaptation Mechanisms:*** Detection latency may temporarily allow malicious nodes to participate in routing decisions. To mitigate this impact, WOACO-R incorporates trust as a weighted parameter in its fitness function, as given in Eq. (20). During the latency window, nodes exhibiting abnormal behaviour experience gradual trust degradation; their probability of selection in route formation also degrades, and route stability is preserved by prioritizing higher trust nodes. However, once STAGNet confirms the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

malicious activity, the node is added to the suspicious list, TrustFuzz updates cluster membership, and WOACO-R immediately triggers route re-optimization, excluding the flagged node. Therefore, the total reaction time of the system depends on detection latency and route re-optimization. Since route optimization is executed in the next routing cycle, the time required for route re-optimization remains minimal relative to the overall simulation duration.

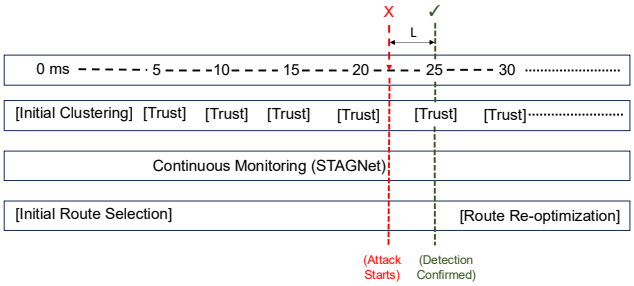

Figure 3. Temporal Workflow of the proposed architecture showing periodic trust update, continuous STAGNet monitoring, detection latency (L), and WOACO-R route re-optimization

3.5. Computation Complexity and Convergence Analysis

This section discusses the complexity analysis for STAGNet and WOACO-R, and also provides the convergence analysis.

- ***Computational Complexity of STAGNet:*** Let N denote the number of nodes in the MANET, E be the number of communication links, T be the temporal window size, and F be the feature dimension. The spatial attention mechanism operates over graph edges, requiring an attention coefficient per edge. Thus, the spatial complexity is $O(EF)$. The temporal modeling component processes node features across T time steps, and therefore, the complexity is $O(TNF)$. The total complexity of STAGNet is therefore $O(EF + TNF)$. In dense MANET scenarios where $E \approx N^2$, the worst-case complexity becomes $O(N^2F + TNF)$.

- ***Computational Complexity of WOACO-R:*** Let N be the number of nodes, A be the number of ants, and I be the number of iterations. The ACO component evaluates path construction with complexity $O(AN^2)$ per iteration, as route selection considers pair-wise node transitions. The WOA component performs a position update with complexity $O(IN)$. The hybrid WOACO-R complexity is $O(I(AN^2 + N)$ which becomes $O(IAN^2)$ in dense networks.

- ***Convergence Analysis of proposed WOACO-R***: *Figure 4* illustrates the convergence behaviour of WOA, ACO, and proposed WOACO-R over 100 iterations. The graph shows that the proposed WOACO-R achieves faster, smoother convergence than both ACO and WOA. It indicates that the proposed algorithm effectively balances global and local search, efficiently optimizing routing paths under dynamic, adversarial MANET conditions.

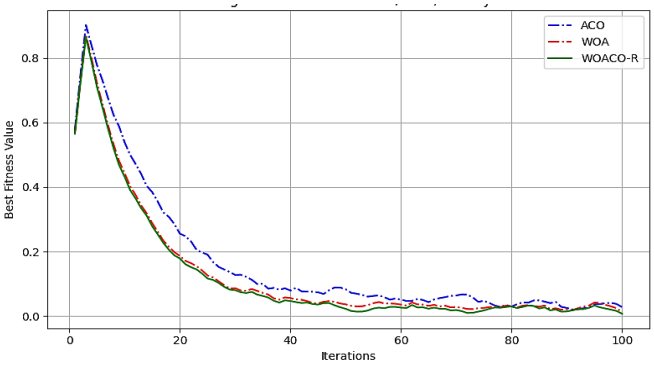

Figure 4. Convergence behavior of WOA, ACO, and WOACO-R over 100 iterations

4. EXPERIMENTATION AND RESULT ANALYSIS

The experimentation is conducted to analyze the accuracy of the proposed STAGNet-COpt. The network simulator version 2 (NS-2) is used for both network simulation and dataset generation. Different network scenarios are created under blackhole, wormhole, grayhole, denial of service (DoS), and integrated attacks and varying numbers of nodes. Additionally, an ablation study is conducted to analyze the impact of each proposed module, including STAGNet, TrustFuzz, and WOACO-R. All the simulation parameters are given in *table 3*, and performance is computed in terms of packet delivery ratio (PDR), throughput, delay, loss, overhead, and detection accuracy.

Table 3. Simulation Parameters

Parameter	Value
Simulation area	1000 x1000
Number of Nodes	50,100,150,200
Number of Attacker nodes	04
Attack Type	Blackhole, wormhole, grayhole, DoS, and Integrated Attack
Speed of nodes	30m/s
Packet Size	16 bytes
Simulation Time	100ms
Node Location	Random and Dynamic
Number of Connections	20

4.1. Dataset Generation

The input dataset for training and evaluating STAGNet is generated from NS-2 traces as given in *table 3*. Each trace records different behaviour metrics such as transmission, reception, drop, delay and routing control messages. The trace logs are parsed and pre-processed to extract spatio-temporal features for each node. In total, the dataset consists of seven different attributes except label attributes, and these are packet transmission and receiving count, RREQ/RREP frequency, routing table updates, node movements, delay variance, cluster ID, and trust score. The label dataset is created under both normal and attack scenarios. In total, five different datasets with nodes 50-200 are created, where each dataset consists of normal

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

and attack traffic. The labels are assigned to each record as per attack type, based on which 6 different class labels are assigned to the data records. *Table 4* presents a detail about these class labels:

Table 4. Class Labels in the dataset

0	1	2	3	4	5
Normal	Blackhole	Wormhole	Grayhole	DoS	Integrated

4.2. Ablation Study

The ablation study is conducted to analyze the impact of each proposed module. So, eight different methods as given in *table 5* are evaluated on a simulation scenario with 100 nodes and 04 attacker nodes (integrated attacks). The performance in terms of PDR, throughput, delay, etc., is measured, and the results are presented in this section.

Table 5. Methods in Ablation Study

Methods	Different Modules			
	AODV	STAGNet	TrustFuzz	WOACO-R
M1	✓	-	-	-
M2	✓	✓	-	-
M3	✓	-	✓	-
M4	✓	-	-	✓
M5	✓	✓	✓	-
M6	✓	✓	-	✓
M7	✓	-	✓	✓
M8 (Proposed)	✓	✓	✓	✓

The computed results are presented in *table 6*, which compares the performance of different methods based on different performance metrics. M1 is a baseline architecture with only AODV protocol implementation, and it has been noticed that the AODV does not have any capability to deal with the integrated attacks, as PDR and throughput are extremely low, and delay, loss, and overhead are extremely high. When STAGNet is integrated in M2, it improves PDR, reduces delay and loss, and slightly reduces overhead, which represents its spatio-temporal understanding and trusted decisions. TrustFuzz, when integrated with M1 in M3, reduces exposure to malicious nodes. Again, a gain in the PDR has been seen; however, owing to a lack of routing optimization, delay and overhead are very slightly reduced. WOACO-R in M4 has shown the highest gain compared to other methods (M1, M2, M3), as routes are optimized using trust, energy, etc. and help in avoiding compromised and overloaded paths.

Table 6. Performance Analysis of different methods in the ablation study

Methods	Performance Metrics				
	PDR (in %)	Throughput (in kbps)	Delay (in ms)	Loss (in %)	Overhead (packets)
M1	52.34	68.05	21.835	47.66	1037
M2	71.25	79.37	17.025	28.75	856
M3	68.23	75.86	19.751	31.77	915
M4	76.34	86.25	14.032	23.66	812
M5	82.35	91.27	8.592	17.65	705
M6	89.43	102.45	5.268	10.57	423
M7	85.52	98.49	7.056	14.48	602
M8 (Proposed)	**95.38**	**124.76**	**3.251**	**4.62**	**253**

Further, the combination of different modules in M5 shows cooperation between detection and clustering, a significant reduction in the delay and a gain in PDR in comparison to others has been seen. This combination also reduces overhead as it reduces packet retransmissions. M6 combines STAGNet and WOACO-R, which is the most effective partial setup to date, with the highest PDR and the lowest loss. This is a combination where one detects the attacker efficiently and the other avoids them through optimized paths. Delay and overhead are also very less in this case. M7 combines TrustFuzz and WOACO-R, which performs better than M5 but not M6. Finally, the proposed M8 module, which combines every module, achieved the highest performance among all with improved PDR, throughput, delay, loss, and overhead. Therefore, it is clear that the proposed STAGNet-COpt is carefully designed for critical scenarios of MANET in order to improve its effectiveness and efficacy.

4.3. Result Analysis

The performance of the proposed STAGNet-COpt is evaluated under a network scenario, including the number of normal nodes that represent congestion in the network under different attacks as mentioned in previous sections. Different performance metrics have been computed and analyzed under different conditions. *Figure 5* presents the analysis of the proposed approach on different attacks based on PDR.

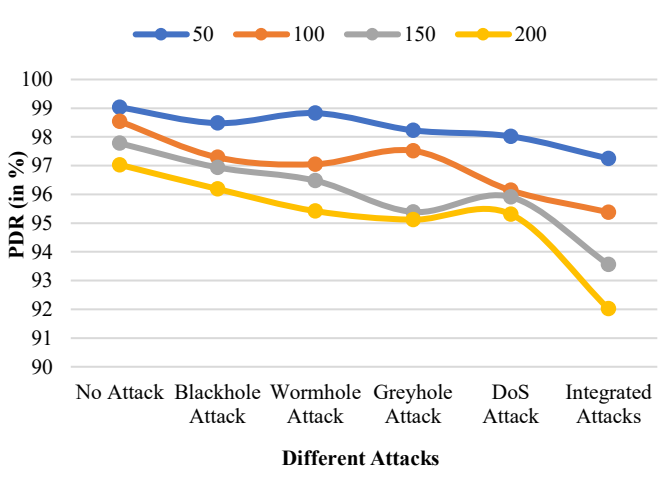

Figure 5. PDR of the proposed STAGNet-COpt with varying nodes under different attacks

The results show that the PDR remains consistent and above 90% under all scenarios that showcase the robustness of the

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

proposed method. As the network scale increases, PDR gradually decreases due to increased routing complexity and congestion. Results also highlight that the performance is poor in the presence of integrated attacks, highlighting the compounding effect of multiple attacker nodes. *Figure 6* presents the analysis of the proposed approach on different attacks based on throughput.

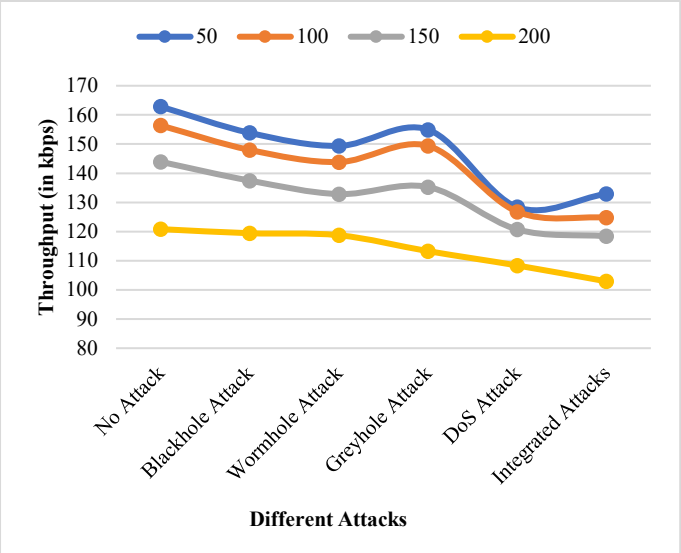

Figure 6. Throughput of the proposed STAGNet-COpt with varying nodes under different attacks

Throughput is also relatively high under all attacks, but decreases with increasing number of nodes, as given in *figure 6*. Out of all different attacks, DoS and integrated attack has more impact on deteriorating a performance of the network. *Figure 7* presents the analysis of the proposed approach on different attacks based on Loss ratio.

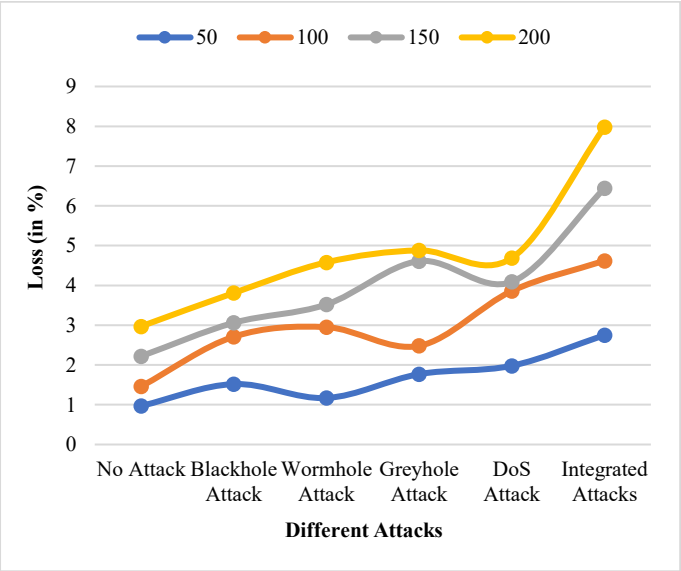

Figure 7. Loss Ratio of the proposed STAGNet-COpt with varying nodes under different attacks

The loss ratio is also under control and is <8% under all scenarios. However, loss increases with network scaling and in the presence of integrated attacks. *Figure 8* presents the analysis of the proposed approach on different attacks based on delay.

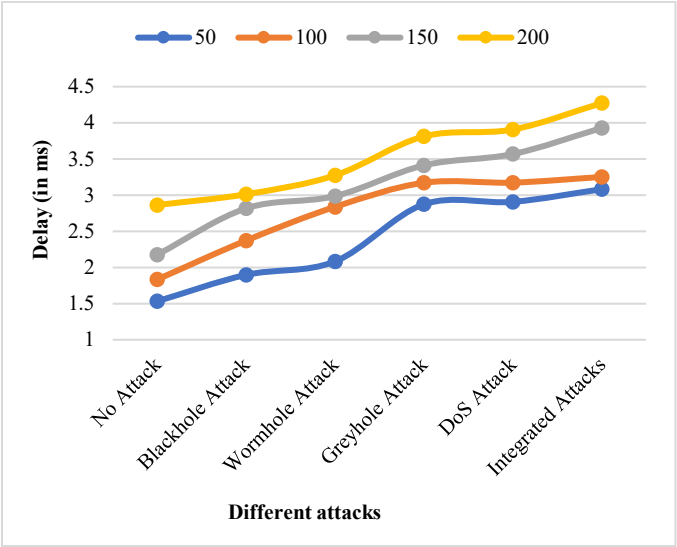

Figure 8. Delay of the proposed STAGNet-COpt with varying nodes under different attacks

The minimum and maximum delays have been seen in the normal node and integrated attacker nodes scenario. Overall delay is maintained, and it is because STAGNet helps anticipate traffic patterns, while WOACO-R avoids congested/malicious paths. *Figure 9* presents the analysis of the proposed approach on different attacks based on overhead.

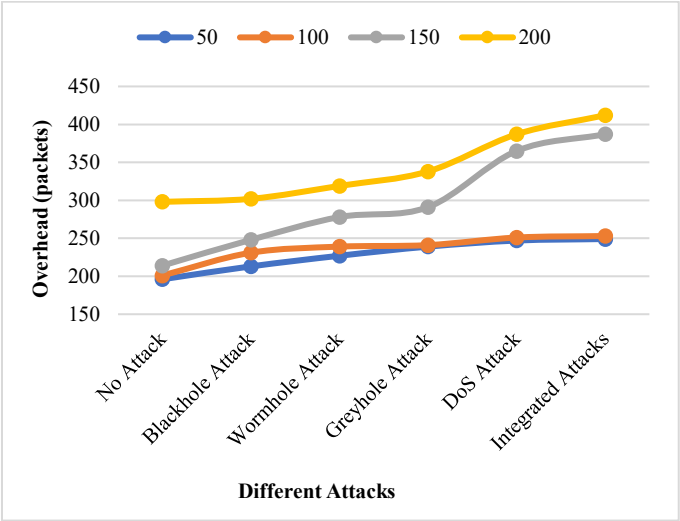

Figure 9. Overhead of the proposed STAGNet-COpt with varying nodes under different attacks

Overhead is also minimized specifically because of TrustFuzz and WOACO-R but it also increases with the network scaling. *Figure 10* presents the analysis of the proposed approach on different attacks based on detection accuracy.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

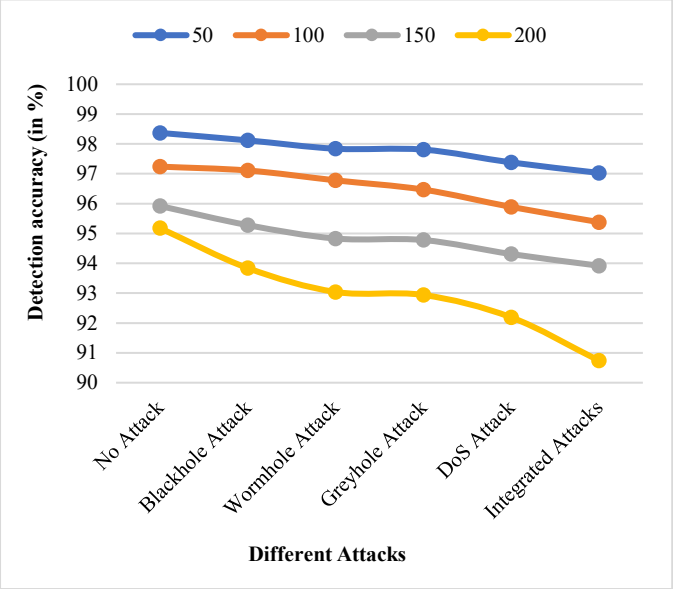

Figure 10. Detection Accuracy of the proposed STAGNet-COpt with varying nodes under different attacks

The detection accuracy decreases slightly with scale, and it is extremely low in the case of integrated scenarios. However, the proposed method achieved an accuracy of more than 90% in all cases. *Table 7* summarizes all these results and provides the exact values for each performance metric. These results, therefore, represent the effectiveness of the proposed STAGNet-COpt approach under critical conditions.

Table 7. Summary of the results of the proposed STAGNet-COpt with varying nodes under different attacks

Attacks	Number of Nodes			
	50	100	150	200
PDR (in %)				
No Attack	99.03	98.54	97.78	97.03
Blackhole Attack	98.48	97.29	96.94	96.19
Wormhole Attack	98.83	97.05	96.48	95.42
Grayhole Attack	98.23	97.52	95.39	95.12
DoS Attack	98.02	96.14	95.91	95.31
Integrated Attacks	97.25	95.38	93.56	92.02
Throughput (in kbps)				
No Attack	162.84	156.38	143.92	120.83
Blackhole Attack	153.84	147.98	137.47	119.42
Wormhole Attack	149.37	143.84	132.84	118.74
Grayhole Attack	154.93	149.38	135.28	113.28
DoS Attack	128.38	126.82	120.73	108.37
Integrated Attacks	132.93	124.76	118.39	102.93
Loss (in %)				
No Attack	0.97	1.46	2.22	2.97
Blackhole Attack	1.52	2.71	3.06	3.81
Wormhole Attack	1.17	2.95	3.52	4.58
Grayhole Attack	1.77	2.48	4.61	4.88
DoS Attack	1.98	3.86	4.09	4.69
Integrated Attacks	2.75	4.62	6.44	7.98
Delay (in ms)				
No Attack	1.532	1.833	2.176	2.863
Blackhole Attack	1.897	2.372	2.817	3.012
Wormhole Attack	2.083	2.837	2.986	3.273
Grayhole Attack	2.873	3.171	3.412	3.812
DoS Attack	2.907	3.173	3.568	3.907
Integrated Attacks	3.081	3.251	3.928	4.272
Overhead (packets)				
No Attack	196	201	214	298
Blackhole Attack	213	231	248	302
Wormhole Attack	227	239	278	319
Grayhole Attack	239	241	291	338
DoS Attack	247	251	365	387
Integrated Attacks	249	253	387	412
Detection Accuracy (in %)				
No Attack	98.37	97.24	95.92	95.18
Blackhole Attack	98.12	97.11	95.28	93.84
Wormhole Attack	97.84	96.78	94.83	93.04
Grayhole Attack	97.81	96.47	94.78	92.94
DoS Attack	97.38	95.89	94.31	92.19
Integrated Attacks	97.03	95.38	93.92	90.74

4.4. Validation Results

This section validates the experimental results across different factors, including the impact of fitness weights, packet size, and varying simulation times.

- **Impact of different fitness weights:** The impact of fitness weights on routing performance has been evaluated for WOACO-R in the proposed framework using the same simulation scenario as in the ablation study (100 nodes and 4 attacker nodes, integrated attacks). *Table 8* compares the evaluated results across different weight combinations and shows that the selected weight values provide the best trade-off, achieving better performance.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

Table 8. Performance Analysis based on different performance metrics to understand the impact of weights

Weights	Performance Metrics				
	PDR (in %)	Throughput (in kbps)	Delay (in ms)	Loss (in %)	Overhead (packets)
0.4,0.4,0.2	**95.38**	**124.76**	**3.251**	**4.62**	**253**
0.45,0.35,0.2	93.64	122.85	3.859	6.36	268
0.35,0.45,0.2	92.18	121.05	3.965	7.82	274

- **Impact of packet size:** The impact of packet size on performance has been evaluated using the proposed framework using the same simulation scenario as in the ablation study (100 nodes and 4 attacker nodes, integrated attacks). *Table 9* compares the evaluated results across different packet sizes. From the results, it has been seen that the PDR decreases slightly with larger packets, whereas throughput increases because each packet carries more data. Delay also increases because larger packets take longer to transmit, and overhead also decreases because fewer packets are required to send the same total data.

Table 9. Performance Analysis based on different performance metrics to understand the impact of packet size

Packet Size	Performance Metrics				
	PDR (in %)	Throughput (in kbps)	Delay (in ms)	Loss (in %)	Overhead (packets)
16	95.38	124.76	3.251	4.62	253
512	94.28	415.24	4.814	5.72	114

- **Impact of varying simulation time:** The impact of varying simulation time on performance has been evaluated using the proposed framework, using the same simulation scenario as in the ablation study (100 nodes and 4 attacker nodes, integrated attacks) except for packet size. The packet size used for experimentation here is 512. *Table 10* compares the evaluated results across different simulation times. From the results, it has been seen that both PDR and throughput increase with increasing simulation time, as longer simulation times allow more successful transmissions and fewer packet drops. The delay also increases due to more packets in the network, and the overhead increases slightly due to routing updates and the detection mechanism.

Table 10. Performance Analysis based on different performance metrics to understand the impact of varying simulation time

Simulation Time	Performance Metrics				
	PDR (in %)	Throughput (in kbps)	Delay (in ms)	Loss (in %)	Overhead (packets)
100	94.28	415.24	**4.814**	5.72	**114**
200	95.81	428.15	5.865	4.19	116
300	96.29	431.65	6.954	3.71	121
400	97.18	448.29	8.025	2.82	126
500	**98.25**	**451.27**	8.956	**1.75**	129

4.5. Statistical Analysis

The performance of the proposed framework was also evaluated across different attacks and varying nodes. All experiments are repeated 10 independent simulation runs, and their mean and standard deviation results are reported in *table 11*.

Table 11. Performance Analysis based on Mean + Standard Deviation over 10 simulation runs

Attacks	50	100	150	200
PDR (in %)				
No Attack	98.75 ± 0.4	98.6 ± 0.49	97.8 ± 0.57	97.16 ± 0.46
Blackhole Attack	98.61 ± 0.53	97.16 ± 0.59	96.85 ± 0.41	96.32 ± 0.68
Wormhole Attack	98.79 ± 0.57	96.94 ± 0.35	96.27 ± 0.47	95.32 ± 0.25
Grayhole Attack	98.35 ± 0.58	97.42 ± 0.39	95.16 ± 0.22	95.07 ± 0.59
DoS Attack	98.24 ± 0.39	96.08 ± 0.54	95.75 ± 0.34	95.3 ± 0.26
Integrated Attacks	97.19 ± 0.41	95.57 ± 0.47	93.49 ± 0.42	92.11 ± 0.57
Throughput (in kbps)				
No Attack	163.25 ± 0.42	156.18 ± 0.49	143.68 ± 0.34	120.89 ± 0.61
Blackhole Attack	154.0 ± 0.68	148.04 ± 0.67	137.09 ± 0.84	119.63 ± 0.69
Wormhole Attack	149.69 ± 0.51	143.47 ± 0.58	132.63 ± 0.84	118.62 ± 0.35
Grayhole Attack	155.07 ± 0.72	149.96 ± 0.77	135.41 ± 0.63	113.36 ± 0.52
DoS Attack	128.45 ± 0.84	127.08 ± 0.75	120.9 ± 0.39	108.15 ± 0.44
Integrated Attacks	133.15 ± 0.69	124.56 ± 0.64	118.39 ± 0.75	103.27 ± 0.37
Delay (in ms)				
No Attack	1.54 ± 0.01	1.84 ± 0.01	2.18 ± 0.01	2.86 ± 0.02
Blackhole Attack	1.9 ± 0.01	2.37 ± 0.01	2.81 ± 0.02	3.02 ± 0.01
Wormhole Attack	2.08 ± 0.01	2.83 ± 0.02	3.0 ± 0.02	3.27 ± 0.02
Grayhole Attack	2.87 ± 0.01	3.17 ± 0.02	3.41 ± 0.02	3.82 ± 0.03
DoS Attack	2.91 ± 0.01	3.16 ± 0.02	3.57 ± 0.02	3.91 ± 0.02
Integrated Attacks	3.08 ± 0.01	3.24 ± 0.01	3.92 ± 0.02	4.28 ± 0.03

The one-way ANOVA is performed on the metrics PDR, throughput, and delay across different attacks with varying numbers of nodes to assess the statistical significance of the differences. The results confirm that the performance is significantly affected by the attack type, with integrated attacks consistently reducing PDR and throughput while increasing

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

delay compared to no attack or single attacks. *Figure 11* presents the F-value graph for different metrics, which indicates the variance between attack types relative to within-group variance. The results also indicate that all differences are statistically significant ($p < 0.001$). The statistical significance demonstrates that the observed variations are not due to random chance, which also confirms the robustness and reliability of the proposed method.

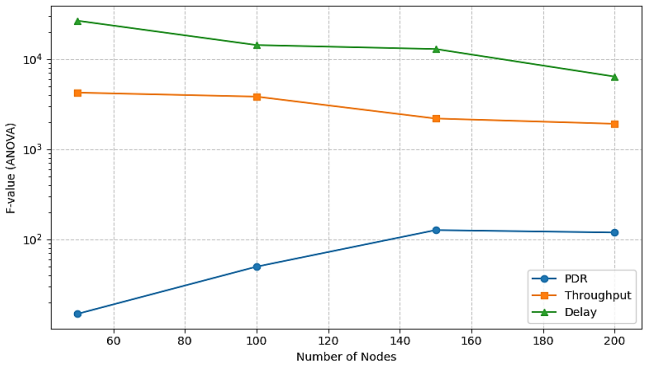

Figure 11. ANOVA test: F-values for PDR, Throughput, and Delay with varying number of nodes

4.6. Comparative Analysis

The proposed STAGNet-COpt module is also compared with some of the existing approaches by implemented them in integrated attack scenario. All the simulation parameters are kept the same as given in *table 3*. *Table 12* shows the comparison of existing ATSORS-HFO [19], TrustOpt [25], and proposed STAGNet-COpt under a varying number of nodes.

Table 12. Comparative Analysis of Proposed STAGNet-COpt with existing State-of-the-art Methods

Approaches	Number of Nodes			
	50	100	150	200
PDR (in %)				
ATSORS-HFO [19]	68.09	77.58	81.23	82.54
TrustOpt [25]	85.05	90.34	91.25	**93.51**
Proposed STAGNet-COpt	**97.25**	**95.38**	**93.56**	92.02
Throughput (in kbps)				
ATSORS-HFO [19]	70.07	78.29	83.27	85.47
TrustOpt [25]	88.29	93.54	94.76	96.57
Proposed STAGNet-COpt	**132.93**	**124.76**	**118.39**	**102.93**
Loss (in %)				
ATSORS-HFO [19]	31.91	22.42	18.77	17.46
TrustOpt [25]	14.95	9.66	8.75	**6.49**
Proposed STAGNet-COpt	**2.75**	**4.62**	**6.44**	7.98
Delay (in ms)				
ATSORS-HFO [19]	21.047	17.932	15.0892	11.386
TrustOpt [25]	13.982	10.831	9.647	7.037
Proposed STAGNet-COpt	**3.081**	**3.251**	**3.928**	**4.272**
Overhead (packets)				
ATSORS-HFO [19]	845	902	993	1062
TrustOpt [25]	546	586	604	637
Proposed STAGNet-COpt	**249**	**253**	**387**	**412**

From these results, it is clear that the proposed STAGNet-COpt architecture consistently outperforms baseline methods ATSORS-HFO and TrustOpt across all evaluated performance metrics and network densities. *Figure 12* compare the performance of different methods in terms of PDR.

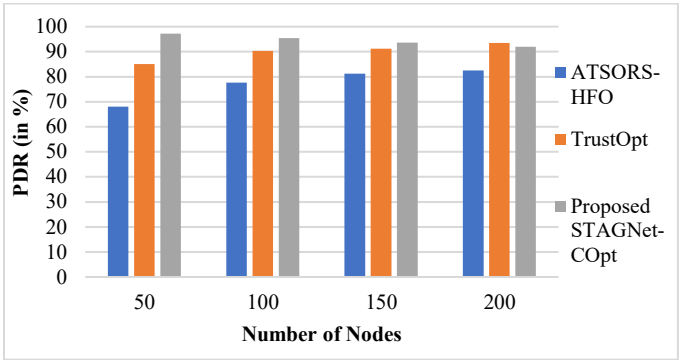

Figure 12. Comparative Analysis with varying nodes under integrated attacks in terms of PDR

In terms of Packet Delivery Ratio (PDR), it achieves a peak of 97.25% at 50 nodes and maintains >92% even at 200 nodes, significantly surpassing the others due to its spatio-temporal modeling using Graph Attention and LSTM layers. *Figure 13* compare the performance of different methods in terms of throughput.

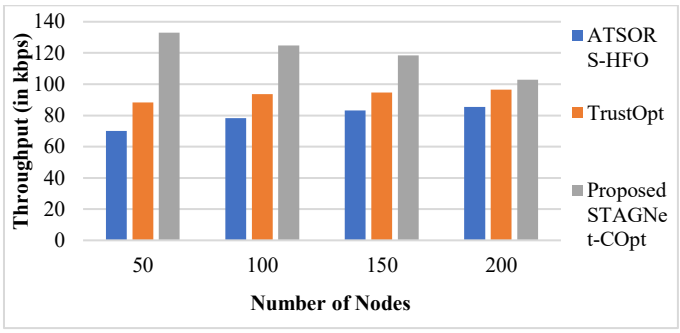

Figure 13. Comparative Analysis with varying nodes under integrated attacks in terms of throughput

STAGNet-COpt also delivers the highest throughput, maintaining over 100 kbps across all scenarios, thanks to optimized trust-aware routing and fewer retransmissions. *Figure 14* compare the performance of different methods in terms of loss ratio.

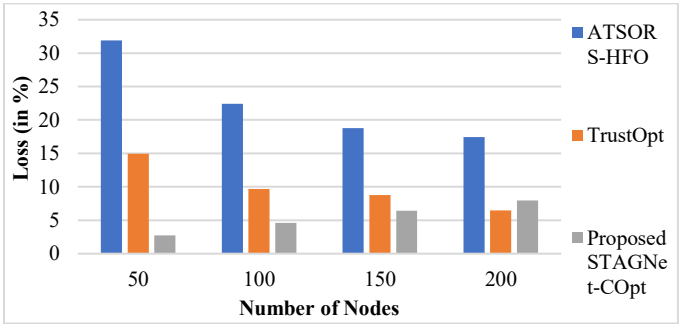

Figure 14. Comparative Analysis with varying nodes under integrated attacks in terms of loss ratio

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

Packet loss remains minimal (<8%) even in dense networks, unlike ATSORS-HFO, which experiences up to 31.91% loss due to poor attack resilience. *Figure 15* compare the performance of different methods in terms of delay.

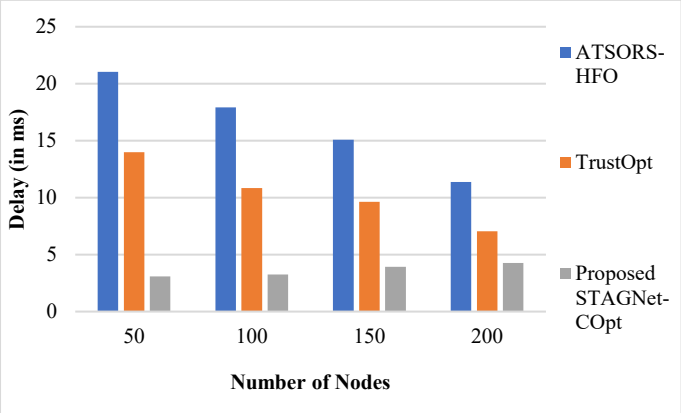

Figure 15. Comparative Analysis with varying nodes under integrated attacks in terms of delay

Remarkably, the proposed STAGNet-COpt also achieves the lowest end-to-end delay (as low as 3.08 ms) highlighting its efficiency in both detection and communication. *Figure 16* compare the performance of different methods in terms of overhead.

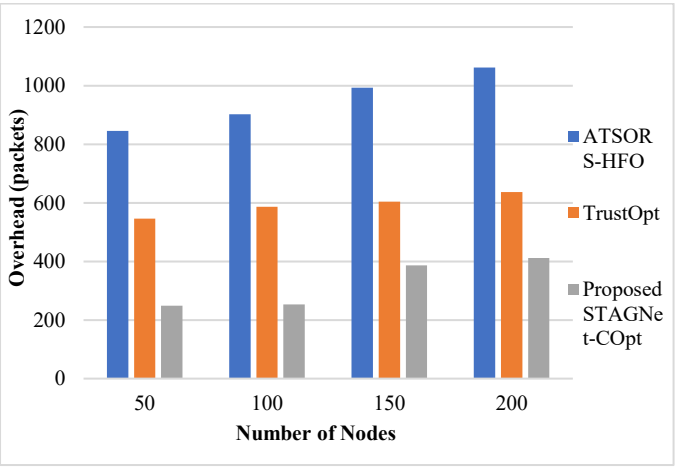

Figure 16. Comparative Analysis with varying nodes under integrated attacks in terms of overhead

Remarkably, it also achieves the smallest routing overhead (249–412 bytes), highlighting its efficiency in both detection and communication. These results validate the effectiveness of integrating TrustFuzz, STAGNet, and WOACO-R into a unified and scalable defense framework for MANETs.

The performance of the proposed method (STAGNet-COpt) is also compared with existing state-of-the-art (SOTA) methods from the literature. The comparison of the proposed method in different attack scenarios with the SOTA methods is presented in *table 13*.

Table 13. Comparison of the proposed method (STAGNet-COpt) with different SOTA methods

	PDR (in %)	Throughput (in kbps)	Delay (in sec)	Detection Accuracy (in %)
CChOA [16]	93.7	98.304	0.096	-
CNN [28]	-	-	17	85
Improved GRU [29]	93.86	167	-	-
ACO-NB [30]	60	80	0.2	-
Hybrid DL [33]	93.76	166	-	-
IGOA with DRNN [34]	-	-	-	96
HIDE-MAN [35]	-	-	-	97.4
COCG-MSA-GCNN-MA [36]	-	-	-	97.12
Proposed Method with No Attack	99.03	162.84	0.0015	98.37
Proposed Method with Blackhole Attack	98.48	153.84	0.0019	98.12
Proposed Method with Wormhole Attack	98.83	149.37	0.0021	97.84
Proposed Method with Grayhole attack	98.23	154.93	0.0029	97.81
Proposed Method with DoS attack	98.02	128.38	0.0029	97.38
Proposed Method with Integrated Attack	97.25	132.93	0.0031	97.03

The existing SOTA methods are evaluated under different simulation settings, datasets, and attack models. Despite this heterogeneous evaluation, the results demonstrated that the proposed method consistently achieved robust performance under dynamic and integrated scenarios.

5. CONCLUSION

This study introduces STAGNet-COpt, a novel and unified defense architecture for MANETs, integrating spatio-temporal attack detection, fuzzy trust-based clustering, and hybrid meta-heuristic route optimization. The proposed framework synergistically combines the strengths of GAT and LSTM for deep behavioral modeling (STAGNet), TrustFuzz for dynamic and secure cluster formation based on trust values, and WOACO-R, a hybrid Whale Optimization and Ant Colony Optimization method, for adaptive and resilient route discovery. Extensive simulations were conducted using NS-2 under diverse attack scenarios, including blackhole, wormhole, grayhole, DoS, and integrated attacks, with varying node densities. Comparative analysis against existing approaches, namely ATSORS-HFO and TrustOpt, demonstrates that STAGNet-COpt significantly enhances detection precision and routing robustness.

On average, the proposed system achieves a PDR of 94.05%, reduces packet loss to 5.45%, maintains a throughput of 119.5 kbps, achieves a low end-to-end delay of 3.63 ms, and limits routing overhead to 325.25. These results confirm that STAGNet-COpt provides superior resilience and scalability in dynamic and adversarial MANET environments. The integration of deep learning with trust-aware and optimization strategies presents a promising direction for autonomous and intelligent MANET defense systems. Future research will explore real-time deployment aspects, cross-layer optimizations, and lightweight transformer-based alternatives for further efficiency gains on edge devices.

List of Abbreviations

ACO – Ant Colony Optimization
AI – Artificial Intelligence
CCOA – Coot Chimp Optimization Algorithm
COpt – Cluster-based Optimization
DL – Deep Learning
EHO – Elk-Herd Optimization
GAT – Graph Attention Network
GA – Genetic Algorithm
HMRFOA – Hierarchical Manta Ray Foraging Optimization Algorithm
IDS – Intrusion Detection System
IEHO – Improved Elephant Herd Optimization
IoT – Internet of Things
LOA – Lyrebird Optimization Algorithm
LSTM – Long Short-Term Memory
MANET – Mobile Ad Hoc Network
ML – Machine Learning
PSO – Particle Swarm Optimization
QoS – Quality of Service
RPO – Red Panda Optimization
STAGNet – Spatio-Temporal Attention Graph Network (integrating GAT with LSTM)
STAGNet-COpt – Spatio-Temporal Attention Graph Network with Cluster-based Optimized Trust Routing
WOA – Whale Optimization Algorithm
WOACO-R – Hybrid Whale Optimization and Ant Colony Optimization-based Routing

Availability of data and material: The datasets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding: This research received no external funding from any funding agency in the public, commercial, or not-for-profit sectors.

Authors' contributions:

- **MK Brar**: Conceptualization, methodology design, development of the proposed STAGNet-COpt framework, experimental validation, and manuscript drafting.
- **S. Singh**: Data preparation, software implementation, simulation, and result analysis.
- **S. Singh**: Supervision, critical review, manuscript editing, and overall guidance of the research work.

All authors read and approved the final manuscript.

Acknowledgements: The authors would like to thank Chandigarh Engineering College, CGC Jhanjeri, and Chandigarh University for providing the necessary research facilities and academic support during this work.

Conflicts of Interest: The authors declare no conflict of interest.

Ethical Approval: The material is the author's original work, which has not been previously published.

REFERENCES

[1] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, Jul. 2003, doi: 10.1016/S1570-8705(03)00013-1.

[2] R. Sheikh, Mahakal Singh Chande, and D. K. Mishra, "Security issues in MANET: A review," in *2010 Seventh International Conference on Wireless and Optical Communications Networks - (WOCN)*, IEEE, Sep. 2010, pp. 1–4. doi: 10.1109/WOCN.2010.5587317.

[3] I. Baird, I. Wadhaj, B. Ghaleb, and C. Thomson, "Impact Analysis of Security Attacks on Mobile Ad Hoc Networks (MANETs)," *Electronics*, vol. 13, no. 16, p. 3314, Aug. 2024, doi: 10.3390/electronics13163314.

[4] A. Priyam and A. Yadav, "Challenges, Attacks, and Countermeasures for Security in MANETs-IoT," in *Cryptology and Network Security with Machine Learning*, Springer Nature, 2024, pp. 383–395. doi: 10.1007/978-981-97-0641-9_27.

[5] P. Mitra and S. Mukherjee, "A review of trust based secure routing protocols in MANETs," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, IEEE, Oct. 2015, pp. 1–7. doi: 10.1109/IEMCON.2015.7344490.

[6] G. Vidhya Lakshmi and P. Vaishnavi, "An Efficient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution," *Wirel. Pers. Commun.*, vol. 124, no. 1, pp. 333–348, May 2022, doi: 10.1007/s11277-021-09359-2.

[7] R. Popli, M. Sethi, I. Kansal, A. Garg, and N. Goyal, "Machine Learning Based Security Solutions in MANETs: State of the art approaches," *J. Phys. Conf. Ser.*, vol. 1950, no. 1, p. 012070, Aug. 2021, doi: 10.1088/1742-6596/1950/1/012070.

[8] V. R. Sugumaran, E. Dinesh, R. Ramya, and E. Muniyandy, "Distributed blockchain assisted secure data aggregation scheme for risk-aware zone-based MANET," *Sci. Rep.*, vol. 15, no. 1, p. 8022, Mar. 2025, doi: 10.1038/s41598-025-92656-8.

[9] S. Majumder, D. Bhattacharyya, and S. Chowdhuri, "ABCD: advanced blockchain DSR algorithm for MANET to mitigate the different security threats," *EURASIP J. Wirel. Commun. Netw.*, vol. 2025, no. 1, p. 8, Feb. 2025, doi: 10.1186/s13638-025-02430-7.

[10] S. S. Priya, R. Vijayabhasker, and A. Rajaram, "Advanced Security and Efficiency Framework for Mobile Ad-Hoc Networks Using Adaptive Clustering and Optimization Techniques," *J. Electr. Eng. Technol.*, vol. 20, no. 3, pp. 1815–1826, Mar. 2025, doi: 10.1007/s42835-024-02119-9.

[11] K. S. Prasanna and B. Ramesh, "Multiobjective Secure Trust Aware Redundant Array Shifting Encryption and Clustering Based Routing in Mobile Ad Hoc Networks," *Int. J. Commun. Syst.*, vol. 38, no. 5, Mar. 2025, doi: 10.1002/dac.6074.

[12] V. Nivedita, C.-S. Shieh, and M.-F. Horng, "An integrated trust-based secure routing with intrusion detection for mobile Ad Hoc network using adaptive snow geese optimization algorithm," *Ain Shams Eng. J.*, vol. 16, no. 7, p. 103385, Jul. 2025, doi: 10.1016/j.asej.2025.103385.

[13] S. Jeganathan, G. Kulandaivelu, D. Muthusamy, and K. V. Samraj, "Trust-Aware Routing Protocol Using Hierarchical Manta Ray Foraging Optimization Algorithm with Selfish Node Detection in MANET," *Int. J. Commun. Syst.*, vol. 38, no. 5, Mar. 2025, doi: 10.1002/dac.70011.

[14] K. Dalal, "Hybrid optimization-based secured routing in mobile ad-hoc network," *Intell. Decis. Technol.*, vol. 19, no. 1, pp. 312–336, Jan. 2025,

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 1| Pages 225-241|e-ISSN: 2347-470X

doi: 10.3233/IDT-240739.

[15] V. A. Khandekar and P. Gupta, "Machine learning-based hybrid SSO-MA with optimized secure link state routing protocol in Manet," *China Commun.*, vol. 22, no. 3, pp. 164–180, Mar. 2025, doi: 10.23919/JCC.ja.2023-0401.

[16] S. D and L. PH, "A secure routing and black hole attack detection system using coot Chimp Optimization Algorithm-based Deep Q Network in MANET," *Comput. Secur.*, vol. 148, p. 104166, Jan. 2025, doi: 10.1016/j.cose.2024.104166.

[17] M. V. Anand, A. Krishnamurthy, A. Kannan, and N. Govindarajan, "Secure Routing in Mobile Ad Hoc Networks with Hybrid Tasmanian Gazelle Optimization," *IETE J. Res.*, pp. 1–12, Mar. 2025, doi: 10.1080/03772063.2025.2466683.

[18] K. Saminathan, L. Perumal, F. H. Shajin, and R. K. Shakya, "Multicast On-Route cluster propagation to detect network intrusion detection systems on MANET using Deep Operator Neural networks," *Expert Syst. Appl.*, vol. 271, p. 125864, May 2025, doi: 10.1016/j.eswa.2024.125864.

[19] S. Ravi, S. Matheswaran, U. Perumal, S. Sivakumar, and S. K. Palvadi, "Adaptive trust-based secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 1, pp. 22–34, Jan. 2023, doi: 10.1007/s12083-022-01351-2.

[20] S. M. Hassan, M. Murtadha Mohamad, F. Binti Muchtar, and F. Bin Yusuf Patel Dawoodi, "Enhancing MANET Security Through Federated Learning and Multiobjective Optimization: A Trust-Aware Routing Framework," *IEEE Access*, vol. 12, pp. 181149–181178, 2024, doi: 10.1109/ACCESS.2024.3505236.

[21] J. A. Rathod and M. Kotari, "Secure and efficient message transmission in MANET using hybrid cryptography and multipath routing technique," *Multimed. Tools Appl.*, vol. 84, no. 13, pp. 12633–12656, Jun. 2024, doi: 10.1007/s11042-024-19542-9.

[22] N. Saravanan, R. Arunachalam, A. S. A. Nisha, and A. Karthikayen, "An innovative energy efficient routing protocol in MANET with hybridized osprey-fire hawk optimization algorithm to attain optimal routing constraints," *Wirel. Networks*, vol. 31, no. 3, pp. 2005–2026, Mar. 2025, doi: 10.1007/s11276-024-03867-2.

[23] P. Satyanarayana, U. B. Sofi, B. F. Ahmed, N. N. Saranya, G. V. S. P. Rao, and V. G. Krishnan, "Enhancement of Network Security in MANET Using Refined Adaptive Harris Hawks Optimization Algorithm (RAHHO) for IoT Applications," in *2024 International Conference on Emerging Smart Computing and Informatics (ESCI)*, IEEE, Mar. 2024, pp. 1–5. doi: 10.1109/ESCI59607.2024.10497254.

[24] 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," *Int. J. Inf. Technol.*, Apr. 2024, doi: 10.1007/s41870-024-01859-1.

[25] M. K. Brar, S. Singh, and S. Singh, "TrustOpt: An optimized trust-based approach for integrated attacks in MANETs," in *2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, IEEE, May 2024, pp. 534–540. doi: 10.1109/InCACCT61598.2024.10551211.

[26] R. Saravanan, K. Suresh, and S. S. Arumugam, "A modified k-means-based cluster head selection and Philippine eagle optimization-based secure routing for MANET," *J. Supercomput.*, vol. 79, no. 9, pp. 10481–10504, Jun. 2023, doi: 10.1007/s11227-023-05053-1.

[27] N. S. Naga Malleswari, D. Kalpana, S. Marlin, N. B. Sundara Ganapathy, M. Arun, and P. Satyanarayana, "Enhancement of Network Security in MANET By Using Guided Whale Optimization Algorithm (GWOA) for Solving Multiobjective Optimization," in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, Mar. 2023, pp. 1471–1476. doi: 10.1109/ICACCS57279.2023.10112966.

[28] S. R. Addula, U. Mamodiya, W. Jiang, and M. A. Almaiah, "Generative AI-Enhanced Intrusion Detection Framework for Secure Healthcare Networks in MANETs," *SHIFRA*, vol. 2025, pp. 62–68, Feb. 2025, doi: 10.70470/SHIFRA/2025/003.

[29] E. P. Krishna *et al.*, "Enhancing intrusion detection in MANETs with blockchain-based trust management and enhanced GRU model," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 1, p. 27, Jan. 2025, doi: 10.1007/s12083-024-01877-7.

[30] A. A. Abdalhameed and A. I. Kadhim, "Molecular Swarm Optimization Analysis of Data Transmission and Recurrent Neural Networks (RNNs) for Attack Prevention in Mobile Ad Hoc Networks (MANETs)," *KSII Trans. Internet Inf. Syst.*, vol. 19, no. 3, Mar. 2025, doi: 10.3837/tiis.2025.03.014.

[31] 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*, vol. 12, pp. 150046–150090, 2024, doi: 10.1109/ACCESS.2024.3457682.

[32] A. A. Alkasasbeh, "Machine Learning Approach to Detect Blackhole Attack over MANETs," in *ResearchGa*, 2025. doi: 10.1109/ICIT64950.2025.11049211.

[33] P. K. D. *et al.*, "Enhancing security and efficiency in Mobile Ad Hoc Networks using a hybrid deep learning model for flooding attack detection," *Sci. Rep.*, vol. 15, no. 1, p. 818, Jan. 2025, doi: 10.1038/s41598-024-84421-0.

[34] S. Pushpalatha and N. Narasimhulu, "A hybrid approach for detecting network layer attacks in MANET," *Int. J. Syst. Assur. Eng. Manag.*, Jun. 2025, doi: 10.1007/s13198-025-02854-w.

[35] S. F. M. Hussain and S. M. H. S. S. Fathima, "Federated Learning-Assisted Coati Deep Learning-Based Model for Intrusion Detection in MANET," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, p. 285, Nov. 2024, doi: 10.1007/s44196-024-00590-w.

[36] R. Reka, R. Karthick, R. Saravana Ram, and G. Singh, "Multi head self-attention gated graph convolutional network based multi-attack intrusion detection in MANET," *Comput. Secur.*, vol. 136, p. 103526, Jan. 2024, doi: 10.1016/j.cose.2023.103526.

[37] R. Meddeb, F. Jemili, B. Triki, and O. Korbaa, "A deep learning-based intrusion detection approach for mobile Ad-hoc network," *Soft Comput.*, May 2023, doi: 10.1007/s00500-023-08324-4.

[38] S. Shafi, S. Mounika, and S. Velliangiri, "Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET," *Procedia Comput. Sci.*, vol. 218, pp. 2309–2318, 2023, doi: 10.1016/j.procs.2023.01.206.

[39] J. Zeng, Y. Shen, S. Xu, and R. Yang, "Analysis of gastrin-17 and its related influencing factors in physical examination results," *Immunity, Inflamm. Dis.*, vol. 11, no. 10, pp. 1–5, 2023, doi: 10.1002/iid3.993.

[40] W. Villegas-Ch, J. Govea, A. Maldonado Navarro, and P. Palacios Játiva, "Intrusion Detection in IoT Networks Using Dynamic Graph Modeling and Graph-Based Neural Networks," *IEEE Access*, vol. 13, pp. 65356–65375, 2025, doi: 10.1109/ACCESS.2025.3559325.

[41] Z. Li, L. Zheng, Q. Zhang, H. Wang, Z. Du, and J. Liu, "GNSS Jamming Attacks Recognition Based on Dual GCN With Adaptive Weight Learning," *IEEE Sens. J.*, vol. 25, no. 13, pp. 26152–26168, Jul. 2025, doi: 10.1109/JSEN.2025.3571189.

[42] F. Huang, Y. Wang, W. Jiang, J. Wang, and K.-L. Hsiung, "GCAT-Based Localization of Eavesdropping Node for Power Internet of Things," *IEEE Internet Things J.*, vol. 12, no. 13, pp. 25804–25822, Jul. 2025, doi: 10.1109/JIOT.2025.3559503.