MilitaryChain: Blockchain Routing Protocol in 6G Military Networks Using Cryptographic Addresses

Jonathan Mukisa Kalibbala [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 of Technology*, Gumi, South Korea
(kjonmukisa, loveahakonye, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—The emergence of 6G integrating Non-Terrestrial Networks (NTN) and Terrestrial Networks (TN) presents challenges in routing IoT-enabled military assets like drones and autonomous systems. Traditional protocols like the open shortest path first (OSPF) and border gateway protocol (BGP) are insufficient due to vulnerabilities and limited security, rendering them ineffective in the dynamic 6G networks. This study introduces MilitaryChain, a blockchain-driven routing framework using cryptographic key addresses for authentication and secure data packet routing. It leverages the blockchain's immutability and a custom proof of authority and association (PoA^2) consensus mechanism, thus enhancing security, scalability, and resilience. The experimentation demonstrates a 100% packet delivery ratio, 52.63 TPS throughput, and an average latency of 0.0248s, surpassing OSPF and BGP in security while maintaining comparable latency. This positions MilitaryChain as a robust solution for mission-critical military communications.**

***Index Terms*—Blockchain-Based Routing, PoA^2, 6G, Military Networks, Cryptographic Key Authentication**

I. Introduction

The 6G network innovation heralds a transformative shift in military communications, demanding innovative routing protocols to meet the unique operational needs in dynamic battlefield environments [1]. Unlike civilian networks, 6G military networks require seamless integration of terrestrial (TNs) and non-terrestrial (NTNs) nodes, such as satellites, unmanned aerial vehicles, and ground-based IoT devices, while contending with terahertz-driven data rates, massive device connectivity, and stringent real-time requirements [2]. Traditional routing protocols, such as open shortest path first (OSPF) and border gateway protocol (BGP), designed primarily for predictable and centralized civilian infrastructures, fall short in addressing these challenges. OSPF, a link-state protocol [3], optimizes paths using static metrics, while BGP prioritizes policy-driven stability for inter-domain routing [4]. However, their reliance on centralized architectures and lack of adaptability render them inadequate for military scenarios, where rapid topology changes, adversarial threats, and the need for decentralized trust are paramount [5], [6].

Military networks demand routing solutions that guarantee data integrity [6], [7], low-latency communication, and scalability across heterogeneous devices. The BGP and OSPF are insufficient due to a lack of adaptation to rapid topology shifts and secure data against cyber threats. Mahmoud et al. [2] showed the ability of 6G to provide ultra-reliable low-latency communications (URLLC) that facilitate real-time applications like autonomous drones and battlefield analysis. However, this study reveals a critical gap in securing the dataflows against exploitation vulnerabilities. Nguyen et al. [1] highlight privacy challenges in 6G, proposing a blockchain-based solution. Blockchain is gaining traction in military applications due to its tamper-proof ledger and ability to support decentralized devices. Hewa et al. [8] suggest that blockchain's immutability and trustless nature could enhance security and scalability in 6G. Jadev et al. [6] explored blockchain for secure data dissemination using their block-USB framework for UAVs in battlefield scenarios. The approach leverages blockchain to tamperproof the UAVs' high imagery and surveillance data. Also, Kostopoulos et al. [9] employed blockchain to secure military logistics, emphasizing smart contract transparency for resource tracking and immutable record-keeping across distributed units.

Despite these advancements and flaws in the existing routing frameworks and blockchain implementations, there is a need for a specialized solution that addresses the diverse demands of 6G military IoT networks. While traditional protocols like OSPF and BGP falter under the dynamic and adversarial conditions of military operations, and blockchain approaches such as those reviewed by Xiao et al. [5] and Jadav et al. [6] offer partial remedies through decentralization and security, they remain hamstrung by scalability bottlenecks, excessive latency, and poor interoperability with legacy systems, as critiqued by Kostopoulos et al. [9]. Existing blockchain applications demonstrate potential but fail to provide a comprehensive routing solution that balances efficiency and real-time performance.

To this end, this study proposes MilitaryChain, a routing solution tailored to meet the unique challenges of military 6G networks [4]. It leverages the decentralized properties of blockchain technology, enhancing connectivity and ensuring robust and secure communications in demanding scenarios. MilitaryChain substitutes conventional IP addresses with cryptographic key pairs as the addresses, boosting security in tactical warfare scenarios [10]. The specific contributions of this study are outlined as follows:

- **Development of MilitaryChain**: A tailored blockchain network for 6G military environments, integrating cryptographic key addresses with proof of authority with

association (PoA^2) consensus mechanism [11].

- **Design of a smart contract-driven routing system**: This system enforces permissioned access, optimal path selection, and key revocation, enhancing security and operational efficiency.
- **Comprehensive simulation analysis**: The results demonstrate MilitaryChain's efficiency, achieving a **100% packet delivery ratio**, **52.63 TPS** throughput, and **0.0248s latency**, surpassing OSPF and BGP in security while maintaining competitive performance.

II. Background of Study and Related Works

The broader transmission spectrum and the hyper-connectivity envisaged by 6G networks would enhance advanced military operations like autonomous systems and battlefield analytics. Recent studies highlight blockchain's capacity to enhance 6G networks by reinforcing data integrity, enabling decentralized management, and facilitating a secure spectrum [12], [13]. Gupta et al. [12] demonstrate blockchain's role in fostering trust in decentralized 6G architectures, reducing reliance on vulnerable central nodes [6]. In contrast, Wang et al. [14] highlight its efficacy in ensuring data integrity across distributed systems. However, most of these studies fall short of addressing military-specific demands.

Morales et al. [15] review blockchain's strengths, secure communications, immutable records, and IoT-AI integration but overlook tailored designs for 6G military networks. Conventional protocols like OSPF and BGP, critiqued for static optimization and policy-driven delays [3], [16], fail under battlefield pressures, as Mahmoud et al. [2] note, exposing gaps in dynamic, decentralized routing.

As pinpointed in the introduction section, OSPF and BGP are insufficient in the military 6G domain due to their dynamic, decentralized, unpredictable nature [3], [16]. OSPF's inflexible paths optimization and BGP's policy-laden routing falter under the dynamic multi-domain pressures of battlefield conditions, jeopardizing operations where unwavering dependability is critical. Emerging studies such as [6] suggest blockchain emergence as a key technology to enhance combat identification at scale, accelerating decision-making processes.

Nevertheless, hurdles persist with current blockchain networks, including scalability, latency, and integration with legacy systems. Recently, sharding and hybrid approaches have been explored. Despite being promising [17], they prove inadequate amidst the complexity of military fields. Sugumaran [18] implements a simplified consensus blockchain that boosts security in mobile ad hoc networks (MANETS). Similarly, [19] enhances the blockchain [4] with AI integration in vehicular networks [20]. However, challenges associated with blockchain deployment in 6G networks, particularly data packets, remain under study. Blockchain's latency and high energy usage render it less adaptable to the rapidly evolving military 6G environments.

The study presents MilitatryChain to address the above limitations with a blockchain routing protocol specifically for the dynamic 6G military IoT networks. The proposed MilitaryChain is a custom blockchain network with an enhanced consensus mechanism, PoA^2 [11]. Each of the Validators in the MilitaryChain is a trusted military base. Every validator is assigned a standby backup to ensure continuous data packet flow, even with node failures. MilitaryChain prioritizes robust performance under battlefield conditions and can handle the scale required for military applications [4].

III. System Methodology

This section introduces MilitaryChain's system methodology, starting with its core architecture and secure routing framework.

A. MilitaryChain Core Architecture

The backbone of MilitaryChain is its core architecture, which is shown in Figure 1. Its design setup combines advanced components to tackle the challenging demands of military 6G networks. At the center is the MilitaryChain core ledger, a private blockchain [17] that keeps an immutable record of all routing transactions and network states. Unlike public blockchain networks, MilitaryChain is a private permissioned network that permits only authorized military entities with clearance [11]. MilitaryChain is designed to keep in mind a continuation of all operations with no downtime or network loss. To this end, it employs a customized PoA^2 consensus mechanism and guarantees efficiency, security, and scalability in high-stakes and unpredictable military tactical operations [4].

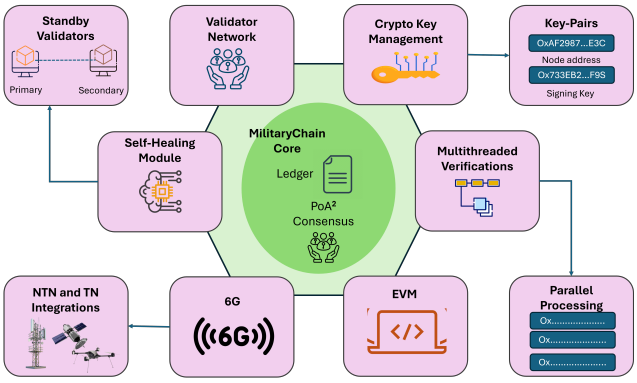

Fig. 1: MilitaryChain core Architecture

The PoA^2 consensus [11] mechanisms enable a set of verified trusted validators that maintain the blockchain ledger and authenticate routing requests. The validators are of two types, the active and standby validators, both authorized trusted military bases. These validators are pre-registered military entities with cryptographic key pairs to ensure that only authorized nodes can participate in the consensus. The standby validators to each active one ensure that the network stays online in case of compromise or failure of the other [11].

MilitaryChain replaces traditional IP addressing with cryptographic key pairs for node addressing and discovery.

Whichever node is in the network, whether a military base [4], drone, or submarine, it is assigned a public key for identification or an address, and the private key is one for signing off on the transactions. This ensures that all the communications are cryptographically [21] authenticated. An illustration of the key pair is shown with examples like ***0xAF2987...E3C*** for the node address and ***0x733EB2...F9S*** for the signing key ***(the signing key is kept private)***. The keys are generated using elliptic curve cryptography (ECC), specifically the secp256k1 curve, which is highly secure and efficient [6].

Due to the high velocity and volume of data in 6G networks, MilitaryChain uses a multithreaded verification process, which allows validators to process multiple routing requests in parallel. This reduces latency in dynamic battlefield scenarios. In addition, a self-healing module is integrated into MilitaryChain to mitigate network disruptions, for example, node failures and cyberattacks, by rerouting traffic through alternative paths as the compromised nodes are removed. This enables continuous operations even in contested environments.

The emerging military 6G networks positions to benefit from the integration of Militarychain, which brings together NTNs, such as the LEO satellites, and the TNs [5], [17], such as ground military bases and vehicles, enabling communication across diverse domains, including land, sea, air, and space. MilitaryChain routing soars on the 6G's terahertz frequencies and URLLC, allowing high-speed, low-latency communication between military assets like drones, submarines, and army vehicles. Furthermore, the system incorporates an Ethereum virtual machine to enable smart contract executions. The smart contracts contain rules, enforce the routing policies, and ensure secure communication between nodes. Additionally, parallel processing of transactions is supported to handle the massive scale of military IoT devices in the 6G network.

B. Battle Field Scenario

Figure 2 captures a battlefield scenario comprising various military entities such as the LEO satellites, armed UAVs, military bases, army vehicles, and several military IoT devices; all interconnected through the MilitaryChain network. Each entity is assigned a cryptographic key pair, ensuring only authorized nodes can join and communicate on the network. The smart contract deployed on the MilitaryChain

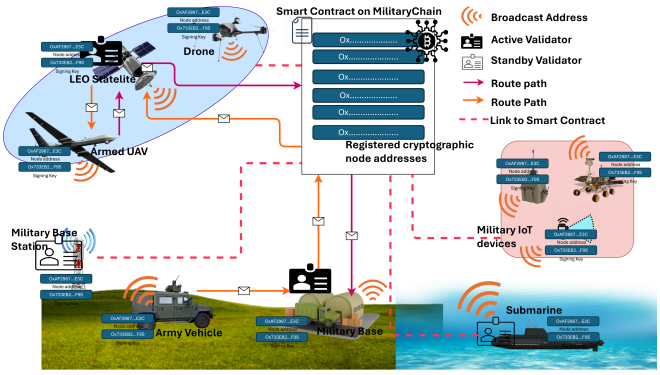

Fig. 2: Battlefield scenarios with Military IoT assets

provides a centralized role in securing the routing of the data packets amongst the military assets over the 6G network. The addresses in the smart contract are public keys for the registered military assets. This prevents unauthorized parties from accessing the network [15], [17]. Addresses of active validators are broadcast through the smart contract on the blockchain to all the nodes on the network. This enables efficient route discovery and path selection. The MilitatryChain records all the transactions on the ledger for audibility and after mission assessment. Also, it can revoke keys if a node is compromised or no longer authorized, assuring the network remains secure even in the face of internal threats.

The routing process begins when a node, such as an armed UAV, initiates a communication request. The request is signed with the node's private key and broadcast to the network. The validators on MilitaryChain verify the signature using the corresponding public key that acts as the node identity and checks the smart contract's registry to confirm the node's authorization. Once validated, the smart contract determines the optimal route path, and the data packet is transmitted securely through the selected path. This system ensures that all communications are tamper-proof, verifiable, and resistant to spoofing or interception [5].

C. Cryptographic Key Pair Generation

This is a critical aspect of MilitaryChain's security. It uses the ECC with the secp256k1 curve for its cryptographic key pair generation. The secp256k1 curve is defined over a finite field $\mathbb{F}_p$, where p is a large prime number given in Equation 1.

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1. \quad (1)$$

The curve equation $y^2 = x^3 + ax + b \mod p$, for secp256k1 with parameters a = 0, b = 7, simplifies the equation to $y^2 = x^3 + 7 \mod p$. The curve has a base point G, a generator point with a large prime order n, where n is the number of points on the curve, approximately 2^{256}. The private key d is a randomly generated integer in the range $[1, n-1]$. To ensure randomness and security, a cryptographically secure pseudo-random number generator (CSPRNG) was utilized to derive random numbers based on high entropy. The public key Q is then computed by performing scalar multiplication of the private key d with the base point G, illustrated as $Q = d \cdot G$. Here, the operation "$\cdot$" denotes ECC point multiplication, which involves a series of point additions and doublings on the curve. The generated public key Q is a point on the curve with coordinates (x, y).

For use as a node address, the public key is serialized as a 65-byte string $(04||x||y)$ or compressed to 33 bytes $(02/03||x)$, depending on the parity of y. To derive the node address, the public key is hashed using the Keccak-256 hash function with the address computed as Node Address = Keccak-256(Q) $[12 : 32]$. This produces a 20-byte address, which is prefixed with "0x" to form the final node address. The security of ECC relies on the difficulty of the elliptic curve discrete logarithm problem, which states that given Q and G, it is computationally infeasible to determine d. The

secp256k1 curve provides 128 bits of security, making it resistant to attacks even with quantum computers. Additionally, using a CSPRNG for private key generation ensures that the keys are unpredictable and resistant to brute-force attacks.

D. Simulation Setup

After running the MilitaryChain and deploying the smart contract, multiple simulations were executed to test the performance of the routing protocol for star, mesh, ring, and bus network scenarios. Table I shows the configuration settings for the four tested network scenarios, each with a different number of active validators and total nodes.

TABLE I: Scenarios with active validators and total nodes

Scenario	Active Validators	Total no. of Nodes
1	1	5
2	3	10
3	5	15
4	5	20

All experimental evaluations were conducted on a standard computing workstation equipped with NVIDIA GeForce RTX 3090 GPU, featuring 23.57 GB of VRAM and an Intel Core i7 processor with 4 physical cores, and the Smart contracts were written in Solidity version 0.8.21. The data packets were routed across the star, mesh, ring, and bus network topologies at 1000 data packets per time. The evaluation considered the packet delivery ratio (PDR), packet loss rate, end-end-end delay, jitter, throughput, average hop count, packet overhead ratio, and route acquisition latency metrics.

Algorithm 1 establishes a cryptographic framework for the smart contract for the routing protocol in MilitaryChain through hierarchical role-based access control. This protocol implements a comprehensive cryptographic key management lifecycle, including registration, validation, verification, and revocation processes enforced through smart contract mechanisms. This ensures tamper-proof key management by requiring multi-level authorization while maintaining an immutable audit trail of all operations on the blockchain. The routing process begins when a node (e.g., an armed UAV) initiates a communication request R_i, signed as S_{R_i} = Sign(R_i, d_i). After which the validators verify using V_{R_i} = Verify(S_{R_i}, A_i). If V_{R_i} = True, the smart contract checks authorization and selects the optimal path P^* as in Equation 2.

$$P^* = \arg\min_{P \in \mathcal{P}} \left(\sum_{j=1}^{k-1} w_{j,j+1} + \lambda \cdot L_v \right) \tag{2}$$

where $L_v = T_{\text{active}} + \alpha \cdot T_{\text{standby}}$ is the consensus latency, with $\alpha = 1$ on validator failure, else 0.

The smart contract enforces routing policies, broadcasting active validator addresses for route discovery. The total delivery time is in Equation 3.

$$T_{\text{total}} = L_v + \sum_{j=1}^{k-1} t_{j,j+1}. \tag{3}$$

Algorithm 1 MilitaryChain Key Management Protocol

Require: Contract deployer $addr_{deploy}$, roles NODE_ROLE, VALIDATOR_ROLE
Ensure: Secure public key management for military routing
$nodeCounter \leftarrow 0$
Grant $addr_{deploy}$ VALIDATOR_ROLE and ADMIN_ROLE
procedure REGISTERKEY(key_{public})
Require: NODE_ROLE, valid key_{public}
    $nodeId \leftarrow$ hash$(msg.sender, nodeCounter++, timestamp)$
    $nodeKeys[nodeId] \leftarrow \{key_{public}, false, false, timestamp\}$
    Emit KeyRegistered event
end procedure
procedure APPROVEKEY($nodeId$)
Require: VALIDATOR_ROLE, $nodeId$ exists and not approved/revoked
    $nodeKeys[nodeId].isApproved \leftarrow true$
    Emit KeyApproved event
end procedure
procedure REVOKEKEY($nodeId$, $reason$)
Require: VALIDATOR_ROLE, $nodeId$ approved and not revoked
    $nodeKeys[nodeId].isRevoked \leftarrow true$
    Emit KeyRevoked event
end procedure
procedure VERIFYKEY($nodeId$)
Require: NODE_ROLE, $nodeId$ exists
    $isValid \leftarrow nodeKeys[nodeId].isApproved \wedge \neg nodeKeys[nodeId].isRevoked$
    return $(nodeKeys[nodeId].publicKey, isValid)$
end procedure
procedure ADDNODE/VALIDATOR($addr_{new}$)
Require: Appropriate role, valid $addr_{new}$ without target role
    Grant role to $addr_{new}$
end procedure

IV. RESULTS AND PERFORMANCE DISCUSSION

This section presents the practical evaluation of MilitaryChain, building on the cryptographic foundation and architectural design outlined earlier. This includes the secure key generation process with elliptic curve cryptography and the smart contract-based routing system. It was noted that the packet delivery ratio stayed perfectly at 100% in each of the simulations with a packet loss rate of 0%, thus proving the significance of the proposed MilitaryChain routing protocol regarding packet delivery, which is critical for military communication where every message counts.

Table II presents the performance evaluation of an extensive simulation scenario with five (5) validators and 20 nodes across mesh, ring, star, and tree network topologies. It analyzes how MilitaryChain manages different network configurations. The system achieved a 100% delivery ratio and no packet loss, showing its reliability. The mesh topology had the shortest end-to-end delay at $257.78ms$, while the ring had the longest at $683.86ms$, illustrating structural influences. Mesh throughput was 3.88 packets per second, compared to 1.46 for the ring. These disparities arise from the mesh's numerous direct connections versus the ring's sequential path. Jitter ranged from $70.71ms$ for the star and $476.59ms$ for the ring. It indicates potential stability issues in constrained layouts. The average hop count of 1.85 (mesh) highlights its efficiency, emphasizing its ability to route through direct connections. Ring's higher hop count of 4.90 reflects its circular structure, where packets must pass through multiple

nodes, extending path length and affecting performance.

TABLE II: Performance evaluation of 5 active validators, 20 nodes across mesh, ring, star, and tree topologies

Topologies	Mesh	Ring	Star	Tree
Packet Delivery Ratio (%)	100.00	100.00	100.00	100.00
Packet Loss Rate (%)	0.00	0.00	0.00	0.00
End-to-End Delay (ms)	257.78	683.86	278.71	619.70
Jitter (ms)	120.97	476.59	70.71	278.39
Throughput (packets/sec)	3.88	1.46	3.59	1.61
Throughput (kbps)	31.03	11.70	28.70	12.91
Average Hop Count	1.85	4.90	2.00	4.42
Packet Overhead Ratio	1.85	4.90	2.00	4.42
Route Acquisition Latency (ms)	6225.42	6216.61	6284.42	6248.93

Table III provides a comparative analysis of the performance of the evaluated routing protocols. It highlights the efficiency of MilitaryChain relative to traditional routing protocols. The lower hop count (2.00) recorded by the Militarychain compared to OSPF $(2.1-2.5)$ and BGP $(3.0-3.5)$ suggests that the proposed approach facilitates more direct and efficient routing, potentially reducing congestion and improving data transfer rates. The throughput of 28.49 kbps for MilitaryChain indicates that it can sustain transmission rates comparable to OSPF while outperforming BGP, which is beneficial in high-demand environments. Furthermore, MilitaryChain's lower jitter of $70.20ms$ compared to OSPF $(80-95ms)$ and BGP $(100-120ms)$ suggests more consistent data delivery, which is crucial in scenarios such as encrypted communications and remote operational networks. The findings indicate that MilitaryChain presents a viable alternative to existing routing protocols, balancing performance, security, and efficiency in dynamic network scenarios.

TABLE III: Comparison of Performance Metrics Between MilitaryChain and Traditional Routing Protocols [22], [23]

Metric	MilitaryChain(Ours)	OSPF	BGP
End-To-end Delay (ms)	280.81	256-300	300-350
Jitter (ms)	70.20	80-95	100-120
Throughput (kbps)	28.49	25-30	22-28
Hop Count	2.00	2.1-2.5	3.0-3.5

The radar chart in Figure 3 demonstrates the normalized performance of MilitaryChain, OSPF, and BGP across several key network parameters. A notable observation is that MilitaryChain outperforms traditional routing protocols in security and scalability, reinforcing its potential for applications where data integrity and network resilience are critical. Contrarily, OSPF and BGP perform competitively in throughput and jitter, suggesting that while they remain effective in conventional networking scenarios, they require additional security enhancements to meet the robustness of MilitaryChain. The end-to-end delay performance of MilitaryChain aligns closely with OSPF, demonstrating that the blockchain-based protocol maintains competitive latency without compromising its security architecture. This makes it particularly relevant for mission-critical deployments where network stability and security are equally important.

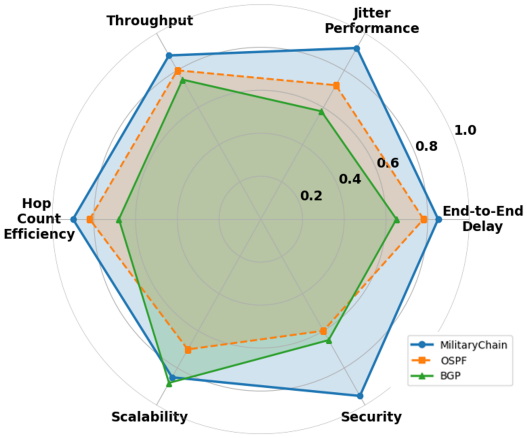

Fig. 3: Normalized performance analysis: MilitaryChain vs. OSPF vs. BGP

The graph analyzes the performance of the MilitaryChain with its enhanced PoA^2 consensus mechanism. It achieved a throughput of 52.63 transactions per second. It highlights the system's capacity to manage substantial transaction volume with negligible delays. MilitaryChain had a latency of $0.0248s$, demonstrating its robustness in securing data packets routed in military 6G networks. Also, a 100% success rate across all processed transactions ensures that every validation and record is executed flawlessly, guaranteeing absolute data integrity throughout the network's activities. The PoA^2 consensus mechanism adeptly prioritizes validators with superior performance while maintaining a robust standby system, ensuring smooth transitions during potential node failures.

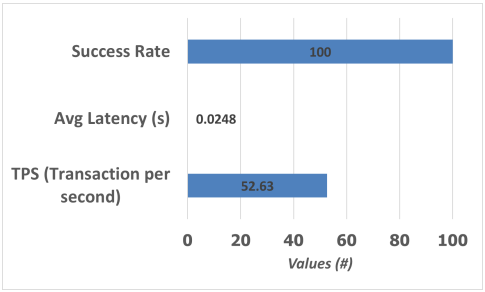

Fig. 4: Normalized Performance Analysis: MilitaryChain vs. Traditional Routing Protocols

V. Conclusion

This study develops MilitaryChain, a custom blockchain network with enhanced proof of authority and association for secure, fast data packet routing in military 6G environments. It proposes MilitaryChain routing, addressing the shortcomings of traditional protocols like OSPF and BGP. It delivers unparalleled security, scalability, and resilience for dynamic battlefield communications. Simulation results demonstrate its robustness, boasting 100% packet delivery ratio, 52.63 TPS throughput, and $0.0248s$ average latency while outperforming OSPF and BGP in security, competing with their latency. These findings validate MilitaryChain's

suitability for mission-critical applications, offering a reliable framework for decentralized command operations across terrestrial and non-terrestrial networks of military environments. Future research could explore hybrid topologies and enhanced energy efficiency to elevate further battlefield readiness and adopt AI validators.

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-2026-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2026-RS-2024-00438430, 34%).

REFERENCES

[1] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware Blockchain innovation for 6G: Challenges and Opportunities," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[2] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6G: A Comprehensive Survey on Technologies, Applications, Challenges, and Research Problems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4233, 2021.

[3] N. Miswar, H. Herman, and I. Riadi, "Comparing the Performance of OSPF and OSPF-MPLS Routing Protocol in Forwarding TCP and UDP Packet," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1237–1247, 2023.

[4] A. R. Lt Gen TSA Narayanan and S. C. Padhy, "Blockchain Technology for Military Application," *European Economic Letters (EEL)*, vol. 13, no. 5, pp. 463–469, November 2023.

[5] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[6] N. K. Jadav, T. Rathod, R. Gupta, S. Tanwar, N. Kumar, R. Iqbal, S. Atalla, H. Mohammad, and S. Al-Rubaye, "Blockchain-based Secure and Intelligent Data Dissemination Framework for UAVs in Battlefield Applications," *IEEE Communications Standards Magazine*, vol. 7, no. 3, pp. 16–23, 2023.

[7] G. Gkagkas, D. J. Vergados, A. Michalas, and M. Dossis, "The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network," *Sensors*, vol. 24, no. 8, p. 2455, 2024.

[8] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of bloheckchain in 6g: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[9] N. Kostopoulos, Y. C. Stamatiou, C. Halkiopoulos, and H. Antonopoulou, "Blockchain Applications in the Military Domain: A Systematic Review," *Technologies*, vol. 13, no. 1, p. 23, 2025.

[10] H. Saarnisaari, M. Höyhtyä, H. Rantanen, and J. Mäkelä, "Military Communications in the 6G Era: Finnish Perspective," *IEEE Military Communications Conference (MILCOM)*, pp. 135–140, 2024.

[11] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," *IEEE International Conference on Consumer Electronics (ICCE)*, 2025.

[12] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-Assisted Secure UAV Communication in 6G Environment: Architecture, Opportunities, and Challenges," *IET Communications*, vol. 15, pp. 1352–1367, 2021.

[13] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys &Amp; Tutorials*, vol. 21, pp. 1676–1717, 2019.

[14] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain-Enabled Wireless Communications: A New Paradigm Towards 6G," *National Science Review*, vol. 8, 2021.

[15] D. C. Morales, T. M. T. Nguyen, and G. Pujolle, "Towards a Blockgraph-Based Trustless Authentication Scheme for Future 6G Technology," *2023 2nd International Conference on 6G Networking (6GNet)*, 2023.

[16] Z. Cheng, N. A. Abbasi, J. Gomez-Ponce, J. C. Zhang, and A. F. Molisch, "Multipath Cluster Analysis for Device-to-Device Terahertz Outdoor Measurements," *IEEE Military Communications Conference (MILCOM)*, pp. 105–110, 2024.

[17] J. Asim, A. S. Khan, R. M. Saqib, J. Abdullah, Z. Ahmad, S. Honey, S. Afzal, M. S. Alqahtani, and M. Abbas, "Blockchain-Based Multi-factor Authentication for Future 6G Cellular Networks: A Systematic Review," *Applied Sciences*, vol. 12, p. 3551, 2022.

[18] V. Sugumaran and A. Rajaram, "Lightweight Blockchain-Assisted Intrusion Detection System in Energy Efficient MANETs," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 3, pp. 4261–4276, 2023.

[19] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 3614–3637, 2023.

[20] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in iot cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[21] M. TUNSTALL[1] and G. BARBU, "Cryptographic Algorithms," *Embedded Cryptography 1*, p. 311, 2025.

[22] A. Nasir and U. Tariq, "A Comparative Study of Routing Protocols Including RIP, OSPF, and BGP, journal = Lahore Garrison University Research Journal of Computer Science and Information Technology," vol. 2, pp. 47–56, 2018.

[23] Y. H. Jazyah, "Mathematical Model of the Relationship Between BGP Convergence Delay and Network Topologies," *Journal of Computer Science*, vol. 14, pp. 1–13, 2018.