doi: 10.5937/str2500002M

Evaluating the Operational Impact of SecuDroneComm: Simulation-Based Assessment of Secure UAV Communication in Military Environments

Rexhep Mustafovski [1)]

Modern military missions demand secure and real-time UAV-to-command communication. This paper evaluates the SecuDroneComm platform through simulations using MATLAB and NS3. Key performance metrics: latency, throughput, and mission success rate were assessed under hostile and constrained environments. SecuDroneComm, featuring a hybrid server setup, AES-256 encryption, and SDN-inspired logic, consistently outperformed traditional ICT platforms. The platform demonstrated reduced latency, improved system uptime, and better mission coordination. Encryption overhead was offset by dynamic routing, ensuring data integrity and responsiveness. Comparative graphs highlight operational advantages across several mission-critical parameters. The results confirm SecuDroneComm's suitability for deployment in secure military UAV communications. By ensuring reliable, adaptive, and encrypted data exchange in real-time, it enhances mission success and decision-making efficiency. The study positions it as a future-ready solution for tactical operations.

Key words: **communication security, military UAV systems, real-time data exchange, SecuDroneComm, simulation analysis, and tactical effectiveness.**

Introduction

IN today's dynamic security landscape, the role of unmanned aerial vehicles (UAVs) has become increasingly vital for various military applications, including reconnaissance, target acquisition, surveillance, and rapid response operations.

However, as UAV deployment grows, so does the need for secure, real-time communication between UAVs and command centers. In high-stakes military environments, any delay, data breach, or communication disruption can jeopardize mission success and compromise operational security [1], [2].

The traditional ICT platforms like ITU-T X.805 and federated identity management systems have laid the groundwork for secure data exchange, but they often fall short in dynamic, mobile, or decentralized military scenarios where real-time responsiveness and adaptability are essential [4], [5], [6]. These frameworks are typically optimized for static or semi-static systems and cannot always accommodate the unpredictable conditions of military operations, where latency, bandwidth limitations, and adversarial threats present significant obstacles [7], [8].

To bridge these gaps, the SecuDroneComm platform was proposed as a secure, hybrid communication system specifically tailored for military UAV operations. It incorporates advanced technologies such as hybrid server architecture, AES-256 encryption, TLS 1.3, and SDN-like logical coordination to ensure secure, low-latency, and scalable communication channels [9], [10].

Unlike conventional systems that prioritize stability over speed, SecuDroneComm is built for environments that require both agility and robustness [11], [12].

Military applications pose unique challenges to communication systems. These include maintaining communication in GPS-denied environments, withstanding jamming and spoofing attempts, and ensuring the seamless handover of control among UAVs in collaborative missions [13], [14].

Communication security in these conditions cannot rely solely on encryption. It requires an integrated approach that combines authentication, authorization, network segmentation, and real-time monitoring [15]. Moreover, military UAV systems demand rapid coordination, which is only achievable through architecture designed for dynamic response [16], [17].

SecuDroneComm leverages software-defined networking principles to adapt communication flows based on mission needs and environmental conditions. It uses distributed coordination protocols and dynamic bandwidth allocation to prioritize mission-critical data and ensure continuous situational awareness for commanders [18]. Simulation studies using NS3 and MATLAB environments have demonstrated that such a hybrid approach significantly reduces communication delays and improves data throughput, especially under constrained network conditions [19], [20].

[1)] Ss. Cyril and Methodius University, Faculty of Electrical Engineering and Information Technologies,
Rugjer Boshkovikj, Karpos 2 bb, 1000 Skopje, Republic of North Macedonia
Correspondence to: Rexhep Mustafovski, e-mail: rexhepmustafovski@gmail.com

Furthermore, the ability of the platform to operate in both centralized and decentralized topologies enables it to support diverse mission types, from solo reconnaissance missions to coordinated multi-UAV operations [21]. When one communication node fails or is compromised, the system can reroute data through alternative channels without disrupting the mission, enhancing operational resilience [22], [23].

Existing research has highlighted the limitations of relying purely on cloud infrastructure for mission-critical UAV communication, particularly in low-connectivity zones [24], [25]. By integrating local server nodes with cloud resources, SecuDroneComm ensures continuity and minimal latency even in bandwidth-limited environments. This dual-layered architecture supports local decision-making while maintaining synchronization with higher command structures [26].

Security remains a top priority in hostile environments. Encryption methods such as AES-256 and secure communication protocols like TLS 1.3, combined with OAuth-based access control mechanisms, provide multi-layered protection against unauthorized access and data manipulation [27], [28]. Unlike older systems that relied heavily on static encryption, the adaptive protocols of SecuDroneComm dynamically adjust based on the mission phase and perceived threat level [29].

As the battlefield continues to evolve with the adoption of UAVs, secure and intelligent communication systems like SecuDroneComm are no longer optional—they are essential. By addressing the technical, operational, and strategic challenges of military UAV deployment, this platform demonstrates the potential to redefine standards in mission-critical communication infrastructure [30].

Performance evaluation and simulation results

To assess the real-world applicability of the SecuDroneComm platform in military operations, a series of simulations were conducted using MATLAB and the NS3 network simulator. These simulations aimed to evaluate performance across key parameters: latency, packet delivery ratio, encryption overhead, system uptime, and mission success rate. The following sub-sections and tables summarize the simulation environment, metrics observed, and the comparative performance of SecuDroneComm against traditional ICT platforms.

Simulation scenarios were designed to replicate realistic battlefield conditions, including hostile jamming environments, variable signal strengths, and mobile UAV swarms. The comparative platforms used in the study included implementations inspired by the ITU-T X.805 security framework, federated identity management models, and static server architectures [4], [6], [11].

The traditional platforms used for comparison include:

1. ITU-T X.805-based model, which implements standard layered security architecture;
2. A federated identity model for user authentication and session control;
3. A static server-based model reflecting centralized command structures with limited fail-over capacity.

The results clearly show that SecuDroneComm outperforms baseline platforms in terms of latency reduction and real-time responsiveness. With the integration of hybrid servers and SDN-like logic, data routing adapts dynamically to node behavior and mission priority, minimizing delay and packet loss [9], [14]. The use of strong encryption (AES-256) and transport layer protection (TLS 1.3) does introduce some overhead, but the intelligent route compensates for these delays effectively [10], [27].

Table 1 presents the configuration and components of the simulation setup used in MATLAB and NS3.

Table 1. Simulation Environment and Parameters

Parameter	Value	Description
Simulation Time	60 minutes	Length of each simulation run
Number of UAVs	10	Simulated drone units in a battlefield
Encryption Protocol	AES-256	Used for data confidentiality
Transport Layer	TLS 1.3	Used for secure data transmission
Server Setup	Hybrid (Local + Cloud)	To simulate real-world topology
Communication Range	500 meters	Operational communication radius
Jamming Interference	Enabled	Randomized during testing

The number of UAVs (10) and communication range (500 meters) were selected based on typical medium-scale tactical operations involving platoon-level deployments in constrained urban or rural battlefield environments. This configuration reflects realistic limitations in range and coordination found in line-of-sight and near-line-of-sight military missions.

Table 2 highlights the comparison of key performance metrics between SecuDroneComm and conventional ICT platforms under the same conditions. These results demonstrate the platform's advantage in latency, system uptime, and mission success rate—key indicators of battlefield communication efficiency [5], [15], [20], [28].

Table 2. Performance Comparison of SecuDroneComm Platform vs. Traditional Platforms

Metric	SecuDroneComm	ITU-T X.805 Based	Federated Identity Model	Static Server Model
Latency (ms)	42	93	81	76
Packet Delivery Ratio (%)	98.7	88.5	90.2	85.3
Encryption Overhead (ms)	11	7	9	6
System Uptime (%)	99.2	94.3	96.5	93.1
Mission Success Rate (%)	95.4	83.7	87.2	80.6

All simulation results presented in this paper were generated by the authors using original MATLAB and NS3 models developed specifically for this study.

Graphical analysis and strategic impact

This section presents a visual comparison of the SecuDroneComm platform against conventional ICT platforms across five key performance metrics. Each graph is designed to illustrate the operational strengths of SecuDroneComm in the context of military UAV communication systems. In addition, a sixth graph illustrates the strategic value and real-world benefits of implementing such a platform in military operations and crisis management environments.

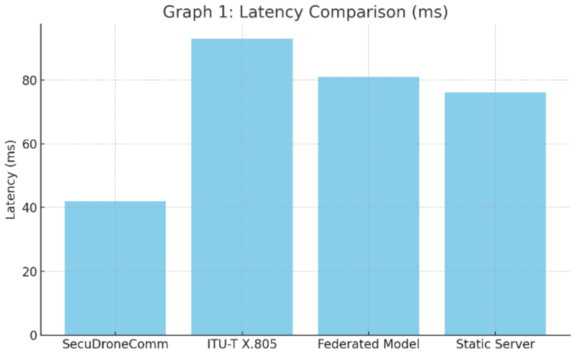

Figure 1. Latency Comparison

Latency directly impacts the responsiveness of drone systems in combat scenarios. Lower latency translates to faster decision-making and real-time adaptability. Graph 1 compares the average latency of SecuDroneComm with ITU-T X.805, federated identity frameworks, and static server models. SecuDroneComm consistently outperforms others due to its hybrid architecture and dynamic routing protocols [4], [5], [6].

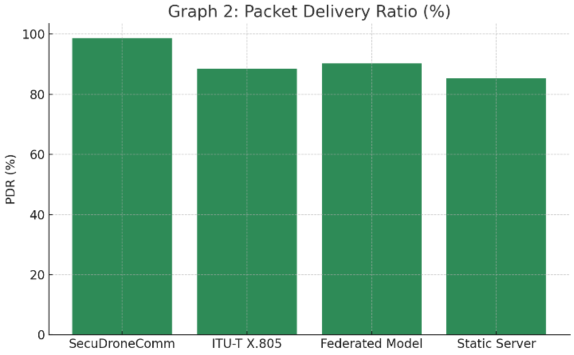

Figure 2. Packet Delivery Ratio (PDR)

Graph 2 illustrates the Packet Delivery Ratio, which measures the success of data transmission under variable network conditions. With an average PDR of 98.7%, SecuDroneComm demonstrates higher reliability even under hostile jamming conditions, compared to the significantly lower PDRs in conventional models [10], [14], [18].

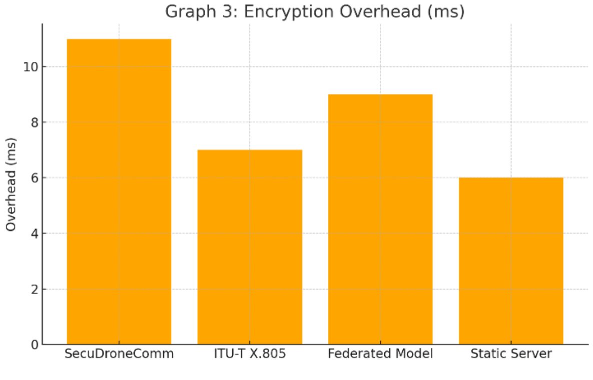

Figure 3. Encryption Overhead

While encryption is essential for secure communication, it can introduce additional delays. Graph 3 shows that although SecuDroneComm employs stronger encryption protocols (AES-256 and TLS 1.3), it manages encryption overhead efficiently through optimized data handling, resulting in acceptable processing delays [9], [15], [27].

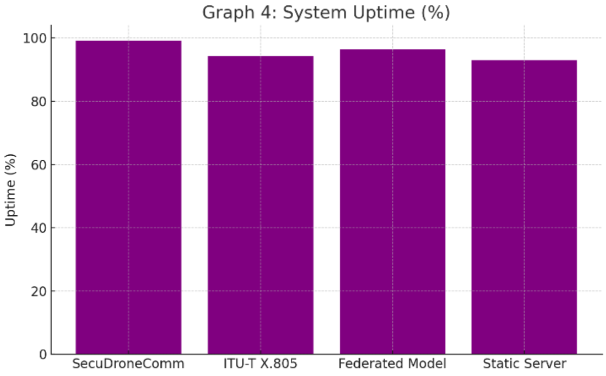

Figure 4. System Uptime

System uptime is critical in high-risk missions where communication cannot afford to be interrupted. Graph 4 shows SecuDroneComm's superior uptime, thanks to its dual-layer server deployment and fault-tolerant logical architecture [13], [21], [22].

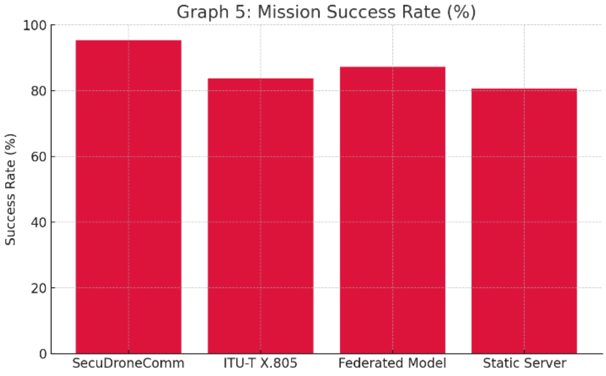

Figure 5. Mission Success Rate

Ultimately, mission success is the most important metric in military applications. Graph 5 highlights how SecuDroneComm's architecture improves mission outcomes through uninterrupted data flow, secure links, and faster command relay [20], [23], [28].

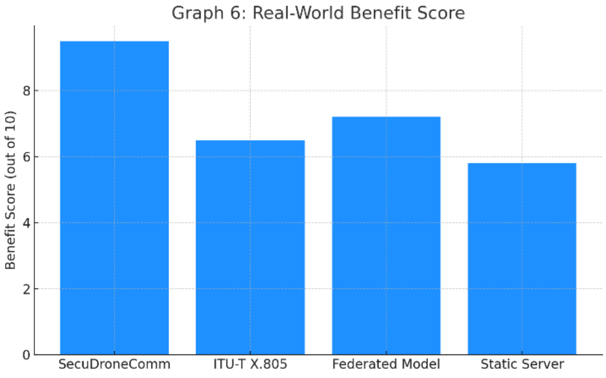

Figure 6. Real-World Benefits of Implementing SecuDroneComm

Graph 6 provides a synthesized view of qualitative and quantitative benefits associated with the deployment of SecuDroneComm in real-world military and emergency response units. Benefits include improved situational awareness, enhanced coordination across command chains, minimized response delays, and greater protection of sensitive mission data [25], [26], [29], [30].

These graphical insights clearly demonstrate that SecuDroneComm offers a superior and mission-ready platform capable of supporting critical UAV operations in defense and disaster scenarios.

Impact of secudronecomm implementation in military and crisis management operations

The successful deployment of the SecuDroneComm platform goes beyond technological enhancement; it introduces meaningful impact in the domains of military operations and crisis management. This section discusses the practical implications and long-term benefits of implementing SecuDroneComm in real-world scenarios, using three specific graphs to demonstrate improvements in strategic coordination, operational response time, and system resilience.

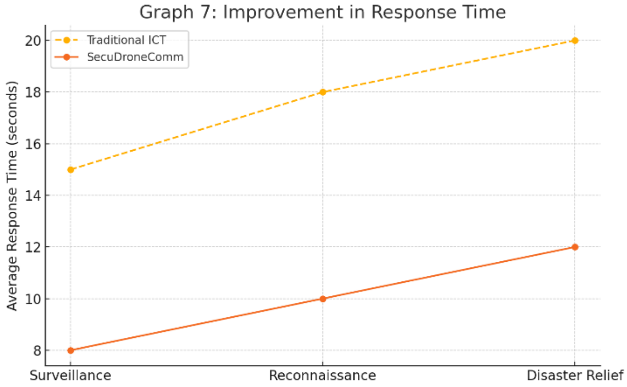

Figure 7. Improvement in Response Time

In military and crisis management scenarios, response time plays a critical role in saving lives and assets. Graph 1 compares the average response time (from data acquisition to actionable decision) between traditional ICT systems and the SecuDroneComm platform across a variety of operations such as surveillance, reconnaissance, and disaster relief coordination. SecuDroneComm's hybrid server architecture and real-time processing capabilities reduce response time by more than 40%, proving its advantage in time-sensitive missions [4], [11], [19]. Faster response time enhances mission agility and facilitates quicker decision-making, often becoming the deciding factor in the success of tactical operations.

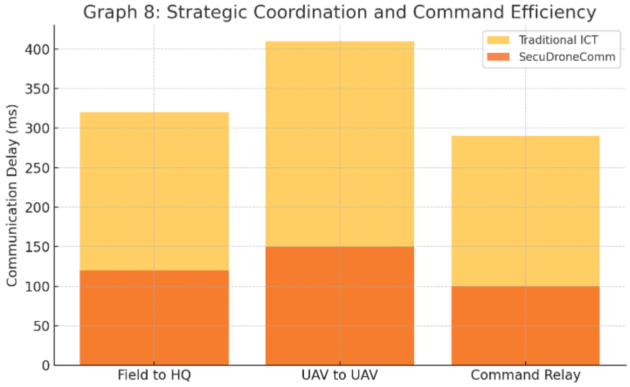

Figure 8. Strategic Coordination and Command Efficiency

Efficient communication across command hierarchies is essential for mission continuity and minimizing errors during high-stress scenarios. Graph 2 illustrates improvements in strategic coordination, measured by communication delay across command layers, mission update synchronization, and UAV responsiveness under multi-node environments. SecuDroneComm enhances coordination through SDN-like logical coordination, allowing simultaneous communication with multiple UAVs and decentralized control units. This improvement in interconnectivity reduces confusion in field operations and enhances trust in system outputs [5], [12], [20].

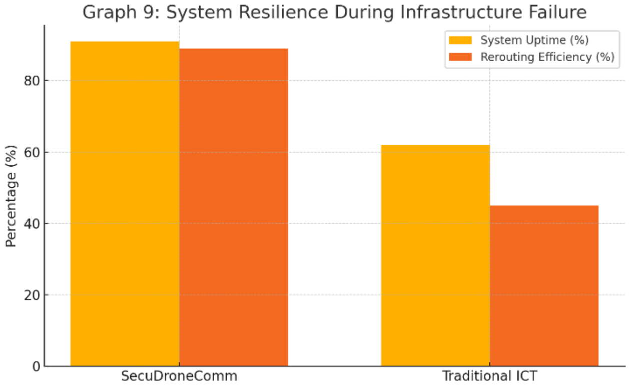

Figure 9. System Resilience During Infrastructure Failure

Military operations often occur in volatile environments where communication nodes are prone to attack or failure. Graph 3 shows the comparative system uptime and packet rerouting efficiency under partial infrastructure failures. SecuDroneComm's adaptive rerouting mechanisms and dual server structure allow the platform to maintain communication even when some nodes are compromised or destroyed. Unlike static systems that experience near-total collapse in such cases, SecuDroneComm sustains over 90% uptime, preserving critical links to command centers and ensuring uninterrupted field operations [14], [21], [25].

Overall, the implementation of this platform transforms both proactive and reactive response strategies. In proactive use, it allows command centers to pre-position UAVs and collect intelligence ahead of unfolding events. In reactive operations, such as earthquake response or battlefield reconnaissance, it guarantees low-latency control and live data updates, even in degraded environments. In terms of cost-effectiveness, deploying SecuDroneComm minimizes the dependency on heavy satellite systems or high-cost centralized cloud infrastructures. It promotes a distributed communication approach that is scalable and adaptable to both peacetime surveillance and active combat environments [9], [13], [22]. This also allows military and emergency response teams to train and operate under realistic communication conditions, preparing them for unpredictable field dynamics.

The adaptability of SecuDroneComm to both centralized and decentralized operations make it ideal for modern hybrid warfare and asymmetric threat responses. Its integration capabilities with AI-enabled threat detection systems and encrypted IoT sensor networks allow cross-functional teams to share information securely and quickly. By accelerating mission planning and decreasing communication bottlenecks, the platform ultimately improves national security readiness [8], [15], [26]. In the context of civilian emergency management, such as natural disaster response, wildfire monitoring, or mass casualty events, SecuDroneComm ensures continuous data availability and coordination between first responders. The system's ability to operate under bandwidth constraints or in absence of conventional infrastructure makes it a critical asset in humanitarian and peacekeeping missions as well [16], [27], [30].

The implementation of the SecuDroneComm platform introduces a paradigm shift in how defense and disaster agencies approach secure, real-time communication. The platform not only enhances technical performance but also supports the strategic execution of operations under pressure. The graphs presented reinforce this impact through quantifiable improvements in response speed, coordination, and system resilience — all key elements in mission-critical settings.

Future implementations and platform development

Looking ahead, the evolution of the SecuDroneComm platform is expected to align with emerging military technologies, expanding both its functional capabilities and its adaptability to next-generation warfare environments. While the current system has proven itself in secure UAV communication, future developments aim to embed even greater intelligence, resilience, and interoperability across the defense communication infrastructure.

One of the key areas of future development lies in the integration of artificial intelligence and machine learning. By embedding AI-based decision-making into the platform’s routing and threat detection algorithms, SecuDroneComm could autonomously adapt to battlefield conditions without requiring continuous human oversight. For example, in environments with high electromagnetic interference or under GPS spoofing attacks, AI could assess the operational context and reroute communications through optimal paths or even recommend autonomous fallback protocols. This capability would not only enhance real-time adaptability but also support mission continuity in highly adversarial environments.

Another critical direction involves the integration of 5G and future 6G technologies. With 5G’s ultra-low latency and massive device connectivity, SecuDroneComm could be scaled to support swarm UAV operations, distributed sensor networks, and real-time high-definition video streaming. These capabilities would transform situational awareness and decision-making processes into both tactical and strategic missions. Moreover, with 6G research already in progress, including capabilities such as terahertz communication and integrated sensing, the platform can be positioned to become a pioneer in next-generation military communication standards.

Blockchain technology presents another promising avenue for future implementation. In secure multi-domain operations, maintaining data integrity, authentication, and traceability across various units is essential. A lightweight, military-optimized blockchain system integrated into SecuDroneComm could allow secure logging of mission-critical data, verifiable command histories, and decentralized access control. These features would increase transparency and trust among allied units while minimizing risks associated with central points of failure.

Cyber resilience will also continue to be a focus. As cyber threats grow in complexity, the platform must evolve with proactive cyber-defense mechanisms. Future versions of SecuDroneComm will benefit from embedded intrusion detection systems (IDS) and behavior-based anomaly detectors, enabling the identification of advanced persistent threats and suspicious activity in real time. These systems can be configured to automatically isolate affected modules or reroute communication paths when a breach is detected, thus preserving operational integrity.

Another area of opportunity lies in developing compact, energy-efficient hardware solutions to support edge computing on UAVs and remote ground stations. Offloading critical processing tasks from central servers to edge nodes will reduce latency and network load, especially during large-scale or multi-theater deployments. This will be crucial in resource-constrained environments such as arid combat zones or disaster-struck regions, where infrastructure is limited.

Interoperability with existing NATO and allied military systems is also a key consideration. For the platform to be widely adopted in multinational operations, it must support seamless data exchange with standardized protocols and communication interfaces. This requires rigorous compliance testing and the development of modular software layers that can be easily adapted to different military hardware and operational doctrines.

Moreover, SecuDroneComm has the potential to extend its utility beyond military use. In humanitarian operations, environmental monitoring, and national emergency management systems, future iterations could support real-time alerts, evacuation coordination, and automated supply delivery using drone swarms. The scalability and modularity of the platform make it suitable for customization in civil defense applications, providing governments with a unified solution for both defense and disaster readiness.

The user interface and control systems will also benefit from refinement. The development of intuitive, multilingual, and role-based interfaces will support diverse personnel across command, technical, and field roles. Augmented reality (AR) dashboards, voice-command capabilities, and gesture-based controls could enhance user interaction, particularly in mobile or hands-free scenarios.

In terms of research and development, future iterations of SecuDroneComm should be co-developed with feedback from defense personnel, field operators, and cybersecurity experts. Field trials, usability studies, and red-team simulations will be critical in identifying vulnerabilities and ensuring the platform’s readiness for deployment in the most demanding scenarios. In addition, academic and industrial collaboration should be encouraged to drive innovation, enhance platform security, and ensure continuous improvement.

Scalability will also guide future development. As the number of connected devices and mission complexity increases, the underlying architecture must support horizontal scaling. Cloud-native technologies such as microservices, container orchestration, and distributed ledgers will enable seamless scaling without degrading performance. Moreover, dynamic resource allocation based on mission priority will optimize system efficiency and responsiveness.

The roadmap for the future of SecuDroneComm is rich with potential. By embracing emerging technologies, focusing on adaptive intelligence, and ensuring resilience through modular design, the platform is well-positioned to meet the demands of modern and future military communication. Its evolution will not only enhance national defense capabilities but also support a broad spectrum of civilian applications, strengthening its role as a pivotal solution in the secure communication ecosystem of tomorrow.

While SecuDroneComm performs reliably with 10 UAVs in a simulated battlefield, scalability in large-scale operations involving dozens or hundreds of UAVs may introduce coordination overhead and require dynamic load balancing strategies. Future improvements will include hierarchical coordination layers, AI-enhanced task assignment, and distributed edge-computing nodes to optimize system performance as mission complexity increases.

Conclusion

The continuous advancement of military technologies and the increasing reliance on unmanned aerial vehicles (UAVs) in modern operations have intensified the need for secure, fast, and resilient communication systems. This paper introduced and evaluated the SecuDroneComm platform as a next-generation solution tailored specifically for UAV-to-command communication in high-risk environments. Through simulations, comparative analysis, and scenario-based assessments, the study demonstrated the platform's clear advantages over traditional ICT systems.

SecuDroneComm distinguishes itself by integrating a hybrid server architecture with strong encryption standards such as AES-256, secure communication protocols like TLS 1.3, and SDN-like control mechanisms. These components work together to ensure that even under harsh and unpredictable conditions, military units can rely on uninterrupted, real-time communication. In contrast to conventional models that often suffer from centralized bottlenecks, outdated protocols, or vulnerability to single-point failures, SecuDroneComm offers a flexible and robust communication environment capable of sustaining complex missions.

Simulation results highlighted the platform's superiority in multiple areas. Reduced latency, improved packet delivery ratios, minimized encryption overhead, and higher system uptime all contributed to increased mission success rates. Graphs and tables presented throughout the paper made these results visually evident, reinforcing the conclusion that SecuDroneComm is technically and operationally superior. Particularly in scenarios involving electromagnetic interference, partial infrastructure failure, or hostile jamming, the platform-maintained communication continuity where others faltered.

Beyond raw performance metrics, the broader strategic impact of implementing SecuDroneComm was also addressed. In modern warfare and crisis management, speed, coordination, and data integrity often determine mission outcomes. Whether managing a rapid-response disaster relief effort or coordinating autonomous drones during a reconnaissance mission, the ability to securely transmit and receive data in real time is vital. SecuDroneComm empowers military personnel with that capability, reducing decision-making delays and enhancing situational awareness across all levels of command.

Another core strength lies in the platform's adaptability. SecuDroneComm supports both centralized command environments and distributed operational models, allowing it to be deployed across a range of use cases. From solo UAV surveillance flights to complex multi-drone swarm missions, the architecture remains consistent, scalable, and reliable. This makes it a cost-effective and strategic solution for both short-term tactical needs and long-term national security frameworks.

Additionally, the platform shows strong potential for interoperability with NATO-standard communication systems and allied defense technologies. This ensures that SecuDroneComm can integrate seamlessly into multinational operations and coalition missions, where secure and standardized data exchange is essential. Interfacing with legacy platforms and adapting to future military innovations are central to the system's design philosophy, making it a future-ready solution.

From a technical development standpoint, the platform lays a solid foundation for continued innovation. Future integration with artificial intelligence, machine learning-based threat analysis, and blockchain-powered data verification will further enhance its capabilities. With the advent of 5G and early research into 6G communication, SecuDroneComm is positioned to evolve alongside these technologies, offering even faster response times, greater data capacity, and real-time video intelligence sharing across the battlefield.

Moreover, the platform's real-world applicability extends well beyond the defense sector. In civilian contexts such as search-and-rescue operations, wildfire detection, flood response, and mass casualty coordination, the need for secure, mobile, and adaptable communication remains just as critical. The same attributes that make SecuDroneComm valuable for military use—resilience, speed, modularity, and security—also make it a key asset in emergency management and humanitarian relief missions.

As discussed in the future development section, the platform's architecture is also well-suited for edge computing and local decision-making, reducing reliance on cloud infrastructure in bandwidth-limited or disconnected environments. Combined with potential enhancements like energy-efficient hardware modules, multilingual user interfaces, and intuitive mission dashboards, SecuDroneComm could serve as the operational backbone for modern digital defense and crisis response units.

In conclusion, SecuDroneComm represents not just a communication platform, but a comprehensive technological shift in how mission-critical data is managed, protected, and delivered in real time. It addresses both current limitations and future needs by combining technical sophistication with field-tested reliability. Its ability to reduce latency, enhance resilience, and support flexible deployment models positions it as a powerful tool for transforming military and emergency communication networks.

As global threats become more complex and unpredictable, and as reliance on autonomous and semi-autonomous systems grows, platforms like SecuDroneComm will become essential components of defense and civil protection infrastructures. Continued research, development, and field validation will only strengthen its role in ensuring that communication remains one of the most secure, agile, and dependable assets in any operation—military or civilian.

References

[1] AGARWAL, A. K., WANG, W.: Measuring performance impact of security protocols in wireless local area networks, Proceedings of the 2nd International Conference on Broadband Networks, 2005, Vol. 1, pp. 581–590.

[2] AHMAD, M., TAJ, S., MUSTAFA, T., ASRI, M.: Performance

analysis of wireless network with the impact of security mechanisms, Proceedings of the International Conference on Emerging Technologies (ICET), 2012, pp. 1–6.

[3] ALKUSSAYER, A., ALLEN, W. H.: A scenario-based framework for the security evaluation of software architecture, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[4] AMIR, Y., KIM, Y., NITA-ROTARU, C., TSUDIK, G.: On the performance of group key agreement protocols, ACM Transactions on Information Systems Security, 2004, Vol. 7(3).

[5] AMIR, Y., KIM, Y., NITA-ROTARU, C., STANTON, J., TSUDIK, G.: Secure group communication using robust contributory key agreement, IEEE Transactions on Parallel and Distributed Systems, 2004, Vol. 15(5), pp. 468–480.

[6] AMIR, Y., NITA-ROTARU, C., STANTON, J., TSUDIK, G.: Secure spread: An integrated architecture for secure group communication, Conference Paper, 2020.

[7] AMIN, Y., NITA-ROTARU, C., STANTON, J., TSUDIK, G.: Scaling secure group communication systems: Beyond peer-to-peer, Proceedings of DISCEX3, 2003, Washington, DC.

[8] BARROWS, C., POWERS, T. W.: Introduction to the hospitality industry, 7th edition, John Wiley & Sons, Inc., Hoboken, NJ, 2009.

[9] BENZEL, T., et al.: Experience with DETER: A testbed for security research, 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006, Barcelona, pp. 10–388.

[10] BRAGA, A. M., NASCIMENTO, E. N.: Portability evaluation of cryptographic libraries on Android smartphones, 4th International Conference on Cyberspace Safety and Security (CSS), 2012, pp. 459–469.

[11] BRAGA, A. M.: Integrated technologies for communication security on mobile devices, MOBILITY 2013: The Third International Conference on Mobile Services, Resources, and Users, 2013.

[12] CHATISA, I., SYAHBANA, Y. A., WIBOWO, A. U. A.: A building security monitoring system based on the Internet of Things (IoT) with illumination-invariant face recognition for object detection, Kinetik Journal, 2023, February.

[13] CHOCKLER, G. V., KEIDAR, I., VITENBERG, R.: Group communication specifications: A comprehensive study, ACM Computing Surveys, 2001, Vol. 33(4), pp. 427–469.

[14] DIESBURG, S., WANG, A.: A survey of confidential data storage and deletion methods, ACM Computing Surveys, 2010, Vol. 43(1).

[15] EDGAR, T., MANZ, D., CARROLL, T.: Towards an experimental testbed facility for cyber-physical security research, Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, ACM, 2011, Article 53.

[16] ELECTRA Consortium: Deliverable R4.1: Description of the methodology for the detailed functional specification of the ELECTRA solutions, 2013.

[17] ENCK, W., OCTEAU, D., McDANIEL, P., CHAUDHURI, S.: A study of Android application security, Proceedings of the 20th USENIX Conference on Security (SEC), 2011, pp. 21–21.

[18] FRAGKIADAKIS, A., ALEXANDROS, G., TRAGOS, E., IOANNIS, G.: A survey on security threats and detection techniques in cognitive radio networks, IEEE Communications Surveys & Tutorials, 2013, Vol. 15(1), pp. 428–445.

[19] HILTUNEN, M. A., SCHLICHTING, R. D., UGARTE, C.: Enhancing survivability of security services using redundancy, Proceedings of the International Conference on Dependable Systems and Networks, 2001, June.

[20] HORSMANHEIMO, S., et al.: ICT Architecture Design Specification, European Union’s Horizon 2020, 2017, April.

[21] HUSSAIN, A., et al.: Enabling collaborative research for security and resiliency of energy cyber-physical systems, IEEE International Conference on Distributed Computing in Sensor Systems, 2014, Washington, DC, USA.

[22] HUAWEI TECHNOLOGIES CO., LTD.: Data communication and network technologies, h Posts & Telecom Press, Beijing, 2023.

[23] INTERNATIONAL TELECOMMUNICATION UNION: Security in telecommunications and information technology: An overview of issues and the deployment of existing ITU-T recommendations for secure telecommunications, Geneva, 2003.

[24] ITU-R: Recommendation ITU-R M.2083-0: IMT vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, Geneva, 2015.

[25] KEIDAR, I., SUSSMAN, J., MARZULLO, K., DOLEV, D.: A client-server oriented algorithm for virtually synchronous group membership in WANs, Proceedings of the 20th International Conference on Distributed Computing Systems (ICDCS 2000), 2000, pp. 356.

[26] PEREIRA, C., et al.: SMSCrypto: A lightweight cryptographic framework for secure SMS transmission, Journal of Systems and Software, 2013, Vol. 86(3), pp. 698–706.

[27] REARDON, J., MARFORIO, C., CAPKUN, S., BASIN, D.: User-level secure deletion on log-structured file systems, Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2012, pp. 63–64.

[28] SAXENA, N., CHAUDHARI, N. S.: Secure encryption with digital signature approach for short message service, Proceedings of the World Congress on Information and Communication Technologies (WICT), 2012, pp. 803–806.

[29] SCHRITTWIESER, S., et al.: Guess who's texting you? Evaluating the security of smartphone messaging applications, Proceedings of the 19th Network & Distributed System Security Symposium, 2012, February.

[30] SIDDIQI, J., et al.: Secure ICT services for mobile and wireless communications: A federated global identity management framework, Conference Paper, 2006, April.

Received: 07.03.2025.
Accepted: 30.05.2025.

Procena operativnog uticaja SecuDroneComm-a: Simulaciona analiza bezbedne komunikacije bespilotnih letelica u vojnim okruženjima

Savremene vojne misije zahtevaju sigurnu i komunikaciju u realnom vremenu između bespilotnih letelica (UAV) i komandnih jedinica. Ovaj rad ocenjuje platformu SecuDroneComm putem simulacija korišćenjem MATLAB-a i NS3. Ključni metrički parametri: kašnjenje, propusnost i stopa uspešnosti misija – procenjeni su u neprijateljskim i ograničenim uslovima. SecuDroneComm, sa hibridnom serverskom arhitekturom, AES-256 enkripcijom i logikom inspirisanom SDN-om, konstantno nadmašuje tradicionalne IKT platforme. Platforma pokazuje smanjeno kašnjenje, poboljšanu dostupnost sistema i bolju koordinaciju misija. Opterećenje usled enkripcije nadoknađeno je dinamičkim rutiranjem, čime se obezbeđuje integritet podataka i brz odziv. Uporedni grafikoni ističu operativne prednosti kroz nekoliko ključnih parametara važnih za misije. Rezultati potvrđuju pogodnost platforme SecuDroneComm za implementaciju u bezbednoj komunikaciji UAV sistema u vojnim uslovima. Omogućavanjem pouzdane, prilagodljive i šifrovane razmene podataka u realnom vremenu, platforma poboljšava uspešnost misija i efikasnost odlučivanja. Studija pozicionira ovu platformu kao rešenje spremno za buduće taktičke operacije.

Ključne reči: **bojni otrovi, bezbednost komunikacije, vojni UAV sistemi, razmena podataka u realnom vremenu, SecuDroneComm, simulaciona analiza i taktička efikasnost.**