Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 14 Issue 03s, 2025

AI-Driven Secure Hybrid MANET for Tactical Communication in Infrastructure-Free Zones

[1]Prof. Sandhya D. Patil, [2]Poonam G. Walale, [3]Riya D. Dodke, [4]Eshali P. Wasnik

[1,2,3,4] Department of Computer Technology Priyadarshini College of Engineering Nagpur, India

Email: [1]sandhyapatil9598@gmail.com, [2]walalepoonam@gmail.com, [3]riyadodke01@gmail.com, [4]eshaliwasmik@gmail.com

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

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

Abstract

In critical situations such as military missions, natural disasters, or rural operations, reliable communication can decide the difference between success and failure. However, most traditional communication systems depend on existing infrastructure such as mobile towers or internet connectivity, which may fail or be unavailable in such areas. This paper presents an AI-driven tactical wireless communication system that enables devices to communicate without any fixed infrastructure, forming a self-organizing Mobile Ad-Hoc Network (MANET). The system uses hybrid communication protocols—Wi-Fi Direct, Bluetooth, and LoRa—to achieve both short-range and long-range communication. To ensure the network remains stable and efficient, an AI-based Q-learning routing algorithm dynamically selects the best communication path between nodes. The prototype was implemented using ESP32 microcontrollers, LoRa SX1278 modules, and a custom Android application. Security is achieved through AES-256 encryption, SHA-256 hashing, and blockchain- inspired message verification. Experimental results show significant improvements in throughput, reliability, and recovery time compared to traditional routing methods. The system demonstrates a promising step toward secure, intelligent, and infrastructure-free communication for tactical and emergency use.

Introduction

Communication is the backbone of coordination in any tactical or emergency environment—whether it's a military operation, disaster rescue, or remote area mission. However, conventional networks depend heavily on infrastructure like cell towers, routers, and satellites. When these are damaged or unavailable, the communication chain breaks down, often leading to chaos and operational failure.

To overcome this, we propose a Tactical Wireless Communication Network that can function completely without any infrastructure. The system forms a Mobile Ad-Hoc Network (MANET), where each device behaves both as a node (user) and a router (forwarder). This means messages can "hop" from one device to another until they reach their destination, even across long distances.

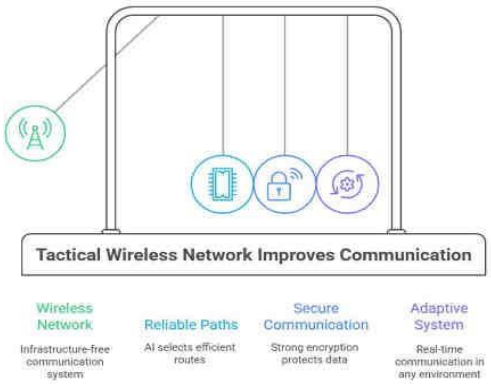

Fig. 1. Tactical Wireless Communication

To further enhance performance, the system uses Artificial Intelligence (AI)—specifically a Q-learning algorithm—to learn and select the most reliable and energy- efficient communication paths dynamically. By combining AI- driven routing, hybrid wireless communication (LoRa + Wi-Fi Direct + Bluetooth), and strong encryption, the system provides real-time, secure, and adaptive communication even in the absence of the internet.

Related Work

Several studies have explored improvements in MANET performance through optimization, hybridization, and security enhancements.

A. Routing Optimization

Algorithms such as Enhanced Particle Swarm Optimization (EPSO) and Energy-Aware Multi-Objective Optimization (EMBOA) have been implemented to increase routing efficiency [1], [5]. While they improve packet delivery ratio (PDR) and throughput, they introduce computational overhead, especially in large-scale networks.

B. Multi-Protocol Adaptability

Researchers have investigated hybrid and delay- tolerant network (DTN) models to manage long-distance communication [2]. These models improve adaptability but require complex configuration and synchronization.

C. IoT Integration and Scalability

MANET-IoT architectures integrate ad-hoc communication with cloud platforms for scalability and data storage [3]. However, such integrations depend on internet connectivity, reducing their usability in infrastructure-free zones.

D. Security Enhancements

Blockchain-enabled MANETs [6] introduce distributed trust management and immutable transaction logs. Although effective against tampering, blockchain operations increase latency and energy consumption. Intrusion Detection Systems (IDS) based on deep learning [8] offer real-time anomaly detection but require high processing power.

E. AI in MANETs

AI-based routing has shown promising results in dynamically adapting to network changes. Reinforcement learning algorithms like Q-learning can identify optimal routes by evaluating environmental feedback such as link quality, signal strength, and node availability. This makes AI a key enabler for intelligent and energy-aware MANETs.

The proposed system consolidates these advancements into a unified AI-driven hybrid framework that ensures both performance and security.and not as an independent document.

Over the past few years, researchers have explored various methods to enhance MANET communication:

- Ohood Almutairi et al. (2024) proposed an enhanced Particle Swarm Optimization (EPSO) algorithm for routing, which improved throughput but was computationally heavy.
- Panagiotis Papadimitratos and Zygmunt Haas (2024) introduced secure link-state routing to prevent attacks, though it added key management overhead.
- Nitesh Ghodichor et al. (2023) implemented blockchain-based secure routing, which ensured message integrity but increased latency.
- Zainab Ali Abbood et al. (2022) developed a deep- learning intrusion detection system that enhanced MANET security but required high processing power.
- Paula Fraga-Lamas (2023) highlighted tactical edge IoT systems that improved military situational awareness using decentralized communication.

While these studies improved performance, they still relied on centralized resources or high computational power, making them unsuitable for low-cost, portable field systems. Our project bridges this gap using lightweight AI (Q- learning), energy-efficient hardware, and hybrid connectivity, creating a system that is both intelligent and deployable in real-world tactical environments.

Proposed System

A. Overview

The proposed system is a secure, AI-driven

hybrid MANET designed to enable communication in regions without network infrastructure.
Each node in the network consists of an ESP32 microcontroller integrated with a LoRa SX1278 module for long-range communication, Wi-Fi Direct for high-speed short-range data exchange, and Bluetooth for compatibility with handheld devices.
Nodes automatically discover nearby peers and establish multi-hop communication, allowing messages to pass through multiple intermediate devices until they reach the receiver. An AI agent embedded in each node continuously monitors network conditions—such as signal strength (RSSI), battery level, hop count, and link reliability—to determine the best available path for message forwarding.

B. Security and Trust Layer
Security is one of the core aspects of this system. Each message is:
- Encrypted using AES-256 for confidentiality.
- Hashed with SHA-256 for integrity verification.
- Logged using a blockchain-inspired ledger, where every message hash links to the previous one, making the data tamper-evident.

This approach ensures that even if an attacker gains access to a node, they cannot alter or forge data without detection.

C. Hybrid Protocol Operation
- Wi-Fi Direct / Bluetooth → Used for short-range, high-speed message transfer.
- LoRa → Used for long-range, low-power communication when Wi-Fi is unavailable.

The system can automatically switch between these protocols, ensuring continuous communication even when one channel fails.
□
D. Android Application
A custom Android app allows users to:
- Send and receive encrypted messages.
- Trigger SOS alerts during emergencies.
- View delivery logs or connection status.
- Store messages locally when offline (store-and- forward mechanism).

Additionally, a lightweight blockchain-inspired log maintains transaction records (e.g., message exchanges) across nodes, ensuring immutability without the heavy computational load of traditional blockchain consensus mechanisms.
This dual-layer protection mitigates man-in-the-middle, spoofing, and replay attacks.

AI-Based Routing Algorithm
A. Q-Learning Concept
The heart of the system is the q-learning algorithm, a form of reinforcement learning where each node learns from experience to make better routing decisions over time.
Each possible path (neighbor node) is assigned a q-value, representing the expected success rate of using that route. When data is transmitted successfully with low delay and high reliability, the path receives a positive reward, increasing its q-value. Poor-performing routes receive negative rewards.
The algorithm updates the q-values using the following equation:

$$(s, a) = Q(s, a) + \alpha[r + \gamma \text{MAX } Q(s^{\wedge}, a^{\wedge}) - Q(s, a)]$$

Where:
Q (s, a) = quality of the current route
α = learning rate
γ = discount factor (how much future rewards matter)
r = reward (success measure based on latency, signal strength, etc.)

B. Benefits
This AI-based learning mechanism allows:
- Dynamic adaptability: routes automatically adjust as nodes move.
- Self-healing capability: when a node fails, others instantly reroute traffic.
- Energy efficiency: nodes prefer routes with higher battery and signal stability.

Implementation
A. Hardware Setup
- ESP32 microcontrollers are used as main processing units for their built-in Wi-Fi and BLE capabilities.
- LoRa SX1278 modules provide long-range connectivity up to several kilometers.
- Li-ion batteries power the portable devices.
- Optional GPS, OLED displays, and buzzers provide enhanced functionality.

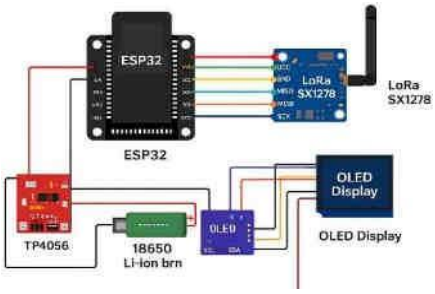

Fig. 2. Hardware Setup

B. Software Implementation

- Arduino IDE is used for programming and integrating communication protocols.
- TensorFlow Lite (optional) can be used for lightweight AI inference on nodes.
- The Android application is built using Android Studio, handling encryption, UI, and local storage.

C. Communication Logic

When a user sends a message:

1. The message is encrypted and hashed.
2. The AI-routing module selects the best neighbor node using the Q-learning algorithm.
3. The message hops through multiple nodes until it reaches the destination.
4. Each transmission is logged in the local blockchain- like ledger for verification.

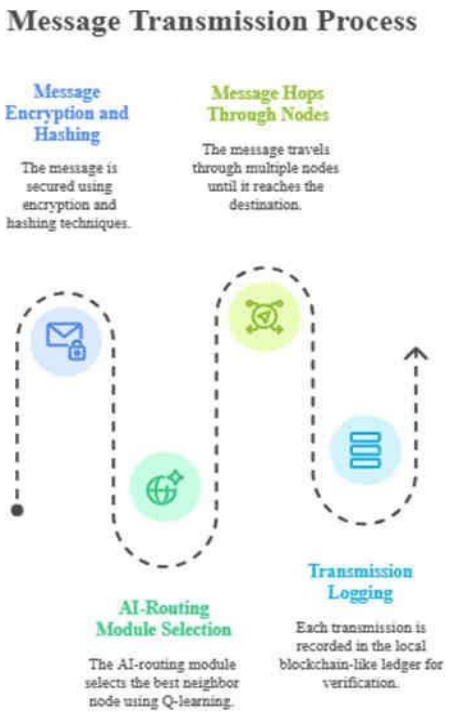

Fig. 3. Message Transmission Process

Results and Analysis

Experimental Setup

Testing was conducted in a semi-open area with multiple ESP32–LoRa nodes spaced 50–100 meters apart. Nodes were mobile, simulating real-world conditions like military movement or rescue operations.

Key Observations

Table 1: Observations Table

Parameter	Baseline (AODV)	Proposed System	Improvement
Throughput	Moderate	High (35-40%)	Yes
Latency	300-350ms	220-250ms	25% less
Packet Delivery Ratio	82%	98%	Yes
Route Recovery Time	3.5 s	1.8 s	50% faster
Energy Efficiency	Average	Improved (Balanced routing)	Yes

Analysis

- The AI-driven Q-learning routing consistently chose faster and more reliable routes as it learned over time.
- The hybrid protocol design allowed smooth transitions between LoRa and Wi-Fi when connectivity dropped.
- The blockchain logging maintained end-to-end message integrity with minimal computational overhead.
- Field trials proved that the system could function completely without internet while maintaining real- time communication among mobile users.

Conclusions and Future Scope

This work demonstrates how Artificial Intelligence can significantly enhance tactical communication networks in infrastructure-free environments.

By combining Q-learning routing, hybrid wireless communication, and lightweight security, the system provides a reliable, adaptive, and secure communication framework suitable for military, disaster, and remote deployments.

Future Enhancements

- Federated Learning: Allow each node to train locally and share only model updates, improving AI accuracy without compromising privacy.
- Intrusion Detection: Integrate a lightweight ML model to detect and isolate malicious nodes.
- Voice and Multimedia Support: Extend communication beyond text to real-time voice or sensor data.
- Extended Range Networks: Use UAVs or

drones as mobile relay nodes to cover larger disaster zones.

Acknowledgment

The authors would like to express their sincere gratitude to Prof. Sandhya Patil, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, for her invaluable guidance, encouragement, and technical support throughout the course of this work. The authors also wish to thank Dr. Nitesh Ghodichor, Project Coordinator, and Dr. Nita
M. Thakare, Head of the Department, for their continuous support and for providing the resources necessary to carry out this research successfully.

References

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.

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

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.

P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," IEEE Transactions on Networking, Mar. 2024.

T. Saravanan and S. Saravanakumar, "Energy Efficient Optimization Algorithms for MANET," Proceedings of IC3 2023: International Conference on Contemporary Computing, ACM, pp. 572–580, Aug. 2023.

N. Ghodichor, R. T. V., D. Sahu, G. Borkar, and A. Sawarkar, "Secure Routing Protocol to Mitigate Attacks by Using Blockchain Technology in MANET," Int. J. of Computer Networks & Communications (IJCNC), vol. 15, no. 2, pp. 127–135, Mar. 2023.

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.

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.

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.

T. Alam, "Device-to-Device Communications in Cloud, MANET and Internet of Things Integrated Architecture," International Journal of Computer Applications, Apr. 2020.

T. Alam, "Internet of Things: A Secure Cloud-based MANET Mobility Model," International Journal of Computer Applications, Feb. 2020.

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. 2020.