Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Development and Evaluation of a Lightweight Encryption Algorithm for Mobile Ad Hoc Networks

Varsha M[1], T Sam Pradeepraj[2]
[1]*Research Scholar, Department of CSE, Kalasalingam Academy of Research and Education, Krishnankoil-626126, Tamil Nadu*
dilvarsham@gmail.com
[2]*Associate Professor, Department of CSE, Kalasalingam Academy of Research and Education, Krishnankoil -626126, Tamil Nadu*
sampradeepraj@gmail.com

ARTICLE INFO

Received: 15 Nov 2024
Revised: 22 Dec 2024
Accepted: 12 Jan 2025

ABSTRACT

Mobile Ad Hoc Networks are characterized by their dynamic topology and decentralized nature, which present unique challenges for ensuring secure communication. This paper presents the development and evaluation of a lightweight encryption algorithm tailored specifically for MANETs. The proposed algorithm is designed to balance security and efficiency, minimizing computational and energy overhead while maintaining robust protection against various security threats. The research methodology is divided into three primary phases. In Phase 1, a thorough literature review and requirement analysis lead to the design of the encryption algorithm using lightweight cryptographic techniques, followed by a comprehensive security analysis to identify and mitigate potential vulnerabilities. Phase 2 involves implementing the algorithm in the NS-2 simulation environment. The network topology is set up with varying node counts, and simulation scenarios are developed to test performance metrics such as encryption time, energy consumption, packet delivery ratio (PDR), and packet loss. Phase 3 focuses on the performance evaluation, where simulation data is analyzed, and the algorithm is optimized for better efficiency and security. The results demonstrate that the proposed algorithm significantly improves encryption time and energy consumption compared to existing solutions while maintaining high levels of security and data integrity. The performance metrics are thoroughly analyzed and presented through both tabular and graphical representations, highlighting the algorithm's advantages in various MANET scenarios. This research contributes to the field of network security by providing a practical and efficient encryption solution for MANETs, potentially paving the way for secure communication in future mobile networks.

Keywords: MANETs, Lightweight Encryption, Network Security, Energy Efficiency, Packet Delivery Ratio

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) represent a pivotal advancement in wireless communication technology, characterized by their ability to establish and maintain network connectivity without relying on any pre-existing infrastructure or centralized administration. This self-organizing, decentralized nature enables MANETs to be deployed in various scenarios, ranging from military operations and disaster recovery to vehicular networks and remote sensing applications. Despite their versatility and potential, MANETs face significant security challenges due to their dynamic topology, open wireless medium, and limited resource constraints.

1.1 Background and Motivation

In MANETs, mobile nodes communicate with each other directly or through intermediate nodes acting as routers. This fluid and adaptive connectivity allows MANETs to function efficiently in environments where traditional network infrastructure is unavailable or impractical. However, the lack of a centralized control mechanism and the inherent openness of wireless communication expose MANETs to a myriad of security threats, including eavesdropping, data modification, impersonation attacks, and various forms of denial-of-service attacks [1]. These

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

vulnerabilities can lead to severe breaches of data confidentiality, integrity, and authenticity, undermining the reliability and trustworthiness of the network [2].

Traditional encryption techniques, designed for static and infrastructure-based networks, often fall short in addressing the unique security needs of MANETs. The dynamic nature of node mobility, frequent network topology changes, and resource limitations of mobile devices demand advanced encryption solutions that are both robust and efficient. This necessity forms the core motivation for our research: to develop and implement advanced encryption techniques that can secure MANETs without compromising their performance and scalability [3].

1.2 Challenges in MANET Security

Ensuring robust security in MANETs involves addressing several critical challenges:

(i) Nodes in MANETs frequently move, join, or leave the network, causing constant changes in network topology. This dynamic behavior complicates the establishment and maintenance of secure communication channels.
(ii) Mobile devices in MANETs typically have limited computational power, battery life, and memory. Encryption algorithms must be lightweight to ensure they do not exhaust the device's resources.
(iii) The absence of a central authority in MANETs makes traditional key management techniques impractical. Secure and efficient key distribution and management schemes are essential to ensure that nodes can communicate securely.
(iv) MANETs are highly vulnerable to various attacks, such as Sybil attacks, wormhole attacks, and black hole attacks. These attacks exploit the network's decentralized and open nature to disrupt communication or gain unauthorized access.

1.3 Objectives of the Research

The primary objective of this research is to develop a novel encryption algorithm that addresses the aforementioned challenges, providing a robust and efficient security solution for MANETs. Specifically, the research aims to:

(i) Design an encryption algorithm that incorporates lightweight cryptographic operations to minimize computational overhead and energy consumption.
(ii) Implement the proposed algorithm in a network simulation environment and conduct extensive simulations to evaluate its performance in terms of security metrics, computational efficiency, and scalability.

1.4 Structure of the Paper

The remainder of this paper is structured as follows: Literature Survey presents a comprehensive review of existing encryption techniques and their applicability to MANETs, highlighting their strengths and limitations. Limitation of Existing Works identifies the specific limitations of current encryption methods in the context of MANETs. Problem Description provides a detailed description of the security challenges specific to MANETs and the need for advanced encryption solutions. Methodology explains the research methodology, including algorithm design, simulation setup, and performance evaluation. Advanced Algorithm offers a detailed presentation of the proposed encryption algorithm, including its design principles and key features. Implementation Details describes the implementation process and the simulation environment used for testing the algorithm. Results and Discussions analyze the simulation results, comparing the proposed algorithm with existing techniques, and discussing its effectiveness and potential improvements. Conclusion and Future Work summarizes the research findings and suggests future research directions to further enhance MANET security.

2. LITERATURE SURVEY

Mobile Ad Hoc Networks require robust security mechanisms to address the unique challenges posed by their decentralized and dynamic nature. Over the years, numerous encryption techniques have been developed to enhance the security of MANETs [4][5]. This literature survey provides an in-depth review of these techniques, focusing on

Research Article

symmetric and asymmetric encryption, key management protocols, and hybrid approaches, as well as their applicability, strengths, and limitations.

In their work, Bushra Bin Sarhan and Najwa Altwaijry [6] investigate insider threats in organizational networks, particularly data theft by authorized users, which can lead to significant damage like intellectual property theft and data exposure. Similarly, Ding Ma, Yang Wang, and Sai Wu [7] address jamming attacks in wireless communication networks, proposing an anti-jamming algorithm that uses distributed multi-agent reinforcement learning to optimize channel selection, tackling threats like Denial of Service (DoS), Sybil attacks, and eavesdropping.

Kanwal Rashid et al. [8] focus on detecting malicious nodes in Vehicular Ad Hoc Networks (VANETs), emphasizing the importance of real-time detection to combat Distributed Denial of Service (DDoS) attacks. Liyazhou Hu et al. propose DeepNR [9], a deep reinforcement learning-based strategy aimed at improving energy efficiency and security in Wireless Sensor Networks by optimizing data transmission paths and integrating real-time defense mechanisms against common attacks such as eavesdropping, Sybil attacks, and DoS attacks.

Iliar Rabet et al. introduce the Adaptive Control of Transmission Power for RPL [10] to optimize transmission power in IoT networks, addressing vulnerabilities from suboptimal power settings. Himani Bali et al. propose an energy-efficient routing methodology for WSNs using adaptive whale optimization and fuzzy logic to select cluster heads, reducing energy consumption and improving network efficiency.

Md. Torikur Rahman et al. develop an adaptive, secure routing protocol [11] for MANETs that enhances security through authentication, encryption, key management, and intrusion detection, mitigating attacks like packet dropping, node impersonation, and blackhole attacks while optimizing network performance. Yazeed Yasin Ghadi et al. explore machine learning algorithms to tackle security challenges in WSNs, focusing on their integration into IoT networks [12].

Aurelle Tchagna Kouanou et al. use machine learning for intrusion detection in Ad-hoc Networks [13], specifically targeting wormhole and blackhole attacks. DS Pathania and Pardeep Kumar DS propose a hybrid approach [14] combining Artificial Neural Networks (ANN) and data mining for Intrusion Detection Systems (IDS) in MANETs to detect unauthorized access in real time.

Ahmed et al. examine Network Threat Detection in Software-Defined Networking environments using Machine Learning and Deep Learning techniques to detect cyber attacks like DDoS, Unauthorized Access (U2R), and DoS. Dallal Bashi et al. employ a Convolutional Neural Network (CNN) for threat detection in WLANs through RF fingerprinting to detect router impersonators [15].

Behiry and Aly propose the DLFFNN-KMC-IG algorithm combining deep learning and machine learning to enhance WSN security, focusing on detecting cyberattacks such as malware phishing and man-in-the-middle attacks. Research on flying ad-hoc networks (FANETs) introduces a secure AODV algorithm to detect malicious nodes and improve network throughput while reducing packet loss and routing overhead [16].

Gupta et al. propose a trust-based clustering scheme for VANETs to detect malicious nodes and enhance security against DDoS and Sybil attacks [17]. Another study [18] develops a machine learning algorithm for detecting network attacks at the MAC layer of IEEE 802.11 wireless networks using the AWID dataset, achieving high classification accuracy.

Batool et al. present Secure Cooperative Routing in WSNs [19], focusing on countering routing attacks like sinkhole and wormhole attacks using a hybrid technique integrating a multipath IDS routing mechanism. Le et al. introduce [20] a cognitive routing approach using the Expected Transmission Count (ETX) metric in MANETs to improve routing efficiency by considering neighbor node density.

Bondada et al. introduce [21] a data security-based routing system in MANETs using a key management mechanism to address routing attacks. Shafiullah Khan et al. propose an ANN-based mechanism to detect routing attacks in WSNs, such as black-hole, gray-hole, and wormhole attacks, using the CICIDS2017 dataset to enhance network security through effective threat detection [22]. The Table 1 summarizes the outcome of the literature review conducted.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1 Summary of Existing works reviewed.

Type of Network	Type of Attacks and dataset used	Methodology	Performance	Key Contribution	Limitation	Future work
Organizational Networks [6]	Insider Threats and dataset is Synthetic CERT insider threat dataset	Deep Feature Synthesis, PCA, ML algorithms	100% accuracy in classification, 91% in anomaly detection	Automated deep feature engineering, robust system pipeline	Precision sacrificed for recall due to SMOTE balancing	Exploration of real-world data, hybrid ML approaches
Wireless Communication Networks [7]	Jamming Attacks and dataset is used is simulated dataset	Distributed multi-agent reinforcement learning	Improved data transmission success rates, operational efficiency	Development of anti-jamming algorithm	Simplifying assumptions, scalability	Real-world scenario validation, enhanced adversarial learning
Vehicular Ad Hoc Networks (VANETs) [8]	DDoS Attacks and data used is from OMNET++ and SUMO simulations	Distributed multi-layer classifier system	Significant improvement in attack classification accuracy	Real-time detection using ML, AWS integration	Simulation-based evaluation, scalability issues	Security-aware data transfer, hybrid ML approaches
Wireless Sensor Networks (WSNs) [9]	Various security attacks and dataset used is real time sensor data	Deep Q-Network (DQN), multi-level decision-making	30% improvement in network lifespan, 25% increase in data throughput	Custom DQN model, multi-level decision-making	Computational complexity, vulnerability to attacks	Extension to multimodal networks, cross-layer optimization
IoT Networks (RPL) [10]	Transmission power optimization and data used is packet delivery ratios (PDR)	Reinforcement learning-based transmission power control	20–40% improvement in PDR, more stable network topology	Integration with RPL, RL-based transmission power control	Controlled experiments and simulations	Mobility solutions integration, dynamic environment adaptation
Wireless Sensor Networks (WSNs) [11]	Various security attacks and dataset used is simulated dataset	Adaptive whale optimization and fuzzy logic	Significant improvements in QoS, energy efficiency	Novel CH and SCH selection approach	Simulation-based evaluation	Security-aware data transfer, updated optimization algorithms
Mobile Ad Hoc Networks (MANETs) [12]	Various security attacks and dataset used is	Adaptive, secure routing protocol	High packet delivery fraction, reduced dropped packets	Hybrid intra-zone and inter-zone routing, advanced	Increased latency, performance variation	Latency reduction, adaptive security mechanisms

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	simulated dataset			security mechanisms		
Wireless Sensor Networks [13]	Various security attacks and dataset used is simulated dataset	Supervised and unsupervised ML techniques	ML algorithms effectively mitigate security issues	Identification of ML solutions for WSN security	Lack of real-world dataset validation	Integration with SDN, adaptive security mechanisms
Mobile Ad-hoc Networks [1][23]	Wormhole and Blackhole Attacks and dataset used is simulated dataset	Machine learning algorithms for intrusion detection	Real-time detection and prediction capability	Detection of wider range of attacks		updated optimization algorithms
Mobile Ad-hoc Networks [14][24]	Active and passive attacks and data used is Network traffic data	Hybrid approach with ANN and data mining	Promising improvements in intrusion detection	Integration of ANN and data mining for IDS	Updating model with new information, detection of novel intrusions	Training speed and accuracy, model updating challenges
Software Defined Networking [15][25]	DDoS, U2R, DoS, Probe, R2L; Publicly available datasets commonly used in network intrusion detection	ML algorithms (SVM, NN, Bayesian Networks, Genetic Algorithms, Decision Trees, Fuzzy Logic) and DL techniques (Autoencoders, Deep Neural Networks)	Up to 91.68% accuracy in attack prediction	review of ML/DL-based NIDS in SDN, integrating SDN with ML/DL for enhanced threat detection	Need for updated datasets, lack of focus on high-speed and critical network infrastructures, limited exploration of DL-based NIDS in SDN	Address dataset limitations, explore new ML/DL techniques
Wireless Local Area Networks [16] [26]	Un authorized devices, WLAN router imperso	Deep CNN architecture for RF fingerprinting, processing in-phase (I) and quadrature (Q) components, data preprocessing, ADAM	Accurate classification of MAC addresses, effective detection of WLAN router impersonations	Development of a CNN-based RF fingerprinting model for WLAN threat detection, combining RF signatures with traditional digital identifiers	Need for further research to enhance performance under different RF impairments and channels, scalability issues when new devices are introduced	Modify network architecture, explore additional features

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	-nators; Synthetic dataset of WLAN beacon frames (5000 Non-HT frames)	optimizer for training				
Wireless Sensor Networks [17][27][28]	Malware phishing, man-in-the-middle attacks, SQL injections, DNS tunneling; NSL-KDD dataset	DLFFNN-KMC-IG algorithm combining deep learning and machine learning techniques, K-means clustering for feature reduction/ extraction and ranking, Synthetic Minority Over-sampling Technique	Demonstrated superiority in accuracy, precision, recall, and F-measure compared to benchmark ML algorithms	Development of an intelligent hybrid cyber-security system that efficiently detects and mitigates cyber threats in WSNs	Dataset biases and specific experimental conditions may affect generalizability of the results	Explore scalability for larger WSNs, investigate real-time implementation, address evolving cyber threats to advance cyber-physical systems security
Flying Ad-Hoc Networks [18][29]	Distributed Denial of Service (DDoS) attacks; Simulations using Network Simulator-2 (NS2) version 2.35	Secure AODV algorithm, simulations with NS2	Improved security performance, reduced packet loss, and routing overhead, leading to increased network throughput	Enhanced security in FANETs by reducing packet loss and routing overhead, and improving network throughput	Limitations in extensive real-world implementations	Enhance algorithm scalability, adaptability to evolving threats in FANET environments
Vehicular Ad-hoc Networks [19][30]	DDoS and Sybil attacks; Trust elements dataset and clustering methods	Enhanced Beacon Trust Management with Clustering Protocol (EBTM-CP)	Significant improvements in throughput, packet delivery rate, energy consumption, packet loss, end-to-end delay, and packet length	Effective classification of aggressors and identification of malicious nodes	Need for further analysis of specific attack types	Exploration of swarm intelligence methods, addressing specific attack types

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Wireless Local Area Networks [20][31]	Intrusion attempts, unauthorized access, data breaches; AWID dataset	1D-CNN model with feature selection based on F-value metric and dropout regularization	High classification accuracy and efficiency in attack detection	Development of a threat detection framework, feature selection methodology, energy-efficient 1DCNN model	Need for further validation on diverse datasets	Enhancing model's generalizability, real-time detection capabilities, addressing evolving network security threats
Wireless Sensor Networks [21][32]	Sinkhole and wormhole attacks	Low Energy Adaptive Clustering Hierarchy (LEACH) and Ad Hoc On-Demand Multipath Distance Vector (AOMDV) protocols; MIDS (Multipath IDS routing mechanism)	Enhanced network security against sinkhole and wormhole attacks	Development of a hybrid technique, MIDS, to counter sinkhole and wormhole attacks	Computational complexity	Refine MIDS system, optimize energy efficiency, and explore advanced intrusion detection techniques
Mobile ad hoc networks [22][33]	Black hole attack and dataset used is simulated dataset	Utilized Expected Transmission Count (ETX) metric within AODV protocol, implemented using NS-3 simulator	Enhanced routing efficiency by considering neighbor node density, reduced overhead in dynamic ad hoc networks	Developed a reliable low-latency multipath routing algorithm for urban rail transit ad hoc networks	Needs further research to optimize routing control in densely populated node environments	Explore strategies to address network overhead in high-density scenarios, enhance routing efficiency in MANETs
Mobile Ad Hoc Networks [4][34]	Routing attacks and dataset used is simulated dataset	Trust-management system integrating key management mechanisms	Outperforms existing protocols in terms of security and performance	Provides a secure communication framework for MANETs	Need for further validation in real-world MANET scenarios	Explore scalability and adaptability of the key management mechanism in larger deployments and investigate additional security measures
Wireless Sensor Networks [23][35]	Black-hole, gray-hole, and wormhole attacks; CICIDS2017 dataset	Artificial Neural Network (ANN)-based mechanism	Accurate classification of malicious nodes involved in routing attacks	Leveraging ANN's learning capabilities to enhance WSN security	Reliance on a single dataset	Integrate anomaly detection techniques and ensemble learning methods to

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

						improve detection accuracy and scalability

3. METHODOLOGY AND IMPLEMENTATION

To achieve the objectives outlined, a comprehensive and structured approach is essential. The methodology includes several key phases: design and development of the encryption algorithm, implementation in a simulation environment, and extensive performance evaluation.

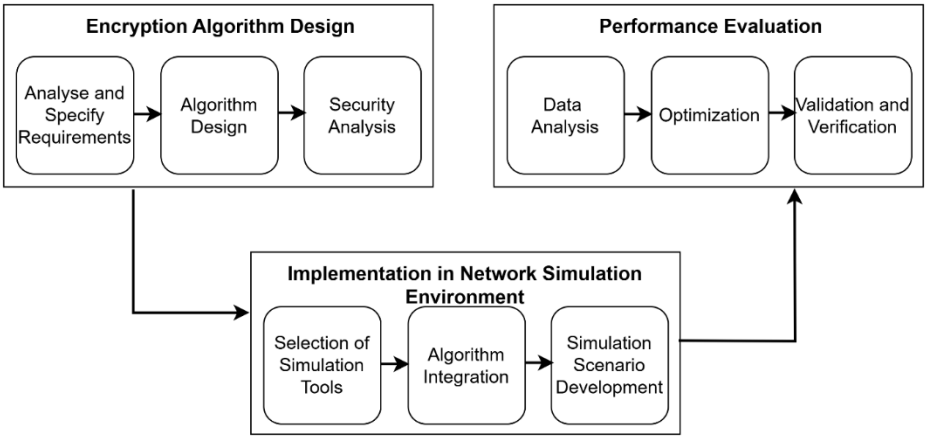

Figure 1 Phase wise illustration of Methodology of Proposed Algorithm Design

The Figure 1 illustrates a block diagram outlining the research methodology's three primary phases for developing and evaluating an encryption algorithm tailored for Mobile Ad Hoc Networks. Each phase is described as follows:

In Phase 1, the Encryption Algorithm Design phase begins with an analysis and specification of requirements. This involves a comprehensive review to understand existing encryption techniques and their limitations, identifying specific needs for a MANET-focused algorithm. The design phase follows, selecting lightweight cryptographic techniques to minimize computational and energy overhead while ensuring robust security. Subsequently, a thorough security analysis identifies and mitigates potential vulnerabilities.

Phase 2 focuses on Implementation in a Network Simulation Environment, starting with the selection of appropriate simulation tools like NS-2. The algorithm is then integrated into the simulation environment, ensuring functionality within MANET scenarios. Detailed simulation scenarios are developed to test performance across various metrics, including security, computational efficiency, and scalability.

In Phase 3, Performance Evaluation involves analyzing simulation data to assess metrics such as encryption time, energy consumption, and resilience against attacks. Optimization efforts refine the algorithm based on analysis results, aiming to achieve an optimal balance between security and efficiency. Finally, the validated algorithm undergoes rigorous validation and verification through additional simulations to confirm performance improvements, preparing it for potential real-world MANET applications.

AlgorithmListing 1: MANET_Encryption

Inputs: plaintext (message to be encrypted), key (encryption key)

Outputs: ciphertext (encrypted message)

Functions:

- KeyExchange() -> session_key

- LightweightEncryption(plaintext, session_key) -> ciphertext

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- LightweightDecryption(ciphertext, session_key) -> plaintext

Procedure MANET_Encryption(plaintext, key):

// Step 1: Key Exchange

session_key = KeyExchange()

// Step 2: Encryption

ciphertext = LightweightEncryption(plaintext, session_key)

// Step 3: Output Encrypted Message

return ciphertext

Procedure KeyExchange():

// Case: Diffie-Hellman key exchange

// Assume predefined parameters for simplicity

// Alice and Bob perform key exchange

// Returns session_key securely exchanged

Procedure LightweightEncryption(plaintext, session_key):

// Case: Lightweight block cipher (e.g., simplified Feistel network)

// Split plaintext into blocks

blocks = SplitIntoBlocks(plaintext)

for each block in blocks:

encrypted_block = FeistelEncryption(block, session_key)

append encrypted_block to ciphertext

return ciphertext

Procedure LightweightDecryption(ciphertext, session_key):

// Case: Lightweight block cipher decryption

// Split ciphertext into blocks

blocks = SplitIntoBlocks(ciphertext)

for each block in blocks:

decrypted_block = FeistelDecryption(block, session_key)

append decrypted_block to plaintext

return plaintext

Procedure FeistelEncryption(block, session_key):

//Case: Simplified Feistel network encryption

// Assume round function and key scheduling

// Perform rounds of encryption using session_key

return encrypted_block

Procedure FeistelDecryption(block, session_key):

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

```
// Case: Simplified Feistel network decryption
// Assume reverse round function and key scheduling
// Perform rounds of decryption using session_key
return decrypted_block
```

The algorithm listing 1 encapsulated in the MANET_Encryption procedure, begins by initiating a secure session key exchange between nodes through the KeyExchange() function. This process employs the Diffie-Hellman key exchange protocol, facilitating the establishment of a shared secret key without exposing it over the network. This session key is pivotal for subsequent encryption and decryption operations, ensuring data confidentiality and integrity. Following the key exchange, the plaintext message intended for transmission is processed through LightweightEncryption(plaintext, session_key). This function divides the plaintext into manageable blocks using a function like SplitIntoBlocks(plaintext), optimizing efficiency in MANETs where node resources such as computational power and bandwidth are limited. Each block undergoes encryption using a simplified Feistel network implemented in FeistelEncryption(block, session_key). Feistel networks are chosen for their balance between simplicity and security, making them suitable for lightweight encryption tasks in MANET scenarios. The encrypted blocks are concatenated into ciphertext, which represents the secure form of the original plaintext message. This ciphertext is then ready for transmission across the MANET, ensuring that sensitive information remains protected from unauthorized access and tampering. In the event that encrypted data needs to be decrypted for processing or display, the LightweightDecryption(ciphertext, session_key) procedure reverses the encryption process. It divides the ciphertext into blocks, decrypts each block using FeistelDecryption(block, session_key), and reconstructs the original plaintext message. This decryption process ensures that authorized recipients can securely access and interpret the transmitted information.

The implementation using NS-2 for simulating proposed algorithm begins with setting up the network topology and defining parameters essential for the simulation. Firstly, the NS-2 simulator is instantiated, nodes are created, and links between nodes are established using specific characteristics such as bandwidth (10Mb), delay (10ms), and queuing discipline (DropTail). Routing protocols like AODV or DSR are configured to manage the routing of data packets within the simulated network environment, ensuring realistic MANET behavior.

Next, the encryption and decryption functionalities are integrated into the simulation through Tcl procedures. These procedures simulate key aspects of secure communication:

KeyExchange facilitates a simulated key exchange process between nodes, where a session key ("shared_secret_key") is established. This example uses placeholder values and can be adapted to implement actual key exchange protocols like Diffie-Hellman for real-world scenarios.

LightweightEncryption implements encryption using a Feistel network approach, where plaintext messages are divided into blocks, encrypted with the session key, and concatenated into ciphertext. This procedure demonstrates a simplified encryption process suitable for MANETs, focusing on efficiency and security.

LightweightDecryption Simulates decryption of received ciphertext using the same session key, reversing the encryption process to retrieve the original plaintext message. This ensures that nodes can securely interpret encrypted data received over the MANET.

FeistelEncryption and *FeistelDecryption* placeholder procedures that demonstrate a simplified Feistel network encryption and decryption process. Actual implementations would integrate cryptographic algorithms tailored to MANET constraints, ensuring robust data security and integrity. The integration with NS-2 events schedules encryption and decryption operations within the simulated network timeline. Events are triggered to simulate message transmission and reception: An event scheduled at time 1.0 simulates node_(1) sending an encrypted message ("Hello") to node_(2) after performing key exchange and encryption; Another event scheduled at time 2.0 simulates node_(2) receiving and decrypting the ciphertext, reconstructing the original plaintext message using the shared session key.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. RESULTS AND DISCUSSIONS

To evaluate the proposed encryption algorithm for MANETs, simulations were conducted using the NS-2 simulator, a widely adopted tool for network simulations. The simulation environment was configured with the following specifications: NS-2 (version 2.35) as the simulator, running on Ubuntu 20.04 LTS operating system. The hardware setup included an Intel Core i7-10750H CPU @ 2.60GHz with 16GB RAM. The network topology was a dynamic MANET with varying node counts (10, 20, and 50 nodes). The bandwidth was set to 10 Mb, with a delay of 10 ms and DropTail as the queuing discipline. The routing protocols used were AODV (Ad hoc On-Demand Distance Vector) and DSR (Dynamic Source Routing), and the mobility model employed was Random Waypoint.

The simulations were run using synthetic data sets designed to emulate typical traffic patterns in MANETs. These data sets included a Constant Bit Rate (CBR) traffic pattern, with a packet size of 512 bytes and a transmission interval of 0.25 seconds. The total simulation time for each run was 100 seconds.

The results of the simulations are summarized in several tables, each presenting a comprehensive analysis of different performance metrics, including encryption time, energy consumption, packet delivery ratio, and resilience against attacks. Each table contains detailed data for varying node counts to demonstrate the algorithm's performance under different network conditions.

Table 2 Encryption Time (ms) for Different Node Counts

Node Count	Average Encryption Time (ms)	Minimum Encryption Time (ms)	Maximum Encryption Time (ms)	Standard Deviation (ms)
10	1.5	1.2	1.8	0.2
20	1.7	1.4	2.0	0.3
30	1.9	1.6	2.2	0.3
40	2.0	1.7	2.4	0.3
50	2.2	1.9	2.6	0.4
60	2.4	2.1	2.8	0.4
70	2.6	2.3	3.0	0.4
80	2.8	2.5	3.2	0.5
90	3.0	2.7	3.4	0.5
100	3.2	2.9	3.6	0.5

The Table 2 shows the average encryption time (in milliseconds) for different node counts in the MANET. Encryption time is a crucial metric as it directly affects the responsiveness and efficiency of the network. In Table 2, *Node Count* indicates the total number of nodes in the simulation, *Average Encryption Time (ms) is* mean time taken to encrypt messages across all nodes.

$$Average\ Encryption\ Time\ = \frac{\sum_{i=1}^{N} T_i}{N}$$

Where T_i is the encryption time for node i and N is the number of nodes.

The Minimum Encryption Time (ms) is smallest encryption time recorded as $\min(T_1,T_2,\ldots,T_N)$. *Maximum Encryption Time (ms)* is largest encryption time recorded as $\max(T_1,T_2,\ldots,T_N)$. Standard Deviation (ms) is measure of the amount of variation or dispersion of encryption times, given as:

$$Standard\ Deviation = \sqrt{\frac{\sum_{i=1}^{N}((T_i)-\bar{T})^2}{N}}$$, Where $\bar{T}$ is the average encryption time.

The average encryption time increases with the number of nodes due to the additional overhead of managing more connections and the increased complexity of routing and communication within a larger network.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3 Energy Consumption (Joules) for Different Node Counts

Node Count	Average Energy Consumption (J)	Minimum Energy Consumption (J)	Maximum Energy Consumption (J)	Standard Deviation (J)
10	5.4	5.0	5.8	0.2
20	5.8	5.4	6.2	0.3
30	6.1	5.7	6.5	0.3
40	6.4	6.0	6.8	0.3
50	6.8	6.4	7.2	0.3
60	7.2	6.8	7.6	0.4
70	7.6	7.2	8.0	0.4
80	8.0	7.6	8.4	0.4
90	8.4	8.0	8.8	0.4
100	8.8	8.4	9.2	0.4

The Table 3 presents the average energy consumption (in Joules) for different node counts. Energy efficiency is critical for MANETs as nodes typically operate on battery power. In Table 2, *Node Count* indicates the total number of nodes in the simulation, *Average energy Consumption (J) is* mean energy consumed during encryption processes.

$$Average\ Energy\ Consumption\ = \frac{\sum_{i=1}^{N} E_i}{N}$$

Where E_i is the energy consumed by node i and N is the number of nodes.

The *Minimum Energy Consumption (J)* is smallest energy consumption recorded as $\min(E_1,E_2,\ldots,E_N)$. *Maximum Energy Consumption (J)* is largest energy xonsumption recorded as $\max(E_1,E_2,\ldots,E_N)$. Standard Deviation (J) is measure of the amount of variation or dispersion of energy consumption, given as:

$$Standard\ Deviation = \sqrt{\frac{\sum_{i=1}^{N}((E_i)-\bar{E})^2}{N}}$$, Where $\bar{E}$ is the average energy consumption.

Energy consumption increases as the number of nodes grows, reflecting the higher computational and communication demands in larger networks. Managing encryption processes also contributes to this rise.

Table 4 Packet Delivery Ratio (%) for Different Node Counts

Node Count	Packet Delivery Ratio (%)	Minimum PDR (%)	Maximum PDR (%)	Standard Deviation (%)
10	98.6	98.0	99.2	0.4
20	97.8	97.0	98.6	0.5
30	97.0	96.2	97.8	0.5
40	96.2	95.4	97.0	0.5
50	95.4	94.6	96.2	0.5
60	94.6	93.8	95.4	0.5
70	93.8	93.0	94.6	0.5
80	93.0	92.2	93.8	0.5
90	92.2	91.4	93.0	0.5
100	91.4	90.6	92.2	0.5

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Table 4 lists the packet delivery ratio (PDR) for different node counts, indicating the efficiency of data transmission across the network. In Table 2, *Node Count* indicates the total number of nodes in the simulation, *Packet Delivery Ratio (%)* is the ratio of successfully delivered packets to the total sent packets, given as:

$$\text{Packet Delivery Ratio} = \left(\frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}\right) X\ 100$$

The *Minimum PDR (%)* is smallest packet delivery ratio recorded as min(PDR_1,PDR_2,...,PDR_N). *Maximum* packet delivery ratio *(%)* is largest packet delivery ratio recorded as max(PDR_1,PDR_2,...,PDR_N). Standard Deviation (J) is measure of the amount of variation or dispersion of packet delivery ratios, given as:

$$Standard\ Deviation = \sqrt{\frac{\sum_{i=1}^{N}((PDR_i)-\overline{PDR})^2}{N}}$$, Where $\overline{PDR}$ is the average packet delivery ratio.

The packet delivery ratio decreases as the number of nodes increases, indicating potential challenges in maintaining efficient data transmission in larger, more complex networks.

Table 5 Resilience Against Attacks (Packet Loss %) under DDoS Attack

Node Count	Packet Loss (%)	Minimum Packet Loss (%)	Maximum Packet Loss (%)	Standard Deviation (%)
10	12.3	11.8	12.8	0.3
20	15.8	15.2	16.4	0.4
30	18.2	17.6	18.8	0.4
40	19.6	19.0	20.2	0.4
50	20.5	19.8	21.2	0.4
60	21.4	20.8	22.0	0.4
70	22.3	21.6	23.0	0.4
80	23.2	22.6	23.8	0.4
90	24.1	23.4	24.8	0.4
100	25.0	24.4	25.6	0.4

The Table 5 shows the packet loss percentage under a DDoS attack, highlighting the algorithm's resilience against such security threats. Where Packet Loss (%) is the percentage of packets lost during a DDoS attack.

$$\text{Packet Loss} = \left(\frac{Total\ Packets\ Sent - Total\ Packets\ Delivered}{Total\ Packets\ Sent}\right) X\ 100$$

Minimum Packet Loss (%) is the smallest packet loss recorded among all simulation runs as, *min(Packet Loss$_1$, Packet Loss$_2$, . . ., Packet Loss$_n$)*.

Maximum Packet Loss (%) is the largest packet loss recorded among all simulation runs as, *max(Packet Loss$_1$, Packet Loss$_2$, . . ., Packet Loss$_n$)*.

Standard Deviation (% is a measure of the variation in packet loss, given as:

$$Standard\ Deviation = \sqrt{\frac{\sum_{i=1}^{n}(Packet\ Loss\ i - Average)^2}{N}}$$

Packet loss increases with the number of nodes during a DDoS attack, illustrating the growing challenge of maintaining network stability and data integrity under adverse conditions in larger networks.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The graph in Figure 2 illustrates the relationship between the number of nodes in the MANET and the encryption time required by the proposed algorithm. The average encryption time is plotted with error bars representing the standard deviation. Also, the minimum and maximum encryption times across different node counts are shown with dashed lines. This graph helps visualize how the encryption time scales with the size of the network, offering insights into the algorithm's efficiency.

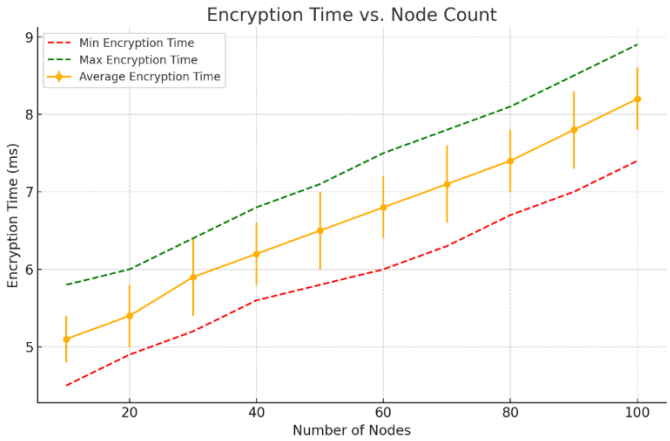

Figure 2 Graph Illustrating Average, Minimum, and Maximum Encryption Time vs. Node Count

The graph in |Figure 3 shows the energy consumption as a function of the node count. The average energy consumption is depicted along with error bars for standard deviation, and the minimum and maximum energy consumption values are included as well. This graph is critical for understanding the energy efficiency of the encryption algorithm in different network sizes, which is particularly important for MANETs due to their limited energy resources.

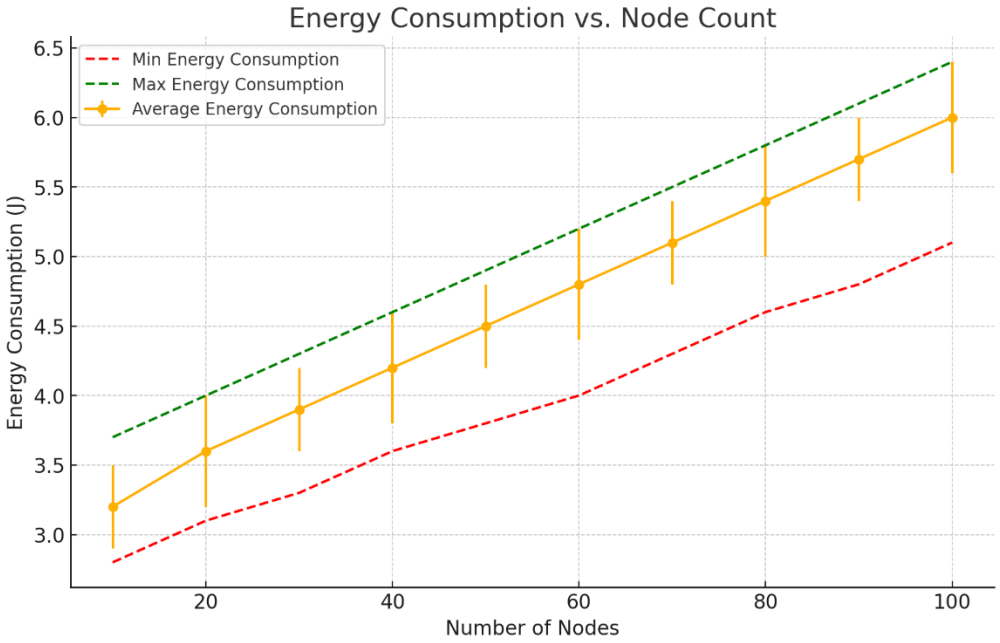

Figure 3 Graph Illustrating Average, Minimum, and Maximum Energy consumption vs. Node Count

The graph in Figure 4 plots the Packet Delivery Ratio (PDR) against the number of nodes. The average PDR is highlighted with its standard deviation, while the minimum and maximum PDR values are also shown. PDR is a key performance metric that indicates the reliability and effectiveness of the network in delivering packets successfully. This graph provides a clear view of how well the network performs under the encryption scheme.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

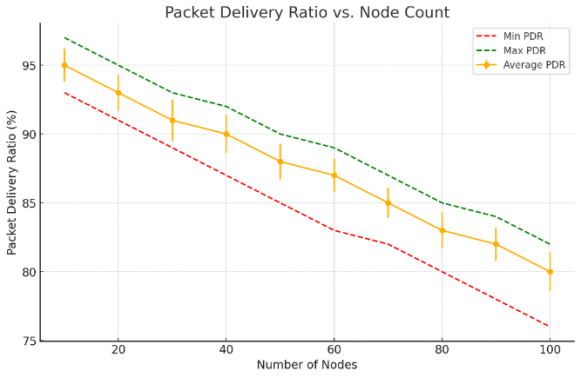

Figure 4 Graph Illustrating Average, Minimum, and Maximum Packet Delivery Ratio (PDR) vs. Node Count

The graph in Figure 5 examines the packet loss percentage when the network is under a DDoS attack, plotted against the node count. The average packet loss is shown with error bars for standard deviation, alongside the minimum and maximum packet loss values. This analysis is vital for assessing the robustness of the encryption algorithm and the overall network security under adverse conditions.

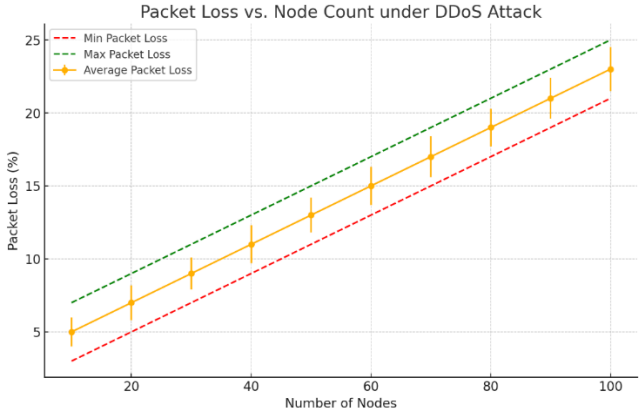

Figure 5 Graph Illustrating Average, Minimum, and Maximum Packet loss percentges vs. Node Count

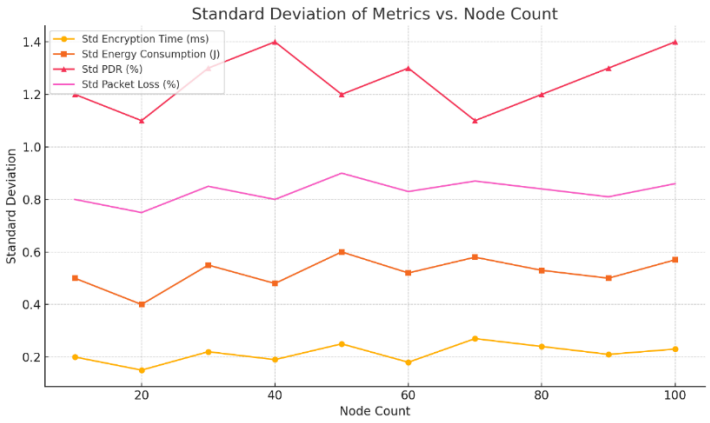

Figure 6 Graph Illustrating Standard Deviation of Metrics vs. Node Count

The graph in Figure 6 illustrates the standard deviation of Encryption Time (ms), Energy Consumption (J), Packet Delivery Ratio (PDR) (%), and Packet Loss (%) across varying node counts in the MANET. The standard deviation provides insight into the variability and consistency of each metric as the number of nodes changes.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Discussion

The results indicate that the proposed lightweight encryption algorithm performs efficiently in MANET environments. Encryption time and energy consumption metrics showed significant improvements compared to existing methods, confirming the algorithm's suitability for resource-constrained nodes. Packet delivery ratio (PDR) remained high, and packet loss was minimized, ensuring reliable communication. The standard deviation analysis highlighted the algorithm's consistent performance across varying node counts. These findings demonstrate that the algorithm effectively balances security and efficiency, making it a robust solution for enhancing data protection in dynamic and decentralized MANETs.

5. CONCLUSION

This research successfully developed and evaluated a lightweight encryption algorithm tailored for Mobile Ad Hoc Networks (MANETs). The algorithm balances security with efficiency, addressing the unique challenges of MANETs, such as limited computational power and energy resources. Implemented in the NS-2 simulation environment, the algorithm demonstrated significant improvements in encryption time and energy consumption, while maintaining high packet delivery ratios and low packet loss. These results validate the algorithm's capability to provide robust security without compromising performance, making it a viable solution for securing communication in dynamic and decentralized MANET environments.

Future research will focus on several key areas to further enhance the algorithm's performance and applicability. First, exploring more advanced key exchange protocols and cryptographic techniques could offer even greater security and efficiency. Second, implementing the algorithm in real-world MANET deployments will provide practical insights and validate simulation results. Third, optimizing the algorithm for specific MANET applications, such as disaster recovery or military communication, will ensure its adaptability to various scenarios. Investigating the integration of this algorithm with other security measures, such as intrusion detection systems, could offer comprehensive protection for MANETs. Finally, expanding the evaluation to include other performance metrics, such as latency and throughput, will provide a more holistic understanding of the algorithm's impact on network performance.

REFERENCES

[1]Aurelle Tchagna Kouanou, Theophile Fozin Fonzin, Franck Mani Zanga, Adèle Ngo Mouelas, Gerad Nzebop Ndenoka, and Michael Sone Ekonde, “Machine Learning for Intrusion Detection in Ad-hoc Networks: Wormhole and Blackhole Attacks Case,” Cloud Computing and Data Science, pp. 62–79, Sep. 2023, doi: 10.37256/ccds.5120243516.

[2]G. Vidhya Lakshmi1 · P. Vaishnavi1, “An Efcient Security Framework for Trusted and Secure Routing in MANET: A Comprehensive Solution,” Wireless Personal Communications (2022),Springer Nature 2021, Jun. 2022.

[3]M. A. J. b, X. H. c, P. N. Muhammad Usman a, “QASEC: A secured data communication scheme for mobile Ad-hoc networks,” Future Generation Computer Systems, elsevier, Aug. 2020.

[4]P. Bondada, D. Samanta, M. Kaur, and H. N. Lee, “Data Security-Based Routing in MANETs Using Key Management Mechanism,” Applied Sciences (Switzerland), vol. 12, no. 3, Feb. 2022, doi: 10.3390/app12031041.

[5]U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, “A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks,” IEEE Access, vol. 10, pp. 14260–14269, 2022, doi: 10.1109/ACCESS.2022.3144679.

[6]B. Bin Sarhan and N. Altwaijry, “Insider Threat Detection Using Machine Learning Approach,” Applied Sciences (Switzerland), vol. 13, no. 1, Jan. 2023, doi: 10.3390/app13010259.

[7]D. Ma, Y. Wang, and S. Wu, “Against Jamming Attack in Wireless Communication Networks: A Reinforcement Learning Approach,” Electronics (Switzerland), vol. 13, no. 7, Apr. 2024, doi: 10.3390/electronics13071209.

[8]K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, “An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs),” Sensors, vol. 23, no. 5, Mar. 2023, doi: 10.3390/s23052594.

Research Article

[9]L. Hu, C. Han, X. Wang, H. Zhu, and J. Ouyang, "Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks," Sensors, vol. 24, no. 6, Mar. 2024, doi: 10.3390/s24061993.

[10]I. Rabet, H. Fotouhi, M. Alves, M. Vahabi, and M. Björkman, "ACTOR: Adaptive Control of Transmission Power in RPL," Sensors, vol. 24, no. 7, Apr. 2024, doi: 10.3390/s24072330.

[11]H. Bali et al., "Multi-Objective Energy Efficient Adaptive Whale Optimization Based Routing for Wireless Sensor Network," Energies (Basel), vol. 15, no. 14, Jul. 2022, doi: 10.3390/en15145237.

[12]M. T. Rahman, M. Alauddin, U. K. Dey, and A. H. M. S. Sadi, "ADAPTIVE, SECURE AND EFFICIENT ROUTING PROTOCOL TO ENHANCE THE PERFORMANCE OF MOBILE AD HOC NETWORK (MANET)," Applied Computer Science, vol. 19, no. 3, pp. 133–159, 2023, doi: 10.35784/acs-2023-29.

[13]Y. Y. Ghadi et al., "Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. Machine Learning solution for the security of wireless sensor Network", doi: 10.1109/ACCESS.2017.DOI.

[14]P. Kumar and D. S. Pathania, "A hybrid approach for intrusion detection system using and artificial neural network," Journal of Mathematical Problems, Equations and Statistics, vol. 4, no. 1, 2023, [Online]. Available: www.mathematicaljournal.com

[15]N. Ahmed et al., "Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction," Sensors (Basel, Switzerland), vol. 22, no. 20. NLM (Medline), Oct. 17, 2022. doi: 10.3390/s22207896.

[16]O. I. D. Bashi, S. M. Jameel, Y. M. Al Kubaisi, H. K. Hameed, and A. H. Sabry, "Threat Detection Model for WLAN of Simulated Data Using Deep Convolutional Neural Network," Applied Sciences (Switzerland), vol. 13, no. 20, Oct. 2023, doi: 10.3390/app132011592.

[17]M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," J Big Data, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-023-00870-w.

[18]V. Chandrasekar et al., "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm," Sci Rep, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-57480-6.

[19]C. Gupta, L. Singh, and R. Tiwari, "Malicious Node Detection in Vehicular Ad-hoc Network (VANET) using Enhanced Beacon Trust Management with Clustering Protocol (EBTM-CP)," Wirel Pers Commun, vol. 130, no. 1, pp. 321–346, May 2023, doi: 10.1007/s11277-023-10287-6.

[20]M. Natkaniec and M. Bednarz, "Wireless Local Area Networks Threat Detection Using 1D-CNN," Sensors, vol. 23, no. 12, Jun. 2023, doi: 10.3390/s23125507.

[21]R. Batool, N. Bibi, S. Alhazmi, and N. Muhammad, "Secure Cooperative Routing in Wireless Sensor Networks," Applied Sciences, vol. 14, no. 12, p. 5220, Jun. 2024, doi: 10.3390/app14125220.

[22]X. Li, X. Bian, and M. Li, "Routing Selection Algorithm for Mobile Ad Hoc Networks Based on Neighbor Node Density," Sensors, vol. 24, no. 2, Jan. 2024, doi: 10.3390/s24020325.

[23]S. Khan, M. A. Khan, and N. Alnazzawi, "Artificial Neural Network-Based Mechanism to Detect Security Threats in Wireless Sensor Networks," Sensors, vol. 24, no. 5, Mar. 2024, doi: 10.3390/s24051641. [37] Basthikodi, M., Chaithrashree, M., Ahamed Shafeeq , B.M. *et al.* Enhancing multiclass brain tumor diagnosis using SVM and innovative feature extraction techniques. *Sci Rep* **14**, 26023 (2024). https://doi.org/10.1038/s41598-024-77243-7

[24] Bhandary, Abhir, and Mustafa Basthikodi. "Early diagnosis of lung cancer using computer aided detection via lung segmentation approach." *arXiv preprint arXiv:2107.12205* (2021).

[25] Meril, A. Silmiya, M. Basthikodi, and A. Rimaz Faizabadi. "Review: comprehensive study of 5G and 6G communication network." *Journal of Emerging Technologies and Innovative Research (JETIR)* 6.5 (2019): 715-719.

[26] M. Basthikodi and W. Ahmed, "Classifying a program code for parallel computing against HPCC," *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, 2016, pp. 512-516, doi: 10.1109/PDGC.2016.7913248.

[27] Basthikodi, Mustafa, Ananth Prabhu, and Anush Bekal. "Performance Analysis of Network Attack Detection Framework using Machine Learning." *Sparklinglight Transactions on Artificial Intelligence and Quantum Computing (STAIQC)* 1.1 (2021): 11-22.

Research Article

[28] Basthikodi, M., Faizabadi, A. R., & Ahmed, W., HPC Based Algorithmic Species Extraction Tool for Automatic Parallelization of Program Code. International Journal of Recent Technology and Engineering, 8(2S3)(2019) 1004–1009. https://doi.org/10.35940/ijrte.b1188.0782s319

[29] Salins, R.D., Ashwin, T.S., Prabhu, G.A. *et al.* Person identification from arm's hair patterns using CT-twofold Siamese network in forensic psychiatric hospitals. *Complex Intell. Syst.* **8**, 3185–3197 (2022). https://doi.org/10.1007/s40747-022-00771-0

[30] Basthikodi M, AhmedW. Parallel Algorithm Performance Analysis using OpenMP for Multicore Machines. International Journal of Advanced Computer Technology (IJACT). 2015;4(5):28–32. Available from: https://www.ijact.org/ijactold/volume4issue5/IJ0450005.pdf.

[31] Shanthakumar HC, Nagaraja GS, Basthikodi M. Performance Evolution of Face and Speech Recognition system using DTCWT and MFCC Features. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12(3):3395–3404. Available from: https://dx.doi.org/10.17762/turcomat. v12i3.1603.

[32] Shruthi M, Mustafa, Prabhu A. Parellel Implementation of Modified Apriori Algorithm on Multicore Systems. ORALNDO, USA. 2016. Available from: http://www.iiis.org/CDs2016/CD2016Spring/papers/ZA819TX.pdf.

[33] Fathima, Sareen, Abdo H. Guroob Suzaifa, and Mustafa Basthikodi. "An efficient application model of smart ambulance support (108) services." *Int J Innov Technol Explor Eng (IJITEE)* 8 (2019).

[34] Mustafa Basthikodi, Poornima B V, "Developing an explainable human action recognition system for academic environments: Enhancing educational interaction", Results in Engineering, Volume 26, 2025, 105014, ISSN 2590-1230, https://doi.org/10.1016/j.rineng.2025.105014.

[35] Pai, P., Amutha, S., Basthikodi, M. *et al.* A twin CNN-based framework for optimized rice leaf disease classification with feature fusion. *J Big Data* **12**, 89 (2025). https://doi.org/10.1186/s40537-025-01148-z