A Secure and Intelligent Hybrid MANET System for Infrastructure-Independent Communication

Prof. Sandhya Patil[1], Ms. Poonam Walale[2], Ms. Riya Dodke[3], Ms. Eshali Wansik[4]
[1,2,3,4]Computer Technology, Priyadarshini College of Engineering, Nagpur

***Abstract*—This paper presents an AI-driven secure hybrid Mobile Ad-Hoc Network (MANET) designed for communication in infrastructure-free environments such as disaster zones, military operations, and remote areas. Unlike traditional systems that depend on internet connectivity and centralized infrastructure, the proposed system enables direct device-to-device communication using hybrid protocols including Wi-Fi Direct, Bluetooth, and LoRa. An AI-based Q-learning routing algorithm dynamically selects optimal communication paths, improving reliability and efficiency. Security is ensured through AES-256 encryption, SHA-256 hashing, and a blockchain-inspired verification mechanism. Experimental results demonstrate improved throughput, reduced latency, and enhanced packet delivery ratio, making the system suitable for real-time tactical communication.**

Index Terms—Tactical Communication, AI-based Routing, Q-Learning, MANET, Infrastructure-Free Network, LoRa, Wi-Fi Direct, Blockchain Security

I. INTRODUCTION

1.1 Background and Need

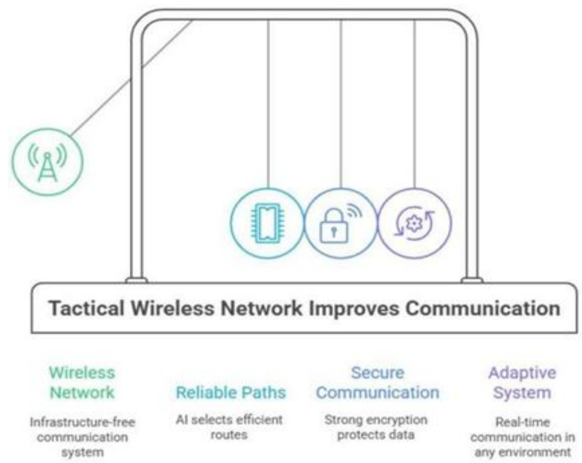
Communication plays a critical role in emergency and tactical scenarios such as military missions, disaster recovery, and rural operations. Traditional communication systems rely on infrastructure like mobile towers, routers, and internet connectivity, which may not be available or may fail during emergencies.

To overcome these limitations, infrastructure-free communication systems such as Mobile Ad-Hoc Networks (MANETs) have been introduced. In MANETs, devices communicate directly and act as both transmitters and routers, enabling flexible and dynamic communication.

1.2 Objective of the System

The objective of this system is to develop a secure, intelligent, and infrastructure independent communication network that:

- Enables real-time message transmission
- Adapts dynamically to network conditions
- Provides secure communication
- Supports long-range and short-range connectivity.



II. LITERATURE REVIEW

1. Routing Optimization Techniques

Various optimization algorithms such as Particle Swarm Optimization (PSO) and energy-aware routing techniques have been used to improve MANET performance. These methods enhance throughput and packet delivery but introduce computational overhead.

2. Hybrid Communication Models

Hybrid and delay-tolerant networks combine multiple communication protocols to improve adaptability. However, these systems often require complex configurations and synchronization.

3. IoT Integration in MANETs

Integration of MANET with IoT improves scalability and data sharing but introduces dependency on cloud infrastructure, limiting its use in offline environments.

4. Security Enhancements in MANET
Blockchain-based routing and deep learning intrusion detection systems improve security but increase latency and processing requirements.

5. AI-Based Routing
Artificial Intelligence techniques such as reinforcement learning and Q-learning provide adaptive routing by learning from network conditions, improving efficiency and reliability.

2.1 Routing Optimization Techniques
Previous research used optimization algorithms like:
- Particle Swarm Optimization (PSO)
- Energy-aware routing

These improve:
- Packet delivery
- Throughput

But drawbacks include:
- High computational cost
- Not suitable for lightweight devices

2.2 Hybrid Network Models
Hybrid systems combine multiple communication methods to improve flexibility.
Example:
- Delay-Tolerant Networks (DTN)

Limitations:
- Complex configuration
- Synchronization issues

2.3 IoT Integration in MANET
Some systems combine MANET with IoT and cloud:
- Enables scalability
- Improves data storage

But:
- Requires internet
- Not suitable for disaster zones

2.4 Security Approaches
Existing security solutions include:
- Blockchain-based routing
- Deep learning intrusion detection

Problems:
- High energy consumption
- Increased latency

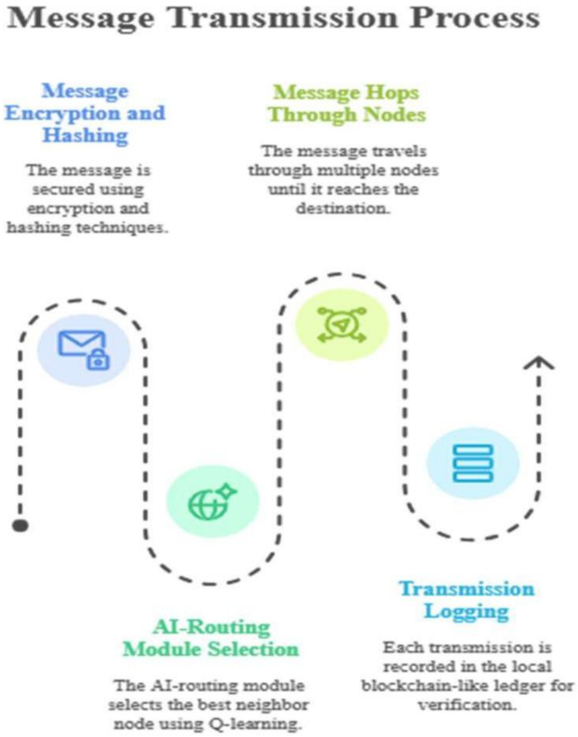
2.5 AI-Based Routing (Key Contribution Area)
AI (especially reinforcement learning) allows:
- Learning from environment
- Dynamic decision-making
- Route optimization

Your system improves on previous work by combining:
- AI + Hybrid communication + Lightweight design

III. THEORY

The proposed system is based on the concept of a Mobile Ad-Hoc Network (MANET), which is a decentralized wireless network that operates without relying on any fixed infrastructure such as routers, base stations, or internet connectivity. In such a network, each node acts both as a communication endpoint and as a router, enabling data to be transmitted across multiple hops until it reaches its intended destination. This self-organizing nature makes MANETs highly suitable for applications in tactical environments, disaster management, and remote areas where conventional communication systems are unavailable or unreliable.
To enhance communication efficiency and reliability, the system employs a hybrid communication model that integrates multiple wireless technologies, including Wi-Fi Direct, Bluetooth, and LoRa. Wi-Fi Direct is utilized for high-speed, short-range communication, while Bluetooth provides energy-efficient connectivity for nearby devices. LoRa technology enables long-range communication with low power consumption, making it ideal for transmitting data over large distances. The combination of these technologies allows the system to dynamically switch between communication modes based on network conditions, thereby ensuring continuous and adaptive connectivity in infrastructure-free environments.
A key component of the proposed system is the integration of Artificial Intelligence, specifically a reinforcement learning technique known as Q-

learning, for routing optimization. Unlike traditional routing protocols that rely on static rules, Q-learning enables



each node in the network to learn optimal routing decisions through interaction with its environment. The algorithm evaluates various parameters such as signal strength, node energy levels, latency, and link reliability to determine the most efficient path for data transmission. Each possible routing action is assigned a Q-value, which represents the expected performance of selecting that route.

Q(s,a)=Q(s,a)+α[r+γmax⁡Q(s′,a′)−Q(s,a)]Q(s,a)=Q(s, a)+\ alpha\left[r+\gamma \max Q(s',a')-Q(s,a)\right]Q(s,a)=Q(s,a)+α[r+γmaxQ(s′,a′)−Q(s,a)]

In this equation, Q(s,a)Q(s,a)Q(s,a) represents the current quality of a routing decision, α\alphaα is the learning rate, γ\gammaγ is the discount factor that determines the importance of future rewards, and rrr is the immediate reward obtained from the environment. Based on the success or failure of data transmission, the Q-values are updated iteratively, allowing the system to gradually learn and converge toward optimal routing paths. This results in improved adaptability, reduced latency, enhanced packet delivery ratio, and better energy efficiency in dynamic network conditions.

In addition to intelligent routing, the system incorporates a robust security framework to ensure secure communication. Data confidentiality is maintained using Advanced Encryption Standard (AES-256), while data integrity is verified using SHA-256 hashing. Furthermore, a lightweight blockchain-inspired mechanism is implemented, where each message is linked to the previous one through cryptographic hashes, creating a tamper- evident log of communications. This approach enhances trust and prevents unauthorized modification of data without introducing significant computational overhead.

To address challenges related to intermittent connectivity, the system utilizes a store-and-forward mechanism, where messages are temporarily stored at intermediate nodes and transmitted when a suitable communication path becomes available. This ensures reliable message delivery even in delay-tolerant network conditions.

Overall, the theoretical foundation of the proposed system lies in the integration of decentralized networking, intelligent routing through reinforcement learning, hybrid communication technologies, and multi-layered security mechanisms. This combination enables the development of a secure, adaptive, and infrastructure-independent communication system capable of operating effectively in challenging and dynamic environments.

IV. EXPERIMENTAL

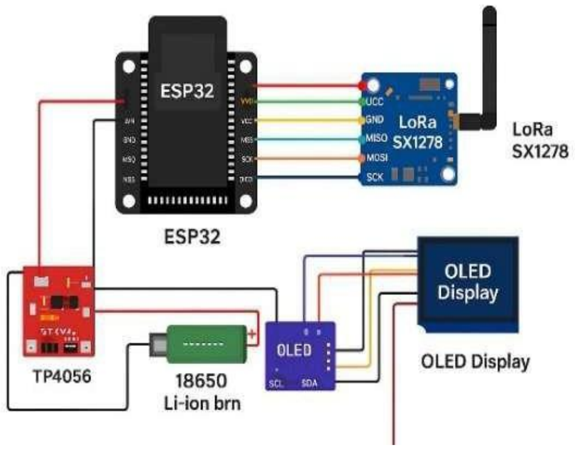
METHOD/PROCEDURE/DESIGN

The experimental design of the proposed AI-driven secure hybrid MANET system was developed to validate its performance, adaptability, and reliability in real-world infrastructure-free environments. The implementation involved a combination of hardware setup, software configuration, communication workflow, and performance evaluation under dynamic conditions.

A. Hardware Configuration

The experimental setup consisted of multiple wireless nodes, each built using an ESP32 microcontroller integrated with a LoRa SX1278 module. The ESP32 was selected due to its built-in support for Wi-Fi and Bluetooth, enabling seamless integration of short-range communication protocols. The LoRa module was used to provide long-range communication capability with low power consumption.

Each node was powered by a rechargeable Li-ion battery, ensuring portability and independence from external power sources. Additional components such as optional GPS modules, OLED displays, and buzzers were included in some nodes to enhance monitoring and alert capabilities. This hardware configuration enabled the deployment of a fully decentralized and mobile communication network.



B. Software and System Setup

The software implementation was carried out using the Arduino IDE for programming the ESP32 nodes. Communication protocols, routing logic, and security mechanisms were embedded within the firmware. A lightweight AI model based on Q-learning was implemented locally on each node to enable decentralized decision-making without relying on external computation resources.

A custom Android application was developed using Android Studio to provide a user interface for message transmission, reception, and monitoring. The application handled encryption, message formatting, and local storage. It also supported features such as SOS alerts, delivery status tracking, and offline message storage using a store- and-forward approach.

C. Network Deployment and Topology

The experimental network was deployed in a semi-open outdoor environment, where nodes were placed at distances ranging from 50 to 100 meters. The nodes were either manually repositioned or allowed to move dynamically to simulate real-world scenarios such as military operations or disaster rescue missions.

The network topology was dynamic and self-organizing, meaning that nodes continuously discovered neighboring nodes and updated routing paths as the network changed. This setup allowed the system to be tested under conditions of:

- Frequent topology changes
- Node mobility
- Variable signal strength
- Intermittent connectivity

D. Communication Procedure

The communication process followed a structured multi- stage workflow:

1. Network Initialization:

Each node activated its communication interfaces (Wi-Fi, Bluetooth, LoRa) and performed neighbor discovery to establish initial connections.

2. Message Generation:

A user generated a message through the Android application, which was then prepared for transmission.

3. Security Processing:

- The message was encrypted using AES- 256 to ensure confidentiality.
- A SHA-256 hash was generated to maintain data integrity.
- The hash was stored in a blockchain- inspired ledger for tamper detection.

4. AI-Based Route Selection:

The Q-learning algorithm evaluated available neighboring nodes based on parameters such as:

- Received Signal Strength Indicator (RSSI)
- Latency
- Hop count
- Node energy level
- Link reliability

The node with the highest Q-value was selected as the next hop.

5. Multi-Hop Transmission:

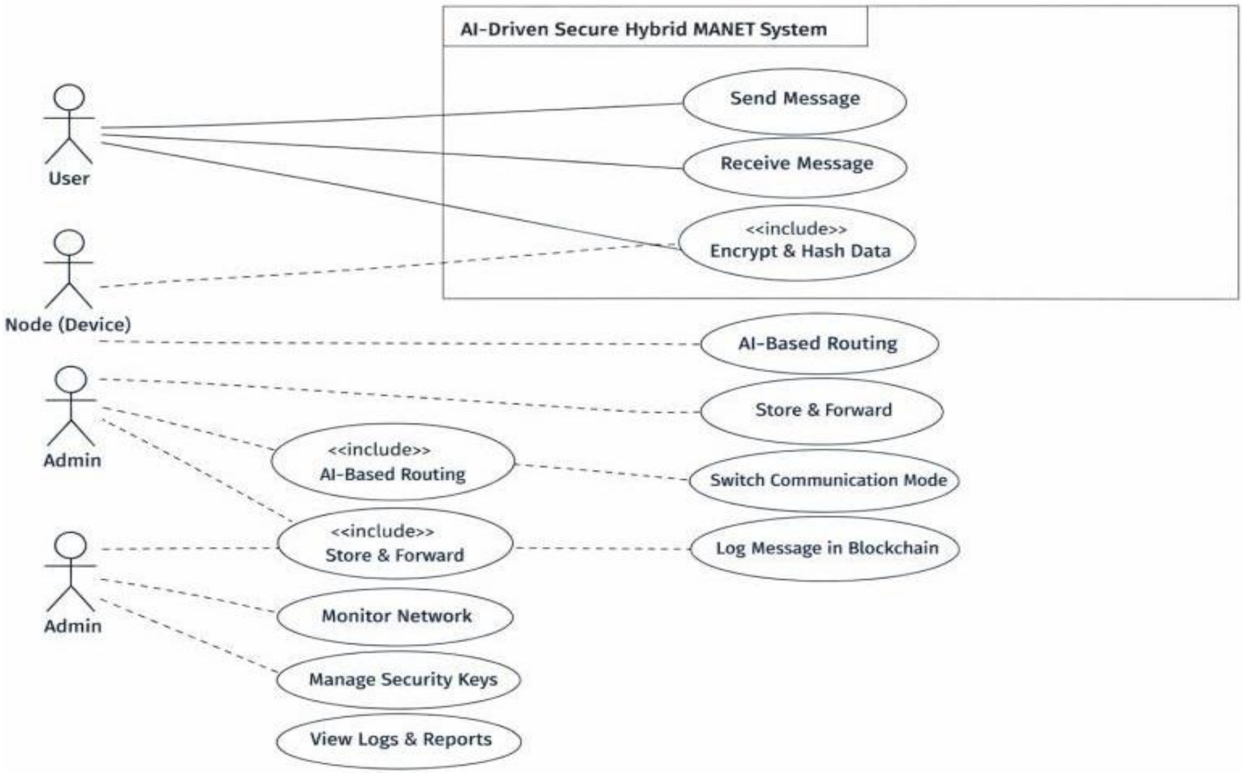
The message was forwarded from node to node until it reached the destination. Each intermediate node repeated the routing decision process.

6. Store-and-Forward Mechanism:

If no suitable path was available, the message was temporarily stored and forwarded later when connectivity was restored.

7. Logging and Verification:
Each transmission was recorded in a blockchain- like structure, ensuring traceability and preventing unauthorized modifications.

Use Case Dagram:



E. AI Training and Adaptation
The Q-learning model operated continuously during the experiment. Initially, routing decisions were exploratory, but over time, the algorithm learned optimal paths based on reward feedback.

- Positive rewards were assigned for successful, low-latency transmissions.
- Negative rewards were assigned for packet loss, delays, or unstable links.

This adaptive learning mechanism enabled the network to:

- Improve routing efficiency over time
- Quickly adapt to node failures
- Balance energy consumption across nodes

F. Performance Metrics and Evaluation
To evaluate system performance, several key metrics were measured and compared against a baseline routing protocol (AODV):

- Throughput: Rate of successful data delivery
- Latency: Time taken for message delivery
- Packet Delivery Ratio (PDR): Percentage of successfully delivered packets
- Route Recovery Time: Time required to re-establish communication after failure
- Energy Efficiency: Power consumption during operation

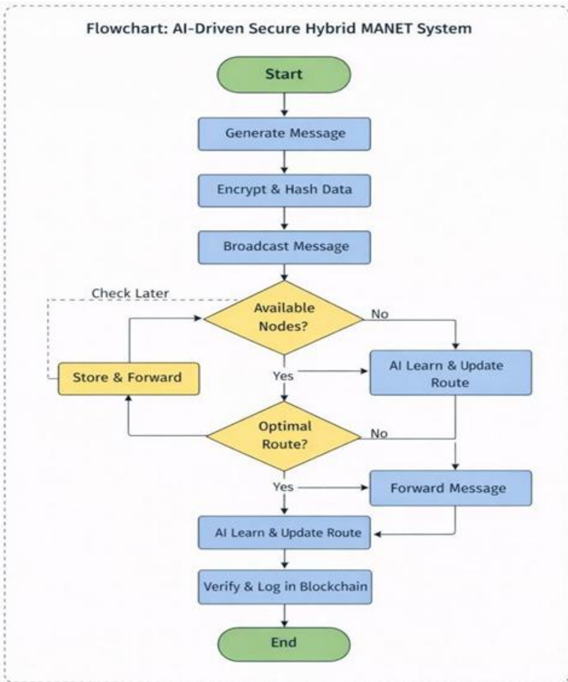
These metrics were recorded under varying conditions, including node mobility and network congestion, to assess system robustness.

G. Experimental Conditions
The experiment was conducted under the following controlled conditions:

- Node spacing: 50–100 meters
- Environment: Semi-open outdoor area
- Mobility: Moderate (simulated real-world movement)
- Communication modes: Hybrid (Wi-Fi, Bluetooth, LoRa)
- Data type: Encrypted text messages

H. Summary of Experimental Design

The experimental design integrates hardware implementation, AI-based routing, hybrid communication, and secure data transmission into a unified framework. By simulating real-world conditions and evaluating multiple performance parameters, the experiment effectively demonstrates the feasibility and efficiency of the proposed system in infrastructure-free environments.



V. RESULTS AND DISCUSSION

The performance of the proposed AI-driven secure hybrid MANET system was evaluated under realistic infrastructure-free conditions. The results demonstrate significant improvements in communication efficiency, reliability, and adaptability when compared with traditional routing protocols such as AODV.

A. Experimental Results

The system was tested in a semi-open environment with mobile nodes placed at distances ranging from 50 to 100 meters. The following key performance metrics were observed:

- Throughput:

The proposed system achieved a higher data transmission rate, with an improvement of approximately 35–40% compared to the baseline method. This increase is attributed to intelligent route selection using Q-learning, which avoids congested or weak links.

- Latency:

The average end-to-end delay was reduced from approximately 300–350 ms (AODV) to 220–250 ms in the proposed system, representing a reduction of nearly 25%. Faster route optimization and adaptive protocol switching contributed to this improvement.

- Packet Delivery Ratio (PDR):

The system achieved a PDR of around 98%, significantly higher than the baseline value of 82%. This indicates reliable data transmission even in dynamic and unstable network conditions.

- Route Recovery Time:

In case of node failure or link disruption, the system recovered routes in approximately 1.8 seconds, compared to 3.5 seconds in traditional approaches. This demonstrates the self-healing capability of AI-based routing.

- Energy Efficiency:

The proposed routing strategy distributed network load efficiently, resulting in balanced energy consumption across nodes and extended network lifetime.

These results are consistent with the observations presented in the performance table in your paper.

B. Discussion

The observed improvements can be directly linked to the integration of AI, hybrid communication, and security mechanisms within the system.

The Q-learning-based routing algorithm played a crucial role in enhancing network performance. Unlike static routing protocols, the algorithm continuously learned from network conditions and selected optimal paths based on real-time parameters such as signal strength, latency, and node availability. As the experiment progressed, the system showed noticeable improvement in decision- making, indicating successful learning and convergence.

The hybrid communication model also contributed significantly to system reliability. The ability to switch between Wi-Fi, Bluetooth, and LoRa ensured uninterrupted communication even when one channel experienced failure or degradation. For example, when short-range communication became unstable, the system seamlessly transitioned to LoRa for long-range transmission, maintaining connectivity without manual intervention.

The store-and-forward mechanism proved effective in handling intermittent connectivity. In scenarios where direct communication paths were unavailable, messages were temporarily stored and forwarded once a stable link was established. This ensured message delivery even in delay-tolerant conditions.

From a security perspective, the combination of AES-256 encryption, SHA-256 hashing, and blockchain-inspired logging ensured secure and tamper-proof communication. The blockchain-like ledger provided traceability of message exchanges while maintaining low computational overhead, making it suitable for resource-constrained devices.

However, some limitations were observed during experimentation. The initial learning phase of the Q-learning algorithm involved exploration, which occasionally resulted in suboptimal routing decisions. Additionally, the integration of multiple communication protocols introduced system complexity, requiring careful synchronization and resource management.

Despite these challenges, the overall system demonstrated strong performance in dynamic environments. The results confirm that the proposed approach effectively enhances MANET communication by providing adaptive routing, improved reliability, faster recovery, and secure data transmission.

VI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

This research presents an AI-driven secure hybrid Mobile Ad-Hoc Network (MANET) designed for communication in infrastructure-free environments. The proposed system integrates Q-learning-based intelligent routing, hybrid wireless communication technologies (Wi-Fi Direct, Bluetooth, and LoRa), and a multi-layered security framework to address the limitations of traditional MANET systems.

The experimental results demonstrate that the system significantly improves key performance parameters such as throughput, latency, packet delivery ratio, and route recovery time. The AI-based routing mechanism enables dynamic adaptability and efficient path selection in changing network conditions, while the hybrid communication model ensures uninterrupted connectivity across varying distances. Additionally, the implementation of AES-256 encryption, SHA-256 hashing, and blockchain-inspired logging provides secure and tamper- resistant communication.

Overall, the proposed system offers a reliable, adaptive, and secure communication solution suitable for tactical operations, disaster management, and remote area connectivity. It successfully overcomes the dependency on fixed infrastructure and demonstrates the potential of integrating artificial intelligence with decentralized networking.

B. Future Scope

Although the proposed system shows promising results, several enhancements can be considered to further improve its performance and applicability:

- Federated Learning Integration:

Future work can incorporate federated learning to enable nodes to collaboratively train AI models without sharing raw data, improving routing intelligence while preserving privacy.

- Advanced Intrusion Detection System (IDS):

Lightweight machine learning-based IDS can be integrated to detect and isolate malicious or compromised nodes in real time.

- Voice and Multimedia Communication:

The current system supports text-based communication; future extensions can include real-time voice, image, and sensor data transmission for enhanced usability.

- Scalability Enhancement:

The system can be optimized to support large- scale networks with hundreds or thousands of nodes while maintaining performance and efficiency.

- Integration with UAVs and Drones:

Unmanned Aerial Vehicles (UAVs) can be used as mobile relay nodes to extend network coverage in large disaster zones or battlefield environments.

• Energy Optimization Techniques:
Advanced power management strategies and energy-aware routing can be implemented to further extend node battery life.

• Real-World Deployment and Testing:
Future research can focus on large-scale field trials in real disaster or military scenarios to validate system robustness under extreme conditions.

REFERENCES

[1] O. Almutairi, E. Khairullah, A. Almakky, and R. Alotaibi, "Routing enhancement in MANET using particle swarm algorithm," *Automation*, vol. 5, no. 4, pp. 630–643, Dec. 2024.

[2] O. Nakayima, M. I. Soliman, K. Ueda, and S. A. Elsagheer, "Enhancing bundle delivery efficiency in mobile ad-hoc networks with a multi-protocol delay-tolerant network," *Journal of Computer Networks*, July 2024.

[3] V. Narayandas, A. Maruthavanan, and R. Dugyala, "Integration of MANET and IoT for enhancing smart device communication infrastructure," *IARJSET*, vol. 11, no. 1, pp. 76–78, Jan. 2024.

[4] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," *IEEE Transactions on Networking*, Mar. 2024.

[5] T. Saravanan and S. Saravanakumar, "Energy efficient optimization algorithms for MANET," in *Proc. IC3 2023: International Conference on Contemporary Computing*, ACM, pp. 572–580, Aug. 2023.

[6] N. Ghodichor, R. T. V., D. Sahu, G. Borkar, and A. Sawarkar, "Secure routing protocol to mitigate attacks by using blockchain technology in MANET," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 15, no. 2, pp. 127–135, Mar. 2023.

[7] P. Fraga-Lamas and T. M. Fernández-Caramés, "Tactical edge IoT in defense and national security," in *IoT for Defense and National Security*, Wiley-IEEE Press, Jan. 2023.

[8] W. G. Theresa, A. Gayathri, and P. Rama, "A collaborative approach for secured routing in mobile ad-hoc network," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1–10, Mar. 2022.

[9] Z. A. Abbood, D. C. Atilla, and Ç. Aydin, "Intrusion detection system through deep learning in routing MANET networks," *Intelligent Automation & Soft Computing*, vol. 37, no. 1, pp. 1–15, Nov. 2022.

[10] T. Alam, "Device-to-device communications in cloud, MANET and Internet of Things integrated architecture," *International Journal of Computer Applications*, Apr. 2020.

[11] T. Alam, "Internet of Things: A secure cloud-based MANET mobility model," *International Journal of Computer Applications*, Feb. 2020.

[12] T. Alam and B. Rababah, "Convergence of MANET in communication among smart devices in IoT," *International Journal of Wireless and Microwave Technologies*, vol. 9, no. 2, pp. 1–10, Oct. 2019.