GOCE DELCEV UNIVERSITY, STIP, NORTH MACEDONIA

FACULTY OF ELECTRICAL ENGINEERING

ETIMA 2025

THIRD INTERNATIONAL CONFERENCE

24-25 SEPTEMBER, 2025

TECHNICAL SCIENCES APPLIED IN ECONOMY, EDUCATION AND INDUSTRY

УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“, ШТИП
ЕЛЕКТРОТЕХНИЧКИ ФАКУЛТЕТ

GOCE DELCEV UNIVERSITY, STIP
FACULTY OF ELECTRICAL ENGINEERING

ТРЕТА МЕЃУНАРОДНА КОНФЕРЕНЦИЈА
THIRD INTERNATIONAL CONFERENCE

ЕТИМА / ETIMA 2025

ЗБОРНИК НА ТРУДОВИ
CONFERENCE PROCEEDINGS

24-25 септември 2025 | 24-25 September 2025

ISBN: 978-608-277-128-1
DOI: https://www.doi.org/10.46763/ETIMA2531

Главен и одговорен уредник / Editor in Chief
проф.д-р Сашо Гелев
Prof.d-r Saso Gelev

Јазично уредување / Language Editor
Весна Ристова (македонски) / Vesna Ristova (Macedonian)

Техничко уредување / Technical Editing
Дарко Богатинов / Darko Bogatinov

Издавач / Publisher
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering

Адреса на организационен комитет / Adress of the organizational committee
Универзитет „Гоце Делчев", Штип / Goce Delcev University, Stip
Електротехнички факултет / Faculty of Electrical Engineering
Адреса: ул. „Крсте Мисирков" бр. 10А / Adress: Krste Misirkov, 10A
Пош. фах 201, Штип - 2000, С. Македонија / PO BOX 201, Stip 2000, North Macedonia
E-mail: conf.etf@ugd.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

62-049.8(062)
004-049.8(062)

МЕЃУНАРОДНА конференција ЕТИМА (3 ; 2025 ; Штип)
Зборник на трудови [Електронски извор] / Трета меѓународна конференција ЕТИМА 2025, 24-25 септември 2025 ; [главен и одговорен уредник Сашо Гелев] = Conference proceedings / Third international conference, 24-25 September 2025 ; [editor in chief Saso Gelev]. - Текст во PDF формат, содржи 357 стр., илустр. - Штип : Универзитет "Гоце Делчев", Електротехнички факултет ; Stip : "Goce Delchev" University, Faculty of Electrical engineering, 2025

Начин на пристапување (URL): https://js.ugd.edu.mk/index.php/etima/en. - Наслов преземен од екранот. - Опис на изворот на ден 30.10.2025. - Трудови на мак. и англ. јазик. - Библиографија кон трудовите

ISBN 978-608-277-128-1

а) Електротехника -- Примена -- Собири б) Машинство -- Примена -- Собири
в) Автоматика -- Примена -- Собири г) Инфоматика -- Примена -- Собири

COBISS.MK-ID 67297029

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ОРГАНИЗАЦИОНЕН ОДБОР
ORGANIZING COMMITTEE

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Маја Кукушева Панева / Maja Kukuseva Paneva
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Дарко Богатинов / Darko Bogatinov
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Трета меѓународна конференција ЕТИМА
24-25 Септември 2025
Third International Conference ETIMA
24-25 September 2025

ПРОГРАМСКИ И НАУЧЕН ОДБОР
SCIENTIFIC COMMITTEE

Георги Иванов Георгиев / Georgi Ivanov Georgiev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Антон Белан / Anton Beláň
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Ивелина Стефанова Балабанова / Ivelina Stefanova Balabanova
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Бојан Димитров Карапенев / Boyan Dimitrov Karapenev
Технички Универзитет во Габрово, Бугарија
Technical University in Gabrovo, Bulgaria

Сашо Гелев / Saso Gelev
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Влатко Чингоски / Vlatko Cingoski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Божо Крстајиќ / Bozo Krstajic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Милован Радуловиќ / Milovan Radulovic
Електротехнички факултет
Универзитет во Црна Гора, Црна Гора
Faculty of Electrical Engineering,
University in Montenegro, Montenegro

Гоце Стефанов / Goce Stefanov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирјана Периќ / Mirjana Peric
Електронски факултет
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Ана Вучковиќ / Ana Vuckovic
Електронски факултет,
Универзитет во Ниш, Србија
Faculty of Electronic Engineerig,
University of Nis, Serbia

Тодор Чекеровски / Todor Cekerovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Далибор Серафимовски / Dalibor Serafimovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Мирослава Фаркаш Смиткова / Miroslava Farkas Smitková
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Петер Јанига / Peter Janiga
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Јана Радичова / Jana Raditschová
Факултет за електротехника и информациони технологии
Словачки Технички Универзитет во Братислава, Словачка
Faculty of Electrical Engineering and Information Technology
Slovak Technical University in Bratislava, Slovakia

Драган Миновски / Dragan Minovski
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Василија Шарац / Vasilija Sarac
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Александар Туџаров / Aleksandar Tudzarov
Електротехнички факултет,
Универзитет „Гоце Делчев", Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владимир Талевски / Vladimir Talevski
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Владо Гичев / Vlado Gicev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Марија Чекеровска / Marija Cekerovska
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Мишко Џидров / Misko Dzidrov
Машински факултет,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Mechanical Engineering,
Goce Delcev University, Stip, North Macedonia;

Александар Крстев / Aleksandar Krstev
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ванчо Аџиски / Vancho Adziski
Факултет за природни и технички науки,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Natural and Technical Sciences,
Goce Delcev University, Stip, North Macedonia;

Томе Димовски / Tome Dimovski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Зоран Котевски / Zoran Kotevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Никола Рендевски / Nikola Rendevski
Факултет за информатички и комуникациски технологии,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Information and Communication Technologies,
University St Climent Ohridski, North Macedonia;

Илија Христовски / Ilija Hristovski
Економски факултет,
Универзитет „Св. Климент Охридски “, Северна Македонија;
Faculty of Economy,
University St Climent Ohridski, North Macedonia;

Христина Спасовска / Hristina Spasovska
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Роман Голубовски / Roman Golubovski
Природно-математички факултет,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Mathematics and Natural Sciences,
Ss. Cyril and Methodius University, North Macedonia;

Маре Србиновска / Mare Srbinovska
Факултет за електротехника и информациски технологии,
Универзитет „Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Златановска / Biljana Zlatanovska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Александра Стојанова Илиевска / Aleksandra Stojanova Ilievska
Факултет за информатика,
Универзитет „Гоце Делчев “, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Мирјана Коцалева Витанова / Mirjana Kocaleva Vitanova
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

Ивана Сандева / Ivana Sandeva
Факултет за електротехника и информациски технологии,
Универзитет „ Св. Кирил и Методиј “, Скопје, Северна Македонија;
Faculty of Electrical Engineering and Information Technologies,
Ss. Cyril and Methodius University, North Macedonia;

Билјана Читкушева Димитровска / Biljana Citkuseva Dimitrovska
Електротехнички факултет,
Универзитет „Гоце Делчев”, Штип, Северна Македонија
Faculty of Electrical Engineering,
Goce Delcev University, Stip, North Macedonia

Наташа Стојковиќ / Natasa Stojkovik
Факултет за информатика,
Универзитет „Гоце Делчев“, Штип, Северна Македонија;
Faculty of Computer Science,
Goce Delcev University, Stip, North Macedonia;

PREFACE

The Third International Conference “Electrical Engineering, Technology, Informatics, Mechanical Engineering and Automation – Technical Sciences in the Service of the Economy, Education and Industry” (ETIMA’25), organized by the Faculty of Electrical Engineering at the “Goce Delchev” University – Shtip, represents a significant scientific event that enables interdisciplinary exchange of knowledge and experience among researchers, professors, and experts in the field of technical sciences. The conference was held in an online format and brought together 78 authors from five different countries.

The ETIMA conference aims to establish a forum for scientific communication, encouraging multidisciplinary collaboration and promoting technological innovations with direct impact on modern life. Through the presentation of scientific papers, participants shared the results of their research and development activities, contributing to the advancement of knowledge and practice in relevant fields.
The first ETIMA conference was organized four years ago, featuring 40 scientific papers. The second conference took place in 2023 and included over 30 papers. ETIMA’25 continued this scientific tradition, presenting more than 40 papers that reflect the latest achievements in electrical engineering, technology, informatics, mechanical engineering, and automation.

At ETIMA’25, papers were presented that addressed current topics in technical sciences, with particular emphasis on their application in industry, education, and the economy. The conference facilitated fruitful discussions among participants, encouraging new ideas and initiatives for future research and projects.

ETIMA’25 reaffirmed its role as an important platform for scientific exchange and international cooperation. The organizing committee extends sincere gratitude to all participants for their contribution to the successful realization of the conference and its scientific value.

We extend our sincerest gratitude to all colleagues who, through the presentation of their papers, ideas, and active engagement in discussions, contributed to the success and scientific significance of ETIMA’25.

The Organizing Committee of the Conference

ПРЕДГОВОР

Третата меѓународна конференција „Електротехника, Технологија, Информатика, Машинство и Автоматика – технички науки во служба на економијата, образованието и индустријата“ (ЕТИМА’25), организирана од Електротехничкиот факултет при Универзитетот „Гоце Делчев“ – Штип, претставува значаен научен настан кој овозможува интердисциплинарна размена на знаења и искуства меѓу истражувачи, професори и експерти од техничките науки. Конференцијата се одржа во онлајн формат и обедини 78 автори од пет различни земји.

Конференцијата ЕТИМА има за цел да создаде форум за научна комуникација, поттикнувајќи мултидисциплинарна соработка и промовирајќи технолошки иновации со директно влијание врз современото живеење. Преку презентација на научни трудови, учесниците ги споделуваат резултатите од своите истражувања и развојни активности, придонесувајќи кон унапредување на знаењето и практиката во релевантните области.

Првата конференција ЕТИМА беше организирана пред четири години, при што беа презентирани 40 научни трудови. Втората конференција се одржа во 2023 година и вклучи над 30 трудови. ЕТИМА’25 продолжи со истата научна традиција, презентирајќи повеќе од 40 трудови кои ги отсликуваат најновите достигнувања во областа на електротехниката, технологијата, информатиката, машинството и автоматиката.

На ЕТИМА’25 беа презентирани трудови кои обработуваат актуелни теми од техничките науки, со посебен акцент на нивната примена во индустријата, образованието и економијата. Конференцијата овозможи плодна дискусија меѓу учесниците, поттикнувајќи нови идеи и иницијативи за идни истражувања и проекти.

ЕТИМА’25 ја потврди својата улога како значајна платформа за научна размена и интернационална соработка. Организациониот одбор упатува искрена благодарност до сите учесници за нивниот придонес кон успешната реализација на конференцијата и нејзината научна вредност. Конференцијата се одржа онлајн и обедини седумдесет и осум автори од пет различни земји.

Изразуваме голема благодарност до сите колеги кои со презентирање на своите трудови, идеи и активна вклученост во дискусиите придонесоа за успехот на ЕТИМА’25 и нејзината научна вредност.

Организационен одбор на конференцијата

СОДРЖИНА / TABLE OF CONTENTS:

Трета меѓународна конференција ЕТИМА
Third International Conference ETIMA
UDC: 629.7.014.0:[355.5:621.39]
https://www.doi.org/10.46763/ETIMA2531148m

CHALLENGES AND SOLUTIONS FOR ENHANCING DRONE-TO-TOC COMMUNICATION PERFORMANCE IN MILITARY AND CRISIS OPERATIONS

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

Drone-to-TOC (Tactical Operations Center) communication is increasingly essential for military and crisis management operations, offering significant advantages in operational flexibility, real-time situational awareness, and rapid response capabilities. However, these advancements introduce numerous technical and operational challenges that must be addressed to fully exploit the benefits of drone communication. This paper provides a comprehensive analysis of the current challenges facing drone-to-TOC communications, including vulnerabilities to electronic warfare, cyber threats, interoperability issues, and bandwidth limitations. Electronic warfare, such as jamming and spoofing, significantly affects the reliability of UAV communication systems, demanding resilient, adaptive solutions. Cybersecurity threats further complicated secure data transmission, creating a need for advanced encryption, robust authentication protocols, and secure communication frameworks. Interoperability among multinational forces remains a persistent challenge due to varying encryption standards, data-sharing protocols, and differing technological platforms. Additionally, managing the increasing data volume and ensuring low latency transmission are critical concerns for maintaining seamless communication. Drawing on the latest developments from tactical radio networks, advanced military communications strategies, quantum-safe encryption technologies, and AI-driven cybersecurity measures, this paper proposes a set of solutions aimed at enhancing drone-to-TOC communication performance. Recommendations include implementing adaptive software-defined radios, integrating decentralized security mechanisms, and developing unified interoperability standards. These approaches aim to strengthen operational effectiveness, cybersecurity resilience, and reliability of drone communications during critical military and crisis management scenarios.

Key words:

Adaptive Communication, Bandwidth Optimization, Decentralized Networks, Drone-to-TOC Communication.

Introduction

The effectiveness of military and crisis management operations depends significantly on secure, reliable, and resilient communication systems. As modern warfare shifts towards greater digitization and network-centric capabilities, the role of drones and their integration into Tactical Operations Centers (TOC) has emerged as crucial for achieving strategic operational superiority. The ability to reliably transmit real-time information from drones directly to TOCs across operational domains—land, air, sea, space, and cyberspace—has evolved into a strategic imperative. Advanced military communication systems now integrate state-of-the-art radio networks, encrypted data exchanges, and satellite-based platforms, providing seamless coordination between command structures and deployed operational units [4], [6], [9].

The proliferation of Unmanned Aerial Vehicles (UAVs) has notably reshaped battlefield communications. UAV swarms enable enhanced situational awareness, precise targeting, and agile operations, particularly critical during rapidly changing scenarios. Their capability to relay real-time intelligence, surveillance, and reconnaissance (ISR) data back to the command centers significantly reduces response times and enhances decision-making efficiency [1], [7], [10]. Despite these capabilities, drone-to-TOC communication faces numerous technical, operational, and cybersecurity challenges.

Electronic warfare presents significant vulnerabilities to UAV communications, introducing risks such as jamming, spoofing, and interference. These risks can disrupt critical drone missions and compromise overall operational effectiveness [4], [14]. The rise in electronic threats requires communication systems to adopt resilient strategies such as dynamic frequency allocation, adaptive modulation schemes, and agile spectrum management approaches [6], [14]. Additionally, cybersecurity threats have become increasingly prevalent and sophisticated, presenting substantial risks for drone-to-TOC communication platforms. The security of data transmitted between UAVs and TOCs demands robust protection through advanced encryption and blockchain-based decentralized authentication methods [12], [16]. Quantum-safe encryption technologies, now being explored and implemented, promise significant enhancements to drone communication security, providing resilience against future quantum computing threats [16].

Interoperability between multinational military forces poses another major challenge for drone-to-TOC communication. Joint and coalition operations rely heavily on unified communication standards and compatible encryption protocols. However, differing national standards, encryption practices, and data-sharing policies often complicate effective communication and information exchange [7], [17]. This challenge underscores the need for universal or widely accepted interoperability standards and protocols, allowing seamless integration of UAV systems across multiple coalition partners [17].

The large-scale deployment of UAV swarms further exacerbates bandwidth and latency challenges. Traditional military communication infrastructures often struggle to handle the significant volume of real-time data transmitted from UAVs, resulting in congestion and potentially delayed decision-making [6], [11]. The necessity for real-time responsiveness mandates the implementation of advanced, high-bandwidth communication systems that can effectively support extensive drone operations. Emerging technologies such as software-defined radios (SDRs) offer promising solutions by dynamically managing bandwidth allocation and optimizing data flows [8], [10].

Addressing these challenges requires strategic investment, comprehensive technological upgrades, and proactive regulatory frameworks. Military organizations and governments must foster an environment conducive to continuous innovation, technological advancements, and the implementation of cutting-edge communication solutions. Collaborative research and development initiatives focusing on adaptive communication methods, cybersecurity resilience, and interoperability solutions are essential to overcoming the current limitations and future-proofing drone-to-TOC communication systems [7], [10], [13].

This paper explores the existing landscape of drone-to-TOC communication, analyzing critical challenges and proposing strategic solutions. Drawing from a comprehensive review of military communication infrastructures, tactical radio networks, electronic warfare environments, and cybersecurity frameworks, the study provides insights that aim to enhance communication efficiency, security, and resilience in future military and crisis management operations. The proposed solutions include the integration of adaptive frequency allocation via SDR, robust quantum-safe encryption, decentralized authentication mechanisms, and the establishment of unified standards for multinational interoperability [7], [9], [14], [16]. Ultimately, by addressing

the outlined challenges and implementing recommended solutions, drone-to-TOC communication platforms can significantly enhance military capability, strengthen situational awareness, and ensure operational effectiveness in the rapidly evolving landscape of modern warfare and crisis response scenarios.

1. Challenges in Drone-to-TOC Communication and Proposed Solutions

Drone-to-Tactical Operations Center (TOC) communication is integral to modern military operations and crisis management, enabling real-time intelligence sharing, operational coordination, and situational awareness. However, ensuring secure, reliable, and efficient communication remains a significant challenge due to a variety of factors, including electronic warfare threats, cybersecurity vulnerabilities, bandwidth limitations, and interoperability constraints. This section provides a detailed analysis of these challenges, along with proposed solutions to enhance the effectiveness of drone-to-TOC communication.

1. Electronic Warfare Vulnerabilities

One of the primary threats to drone-to-TOC communication is electronic warfare (EW), which encompasses jamming, spoofing, and signal interception techniques used by adversaries to disrupt UAV operations.

- **Jamming:** Adversaries use radio frequency (RF) jamming techniques to block communication signals between drones and TOCs. This can lead to loss of control over UAVs, disrupting mission objectives and compromising intelligence collection [4], [6].
- **Spoofing:** Attackers can transmit false signals to deceive the drone's navigation and communication systems, leading to UAV misdirection or capture [14], [16]. This is particularly concerning GPS-based UAV navigation.
- **Signal Interception:** Unsecured UAV communication channels are susceptible to eavesdropping, enabling adversaries to gather classified intelligence and counter UAV operations [7], [15].

Proposed Solutions for EW Countermeasures

To mitigate the risks posed by electronic warfare, several defensive strategies can be employed:

- **Adaptive Frequency Hopping (AFH):** Using Software-Defined Radios (SDRs) to dynamically switch frequencies and avoid jamming attempts [8], [14].
- **Anti-Jamming Antennas:** Directional and phased-array antennas reduce susceptibility to jamming by focusing transmission in secure directions [10].
- **Encrypted Communication Channels:** Ensuring that all drone-to-TOC communications are secured using advanced cryptographic techniques reduces interception risks [6], [12].
- **Artificial Intelligence-based Threat Detection:** AI-driven threat monitoring systems can identify and counteract jamming and spoofing attempts in real time [1], [5].

Table 1. Impact of Electronic Warfare on Drone-to-TOC Communication

Electronic Warfare Threat	Impact on UAV Operations	Proposed Mitigation Strategy

Jamming	Communication loss, mission failure	Adaptive Frequency Hopping (AFH), AI-based detection
Spoofing	UAV misdirection, unauthorized control	GPS authentication, encrypted signals
Signal Interception	Classified data leaks, compromised operations	End-to-end encryption, secure transmission protocols

2. Cybersecurity Threats in Drone Communication

UAV communication systems are prime targets for cyber-attacks, which can result in unauthorized access, data manipulation, and drone hijacking. The following cybersecurity challenges impact drone-to-TOC communication:

- **Unauthorized Access:** Weak authentication mechanisms can allow adversaries to take control of UAVs or manipulate their data streams [9], [16].
- **Data Integrity Attacks:** Attackers may alter mission-critical data, resulting in incorrect situational assessments and misguided operational decisions [7].
- **Denial-of-Service (DoS) Attacks:** Adversaries can flood UAV communication channels with excessive traffic, disrupting connectivity between drones and TOCs [3], [11].

Proposed Solutions for Cybersecurity Enhancement

To safeguard drone communication networks, a multi-layered cybersecurity approach is necessary:

- **Blockchain-based Authentication:** Decentralized authentication mechanisms prevent unauthorized access and ensure data integrity [12].
- **Quantum-Safe Encryption:** Advanced encryption techniques protect drone transmissions against future quantum computing threats [16].
- **Intrusion Detection Systems (IDS):** AI-powered IDS continuously monitor UAV networks for signs of cyber threats and anomalies [1], [7].
- **Secure Cloud Integration:** Ensuring that UAV data is securely stored and transmitted via encrypted cloud platforms prevents unauthorized interception [10].

Table 2. Cybersecurity Risks and Countermeasures in Drone Communication

Cybersecurity Threat	Potential Consequences	Mitigation Strategy
Unauthorized Access	Drone hijacking, loss of mission control	Blockchain-based authentication, multi-factor authentication
Data Integrity Attacks	False intelligence, misinformed command decisions	Quantum-safe encryption, real-time validation protocols
Denial-of-Service Attacks	Communication failure, delayed response times	AI-driven intrusion detection, traffic filtering

3. Bandwidth and Latency Constraints

The high volume of real-time data transmission required for UAV operations places significant strain on available bandwidth, particularly in large-scale drone deployments. Bandwidth limitations lead to:

- **Network Congestion:** As multiple UAVs transmit ISR (Intelligence, Surveillance, and Reconnaissance) data, networks become overwhelmed, causing delays in data processing [6], [11].
- **Increased Latency:** Delayed communication between UAVs and TOCs reduces real-time responsiveness, which is critical for dynamic military operations [5], [8].

Proposed Solutions for Bandwidth Optimization

To optimize bandwidth usage and reduce latency, the following measures should be implemented:

- **Software-Defined Networking (SDN):** SDN enables efficient traffic management and prioritization of mission-critical data [8], [13].
- **Edge Computing for UAVs:** Processing data closer to the source (onboard drones) reduces reliance on centralized data centers, decreasing transmission delays [3].
- **Compressed Data Transmission:** Using optimized compression algorithms minimizes bandwidth consumption without compromising data quality [5].

4. Interoperability Challenges in Multi-Nation Operations

Military coalitions and joint task forces often use varying communication standards, encryption protocols, and frequency bands, leading to interoperability issues. These discrepancies:

- **Limit Real-Time Coordination:** Differing data formats and protocols hinders seamless information exchange between allied forces [7], [17].
- **Increase Security Risks:** Inconsistent encryption standards may expose sensitive mission data to unauthorized parties [6].

Proposed Solutions for Enhanced Interoperability

- **Unified Communication Standards:** Establishing NATO-compliant protocols ensures seamless integration across allied forces [17].
- **Standardized Encryption Frameworks:** Ensuring all coalition partners utilize a common encryption methodology enhances secure information exchange [6].
- **Cloud-Based Data Sharing Platforms:** Secure, encrypted cloud systems enable real-time intelligence sharing across multi-national forces [10].

2. Proposed Model for Secure and Efficient Drone-to-TOC Communication

To address the challenges in drone-to-TOC communication, a Secure and Efficient Drone-to-TOC Communication Model (SEDCOM) is proposed. This model integrates multiple layers of security, adaptive communication strategies, and efficient bandwidth utilization methods to enhance real-time data exchange, cybersecurity, and resilience against electronic warfare

threats. The proposed model is designed to operate in highly dynamic and contested military environments, ensuring uninterrupted and secure communication.

1. Key Components of the SEDCOM Model

The SEDCOM model is based on the following core components:

- **Decentralized Authentication Mechanism:** Utilizing blockchain-based authentication to prevent unauthorized access to the UAV communication network.
- **Software-Defined Radio (SDR) with Adaptive Frequency Management:** Enhancing resilience to jamming by dynamically switching communication frequencies.
- **Quantum-Safe Encryption:** Implementing encryption mechanisms resistant to quantum computing threats to secure UAV transmissions.
- **AI-Driven Intrusion Detection System (IDS):** Continuously monitoring UAV communication networks for anomalies and cyber threats.
- **Multi-Layered Communication Architecture:** Integrating satellite, radio, and tactical data links to ensure robust connectivity under various operational conditions.
- **Cloud-Enabled Data Processing:** Utilizing secure cloud platforms to facilitate real-time intelligence sharing and mission planning.

2. Workflow of the SEDCOM Model

The SEDCOM model follows a structured workflow to ensure seamless and secure drone-to-TOC communication. The process is divided into five key phases:

1. **Authentication and Secure Connection Establishment**
    - Each UAV in the swarm undergoes blockchain-based authentication before gaining access to the communication network.
    - A decentralized ledger ensures that only authorized entities can communicate within the network.
    - Quantum-safe encryption is applied to all data exchanges between drones and TOCs.
2. **Adaptive Frequency Allocation and Spectrum Optimization**
    - SDR technology dynamically scans the electromagnetic spectrum for interference.
    - AI-driven algorithms adjust frequency usage to avoid jamming attempts and optimize bandwidth.
    - Multi-path communication ensures redundancy, maintaining connectivity even if some links are compromised.
3. **Real-Time Data Transmission and Command Execution**
    - Encrypted telemetry, video feeds, and sensor data are transmitted securely to the TOC.
    - TOC operators issue commands via secure tactical radio and satellite communication links.
    - AI-powered data compression algorithms optimize bandwidth consumption, ensuring high-speed data transfer.
4. **Cybersecurity Monitoring and Threat Mitigation**
    - AI-driven IDS continuously scans for intrusion attempts, malware, and unauthorized access.
    - Anomaly detection mechanisms flag suspicious activities, allowing real-time countermeasures.

- Cyber threat intelligence (CTI) feeds provide predictive insights into potential attack vectors.

5. **Post-Mission Data Analysis and System Optimization**
   - UAVs transmit mission logs to a secure cloud-based storage system for post-mission analysis.
   - Machine learning algorithms analyze communication patterns to improve future deployments.
   - Network configurations and security policies are updated dynamically based on the latest threat intelligence.

Table 3. Key Functional Components of the SEDCOM Model

Component	Function	Expected Benefit
Blockchain-Based Authentication	Decentralized identity verification for UAVs	Prevents unauthorized access and reduces risk of hijacking
Software-Defined Radio (SDR)	Adaptive frequency selection and interference mitigation	Enhances resistance to jamming and EW threats
Quantum-Safe Encryption	Advanced encryption algorithms resistant to quantum attacks	Ensures long-term confidentiality of mission-critical data
AI-Powered IDS	Real-time anomaly detection and cyber threat monitoring	Proactively prevents cyber intrusions and network disruptions
Multi-Layered Communication	Integration of satellite, tactical radio, and mesh networks	Provides redundancy and ensures continuous connectivity
Cloud-Enabled Data Processing	Secure cloud-based storage and analysis	Enhances intelligence sharing and operational efficiency

2.1. Comparative Analysis of SEDCOM vs. Traditional UAV Communication Models

To evaluate the effectiveness of the SEDCOM model, it is compared against traditional UAV communication models. The comparison is based on key performance metrics such as security, reliability, and adaptability to dynamic environments.

Table 4. Comparative Analysis of UAV Communication Models

Feature	Traditional UAV Model	Proposed SEDCOM Model
Authentication Mechanism	Centralized password-based authentication	Blockchain-based decentralized authentication
Frequency Management	Fixed frequency allocation, vulnerable to jamming	AI-driven adaptive frequency allocation
Encryption Standard	Traditional AES encryption	Quantum-safe encryption

Intrusion Detection	Basic firewall protection	AI-powered real-time intrusion detection system
Network Architecture	Hierarchical, single-point failure risk	Decentralized mesh network with multi-layered communication

2.2. Implementation and Testing Considerations

To ensure the practical deployment of the SEDCOM model in military and crisis management operations, a series of implementation and testing considerations must be addressed:

- **Simulation-Based Performance Evaluation:** The model should be tested under simulated electronic warfare and cyber-attack scenarios to validate its robustness.
- **Field Deployment in Tactical Exercises:** UAV swarms should be integrated into real-world military exercises to assess operational effectiveness.
- **Interoperability with Existing Systems:** Compatibility testing with NATO and allied force communication infrastructures is necessary to ensure seamless integration.
- **Scalability and Futureproofing:** The model should be adaptable to accommodate advancements in quantum computing, AI-driven threat detection, and emerging tactical network technologies.

2.3. Strategic Benefits of Implementing SEDCOM

The deployment of the SEDCOM model in military and crisis response operations provides several strategic advantages:

- **Enhanced Communication Security:** The integration of blockchain and quantum-safe encryption ensures robust security against cyber threats and unauthorized access.
- **Resilience Against Electronic Warfare:** Adaptive frequency hopping and AI-driven interference mitigation enhance the model's resistance to jamming and spoofing.
- **Real-Time Decision-Making:** Low-latency, high-bandwidth communication ensures that commanders receive timely intelligence to make informed strategic decisions.
- **Operational Flexibility:** The decentralized nature of the communication framework allows UAVs to operate autonomously in contested environments with minimal reliance on central infrastructure.
- **Future-Proof Architecture:** The modular design of SEDCOM ensures compatibility with emerging technologies, including AI-based threat prediction and next-generation communication protocols.

Conclusion

The increasing reliance on UAVs for military operations and crisis management highlights the critical need for secure, resilient, and efficient drone-to-TOC communication. However, significant challenges, including electronic warfare threats, cybersecurity vulnerabilities, bandwidth limitations, and interoperability constraints, hinder seamless data transmission and mission effectiveness. Addressing these challenges requires an advanced communication framework that ensures real-time, secure, and adaptable operations in contested environments. The proposed Secure and Efficient Drone-to-TOC Communication Model (SEDCOM) introduces a multi-layered approach that integrates blockchain-based authentication, software-defined radios (SDRs) with adaptive frequency management, quantum-safe encryption, AI-powered intrusion detection systems, and cloud-enabled data processing. By leveraging these

advanced technologies, SEDCOM significantly enhances communication security, mitigates electronic warfare risks, optimizes bandwidth utilization, and ensures interoperability among coalition forces.

Comparative analysis demonstrates that the SEDCOM model outperforms traditional UAV communication systems by providing real-time threat mitigation, decentralized security mechanisms, and enhanced operational resilience. Its adaptive architecture ensures uninterrupted connectivity, even in heavily contested environments where traditional communication networks would be compromised. Additionally, its ability to scale and integrate with future AI-driven and quantum-resistant technologies ensures long-term viability and operational superiority.

Implementing the SEDCOM model can revolutionize drone-to-TOC communication by ensuring data integrity, mission continuity, and tactical advantages in military and crisis operations. By adopting this model, defense organizations can strengthen national security, improve situational awareness, and enhance command efficiency, ensuring that UAVs remain a formidable asset in modern warfare and emergency response scenarios. Future research should focus on real-world deployment testing and further integration with evolving tactical network technologies to maximize operational effectiveness.

References

[1] Ali, Atif / Changazi, Sabir Ali / Jadoon, Yasir Khan / Qasim, Muhammad: *Military Operations: Wireless Sensor Networks Based Applications to Reinforce Future Battlefield Command System*. IEEE, 2020.

[2] Cotton, Simon L. / Scanlon, William G. / Madahar, Bhopinder K.: *Millimeter-Wave Soldier-to-Soldier Communications for Covert Battlefield Operations*. IEEE Communications Magazine, 2009.

[3] Demori, André M. / Tesolin, Julio Cesar Cardoso / Cavalcanti, Maria Cláudia Reis / Moura, David Fernandes Cruz: *Supporting Simulation of Military Communication Systems Using Well-Founded Modeling*. Instituto Militar de Engenharia, 2022.

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

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

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

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

[8] Land Warfare Studies Centre: *The Role of Tactical Networks in Multi-Domain Operations*. Australian Defense Research Report, 2021.

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

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

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

[12] PwC: *The Connected Battlefield: A Military Internet of Things is Emerging*. PwC Global Defense Report, 2023.

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

[14] Scanlon, William G.: *Tactical Radio Networks in Electronic Warfare Environments*. IEEE Military Communications Conference, 2016.

[15] The European Defense Agency: *Artificial Intelligence in Military Communication Platforms*. EDA Research Bulletin, 2023.

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

[17] U.S. Joint Forces Command: *Military Satellite Communications: Current Capabilities and Future Developments*. 2024.