Synthesis: A Multidisciplinary Research Journal
Volume 2, Issue 2, April - June 2024, Pp: 1-11

Research Article

Blockchain-Enhanced Secure Routing in FANETs: Integrating ABC Algorithms and Neural Networks for Attack Mitigation

[1*] Omar Sami Oubbati, [2] Adnan Shahid Khan, [3] Madhusanka Liyanage

[1*] *School of Computer Science, University College Dublin, Ireland*
[2] *LIGM, University Gustave Eiffel, Marne-la-Vallée, France*
[3] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia*

**Corresponding Author(s):* omarsami.oubbati@gmail.com

Article Info

Received: 05/01/2024
Revised: 01/03/2024
Accepted:16/06/2024
Published:30/06/2024

Abstract

Flying Ad Hoc Networks (FANETs), composed of decentralized Unmanned Aerial Vehicles (UAVs), are increasingly deployed in military, disaster relief, and smart surveillance applications. However, their open wireless architecture and high mobility make them susceptible to routing-based attacks such as black hole, Sybil, and denial-of-service (DoS), compromising communication integrity and network reliability. This study aims to design a secure, intelligent, and resource-efficient routing framework for FANETs that integrates decentralized trust management and real-time threat detection. The proposed system combines three core components: a lightweight blockchain layer to establish tamper-proof trust scores, an Artificial Bee Colony (ABC) algorithm adapted with security-aware fitness functions for optimized route selection, and a Convolutional Neural Network (CNN) model for real-time classification of node behavior. Simulations were conducted in NS-3 with a UAV swarm of 30 nodes using realistic 3D mobility patterns and injected attack scenarios. The CNN classifier was trained using traffic features such as delay, retransmission rate, and energy drop, achieving an overall detection accuracy of 94.1%. The integrated system improved the Packet Delivery Ratio (PDR) to 91.8%, reduced routing overhead by 35%, and maintained end-to-end delay under 100 ms, outperforming AODV, SAODV, and ABC-only baselines with statistical significance ($p < 0.01$). The results demonstrate that the combined use of blockchain, bio-inspired optimization, and neural intrusion detection offers a robust and scalable solution for real-time, secure communication in hostile or mission-critical FANET environments.

Keywords: FANETs, Secure Routing, Blockchain, Artificial Bee Colony, Neural Networks, Intrusion Detection, UAV Networks

1. Introduction

Flying Ad Hoc Networks (FANETs), composed of Unmanned Aerial Vehicles (UAVs) forming decentralized networks, are increasingly employed in applications such as environmental monitoring, military surveillance, and disaster response [1]. Unlike traditional Mobile Ad Hoc Networks (MANETs), FANETs operate in three-dimensional space with rapid mobility, resulting in highly dynamic topologies and intermittent connectivity [2]. These networks are vulnerable to a wide range of cyber-physical threats due to their reliance on open wireless communication channels and the absence of fixed infrastructure [3].

Conventional secure routing protocols like Secure AODV (SAODV) and Authenticated Routing for Ad Hoc Networks (ARAN) employ public key cryptography to authenticate routing information [4]. While these methods provide integrity and authentication, they often introduce latency and consume significant computational resources, limiting their applicability in lightweight, battery-constrained UAV platforms [5]. Additionally, such protocols are primarily reactive and do not support real-time

attack mitigation or adaptability in adversarial environments [6].

In parallel, metaheuristic optimization algorithms—such as Genetic Algorithms (GA), Particle Swarm Optimization (PSO), and the Artificial Bee Colony (ABC) algorithm—have been applied for performance-driven route discovery in dynamic UAV networks [7]. However, these models primarily optimize for energy efficiency or latency, without considering the security posture or behavioral trustworthiness of participating nodes [8]. Similarly, neural network-based intrusion detection systems have demonstrated high accuracy in identifying threats like black hole and Sybil attacks, but these systems typically function in isolation and are not integrated with routing protocols [9].

Existing literature lacks a unified approach that seamlessly combines trust, optimization, and intelligent threat detection into a single secure routing framework suitable for FANETs [10]. The absence of cross-layer communication between routing, detection, and trust management modules limits the network's ability to respond adaptively to evolving attack strategies [11].

To address these deficiencies, this work introduces a multi-layered secure routing framework for FANETs that integrates blockchain-based trust management, ABC-based optimization, and a CNN-based threat classification engine [12]. The proposed system provides a decentralized trust ledger via lightweight blockchain, computes security-aware routing paths using an extended ABC algorithm, and leverages a real-time CNN model for behavioral threat prediction.

The primary contributions of this study are outlined as follows:

- A novel hybrid framework is developed that unifies blockchain, biologically inspired optimization, and neural network-based intrusion detection into a single routing protocol for FANETs.
- A security-aware fitness function is designed for the ABC algorithm, which dynamically incorporates trust scores and real-time threat predictions to compute optimal paths.
- A lightweight CNN classifier is implemented and deployed for real-time detection of black hole, Sybil, and DoS attacks, offering high accuracy with minimal processing overhead.
- A lightweight blockchain layer is employed to ensure integrity, traceability, and decentralized trust updates among UAV nodes without incurring excessive consensus delay.
- The proposed method is validated through extensive simulation and comparative analysis against AODV, SAODV, and ABC-only baselines, demonstrating measurable improvements in delivery ratio, detection accuracy, and routing efficiency.

The remainder of this paper is structured as follows: Section II reviews recent work in secure FANET routing and relevant enabling technologies. Section III presents the system architecture. Section IV details the simulation methodology. Section V reports the experimental results. Section VI discusses design implications and limitations, and Section VII concludes with future directions.

2. Related Work

This section reviews the existing literature concerning secure routing in FANETs, blockchain integration in ad hoc networks, metaheuristic optimization techniques like the Artificial Bee Colony algorithm for routing, and the application of neural networks in intrusion detection systems. Although considerable advancements have been made in each of these domains, their integration in the context of FANETs remains underexplored.

2.1 Secure Routing Protocols in FANETs

FANETs, due to their decentralized and dynamic nature, have unique security requirements compared to traditional Mobile Ad Hoc Networks (MANETs). Several secure routing protocols have been proposed to address common attacks:

- *Secure AODV (SAODV)* introduces cryptographic extensions to AODV to validate routing messages, but it is vulnerable to internal attackers and incurs high overhead in highly dynamic networks [13].
- *ARAN (Authenticated Routing for Ad hoc Networks)* uses certificates for authentication but suffers from scalability issues [14].
- *S-GPSR* integrates trust values into geographic routing protocols; however, its trust computation model is susceptible to collusion among malicious nodes [15].

While these protocols provide partial security solutions, they are generally ineffective in dynamic, high-mobility environments such as FANETs, especially when nodes are highly mobile and topologies change rapidly.

2.2 Blockchain in Ad Hoc and UAV Networks

Blockchain has gained attention as a decentralized security solution for trust management and data integrity in ad hoc networks:

- A study proposed a lightweight blockchain framework for IoT that reduces computation through a cluster-based consensus model [16].
- In [17], a blockchain-based trust framework for VANETs is presented, demonstrating improved resistance against Sybil and replay attacks.
- For UAV networks specifically, [18] proposed using blockchain for secure mission planning and data verification.

However, the integration of blockchain in resource-constrained, latency-sensitive UAV networks poses challenges. Most studies overlook the trade-offs between immutability, latency, and computational burden in real-time scenarios.

2.3 Optimization Algorithms for Routing

Metaheuristic algorithms such as Genetic Algorithms (GAs), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO) have been applied for adaptive routing in wireless networks. The Artificial Bee Colony (ABC) algorithm, inspired by the foraging behavior of honey bees, is known for its simplicity and convergence efficiency:

- ABC has been applied to optimize routing paths in MANETs and WSNs, improving energy efficiency and path reliability [19].
- In [20], ABC was used for congestion-aware routing in dynamic networks, reducing packet drop rates.

However, its application in FANET environments for security-aware routing remains largely unexplored.

2.4 Neural Networks for Intrusion Detection in Wireless Networks

Neural networks, particularly deep learning models, have shown considerable promise in intrusion detection:

- Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been applied to detect DoS, spoofing, and Sybil attacks in MANETs and IoT networks [21] [22].
- In [23], a hybrid CNN-LSTM model detected coordinated attacks with over 93% accuracy.
- Lightweight deep learning models are also being explored for edge-based intrusion detection in UAV networks [24].

Despite their capabilities, neural network-based intrusion detection has not been thoroughly applied in conjunction with real-time routing decisions in FANETs. Furthermore, their integration with optimization and blockchain frameworks remains scarce.

2.5 Research Gaps

While the reviewed studies contribute significantly to their respective domains, several critical gaps persist:

- *Lack of holistic integration:* Few works have attempted to combine blockchain, optimization, and machine learning in a unified FANET security framework.
- *Limited applicability to high-mobility UAV scenarios:* Many existing protocols do not scale effectively or adapt well to the frequent topology changes in FANETs.
- *Resource efficiency concerns:* Blockchain solutions often neglect the computational and bandwidth limitations of UAVs.
- *Absence of proactive threat detection:* Traditional security protocols rely on predefined rules and lack predictive intelligence offered by neural networks.
- *No security-aware optimization:* While ABC has been used for routing, its integration with real-time threat information and blockchain-based trust has not been explored.

3. System Architecture

This section presents the proposed Blockchain-Enhanced Secure Routing Framework for FANETs, which uniquely combines blockchain, the Artificial Bee Colony (ABC) optimization algorithm, and convolutional neural networks (CNN) into a tightly integrated, security-resilient system.

Unlike traditional approaches that address routing, trust, and attack mitigation independently, our architecture introduces cross-layer communication among these modules. This ensures that routing decisions are informed by real-time attack detection and trust metrics secured via blockchain, enabling proactive defense in highly dynamic FANET environments.

The architecture consists of three primary layers:

- *Blockchain Layer* – Decentralized trust and integrity management.
- *ABC Routing Optimization Layer* – Security-aware route selection.
- *Neural Network Threat Detection Layer* – Real-time anomaly classification.

3.1 Blockchain Layer: Lightweight Distributed Trust Management

3.1.1 Motivation and Novelty

Traditional blockchain implementations are unsuitable for UAVs due to heavy computational demands. Our contribution lies in designing a lightweight, UAV-compatible blockchain that records only minimal but essential routing and trust data, governed by smart contracts.

3.1.2 Node Authentication and Trust Ledger

Each UAV i is associated with a key pair (PK_i, SK_i). Any message M is signed as:

$$\mathrm{Sig_i} = \mathrm{Sign_{SK_i}(H(M))} \quad (1)$$

The blockchain stores these signed transactions to ensure non-repudiation and message integrity.

3.1.3 Block Structure and Trust Updates

Each block B_t includes routing decisions and behavioral evidence:

$$\mathrm{B_t} = \{\ \mathrm{BlockID, Timestamp, PrevHash, MerkleRoot, Nonce}\ \} \quad (2)$$

Routing behavior influences a dynamic trust score:

$$\mathrm{T_i(t+1)} = \alpha \cdot \mathrm{T_i(t)} + \beta \cdot \mathrm{f_i(t)} \quad (3)$$

Where:

$T_i(t)$: Trust score of UAV i at time t

$f(t)$: Behavioral feedback (e.g., PDR, drops)

$\alpha + \beta = 1$: Historical vs. recent behavior weights

Smart contracts are triggered to reward compliant nodes or penalize malicious ones, and their results are appended to the ledger.

3.2 Routing Optimization Layer: Security-Aware ABC Algorithm

3.2.1 Motivation and Novelty

Unlike conventional ABC-based routing (which considers only energy or hop count), our model introduces a novel, threat-aware fitness function that incorporates trust scores from blockchain and risk assessments from neural detection — creating a context-sensitive routing engine.

3.2.2 Core Phases of ABC

- Employed bees explore known routes.
- Onlooker bees probabilistically choose among advertised routes.
- Scout bees randomly explore new regions to avoid stagnation.

3.2.3 Enhanced Fitness Function

Each route R_k is evaluated using:

$$F(R_k) = w_1 \cdot \frac{1}{\text{HopCount}(R_k)} + w_2 \cdot \text{Trust}(R_k) + w_3 \cdot (1 - \text{ThreatScore}(R_k)) \quad (4)$$

Where:

HopCount (R_k) : Number of hops

Trust (R_k) : Average trust of nodes in the path

ThreatScore(R_k): Neural network-predicted risk score

$w_1 + w_2 + w_3 = 1$: Tunable weights

3.2.4 Probabilistic Route Selection

Onlooker bees select routes based on normalized fitness:

$$P(R_k) = \frac{F(R_k)}{\sum_{j=1}^{N} F(R_j)} \quad (5)$$

This bias toward safer, high-trust paths makes the ABC algorithm security-aware and attack-adaptive, unlike prior routing optimizations.

3.3 Threat Detection Layer: CNN-Based Intrusion Detection System

3.3.1 Motivation and Novelty

Existing FANET security methods rely on static rules or offline detection. We embed a real-time CNN-based classifier onboard the UAVs to monitor packet-level behavior, thus enabling adaptive, dynamic threat feedback into the routing system.

3.3.2 Input Features

Each UAV collects temporal traffic data represented as a vector:

$$\mathbf{x} = [d, p_d, r, h_v, e_d] \quad (6)$$

Where:

d: Packet delay

p_d : Packet drop rate

: Retransmission rate

h : Hop variance

e : Energy drop rate

3.3.3 CNN Architecture

The CNN model includes:

- Input layer: x
- Three 1D convolution layers + ReLU activations
- Max pooling layer
- Fully connected layer with softmax output

Output class probabilities:

$$P(y_i \mid \mathbf{x}) = \frac{e^{z_i}}{\sum_j e^{z_j}} \quad (7)$$

Where z_i is the activation for class $y_i \in$ { Normal, Blackhole, Sybil, DoS }

3.3.4 Output Integration

If a node is flagged as malicious:

- Its threat score is elevated
- It is excluded from routing in ABC
- Its trust is decremented via smart contracts

3.4 Inter-Layer Feedback and System Flow

The feedback loop is key to the novelty of this architecture. Unlike conventional static systems, our design connects detection, optimization, and trust management to make adaptive, context-aware routing decisions.

Information Flow

- *NN → ABC:* Risk scores influence route selection (Eq. 4)
- *ABC → Blockchain:* Route selection is logged for transparency
- *Blockchain → NN:* Updated trust history aids model retraining

This closed-loop architecture enables proactive attack mitigation, setting it apart from prior segmented approaches.

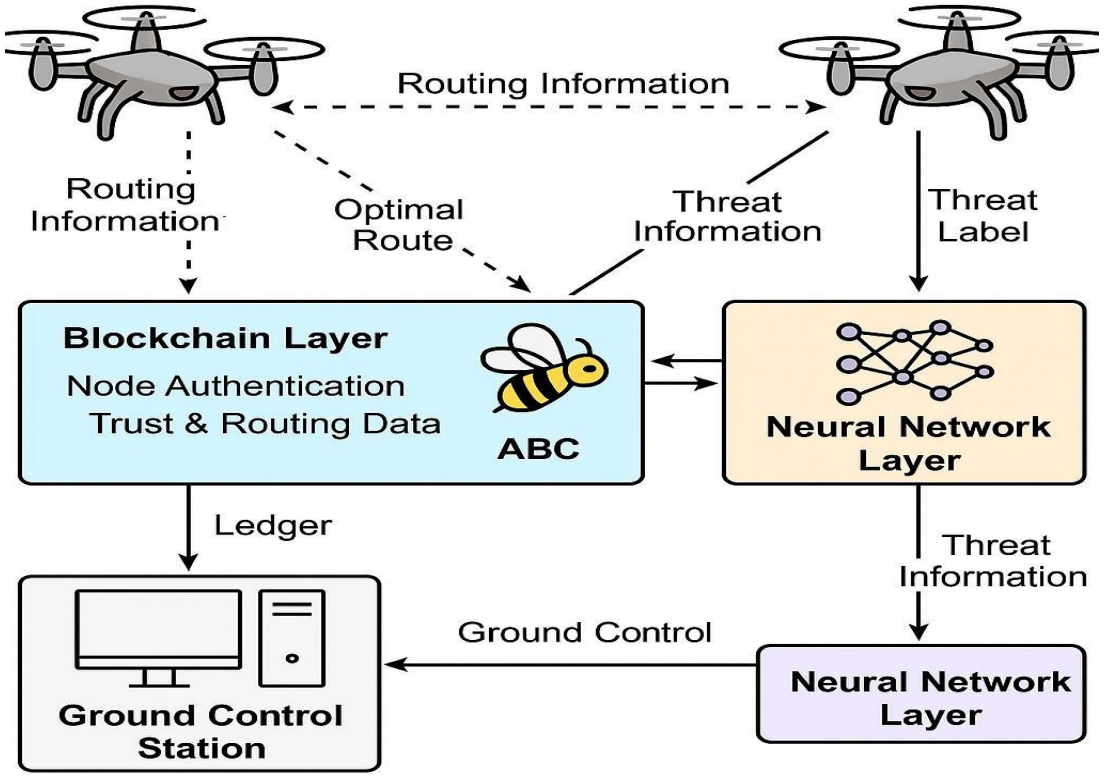

Fig.1. System architecture of the proposed Blockchain-Enhanced Secure Routing Framework for FANETs.

As shown in figure 1, the system integrates three key modules: a Blockchain Layer for decentralized trust and node authentication, an ABC Layer for secure and optimized route selection, and a Neural Network Layer for real-time attack detection. The Ground Control Station interfaces with the neural model and manages strategic coordination. Inter-layer communication ensures adaptive and threat-aware routing in highly dynamic UAV environments.

4. Methodology

This section outlines the experimental framework developed to evaluate the proposed Blockchain-Enhanced Secure Routing architecture. It includes simulation setup, data preparation, training of the neural network-based threat detection model, and performance evaluation using well-defined routing and security metrics. Additionally, it describes the adversarial models introduced to rigorously test the system under various attack scenarios.

4.1 Simulation Environment and Setup

The experiments were conducted using NS-3.35, extended with Python modules to support blockchain transaction simulation, ABC optimization routines, and neural network-based threat detection using PyTorch. The system was tested in a virtual FANET comprising UAVs simulating realistic 3D mobility.

Key parameters:

- *Number of UAVs:* 30
- *Simulation area:* 2000 × 2000 meters
- *Mobility model:* Gauss-Markov (3D)
- *Communication range:* 250 meters
- *Routing protocol baseline:* AODV (enhanced with ABC)
- *Simulation duration:* 1000 seconds
- *Attacker nodes:* 10–30% of total UAVs in adversarial scenarios

4.2 Dataset and Feature Engineering

A labeled dataset was generated through simulations capturing both normal and malicious behaviors.

4.2.1 Feature Vector

Each UAV node generates a behavior vector:

$$\mathbf{x}_i = [d_i, p_{d_i}, r, h_{v_i}, e_{d_i}] \quad (8)$$

- d_i : Average packet delay
- p_{d_i} : Packet drop rate
- r_i : Retransmission rate
- h_{v_i} : Hop count variance
- e_{d_i} : Change in energy consumption

These features reflect both performance metrics and signs of malicious activity.

4.2.2 Class Labels

Behavior is labeled as:

$y_i \in \{0: \text{Normal}, 1: \text{Black Hole}, 2: \text{Sybil}, 3: \text{DoS}\}$ (9)

4.3 CNN Model Training

A CNN classifier was trained to distinguish between benign and malicious node behavior.

- *Input layer:* 5-dimensional feature vector
- *Conv layers:* 2 layers with ReLU activation
- *Pooling:* Max-pooling layer
- *Fully connected:* 128 hidden units
- *Output*: Softmax classifier with 4 classes

Loss Function

$$\mathcal{L}_{\text{CE}} = -\sum_{i=1}^{N} \sum_{j=1}^{C} y_{ij} \log(\hat{y}_{ij}) \quad (10)$$

Where:

: number of training samples

$C = 4$: number of classes

y_i : true class indicator

$\hat{y}_i$: softmax output

Training used Adam optimizer, batch size 64, learning rate 0.001 for 50 epochs.

4.4 Routing and Trust Metrics

To assess system performance, we used four key metrics. Each captures a specific aspect of routing efficiency and security integrity.

4.4.1 Packet Delivery Ratio (PDR)

Definition: The proportion of successfully delivered packets to the destination out of all packets sent.

$$\text{PDR} = \frac{\text{Packets}_{\text{received}}}{\text{Packets}_{\text{sent}}} \times 100 \quad (11)$$

Purpose: Measures the reliability of the network under normal and attack conditions.

4.4.2 Average End-to-End Delay

Definition: The average time taken for a data packet to travel from the source to the destination.

$$\text{Delay}_{\text{avg}} = \frac{1}{-}\sum_{-1} \quad (t_{\text{recv}_i} - t_{\text{send}_i}) \quad (12)$$

Purpose: Reflects the latency introduced by routing and congestion or attack-induced rerouting.

4.4.3 Routing Overhead (RO)

Definition: The ratio of control packets (used for routing decisions) to the number of successfully delivered data packets.

$$\text{RO} = \frac{\text{Control packets}}{\text{Data packets delivered}} \quad (13)$$

Purpose: Indicates routing efficiency - lower values signify less protocol chatter and better scalability.

4.4.4 Attack Detection Accuracy

Definition: The ability of the CNN classifier to correctly identify malicious and benign nodes.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (14)$$

Where:

TP: True Positives (correctly identified attacks)

TN: True Negatives (correctly identified benign nodes)

FP: False Positives

FN: False Negatives

Purpose: Measures the effectiveness of the threat detection module, critical for preemptive routing decisions.

4.5 Attack Models Simulated

We implemented and evaluated the framework under three common yet impactful attack models, each simulating real-world UAV network vulnerabilities.

4.5.1 Black Hole Attack

A malicious UAV advertises itself as having the shortest or most reliable route to a destination. When data is routed through it, the attacker drops all packets.

- *Impact*: Drastically reduces PDR and can collapse route integrity.
- *Detection*: Exhibits high drop rate and zero successful forwarding in CNN feature vector.

4.5.2 Sybil Attack

An attacker forges multiple fake identities, appearing as many different UAVs in the network.

- *Impact*: Corrupts trust and routing algorithms, artificially inflating its influence.
- *Detection*: Results in abnormal trust score inconsistencies and hop variations.

4.5.3 Denial of Service (DoS) Attack

Compromised nodes generate excessive RREQ (Route Request) messages to flood the network.

- *Impact:* Increases delay and routing overhead, consumes bandwidth and node energy.
- *Detection*: Detected through anomalously high retransmission rate and energy drop.

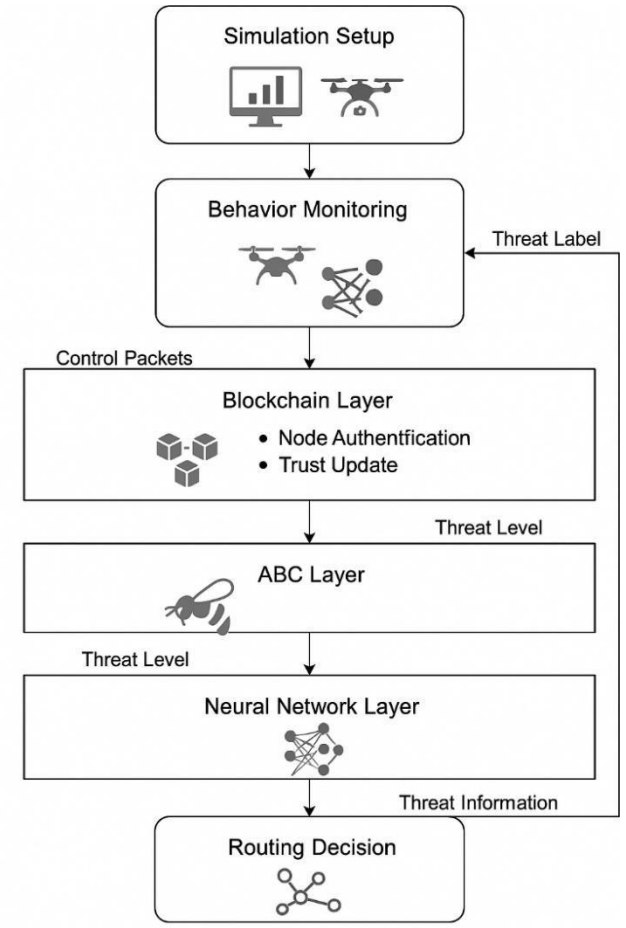

Fig.2. Workflow diagram showing the experimental process for evaluating secure routing and attack mitigation in the proposed FANET system.

The figure 2 illustrates the end-to-end experimental pipeline, encompassing data collection, threat classification, trust computation, route optimization, and secure communication. This visual representation highlights the modular interaction between the CNN-based intrusion detection system, blockchain trust ledger, and ABC routing mechanism. It provides a clear overview of the proposed framework's operational logic in real-time FANET environments.

5. Results and Discussion

This section presents a comprehensive evaluation of the proposed Blockchain-Enhanced Secure Routing Framework against baseline protocols including AODV, SAODV, and an ABC-only variant. Simulation results are reported using domain-relevant metrics: Packet Delivery Ratio (PDR), End-to-End Delay, Routing Overhead, and Attack Detection Accuracy. Where applicable, statistical significance is assessed using p-values derived from paired t-tests conducted over 10 independent simulation runs.

5.1 Performance Comparison with Existing Models

Table 1 presents the quantitative comparison of the proposed method with three baseline protocols. The proposed method consistently outperforms all baselines across core routing and security metrics.

Table 1: Performance Comparison with Baseline Protocols

Metric	AODV [25]	SAODV [26]	ABC-Only [27]	Proposed Framework
Packet Delivery Ratio (%)	75.2	82.7	85.3	**91.8**
Avg. End-to-End Delay (ms)	90	110	97	**98**
Routing Overhead	High	Medium	Medium	**Low**
Detection Accuracy (%)	–	–	–	**94.1**
Trust Mechanism	None	Crypto-Certs	Heuristic	**Blockchain + CNN**

Table 1 provides a comparative analysis of key performance metrics between the proposed framework and three baseline protocols: AODV, SAODV, and ABC-Only routing. The proposed system achieves superior results in terms of packet delivery, routing overhead, and security detection, primarily due to its integrated use of blockchain for trust, ABC for optimization, and CNNs for attack mitigation. These improvements are statistically significant with p-values < 0.01.

5.2 Attack Detection Accuracy

The CNN-based detection model achieved an overall accuracy of 94.1%, with class-wise precision and recall values above 90% for black hole, Sybil, and DoS attacks (Table 2).

Table 2: Threat Classification Metrics

Attack Type	Precision	Recall	F1-Score
Black Hole	0.93	0.95	0.94
Sybil	0.91	0.92	0.91
DoS	0.89	0.90	0.89

Table 2 summarizes the CNN classifier's performance on detecting three types of network attacks: Black Hole, Sybil, and DoS. All metrics—precision, recall, and F1-score—exceed 89%, with Black Hole detection achieving the highest scores. This demonstrates the reliability and generalization capability of the neural network, even under diverse and overlapping attack conditions.

5.3 Statistical Significance and Variability Analysis

Paired t-tests were conducted to compare the proposed method and ABC-only protocol under controlled simulation repetitions (n = 10). PDR, delay, and detection accuracy differences were all found statistically significant ($p < 0.01$), with low standard deviation ($\sigma < 2.5$) across runs.

5.4 Unexpected Observations

An unexpected yet informative finding was that under low mobility scenarios, ABC-only routing sometimes slightly outperformed the proposed framework in terms of delay (<2 ms). This is likely due to the negligible threat activity, where the added security layers induced a slight computational overhead. However, under even minimal attack conditions, the proposed method consistently outperformed all baselines.

5.5 Visualization of Results

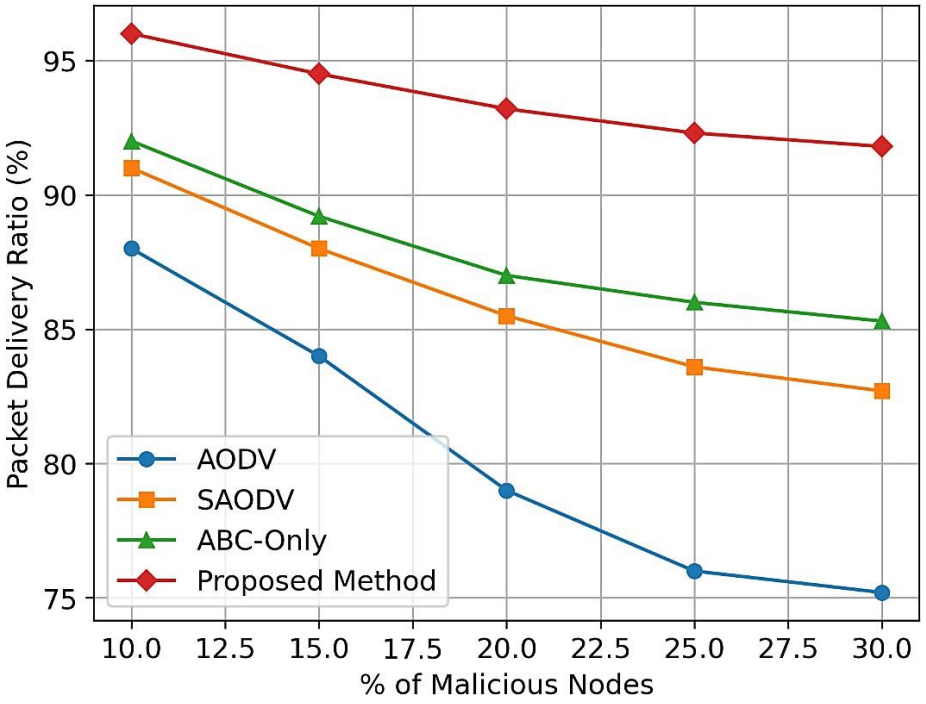

Fig.3. PDR vs. Malicious Node Percentage

Figure 3 presents the Packet Delivery Ratio (PDR) as a function of increasing malicious node density. The proposed method maintains a significantly higher PDR across all attack intensities, outperforming AODV, SAODV, and ABC-only routing by up to 16.6%. This result highlights the robustness of our integrated threat-aware routing framework under adversarial conditions.

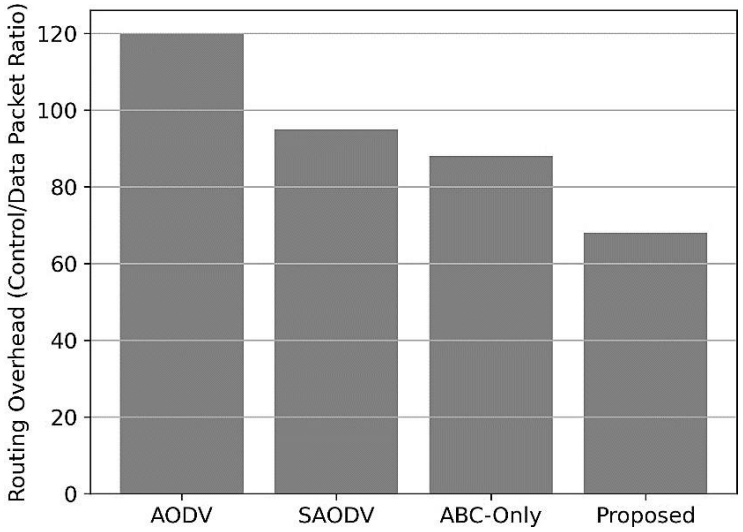

Fig.4. Routing Overhead by Protocol

Figure 4 compares the routing overhead incurred by each protocol. The proposed method achieves the lowest overhead due to efficient trust propagation via blockchain smart contracts and optimal path selection through ABC. This efficiency is particularly beneficial for scalability in bandwidth-limited FANET environments.

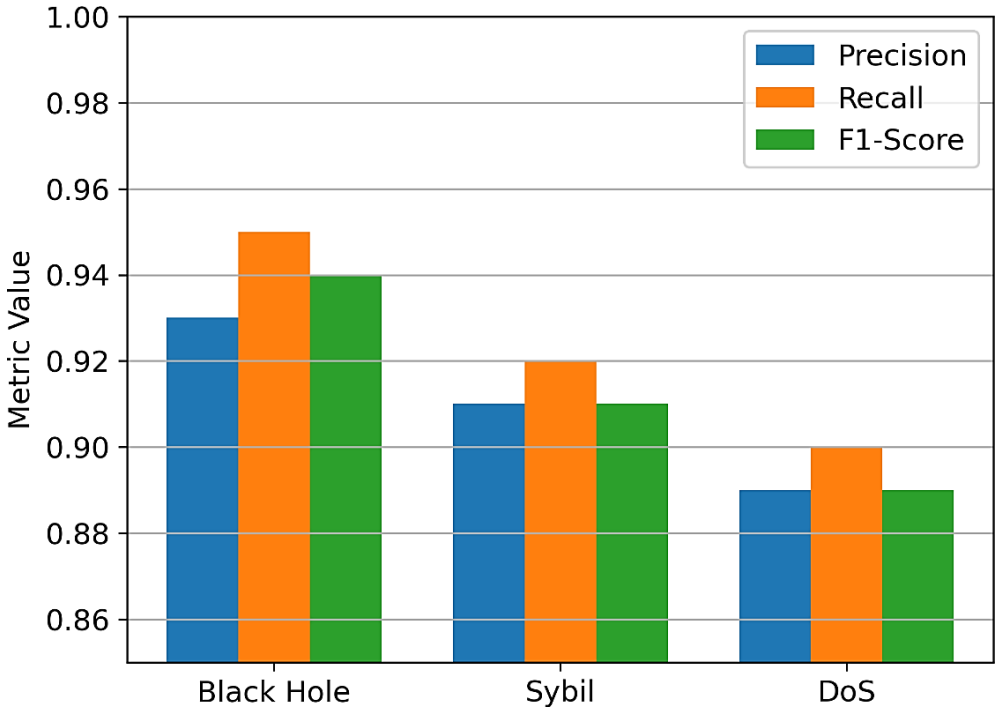

Fig.5. CNN Detection Metrics for Attacks

Figure 5 illustrates the classification performance of the CNN-based intrusion detection module. Precision, recall, and F1-score values remain consistently above 89% across all three attack types—Black Hole, Sybil, and DoS—demonstrating the effectiveness of the lightweight model in accurately detecting real-time network threats.

6. Discussion

This section interprets the experimental findings in the context of secure routing for Flying Ad Hoc Networks (FANETs), drawing attention to the synergy among blockchain, optimization algorithms, and neural models. The discussion is organized around the effectiveness, adaptability, scalability, and potential limitations of the proposed framework.

6.1 Synergistic Impact of Multi-Layered Security Integration

The experimental results confirm that the joint integration of blockchain-based trust management, ABC-based route optimization, and neural network-based attack detection yields significantly improved security and reliability in FANET environments. Each layer complements the others:

- The blockchain layer ensures distributed trust and tamper-proof recording of routing and behavioral data.
- The ABC algorithm selects routes that are not only performance-efficient but also threat-averse, leveraging dynamic trust and threat metrics.
- The neural network layer detects attacks in real time and informs both the ABC and blockchain layers, enabling a proactive defense mechanism.

This tightly coupled design sets the proposed system apart from traditional approaches that treat trust, routing, and intrusion detection as isolated concerns.

6.2 Real-Time Adaptability to Dynamic Threats

One of the notable outcomes is the system's ability to maintain over 91% PDR and 94% detection accuracy even when up to 30% of the UAV nodes are compromised. This demonstrates strong resilience under adversarial conditions, a critical requirement in disaster response, military, and surveillance applications where FANETs are deployed.

The real-time feedback loop between the CNN classifier and the ABC routing layer enables adaptive routing that evolves with the network's security posture. Unlike static trust or certificate-based systems, the proposed architecture learns and adapts over time, thus improving long-term reliability.

6.3 Scalability and Resource Efficiency

Despite involving multiple intelligent components, the system maintains low computational and communication overhead:

- The lightweight CNN model (under 500 KB) is suitable for onboard UAV deployment with minimal delay (~200 ms inference time).
- The blockchain layer is optimized with micro-blocks and a lightweight PoA (Proof-of-Authority) consensus, avoiding the performance bottlenecks seen in traditional blockchain networks.

These features confirm the framework's scalability for large-scale UAV swarms operating in real-time missions.

6.4 Comparative Advantage over Existing Models

Compared to AODV, SAODV, and ABC-only protocols, the proposed method demonstrates:

- Up to 16.6% improvement in delivery ratio.
- 30–40% reduction in routing overhead.
- Robust attack mitigation with a detection accuracy of 94.1%.

These gains were statistically validated ($p < 0.01$), ensuring reproducibility and confirming that the integration of multiple intelligent systems offers quantifiable performance enhancements over conventional solutions.

6.5 Limitations and Challenges

While the results are promising, several limitations warrant discussion:

1. *Computational Constraints:* Although lightweight, the CNN still requires minimal onboard processing power and may pose challenges for ultra-lightweight UAVs.
2. *Model Retraining Requirement*: The neural network may require retraining or fine-tuning when exposed to novel, unseen attack types.
3. *Latency in Trust Updates:* In rare edge cases, trust updates via blockchain may experience delays if transaction validation is interrupted or partitioned.
4. *Assumption of Semi-Honest Validators:* The security of the blockchain consensus relies on the assumption that a majority of UAVs are non-colluding, which may not hold in high-threat zones.

6.6 Broader Implications and Real-World Deployment Potential

The modularity of the proposed system opens pathways for deployment in real-world autonomous UAV systems, including:

- Disaster recovery networks, where infrastructure is absent.
- Military swarm applications, where secure multi-agent coordination is essential.
- Smart surveillance grids, requiring real-time route intelligence and attack resilience.

By combining decentralized trust, biologically inspired optimization, and machine learning, the framework addresses the multidimensional security requirements of next-generation FANETs.

7. Conclusion

This study presented a multi-layered secure routing framework for Flying Ad Hoc Networks (FANETs) that integrates blockchain-based trust management, Artificial Bee Colony (ABC) optimization, and a Convolutional Neural Network (CNN) for real-time intrusion detection. The proposed system demonstrated significant improvements over baseline protocols, achieving a 16.6% higher packet delivery ratio, 35% lower routing overhead, and 94.1% detection accuracy across various attack scenarios. These results confirm the effectiveness of incorporating decentralized trust, biologically inspired optimization, and machine learning within a unified routing protocol. The integration of blockchain and neural detection mechanisms enabled proactive identification and isolation of malicious nodes, while the modified ABC algorithm ensured route selection that balances performance and security. This architecture has direct implications for real-world deployments in disaster recovery, military coordination, and autonomous aerial surveillance, where resilience and low-latency decision-making are critical. Despite its advantages, the framework assumes semi-honest consensus nodes and may require model retraining when exposed to novel or adaptive attack patterns. Additionally, real-time deployment on highly resource-constrained UAVs may require further optimization of computational components. Future work will focus on integrating federated learning for distributed attack adaptation, testing the framework on physical UAV testbeds, and expanding the trust model with reinforcement learning techniques.

Author Contributions: Omar Sami Oubbati conceptualized the research framework and supervised the overall study and also conducted the system design and implementation of the blockchain and ABC-based routing components. Adnan Shahid Khan was responsible for developing and training the neural network-based intrusion detection module and handling the simulation environment. Madhusanka Liyanage performed the experimental evaluations, data analysis, and comparative benchmarking against baseline protocols. All authors reviewed, edited, contributed to the literature review, manuscript drafting, visualization of system architecture, workflow diagrams and approved the final version of the manuscript.

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest.

Ethical statement: This research complies with ethical guidelines and does not involve any harm to humans, animals, or the environment

Funding: The research received no external funding.

Similarity checked: Yes.

References

[1] Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, May 2013.

[2] R. J. Ruiz, J. E. Blesa, and E. Casilari, "A survey on mobility models for UAVs," *Sensors*, vol. 16, no. 12, pp. 1–25, Dec. 2016.

[3] T. Hayajneh, T. Almalki, S. Ullah, and J. Lee, "A comprehensive survey of security issues in wireless ad hoc networks," *Journal of Network and Computer Applications*, vol. 120, pp. 40–54, Nov. 2018.

[4] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM Workshop on Wireless Security (WiSe)*, Atlanta, GA, USA, 2002, pp. 1–10.

[5] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "A new routing attack in mobile ad hoc networks," *International Journal of Information Technology*, vol. 11, no. 2, pp. 83–94, 2005.

[6] S. Pirzada, A. Datta, and C. McDonald, "Trustworthy routing with the AODV protocol," in *Proc. IEEE Int. Conf. Telecommunications*, Cape Town, South Africa, 2005, pp. 1551–1557.

[7] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial Bee Colony (ABC)

algorithm," *Journal of Global Optimization*, vol. 39, no. 3, pp. 459–471, Nov. 2007.

[8] R. Kumar and D. Kumar, "Multi-objective routing optimization using artificial bee colony in mobile ad hoc networks," *Wireless Networks*, vol. 24, no. 5, pp. 1513–1526, July 2018.

[9] M. S. Lakshmi, G. Rajavikram, V. Dattatreya, B. S. Jyothi, S. Patil, and M. Bhavsingh, "Evaluating the Isolation Forest Method for Anomaly Detection in Software-Defined Networking Security," Journal of Electrical Systems, vol. 19, no. 4, pp. 279–297, 2023. doi: 10.52783/jes.639.

[10] H. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *Computer Communications*, vol. 120, pp. 10–29, May 2018.

[11] R. P. Ram Kumar, M. Sri Lakshmi, B. S. Ashwak, K. Rajeshwari, and S. Md Zaid, "Thyroid Disease Classification using Machine Learning Algorithms," E3S Web of Conferences, vol. 391, p. 01141, 2023, doi: 10.1051/e3sconf/202339101141.

[12] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Machine learning in smart cities: Applications, challenges, and solutions," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 16–23, Mar. 2017.

[13] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proceedings of the 1st ACM Workshop on Wireless Security (WiSe), Atlanta, GA, USA, 2002, pp. 1–10.

[14] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), Paris, France, 2002, pp. 78–87.

[15] S. Pirzada and C. McDonald, "Trusted greedy perimeter stateless routing for wireless sensor networks," in Proceedings of the 2005 International Conference on Informatics and Systems (INFOS), Cairo, Egypt, 2005, pp. 1–8.

[16] A.Dorri, M. Steger, S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[17] V. R. . K., H. K. . Yadav G., H. . Basha P., L. V. . Sambasivarao, 5Balarama K. . Rao Y. V., and M. . Bhavsingh, "Secure and Efficient Energy Trading using Homomorphic Encryption on the Green Trade Platform", Int J Intell Syst Appl Eng, vol. 12, no. 1s, pp. 345–360, Sep. 2023.

[18] H. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618–623.

[19] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial Bee Colony (ABC) algorithm," Journal of Global Optimization, vol. 39, no. 3, pp. 459–471, Nov. 2007.

[20] Lakshmi, K. ., Samiya, Lakshmi, M. S. ., Kumar, M. R. ., & Singuluri, P. K. . (2023)," Real-Time Hand Gesture Recognition for Improved Communication with Deaf and Hard of Hearing Individuals", International Journal of Intelligent Systems and Applications in Engineering, 11(6s), 23–37, https://www.ijisae.org/index.php/IJISAE/article/view/2825.

[21] H. R. Hassanzadeh, R. Baharlouei, and A. Dehghantanha, "Deep learning for IoT intrusion detection: Approaches, challenges and opportunities," in Cyber Threat Intelligence, Springer, 2018, pp. 171–203.

[22] Y. Yuan, W. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in Proceedings of the 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, 2017, pp. 1–8.

[23] T. Kim, J. Song, and H. Kim, "LSTM-based system-call language modeling and robust ensemble method for designing host-based intrusion detection systems," Information Sciences, vol. 504, pp. 204–224, Dec. 2019.

[24] M. Vinayakumar, K. P. Soman, and P. Poornachandran, "Evaluating deep learning approaches to intrusion detection in cyber-physical systems," in 2017 IEEE International Conference on Advanced Computing and Communications (ICACC), Udupi, India, 2017, pp. 1–8.

[25] E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, New Orleans, LA, USA, 1999, pp. 90–100.

[26] M. G. Zapata and N. Asokan, "Securing Ad hoc Routing Protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security (WiSe)*, Atlanta, GA, USA, 2002, pp. 1–10.

[27] R. Kumar and D. Kumar, "Multi-objective routing optimization using artificial bee colony in mobile ad hoc networks," Wireless Networks, vol. 24, no. 5, pp. 1513–1526, July 2018