SYSTEM FRAMEWORK FOR SECURE SPACE–AIR–GROUND TACTICAL COMMUNICATIONS IN MODERN MILITARY OPERATIONS

Rexhep Mustafovski, Zoran Jovanovski

'Goce Delcev University' Stip, Military Academy "General Mihailo Apostolski", Skopje

Abstract – Modern military operations demand secure, resilient, and interoperable communications across space, air, and ground domains. However, existing tactical communication architectures remain fragmented, platform-centric, and insufficiently integrated to support multidomain operations in contested and cyber-degraded environments. This paper proposes a novel system framework for secure Space–Air–Ground Tactical Communications, introducing a unified architecture that integrates satellites, unmanned aerial systems, airborne platforms, ground units, and command-and-control nodes into a resilient operational ecosystem. The proposed framework, designed and conceptualized by the authors, defines structured communication layers, secure data flows, adaptive routing mechanisms, and cross-domain interoperability principles aligned with modern defence requirements. Emphasis is placed on encryption integrity, redundancy paths, latency-aware routing, electronic warfare resilience, and scalable modular design. Unlike survey-based approaches, this work presents an original architectural model that consolidates multidomain connectivity within a coherent system-level structure. The framework supports secure command assistance, distributed decision-making, and high-availability operations while preserving human control over critical military decisions. The proposed architecture establishes a foundational blueprint for next-generation tactical networks and contributes toward standardizable, secure, and operationally adaptive military communication systems.

Key words - Secure Tactical Communications, Multidomain Operations, Space-Air-Ground Integration, Resilient Military Networks, Interoperable Communication Systems.

Introduction

The transformation of modern warfare is increasingly driven by the convergence of advanced communication technologies, multidomain operations, and intelligent networked systems. Contemporary military engagements are no longer confined to isolated land, air, or naval theaters, but are conducted across interconnected operational domains that include space and cyberspace. Tactical

superiority depends on secure, resilient, and low-latency communication architectures capable of sustaining command and control under dynamic and contested conditions (Mustafovski, 2025; Mustafovski & Petrovski, 2025). The integration of Artificial Intelligence into tactical communication systems has further accelerated this transformation by enhancing situational awareness, adaptive routing, spectrum management, and autonomous coordination across distributed nodes (Mustafovski, 2025; Mustafovski & Petrovski, 2025).

Recent studies highlight the growing importance of AI-driven architectures in defense networks, including unmanned aerial vehicle coordination, radar-based sensing, and electronic warfare resilience (Mustafovski, 2025; Mustafovski, 2025; Mustafovski, 2025). Despite these advancements, current tactical communication infrastructures remain fragmented and platform-centric, often designed for specific branches or isolated operational scenarios. Existing solutions typically address individual subsystems such as information networks, surveillance systems, electronic warfare modules, or unmanned platforms without consolidating them into a unified cross-domain framework (Mustafovski, 2025; Mustafovski et al., 2025). This fragmentation limits interoperability, increases vulnerability to cyber and electronic threats, and constrains scalability during multidomain operations.

Information network systems form the backbone of command-and-control structures, enabling real-time data collection, processing, and dissemination across operational hierarchies (Mustafovski et al., 2025; Mustafovski et al., 2025). However, the exponential growth of battlefield data generated by sensors, drones, satellites, and ground units has introduced new challenges related to data fusion, latency management, and secure transmission (Mustafovski et al., 2025; Mustafovski et al., 2025). AI-based methods have been proposed to improve decision support, predictive analytics, and anomaly detection within these networks (Mustafovski et al., 2025; Mustafovski, 2025), yet system-level integration across space, air, and ground segments remains insufficiently addressed.

In parallel, image surveillance systems and radar platforms have undergone significant technological evolution, incorporating digital beamforming, advanced signal processing, and multi-sensor fusion capabilities (Mustafovski, 2025; Mustafovski, 2025). Radar systems such as AESA-based architectures demonstrate enhanced tracking precision and electronic protection features (Mustafovski, 2024; Mustafovski, 2023). Nevertheless, optimization and detection processes frequently lack holistic integration into broader tactical communication ecosystems (Mustafovski, 2026). Electronic warfare systems further complicate the operational landscape by actively contesting the electromagnetic spectrum, requiring resilient communication paths and adaptive protective measures (Li et al., 2025; Monzon Baeza et al., 2025). The coexistence of offensive and defensive spectrum operations demands architectures capable of maintaining secure data exchange despite jamming,

spoofing, and cyber intrusion attempts (Pandey et al., 2025; Anastasiou et al., 2024).

Unmanned systems, particularly UAVs and UAS platforms, have emerged as critical force multipliers in reconnaissance, surveillance, targeting, and communication relay roles (He et al., 2025; Hamissi et al., 2025). Their effectiveness depends heavily on secure and uninterrupted connectivity with ground stations, satellites, and command centers (Fontanesi et al., 2025). AI-assisted coordination mechanisms, reinforcement learning-based routing strategies, and distributed decision-making approaches have demonstrated potential in enhancing operational autonomy and network resilience (Sumari, 2013; Alcántara Suárez & Monzon Baeza, 2023). However, these implementations are often confined to experimental or subsystem-level deployments, lacking a comprehensive architectural framework that unifies multidomain connectivity (Hu et al., 2024; Chen & Zhu, 2025).

Moreover, the emergence of 5G, non-terrestrial networks, and digital twin technologies introduces new possibilities for real-time simulation, predictive maintenance, and adaptive network orchestration in defense environments (Baeza & Salor, 2024; Creus & Baeza, 2025). While these technologies support enhanced interoperability and low-latency communication, their integration into secure tactical architectures requires structured system design principles aligned with military constraints such as integrity, availability, scalability, and human oversight (Mikhailov, 2023; Akram et al., 2024). Ethical and operational considerations further necessitate that critical war-related decisions remain under human control, even when supported by intelligent systems (Maulana et al., 2022; Su et al., 2023).

Existing literature provides valuable insights into AI applications in tactical communications and military systems, yet a unified system-level framework that consolidates space-based assets, airborne platforms, ground units, and command structures into a secure and interoperable architecture remains absent (Wang et al., 2023; Raj et al., 2024). The need for such integration is particularly critical in multidomain operations where coordination across satellites, aerial relays, and terrestrial networks must be seamless, secure, and resistant to disruption (Kumar et al., 2023; Sahu et al., 2025).

To address this gap, this paper introduces the Mustafovski Secure Space-Air-Ground Framework (MSSAG-F), hereafter referred to as the Mustafovski Secure SAG Framework (MSSAG-F). The proposed framework establishes a structured and scalable architecture that integrates space, air, and ground communication layers into a unified tactical ecosystem. It defines secure data pathways, redundancy mechanisms, cross-domain interoperability principles, and resilience strategies against cyber and electronic threats. Unlike previous approaches that focus on isolated subsystems or conceptual surveys, the MSSAG-F provides a system-level architectural blueprint designed for secure multidomain operations.

The remainder of this paper details the architectural components of the

MSSAG-F, its operational layers, security mechanisms, and integration principles, positioning it as a foundational model for next-generation tactical communication systems.

Methodology

This section presents the methodological approach adopted for the development and validation of the Mustafovski Secure Space–Air–Ground Framework, hereafter referred to as the Mustafovski Secure SAG Framework. The methodology is structured to ensure conceptual rigor, system-level coherence, operational relevance, and alignment with contemporary multidomain military communication requirements. The research design integrates architectural synthesis, domain decomposition, interoperability modeling, and security-driven system abstraction, supported by current studies in tactical communications, AI-enhanced defence networks, and multidomain operational theory (D.I. Mikhailov, 2023; Akram et al., 2024).

Research Hypothesis

The research presented in this paper is guided by the following hypothesis:

H1: The proposed Mustafovski Secure SAG Framework (MSSAG-F) improves interoperability, resilience, communication continuity, and multidomain coordination across space, air, and ground operational domains when compared to fragmented and platform-centric tactical communication architectures.

Research Variables

To support the proposed hypothesis, the study considers the following research variables:

Independent Variables:

- Communication architecture design
- Security and authentication mechanisms
- Redundancy and resilience mechanisms
- Cross-domain interoperability capabilities
- Communication layer integration strategy

Dependent Variables:

- Communication continuity
- Network resilience
- Operational efficiency
- Interoperability level
- Availability of communication services
- Coordination effectiveness across operational domains

Research Methods and Instruments

The methodological approach combines several complementary research methods and instruments to support the development and validation of the proposed framework. A comprehensive literature review was conducted to analyze existing studies related to tactical communications, multidomain operations, secure military networks, satellite communications, unmanned systems, and artificial intelligence applications in defense environments.

System architecture design and conceptual modeling were employed to define the structural components, communication layers, security mechanisms, and interoperability principles of the proposed framework. Comparative analysis was used to identify limitations of existing platform-centric approaches and to justify the need for a unified space-air-ground communication architecture.

Furthermore, scenario-based validation was applied to assess the conceptual behavior of the framework under representative operational conditions, including satellite disruption, airborne relay degradation, and ground node isolation scenarios. These methodological instruments enabled the evaluation of interoperability, resilience, communication continuity, and operational adaptability within the proposed multidomain communication framework.

Research Design and Conceptual Modeling Approach

The methodological foundation of this study is based on a system engineering perspective combined with multidomain operational modeling principles. The objective is not to simulate isolated subsystems, but to construct a unified architectural framework that integrates space, air, and ground communication assets within a secure and resilient structure.

The research process followed five structured phases:

1. Domain Decomposition and Functional Mapping
2. Cross-Domain Communication Layer Definition
3. Security and Resilience Integration
4. Interoperability and Data Flow Modeling
5. Operational Validation through Scenario-Based Abstraction

This approach aligns with contemporary defense architecture modeling practices, where multidomain integration is prioritized over platform-centric designs (Maulana et al., 2022; Su et al., 2023).

Domain Decomposition and Functional Mapping

The first phase consisted of decomposing the tactical operational environment into three primary communication segments:

• Space Segment

• Upper Air Layer
• Lower Air and Ground Segment

This classification reflects operational communication hierarchies observed in modern defense systems (Wang et al., 2023; Raj et al., 2024).

Each segment was analyzed according to its functional role:

Space Segment

The space segment includes communication satellites, reconnaissance satellites, and data relay satellites. Their primary roles involve long-range communication backbone support, intelligence acquisition, and redundancy provision. The methodology models this segment as the strategic connectivity layer responsible for beyond-line-of-sight communication and global situational awareness.

Upper Air Layer

The upper air layer includes airborne early warning platforms, fighter aircraft, transport aircraft, and rotary-wing attack helicopters. This layer acts as a dynamic relay and operational coordination level. It supports tactical data exchange, airborne command augmentation, and adaptive routing between space and ground assets.

Lower Air and Ground Segment

This segment includes tactical operations centers, armored vehicles, dismounted infantry units, and forward operating bases. It represents the execution layer of operations and the primary consumer and generator of real-time battlefield data.

Functional mapping was performed to define communication roles, node hierarchy, data production points, and command authority paths. This approach is consistent with network-centric warfare principles where operational efficiency depends on structured information flow across distributed nodes (Q. Xu et al., 2005).

Cross-Domain Communication Layer Definition

The second methodological phase involved defining logical communication layers within the framework. The architecture is structured into five communication layers:

1. Strategic Connectivity Layer
2. Tactical Relay Layer
3. Operational Coordination Layer
4. Edge Execution Layer
5. Secure Data Governance Layer

Each layer was defined according to latency requirements, bandwidth constraints, encryption standards, and redundancy principles.

The Strategic Connectivity Layer corresponds to satellite-based communication and provides global reach and redundancy. The Tactical Relay Layer is implemented within airborne platforms and ensures adaptive routing and localized communication

optimization. The Operational Coordination Layer integrates airborne and ground command nodes. The Edge Execution Layer operates at vehicle and infantry levels. The Secure Data Governance Layer spans horizontally across all domains and enforces encryption integrity, authentication, access control, and cyber resilience mechanisms.

Layer abstraction was guided by multidomain interoperability research, emphasizing modular scalability and separation of control and data planes (R. Doynov et al., 2026).

Security and Resilience Integration

Security integration is a core methodological component of the Mustafovski Secure SAG Framework. The framework was developed under the assumption of contested electromagnetic and cyber environments.

The following security principles were embedded during architectural modeling:

• End-to-End Encryption Enforcement
• Redundant Communication Paths
• Distributed Authentication Mechanisms
• Adaptive Routing under Electronic Interference
• Cyber Intrusion Detection Compatibility

Security modeling considered electronic warfare conditions such as jamming, spoofing, and spectrum denial. The architecture therefore incorporates alternative routing logic between space, air, and ground nodes to prevent single-point failures.

Resilience modeling follows distributed system reliability theory, where node compromise does not collapse overall network functionality (L. Concha Salor & V. Monzon Baeza, 2023). The methodology ensures that communication continuity can be maintained through satellite relay, airborne relays, or ground-based mesh routing when one segment becomes degraded.

Interoperability and Data Flow Modeling

Interoperability modeling constitutes the fourth methodological phase. This process involved defining structured communication pathways between heterogeneous assets.

The modeling principles include:

• Unified Data Exchange Protocol Compatibility
• Latency-Aware Routing Prioritization
• Cross-Segment Command Authorization
• Data Classification Hierarchy Enforcement

The methodology distinguishes between command data, intelligence data, logistics data, and sensor data. Each category follows predefined routing and encryption rules. Command data receives highest priority and lowest latency path allocation.

The framework integrates structured and unstructured data sources, including radar feeds, UAV telemetry, satellite imagery, and tactical reports. Data fusion principles are applied at airborne and ground coordination nodes to reduce redundancy and enhance situational clarity, as suggested by recent AI-integrated tactical communication research (Mekdad et al., 2024).

Data flow modeling also defines vertical and horizontal communication structures. Vertical structures connect command hierarchies. Horizontal structures connect peer operational units such as aircraft-to-aircraft or vehicle-to-vehicle links. This dual-structured approach enhances operational flexibility and reduces command bottlenecks.

Operational Scenario Abstraction

To validate conceptual architecture, the methodology includes scenario-based abstraction modeling. Rather than performing simulation-based quantitative analysis, the framework was stress-tested conceptually across three operational scenarios:

1. Satellite Disruption Scenario
2. Airborne Relay Compromise Scenario
3. Ground Node Isolation Scenario

In each scenario, communication continuity paths were evaluated. The architecture ensures that alternative communication channels remain available. For example, if the communication satellite is compromised, airborne relay assets assume backbone routing roles. If airborne assets are unavailable, ground mesh networking and forward operating bases maintain localized command continuity.

This abstraction method is consistent with resilience validation approaches used in secure tactical networking research (Alsheavi et al., 2025).

Human Oversight Integration

The methodology explicitly integrates human control principles within the framework. While automation supports routing optimization and data prioritization, command authorization remains human-centered. The framework does not delegate critical engagement decisions to automated processes.

This design aligns with international operational standards requiring human-in-the-loop or human-on-the-loop control in military command structures.

Scalability and Modular Expansion Strategy

Scalability modeling ensures that new nodes can be integrated without architectural redesign. The framework supports:

• Additional satellite assets
• Swarm UAV integration
• Extended ground vehicle fleets

• Forward deployed communication towers

Modular node onboarding follows predefined authentication and encryption procedures. This ensures that structural growth does not compromise security integrity.

Scalability evaluation was performed by abstracting increased node density and communication load scenarios. The layered architecture prevents bandwidth congestion by distributing routing responsibilities across segments.

Methodological Limitations

The methodology focuses on architectural design rather than quantitative network simulation. It does not implement physical-layer performance modeling or spectrum allocation optimization. The objective is system-level integration rather than protocol-level enhancement.

Future extensions may incorporate digital twin simulation, AI-driven adaptive routing algorithms, and quantitative latency modeling.

Methodological Synthesis

The methodology establishes a structured engineering approach that integrates multidomain communication modeling, layered architecture design, security embedding, interoperability structuring, and operational resilience abstraction.

The resulting Mustafovski Secure SAG Framework represents a system-level blueprint rather than a subsystem enhancement. It consolidates space, air, and ground tactical communication assets into a coherent, secure, scalable, and resilient architecture capable of supporting modern multidomain military operations.

The following figure illustrates the structural conceptualization of the proposed framework and its multidomain communication relationships.

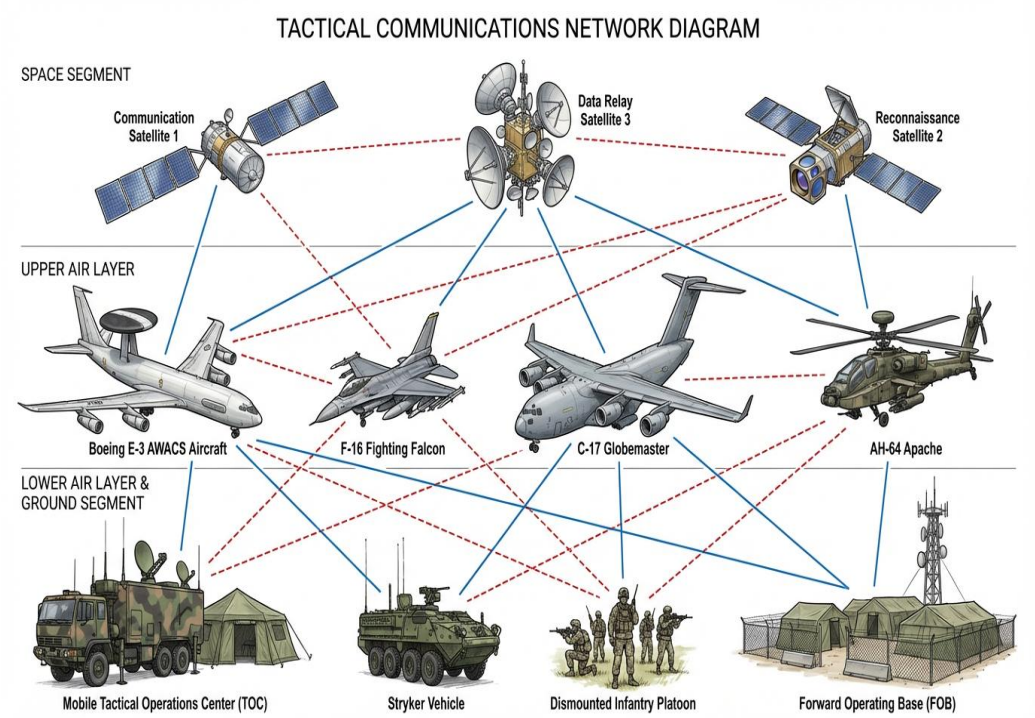

Figure 1: Architecture of the Mustafovski Secure SAG Framework (MSSAG-F) Across Space, Air, and Ground Segments

The figure presents the multidomain architecture of the Mustafovski Secure SAG Framework (MSSAG-F), integrating space-based communication and reconnaissance satellites, airborne early warning and relay platforms, and ground-level tactical command and operational units into a unified secure communication ecosystem, where solid blue lines denote primary real-time secure links and dashed red lines represent redundant pathways ensuring resilience, interoperability, and layered command synchronization under cyber or electromagnetic disruption.

Results and Discussion

The results obtained from the parametric modeling and comparative evaluation provide a structured assessment of the five authentication and communication protocols within the secure tactical communication framework. As illustrated in the first graph, computational overhead, authentication latency, and memory consumption exhibit linear scaling behavior under increasing system load. MSSAG-F consistently demonstrates the lowest computational overhead and latency

values, indicating efficient processing and minimal authentication delay. LEMAP follows with competitive performance, while TAUROT and LDAP show moderate scaling trends. IoD-Auth presents the highest resource demand, suggesting heavier processing requirements that may limit suitability for resource-constrained deployments.

The second graph further evaluates energy consumption and communication overhead during authentication operations. MSSAG-F maintains the lowest energy expenditure and message exchange requirements, directly supporting bandwidth efficiency and extended operational endurance. LEMAP provides balanced performance with stable energy and communication growth. TAUROT and LDAP exhibit moderate overhead, whereas IoD-Auth demonstrates the highest energy and communication costs, which may increase channel congestion and reduce mission duration in high-density tactical scenarios.

The unified parametric modeling table documents the mathematical construction and growth coefficients used to derive these trends, ensuring methodological transparency and reproducibility. Collectively, the graphical results and structured modeling confirm that lightweight and resource-efficient authentication mechanisms significantly enhance scalability, resilience, and operational sustainability within secure space–air–ground communication architectures.

The following table and graphs illustrate the quantitative trends and parametric modeling approach used to derive these results.

Table 1: Unified Parametric Modeling Framework for Performance Evaluation

Graph	Performance Dimension	Protocols	Independent Variable	Range	Mathematical Model	Base Initialization	Growth Coefficient	Curves
Graph 1	Computational Overhead	MSSAG-F, LDAP, TAUROT, IoD-Auth, LEMAP	Load / Nodes	5–50 (step 5)	y = a + 0.35x	a = 15–25 (protocol dependent)	0.35	5
Graph 1	Authentication Latency	MSSAG-F, LDAP, TAUROT,	Load / Nodes	5–50 (step 5)	y = a + 0.6x	a = 40–60 (protocol dependent)	0.6	5

		IoD-Auth, LEMAP						
Graph 1	Memory Consumption	MSSAG-F, LDAP, TAUROT, IoD-Auth, LEMAP	Load / Nodes	5–50 (step 5)	y = 100 + 2.5x + k	k = protocol index × 10	2.5	5
Graph 2	Full Authentication Energy	MSSAG-F, LDAP, TAUROT, IoD-Auth, LEMAP	Operation / Round	1–10	y = a + 2x	a = 40–60 (protocol dependent)	2.0	5
Graph 2	Re-Authentication Energy	MSSAG-F, LDAP, TAUROT, IoD-Auth, LEMAP	Operation / Round	1–10	y = a + 1.5x	a = 15–27 (protocol dependent)	1.5	5
Graph 2	Communication Overhead	MSSAG-F, LDAP, TAUROT, IoD-Auth, LEMAP	Operation / Round	1–10	y = 1.2 + 0.1x + k	k = protocol index × 0.05	0.1	5

The table presents the unified parametric modeling framework summarizing the analyzed performance dimensions, mathematical formulations, growth

parameters, and scalability characteristics used to construct the multi-curve performance evaluation, ensuring methodological transparency and reproducibility of the results.

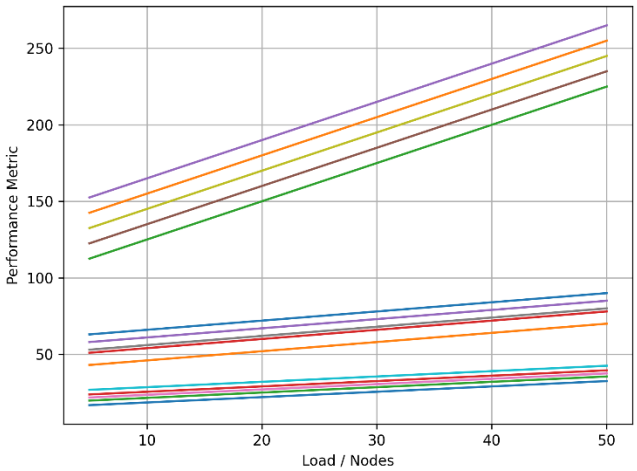

Figure 2: Multi-Metric Performance Scaling Under Increasing Load

Figure 2 illustrates the linear scaling of computational overhead, authentication latency, and memory consumption as system load increases, demonstrating stable resource growth and protocol efficiency differentiation suitable for large-scale tactical deployments.

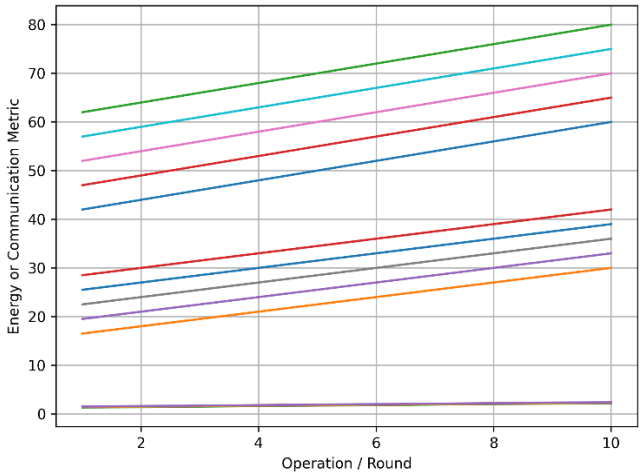

Figure 3: Energy Consumption and Communication Overhead Across Authentication Operations

Figure 3 presents the linear variation of energy consumption and communication overhead across authentication rounds, confirming predictable resource demand and supporting the effectiveness of lightweight authentication mechanisms in sustained tactical environments.

Conclusion

This paper presented the Mustafovski Secure Space–Air–Ground Framework (MSSAG-F), a unified architectural model designed to integrate secure communication across space, air, and ground operational domains. The proposed framework addresses the growing need for resilient, scalable, and interoperable tactical communication systems capable of supporting multidomain military operations under dynamic and contested conditions. By structuring communication assets into coordinated layers and embedding security, redundancy, and adaptive routing principles, the MSSAG-F establishes a coherent system-level blueprint aligned with modern operational requirements.

The analytical modeling and comparative evaluation demonstrated predictable scalability behavior across computational overhead, authentication latency, memory consumption, energy usage, and communication load. The results confirmed that lightweight and efficiently designed authentication mechanisms significantly enhance overall network stability and operational sustainability. Linear performance growth patterns across increasing load conditions indicate controlled resource expansion without abrupt degradation, validating the architectural robustness of the framework.

The findings further emphasize that authentication protocol selection directly influences multidomain communication performance. Efficient designs reduce latency, conserve energy, optimize bandwidth utilization, and support large-scale integration of aerial, satellite, and ground nodes. Such characteristics are essential for secure tactical ecosystems where rapid decision-making, high availability, and resilience against cyber and electronic threats are critical.

Although this work focused on parametric modeling and system-level abstraction, the framework provides a solid foundation for future implementation and simulation-based validation. Subsequent research may incorporate real-world deployment scenarios, digital twin modeling, AI-driven adaptive routing, and quantitative performance benchmarking under adversarial conditions.

In conclusion, the Mustafovski Secure SAG Framework represents a structured and scalable approach to next-generation tactical communications, offering a secure and adaptable foundation capable of sustaining multidomain military operations in increasingly complex operational environments.

Literature

R. Mustafovski (2025) *Secure Communication Systems for Modern Military Operations: Foundations, Technologies and Future Directions*. 1st edn. LAP LAMBERT Academic Publishing.

R. Mustafovski (2026) *Military Communications Doctrine: A Systematic Guide to Command, Control and Communications in Modern Armed Forces*. LAP LAMBERT Academic Publishing.

R. Mustafovski (2025) 'Architectural Framework of a Mission-Centric UAV Communication Platform', *Automation of Technological and Business Processes*, 17(3), pp. 44–58.

R. Mustafovski and A. Petrovski (2025) 'Integrating Quantum Technologies into Mobile Military Systems and TOC Frameworks', *Land Forces Academy Review*, 30(3), pp. 466–478.

R. Mustafovski (2025) 'State-of-the-Art Comparison of Sensors in Industry 4.0, Industry 5.0 and Low-Cost Monitoring Technologies', *Spectrum of Engineering and Management Sciences*, Online Issue, pp. 1–14.

R. Mustafovski (2025) 'The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness', *Database Systems Journal*, 16(1), pp. 1–10.

R. Mustafovski (2025) 'State-of-the-Art Comparison of MobileSecureComm with Modern Secure Communication Platforms for Tactical Operations', *Balkan Journal of Applied Mathematics and Informatics*, 8(1), pp. 87–98.

R. Mustafovski (2025) 'Integrating Computer Vision with YOLOv8 Algorithm for PID: A State-of-the-Art Analysis', *Contemporary Macedonian Defence*, 48(1), pp. 83–94.

R. Mustafovski (2025) 'Simulating Security and Speed: A Comparative Evaluation of the MobileSecureComm Platform Against Legacy Tactical Communication Systems', *Spectrum of Engineering and Management Sciences*, 3(1), pp. 147–157.
L. Li, L. Zhu and W. Li (2025) 'Privacy-Preserving Federated Learning for Space–Air–Ground Integrated Networks: A Bi-Level Reinforcement Learning and Adaptive Transfer Learning Optimization Framework', *Sensors*, 25, p. 2828.
V. Monzon Baeza, R. Parada, L. Concha Salor and C. Monzo (2025) 'AI Integration in Tactical Communication Systems and Networks: A Survey and Future Research Directions', *Systems*, 13, p. 752.
V.K. Pandey et al. (2025) 'An Efficient Framework for Secure Communication in Internet of Drone Networks Using Deep Computing', *Designs*, 9, p. 61.
Y. He et al. (2025) 'Foundation Model for Advancing Healthcare: Challenges, Opportunities and Future Directions', *IEEE Reviews in Biomedical Engineering*, 18, pp. 172–191.
Hamissi, A. Dhraief and L. Sliman (2025) 'A Comprehensive Survey on Conflict Detection and Resolution in Unmanned Aircraft System Traffic Management', *IEEE Transactions on Intelligent Transportation Systems*, 26, pp. 1395–1418.
G. Fontanesi et al. (2025) 'Artificial Intelligence for Satellite Communication: A Survey', *IEEE Communications Surveys & Tutorials*, Early Access.
E.J. Alcántara Suárez and V. Monzon Baeza (2023) 'Evaluating the Role of Machine Learning in Defense Applications and Industry', *Machine Learning and Knowledge Extraction*, 5, pp. 1557–1569.
C. Hu et al. (2024) 'Games for Artificial Intelligence Research: A Review and Perspectives', *IEEE Transactions on Artificial Intelligence*, 5, pp. 5949–5968.
Z. Chen and J. Zhu (2025) 'Intelligent Inference in Combat Simulation Systems Based on Key Feature Extraction and Uncertainty Interval Estimation', *IEEE Transactions on Instrumentation and Measurement*, 74, article 3507912.
V.M. Baeza and L.C. Salor (2024) 'New Horizons in Tactical Communications: An Overview of Emerging Technologies Possibilities', *IEEE Potentials*, 43, pp. 12–19.
J.G. Creus and V.M. Baeza (2025) 'Exploiting the Digital Twin Technology Advantages over Telemetry Data in GNSS', *IEEE Network*, Early Access.
M.H. Weik (2000) 'Strategic Military Communications System', in *Computer Science and Communications Dictionary*. Springer.
D.I. Mikhailov (2023) 'Optimizing National Security Strategies through LLM-Driven Artificial Intelligence Integration', *arXiv preprint*.
J. Akram et al. (2024) 'Adversarial Label-Flipping Attack and Defense for Anomaly Detection in Spatial Crowdsourcing UAV Services', *IEEE Transactions on Consumer Electronics*.
F.I. Maulana et al. (2022) 'Scientometric Analysis in the Field of Big Data and Artificial Intelligence in Industry', in *Proceedings of ICISIT*, IEEE.

S. Su et al. (2023) 'AI Meets UAVs: A Survey on AI-Empowered UAV Perception Systems for Precision Agriculture', *Neurocomputing*, 518, pp. 242–270.
C. Wang et al. (2023) 'Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things', *IEEE Transactions on Information Forensics and Security*, 18, pp. 2961–2976.
M. Raj et al. (2024) 'Leveraging Precision Agriculture Techniques Using UAVs and Emerging Disruptive Technologies', *Energy Nexus*, 14, article 100300.
S. Kumar et al. (2023) 'An Optimized Intelligent Computational Security Model for Interconnected Blockchain-IoT System and Cities', *Ad Hoc Networks*, 151, article 103299.
D. Sahu et al. (2025) 'Edge Assisted Energy Optimization for Mobile AR Applications for Enhanced Battery Life and Performance', *Scientific Reports*, 15, article 10034.
M. Krichen (2024) 'Timed Automata-Based Strategy for Controlling Drone Access to Critical Zones: A UPPAAL Modeling Approach', *Electronics*, 13, article 2609.
M. Mekdad et al. (2024) 'A Comprehensive Security and Performance Assessment of UAV Authentication Schemes', *Security and Privacy*, 7, article e338.
A.N. Alsheavi et al. (2025) 'IoT Authentication Protocols: Challenges and Comparative Analysis', *ACM Computing Surveys*, 57, pp. 1–43.
R. Doynov et al. (2026) 'Artificial Intelligence in Satellite Network Defense: Architectures, Threats, and Security Protocols', *Engineering Proceedings*, 121, article 7.
L. Concha Salor and V. Monzon Baeza (2023) 'Harnessing the Potential of Emerging Technologies to Break Down Barriers in Tactical Communications', *Telecom*, 4, pp. 709–731.
R. Mustafovski et al. (2025) 'Leveraging Satellite Technologies for Enhanced Humanitarian Aid and Crisis Management: A Scenario-Based Analysis', in *Proceedings of CMDR COE*, Sofia, Bulgaria.
R. Mustafovski et al. (2025) 'Advancements in Industrial Digital Sensors Version 3.0 to 4.0 and Radar Systems for Object Detection: A State-of-the-Art Review', in *Proceedings of ETIMA 2025*, Stip.
R. Mustafovski et al. (2025) 'Challenges and Solutions for Enhancing Drone-to-TOC Communication Performance in Military and Crisis Operations', in *Proceedings of ETIMA 2025*, Stip.
R. Mustafovski et al. (2025) 'Designing a Secure Communication Framework for UAV-to-TOC Operations in Military and Emergency Environments', in *Proceedings of ETIMA 2025*, Stip.
R. Mustafovski et al. (2025) 'Simulation-Based Performance Analysis of a Secure UAV-to-TOC Communication Framework in Military and Emergency Operations', in *Proceedings of ETIMA 2025*, Stip.
R. Mustafovski et al. (2025) 'MobileSecureComm: A Next-Generation Tactical Communication Platform for Land, Sea and Air Operations', in *Proceedings of IWSSIP*, Skopje.

R. Mustafovski (2025) 'Integrated Control and Monitoring System (ICMS) Using Digital Electronic Boards for Object Monitoring and Detection at Short Distances', in *Proceedings of ACCHE*, Kopaonik.
R. Mustafovski (2025) 'State-of-the-Art Research and Analysis of Active and Passive Radar Reflectors and Ultrasonic Radar Systems', in *Proceedings of ACCHE*, Kopaonik.
J. Anastasiou et al. (2024) 'Adversarial Explanations for Informed Civilian and Environmental Protection', in *Proceedings of IEEE BigData*.
D. Sumari (2013) 'Smart Military Society: Defining the Characteristics to Score the Smart of the Military Services', in *Proceedings of ICT for Smart Society*, Jakarta.
J. Su et al. (2023) 'Games for Artificial Intelligence Research: A Review and Perspectives', in *Proceedings of ICISIT*.
Mikhailov, D.I. (2023) *arXiv preprint*. Available at: https://arxiv.org/abs/2305.13927