ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SECURE COMMUNICATION FOR MUM-T: A BLOCKCHAIN AND LIGHTWEIGHT CRYPTOGRAPHY FRAMEWORK

M.Sc. THESIS

Halimcan YAŞAR

Department of Computer Engineering

Computer Engineering Programme

JUNE 2025

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

SECURE COMMUNICATION FOR MUM-T: A BLOCKCHAIN AND LIGHTWEIGHT CRYPTOGRAPHY FRAMEWORK

M.Sc. THESIS

Halimcan YAŞAR
(504231520)

Department of Computer Engineering

Computer Engineering Programme

Thesis Advisor: Prof. Dr. Şerif BAHTİYAR

JUNE 2025

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MUM-T İÇİN GÜVENLİ İLETİŞİM: BİR BLOKZİNCİR VE HAFİF KRİPTOGRAFİ ÇERÇEVESİ

YÜKSEK LİSANS TEZİ

Halimcan YAŞAR
(504231520)

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Şerif BAHTİYAR

HAZİRAN 2025

Halimcan YAŞAR, a M.Sc. student of ITU Graduate School student ID 504231520 successfully defended the thesis entitled "SECURE COMMUNICATION FOR MUM-T: A BLOCKCHAIN AND LIGHTWEIGHT CRYPTOGRAPHY FRAMEWORK", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. Şerif BAHTİYAR** Istanbul Technical University	.....
Jury Members :	**Assoc. Prof. Dr. Yusuf Yaslan** İstanbul Technical University	.....
	Prof. Dr. Muhammet Ali Aydın İstanbul University Cerrahpaşa	.....
		.....

Date of Submission : **25 May 2025**
Date of Defense : **27 June 2025**

To my family and friends,

FOREWORD

This thesis marks the culmination of a research journey that has allowed me to explore the intersection of cybersecurity, blockchain technology, and autonomous systems. What began as a focused research paper on secure communication for MUM-T systems evolved into a more comprehensive framework, supported by analytical models and simulations implemented in Python and OMNeT++.

The work presented here addresses a critical challenge in modern military communication: ensuring both the integrity and real-time responsiveness of mission-critical data exchanged between manned aircraft and UAVs. By integrating PoA-based blockchain mechanisms with lightweight cryptographic methods, I sought to develop a solution that is not only secure but also efficient and scalable.

This journey would not have been possible without the support and guidance of several individuals and institutions. I would like to express my deepest gratitude to my advisor, Professor Şerif Bahtiyar, for his unwavering support, insightful feedback, and technical expertise throughout this research. His mentorship was instrumental in shaping both the direction and quality of this work.

I am grateful to the Cyber Security and Privacy Research Lab (SPFLab) at Istanbul Technical University for providing the academic environment and resources necessary for this research.

I would like to acknowledge the financial support provided by the Research Fund of Istanbul Technical University, under project number 45654, which enabled the successful execution of this study.

On a more personal note, I am deeply thankful to my family and close friends for their patience, encouragement, and belief in me throughout this process. Their presence has been a constant source of motivation.

With this thesis, I hope to contribute to the growing body of work in secure autonomous systems and inspire further research in this crucial area of modern technology.

JUNE 2025 Halimcan YAŞAR

TABLE OF CONTENTS

ABBREVIATIONS

MUM-T	**:** Manned Unmanned Teaming
UAV	**:** Unmanned Aerial Vehicle
MAV	**:** Manned Aerial Vehicle
PoA	**:** Proof of Authority
SPOF	**:** Single Points of Failure
IoT	**:** Internet of Things
ECC	**:** Elliptic Curve Cryptography
SOC	**:** Security Operations Centers
LOA	**:** Levels of Automation
PLS	**:** Physical Layer Security
PoW	**:** Proof of Work
ECDSA	**:** Elliptic Curve Digital Signature Algorithms
PUF	**:** Physical Unclonable Functions
PBFT	**:** Practical Byzantine Fault Tolerance

SYMBOLS

$N_{\mathbf{UAV}}$	: Number of Unmanned Aerial Vehicles in the MUM-T system
$T_{\mathbf{msg}}$	: Interval between UAV control messages
$T_{\mathbf{mc}}$	: Interval between mission-critical data transmissions
$\mathbf{Txn}_i$	: i^{th} transaction generated by a UAV
$\mathbf{Block}_i$	: i^{th} block created by the MAV
$L_{\mathbf{xor}}$	: Latency of XOR-based lightweight authentication
$L_{\mathbf{block}}$	: Latency of blockchain transaction confirmation
H	: Cryptographic hash function used in block generation
K	: Shared symmetric key used for XOR encryption

LIST OF TABLES

Page

LIST OF FIGURES

Page

SECURE COMMUNICATION FOR MUM-T:
A BLOCKCHAIN AND LIGHTWEIGHT CRYPTOGRAPHY FRAMEWORK

SUMMARY

MUM-T systems are becoming increasingly central to modern defense and surveillance operations, enabling the coordinated deployment of MAVs and UAVs in complex, mission critical scenarios. While these systems offer significant tactical advantages, they also introduce unique challenges in maintaining secure, reliable, and real-time communication. In particular, MUM-T environments demand a delicate balance between high data integrity, low latency responsiveness, and computational efficiency requirements that conventional cryptographic and network security architectures often struggle to fulfill, especially within the resource-constrained platforms typical of UAVs.

In response to these challenges, this thesis proposes a novel hybrid communication security framework designed specifically for MUM-T systems. The proposed architecture integrates two complementary technologies: a PoA-based blockchain to ensure tamper-resistant logging of mission-critical data, and a XOR-based lightweight cryptographic authentication scheme to facilitate high frequency, low-latency control messaging. By decoupling data assurance and real-time control into two dedicated communication layers, the framework seeks to maximize both operational integrity and responsiveness without overburdening the limited computational resources of UAVs.

The research is anchored in a clear hypothesis: that the combined use of a PoA blockchain and lightweight symmetric encryption can provide a secure and efficient communication backbone suitable for MUM-T applications. To evaluate this hypothesis, the thesis employs both analytical modeling and simulation-based validation across two environments. The first, a custom Python-based simulation, models transaction generation, XOR-based encryption, and PoA block validation with fine-grained timing control. This simulation tracks end-to-end latency, throughput, and computational load under realistic scheduling parameters, revealing that the PoA component maintains transaction latencies well below 750 milliseconds, while the XOR mechanism introduces only microsecond-level processing delay making both viable for real-world deployment.

The second simulation, developed in OMNeT++, models a network level implementation of the proposed framework, capturing the behavior of MAV and UAV nodes as modular entities within a time accurate, message driven environment. This simulation validates system-level coordination, concurrent operation of both communication layers, and the effectiveness of the hierarchical topology under realistic operating constraints. Collected scalar and vector metrics confirm that mission

critical blocks are consistently generated and broadcast by the MAV, while UAVs engage in continuous transaction and control message generation. Time series data further demonstrate a stable and scalable increase in system activity, reinforcing the framework's responsiveness and throughput capacity.

Together, the simulation results confirm that the proposed hybrid framework meets its design objectives. It provides a scalable, efficient, and secure communication model that is well suited to the hierarchical structure and operational demands of MUM-T systems. By leveraging the strengths of both blockchain and lightweight encryption, the framework supports the integrity and auditability of mission data while ensuring that time sensitive control messages are delivered with minimal delay.

This thesis contributes to the growing field of secure autonomous system communication by offering a practical architecture that bridges the gap between real time responsiveness and high assurance data integrity. Future work may involve exploring more advanced lightweight encryption schemes, incorporating adaptive key management, or extending the consensus model to support partially decentralized architectures. Additional simulation scenarios involving adversarial threats or mission disruption can also enhance the robustness and applicability of the system in the real world.

MUM-T İÇİN GÜVENLİ İLETİŞİM: BİR BLOKZİNCİR VE HAFİF KRİPTOGRAFİ ÇERÇEVESİ

ÖZET

MUM-T sistemleri, günümüzün modern savunma ve gözetleme operasyonlarında giderek daha merkezi bir rol oynamakta ve MAV ile UAV karmaşık, görev açısından kritik senaryolarda eşgüdümlü şekilde konuşlandırılmasını mümkün kılmaktadır. Bu sistemler, görev etkinliğini artırmanın yanı sıra, yüksek riskli bölgelerde insan kaybı riskini azaltmakta ve aynı anda çoklu görevlerin yürütülmesine olanak tanımaktadır. Ancak, bu operasyonel avantajlara rağmen, MUM-T uygulamalarında karşılaşılan en temel zorluklardan biri, sistemler arası güvenli, güvenilir ve gerçek zamanlı iletişimin sağlanmasıdır. MUM-T ortamlarında, görev başarısını doğrudan etkileyen üç temel güvenlik ve performans gereksinimi öne çıkmaktadır: yüksek veri bütünlüğü, düşük gecikme süresi ve hesaplama açısından verimli iletişim. Özellikle savaş alanı gibi stresli ve dinamik ortamlarda, bu üç gereksinimin aynı anda karşılanması büyük önem taşımaktadır. Ne var ki, geleneksel kriptografik yaklaşımlar ve merkezi ağ güvenliği çözümleri, özellikle kaynakları kısıtlı olan insansız hava araçlarında bu gereksinimleri karşılamakta yetersiz kalabilmektedir. Örneğin, RSA gibi yoğun hesaplama gerektiren algoritmalar, sınırlı işlem gücüne sahip UAV platformlarında ciddi performans kayıplarına yol açabilirken, gecikme hassasiyeti yüksek görevlerde iletişim protokollerinin yükü, karar verme sürelerini olumsuz etkileyebilmektedir. Ayrıca, merkezi yapıdaki güvenlik çözümleri tek bir arıza noktasına bağımlı oldukları için, askeri operasyonlar gibi yüksek güvenilirlik gerektiren uygulamalarda risk teşkil etmektedir. Bu nedenle, MUM-T sistemlerinin ihtiyaçlarına özel, hem güvenli hem de hafif yapıda çalışan, aynı zamanda düşük gecikme ile gerçek zamanlı iletişimi mümkün kılan yeni nesil çözümlerin geliştirilmesi kritik bir ihtiyaç hâline gelmiştir.

Bu tez, MUM-T sistemlerinin iletişim güvenliğini hem yüksek performans hem de sağlamlık açısından optimize edebilmek amacıyla özel olarak tasarlanmış yeni ve özgün bir hibrit güvenlik çerçevesi önermektedir. Önerilen mimari, farklı görev türlerinin ihtiyaçlarına uygun olacak şekilde iki tamamlayıcı teknolojinin bir arada kullanıldığı katmanlı bir yaklaşım sunmaktadır. Bunlardan ilki, görev açısından kritik kabul edilen veri türlerinin değiştirilemez ve denetlenebilir bir biçimde kaydedilmesini sağlayan, PoA algoritmasına dayalı özel bir blokzincir yapısıdır. PoA yapısı, klasik blokzincirlerdeki yüksek işlem yükünü azaltırken, güvenilir düğümler arasında hızlı ve tutarlı veri bütünlüğü sağlar. İkinci teknoloji ise, gerçek zamanlı sistemlerde çok önemli olan hız ve verimlilik gereksinimlerini karşılamak üzere tasarlanmış olan, XOR tabanlı hafif bir kimlik doğrulama ve veri şifreleme mekanizmasıdır. Bu yöntem, özellikle İHA'ların sınırlı işlem kapasitesi göz önünde bulundurulduğunda, son derece düşük işlem yükü ve mikro-saniye düzeyinde gecikmeyle çalışarak sistemin operasyonel tepki süresini önemli ölçüde iyileştirmektedir. Böylece, iletişim güvenliği

iki farklı eksende ele alınmakta; blokzincir bileşeni, kalıcı güvenlik ve veri doğruluğu sağlarken, XOR temelli hafif kriptografi ise anlık kontrol ve yönlendirme mesajlarının hızlı ve güvenli iletimine olanak tanımaktadır. Bu bütünsel yaklaşım sayesinde, MUM-T sistemlerinin en büyük sınırlamalarından biri olan hem güvenlik hem de hız ihtiyacının aynı anda karşılanması hedeflenmekte; veri bütünlüğü sağlanırken, sistemin gerçek zamanlı tepkiselliği ve operasyonel sürdürülebilirliği de koruma altına alınmaktadır.

Araştırma, PoA tabanlı blokzinciri teknolojisinin ve hafif simetrik şifreleme yaklaşımının birlikte kullanılmasıyla, MUM-T uygulamaları için hem güvenli hem de performans açısından verimli bir iletişim altyapısı oluşturulabileceği yönündeki temel hipoteze dayanmaktadır. Bu varsayım, yalnızca teorik düzeyde kalmamış; aynı zamanda iki farklı ve birbirini tamamlayan simülasyon ortamında gerçekleştirilen kapsamlı deneysel doğrulamalarla desteklenmiştir. İlk doğrulama ortamı olan Python tabanlı simülasyon platformu, önerilen sistemin temel bileşenlerini modellemek amacıyla özel olarak geliştirilmiştir. Bu simülasyonda; işlem üretimi, XOR algoritmasına dayalı veri şifreleme, PoA algoritması ile blok oluşturma ve onaylama süreçleri zaman etkeni gözetilerek ayrıntılı biçimde modellenmiş; her bir işlem adımının sistem üzerindeki etkileri, zaman gecikmeleri ve işlem yoğunluğu gibi metriklerle detaylı olarak analiz edilmiştir. Elde edilen sonuçlar, PoA tabanlı blokzincir yapısının ortalama işlem gecikmesini 750 milisaniyenin altında tuttuğunu göstermiştir ki bu, özellikle göreve duyarlı sistemlerde kabul edilebilir bir sınır olarak değerlendirilmektedir. Öte yandan XOR tabanlı hafif kimlik doğrulama mekanizması, mikro-saniyeler düzeyinde gerçekleşen şifreleme ve doğrulama süresiyle neredeyse gerçek zamanlı iletişim imkânı sağlamaktadır. Bu sonuçlar, hem PoA blokzincirinin güvenli ve tutarlı veri kaydı sağlama potansiyelini, hem de XOR temelli hafif şifrelemenin düşük gecikme gerektiren operasyonlar için ne denli uygun olduğunu ortaya koyarak, önerilen yaklaşımın pratik uygulamalar açısından güçlü bir çözüm sunduğunu doğrulamaktadır.

İkinci olarak geliştirilen OMNeT++ tabanlı ağ seviyesi simülasyon ise, önerilen hibrit güvenlik çerçevesinin pratikte düğüm-temelli nasıl işleyeceğini değerlendirmek amacıyla tasarlanmış, zamana duyarlı ve olay tabanlı bir modelleme ortamı sunmaktadır. Bu simülasyon, gerçek dünyadaki MUM-T senaryolarına benzer biçimde yapılandırılmış ve hem MAV yani insanlı hava aracı, hem de birden fazla İHA modüler bileşenler şeklinde modellenmiştir. MAV, sistemde blokzincir ağının otorite düğümü olarak konumlandırılmış; her bir İHA ise hem işlem üretme hem de kontrol mesajları alma/yollama yetenekleriyle donatılmıştır. Zamanlayıcılar ve mesaj odaklı olay yönetimi sayesinde, ağ trafiği, mesaj gecikmeleri, işlem yoğunluğu ve blok üretim periyotları gibi önemli parametreler detaylı olarak izlenmiştir. Toplanan sayısal metrikler, MAV'in belirli aralıklarla yeni bloklar oluşturduğunu ve bunları tüm İHA'lara başarıyla ilettiğini göstermiş; bu da blokzincir bileşeninin önerildiği şekilde çalıştığını doğrulamıştır. Aynı zamanda İHA'lar, senaryo boyunca hem görev verisi hem de kontrol mesajları üretmiş, böylece simülasyon ortamında çift yönlü iletişim döngüsü sağlanmıştır. Ek olarak, elde edilen vektörel zaman serisi verileri, sistemin görev süresince kararlı, ölçeklenebilir ve senkronize bir iletişim trafiği yürüttüğünü ortaya koymuş; bu da önerilen sistemin çoklu İHA senaryolarında dinamik yükler altında bile güvenilir şekilde çalışabileceğini göstermiştir.

Simülasyon sonuçları, önerilen hibrit güvenlik çerçevesinin önceden belirlenen tasarım hedeflerini başarıyla karşıladığını açık biçimde ortaya koymaktadır. Özellikle, blokzincir bileşeni aracılığıyla elde edilen güvenilir ve denetlenebilir veri kaydı sayesinde, görev süresince oluşturulan tüm kritik verilerin değiştirilemez biçimde saklandığı ve sonradan doğrulanabilir olduğu gösterilmiştir. Bu, operasyon sonrası analiz, görev raporlama ve olası güvenlik denetimleri açısından büyük avantaj sağlamaktadır. Öte yandan, hafif XOR tabanlı şifreleme mekanizmasının uçuş kontrolü ve anlık karar mekanizmaları gibi zaman hassasiyeti yüksek uygulamalarda yalnızca mikrosaniyelik seviyede gecikme oluşturduğu tespit edilmiştir. Bu da sistemin gerçek zamanlı iletişim ihtiyaçlarına başarıyla yanıt verdiğini göstermektedir. Hem blokzincir hem de hafif şifreleme katmanlarının birlikte kullanılması, sistemin bütünlük, güvenilirlik ve tepki süresi bakımından dengeli bir yapı sunduğunu doğrulamaktadır. Sonuç olarak, bu hibrit yaklaşımın, MUM-T gibi hem güvenli hem de hızlı iletişimin kritik olduğu ortamlarda uygulanabilirliği yüksek, pratik ve ölçeklenebilir bir çözüm sunduğu kanıtlanmıştır. Böylece sistem, hem güvenlik hem de performans gereksinimlerinin eşzamanlı olarak karşılandığı, görev-kritik askeri uygulamalara uygun bir altyapı olarak öne çıkmaktadır.

Bu tez, güvenli otonom sistem iletişimi alanına önemli bir katkı sunarak, veri bütünlüğü ile zaman duyarlılığını aynı mimaride başarıyla birleştiren, hem pratik hem de ölçeklenebilir bir hibrit güvenlik yaklaşımı ortaya koymaktadır. Geliştirilen çerçevenin, farklı güvenlik önceliklerine sahip iletişim katmanlarını ayrı araçlarla ele alarak performans ve güvenilirlik arasında denge kurması, MUM-T gibi yüksek riskli ve karmaşık operasyonlarda önemli bir tasarım avantajı sunmaktadır. Bu çalışmanın oluşturduğu altyapı, gelecekteki araştırmalar için de çok sayıda potansiyel gelişim alanı barındırmaktadır. Örneğin, XOR yerine daha gelişmiş ve saldırılara karşı daha dayanıklı olan hafif kriptografik algoritmaların sistemle entegre edilmesi, hem güvenlik seviyesini artıracak hem de farklı senaryolarda daha esnek çözümler sunacaktır. Bununla birlikte, şu anki yapıda idealize edilmiş olan anahtar yönetimi süreçleri de dinamik ve dağıtık bir yapıya dönüştürülerek, sistemin ölçeklenebilirliği ve uzun vadeli sürdürülebilirliği güçlendirilebilir. Özellikle, merkeziyetsiz mimarilerde kullanılabilecek daha esnek ve güvenli konsensüs algoritmalarının araştırılması, PoA modelinin sınırlamalarını aşmak adına yeni ufuklar açabilir. Ayrıca, mevcut simülasyon ortamı barışçıl bir iletişim senaryosu üzerine kurulmuşken, gerçekçi bir operasyonel güvenlik değerlendirmesi için aktif saldırı simülasyonlarının dahil edilmesi büyük önem taşımaktadır. Bu tür tehdit senaryoları, sistemin sadece verimliliğini değil, aynı zamanda güvenlik dayanıklılığını da test edebileceğimiz bir çerçeve sunacaktır. Bu bağlamda, çalışmanın sunduğu temel mimari hem akademik hem de uygulamalı güvenlik alanında daha derinlemesine araştırmalar için sağlam bir zemin oluşturmaktadır.

1. INTRODUCTION

MUM-T integrates UAVs with a MAV, enabling a single pilot to coordinate and control multiple UAVs that autonomously perform reconnaissance, targeting, and communication functions. This configuration reduces the cognitive burden on the pilot, allowing greater strategic focus while delegating specific tactical operations to UAVs, thereby improving overall mission effectiveness [1]. In such scenarios, UAVs are often deployed to assist MAVs in high-risk environments, enhancing survivability and mission outcomes by extending situational awareness and operational reach [2]. For example, in complex missions such as emergency medical response, UAVs support the MAV by detecting environmental hazards and obstacles, contributing to both mission safety and efficiency [3]. A notable instance is the U.S. Air Force's XQ-58A Valkyrie, which acts as a loyal wingman to fighter jets, scouting threats, engaging adversaries, and absorbing fire, thus extending combat capabilities and improving pilot safety [4]. As highlighted in [5], MUM-T is positioned at the core of long-term U.S. defense strategies, envisioned as critical to sustaining air superiority over the next two decades.

Despite the operational advantages, MUM-T systems introduce significant security challenges, particularly concerning the transmission of mission-critical data, including command, control, and intelligence information. These systems require robust and efficient authentication protocols to prevent unauthorized access, eavesdropping, and spoofing attacks. However, current MUM-T architectures are often hindered by insufficient threat modeling and reliance on centralized security structures, which create vulnerabilities such as SPOF and limited interoperability across distributed control units [6] [7] [8]. Several existing approaches seek to address these issues by incorporating lightweight authentication mechanisms, public-key cryptography for secure key exchange, and blockchain technologies for decentralized trust management. These strategies aim to enhance security while accommodating the computational constraints typical of UAV systems [8] [9].

For instance, [7] explores lightweight cryptographic protocols tailored for Internet of Things (IoT) environments, emphasizing efficiency. Yet, these methods often exhibit limited integrity verification capabilities and dependence on centralized servers, reintroducing SPOF vulnerabilities. Conversely, [8] advocates for blockchain-based solutions due to their inherent strengths in integrity assurance and decentralization. However, the computational complexity of consensus protocols poses practical limitations in real-time, resource-constrained aerial networks. Meanwhile, [9] proposes an architecture that enables direct UAV interaction with distributed control nodes via ground stations, offering improved flexibility. Nonetheless, this model raises concerns about communication performance, particularly when MAVs and UAVs operate at extended distances from centralized coordination points.

1.1 Purpose of Thesis

This thesis thoroughly investigates the critical challenge of ensuring secure communication within MUM-T systems, while simultaneously maintaining high operational performance without introducing unacceptable trade-offs or system inefficiencies. The primary objective is to design a network architecture that effectively balances decentralization, data integrity, and real-time responsiveness, core requirements for mission-critical aerial operations. To this end, the thesis proposes a hybrid security framework that integrates blockchain technology and lightweight cryptographic mechanisms.

The blockchain component provides tamper-resistant and verifiable logging of mission-critical data, ensuring traceability, accountability, and auditability throughout the operation lifecycle. In parallel, the use of lightweight cryptographic methods enables low-latency, high-throughput communication necessary for real-time control and coordination between the MAV and UAVs. This dual-layered approach is specifically tailored to meet the stringent constraints of MUM-T environments, where both operational agility and robust security are paramount. By addressing these dual demands, the proposed framework contributes a practical and scalable solution suited for deployment in dynamic, resource-constrained, and high-threat military settings.

1.2 Security in MUM-T Similar Networks

Security challenges of MUM-T align closely with IoT ecosystems, where interconnected, resource-constrained devices must maintain real-time communication across decentralized and potentially adversarial environments. As MUM-T systems evolve to include greater autonomy, dynamic coordination, and mission-critical communication, the need for robust yet efficient security mechanisms becomes increasingly urgent. Unlike traditional networks, MUM-T operations demand simultaneous guarantees of data integrity, low latency, and decentralized trust, which are difficult to achieve using conventional architectures. Accordingly, the literature offers three prominent lines of defense: blockchain technologies for distributed trust and tamper resistance, lightweight cryptographic schemes for computational efficiency, and human-autonomy teaming protocols for adaptive, context-aware security support. Each of these approaches offers partial solutions to the MUM-T security problem, but no single model fully addresses its complexity.

Recent studies have emphasized that MUM-T configurations increasingly involve dynamic, multi-role UAV operations with varying levels of autonomy and operational range, placing new demands on the communication and coordination architecture [10]. These configurations not only enhance tactical versatility but also increase the architectural complexity and surface area for potential cyber threats. As CENJOWS highlights, MUM-T platforms are now integral to enhancing lethality and responsiveness in military operations, necessitating secure, interoperable communication mechanisms that can scale alongside increasing mission complexity [11].

Blockchain-based systems have garnered attention for their ability to decentralize authentication and data validation processes while ensuring traceability and tamper-proof record-keeping. In [12], a lightweight blockchain framework is proposed for fog-enabled IoT environments, leveraging ECC to establish secure communication among clustered devices. The framework introduces angular distance metrics to form device clusters and integrates trust management via smart contracts, allowing the system to detect and isolate colluding nodes efficiently. This decentralized

trust calculation is particularly applicable to MUM-T scenarios, where UAVs must dynamically authenticate one another during coordinated missions. By offloading computational tasks to fog nodes, the system achieves a balance between security and energy efficiency, showing that blockchain can be adapted to environments with strict performance constraints.

Building on this, [13] proposes the DIA-BC architecture, a blockchain-based identity management system optimized for 5G-enabled IoT ecosystems. The model anchors device identities in immutable blockchain ledgers and employs smart contracts to enforce access control, removing the need for centralized identity providers. The relevance to MUM-T is clear: UAVs and ground systems require scalable, verifiable identity schemes to prevent spoofing and unauthorized access, especially in fast-moving operational contexts. DIA-BC achieves this through a hybrid of PKI and blockchain consensus, showing substantial gains in scalability, latency, and trust assurance across large-scale deployments.

Edge authentication is further advanced in [14], which introduces a permissioned blockchain model for securing edge devices in fog computing environments. The system uses ECC (specifically the secp256k1 curve) for cryptographic operations and MQTT to streamline device communications. The fog nodes serve as blockchain validators, facilitating decentralized identity verification while maintaining real-time responsiveness. When mapped to MUM-T, this model reflects a viable way to distribute authentication responsibilities across UAV swarms and supporting ground stations, allowing for secure operation even in bandwidth-constrained or disconnected environments.

An additional fog-centric solution, BlocFogSec, is introduced in [15], which uses dual smart contracts to govern key management and secure data sharing in IoT-fog infrastructures. By combining PBFT consensus with contract-based access control, the framework provides integrity, low latency, and decentralized policy enforcement. These qualities are critical for scalable MUM-T operations where data consistency must be preserved without centralized overhead.

A broader theoretical foundation for these approaches is outlined in [16], which surveys blockchain-based authentication techniques in IoT systems. The review categorizes solutions by architectural model, consensus protocol, and application scope, highlighting trust management and decentralized key exchange as core enablers of secure interoperability. It emphasizes the need for adaptive, scalable security mechanisms capable of operating under uncertainty, conditions common to MUM-T deployments. It also forecasts future developments in machine learning-integrated blockchain frameworks for real-time trust evaluation, which could provide predictive and context-aware security layers for autonomous air networks.

Focusing on remote user authentication, the Lightchain protocol presented in [17] integrates smart contracts with hash-based obfuscation to deliver mutual authentication in fog-IoT networks. Its use of fog-layer consensus mechanisms eliminates central failure points and enhances scalability. Formally validated via AVISPA and implemented on Ethereum, Lightchain presents a robust, lightweight solution for securing dynamic edge networks, features aligned with the layered architecture and mobility patterns of MUM-T systems.

A similar model is proposed in [18], where blockchain-based identity management is distributed through fog nodes to achieve fast and secure authentication. By using ECC and smart contracts for certificate handling and access control, the protocol enables lightweight authentication, verified through AVISPA simulations. This further reinforces the practical viability of fog-blockchain fusion models for real-time, secure identity management in unmanned networks.

Although blockchain ensures integrity and auditability, its consensus mechanisms often introduce delays and resource demands that are unsustainable for real-time UAV communication. This has driven significant research into lightweight cryptographic protocols, particularly those optimized for embedded systems. In [19], a Rabin-based anonymous authentication scheme is introduced for asymmetric IoT environments. It minimizes computational overhead by allocating intensive operations to gateways, while ensuring mutual authentication, user anonymity, and session key establishment. The protocol is designed to resist various attacks, including replay and impersonation,

making it well-suited to MUM-T networks where UAVs frequently join and leave a mission group.

Complementary to this, [20] explores advanced cryptographic primitives tailored for zero-trust models in IoT, including PUFs and zero-knowledge proofs. PUFs derive secure identifiers from intrinsic hardware properties, removing the need for stored keys, while zero-knowledge proofs allow authentication without revealing secrets. These techniques improve both privacy and integrity, particularly in systems with adversarial risk and no centralized authority. For MUM-T, this enables identity assurance even in untrusted environments, where UAVs may be deployed without prior configuration or infrastructure.

Scalable authentication for dense networks is addressed in [21], which introduces a hash-chain-based mutual authentication protocol. This scheme supports multi-node authentication using shared hash sequences, significantly reducing communication and computational costs. The use of xxHash ensures fast hash generation, and the protocol tolerates message tampering and delayed delivery, making it robust for dynamic, decentralized operations like those in UAV swarms. By reducing complexity from quadratic to linear, this approach enables simultaneous mutual authentication across numerous devices with minimal delay.

The benefits of ECC in constrained systems are reaffirmed in [22], which offers a systematic analysis of ECC-based IoT authentication schemes. ECC provides strong cryptographic protection using small key sizes and low power consumption, aligning well with the hardware limitations of UAVs. The review emphasizes ECC's flexibility, security, and performance, making it a default choice for secure key exchange and digital signatures in real-time embedded systems. This position is further supported in [23], which evaluates ECC in comparison with RSA and DSA, highlighting its efficiency in energy-constrained deployments and its growing importance in IoT-focused cryptographic protocols.

Alongside cryptographic mechanisms, human-autonomy teaming has emerged as a critical dimension of MUM-T security. In [24], a security-aware human-UAV protocol is developed that integrates human-aided geolocation with UAV autonomy to detect

GPS spoofing attacks. The framework uses delayed-action games to model when and how humans should intervene, creating resilient decision-making protocols that balance machine speed with human judgment. This is especially valuable in MUM-T, where stealthy adversarial actions may evade algorithmic detection.

The importance of human involvement in cyber defense is further emphasized in [25], which presents the A²C framework for human-AI collaboration in SOCs. This model assigns tasks based on complexity, with routine alerts handled by AI and ambiguous events escalated to human analysts. Such collaborative autonomy improves decision-making accuracy and reduces analyst fatigue. In MUM-T control centers, this framework could be adapted to dynamically balance human and machine control based on threat level, mission urgency, and operator workload.

To formalize human-autonomy collaboration, [26] proposes a taxonomy involving LOA, MI, and COAD. The framework is applied in military use cases, such as coordination between F-35 aircraft and loyal wingman drones, highlighting the value of dynamic control delegation and shared situational awareness. These principles directly apply to MUM-T, where human operators must flexibly oversee multiple autonomous UAVs across changing mission contexts.

Further empirical insights are provided by [27], whose comprehensive review of HAT literature identifies key factors influencing trust, communication, and performance in human-agent teams. The authors argue that HAT success depends not just on technology but also on designing roles, feedback channels, and interdependence structures that support mutual adaptation, principles that are highly relevant to secure, mission-critical teaming in MUM-T networks.

Finally, [28] introduces a physical layer security technique for multi-UAV systems that leverages cooperative jamming. Slave UAVs generate interference to shield communications between ground stations and master UAVs, protecting against eavesdropping and spoofing. Human operators maintain supervisory control, activating fallback mechanisms during anomalies. This blend of cryptographic shielding and human oversight embodies the multi-layered defense required in high-risk MUM-T deployments.

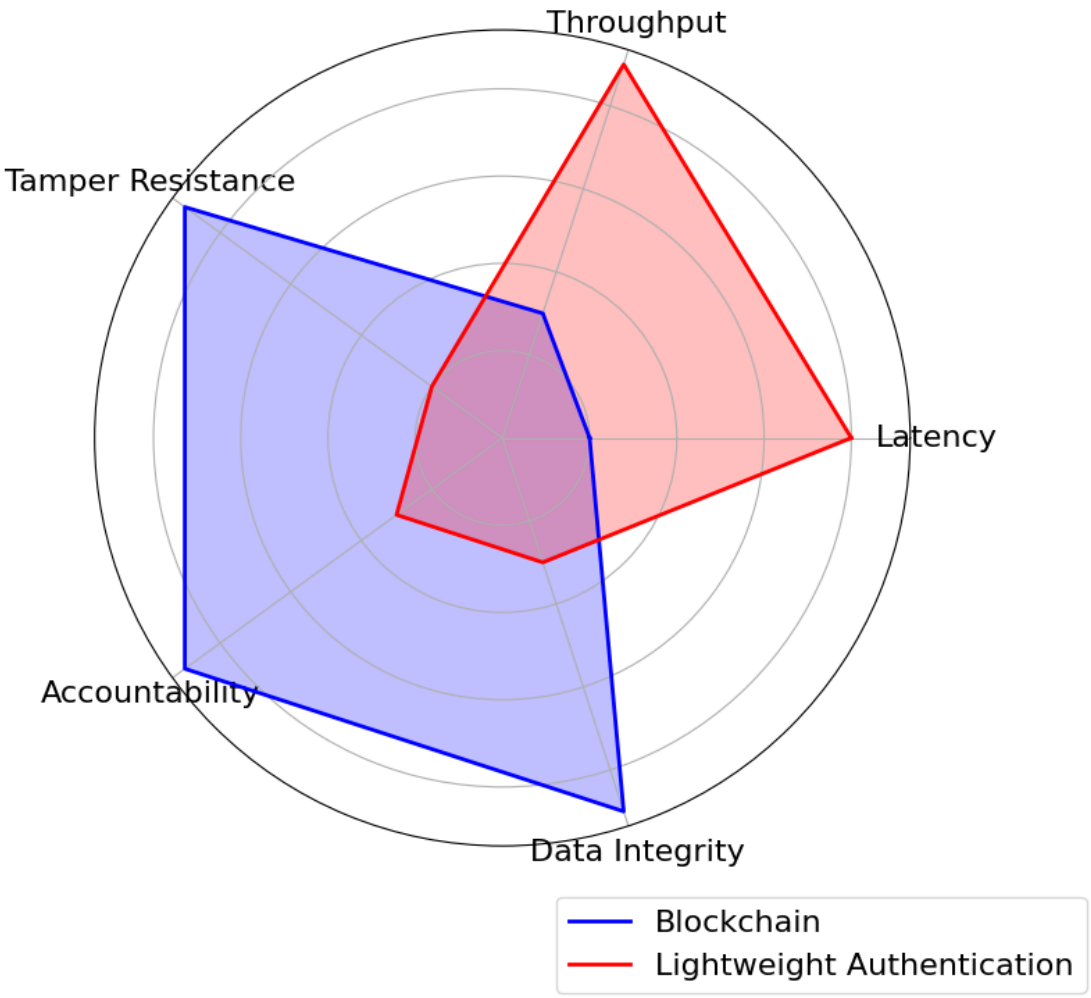

Figure 1.1: A comparison of blockchain and lightweight authentication.

Figure 1.1 provides a comparative analysis of blockchain and traditional communication architectures across critical metrics. Traditional models generally outperform in throughput and latency due to centralized control, but they fall short in auditability, tamper resistance, and data integrity. Blockchain systems, by contrast, offer superior transparency and trust but suffer from latency and energy cost. Hybrid models, such as the probabilistic schemes in [29] and Authentication-Chains in [30], attempt to bridge this gap by streamlining consensus and reducing computational complexity, but often compromise on absolute security guarantees or full decentralization.

Despite these advancements, the literature reveals a gap in unified frameworks that can simultaneously offer integrity, responsiveness, scalability, and adaptability. Most

existing models prioritize one security dimension while neglecting others, leaving MUM-T systems exposed to trade-offs that are untenable in real-world missions. Blockchain ensures integrity but hinders speed. Lightweight cryptography is efficient but lacks decentralization. Human-autonomy teaming enhances adaptability but does not fulfill cryptographic security needs.

To overcome these limitations, this thesis proposes a hybrid architecture combining PoA-based blockchain for tamper-proof mission data recording with XOR-based lightweight cryptography for real-time control authentication. This dual-layer framework aligns with the hierarchical structure of MUM-T systems, leveraging the MAV as a trusted validator while enabling scalable, efficient communication among UAVs. By integrating security, latency, and adaptability into one model, the proposed solution aims to meet the operational and computational demands of future MUM-T environments.

1.3 Hypothesis

MUM-T systems are emerging as indispensable components of next-generation autonomous operations, combining the strategic oversight of manned platforms with the agility, scalability, and reach of UAVs. These systems operate in increasingly complex, dynamic, and adversarial environments where secure, efficient, and real-time communication is paramount. The communication infrastructure must be capable of simultaneously ensuring the confidentiality, integrity, and authenticity of mission-critical data, while maintaining ultra-low latency for effective command, control, and coordination. However, the expansion of autonomous roles and inter-vehicle interactions in MUM-T architectures also increases the surface for cyber vulnerabilities, including message interception, spoofing, unauthorized command injection, and malicious manipulation. Traditional security mechanisms, while cryptographically strong, often introduce latency, energy, or computational demands that are impractical for constrained aerial platforms. This presents a fundamental and unresolved challenge: how to secure MUM-T communications without undermining their responsiveness and operational agility.

This thesis advances the hypothesis that a hybrid communication security framework, tailored to the unique structural and performance characteristics of MUM-T systems, can fulfill both integrity and latency requirements without compromise. The proposed framework synergistically integrates two complementary technologies: a blockchain mechanism based on the PoA consensus model, and a lightweight symmetric encryption scheme using XOR operations. Within this architecture, the PoA blockchain provides a secure, tamper-resistant ledger for logging and validating mission data. By delegating consensus authority to a trusted node, typically the MAV, the blockchain layer ensures high transaction throughput and low confirmation latency, addressing the shortcomings of more decentralized but slower consensus protocols like Proof of Work or Proof of Stake. Concurrently, the XOR-based cryptographic layer secures the high-frequency control and telemetry messages exchanged between the MAV and UAVs. This layer is designed to offer fast encryption and authentication with minimal computational overhead, thus supporting the stringent timing and resource constraints characteristic of embedded UAV platforms.

The hypothesis is substantiated by a growing body of literature highlighting the limitations of existing approaches. Public key infrastructures, while secure, are often infeasible for real-time UAV applications due to their reliance on intensive computation and key management. Decentralized blockchain consensus models, although trusted and transparent, suffer from latency and energy inefficiencies that are incompatible with fast-moving aerial networks. In contrast, PoA offers a pragmatic balance by enabling deterministic and rapid validation through a known, trusted party. Similarly, XOR-based cryptography, while not suitable for general-purpose encryption, can be highly effective for securing time-critical UAV communications when paired with integrity verification mechanisms such as checksums or hash-based authentication codes.

From this hypothesis, several operational expectations are derived. The framework is anticipated to maintain sufficient throughput to accommodate frequent transaction generation without causing backlog or bottlenecks. It should consistently deliver low-latency performance for both blockchain-based data recording and real-time control message transmission. The total computational and energy burden should

remain within the tolerances of typical UAV hardware, ensuring compatibility with constrained processing environments. Additionally, the architecture is expected to provide resilience against prevalent attack vectors, including message tampering, replay attacks, and unauthorized data injection, without degrading mission performance or system responsiveness. Importantly, the solution must be scalable, allowing seamless integration of additional UAV nodes without exponential increases in overhead or delay.

To evaluate this hypothesis rigorously, the research employs a dual approach combining analytical modeling and simulation-based validation. Analytical models are developed to estimate expected performance parameters, such as latency, throughput, and computational cost, under realistic operating conditions. These models are then validated through implementation in two independent simulation environments: Python-based modeling for detailed cryptographic and communication behavior, and OMNeT++ for network-level performance evaluation under simulated mission scenarios. These simulations reflect the hierarchical structure, timing constraints, and message flow patterns typical of MUM-T deployments, providing empirical data to assess the practical feasibility and advantages of the proposed architecture. Comparative benchmarks with conventional security models allow for a nuanced understanding of trade-offs and confirm whether the hybrid solution meaningfully improves performance, efficiency, and reliability.

In essence, the hypothesis reflects the core assertion of this thesis: that security and performance in MUM-T communications are not mutually exclusive. Rather, with a carefully engineered integration of lightweight cryptography and streamlined consensus mechanisms, it is possible to build a secure, low-latency, and scalable communication architecture that aligns with the operational and architectural realities of future autonomous aerial networks.

2. ADAPTIVE BLOCKCHAIN-CRYPTOGRAPHY FRAMEWORK FOR MUM-T

2.1 Purpose

This study addresses the limitations of existing security solutions in MUM-T systems, with particular attention to their inability to concurrently deliver high data integrity, decentralization, and low-latency communication. These shortcomings are especially critical in environments where both secure mission data transmission and real-time control are operational imperatives. The objective of this research is to design and evaluate a hybrid communication security architecture that aligns with the performance constraints of MUM-T systems, particularly those imposed by the limited computational resources of unmanned aerial vehicles.

The proposed framework integrates a PoA blockchain mechanism with a lightweight cryptographic authentication method based on XOR operations. The blockchain component provides a verifiable, tamper-resistant ledger for mission-critical data, ensuring traceability and data integrity throughout the operational lifecycle. In parallel, the XOR-based cryptographic layer enables high-frequency, low-overhead message authentication, supporting real-time telemetry and control with minimal processing burden. The framework is structured around the hierarchical nature of MUM-T communication networks, with the manned aerial vehicle acting as a central authority responsible for validating and broadcasting blockchain data.

By uniting these two complementary approaches, the framework seeks to balance long-term data assurance with immediate operational responsiveness. The design intentionally reduces cryptographic and consensus overhead while maintaining essential security guarantees. The subsequent section introduces the architecture in detail, describing its structural components, transaction flow, and the underlying rationale for its design choices within the context of mission-oriented communication.

2.2 Framework Details

The proposed solution, termed the Adaptive Blockchain-Cryptography Framework, seamlessly integrates lightweight authentication mechanisms with blockchain technology to strike an optimal balance among high data integrity, decentralization, and low latency, three fundamental requirements for secure and responsive MUM-T operations. As illustrated in Figure 2.1, the architecture of the MUM-T blockchain network is centered around a PoA consensus mechanism, which governs the interaction between the MAV and its associated UAVs. In this hierarchical setup, the MAV operates as the trusted authority node, responsible for validating incoming transactions and assembling them into blocks. Conversely, the UAVs function as distributed transaction generators, continuously transmitting mission-critical data, such as reconnaissance imagery, flight telemetry, and situational updates, to the MAV via a shared transaction pool. This architectural design ensures that control communications remain lightweight and low-latency, while mission data is reliably recorded in a tamper-resistant ledger. In doing so, the framework reinforces both operational efficiency and the overall security posture of the MUM-T system.

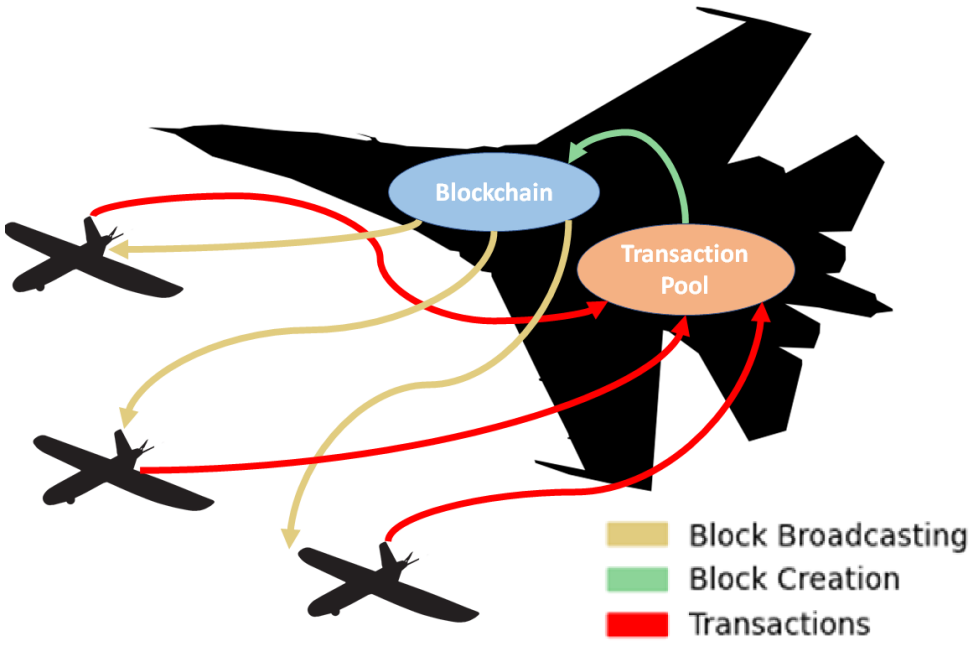

Figure 2.1: MUM-T blockchain network.

2.2.1 Transaction and block creation flow

Within this network, UAVs continuously generate transactions that encapsulate mission-relevant data and control messages, such as sensor readings, positional telemetry, and operational status updates. These transactions are first submitted to a shared transaction pool, where they remain temporarily queued for processing. The MAV, acting as the network's authority node under the PoA consensus model, periodically retrieves pending transactions from the pool, performs validation checks to ensure their authenticity and integrity, and subsequently assembles them into a new block. Once validated, the block is appended to the blockchain, forming an immutable and verifiable record of mission activity. This transaction-to-block workflow is formally represented as follows.

$$Block_i = \{Txn_1, Txn_2, \ldots, Txn_n\} \tag{2.1}$$

Where Block_i denotes the newly constructed block generated by the MAV, while $\text{Txn}_1, \ldots, \text{Txn}_n$ represent the validated transactions selected from the transaction pool for inclusion. Before appending Block_i to the blockchain, the MAV applies a cryptographic hash function to ensure immutability and signs the block using its private key to guarantee authenticity and integrity. This process ensures that all recorded data is tamper-evident and verifiable by other network participants.

2.2.2 Broadcasting

Once the MAV successfully creates a block, it broadcasts the updated blockchain to all connected UAVs. This broadcasting step ensures that each UAV maintains a synchronized and immutable copy of the blockchain, which serves as a tamper-resistant ledger for all mission-critical data. As illustrated in Figure 2.1, the block creation and broadcast steps are visually represented, with arrows denoting the data flow from the MAV to the UAVs. This mechanism guarantees that data integrity is consistently upheld across the entire network.

Maintaining a consistent blockchain state across all UAVs is particularly vital in military operations, where unified situational awareness and coordinated

decision-making are paramount. The broadcasting step mitigates discrepancies between nodes and reinforces trust in the recorded data. The inherent immutability of blockchain further ensures that once data is committed to the ledger, it cannot be altered, even in the presence of adversarial actors, thereby strengthening the network's resilience to tampering.

The proposed network adopts PoA as its consensus mechanism, primarily due to PoA's ability to deliver high transaction throughput with minimal computational overhead. In contrast to resource-intensive approaches like PoW, PoA leverages a designated set of trusted validators, significantly reducing processing requirements and energy consumption [31]. Validators are pre-selected and incentivized to behave honestly, enhancing network reliability without incurring excessive computational costs [32]. Additionally, PoA is characterized by low latency and minimal transaction fees, making it well-suited for environments where performance, predictability, and operational efficiency take precedence over full decentralization [31]. While PoA may exhibit reduced resistance to censorship in open networks, its reliance on validator trust is well-aligned with MUM-T architectures, where the MAV naturally assumes the role of a reliable authority. As such, PoA offers an ideal balance between efficiency and security in the context of hierarchical and trust-anchored aerial systems.

Algorithm 1 MUM-T Blockchain Network: Transaction and Block Flow

for each mission cycle **do**
    for each UAV $i = 1, 2, \ldots, N$ **do**
        Generate transaction (message) `txn_i`
        Send `txn_i` to transaction pool
    end for
    if transaction pool not empty **then**
        Retrieve transactions from transaction pool
        Validate transactions
        Create block with validated transactions
        Broadcast block to the UAVs
    end if
end for

In the proposed framework, UAVs are not tasked with validating transactions. Their role is limited to the generation and transmission of mission-relevant data encapsulated as transactions. The MAV, functioning as the sole validator, is exclusively responsible

for verifying the authenticity of transactions and aggregating them into blocks. This deliberate division of labor significantly reduces the computational burden on UAVs, allowing them to focus on core mission tasks such as sensing, navigation, and coordination. By centralizing validation at the MAV, the framework ensures consistent enforcement of data integrity without overtaxing UAV resources. The transaction processing logic and block creation workflow are summarized in the above pseudo-code, which delineates the respective responsibilities of the MAV and UAVs in the secure communication process.

2.2.3 Blockchain with lightweight authentication

In a MUM-T system, both blockchain and traditional lightweight cryptographic solutions offer unique advantages depending on the specific operational requirements. To optimize the network for both performance and security, it is important to determine when blockchain is the most appropriate and when traditional solutions should be used.

Blockchain technology, with its decentralized, tamper-resistant ledger, is particularly suitable for scenarios where data integrity, accountability, and traceability are paramount. Blockchain technology is increasingly suitable for logging mission-critical data, such as reconnaissance intelligence, command approvals, and mission outcomes. Once data is validated and stored on the blockchain, it becomes immutable, preventing unauthorized alterations and ensuring that mission logs remain secure from tampering by any malicious actor. This immutable nature guarantees accountability and facilitates audit during post-mission reviews and investigations, allowing military leaders to trace each decision and action. For instance, crucial authorizations, like those required for a weapon deployment, can be permanently recorded on the blockchain, offering a reliable trail of all decisions made during operations. This makes it ideal for use in logging and validating critical mission events, decision-making processes, and mission logs that require post-mission audit. However, the process of a block creation and a transaction validation introduces additional latency, making blockchain less suitable for real-time operations that require instantaneous responses.

Traditional lightweight cryptographic solutions, such as symmetric encryption, XOR-based encryption, and stream ciphers, are well-suited for real-time communica-

Table 2.1: Use Cases For Blockchain and Traditional Cryptographic Solutions in MUM-T Networks

Use Case	Preferred Solution	Reason
Mission-Critical Data Logging	Blockchain	Ensures immutability and auditability of key mission data.
Authorization and Command Validation	Blockchain	Logs critical decisions immutably for secure review.
Post-Mission Data Integrity and Review	Blockchain	Tamper-proof records ensure data accuracy during review.
Real-Time Flight Control	Lightweight Authentication	Requires low latency and fast response times.
Telemetry Data and Video Feeds	Lightweight Authentication	High throughput needed for continuous data streams.

tion tasks like flight control signals, telemetry data, and video streaming, where a low latency and a high throughput are critical. These methods, including AES encryption and stream ciphers that offer a fast communication with minimal computational overhead, making them ideal for scenarios that require rapid responses. For example, in the real-time navigation of UAVs, an immediate feedback from ground control stations or other aircraft is essential to the mission success, as any delay could compromise the outcome. While these traditional cryptographic methods may not provide the same level of data immutability as blockchain, they are highly efficient in contexts where speed is prioritized over long-term data integrity. Therefore, for tasks where immediacy is essential, conventional cryptographic solutions are preferable.

We propose a hybrid approach to address both security and performance requirements as summarized in the Table 2.1. Blockchain technology is used to ensure the integrity and traceability of high-stakes mission decisions, while traditional cryptographic methods support secure, low-latency communication essential for real-time operations. By combining these technologies within the MUM-T network, the system may achieve robust security measures alongside the performance needed in mission-critical

environments. This approach allows for reliable data integrity in critical event logging without compromising the speed and efficiency required for tasks demanding immediate feedback. In doing so, the MUM-T blockchain network may deliver both secure and high-performance communications, effectively meeting the complex demands of military operations.

In scenarios where a problem arises with the MAV, UAVs are notified through a lightweight, real-time communication channels. This allows them to autonomously determine whether to complete their tasks or initiate a return-to-home protocol. Upon return, mission-critical data recorded by UAVs can be accessed through a secure master key system, allowing post-mission analysis and a review of critical events. This master key mechanism enables an authorized personnel to retrieve immutable mission data from the blockchain, facilitating detailed analysis while preserving data integrity. By leveraging this structure, the MUM-T system ensures not only resilient real-time performance but also secure and traceable post-mission data handling, supporting accountability and informed decision-making in high-stakes environments.

In summary, the MUM-T blockchain network may benefit from using a blockchain for data integrity and accountability in critical events and traditional lightweight encryption for real-time communications where speed is essential. By leveraging both technologies appropriately, the system provides both secure and high-performance communications for military operations.

3. ANALYSIS

3.1 Purpose

The purpose of this section is to conduct a comprehensive evaluation of the proposed hybrid security framework and its suitability for addressing the unique operational demands of MUM-T systems. These systems require a delicate balance between stringent security assurances and the low-latency, high-frequency communication necessary for real-time mission coordination. The framework under evaluation integrates two distinct yet complementary components: a PoA-based blockchain for verifiable, tamper-resistant data logging, and an XOR-based lightweight authentication mechanism designed for efficient and rapid message-level security.

The evaluation approach is structured in two distinct but interrelated phases. The first phase involves a theoretical performance analysis grounded in analytical modeling. This includes latency estimation, throughput calculations, and computational cost projections based on parameters aligned with typical MUM-T environments, such as the number of UAVs, control message frequency, and resource limitations of onboard systems. These analytical insights provide upper and lower performance bounds, enabling a baseline understanding of the system's theoretical feasibility.

The second phase transitions from theoretical modeling to empirical validation through simulation. Two simulation environments were developed for this purpose. A Python-based discrete-event simulation captures fine-grained control over event scheduling, cryptographic operations, and communication delays, offering detailed latency and performance measurements. Complementing this, an OMNeT++-based network simulation reproduces modular MUM-T behavior at the system level, modeling communication timing, network load, and consensus cycles under realistic operational conditions. These simulations are instrumental in capturing performance dynamics that cannot be fully addressed through static analysis alone, such as the

interplay between concurrent processes and the impact of communication latency under load.

By combining theoretical and simulation-based evaluations, this section aims to validate whether the proposed architecture can reliably support secure, scalable, and time-sensitive communication in resource-constrained MUM-T networks. The subsequent discussion presents quantitative results on key performance metrics, including latency, message throughput, and computational overhead, providing empirical evidence of the framework's capability to meet the dual imperatives of security and operational efficiency in mission-critical scenarios.

3.2 Analytical Estimations

The proposed hybrid security framework for MUM-T systems was initially evaluated through analytical modeling to assess its performance under conditions reflective of realistic operational scenarios. This analysis draws upon performance benchmarks derived from established PoA blockchain implementations [33,34], in conjunction with theoretical estimates for XOR-based operations as a lightweight authentication mechanism. The analytical evaluation centers on three key performance dimensions: end-to-end communication latency, sustainable transaction throughput, and the computational overhead incurred by both MAV and UAV nodes. These dimensions are critical to determining whether the architecture can meet the dual requirements of responsiveness and security in resource-constrained, mission-critical environments.

By quantifying these parameters, the analysis establishes a baseline understanding of the framework's operational feasibility and identifies potential performance trade-offs. The results indicate that the proposed architecture is well-positioned to deliver low-latency communication and maintain efficient use of computational resources, all while preserving the integrity and authenticity of mission-critical data exchanges. Moreover, the modeling highlights the synergy between PoA consensus and XOR-based encryption, confirming their suitability for layered deployment in latency-sensitive aerial networks. This foundational insight affirms the

architecture's potential to support secure and responsive communication workflows within hierarchical MUM-T deployments.

3.2.1 Analysis of blockchain

The blockchain component of the proposed framework is built upon a PoA consensus mechanism, wherein the MAV serves as the sole authority node responsible for validating transactions and generating blocks, while the UAVs operate as transaction initiators. This hierarchical configuration closely mirrors the command structure of typical MUM-T systems, in which centralized control is maintained by the MAV to facilitate efficient coordination and secure data validation. For the purpose of analytical modeling, system parameters were derived from empirical benchmarks reported in established PoA blockchain deployments, as referenced in [33] and [34]. These sources provided concrete values for block creation intervals, transaction confirmation latency, and validator throughput, thereby enabling a realistic and context-aware assessment of the blockchain layer's expected performance. The use of MAV as a trusted validator aligns with the operational dynamics of MUM-T networks, where trust can be centralized without compromising the scalability or responsiveness of distributed UAV operations.

3.2.1.1 Block time and transaction throughput

In PoA networks, the block time is a crucial parameter that affects transaction throughput and the network latency. According to [33], a typical block time for a PoA network can be configured to as low as 1 second. We assume a conservative block time to be $T_b = 5$ seconds that is used for MAV's computational limitations and network conditions in a MUM-T environment.

The maximum transaction throughput ($\lambda_{\max}$) is computed as follow.

$$\lambda_{\max} = \frac{N_t}{T_b} \tag{3.1}$$

N_t is the maximum number of transactions per block. We assume that the MAV may process up to $N_t = 100$ transactions per block, which is a reasonable estimate given the MAV's computational capabilities, the maximum transaction throughput is:

$$\lambda_{\max} = \frac{100}{5\,\text{seconds}} = 20\,\text{transactions/second} \tag{3.2}$$

The throughput is sufficient for typical MUM-T operations, where UAVs send mission-critical updates at lower frequencies.

3.2.1.2 Latency analysis

The end-to-end latency (L_{bc}) for a transaction in the blockchain component consists of the following components.

$$L_{\text{bc}} = T_{\text{tx\_gen}} + T_{\text{net\_tx}} + T_{\text{validation}} + T_{\text{block\_creation}} + T_{\text{net\_block}} \tag{3.3}$$

where,

- $T_{\text{tx\_gen}}$: Time for UAV to generate the transaction.
- $T_{\text{net\_tx}}$: Network transmission time from UAV to MAV.
- $T_{\text{validation}}$: Time for MAV to validate the transaction.
- $T_{\text{block\_creation}}$: Time to create and sign the new block.
- $T_{\text{net\_block}}$: Time to broadcast the block to all UAVs.

The following average times are based on [33] and practical network considerations.

- $T_{\text{tx\_gen}} \approx 10\,\text{ms}$
- $T_{\text{net\_tx}} \approx 50\,\text{ms}$
- $T_{\text{validation}} \approx 5\,\text{ms}$
- $T_{\text{block\_creation}} \approx 500\,\text{ms}$

- $T_{\text{net\_block}} \approx 50\,\text{ms}$

The total latency is

$$L_{\text{bc}} = 10\,\text{ms} + 50\,\text{ms} + 5\,\text{ms} + 500\,\text{ms} + 50\,\text{ms} = 615\,\text{ms} \tag{3.4}$$

Thus, the blockchain component introduces an approximate latency of 615 milliseconds per transaction.

3.2.1.3 Computational overhead

The computational overhead on the MAV for processing transactions and creating blocks can be computed based on the time complexity of cryptographic operations.

- **Transaction Validation**: Involves verifying the transaction's signature, which typically ECDSA. The time complexity is $O(1)$ per transaction.
- **Block Creation**: Includes hashing the block's contents and signing the block. The hashing operation has a time complexity of $O(N_t)$, where N_t is the number of transactions in the block.

We assume the MAV processes $N_t = 100$ transactions per block and the following average computational times.

- Transaction signature verification: $T_{\text{verify}} \approx 1\,\text{ms}$ per transaction.
- Hashing and block signing: $T_{\text{hash}} \approx 100\,\text{ms}$ (proportional to N_t).

Total computational time per block on MAV is computed as follows.

$$\begin{aligned} T_{\text{comp\_MAV}} &= N_t \times T_{\text{verify}} + T_{\text{hash}} \\ &= 100 \times 1\,\text{ms} + 100\,\text{ms} = 200\,\text{ms} \end{aligned} \tag{3.5}$$

The computational overhead is acceptable for the MAV, which typically has more robust processing capabilities than UAVs.

3.2.2 Analysis of lightweight authentication

For real-time communication tasks within the MUM-T framework, XOR-based lightweight authentication is employed due to its exceptionally low computational footprint and its effectiveness in supporting high-frequency message exchanges. This cryptographic approach enables rapid encryption and verification cycles, allowing control messages to be secured with minimal delay. Its simplicity and efficiency make it particularly well-suited for deployment on resource-constrained UAV platforms, where both processing power and energy availability are limited. Moreover, the deterministic and low-latency nature of XOR operations aligns with the stringent timing requirements of real-time UAV coordination, ensuring that security mechanisms do not interfere with mission responsiveness.

3.2.2.1 XOR encryption and decryption

The XOR operation is one of the simplest forms of encryption that is defined as follows.

$$C = P \oplus K \tag{3.6}$$

$$P = C \oplus K \tag{3.7}$$

where,

- P is the plaintext.
- C is the ciphertext.
- K is the key.
- $\oplus$ denotes the bitwise XOR operation.

The time complexity for XOR encryption or decryption is $O(n)$, where n is the length of the data in bits.

3.2.2.2 Latency analysis

The latency introduced by XOR-based authentication is negligible. For a data packet of size S bytes, the encryption or decryption time (T_{xor}) is computed as follows.

$$T_{\text{xor}} = \frac{n}{R_{\text{cpu}}} \tag{3.8}$$

where:

- $n = 8S$ bits.
- R_{cpu} is the processor's bitwise operation rate in bits per second.

Assume that a UAV processor with $R_{\text{cpu}} = 100\,\text{Mbps}$, which is a conservative estimate for embedded processors, for a data packet of $S = 256$ bytes is ($n = 2048$ bits).

$$T_{\text{xor}} = \frac{2048\,\text{bits}}{100 \times 10^6\,\text{bits/s}} = 20.48\,\mu\text{s} \tag{3.9}$$

The analyses results show that the encryption or decryption time per packet is approximately 20.48 microseconds, which is negligible compared to network transmission times.

3.2.2.3 Computational overhead

The computational overhead imposed on both UAVs and the MAV by XOR-based operations is effectively negligible, making this method highly suitable for real-time applications in resource-constrained aerial platforms. Its simplicity allows cryptographic operations to be executed with minimal processor cycles, ensuring that security functions do not interfere with mission-critical control tasks. Furthermore, the energy consumption associated with XOR-based authentication is substantially lower than that of conventional cryptographic algorithms such as AES or RSA. This reduced power demand contributes to extended flight durations and overall system endurance, which are critical factors in autonomous and long-range missions. As a result, XOR-based authentication not only supports real-time responsiveness but

also aligns with the stringent energy efficiency requirements of modern MUM-T deployments.

3.2.3 Network performance evaluation

To further validate the viability of the proposed framework, a numerical performance evaluation was conducted using scenario-based metrics relevant to MUM-T communication architectures. The analytical assessment considered key parameters such as the number of UAVs, message transmission intervals, and blockchain transaction rates. Specifically, with 10 UAVs sending control messages every 100 milliseconds, the lightweight authentication channel achieves a throughput of 100 messages per second, demonstrating its suitability for real-time operations. In parallel, mission-critical data sent every 5 seconds generates a blockchain load of 2 transactions per second, well within the 20 transactions per second limit comfortably handled by typical PoA blockchain networks. This analysis confirms that the XOR-based lightweight cryptography introduces only negligible latency (approximately 20.48 µs per 256-byte message), while the PoA mechanism, validated through existing implementations, supports timely consensus with predictable latency characteristics. Altogether, the results underscore the framework's capacity to meet the stringent latency and throughput demands of MUM-T systems while maintaining computational feasibility across heterogeneous airborne platform

3.2.3.1 Scenario parameters

Consider a representative MUM-T operational scenario involving a fleet of ten UAVs $N_{\mathrm{UAV}} = 10$. In this configuration, each UAV transmits control messages to the MAV at intervals of $T_{\mathrm{msg}} = 100\,\mathrm{ms}$, utilizing a lightweight XOR-based authentication mechanism to ensure both speed and integrity in real-time communication. In parallel, mission-critical data is generated and transmitted every $T_{\mathrm{mc}} = 5\,\mathrm{s}$, with each payload intended for secure logging through the PoA-based blockchain component of the framework. This setup reflects a realistic balance between high-frequency control messaging and periodic data recording, allowing for a comprehensive evaluation of the proposed architecture's performance under typical mission conditions.

3.2.3.2 Throughput calculation

- **Lightweight Authentication Channel**:

  Total messages per second:

$$\lambda_{\text{light}} = N_{\text{UAV}} \times \frac{1}{T_{\text{msg}}} = 10 \times \frac{1}{0.1\,\text{s}} = 100\,\text{messages/s} \tag{3.10}$$

- **Blockchain Channel**:

  Total transactions per second:

$$\lambda_{\text{bc}} = N_{\text{UAV}} \times \frac{1}{T_{\text{mc}}} = 10 \times \frac{1}{5\,\text{s}} = 2\,\text{transactions/s} \tag{3.11}$$

The blockchain network may comfortably handle this transaction rate given the calculated maximum throughput of 20 transactions/s.

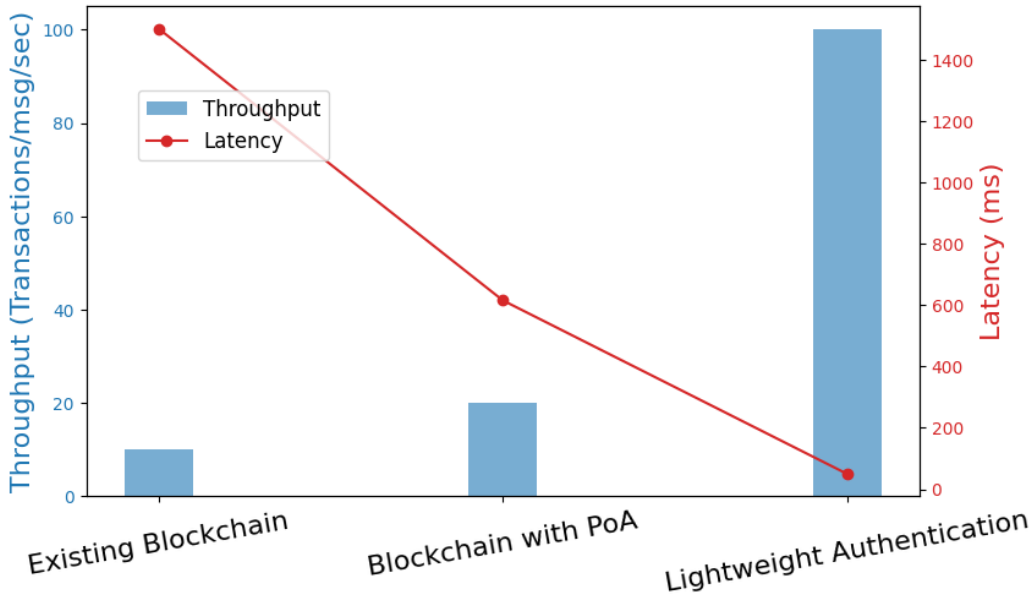

Figure 3.1: Performance results.

Figure 3.1 presents a comparative evaluation of widely adopted blockchain consensus mechanisms, a PoA-based blockchain configuration, and a lightweight authentication scheme based on XOR operations, measured in terms of latency and throughput. The results provide strong empirical support for the core design rationale of the proposed

framework. Specifically, the XOR-based method demonstrates minimal latency and high throughput, confirming its suitability for real-time communication tasks such as UAV telemetry and control signaling. In contrast, the PoA-based blockchain exhibits higher latency but offers deterministic performance and secure, tamper-resistant data logging, making it well-suited for mission-critical logging and audit functions where real-time speed is less critical. This dual-path design enables the system to meet the divergent demands of MUM-T networks: ultra-low latency for control operations and high integrity for data persistence. Overall, the numerical findings affirm that the integrated framework, merging PoA blockchain with XOR-based lightweight cryptography, strikes a practical and robust balance between efficiency and security, aligning well with the operational requirements of complex, time-sensitive military environments.

3.3 Simulation of the Design

To evaluate the performance, scalability, and practical feasibility of the proposed hybrid communication security framework for MUM-T systems, a series of targeted simulations were conducted. These simulations serve as a critical validation mechanism, complementing the analytical modeling presented earlier in the thesis. While analytical evaluations provide theoretical performance bounds under idealized assumptions, simulation allows for the observation of system behavior under more realistic and dynamic conditions, accounting for factors such as concurrent task execution, network latency, and the computational characteristics of cryptographic operations.

Given the dual-layered design of the framework, integrating blockchain-based data logging with lightweight cryptographic authentication, two distinct simulation environments were employed. The first, developed in Python using the SimPy discrete-event simulation library, models the end-to-end communication flow between the MAV and UAVs. It simulates both the generation and processing of blockchain transactions, as well as real-time control message exchange secured through XOR-based lightweight encryption. This setup offers fine-grained control over system

timing and event orchestration, enabling detailed measurement of latency, throughput, and resource utilization.

The second simulation environment, referred to as the Simulation with Blockchain, focuses exclusively on the blockchain component and is implemented using a real blockchain platform. It emulates the operational behavior of a PoA-based consensus network, offering insight into key performance metrics such as consensus latency, transaction validation overhead, and block generation dynamics under representative network conditions.

Together, these complementary simulation environments enable a thorough and multidimensional evaluation of the proposed framework. They capture both the high-frequency, real-time demands of UAV control and the integrity-focused requirements of mission data logging. The following subsections detail the implementation methodologies and present the results derived from each simulation environment, highlighting the framework's suitability for deployment in complex, time-sensitive MUM-T operations.

3.3.1 Simulation with python

To emulate the communication behavior and architectural logic of the proposed hybrid security framework, a discrete-event simulation was implemented using Python and the SimPy library. The simulation models a simplified MUM-T network composed of a single MAV and ten UAVs. It captures two parallel communication layers: the logging of mission-critical data via a blockchain-inspired mechanism, and the real-time exchange of control messages secured through lightweight XOR-based cryptography with integrity verification.

The simulation begins by defining two cryptographic utility functions. The first is a basic XOR cipher used to symmetrically encrypt and decrypt control messages, providing minimal computational overhead. The second is a truncated SHA-256 based checksum function that appends a short integrity code to each message. This checksum is verified upon receipt to detect tampering or data corruption.

Each UAV runs two concurrent processes within the simulation environment. The first process models blockchain transaction generation, where the UAV periodically produces a mission data payload, timestamped and uniquely identified. This transaction is submitted to a shared pool, simulating an asynchronous broadcast to the MAV. The second process models secure control communication. Every 100 milliseconds, the UAV constructs a control message, appends a checksum, encrypts the message using XOR, and then simulates its decryption and validation. Any checksum mismatch results in a simulated authentication failure.

The MAV runs a blockchain validator process that operates in a loop. At fixed intervals, it retrieves pending transactions from the pool, validates each transaction, assembles a block, and simulates broadcasting it back to the UAVs. Latencies associated with network transmission, transaction validation, block creation, and broadcasting are explicitly modeled using fixed delay values derived from expected performance ranges of embedded systems. For each processed transaction, the simulation tracks the time elapsed from its creation to its inclusion in a block.

Performance monitoring is embedded throughout the simulation. Global counters track the number of blockchain transactions submitted and processed, the number of control messages successfully authenticated, the number of failed checksum verifications, and latency metrics for both transaction confirmation and XOR operations. Additionally, several visualization functions are defined to produce graphical summaries of the simulation state, including latency trends, message throughput, and comparative latency-performance analysis between the blockchain and lightweight authentication components.

The entire simulation has been carefully configured to execute over a continuous 60-second period, throughout which all participating UAVs are programmed to operate simultaneously and maintain concurrent activity within the network. The configuration parameters, including message intervals, block creation delays, and processing times, can be adjusted to reflect varying mission profiles and hardware capabilities. This simulation serves as a foundational environment to explore how

the proposed framework performs under concurrent load, constrained processing resources, and real-time communication demands.

3.3.1.1 Results of python simulation

This section presents the outcomes of the Python-based simulation developed to evaluate the proposed hybrid communication security framework in a MUM-T environment. The primary goal of this evaluation is to determine whether the integration of a PoA-based blockchain with XOR-based lightweight cryptographic authentication can meet the stringent performance demands of real-time, mission-critical operations. The analysis focuses on two critical performance indicators: transaction latency in the blockchain component and a comparative assessment of latency and throughput between the blockchain and lightweight authentication mechanisms.

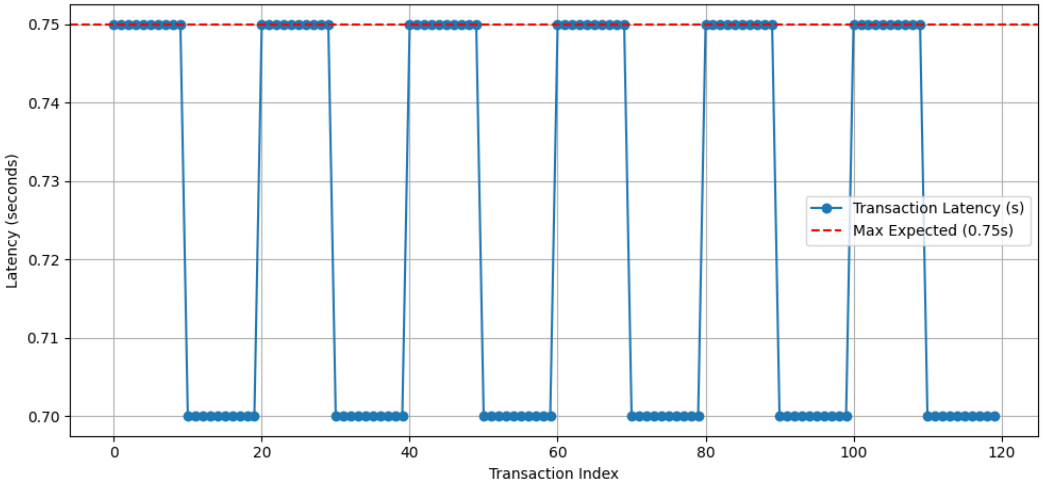

Figure 3.2: Blockchain transaction latency over time.

One of the most essential performance aspects of the blockchain layer is the time it takes for a UAV-generated mission-critical transaction to be confirmed and recorded on the ledger. The simulation results, visualized in the figure 3.2, reveal a stable and predictable system. Latency values consistently fall within a narrow range, alternating between approximately 0.70 and 0.75 seconds. This behavior aligns with the design of the MAV's block creation cycle, where transactions are grouped and processed in regular intervals. Notably, all transactions remained below the maximum expected threshold of 0.75 seconds, indicating that the blockchain layer fulfills its role in

providing secure and timely data logging. The uniformity in latency over the full duration of the simulation further reinforces the reliability and determinism of the validation and broadcasting process.

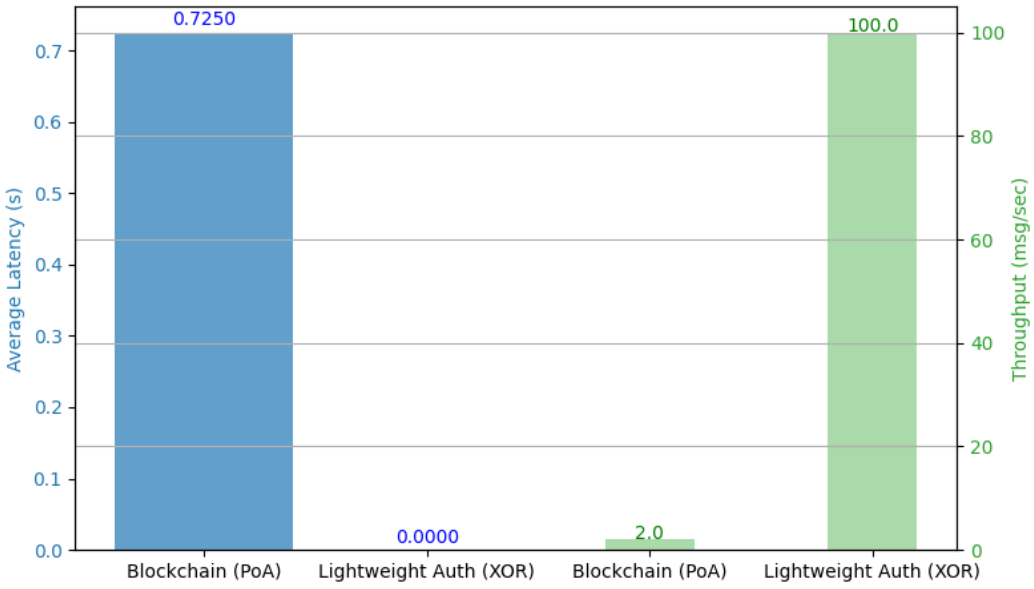

Figure 3.3: Latency and throughput comparison.

To complement the analysis of transaction timing, a second figure compares the average latency and throughput of the blockchain and lightweight authentication components. This comparison clearly illustrates the intended functional separation between the two communication layers. The blockchain component, tasked with preserving data integrity and enabling traceability, operates with an average latency of approximately 0.725 seconds and achieves a throughput of 2 transactions per second. In contrast, the XOR-based lightweight authentication mechanism demonstrates near-zero latency and supports a sustained throughput of 100 messages per second. This stark contrast affirms the architectural decision to handle time-sensitive control messages and log-oriented mission data through distinct channels. Each component operates within its optimal performance envelope, blockchain prioritizes security and auditability, while the XOR scheme ensures speed and efficiency for continuous command and telemetry exchanges.

In summary, the simulation results confirm that the proposed hybrid framework effectively balances the trade-offs between data integrity and real-time responsiveness. The

blockchain component performs reliably within acceptable latency bounds, ensuring mission-critical data is securely logged without delay violations. Simultaneously, the lightweight authentication layer provides the ultra-low latency and high throughput necessary for dynamic UAV coordination. These findings validate the core hypothesis of the study and demonstrate the feasibility of deploying the proposed architecture in operational MUM-T scenarios.

3.3.2 Simulation with OMNeT++

To model the operational behavior of the proposed hybrid communication security framework in a modular, networked setting, a simulation was developed using the OMNeT++ discrete-event simulation environment. This model aims to replicate a realistic MUM-T communication scenario by explicitly capturing asynchronous message flows, protocol execution timing, and the interaction between manned and unmanned aerial units within a controlled virtual topology.

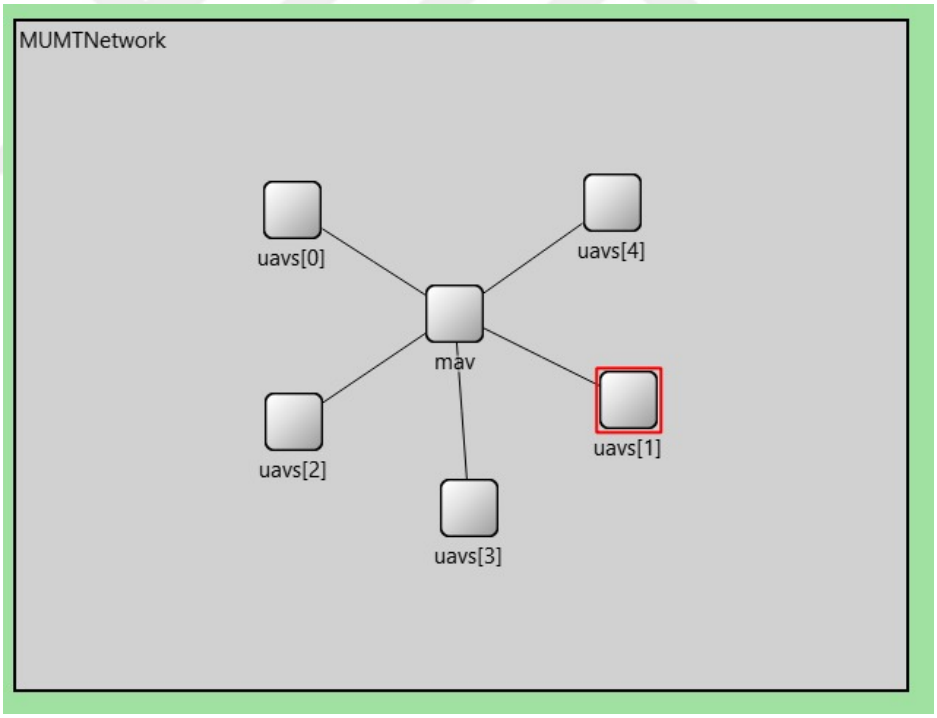

Figure 3.4: MUM-T network designed in OMNet++.

The simulated architecture reflects a hierarchical structure in which a single MAV operates as a central authority node, while multiple UAVs act as lightweight

clients. As depicted in Figure 3.4, the MAV is centrally positioned and directly connected to each UAV in a star-like configuration. This topology models a typical MUM-T communication setup in which the MAV coordinates and authenticates communication, acting as both a control authority and a blockchain validator.

In this model, each UAV performs two concurrent communication functions. The first involves the periodic generation of mission-critical data transactions, which are submitted to the MAV for logging in a simplified blockchain structure. These transactions simulate telemetry, reconnaissance, or targeting information, and are accumulated by the MAV until a block is created. The block creation process is time-driven and models the behavior of a PoA consensus mechanism, in which the MAV acts as the sole validator. Upon block generation, the MAV disseminates the confirmed data back to the network, ensuring tamper-resistant and auditable storage.

The second function implemented at each UAV concerns real-time control signaling secured using lightweight cryptographic techniques. Specifically, XOR-based symmetric encryption is employed to protect message confidentiality, while a checksum mechanism ensures integrity validation. These control messages are generated at high frequency to reflect time-sensitive operations such as UAV maneuvering and formation updates. Upon reception, the MAV decrypts and verifies each message, simulating real-time responsiveness and low processing overhead.

All communication activities, including transaction generation, block creation, encryption, decryption, and message validation, are triggered by internal timers and message events. This allows the simulator to capture realistic temporal behavior across distributed agents. Communication delays, cryptographic processing time, and validation intervals are explicitly modeled to assess their cumulative impact on performance.

The diagram in Figure 3.4 not only illustrates the static network topology but also highlights the communication flow paths and hierarchical authority distribution. The centralized design ensures that while UAVs can operate semi-independently, all critical communication is verified and logged by the MAV, thereby maintaining operational cohesion and data integrity.

This simulation architecture was deliberately designed to be modular and extensible. Parameters such as the number of UAVs, communication frequency, block interval, and cryptographic complexity can be modified independently, allowing the framework to be adapted for testing under a wide range of mission profiles and constraints. This flexibility makes the simulation suitable for future experimentation involving more complex consensus mechanisms, adversarial behavior, or heterogeneous UAV configurations.

In conclusion, the OMNeT++ simulation provides a structured, message-driven environment for examining the integrated behavior of secure communication layers in a MUM-T system. It models both blockchain-based data assurance and lightweight real-time control in a unified framework, supported by an explicit and easily interpretable network topology, as visualized in the accompanying diagram.

3.3.2.1 Results of OMNeT++ simulation

The OMNeT++ simulation environment was used to further assess the behavior of the proposed hybrid communication security framework under realistic network conditions. To evaluate system functionality and activity across both the blockchain and lightweight authentication components, scalar and vector performance metrics were recorded and visualized.

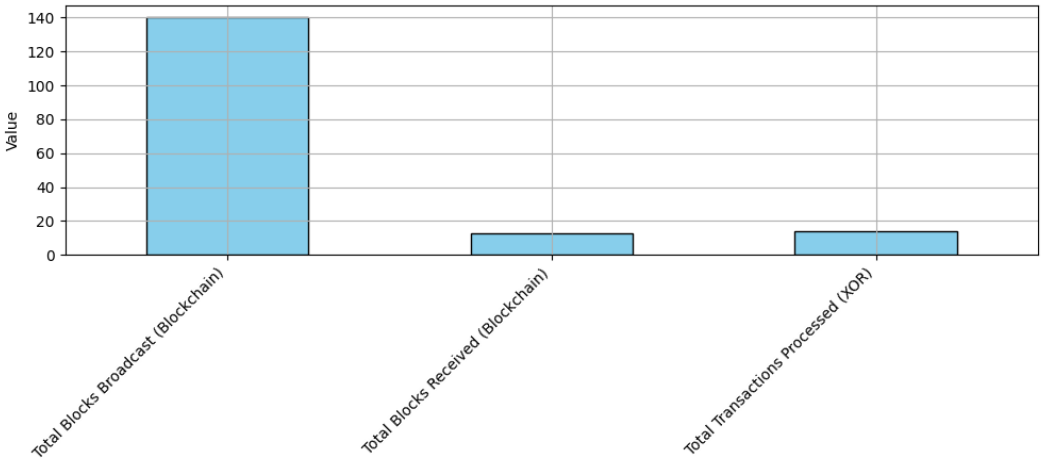

Figure 3.5: OMNeT++ scalar metrics.

The first result, illustrated in Figure 3.5, presents a summary of scalar metrics collected during the simulation. These include the total number of blockchain blocks broadcast

by the MAV, the total number of blocks received by the UAVs, and the total number of XOR-encrypted control messages processed within the network. The MAV is shown to have broadcast approximately 140 blocks during the simulation period, demonstrating that the blockchain component was actively generating and disseminating confirmed mission-critical data. The number of blocks received by the UAVs, although lower, confirms that dissemination mechanisms were functioning correctly. The discrepancy between broadcast and received block counts may be attributed to timing gaps at the end of the simulation window, propagation delays, or limitations in reception event logging. Furthermore, the scalar data shows that XOR-authenticated control messages were also successfully processed, indicating that the lightweight cryptographic layer operated in parallel with the blockchain mechanism. Together, these values validate that both security layers were engaged concurrently and continuously during the simulation, aligning with the architectural objectives of the framework.

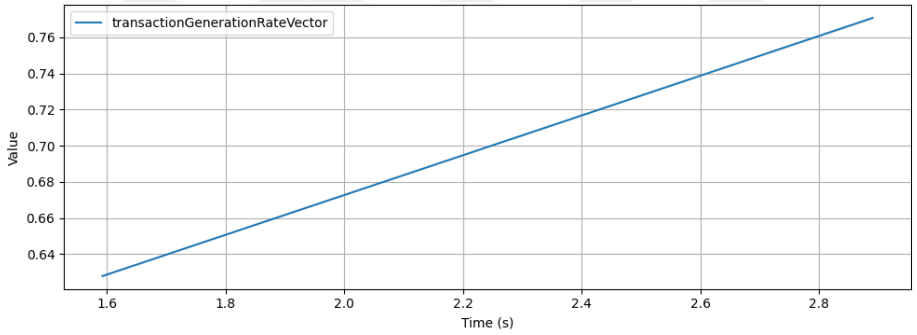

Figure 3.6: Time series for transaction generation rate vector.

In addition to scalar metrics, time-series data were recorded to observe dynamic changes in system behavior during runtime. Figure 3.6 presents the time series for a variable labeled transactionGenerationRateVector, which tracks the rate at which UAVs generate mission transactions. The plot reveals a steadily increasing trend from approximately 0.63 to 0.77 over a short time interval between 1.6 and 2.9 seconds. This increase reflects a consistent and growing transaction generation process, suggesting that UAV nodes progressively activate or ramp up their communication as the simulation begins. Although this plot captures only an early segment of the simulation, it serves as evidence that the system begins transaction generation immediately and sustains it without early failure or bottlenecks. The linear growth pattern may

result from either a cumulative rate across multiple UAVs or an aggregated view of system-wide transaction activity. This behavior supports the claim that the blockchain layer is capable of accommodating transaction input at increasing rates without degradation or delay during the early operational phase.

Combined, these results demonstrate that the OMNeT++ simulation faithfully reflects the intended design of the proposed framework. The blockchain component processes and propagates blocks consistently, while the lightweight cryptographic layer enables real-time message exchange. The scalar and vector metrics together confirm that the framework achieves its primary objective: supporting secure, dual-layer communication in a mission-oriented MUM-T architecture. These observations align with the system's analytical model and simulation design, providing further empirical validation for its operational feasibility.

4. CONCLUSIONS

This thesis has presented a novel secure communication framework specifically designed to address the dual requirements of data integrity and real-time responsiveness in MUM-T systems. Recognizing the performance and scalability limitations of conventional cryptographic approaches in resource-constrained aerial platforms, the proposed solution integrates a PoA-based blockchain mechanism with XOR-based lightweight cryptographic authentication. This hybrid architecture is intentionally structured to separate communication flows based on sensitivity and latency requirements, enabling high-frequency, low-overhead control messaging alongside secure, tamper-resistant logging of mission-critical data.

A formal hypothesis was established, asserting that this hybrid model could satisfy the stringent operational demands of MUM-T systems without incurring unacceptable trade-offs in performance, scalability, or energy efficiency. To rigorously evaluate this hypothesis, the thesis employed both analytical modeling and simulation-based validation. A discrete-event simulation environment developed in Python allowed for fine-grained control over cryptographic processes, transaction lifecycles, and communication timing. Empirical results from this simulation demonstrated that blockchain transaction confirmation latency remained well within the 0.75-second threshold, while XOR-based control messages consistently achieved sub-millisecond latency with minimal computational overhead, validating the framework's suitability for real-time UAV coordination.

To complement the fine-grained Python simulation, a second simulation environment was developed using OMNeT++ to assess network-level behavior under realistic deployment conditions. This model implemented modular representations of MAV and UAV nodes with message-driven logic and realistic temporal constraints. Scalar and vector metrics collected during simulation confirmed the correct and consistent operation of both blockchain and lightweight authentication layers in parallel.

The MAV successfully executed periodic block creation and dissemination, while UAVs maintained continuous transaction generation and control message exchange. Time-series analyses revealed stable communication patterns and sustained throughput under operational load, further reinforcing the system's scalability and responsiveness in dynamic mission contexts.

Collectively, the analytical findings and simulation results validate the effectiveness of the proposed communication architecture. The hybrid framework supports secure, efficient, and scalable communication across hierarchical UAV networks, enabling MUM-T systems to function reliably even in adversarial or resource-constrained environments. Its modular design and low resource footprint make it highly adaptable to diverse mission profiles, deployment scales, and system topologies, positioning it as a robust candidate for future autonomous aerial communication infrastructures.

Future work could explore adaptive key management mechanisms for the XOR-based authentication layer. While the current implementation assumes a static shared key between the MAV and UAVs, real-world deployments may benefit from dynamic key exchange protocols or periodic key rotation strategies to enhance confidentiality and mitigate risks associated with key compromise. Such mechanisms must be lightweight enough to align with the computational constraints of UAV platforms while ensuring forward secrecy and resistance to key-related attacks. Integration with hardware-based security modules, such as PUFs, may offer an additional layer of protection by binding key generation to device-specific characteristics.

Another promising direction involves the incorporation of stronger lightweight cryptographic primitives in place of or in combination with XOR operations. Algorithms such as PRESENT, SPECK, or Simon, designed specifically for resource-constrained environments, may provide enhanced security properties, including resistance to known cryptanalytic attacks, while maintaining low computational and energy overhead. Evaluating the trade-offs between cryptographic strength, latency, and power consumption across various mission profiles could guide the selection of optimal primitives tailored to different UAV roles or operational tiers within a MUM-T

network. Additionally, the integration of post-quantum lightweight cryptography may be considered to future-proof the system against emerging threats.

Beyond individual cryptographic enhancements, system-level improvements could focus on expanding the decentralization of the blockchain layer. While PoA offers deterministic consensus with minimal overhead, it inherently relies on a trusted validator, limiting fault tolerance in highly autonomous swarm scenarios. Future work could investigate distributed consensus protocols, such as PBFT, Raft, or DAG-based ledgers, that allow for peer-coordinated validation among UAVs. Furthermore, adversarial simulation scenarios, including message injection, GPS spoofing, communication jamming, or blockchain forking attacks, should be incorporated to rigorously test system resilience under hostile conditions. These evaluations would strengthen the framework's readiness for real-world deployment in contested or unreliable environments.

REFERENCES

[1] **Andrews, J.M.**, **Rusnock, C.F.**, **Miller, M.E. and Meador, D.P.** (2020). Simulation-based evaluation of the effects of varying degrees of control abstraction for manned-unmanned teaming on mental workload of Pilots, *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp.2680–2686.

[2] **He, J.**, **Liao, Z.**, **Qiu, Z. and Duan, K.** (2023). Modeling and analysis for manned-unmanned bistatic airborne radar, *2023 6th International Conference on Information Communication and Signal Processing (ICICSP)*, pp.585–591.

[3] **Roncolini, F.**, **Galante, G.**, **Quaranta, G. and Masarati, P.** (2024). Constrained Path planning for manned–unmanned rotorcraft teaming in Emergency Medical Service Missions, *CEAS Aeronautical Journal*, *15*(3), 619–641.

[4] **"Wright-Patterson**. *Medical Center Pharmacy: The intersection of innovation and dedication in an ever-changing world of Patient Care, " News*, `https://www.wpafb.af.mil/News/Article-Disp`.

[5] *Flight plan outlines next 20 years for RPA, Air Force*, `https://www.af.mil/News/Article-Display/Article/774728/flight-plan-outlines-next-20-years-for-rpa`.

[6] **Choi, J.K.**, **Lee, Y.T.**, **Park, H.**, **Kim, B. and Kim, B.W.** (2022). Challenges to the development of manned and unmanned Combat Systems, *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, pp.2362–2364.

[7] **Guo, Y. and Guo, Y.** (2023). CS-Laka: A lightweight authenticated key agreement protocol with Critical Security Properties for IOT Environments, *IEEE Transactions on Services Computing*, *16*(6), 4102–4114.

[8] **Lee, J. and Lee, M.** (2024). A blockchain system for MUM - T in Tactical Wireless Networks, *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp.73–75.

[9] **Yang, H.**, **Guo, Y. and Guo, Y.** (2024). Fault-tolerant security-efficiency combined authentication scheme for manned-unmanned teaming, *Computers & Security*, *146*, 104052.

[10] **UAV Navigation** (2024). *MUM-T (Manned Unmanned Teaming): What is it?*, `https://www.uavnavigation.com/company/blog/mum-t-manned-unmanned-teaming`, accessed: 2025-05-14.

[11] **Centre for Joint Warfare Studies (CENJOWS)** (2024). *Manned-Unmanned Teaming: Enhancing Lethality*, `https://cenjows.in/manned-unmanned-teaming-enhancing-lethality/`, accessed: 2025-05-14.

[12] **Bajwa, N.T.**, **Anjum, A. and Khan, M.A.** (2023). A blockchain-based Lightweight Secure Authentication and Trust Assessment Framework for IOT devices in fog computing, *2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET), vol. X*, pp.30–35.

[13] **Aanandaram, V. and Deepalakshmi, P.** (2024). Blockchain-based digital identity for secure authentication of IOT devices in 5G networks, *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, pp.1–6.

[14] **Babu, E.S.**, **Devi, A.A.**, **Kavati, I. and Srinivasarao, B.K.** (2023). Blockchain-based authentication mechanism for EDGE devices in fog-enabled IOT Networks, *TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON)*, pp.558–563.

[15] **Bathula, P.N. and Sreenivasulu, M.** (2025). An Integrated Blockchain Framework for Secure Data Sharing in IoT Fog Computing, *Tsinghua Science and Technology*, *30*(3), 957–977.

[16] **Pannyagol, B.B. and Deshpande, S.** (2024). Authentication in Blockchain-based IOT devices: A Review, *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, pp.1–5.

[17] **Harbi, Y.**, **Aliouat, Z.**, **Harous, S. and Gueroui, A.M.** (2024). Lightweight Blockchain-Based Remote User Authentication for Fog-Enabled IoT Deployment, *Computer Communications*, *221*, 90–105.

[18] **Abdalah, A.N.**, **Mohamed, A. and Hefny, H.A.** (2020). Proposed Authentication Protocol for IoT Using Blockchain and Fog Nodes, *International Journal of Advanced Computer Science and Applications*, *11*(4), 710–716.

[19] **Bai, L.**, **Hsu, C.**, **Harn, L.**, **Cui, J. and Zhao, Z.** (2023). A practical lightweight anonymous authentication and key establishment scheme for resource-asymmetric Smart Environments, *IEEE Transactions on Dependable and Secure Computing*, *20*(4), 3535–3545.

[20] **Bast, C. and Yeh, K.H.** (2024). Emerging authentication technologies for zero trust on the internet of things, *Symmetry*, *16*(8), 993.

[21] **Yuan, S.**, **Phan-Huynh, R. and Thornton, T.** (2023). An enhanced lightweight hash-chain-based multi-node mutual authentication algorithm for large and dense IOT networks, *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp.988–991.

[22] **V., A. and Kwatra, C.V.** (2023). Exploring state-of-the-art cryptography: A systematic exploration of advanced approaches for IOT device authentication, *2023 2nd International Conference on Ambient Intelligence in Health Care (ICAIHC), vol. 9.4, pp. 0*, pp.1–06.

[23] **Shah, N.H.**, **Ismail, S.A.**, **Azizan, A.**, **Anoop, A.**, **Khan, D.T. and Ahamed, S.B.** (2025). Lightweight Authentication Protocols in Internet of Things – A Review, *International Journal of Engineering Trends and Technology*, *73*(3), 104–119.

[24] **Elfar, M.**, **Zhu, H.**, **Cummings, M.L. and Pajic, M.** (2019). Security-aware synthesis of human-UAV protocols, *2019 International Conference on Robotics and Automation (ICRA)*, pp.8011–8017.

[25] **Chhetri, M.B.** *et al.* (2024). Towards human-ai teaming to mitigate alert fatigue in security operations centres, *ACM Transactions on Internet Technology*, *24*(3), 1–22.

[26] **Stensrud, R.**, **Valaker, S. and Mikkelsen, B.** (2023). Orchestrating humans and teammates to counter security threats: human-autonomy teaming in high and low environmental complexity and dynamism, *AHFE International*.

[27] **O'Neill, T.A.**, **McNeese, N.J.**, **Barron, A. and Schelble, B.** (2022). Human–Autonomy Teaming: A Review and Analysis of the Empirical Literature, *Human Factors*, *64*(5), 904–938.

[28] **Chen, Y.**, **Liu, G.**, **Zhang, Z. and He, L.** (2022). Secure Remote Control for Multi-UAV systems: A Physical Layer Security Perspective, *2022 IEEE International Conference on Unmanned Systems (ICUS)*, pp.916–921.

[29] **Tahir, M.**, **Sardaraz, M.**, **Muhammad, S. and Khan, M.S.** (2020). A lightweight authentication and authorization framework for blockchain-enabled IOT network in health-informatics, *Sustainability*, *12*(17), 6960.

[30] **Ahmed, M.T.A.**, **Hashim, F.**, **Hashim, S.J. and Abdullah, A.** (2023). Authentication-chains: Blockchain-inspired Lightweight Authentication Protocol for IOT Networks, *Electronics*, *12*(4), 867.

[31] **Chaudhry, N. and Yousaf, M.M.** (2018). Consensus algorithms in Blockchain: Comparative Analysis, challenges and opportunities, *2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Dec*.

[32] **Hussein, Z.**, **Salama, M.A. and El-Rahman, S.A.** (2023). Evolution of blockchain consensus algorithms: A review on the latest milestones of

blockchain consensus algorithms, *Consensus algorithms in Blockchain: Comparative Analysis, challenges and opportunities*, 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Dec. 2018.

[33] **Azzarello, L.** *Building a proof of authority network with parity, https://medium.com/quantstamp/building-a-proof-of-authority-network-with-parity-654d18bce321*.

[34] *Setup your own private proof-of-authority ethereum network with Geth, HackerNoon, https://hackernoon.com/setup-your-own-private-proof-of-authority-ethereum-network-with-geth-9a0a3750cda8*.

APPENDICES

APPENDIX A : Python Simulation Codes
APPENDIX B : OMNeT++ Simulation Codes

Appendix A: Python Simulation Codes

Algorithm 2 Simulation Logic of the Adaptive Blockchain-Cryptography Framework

Initialize simulation environment and parameters
Define XOR-based encryption and checksum functions
Launch MAV blockchain validator process
for each UAV $i = 1, 2, \ldots, N$ **do**
    Start `uav_transaction_process` for mission data
    Start `uav_control_process` using XOR authentication
end for
while simulation is running **do**
    if transaction pool contains pending transactions **then**
        MAV retrieves and validates transactions
        Create a new block with validated transactions
        Broadcast the block to all UAVs
        Record transaction latency metrics
    end if
end while
Log total processed messages and authentication results
Generate performance plots (latency, throughput, comparison)

Appendix B: OMNeT++ Simulation Codes

Algorithm 3 OMNeT++ Simulation Logic for MUM-T Secure Communication Framework

Initialize network with 1 MAV node and N UAV nodes
Assign roles: MAV $\rightarrow$ validator; UAVs $\rightarrow$ data generators
for each UAV **do**
    Periodically generate control messages
    Encrypt messages using XOR-based lightweight authentication
    Transmit messages to MAV with timestamp
    Periodically generate mission-critical data as blockchain transactions
    Send transactions to MAV for validation
end for
MAV Process:
loop
    Collect transactions from UAVs
    if transaction pool not empty **then**
        Validate each transaction
        Create a new block with valid transactions
        Broadcast the block to all UAVs
    end if
    Listen for incoming control messages
    Verify XOR checksum of each control message
end loop
Monitor: Log control throughput, block generation, and transaction latency

CURRICULUM VITAE

Name SURNAME: Halimcan Yasar

EDUCATION:

- **B.Sc.:** 2022, Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Electronics and Communication Engineering

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2022-Still Software Design Engineer at Turkish Aerospace.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Yaşar, H.**, and Bahtiyar, Ş. (2024) 'Secure communication for mum-T: A Blockchain and lightweight cryptography framework', *2024 17th International Conference on Security of Information and Networks (SIN), pp. 1–8.*, doi:10.1109/sin63213.2024.10871653.

OTHER PUBLICATIONS, PRESENTATIONS AND PATENTS:

- **Yildiz, G. et al.** (2022) ‘Antenna excitation optimization with deep learning for microwave breast cancer hyperthermia’, Sensors, 22(17), p. 6343. doi:10.3390/s22176343.
- **Yildiz, G. et al.** (2022), "Antenna Array Optimization via Deep Learning For Breast Cancer Microwave Hyperthermia Application: Preliminary Results," 2022 IEEE International Symposium on Antennas and Propagation and USNC-URSI Radio Science Meeting (AP-S/URSI), Denver, CO, USA, pp. 697-698, doi: 10.1109/AP-S/USNC-URSI47032.2022.9887012.
- **Tashan, W. et al.** (2024) ‘Rain rate and rain attenuation analysis over millimeter wave in microwave 5G/6G Link Systems’, AIP Conference Proceedings, 3240, p. 020008. doi:10.1063/5.0240181.