A Token-Based Handshake Protocol for Secure Offline Communication in Tactical MANETs

Hope Leticia Nakayiza [1], Love Allen Chijioke Ahakonye [2], Dong-Seong Kim [1] *, Jae Min Lee [1]
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
(hopeleticia, loveahakonye, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Military vehicles operating in tactical mobile ad-hoc networks (MANETs) frequently encounter adversarial environments where connectivity to conventional communication infrastructure is unavailable or disrupted. Ensuring continuous, secure, and verifiable message exchange under such constraints remains a significant challenge. This paper presents a lightweight, infrastructure-independent message delivery framework based on a self-contained cryptographic token that combines authentication, integrity verification, and payload in a single structure. To support secure peer-to-peer exchange, a Schnorr-based mutual authentication handshake prevents spoofing and replay attacks. The framework is evaluated under varying communication ranges and connectivity levels, using metrics such as packet delivery ratio, latency, and SNR-based drops. Simulation results confirm the system's ability to maintain secure and efficient message delivery even in fully disconnected scenarios, demonstrating its suitability for tactical military deployments.**

***Index Terms*—Mobile Ad Hoc Networks, Offline Communication, Tactical MANETs, Token-based Protocol**

I. Introduction

Mobile ad hoc networks (MANETs) are decentralized, dynamic systems where mobile nodes exchange data via multi-hop wireless communication [1]. Military tactical MANETs (Figure 1) enable military platforms to share information, enhancing operational efficiency, command control, and situational awareness in contested environments [2]. These networks support secure, resilient communication for military mobility units like tanks and UAVs, ensuring the timely dissemination of critical information (e.g., enemy positions, tactical updates) despite challenges like jamming, terrain, and remote deployments [3], [4]. In contested scenarios, reliance on centralized infrastructure can be unreliable or disrupted, highlighting the need for robust alternative communication methods [5], [6].

The growing relevance of delay-tolerant networking (DTN) and opportunistic communication strategies is particularly evident in environments with sparse connectivity [7], [8]. Dedicated Short-Range Communication (DSRC) enables high-bandwidth [9], low-latency vehicle-to-vehicle communication over distances of 300 to 900 meters. Similarly, LoRa 2.4 GHz extends communication to 15 km in rural areas and 2 km in urban environments [10]. The challenges in military tactical

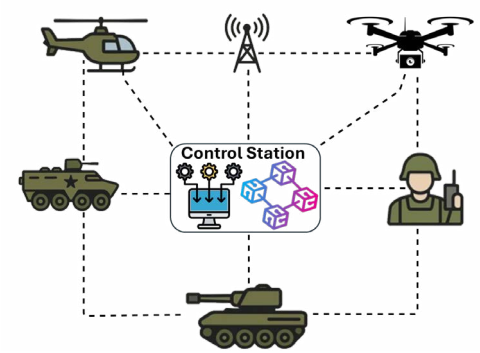

Fig. 1: Simplified Overview of Military Tactical MANETs

MANETs, including dynamic topology, limited bandwidth, and pervasive security threats [11], highlight the need for secure communication protocols that perform effectively in disconnected or adversarial environments [2].

In disconnected tactical environments where conventional command infrastructure is unavailable, ensuring message authenticity and integrity becomes essential [12]. While existing pre-signature schemes [13] provide offline authentication capabilities, they often fall short in supporting dynamic message delivery among mobile military units under intermittent connectivity [14]. To address these gaps, this study introduces a token-based secure message delivery framework that enables military vehicles to communicate continuously without relying on centralized infrastructure. The token-based secure handshake protocol for military communications within intermittent connectivity facilitates direct peer-to-peer interactions between tactical nodes, eliminating dependency on centralized infrastructure.

The contributions of this paper can be summarized as follows:

1) A self-contained token design that encapsulates the message payload, authentication, and integrity metadata, enabling secure and verifiable communication during offline or intermittently connected states with reduced computational overhead.
2) A lightweight challenge–response handshake protocol

that facilitates mutual authentication between tactical vehicles without requiring real-time connectivity to centralized command infrastructure, ensuring trust establishment in dynamic and adversarial environments.

3) An efficient tokenized message exchange scheme that supports low-bandwidth, delay-tolerant communication by combining pre-signature reuse and Schnorr-based signing to minimize cryptographic operations during offline mission-critical message dissemination.

The study arrangement is thus as follows: Following the introduction in Section I, Section II reviews existing works related to the study. Section III discusses the proposed token-based handshake protocol. Section IV highlights the experimentation and results. Section V concludes the study.

II. Related Works

The development of secure and resilient communication systems has been a focal point of research in critical military networks. In their study, Abhisek et al. [15] integrated an XOR-based secret-sharing scheme with multipath communication to ensure protection against possible threats along communication paths. To enhance message dissemination in tactical ad-hoc networks, regardless of the routing protocol in use, Ruffieux et al. [16] proposed a messaging application based on the GetCloser algorithm. This approach introduced an application-level layer above the networking stack to facilitate efficient message exchange and transmission. Namgon et al. [17] proposed a secure in-vehicle network for military unmanned ground vehicles by segmenting components into virtual networks based on their roles and blocking unnecessary connections even within the same virtual network through security policies to reduce the risk of potential security breaches within the vehicle.

Ensuring reliable communication in Internet of Things (IoT) applications under intermittent connectivity has emerged as a significant challenge. Numerous studies have explored strategies to address the limitations posed by network disruptions during device-to-device communication. Khalid et al. [18] proposed a hybrid online and offline multi-factor authentication method for connected car-sharing environments. To enable interoperable communication in environments with intermittent connectivity, [19] introduced an asynchronous message-forwarding architecture built upon a message-switching abstraction. However, the centralized nature of these approaches suggests a risk of tampering with identification data.

To address the challenges of irregular roadside unit coverage in rural areas, [20] implemented a pre-signature scheme to improve communication trust and reliability in vehicle-to-vehicle communication. To facilitate rapid authentication at roadside units, Rabiah et al. [21] leveraged tokens to eliminate the dependency on back-end servers during the brief communication window between moving vehicles and the infrastructure. To enhance message transmission reliability in urban vehicular ad hoc networks, Balador et al. [22] introduced a dynamic token-based medium access control protocol that integrates random access with token passing, effectively reducing channel contention.

Nonetheless, these approaches rely on the assumption of constant network availability for data transmission and verification, which limits their applicability in fully offline military scenarios. This gap highlights the importance of developing a resilient protocol that can maintain secure, efficient, and uninterrupted communication among military vehicles operating without persistent connectivity.

III. System methodology

A. System Overview and Architecture

The proposed system architecture enables secure and continuous vehicle-to-vehicle (V2V) communication under intermittent connectivity and complete offline conditions. The system in Figure 2 consists of three main components: military vehicle nodes, a central synchronization node (CSN), and structured cryptographic tokens.

The CSN serves as a trusted online authority, issuing public key certificates and pre-signature tokens to military vehicles. These certificates associate a vehicle's identity with its Schnorr public key, following a public-key infrastructure (PKI) model. Military vehicles, as autonomous nodes, are equipped with a Schnorr key pair and a certificate issued by CSN. They also store pre-signature tokens, which are cryptographic structures signed by the CSN using its private key. These tokens, created during online interactions, allow vehicles to efficiently handle secure communication in offline scenarios by pre-computing authentication commitments. This reduces the cryptographic burden during message exchanges, enabling lightweight operations.

B. Initialization Phase: Credential Issuance and Pre-signature Generation

During periods of online connectivity, each vehicle undergoes the following process with the CSN:

1) Vehicle Authentication and Certification: Each vehicle V_i generates its Schnorr public-private key pair $(Priv_{V_i}, Pub_{V_i})$ locally. The vehicle transmits its identity and public key to the CSN, which authenticates the request and issues a signed certificate, $Cert_{V_i}$, binding V_i's identity to Pub_{V_i}, as shown in Equation 1.

$$Cert_{V_i} = Sign_{Priv_{CSN}}(V_i, Pub_{V_i}). \tag{1}$$

2) Pre-signature Tokens Generation and Distribution: The CSN periodically generates a fresh timestamp T_S to ensure temporal validity. The CSN then computes a pre-signature σ using its private key under the Schnorr signature scheme [23] to reduce computational costs for offline vehicles in Equation 2.

$$\sigma = Sign_{Priv_{CSN}}(T_S). \tag{2}$$

The tuple (T_S, σ) is securely distributed to vehicles for later offline use.

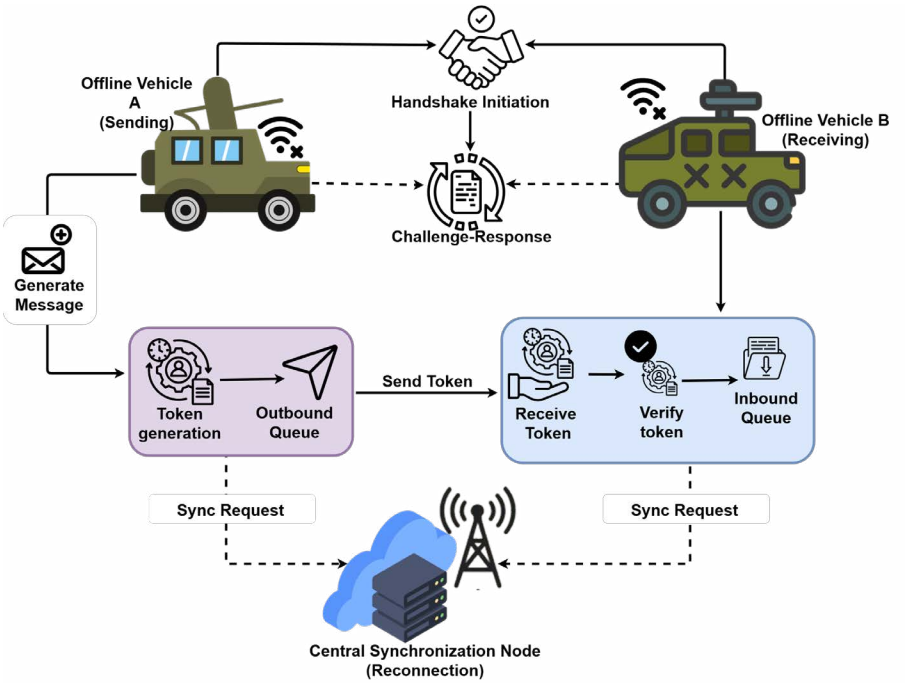

Fig. 2: Proposed Token-Based Handshake Protocol Architecture

C. Mutual Authentication: Challenge–Response Handshake

Before exchanging tokenized messages offline, the two vehicles, V_A and V_B, engage in a Schnorr-based mutual authentication handshake to confirm their liveliness and trust. Before transmitting the message, vehicles engage in mutual authentication to ensure that at the moment of communication, both parties are live and genuine. This handshake phase establishes session-level trust by allowing vehicles to prove their identities before exchanging messages. This prevents relay and replay attacks where a malicious entity resends an old token without being legitimate.

1) Challenge Generation and Verification: V_B generates a random nonce N_B and timestamp T_B, then signs their concatenation in Equation 3.

$$Challenge_{B\to A} = Sign_{Priv_{V_B}}(N_B||T_B). \tag{3}$$

This signed challenge is sent to V_A, which verifies V_B's challenge using V_B's public key from $Cert_{V_B}$ in Equation 4.

$$Verify(Pub_{V_B}, Challenge_{B\to A}, N_B||T_B). \tag{4}$$

2) Response Generation and Verification: Upon successful verification, V_A generates its own random nonce N_A and timestamp T_A, then constructs a response signing it with V_B's nonce in Equation 5.

$$Response_{A\to B} = Sign_{Priv_{V_A}}(N_B||N_A||T_A). \tag{5}$$

This response is sent back to V_B, which verifies V_A's response using V_A's public key from $Cert_{V_A}$ in Equation 6.

$$Verify(Pub_{V_A}, Response_{A\to B}, N_B||N_A||T_A). \tag{6}$$

Successful completion of this handshake establishes mutual trust between V_A and V_B for secure message delivery.

D. Offline Token Completion and Message Signing

1) Message Signing: After mutual authentication, when vehicles are offline and need to broadcast messages securely, V_A creates a message payload M and generates its Schnorr digital signature over the message in Equation 7.

$$VehicleSignature = Sign_{Priv_{V_A}}(M). \tag{7}$$

2) Pre-signature Token Completion: V_A completes the previously obtained pre-signature token using a random blinding scalar b to generate the $CompletedToken$ in Equation 8.

$$CompletedToken = \sigma + b \mod \text{curve}. \tag{8}$$

This prevents linking attacks and protects token uniqueness during offline operation. The complete tokenized message shown in Figure 3 is broadcast to nearby vehicles.

```
TokenizedMessage
{
      "sender": sender_id,
       "receiver": recipient_id,
       "Message": M,
       "VehicleSignature": vehicle_signature,
       "Certificate": Cert,
       "Timestamp": timestamp,
       "CompletedToken": σ + b mod curve
}
```

Fig. 3: Completed Offline Tokenized Message

Upon receiving the $TokenizedMessage$, a peer vehicle performs multi-step offline validation. The receiver verifies $Cert_{V_A}$ using the CSN's public key, which is already known to all vehicles. The receiver validates the message signature using the public key obtained from the validated certificate $Cert_{V_A}$ as $Verify(Pub_{V_A}, VehicleSignature, M)$.

3) Completed Token Verification: Finally, the receiver checks the integrity of the $CompletedToken$ against the original pre-signature σ and known parameters as $VerifyPreSignature(CompletedToken, \sigma, T_S)$. If all checks succeed, the message is accepted as authentic and trustworthy. Tokenized messages can be locally stored with a "pending synchronization" flag until full connectivity with the CSN is restored.

IV. Experimentation and Result Discussion

A. Simulation Overview

The simulation environment, developed using a Tkinter-based GUI, modeled vehicle dynamics and assessed offline V2V tokenized message exchanges under realistic conditions, as shown in Figure 4. It simulated dynamic positioning, variable communication ranges as supported by DSRC, and vehicle interactions with a single CSN node during credential issuance in online phases. The offline mode emulated CSN unreachability, simulating partial infrastructure availability, while step delays approximated the dynamics of real-time communication. Signal degradation is simulated with noise. Key performance metrics, outlined in Table I, were collected to assess the effectiveness of the framework.

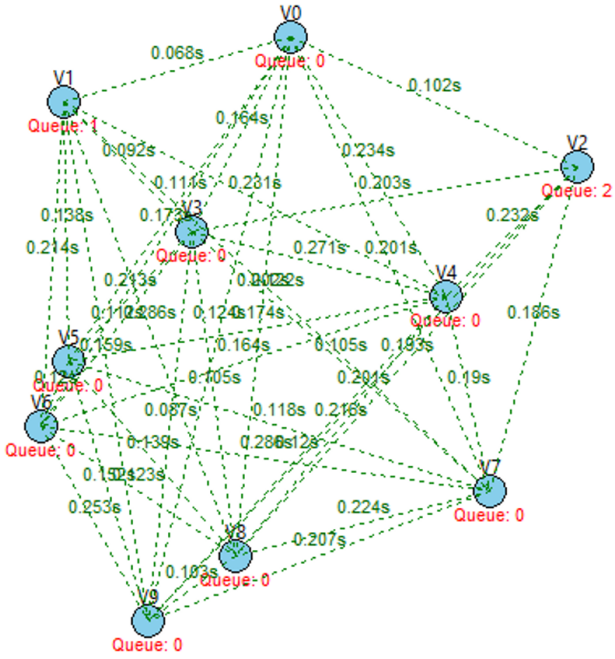

Fig. 4: Offline V2V Tokenized Message Exchange and Mobility Simulation Design

TABLE I: Simulation Parameters

Parameter	Value
Simulation Rounds	100
Step Delay	0.5 s
Area Width	2000 px
Number of Vehicles	10
Number of CSNs	1
Communication Range (m)	300 m - 1000 m
Intermittent Connectivity Status	50%
Offline Connectivity Status	0%
Signature Scheme	Schnorr
Noise	10%
Dropped Packets	if SNR <20dB

B. Transmission Latency

Latency in this study refers to the time for the mutual authentication handshake and the exchange of tokenized messages between vehicles. Figure 5 shows the maximum average latency of $0.0845s$ across all communication ranges 300–$900m$, in 0% and 50% CSN connectivity. This performance is due to the lightweight Schnorr-based handshake, which ensures rapid authentication once vehicles are within range. Slightly higher delays in the online case at lower ranges occur due to synchronization attempts with the CSN, while the offline scenario benefits from direct peer-to-peer interaction. It demonstrates the system's ability to deliver secure and low-latency communication suitable for tactical MANETs operating in contested or disconnected environments.

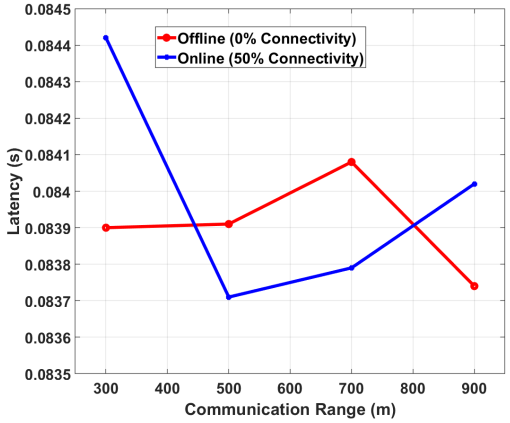

Fig. 5: Average Latency vs Communication Range

C. Offline Successful Transmissions

Successful transmissions track the number of tokenized messages exchanged between vehicles per simulation step at 0% connectivity, where CSN support is unavailable. Queued messages are those delayed by factors like range limitations or SNR drops and stored for future delivery. Figure 6 shows that as the communication range increases from $300m$ to $900m$, successful transmissions rise from 10 to 35 packets,

while queued messages decrease from 35 to 5. This inverse relationship indicates that increased range enables frequent exchanges and reduces the queue.

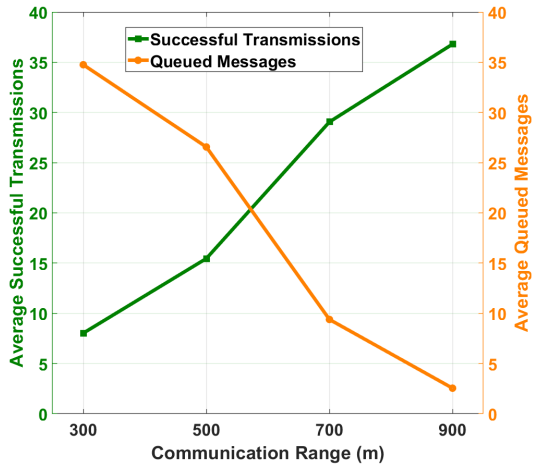

Fig. 6: Successful Offline Delivered Messages and Queued Messages vs Communication Range

D. Packet Delivery Ratio (PDR)

PDR evaluates the percentage of successfully delivered packets within the offline and intermittent CSN connectivity relative to total transmission attempts, as illustrated in Figure 7. PDR increases from 20% at $300m$ to 80% at $900m$, demonstrating the system's ability to improve delivery as communication range extends. This is a result of reduced interference at longer ranges, which enhances successful token exchanges.

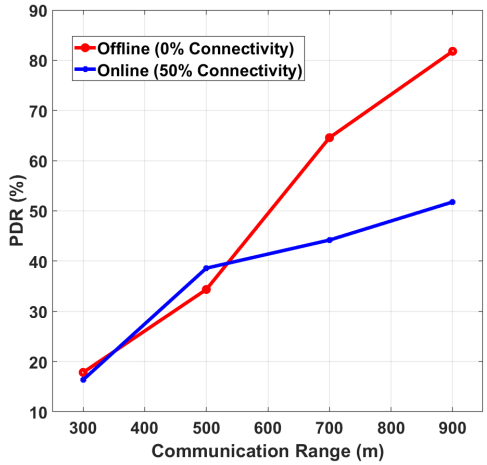

Fig. 7: Packet Delivery Ratio vs Communication Range

E. Signal-to-Noise Ratio (SNR) Drop

SNR drop quantifies packet transmission failures due to insufficient SNR, resulting from noise and distance. In the experiment, packets drop when SNR falls below 20 dB. Figure 8 illustrates the relationship between SNR-based drops and communication range.

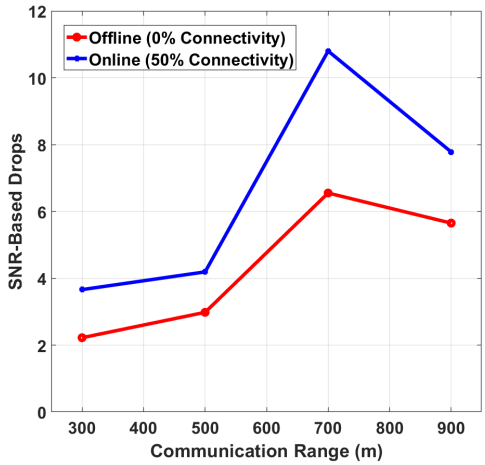

Fig. 8: SNR Drops with offline and partially online connectivity

F. Packet Loss

Packet loss refers to messages failing to reach their destination due to range limits, poor link quality (low SNR), or queuing overflow. Figure 9 illustrates the relationship between average packet loss and communication range. In tactical operations, high packet loss can disrupt the transmission of command, warning, or coordination data, making it a critical reliability factor. A larger communication range improves connectivity, reducing packet loss by allowing nodes to link more easily. Offline mode benefits more from range increases, as it relies solely on direct peer-to-peer links. Online mode experiences slightly higher packet loss due to unstable CSN dependence, which introduces delays or missed acknowledgments, particularly under 50% connectivity. The ability of the offline framework to drastically minimize packet loss, even with a modest communication range (700–900m), ensures that tactical information is reliably shared, even during temporary isolation from the CSN.

V. CONCLUSION

This study presents a lightweight cryptographic framework for secure communication in military operations lacking centralized infrastructure. The framework uses a self-contained token that integrates authentication, integrity metadata, and the message payload. The token supports message delivery and delayed synchronization without requiring live CSN validation. A central node pre-signs a timestamp with Schnorr signatures

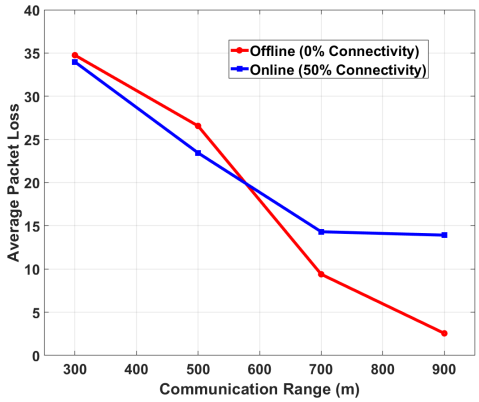

Fig. 9: Average Packet Loss vs Communication Range

to generate a reusable commitment across connected states. The results show high packet delivery rates, low latency, and resilient message delivery even with limited or no central connectivity. It reduces communication overhead and ensures reliable message exchange in disconnected tactical scenarios. Future work will focus on efficient message synchronization upon reconnection and real-world validation using network emulation and physical vehicular platforms.

ACKNOWLEDGMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government(MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%). This work was also supported by the IITP(Institute of Information and Communications Technology Planning and Evaluation)-ICAN (ICT Challenge and Advanced Network of HRD) grant funded by the Korea government(Ministry of Science and ICT) (IITP-2025-RS-2022-00156394, 25%).

REFERENCES

[1] N. Khanna and M. Sachdeva, "A Comprehensive Taxonomy of Schemes to Detect and Mitigate Blackhole Attack and its Variants in MANETs," *Computer Science Review*, vol. 32, pp. 24–44, 2019.

[2] Z. Patel, P. Khanpara, S. Valiveti, and G. Raval, "The Evolution of Ad Hoc Networks for Tactical Military Communications: Trends, Technologies, and Case Studies," in *Proceedings of Third International Conference on Sustainable Expert Systems* , S. Shakya, V. E. Balas, and W. Haoxiang, Eds. Springer Nature Singapore, 2023, pp. 331–346.

[3] S. Al Ajrawi and B. Tran, "Mobile Wireless Ad-Hoc Network Routing Protocols Comparison for Real-Time Military Application," *Spatial Information Research*, vol. 32, 09 2023.

[4] Y. Heo, M. Lee, and E. Jeong, "Frequency Diversity Using Random Time Delay in Amplify-and-Forward Relay," *International Journal of Electrical and Electronics Research*, vol. 11, pp. 513–517, 2023.

[5] A. Poirrier, L. Cailleux, and T. Clausen, "An Interoperable Zero Trust Federated Architecture for Tactical Systems," *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*, pp. 405–410, 2023.

[6] H. Feng and B. Cai, "A Provably Secure and Lightweight Two-Factor Authentication Protocol for Wireless Sensor Network," *Electronics*, vol. 13, no. 21, 2024.

[7] W. Qichen, "Research Progress on Wireless Sensor Network (WSN) Security Technology," in *Journal of Physics: Conference Series*, vol. 2256, no. 1. IOP Publishing, 2022, p. 012043.

[8] N. Patle and D. S. Singh, "Comprehensive Review of Routing Protocols in Delay-Tolerant Networks (DTNs)," in *International Journal of Research Publication and Reviews*, 2024.

[9] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Blockchain-Enabled Intrusion Detection System for Distributed Vehicular Networks," , pp. 463–464, 2024.

[10] E. Zadobrischi and Havriliuc, "Enhancing Scalability of C-V2X and DSRC Vehicular Communication Protocols with LoRa 2.4 GHz in the Scenario of Urban Traffic Systems," *Electronics*, vol. 13, no. 14, 2024.

[11] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Resource-Aware Adaptive Federated Learning for Enhanced DDoS Detection in Vehicular Ad Hoc Networks," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2024, pp. 1262–1267.

[12] P. H. L. Rettore, J. Loevenich, and R. R. F. Lopes, "TNT: A Tactical Network Test Platform to Evaluate Military Systems Over Ever-Changing Scenarios," *IEEE Access*, vol. 10, pp. 100 939–100 954, 2022.

[13] D. Almani, T. Muller, S. Furnell, X. Carpent, and T. Yoshizawa, "A Pre-signature Scheme for Trustworthy Offline V2V Communication," in *Trust Management XIV*, T. Muller, C. Fernandez-Gago, D. Ceolin, E. Gudes, and N. Gal-Oz, Eds. Cham: Springer Nature Switzerland, 2024, pp. 72–88.

[14] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Priority Messaging System for Emergency Vehicle Communication: A Blockchain Approach," , pp. 571–572, 2025.

[15] A. Jha, S. Kashani, M. Hossein, A. Kirchner, M. Zhang, R. A. Chou, S. W. Kim, H. M. Kwon, V. Marojevic, and T. Kim, "Enhancing NextG Wireless Security: A Lightweight Secret Sharing Scheme with Robust Integrity Check for Military Communications," in *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 2024, pp. 1–6.

[16] S. Ruffieux, C. Gisler, J.-F. Wagen, F. Buntschu, and G. Bovet, "TAKE — Tactical ad-hoc network emulation," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 2018, pp. 1–8.

[17] N. Kim, G. Sung, and D. Kim, "A Secure In-Vehicle Network of Military Unmanned Ground Vehicle based on SDN," *The Journal of Korean Institute of Information Technology*, vol. 19, pp. 99–107, 06 2021.

[18] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "A New Hybrid Online and Offline Multi-Factor Cross-Domain Authentication Method for IoT Applications in the Automotive Industry," *Energies*, vol. 14, no. 21, 2021.

[19] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," vol. 33, 12 2003, pp. 27–34.

[20] D. Almani, T. Muller, X. Carpent, T. Yoshizawa, and S. Furnell, "Enabling Vehicle-to-Vehicle Trust in Rural Areas: An Evaluation of a Pre-Signature Scheme for Infrastructure-Limited Environments," *Future Internet*, vol. 16, no. 3, p. 77, 2024.

[21] A. B. Rabiah, A. Alsoliman, Y. Shashwat, S. Richelson, and N. Abu-Ghazaleh, "Token-based Vehicular Security System (TVSS): Scalable, Secure, Low-latency Public Key Infrastructure for Connected Vehicles," 2024.

[22] A. Balador, A. Böhm, C. T. Calafate, and J.-C. Cano, "A Reliable Token-Based MAC protocol for V2V communication in Urban VANET," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1–6.

[23] C.-P. Schnorr, "Efficient Signature Generation By Smart Cards," *Journal of cryptology*, vol. 4, pp. 161–174, 1991.