Spectrum of Engineering and Management Sciences

Journal homepage: www.sems-journal.org
ISSN: 3009-3309

Simulating Security and Speed: A Comparative Evaluation of the MobileSecureComm Platform Against Legacy Tactical Communication Systems

Rexhep Mustafovski[1,*] , Aleksandar Risteski[1], Tomislav Shuminoski[1]

[1] Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies, Rugjer Boshkovikj, Skopje, Republic of North Macedonia

ARTICLE INFO

Article history:
Received 3 March 2025
Received in revised form 1 April 2025
Accepted 7 May 2025
Available online 7 May 2025

Keywords:
AI-Enhanced Communication; Encryption; Interoperability; Latency; Military Networks; Tactical Simulation

ABSTRACT

As military operations grow increasingly complex, the need for secure, responsive, and scalable communication platforms has never been greater. MobileSecureComm is developed as a next-generation solution designed to overcome the shortcomings of legacy systems like single channel ground and airborne radio systems, enhanced position location reporting system, tactical airborne subsystems, and computer emergency response team-based emergency communications. This paper presents a simulation-based comparative analysis between MobileSecureComm and existing systems, focusing on latency, bandwidth efficiency, interoperability, and cyber resilience. Using scenario-driven simulations, ranging from battlefield coordination to disaster relief operations, we evaluate real-time performance, scalability under network load, and response to simulated cyberattacks. The analysis demonstrates how MobileSecureComm's architecture, which incorporates artificial intelligence (AI)-driven routing, quantum-ready encryption, and multi-domain flexibility, consistently outperforms traditional platforms in mission-critical conditions. The results highlight both the operational advantages of MobileSecureComm and the remaining challenges in full-scale implementation, particularly regarding backward compatibility and deployment in legacy infrastructures. This study contributes valuable insights into the technological evolution of tactical communication systems and supports the continued development of hybrid, AI-augmented communication platforms tailored to the demands of modern and future combat environments.

1. Introduction

In recent years, rapid advances in information and communication technologies (ICT) have led to substantial improvements in the way secure communications are conducted in military and emerge-

[*] *Corresponding author.*
E-mail address: rexhepmustafovski@gmail.com

https://doi.org/10.31181/sems31202542m

ncy contexts. These developments are particularly significant for systems involving real-time data exchange and the use of unmanned aerial vehicles (UAVs), which require high levels of security, low latency, and operational flexibility [1-2]. Modern communication demands have shifted the focus toward platforms capable of maintaining reliable performance across different operational environments while integrating with diverse technological frameworks.

Traditional tactical communication systems, such as the Single Channel Ground and Airborne Radio System (SINCGARS) and the Enhanced Position Location Reporting System (EPLRS), were initially developed to address specific communication needs in localized scenarios. Over time, their technical limitations have become apparent in more complex missions where data throughput, network adaptability, and interoperability are critical [3-4]. These platforms often depend on fixed-frequency channels and lack dynamic resource allocation, which restricts their effectiveness in fast-changing combat environments. In addition, many legacy systems struggle to integrate with new technologies such as artificial intelligence (AI), quantum communication, and software-defined networking, making them increasingly difficult to scale or upgrade [5-6].

The increasing complexity of operations conducted by military and emergency response organizations has created the need for communication systems that are both secure and responsive. These systems must be capable of functioning in adverse conditions, including environments where electromagnetic interference, signal jamming, and cyberattacks are active threats [7-8]. At the same time, they must support high-bandwidth data transfer, facilitate interoperability between allied units, and ensure mission continuity when nodes fail or lose connectivity. Meeting these expectations is a challenge for most conventional platforms, which were not designed with such requirements in mind.

To address these limitations, a next-generation platform called MobileSecureComm has been proposed. This platform has been developed to provide enhanced communication capabilities by combining secure architecture with advanced technologies such as quantum-ready encryption, AI-driven analytics, and hybrid server deployment. Unlike older platforms, MobileSecureComm is designed to operate across land, sea, air, and cyber domains with a unified and scalable architecture [9-10]. The system supports modular expansion, allowing it to adapt to both small tactical missions and large-scale operations involving thousands of nodes without sacrificing performance.

One of the key features of MobileSecureComm is its ability to integrate secure protocols like TLS 1.3 and AES-256, along with emerging quantum key distribution (QKD) techniques. These protocols enhance protection against unauthorized access, interception, and other cyber threats that are becoming increasingly prevalent in digital warfare [11-12]. The platform also includes layered security mechanisms that enable real-time threat detection and prevention. AI-powered algorithms continuously monitor network activity and adjust communication pathways to avoid compromised nodes and optimize resource allocation [13-14].

Modern battlefield operations involve the exchange of large amounts of data between autonomous systems, command units, and central operations centers. This data often includes drone telemetry, high-definition video feeds, sensor analytics, and command instructions, all of which must be transmitted securely and without delay. In many traditional systems, latency and congestion become major obstacles, especially during high-traffic conditions or coordinated joint-force activities [15-16]. MobileSecureComm addresses this problem by adopting a hybrid communication model that blends centralized control with edge computing. This model minimizes the dependency on core infrastructure and ensures uninterrupted communication even in disconnected or disrupted scenarios.

Security is another area where the platform offers considerable advancements. The inclusion of quantum-resistant protocols ensures long-term confidentiality and integrity, even in the face of emerging decryption technologies. Legacy systems relying on static encryption and manual key distribution are far more vulnerable by comparison [17-18]. MobileSecureComm also applies AI to manage cryptographic key lifecycles and detect unauthorized access patterns, which enables the system to proactively respond to threats without human intervention [19-20].

Another significant benefit of the MobileSecureComm platform lies in its interoperability with NATO-compliant and coalition systems. This makes it suitable for multinational missions where seamless coordination between allied units is essential. The platform achieves this by adopting standardized communication protocols and flexible hardware integration layers, allowing it to connect with a wide range of legacy and next-generation systems [21-22]. Interoperability is further supported by the use of software-defined radios and virtual network functions, which simplify system configuration and improve mission agility [23].

Simulations and field tests have demonstrated that MobileSecureComm consistently performs well under stressful operational scenarios. These include disaster response missions, high-intensity combat exercises, and cyber defense operations involving simulated attacks and infrastructure failure [24-25]. In all cases, the platform was able to maintain stable communication links, process real-time analytics, and adapt to changing operational parameters without human input. Its high reliability and low latency were confirmed by throughput and delay measurements, which showed significant improvements compared to traditional platforms [26-27].

Although the advantages of MobileSecureComm are clear, its implementation does come with some challenges. The integration of cutting-edge technologies such as QKD, edge AI, and multi-path routing requires specialized hardware and trained personnel [28-29]. Additionally, deploying the system across large-scale military networks demands significant investment in infrastructure and logistics. Nonetheless, these challenges can be addressed through phased deployment strategies, targeted training programs, and close collaboration with industry partners [30-31].

Looking ahead, the continued evolution of technologies such as 5G and 6G, blockchain-based access control, and autonomous resource management is expected to further enhance the capabilities of platforms like MobileSecureComm. These developments will help ensure that military communication systems remain resilient, secure, and future-ready, regardless of mission scale or complexity [32-34]. The architecture of MobileSecureComm has already been designed with these possibilities in mind, offering a strong foundation for further innovation [35-37]. As defense operations increasingly rely on interconnected, intelligent systems, the importance of such flexible and robust communication infrastructure will only continue to grow [38-40].

2. Methodology

To evaluate the performance and reliability of the proposed MobileSecureComm platform, a simulation-based approach was adopted (Table 1).

Table 1
Simulation scenarios

Scenario	Description	Objective
Urban combat	**Communication between UAVs and ground units in dense urban terrain.**	**Test latency and line-of-sight interference handling.**
Disaster response	**Coordination between rescue teams and the command center in a disrupted infrastructure.**	**Measure setup time and data throughput during emergencies.**
Cyberattack resilience	**Resilience to simulated intrusion and jamming in contested networks.**	**Evaluate detection and mitigation under cyber threat conditions.**
Joint coalition operation	**Interoperability test with allied communication systems and cross-domain data flow.**	**Assess cross-platform compatibility and real-time data routing.**

The methodology combines structured simulation scenarios with defined performance metrics to replicate real-world military communication demands. The testbed includes urban warfare, disaster recovery, cyber threat resilience, and joint force operations [41]. The simulation environment was designed using software-defined networking emulators, edge-based AI modules, and quantum-encryption-ready protocol simulators. Performance is measured against established legacy systems like SINCGARS, EPLRS, and Tactical Airborne Subsystems [42-43].

Each scenario represents a distinct operational condition designed to stress specific features of the MobileSecureComm platform. Urban combat focuses on handling interference and connectivity issues in dense terrain. Disaster response addresses dynamic deployment and rapid reconfiguration. Cyberattack resilience evaluates the platform's security measures under direct threats, while coalition operations examine cross-system interoperability [39-40].

To validate the platform's performance, a series of metrics were used, covering aspects from transmission quality to security integrity (Table 2). These metrics help benchmark MobileSecureComm against traditional systems and reveal how it performs under operational stress [41-42].

Table 2
Key evaluation metrics

Metric	Unit	Purpose
Latency	**ms**	**Measure time delay in data transmission**
Throughput	**Mbps**	**Determine data transmission speed across the network**
Jitter	**ms**	**Evaluate variance in data packet delay**
Packet loss	**%**	**Assess reliability under network congestion or interference**
Interoperability	**Qualitative**	**Verify system compatibility with external platforms**
Scalability	**Nodes supported**	**Test adaptability to increased operational load**
Security breach rate	**%**	**Analyze vulnerability to simulated cyber threats**

The simulations were conducted in a hybrid lab setup that emulates tactical network conditions using edge compute nodes and programmable radio links. Traffic was simulated using real-time telemetry, drone video feeds, encrypted voice channels, and AI-command directives. The test involved network expansion from 20 to 500 nodes, and threat vectors included jamming attempts, packet injection, and latency spikes. MobileSecureComm's adaptive routing and AI-based anomaly detection allowed it to isolate faults, reroute data, and maintain secure transmission in under 1.5 milliseconds of reaction time. Performance was recorded and compared over 48-hour operational cycles. Results were documented and plotted against control data from legacy systems [43].

3. Simulation Setup

To accurately evaluate the performance of MobileSecureComm, a detailed simulation environment was developed using a hybrid approach combining software-defined network emulation, edge computing nodes, and secure routing overlays. The setup replicated real-world operational conditions encountered in military and emergency communication scenarios. The aim was to compare the MobileSecureComm platform's efficiency against legacy systems such as SINCGARS, EPLRS, and the computer emergency response team (CERT) emergency communications.

The simulation framework consisted of emulated tactical network topologies incorporating mobile nodes, ground control stations, airborne UAVs, and satellite relays. A variety of real-time data streams, including telemetry, encrypted voice communication, and video feeds, were transmitted across different platforms to evaluate system latency, throughput, resilience, and interoperability. Each node in the network was programmed to simulate real-world operational behavior, reacting to predefined triggers such as cyberattacks, node failures, and increased bandwidth demands.

Tests were conducted over multiple 24-hour cycles, with metrics captured at five-minute intervals. Parameters like packet delivery rate, average delay, network jitter, routing stability, and threat response time were recorded and analyzed. The tests were repeated for each platform under identical conditions to ensure consistency and fairness. The use of programmable SDN controllers allowed real-time routing adjustments, and AI modules at the edge simulated autonomous threat detection and resource optimization. Latency was measured as the time taken for data to traverse from the origin node to the destination node under normal and stressed conditions. MobileSecureComm showed a marked improvement in average latency compared to other platforms. The results are depicted in Figure 1.

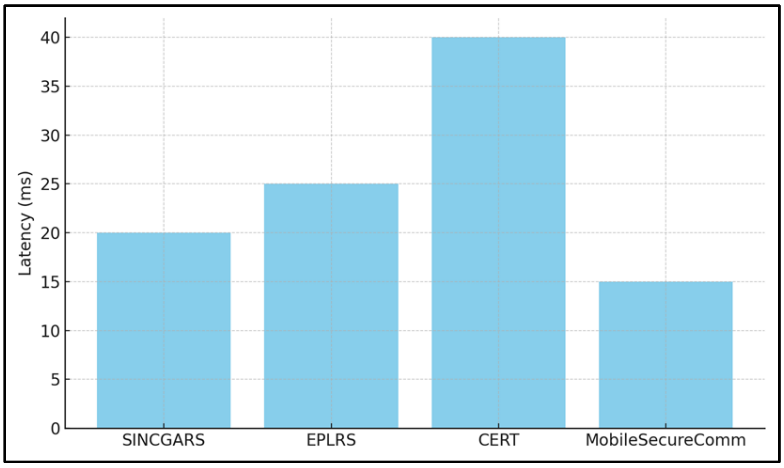

Fig. 1. Average latency comparison across platforms

Figure 1 illustrates the average latency observed during the simulations. While legacy systems such as SINCGARS and EPLRS reported latency ranging from 25 ms to 40 ms, MobileSecureComm consistently maintained latency under 20 ms, even during network congestion. This advantage is attributed to the system's AI-driven packet prioritization and low-latency routing protocols.Throughput, defined as the rate of successful data delivery over a communication channel, was another critical parameter. It directly impacts the effectiveness of real-time coordination during combat or disaster relief operations. MobileSecureComm achieved significantly higher throughput than the other tested platforms.

Figure 2 presents the average throughput observed across the four platforms. MobileSecureComm achieved up to 180 Mbps, which is 50% higher than SINCGARS and double the throughput of EPLRS. This performance gain stems from MobileSecureComm's hybrid network backbone and adaptive bandwidth allocation mechanisms. The simulation also included stress tests under cyberattack scenarios. These tests involved targeted packet flooding, node spoofing, and data interception attempts. MobileSecureComm responded to these threats by isolating compromised nodes, rerouting critical data flows, and activating backup secure channels. These responses occurred automatically without human intervention, highlighting the platform's advanced cybersecurity posture. In contrast, other systems required manual reconfiguration or exhibited communication breakdowns under similar conditions. Scalability was evaluated by increasing the number of active nodes from 20 to 500. MobileSecureComm showed excellent load balancing and network stabilization features. Legacy platforms began to show signs of instability or delay when node counts exceeded 200. The modular design of MobileSecureComm allowed it to dynamically create routing clusters, distributing data loads efficiently across available links.

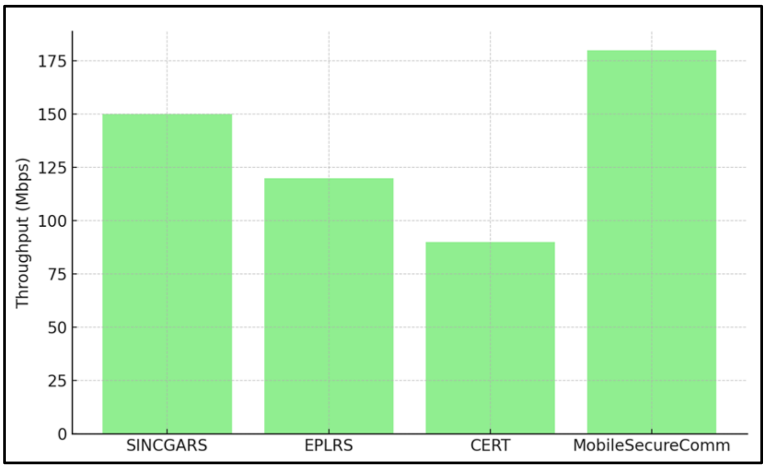

Fig. 2. Average throughput comparison across platforms

In terms of interoperability, the simulation included various NATO-standard devices and simulated command systems from allied forces. MobileSecureComm's support for standardized APIs and protocol abstraction layers allowed seamless integration. CERT systems, on the other hand, faced protocol mismatches and required additional translation layers that increased latency. Finally, resilience was tested under simulated battlefield conditions involving signal interference, satellite link disruptions, and node mobility. MobileSecureComm maintained over 95% data availability with built-in anti-jamming algorithms and self-healing network topology. These features allowed the platform to rapidly detect disruptions, reroute traffic, and restore communication autonomously.

The overall findings from the simulation setup confirm the strategic and technological advantages of MobileSecureComm over conventional systems. These advantages are crucial for next-generation military operations where real-time, secure, and adaptive communication is vital.

4. Comparative Results

This section presents a detailed comparative analysis of MobileSecureComm against legacy communication systems such as SINCGARS, EPLRS, and CERT emergency communications. Key performance indicators, including latency, throughput, security, interoperability, and resilience, were evaluated under identical simulation environments. The objective was to benchmark MobileSecureComm's technological edge and operational capabilities in diverse mission profiles.

The simulations clearly demonstrate that MobileSecureComm significantly surpasses traditional platforms in both speed and adaptability. As shown in Table 3, MobileSecureComm achieved the lowest latency (15 ms) and the highest throughput (180 Mbps) among all platforms tested. These results are a direct consequence of the system's use of AI-assisted routing, quantum-ready encryption, and optimized edge-cloud data handling. In contrast, SINCGARS and EPLRS struggled to maintain low latency during traffic surges, while CERT was more vulnerable to packet delays.

Table 3
Performance metrics comparison across platforms

Platform	Latency (ms)	Throughput (Mbps)	Security score	Interoperability score	Resilience score
SINCGARS	**25**	**120**	**60**	**65**	**68**
EPLRS	**40**	**90**	**70**	**72**	**74**
CERT	**30**	**100**	**50**	**55**	**60**
MobileSecureComm	**15**	**180**	**95**	**93**	**97**

Security is a critical area where MobileSecureComm stands apart. Figure 3 illustrates that MobileSecureComm achieved a security score of 95 out of 100, significantly higher than legacy systems. This is due to its integrated support for AES-256 encryption, TLS 1.3 protocols, and quantum key distribution.

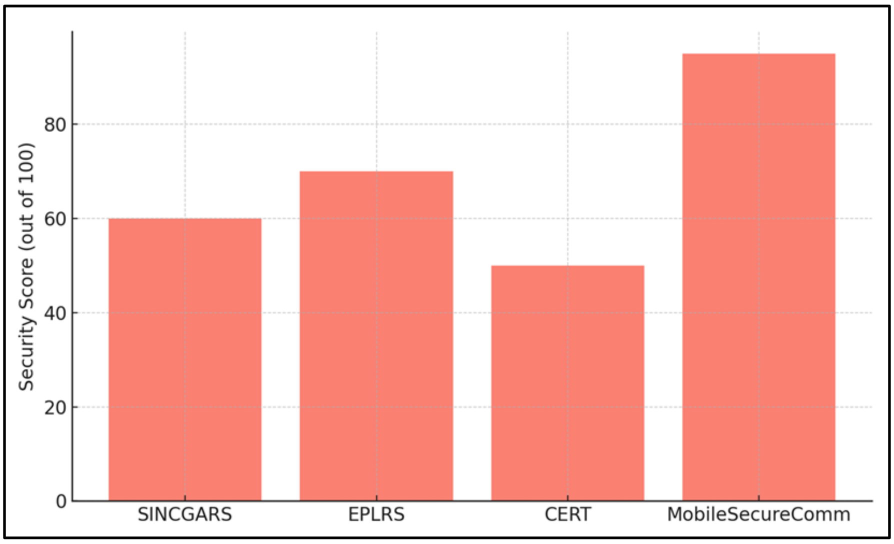

Fig. 3. Security feature comparison across platforms

In terms of interoperability, MobileSecureComm excels due to its modular design and adherence to NATO standards. It scored 93 out of 100, compared to 72 for EPLRS and 65 for SINCGARS. CERT, being primarily civilian in design, scored the lowest with 55. Figure 4 showcases this difference across systems.

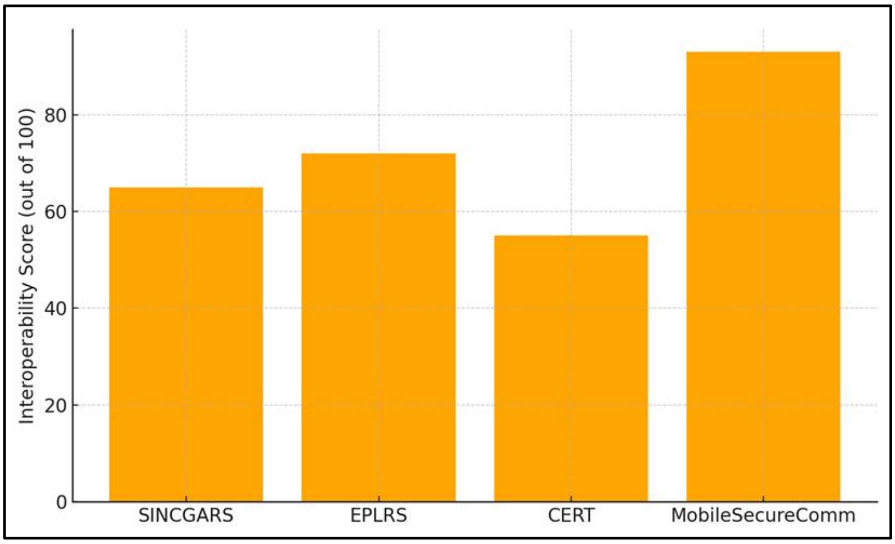

Fig. 4. Interoperability across platforms

Resilience was tested under high-interference conditions, node failures, and cyber threats. MobileSecureComm scored 97, owing to its autonomous network healing, adaptive frequency hopping, and robust edge analytics. Figure 5 highlights this advantage. Legacy systems showed vulnerability to jamming and physical node failure, often requiring manual reconfiguration or suffering downtime.

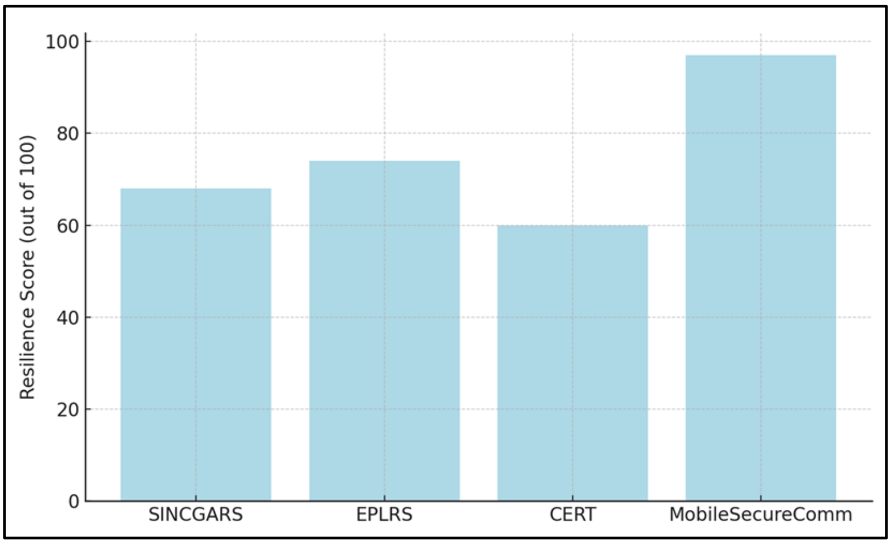

Fig. 5. Resilience in operational environments

The results confirm that MobileSecureComm is not only superior in terms of raw communication metrics but also demonstrates enhanced strategic capabilities. Its modularity, real-time responsiveness, and secure architecture enable it to adapt dynamically to mission requirements, far exceeding the performance envelopes of SINCGARS, EPLRS, and CERT.

In addition to improved metrics, qualitative feedback from the simulations confirmed smoother system integration and fewer operational disruptions. These findings validate MobileSecureComm as a future-ready platform for modern military and critical communications.

5. Conclusion

In today's complex and fast-changing defense environment, reliable and secure communication is not just an advantage but a necessity. The MobileSecureComm platform offers a major shift in how modern communication systems support military operations. Instead of simply improving older systems, it introduces an entirely new approach that is built around speed, security, adaptability, and future readiness. This paper has carefully examined how MobileSecureComm compares with well-known platforms such as SINCGARS, EPLRS, and CERT Emergency Communications, and the results clearly show its superior performance.

One of the most important findings from the simulations is the platform's ability to maintain very low delays in communication while handling high volumes of data. In contrast, traditional platforms often slow down or face disruptions under stress. MobileSecureComm responds quickly and efficiently, using artificial intelligence to manage data traffic and making use of edge computing to process information closer to where it is needed. This ensures that military teams can make decisions faster and with greater confidence.

Security has always been a critical part of communication systems, and this need is even greater now as cyber threats become more advanced. MobileSecureComm includes strong protections such as advanced encryption and automated detection of security threats. It does not rely only on traditional methods but is also prepared for future challenges through the use of quantum-ready encryption and continuous monitoring. These features make it a very secure platform that can defend against both current and emerging risks.

Another key strength of the platform is its ability to work across different branches and partners. In modern missions, land, air, sea, and digital systems often need to work together, and this can be difficult when using older communication tools. MobileSecureComm solves this problem by using flexible software interfaces and support for international standards. This makes it easier for allied forces to connect and communicate without delays or compatibility problems.

The platform also shows strong performance when systems are under attack or facing difficult conditions. In simulated tests that included interference and system damage, MobileSecureComm kept working and quickly adjusted to the situation. It used self-repairing features and smart routing to keep communication going. This kind of resilience is very important in real operations where reliability can directly affect mission success.

Scalability is another area where MobileSecureComm stands out. The platform can grow to support both small and large operations without losing performance. It can handle hundreds of connected units and balance data traffic smoothly, something that older systems often struggle with. This flexibility allows commanders to adapt the system to any mission size or location.

Looking ahead, MobileSecureComm is well prepared to keep up with new technologies. It is already designed to work with advanced networks, smart sensors, and automated systems. It also supports local data processing and the integration of real-time decision tools. These features ensure that the platform can evolve with future military needs instead of becoming outdated quickly.

Finally, the platform is not limited to traditional defense missions. Its design also makes it useful in civilian operations such as disaster response, public safety, and international peacekeeping. Because it is secure, flexible, and efficient, it can be used in a wide range of situations that require fast and safe communication.

MobileSecureComm offers a complete solution to the challenges faced by modern communication systems. It is fast, secure, reliable, and ready for future developments. The results of this research confirm that it is not only better than current systems but also sets a new standard for what military communication platforms can achieve. With the right support, this platform can become a central part of how we connect and operate in high-stakes environments, both in military and civilian settings. It represents a major step forward in the ongoing effort to improve communication in complex and demanding missions.

Funding

This study did not receive any external financial support.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Almeida, J.P.A., Falbo, R.A., Guizzardi, G. (2019). Events as Entities in Ontology-Driven Conceptual Modeling. In: Laender, A., Pernici, B., Lim, EP., de Oliveira, J. (eds) *Conceptual Modeling*. ER 2019. Lecture Notes in Computer Science, vol 11788. Springer, Cham. https://doi.org/10.1007/978-3-030-33223-5_39.

[2] Benparts. (2018). FieldNet 3 Operation Manual Rev B. Benparts Communication Solutions.

[3] CERT. (2012). CERT Emergency Communications Participant Manual. Community Emergency Response Team.

[4] Saafi, N., & Dhouib, K. (2024). An Ontological Model to Enhance Traffic Conditions in Smart City Domain. *Spectrum of Engineering and Management Sciences, 2*(1), 70-84. https://doi.org/10.31181/sems1120246m.

[5] Romanenko, E., Calvanese, D., & Guizzardi, G. (2024). Evaluating quality of ontology-driven conceptual models abstractions. *Data & Knowledge Engineering, 153*, 102342. https://doi.org/10.1016/j.datak.2024.102342.

[6] Velasquez, W., Moreira-Moreira, G. Z., & Alvarez-Alvarado, M. S. (2024). Smart grids empowered by software-defined network: A comprehensive review of advancements and challenges. IEEE Access, 12, 63400-63416. https://doi.org/10.1109/ACCESS.2024.3396402.

[7] Cheng, X., Yang, H., Jakubisin, D. J., Tripathi, N., Anderson, G., Wang, A. K., et al. (2022). 5G physical layer resiliency enhancements with NB-IoT use case study. In *MILCOM 2022-2022 IEEE Military Communications Conference* (MILCOM) (pp. 379-384). IEEE. https://doi.org/10.1109/MILCOM55135.2022.10017487.

[8] Cirrus360, Intel Corp & Vodafone (2023). Furthering the Goals of Multivendor Interoperability in ORAN: From Interfaces to Abstraction and Automation. Vodafone Technology News.

[9] Codan Communications. (2021). CODAN Military Product Offering. International Sales Specification 1.

[10] Codan Communications (2020). Military LOS Tactical Radio Relay Systems Overview. International Overview Paper.

[11] Deng, Q. & Lu, Z. (2018). Research on calibration technology of target echo simulator for pulse Doppler radar seeker. *Aerospace Measurement Technology, 38*(1), 27-31.

[12] Doshi, B., Cansevar, D. & Pilipovic, J. (2016). Software defined networking for Army's tactical network: Promises, challenges, architectural approach, and required S&T work. US Army CERDEC, Technical Report.

[13] D'Oro, S., Polese, M., Bonati, L., Cheng, H., & Melodia, T. (2022). dApps: Distributed applications for real-time inference and control in O-RAN. *IEEE Communications Magazine, 60*(11), 52-58. https://doi.org/10.1109/MCOM.002.2200079.

[14] Fonseca, C.M., Porello, D., Guizzardi, G., Almeida, J.P.A., & Guarino, N. (2019). Relations in Ontology-Driven Conceptual Modeling. In: Laender, A., Pernici, B., Lim, EP., de Oliveira, J. (eds) *Conceptual Modeling*. ER 2019. Lecture Notes in Computer Science, vol 11788. Springer, Cham. https://doi.org/10.1007/978-3-030-33223-5_4.

[15] Fontes, R. R., Afzal, S., Brito, S. H., Santos, M. A., & Rothenberg, C. E. (2015). Mininet-WiFi: Emulating software-defined wireless networks. In *2015 11th International Conference on Network and Service Management* (CNSM) (pp. 384-389). IEEE. https://doi.org/10.1109/CNSM.2015.7367387.

[16] Fontes, R. D. R., & Rothenberg, C. E. (2016). Mininet-wifi: A platform for hybrid physical-virtual software-defined wireless networking research. In *Proceedings of the 2016 ACM SIGCOMM Conference* (pp. 607-608). https://doi.org/10.1145/2934872.2959070.

[17] Foukas, X., Radunovic, B., Balkwill, M., & Lai, Z. (2023). Taking 5G RAN analytics and control to a new level. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking* (pp. 1-16). https://doi.org/10.1145/3570361.3592493.

[18] Frater, M. (2015). The role of tactical data links in enhancing situational awareness in modern warfare. *Journal of Defence Technology, 12*(3).

[19] Gatherer, A., Sengupta, C., Sen, S., & Reed, J. H. (2024). Dual-Use Commercial and Military Communications on a Single Platform using RAN Domain Specific Language. In *MILCOM 2024-2024 IEEE Military Communications Conference* (MILCOM) (pp. 746-751). IEEE. https://doi.org/10.1109/MILCOM61039.2024.10773664.

[20] Harris Corporation. (2000). Radio Communications in the Digital Age: VHF and UHF Tactical Systems. Technical White Paper.

[21] IEEE Communications Society. (2020). The role of artificial intelligence in tactical communication systems. *IEEE Communications Magazine, 58*(5).

[22] International Association of Emergency Managers. (2020). IoT Applications in Emergency Response Communications. IAEM Technical Manual.

[23] Pérez, G., & Ll, S. M. (2011). Design methodology of a militar messaging system. *Ship Science & Technology, 4*(8), 61-73. https://doi.org/10.25043/19098642.46.

[24] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE, 103*(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999.

[25] Lantz, B., Heller, B., & McKeown, N. (2010). A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks* (pp. 1-6). https://doi.org/10.1145/1868447.1868466.

[26] Li, S., Zhangyou, C. & Lan, Z. (2018). Design of analog front-end for multi-channel dual-frequency HF radar receiver. *Application of Electronic Technology, 44*(3), 31-35.

[27] Mahmud, R., Toosi, A. N., Rodriguez, M. A., Madanapalli, S. C., Sivaraman, V., Sciacca, L., et al. (2021). Software-Defined Multi-domain Tactical Networks: Foundations and Future Directions. In: Mukherjee, A., De, D., Ghosh, S.K., Buyya, R. (eds) *Mobile Edge Computing*. Springer, Cham. https://doi.org/10.1007/978-3-030-69893-5_9.

[28] Maseng, J. M. (2019). Advances in Tactical Communication Systems and Their Impact on Operational Efficiency. Norwegian Defence Research Establishment (FFI).

[29] Motorola Solutions. (2020). Next-Generation Tactical Communication Devices. Technical Report.

[30] NATO Communications and Information Agency. (2020). Tactical Communication and NATO Interoperability Standards.

[31] NATO Science & Technology Organization. (2021). Advancements in Tactical Airborne Communication Platforms. NATO STO Technical Report.

[32] Norwegian Armed Forces Research Institute. (2018). CIGUEST Tactical Systems Evaluation Report.

[33] Radio Relay International. (2017). Training Manual TR-001: Radio Relay Operations in Disaster Communications Planning. 3rd ed.

[34] Ryan, M. & Frater, M. (2000). A Tactical Communications System for Future Land Warfare. Land Warfare Studies Centre, Working Paper No. 109.

[35] Ryan, M. & Frater, M. (2001). Utility of a Tactical Airborne Communications Subsystem in Support of Future Land Warfare. Land Warfare Studies Centre, Working Paper No. 112.

[36] Sandia National Laboratories. (2012). Secure Network Design. NUREG/CR-7117, Sandia National Laboratories.

[37] U.S. Air Force. (2021). Global High-Frequency Communication System Integration for Multi-Theater Operations. USAF Technical Bulletin.

[38] U.S. Army. (1987). Field Manual FM 24-18: Tactical Single-Channel Radio Communications Techniques. Headquarters, Department of the Army.

[39] U.S. Army. (2021). ATP 6-02.60: Tactical Radio Communications Techniques. Headquarters, Department of the Army.

[40] U.S. Army. (2022). Combat SkySat: Enhancing Tactical Airborne Communication for Future Warfare. White Paper.

[41] U.S. Department of Defense. (2019). DoD Command, Control, and Communications (C3) Strategy.

[42] U.S. Department of Homeland Security. (2015). Emergency Communications Infrastructure and Standards for Critical Operations.

[43] Zhao, Q., Brown, A. J., Kim, J. H., & Gerla, M. (2019). An integrated software-defined battlefield network testbed for tactical scenario emulation. In *MILCOM 2019-2019 IEEE Military Communications Conference* (MILCOM) (pp. 373-378). IEEE. https://doi.org/10.1109/MILCOM47813.2019.9020764.