DESIGNING A SECURE COMMUNICATION FRAMEWORK FOR UAV-TO-TOC OPERATIONS IN MILITARY AND EMERGENCY ENVIRONMENTS

Rexhep Mustafovski[1], Aleksandar Risteski[1], Tomislav Shuminoski[1]
[1] Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, ul. Ruger Boshkovikj, 1000 Skopje, North Macedonia
email: rexhepmustafovski@gmail.com

Abstract

Ensuring secure and reliable communication between Unmanned Aerial Vehicles (UAVs) and Tactical Operations Centers (TOCs) is critical for mission success in military and emergency response operations. Traditional UAV-to-TOC communication frameworks often suffer from vulnerabilities, including electronic warfare threats, cyberattacks, bandwidth limitations, and interoperability constraints. This paper proposes a Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC) designed to enhance resilience, security, and efficiency in hostile and high-risk environments. The framework integrates end-to-end encryption, blockchain-based authentication, and adaptive frequency management to mitigate jamming and signal interception risks. Additionally, software-defined radios (SDR) optimize spectrum utilization, ensuring reliable communication even in contested environments. To counter cyber threats, intrusion detection systems (IDS) powered by real-time AI monitoring are incorporated, enabling proactive threat mitigation. Furthermore, the framework ensures multi-protocol interoperability, allowing seamless integration of UAV systems within joint military and emergency response operations. The effectiveness of the SCF-UAVTOC model is validated through comparative analysis and simulation-based testing, demonstrating superior performance in secure data transmission, resilience to electronic warfare, and adaptability to dynamic operational conditions. By adopting this framework, defense organizations and emergency agencies can significantly enhance UAV communication security, mission reliability, and overall operational effectiveness in complex battlefield and disaster scenarios.

Key words:

Bandwidth Optimization, Blockchain, Military UAV Communication, Network Security, Secure UAV-to-TOC Communication, Tactical Data Links.

Introduction

The increasing integration of Unmanned Aerial Vehicles (UAVs) into military and emergency operations has transformed modern warfare and crisis management by enhancing situational awareness, surveillance, reconnaissance, and tactical response capabilities. UAVs provide real-time intelligence, reducing operational risks and improving decision-making efficiency in high-risk environments. However, the success of these UAV missions depends on secure, reliable, and efficient communication between UAVs and Tactical Operations Centers (TOCs), ensuring seamless data exchange, command execution, and threat mitigation [1], [4], [9].

Despite technological advancements, UAV-to-TOC communication faces several challenges, including electronic warfare threats, cybersecurity vulnerabilities, bandwidth limitations, and interoperability constraints across multi-national coalition forces. Adversaries continuously develop sophisticated jamming and spoofing techniques to disrupt UAV operations, posing significant risks to mission-critical communications. Conventional communication frameworks relying on fixed-frequency channels and centralized network architectures remain highly susceptible to electronic warfare, leading to potential mission failures and compromised intelligence [6], [14], [19]. Additionally, cyber threats such as data breaches, unauthorized

access, and denial-of-service (DoS) attacks further undermine UAV security, necessitating the adoption of robust encryption protocols and real-time intrusion detection mechanisms [12], [16].

Another major challenge in UAV-to-TOC communication is the management of bandwidth and latency constraints. UAVs generate and transmit vast amounts of real-time intelligence, including high-resolution video feeds, telemetry data, and sensor outputs. Traditional bandwidth allocation methods often struggle to handle this immense data load, leading to congestion, delayed transmission, and reduced operational efficiency [6], [11]. In military and emergency scenarios, where real-time responsiveness is critical, any delay in data transmission can result in strategic disadvantages and potential mission failures. To overcome these challenges, software-defined radios (SDR) and adaptive frequency management solutions are being explored to optimize bandwidth utilization and maintain continuous connectivity even in contested environments [8], [10].

Interoperability between UAV platforms and TOCs across different military branches and allied forces presents another critical challenge. Joint military operations require seamless data sharing and coordinate efforts among UAVs operated by various defense organizations. However, differences in encryption standards, communication protocols, and data exchange formats often hinder smooth interoperability, leading to delays and inefficiencies in coordinated missions [7], [18]. Standardizing encryption frameworks and establishing unified communication protocols can significantly enhance interoperability, ensuring effective collaboration between UAV assets and TOCs in multinational operations.

To address these critical challenges, this paper proposes a Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC), integrating multi-layered cybersecurity measures, adaptive communication strategies, and robust interoperability solutions. The framework leverages blockchain-based authentication to prevent unauthorized access, ensuring that only verified UAVs and TOCs participate in mission-critical communications. Additionally, quantum-safe encryption protocols are employed to safeguard transmitted data against cyber threats and unauthorized interception, providing long-term security resilience [16], [18]. To counter electronic warfare threats, the proposed framework incorporates frequency-hopping SDR technology, dynamically adjusting communication frequencies to evade jamming and interference attempts [8], [14].

Furthermore, the SCF-UAVTOC framework enhances operational efficiency through AI-powered intrusion detection systems (IDS), which continuously monitor network traffic for anomalies and potential cyber intrusions. AI-driven security algorithms analyze behavioral patterns, detecting and mitigating threats in real time to ensure uninterrupted UAV-to-TOC communication [1], [5], [7]. By implementing cloud-enabled secure data processing, the framework enables seamless intelligence sharing between UAVs and TOCs, optimizing decision-making and mission execution in both military and emergency environments [10].

Another critical aspect of the SCF-UAVTOC model is multi-protocol interoperability, allowing seamless integration of UAV systems within joint military task forces and international coalition operations. By standardizing encryption methodologies, data transmission formats, and communication interfaces, the framework enhances cross-platform collaboration, enabling real-time coordination among diverse UAV assets and TOCs [13], [18]. The proposed framework also includes secure tactical data links that support high-speed, low-latency data exchange, ensuring reliable command-and-control operations in dynamic and contested environments [9], [15].

This paper explores the existing limitations of UAV-to-TOC communication, presents a detailed analysis of the proposed SCF-UAVTOC model, and evaluates its effectiveness through simulation-based performance testing. By integrating cutting-edge security protocols, adaptive

communication mechanisms, and advanced interoperability solutions, the SCF-UAVTOC model aims to revolutionize secure drone communication in military and emergency response operations. The findings of this study will contribute to the ongoing efforts in enhancing secure UAV-to-TOC communication, ensuring mission success, and maintaining strategic superiority in modern warfare and crisis management scenarios [7], [12], [19].

By addressing these fundamental challenges and implementing advanced technological solutions, military organizations and emergency response agencies can strengthen UAV communication security, improve mission reliability, and enhance operational effectiveness in high-risk environments. The adoption of a secure, adaptive, and interoperable UAV-to-TOC communication framework is essential for safeguarding critical intelligence, mitigating security threats, and ensuring the seamless execution of military and crisis operations in the evolving landscape of modern security challenges.

1. Challenges and Solutions in UAV-to-TOC Communication

Ensuring seamless and secure communication between Unmanned Aerial Vehicles (UAVs) and Tactical Operations Centers (TOCs) is critical for modern military and emergency response operations. However, multiple challenges impact the efficiency, security, and interoperability of UAV-to-TOC communication. These challenges include electronic warfare threats, cybersecurity vulnerabilities, bandwidth limitations, and interoperability issues across multinational operations. Addressing these concerns requires the integration of advanced security protocols, adaptive communication technologies, and robust interoperability frameworks. This section explores these challenges and presents viable solutions to enhance UAV-to-TOC communication performance in high-risk environments.

1. Electronic Warfare (EW) Threats and Countermeasures

Electronic warfare (EW) remains one of the most significant threats to UAV-to-TOC communication. Adversaries deploy radio frequency (RF) jamming, spoofing attacks, and signal interception to disrupt drone communication, causing operational failures and potential intelligence leaks [4], [6], [10]. Traditional communication systems, which rely on fixed-frequency channels, are particularly vulnerable to jamming and interference, making UAV operations susceptible to disruption in contested environments.

To counter EW threats, adaptive frequency hopping and software-defined radio (SDR) technology can be integrated into UAV communication systems. SDR-based adaptive frequency allocation allows drones to dynamically switch between frequencies, reducing the likelihood of signal jamming [8], [14]. Additionally, directional antennas and low probability of intercept (LPI) waveforms improve UAV communication resilience by reducing detectability [7], [15].

Table 1. Impact of Electronic Warfare on UAV-to-TOC Communication and Countermeasures

Electronic Warfare Threat	Impact on UAV Communication	Proposed Countermeasures
Jamming	Loss of UAV control, disrupted command execution	Adaptive Frequency Hopping (AFH), SDR-based communication
Spoofing	UAV misdirection, unauthorized control	Encrypted GPS signals, AI-based anomaly detection
Signal Interception	Exposure of classified intelligence	Quantum-safe encryption, encrypted tactical data links

By implementing AI-powered anomaly detection, UAV systems can identify and respond to abnormal communication patterns in real-time, further enhancing resilience against EW threats [5], [9], [12].

2. Cybersecurity Risks and Mitigation Strategies

Cyber threats pose another major challenge in UAV-to-TOC communication, increasing the risk of data breaches, hacking attempts, and denial-of-service (DoS) attacks [11], [17]. UAV networks, particularly those transmitting sensitive military or emergency response data, are prime targets for adversaries attempting to intercept mission-critical intelligence or manipulate drone operations.

To enhance cybersecurity resilience, the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC) integrates blockchain-based authentication, quantum-safe encryption, and real-time intrusion detection systems (IDS) [14], [18]. Blockchain ensures decentralized, tamper-proof authentication, preventing unauthorized access to UAV networks. Quantum-safe encryption techniques protect UAV data from future quantum computing threats, securing UAV-to-TOC communication against evolving cyber threats [16], [20].

Table 2. Cybersecurity Risks in UAV Communication and Solutions

Cyber Threat	Potential Consequences	Mitigation Strategies
Unauthorized Access	Drone hijacking, mission compromise	Blockchain-based authentication, multi-factor authentication
Data Breaches	Exposure of classified mission data	End-to-end encryption, secure cloud storage
Denial-of-Service (DoS) Attacks	Network congestion, disrupted operations	AI-driven traffic filtering, intrusion detection systems

By implementing real-time IDS, UAV systems can detect and neutralize cyber threats before they compromise mission security, ensuring uninterrupted UAV-to-TOC operations [1], [6], [13].

3. Bandwidth and Latency Challenges in UAV-to-TOC Communication

UAVs generate massive volumes of data, including real-time video feeds, sensor outputs, and telemetry information, leading to bandwidth congestion and increased latency in communication [3], [11], [19]. Traditional bandwidth allocation methods struggle to handle high-volume UAV transmissions, causing delays in command execution and intelligence analysis.

To optimize bandwidth usage and reduce latency, UAV communication systems must integrate software-defined networking (SDN) and edge computing. SDN enables dynamic bandwidth allocation, prioritizing mission-critical data while minimizing unnecessary transmissions [8],

[14]. Edge computing allows UAVs to process data locally, reducing reliance on central processing hubs and decreasing latency in decision-making [7], [10].

4. Interoperability Issues in Multi-Nation Military Operations

Interoperability remains a persistent challenge in UAV-to-TOC communication, particularly in joint military operations involving multinational forces. Different nations utilize varying encryption standards, communication protocols, and data formats, complicating seamless integration between UAV platforms and TOCs [6], [18]. The lack of unified communication frameworks results in delays, miscommunication, and security vulnerabilities in joint operations.

To enhance interoperability, military organizations must adopt standardized encryption methodologies and multi-protocol communication interfaces. The NATO STANAG-compliant encryption framework facilitates seamless integration across allied forces, enabling real-time intelligence sharing and coordinated UAV operations [15], [18]. Furthermore, cloud-based secure data sharing platforms allow UAVs to exchange mission-critical information while maintaining high-security standards [10], [17].

5. Proposed Model for Secure UAV-to-TOC Communication

To address the security, interoperability, and efficiency challenges in UAV-to-TOC communication, a Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC) is proposed. This model integrates blockchain authentication, software-defined radios (SDR), quantum-safe encryption, AI-driven intrusion detection, and cloud-based secure data processing to ensure resilient, low-latency, and secure communication between UAVs and TOCs in military and emergency response environments. The framework is designed to counteract electronic warfare (EW) threats, mitigate cyber risks, optimize bandwidth usage, and enhance interoperability across multinational operations [1], [6], [14].

1. Core Components of the SCF-UAVTOC Model

The SCF-UAVTOC model consists of five fundamental components that collectively enhance UAV communication security and efficiency:

1. **Decentralized Authentication and Secure Access Control**
    - Blockchain-based authentication eliminates the risk of unauthorized access by using a decentralized ledger for secure identity verification [5], [12].
    - Multi-factor authentication ensures only authorized UAVs and TOCs can exchange mission-critical data, reducing the threat of UAV hijacking or data breaches [16].
2. **Adaptive Spectrum Management via Software-Defined Radios (SDR)**
    - SDR technology enables real-time frequency hopping, allowing UAVs to dynamically adjust their communication channels to avoid jamming and interference [8], [15].
    - AI-driven adaptive spectrum allocation ensures optimal bandwidth usage, prioritizing mission-critical data transmission while preventing congestion [10].

3. **Quantum-Safe Encryption and Secure Data Transmission**
    - Advanced quantum-resistant cryptographic protocols protect UAV-to-TOC data against potential future decryption threats posed by quantum computing [18].
    - Secure end-to-end encryption ensures data integrity and confidentiality, mitigating the risk of man-in-the-middle (MITM) attacks [7].
4. **AI-Powered Intrusion Detection and Electronic Warfare Countermeasures**
    - AI-driven intrusion detection systems (IDS) continuously monitor UAV network traffic for anomalous behavior, preventing cyber intrusions and unauthorized access attempts [2], [9].
    - AI-enhanced electronic warfare (EW) threat mitigation proactively detects and neutralizes jamming, spoofing, and signal interception attempts [14].
5. **Cloud-Enabled Secure Data Processing and Interoperability Solutions**
    - Secure cloud-based platforms facilitate real-time data sharing between UAVs and TOCs, ensuring seamless intelligence exchange in coalition operations [6], [13].
    - Standardized NATO-compliant encryption and communication protocols improve cross-platform interoperability between multinational forces [18].

2. Workflow of the SCF-UAVTOC Model

The proposed model operates through a structured workflow that ensures security, adaptability, and efficiency in UAV-to-TOC communication. The process consists of five key phases:

1. **Authentication and Secure Link Establishment**
    - UAVs established a secure connection with TOCs using blockchain-based authentication and quantum-safe encryption [12], [16].
    - Each UAV's identity is verified using smart contracts, ensuring only trusted nodes participate in mission-critical communication.
2. **Adaptive Frequency Allocation and Dynamic Spectrum Optimization**
    - SDR-based adaptive frequency management allows UAVs to dynamically switch channels to avoid jamming and optimize bandwidth allocation [8], [14].
    - AI-driven real-time spectrum monitoring detects interference patterns and adjusts communication frequencies accordingly [10].
3. **Real-Time Data Transmission and Secure Command Execution**
    - Secure data packets, including video feeds, telemetry information, and sensor data, are encrypted and transmitted over a low-latency tactical data link [4], [7].
    - AI-based data compression algorithms optimize transmission efficiency, ensuring minimal bandwidth consumption [5].
4. **Cybersecurity Threat Monitoring and EW Countermeasures**
    - AI-powered intrusion detection continuously scans network activity for cyber threats, deploying automated countermeasures to prevent intrusions [2], [9].
    - UAVs use low-probability-of-intercept (LPI) signals and directional antennas to reduce vulnerability to electronic eavesdropping [6], [15].

5. **Post-Mission Data Analysis and Intelligence Sharing**
    - Collected UAV data is securely uploaded to a cloud-based encrypted storage system, ensuring secure archival and post-mission analysis [13].
    - AI-based data analytics refine UAV network configurations, improving future communication efficiency and security [11], [17].

Table 3. Functional Components of the SCF-UAVTOC Model

Component	Function	Expected Benefit
Blockchain Authentication	Decentralized identity verification for UAVs	Prevents unauthorized access and cyber intrusions
SDR Adaptive Frequency	Real-time frequency hopping and interference evasion	Enhances resilience to jamming and EW threats
Quantum-Safe Encryption	Encrypts UAV-TOC data against future quantum threats	Ensures long-term data security and integrity
AI-Powered IDS	Detects cyber intrusions and suspicious network activity	Prevents hacking, spoofing, and data breaches
Cloud-Based Intelligence Sharing	Secure storage and data exchange for multinational forces	Enhances interoperability and real-time collaboration

2.1. Comparative Performance Analysis of the SCF-UAVTOC Model

To evaluate the effectiveness of the SCF-UAVTOC model, its performance is compared against traditional UAV communication frameworks based on key operational metrics.

Table 4. Comparative Analysis of UAV Communication Models

Performance Metric	Traditional UAV Model	Proposed SCF-UAVTOC Model
Authentication Method	Centralized password-based authentication	Blockchain-based decentralized authentication
EW Resilience	Fixed frequency, vulnerable to jamming	AI-driven SDR adaptive frequency hopping

Data Encryption	Standard AES encryption	Quantum-safe encryption
Intrusion Detection	Basic firewall protection	AI-powered real-time IDS
Interoperability	Limited cross-platform integration	NATO-compliant standardized communication
Bandwidth Optimization	Manual prioritization	AI-driven traffic management

2.2. Strategic Advantages of the SCF-UAVTOC Model

By implementing the SCF-UAVTOC model, military and emergency response teams gain several strategic advantages:

- **Enhanced Communication Security**: The combination of blockchain authentication, quantum-safe encryption, and AI-driven IDS significantly enhances cybersecurity resilience [5], [10].
- **Resilience Against EW Threats**: Adaptive frequency hopping and SDR-based spectrum management mitigate the impact of jamming and spoofing attacks [8], [14].
- **Real-Time Decision-Making**: Secure low-latency tactical data links ensure that TOCs receive timely mission intelligence, improving operational response times [6], [13].
- **Interoperability in Multinational Operations**: Standardized encryption and cloud-based secure data sharing facilitate seamless UAV collaboration among allied forces [18].

Conclusion

Ensuring secure and resilient UAV-to-TOC communication is critical for military and emergency response operations. Traditional UAV communication frameworks face electronic warfare threats, cybersecurity vulnerabilities, bandwidth limitations, and interoperability challenges, all of which compromise mission effectiveness. To address these issues, this paper proposed the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC), a comprehensive model that integrates blockchain authentication, adaptive frequency management, quantum-safe encryption, AI-driven intrusion detection, and cloud-enabled intelligence sharing.

The SCF-UAVTOC model significantly enhances electronic warfare resilience by employing software-defined radios (SDR) and adaptive frequency hopping, reducing the impact of jamming and interference. Cybersecurity threats are mitigated through decentralized authentication, intrusion detection systems (IDS), and end-to-end encryption, ensuring data integrity and mission confidentiality. Furthermore, cloud-based secure data processing and NATO-compliant encryption standards enable seamless interoperability across multinational forces, improving real-time intelligence exchange and coalition mission coordination.

The comparative analysis demonstrated that the SCF-UAVTOC model outperforms traditional UAV communication frameworks by offering superior resilience, security, and operational

efficiency. Its ability to dynamically adapt to cyber and EW threats, optimize bandwidth usage, and facilitate secure, low-latency data transmission makes it a transformative solution for UAV communication in high-risk environments.

Future research should focus on real-world field testing, hardware integration, and large-scale implementation of the SCF-UAVTOC model to further validate its effectiveness. By adopting this model, military forces and emergency response agencies can enhance mission success, safeguard critical intelligence, and maintain strategic superiority in evolving warfare and crisis scenarios. Implementing secure, adaptive, and interoperable UAV-to-TOC communication is essential for maintaining dominance in modern operational landscapes.

References

[1] Alotaibi, Ahad / Chatwin, Chris / Birch, Phil: A Secure Communication Framework for Drone Swarms in Autonomous Surveillance Operations. *Journal of Computer and Communications*, 2024, pp. 1–25.

[2] Bedford, John C. / Davis, Sandra / Levis, Alexander H.: *The Limitless Sky: Air Force Science and Technology Contributions to the Nation*. Air Force History and Museums Program, 2004.

[3] Duguma, Daniel Gerbi / Astillo, Philip Virgil / Kim, Jiyoon / Ko, Yongho / Pau, Giovanni / You, Ilsun: Drone Secure Communication Protocol for Future Sensitive Applications in Military Zones. *Sensors*, 2021, 21, 2057, pp. 1–25.

[4] Frater, Michael / Ryan, Michael: *Communications Electronic Warfare and the Digitized Battlefield*. Land Warfare Studies Centre, 2001.

[5] Friesendorf, Cornelius (Ed.): *Strategies Against Human Trafficking: The Role of the Security Sector*. National Defence Academy & Austrian Ministry of Defence and Sports, Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2009.

[6] Gao, Jing: Analysis of Military Application of Software Radio Communication Technology. *Operation Software and Simulation Research Institute of Dalian Naval Academy, China*, 2019.

[7] Hammons, Terry: Future Tactical Communications Networks: Challenges and Opportunities. *U.S. Army Research Laboratory*, 2004.

[8] Ko, Yongho / Kim, Jiyoon / Duguma, Daniel Gerbi / Astillo, Philip Virgil / You, Ilsun / Pau, Giovanni: Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone. *Sensors*, 2021, 21, 2057, pp. 1–25.

[9] Kravaica, Tomislav: *Advanced Military Communications: Strategies for the Next Generation*. NATO Research Report, 2020.

[10] Levis, Alexander H. / Bedford, John C. / Davis, Sandra: The Limitless Sky: Air Force Science and Technology Contributions to the Nation. *Air Force History and Museums Program*, 2004.

[11] Marine Corps Combat Development Command (MCRP 5-12A): *Operational Terms and Graphics*. Department of the Army, 2004.

[12] Mustafovski, Rexhep: The Security Vulnerabilities and Challenges on the IoT Technologies. 2024.

[13] NATO Science & Technology Organization: Resilient and Adaptive Battlefield Communications: The Path Forward. *NATO Technical Report*, 2023.

[14] Ouadah, Meriem / Merazka, Fatiha: Securing UAV Communication: Authentication and Integrity. *IEEE Conference on Telecommunications and UAV Security*, 2024, pp. 1–10.

[15] Ryan, Michael / Frater, Michael: *Electronic Warfare for the Digitized Battlefield*. Artech House, 2001.

[16] U.S. Army: *Army Unmanned Aircraft System Operations* (FMI 3-04.155). *Department of the Army*, 2006.

[17] U.S. Department of Defense: Military Communication Systems Study: Battlefield Networking and Secure Tactical Radio Systems. *Department of Defense*, 2018.

[18] U.S. Defense Advanced Research Projects Agency (DARPA): Quantum-Safe Encryption for Military Networks. *DARPA Technical Report*, 2024.

[19] U.S. Joint Forces Command: Military Satellite Communications: Current Capabilities and Future Developments. *Department of Defense*, 2024.

[20] U.S. Marine Corps: *Operational Terms and Graphics (MCRP 5-12A). Department of the Navy*, 2004.