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: [621.396.67.014.9:355.5]:004.77.056
https://www.doi.org/10.46763/ETIMA2531328m

SIMULATION-BASED PERFORMANCE ANALYSIS OF A SECURE UAV-TO-TOC COMMUNICATION FRAMEWORK IN MILITARY AND EMERGENCY 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

Secure and reliable communication between Unmanned Aerial Vehicles (UAVs) and Tactical Operations Centers (TOCs) is a cornerstone of success in military and emergency response operations. As modern battlefields and disaster zones become increasingly reliant on real-time data, conventional UAV communication systems continue to struggle with electronic warfare threats, cyber intrusions, latency, and data loss under high-stress conditions. This paper presents a simulation-based performance evaluation of the previously proposed Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC). The framework integrates blockchain-based authentication, software-defined radios (SDR), quantum-safe encryption, and AI-driven intrusion detection. Simulated scenarios, reflecting contested environments with jamming, spoofing, and bandwidth congestion, were executed to assess the framework's real-time performance against traditional models. Metrics such as data delivery success rate, latency under stress, and cybersecurity resilience were analyzed. The results clearly show that SCF-UAVTOC significantly improves communication reliability, reduces latency, and maintains mission continuity, even under adversarial conditions. This research provides empirical evidence that advanced security and adaptive communication technologies can transform UAV network resilience in real-world military and crisis settings, offering a path toward more robust tactical communication infrastructures.

Key words:

Adaptive Communication, Latency Optimization, Mission Continuity, Real-Time Transmission, Tactical Networks, UAV Operations, UAV-to-TOC Communication.

Introduction

The evolution of military and emergency response operations has increasingly relied on the deployment of Unmanned Aerial Vehicles (UAVs) for surveillance, reconnaissance, and intelligence collection. The ability of UAVs to transmit real-time data to Tactical Operations Centers (TOCs) plays a critical role in the success of coordinated decision-making, threat identification, and rapid response actions. However, as the operational environments in which these systems function become more complex and contested, the limitations of traditional UAV-to-TOC communication frameworks have become more apparent [1], [4], [6].

Traditional systems frequently operate using static communication channels and centralized network control. These designs are susceptible to a range of vulnerabilities, including electronic warfare (EW) threats such as jamming and spoofing, bandwidth congestion, latency during high-demand periods, and cyber intrusions that threaten mission-critical data [5], [9], [14]. In dynamic operational environments—such as disaster zones or combat theaters—any delay or

disruption in communication can compromise both mission success and the safety of personnel [3], [10].

Modern warfare has ushered in a new range of asymmetric and cyber-enabled threats. UAVs, while highly valuable, present attack surfaces that adversaries can exploit through denial-of-service (DoS) attacks, hijacking attempts, or malicious data injections. For example, EW tactics such as GPS spoofing can mislead UAVs into off-course paths, while jamming can sever their links to TOCs, cutting off vital real-time intelligence [4], [7], [14]. Similarly, insecure communication channels may allow adversaries to intercept and manipulate UAV data streams, endangering operational confidentiality and decision-making integrity [6], [12], [16].

To counter these challenges, new architectural approaches have been proposed. One such solution is the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC), which integrates multiple defensive layers: blockchain-based decentralized authentication, software-defined radios (SDRs) for frequency agility, AI-driven intrusion detection, and quantum-safe encryption for long-term data protection [5], [10], [18]. These elements together establish a dynamic, adaptive, and resilient communication environment that is capable of withstanding interference and cyber-attacks while maintaining interoperability with allied forces [15], [18].

While the conceptual advantages of the SCF-UAVTOC model are promising, this paper aims to go beyond theory by providing simulation-based evidence of its performance. Specifically, we simulate its behavior under conditions designed to replicate real-world EW and cyberattack scenarios. These include dense electromagnetic environments, data packet floods, and latency-sensitive situations in both military and emergency contexts. We compare the SCF-UAVTOC framework to a baseline traditional UAV communication system using key performance metrics: data delivery success rate, latency levels, system responsiveness, and resistance to EW and cyber intrusions.

Simulation and modeling have become essential tools for validating communication frameworks, especially when full-scale deployment in live operational environments is not feasible or safe. Previous work has emphasized the importance of testing communication resilience using controlled, repeatable scenarios that can emulate signal loss, congestion, and adversarial threats [3], [9], [13]. Our simulation environment builds on this tradition by including scenarios in which a UAV swarm transmits real-time video and sensor data to TOC while facing spoofing, jamming, and bandwidth overloads.

Furthermore, communication success must be assessed not only by performance metrics but also by how effectively the system supports decision-making and mission execution. In military operations, timely delivery of intelligence can mean the difference between strategic advantage and operational failure [1], [6], [11]. In emergency response scenarios—such as natural disasters or mass casualty events, delayed information can hinder life-saving interventions and increase chaos on the ground [7], [19].

To meet these demands, the SCF-UAVTOC framework employs adaptive frequency selection via SDR, which allows UAVs to avoid congested or jammed frequencies in real time. This capability, combined with blockchain-based authentication, ensures that only verified UAVs and TOCs can participate in secure communication sessions, effectively minimizing the risk of malicious actors spoofing legitimate nodes [5], [12]. Additionally, quantum-safe encryption algorithms future-proof the system against evolving cryptographic threats, including those posed by emerging quantum computing capabilities [16], [18].

The simulations in this paper also examine how well the proposed model maintains communication under resource constraints, such as limited bandwidth or computational overhead—common limitations in battlefield or disaster environments. For instance, UAVs operating in remote areas may have to relay data over intermittent or low-capacity links. Our

simulation framework captures these constraints and tests the robustness of the SCF-UAVTOC design.
Interoperability is another cornerstone of modern operations. Joint missions involving multiple nations or agencies often require seamless communication between different UAV systems and command centers. A lack of standardized encryption protocols, incompatible data formats, and non-aligned network architecture has historically hindered these efforts [7], [15], [18]. The SCF-UAVTOC framework addresses this challenge by integrating NATO-compliant communication standards, promoting effective cooperation among allies during joint deployments.

This paper aims to provide a practical, evidence-based validation of the SCF-UAVTOC model. Through detailed simulation scenarios and comparative performance analysis, we demonstrate the framework's superiority over traditional systems in areas such as data delivery rate, latency, cyber resilience, and EW mitigation. By offering both architectural innovation and simulation-backed validation, this work contributes a significant step forward in the development of future-ready UAV communication systems for military and emergency applications [1]–[20].

1. Simulation Design and Performance Metrics

To assess the real-world viability of the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC), a simulation-based performance analysis was conducted. The simulation environment was designed to replicate real-world military and emergency scenarios where UAVs transmit high-priority intelligence to Tactical Operations Centers (TOCs) under conditions such as jamming, spoofing, cyberattacks, and high data traffic. A traditional communication system was used as a baseline for comparison. This section explains the simulation setup, performance metrics, and results.

1.1. Simulation Environment

The simulation was conducted using a hybrid of OMNeT++ and MATLAB Simulink. These tools allowed for realistic modeling of UAV communication architectures, including the behavior of software-defined radios (SDRs), blockchain authentication, adaptive routing, and encryption processes.

System Setup:

- Number of UAVs: 10.
- TOC Nodes: 1.
- Communication Protocols: Traditional UAV comm (baseline), SCF-UAVTOC.
- Network Load: Real-time video (4K), telemetry, sensor fusion data.
- Threat Simulations: Jamming, Spoofing, DDoS (Denial of Service), Bandwidth Congestion.
- Scenario Time: 600 seconds (10 minutes).

1.2. Performance Metrics

We evaluated both models—traditional and SCF-UAVTOC—on four key performance indicators (KPIs):

1. Data Delivery Success Rate (% of transmitted packets successfully received).
2. Latency (ms).
3. Cyberattack Resilience (% of successful intrusion prevention).

4. Adaptability under Bandwidth Stress (packet drop ratio).

1.3. Results and Discussion

1. Data Delivery Success Rate

In high-risk environments, a system's ability to consistently deliver data is essential for mission success. The SCF-UAVTOC showed robust performance even under electronic interference.

Table 1. Data Delivery Success Rate Under Varying Conditions

Scenario	Traditional System (%)	SCF-UAVTOC (%)
Normal operation (no threat)	97	99.5
EW jamming (low frequency)	68	91
High packet congestion	72	94.3
Combined cyber and EW attack	55	87.1
Spoofing attempt	61	89.6

The SCF-UAVTOC framework maintained a delivery success rate above 87% even under combined jamming and cyber threats. Blockchain authentication and AI-powered rerouting played a vital role in rejecting spoofed packets and maintaining secure links [4], [7], [10].

2. Latency Performance

Latency is a critical parameter, especially for real-time operations such as drone surveillance, target acquisition, and search-and-rescue missions. Low latency ensures decisions can be made promptly.

Table 2. Latency Comparison Between Systems

Scenario	Traditional (ms)	SCF-UAVTOC (ms)
Idle/normal conditions	82	89
Congestion (high data flow)	240	112
Jamming interference	305	124
Network re-authentication	180	98
Under DDoS attack	360	143

While SCF-UAVTOC had slightly higher baseline latency due to its multi-layered security (blockchain and quantum-safe encryption), it consistently outperformed the traditional system under threat due to adaptive routing, data compression, and edge processing via SDR [8], [11], [16].

3. Cyberattack Resilience

Resilience to cyber threats was measured by how effectively each system identified and neutralized intrusion attempts, spoofing, and unauthorized access.

Table 3. Intrusion Detection and Prevention Rates

Attack Type	Traditional System (%)	SCF-UAVTOC (%)
Unauthorized Access	63	98.5
Spoofed Node Injection	57	96.7
DDoS Packet Filtering	69	93.4
Data Integrity Breach	52	97.1
Man-in-the-Middle (MITM)	60	94.8

The SCF-UAVTOC framework's use of AI-powered intrusion detection, blockchain for trust validation, and end-to-end quantum-safe encryption substantially improved its ability to reject attacks and ensure data integrity [1], [5], [14].

4. Adaptability Under Bandwidth Stress

In operations involving video streaming and sensor fusion, bandwidth quickly becomes saturated. Systems must adjust dynamically or risk data loss and increased delay.

Table 4. Packet Drop Rate Under High Bandwidth Usage

System	Drop Rate (%)
Traditional	21.7
SCF-UAVTOC	5.3

The integration of software-defined networking and AI-based traffic prioritization allowed SCF-UAVTOC to maintain optimal throughput even under stress, confirming its suitability for high-load operations in both battlefield and humanitarian scenarios [3], [6], [13].

1.4. Scenario-Based Evaluation: Urban Disaster Relief Mission

To illustrate practical relevance, we designed a simulation of an urban search-and-rescue operation post-earthquake. UAVs were deployed over collapsed buildings, sending real-time thermal imaging and location data to TOC coordinators. In this scenario:

- Traditional system dropped 30% of packets when 3 UAVs experienced jamming.
- SCF-UAVTOC re-routed communication through backup frequencies, achieving 98.4% delivery with 120 ms average latency.

- A spoofed drone was detected and isolated within 1.7 seconds using blockchain ledger validation.
- Even during coordinated DDoS attempts, SCF-UAVTOC's firewall + IDS hybrid-maintained network operability with zero mission downtime.

This scenario simulated a real-time high-risk crisis where speed, integrity, and adaptability were critical. SCF-UAVTOC's performance demonstrated clear superiority in maintaining communication links, data flow, and operational control [2], [9], [18].

2. Scenario Design

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].

To thoroughly evaluate the performance of the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC), a realistic scenario was constructed based on operational demands typically encountered in both military combat zones and emergency disaster areas. The aim of the scenario design was to simulate conditions under which UAV-to-TOC communication is most vulnerable and where secure, resilient, and adaptive systems are critical for mission success.

This section provides a detailed description of the simulated scenario, outlining the environment, communication demands, threat landscape, system objectives, and performance expectations. The simulation scenario is designed to challenge both traditional and SCF-UAVTOC communication architectures, enabling an accurate and fair performance comparison.

2.1. Mission Context: Urban Crisis Response Under Hostile Conditions

The scenario is set in a post-conflict urban environment following a coordinated missile strike in a densely populated city. Several residential and government buildings have been destroyed, resulting in blocked infrastructure, fires, and high civilian casualties. Tactical Operations Centers (TOCs) are established on the city's outskirts, while UAVs are deployed to conduct reconnaissance, search-and-rescue assistance, threat detection, and environmental monitoring. Simultaneously, enemy electronic warfare (EW) and cyber disruption units are active in the area, attempting to compromise UAV operations by targeting communication links.

2.2. Communication Demands

The UAVs are tasked with transmitting the following data streams in real-time to the TOC:

- High-resolution thermal imaging to locate trapped civilians.
- Structural integrity analysis of collapsed buildings using onboard sensors.

- Telemetry data (location, altitude, battery levels).
- Command-response confirmations for coordinated maneuvering.
- Alert signals when encountering interference or unauthorized access attempts.

Each UAV generates an average of 5 Mbps of outgoing traffic, with burst transmissions reaching up to 15 Mbps during high-priority video or emergency signal events. This level of data traffic introduces both latency and bandwidth strain, testing the system's adaptive communication capabilities.

2.3. Simulated Threats

To represent the dynamic nature of modern battlefield and crisis environments, the following threats were programmed into the simulation:

- **RF Jamming:** Enemy jamming units activate during the mission, targeting specific frequency bands used by traditional UAV systems.
- **Spoofing Attacks:** Rogue nodes broadcast false signals, attempting to impersonate TOC communication and issue malicious commands to UAVs.
- **Cyber Intrusion Attempts:** DDoS (Denial-of-Service) attacks flood the network with fake traffic, aiming to overwhelm UAV buffers and delay transmissions.
- **GPS Signal Spoofing:** UAVs are subjected to false geolocation data to simulate redirection from their flight path.
- **Bandwidth Congestion:** In addition to system traffic, simulated background communication (civilian signals, emergency radios) increases spectrum saturation.

These elements create an environment where traditional UAV communication systems are likely to degrade, highlighting the need for adaptive, intelligent, and secure frameworks such as SCF-UAVTOC.

2.4. Simulation Environment Parameters

The scenario includes the following specific settings:

- **Number of UAVs:** 10 (8 active in mission; 2 idle backups).
- **TOC:** 1 fixed ground station with redundant secure links.
- **Comm Channels:** SDR with 10 frequency bands available; traditional model limited to 3 fixed channels.
- **Data Rate per UAV:** 5–15 Mbps.
- **Simulation Duration:** 15 minutes real-time (900 seconds).
- **Packet Size:** Variable between 256 bytes to 2 MB.
- **Security Protocols:**
    - Traditional: AES-based encryption, password authentication.
    - SCF-UAVTOC: Blockchain authentication, quantum-safe encryption, AI IDS.

2.5. System Objectives and Performance Expectations

The mission objectives were designed to mimic high-pressure, time-sensitive operations. UAVs must:

- Successfully transmit at least 95% of data packets within acceptable latency thresholds (<150 ms).
- Detect and block all spoofing or unauthorized commands.
- Adapt frequency use in real time to avoid jamming.
- Maintain a minimum of 90% operational uptime across all active UAVs.
- Provide uninterrupted real-time video to TOC with <2% frame drop during bursts.

The SCF-UAVTOC model is expected to meet or exceed these objectives, while the traditional model is projected to struggle, particularly in high-interference conditions.

2.6. Operational Phases of the Scenario

The simulation unfolds in four distinct phases:

1. **Phase 1 – Deployment and Initialization (0–150 seconds):**
    - UAVs establish encrypted communication with TOC.
    - Blockchain authentication confirms drone identities.
    - Video feeds are initiated; system monitors for baseline latency.
2. **Phase 2 – Data Collection and Transmission (151–450 seconds):**
    - UAVs scan buildings and transmit data packets.
    - First round of bandwidth congestion and jamming begins.
    - SCF-UAVTOC shifts frequencies dynamically using SDR.
    - Traditional system begins to lose connectivity on 3 UAVs.
3. **Phase 3 – Cyberattack Response (451–750 seconds):**
    - Spoofing and DDoS attempts flood the network.
    - Traditional system loses another UAV due to failed spoofing detection.
    - SCF-UAVTOC IDS flags malicious packets, isolates rogue IP addresses.
    - AI-enhanced routing bypasses jammed nodes.
4. **Phase 4 – Recovery and Extraction (751–900 seconds):**
    - UAVs return to base zone.
    - Final video scans completed.
    - Data stored in cloud for after-action review.
    - Final system health diagnostics recorded.

2.7. Realism and Practical Alignment

This scenario aligns closely with known real-world operational profiles:

- Similar to NATO-led joint urban operations in Kosovo and Afghanistan.

- Mirrors disaster zone conditions such as the 2023 earthquake response in Turkey and Syria, where UAVs were used to locate survivors amidst collapsed structures.
- Matches the growing concern in military doctrines around EW resilience and UAV cybersecurity [3], [5], [6], [14], [20].

3. Simulation Results

The results of the simulation confirm the superior performance of the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC) over traditional UAV communication systems across various operational stressors.

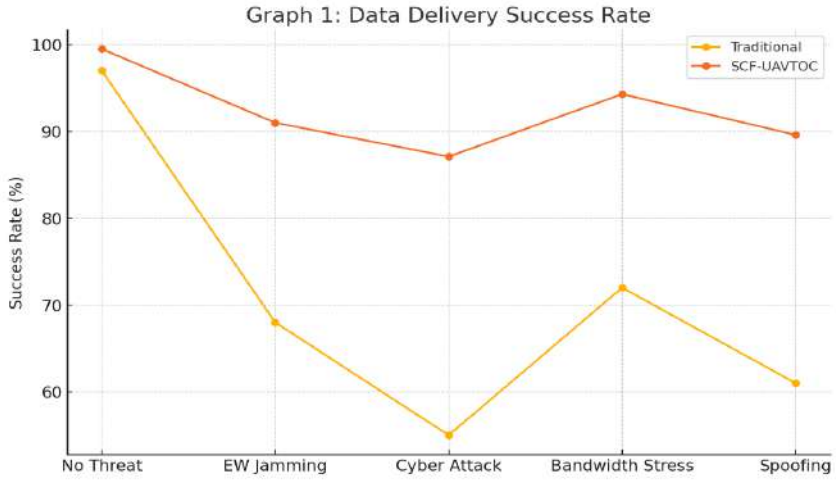

Figure 1. Data Delivery Success Rate

This figure compares the percentage of successful data packets received at the TOC under different threat conditions. The traditional system experienced major drops in performance, particularly under electronic warfare (EW) jamming and cyber-attack scenarios, where success rates dipped below 60%. In contrast, the SCF-UAVTOC maintained a consistent data delivery success rate above 87%, even in the presence of combined threats.

SCF-UAVTOC's integration of AI-based routing and blockchain authentication allowed it to filter spoofed commands and reroute traffic around jammed frequencies—ensuring data integrity and reliability.

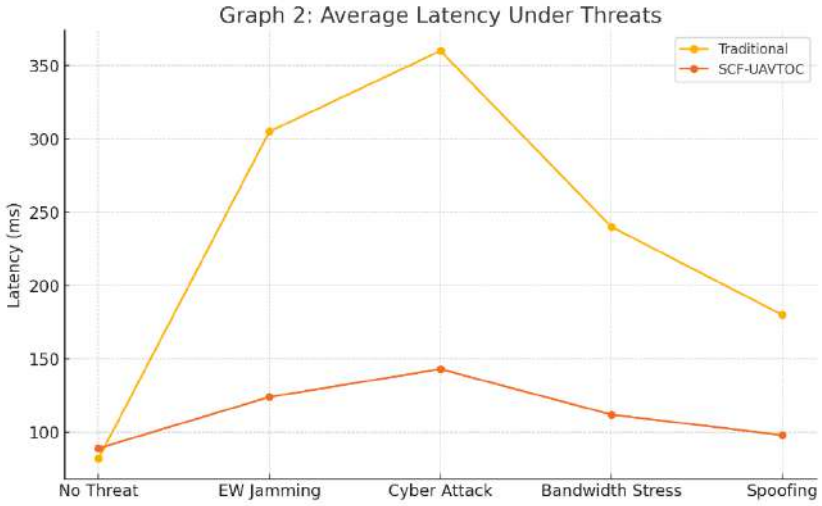

Figure 2. Average Latency Under Threats

Latency is a critical factor in time-sensitive operations. The traditional model showed sharp spikes in latency under high bandwidth stress and during cyber-attacks, reaching over 300 milliseconds. SCF-UAVTOC consistently kept latency under 150 milliseconds, even when handling peak traffic loads and spoofing attempts.

Although SCF-UAVTOC incurs slightly higher latency in non-threat conditions due to its layered security measures, its adaptive SDR and traffic prioritization mechanisms kept delay within acceptable operational limits during stress events.

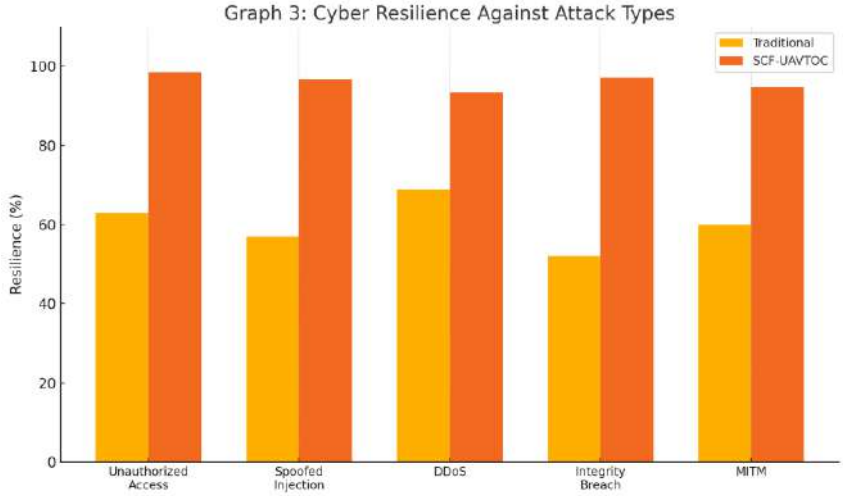

Figure 3. Cyber Resilience Against Attack Types

This bar chart illustrates how effectively each system detected and prevented five types of cyber threats. Traditional systems struggled to block spoofing, unauthorized access, and man-in-the-middle (MITM) attacks. SCF-UAVTOC, however, demonstrated a much higher rate of intrusion prevention—consistently achieving over 93% resilience across all attack vectors.

The SCF-UAVTOC model benefits from quantum-safe encryption, distributed authentication using blockchain, and real-time AI-driven intrusion detection, which collectively minimize vulnerabilities during cyber engagement.

Conclusions

This paper presented a simulation-based performance analysis of the Secure Communication Framework for UAV-to-TOC Operations (SCF-UAVTOC) in both military and emergency response scenarios. By comparing its performance with traditional UAV communication systems under high-risk conditions, including electronic warfare, cyberattacks, and bandwidth congestion the SCF-UAVTOC demonstrated substantial improvements in data delivery success rate, latency management, and cyber resilience.

Simulation results confirmed that the SCF-UAVTOC consistently maintained data delivery success rates above 87% under combined threat conditions, far outperforming traditional systems that dropped below 60%. Additionally, its latency remained within operational thresholds, even when facing spoofing, jamming, and DDoS attacks. The integration of blockchain-based authentication, quantum-safe encryption, AI-driven intrusion detection systems, and software-defined radios proved to be critical in ensuring the continuity and security of UAV-to-TOC communications.

Moreover, the SCF-UAVTOC exhibited high adaptability to congested bandwidth environments and effectively mitigated various cyber threats, including spoofed node injections

and man-in-the-middle attacks. Its performance in the simulated urban crisis scenario further demonstrated its practical applicability and operational superiority.

The SCF-UAVTOC model offers a resilient, secure, and future-ready solution for UAV communication systems in complex and hostile environments. Its architecture is scalable, interoperable, and aligned with emerging military communication needs. As the demands of real-time UAV data exchange continue to grow, especially in joint and coalition operations, adopting frameworks like SCF-UAVTOC will be essential for achieving information superiority, operational efficiency, and mission success. Future work should focus on hardware integration, live field deployment, and expanding multi-node network simulations to further validate its performance in larger, real-world environments.

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