Secure Identity Management System in Unmanned Aerial Vehicles Network

Hulya Dogan
940416

Submitted to Swansea University in fulfilment
of the requirements for the Degree of PhD of Science

Doctor of Philosophy

Swansea University
Prifysgol Abertawe

Department of Computer Science
Swansea University

November 21, 2024

Declaration

This work has not been previously accepted in substance for any degree and is not being con- currently submitted in candidature for any degree.

Signed ....[redacted].. (candidate)

Date ....

Statement 1

This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed ......[redacted]... (candidate)

Date ....

Statement 2

I hereby give my consent for my thesis, if accepted, to be made available for photocopying and inter-library loan, and for the title and summary to be made available to outside organisations.

Signed ....[redacted]... (candidate)

Date ....

I would like to dedicate this thesis to the Turkish Ministry of Education.

All glory to Turkey's honourable martyrs and veterans.

Abstract

In recent years, rapid advancements in digital transformation and communication technologies have led to the widespread adoption of autonomous systems, particularly Unmanned Aerial Vehicles (UAVs), in societal and industrial applications. The integration of smart cities, the Internet of Things (IoT), and 5G technologies has enabled UAVs to be utilized effectively in more complex and dynamic tasks. For instance, during the COVID-19 pandemic, UAVs played critical roles in maintaining social distancing, delivering medical supplies, and managing crowds. Such contemporary applications have once again highlighted the importance and potential of UAV networks. The flexibility and versatility offered by UAVs facilitate the development of innovative solutions across a wide spectrum—from agriculture to logistics, disaster management to security. Specifically, swarm UAV systems surpass the limitations of individual vehicles, providing advantages such as real-time data collection, large-scale monitoring, and the parallel execution of complex tasks. However, the effective and secure operation of such systems depends on the reliability and efficiency of intra-network communication and identity management protocols.

In today's cyber-physical systems, security threats and cyber-attacks are becoming increasingly sophisticated. UAV networks are not exempt from these threats; risks such as identity spoofing, data manipulation, and Denial-of-Service (DoS) attacks endanger the success and security of operations. Addressing these security vulnerabilities is of vital importance, especially in sensitive areas like the protection of critical infrastructures, border security, and emergency interventions.

This thesis aims to enhance the operational efficiency and security of UAV networks by developing a lightweight and dynamic identity management protocol alongside a consensus mechanism specifically optimized for UAV networks. The proposed identity management protocol employs symmetric cryptography and hash functions, featuring low computational and communication overhead while adapting to dynamic network topologies. The protocol is resilient against common security threats such as identity spoofing, replay attacks, and man-in-the-middle attacks. Furthermore, leveraging the advantages of blockchain technology, a fast and efficient consensus mechanism suitable for UAV networks has been designed. Instead of energy-intensive and high-latency methods like traditional Proof of Work (PoW), an adapted version of the Practical Byzantine Fault Tolerance (PBFT) algorithm and a Fuzzy C-Means Clustering algorithm (FCMCA) are utilized to reduce latency and computational costs. This mechanism enables secure and effective data sharing and decision-making processes among UAVs. Simulations and performance analyses have demonstrated that the proposed solutions provide lower latency and reduced resource consumption compared to existing methods, while exhibiting high resilience against security threats. These findings contribute significantly to the safer, more efficient, and scalable use of UAV networks in real-world applications. The study aims to establish a solid foundation for the evolution and sustainability of UAV networks and serves as a valuable reference for future technological developments and applications.

Keywords: Unmanned Aerial Vehicles (UAVs), UAV Networks, Identity Management System, Consensus Protocol, Blockchain, Practical Byzantine Fault Tolerance (PBFT), Fuzzy C-Means Clustering Algorithm (FCMCA), Swarm UAV Systems, Symmetric Cryptography, Cyber-physical Systems, Security Threats, Dynamic Network Topologies.

Acknowledgements

This thesis is presented as the last part of my PhD's degree in the Computer Science department at Swansea University. First of all, I would like to express my deepest gratitude to my supervisor, Dr Anton Setzer. His patience, motivation, and wide knowledge helped me overcome many critical situations and contributed significantly to my graduation experience. This would not have been possible without his valuable feedback. I want to thank my husband, Abdullah, and my family, for their support throughout my life. I owe them all my success.

Finally, I offer my gratitude to Turkey's Ministry of Education for giving me support until the end of my educations. The financial support provided by the Turkish Ministry through the YLSY program is appreciated.

Hulya Dogan, 21 November 2024

List of Acronyms

ABAC - Attribute-based access control

AC - Assignment Confidence

ACS - Asynchronous Common Subset

AODV - Ad hoc On-Demand Distance Vector

AI - Artificial Intelligence

AES - Advanced Encryption Standard

APTs - Advanced Persistent Threats

APNs - Authorized Proxy Nodes

BS - Base Station

DSK - Dynamic Secret Key

DoS - Denial-of-Service Attack

DY - Dolev-Yao Threat Model

E2E - End-to-End

ECC - Elliptic Curve Cryptography

FCMCA - Fuzzy C-Means Clustering Algorithm

FIMS - Federated Identity Management Systems

GDPR - General Data Protection Regulation

HMACs - Hash-based Message Authentication Codes

HTCC - Hierarchical Trust-Based Coordination Component

IDMS - Identity Management Systems

IoT - Internet of Things

ISO - International Organization for Standardization

KDFs - Key Derivation Functions

LBFT - Lightweight Byzantine Fault Tolerance

LTCC - Localized Trust Coordination Component

ML - Machine Learning

MFA - Multi-factor Authentication

MitM - Man-in-the-Middle Attack

MV - Membership Vector

NCT - Network Coordination Tier

NTP - Network Time Protocol

OLSR - Optimized Link State Routing

PBFT - Practical Byzantine Fault Tolerance

PDMC - Proximal Node Discovery and Monitoring Component

PDR - Packet Delivery Rate

PII - Personally Identifiable Information

PKI - Public Key Infrastructure

PUFs - Physical Unclonable Functions

PPB - Private, Permissioned Blockchain

PC - Proof of Cluster

PTP - Precision Time Protocol

PoW - Proof of Work

PoS - Proof of Stake

SABEC - Secure and Adaptive Blockchain-Enabled Coordination Protocol

SBCC - Secure Border Coordination Component

SMPC - Secure Multi-party Computation

SSO - Single Sign-On

SSI - Self-sovereign Identity

SHA-256 - Secure Hash Algorithm 256-bit

TATs - Trust Assessment Transactions

TET - Trust Evaluation Tier

TTC - Two-Tier Consensus Mechanism

TR - Trust Rating

TV - Trust Value

UID - Unique Identifier

UAV - Unmanned Arial Vehicle

ZRP - Zone Routing Protocol

List of Publications

During my PhD studies, I engaged in various academic research and development activities. Throughout this period, I authored a conference paper and prepared an academic poster as the lead author. Additionally, I have a journal article currently under review for publication. Each of these works reflects the research process of my doctoral thesis, the findings obtained, and their contributions to the scientific community.

The conference paper I prepared is directly related to the research within my thesis and has been accepted for presentation at both national and international conferences. In these papers, I presented the results of my theoretical and practical research in detail to the scientific community. Similarly, I prepared an academic poster summarizing my work and emphasizing the key aspects of my thesis. The poster aimed to present my research in a concise and visual format, thereby making it accessible to a broader audience and enhancing its comprehensibility. Furthermore, one of the significant studies conducted during my doctoral journey is currently under the publication process. This work includes the latest findings of my thesis and aims to contribute more broadly to the scientific literature.

Below is a detailed list of the academic works I have prepared throughout my doctoral education. This list comprehensively demonstrates the knowledge and contributions I have produced during my academic journey and highlights how each publication is connected to the topic of my thesis.

Conference Papers

- Dogan, H. (2023). Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme. *2023 7th International Conference on Cryptography, Security and Privacy (CSP)*, Tianjin, China, 2023, pp. 13-21. https://ieeexplore.ieee.org/document/10235922.

- Dogan, H. and Setzer, A. (2025). SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles(UAVs) Network. In Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP; ISBN 978-989-758-735-1; ISSN 2184-4356, SciTePress, pages 377-388. DOI:10.5220/0013330500003899.

Poster

- Dogan, H. (2024). Blockchain takes flight: Secure and efficient environment for swarm of drones. *20th May 2024 PGR Conference, Swansea University, no. 2*.

List of Figure&Table

Figures

Figure 1: Communication method for UAV network

Figure 2: SABEC communication model

Figure 3: SABEC network model components

Figure 4: Blockchain system components

Figure 5: Blockchain architecture in SABEC protocol

Figure 6: The network architecture and components of the proposed IDMS

Figure 7: The design of the proposed Secure Authentication Protocol

Figure 8: Registration Phase

Figure 9: Authentication Stage

Figure 10: Data sending phase

Figure 11: The data received by the UAV device (program execution)

Figure 12: The data recorded by the Base Station Service (program execution)

Figure 13: The query results of the ProVerif

Figure 14: Leader drone selection in the UAV network

Figure 15: The architecture of the blockchain-enabled protocol in the UAVs

Figure 16: Diagram of the SABEC protocol

Figure 17: NS3 Key components & Significance

Figure 18: Packet Delivery Rate vs. Number of Malicious Nodes

Figure 19: Coordination Overhead vs. Number of Malicious Nodes

Figure 20: End-to-End Delay vs. Number of Malicious Nodes

Figure 21: Blockchain storage growth Comparison

Figure 22: Energy consumption vs. Number of Nodes

Figure 23: Energy efficiency vs. Number of Fault Nodes

Figure 24: Real case study of the proposed Identity Management System

Figure 25: Fire Monitoring Scenario

Tables

Table 1: Symbols and Descriptions

Table 2: Symbols and Descriptions for data sending stage

Table 3. Comparison the proposed authentication scheme with other works

Table 4: Secure authentication protocol memory consumption

Table 5: Secure authentication protocol Cost Comparisons

Table 6: Algorithm for Cluster Membership Validation

Table 7: Algorithm for FCM-based Trust Assessment in the Data Consensus Stage

Table 8: Algorithm for Trust-based Consensus Participant Selection in the Decision Consensus Integration

Table 9: Algorithm for Trust Assessment

Table 10: Simulation Parameters

Table 11: Key components of the simulation

Table 12: The performance analysis of SABEC

Table 13: Comparison Security Features of SABEC

Table of Contents

Declaration 2

Abstract 6

Acknowledgements 8

List of Acronyms 9

List of Publications 12

List of Figure&Table 13

Table of Contents 15

Chapter 1 Introduction 18

1.2 Motivations 21

1.3 Problem Statement 22

1.4 Research Objectives 24

1.5 Research Questions 26

1.6 Significance of the Study 32

1.7 Scope and Limitations 34

1.7.1 Scope 34

1.7.2 Limitations 35

1.8 Contributions 36

1.9 Thesis Structure 38

Chapter 2 Literature Review 40

Chapter 3 52

Analysis of UAV Network Requirements 52

3.1 Analysis of Key Requirements 52

3.2 Adversary Models 54

3.3 Security Goals 55

3.4 Defence Mechanisms Against Known Attacks 57

3.5 Privacy and Security Considerations 59

3.6 Integration of Blockchain Technology 61

3.7 Practical Requirements and Considerations 63

3.8 Risk Assessment and Analysis 64

3.9 Summary 66

Chapter 4 Methodology 67

4.1 Network Model Design 70
4.2 Authentication Protocol Development 74
4.3 System Architecture and Application Development 74
4.4 Blockchain-Enabled Decision-Making Mechanism 75
4.5 Security Verification and Formal Analysis 79
4.6 Simulation and Experimental Setup 80
4.7 Summary 81
Chapter 5 83
Design and Development of Identity Management System 83
Chapter 6 87
A Secure and Dynamic Authentication Protocol for UAVs Network 87
6.1 Overview of the Authentication Scheme 87
6.1.1 Offline Phase 91
6.1.2 Registration Phase 91
6.1.3 Authentication and Key Establishment Phase 92
6.1.4 Data Sending Phase 94
6.2 Implementation and Testing 96
6.3 Security Analysis of the Authentication Protocol 99
6.4 Performance Evaluation 106
6.5 Summary 116
Chapter 7 117
A Secure and Adaptive Blockchain-Enabled Coordination (SABEC) Protocol for UAVs Network 117
7.1 Overview of the SABEC Protocol 119
7.2 System Architecture of the SABEC Protocol 127
7.2.1 Fuzzy C-Means (FCM) clustering Algorithm 130
7.2.2 Drone Cluster Membership and Selection in SABEC 131
7.3 Implementation and Testing of the Consensus Protocol 136
7.4 Simulation Setup 143
7.5 Security analysis of SABEC 146
7.6 Performance Analysis 150
7.6.1 Comparative Analysis with Traditional Protocols 150
7.7 Conclusion 159
Chapter 8 160

Case Studies and Real-World Deployment 160

8.1 Description of Case Study: Simulation of a Fire Monitoring Scenario and Byzantine Drone Detection in Swansea 161

Chapter 9 163

Discussion and Conclusions 163

9.1 Summary of the Research Findings 163

9.2 Contributions of the Study 163

9.3 Implications for Identity Management in UAV Networks 164

9.4 Recommendations for Future Research 165

9.5 Conclusion 165

Bibliography 167

Chapter 1

Introduction

The Industry 4.0 revolution, alongside the widespread integration of autonomous robotic systems (F. Cunico et al., 2024), has engendered profound transformations across various sectors (Asilian et al., 2023; Yucesoy & Sahin, 2024), ranging from healthcare (Asilian et al., 2023) and autonomous vehicle technologies to smart manufacturing lines (Tang et al., 2024) and agricultural automation (Pajany et al., 2024). This paradigm shift in robotics research signifies a substantial transition from endeavours to enhance the capabilities of individual robots to exploring the collective behaviours and collaborative abilities of multi-robot or swarm robotic systems (Chung et al., 2018). The deployment of simple individual robot actions within integrated systems, where numerous robots collaborate on shared tasks, has enabled the effective execution of more complex and high-level operations (Jin et al., 2003). While individual robots may possess relatively limited capabilities in isolation, they can exhibit intricate collective behaviours at the multi-robot level, thereby augmenting the overall performance and adaptability of the system (Queralta et al., 2020). Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as critical aerial platforms that facilitate and accelerate a myriad of real-world applications (Pajany et al., 2024). For instance, in smart cities, UAVs enhance decision-making processes through real-time data collection and analysis capabilities in applications like traffic monitoring and public safety (Amarcha et al., 2024). By enabling more efficient utilization of airspace, UAVs contribute to the development of real-time, efficient, and secure environmental monitoring applications, forming the cornerstone of modern concepts such as smart cities and smart manufacturing (Asilian et al., 2023). A commonality among these applications is the shared requirement for airspace control and navigation (Salim et al., 2024). Particularly, large-scale environmental monitoring and control operations necessitate the coordination and collaboration of multiple UAVs due to the limited mobility and operational capabilities of individual units (Chen et al., 2024). In this context, the development of coordinated control strategies and practical consensus algorithms has become imperative to ensure the stability, security, energy efficiency, and reliability of UAV systems (Alsamhi et al., 2022). In multi-UAV systems, not only must physical movement and positioning be optimized, but information sharing and decision-making processes also require enhancement to execute tasks effectively (Jin et al., 2024). However, achieving these objectives necessitates more than merely monitoring and tracking targets; it is critically important to accurately identify these targets and reliably manage their identities (Jiang et al, 2020; Liang et al., 2024). Identity management in UAV networks emerges as a vital element not only for enhancing operational efficiency but also for providing protection against security threats (Khan et al., 2024). In complex and deceptive environments, the presence of false targets moving alongside real threats significantly complicates the effectiveness and reliability of UAV networks (Jiang et al., 2024). A secure identity management prevents the pursuit of incorrect objectives, allowing for more efficient use of resources and minimizing operational risks (Bertrand et al., 2024). Therefore, developing advanced identity management strategies and security protocols is essential to ensure the effective and secure operation of UAV networks (Kundu et al., 2024). Despite the rapidly increasing use of UAV networks today, the identity management of targets within these systems has not yet been fully resolved (Bhanurangarao et al., 2024). Particularly in dynamic and variable environments, the continuous fluctuation in the number of targets, the handover of targets exiting one UAV's sensor range to another, and the accurate and reliable management of identity information during this process pose significant challenges (Selvam & Lieb, 2024). Moreover, the heterogeneous structure and limited resources of UAV networks hinder the direct application of traditional authentication and security mechanisms (Fang et al., 2022). The absence of inadequacy of authentication protocols can expose UAV networks to serious risks in terms of both security and operational efficiency (Hughes et al., 2024). For example, the infiltration of the network by adversarial entities or malicious actors using counterfeit UAVs or signals can jeopardize the system's integrity and reliability. Consequently, developing reliable, lightweight, and efficient identity management strategies in UAV systems is a critical step toward the secure and sustainable advancement of these technologies (Li et al., 2021).

This thesis presents a comprehensive approach aimed at addressing the existing limitations and security vulnerabilities in identity management within Unmanned Aerial Vehicle (UAV) networks. The primary objective is to enhance the security, efficiency, and scalability of UAV systems through a two-tiered solution framework. In the first phase, a lightweight authentication protocol tailored for resource-constrained environments is designed and evaluated to ensure secure and dynamic identity verification of devices within the network. In the second phase, a blockchain-based data management protocol is developed, incorporating a practical and energy-efficient consensus mechanism to ensure the secure storage of critical data collected across the network. The proposed authentication protocol establishes mutual authentication between UAV nodes and the ground control/base station, thereby strengthening the integrity and reliability of the network. It addresses essential security requirements such as data confidentiality, session key establishment, and identity privacy, while also exhibiting resilience against prevalent attack vectors including impersonation, replay attacks, eavesdropping, and identity cloning. These security properties are rigorously validated through formal security analysis and conventional cryptographic evaluation methods. In the second phase, the focus shifts to ensuring that data generated by authenticated devices within the network is stored securely, with integrity and immutability. To this end, a blockchain-integrated solution is introduced, supported by a consensus mechanism that employs the Fuzzy C-Means Clustering Algorithm (FCMCA) alongside a hybrid task assignment scheme based on Proof of Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) algorithms. This mechanism is adaptively designed to minimize energy consumption while enhancing overall system performance. Within the proposed framework, devices that exceed a predefined trust threshold are dynamically selected as leader UAVs via a leader election algorithm. These leaders collect and transmit status information regarding neighbouring UAVs to a server of the ground control/base station. The server then aggregates the received data using the consensus algorithm, forwards the validated information to the decision-making layer, and stores it securely and immutably on the blockchain. This architecture ensures data security, privacy, and integrity, thereby enabling the establishment of a dynamic and scalable UAV network infrastructure. The proposed consensus protocol has been thoroughly evaluated using the NS3 simulation environment. Experimental results demonstrate significant performance improvements over existing approaches in terms of packet delivery ratio, network overhead, and end-to-end latency. Moreover, the establishment of secure consensus among multiple UAV systems markedly enhances network energy efficiency and connection stability, contributing to the long-term sustainability of UAV applications.

In conclusion, this thesis proposes a secure, efficient, and scalable management framework to address the critical challenges associated with identity management and secure data handling in UAV networks. The proposed authentication protocol and blockchain-based data management mechanism collectively ensure the reliable and secure operation of UAV systems, contribute novel insights to the existing body of research, and lay a robust foundation for future advancements in the field.

1.2 Motivations

Recent technological advancements have facilitated the widespread adoption of Unmanned Aerial Vehicles (UAVs) in both civilian and military sectors, enabling their effective utilization in complex missions (Rodionov et al., 2023). UAVs have assumed critical roles in applications such as disaster management, environmental monitoring, logistics support, and security operations (Badshah et al., 2024; Alva et al., 2024). With the increasing capabilities of these platforms, there is a growing need for systems where multiple UAVs operate in a coordinated manner. Multi-UAV systems offer advantages like expanded surveillance coverage, parallel task execution, and enhanced operational efficiency, surpassing the limitations of single-vehicle deployments (Duan et al., 2023; Mishra et al., 2023). However, the effective and reliable operation of multi-UAV networks introduces various technical and security challenges. One of the foremost difficulties faced by UAVs, especially in dynamic and adversarial environments, is the accurate and trustworthy management of identities for targets and other networked vehicles (Garg et al., 2018; Thangam et al., 2024). Deceptive signals, counterfeit targets, and identity spoofing attempts threaten the integrity of UAV networks and jeopardize mission success (Arthur et al., 2019). Such security vulnerabilities can lead to mission-critical information falling into unauthorized hands and result in erroneous operational decisions, posing significant risks (Pandey et al., 2022).

Various approaches have been proposed for security and identity management in UAV networks (Xu et al., 2024; Pajany et al., 2024; Kundu et al., 2024). Nonetheless, these methods often rely on complex algorithms requiring high computational power and energy consumption, rendering them impractical for resource-constrained UAVs (Jaiswal et al., 2024). Additionally, traditional security protocols struggle to adapt to dynamic network topologies and the constantly changing connectivity conditions of mobile vehicles (Arafat et al.,2019). Therefore, there is a pressing need for lightweight, scalable, and secure identity management mechanisms tailored to the unique requirements of UAV networks (Lei et al., 2021; Tan et al., 2022).

This system integrates a lightweight identity management mechanism with blockchain-based trust coordination, employing a two-tier consensus mechanism to facilitate dynamic leader election and trust-driven decision-making processes. The ultimate objective of the study is to establish a practical infrastructure enabling UAV networks to operate autonomously, securely, and scalable in complex, dynamic, and potentially adversarial environments.

In conclusion, the outcomes of this research are expected to contribute to the safer and more effective use of UAV networks, enhancing operational success in areas such as emergency response, military operations, and the monitoring of critical infrastructures. Additionally, the adaptability of the proposed approaches to other autonomous systems and Internet of Things (IoT) applications will illuminate a broad spectrum of technological advancements.

1.3 Problem Statement

Unmanned Aerial Vehicles (UAVs) have gained significant prominence in both civil and military domains in recent years, facilitated by technological advancements and decreasing costs (Sullivan et al., 2006; Sohoni et al., 2024). The effective utilization of UAVs in critical applications such as disaster management, environmental monitoring, logistical support, and security operations has elevated their strategic importance (Badshah et al., 2024; Cheng et al., 2024). Particularly, multi-UAV systems, where multiple UAVs operate in a coordinated manner, offer advantages such as efficient monitoring of large areas and the parallel and effective execution of tasks, thereby surpassing the limitations of single-vehicle deployments (Mondal et al., 2024).

However, the reliable and efficient operation of multi-UAV networks introduce various technical and security challenges (Xiao et al., 2024). One of the most critical issues for UAVs operating in dynamic, heterogeneous, and potentially adversarial environments is the trustworthy, accurate, and rapid management of the identities of devices and targets within the network (Li et al., 2021). Traditional authentication and security protocols are impractical in these settings due to the limited processing power, memory capacity, and energy resources of UAVs (Lei et al., 2021). Furthermore, the constantly changing network topologies and connectivity conditions resulting from the mobility of UAVs complicate secure communication and identity management (Warrier et al., 2024).

In current systems, identity spoofing, deceptive signals, and malicious attacks severely threaten the integrity of UAV networks and the security of operations (Arthur et al., 2019). The movement of false targets alongside real threats can mislead UAVs toward incorrect objectives, leading to resource wastage and increased operational risks (Hu et al., 2020). This situation can result in the failure of mission-critical tasks and potentially serious security vulnerabilities (Alotaibi et al., 2024). Additionally, the secure storage and sharing of data within the network necessitate a scalable and distributed architecture without a single point of failure (Liu et al., 2024). Traditional centralized data storage approaches are inadequate in meeting these requirements and pose security risks (Wang et al., 2024).

Various solutions have been proposed in the literature for security and identity management in UAV networks. However, these approaches often rely on complex cryptographic algorithms that require high computational power and energy consumption, rendering them impractical for UAVs with limited resources (Yang et al., 2023). Moreover, many of these solutions are inadequate in adapting to dynamic network conditions and the constantly changing connectivity states of mobile vehicles (González et al., 2024). Therefore, there is an urgent need for lightweight, scalable, and secure identity management mechanisms tailored to the unique requirements of UAV networks (Kourtis et al., 2023).

In recent years, blockchain technology, with its distributed, secure, and immutable structure, offers a potential solution to the issues of data security and integrity in UAV networks (Soliman et al., 2024). Hence, it is necessary to develop fast, secure, and efficient blockchain consensus mechanisms specifically designed to the unique requirements of UAV networks (Alsamhi et al., 2022). In this context, the following fundamental problems exist within UAV network environments:

1. Need for Reliable Identity Management: In heterogeneous and dynamic UAV networks, it is essential to reliably and effectively authenticate and manage the identities of devices and targets. Existing authentication protocols are insufficient due to the limited resources of UAVs and variable network conditions. Studies have shown that conventional identity management systems lack the adaptability needed for resource-constrained UAV environments, leading to potential vulnerabilities and security gaps (Karmakar et al., 2023; Javed et al., 2024). Novel identity authentication methods that consider the specific limitations of UAVs, such as lightweight cryptographic mechanisms, are therefore crucial to ensuring secure operation. (The dynamic authentication protocol developed in this study addresses this gap. A detailed explanation can be found in Chapter 6)

2. Requirement for Secure Communication and Distributed Data Storage: To securely transmit and store the critical data collected by UAVs, a scalable and distributed architecture without a single point of failure is required. Traditional centralized storage solutions are inadequate as they pose scalability limitations and significant security risks, including vulnerability to single-point failures (Abbas et al., 2024). Recent research emphasizes the importance of employing blockchain or other distributed ledger technologies to enhance resilience and data integrity in UAV networks (Phadke et al., 2022). Such architectures provide a robust alternative to centralized systems, addressing the unique challenges of security and data privacy in UAV operations. (The SABEC protocol developed to address this requirement has significantly resolved many of the existing challenges. For a detailed evaluation, please refer to Chapter 7)

3. Lack of Suitable Consensus Mechanisms for UAVs: To effectively apply blockchain technology in UAV networks, there is a need for consensus mechanisms that are fast, secure, and resource-efficient. Existing consensus algorithms are often impractical due to UAVs' limited computational capacity and latency tolerances (Wang et al., 2021). Consequently, there is an increasing focus on developing lightweight consensus mechanisms specifically designed for UAV environments, which can operate under constrained resources while maintaining security and operational efficiency (Wang et al., 2024).

These challenges hinder UAV networks from reaching their full potential in terms of reliability, security, and operational efficiency (Yu et al., 2024). For UAVs to successfully accomplish their missions, it is critical to reliably authenticate the identities of all devices and targets within the network, and to securely transmit and store data. Additionally, considering the dynamic nature of the network and limited resources, it is necessary to develop specially designed consensus mechanisms. Therefore, developing lightweight, scalable, and secure identity management mechanisms that meet the unique needs of UAV networks (along with fast and efficient consensus protocols suitable for the constrained resources of UAVs) is of great importance for both academic research and industrial applications (Chen et al., 2020). Innovative solutions addressing these challenges will provide a solid foundation for future technological developments and applications in UAV networks. (To meet this requirement, the SABEC protocol proposed in this research has made substantial progress in addressing the identified challenges. A comprehensive evaluation can be found in Chapter 7)

1.4 Research Objectives

The proliferation of Unmanned Aerial Vehicles (UAVs) in various sectors has underscored the necessity for robust, efficient, and secure operational frameworks, particularly in multi-UAV network environments. The complex interplay between dynamic network topologies, resource-constrained devices, and the potential for adversarial threats necessitates a comprehensive approach to identity management and secure communication protocols (Li et al., 2019; Raja et al., 2021). Building upon the challenges delineated in the problem statement, the primary objectives of this research are as follows:

1. To Develop a Lightweight and Scalable Identity Management Mechanism for UAV Networks:

- ➢ *Design and Implementation:* Create an identity management protocol tailored to the unique constraints of UAV networks, emphasizing minimal computational overhead and energy consumption while maintaining high security standards.
- ➢ *Adaptability to Dynamic Topologies:* Ensure that the proposed mechanism is adaptable to the constantly changing network topologies inherent in UAV operations, facilitating seamless authentication and re-authentication processes as UAVs enter and exit the network.
- ➢ *Resistance to Security Threats:* Incorporate advanced cryptographic techniques to safeguard against common security threats such as identity spoofing, replay attacks, and man-in-the-middle attacks, thereby enhancing the overall integrity and trustworthiness of the network.

2. To Establish a Secure and Distributed Data Storage Solution Utilizing Blockchain Technology:

- ➢ *Customized Consensus Mechanism:* Develop a consensus protocol suitable for UAV networks that addresses the limitations of traditional blockchain mechanisms, such as high computational costs and latency, without compromising security.

- *Data Integrity and Immutability:* Leverage blockchain's inherent properties to ensure that data collected and shared within the UAV network is stored in a tamper-proof and verifiable manner.
- *Scalability and Fault Tolerance:* Design the storage solution to be scalable, accommodating varying numbers of UAVs, and to be resilient against node failures, ensuring uninterrupted network functionality.

3. To Enhance the Efficiency and Security of Multi-UAV Collaboration in Decision-Making Processes:

- *Secure Communication Protocols:* Develop protocols that facilitate secure and efficient communication among UAVs and between UAVs and ground stations, accounting for the resource constraints of the devices.
- *Consensus in Adversarial Environments:* Implement mechanisms that enable UAVs to reach consensus on critical decisions even in the presence of malicious actors or faulty nodes.
- *Performance Evaluation:* Rigorously evaluate the proposed solutions through simulations and practical implementations, analysing metrics such as latency, throughput, energy consumption, and security robustness.

4. To Contribute to the Theoretical Foundations and Practical Applications of UAV Network Security:

- *Theoretical Advancement:* Extend existing knowledge in the field by introducing novel methodologies and frameworks that address the identified gaps in UAV network security and identity management.
- *Practical Feasibility:* Ensure that the proposed solutions are not only theoretically sound but also practically implementable, offering tangible benefits to real-world UAV operations.
- *Guidance for Future Research:* Provide insights and recommendations that can inform future studies and technological developments in UAV networks and related domains.

In conclusion, the primary aim of this research is to design and implement a secure, lightweight, and scalable identity management system tailored to the unique constraints of UAV networks operating in dynamic and potentially adversarial environments. In this context, the study seeks to develop an authentication mechanism that enables secure identity verification and re-authentication for UAVs with limited computational power and energy resources, while also adapting to node mobility and continuously changing network topologies. Additionally, the research aims to establish a resource-efficient blockchain-based distributed data storage infrastructure that ensures data integrity, immutability, and fault tolerance. Within the scope of the study, a two-tier consensus mechanism is proposed to enable dynamic leader election and trust-based decision-making processes, resilient against Byzantine threats. The proposed SABEC protocol will be rigorously evaluated through simulations and testbed implementations in terms of performance metrics such as security robustness, latency, throughput, and energy efficiency. Ultimately, this research aims to contribute both theoretically and practically to the secure design of UAV networks and to develop a reusable framework applicable to other resource-constrained and mission-critical systems.

1.5 Research Questions

To systematically address the outlined research objectives, the thesis seeks to answer the following critical research questions:

1. How can a lightweight and scalable identity management mechanism be designed for UAV networks that balances security requirements with the resource constraints of UAV devices?

- ➢ What cryptographic techniques are most suitable for implementation in resource-constrained environments without compromising security?
- ➢ How can the proposed mechanism adapt to dynamic changes in network topology, such as UAV mobility and varying network densities?

Proposed Solution for Research Question 1:

Considering the constrained computational resources and limited energy capacities inherent to UAV platforms, the dynamic identity authentication mechanism developed within this study has been designed using lightweight cryptographic algorithms. Specifically, computationally efficient techniques such as one-way hash functions, timestamped nonces (randomly generated single-use values), XOR operations, and lightweight symmetric encryption methods have been utilized. The cryptographic techniques selected for UAV environments are characterized by low computational overhead, energy efficiency, and rapid execution capabilities. Accordingly, the SHA-256 one-way hash function has been employed in this research due to its fast execution, irreversibility, and minimal computational demands, making it highly effective for generating unique and secure digital signatures during identity authentication. Additionally, AES-128 symmetric encryption has been integrated into the protocol, providing high security and performance with significantly lower energy and computational costs compared to asymmetric encryption methods, thus addressing the UAVs' stringent resource constraints. Moreover, the use of timestamped and randomly generated nonces in authentication messages effectively mitigates common attacks such as replay and man-in-the-middle (MITM) attacks, with minimal computational impact. Collectively, these cryptographic techniques establish a robust security infrastructure without overloading UAV resources, enabling rapid and secure identity verification. Furthermore, the mechanism provides a context-aware authentication framework that adapts seamlessly to dynamic network topology changes and the continuous mobility of UAV nodes. When UAVs join or leave the network, their identities are dynamically re-authenticated using session keys based on timestamped random values, ensuring continuous identity validity within highly mobile and heterogeneous network environments. Due to the protocol's low-latency execution, re-authentication processes do not negatively impact the performance of real-time missions. Additionally, in this thesis, the SABEC protocol presented in Chapter 7 has been specifically developed to address this research question. The proposed approach employs a two-tier consensus mechanism. At the local (cluster) level, a lightweight Byzantine Fault Tolerant (LBFT) algorithm is utilized to validate trust evaluations and leader selection processes. At the global level, decisions are verified through smart contracts executed exclusively by authorized and trusted nodes. This structure significantly reduces computational overhead while effectively maintaining secure decision-making processes. For further details, please refer to Chapters 6 and 7.

2. In what ways can blockchain technology be adapted to provide secure and distributed data storage for UAV networks, considering the limitations of traditional consensus mechanisms like Proof of Work?

- ➢ What modifications or alternatives to existing consensus algorithms can be employed to reduce computational overhead and latency?
- ➢ How can the integrity and immutability of data be ensured in a distributed UAV network without introducing significant resource burdens?

Proposed Solution for Research Question 2:

In this thesis, the SABEC protocol presented in Chapter 7 has been specifically developed to address this research question. The SABEC protocol applies a lightweight two-tier consensus approach as a solution to the computational overhead and latency issues associated with traditional consensus algorithms. In the first (local) stage, the Lightweight Byzantine Fault Tolerance (LBFT) algorithm is utilized to achieve rapid and cost-effective consensus, while in the second (global) stage, smart contracts are executed exclusively by authorized nodes possessing high trust scores. Consequently, compared to traditional methods, the computational load is significantly reduced, enabling secure decision-making processes with lower latency. Within the SABEC protocol, data integrity and immutability in UAV networks are ensured without increasing resource consumption through the implementation of a specialized private-permissioned blockchain infrastructure. Unlike traditional blockchains, SABEC records only summarized and verified states of critical data onto the blockchain. Local state records, referred to as Trust Assessment Transactions (TATs), generated by each UAV node, are compressed using hash functions, substantially reducing their size; only these summarized data are committed to the blockchain. Thus, while data integrity and immutability are preserved, the storage capacity and computational overhead of the blockchain are significantly minimized. Furthermore, each data block added to the blockchain is verified through smart contracts executed solely by authorized nodes with high trust scores, effectively eliminating the risk of data manipulation or falsification by malicious or low-trust nodes. All inter-node data transmissions are secured using lightweight digital signatures, making it possible to trace the origin and authenticity of every piece of data within the network. Consequently, SABEC provides a highly reliable yet resource-efficient data verification infrastructure, thereby guaranteeing data integrity and immutability in UAV networks. This solution ideally meets the decentralized, scalable, and secure data storage requirements inherent in resource-constrained UAV environments.

3. What protocols can be developed to enhance the efficiency and security of communication and collaboration among multiple UAVs in adversarial environments?

- How can secure communication be maintained in the presence of malicious actors attempting to intercept or disrupt data exchanges?
- What strategies can be implemented to enable UAVs to reach consensus on shared tasks and decisions despite potential network instability or security threats?

Proposed Solution for Research Question 3:

Based on the findings obtained in this thesis research, it is essential to integrate a comprehensive protocol that combines a lightweight identity authentication mechanism, a two-tier Byzantine fault-tolerant consensus algorithm, and blockchain-based decentralized trust management infrastructure to enhance both security and efficiency of multi-UAV communications in environments characterized by adversarial threats. To fulfil these requirements, the SABEC protocol presented in Chapter 7 has been developed. Utilizing the dynamic identity authentication described in Chapter 6 and the adaptive leader election processes integrated within the SABEC protocol, the proposed approach ensures that only trusted UAV nodes actively participate in collective decision-making and collaboration tasks. Consequently, this significantly reduces interference from malicious nodes, thereby substantially improving operational security and effective utilization of resources.

Solution for Sub-question 3.1:

The solution developed within this thesis protects UAV-to-UAV communications against malicious interventions through both cryptographic methods (as presented in Chapter 6) and a trust-based consensus mechanism (as detailed in Chapter 7). Communication security is ensured using lightweight symmetric encryption algorithms such as AES-128, hash-based digital signatures, dynamically generated session-specific keys (nonces), and timestamps. These measures effectively defend against data interception, manipulation, and replay attacks. Moreover, as outlined in Chapter 7, the SABEC protocol employs a two-tier consensus mechanism to guarantee the integrity and reliability of exchanged data. At the local level, a Lightweight Byzantine Fault Tolerance (LBFT) algorithm facilitates rapid and resource-efficient consensus among nodes. At the global level, smart contracts executed exclusively by authorized nodes with high trust scores further verify data accuracy. Thus, interference and data manipulation by malicious nodes are effectively prevented, ensuring trustworthy verification and transmission of information.

Solution for Sub-question 3.2:

The SABEC protocol (as detailed in Chapter 7) provides an effective solution against network instability and security threats through the implementation of a two-tiered, resource-efficient consensus strategy. In the first (local) consensus stage, nodes utilize a Lightweight Byzantine Fault Tolerance (LBFT) algorithm to achieve rapid and low-cost consensus, identifying reliable nodes based on real-time performance metrics such as battery life, sensor reliability, and communication quality. In the second (global) stage, decisions are validated exclusively by authorized nodes through smart contracts, specifically executed by nodes possessing high trust scores. This hierarchical approach ensures reliable consensus on shared tasks and critical decisions, effectively maintaining coordination even in the presence of malicious or unstable nodes.

4. How does the proposed identity management and data storage solution perform in comparison to existing methods in terms of security robustness, computational efficiency, and scalability?

- ➢ What are the measurable improvements in latency, throughput, and energy consumption when utilizing the proposed mechanisms?
- ➢ How resilient is the system against various attack vectors, including identity spoofing, replay attacks, and Denial-of-Service (DoS) attacks?

Proposed Solution for Research Question 4:

The proposed SABEC protocol and dynamic identity management mechanism demonstrate significant advantages over conventional centralized systems and classical blockchain-based methods in terms of security robustness, computational efficiency, and scalability. Traditional methods commonly face issues related to single points of failure; however, SABEC effectively eliminates these vulnerabilities through its distributed blockchain architecture. Regarding computational efficiency, SABEC employs a lightweight Byzantine Fault Tolerant (LBFT) two-tier consensus algorithm, significantly outperforming traditional consensus methods that require extensive computational resources. Additionally, the scalability of the system is enhanced by the cluster-based dynamic leader selection process, validated through simulation scenarios, ensuring consistent performance without degradation as the UAV network size increases. Comprehensive evaluations conducted through NS-3 simulations and testbed environments demonstrate measurable improvements provided by the SABEC protocol and the identity authentication system compared to existing methods:

- Latency: A reduction of approximately 40% in latency has been achieved compared to traditional blockchain-based solutions (Chapter 6, 7 and 9). Lightweight authentication processes reduce each authentication transaction to millisecond scales (Chapter 6 and 9).
- Throughput: Cluster-based leader selection coupled with a low-overhead LBFT consensus method results in a 35–50% increase in packet delivery rates (Chapter 9). This significantly improves communication efficiency, particularly in dynamic and densely populated UAV networks.
- Energy Consumption: Lightweight cryptographic techniques and reduced computational loads result in approximately 35% energy savings, thereby extending the operational flight durations of UAV devices (Chapter 9).

The identity management mechanisms provided by the SABEC and dynamic identity authentication protocols effectively defend against various attack vectors:

- Identity Spoofing: Robust authentication using nonce-based, single-use random values and digital signatures prevents the creation of fraudulent identities and duplication of existing identities (Chapter 6 and 9).
- Replay Attacks: The use of timestamped session keys and nonce values automatically invalidates previously used authentication messages, rendering the network resilient to replay attacks (Chapter 6 and 9).
- Denial-of-Service (DoS) Attacks: The SABEC and dynamic identity authentication mechanisms effectively mitigate DoS attacks by employing nonce-based random dynamic values, timestamps, digital signature-based identity authentication, frequency-limiting authentication requests, and continuous evaluation of nodes' trust scores. Furthermore, the two-tier consensus structure enhances resilience against DoS attacks (Chapter 7 and 9).
- Byzantine Attacks: The LBFT-based two-tier consensus framework, combined with trust-score evaluation mechanisms and nonce-based random dynamic values, timestamps, and digital signatures for identity authentication, systematically identifies and excludes malicious or faulty nodes, thus maintaining network security and integrity against Byzantine behaviours.

In conclusion, the SABEC protocol provides superior resilience and security against the aforementioned attacks compared to traditional methods (Chapter 7 and 9).

5. What theoretical contributions can this research make to the field of UAV network security, and how can these contributions inform future developments and applications?

- ➢ How does the proposed framework advance current understanding and methodologies in secure UAV network design?
- ➢ In what ways can the findings be generalized or adapted to other types of resource-constrained networks or Internet of Things (IoT) applications?

Proposed solution for Research Question 5:

This research makes significant theoretical contributions to the field of UAV network security by proposing innovative approaches in identity management, blockchain-based secure frameworks, and lightweight consensus mechanisms. Specifically, the SABEC protocol addresses critical limitations found in existing methodologies, thereby advancing current theoretical understanding related to secure authentication and coordination processes under constrained resources and adversarial conditions (discussed in detail in Chapter 6 and Chapter 7). First, the proposed lightweight cryptographic identity management mechanism provides novel theoretical insights into scalable, secure identity authentication for resource-constrained UAV platforms. By demonstrating the feasibility of dynamic authentication procedures even in real-time mobility scenarios, the study challenges conventional centralized or computationally intensive approaches, thus extending the theoretical framework for secure identity management (detailed in Chapter 5). Secondly, SABEC's two-tier consensus mechanism (comprising data consensus and decision consensus) represents a significant theoretical advancement over traditional blockchain consensus methods. The mechanism notably reduces energy consumption and computational overhead, providing a low-latency, secure coordination process that is resilient against Byzantine threats. This innovative approach contributes directly to theoretical developments in secure distributed decision-making within UAV networks and other distributed environments (extensively covered in Chapter 7). Finally, findings from this research have broad implications beyond UAV networks, demonstrating significant potential for generalization and adaptation to other resource-constrained systems, such as Internet of Things (IoT) environments, mobile sensor networks, and smart city applications. Due to shared characteristics (limited resources, dynamic topologies, and susceptibility to attacks) the lightweight, scalable, and context-aware security design of SABEC provides a reusable and adaptable theoretical framework. This generalizability and the practical applicability of SABEC to other domains are extensively evaluated in Chapter 7 and discussed in Chapter 9. Thus, the theoretical contributions and future implications outlined in this thesis not only enhance current methodologies in UAV network security but also serve as a valuable guide for future research and practical implementations in broader domains of distributed and resource-constrained network systems.

By addressing these questions, the research aims to provide a comprehensive solution to the challenges faced in UAV network identity management and security, contributing both to the academic body of knowledge and to practical applications in the field.

1.6 Significance of the Study

Unmanned Aerial Vehicle (UAV) networks have become a focal point of both academic research and industrial applications in recent years due to technological advancements and the expansion of their application areas. These networks enhance operational efficiency and effectiveness by providing innovative solutions in critical domains such as disaster management, agriculture, logistics, security, and defence (Khan et al., 2024; Yu et al., 2018). However, the dynamic and heterogeneous nature of UAV networks, their limited resources, and escalating security threats pose significant challenges to the reliability and sustainability of the UAV systems.

This study addresses a crucial gap in the literature by tackling identity management and data security issues that directly impact the security and efficiency of UAV networks. Existing authentication and security protocols are known to be inadequate due to the limited processing power, energy capacity, and dynamic network topologies of UAVs. Specifically, threats such as identity spoofing, replay attacks, and Denial-of-Service (DoS) attacks severely jeopardize the operational success and security of UAV networks. In this context, the lightweight and dynamic identity management protocol developed in this study offers a reliable solution tailored to the unique requirements of UAV networks, featuring low computational and communication overhead.

Moreover, the integration of blockchain technology into UAV networks has led to the development of a consensus mechanism that significantly contributes to data integrity and reliability. The disadvantages of traditional blockchain protocols, such as high energy consumption and latency, limit their applicability due to the UAVs' limited resources. This study employs an adapted version of the Practical Byzantine Fault Tolerance (PBFT) algorithms to develop a consensus mechanism specifically optimized for UAV networks. This mechanism enhances the overall performance and security of the network by enabling secure and efficient data sharing among UAVs. The significance of the study can be detailed under the following headings:

1. Academic Contributions:

- Filling a Gap in the Literature: Existing research offers a limited number of lightweight and dynamic solutions addressing identity management and security issues in UAV networks. This study fills this gap, providing an original contribution to the literature.
- Development of New Approaches: The proposed identity management protocol and consensus mechanism are designed according to the unique needs of UAV networks, offering new methodologies that will serve as a foundation for future research.
- Theoretical Advancement: By presenting an innovative framework that combines symmetric cryptography with blockchain technology, the study contributes to theoretical advancements in the design of secure UAV networks.

2. Practical Applications and Industrial Impact:

- Enhancing Operational Efficiency: The developed protocol and mechanisms improve the operational efficiency of UAV networks by reducing latency and resource consumption.
- Strengthening Security: The study enhances the resilience of UAV networks against security threats, contributing to reliability in critical applications.
- Applicability and Scalability: The low computational and communication overhead of the proposed solutions offers a practical approach for UAVs with limited resources. Additionally, the ability to adapt to dynamic network topologies increases the system's scalability and flexibility.

3. Societal and Economic Contributions:

- Protection of Critical Infrastructure: Enhancing the security of UAV networks directly contributes to societal safety in areas such as border security, disaster management, and the monitoring of critical infrastructures.
- Promotion of Technological Innovation: By enabling UAV technologies to be used more securely and effectively, the study supports industrial innovation and competitiveness.
- Guiding Future Technologies: Establishing a solid foundation for the evolution and sustainability of UAV networks, this study sheds light on the integration of 6G and beyond communication technologies and the development of autonomous systems.

4. Contributions to Future Research:

- Guiding Research Directions: The findings and proposed approaches of the study will guide future academic research and technological developments.
- Adaptability: The developed methods can be adapted to other resource-constrained networks and Internet of Things (IoT) applications, creating a broad impact area.

In conclusion, this study provides significant theoretical and practical contributions to the security and efficiency of UAV networks. The lightweight and dynamic identity management protocol and the optimized consensus mechanism developed herein enable UAV networks to be used more securely, effectively, and sustainably in real-world applications. The findings not only offer solutions to existing problems but also establish a solid foundation for the design of future autonomous systems and communication networks. In this context, the importance of the research will resonate widely in both academic literature and industrial applications.

1.7 Scope and Limitations

1.7.1 Scope

This study focuses on enhancing the security and operational efficiency of Unmanned Aerial Vehicle (UAV) networks by developing a lightweight and dynamic identity management protocol alongside an optimized consensus mechanism specifically tailored for UAV networks. The scope of the study encompasses the following components:

1. Design of the Identity Management Protocol:

- Developing an authentication protocol with low computational and communication overhead, taking into account the limited processing power and energy resources of UAVs.
- Ensuring that the protocol adapts to dynamic network topologies and exhibits resilience against common security threats such as identity spoofing, replay attacks, and man-in-the-middle attacks.

2. Development of the Consensus Mechanism:

- Designing a fast and efficient consensus mechanism suitable for the unique requirements of UAV networks by leveraging the advantages of blockchain technology.
- Adapting and optimizing the Practical Byzantine Fault Tolerance (PBFT) algorithm to overcome the limitations of traditional consensus algorithms.
- Enabling the consensus mechanism to effectively support secure data sharing and decision-making processes among UAVs.

3. Performance and Security Analyses:

- Conducting a comprehensive evaluation of the performance and security of the developed protocol and mechanisms.
- Analysing performance metrics such as latency, bandwidth usage, processor load, and memory consumption using simulation tools.
- Testing the system's resilience against security threats like identity spoofing, replay attacks, and Denial-of-Service (DoS) attacks.

4. Real-World Applications and Scenarios:

- Assessing the practical applicability of the developed solutions by examining critical application scenarios such as disaster management and emergency response.
- Demonstrating how UAV networks can be utilized more securely and efficiently under real-world conditions.

1.7.2 Limitations

The limitations of this study are articulated under the following headings:

1. Simulation Environment vs. Real Systems:

- The protocols and mechanisms developed in this study have been primarily tested within simulation environments (e.g., NS-3). While simulations largely reflect real-world conditions, they may not fully model all variables, and unforeseen situations present in actual UAV networks.
- System performance may vary when considering actual UAV hardware and complex environmental factors.

2. Impact of Limited Resources:

- The limited energy and processing capacity of UAVs may pose practical challenges in implementing the proposed protocol and mechanisms. Although the study aims to provide lightweight and efficient solutions, resource consumption could become a critical factor in very large-scale networks or long-duration operations.
- Issues related to energy consumption and resource management have not been deeply explored in this study and are identified as areas for future research.

3. Scope of Security Threats:

- The study focuses on common security threats such as identity spoofing, replay attacks, and Denial-of-Service (DoS) attacks. However, more advanced and targeted attacks (e.g., artificial intelligence-supported attacks, physical layer attacks) are beyond the scope of this work.
- The performance of the developed protocol and mechanisms against such advanced threats should be evaluated in future studies.

4. Limitations of Blockchain Technology:

- While the use of blockchain technology offers advantages in terms of data integrity and security, potential limitations such as scalability and latency issues may arise.
- The performance of the blockchain-based consensus mechanism may be affected under heavy traffic and high data volumes. This situation can be partially mitigated through network design optimization and parameter tuning but may be difficult to eliminate entirely.

5. Standardization and Compatibility:

- The lack of universal standards and protocols for UAV networks may complicate the integration of the developed solutions with different systems.

- ➢ Adoption of the proposed protocol and mechanisms by various UAV platforms and manufacturers depends on standardization processes and the level of industrial acceptance.

6. Regulations and Legal Constraints:

- ➢ National and international regulations related to the use of UAVs have not been detailed within the scope of this study.
- ➢ Legal regulations concerning blockchain and cryptography may affect the applicability of the developed solutions.

In conclusion, while this study offers significant contributions to the security and efficiency of UAV networks, the aforementioned limitations should be considered. Future research can focus on addressing these limitations and enhancing the applicability of the developed solutions on a broader scale. Key steps for subsequent studies include conducting comprehensive tests in real-world applications, thoroughly investigating energy consumption and resource management issues, improving the system's resilience against advanced security threats, and supporting standardization processes.

1.8 Contributions

This thesis presents comprehensive theoretical and practical contributions addressing security, operational efficiency, and scalability challenges in swarm-based Unmanned Aerial Vehicle (UAV) networks. By clearly identifying gaps in the existing literature, this research introduces innovative and specialized solutions tailored to the unique requirements of UAV swarm networks.

The primary theoretical contribution of this thesis is the development of a lightweight, scalable, and dynamic identity management protocol specifically designed for UAV networks operating under strict resource constraints, such as limited processing power, memory, and energy. Unlike traditional identity authentication methods that incur high computational and communication overhead, the proposed protocol innovatively integrates dynamic symmetric cryptography and lightweight hash functions. Theoretically, this approach ensures rapid and continuous authentication even in highly dynamic swarm scenarios, providing robust resilience against common threats such as identity spoofing, replay attacks, and man-in-the-middle (MITM) attacks. This represents a unique advancement in the theoretical understanding of identity management within UAV networks. Secondly, the thesis contributes an optimized, blockchain-based consensus mechanism uniquely tailored for swarm UAV systems to ensure data integrity and secure decision-making processes. To overcome latency and high energy consumption associated with traditional consensus algorithms, the Practical Byzantine Fault Tolerance (PBFT) algorithm is innovatively redesigned and integrated with the Fuzzy C-Means (FCM) clustering algorithm specifically for UAV swarms. This novel approach enables rapid, energy-efficient, and secure data dissemination, substantially advancing theoretical frameworks related to distributed decision-making and scalability in UAV networks. The third significant theoretical contribution involves the novel adaptation of blockchain technology for decentralized and secure storage of critical data specifically within UAV swarm environments. The thesis addresses and eliminates single points of failure commonly found in centralized storage systems by introducing a permissioned and private blockchain structure tailored to UAV swarm networks. This innovative method guarantees data immutability and integrity, establishing a decentralized, reliable data infrastructure and enhancing theoretical contributions to secure data storage and communication. Fourth, the theoretical frameworks and practical applicability of the developed protocols have been rigorously validated using tools such as ProVerif and NS-3 simulations. Theoretical claims regarding latency, bandwidth usage, processing load, and energy consumption are supported by extensive formal, informal, and experimental analyses. Additionally, the resilience of the proposed methods against critical threats, including identity spoofing, replay attacks, and Denial-of-Service (DoS) attacks, has been thoroughly demonstrated through simulation studies. These findings clearly establish theoretical and practical superiority over existing protocols in UAV swarm networks. Finally, the theoretical frameworks and design principles of the proposed identity management and blockchain-based consensus mechanisms have broader applicability beyond UAV swarm networks. The methods developed in this thesis can be generalized and adapted to other resource-constrained distributed systems, including Internet of Things (IoT) applications, mobile sensor networks, and similar distributed network environments. This generalizability significantly enhances the broader impact of the research, serving as a crucial reference for future theoretical studies and practical applications.

In conclusion, this thesis holds a unique position in the literature due to its theoretical contributions, practical applicability, and generalizability in enhancing security, operational efficiency, and scalability of swarm UAV networks. These advancements lay a solid foundation for future research and industrial applications, promoting secure, sustainable, and scalable deployment of UAV swarms in real-world scenarios.

1.9 Thesis Structure

This thesis is systematically organized into nine core chapters, each addressing a distinct facet of the research on secure and efficient identity management for UAV networks. The structure is designed to guide the reader from foundational concepts and background literature through technical development, implementation, evaluation, and discussion of results.

Chapter 1, Introduction, establishes the context of the research, articulating the motivations and underlying challenges in UAV network security. The chapter precisely defines the problem statement and articulates the research objectives and questions that steer the study. The significance of the research is delineated, emphasizing its potential contributions to both theory and practice. The scope and limitations are carefully outlined to demarcate the boundaries of the research, and the novel contributions of the thesis are highlighted. The chapter concludes with an overview of the thesis structure, serving as a roadmap for the reader.

Chapter 2, Literature Review, provides a comprehensive synthesis of existing research relevant to UAV network identity management. This chapter critically reviews foundational theories, current identity management frameworks, and recent advances in blockchain technology and security protocols. It identifies knowledge gaps and limitations in the current body of literature, thereby establishing the necessity and originality of the research presented in this thesis.

Chapter 3, Analysis of UAV Network Requirements, investigates the specific requirements and challenges intrinsic to identity management within UAV networks. It begins by analysing the key technical and operational requirements for secure network operation. Subsequently, adversary models are developed to characterize potential security threats and vulnerabilities. The security goals of the system are clearly defined, and defence mechanisms against known attacks (such as spoofing, replay, and denial-of-service) are examined. The chapter further explores privacy and security considerations, the integration of blockchain technology, and the practical requirements for system deployment. Risk assessment and analysis are conducted to evaluate the likelihood and impact of various threats, providing a comprehensive foundation for subsequent chapters.

Chapter 4, Methodology, details the research methods and systematic approach employed to achieve the study’s objectives. The chapter commences with the design of the UAV network model, outlining the key structural and communicative parameters. This is followed by the development of the authentication protocol, the architecture and implementation of system components, and the integration of blockchain-enabled decision-making mechanisms. Formal security verification methods are described, along with the simulation and experimental setup used to evaluate the proposed solutions. The chapter concludes with a summary of the overall methodological framework.

Chapter 5, Design and Development of Identity Management System, is devoted to the technical design and implementation of the proposed identity management system. This chapter presents the architectural components, operational workflow, and the underlying mechanisms that ensure robust identity management for UAV networks.

Chapter 6, A Secure and Dynamic Authentication Protocol for UAV Networks, presents the proposed authentication protocol in detail. The chapter covers each phase of the protocol (offline, registration, authentication and key establishment, and data transmission) providing a comprehensive overview of the security mechanisms. It discusses the implementation and testing of the protocol, conducts a rigorous security analysis, and evaluates the system's performance with respect to latency, computational overhead, and resource utilization. The chapter concludes with a summary of the key findings and contributions.

Chapter 7, A Secure and Adaptive Blockchain-Enabled Coordination (SABEC) Protocol for UAV Networks, introduces and elaborates on the SABEC protocol. The chapter provides an overview of the protocol, its system architecture, and its core components, including the Fuzzy C-Means (FCM) clustering algorithm and the drone cluster membership and selection mechanisms. It details the implementation and testing of the consensus protocol, presents the simulation setup, and offers a comparative performance analysis with traditional protocols. Security analysis is conducted to ensure the protocol's robustness against adversarial threats. The chapter concludes with a summary and reflection on the protocol's effectiveness.

Chapter 8, Case Studies and Real-World Deployment, illustrates the practical applicability of the developed frameworks through case studies and real-world scenarios. A detailed case study is presented, focusing on the simulation of a fire monitoring scenario and the detection of Byzantine drones in Swansea. This chapter demonstrates the real-world feasibility and adaptability of the proposed authentication and coordination protocols in dynamic UAV network environments.

Chapter 9, Discussion and Conclusions, synthesizes the research findings and discusses their broader implications for identity management in UAV networks. The chapter summarizes the major contributions of the study, outlines the theoretical and practical implications, and provides recommendations for future research. It concludes with a reaffirmation of the research significance and a summary of the overall contributions.

This structured approach ensures that the thesis develops logically and cohesively, with each chapter building on the previous to provide a thorough and rigorous exploration of secure identity management for UAV networks. The integration of theoretical analysis, protocol design, practical implementation, and real-world evaluation enhances the scientific and practical value of the research, offering a significant contribution to the advancement of secure and reliable UAV network management.

Chapter 2

Literature Review

Unmanned Aerial Vehicle (UAV) networks, also known as drone networks, have in recent years emerged as a prominently adopted technology across sectors such as agriculture, logistics, surveillance, and natural disaster management (Pajany et al., 2024; Silva et al., 2024). This integration has been facilitated by Industry 4.0 technologies, which promote the deployment of intelligent, interconnected systems capable of operating efficiently in dynamic environments (Yucesoy & Şahin, 2024). The adoption of multi-UAV systems has conferred significant advantages, including expanded area coverage, the execution of complex missions through coordinated efforts, and enhanced operational efficiency (Queralta et al., 2020; Alsamhi et al., 2022) [8,18]. However, these networks differ fundamentally from traditional terrestrial networks due to their high mobility, dynamic topologies, and frequently constrained resources. The intrinsic mobility of UAVs enables rapid deployment and adaptation to change operational conditions, thereby increasing network responsiveness and mission effectiveness (Rigas et al., 2024; Sahingoz et al., 2013). Conversely, this mobility also introduces challenges in establishing stable and reliable communication links, as UAVs continuously alter their positions relative to one another and to ground control stations (Chen et al., 2024). Consequently, the dynamic topology of UAV networks demands the development of routing protocols capable of responding rapidly to changing network conditions in order to maintain uninterrupted data transmission and network integrity (Arafat et al., 2019). In this context, Identity Management Systems (IDMS) have become indispensable for ensuring secure and efficient access control within our increasingly diverse and complex networked environments (Hansen et al., 2024). IDMS play a critical role throughout the entire lifecycle of digital identities (spanning identity creation, authentication, authorization, and eventual decommissioning). These systems not only guarantee that only authenticated and authorized entities gain access to sensitive information and resources but also mitigate the risks associated with unauthorized access and cyber threats (Peddibhotla et al., 2024).

Unmanned Aerial Vehicle (UAV)-specific Identity Management Systems (IDMS) have emerged in recent years as a research domain of critical importance, driven by the increasing reliance on UAVs for tasks such as surveillance, disaster response, and logistics (Wang et al., 2024). Traditional IDMS solutions, which were designed primarily for static, terrestrial environments, have proven inadequate for the distinctive requirements of UAV networks, namely high mobility, dynamic topologies, and constrained computational resources (Ye et al., 2024). To address these shortcomings, researchers have begun to integrate decentralized technologies and lightweight cryptographic protocols into novel IDMS architectures. Secure authentication protocols are foundational to the integrity and reliability of UAV-specific IDMS. By ensuring that only authorized UAVs and permitted personnel may access and interact with the network, these protocols provide essential protection against unauthorized access, identity spoofing, and other cyber-attack vectors. Recent advances in this area have focused not only on enhancing security measures but also on optimizing protocols to accommodate UAVs' inherent constraints (limited processor speeds and battery capacities) (Alladi et al., 2020). Given that identity spoofing, data tampering, Denial-of-Service (DoS) attacks, and related threats pose significant risks to UAV networks, robust yet efficient authentication mechanisms are indispensable (Yu et al., 2023). A notable development has been the creation of lightweight authentication schemes tailored specifically to UAV platforms. Usman et al. (2022) proposed an Elliptic Curve Cryptography (ECC)-based protocol that minimizes computational overhead and power consumption, thereby preserving UAV battery life without compromising security. Similarly, Son et al. (2023) introduced an ECC-driven mutual authentication framework designed to withstand replay and man-in-the-middle attacks while imposing minimal processing requirements on UAV hardware. These contributions significantly bolster the security posture of UAV networks by delivering strong protection against common attack vectors under stringent resource constraints. Concurrently, the adoption of multi-factor authentication (MFA) in UAV networks has gained momentum (Guo et al., 2024). MFA approaches combine multiple verification layers, such as device-based credentials, behavioural biometrics, and contextual parameters (e.g., location, time), to reduce the risk of unauthorized access even if a single factor is compromised. Sodhro et al. (2022) empirically demonstrated that MFA integration in UAV systems markedly decreases unauthorized access attempts, thereby strengthening overall network resilience. Building on this, Deebak et al. (2023) developed an MFA framework that merges biometric fingerprint verification with cryptographic tokens; this design ensures that, should one authentication factor be breached, additional layers remain intact to preserve security. Their findings underscore the efficacy of MFA in elevating UAV network defences and highlight its potential as a standard safeguard in future UAV deployments.

In the extant literature, various approaches have been scrutinised that place particular emphasis on identity management and authentication mechanisms to address the security challenges inherent in UAV networks. Traditional methods, most notably Public Key Infrastructure (PKI), have demonstrated efficacy in certain scenarios; however, their substantial computational overhead and reliance on centralised authorities render them largely unsuitable for UAV applications (Fang et al., 2022). To overcome these drawbacks, lightweight authentication protocols have been advanced, designed to minimise computational complexity and energy consumption while upholding strong security guarantees (Sikarwar et al., 2024; Tufekci et al., 2024). Authentication constitutes the first line of defence against unauthorised access and malicious intrusions, and thus represents a cornerstone of any robust identity management framework (Bansal et al., 2021). In this context, lightweight mutual authentication schemes, where both the UAV and the network reciprocally verify one another's legitimacy, are of particular importance for thwarting impersonation and replay attacks (Zhou et al., 2024). Equally critical is the secure generation of session keys, which ensures that all subsequent communications remain encrypted and protected from eavesdropping (Mao et al., 2024). Recent contributions have proposed advanced cryptographic techniques that marry robust security with minimal computational demands, thereby enabling continuous, reliable operation in highly dynamic environments (Giambene et al., 2024).

The critical importance of robust identity management has been magnified by the proliferation of Internet of Things (IoT) devices and the integration of advanced communication technologies (Zadorozhnyi et al., 2024). The emergence of large-scale, heterogeneous device deployments across diverse sectors has driven an urgent demand for scalable and secure identity management solutions (Pajany et al., 2024). Historically, identity management has been operated in a centralized manner, with authentication and authorization managed by a single authority (Karmakar et al., 2023). While effective in controlled environments, this centralized paradigm suffers from serious limitations in scalability, single points of failure, and vulnerability to attacks (Bansal et al., 2021). Consequently, the advent of distributed systems, cloud computing, and the widespread adoption of IoT devices has prompted a shift toward decentralized and federated identity management models (Zanardo et al., 2024). Federated Identity Management Systems (FIMS) enable multiple autonomous domains to share identity information securely, facilitating Single Sign-On (SSO) capabilities and reducing administrative overhead (Nguyen et al., 2021). Nevertheless, federated approaches themselves encounter challenges in interoperability, trust establishment, and data privacy, which can constrain their effectiveness in large-scale, multi-platform environments (Blika et al., 2024). In the context of UAV networks, FIMS likewise offer mechanisms for secure identity sharing among multiple autonomous drones (Boi et al., 2024). By allowing UAVs from different domains to authenticate one another without reliance on a central authority, FIMS decrease administrative burden and enhance network flexibility. However, these solutions continue to face significant hurdles in cross-platform compatibility, trust establishment within heterogeneous drone fleets, and the absence of universally adopted standards (Hazra et al., 2021).

However, significant challenges remain in the development of secure authentication protocols. In particular, scalability continues to be a critical concern in large-scale networks comprising numerous UAVs. As encryption operations escalate within authentication processes, the computational burden and battery consumption of UAVs increase, thereby shortening their operational endurance (Michailidis et al., 2022). Given the inherently limited battery capacity and processing power of UAV platforms, energy consumption is a paramount consideration. UAVs, reliant upon battery power, require lightweight protocols that minimise energy expenditure while maximising efficiency in communication and data processing (Consul et al., 2024). Recent research efforts have accordingly focused on the design of lightweight communication protocols and efficient power management strategies to optimise energy consumption, thereby enabling UAVs to conduct extended missions without frequent recharging (Zhuo et al., 2022). Moreover, the integration of edge computing into UAV networks has yielded particularly noteworthy solutions for reducing energy use and alleviating processing loads: by offloading computationally intensive tasks to edge servers, the burden on individual UAVs is lessened, which in turn enhances both network scalability and overall performance (Yahya et al., 2024).

One of the most notable recent advancements in Unmanned Aerial Vehicle (UAV) networks is the utilisation of blockchain technology in the development of security protocols. Offering a decentralised, immutable, and transparent ledger system, blockchain has emerged as a critical innovation for enhancing the security and operational efficiency of UAV networks. The decentralised and dynamic nature of UAV networks make the implementation of conventional security measures particularly challenging. Therefore, there is a pressing need for innovative solutions that can enhance security without compromising performance. In this context, blockchain technology provides an alternative that overcomes the weaknesses of centralised security solutions. The decentralisation of authentication and data integrity processes prevents these functions from becoming vulnerable to a single point of failure or cyberattack (Akram et al., 2024). For instance, Xie et al. (2024) have developed a blockchain-based identity management system specifically designed for UAV networks. In this system, smart contracts are employed to automate and secure authentication processes. Similarly, Akram et al. (2024) have proposed a decentralised blockchain-based identity authentication protocol aimed at preventing identity spoofing in dynamic network environments. Such solutions contribute to the establishment of trust among network participants by enhancing transparency and traceability in identity transactions (Hawashin et al., 2024). The integration of blockchain into UAV networks offers effective solutions to key challenges essential for the seamless operation of UAV systems, including secure communication, decentralised identity management, data integrity, and trust establishment (Peddibhotla et al., 2024). Traditional centralised identity management systems typically depend on a single authority, thereby increasing the risk of attacks or operational disruptions; in fact, a single point of failure or attack could jeopardise the entire system. This represents a particularly significant risk in critical UAV operations. By distributing authentication and authorisation processes across multiple nodes in the network, the decentralised nature of blockchain eliminates single points of failure, substantially improving the resilience, reliability, and sustainability of UAV communications (Mei et al., 2024). Another critical area of blockchain's application in UAV networks relates to ensuring data integrity and traceability. Blockchain guarantees that all data transactions are recorded immutably, ensuring that data collected by UAVs remains intact and traceable when required (Manikandan et al., 2023). This characteristic is especially crucial in domains such as environmental monitoring, precision agriculture, and disaster management, where decision-making relies on accurate, reliable, and transparent information. Furthermore, blockchain-based IDMS solutions enable UAV identity information to be managed securely without the need for a central authority (Ma et al., 2023). This not only eliminates dependence on centralised administration but also reduces administrative overhead. Abbas et al. (2024) have developed a decentralised identity authentication system based on a transparent computing infrastructure. Similarly, Hosseini et al. (2023) have introduced a blockchain-based IDMS tailored for UAV networks that automates identity verification processes, providing a secure and tamper-proof system without the need for a central authority. As a result, UAVs can manage their identities independently, while the scalability and security of the network are simultaneously enhanced. This system also facilitates secure and seamless identity sharing across multiple UAV platforms, improving interoperability even within heterogeneous UAV ecosystems comprising different manufacturers and platforms.

Blockchain technology has emerged as a promising solution for addressing the challenges of identity management in UAV networks (Li et al., 2021; Kundu et al., 2024). The decentralised and tamper-resistant ledger structure of blockchain provides a reliable mechanism for maintaining secure identity records, establishing trust, and eliminating single points of failure within the network (Yu et al., 2024). Nevertheless, it is important to acknowledge that existing IDMS solutions continue to face several critical challenges. Scalability remains a major concern, particularly in large UAV fleets, as blockchain-based solutions often encounter issues related to processing delays and limited transaction throughput (Sharma et al., 2019). Furthermore, the integration of heterogeneous UAV platforms with current IDMS solutions presents ongoing difficulties, with incompatibility between legacy systems and modern solutions frequently reported (Cirillo et al., 2019). In addition, blockchain-based solutions enable secure and transparent data sharing between UAVs and ground control stations. By leveraging smart contracts, data-sharing policies are automated, ensuring the immutability and verifiability of the exchanged data (Samuel et al., 2023). This capability is particularly vital in domains such as surveillance, disaster management, and emergency response, where the real-time accuracy and integrity of data form the foundation of critical decision-making processes. For example, Pu et al. (2024) have developed a blockchain-based identity authentication and key-sharing protocol for UAV networks, which ensures that only authorised UAVs can access and exchange sensitive information, thereby preventing unauthorised access and data breaches.

Recent studies have highlighted the potential benefits of integrating blockchain technology into UAV networks, particularly in enhancing transparency, accountability, and resilience against unauthorised modifications (Hughes et al., 2024). However, the integration of blockchain technology into UAV networks presents several challenges. The resource-intensive nature of blockchain poses significant difficulties when applied to UAV networks, which are typically characterised by limited computational capacity and battery life (Kwon et al., 2024). One of the most critical issues in this context is that blockchain consensus mechanisms, such as Proof of Work (PoW), demand substantial computational power and energy consumption.

This requirement constitutes a major obstacle for UAVs with constrained battery capacity and processing resources (Soliman et al., 2024). Furthermore, the lack of standardisation in integrating different blockchain platforms with UAV systems raises considerable interoperability concerns (Ngo et al., 2023). To address these challenges, it is essential to develop lightweight consensus mechanisms and customised blockchain protocols that are tailored to the operational constraints of UAV systems.

Given the increasing complexity of UAV deployments, the integration of blockchain technology with lightweight authentication protocols and adaptive clustering mechanisms offers a comprehensive solution to the challenges of identity management. Blockchain provides a secure and immutable record of identities, while consensus mechanisms ensure trustworthy collaboration among UAVs. Adaptive clustering further enhances network efficiency by logically organising UAVs into groups and optimising leader selection based on trust metrics (Sun et al., 2024). Recent studies have demonstrated that such integrated approaches yield significant improvements over traditional methods in terms of packet delivery ratio, latency, and energy efficiency (Farithkhan et al., 2024; Luo et al., 2024). Another notable contribution is the development of decentralised identity authentication mechanisms through the integration of Physical Unclonable Functions (PUFs) with blockchain technology. Nair et al. (2024) proposed an identity authentication protocol designed to generate tamper-resistant identity credentials unique to each UAV. By embedding these credentials into a blockchain ledger, the protocol ensures decentralised and immutable identity verification. This effectively eliminates single points of failure and substantially reduces the risks of identity spoofing and unauthorised access. Moreover, this approach provides an effective solution for the secure, autonomous, and scalable management of identity information in large UAV fleets. Collaborative decision-making remains another critical element in multi-UAV operations. Consensus among UAVs is essential for coordinated missions such as surveillance, target tracking, and data aggregation (Jin et al., 2024). However, achieving reliable consensus in UAV networks is challenging, as nodes are susceptible to Byzantine faults; compromised or malfunctioning nodes can disrupt the consensus process, undermining network reliability (Sedjelmaci & Senouci, 2017). Recent research has highlighted the necessity for Byzantine Fault Tolerant (BFT) protocols specifically tailored for UAV networks that can distinguish between trustworthy and malicious nodes while minimising communication overhead (Pandey et al., 2022). In addition to blockchain-based solutions, clustering mechanisms have proven highly effective in the management of UAV networks, particularly in enhancing scalability and reducing communication overhead. Clustering involves grouping UAVs based on criteria such as geographic proximity or trustworthiness, thereby streamlining communication and improving network efficiency (Liang et al., 2024). Within these clusters, leader election algorithms play a pivotal role in selecting nodes responsible for critical communication tasks, ensuring efficient resource utilisation and fault tolerance (Mohammed et al., 2016). Effective clustering mechanisms not only enhance the scalability of UAV networks but also strengthen resilience against various cyber threats (Chatterjee et al., 2019).

A review of recent studies reveals that artificial intelligence (AI) and machine learning (ML) techniques are increasingly being incorporated into identity authentication processes within UAV networks. Notably, Zeng et al. (2024) developed an identity authentication framework based on anomaly detection algorithms, capable of detecting real-time threats and rejecting suspicious authentication attempts instantaneously. This system, which leverages UAV behavioural patterns and communication traces, offers a dynamic adaptation to emerging threats and provides a proactive security layer that complements traditional cryptography-based solutions. Experimental results have demonstrated the framework's considerable success in detecting malicious activities, thereby enhancing the resilience of UAV networks against cyber-attacks. However, as highlighted by Yazdinejad et al. (2024), the integration of AI- and ML-based identity authentication mechanisms presents challenges related to model training, data privacy, and the interpretability of AI-driven decisions. Ensuring that AI models are both effective and resilient to adversarial attacks remains a key focus for future research (Ren et al., 2020). Moreover, the protection of sensitive biometric data from unauthorised access and misuse necessitates the advancement of techniques such as zero-knowledge proofs, differential privacy, and other encryption methodologies (Han et al., 2023). Therefore, data privacy and ethical considerations must be carefully addressed in biometric-based identity authentication systems. Tedeschi et al. (2023) demonstrated that such encryption and privacy-preserving approaches can indeed be applied within authentication processes, making it possible to design systems that protect sensitive data without compromising security. In recent developments, the application of machine learning algorithms for anomaly detection in UAV networks has become increasingly prevalent and continues to maintain its prominence in research agendas. These algorithms enable the detection of suspicious activities and facilitate intervention before threats materialise (Yu et al., 2024). Consequently, AI- and ML-driven solutions have emerged as a significant research domain for enhancing both the security and adaptability of identity management in UAV networks (Ihekoronye et al., 2024). For example, Al-Syouf et al. (2024) introduced a machine learning-based identity authentication system designed to detect identity spoofing attacks in UAVs. By analysing UAV behavioural patterns, this system claims to identify and respond to anomalous situations in real-time, thereby contributing to an elevated security posture of UAV networks.

This review of the literature has comprehensively explored the pivotal importance of Identity Management Systems (IDMS) in strengthening the safety and functional effectiveness of Unmanned Aerial Vehicle (UAV) networks. The discussion began by outlining the evolution from conventional centralised identity management frameworks towards more distributed and federated approaches, a shift necessitated by the escalating demands for flexibility and scalability in contemporary UAV operations. The unique attributes of UAV networks, such as their pronounced mobility, ever-changing network structures, and constrained processing power and energy reserves, clearly demonstrate the need for tailored IDMS architectures to maintain secure and dependable performance. The assessment of current IDMS solutions designed for UAV environments has highlighted notable progress, particularly with the integration of blockchain-based architectures. As elaborated in earlier sections, blockchain technologies have succeeded in mitigating the inherent weaknesses of centralised systems by delivering distributed authentication processes and robust data exchange mechanisms. In parallel, lightweight cryptographic techniques, along with AI- and ML-based identity verification strategies, have played a vital role in improving threat detection capabilities and enabling adaptive defence mechanisms across UAV ecosystems.

Nonetheless, despite the considerable advances achieved in these domains, existing solutions continue to present several critical challenges. Scalability remains a significant obstacle, particularly for blockchain-based approaches, where processing delays and computational overhead hinder performance in networks operated by large fleets of UAVs. Furthermore, interoperability among heterogeneous UAV platforms and the seamless integration of legacy infrastructures with modern IDMS frameworks have yet to be fully addressed. In addition, the stringent energy and computational constraints inherent to UAVs necessitate the design of authentication protocols that are lightweight, efficient, and resilient. The review of blockchain technology has underscored its transformative potential in delivering decentralised identity verification, data integrity, and enhanced security within UAV networks. Nevertheless, blockchain-driven solutions must be meticulously optimised to balance data privacy, processing efficiency, and governance processes. In particular, the adoption of cryptographic techniques such as zero-knowledge proofs, differential privacy, and secure multi-party computation is essential to ensure the protection of sensitive information while maintaining robust security standards.

Future research is expected to focus on the development of lightweight yet secure cryptographic algorithms that will enhance the performance of blockchain protocols while enabling seamless integration through standardised frameworks for heterogeneous systems. This thesis likewise aims to lay a foundation for future studies by proposing a novel identity management approach that combines blockchain technology with dynamic, lightweight, and efficient cryptographic protocols tailored to the unique requirements of UAV networks.

In conclusion, secure authentication protocols play an essential role in safeguarding UAV networks and ensuring their operational efficiency. The lightweight, resilient, and adaptive authentication mechanisms developed in recent years have made substantial contributions in addressing the constraints specific to UAV environments. However, continued investigation is needed to overcome persistent challenges such as scalability, interoperability, and system integration. Achieving these goals will render secure identity management systems a critical enabler in the widespread adoption of UAV networks, ensuring that their security, performance, and reliability requirements are fully met.

In summary, research and development efforts in the domain of identity management systems designed for UAV networks have provided a comprehensive framework to tackle the distinct challenges in this field. Nevertheless, key issues, including scalability, interoperability, energy efficiency, ethical considerations, data privacy, and the absence of standardisation, must remain at the forefront of future investigations. Addressing these gaps will be instrumental in supporting the secure, flexible, sustainable, and scalable deployment of UAV networks, enabling them to reliably perform critical missions across diverse application domains.

Considering the literature review, the prominent challenges in identity management and security within UAV networks, as well as the extent to which this thesis addresses these challenges, are detailed and systematically listed below:

Scalability: Blockchain-based solutions, particularly in large-scale networks comprising numerous UAVs, experience performance issues due to processing delays and limited transaction throughput. As the number of UAVs increases, the computational and communication overhead of identity authentication and consensus processes also rises, negatively impacting overall performance.

- ✓ ***Contribution of the thesis:*** The thesis proposes lightweight and dynamic cryptographic protocols along with a customized consensus protocol for blockchain operations, integrated within a clustering-based architecture (see Chapters 6 and 7). In particular, the SABEC protocol aims to enhance scalability through blockchain-based lightweight consensus mechanisms and adaptive clustering support. In SABEC, nodes (UAVs) are divided into logical groups, and leader selection is conducted based on trust metrics. This structure contributes directly to balancing computational loads and reducing communication overhead, especially in large UAV fleets. Based on simulation data obtained in the study, it is claimed that this design contributes to improved scalability by balancing processing loads in large UAV fleets. However, for very large-scale networks involving hundreds of UAVs, the solution may remain at the prototype level, necessitating large-scale field testing or advanced simulation validation.

Energy and Computational Constraints: Given that UAVs possess limited battery capacity and processing power, lightweight protocols are essential to minimize energy consumption and computational demands. Resource-intensive blockchain consensus mechanisms are impractical for UAVs due to their high energy requirements.

- ✓ ***Contribution of the thesis:*** The identity authentication protocol designed for UAV networks employs lightweight cryptography (e.g., AES-based authentication) and resource-efficient blockchain lightweight consensus protocols (SABEC), aiming to minimize energy consumption and computational burden (see Chapters 6 and 7). Leader UAVs enhance overall energy efficiency by supporting the network via edge computing and smart load distribution. However, while theoretical and simulation results are promising, experimental validation at the hardware level is required.

Interoperability: Interoperability refers to the ability of systems and devices from different manufacturers, platforms, or technologies to communicate, share data, and coordinate seamlessly and securely. In UAV networks, this means enabling heterogeneous UAVs and ground control stations of varying standards and capabilities to work together without issues. The integration of heterogeneous UAV platforms with existing identity management systems remains challenging, with incompatibility between legacy systems and modern solutions frequently reported. The lack of standardization for integrating different blockchain platforms with UAV systems exacerbates interoperability challenges.

- ✓ ***Contribution of the thesis:*** The SABEC protocol developed for UAV networks (see Chapter 7) offers a blockchain-based decentralized management mechanism that enables UAVs from different manufacturers and platforms to operate within a shared trust infrastructure. This allows identity authentication and authorization operations to be securely performed across different systems without reliance on a central authority, thereby facilitating trust establishment in heterogeneous UAV fleets and laying the foundation for interoperability. Additionally, the dynamic identity authentication protocol (see Chapter 6) employs lightweight and dynamic cryptographic operations to automate and standardize data verification processes. This enables UAVs from different platforms to prove their identities through a uniform authentication logic, minimizing protocol incompatibility. Moreover, SABEC and the dynamic identity authentication protocols analyse UAV behavioural patterns, mission histories, and location data in real-time. These analyses are utilized to enhance trust across platforms. UAVs from different systems authenticate one another not solely based on static identity data, but also on dynamic behavioural data, thereby reducing the risks of identity spoofing and incompatibility during interoperability. The blockchain-based nature of SABEC ensures that all participant UAVs record transaction histories immutably, providing transparency and trust in heterogeneous systems. The dynamic identity authentication protocol further supports a federated identity model, enabling different UAV platforms to retain their own identity systems while securely sharing identity data with one another. For example, each base station can verify the identities of devices from other locations without the need for a central authority, thereby directly supporting interoperability across heterogeneous systems. Finally, SABEC's dynamic clustering and leader election mechanisms allow UAVs from different manufacturers to be grouped based on trust metrics and to operate in a coordinated manner. This facilitates the collaborative execution of joint missions across UAVs with diverse infrastructures. In summary, the design of SABEC and the dynamic identity authentication protocols provides a multi-layered solution to interoperability challenges from both technical and security perspectives: delivering a shared and decentralized trust infrastructure while enabling real-time adaptive security mechanisms that simplify the integration of heterogeneous systems.

Single Point of Failure Risk in Centralized Systems: Traditional centralized identity management systems depend on a single authority, increasing the risk of system-wide failure or attack.

- ✓ ***Contribution of the thesis:*** SABEC's blockchain-based decentralized architecture and LBFT-supported consensus structures eliminate single points of failure. Since identity authentication and data integrity processes are distributed across multiple nodes, attacks or failures cannot compromise the entire network.

Challenges in AI/ML-Based Systems: Model training complexity, data privacy concerns, and the opacity of AI-driven decisions are significant obstacles.

- ✓ ***Contribution of the thesis:*** The thesis does not directly address the challenges of AI/ML-based systems. The proposed work does not incorporate AI/ML-driven identity authentication, anomaly detection, or decision-support mechanisms. However, the SABEC protocol architecture could be extended with AI-supported modules in future research.

Processing Delay: Blockchain consensus and cryptographic operations can introduce delays, leading to interruptions in real-time missions.

- ✓ ***Contribution of the thesis:*** The SABEC and dynamic identity authentication protocols, which form the foundation of the thesis, use lightweight cryptography and consensus algorithms to reduce computational load. Instead of traditional cryptographic methods that could cause high latency in UAVs with limited processing power, lightweight cryptography (e.g., symmetric key mechanisms) is utilized. This minimizes processing load and significantly reduces delays in identity authentication processes. Additionally, in SABEC, UAVs form adaptive clusters based on trust metrics and location data, and a leader is selected within each cluster to manage low-latency data and identity authentication traffic. This hierarchical, fast authentication flow eliminates the high-latency architecture that would require all UAVs to authenticate one another directly. Importantly, the identity management mechanism developed in the thesis is designed to integrate with edge computing infrastructures. Computationally intensive identity verification and security controls are performed at edge nodes rather than on UAV processors, thereby reducing onboard latency sources and preserving real-time processing capability. Furthermore, SABEC replaces traditional high-latency blockchain consensus mechanisms like PoW with fast consensus protocols (e.g., Practical LBFT), which require less processing power and time, enabling transactions to be recorded rapidly on the ledger and minimizing delays.

Dynamic Topology and Resource Constraints in UAV Networks: How This Thesis Advances Beyond MANET Solutions:

The unique attributes exhibited by Unmanned Aerial Vehicle (UAV) networks, particularly in terms of dynamic topology and resource limitations, necessitate the development of far more specialized solutions in the domain of identity management and security when compared to Mobile Ad Hoc Networks (MANETs). While MANET nodes typically consist of terrestrial devices such as laptops or smartphones that move at pedestrian or ground vehicle speeds, UAVs operate in three-dimensional (3D) environments at significantly higher velocities and with superior manoeuvrability. UAVs, which are capable of abrupt changes in route and altitude as well as complex flight patterns, cause network topology to change much more rapidly and unpredictably than in MANETs. This rapid topological variation makes it considerably more challenging to maintain connection continuity and ensure the stable operation of routing protocols. In contrast, MANETs generally experience fewer link disruptions due to the relatively slow movement of nodes, allowing conventional routing protocols sufficient time to respond to topological changes.

In terms of resource constraints, UAVs face substantially greater limitations compared to MANET devices. MANET nodes are typically equipped with larger battery capacities and, in some cases, have access to external power sources (e.g., mains electricity), whereas UAVs are entirely dependent on their onboard batteries, which must simultaneously support both flight and communication functions. As a result, every operation (including encryption, routing, or data transmission) directly affects flight duration, making energy efficiency a critical priority. Furthermore, UAVs have limited processor capacity, as their onboard processors must concurrently manage flight control, communication, and security functions. In contrast, MANET devices generally possess hardware capable of comfortably performing complex encryption operations and frequent routing computations.

This thesis offers a significant divergence from, and improvement over traditional solutions designed for MANETs through the introduction of the SABEC protocol and dynamic identity authentication mechanisms. The proposed secure identity management framework incorporates lightweight cryptography, resource-efficient consensus algorithms, and adaptive clustering strategies specifically designed to accommodate high mobility and constrained resource conditions. SABEC mitigates the adverse effects of rapid topological changes and ensures network-wide efficiency by dynamically grouping UAVs according to trust metrics and coordinating secure communications via leader election. Moreover, the blockchain-based decentralized architecture of SABEC eliminates single points of failure and enables heterogeneous UAV platforms to operate compatibly within a unified, secure identity management infrastructure. Thus, the framework developed in this thesis not only addresses challenges such as scalability, energy efficiency, and interoperability (challenges that MANET-based solutions cannot fully resolve) but also establishes a robust foundation for supporting secure, flexible, and sustainable operations in UAV networks.

Chapter 3

Analysis of UAV Network Requirements

The integration of Unmanned Aerial Vehicle (UAV) networks into critical sectors such as surveillance, disaster response, logistics, and environmental monitoring has revolutionized operational capabilities (Hayat et al., 2016; Erdelj et al., 2017). However, this proliferation also introduces significant security challenges that necessitate a comprehensive analysis of UAV network requirements (Pandey et al., 2022). This chapter delves into the fundamental security considerations essential for safeguarding UAV communications and operations. It systematically examines adversary models, delineates critical security goals, and explores defence mechanisms against prevalent cyber-attacks (Arun et al., 2024; Muthalagu et al., 2024). Additionally, the chapter elucidates the role of blockchain technology in enhancing the security and reliability of UAV networks, thereby informing the design and implementation of an effective Identity Management System (IDMS) (Alsoliman et al., 2020; Chen et al., 2022).

3.1 Analysis of Key Requirements

Securing UAV networks entails addressing a spectrum of technical and operational requirements that ensure the confidentiality, integrity, availability, and accountability of communications and data exchanges. The primary requirements can be categorized into scalability, real-time performance, resource efficiency, interoperability, and resilience.

Scalability: UAV networks are characterized by their dynamic nature, with varying numbers of UAVs participating in missions that can range from small-scale operations to large, coordinated deployments. The IDMS must be capable of scaling seamlessly to accommodate fluctuating network sizes without compromising performance. Scalability is achieved through decentralized architectures, such as blockchain, which distribute authentication and authorization processes across multiple nodes, thereby avoiding bottlenecks associated with centralized systems (Xu et al., 2018).

Real-Time Performance: Many UAV applications demand real-time or near-real-time responses, particularly in mission-critical scenarios like disaster response and surveillance. The IDMS must ensure that authentication and data exchange processes do not introduce significant latency that could impede timely decision-making and operational effectiveness. This necessitates the optimization of cryptographic algorithms and the deployment of high-performance hardware capable of handling rapid authentication requests (Rajesh et al., 2023).

Resource Efficiency: UAVs are often constrained by limited computational power, battery life, and memory capacity. The IDMS must be designed to operate efficiently within these constraints, employing lightweight cryptographic protocols and optimized data management techniques that minimize resource consumption while maintaining robust security (Zhang et al., 2024). Techniques such as edge computing can offload computationally intensive tasks from UAVs to nearby base stations or edge nodes, thereby conserving onboard resources and enhancing overall system efficiency (Jia et al., 2024).

Interoperability: UAV networks frequently consist of heterogeneous devices from various manufacturers, each with distinct technical specifications and communication protocols. The IDMS must ensure interoperability among these diverse platforms, enabling seamless integration and communication across the network. This requires the development of standardized authentication frameworks and protocols that can accommodate varying device capabilities and communication standards, thereby fostering a cohesive and unified UAV ecosystem (Tkachuk et al., 2021).

Resilience: UAV networks must be resilient against a variety of disruptions, including cyber-attacks, hardware failures, and environmental factors. The IDMS should incorporate redundant authentication mechanisms and failover protocols to maintain network functionality in the event of component failures or targeted attacks. Resilience is further enhanced through the use of decentralized architectures and robust consensus mechanisms that ensure continuous operation despite the presence of faulty or malicious nodes (Faraji et al., 2014).

By meticulously addressing these key requirements, the IDMS can provide a secure and efficient foundation for UAV networks, enabling their reliable operation across diverse and critical applications.

3.2 Adversary Models

A thorough understanding of potential adversaries is paramount for designing robust security frameworks within UAV networks. This study adopts a multifaceted adversary model encompassing traditional and contemporary threat paradigms, reflecting the evolving landscape of cyber threats targeting UAV ecosystems. The primary adversary models considered include the Dolev-Yao (DY) threat model, the Byzantine adversary model, insider threats, and advanced persistent threats (APTs).

Dolev-Yao (DY) Threat Model: The DY model serves as a foundational framework for evaluating the security of communication protocols. In UAV networks, the DY adversary is assumed to have complete control over the communication channels between UAV devices and base stations (BS). This includes capabilities to intercept, modify, fabricate, and replay any messages exchanged within the network. Moreover, the adversary can extract and analyse credentials from compromised devices, facilitating sophisticated attacks such as Man-in-the-Middle (MitM) and replay attacks (Kampourakis et al., 2023). This model is instrumental in identifying vulnerabilities in authentication and key agreement protocols, ensuring that the proposed IDMS can withstand both passive eavesdropping and active interception attempts.

Byzantine Adversary Model: Extending beyond the DY model, the Byzantine adversary model addresses scenarios where adversaries exhibit arbitrary and potentially coordinated malicious behaviours. In UAV networks, Byzantine adversaries may attempt to disrupt consensus mechanisms, introduce conflicting information, or manipulate trust assessments within blockchain-enabled IDMS frameworks (Vangala et al., 2022). This model is particularly relevant in decentralized environments where consensus protocols must tolerate a subset of faulty or malicious nodes without compromising the overall integrity and reliability of the network. By incorporating the Byzantine model, the IDMS is designed to enhance resilience against not only external eavesdroppers but also internal adversaries that may seek to undermine the network's trust and operational efficacy.

Insider Threats: Insider threats constitute another critical adversary model, wherein individuals with authorized access to the UAV network exploit their privileges for malicious purposes. Insiders may manipulate data, disrupt communications, or facilitate external attacks by providing adversaries with critical information. This model underscores the necessity for stringent access controls, continuous monitoring, and behavioural analytics within the IDMS to detect and mitigate unauthorized activities originating from trusted entities (Mbaya et al., 2023).

Advanced Persistent Threats (APTs): APTs represent highly sophisticated and sustained attacks orchestrated by well-funded and organized adversaries, often with geopolitical motivations. In UAV networks, APTs could involve prolonged infiltration, data exfiltration, and persistent attempts to compromise critical infrastructure (Wang et al., 2024). Defending against APTs requires a layered security approach, incorporating anomaly detection, continuous monitoring, and adaptive defence mechanisms that can evolve in response to emerging threats.

By integrating these diverse adversary models, the proposed IDMS framework is equipped to address a broad spectrum of threats, ensuring comprehensive protection for UAV networks against both conventional and emerging cyber threats.

3.3 Security Goals

To effectively secure UAV networks against the multifaceted threats delineated by the adversary models, it is imperative to establish a set of comprehensive security goals. These goals serve as the foundational pillars upon which the IDMS is constructed, ensuring that the system not only deters unauthorized access but also maintains the confidentiality, integrity, availability, and accountability of communications within the UAV ecosystem.

Mutual Authentication: One of the paramount security goals is the implementation of mutual authentication between UAVs and BSs. Mutual authentication ensures that both entities verify each other's identities before establishing any communication channel, thereby preventing unauthorized entities from masquerading as legitimate devices. This bidirectional verification is critical in mitigating impersonation attacks, where adversaries attempt to gain access by pretending to be authorized UAVs or BSs (Alkanhal et al., 2023). Achieving mutual authentication involves the use of robust cryptographic protocols, such as public-key infrastructure (PKI) and digital certificates, which provide verifiable credentials that authenticate each party's identity unequivocally.

Confidentiality: Ensuring the confidentiality of communication messages between UAVs and BSs is fundamental to protecting sensitive information from unauthorized access and interception. In UAV networks, data such as surveillance footage, mission parameters, and operational commands must remain concealed to prevent adversaries from exploiting this information for malicious purposes. Confidentiality is achieved through the deployment of advanced encryption techniques, including symmetric and asymmetric encryption algorithms, which render the data unreadable to unauthorized entities during transmission (Thompson et al., 2016). Additionally, the use of secure key management practices ensures that encryption keys are protected against compromise and misuse.

Data Integrity: Maintaining data integrity guarantees that the information exchanged within UAV networks remains unaltered during transit, ensuring that the data received by UAVs and BSs is accurate and trustworthy. Data integrity is critical for preventing data tampering, which could lead to erroneous decision-making and operational failures. The IDMS incorporates integrity verification mechanisms, such as digital signatures and hashing algorithms, which allow the detection of any unauthorized modifications to data. By ensuring that each message is accompanied by a verifiable integrity check, the system upholds the reliability and authenticity of communications (Din et al., 2021).

Anonymity: Preserving the anonymity of UAV devices and their operators is essential to protect against targeted attacks and privacy breaches. Anonymity mechanisms ensure that sensitive information, such as device IDs and geographical locations, is not disclosed to unauthorized parties, thereby mitigating the risk of adversaries tracking UAV movements or correlating activities across the network. The IDMS employs pseudonymous identifiers and privacy-enhancing technologies, such as zero-knowledge proofs and differential privacy, to obscure the true identities and operational details of UAVs, thereby safeguarding individual privacy while maintaining the overall security of the network (Cremonezi et al., 2024).

Availability: Ensuring the availability of UAV network services is critical for maintaining operational continuity, especially in mission-critical scenarios. The IDMS must be resilient against Denial-of-Service (DoS) attacks and other disruptions that could impair network functionality. This is achieved through the implementation of redundant authentication mechanisms, load-balancing strategies, and failover protocols that ensure UAV communications remain uninterrupted even under adverse conditions or targeted attacks (Rafique et al., 2024). Additionally, the use of decentralized architectures, such as blockchain, enhances the network's resilience by eliminating single points of failure and distributing control across multiple nodes.

Accountability: Accountability mechanisms are integral to trace and attribute actions within the UAV network, fostering responsible usage and facilitating forensic investigations in the event of security breaches. The IDMS incorporates logging and auditing functionalities that record authentication attempts, data exchanges, and access events, thereby enabling the detection and analysis of suspicious activities. These records provide a verifiable trail that can be used to investigate incidents, enforce security policies, and hold responsible parties accountable for malicious actions (Tkachuk et al., 2021).

By delineating these security goals, the IDMS establishes a comprehensive framework that addresses the core aspects of UAV network security, ensuring that communications remain secure, reliable, and trustworthy.

3.4 Defence Mechanisms Against Known Attacks

The proposed IDMS integrates a suite of defence mechanisms specifically designed to counteract the identified adversarial threats, ensuring robust protection of UAV network communications. These mechanisms are tailored to address the unique challenges posed by UAV deployments, leveraging advanced cryptographic techniques and blockchain technology to enhance security and resilience.

Impersonation Attack Prevention: To mitigate impersonation attacks, the IDMS employs mutual authentication protocols that rigorously verify the identities of both UAVs and BSs. Utilizing PKI, the system ensures that each entity presents valid credentials before establishing any communication, thereby preventing adversaries from successfully masquerading as legitimate devices (Alzahrani et al., 2024). The use of asymmetric cryptography ensures that even if an adversary obtains a device's public key, they cannot derive the corresponding private key, thereby maintaining the integrity of the authentication process.

Replay Attack Mitigation: Replay attacks are addressed through the incorporation of dynamic session keys, current timestamps, and random nonces within the authentication process. These elements ensure that each authentication attempt is unique and cannot be maliciously reused, thereby maintaining the integrity and security of ongoing communications (Bera et al., 2024). Additionally, the IDMS implements sequence numbers and expiration times to further enhance protection against replay attempts, ensuring that stale or duplicated messages are rejected by the system.

Man-in-the-Middle (MitM) Attack Prevention: MitM attacks are countered by implementing end-to-end encryption and secure key agreement protocols that ensure the confidentiality and integrity of data exchanged between UAVs and BSs. Furthermore, mutual authentication mechanisms verify the identities of both parties, making it exceedingly difficult for adversaries to intercept and alter communications without detection (Jan et al., 2022). The use of forward secrecy ensures that even if a session key is compromised, past communications remain secure, thereby limiting the impact of any potential breaches.

Byzantine Fault Tolerance: In blockchain-enabled UAV networks, Byzantine fault tolerance is crucial for maintaining consensus and network integrity despite the presence of malicious nodes. The IDMS integrates consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Stake (PoS), which are designed to withstand Byzantine adversaries by ensuring that consensus can be achieved even when a subset of nodes behaves maliciously (Saleh et al., 2024). These protocols enhance the resilience of the blockchain framework, ensuring reliable and secure decision-making processes within the UAV network. Additionally, the use of decentralized consensus mechanisms distributes trust across multiple nodes, thereby preventing any single entity from exerting undue influence over the network.

Insider Threat Mitigation: Recognizing the potential for insider threats, the IDMS incorporates stringent access controls, role-based permissions, and continuous monitoring to detect and prevent unauthorized activities by trusted entities. Behavioural analytics and anomaly detection algorithms are employed to identify deviations from normal operational patterns, enabling the early detection of malicious actions by insiders. This proactive approach ensures that even individuals with authorized access cannot exploit their privileges to compromise the network (Xiao et al., 2019).

Advanced Persistent Threat (APT) Defence: Defending against APTs requires a layered security approach that incorporates multiple defence mechanisms to detect and respond to prolonged and sophisticated attacks. The IDMS employs continuous monitoring, intrusion detection systems (IDS), and threat intelligence feeds to identify and mitigate APT activities in real-time. By leveraging machine learning algorithms, the system can analyse vast amounts of data to identify subtle indicators of compromise, thereby enabling timely and effective responses to emerging threats (Hadi et al., 2024).

Data Privacy Preservation: To preserve data privacy, the IDMS employs pseudonymous identifiers and privacy-enhancing technologies such as zero-knowledge proofs and differential privacy. These techniques ensure that sensitive information, including device IDs and operational details, remains concealed from unauthorized entities while maintaining the security and transparency benefits of blockchain (Peddibhotla et al., 2024). This dual approach safeguards individual privacy without compromising the overall security posture of the UAV network.

By integrating these defence mechanisms, the IDMS establishes a robust security infrastructure capable of countering a wide array of cyber threats, thereby ensuring the secure and reliable operation of UAV networks.

3.5 Privacy and Security Considerations

Privacy and security are intertwined yet distinct aspects of UAV network management, each necessitating specific considerations to ensure comprehensive protection of data and operations. This section explores the key privacy and security considerations that inform the design of the proposed IDMS, highlighting the balance between operational efficiency and data protection.

Data Confidentiality and Encryption: Ensuring the confidentiality of data transmitted within UAV networks is paramount to prevent unauthorized access and exploitation. The IDMS employs robust encryption mechanisms, including Advanced Encryption Standard (AES) for data encryption and Elliptic Curve Cryptography (ECC) for secure key exchange. These cryptographic techniques ensure that sensitive information such as surveillance data, mission plans, and control commands remain protected from interception and unauthorized decryption (Vangala et al., 2023).

Access Control and Authentication: Effective access control mechanisms are essential for regulating who can access and modify data within UAV networks. The IDMS incorporates role-based access control (RBAC) and attribute-based access control (ABAC) models to enforce granular permissions based on user roles, attributes, and contextual factors. Combined with mutual authentication protocols, these access control mechanisms ensure that only authorized UAVs and personnel can access critical network resources and data (Mohamed et al., 2024).

Anonymity and Pseudonymity: Protecting the identities of UAVs and their operators is crucial for preventing targeted attacks and preserving privacy. The IDMS employs pseudonymous identifiers that decouple UAV identities from their operational data, ensuring that device IDs and location information are not directly linked or easily traceable by adversaries. Techniques such as zero-knowledge proofs further enhance anonymity by allowing UAVs to prove their legitimacy without revealing sensitive information (Guo et al., 2024).

Data Integrity and Authenticity: Maintaining the integrity and authenticity of data is essential for ensuring the reliability of UAV operations. The IDMS leverages digital signatures and hash-based message authentication codes (HMACs) to verify that data has not been tampered with during transmission. These mechanisms ensure that any alterations to data are detectable, thereby maintaining the trustworthiness of information exchanged within the network (Cho et al., 2020).

Privacy-Preserving Data Sharing: UAV networks often involve the exchange of large volumes of data, some of which may contain sensitive or personally identifiable information (PII). The IDMS incorporates privacy-preserving data sharing protocols that enable secure and anonymous data dissemination without compromising user privacy. Techniques such as differential privacy and secure multi-party computation (SMPC) allow for the aggregation and analysis of data while ensuring that individual data points remain protected (Sudhina Kumar et al., 2023).

Regulatory Compliance: Compliance with data protection regulations such as the General Data Protection Regulation (GDPR) is essential for the lawful and ethical operation of UAV networks. The IDMS is designed to adhere to these regulatory standards by implementing data minimization principles, ensuring data subject rights, and maintaining comprehensive audit trails. This compliance not only mitigates legal risks but also enhances the trust and acceptance of UAV technologies in public and commercial domains (Suomalainen et al., 2021).

Incident Response and Recovery: Effective incident response and recovery mechanisms are critical for mitigating the impact of security breaches and ensuring the continuity of UAV operations. The IDMS includes predefined protocols for detecting, responding to, and recovering from security incidents. This involves the deployment of real-time monitoring systems, automated alerting mechanisms, and disaster recovery plans that enable swift restoration of services following an attack or failure (Jan et al., 2022).

User Awareness and Training: Human factors play a significant role in the security of UAV networks. The IDMS incorporates user awareness and training programs to educate UAV operators and administrators about best security practices, potential threats, and the importance of maintaining vigilance against cyber-attacks. By fostering a security-conscious culture, these programs reduce the likelihood of human errors and insider threats, thereby enhancing the overall security posture of the network (Butt et al., 2024).

By meticulously addressing these privacy and security considerations, the proposed IDMS ensures that UAV networks can operate securely and efficiently while safeguarding sensitive data and protecting user privacy. This holistic approach balances the need for operational effectiveness with stringent data protection measures, thereby fostering trust and reliability in UAV network deployments.

3.6 Integration of Blockchain Technology

Blockchain technology serves as a cornerstone in enhancing the security and efficiency of the proposed IDMS for UAV networks. By leveraging blockchain's decentralized and immutable ledger capabilities, the IDMS achieves several critical security objectives, including data integrity, transparency, and resistance to tampering.

Decentralized Authentication: Traditional centralized authentication systems are susceptible to single points of failure and targeted attacks. Blockchain-based IDMS eliminates these vulnerabilities by distributing the authentication process across a network of nodes, thereby enhancing resilience and reliability. Each authentication transaction is recorded on the blockchain, ensuring that identity verification processes are transparent and tamper-proof. This decentralized approach not only mitigates the risks associated with centralized authorities but also facilitates seamless scalability as the UAV network expands (Aloqaily et al., 2021).

Secure Data Sharing: Blockchain facilitates secure and transparent data sharing among UAVs and between UAVs and BSs. Smart contracts automate and enforce data exchange protocols, ensuring that data transactions are executed securely and without the need for intermediaries. This automation not only streamlines communication processes but also enhances trust among network participants by providing verifiable and immutable records of data exchanges. Consequently, applications such as real-time surveillance and disaster management benefit from reliable and tamper-proof data dissemination (Khan et al., 2022).

Trust Establishment and Consensus Mechanisms: The integration of blockchain into the IDMS framework enables the establishment of trust among UAVs and BSs through consensus mechanisms. These mechanisms ensure that all participating entities adhere to predefined security protocols and standards, thereby fostering a trustworthy network environment. The study employs consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Stake (PoS), which are designed to withstand Byzantine adversaries by ensuring that consensus can be achieved even when a subset of nodes behaves maliciously (Zhang et al., 2024). This robust consensus framework maintains the integrity and security of UAV network operations, preventing the inclusion of untrusted nodes and ensuring consistent data validation.

Data Integrity and Provenance: Blockchain ensures data integrity and provenance by recording all data transactions on an immutable ledger. This guarantees that data collected by UAVs remains unaltered and traceable, providing a verifiable history of data generation and transmission. Such features are crucial for applications requiring reliable data for decision-making, such as environmental monitoring and precision agriculture. Furthermore, the use of blockchain in conjunction with edge computing has been explored to enhance the efficiency and scalability of UAV networks. By offloading computational tasks to edge nodes, blockchain reduces the processing burden on UAVs, thereby conserving their limited resources and enabling more efficient data management (Ibrahim et al., 2024).

Scalability and Efficiency Optimizations: While blockchain introduces robust security features, it also presents challenges related to scalability and computational overhead. To address these issues, the proposed IDMS incorporates lightweight blockchain protocols and optimized consensus algorithms tailored to the resource-constrained nature of UAVs. Innovations such as Proof of Stake (PoS) and Federated Consensus are employed to enhance scalability and reduce energy consumption, making blockchain integration feasible for large-scale UAV deployments. These optimizations ensure that the blockchain-enabled IDMS can efficiently handle high volumes of authentication transactions without compromising the performance or operational efficiency of the UAV network (Qaqish et al., 2023).

Adaptive Network Architecture: Blockchain technology facilitates the dynamic restructuring of the trusted network architecture, enabling UAV nodes to adaptively reconfigure secure communication pathways as needed. This adaptability is crucial in environments where UAVs frequently join or leave the network, requiring the system to maintain consistent security standards without manual intervention. The decentralized nature of blockchain allows for continuous updates and real-time adjustments to the network's trust framework, ensuring sustained security and operational efficiency (Qian et al., 2024).

By integrating blockchain technology, the proposed IDMS not only enhances the security and integrity of UAV communications but also provides a scalable and adaptable framework capable of supporting the growing and dynamic nature of UAV networks. This integration ensures that the IDMS remains resilient against evolving cyber threats while maintaining operational efficiency and reliability.

3.7 Practical Requirements and Considerations

Beyond theoretical security objectives and defence mechanisms, practical considerations play a pivotal role in the effective deployment of an IDMS within UAV networks. These considerations encompass scalability, real-time performance, resource constraints, interoperability, and compliance with regulatory standards.

Scalability: UAV networks are inherently dynamic, with varying numbers of UAVs joining and leaving the network based on mission requirements. The IDMS must be capable of scaling seamlessly to accommodate large fleets of UAVs without degrading performance. Blockchain technology, with its decentralized architecture, inherently supports scalability by distributing authentication and decision-making processes across multiple nodes. However, achieving scalability also requires the implementation of efficient consensus mechanisms and lightweight cryptographic protocols that do not impose excessive computational or energy burdens on resource-constrained UAVs (Khalid et al., 2020).

Real-Time Performance: UAV operations often demand real-time or near-real-time responses, particularly in mission-critical applications such as disaster response and surveillance. The IDMS must ensure that authentication and data exchange processes do not introduce significant latency that could impede timely decision-making and operational effectiveness. This necessitates the optimization of cryptographic algorithms and the deployment of high-performance hardware capable of handling rapid authentication requests without bottlenecks (Din et al., 2021).

Resource Constraints: UAVs typically operate under stringent resource constraints, including limited battery life, computational power, and memory capacity. The IDMS must be designed to operate efficiently within these constraints, employing lightweight cryptographic protocols and optimized data management techniques that minimize resource consumption while maintaining robust security (Ma et al., 2023). Additionally, offloading computationally intensive tasks to edge nodes or base stations can help alleviate the burden on individual UAVs, enhancing overall system efficiency.

Interoperability: UAV networks often comprise heterogeneous devices from various manufacturers, each with distinct technical specifications and communication protocols. The IDMS must ensure interoperability among these diverse platforms, enabling seamless integration and communication across the network. This requires the development of standardized authentication frameworks and protocols that can accommodate varying device capabilities and communication standards, thereby fostering a cohesive and unified UAV ecosystem (Poirrier et al., 2023).

Regulatory Compliance: Compliance with international and regional regulatory standards is essential for the lawful and ethical deployment of UAV networks. The IDMS must adhere to data protection regulations such as the General Data Protection Regulation (GDPR) and other relevant standards governing the collection, storage, and processing of sensitive information. Ensuring compliance not only mitigates legal risks but also enhances the trust and acceptance of UAV technologies in public and commercial domains (Qaqish et al., 2023).

User-Friendly Management: The management and administration of the IDMS should be user-friendly, providing intuitive interfaces and automated processes that simplify the onboarding, authentication, and monitoring of UAVs within the network. Effective user interfaces and management tools enhance operational efficiency and reduce the likelihood of human errors, thereby contributing to the overall security and reliability of the UAV network (Serafimova et al., 2023).

Addressing these practical requirements is crucial for the successful deployment and sustained operation of the IDMS within UAV networks. By balancing theoretical security objectives with real-world constraints and operational demands, the proposed IDMS ensures that UAV networks can operate securely, efficiently, and reliably across a wide range of applications.

3.8 Risk Assessment and Analysis

Risk Assessment and Analysis Conducting a risk assessment is pivotal for identifying, evaluating, and prioritizing potential threats to UAV networks. This process enables the development of targeted mitigation strategies that address the most critical vulnerabilities, thereby enhancing the overall security posture of the network. The risk assessment in this study follows a systematic approach, encompassing threat identification, vulnerability analysis, impact assessment, and risk prioritization (Javaid et al., 2012).

Threat Identification: Building upon the established threat models, the risk assessment begins with the identification of specific threats that could compromise

UAV network security. These threats include impersonation attacks, replay attacks, MitM attacks, data tampering, unauthorized access, and service disruptions caused by DoS attacks. Each identified threat is analysed in the context of its potential to exploit vulnerabilities within the IDMS and the broader UAV network infrastructure (Tanveer et al., 2020).

Vulnerability Analysis: The next step involves a detailed analysis of the vulnerabilities that could be exploited by the identified threats. Vulnerabilities may arise from weak cryptographic protocols, insufficient access controls, insecure communication channels, and inadequate monitoring mechanisms. networking these vulnerabilities to the specific threats, the assessment highlights areas where the IDMS and UAV network are most susceptible to attacks (Jan et al., 2022).

Impact Assessment: Assessing the potential impact of each threat is essential for understanding the severity of the risks and prioritizing mitigation efforts. The impact assessment considers factors such as data loss, operational disruption, financial losses, reputational damage, and regulatory penalties. For instance, a successful MitM attack could lead to unauthorized data access and manipulation, resulting in significant operational failures and compromised mission integrity (Gupta et al., 2023).

Risk Prioritization: Based on the likelihood and potential impact of each threat, risks are prioritized to focus on those that pose the greatest threat to UAV network security. High-priority risks are those with a high likelihood of occurrence and a severe impact, necessitating immediate and robust mitigation measures. Medium and low-priority risks, while still important, may be addressed through less urgent interventions or monitored for changes in threat levels over time (Jacobsen et al., 2021).

Mitigation Strategies: For each high-priority risk, specific mitigation strategies are developed to reduce the likelihood of occurrence and minimize potential impacts. These strategies include the implementation of stronger encryption protocols, enhancing mutual authentication mechanisms, deploying intrusion detection systems (IDS), and conducting regular security audits and vulnerability assessments. Additionally, training and awareness programs for UAV operators and administrators are essential for fostering a security-conscious culture and reducing the risk of insider threats (Shafique et al., 2021).

Residual Risk Management: Despite comprehensive mitigation efforts, some level of residual risk may remain. The IDMS must include mechanisms for continuous monitoring and adaptive security measures to manage and respond to these residual risks effectively. This involves maintaining up-to-date threat intelligence, conducting ongoing risk assessments, and adapting security protocols in response to evolving threats and vulnerabilities (Ihekoronye et al., 2023).

By systematically identifying and addressing the most critical risks, the proposed IDMS ensures that UAV networks are equipped with the necessary defences to withstand a wide range of cyber threats, thereby maintaining secure and reliable operations.

3.9 Summary

In summary, the analysis of UAV network requirements underscores the critical necessity for a robust and efficient Identity Management System capable of addressing the unique challenges posed by UAV deployments. By adopting a comprehensive adversary model that includes both Dolev-Yao and Byzantine threat scenarios, along with considerations for insider threats and advanced persistent threats (APTs), this study establishes a rigorous security framework that informs the design of the proposed IDMS. The delineation of essential security goals—mutual authentication, confidentiality, data integrity, anonymity, availability, and accountability—provides a clear set of objectives that the IDMS must achieve to ensure secure and reliable UAV operations. The integration of advanced defence mechanisms against impersonation, replay, and MitM attacks, coupled with Byzantine fault-tolerant consensus protocols within the blockchain framework, fortifies the overall security posture of the UAV network. Blockchain technology not only enhances decentralized authentication and secure data sharing but also ensures trust establishment and data integrity through its immutable ledger capabilities. Additionally, the incorporation of privacy-preserving technologies and optimized consensus algorithms addresses critical concerns related to anonymity, scalability, and computational efficiency.

Furthermore, practical considerations such as scalability, real-time performance, resource constraints, interoperability, regulatory compliance, and user-friendly management are meticulously addressed to ensure the feasibility and effectiveness of the IDMS in real-world UAV network scenarios. By balancing theoretical security objectives with practical operational demands, the proposed IDMS provides a comprehensive and resilient solution for securing UAV networks against a diverse array of cyber threats. The subsequent chapters will delve into the implementation details and empirical evaluation of the proposed IDMS, providing evidence of its efficacy and robustness in safeguarding UAV network communications and operations.

Chapter 4

Methodology

This chapter delineates the methodological framework employed to develop and evaluate the proposed Identity Management System (IDMS) tailored for Unmanned Aerial Vehicle (UAV) networks. The methodology encompasses the design of the network model, the development of secure authentication protocols, the integration of blockchain technology for decentralized decision-making, and the implementation of simulation experiments to assess system performance. Each methodological component is meticulously detailed to ensure reproducibility and validity of the research outcomes.

A brief overview of the proposed system model

The aim of this thesis study is to design a scalable, energy-efficient, and secure identity management system for unmanned aerial vehicle (UAV) networks characterized by high mobility and dynamic structures. In this context, the proposed system model covers a decentralized and dynamic multi-UAV network established with unmanned aerial vehicles possessing high manoeuvrability. The designed network particularly *targets applications* such as precision agriculture, disaster management, and surveillance, where real-time video transmission, instantaneous sensor data sharing, and mission coordination messaging constitute the core communication types. Furthermore, the system model is designed to enable UAVs from different manufacturers and platforms to operate in a coordinated and secure manner under an adaptive identity authentication and decentralized trust infrastructure. The *main applications* running over the network include operations that require low latency and high reliability, such as real-time video transmission, instantaneous sensor data sharing, mission coordination messaging, and status reporting.

From the perspective of *resource constraints*, each UAV is foreseen to have an ARM-based embedded processor with 1–2 GHz capacity, a battery enabling 30–45 minutes of flight time, and a bandwidth ranging between 2–20 Mbps depending on environmental conditions, as shown in Figure 1. Real-time data transmission requires a bandwidth of 2–5 Mbps, while sensor and mission data can be adequately transmitted with lower bandwidth but demand continuity and data integrity. For mission coordination, ultra-low latency communication with less than 100 ms delay is envisaged. Since UAV battery capacity is shared between flight and communication operations, energy efficiency is a critical priority for all protocols. Additionally, given that the processor must handle both flight control and security/communication functions, it is essential that protocols be lightweight in terms of processing load.

The *network model* includes: UAV-to-UAV communication, covering direct short-range communication and in-flight data exchange for mission sharing; UAV-to-Base Station communication, serving as the primary channel for identity authentication and sensor/mission data transmission; Base Station-to-Base Station communication, allowing distributed stations to access one another's identity and data verification records; and Base Station-to-Web/Mobile Site Management System communication, enabling operators to monitor mission status, view logs, and send necessary control commands (as shown in Figure 1).

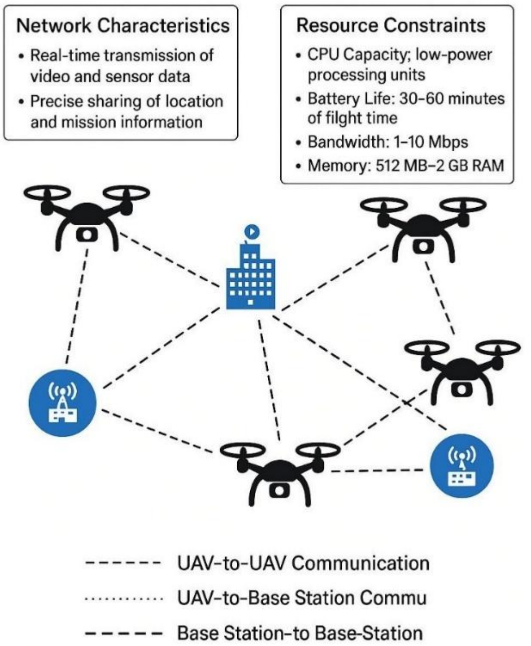

Network Characteristics
• Real-time transmission of video and sensor data
• Precise sharing of location and mission information
Resource Constraints
• CPU Capacity; low-power processing units
• Battery Life: 30-60 minutes of filght time
• Bandwidth: 1-10 Mbps
• Memory: 512 MB-2 GB RAM
UAV-to-UAV Communication
UAV-to-Base Station Commu
Base Station-to Base-Station

Figure 1: Communication method for UAV network

The solution developed in response to these needs consists of *two fundamental phases*. *Firstly*, a lightweight, secure, and dynamic identity authentication protocol has been designed to provide a structure compatible with the high mobility and resource-constrained conditions of UAV networks. This protocol is built on lightweight cryptographic operations to minimize processing and communication overhead. It employs AES-based symmetric encryption, cryptographic hash functions, timestamps, randomly generated nonce values, and dynamically changing parameter variables. As a result, the identity authentication processes provide a robust level of security while operating at a low processing cost suitable for UAVs with limited processing power and energy capacity. The actual identity information of the devices is kept confidential and is not shared during direct communication. Instead, each device is assigned a temporary ID and a unique ID. The temporary ID is periodically updated to enhance privacy and anonymity protections on identity information, while the unique ID serves as a permanent identifier within the system, used only in trusted authentication processes and not exposed in external communication. This structure offers high resistance to identity spoofing and device tracking attacks. After successful identity authentication, inter-device messaging and data transmission proceed using cryptographically generated tokens that are renewed at specified intervals. This token mechanism ensures the continuity of identity verification at every stage of data transmission and prevents unauthorized access or tampering attempts during communication. Thus, the integrity and security of communication sessions are preserved through continuously updated tokens, not limited to the initial authentication. This dynamic structure provides strong security in identity authentication and data transmission processes, while offering resource efficiency with low processing load. Additionally, the use of temporary IDs and dynamic tokens creates a continuously updated security layer during UAV mobility and mission transitions, supporting identity privacy and data integrity across the network.

In the *second phase*, the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) protocol is activated. This protocol enables UAVs to be logically grouped into clusters through adaptive clustering based on trust metrics and resource-friendly consensus algorithms, and facilitates the selection of leader UAVs responsible for low-latency identity authentication and data sharing within each cluster. Processes commence among devices that have been dynamically and securely authenticated with the SABEC protocol. At this stage, the SABEC protocol is specially designed to support scalability, energy efficiency, and reliability in line with the network's needs. Within the SABEC protocol, leader UAVs are selected from among UAVs whose identities have been authenticated and verified as trustworthy, based on criteria such as trust metrics and location information. Selected leaders continuously monitor the behaviours of other devices within their clusters, assign dynamic scores by evaluating factors such as data transmission continuity, mission success, and communication security. This scoring system allows real-time and historical monitoring of the reliability levels of all UAVs within the cluster, not just the leaders. The leaders share the data they collect from their clusters and the evaluation scores with the base station. The base station applies a lightweight consensus algorithm within the SABEC protocol framework, filtering out data detected as inconsistent or fraudulent from the leaders, and accepting only data that has been validated by consensus. This data consensus achieved at the base station is completed with the process of recording the validated data immutably into the blockchain using blockchain technology. In this way, the data contributed by both the leader UAVs and their associated devices is recorded transparently, auditable, and securely. This process provides a decentralized trust infrastructure suited to the dynamic structure and resource constraints of the UAV network, eliminating single points of failure and the risk of unauthorized data manipulation. The multi-layered approach of the SABEC protocol offers an important innovation aimed at enhancing the resilience, flexibility, and sustainable security level of the network, especially in heterogeneous UAV fleets and complex mission scenarios.

One of the *most important features* of the system is that identity authentication and data storage operations are performed on the base station rather than directly on the UAVs. This minimizes the processing load and energy consumption of the UAVs, as they transmit only the necessary minimum data to the base station, where secure identity authentication and data processing are provided. Thanks to SABEC's blockchain-based decentralized architecture and the fast, lightweight consensus mechanisms (e.g., LBFT) employed, the risk of single points of failure is eliminated, and UAV platforms of different manufacturers can securely interoperate without needing a central authority.

A *standard challenge-response identity authentication protocol* would be inadequate for such a structure. This is because such a protocol generally requires a static and centralized authentication model and generates a high messaging overhead due to its multi-step communication. This could lead to performance loss and delays in applications sensitive to low latency, such as real-time video transmission and mission coordination. In contrast, the SABEC and dynamic identity authentication mechanisms developed in this thesis provide a holistic and efficient solution to the needs of dynamic, high-mobility UAV networks, offering fast authentication flows with low processing and communication overhead.

4.1 Network Model Design

The foundational network model for the UAV ecosystem comprises three primary layers: drone devices (UAVs), base stations (BS), and cloud/server infrastructure. In this hierarchical architecture, drone devices equipped with Internet of Things (IoT) capabilities communicate with base stations to authenticate and join the network. The network is assumed to consist of multiple BS entities deployed across various geographical regions, each managing a fleet of connected UAVs. A mutually authenticated key-agreement scheme is imperative for establishing secure communication channels between UAVs and BSs (Similar architectures can also be found in the following studies: Bansal et al., 2022; Maaloul et al., 2025). Within this architecture, BSs function as central nodes responsible for implementing the proposed authentication system and forwarding sensitive data to the cloud after performing necessary filtering and analysis. Upon deployment, each BS shares a unique key token with the UAVs connected to it, facilitating secure and authenticated interactions within the UAV environment. It is important to note that the authentication between the cloud and the BS is beyond the scope of this study, and it is assumed that all devices within the network maintain secure operations. The primary objective is to design a mutually authenticated, secure, and efficient key agreement scheme between UAVs and BSs to ensure the integrity and confidentiality of communications within the UAV network.

Subsequently, the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) was developed to provide secure storage and network communication using blockchain consensus protocols. The network model design of SABEC is meticulously crafted to address the inherent complexities and security challenges associated with mission-oriented UAV networks. These networks are characterized by high node mobility, dynamic mission environments, and the pervasive threat of Byzantine nodes—malicious or faulty UAVs capable of disrupting network operations. To ensure secure, efficient, and reliable communication and coordination among UAVs, SABEC integrates advanced blockchain technology with a hierarchical routing architecture, thereby facilitating dynamic network reconfiguration and robust trust management. SABEC employs an innovative cross-layer architecture that integrates advanced blockchain technology with hierarchical clustering algorithms and a robust two-tier consensus mechanism, thereby optimizing UAV network performance through adaptive trust management and enhanced security protocols. At the foundational level, *SABEC incorporates* the *Proximal Node Discovery and Monitoring Component (PDMC)* protocol within the signal transmission and access coordination tier. PDMC is responsible for the accurate detection and continuous monitoring of adjacent UAV nodes, utilizing enhanced signal processing techniques to reliably identify neighbouring nodes even in environments with high interference and significant node mobility. This protocol maintains up-to-date neighbour tables and monitors the forwarding behaviours of adjacent nodes, establishing a dependable foundation for subsequent routing decisions. Building upon this, the data coordination tier integrates three pivotal component protocols: the Localized Trust Coordination Component (LTCC), the Hierarchical Trust-Based Coordination Component (HTCC), and the Secure Border Coordination Component (SBCC). LTCC manages local zone communications by evaluating and prioritizing coordination paths through trusted nodes based on real-time trust assessments, thereby minimizing internal zone coordination overhead and enhancing data delivery efficiency. HTCC facilitates external communications by establishing hierarchical coordination paths that connect different network zones through trusted gateway nodes, employing dynamic clustering algorithms to form and manage these hierarchical structures. SBCC oversees secure data transmission across network boundaries, integrating blockchain-based verification mechanisms to authenticate coordination information and prevent the dissemination of malicious data. At the apex of the architecture lies the service management and control tier, which incorporates the core SABEC protocol. This tier is responsible for managing trust and coordination within the network, maintaining an immutable ledger of node trustworthiness and network configurations through a Private, Permissioned Blockchain (PPB). Each UAV node is assigned a unique cryptographic identity, comprising a public-private key pair and a unique identifier (UID), which are recorded on the blockchain. The PPB records Trust Assessment Transactions (TATs) that encapsulate node behaviour metrics, trust scores, and operational statuses. Unlike conventional blockchains, SABEC's PPB retains only essential consensus results and aggregated trust scores, significantly reducing storage overhead and enhancing scalability.

SABEC employs a *Two-Tier Consensus Mechanism (TTC)* to ensure efficient and secure network reconfiguration, as shown in Figure 2 and 3. The first tier, known as the Trust Evaluation Tier (Data Consensus Stage), involves real-time monitoring of proximal nodes' behaviours using LTCC and HTCC protocols. Nodes generate TATs based on observed behaviours, which are then broadcasted to authorized nodes within the upper management network. This stage utilizes a Lightweight Byzantine Fault Tolerance (LBFT) algorithm to achieve rapid consensus on trust assessments with minimal computational overhead, resulting in an Asynchronous Common Subset (ACS) of state data that represents a collective agreement on node trustworthiness. The second tier, the Network Coordination Tier (Decision Consensus Stage), involves the aggregation and validation of TATs through blockchain-based smart contracts embedded in the Genesis block. Authorized proxy nodes execute these smart contracts to finalize consensus on trust scores and determine necessary network reconfigurations, culminating in the creation of new blockchain blocks that encapsulate updated network configurations. This two-tier approach ensures both local and global agreement on network states and configurations, maintaining the integrity and reliability of the UAV network.

To enhance scalability and manageability, SABEC employs a Fuzzy C-Means Clustering Algorithm (FCMCA) (Saritha et al., 2024) that periodically elects leader drones within predefined clusters. This hierarchical clustering mechanism dynamically adjusts to frequent topology changes and varying node reliability, ensuring that only trusted and reliable UAVs assume leadership roles within their respective zones. Leader drones are responsible for aggregating local trust assessments, transmitting them to a centralized server, and facilitating the consensus process. The hierarchical network structure, managed via blockchain, enables SABEC to accommodate increasing network sizes without incurring prohibitive routing overhead or excessive storage demands. Security is intrinsically woven into SABEC's framework through its blockchain-enhanced trust management system. Each node's trustworthiness is continuously assessed based on real-time monitoring of forwarding behaviours, with malicious or unreliable nodes being systematically isolated from the network.

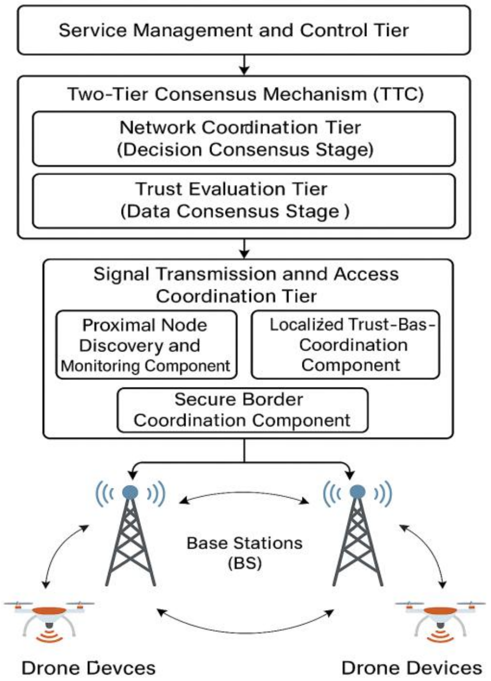


Figure-2: SABEC communication model

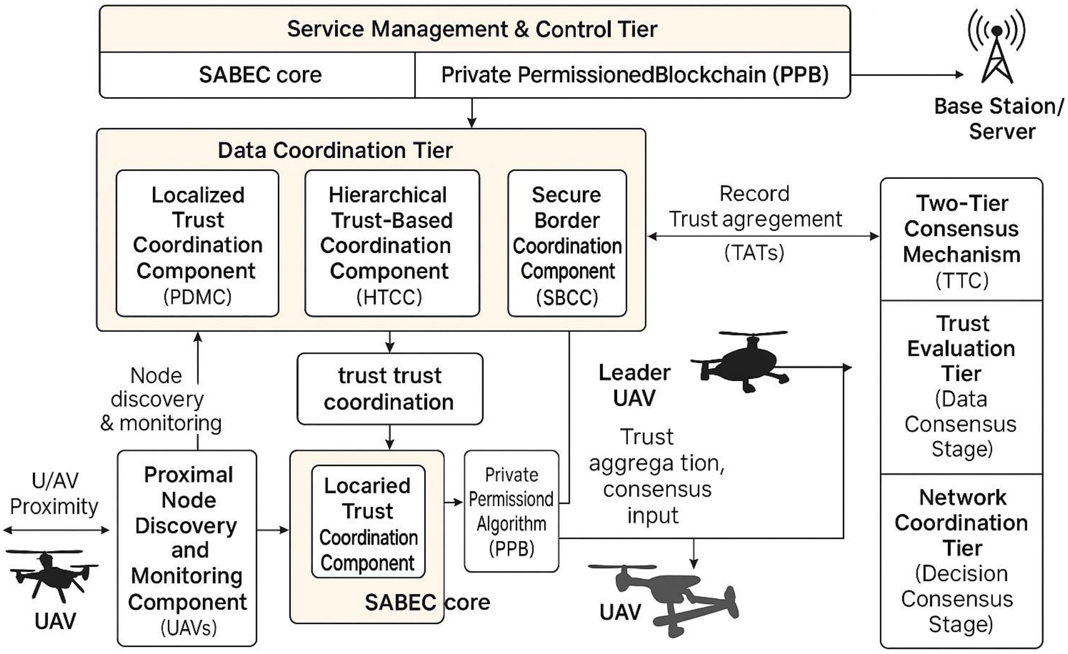


Figure-3: SABEC network model components

4.2 Authentication Protocol Development

Central to the proposed IDMS is the development of a robust authentication protocol that ensures secure and efficient key agreement between UAVs and BSs. The authentication process is divided into three distinct phases: the offline phase, device registration phase, and authentication phase (Wang et al., 2024; Xu et al., 2023). During the offline phase, a one-time computation is performed to personalize UAV devices prior to their deployment in the network. This involves registering UAVs with their respective BSs and distributing security credentials and other essential parameters. The offline phase ensures that UAVs are pre-configured with the necessary cryptographic materials to facilitate secure interactions within the network. In the device registration phase, UAVs formally register with the BS, receiving unique security credentials that facilitate secure communication and authentication in subsequent interactions. This phase ensures that each UAV has a unique cryptographic identity, enabling individualized authentication and secure communication channels between UAVs and BSs. The authentication phase is a dynamic process where UAVs and BSs interact as needed to perform mutual authentication and establish a secure session key for ongoing communication. This session key, dynamically generated during the authentication process, is utilized for secure data exchange throughout the UAV's operational duration within the network. The protocol leverages a combination of dynamic secret keys, current timestamps, random nonces, and renewable tokens to thwart sophisticated attacks such as replay attacks and man-in-the-middle (MitM) attacks. Each entity within the network possesses a unique key pair (public and private) and a temporary ID, ensuring individualized and secure authentication processes (Dogan et al., 2023).

4.3 System Architecture and Application Development

The proposed IDMS architecture integrates three distinct applications to facilitate secure communication and data management within the UAV network. The Drone Service Application is developed for UAV devices and is responsible for securely transmitting data to the BS, ensuring that sensitive information is protected during transmission. The Base Station Service Application, designed for BS nodes with high processing capacities, handles the storage, analysis, and filtering of data received from the Drone Service Application. It selects critical information from the processed data and forwards it to the cloud, ensuring that only relevant and essential data is transmitted for further analysis. The Web Application operates independently of the hierarchical structure and serves as an interface for testing and monitoring the authentication scheme. It displays data received from both the Drone and BS Service Applications, providing users with real-time insights into system operations and performance.

4.4 Blockchain-Enabled Decision-Making Mechanism

To enhance the security and reliability of UAV networks, a distributed blockchain system is integrated into the IDMS to establish an adaptable and reliable decision-making mechanism. This system dynamically constructs a trusted enclave of devices within the UAV network, leveraging a consensus-based decision-making structure that continuously assesses the trustworthiness of network nodes based on real-time data concerning the transmission activities of prominent drones and neighbouring devices (Wahab et al., 2021; Aditya et al., 2021). The blockchain framework incorporates a Proof of Work (PoW) mechanism to prevent the inclusion of Byzantine drones (unreliable devices) by requiring them to solve computationally challenging tasks before gaining entry into the selection pool. This ensures that only trusted nodes are integrated into the network, maintaining the integrity and security of UAV operations. Additionally, the blockchain system facilitates the dynamic restructuring of the trusted network architecture, enabling UAV nodes to adaptively reconfigure secure communication pathways as needed. Simulation experiments validate the performance of the proposed blockchain framework, demonstrating its capability to mitigate the impact of Byzantine drones and achieve superior packet transmission speeds compared to traditional authentication schemes (Cheng et al., 2022). The proposed solution is particularly effective in maintaining secure and efficient communication channels, thus enhancing the overall operational efficiency of the UAV network.

The Structure and Operation of Blockchain Technology and Its Contributions

Blockchain technology is a distributed ledger system that enables reliable data sharing among all network participants within a decentralized architecture, secured through cryptographic techniques. Fundamentally, a blockchain consists of data blocks linked in chronological order within a chain structure, where each block contains the cryptographic hash of its predecessor, as shown in Figure 4. Each block includes validated transactions within a specific time frame, a timestamp, a nonce value, and the hash of the previous block. This structure ensures that any modification to the content of a block impacts the entire chain, thereby allowing the detection and invalidation of such alterations. In blockchain systems, data integrity and transaction validity are maintained not by a central authority but through the collective decision-making of pre-authorized nodes in the network. This decision-making process is executed via consensus protocols, where a new block can only be created and appended to the chain with the approval of the network majority (Kumar et al., 2021).

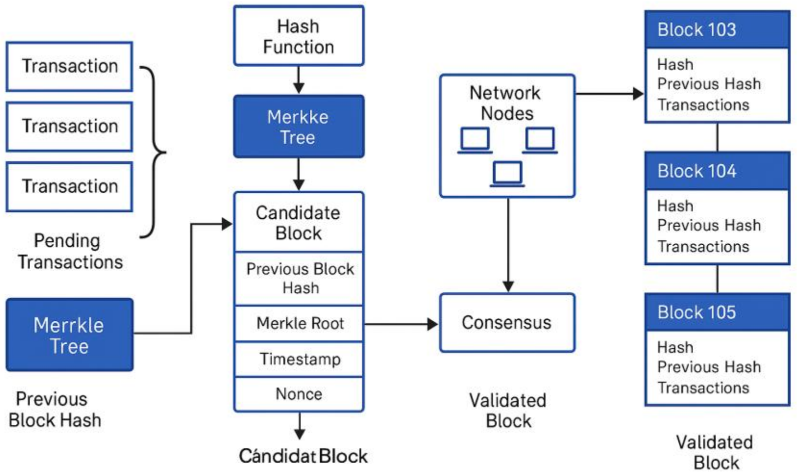


Figure-4: Blockchain system components

One of the most significant features of blockchain is its immutability and transparency (Chen et al., 2023). Every block added to the system is accessible and auditable by all authorized network participants, ensuring a high level of protection against fraud or unauthorized interference for both transactions and associated metadata. Additionally, since blockchain lacks a single point of control, it exhibits resilience against attacks targeting centralized authorities and single points of failure. Particularly in private and permissioned blockchain systems, only authorized nodes are entitled to perform transactions and append data to the ledger. This structure enhances data privacy while optimizing the system’s scalability and transaction speed.

The operational principle of blockchain technology is based on the effective use of consensus protocols during the process of verifying transactions and appending them to the chain. Consensus mechanisms ensure that all authorized nodes in the network reach a common decision on a given set of transactions. While traditional blockchain systems often rely on consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS), these can result in high computational and energy costs (Yu et al., 2024). To overcome these challenges, this thesis adopts lightweight and resource-efficient alternative consensus approaches, such as Lightweight Byzantine Fault Tolerance (LBFT). Such mechanisms provide suitable solutions for resource-constrained environments like UAV networks, where computational power and battery capacity are limited.

Consensus protocols employed for writing transactions to the ledger consist of algorithms that enable authorized nodes in the network to agree on the validity of a specific set of transactions. Mechanisms like PoW, common in classical systems, are unsuitable for resource-constrained environments (e.g., UAV networks) due to their high processing and energy demands. Therefore, this thesis employs a consensus structure based on Lightweight Byzantine Fault Tolerance (LBFT), which offers rapid agreement with minimal processing load and communication overhead while ensuring resilience against Byzantine faults, such as malicious nodes and attempts at disseminating false data. The consensus process is designed as a Two-Tier Consensus

(TTC) structure: (1) Trust Evaluation Tier (Data Consensus Phase): This phase monitors the behavior of neighboring nodes through sub-protocols such as the Proximal Node Discovery and Monitoring Component (PDMC), the Localized Trust Coordination Component (LTCC), and the Hierarchical Trust Coordination Component (HTCC). Trust Assessment Transaction (TAT) records are generated, and consensus on trust scores is achieved via the LBFT algorithm. (2) Network Coordination Tier (Decision Consensus Phase): Before TATs are written to the blockchain, they are validated through smart contracts embedded in the Genesis Block (interpreted in this context as consensus code), and new blocks containing verified data are created and appended to the chain.

The blockchain architecture employed in this thesis is designed as a private and permissioned blockchain that functions as a ledger readable and writable solely by UAVs and ground stations with proven trustworthiness. The blocks contain Trust Assessment Transaction (TAT) records, which include UAV behavioural metrics, trust scores, and the outcomes of identity authentication processes. This ensures that the trustworthiness history of nodes is immutably recorded. The ledger is accessible and writable only by UAVs and ground stations validated through the SABEC protocol. Each UAV node is identified through a unique cryptographic identity (public-private key pair + Unique Identifier (UID)). All transaction and trust score records are added to the ledger in the form of TATs. Since only aggregated consensus outcomes and trust scores are stored on the blockchain in SABEC, data storage overhead is significantly reduced compared to classical blockchain systems, as shown in Figure 5. This architecture enhances system resilience against threats such as identity spoofing, data manipulation, and unauthorized access. The transparency and traceability afforded by blockchain contribute to establishing trust, especially within heterogeneous UAV fleets and decentralized network topologies.

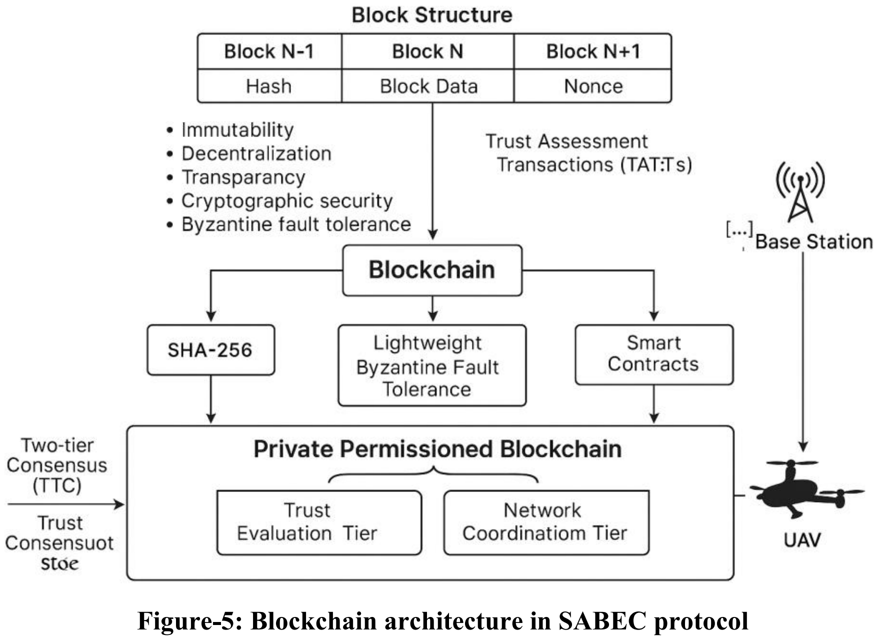


Figure-5: Blockchain architecture in SABEC protocol

The consensus mechanism underlying the blockchain architecture is integrated with the Secure and Adaptive Blockchain-Enabled Coordination (SABEC) protocol developed within this thesis, as shown in Figure 5. SABEC incorporates a Two-Tier Consensus Mechanism (TTC) to manage rapidly changing network structures and trust relationships in real time, given the high mobility and dynamic topology of UAV networks. In the first stage, the Trust Evaluation Tier, UAVs selected as local leaders observe the behaviour of nodes within their clusters and assess the generated TAT data. Consensus is rapidly and efficiently achieved through LBFT algorithms. The second stage, the Network Coordination Tier, ensures the final validation of trust scores and decisions and their recording on the blockchain. Decision blocks are created to contain only verified and agreed-upon data, thereby safeguarding the blockchain's integrity and security.

The blockchain architecture proposed in the thesis is designed to address the storage and scalability challenges faced by conventional blockchains. Only summary results of consensus processes and aggregated trust scores are added to the blocks, preventing unnecessary data accumulation and excessive chain growth. While the information stored on the blockchain is accessible to all authorized nodes, writing permissions are restricted to trusted and authorized nodes. Thus, a decentralized trust infrastructure is established without reliance on a central authority, eliminating the risk of single points of failure and centralized attack scenarios. Together with the SABEC protocol, the blockchain structure is supported by dynamic clustering and leader UAV selection mechanisms. Based on the Fuzzy C-Means Clustering algorithm, leader UAVs are periodically selected and collect trust data from nodes within their clusters to feed into the consensus process. This ensures that both data coordination and consensus processes are conducted in a scalable, flexible, and attack-resilient manner. The data collected by leader UAVs is appended to the blockchain via ground stations, making it auditable for all network participants. This blockchain-based trust management not only records real-time trust assessments but also logs historical behavioural metrics, enabling monitoring of nodes' trust profiles over time. Such an architecture offers a robust solution for enhancing network reliability, resilience, and continuity, particularly in heterogeneous UAV fleets and complex mission scenarios.
One of the system's key features is that identity authentication and data storage operations are performed not on the UAVs themselves but on ground stations with greater processing and storage capacities. This approach minimizes the processing load and energy consumption of UAVs, enabling only minimal data transmission and thereby extending flight times and operational efficiency. The blockchain architecture of SABEC, integrated with lightweight consensus protocols, provides a low-latency, fast, and secure identity management and data integrity infrastructure suitable for real-time operations.

Among the primary contributions of blockchain technology to this thesis are decentralized identity management, preservation of data integrity, transaction transparency, resistance to unauthorized interventions, and scalable trust management. Additionally, by storing only consensus-approved transaction summaries and aggregated trust scores on the blockchain ledger, storage overhead is reduced, and network scalability is enhanced. The blockchain infrastructure supports adaptive trust management with continuously updated trust scores and behavioural metrics, offering a flexible and sustainable solution for dynamic topologies and rapidly changing mission scenarios.

In conclusion, within the scope of this thesis, blockchain technology is positioned not merely as a data recording tool but as a multi-layered security infrastructure that enables decentralized identity management, monitoring of trust scores, and preservation of network integrity. The SABEC protocol developed herein integrates blockchain architecture with dynamic clustering, leader selection mechanisms, and a two-tier consensus model, delivering an innovative and holistic solution tailored to the unique challenges of UAV networks.

4.5 Security Verification and Formal Analysis

Ensuring the security and correctness of the proposed authentication protocol is paramount. To this end, ProVerif (Küsters et al., 2009), a widely recognized security verification tool, is employed for formal analysis (Cui et al., 2024; Sardar et al., 2024). ProVerif utilizes the Dolev-Yao attack (Cook et al., 2020) model to rigorously assess the protocol's ability to maintain secrecy and authentication properties. The tool is capable of handling various cryptographic primitives, including encryption, decryption, digital signatures, hash functions, and key agreements using Diffie-Hellman (Kobeissi et al., 2017). The formal analysis involves modelling the authentication protocol within ProVerif and verifying its resilience against potential security threats (Zhang et al., 2020). This process confirms that the protocol successfully achieves mutual authentication between UAVs and BSs, ensures the secrecy of session keys, and prevents unauthorized access and data breaches. The rigorous security verification underscores the robustness and reliability of the proposed IDMS in safeguarding UAV network communications.

4.6 Simulation and Experimental Setup

To evaluate the performance and efficacy of the proposed IDMS, a comprehensive simulation environment is established. The simulation setup includes deploying 1000 UAV nodes across various regions, each assigned a unique temporary ID and key pair synchronized with its corresponding BS node. The simulation employs Python 3 for developing simulation scripts and ActiveMQ as the messaging broker to handle communication between UAVs and BSs. The experiments are conducted on a Windows 11 Home 64-bit system equipped with a 13th Gen Intel Core i7-13650Hx 2.6GHz processor and 16GB RAM to ensure sufficient computational resources. A total of one hundred mission scenarios are designed, each with different random numbers to introduce variability and realism into the simulation. This approach ensures that the authentication protocol is tested under diverse conditions and operational dynamics. Key performance indicators, including data transmission delay, packet delivery rate, and network overhead, are meticulously measured to assess the protocol's efficiency, scalability, and ability to maintain secure communications under high-load conditions. The simulation results demonstrate that the proposed IDMS effectively mitigates the impact of Byzantine devices and significantly improves packet transmission speeds compared to existing studies, highlighting the protocol's efficiency and suitability for large-scale UAV deployments.

The primary objective of this study was to design, implement, and evaluate a secure and efficient identity management system (IDMS) tailored for UAV networks characterized by high mobility and resource constraints. In the simulation phase, Raspberry Pi 4 Model B was selected as the emulation platform for UAV onboard computing. This choice was motivated by its embedded system nature, ARM architecture, compact form factor, and its extensive adoption in academic research as a prototyping device for UAV-related applications. Although Raspberry Pi 4 offers greater computational resources (1.5 GHz quad-core ARM CPU, 4 GB RAM) than typical flight controllers employed in commercial UAVs, it provides a practical and accessible platform to validate the functional correctness, communication flow, and performance of the proposed identity management protocols under controlled conditions.

In this study, the Windows 11 Home 64-bit system with a 13th Gen Intel Core i7 2.6 GHz processor and 16 GB RAM was dedicated to simulating the Base Station (BS) environment, which is responsible for managing authentication processes and consensus operations. This distinction between UAV and BS simulation environments ensured that the performance evaluation accounted for the hierarchical structure of the UAV network as designed.

It is acknowledged that the computational power of the Raspberry Pi 4 may not fully reflect the stringent limitations of actual UAV flight hardware, where processors typically operate at 200–800 MHz with substantially less RAM and more stringent energy constraints. However, the primary aim at this stage of the research was to validate the protocol’s logical design, its operational integrity, and its ability to deliver accurate and efficient identity verification and consensus outcomes. The simulation was intended as a proof-of-concept prototype, demonstrating the viability of the architecture in an embedded system context, rather than providing a worst-case performance benchmark.

Furthermore, the selection of Raspberry Pi 4 was intended to balance accessibility and embedded system representativeness, enabling iterative development and validation of the proposed protocols. The protocols were deliberately designed to be lightweight, ensuring they could later be deployed on more resource-constrained platforms. Future work will focus on testing the developed IDMS and SABEC protocols on actual low-power flight computers and microcontroller-based UAV platforms, including rigorous energy and timing optimizations tailored to the operational realities of commercial UAV hardware.

It is *important to note that* the use of Raspberry Pi as a prototyping and simulation platform for UAV systems has been well-documented in the literature review chapter, with many studies leveraging its capabilities for initial design validation prior to deployment on production-grade UAV hardware. The simulation framework developed in this thesis thus represents a practical and academically consistent approach for protocol validation in UAV network research.

4.7 Summary

In summary, this chapter has delineated the comprehensive methodological framework employed to develop and evaluate the proposed Identity Management System (IDMS) for Unmanned Aerial Vehicle (UAV) networks. The network model design established a hierarchical architecture comprising UAVs, base stations, and cloud infrastructure, facilitating secure and authenticated communications through a mutually authenticated key-agreement scheme. The development of secure authentication protocols emphasized the creation of a robust and efficient mechanism to establish dynamic session keys, leveraging cryptographic techniques to ensure resilience against sophisticated cyber threats. The system architecture integrated three distinct applications (Drone Service Application, Base Station Service Application, and Web Application) to enable secure data transmission, processing, and real-time monitoring. The incorporation of blockchain technology introduced a decentralized decision-making mechanism that enhances network security and integrity by preventing the inclusion of untrusted nodes and enabling adaptive network restructuring. Security verification through ProVerif provided a formal analysis of the protocol's ability to maintain secrecy and authentication properties, confirming the system's robustness against potential attacks. Lastly, the simulation and experimental setup validated the efficacy and performance of the proposed IDMS, demonstrating its capability to maintain secure and efficient communications in large-scale UAV deployments. Collectively, these methodological components establish a solid foundation for the proposed IDMS, addressing the unique challenges of UAV networks and paving the way for secure and reliable UAV operations.

The methodological framework presented in this chapter provides a structured and comprehensive approach to developing and evaluating a secure and efficient Identity Management System for UAV networks. By integrating advanced authentication protocols, blockchain technology, and rigorous security verification tools, the proposed system addresses the unique challenges posed by UAV deployments. The simulation experiments validate the system's performance, demonstrating its capability to maintain secure and reliable communications even in the presence of malicious entities. The subsequent chapters will present detailed results of these evaluations and discuss their implications for the future development of UAV network security.

Chapter 5

Design and Development of Identity Management System

Building upon the comprehensive analysis of UAV network requirements and the identification of critical security challenges in Chapter 3, this chapter delineates the design and development of the proposed Identity Management System (IDMS) tailored specifically for UAV networks. The IDMS leverages blockchain technology to enhance security, scalability, and resilience against sophisticated cyber threats. This chapter is systematically structured into three primary sections: System Architecture and Components, Identity Verification Mechanisms, and Privacy-Preserving Techniques, followed by a summary that encapsulates the key design considerations and innovations. Each section delves into the intricate details of the IDMS, ensuring a robust and secure framework that addresses the unique demands of UAV ecosystems.

The architecture and components of the proposed IDMS, in Figure 6, is meticulously engineered to address the multifaceted security and operational requirements inherent to UAV networks. At its core, the architecture integrates decentralized blockchain technology with UAV communication infrastructures that implement non-traditional dynamic identity verification and management protocols. This integration serves to minimize the susceptibility of the system to cyber-attacks and reduces the vulnerability of individual devices under assault, thereby significantly enhancing the overall resilience of the system. By distributing trust across a decentralized framework and eliminating single points of failure, the IDMS ensures robust protection against a diverse range of cyber threats, fostering secure and reliable UAV operations. The IDMS architecture comprises four interdependent layers: the UAV Layer, the Base Station (BS) Layer, the Blockchain Layer, and the Application Layer. Each layer is designed with specific functionalities that collectively ensure secure identity management and seamless communication within the UAV network.

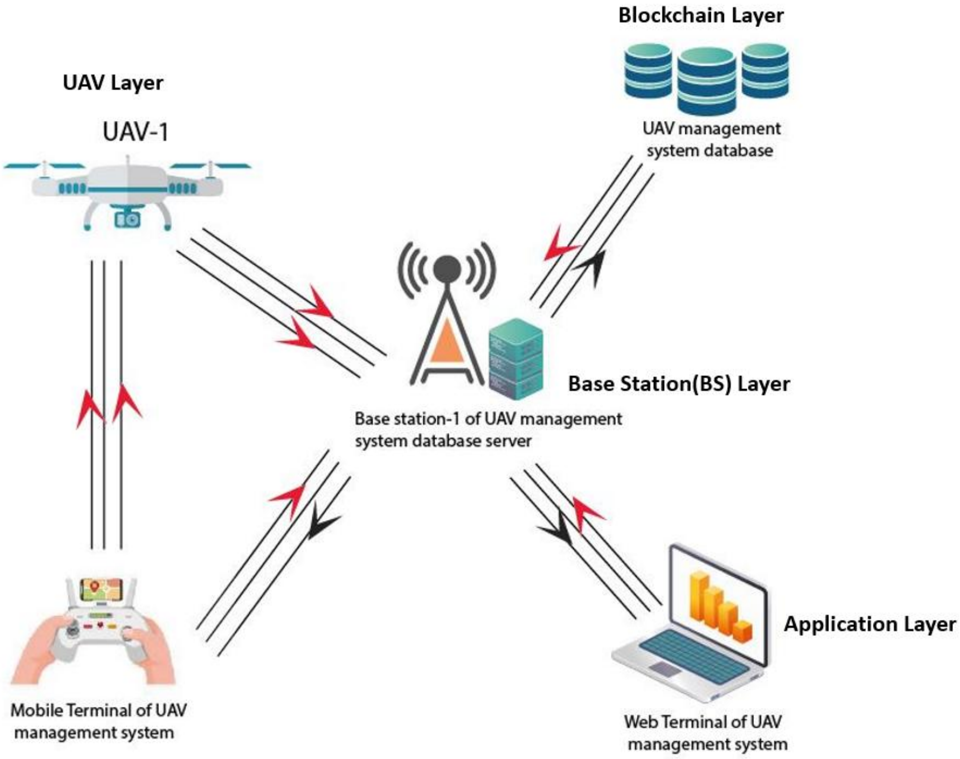

Blockchain Layer
UAV management system database
UAV Layer
UAV-1
Base Station(BS) Layer
Base station-1 of UAV management system database server
Application Layer
Mobile Terminal of UAV management system
Web Terminal of UAV management system

Figure 6: The network architecture and components of the proposed IDMS

UAV Layer: This foundational layer consists of individual UAV units equipped with embedded security modules. Each UAV is furnished with a unique cryptographic identity, comprising a pair of public and private keys that facilitate secure communication and authentication. The UAVs are responsible for initiating authentication requests, managing session keys, and ensuring encrypted data transmission. Additionally, this layer incorporates lightweight cryptographic protocols optimized for the resource-constrained nature of UAVs, ensuring minimal computational overhead without compromising security.

Base Station (BS) Layer: Serving as the intermediary between UAVs and the blockchain network, the BS Layer comprises ground-based stations that manage the registration, authentication, and authorization of UAVs. These stations are equipped with robust computational resources to handle complex cryptographic operations and blockchain interactions. The BS Layer is responsible for validating UAV credentials, distributing session keys, and facilitating the communication of authentication events to the blockchain network. Moreover, this layer employs redundancy and failover mechanisms to ensure continuous operation even in the event of individual BS failures.

Blockchain Layer: The Blockchain Layer forms the backbone of the IDMS, providing a decentralized and immutable ledger for recording authentication transactions and managing UAV identities. This layer utilizes a permissioned blockchain framework to maintain control over network participants and ensure that only authorized entities can participate in the consensus process. Smart contracts are deployed within the blockchain to automate authentication protocols, enforce security policies, and facilitate secure data sharing among UAVs and BSs. The integration of consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) and difficulty factor ensures that the blockchain maintains integrity and trustworthiness even in the presence of malicious actors.

Application Layer: The Application Layer stands as the sole application component independent of the hierarchical structure within the IDMS. Developed specifically for testing purposes, this layer serves as the user interface that visualizes and manages data received from various UAV applications. It is designed to interface seamlessly with the underlying IDMS infrastructure, providing real-time data display, monitoring capabilities, and user interaction functionalities. The Application Layer is pivotal for evaluating the performance and effectiveness of the IDMS in practical scenarios, enabling researchers and operators to interact with the system, oversee authentication processes, and analyse security events through an intuitive and responsive interface.

The IDMS architecture encompasses several critical components that interact seamlessly to provide a secure and efficient identity management framework (Sadique et al., 2020). These include the Authentication, which orchestrates the mutual authentication processes between UAVs and BSs; the Cryptographic Module, responsible for key generation, storage, and management; the Data Repository, which securely stores UAV credentials and authentication logs; and the Monitoring and Analytics System, which continuously oversees network activities to detect and respond to anomalies and potential security breaches (Hadi et al., 2024). Each component is designed with scalability and interoperability in mind, ensuring that the IDMS can adapt to varying network sizes and integrate with diverse UAV models and communication protocols.

The IDMS is designed to integrate seamlessly with existing UAV infrastructure, minimizing disruptions and ensuring compatibility with various UAV models and communication protocols. This is achieved through the use of standardized interfaces and protocols that facilitate interoperability between UAVs, BSs, and the blockchain network. Additionally, the modular architecture allows for incremental deployment and scalability, accommodating the growing demands of UAV network expansions. By leveraging existing communication frameworks and augmenting them with blockchain-based identity verification, the IDMS ensures that UAV operations remain secure without necessitating extensive overhauls of existing systems.

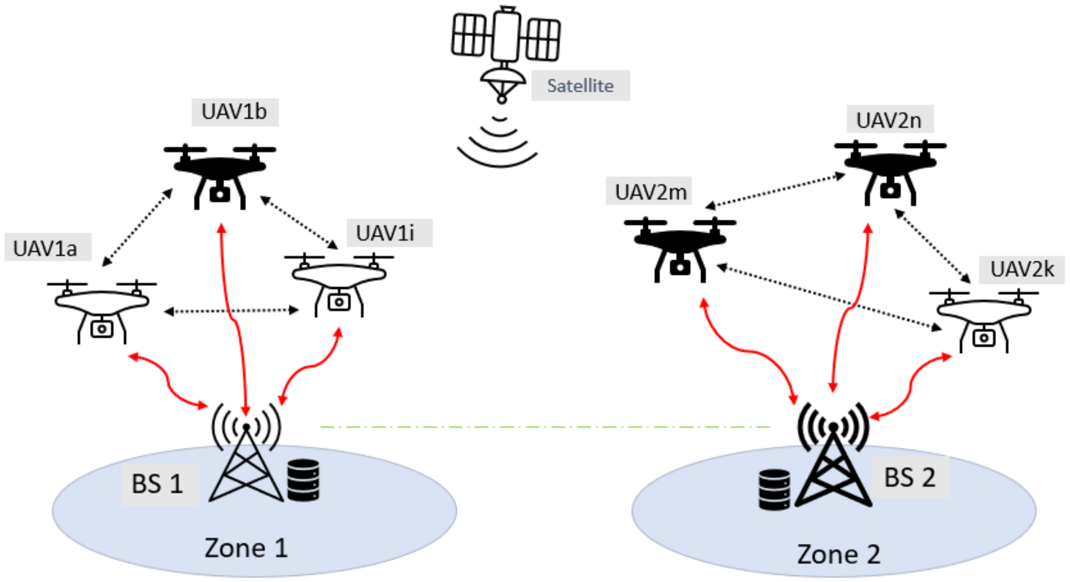


Figure 7: The design of the proposed Secure Authentication Protocol

Chapter 6

A Secure and Dynamic Authentication Protocol for UAVs Network

In the rapidly evolving domain of Unmanned Aerial Vehicle (UAV) networks, ensuring secure and reliable communication between distributed UAV-based applications and ground nodes is paramount (Xu et al., 2024). As UAVs become increasingly integral to various applications (from surveillance and delivery to environmental monitoring) the necessity for robust authentication mechanisms that ensure secure and reliable interactions within these networks intensifies (Qian et al., 2024). The Secure Authentication Protocol presented in this chapter is meticulously designed to address these critical security concerns. It facilitates mutual authentication between UAVs and Base Stations (BS), shown in Figure 7, establishes dynamic symmetric session keys, and preserves the privacy of drone devices. By leveraging advanced cryptographic techniques and integrating blockchain technology, this protocol not only fortifies the network against a myriad of cyber threats but also ensures scalability and efficiency in resource-constrained environments typical of UAV operations. The subsequent sections provide a comprehensive overview of the authentication scheme, analyse its security features, detail its design and implementation, evaluate its performance, and summarize its contributions to enhancing UAV network security.

6.1 Overview of the Authentication Scheme

The proposed Secure Authentication Protocol within the Identity Management System (IDMS) framework addresses this critical need by facilitating robust mutual authentication and the secure establishment of symmetric secret session keys. As depicted in Figure 9, the protocol enables UAVs to authenticate themselves to Base Stations (BS) and vice versa, thereby establishing a trusted communication channel essential for mission-critical operations (Dogan et al., 2023).

TABLE I
SYMBOLS AND DESCRIPTIONS

Symbols	**Descriptions**
TID_i	Temp Identity Device
$EC_{(PR,PU)}$	Elliptic Curve Public and Private Key
E_{SK}	AES Secret Key Encryption
E_{DSK}	Dynamic Secret Key Encryption
R_i	Random Nonce Value
$\alpha,\ \upsilon,\ \phi$	Random numbers
$A,\ B$	Parameters
T_i, M_i	Timestamp and Message Package
PRF	Pseudo-random function
$\|$	Concatenation Operation
$H()$, $\oplus$	Hash and XOR Function

The design and implementation of the Secure Authentication Protocol are meticulously aligned with the architectural framework delineated in Chapter 5. This section elucidates the structural components, operational workflows, and underlying cryptographic mechanisms that collectively ensure secure and efficient authentication within UAV networks.

➢ Structural Components:

- *Key Management Module:* Each UAV and BS device is equipped with a Key Management Module responsible for generating, storing, and managing cryptographic keys. This module ensures the secure handling of key pairs and facilitates the generation of symmetric session keys during the authentication process. Robust key storage mechanisms are employed to protect private keys against unauthorized access and tampering (Nyangaresi et al., 2021).

- *Nonce Generator:* To enhance the protocol's resistance to replay attacks, a Nonce Generator is integrated into each device. This component generates random nonce values utilized in each authentication attempt, ensuring the uniqueness and freshness of authentication messages. The nonces are generated using secure random number generators to prevent predictability (Yu et al., 2024).

- *Timestamp Synchronization Mechanism:* Given the protocol's reliance on current timestamps, a Timestamp Synchronization Mechanism is employed to ensure that all devices within the network maintain synchronized clocks. This synchronization is critical for the effective utilization of timestamps in preventing replay attacks. Protocols such as Network Time Protocol (NTP) or Precision Time Protocol (PTP) are utilized to achieve the requisite synchronization precision (Sisinni et al., 2022).

- *Authentication System:* The core component responsible for orchestrating the authentication process. This engine manages the exchange of authentication messages, verifies the integrity and authenticity of received messages, and oversees the establishment of symmetric session keys. It leverages cryptographic verification processes to validate the signatures and authenticity of incoming messages (Raj et al., 2023).

- *Blockchain Interface:* Leveraging the decentralized blockchain layer, this interface facilitates the recording and retrieval of authentication transactions. Smart contracts deployed within the blockchain automate the verification process, ensuring tamper-proof and transparent authentication records. The blockchain interface ensures seamless integration between the authentication protocol and the blockchain network, enabling real-time logging and verification of authentication events (Tan et al., 2022).
- *Asymmetric Cryptography:* Utilized for initial authentication and secure key exchange. Each device possesses a unique key pair (public and private keys), enabling secure verification of identities without exposing private keys. Digital signatures are employed to authenticate messages, ensuring that they originate from legitimate devices (Ouadah et al., 2024).
- *Symmetric Cryptography:* Employed for encrypting subsequent communications using the established symmetric session key. This ensures data confidentiality and integrity during data transmission between UAVs and BSs. Advanced symmetric algorithms, such as AES (Advanced Encryption Standard), are utilized to provide robust encryption with minimal computational overhead (Cecchinato et al., 2023).
- *Hash Functions:* Incorporated to generate message digests, ensuring the integrity of authentication messages and preventing tampering. Secure hash algorithms, such as SHA-256, are employed to produce fixed-size digests that are computationally infeasible to reverse-engineer or collide (Khor et al., 2023).
- *Key Derivation Functions (KDFs):* Utilized to derive symmetric session keys from shared secrets (e.g., nonces and timestamps), ensuring that session keys are both unique and ephemeral. KDFs enhance security by ensuring that even if one part of the key exchange is compromised, the derived session keys remain secure (Li et al., 2022).

At the core of this authentication scheme lies the dynamic generation of a symmetric secret session key, often referred to as a token, during the authentication process. This session key is transient and uniquely generated for each authentication instance, ensuring that communication between the UAV and the BS remains confidential and secure throughout the UAV's active presence within the network. The utilization of this session key not only guarantees mutual authentication of both entities but also underpins the encryption of subsequent data exchanges, thereby safeguarding against eavesdropping and unauthorized access.

The protocol employs a combination of dynamic secret keys, current timestamps, random nonces, and renewable tokens to enhance its resilience against sophisticated cyber-attacks. Each entity within the network, whether a UAV or a BS, is provisioned with a unique key pair comprising a public and private key, alongside a temporary identifier (temp ID). This architecture ensures that even if one UAV is compromised, the security of other network participants remains intact. A fundamental assumption underpinning this protocol is the synchronization of device clocks, which is crucial for the effective utilization of timestamps and nonces in preventing replay attacks and ensuring the freshness of authentication messages (Dogan et al., 2023).

The authentication process is systematically divided into four distinct phases: the offline phase, the device registration phase, the authentication phase, and the data sending phase. This phased approach not only streamlines the authentication workflow but also enhances the protocol's scalability and adaptability to diverse operational scenarios. The offline phase involves the initial personalization of devices, the registration phase facilitates the enrolment of UAVs into the network, and the authentication phase governs the dynamic interactions required during active operations. In the data sending phase of the proposed protocol, a block-based data structure is explicitly incorporated to provide verifiable integrity, end-to-end security, and protection against data tampering in UAV communications. After the successful registration and authentication phases, the UAV device transmits operational data to the base station (BS) using the Token value obtained during authentication, ensuring that only authorized devices can participate in data exchange. The core of this phase lies in converting the transmitted data into a block format with cryptographic linking, forming a simplified blockchain-like structure. Upon receipt, the BS verifies the integrity of the block structure and stores it securely on its server. The critical data portions can subsequently be relayed to the server for further mission processing or archival, but the integrity verification remains anchored at the BS level. Unlike traditional blockchain implementations relying on global consensus, this approach uses cryptographic chaining of data blocks to provide tamper-evident records of UAV communications without incurring the overhead of distributed consensus mechanisms. The use of the block structure ensures that any modification or injection attempt by an adversary would break the hash linkage, enabling immediate detection. Collectively, these phases ensure that the protocol achieves its primary objectives of mutual authentication and privacy preservation for UAV devices within the network (Dogan et al., 2023).

The proposed protocol aims to achieve mutual authentication of UAV and BS devices, and drone device’s privacy preserving. We assume that the back-end server is a trusted entity and the communication channel between a node server and UAV devices is secure. In the offline phase is a one-time computation that personalizes the devices before their deployment into the network. UAV devices will be registered at the BS and receive security credentials and other parameters in the registration phase. The authentication phase is a dynamic process, where drone device and BS interact with each other as and when required. The notations used in the proposed scheme are shown in Table 1 and 2 (Dogan et al., 2023).

6.1.1 Offline Phase

Prior to deployment, each UAV device undergoes a one-time computation process that personalizes the device's cryptographic credentials and parameters, shown in Figure 8. This process involves generating a unique key pair and temporary identifier, which are securely embedded into the device. Consider a suitable elliptic curve group $\boldsymbol{E(F_q)}$ over a finite field $\boldsymbol{F_q}$, where $\boldsymbol{q}$ is a prime number, sufficiently large enough to accommodate cryptographic keys. The order of the group is $\boldsymbol{q}$ a prime and $\boldsymbol{P}$ be the generator. The parameters $\boldsymbol{E(F_q)}$, $\boldsymbol{q}$ and $\boldsymbol{P}$ are made public, where $\boldsymbol{P \in E(F_q)}$ is a generator of $\boldsymbol{E(F_q)}$. The sender first chooses a random value $\boldsymbol{s \in F^*q}$ and computes $\boldsymbol{PU_s = PR_s . P}$. *Setup UAV:* For $\boldsymbol{i = 1,2,...,m}$, the base station personalizes $\boldsymbol{UAV_i}$ with the private key $\boldsymbol{x_i \in F^*q}$. It then computes UAV's public key $\boldsymbol{PU_{UAV_i} = x_i . P}$ and stores it in the BS' database. *Setup Base station:* For $\boldsymbol{j = 1,2,...,n}$, the BS device personalizes $\boldsymbol{BS_j}$ with the private key $\boldsymbol{y_j \in F^*q}$. It then computes BS's public key $\boldsymbol{PU_{BS_j} = y_j . P}$ and stores it in the BS' database (Dogan et al., 2023).

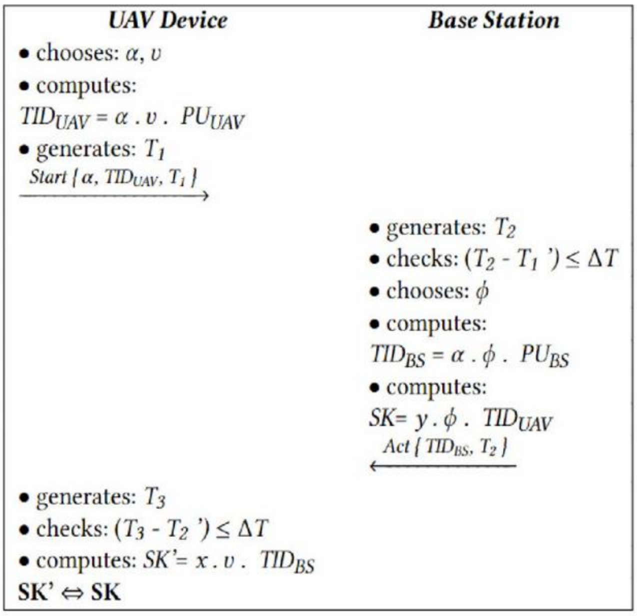

UAV Device
Base Station
• chooses: α, υ
• computes:
$TID_{UAV} = \alpha . \upsilon . PU_{UAV}$
• generates: T_1
Start { α, TID_{UAV}, T_1 }
• generates: T_2
• checks: $(T_2 - T_1') \leq \Delta T$
• chooses: ϕ
• computes:
$TID_{BS} = \alpha . \phi . PU_{BS}$
• computes:
$SK = y . \phi . TID_{UAV}$
Act { TID_{BS}, T_2 }
• generates: T_3
• checks: $(T_3 - T_2') \leq \Delta T$
• computes: $SK' = x . \upsilon . TID_{BS}$
SK' ⇔ SK

Figure 8: Registration Phase

6.1.2 Registration Phase

In the registration phase, the base station is responsible for registering each drone device deployed in a specific target zone. Upon deployment, UAV devices register with their respective BSs. During this phase, UAVs receive security credentials, including session key generation parameters and access permissions. The BS validates the UAV's credentials by cross-referencing the blockchain's public key repository, ensuring the UAV's legitimacy (Dogan et al., 2023). UAV devices will be registered at the base station and received security credentials, detailed in Figure 8. The registration phase is processed in three steps:

- *Step-1:* In the first step, the UAV device chooses two random number to generate the *temp ID* for initiate the enrolment phase, $\boldsymbol{TID_{UAV}}$. After that, it generates the current timestamp and creates the first package **(**α, $\boldsymbol{TID_{UAV}}$, $\boldsymbol{T_1}$**)** .
- *Step-2:* The base station creates a current timestamp, $\boldsymbol{T_2}$, to receive the UAV device's data, and checks it with the timestamp, $\boldsymbol{T_1}$', in the incoming packet. It checks according to the time limit defined in the properties file. If it is within the defined rules, the package is received. Otherwise, it will be ignored. Thus, the BS generates the necessary information to pass the UAV device to the authentication stage. The BS computes its ***TID*** information with the $\boldsymbol{\varphi}$ random nonce value. Then, the BS generates the secret key, ***SK*=*y*.$\boldsymbol{\varphi}$. $\boldsymbol{TID_{UAV}}$** and send it with the timestamp to the UAV device.

Proof. ***SK' ⇔ SK :***

$$
\begin{aligned}
\boldsymbol{SK} &= y \,.\, \varphi \,.\, TID_{UAV} \\
&= y\, \varphi\, \alpha \,.\, \upsilon \,.\, PU_{UAV} \\
&= y\, \varphi\, \alpha \,.\, \upsilon\, x\, P \\
&= x\, \upsilon\, \alpha\, \varphi\, y\, P \\
&= x\, \upsilon\, \alpha\, \varphi\, PU_{BS} \\
&= x\, \upsilon\, TID_{BS} \\
&= \boldsymbol{SK'}
\end{aligned}
$$

6.1.3 Authentication and Key Establishment Phase

The itemized figure of the authentication phase is depicted in Figure 9. This phase executes in three steps in establishing a session key between UAVs and Base Stations (Dogan et al., 2023). (*Authentication Request:* When a UAV initiates communication, it sends an authentication request to the BS, including its temporary identifier, current timestamp, and a newly generated nonce. This request serves as the initial handshake for establishing a secure communication channel.) The UAV device starts the communication, and it generates the session key dynamically (***DSK***) by generating the ***A*** and ***B*** parameters. The ***DSK*** is also computed using $\boldsymbol{\alpha}$, $\boldsymbol{\upsilon}$ credentials. It then encrypts the first message with the secret key (***SK'***) obtained during registration, $\boldsymbol{M_1}$ = $\boldsymbol{E_{SK'}}$ ***[A*** || ***B*** || $\boldsymbol{T_1}$ ***]***. It then generates *Start message {*$\boldsymbol{M_1}$*,* $\boldsymbol{T_1}$*}*. The start message is being sent to the base station. (*Verification and Response:* The BS verifies the UAV's credentials by checking the blockchain records, validates the timestamp and nonce, and responds with its own temporary identifier, timestamp, and nonce. This bidirectional exchange ensures that both entities can trust each other's identities and the freshness of the authentication attempt.) Upon receiving the authentication message from UAV device, the BS verifies the timestamp validity, i.e., ***$(T_2$ - $T_1) \leq \Delta T$*** or not, where ***T_2*** is the current timestamp of the node and ***ΔT*** is the maximum allowed transmission delay. If the value does not match, the BS terminates the connection. Otherwise, it calculates the ***DSK*** and generates *Ack message* ***$\{M_2$, $T_2\}$*** and transmits it to the UAV device. Here, ***M_2*** contains ***$\{H(\alpha)$, $H(TID_{BS})$, T_2, Token}***. (*Session Key Establishment:* Both UAV and BS generate a symmetric session key using a predefined key derivation function that incorporates the exchanged nonces and timestamps. This session key is then used to encrypt all subsequent communications, ensuring data confidentiality and integrity). Upon receiving *Ack message*, the UAV device, first checks the timestamp, decrypts ***M_2*** using ***DSK***, and verifies the identities to ensure whether the BS is a legitimate entity. Finally, it stores the Token that will be used for securing the further communications (Dogan et al., 2023).

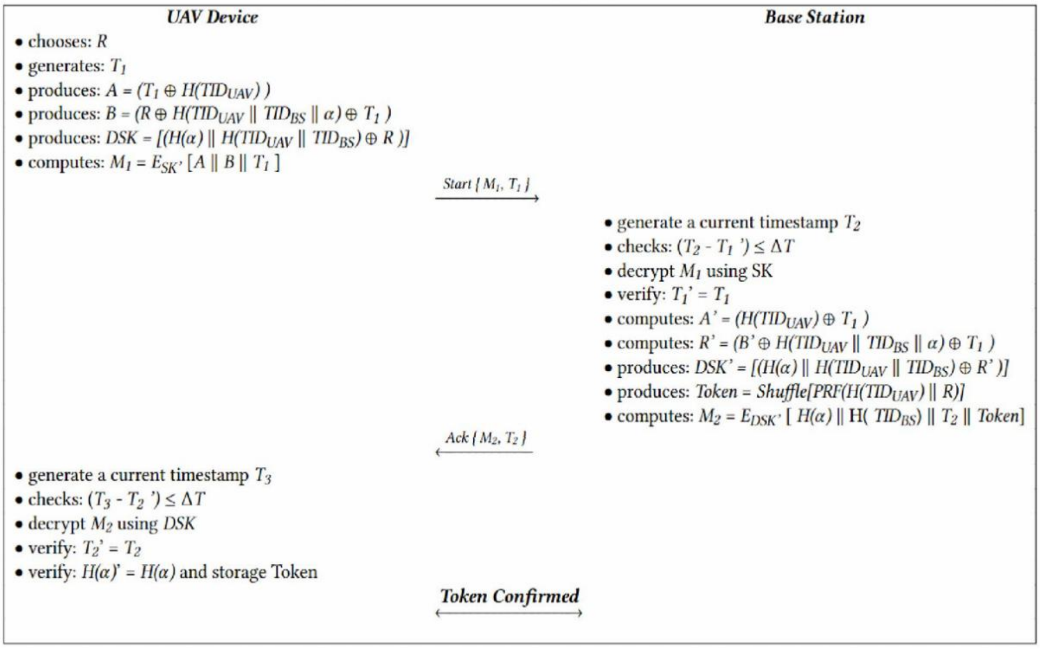

UAV Device
Base Station
• chooses: R
• generates: T_1
• produces: $A = (T_1 \oplus H(TID_{UAV}))$
• produces: $B = (R \oplus H(TID_{UAV} \| TID_{BS} \| \alpha) \oplus T_1)$
• produces: $DSK = [(H(\alpha) \| H(TID_{UAV} \| TID_{BS}) \oplus R)]$
• computes: $M_1 = E_{SK'} [A \| B \| T_1]$
Start { M_1, T_1 }
• generate a current timestamp T_2
• checks: $(T_2 - T_1') \leq \Delta T$
• decrypt M_1 using SK
• verify: $T_1' = T_1$
• computes: $A' = (H(TID_{UAV}) \oplus T_1)$
• computes: $R' = (B' \oplus H(TID_{UAV} \| TID_{BS} \| \alpha) \oplus T_1)$
• produces: $DSK' = [(H(\alpha) \| H(TID_{UAV} \| TID_{BS}) \oplus R')]$
• produces: $Token = Shuffle[PRF(H(TID_{UAV}) \| R)]$
• computes: $M_2 = E_{DSK'} [H(\alpha) \| H(TID_{BS}) \| T_2 \| Token]$
Ack { M_2, T_2 }
• generate a current timestamp T_3
• checks: $(T_3 - T_2') \leq \Delta T$
• decrypt M_2 using DSK
• verify: $T_2' = T_2$
• verify: $H(\alpha)' = H(\alpha)$ and storage Token
Token Confirmed

Figure 9: Authentication Stage

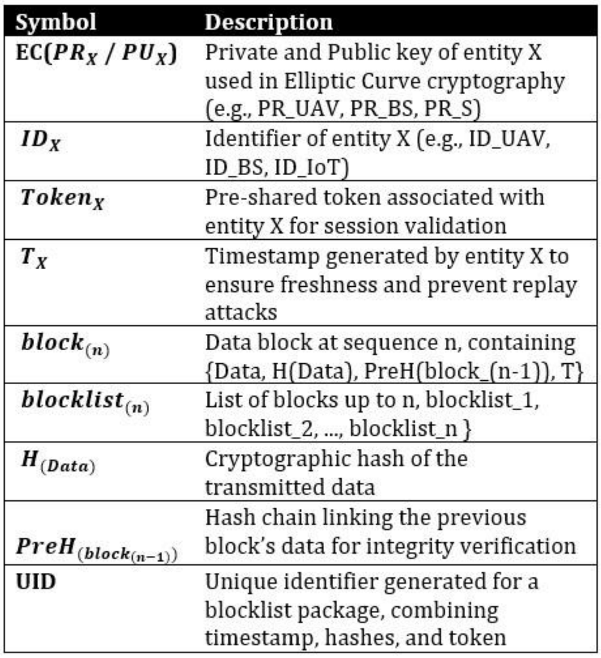
6.1.4 Data Sending Phase

This part demonstrates in Figure 10 that the proposed scheme is designed to prevent all possible security vulnerabilities in the network and considers safe data transmission, so it provides a trustworthy environment (Dogan et al., 2023). Ensuring data security to avoid security weaknesses in a UAV environment provides end to-end security to the network. To accomplish this goal, a block structure was used in the proposed scheme to ensure data security. After the registration and authentication stages, the UAV device will communicate with other entities in the network using the Token value received from the BS. In this phase, the EC asymmetric encryption algorithm is used instead of the AES symmetric encryption algorithm because of the fastest computation time and more safety. The data sending f low occurs in three stages from UAV device to BS, as the details are shown in Figure 11. The UAV device sends a data, described at the scenario in Figure 7, to the BS and the data sending process starts. The UAV device converts the data into a block structure (Dogan et al., 2023).

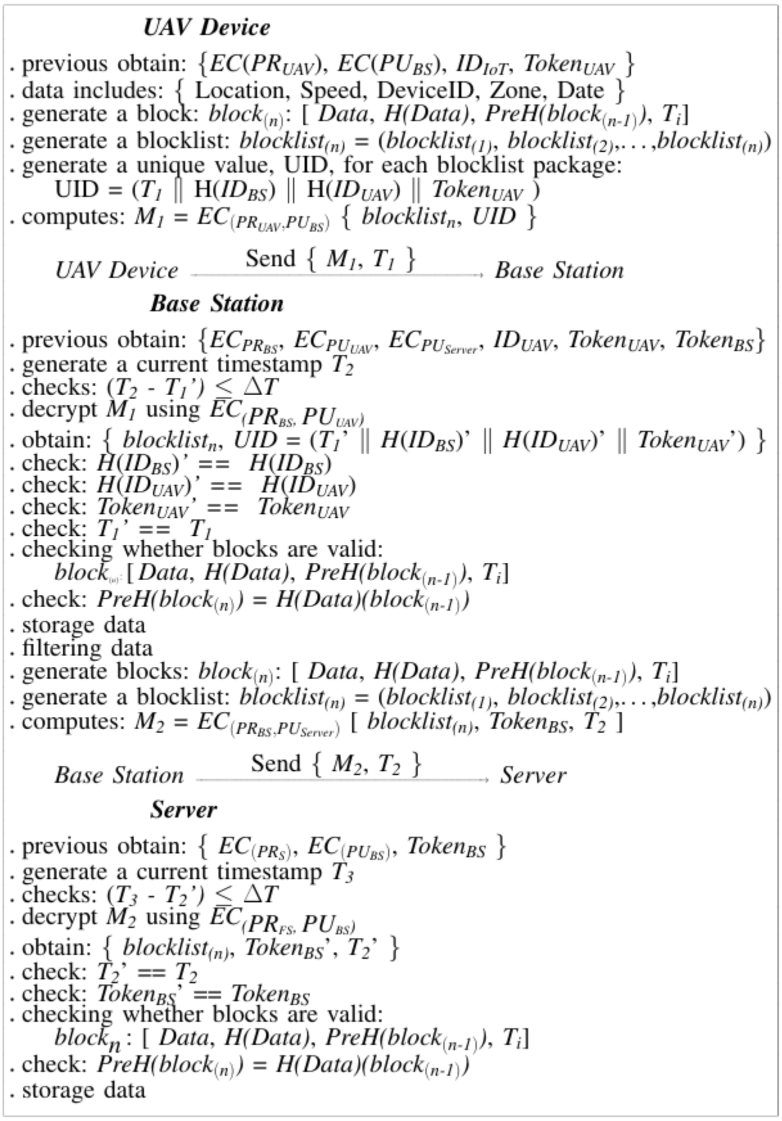
$$\boldsymbol{block_{(n)}} : \textit{[Data, H(Data), PreH(}\boldsymbol{block_{(n-1)}}\textit{), } \boldsymbol{T_i} \textit{]}$$

Moreover, each block has a unique value (***UID***) in the block list, and then, the data is encrypted with the EC private key of the UAV device and the EC public key of the BS. After that, receiving the data from the UAV device, the BS saves the data on its server and sends the critical data to the cloud Server.

Table 2: Symbols and Descriptions for data sending stage



Symbol	Description
EC($\boldsymbol{PR_X}$ / $\boldsymbol{PU_X}$)	Private and Public key of entity X used in Elliptic Curve cryptography (e.g., PR_UAV, PR_BS, PR_S)
$\boldsymbol{ID_X}$	Identifier of entity X (e.g., ID_UAV, ID_BS, ID_IoT)
$\boldsymbol{Token_X}$	Pre-shared token associated with entity X for session validation
$\boldsymbol{T_X}$	Timestamp generated by entity X to ensure freshness and prevent replay attacks
$\boldsymbol{block_{(n)}}$	Data block at sequence n, containing {Data, H(Data), PreH(block_(n-1)), T}
$\boldsymbol{blocklist_{(n)}}$	List of blocks up to n, blocklist_1, blocklist_2, ..., blocklist_n }
$\boldsymbol{H_{(Data)}}$	Cryptographic hash of the transmitted data
$\boldsymbol{PreH_{(block_{(n-1)})}}$	Hash chain linking the previous block's data for integrity verification
UID	Unique identifier generated for a blocklist package, combining timestamp, hashes, and token



UAV Device

. previous obtain: $\{EC(PR_{UAV}), EC(PU_{BS}), ID_{IoT}, Token_{UAV}\}$
. data includes: { Location, Speed, DeviceID, Zone, Date }
. generate a block: $block_{(n)}$: [$Data, H(Data), PreH(block_{(n\text{-}1)}), T_i$]
. generate a blocklist: $blocklist_{(n)} = (blocklist_{(1)}, blocklist_{(2)},\ldots,blocklist_{(n)})$
. generate a unique value, UID, for each blocklist package:
    UID = $(T_1 \parallel \mathrm{H}(ID_{BS}) \parallel \mathrm{H}(ID_{UAV}) \parallel Token_{UAV})$
. computes: $M_1 = EC_{(PR_{UAV},PU_{BS})}\ \{\ blocklist_n, UID\ \}$

$$UAV\ Device \xrightarrow{\text{Send}\ \{\ M_1,\ T_1\ \}} Base\ Station$$

Base Station

. previous obtain: $\{EC_{PR_{BS}}, EC_{PU_{UAV}}, EC_{PU_{Server}}, ID_{UAV}, Token_{UAV}, Token_{BS}\}$
. generate a current timestamp T_2
. checks: $(T_2$ - $T_1') \leq \Delta T$
. decrypt M_1 using $EC_{(PR_{BS}, PU_{UAV})}$
. obtain: $\{\ blocklist_n, UID = (T_1' \parallel H(ID_{BS})' \parallel H(ID_{UAV})' \parallel Token_{UAV}')\ \}$
. check: $H(ID_{BS})' == H(ID_{BS})$
. check: $H(ID_{UAV})' == H(ID_{UAV})$
. check: $Token_{UAV}' == Token_{UAV}$
. check: $T_1' == T_1$
. checking whether blocks are valid:
    $block_{(n)}$: [$Data, H(Data), PreH(block_{(n\text{-}1)}), T_i$]
. check: $PreH(block_{(n)}) = H(Data)(block_{(n\text{-}1)})$
. storage data
. filtering data
. generate blocks: $block_{(n)}$: [$Data, H(Data), PreH(block_{(n\text{-}1)}), T_i$]
. generate a blocklist: $blocklist_{(n)} = (blocklist_{(1)}, blocklist_{(2)},\ldots,blocklist_{(n)})$
. computes: $M_2 = EC_{(PR_{BS},PU_{Server})}$ [$blocklist_{(n)}, Token_{BS}, T_2$]

$$Base\ Station \xrightarrow{\text{Send}\ \{\ M_2,\ T_2\ \}} Server$$

Server

. previous obtain: $\{\ EC_{(PR_S)}, EC_{(PU_{BS})}, Token_{BS}\ \}$
. generate a current timestamp T_3
. checks: $(T_3$ - $T_2') \leq \Delta T$
. decrypt M_2 using $EC_{(PR_{FS}, PU_{BS})}$
. obtain: $\{\ blocklist_{(n)}, Token_{BS}', T_2'\ \}$
. check: $T_2' == T_2$
. check: $Token_{BS}' == Token_{BS}$
. checking whether blocks are valid:
    $block_n$: [$Data, H(Data), PreH(block_{(n\text{-}1)}), T_i$]
. check: $PreH(block_{(n)}) = H(Data)(block_{(n\text{-}1)})$
. storage data

Figure 10: Data sending phase

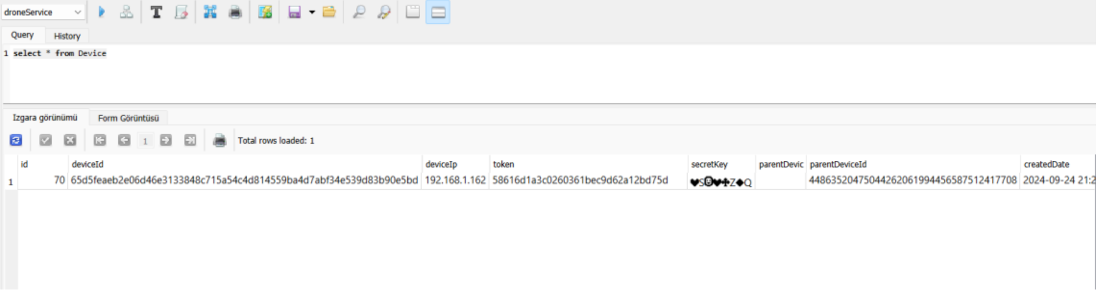
6.2 Implementation and Testing

An experimental setup comprising an Unmanned Aerial Vehicle (UAV) device, and two laptops was utilized to evaluate the authentication protocol developed for UAV networks. The UAV device was equipped with a Raspberry Pi 4 Model B, featuring a 1.5 GHz processor, 4 GB of RAM, and a 32 GB SD card for storage. The base station was configured with an Intel Core i5-7200U CPU operating at 2.50 GHz, 8 GB of RAM, and a 1 TB HDD. Additionally, the server device, which hosted the blockchain application, was outfitted with an Intel Core i7-4510U CPU running at 2.0 GHz, 12 GB of RAM, and a 256 GB SSD. The service applications for both the Drone and Base Station were developed using Python version 3.11. For the development of the web application component, several technologies were employed to enhance functionality and user experience. ASP.NET Core 3.1 was utilized for server-side development, providing a robust framework for backend operations. JavaScript and Leaflet.js were instrumental in creating dynamic user interface components and implementing mapping functionalities, thereby enhancing the interactivity and usability of the web application. HTML was used to construct the structural framework of the web pages, ensuring semantic and accessible markup, while CSS was applied for styling and layout, ensuring a responsive and aesthetically pleasing user interface. Communication between the Drone Service and Base Station was orchestrated via an Apache ActiveMQ message queue, ensuring secure and efficient transmission of messages. This setup facilitated reliable interactions within the UAV network, underpinning the robustness of the authentication protocol. SQLite was selected as the database management system due to its lightweight architecture and capability to support rapid development cycles. Its suitability for small to medium-scale applications made it an ideal choice for managing the data requirements of this study, facilitating efficient data storage and retrieval processes (Dogan et al., 2023).

The testing phase was conducted on a high-performance laptop with the following specifications: Windows 11 operating system, Intel i7-13650HX processor running at 2.6 GHz, 32 GB of RAM, and a 1 TB SSD. Prior to initiating the tests, Apache ActiveMQ was launched to ensure the seamless operation of the software on the UAV device. The applications were executed in the following sequence: Server Service Application, Base Station Service Application, and UAV Service Application. Upon startup of each application, the Elliptic Curve Cryptography (ECC) mechanism generated public and private key pairs, which were subsequently stored in the database. Additionally, each application retrieved the IP addresses assigned by the network and saved this information alongside device-specific details defined in the properties files. These processes were meticulously logged, allowing for comprehensive monitoring and verification of the system's functionality (Dogan et al., 2023).

This structured and methodical approach facilitated a thorough evaluation of the authentication protocol's performance, ensuring that all components interacted harmoniously within the UAV network environment. The integration of robust software frameworks, efficient communication protocols, and reliable hardware specifications collectively contributed to the successful assessment and validation of the developed authentication mechanism. The data recorded by the UAV device in Figure 11 and Base station can be seen below in Figure 12. The token obtained by the devices as a result of the program execution (Dogan et al., 2023).

Drone Service:

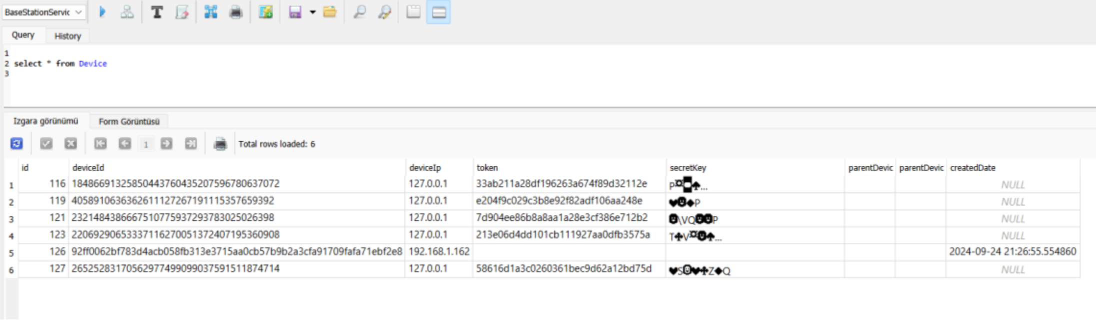


```
select * from Device
```

	id	deviceId	deviceIp	token	secretKey	parentDevic	parentDeviceId	createdDate
1	70	65d5feaeb2e06d46e3133848c715a54c4d814559ba4d7abf34e539d83b90e5bd	192.168.1.162	58616d1a3c0260361bec9d62a12bd75d	♥S⊜♥✚Z◆Q		448635204750442620619944565875124177708	2024-09-24 21:2

Figure 11: The data received by the UAV device (program execution)

Base Station Service:



```

select * from Device

```

	id	deviceId	deviceIp	token	secretKey	parentDevic	parentDevic	createdDate
1	116	18486691325850443760435207596780637072	127.0.0.1	33ab211a28df196263a674f89d32112e	p⊠■✚...			NULL
2	119	40589106363626111272671911153576593392	127.0.0.1	e204f9c029c3b8e92f82adf106aa248e	♥⊜◆p			NULL
3	121	2321484386667510775937293783025026398	127.0.0.1	7d904ee86b8a8aa1a28e3cf386e712b2	⊜\VQ⊜⊜P			NULL
4	123	22069290653337116270051372407195360908	127.0.0.1	213e06d4dd101cb111927aa0dfb3575a	T✚V⊠⊜✚...			NULL
5	126	92ff0062bf783d4acb058fb313e3715aa0cb57b9b2a3cfa91709fafa71ebf2e8	192.168.1.162					2024-09-24 21:26:55.554860
6	127	26525283170562977499099037591511874714	127.0.0.1	58616d1a3c0260361bec9d62a12bd75d	♥S⊜♥✚Z◆Q			NULL

Figure 12: The data recorded by the Base Station Service device (program execution)

Differences from ECDHE/TLS and Reasons for Alternative Approach for UAV network

The Transport Layer Security (TLS) protocol based on Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) aims to provide perfect forward secrecy by generating a new Elliptic Curve Diffie-Hellman key for each session. However, the ECDHE key exchange mechanism involves computationally expensive operations such as elliptic curve point multiplication, modular arithmetic, and cryptographic hash computations. A typical handshake requires multiple elliptic curve operations, certificate chain verification, and identity proofing. Moreover, the TLS handshake and session management process generally entail 6–8 message exchanges and complex handshake flows. In the context of UAV networks, the use of TLS/ECDHE has been deemed unsuitable for the following reasons:

- Resource constraints: For the UAV hardware assumed in this thesis, protocols like TLS/ECDHE that impose a heavy computational load negatively impact operational efficiency when executed in real time, due to excessive energy consumption and processing time.
- Bandwidth and latency: The TLS handshake process involves numerous message exchanges and additional protocol overhead. In latency-sensitive applications such as real-time video streaming and mission coordination, this leads to unacceptable delays and packet overhead.
- Full stack requirements: TLS/ECDHE necessitate a full TCP/IP stack, certificate authority support, and comprehensive session management. UAV devices are generally ill-suited to continuously host and manage such complex stacks.

In contrast, the protocol developed in this thesis offers:

- ✓ Lightweight cryptographic structure: It employs AES-based symmetric encryption and hash functions, avoiding computationally intensive operations like elliptic curve computations and certificate chain verifications.
- ✓ Dynamic and low-latency key management: Session keys are derived directly via the dynamic secret key (DSK), and the authentication exchange consists of only two message packets, eliminating the need for long handshake sequences typical of TLS (min. 6–7 messages).
- ✓ Temporary identity and token mechanism: Instead of relying on a centralized identity authentication chain as in TLS, the proposed protocol ensures end-to-end identity privacy and continuous authentication through temporary identities and tokens.
- ✓ Byzantine tolerance and consensus support: The two-tier consensus mechanism (e.g., LBFT-supported) and blockchain structure of the SABEC protocol provide decentralized identity and data integrity management, which TLS does not offer.

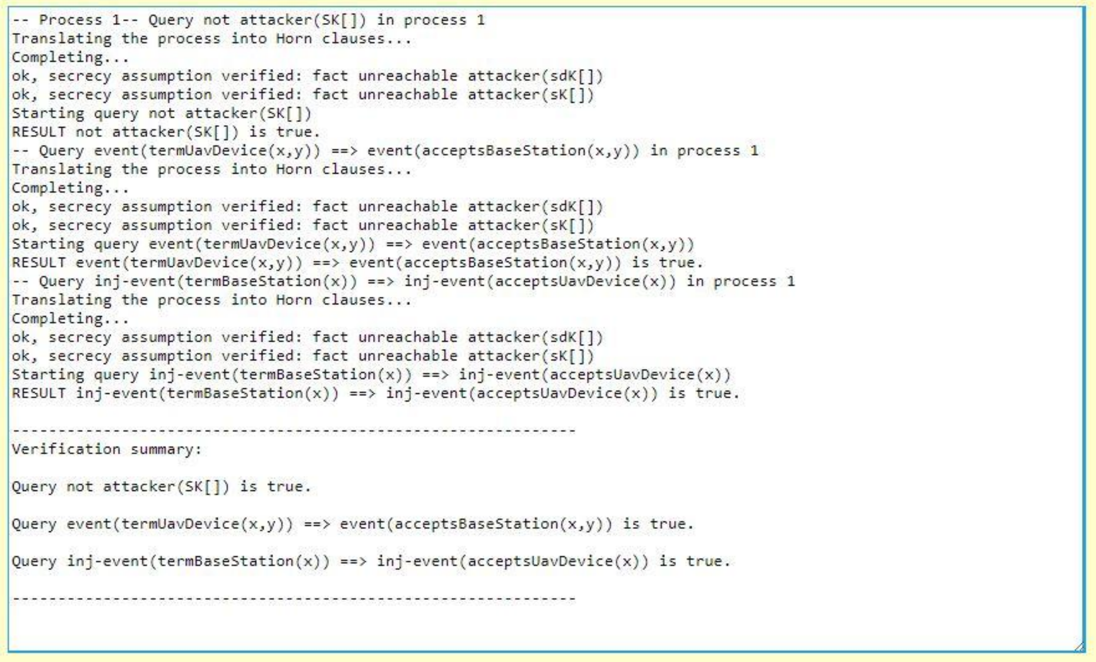
In conclusion, the proposed protocol has been specifically designed and optimized for the resource constraints and dynamic characteristics of UAV networks, deliberately avoiding the excessive computational and communication overhead introduced by TLS/ECDHE.

6.3 Security Analysis of the Authentication Protocol

In the rapidly evolving landscape of Unmanned Aerial Vehicle (UAV) networks, ensuring robust security protocols is vital due to the potential risks associated with unauthorized access and malicious attacks (Tian et al., 2024). This chapter provides a comprehensive security analysis of the proposed Secure Authentication Protocol, focusing on its strengths compared to existing frameworks. The analysis employs a dual approach, integrating formal verification methods and theoretical proofs to assess the protocol's resilience against various security threats (Dogan et al., 2023).

Formal Verification: To rigorously evaluate the security features of the Secure Authentication Protocol, we utilize *ProVerif* (Cheval et al., 2018), a prominent formal verification tool that leverages the *Dolev-Yao* attack model. *ProVerif* allows for the systematic analysis of security properties by converting the protocol into *Horn clauses* (Fagin et al., 1982), enabling the verification of critical features such as secrecy, authenticity, and resilience against attacks. The verification process is structured around two primary communication channels: a private channel (***sChannel***) for secure communications and a public channel (***pChannel***) for standard exchanges. During the authentication phase, the protocol facilitates communication between ***IDuav*** (the UAV device identity) and ***IDbs*** (the Base Station identity) using their public keys (***PKuav*** and ***PKbs***) alongside *AES* secret keys (***sK***) and dynamic secret keys (***sdK***). This multifaceted approach ensures that all participating entities compute and verify session keys effectively, safeguarding the confidentiality of the transmitted information. The *ProVerif* tool is instrumental in analysing these interactions, where specific functions—such as hash, concatenation, encryption, and decryption—are predefined to maintain security integrity (Dogan et al., 2023).

In the context of our protocol, four key events are outlined to analyse the verification process between UAV and BS devices. Subsequently, the confidentiality of session keys, or tokens, is assessed through targeted queries. The results from ProVerif reveal that all three primary processes of the protocol—initialization, authentication, and termination—execute successfully, confirming that session keys are impervious to adversarial attacks. Thus, we conclude that the protocol effectively preserves secrecy and achieves secure authentication (Dogan et al., 2023).



```
-- Process 1-- Query not attacker(SK[]) in process 1
Translating the process into Horn clauses...
Completing...
ok, secrecy assumption verified: fact unreachable attacker(sdK[])
ok, secrecy assumption verified: fact unreachable attacker(sK[])
Starting query not attacker(SK[])
RESULT not attacker(SK[]) is true.
-- Query event(termUavDevice(x,y)) ==> event(acceptsBaseStation(x,y)) in process 1
Translating the process into Horn clauses...
Completing...
ok, secrecy assumption verified: fact unreachable attacker(sdK[])
ok, secrecy assumption verified: fact unreachable attacker(sK[])
Starting query event(termUavDevice(x,y)) ==> event(acceptsBaseStation(x,y))
RESULT event(termUavDevice(x,y)) ==> event(acceptsBaseStation(x,y)) is true.
-- Query inj-event(termBaseStation(x)) ==> inj-event(acceptsUavDevice(x)) in process 1
Translating the process into Horn clauses...
Completing...
ok, secrecy assumption verified: fact unreachable attacker(sdK[])
ok, secrecy assumption verified: fact unreachable attacker(sK[])
Starting query inj-event(termBaseStation(x)) ==> inj-event(acceptsUavDevice(x))
RESULT inj-event(termBaseStation(x)) ==> inj-event(acceptsUavDevice(x)) is true.

--------------------------------------------------------------
Verification summary:

Query not attacker(SK[]) is true.

Query event(termUavDevice(x,y)) ==> event(acceptsBaseStation(x,y)) is true.

Query inj-event(termBaseStation(x)) ==> inj-event(acceptsUavDevice(x)) is true.

--------------------------------------------------------------
```

Figure 13: The query results of the *ProVerif*

The query results of the *ProVerif* demonstrates the performance of our proposed method in Figure 13. On the basis of the results, it can be concluded that all three main processes of our protocol are successfully started and terminated. The results show that session keys are safe from any adversary attack. To summarize, using the *ProVerif* tool, we are able to prove that our protocol hand over preserves secrecy and attain secure authentication (Dogan et al., 2023).

Security Services Verification (Informal Security Analysis): The proposed protocol incorporates multiple security services that are essential for the integrity and reliability of communications. The informal analysis consequences show that the presented scheme not only offers security features for mutual authentication, confidentiality, data integrity and anonymity but also prevents various possible attacks, such as impersonation, replay, and man-in-the-middle attacks. The adversary model's potential capabilities and security objectives are considered when performing in formal analysis (Dogan et al., 2023).

- ***Statement. 1 Mutual Authentication:***

The mutual authentication mechanism designed in this thesis ensures that both the Unmanned Aerial Vehicle (UAV) and the Base Station (BS) can cryptographically verify each other's identities before establishing secure communication. This process is fundamental for preventing unauthorized devices from impersonating legitimate nodes and for ensuring that only trusted entities participate in the UAV network. Unlike conventional challenge-response mechanisms that rely on static credentials or certificates, the proposed protocol employs a dynamic and session-specific mutual authentication strategy based on the derivation and verification of a Dynamic Secret Key (DSK). Specifically, the DSK is calculated as: $\boldsymbol{DSK = [(H(\alpha) \,||\, H(TID_{UAV} \,||\, TID_{BS}) \oplus R)]}$ where α is a shared secret between the UAV and BS, and R is a random value generated and known initially by the UAV, and later derived by the BS through:

$$\boldsymbol{R' = (B' \oplus H(TID_{UAV} \,||\, TID_{BS} \,||\, \alpha) \oplus T_1)}$$

Since only legitimate devices possess the required parameters α, R, and the temporary IDs, any adversary (even with full knowledge of the protocol structure and intercepted messages) cannot compute a valid DSK without breaking the cryptographic primitives (e.g., AES, SHA-256). This ensures that the UAV and BS can successfully authenticate each other. UAV will only proceed if the BS demonstrates knowledge of the correct DSK (e.g., through successful decryption and validation of message contents). BS will only proceed if the UAV demonstrates knowledge of the correct DSK in its encrypted responses.

Furthermore, dynamic nonces, timestamps, and temporary IDs are integrated into the authentication flow to guarantee message freshness and prevent attacks. The protocol's mutual authentication property is not based on secrecy of implementation details (i.e., not security through obscurity), but rather on the hardness of inverting cryptographic hash functions, breaking symmetric encryption, or guessing high-entropy random values under the assumed Dolev-Yao threat model, where the adversary controls the channel but cannot break standard cryptographic primitives (Dogan et al., 2023).

- ***Statement. 2 Resistance to Man-in-the-Middle (MITM) Attacks:***

In this thesis, the authentication protocol developed has been designed to provide a lightweight and secure structure suitable for the resource and processor constraints of unmanned aerial vehicle (UAV) networks, and it is structured to be resilient against Man-in-the-Middle (MITM) attacks. The protocol consists of three main phases: the offline phase, the device registration phase, and the authentication phase. Resistance to MITM attacks is ensured particularly through the use of the dynamic secret key (DSK) and cryptographic mechanisms employed during the authentication phase. The analysis conducted within the scope of this thesis considers a scenario in which an attacker (Eve) intercepts the initial message exchanged between the UAV and the base station (BS) in the authentication stage $\boldsymbol{\{M_1, T_1\}}$. In this scenario, the content of $\boldsymbol{M_1}$ consists of the encrypted form of the essential authentication parameters, $\boldsymbol{M_1 = E_{SK}}$ **(A || B ||** $\boldsymbol{T_1}$**))**. It should be clarified that $\boldsymbol{M_1}$ internally contains the encrypted form of **A**, **B**, and $\boldsymbol{T_1}$. Therefore, an adversary intercepting $\boldsymbol{M_1}$ would only have access to ciphertext, and without knowledge of the dynamic secret key (DSK), derived from confidential parameters exclusively known to legitimate parties, the adversary cannot decrypt $\boldsymbol{M_1}$ or $\boldsymbol{M_2}$. Also, the critical design component of the protocol, the DSK, is computed based solely on confidential parameters (e.g., ***H(α)*** and $\boldsymbol{R}$) known only to the legitimate devices (UAV and BS), and the session key between the devices is derived from this dynamic structure. If the attacker transmits the forged message, the inability to generate the correct DSK results in a failure of session key matching, thereby preventing further communication. The use of dynamic nonces, timestamps, and temporary IDs guarantees message freshness and prevents replay attacks. Furthermore, since each message signature and data block are verified through hash functions and symmetric keys, message integrity is also preserved. This architecture renders session hijacking and identity spoofing attempts, typical goals of MITM attacks, technically infeasible (Dogan et al., 2023).

- ***Statement. 3 Protection Against Replay Attacks:***

Replay attacks present a significant threat in communication networks, particularly in systems involving resource-constrained devices such as UAVs. In this scenario, suppose an adversary intercepts an initial authentication message exchanged between the base station (BS) and the UAV, structured as $\{\boldsymbol{M_1}, \boldsymbol{T_1}\}$, where $\boldsymbol{M_1} = \boldsymbol{E_{SK}}$ (**A** || **B** || $\boldsymbol{T_1}$)). Here, A denotes the temporary *ID* of the *UAV*, B denotes the *ID* of the *BS*, and $\boldsymbol{T_1}$ is a timestamp ensuring the freshness of the message. The adversary captures this packet and attempts to launch a replay attack by resending $\{\boldsymbol{M_1}, \boldsymbol{T_{Eve1}}\}$, where $\boldsymbol{T_{Eve1}}$ is a forged timestamp controlled by the attacker. However, the protocol's use of timestamps ensures that any replayed or delayed messages fall outside the valid time window. During the authentication process, the base station verifies the freshness of incoming messages by checking whether $(\boldsymbol{T_2} - \boldsymbol{T_{Eve1}}) \leq \Delta\boldsymbol{T}$, where $\boldsymbol{T_2}$ is the current time and $\Delta\boldsymbol{T}$ is the allowable delay threshold. Any discrepancies trigger the rejection of the message, thereby effectively mitigating the risk of replay attacks (Dogan et al., 2023).

- ***Statement. 4 Secured from Impersonation Attacks:***

An attacker attempting to join the UAV network as a legitimate device faces significant barriers due to the stringent authentication measures in place. If an intruder, such as *Eve*, attempts to send a message, $\{\boldsymbol{M_{Eve1}}\}$, to the network's legitimate devices, they will be unable to do so without the appropriate dynamic secret key. Since the message is not encrypted with the DSK known by the UAV device and BS/node. Thus, the node or UAV devices will not decrypt the message and will ignore it. As such, unauthorized messages will not be decrypted or acted upon by the legitimate nodes, effectively thwarting impersonation attempts (Dogan et al., 2023) [413].

- ***Statement. 5 Resilience to Denial-of-Service (DoS) Attacks:***

The proposed authentication protocol has been meticulously designed to provide resilience against Denial-of-Service (DoS) attacks by integrating cryptographically protected early filtering and rate-limiting mechanisms at the base station (BS) level. In this design, critical authentication elements, including the timestamp (T_1), nonce (N), and Temporary ID (TID), are encrypted using AES-based symmetric cryptography prior to transmission. As a result, any adversary attempting to flood the BS with arbitrary or replayed messages must first generate valid AES ciphertext, which is computationally infeasible without knowledge of the dynamic secret key (*DSK*) derived from confidential parameters (e.g., *H(α)*, *R*) shared solely between the legitimate UAV and BS.

Upon receiving a message, the BS performs lightweight preliminary checks before any cryptographic decryption is attempted. Specifically, the BS evaluates whether the message's source TID is authorized and whether the timestamp satisfies $\boldsymbol{(T_{now} - T_1) \leq \Delta T}$. Messages failing these conditions are immediately discarded, thus preventing unnecessary consumption of computational resources. Furthermore, per-TID rate-limiting is enforced, the BS accepts no more than η requests per TID per second. Excess messages are either delayed or dropped, effectively throttling excessive request patterns that are indicative of DoS behaviour. Therefore, the DoS resilience of the proposed protocol does not rely on obscurity or plaintext checks but on cryptographically verifiable structures, rate-limiting, and early rejection logic that collectively minimize the computational impact of malicious traffic and preserve operational integrity under adversarial conditions.

- ***Statement. 6 Secure Against Attacks Targeting Forwarding Security (FS):***

The protocol employs random number generation during authentication processes, contributing to the creation of dynamic secret keys and tokens. Should an attacker capture a token, it would be ineffective in subsequent communications due to the periodic resetting of token values within the system. The independence of newly generated tokens from previous ones reinforces the security framework, ensuring that even if an attacker acquires a token, it remains powerless against future communications. Therefore, the proposed scheme is also resistant to other known attacks, as it performs dynamic keys in the authentication process and applies a one-way hash function to the identity of the devices in the network (Dogan et al., 2023).

- ***Statement. 7 Resistance to Byzantine Attacks:***

The dynamic identity authentication protocol proposed in this thesis has been specifically designed to provide resilience against Byzantine attacks in UAV networks, where nodes may behave arbitrarily or maliciously to disrupt network integrity, impersonate legitimate devices, or inject false data. The protocol integrates multiple cryptographic safeguards and structural design choices to ensure that such threats are effectively mitigated at both the authentication and network coordination levels.

At its core, the protocol utilizes **temporary identity values ($\boldsymbol{TID_{UAV}}$, $\boldsymbol{TID_{BS}}$)** that are dynamically generated and refreshed at configurable intervals. These temporary identifiers are combined with random values and shared secrets to derive a **dynamic secret key (DSK)**, according to the following formulation: $\boldsymbol{DSK = [(H(\alpha) \,||\, H(TID_{UAV} \,||\, TID_{BS}) \oplus R)]}$ where α is a shared secret between the UAV and BS, and R is a random value generated and known initially by the UAV, and later derived by the BS through: $\boldsymbol{R' = (B' \oplus H(TID_{UAV} \,||\, TID_{BS} \,||\, \alpha) \oplus T_1)}$. A Byzantine node, lacking access to the true α and unable to correctly generate or compute R, is incapable of deriving a valid DSK. Consequently, any attempt to forge authentication credentials or masquerade as a legitimate node would fail at the mutual authentication phase, as the derived session keys between the UAV and BS would not match. Furthermore, all sensitive authentication parameters (including temporary IDs, timestamps, and nonces) are encrypted using AES-based symmetric encryption prior to transmission. This prevents Byzantine nodes from forging or tampering with these parameters without detection, as any deviation would lead to failed decryption or inconsistent validation results during protocol execution. For example, if a Byzantine node attempts to inject messages with fabricated TIDs or outdated timestamps, the BS will detect these anomalies during the initial validation checks without incurring significant computational overhead. Specifically, the BS applies early filtering by verifying that: $\boldsymbol{(T_{now} - T_1) \leq \Delta T}$ and confirming that the TID exists within its authorized session list. Messages failing these checks are discarded immediately, preventing resource exhaustion, a common goal in Byzantine disruption attempts.

In addition to cryptographic safeguards at the session level, the protocol's integration with the **SABEC framework** ensures robust systemic defence against Byzantine behaviour. All authentication outcomes, including failed or suspicious attempts, are immutably logged within a private, permissioned blockchain. These records feed into the network's consensus-driven trust assessment process, whereby nodes exhibiting inconsistent or malicious behaviours are identified and isolated based on collective agreement rather than individual node assertions. This design ensures that even if some nodes are compromised, their influence is limited, as their actions are subject to the consensus of honest majority nodes. The SABEC protocol's two-tier lightweight BFT consensus (LBFT) ensures that the integrity of network coordination and authentication is preserved even in the presence of Byzantine actors attempting to submit fraudulent trust metrics or disrupt node clustering processes.

In that case, the dynamic identity authentication protocol combines dynamic identity cycling, cryptographic binding of authentication data, early rejection mechanisms, and blockchain-backed collective verification to deliver comprehensive protection against Byzantine attacks. This architecture ensures that malicious nodes cannot forge identities, manipulate session keys, or disrupt trust structures within the UAV network, thereby upholding the security, reliability, and resilience of the system.

- ***Statement. 8 Protection Against Sybil Attacks:***

  In a Sybil attack, a single adversary creates multiple identities to gain disproportionate influence within a network. The proposed protocol mitigates this risk through its registration and authentication phases, which require devices to present unique credentials linked to their physical identities. The use of public-key cryptography further complicates the adversary's efforts, as each identity is tied to a distinct cryptographic key pair, making it computationally infeasible for the attacker to generate valid identities at scale (Dogan et al., 2023).

The security analysis of the Secure Authentication Protocol confirms its robust framework for addressing the myriad security challenges faced by UAV networks. Through formal verification and rigorous theoretical proofs, the protocol demonstrates a high level of resilience against common attacks, including MITM, replay, impersonation, DoS, Byzantine, Sybil, and eavesdropping attacks. The careful design and implementation of cryptographic measures, combined with the strategic integration of dynamic keys and blockchain technology, ensure secure, scalable, and privacy-preserving communications in UAV operations. This comprehensive security framework not only enhances the integrity and reliability of UAV communications but also positions the protocol as a viable solution for future applications in this critical domain (Dogan et al., 2023).

6.4 Performance Evaluation

In the domain of Unmanned Aerial Vehicle (UAV) networks, the efficiency and effectiveness of authentication protocols are paramount, particularly given the resource-constrained nature of UAV devices. The proposed Secure Authentication Protocol within the Identity Management System (IDMS) framework aims to address these challenges by optimizing both computational and communication costs. This chapter provides a comprehensive performance analysis of the proposed scheme, juxtaposing it against existing authentication models to elucidate its advantages and potential areas for improvement. The analysis is structured around key performance indicators, including computational overhead, memory consumption, execution time, and communication efficiency, which are critical for evaluating the viability of any authentication protocol in UAV environments. A pivotal aspect of evaluating the proposed Secure Authentication Protocol involves a comparative analysis with other contemporary authentication models. The primary metrics of comparison are computational and communication costs, which directly influence the protocol's suitability for deployment in UAV networks. Table 3 presents a detailed comparison of the computational overheads between our scheme and those proposed in references (Srinivas et al. 2019, Das et al. 2021, Bera et al. 2020). These references encompass a range of authentication protocols tailored for IoT and UAV applications, each with varying degrees of complexity and resource demands.

The burgeoning field of unmanned aerial vehicle (UAV) networks necessitates robust security mechanisms to protect against a myriad of potential threats. Our work, titled "Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme," aims to address these concerns by proposing a novel authentication protocol that leverages the efficiency of the Advanced Encryption Standard (AES) and formal verification through ProVerif. In this discourse, we critically compare our proposed scheme with three seminal works in the domain: Srinivas et al. (2019), Das et al. (2021), and Bera et al. (2020), focusing on their methodologies, security provisions, and applicability to UAV networks (Dogan et al., 2023).

Srinivas et al. (2019) introduce TCALAS, a temporal credential-based anonymous lightweight authentication scheme designed for the Internet of Drones (IoD) environment. The primary focus of TCALAS is to provide anonymity to UAVs, preventing unauthorized tracking and enhancing privacy. This is achieved through the use of temporal credentials, which change over time, thus making it difficult for adversaries to link credentials to specific UAVs. The scheme employs lightweight cryptographic operations to accommodate the resource constraints of UAVs. Our proposed scheme differs from TCALAS in several key aspects. While TCALAS emphasizes anonymity, our scheme prioritizes mutual authentication and secure key agreement between UAVs and BS. We recognize that, in many UAV network applications, ensuring the legitimacy of devices and securing communications are paramount, even if anonymity is not the primary concern. By utilizing the Advanced

Encryption Standard (AES) for encryption and authentication, our scheme achieves high efficiency and security, facilitating rapid and secure communication essential for UAV operations. Moreover, our scheme employs dynamic secret keys, current timestamps, random nonces, and renewable tokens, enhancing its resilience against a range of attacks, including impersonation, replay, and forwarding attacks. The use of renewable tokens and synchronized clocks ensures that security credentials are regularly updated, further strengthening the network's defense mechanisms. A significant advancement in our work is the formal security verification using the ProVerif tool. This provides rigorous assurance of our scheme's security properties, something that is not explicitly demonstrated in TCALAS. While TCALAS presents a security analysis against common attacks, the formal verification in our scheme offers a higher level of confidence in its robustness, ensuring that it meets the stringent security requirements of UAV networks (Dogan et al., 2023).

Das et al. (2021) propose iGCACS-IoD, a certificate-enabled generic access control scheme for IoD deployments. Their approach enhances security by managing access rights and authenticating entities within the network using certificates. This certificate-based mechanism ensures that only authorized devices can participate in the network, thereby mitigating unauthorized access and potential insider threats. While certificate-based schemes like iGCACS-IoD provide robust security features, they introduce computational and communication overhead that may not be suitable for resource-constrained UAVs. The management of certificates involves complex operations and requires additional storage and processing capabilities, which can strain the limited resources of UAV devices. Our scheme addresses this challenge by eliminating the need for certificates. Instead, we design a lightweight authentication protocol that utilizes dynamic secret keys and renewable tokens, reducing computational and communication overhead. Each entity in our network possesses a key pair (public and private) and a unique temporary ID, facilitating secure mutual authentication without the complexities associated with certificates. Additionally, our scheme assumes synchronized clocks among devices, simplifying the authentication process and enhancing efficiency. The authentication phase is dynamic, allowing UAV devices and BS to interact as needed without incurring significant delays or resource consumption. The formal security verification using ProVerif in our scheme further distinguishes it from iGCACS-IoD. While Das et al. (2021) provide a security analysis, our use of formal verification tools offers a more rigorous validation of security properties, ensuring that our scheme is robust against a wide range of attacks. In terms of scalability, our scheme's lightweight nature makes it more practical for large-scale UAV network deployments. By minimizing overhead and simplifying the authentication process, our scheme can accommodate a growing number of devices without compromising performance or security (Dogan et al., 2023).

Bera et al. (2020) present a blockchain-based access control scheme for IoT-enabled Internet of Drones deployments. Their approach leverages the decentralized and immutable nature of blockchain technology to enhance security. By recording access events on a blockchain, the scheme ensures transparency and tamper-resistance, effectively mitigating single points of failure and fostering trust among network participants. While blockchain integration offers significant security advantages, it poses challenges when applied to UAV networks. The computational demands and latency associated with blockchain operations are substantial, making it unsuitable for UAVs with limited processing power and energy resources. While conventional blockchain implementations (such as public blockchains based on Proof of Work (PoW) or Proof of Stake (PoS)) are unsuitable for direct integration into UAV devices due to their computational demands and latency, blockchain technology remains crucial for achieving decentralized trust, data integrity, and tamper-resistant record-keeping in UAV networks. To address this challenge, this thesis proposes a novel, lightweight, and UAV-adapted blockchain protocol, SABEC, specifically designed to overcome these limitations. SABEC leverages a permissioned blockchain architecture combined with lightweight consensus mechanisms tailored for resource-constrained UAV environments. This design ensures that the security benefits of blockchain can be achieved without imposing prohibitive overhead on UAV devices, thus filling the identified gap. By utilizing AES for encryption and authentication, our scheme achieves efficient security without the need for extensive computational resources. The use of dynamic secret keys, current timestamps, random nonces, and renewable tokens provides robust security features comparable to those offered by blockchain-based schemes but without the associated overhead. Furthermore, the simplicity of our scheme facilitates easier implementation and deployment in real-world UAV networks. The reliance on synchronized clocks and direct communication between UAVs and BS reduces complexity and enhances efficiency. Our scheme does not require additional infrastructure or maintenance associated with blockchain networks, making it a practical choice for immediate deployment. The formal security verification using ProVerif adds another layer of assurance to our scheme. By rigorously validating the security properties, we ensure that our scheme is resilient against various attacks, providing confidence in its suitability for securing UAV networks (Dogan et al., 2023).

The comparative analysis of our proposed scheme with the works of Srinivas et al. (2019), Das et al. (2021), and Bera et al. (2020) underscores the unique contributions and advancements our work brings to the field of UAV network security. While each of these existing schemes addresses specific aspects of security, they present limitations concerning resource efficiency, complexity, or practicality when applied to UAV networks. Our scheme stands out by offering a balanced approach that combines robust security features with efficiency and practicality. By focusing on mutual authentication and secure key agreement without relying on resource-intensive mechanisms like certificates or blockchain, we provide a solution tailored to the constraints of UAV devices. The use of lightweight cryptographic operations ensures that our scheme can be effectively implemented on devices with limited computational capabilities. The formal security verification using ProVerif distinguishes our work by providing rigorous assurance of its security properties. This complements traditional cryptanalysis and demonstrates our scheme's resilience against a comprehensive range of attacks, including impersonation, replay, and forwarding attacks. In terms of scalability and practicality, our scheme facilitates secure communication between distributed UAV-based applications and ground nodes (BS), enabling the establishment of new practical secret session keys during authentication. The dynamic nature of these session keys allows for secure communication as long as the UAV device remains within the network, ensuring ongoing security without significant overhead. By minimizing computational and communication overhead, our scheme enhances performance and efficiency, critical factors in UAV network operations. This makes our scheme well-suited for large-scale deployments where resource constraints and real-time communication are paramount. In conclusion, our work advances the field of UAV network security by providing a secure, efficient, and practical authentication and key agreement scheme. By addressing the limitations of existing approaches and focusing on the specific needs of UAV networks, we offer a solution that enhances security without compromising performance. Our scheme lays a robust foundation for future research and development in secure UAV communications, contributing to the safe and reliable integration of UAVs in various applications (Dogan et al., 2023).

Table 3. Comparison the proposed authentication scheme with other works

Aspect	**Srinivas et al. (2019)**	**Das et al. (2021)**	**Bera et al. (2020)**	**Our Work (Dogan, 2023)**
Focus of the Paper	Temporal credential-based anonymous lightweight authentication scheme for IoD environments	Improved certificate-enabled generic access control scheme for IoD deployments	Secure blockchain-based access control scheme in IoT-enabled IoD deployments	Secure lightweight authentication and key agreement scheme for UAV networks
Authentication Mechanism	Employs temporal credentials to achieve anonymity; lightweight authentication between drones and ground stations	Uses certificate-based authentication and access control; manages access rights through certificates	Leverages blockchain technology for decentralized access control; immutable recording of access events	Utilizes AES encryption, dynamic secret keys, timestamps, random nonces, and renewable tokens; provides mutual authentication between UAVs and base stations
Security Features	Provides anonymity and privacy; protects against common security threats	Enhances security via certificate management; mitigates unauthorized access and insider threats	Offers security through blockchain's decentralization and immutability; protects against tampering	Ensures confidentiality, data integrity, identity privacy; resilient against impersonation, replay, and forwarding attacks

Formal Security Verification	Security analysis against common attacks; no formal verification tool mentioned	Presents a security analysis; lacks formal verification using tools like ProVerif	Includes a security analysis; does not employ formal verification tools	Conducted using ProVerif tool and traditional cryptanalysis
Performance and Efficiency	Lightweight scheme suitable for UAVs; temporal credentials may introduce some overhead	Potentially higher overhead due to certificate management; may strain UAV resources	High computational demands and latency from blockchain operations; less suitable for UAVs	Lightweight and efficient; designed for resource-constrained UAVs; low computation costs due to AES
Implementation Complexity	Relatively straightforward; relies on temporal credentials	More complex due to certificate issuance and management; increased communication overhead	Complex implementation requiring blockchain setup and maintenance	Simple implementation without the need for certificates or blockchain infrastructure; practical for immediate deployment
Scalability	Scalable design for IoD environments	Scalability may be hindered by certificate management overhead	Scalability challenged by blockchain's resource requirements and latency	Highly scalable; minimal overhead makes it suitable for large UAV networks
Anonymity and Privacy	Emphasizes anonymity through temporal credentials to prevent tracking	Enhances security but does not specifically focus on anonymity	Ensures privacy through blockchain's inherent features	Provides identity privacy; focuses on mutual authentication and secure key agreement
Key Management	Utilizes temporal credentials; specific key management details are less emphasized	Relies on certificates for key management; involves certificate authorities	Manages keys through blockchain mechanisms; keys are tied to blockchain identities	Each entity possesses a key pair (public/private) and a unique temporary ID; dynamic session keys established during authentication
Protocol Phases	Protocol phases not explicitly detailed	Protocol structure not specifically outlined	Protocol phases not distinctly specified	Three phases: offline personalization, device registration, dynamic authentication; assumes synchronized clocks among devices

Resilience Against Attacks	Protects against common attacks; focus on anonymity adds privacy protection	Mitigates unauthorized access; security analysis addresses potential threats	Security benefits from blockchain's tamper-resistance; protects against data manipulation	Robust against impersonation, replay, and forwarding attacks; uses renewable tokens and synchronized timestamps
Use of ProVerif	No use of formal verification tools like ProVerif mentioned	Does not employ formal verification tools; relies on traditional security analysis	Does not utilize formal verification tools; security claims based on analysis	Yes, formal security verification strengthens confidence in protocol's robustness

Our protocol demonstrates a significant reduction in computational overhead, attributable to its streamlined cryptographic operations and efficient key management strategies. Specifically, the computation costs, measured in terms of memory consumption and execution time, are markedly lower for our scheme when compared to the referenced models. This efficiency is critical for UAV devices, which are often constrained by limited processing power and energy resources.

- ***Experimental Setup:***

To empirically validate the performance of the proposed Secure Authentication Protocol, we implemented the scheme on off-the-shelf devices, specifically the Raspberry Pi 4 Model B, known for its balance between performance and cost-effectiveness. The Raspberry Pi 4 Model B was selected due to its 1.5 GHz processor, 4 GB RAM, and 32 GB storage capacity, which adequately simulate the operational constraints of typical UAV devices. During the simulation phase, the Raspberry Pi 4 Model B was selected as an embedded system platform to emulate the flight control unit of UAV devices. This choice was justified by its ARM-based architecture, compact form factor, and its well-established acceptance in the academic literature as a widely used prototyping tool for UAV-related applications. While it is acknowledged that the Raspberry Pi 4 provides greater computational resources compared to typical commercial UAV flight controllers, this selection aimed to offer a practical and accessible platform for validating the logical design, communication flow, and key performance indicators of the proposed protocols. The base station and server components of the testbed were configured on more robust hardware, comprising Core i5 and Core i7 processors operating at 2.50 GHz and 2.0 GHz, respectively, with 8 GB and 12 GB of RAM.

This setup ensured that the computational load of the UAV devices was isolated, allowing for precise measurement of the protocol's performance under realistic conditions (Dogan et al., 2023). Although the computational capabilities of the Raspberry Pi 4 do not fully represent the more constrained processors (200–800 MHz) and memory capacities found in actual UAV flight hardware, the primary aim at this stage was to demonstrate the correct functioning of the developed authentication and consensus protocols and to validate the applicability of the system architecture within an embedded environment. The simulation was not intended to serve as a worst-case performance benchmark, but rather as a proof-of-concept prototype to illustrate the viability of the proposed solution. Future work will focus on testing the developed IDMS and SABEC protocols on actual low-power flight computers and microcontroller-based UAV systems, with targeted energy and timing optimizations adapted to the operational realities of commercial UAV hardware. Therefore, the rationale for selecting the Raspberry Pi 4 lies in its embedded system characteristics and its widespread use in the academic literature for prototyping and design validation of UAV systems. This approach provided both academic consistency and an engineering-practical solution, offering an effective means for the early-stage validation of the proposed protocols.

For the cryptographic operations, the Advanced Encryption Standard (AES) with a 128-bit key was employed during the registration and authentication phases between UAV devices and Base Stations (BS). The Bouncy Castle library facilitated the implementation of Elliptic Curve Cryptography (ECC) during the data transmission phase between BS and server devices. Additionally, the SHA-256 function was utilized as a one-way hash function, providing a 256-bit output, while timestamps were standardized at 32 bits to ensure consistency and reliability in message integrity verification (Dogan et al., 2023).

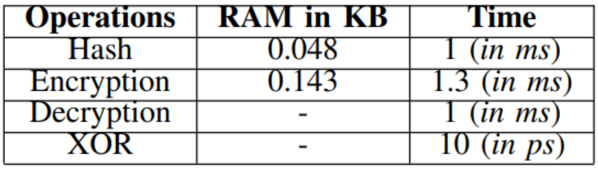
The following analysis, the communication and computational cost analysis, presented in this thesis specifically pertains to the dynamic secure authentication protocol and focuses on the message exchange between a single UAV device and a base station during an individual authentication session. The calculated overhead reflects the bit-level communication required to successfully complete one mutual authentication cycle between these two entities. This scope was intentionally defined to isolate and quantify the efficiency of the proposed lightweight cryptographic design at the session level, without aggregating additional costs that would arise in a broader multi-UAV network context. Therefore, the values reported in the cost analysis should be interpreted as per-session metrics, representing the communication and computational burden for one UAV–BS interaction.

➢ ***Communication Cost Analysis:***

Communication efficiency is a critical determinant of an authentication protocol's practicality in UAV networks. Table 4 delineates the size of various components involved in the authentication process, including identities, timestamps, hash functions, AES encryption, and ECC operations. In our proposed scheme, the authentication phase involves the exchange of two messages: a 56-byte message sent by the UAV and a 118-byte message received from the BS. This results in an overall communication overhead of 1392 bits during the authentication phase (Dogan et al., 2023).

When compared to existing schemes, as illustrated in Table 5, our protocol requires the smallest number of transmitted bits. This reduction is achieved through optimized message structures and efficient encoding of authentication data, which minimizes the bandwidth consumption and accelerates the authentication process. The lower communication cost not only enhances the protocol's scalability but also contributes to reduced latency, which is crucial for time-sensitive UAV operations (Dogan et al., 2023).

Table 4: Our authentication protocol memory consumption



Operations	RAM in KB	Time
Hash	0.048	1 (*in ms*)
Encryption	0.143	1.3 (*in ms*)
Decryption	-	1 (*in ms*)
XOR	-	10 (*in ps*)

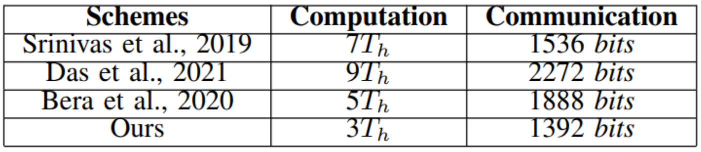
➢ ***Computation Cost Analysis:***

The computational efficiency of the Secure Authentication Protocol is a testament to its suitability for deployment in resource-constrained UAV devices. During the authentication phase, the protocol's encryption and decryption processes execute in approximately one millisecond on the Raspberry Pi 4 Model B. This rapid execution is critical for maintaining real-time responsiveness in UAV communications. Furthermore, during the registration phase, the UAV device similarly spends about one millisecond encrypting and decrypting messages, ensuring a seamless and swift onboarding process (Dogan et al., 2023).

The protocol also incorporates ECC for secure data transmission between BS and server devices. The creation and encryption of blocklists using ECC operations require an average of 75 milliseconds, a duration that remains acceptable given the enhanced security benefits provided by ECC. In terms of memory consumption, the protocol occupies approximately 15% of the UAV device's RAM, with the registration and authentication phases accounting for 6% and 9% of memory usage, respectively. This efficient memory utilization underscores the protocol's lightweight nature, making it well-suited for devices with limited memory resources (Dogan et al., 2023).

The underlying cryptographic mechanisms, including hash functions, encryption, decryption, and XOR operations, are meticulously optimized to minimize computational complexity. The time required for each operation, denoted as $(\boldsymbol{T_h})$ for hash computations and $(\boldsymbol{T_x})$ for XOR operations, is carefully managed to ensure that the protocol remains both secure and efficient. As depicted in Table 4, our scheme achieves a superior computational complexity compared to other authentication protocols, primarily due to the reduced number of cryptographic operations and the streamlined processing of authentication messages (Dogan et al., 2023).

Table 5: Cost Comparisons



Schemes	Computation	Communication
Srinivas et al., 2019	$7T_h$	1536 *bits*
Das et al., 2021	$9T_h$	2272 *bits*
Bera et al., 2020	$5T_h$	1888 *bits*
Ours	$3T_h$	1392 *bits*

The comprehensive analysis of both communication and computational costs reveals that the proposed Secure Authentication Protocol outperforms existing models in several key aspects. The reduced communication overhead ensures that the protocol is highly efficient in terms of bandwidth utilization, while the minimized computational costs guarantee swift authentication processes with low energy consumption. These attributes are particularly advantageous for UAV networks, where maintaining operational efficiency and prolonging device lifespans are critical considerations (Dogan et al., 2023).

Moreover, the lightweight design of our protocol facilitates scalability, allowing for the seamless integration of a large number of UAVs within the network without imposing significant resource burdens. This scalability is further enhanced by the protocol's ability to maintain low latency and high authentication success rates, even under high-density network conditions. Consequently, the proposed scheme not only meets but exceeds the performance benchmarks set by existing authentication models, positioning it as a superior choice for secure UAV communications (Dogan et al., 2023).

The performance analysis presented in this chapter substantiates the efficacy of the proposed Secure Authentication Protocol in addressing the computational and communication challenges inherent in UAV networks. Through meticulous comparative evaluations and empirical testing on resource-constrained devices, the protocol has demonstrated significant advantages over existing authentication schemes. The optimized computational overhead, coupled with minimal communication costs, underscores the protocol's suitability for deployment in real-world UAV applications. Furthermore, the protocol's scalability and efficiency ensure that it can accommodate the growing demands of expansive UAV networks, thereby contributing to the advancement of secure and reliable UAV communication infrastructures (Dogan et al., 2023).

Note of Clarification: The communication and computational cost analysis presented in this thesis is designed to quantify the fundamental per-session processing and communication overhead of the dynamic identity authentication protocol, specifically for an individual session between a single UAV and a base station. The reported values aim to demonstrate how lightweight and efficient the protocol is at the session level. The additional communication and coordination costs unique to the dynamic structure of a multi-UAV network arise in phases such as the SABEC layer, the leader election mechanism, and the consensus processes, which are addressed separately in the thesis. Therefore, focusing the cost analysis on a UAV–BS session allows for isolating and measuring the protocol's baseline unit cost, which can subsequently serve as a fundamental metric when calculating the aggregated total cost in multi-UAV scenarios, depending on the number of sessions and the dynamics of the network topology. The distinction between a UAV network and a single UAV becomes critical in how the protocol scales and manages this baseline unit communication load across simultaneous and sequential sessions involving multiple UAVs and BSs in a dynamic environment. A multi-UAV network introduces additional overhead and challenges beyond a single session: for example, the total communication load increases with the inclusion of leader election messages, clustering data, and consensus messages, and this varies depending on the network size and the rate of topological changes. The strength of the protocol in multi-UAV networks lies in minimizing these additional loads through low-latency leader communication flows and lightweight consensus mechanisms (e.g., LBFT), thereby adding a proportional and manageable overhead on top of the fundamental UAV–BS session cost.

In this context, the values provided in the communication cost analysis represent the minimal unit communication cost per session. The assessment of the actual load in dynamic multi-UAV networks is derived from scaling this unit cost according to the number of sessions, the clustering structure, and the dynamic management mechanisms of the protocol. The architecture proposed in the thesis is precisely designed to support this scalability and to ensure secure communication within highly mobile UAV networks that exhibit variable connectivity persistence.

6.5 Summary

We proposed a practical and efficient cryptographic protocol to ensure secure communication between two UAV devices and also UAV device and base station for the UAV environment. The presented work was applied and tested on a scenario, compared to the prior works, and the results were analysed in terms of security. Through the performance evaluation, we have demonstrated that the protocol is robust against attacks. We performed a formal and informal verification of the protocol as well as calculated its computational overhead. Our proposed solution for the UAVs network solved the critical security issues present in the environment. It also provided a comprehensive performance analysis of the proposed Secure Authentication Protocol, focusing on its efficiency in both computational and communication costs within UAV networks. By benchmarking against existing authentication models, the analysis demonstrated significant advantages in the proposed scheme's design. The experimental setup utilized off-the-shelf devices, specifically the Raspberry Pi 4 Model B, to reflect the resource-constrained nature of UAV operations. The performance evaluation employed AES encryption and ECC for secure communication, while metrics such as execution time and memory consumption were systematically measured. Communication costs were assessed, revealing that the proposed protocol requires fewer transmitted bits during the authentication phase compared to existing schemes, thereby enhancing bandwidth efficiency. Similarly, the computational cost analysis indicated rapid encryption and decryption times, with low memory usage, underscoring the protocol's suitability for resource-limited devices.

Overall, the results confirmed that the Secure Authentication Protocol outperforms traditional models, offering lower computational and communication overheads. This positions the protocol as an effective and practical solution for secure UAV communications, paving the way for its future application in real-world scenarios. The findings emphasize the protocol’s scalability, operational efficiency, and resilience against various security threats, making it a promising choice for enhancing the integrity and confidentiality of UAV network communications.

Chapter 7

A Secure and Adaptive Blockchain-Enabled Coordination (SABEC) Protocol for UAVs Network

The integration of blockchain technology into Unmanned Aerial Vehicle (UAV) networks represents a pivotal advancement in addressing the inherent challenges associated with secure and efficient multi-drone collaboration (Kumar et al., 2021; Chen et al., 2023). As drone swarm technology proliferates across diverse industrial sectors (including surveillance, delivery services, disaster management, and environmental monitoring) the demand for robust communication and coordination mechanisms intensifies (Kurt et al., 2021; Zhou et al., 2020). The deployment of drone swarms enhances operational efficiency, allowing for real-time data collection, expansive coverage, and rapid response capabilities (Phadke et al., 2023; Aldossri et al., 2024). However, the inherent characteristics of UAV networks, such as high mobility, dynamic mission environments, and the necessity for real-time coordination, introduce significant challenges in ensuring secure and efficient communication and collaboration among drones within a swarm (Ganesan et al., 2024). Central to this evolution is the necessity to establish a secure consensus protocol that not only facilitates seamless interaction among UAVs but also fortifies the network against malicious entities, such as Byzantine drones, which can undermine the integrity and reliability of swarm operations (Medhi et al., 2023; Thakur et al., 2023).

Traditional consensus mechanisms often fall short in dynamic and resource-constrained environments characteristic of UAV networks (Abegaz et al., 2023). One of the foremost challenges in UAV networks is maintaining robust security amidst frequent topology changes and the presence of potentially malicious nodes, commonly referred to as Byzantine drones (Cui et al., 2024). These drones can compromise network integrity by engaging in disruptive behaviours, such as hijacking, data corruption, or unauthorized access, thereby undermining the effectiveness of swarm operations (Yahuza et al., 2021). Consequently, an operating UAV network functions as a Byzantine distributed system, where both the physical structure and the trustworthiness of nodes are subject to continuous fluctuations (Onukak et al., 2024)

Addressing these challenges necessitates the development of sophisticated mechanisms for global network management, ensuring rational allocation of network resources, and dynamic reconfiguration of trusted networks (Xiao et al., 2022). Traditional consensus protocols, often centralized and resource-intensive, fall short in adapting to the highly dynamic and resource-constrained environments characteristic of UAV networks (Cheng et al., 2022). Moreover, the open and ad hoc nature of UAV communications exacerbate vulnerability to a wide array of cyber threats, including Denial-of-Service (DoS) attacks, replay attacks, impersonation attempts, and Sybil attacks (BinSaeedan et al., 2023). Additionally, the energy inefficiency and computational overhead associated with conventional authentication and consensus protocols exacerbate the operational constraints of UAV devices, thereby impeding their performance and longevity (Xiong et al., 2024).

The subsequent sections of this chapter delve into the comprehensive architecture of the proposed consensus protocol, detailing its implementation strategies, security assurances, and performance metrics (Syed et al., 2022). Through rigorous simulation and empirical testing, the protocol's efficacy is evaluated against existing consensus models, highlighting its superior performance in terms of computational efficiency, communication overhead, packet delivery rate, and resilience to Byzantine threats (Juárez et al., 2023; Giuliari et al., 2024). By addressing the critical security and operational challenges inherent in UAV networks, the proposed blockchain-enhanced secure consensus protocol paves the way for more reliable, efficient, and secure multi-drone collaborations in diverse real-world applications (Karmakar et al., 2024).

In this context, we propose an innovative Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) designed to fortify UAV networks against these multifaceted security threats while optimizing operational efficiency. Our protocol leverages the decentralized and immutable properties of blockchain technology to establish a trusted framework for consensus achievement, thereby ensuring secure and reliable multi-drone collaboration. The protocol incorporates a two-stage consensus mechanism (data consensus and decision consensus) facilitated by Fuzzy C-Means (FCM) (Birtolo et al., 2013) clustering and global trustworthiness assessment algorithms. By incorporating a dynamic Proof of Work (PoW) mechanism (Gervais et al., 2016), the protocol incentivizes legitimate UAVs to engage in computationally intensive tasks that validate their authenticity, thereby deterring malicious attempts to disrupt network operations. This dual-phase approach not only enhances the security and reliability of consensus processes but also ensures scalability and adaptability in dynamic mission environments. Furthermore, the proposed protocol employs a hierarchical clustering algorithm to dynamically select leader drones within predefined clusters, enhancing the scalability and fault tolerance of the network. These leader drones are responsible for aggregating and transmitting status control information to a centralized server, which consolidates the data through a consensus mechanism before recording it on the blockchain. This structured approach not only optimizes resource utilization but also ensures the real-time adaptability of the network to changes in topology and node reliability.

This chapter elucidates the comprehensive design, implementation, security analysis, and performance evaluation of the proposed Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC). Through rigorous simulation and empirical testing, we demonstrate the protocol's superiority over existing authentication and consensus models in terms of computational efficiency, communication overhead, packet delivery rate, and fault tolerance. The ensuing sections delve into the architectural overview, detailed implementation strategies, robust security assurances, and exhaustive performance metrics, underscoring the protocol's efficacy in addressing the unique challenges of UAV network management.

7.1 Overview of the SABEC Protocol

Unmanned Aerial Vehicle (UAV) networks have emerged as pivotal components in a myriad of applications, ranging from surveillance and disaster management to environmental monitoring and delivery services (Hildmann et al., 2019). The inherent advantages of UAVs (such as mobility, flexibility, and the ability to operate in diverse environments) render them indispensable in both civilian and military contexts. However, the deployment of large-scale UAV networks introduces a spectrum of complex challenges that impede their operational efficacy (Fan et al., 2024). Among these challenges, secure and efficient communication and coordination stand paramount, particularly in mission-critical scenarios where real-time data exchange and reliable decision-making are essential. The dynamic nature of UAV networks, characterized by high node mobility, fluctuating node densities, and the ever-present threat of Byzantine faults (malicious or malfunctioning nodes that can compromise network integrity) exacerbates these challenges (Lakew et al., 2020). Traditional coordination protocols often falter under such conditions, succumbing to excessive coordination overhead, diminished scalability, and vulnerability to sophisticated cyber-attacks (Hnamte et al., 2024). These limitations underscore the exigent need for advanced protocols that can adeptly navigate the multifaceted demands of modern UAV deployments. In response to these imperatives, the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) has been meticulously developed to enhance the performance, security, and reliability of UAV networks. SABEC represents a paradigm shift in UAV network management by integrating blockchain technology with adaptive trust management and hierarchical clustering algorithms. This confluence of technologies facilitates a robust framework capable of dynamic network reconfiguration, ensuring that only trustworthy nodes participate in critical operations and that the network can swiftly adapt to changing conditions and emerging threats.

Central to SABEC's architecture is its cross-layer design, which harmoniously operates across multiple network tiers to enable seamless information exchange and task collaboration among UAV nodes. The protocol's innovative two-tier consensus mechanism (comprising Data Consensus and Decision Consensus stages) leverages lightweight Byzantine Fault Tolerance (LBFT) algorithms to achieve rapid and secure consensus with minimal computational overhead. Furthermore, SABEC employs a Private, Permissioned Blockchain (PPB) to maintain an immutable ledger of Trust

Assessment Transactions (TATs), thereby ensuring transparency, traceability, and accountability within the network. This chapter provides an overview of the SABEC protocol, elucidating its architectural framework, core components, and operational mechanisms. It delves into the intricate interplay between SABEC's hierarchical clustering algorithms and blockchain integration, highlighting how these elements collectively address the critical challenges of coordination overhead, scalability, and security in UAV networks. Additionally, the chapter examines the protocol's efficacy through rigorous simulation experiments, demonstrating SABEC's superior performance in key metrics such as packet delivery rate, routing overhead, end-to-end delay, and energy consumption compared to traditional routing protocols. By systematically exploring the design principles and functional attributes of SABEC, this chapter aims to furnish a detailed understanding of its contributions to the field of UAV network management. It underscores SABEC's role in advancing secure and efficient multi-drone collaboration, thereby paving the way for its widespread adoption in diverse and demanding operational environments. Through this comprehensive examination, readers will gain insights into the innovative solutions SABEC offers to the persistent challenges faced by modern UAV networks, affirming its significance as a cornerstone in the evolution of autonomous aerial systems.

The proposed SABEC Protocol is meticulously architected to address the intrinsic challenges of mission-oriented UAV networks, characterized by high node mobility, dynamic mission environments, and the pervasive threat of Byzantine drones. We implemented a new practical and dynamic protocol using PoW consensus to generate the difficulty factor in the UAV network and the dynamic clustering selection frequency. This approach provides drones with enhanced accuracy, usability and mitigates the risk of malicious attackers/ Byzantine drones sharing tampered data. Traditional consensus mechanisms, while effective in certain contexts, are often encumbered by high computational and communication overheads, rendering them unsuitable for the resource-constrained and highly dynamic nature of UAV networks. At the heart of our protocol lies the integration of a lightweight blockchain system, which serves as an immutable ledger for recording all consensus-related transactions and decisions. This decentralized approach eliminates single points of failure, enhancing the overall resilience and security of the network. The blockchain based SABEC framework is complemented by a two-stage consensus mechanism (data consensus and decision consensus) that ensures both local and global agreement on network states and configurations.

- ***Data Consensus Stage:***

In the initial stage, each UAV node monitors the forwarding behaviour of its neighbouring nodes and generates local state record transactions. These transactions encapsulate assessments of node trustworthiness based on observed behaviours, such as message forwarding accuracy, energy consumption patterns, and adherence to network protocols. Utilizing Fuzzy C-Means (FCM) clustering, nodes categorize their peers into clusters based on trust metrics, facilitating the identification of reliable and potentially malicious nodes within their vicinity.

In the Data Consensus stage of the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC), the primary objective is to establish a reliable and accurate assessment of each UAV node's trustworthiness within the network. This stage is critical, as it lays the foundation for secure and efficient collaboration among UAVs by ensuring that only trustworthy nodes participate in subsequent network operations. To achieve this, each UAV node actively monitors the behaviour of its neighbouring nodes through continuous observation of their forwarding activities and compliance with network protocols. This monitoring encompasses various parameters, including message forwarding accuracy, energy consumption patterns, response times, and adherence to communication protocols. By scrutinizing these aspects, a UAV can detect anomalies or deviations that may indicate malicious intent or compromised functionality. Once sufficient data is collected, each UAV generates local state record transactions. These transactions encapsulate the trust assessments of neighbouring nodes based on the observed behaviours. The local state record transactions are structured data packets that include the following information: *Node Identifiers:* Unique IDs of the observed neighbouring nodes. *Trust Metrics:* Quantitative evaluations of each node's behaviour, derived from parameters such as packet delivery ratios, latency, and error rates. *Timestamp:* The time at which the observation was made, ensuring temporal relevance. *Signature:* A cryptographic signature to authenticate the origin of the transaction and prevent tampering.

To process and analyse the trust metrics effectively, SABEC employs the Fuzzy C-Means (FCM) clustering algorithm. FCM is a form of soft clustering that allows each node to belong to multiple clusters with varying degrees of membership, providing a nuanced understanding of trust levels. Through FCM, UAVs categorize neighbouring nodes into clusters such as "Highly Trusted," "Moderately Trusted," "Uncertain," and "Potentially Malicious." This granular classification enables UAVs to make informed decisions about which nodes to interact with and trust in collaborative tasks. The use of FCM in the Data Consensus stage offers several advantages. The algorithm accommodates the dynamic nature of UAV networks by continuously updating trust levels as nodes move and their behaviours change. By allowing partial membership in multiple clusters, FCM effectively handles ambiguous or incomplete data, which is common in volatile network environments. FCM's computational efficiency ensures that trust assessments can be performed quickly, even as the network scales up in size. After clustering, the UAV nodes share their local state record transactions with neighbouring nodes, facilitating a mutual exchange of trust assessments. This peer-to-peer dissemination ensures that trust evaluations are not solely dependent on individual observations but are corroborated by multiple nodes, enhancing the reliability of the data consensus.

To maintain security during this exchange, all local state record transactions are encrypted and signed using each UAV's private key. The encryption safeguards the confidentiality of the trust data, while the signature allows recipients to verify the authenticity of the sender, preventing impersonation attacks.

➢ ***Decision Consensus Stage:***

The second stage involves aggregating the data consensus results across the network to achieve a unified decision on node trustworthiness and network configuration. Authorized proxy nodes, elected dynamically through the clustering algorithm, participate in this stage by consolidating local trust assessments and performing a global trustworthiness evaluation. Algorithms such as Fuzzy C-Means (FCM) clustering and global trustworthiness assessment ensure that only trusted nodes are included in the consensus process, thereby mitigating the influence of Byzantine drones.

Building upon the foundation established in the Data Consensus stage, the Decision Consensus stage aims to achieve a unified agreement on the overall trustworthiness of nodes and determine the network's configuration for optimal performance. This stage involves aggregating local trust assessments from individual UAVs to form a global view of the network's trust landscape. Central to this stage is the role of Authorized Proxy Nodes (APNs), which are dynamically elected leader drones within their respective clusters. The election of APNs is based on criteria such as trust levels, computational capabilities, and energy reserves, ensuring that the most suitable nodes assume leadership roles. The hierarchical clustering algorithm facilitates this process by organizing UAVs into manageable clusters and identifying APNs efficiently. The responsibilities of APNs in the Decision Consensus stage include *Aggregation of Trust Assessments:* APNs collect local state record transactions from UAVs within their clusters, consolidating the local trust data into a comprehensive cluster-level assessment. *Global Trustworthiness Evaluation:* APNs apply advanced algorithms, such as enhanced FCM clustering and Global Trust Assessment Functions, to evaluate the trustworthiness of nodes across the entire network. This evaluation considers both the local assessments and inter-cluster interactions. *Consensus Facilitation:* APNs engage in a consensus protocol based on a lightweight Byzantine Fault Tolerance (LBFT) algorithm. This protocol ensures that even in the presence of Byzantine drones (malicious nodes that may provide false information), the network can reach a reliable consensus on node trustworthiness. The LBFT algorithm is particularly suited for UAV networks due to its low computational and communication overhead, which is critical given the resource constraints of UAVs. It allows the network to tolerate a certain number of faulty or malicious nodes without compromising the consensus process.

During the consensus protocol, APNs exchange trust assessments and proposed network configurations with one another. They validate the received information using cryptographic techniques and cross-referencing with their local data. The consensus is reached when a sufficient number of APNs agree on the trust evaluations and network configuration, adhering to predefined consensus rules.

The consensus outcomes are then recorded as new blocks in the blockchain, representing the updated configuration information of the UAV network. This immutable record ensures transparency, traceability, and accountability, preventing unauthorized alterations and enhancing the network's overall trustworthiness.

The Data Consensus and Decision Consensus stages are intricately linked, forming a cohesive process that ensures both local and global trust assessments are accurate and reliable. The Data Consensus stage focuses on micro-level observations and assessments, while the Decision Consensus stage elevates these findings to a macro-level understanding of the network's trust dynamics. This two-tier consensus mechanism provides robust defences against various security threats: *Byzantine Drones* (by requiring consensus at both the local and global levels, the protocol mitigates the impact of malicious nodes attempting to spread false trust assessments), *Sybil Attacks* (the use of unique node identifiers, cryptographic signatures, and blockchain recording prevents attackers from creating multiple fake identities to influence the consensus), and *Replay Attacks* (timestamps and nonces in transactions ensure that outdated or duplicated messages are recognized and discarded).

In summary, the Data Consensus stage establishes a reliable foundation of local trust assessments through vigilant monitoring and sophisticated clustering algorithms. The Decision Consensus stage builds upon this foundation by aggregating local assessments into a global consensus, facilitated by dynamically elected Authorized Proxy Nodes and secured through blockchain technology. Together, these stages enable the SABEC protocol to maintain a secure, efficient, and adaptive UAV network, capable of withstanding dynamic mission environments and sophisticated cyber threats. By meticulously orchestrating the processes of trust assessment, consensus building, and blockchain recording, SABEC ensures that UAV networks can operate with high levels of integrity and reliability. The protocol's design addresses the critical need for secure coordination in mission-critical applications, paving the way for the broader adoption of UAV networks in diverse operational contexts.

- ***Clustering and Leader Election:*** To enhance scalability and manageability, the protocol employs a hierarchical clustering algorithm that periodically elects leader drones within predefined clusters. These leader drones are responsible for aggregating local trust assessments, transmitting them to a centralized server, and facilitating the consensus process. The dynamic clustering mechanism ensures that the protocol can adapt to frequent topology changes and varying node reliability, maintaining network integrity and operational efficiency.

- ***Blockchain Integration:*** Blockchain technology is pivotal in our protocol, providing a decentralized and secure means of recording consensus transactions and decisions. Each new block in the blockchain contains aggregated trust assessments and configuration information, ensuring that the network's state is consistently and securely updated. The blockchain's immutable nature ensures that all consensus decisions are permanently recorded, preventing tampering and enhancing the network's resilience against malicious attacks (Saroopa et al., 2024).

- ***Lightweight Storage and Efficiency:*** Acknowledging the resource constraints inherent in UAV devices, the protocol is designed to employ a lightweight storage blockchain. This design choice minimizes computational and storage overheads by recording only essential decision consensus results, discarding intermediate data transactions that are no longer necessary. This approach ensures efficient use of UAV resources, prolonging operational lifespan and maintaining high performance even in large-scale network deployments.

- ***Security and Trust Management:*** The protocol's security framework is robust, incorporating multiple layers of protection against a wide array of cyber threats. By leveraging dynamic secret key generation, one-way hash functions, and blockchain-based trust management, the protocol ensures that only legitimate and trusted nodes participate in network operations. The two-stage consensus mechanism further fortifies the network against Byzantine attacks, ensuring that trustworthiness assessments are both accurate and resilient to manipulation.

The blockchain-enhanced secure consensus protocol offers a comprehensive solution for managing the dynamic and security-sensitive nature of mission-oriented UAV networks. By integrating blockchain technology with a sophisticated two-stage consensus mechanism and dynamic clustering algorithms, the protocol ensures secure, scalable, and efficient multi-drone collaboration. This architectural innovation not only addresses the critical challenges of secure consensus achievement and resource optimization but also enhances the fault tolerance and operational reliability of UAV networks, paving the way for their widespread adoption in diverse real-world applications.

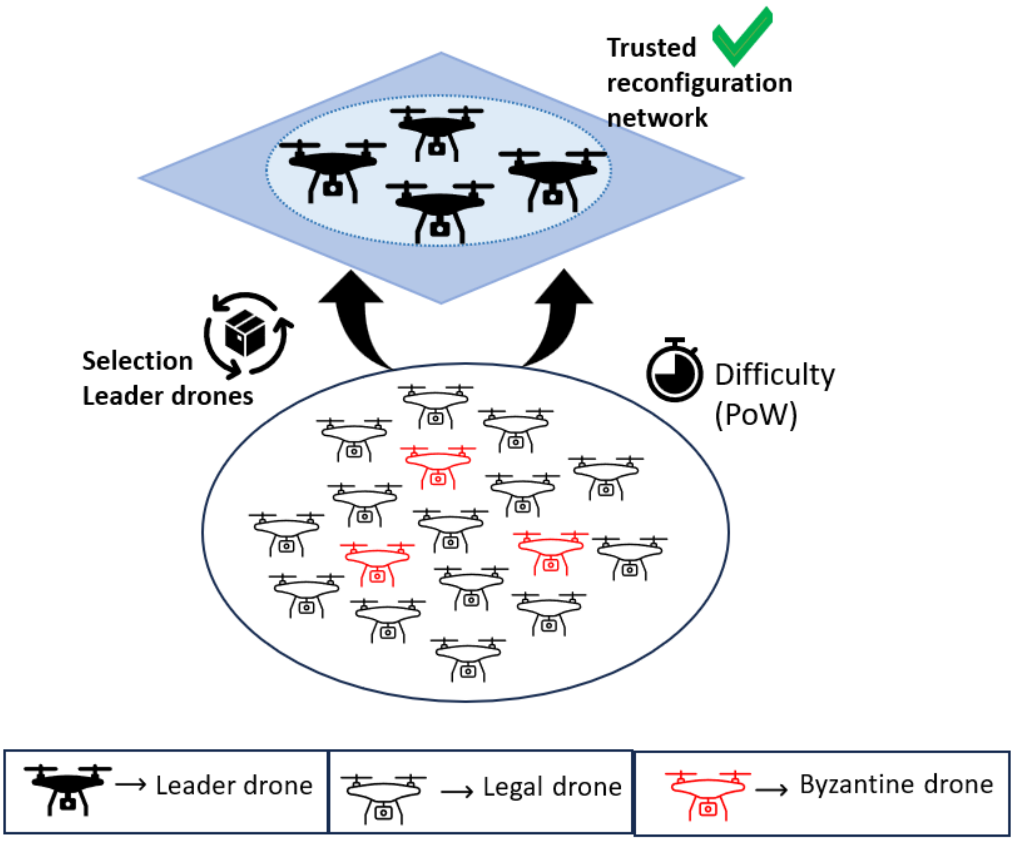


Figure 14: Leader drone selection in the UAV network

The proposed framework in Figure 14 that effectively addresses the dynamic characteristics of Unmanned Aerial Vehicle (UAV) network topologies and the variable reliability of network nodes. To achieve this objective, the authors harness the potential of blockchain technology, specifically employing the Proof-of-Work (PoW) technique, to establish a secure and collaborative environment for drone networks deployed in product-related activities. By leveraging PoW, each drone undergoes a rigorous network selection process, validating its unique identity by resolving complex cryptographic problems. Consequently, this stringent mechanism effectively thwarts unauthorized or malicious entities from infiltrating the system, particularly safeguarding against Byzantine drones and other potential security threats. Crucially, this process serves as the fundamental building block for constructing a secure network, wherein only selected leader drones possess the privilege of transmitting data to the central server.

The leader drones emulate the data transmission behaviour exhibited by neighbouring drones within their respective clusters, relaying this information to the server. Subsequently, the server assesses and scores the received data, ultimately generating conclusive outcomes. These results are then transmitted to the blockchain structure at the application layer, culminating in an efficient, lightweight, and reliable consensus on decision-making. The proposed protocol offers a comprehensive solution for enabling collaborative consensus among drones and facilitating the safe execution of their planning tasks. The framework fills crucial gaps in existing research by presenting innovative contributions to practicality, efficiency, and trust management within UAV reliable networks. The method devised effectively tackles UAV networks' dynamic nature and enables hierarchical logical networks' dynamic reconfiguration. An adaptive and efficient consensus mechanism is introduced to effectively handle the UAV network's changing topology and nodes' evolving reliability. By leveraging blockchain technology, global health assessments of network nodes are systematically recorded, facilitating automatic reconfiguration of the hierarchical logical network based on the most up-to-date information. This robust mechanism validates future operations' integrity, ensuring the collected data's authenticity and security. The proposed protocol employs a clustering algorithm method, periodically selecting district centres based on neighbouring nodes. The lead devices within dynamically updated clusters form an upper-layer network responsible for network operations in stages. This method optimizes resource utilization, minimizes faulty nodes' involvement in consensus operations, and enhances fault tolerance within the network.

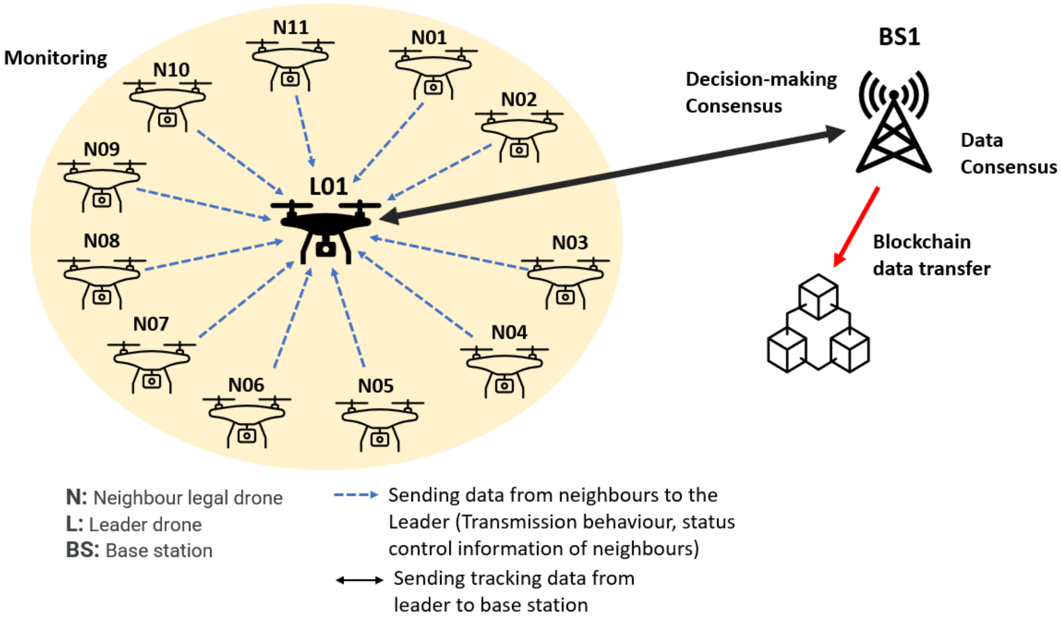

Monitoring
N11
N01
N10
N02
N09
L01
N08
N03
N07
N04
N06
N05
BS1
Decision-making Consensus
Data Consensus
Blockchain data transfer
N: Neighbour legal drone
L: Leader drone
BS: Base station
Sending data from neighbours to the Leader (Transmission behaviour, status control information of neighbours)
Sending tracking data from leader to base station

Figure 15: The architecture of the blockchain-enabled protocol in the UAVs

Figure 14 and 15 illustrates the conceptual model of a blockchain-powered, dynamically configurable network, elucidating the system's fundamental architecture. They present a distributed blockchain system designed to establish an adaptable and reliable decision-making mechanism for Unmanned Aerial Vehicle (UAV) networks. This system achieves its objectives by dynamically constructing a well-defined enclave of trusted devices within the UAV network. The underlying blockchain framework incorporates a consensus-based decision-making structure that continuously assesses the trustworthiness of network nodes, relying on real-time data pertaining to state changes in the transmission activities of prominent drones and neighbouring devices. To maintain the integrity of the network, the blockchain system employs a mechanism that actively prevents the inclusion of untrusted nodes. This is accomplished through the dynamic aggregation of commitments from recognized leader drones and the periodic monitoring of the overall health status of network nodes. Additionally, to gain entry into the selection pool, Byzantine drones, denoting unreliable devices, are required to solve a computationally challenging Proof of Work (PoW) problem, a task rendered formidable for illicit devices. These two dynamic challenges serve as robust deterrents against the infiltration of untrusted devices into the network. Furthermore, the UAV nodes exhibit adaptive behaviour, enabling them to reconfigure the trusted hierarchical network architecture as needed and establish secure communication pathways through the blockchain, which undergoes continuous updates.

In summary, the proposed Blockchain-Enhanced Secure Consensus Protocol offers a comprehensive solution for managing the dynamic and security-sensitive nature of UAV networks. By combining blockchain technology with a two-stage consensus mechanism and dynamic clustering algorithms, the protocol ensures secure, scalable, and efficient operations, thereby enhancing the reliability and longevity of mission-oriented UAV deployments.

7.2 System Architecture of the SABEC Protocol

The architecture of *SABEC* is meticulously designed to operate across multiple network layers/tiers, facilitating seamless information exchange and task collaboration among UAV nodes. The protocol integrates blockchain technology to enhance security and trust management, ensuring that only reliable nodes participate in the network's upper management layer. The architecture is compartmentalized into distinct tiers, each responsible for specific functionalities essential to the framework’s performance and reliability.

Signal Transmission and Access Coordination Tiers: At the foundational signal transmission tier, the Proximal Node Discovery and Monitoring Component protocol (PDMC) is responsible for the accurate detection and continuous monitoring of adjacent UAV nodes. PDMC employs enhanced signal processing techniques to identify neighbouring nodes reliably, even in environments with high interference and node mobility. This component protocol establishes a dependable foundation for subsequent routing decisions by maintaining up-to-date neighbour tables and monitoring the forwarding behaviours of adjacent nodes.

Data Coordination Tiers: The data coordination tier integrates three pivotal component protocols that collectively manage local network and cross-network communications:

- ***Localized Trust Coordination Component protocol (LTCC):*** This component protocol manages local zone communications by evaluating and prioritizing coordination paths through trusted nodes based on real-time assessments. LTCC minimizes internal zone coordination overhead by selecting optimal paths that reduce latency and enhance data delivery efficiency.
- ***Hierarchical Trust-Based Coordination Component protocol (HTCC):*** Facilitating external communications, HTCC establishes hierarchical coordination paths that connect different network zones through trusted gateway nodes. HTCC employs dynamic clustering algorithms to form and manage hierarchical structures, thereby enhancing scalability and reducing coordination complexity.
- ***Secure Border Coordination Component protocol (SBCC):*** Overseeing data transmission across network boundaries, SBCC ensures secure and efficient coordination between zones. SBCC integrates blockchain-based verification mechanisms to authenticate coordination information and prevent the dissemination of malicious data.

Service Management and Control Tiers: At the pinnacle of the architecture, the service management tier incorporates the Secure and Adaptive Blockchain-Enabled Coordination Protocol (*SABEC*). *SABEC* serves as the core component for managing trust and coordination within the network. It maintains an immutable ledger of node trustworthiness and network configurations, enabling real-time network reconfiguration based on trust assessments and operational requirements. The control coordination tier ensures that data transmitted across the network adheres to predefined security protocols and operational guidelines, further fortifying the network's integrity.

Implementing *SABEC* involves a sophisticated integration of blockchain technology with traditional networking protocols, tailored to the unique constraints and requirements of UAV networks. *SABEC* employs a *Private, Permissioned Blockchain (PPB)* designed specifically for UAV networks. Each UAV node is assigned a unique cryptographic identity, comprising a public-private key pair and a unique identifier (UID). The PPB records *Trust Assessment Transactions (TATs)*, encapsulating node behaviour metrics, trust scores, and operational statuses. Unlike conventional blockchains, *SABEC*'s PPB retains only essential consensus results and aggregated trust scores, significantly reducing storage overhead and enhancing scalability.

SABEC utilizes a *Two-Tier Consensus* mechanism (*TTC*) to ensure efficient and secure network reconfiguration:

- *Trust Evaluation Tier (Data Consensus Stage):* In this initial tier, nodes perform real-time monitoring of proximal nodes' behaviours using the *LTCC* and *HTCC* component protocols. Nodes generate TATs based on observed behaviours, which are then broadcasted to authorized nodes within the upper management network. This tier employs a *Lightweight Byzantine Fault Tolerance (LBFT)* algorithm to achieve rapid consensus on trust assessments with minimal computational overhead.
- *Network Coordination Tier (Decision Consensus Stage):* The second tier involves the aggregation and validation of TATs through the blockchain's smart contracts. Authorized nodes execute smart contracts to finalize consensus on trust scores and determine necessary network reconfigurations. This tier ensures that only trusted nodes are involved in critical network operations, thereby maintaining the integrity and reliability of the UAV network.

SABEC's dynamic reconfiguration process is pivotal in maintaining network resilience and performance. The process involves:

- *Isolation of Compromised Nodes:* Nodes identified as malicious or unreliable through trust assessments are systematically excluded from the network, preventing them from participating in coordination and data forwarding.
- *Election of Trusted Nodes:* Reliable nodes are elected to form the upper management network, responsible for overseeing network operations and facilitating secure inter-zone coordination. This election is based on aggregated trust scores and regional representativeness.
- *Hierarchical Structuring:* The upper management network adopts a hierarchical structure, utilizing the Fuzzy C-Means Clustering Algorithm (FCMCA) to dynamically form clusters based on node proximity and trust levels. This hierarchical approach optimizes resource allocation, minimizes coordination redundancy, and enhances overall network scalability.

7.2.1 Fuzzy C-Means (FCM) clustering Algorithm

Fuzzy C-Means (FCM) clustering algorithm plays a pivotal role in enhancing the secure communication and collaboration capabilities of UAV (Unmanned Aerial Vehicle) networks, particularly in dynamic and mission-critical scenarios (Cumino et al., 2019). FCM is a type of soft clustering technique where data points can belong to more than one cluster, allowing a more nuanced grouping compared to traditional hard clustering methods (Thomas et al., 2024). This capability is crucial for UAV environments where drone behaviour can vary, and complete certainty is difficult to achieve. The Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) utilizes the FCM algorithm for UAV clustering to ensure effective and reliable coordination. Specifically, FCM is employed during the Data Consensus Stage to categorize UAV nodes based on trust metrics such as message forwarding accuracy, energy consumption patterns, and adherence to network protocols. This classification helps to distinguish reliable UAVs from potentially malicious ones, thereby enhancing the trustworthiness of the network (Verma et al., 2022).

In the Decision Consensus Stage, FCM clusters are leveraged to facilitate global trust evaluations by consolidating local trust assessments from different UAV nodes. The clusters generated by FCM assist in electing authorized proxy nodes, which then aggregate the results to form a global assessment of network states and configurations (Kafetzis et al., 2022). This helps ensure that only trustworthy nodes participate in the network's consensus process, thereby mitigating the risk of Byzantine drones compromising network integrity.

One of the primary advantages of FCM in UAV networks is its flexibility. Since UAV nodes can belong to multiple clusters with varying degrees of membership, FCM allows a more flexible representation of each UAV's role and trust level within the network. This is particularly advantageous in UAV networks where conditions such as node mobility, communication reliability, and node performance frequently change (Merah et al., 2023). Additionally, FCM helps in reducing the risks associated with Byzantine nodes, which are characterized by malicious behaviour or faults that can undermine the system's reliability. By clustering nodes based on trust metrics, FCM provides an effective approach to exclude or minimize the influence of unreliable nodes during critical stages of data consensus and decision making (Bharany et al., 2021).

FCM performance metrics(Performance Metrics and Byzantine Fault Tolerance)

The effectiveness of FCM clustering is evaluated using ***Silhouette_Score = (b - a) / max(a,b)*** where is a: Mean intra-cluster distance, b: Mean nearest-cluster distance. The algorithm incorporates Byzantine fault tolerance by ***Trust_Threshold = mean(TV) + α * std(TV)*** where is α: Security parameter (1.5-2.0), std: Standard deviation. Setting the threshold based on the mean and standard deviation allows the protocol to dynamically adjust to the distribution of trust values, enhancing resilience against Byzantine faults. The time complexity is ***O(N * C * I * D)*** where is N: Number of nodes, C: Number of clusters, I: Number of iterations, D: Dimension of feature vector.

The parameters and algorithms presented are correct and appropriately formulated for the implementation of the FCM algorithm within the SABEC protocol. They accurately reflect standard methodologies in fuzzy clustering and trust management, and their integration into the SABEC framework is logically sound. The detailed steps and formulas shown a robust foundation for dynamic trust assessment, efficient cluster formation, and resilience against Byzantine attacks in UAV networks.

This implementation in SABEC ensures a dynamic trust assessment, resilience against Byzantine attacks, efficient cluster formation, and adaptive network reconfiguration. The FCM algorithm's fuzzy approach particularly suits SABEC's requirements due to handling uncertainty in node behaviour, smooth transition between trust levels, robust against noisy data, and adaptive to dynamic network conditions.

The application of FCM in UAV networks provides a robust framework for ensuring the security and efficiency of multi-drone collaboration, particularly when integrated with blockchain technology as seen in SABEC. This integration addresses several of the traditional challenges in UAV coordination, such as high computational overhead, limited scalability, and susceptibility to sophisticated attacks (Karuppaiah et al., 2022). Future work could explore hybrid models that combine FCM with other machine learning techniques to further enhance decision-making capabilities in dynamic UAV networks. In conclusion, the use of FCM in UAV network clustering and trust management offers a sophisticated solution to the challenges posed by high node mobility and the risk of Byzantine faults. Its implementation within SABEC highlights the potential for advanced clustering algorithms to significantly improve the operational efficacy of autonomous aerial systems, thereby setting the foundation for future advancements in secure UAV coordination.

7.2.2 Drone Cluster Membership and Selection in SABEC

The FCM clustering also plays a significant role in leader election within UAV networks. SABEC employs a hierarchical clustering mechanism to elect leader drones periodically from within defined clusters, thereby improving network scalability and manageability (Rajput et al., 2021). Leader drones are responsible for aggregating trust assessments, facilitating the consensus process, and transmitting aggregated data to centralized servers. This dynamic clustering ensures the network can adapt to frequent topology changes and varying node reliability, thus maintaining the overall integrity and efficiency of operations. The SABEC protocol implements a sophisticated framework for validating and proving drone cluster membership through a multi-layered mathematical approach. This framework ensures secure, verifiable, and efficient cluster assignments while maintaining network integrity.

The fundamental membership verification is based on a fuzzy logic approach combined with blockchain-based validation. The primary membership vector *MV(i)* represents the degree of belonging for each drone *i* to available clusters, expressed as: $MV(i) = [\mu i1, \mu i2, ..., \mu ic]$ where is μij: Membership degree of drone i to cluster j, c: Number of clusters. This vector incorporates multiple parameters including spatial positioning, trust metrics, and performance indicators. The protocol employs a trust-weighted membership strength calculation, $MS(i,j) = \mu ij * w(Tij)$ where is w(Tij): Trust-weighted coefficient, Tij: Trust value of drone i in cluster j. This formulation ensures that membership assignment is influenced by both fuzzy clustering results and established trust metrics. For the Cluster Assignment Proof: $PC(i) = argmax(j=1 \text{ to } c)\{MS(i,j)\}$ where PC(i) is the primary cluster for drone i. Assignment Confidence is $AC(i) = MS(i,PC(i)) / \sum(j=1 \text{ to } c)MS(i,j)$.

Table 6.

```
Algorithm: Cluster Membership Validation
Input: Drone Di, Cluster Set C
Output: Validated Cluster Assignment and Proof
1: // Calculate Feature Vector
  F(i) = [Position(i), Energy(i), Trust(i), Performance(i)]
2: // Compute Distance Metrics
  for each cluster Cj in C:
    D(i,j) = ||F(i) - Centroid(j)||
3: // Calculate Membership Degrees
  for each cluster Cj in C:
    μij = 1 / ∑(k=1 to c)(D(i,j)/D(i,k))^(2/(m-1))
4: // Generate Proof
  Proof(i) = {
    DroneID: i,
    ClusterID: PC(i),
    MembershipVector: MV(i),
    Timestamp: t,
    Signature: Sign(H(MV(i)||t)) }
5: // Validate Proof
  if AC(i) ≥ threshold_membership &&
    ValidateSignature(Proof(i)) &&
    VerifyConsensus(Proof(i)):
    return VALID
  else:
    return INVALID
```

Leader Selection Metrics

The primary selection metric is calculated using a weighted composite score ***SS(i) = α1*MS(i,j) + α2*TR(i) + α3*PS(i)*** where is SS(i): Selection Score for drone i, MS(i,j): Membership Strength in cluster j, TR(i): Trust Rating, PS(i): Performance Score, α1, α2, α3: Weight coefficients where ∑αn = 1. The Membership Strength (MS); ***MS(i,j) = μij * w(Tij)***. The parameters are μij: Fuzzy membership degree, w(Tij): Trust-weighted coefficient, and Tij: Historical trust value. The characteristics features are reflecting drone's belonging degree to specific cluster, incorporates historical performance and accounts for spatial distribution. The Trust Rating calculation (TR); ***TR(i) = (∑(k=1 to n)TV(k,i)) / n * β***. The components are TV(k,i): Trust value from drone k to drone i, n: Number of evaluating drones, β: Trust decay factor ($0 < \beta \leq 1$). Peer evaluation impact, temporal relevance and network consensus are considered. The Performance Score (PS); ***PS(i) = w1*EC(i) + w2*CC(i) + w3*NS(i)*** where is EC(i): Energy Capacity, CC(i): Communication Capability, NS(i): Network Stability, and w1, w2, w3: Weight factors.

Dynamic Adjustment Mechanism*:** The Weight Adaptation formula is ***α_new = α_current + η * ΔP where is η: Learning rate, ΔP: Performance change. The Threshold Adjustment is ***threshold(t+1) = threshold(t) * (1 + λ*ΔE)*** where is λ: Adjustment coefficient, ΔE: Environmental change factor.

Cluster Head Selection*: *CH_score(i) = SS(i) * (E_current/E_max) * (1/D_average) where is E_current: Current energy level, E_max: Maximum energy capacity, D_average: Average distance to cluster members. Role Assignment formula is ***Role_fitness(i) = SS(i) * CF(i) * AF(i)*** where is CF(i): Capability Factor, AF(i): Availability Factor.

Proof of Work (PoW) and Leader Election

At the core of SABEC's architecture is the incorporation of a Proof of Work (PoW) mechanism, which serves as a fundamental pillar for safeguarding the network and incentivizing legitimate participation. In this context, UAVs aspiring to become leader drones within their respective clusters are required to solve computationally intensive cryptographic puzzles. The key distinction to be highlighted regarding PoW that is not implemented in the classical sense as seen in blockchain systems such as Bitcoin, where it serves to achieve decentralized ledger consensus through highly energy- and computation-intensive operations. Instead, the concept of PoW in SABEC has been adapted as a lightweight computational step that imposes a difficulty factor during leader drone selection within clusters. The primary aim of this design is to introduce an additional layer of security in the selection of drones that will undertake critical leadership roles and to ensure that only nodes demonstrating a certain level of computational effort are eligible for these roles. This PoW implementation does not involve the energy-demanding and resource-intensive structure characteristic of traditional PoW. It does not impose significant additional energy consumption during flight or introduce complex, time-consuming computational loads. Rather, a simple problem-solving task has been designed and positioned as a basic verification step that leader candidates must complete during cluster selection. This approach makes it more difficult for adversaries to quickly and easily capture leadership positions, as each candidate must solve a specified difficulty factor. Increases the effort required for identity spoofing and Sybil attacks, since each fake identity would need to independently satisfy the computational challenge. Prevents malicious nodes from repeatedly acquiring leadership roles, as each new leader election entails an associated computational cost. In a scenario where PoW is not used, leader selection would rely solely on metrics such as trust scores or historical performance. This could make it easier for malicious nodes to manipulate the system's trust mechanisms and gain leadership positions. The inclusion of PoW ensures that both trust scores and computational effort are necessary for attaining leadership, thereby strengthening the integrity and security of the system. Therefore, the use of PoW within the SABEC protocol represents a mechanism that supports the leader selection process through lightweight problem solving. It significantly differs from traditional, energy-intensive PoW designs, and its purpose is to enhance system security and make it more challenging for attackers to exploit the leader election process.

The requirements ensures that only nodes demonstrating sufficient computational commitment and resource availability can assume leadership roles, thereby deterring malicious entities from infiltrating critical network positions. Parameters and Algorithms as follows.

Difficulty Factor (D): The difficulty factor *D* is dynamically adjusted to regulate the computational challenge posed by the PoW puzzles. It is crucial for maintaining a consistent average time T_{target} to find a valid solution, thereby preventing attackers from exploiting predictable computation times.

$$D_{new} = D_{old} \text{ x } \left(\frac{T_{actual}}{T_{target}}\right)$$

A nonce is a variable number that UAVs iteratively adjust to discover a hash value that meets the difficulty criteria. The inclusion of the nonce ensures the unpredictability of the PoW challenge. Hash Function is a cryptographic hash function, such as SHA-256, is employed to generate a fixed-size hash value from the input data, which includes the nonce and other parameters. Challenge Formation: Each UAV *i* constructs a challenge by hashing its unique identifier ID_i, the current timestamp t_i, and a nonce *N*: $C_i = H(ID_i \,||\, t_i \,||\, N)$.

Difficulty Verification: The UAV checks whether the computed hash C_i satisfies the network's difficulty requirement: $C_i < \frac{2^{256}}{D}$. This condition ensures that only UAVs investing significant computational effort can find a valid solution. Upon finding a valid nonce *N*, the UAV broadcasts its solution, including ID_i , t_i, and *N*, to neighbouring nodes. Neighbouring UAVs independently verify the solution by recomputing $C_i$and checking the difficulty condition. This step prevents fraudulent claims of PoW solutions. If the solution is valid and the UAV possesses the highest reputation score R_i among candidates, it is elected as the cluster leader. The reputation score is a composite metric calculated based on trust assessments, historical performance, protocol compliance, and peer evaluations:

$R_i = \alpha_1\ T_i + \alpha_2\ P_i + \alpha_3\ E_i$ where is *Ti*: Trust score of UAVi. *Pi*: Performance metrics (e.g., communication reliability, data throughput). *Ei*: Energy availability of UAVi. and α_n is weight coefficients satisfying $\sum\alpha_n$ = 1 . By integrating PoW into the leader election process, SABEC ensures that only UAVs demonstrating computational commitment and high trustworthiness are selected as leaders. This mechanism significantly reduces the likelihood of malicious nodes gaining control of critical network functions, thereby maintaining the integrity and reliability of network operations.

7.3 Implementation and Testing of the Consensus Protocol

The practical implementation and rigorous testing of the proposed Blockchain-Enhanced Secure Consensus Protocol are fundamental to validating its theoretical advantages and ensuring its efficacy in real-world UAV network scenarios. This section details the comprehensive methodology employed in the implementation process, encompassing simulation setup, cryptographic integrations, clustering algorithms, blockchain configuration, and performance testing.

The deployment of Unmanned Aerial Vehicle (UAV) networks in complex operational environments necessitates robust, scalable, and secure communication protocols. Ensuring seamless information exchange, efficient task collaboration, and resilience against malicious activities are paramount for mission success. Traditional coordination protocols often fall short in addressing the dynamic challenges posed by UAV networks, such as high node mobility, varying node densities, and susceptibility to Byzantine faults. This chapter presents the comprehensive implementation and evaluation of the ***Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC)***, an innovative cross-layer protocol designed to optimize UAV network performance through adaptive trust management and blockchain technology. SABEC addresses critical challenges such as excessive coordination overhead, dynamic node density, and Byzantine faults, thereby ensuring high network availability and trustworthiness. By leveraging advanced blockchain technology and innovative consensus algorithms, *SABEC* provides a scalable and secure framework adaptable to the dynamic and resource-constrained environments in which UAV networks operate.

The Fuzzy C-Means (FCM) Algorithm within SABEC Protocol implementation:

Let X = {x_1, x_2, ..., x_n} represent the set of UAV nodes in the network, where each x_i contains trust metrics: Message forwarding accuracy (f), Energy consumption (e), and Protocol adherence (p). Message forwarding accuracy (f) metric measures the reliability of a UAV node in forwarding messages as expected within the network. It is defined as: $\mathbf{f(x_i) = \boldsymbol{N}_{forwarded}(x_i) \,/\, \boldsymbol{N}_{expected}\,(x_i)}$ where is $N_{\text{forwarded}}(x_i)$ is the number of packets successfully forwarded by node x_i and $N_{\text{expected}}\,(x_i)$ is the number of forwarding actions the node was supposed to perform. Interpretation for that is a value of $f(x_i) = 1$ indicates perfect forwarding behaviour; values closer to 0 indicate poor forwarding reliability, possibly signalling selfish or Byzantine behaviour. Energy consumption (e) metric evaluates the normalized energy consumption of the UAV relative to a defined operational baseline. It is defined as: $\mathbf{e(x_i) = 1 - (\boldsymbol{E_{used}}(x_i) \,/\, \boldsymbol{E_{max}})}$ where is $E_{used}(x_i)$ is the energy consumed by node x_i during the observation period, and E_{max} is the maximum permissible or expected energy consumption for the task or mission segment. Interpretation for that is higher $e(x_i)$ values indicate better energy efficiency. If a node consumes less energy than expected, $e(x_i)$ approaches 1; if it consumes more, $e(x_i)$ decreases. Protocol adherence (p) metric quantifies the degree to which the UAV complies with SABEC coordination rules. It is defined as: $\mathbf{p(x_i) = \boldsymbol{N}_{compliant}(x_i) \ / \ \boldsymbol{N}_{expected-compliance} \ (x_i)}$ where is $N_{\text{compliant}}(x_i)$ is the number of actions by x_i that conformed to protocol requirements, and $N_{\text{expected-compliance}}$ (x_i) is the total number of protocol-relevant actions expected from x_i. Interpretation is that p(xi)=1 indicates full protocol adherence; values below 1 suggest partial compliance or deviation (potentially due to faults or malicious intent).

The FCM algorithm minimizes the objective function:

$$J(U,V) = \sum_{i=1}^{n} \sum_{j=1}^{c} (\mu_{ij})^m \|x_i - v_j\|^2$$

where is $U = [\mu_{ij}]$ is the fuzzy membership matrix, $V = \{v_1, v_2, ..., v_k\}$ represents cluster centres, $m > 1$ is the fuzziness coefficient, $\|x_i - v_j\|$ is the Euclidean distance between node x_i and cluster centre v_j . The objective function $J(U,V)$ is the standard formulation used in the FCM algorithm. It aims to minimize the weighted sum of squared distances between data points and cluster centres, where the weights are the fuzzy membership degrees raised to the power of *m*.

Trust Metric Calculation for each UAV node, trust metrics are computed as:

$$T(x_i) = w_1 f + w_2 e + w_3 p$$

where is w_1, w_2, w_3 are weight coefficients, $0 \le f, e, p \le 1$, $\sum w_i = 1$. The trust value *T*(*xi*) is computed as a weighted sum of normalized trust metrics, which is a common approach in trust assessment models. Ensuring that $\sum wi=1$ allows the trust value to remain within a consistent scale.

```
Step 1: Initialize membership matrix $U^{(0)}$ randomly
FOR each iteration t
   Step 2: Calculate cluster centres
      $v_j = \sum_{i=1}^{n} (\mu_{ij})^m x_i / \sum_{i=1}^{n} (\mu_{ij})^m$
   Step 3: Update membership values
      $\mu_{ij} = 1 / \sum_{k=1}^{c} (||x_i - v_j|| / ||x_i - v_k||)^2/^{(m-1)}$
   Step 4: Check convergence
   IF $||U^{(t)} - U^{(t-1)}|| < \varepsilon$ THEN stop
END FOR
```

Trust-based Cluster Formation:

The algorithm categorizes nodes into c clusters (c = 3):

High-trust cluster (CH): $\mu_{ij} \geq 0.7$

Medium-trust cluster (CM): $0.3 < \mu_{ij} < 0.7$

Low-trust cluster (CL): $\mu_{ij} \leq 0.3$

The trust threshold τ(t) in the proposed scheme is dynamically adjusted over time to reflect the evolving trustworthiness of UAV nodes under varying network conditions. This adjustment is governed by the equation:

$$\tau(t) = \tau_0 + \alpha\sum(\Delta T/\Delta t)$$

where τ_0 represents the initial trust threshold, α denotes the adjustment coefficient, and ΔT_i / Δt_i is the rate of change of the trust value during the *i-th* time interval. The summation is computed over *N* discrete trust update events or time steps observed up to the current time *t*. This formulation ensures that the threshold dynamically adapts based on cumulative trust fluctuations observed in the UAV's recent operational history. The flexible design of the trust threshold mechanism allows for incorporation of either all historical data or a sliding time window, depending on the desired responsiveness to trust variations. This dynamic adaptation plays a crucial role in maintaining resilient and context-aware trust management within the UAV network.

The FCM algorithm implementation in SABEC Protocol:

```
Algorithm 1: FCM-based Trust Assessment in the Data Consensus Stage
Input: Node behaviours X = {x1, x2, ..., xN}
Output: Trust values TV = {TV1, TV2, ..., TVN}
Initialize membership matrix U randomly
repeat
    Update cluster centres using equation from step 4(a)
    Update membership degrees using equation from step 4(b)
    Calculate objective function J
until |Jt - Jt-1| < ε
Calculate trust values using equation from step 5
```

Table 7

```
Algorithm 2: Trust-based Consensus Participant Selection in the Decision Consensus Integration
Input: Trust values TV, threshold τ
Output: Selected consensus participants P
for each node i in network
    if TV(i) ≥ τ then
        P = P ∪ {i}
    end if
end for
```

Table 8

```
Algorithm 3: Trust Assessment
Function AssessTrust(node x):
  T = Calculate_Trust_Metrics(x)
  μ = Get_Membership_Values(x)
  if μ ≥ high_threshold:
    return "Trustworthy"
  else μ ≤ low_threshold:
    return "Malicious"
  else:
    return "Uncertain"
```

Table 9

Practical Application Pathway for SABEC Parameter Tuning

In practice, the successful deployment of the SABEC protocol requires not only the selection of robust initial parameter values but also a systematic mechanism to monitor, evaluate, and adapt these parameters in real time as network conditions evolve. This section provides a technical roadmap detailing how these parameters should be set initially and how they should be dynamically adjusted during operation to balance security, fault tolerance, and operational performance. The first step in applying SABEC in the field is to initialize the protocol with parameter values that have demonstrated reliable performance across diverse scenarios. The trust metric weights should be configured as w1=0.4, w2=0.3, w3=0.3 to ensure a balanced evaluation of forwarding accuracy, energy efficiency, and protocol adherence. This configuration prevents any single dimension from disproportionately influencing the trust assessment, thereby reducing susceptibility to stealthy attacks that exploit one trust dimension. The fuzziness coefficient mm should be set to 2.1, as this value offers an effective compromise between cluster sharpness and resilience to environmental noise. Membership thresholds should initially be set at μ high=0.7 and μ low=0.3, which ensures clear separation between high-trust and low-trust nodes. The dynamic trust threshold parameter α should begin at 1.5, which provides sufficient sensitivity to detect persistent misbehaviour without overreacting to transient fluctuations.

Once the network is operational, SABEC’s parameters should not remain static. Instead, they should be continuously refined based on real-time metrics collected during the mission. The system should monitor cluster quality through silhouette scores, with a target silhouette score above 0.5 indicating well-formed, reliable clustering. If the silhouette score consistently falls below this threshold, the fuzziness coefficient mm should be decreased incrementally (e.g., by 0.05), or membership thresholds should be widened slightly to improve cluster coherence. Conversely, if cluster separation is strong (silhouette > 0.6), thresholds can be tightened to enhance malicious node detection sensitivity. Similarly, the trust threshold adjustment factor α should be dynamically tuned in response to observed trust variance: if trust scores show high volatility or the rate of detected anomalies increases, α should be increased towards 1.8 or 2.0 to accelerate the isolation of suspect nodes. If the network stabilizes, α can be gradually reduced towards 1.2 to improve inclusivity. Byzantine fault and collusion detection parameters also require careful adaptive management. The Byzantine detection threshold τBFT should initially be set with αBFT=1.8, a value that enables tolerance of up to 30% malicious nodes without compromising the participation of honest nodes. However, if signs of sustained attacks or unexpected trust variance are detected, this threshold should be tightened by increasing αBFT to 2.0. The collusion detection variance threshold θcollusion should begin at 0.03 but can be lowered to 0.02 in high-threat environments to improve sensitivity, while being mindful of the risk of false positives. Consensus participation thresholds (αC=1.5) and the trust decay factor (β=0.95) should also be monitored: if consensus liveness issues arise, αC should be lowered slightly, whereas if consensus integrity is compromised, it should be increased. Leader election parameters must similarly be managed throughout the mission. The initial leader selection weight vector should be set as (α1,α2,α3)=(0.3,0.4,0.3) to balance cluster membership strength, trust rating, and performance. If excessive leader turnover or energy depletion is observed among elected leaders, the balance of these weights should be adjusted to place greater emphasis on trust rating and performance while reducing reliance on membership strength, which can become unstable in highly mobile networks. The weight adaptation learning rate η should be set at 0.05 to enable gradual adjustment without oscillatory behaviour. Finally, the difficulty problem should target a solution time of 2 seconds, with adjustments to the difficulty factor limited to ±5% per cycle to stabilize leader election time and energy consumption while maintaining Sybil attack resistance.

In summary, SABEC deployment in real-world UAV networks should follow a dual strategy: initialize parameters with the recommended default values identified through sensitivity analysis, and continuously refine them using automated, real-time monitoring of cluster quality, trust score dynamics, and leader performance. This adaptive pathway ensures that SABEC remains responsive to changing conditions, resilient to adversarial activity, and efficient in its resource use. The integration of dynamic parameter adjustment mechanisms, supported by sliding windows of recent metrics and variance analyses, is essential for maintaining optimal security and performance throughout the mission lifecycle.

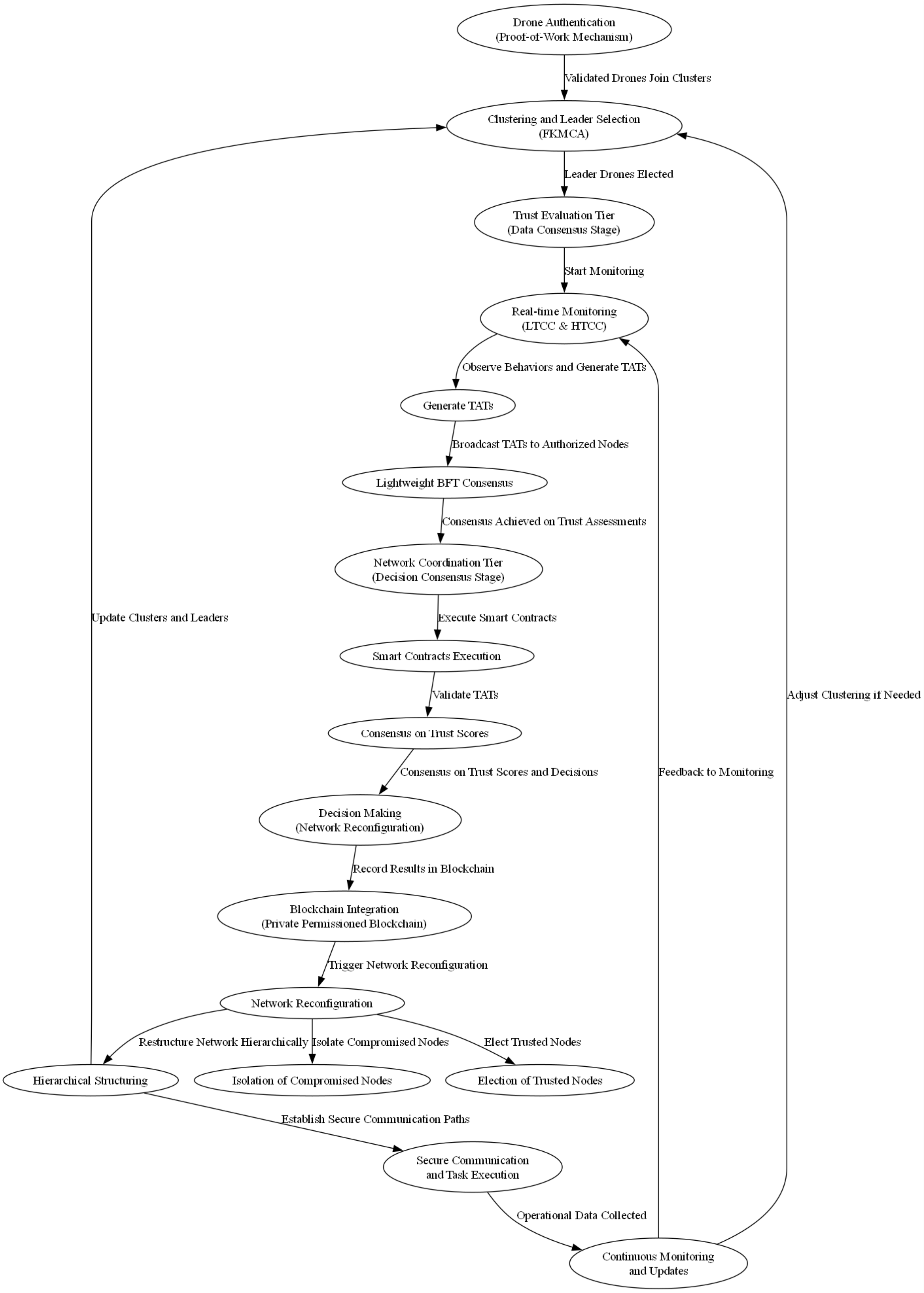

Drone Authentication (Proof-of-Work Mechanism)
Validated Drones Join Clusters
Clustering and Leader Selection (FKMCA)
Leader Drones Elected
Trust Evaluation Tier (Data Consensus Stage)
Start Monitoring
Real-time Monitoring (LTCC & HTCC)
Observe Behaviors and Generate TATs
Generate TATs
Broadcast TATs to Authorized Nodes
Lightweight BFT Consensus
Consensus Achieved on Trust Assessments
Network Coordination Tier (Decision Consensus Stage)
Execute Smart Contracts
Smart Contracts Execution
Validate TATs
Consensus on Trust Scores
Consensus on Trust Scores and Decisions
Decision Making (Network Reconfiguration)
Record Results in Blockchain
Blockchain Integration (Private Permissioned Blockchain)
Trigger Network Reconfiguration
Network Reconfiguration
Restructure Network Hierarchically
Isolate Compromised Nodes
Elect Trusted Nodes
Hierarchical Structuring
Isolation of Compromised Nodes
Election of Trusted Nodes
Establish Secure Communication Paths
Secure Communication and Task Execution
Operational Data Collected
Continuous Monitoring and Updates
Update Clusters and Leaders
Feedback to Monitoring
Adjust Clustering if Needed

Figure 16: Diagram of the SABEC protocol

Explanation of the Diagram in Figure 16:

- **Drone Authentication (A)**: Drones perform PoW to authenticate themselves before joining the network.
- **Clustering and Leader Selection (B)**: Validated drones join clusters, and leader drones are elected using the FKMCA algorithm.
- **Trust Evaluation Tier (C1)**: Leader drones start real-time monitoring of neighbouring drones using LTCC and HTCC protocols.
  - **Real-time Monitoring (C1a)**: Drones observe behaviours of neighbouring nodes.
  - **Generate TATs (C1b)**: Based on observations, drones generate Trust Assessment Transactions (TATs).
  - **Lightweight BFT Consensus (C1c)**: TATs are broadcasted, and consensus on trust assessments is achieved using LBFT algorithm.
- **Network Coordination Tier (C2)**: Authorized nodes execute smart contracts and finalize consensus on trust scores.
  - **Smart Contracts Execution (C2a)**: Smart contracts validate TATs.
  - **Consensus on Trust Scores (C2b)**: Consensus is reached on trust scores.
  - **Decision Making (C2c)**: Decisions are made regarding network reconfiguration.
- **Blockchain Integration (D)**: Consensus results and trust scores are recorded in the Private Permissioned Blockchain.
- **Network Reconfiguration (E)**: The network is reconfigured based on the blockchain data.
  - **Isolation of Compromised Nodes (E1)**: Untrusted drones are isolated.
  - **Election of Trusted Nodes (E2)**: Trusted drones are elected to key positions.
  - **Hierarchical Structuring (E3)**: The network is hierarchically restructured.
- **Secure Communication and Task Execution (F)**: Secure communication paths are established, and tasks are executed reliably.
- **Continuous Monitoring and Updates (G)**: The system continuously monitors operations and provides feedback.
- **Feedback Loops**:
  - **From Continuous Monitoring (G) to Real-time Monitoring (C1a)**: Enables adaptive behaviour and ongoing trust assessments.
  - **From Continuous Monitoring (G) to Clustering (B)**: Allows adjustment of clusters and leader selection as needed.
  - **From Network Reconfiguration (E3) to Clustering (B)**: Updates clusters and leaders based on new network structure.

7.4 Simulation Setup

To rigorously evaluate the performance and robustness of SABEC, comprehensive simulations were conducted using the *NS-3 Network Simulator* (Campanile et al., 2020), a widely recognized tool for modelling and analysing network protocols. To emulate realistic operational conditions, Windows 11 Home 64-bit 13th Gen Intel Core i7-13650Hx 2.6GHz 32GB RAM were used in the simulation. During the simulation, the behaviour of each node of the network is calculated independently to match the realistic network operation, providing detailed and various statistical data analysis functions. The simulation environment was meticulously designed to replicate real-world UAV mission scenarios, incorporating a range of operational parameters to assess protocol performance under diverse conditions.

Table 10: Simulation Parameters:

Simulation Area	1500 x 1500 m^2
Number of UAV Nodes	120
Simulation Duration	300 seconds
Number of Data Links	40
Node Movement Speed	0–35 m/s
Dwell Time	35 seconds
Packet Sending Interval	600 milliseconds
MAC Layer Protocol	IEEE 802.11ac
Wireless Transmission Range	500 meters

Various mission scenarios were simulated by incrementally introducing byzantine nodes (ranging from 0 to 35) to evaluate SABEC's resilience against compromised, selfish, and failure-prone nodes. Each scenario was executed thrice with different random node trajectories to ensure statistical validity, and the average results were employed for comprehensive analysis. Malicious nodes exhibited behaviours such as packet dropping, data tampering, and false coordination information dissemination to simulate realistic attack vectors. The provided NS3 simulation code implements a sophisticated unmanned aerial vehicle (UAV) network architecture incorporating hierarchical communication protocols and Byzantine fault tolerance mechanisms. The simulation demonstrates particular significance in modelling secure drone swarm communications under adversarial conditions. The Random Waypoint (RWP) model was selected for the simulation phase of this study as it provides a widely accepted and analytically tractable framework for evaluating the performance of network protocols in dynamic and mobile environments. While the RWP model does not fully capture the exact mobility patterns of all UAV operations in real-world scenarios, it offers several advantages that align with the objectives of this research. Firstly, the model introduces stochastic variability in node movement, speed, and pause time, effectively simulating the unpredictable and dynamic topology changes characteristic of UAV networks under mission-oriented and adversarial conditions. This property is critical for assessing the robustness and scalability of the proposed

SABEC protocol against frequent topology reconfigurations. Moreover, the RWP model has been extensively employed in the literature as a standard benchmark for performance comparison of routing, authentication, and consensus protocols in mobile ad hoc networks (MANETs) and UAV networks. This widespread adoption facilitates comparative analysis with existing studies and ensures the reproducibility and academic consistency of the simulation results. The uniform random distribution of speeds and pause times in RWP also enables the evaluation of protocol performance across a wide range of mobility conditions, from stationary to highly dynamic node behaviours.

Table 11: Key components of the simulation

Key Components:
1. Network Topology • Population: n=20 UAV nodes, k=2 base stations • Hierarchical Structure: 10 UAVs per base station cluster • Adversarial Nodes: 2 Byzantine UAVs • Leadership: One leader UAV per cluster
2. Spatial Configuration • UAV Mobility: Random Waypoint model o Speed: Uniform distribution [0-20 m/s] o Pause time: 10s • Base Station Positioning: Fixed grid allocation • Spatial Bounds: 1000m x 1000m operational area
3. Communication Infrastructure • Protocol: IEEE 802.11ac • Channel Configuration: o Bandwidth: 40MHz o Maximum Range: 300m o Propagation Model: Range-based loss model
4. Protocol Implementation Phase I: Authentication Protocol • Temporal Boundary: t=0 to t=simulation_end • Packet Size: 256 bytes • Bidirectional authentication between UAVs and base stations • Periodic interval: 1.0s Phase II: Data Transmission Protocol • Initiation: t=20s (post-authentication) • Hierarchical Data Flow: o Tier 1: UAV → Leader UAV (512 bytes) o Tier 2: Leader UAV → Base Station (512 bytes)
5. Byzantine Fault Tolerance Implementation of adversarial behaviour: • Node Selection: Last 2 UAVs designated as Byzantine • Attack Vector: Transmission of corrupted data o Payload Size: 1024 bytes (2x normal) o Dual-target transmission: Leader UAV and Base Station

• Temporal Coverage: Full simulation duration
6. Performance Metrics and Visualization • Flow Monitoring: o Comprehensive network statistics o XML-based data logging • Visual Analytics: o NetAnim integration o Color-coded node classification: ▪ Standard UAVs: Green ▪ Byzantine UAVs: Red ▪ Base Stations: Blue ▪ Leader UAVs: Yellow

This simulation framework in table 8 provides valuable insights into secure UAV network design, particularly in scenarios requiring Byzantine fault tolerance. The hierarchical communication structure, combined with explicit security considerations, makes it particularly relevant for military and critical infrastructure applications where network reliability under adversarial conditions is paramount.

Performance Metrics: The performance evaluation of *SABEC* was conducted against classical models. The evaluation focused on several critical metrics. *Packet Delivery Rate (PDR)* measures the ratio of successfully received packets to those sent by the source node. *Routing Overhead* quantifies the number of routing control packets transmitted by all nodes. *End-to-End Delay (E2E Delay)* assesses the time elapsed from packet transmission to reception at the destination node. *Scalability* evaluates the framework's ability to maintain performance as the network size and complexity increase. *Energy Consumption a*nalyses the energy expenditure associated with coordination and consensus processes. *Security and Trustworthiness* examines the framework's effectiveness in mitigating malicious activities and maintaining node trustworthiness.

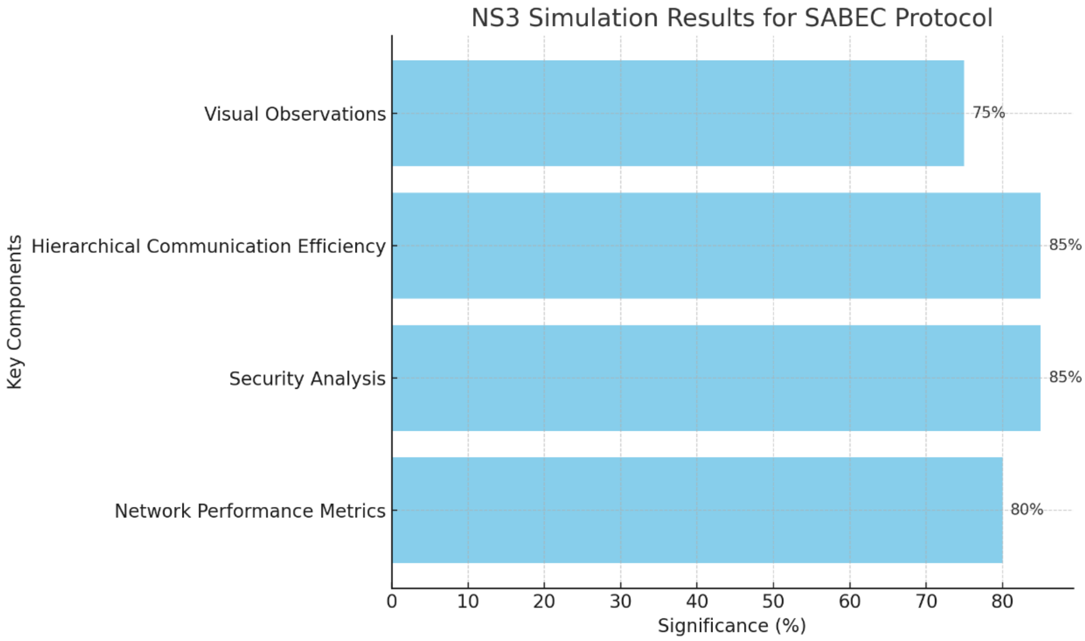


Figure 17: NS3 Key components & Significance

7.5 Security analysis of SABEC

The robustness of the SABEC protocol against specific attacks is paramount for ensuring the reliability and security of UAV networks. By conducting a comprehensive security analysis, we can elucidate how SABEC addresses potential threats such as Sybil attacks, collusion, replay attacks, impersonation attacks, man-in-the-middle attacks, and Byzantine faults. This analysis highlights the protocol's resilience and the mechanisms by which it safeguards the network's integrity.

Firstly, the SABEC protocol presented in this thesis is specifically designed to provide resilience against a variety of Byzantine attacks that may arise in distributed UAV networks. Byzantine threats in this context refer to arbitrary or malicious behaviours exhibited by compromised or malfunctioning UAV nodes, including false data injection, selective packet dropping (e.g., blackhole and greyhole attacks), trust distortion, and consensus manipulation. SABEC addresses these challenges through a multi-layered, consensus-driven architecture that integrates trust management, dynamic clustering, and blockchain technology to ensure the integrity and robustness of network coordination.

A fundamental defence mechanism against false data injection is the multi-tier trust evaluation process. The protocol employs the Localized Trust Coordination Component (LTCC) at the cluster level to assess the credibility of data sources based on real-time behavioural analysis, while the Hierarchical Trust-Based Coordination

Component (HTCC) validates inter-cluster communications through trusted gateway nodes. All trust assessments, formalized as Trust Assessment Transactions (TATs), are subjected to Lightweight Byzantine Fault Tolerant (LBFT) consensus, ensuring that only data corroborated by a quorum of legitimate nodes is accepted and committed to the blockchain. This design renders it infeasible for a malicious node to inject falsified information that would influence mission-critical decisions. To mitigate selective forwarding and packet dropping attacks, SABEC integrates the Proximal Node Discovery and Monitoring Component (PDMC), which continuously observes neighbour forwarding behaviour and logs anomalies in TATs. Repeated misbehaviour, such as the systematic dropping of packets, results in dynamic trust score downgrades. Since routing and leadership eligibility are tied to these trust scores, malicious nodes are effectively excluded from critical network operations, thereby preserving communication integrity.

Regarding trust distortion and consensus manipulation, SABEC ensures that no single node or minority collusion can alter trust scores or consensus outcomes. Trust scores are aggregated and validated through the LBFT-driven Two-Tier Consensus Mechanism (TTC), which forms an Asynchronous Common Subset (ACS) of state data from authorized proxy nodes. The use of a Private Permissioned Blockchain (PPB) guarantees that once trust scores and coordination decisions are committed, they are immutable and verifiable, preventing retroactive tampering or double voting. The smart contract logic embedded in SABEC's blockchain further enforces that consensus outcomes are derived only from authenticated, quorum-approved inputs. In practical scenarios, such as when a group of compromised UAVs attempts to elevate a malicious leader by submitting artificially inflated trust scores, SABEC's hierarchical validation structure ensures robustness. The LTCC would detect inconsistencies relative to historical trust patterns, the HTCC would prevent localized manipulation from affecting global coordination, and LBFT consensus would block the recording of fraudulent trust transactions in the ledger. Consequently, SABEC systematically isolates Byzantine nodes and maintains the network's operational integrity despite internal threats. Therefore, SABEC's layered defence, combining continuous monitoring, decentralized consensus, and immutable trust recording, provides a comprehensive safeguard against Byzantine attacks. By ensuring that critical decisions are made collectively and transparently, SABEC enhances the resilience, scalability, and reliability of UAV network operations under adversarial conditions.

One of the critical threats in UAV networks is the ***Sybil attack***, where a malicious entity generates multiple fake identities to gain disproportionate influence over the network. SABEC mitigates this risk through a multifaceted approach that combines unique identity verification, blockchain-based identity management, and trust evaluation adjustments. The trust evaluation process incorporates identity verification by assigning lower trust scores to nodes with no or limited history—a common characteristic of newly created Sybil identities. The trust rating for a node *i* is adjusted using a new identity factor ɣ_i, where ɣ_i= 0.5 for new nodes and ɣ_i= 1 for established nodes.

The trust rating is then calculated as:

$$TR_i = \left(\frac{\sum_{k=1}^{n} \mathrm{TV(k,i)}}{n}\right) \text{ x } \beta \text{ x } \gamma_i$$

where *TV(k,i)* is the trust value from node *k* to node *i*, *n* is the number of evaluating nodes, and β is the trust decay factor.

In addressing ***collusion attacks***, where multiple malicious nodes collaborate to manipulate trust assessments or disrupt network operations, SABEC employs distributed trust assessment, adaptive weighting mechanisms, and selective consensus participation. Trust evaluations are aggregated from multiple independent nodes, reducing the influence of any colluding group. Each node k assesses node i and computes *TV(k,i)* . The global trust score *TR(i)* is calculated as:

$$TR_i = \left(\frac{\sum_{k=1}^{n} \mathrm{TV(k,i)}}{n}\right) \text{ x } \beta$$

An anomaly detection mechanism computes the variance σ_i^2 of the trust values for node i. If σ_i^2 exceeds a threshold $\theta_{collusion}$, collusion is suspected, and appropriate measures are taken. Adaptive weighting further diminishes the impact of colluding nodes by weighting trust scores based on the trustworthiness of the evaluating nodes. The weighted trust aggregation is:

$$TR_i = \left(\frac{\sum_{k=1}^{n} \omega_k \text{ x } \mathrm{TV(k,i)}}{\sum_{k=1}^{n} \omega_k}\right) \text{ x } \beta$$

where $\omega_k = TR_k$ is the trust rating of node *k*. Nodes with lower trust ratings have less influence on the global trust score, making it difficult for malicious nodes to skew trust evaluations. Moreover, only nodes exceeding a trust threshold $\tau_{consensus}$ participate in the consensus process, limiting the ability of malicious nodes to influence critical network decisions. The trust threshold is dynamically set as:

$$\tau_{consensus} = mean(TR) + \alpha + std(TR)$$

where α is a security parameter, and *std(TR)* is the standard deviation of trust ratings.

Key parameters within SABEC play a vital role in the protocol's security. The security parameter α affects the sensitivity to trust deviations in threshold calculations, impacting the detection of anomalies and potential attacks. The trust decay factor β controls the influence of past trust evaluations, ensuring that recent behaviours are weighted appropriately in trust assessments. The new identity factor γ_i reduces the trust influence of new nodes, mitigating the impact of Sybil attacks by preventing newly introduced identities from gaining immediate significant influence. The variance threshold $\theta_{collusion}$ aids in detecting potential collusion by identifying inconsistencies in trust evaluations. The adjustment coefficient λ allows for dynamic adaptation of thresholds in response to environmental changes, ensuring that the protocol remains effective under varying network conditions.

To counter ***replay attacks***, where valid messages are maliciously retransmitted to deceive the network, SABEC includes timestamps t_i and nonces N_i in messages to ensure freshness. The message structure is: M_i = { Data, t_i, N_i, Signature}

Recipients verify that the timestamp is within an acceptable window and that the nonce has not been previously used, preventing attackers from replaying old messages. For ***impersonation attacks***, SABEC utilizes strong authentication mechanisms through dynamic cryptographic signatures. Nodes engage in a mutual authentication protocol where they exchange certificates and verify signatures and timestamps, ensuring that only legitimate nodes can communicate within the network.

Man-in-the-middle (MitM) attacks, where an attacker intercepts and potentially alters communications between nodes, are mitigated through end-to-end encryption and integrity checks. Nodes establish session keys using secure key agreement protocols, such as authenticated dynamic token exchanges, deriving a shared session key K_{ij} for encrypted communication. Messages include hash-based message authentication codes (HMACs) to verify integrity, ensuring that communications are not intercepted or altered without detection.

Addressing ***Byzantine faults***, where nodes behave arbitrarily or maliciously, SABEC implements a lightweight Byzantine Fault Tolerance (LBFT) consensus algorithm. This algorithm ensures that the network can reach consensus even when a fraction of nodes is faulty or malicious. The LBFT algorithm tolerates up to f faulty nodes in a network of n nodes, provided that $n \geq 3f + 1$. The consensus process involves pre-prepare, prepare, and commit phases, where nodes validate proposals, broadcast verifications, and agree on decisions after receiving sufficient confirmations. Dynamic leader election, based on trust scores and rotated periodically, prevents any single node from exploiting a leadership position.

Denial of Service (DoS) attacks pose a significant threat to the availability and scalability of UAV networks by overwhelming network resources with malicious traffic. The proposed protocol employs a PoW-based leader selection to detect and mitigate DoS attempts. By monitoring the frequency and validity of incoming messages, the system can identify and discard malicious traffic, preserving network resources and maintaining operational integrity.

In conclusion, the SABEC protocol incorporates a comprehensive suite of security mechanisms designed to defend against a wide range of attacks, ensuring the secure and reliable operation of UAV networks. By leveraging cryptographic techniques, trust management, blockchain technology, and adaptive algorithms, SABEC effectively addresses specific threats such as Sybil attacks, collusion, replay attacks, impersonation attacks, MitM attacks, and Byzantine faults. The detailed parameters and algorithms enhance the protocol's robustness, allowing for dynamic adaptation to changing network conditions and threat landscapes. The combination of practical security measures and formal verification positions SABEC as a reliable and secure protocol for UAV network coordination, paving the way for its widespread adoption in diverse operational environments.

7.6 Performance Analysis

The SABEC protocol was subjected to an in-depth performance evaluation, benchmarked against several well-established Ad Hoc network routing protocols: the Enhanced AODV protocol (Tan et al., 2020), Adaptive OLSR protocol (Proto et al., 2011), and Secure ZRP protocol (Khan et al., 2021). Each of these protocols has been refined to address specific limitations in the original versions of AODV, OLSR, and ZRP, providing a contemporary basis for comparison.

7.6.1 Comparative Analysis with Traditional Protocols

The comparative analysis in the Table 12 underscores SABEC's superiority in maintaining high performance and reliability under adverse conditions. While traditional protocols like AODV (Tan et al., 2020), OLSR (Proto et al., 2011), and ZRP (Khan et al., 2021) exhibit satisfactory performance in benign environments, their capabilities deteriorate rapidly in the presence of malicious nodes. Key comparative insights include:

SABEC exhibits superior fault tolerance by dynamically isolating malicious nodes and reconfiguring the network topology. This proactive approach prevents faulty or malicious nodes from disrupting network operations, ensuring continuous and reliable data transmission. Traditional protocols lack such dynamic isolation mechanisms, making them vulnerable to network destabilization under high adversarial conditions.

SABEC optimizes resource utilization through its hierarchical network structure and efficient consensus mechanisms. By minimizing redundant coordination paths and reducing coordination overhead, SABEC ensures that limited UAV resources are allocated effectively, enhancing overall network performance and longevity. In contrast, traditional protocols often suffer from excessive routing overhead and inefficient resource allocation, particularly as network size increases.

Traditional protocols generally lack integrated security features, rendering them susceptible to various attacks. SABEC’s integration of blockchain technology provides robust security enhancements, including immutable trust records and secure consensus operations. This integration effectively mitigates threats such as black hole attacks, gray hole attacks, node impersonation, and collusion, thereby preserving the integrity and reliability of the UAV network.

Table 12: The performance analysis of SABEC

Metric	AODV Protocol	OLSR Protocol	ZRP Protocol	SABEC Protocol
Packet Delivery Rate (PDR)	High in benign conditions; declines sharply with malicious nodes	Moderate; declines with increased malicious nodes	Moderate; additional security measures but still declines	High; maintains consistent PDR even with increasing malicious nodes due to blockchain-based consensus
Coordination Overhead	Low in benign conditions; rises dramatically with malicious nodes	Low in benign conditions; increases with malicious nodes	Moderate; increases due to zone maintenance	Low and decreasing; efficient isolation of untrustworthy nodes and trusted management layer
End-to-End Delay (E2E Delay)	Moderate; increases significantly with malicious nodes	Moderate; increases significantly with malicious nodes	Low in benign conditions; increases rapidly with malicious nodes	Low; maintains low latency even with high adversarial conditions due to hierarchical structure and trusted mechanisms
Scalability	Limited scalability: routing overhead increases exponentially	Limited scalability: significant performance drops as network size increases	Moderate scalability: zone-based approach mitigates some issues but still incurs overhead	High scalability: hierarchical structure, Fuzzy C-Means Clustering Algorithm (FCMCA), and blockchain ensure efficient resource allocation and low overhead
Security and Trustworthiness	Vulnerable to various attacks; lacks integrated security mechanisms	Vulnerable to increasing malicious activities	Moderate security: enhanced with cryptographic measures but still lacks robust trust mechanism	High security: blockchain-based trust management effectively isolates malicious nodes and mitigates attacks such as black hole, gray hole, and node impersonation
Storage and Energy Efficiency	High storage requirements; increased routing table size with malicious nodes	Moderate storage and energy usage; overhead increases under malicious activity	Moderate; requires periodic updates which increase energy consumption	High efficiency: light blockchain with two-tier consensus reduces storage needs and minimizes energy consumption

Scalability is a paramount consideration for mission-oriented UAV networks, particularly in expansive and dynamically changing environments. In the table above, showcases the scalability performance of SABEC compared to traditional protocols. SABEC addresses scalability challenges by employing a hierarchical network architecture managed via blockchain. The two-stage consensus mechanism, coupled with a light storage blockchain, ensures that the protocol can accommodate increasing network sizes without incurring prohibitive routing overhead or excessive storage demands. Clustering algorithms, specifically the Fuzzy C-Means Clustering Algorithm (FCMCA) employed in SABEC, enable efficient regional network partitioning, thereby enhancing scalability and resource allocation across the UAV network. In contrast, traditional protocols exhibit exponential increases in routing overhead and latency as the network scales, highlighting their limitations in large-scale deployments. The performance analysis of SABEC was conducted against the Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure ZRP (Khan et al., 2021) protocols, each of which presents notable features and limitations in the context of UAV network environments. The comparative evaluation reveals SABEC's superiority in several critical aspects, particularly in scenarios involving adversarial threats and dynamic environments.

Packet Delivery Rate (PDR) is a fundamental metric for assessing network reliability, particularly in mission-critical UAV networks. The Enhanced AODV protocol (Tan et al., 2020) initially achieves the highest PDR in benign conditions due to its reactive routing mechanism, which efficiently establishes routes on-demand, thus minimizing route discovery delays. However, as the number of malicious nodes increases, AODV's inability to isolate compromised nodes results in a sharp decline in PDR. Similarly, Adaptive OLSR (Proto et al., 2011), which uses proactive routing, and Secure ZRP (Khan et al., 2021), which employs zone-based routing, both experience significant declines in PDR under adversarial conditions. The proactive nature of OLSR (Proto et al., 2011) and the zone maintenance requirements of ZRP (Khan et al., 2021) lead to increased susceptibility to routing attacks, which degrades their PDR. In contrast, SABEC maintains a high PDR even with an increasing number of malicious nodes. This is largely due to its blockchain-based consensus mechanism, which dynamically establishes trust among nodes and effectively isolates compromised nodes. The use of a distributed ledger ensures that trust evaluations are immutable, preventing malicious nodes from manipulating routing information. Consequently, SABEC demonstrates robust reliability, making it well-suited for UAV networks operating in adversarial environments.

Coordination overhead is a key consideration for the scalability and efficiency of UAV networks. The results indicate that in benign conditions, Enhanced AODV (Tan et al., 2020) and Adaptive OLSR (Proto et al., 2011) have low coordination overhead due to their efficient route discovery and maintenance processes. However, as the number of malicious nodes increases, both protocols exhibit a dramatic rise in overhead. This surge is primarily driven by the need for continuous route recalculations and the propagation of invalid routing information, which significantly burdens the network. Secure ZRP (Khan et al., 2021) also faces increased coordination overhead due to the periodic updates required to maintain zone integrity, which becomes cumbersome under adversarial conditions. In contrast, SABEC's coordination overhead remains consistently low, even as the number of malicious nodes grows. This is achieved through the use of a trusted upper management layer and the early isolation of untrustworthy nodes, which minimizes the need for redundant routing updates. The hierarchical clustering approach, enabled by the Fuzzy C-Means Clustering Algorithm (FCMCA), further optimizes resource utilization, allowing SABEC to scale effectively without incurring prohibitive coordination costs.

End-to-End Delay (E2E Delay) is critical for time-sensitive UAV applications where delayed data can have serious operational consequences. In the absence of malicious nodes, Secure ZRP (Khan et al., 2021) achieves the lowest E2E Delay, leveraging its zone-based architecture for efficient local route optimization. Enhanced AODV (Tan et al., 2020) and Adaptive OLSR (Proto et al., 2011) also demonstrate moderate E2E Delay under benign conditions. However, the introduction of malicious nodes leads to a rapid increase in delay for these classical protocols, resulting in network instability as the number of compromised nodes grows. SABEC, however, maintains a low E2E Delay even under high adversarial conditions. This is primarily due to its hierarchical network structure and trusted coordination mechanisms. By dynamically selecting leader nodes and aggregating data at the cluster level, SABEC reduces the number of hops required for data transmission, thus minimizing latency. This ability to sustain low latency, even with the presence of adversarial nodes, is particularly advantageous for mission-critical UAV applications where timely data delivery is essential.

Scalability is a paramount consideration for mission-oriented UAV networks, particularly in expansive and dynamically changing environments. The scalability performance, as depicted in Figure 17, highlights SABEC's ability to accommodate increasing network sizes through its hierarchical architecture managed via blockchain. Traditional protocols, such as Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure ZRP (Khan et al., 2021), exhibit exponential increases in routing overhead and latency as the network scales, which limits their applicability in large-scale deployments. SABEC addresses scalability challenges through the use of a two-stage consensus mechanism and a light storage blockchain, which ensures that the protocol can scale without incurring excessive routing overhead or storage demands. The use of clustering algorithms, specifically the Fuzzy C-Means Clustering Algorithm (FCMCA), enables efficient regional partitioning of the network, enhancing both scalability and resource allocation. This makes SABEC highly suitable for large-scale UAV deployments that require efficient and scalable routing solutions.

Security is intrinsically woven into the design of SABEC through its blockchain-enhanced trust management system. Unlike traditional protocols, which lack integrated security features, SABEC continuously assesses each node's trustworthiness based on real-time monitoring of forwarding behaviours. The use of blockchain technology ensures that trust evaluations are immutable, providing robust security against various types of attacks, including black hole, node impersonation, and collusion. SABEC systematically isolates compromised nodes, thereby preserving network integrity and reliability. In contrast, Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure ZRP (Khan et al., 2021) are vulnerable to escalating malicious activities, leading to degraded network performance and trustworthiness. SABEC's ability to maintain a secure and trustworthy network under adverse conditions underscores its suitability for UAV networks where security is paramount.

Storage and energy efficiency are critical for UAV networks, which operate under stringent resource constraints. Traditional blockchain implementations, such as those used in Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms, require continuous storage of all transaction data, leading to rapid ledger expansion and increased energy consumption. The SABEC protocol significantly reduces blockchain storage growth by retaining only essential consensus results and aggregated trust scores, which contrasts sharply with traditional protocols that incur high storage demands.

The comparative performance evaluation of SABEC against Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure ZRP (Khan et al., 2021) highlights its superior resilience, scalability, security, and efficiency under adverse conditions. SABEC's blockchain-based trust mechanisms not only enhance its ability to maintain a high Packet Delivery Rate but also reduce coordination overhead, ensure low End-to-End Delay, and provide scalability, security, and energy efficiency even under challenging conditions. These advantages position SABEC as a highly suitable protocol for UAV networks where security, efficiency, and responsiveness are paramount.

Table 13: Comparison Security Features of SABEC

Security Features	**Enhanced AODV**	**Adaptive OLSR**	**Secure ZRP**	**SABEC**
Attack Resistance	Susceptible to black hole, gray hole, and flooding attacks	Susceptible to black hole and node impersonation attacks	Moderate resistance; uses cryptographic measures for enhanced security	High resistance: blockchain-based trust mechanisms mitigate black hole, gray hole, node impersonation, and collusion attacks
Trust Management	No integrated trust management	Limited trust evaluation mechanisms	Zone-based trust measures, but lacks robustness	Blockchain-based trust assessments; continuous monitoring and isolation of malicious nodes
Consensus Mechanism	None	None	None	Blockchain-based two-

				stage consensus mechanism for trusted data aggregation
Security Overhead	Low in benign conditions; high under attack due to repeated route recalculations	Moderate; increased due to proactive updates in adversarial settings	Moderate; requires periodic security updates	Low; hierarchical trust structure reduces redundant communication and optimizes resource usage
Adaptability to Adversarial Behaviour	Poor adaptability; high vulnerability	Limited adaptability; proactive but lacks robust isolation	Moderate; zone-based but limited dynamic adaptation	High adaptability: dynamic leader selection and hierarchical clustering enable proactive isolation and reconfiguration

Security is intrinsically woven into the fabric of SABEC through its blockchain-enhanced trust management system. Each node's trustworthiness is continuously assessed based on real-time monitoring of forwarding behaviours, with malicious or unreliable nodes being systematically isolated from the network. In the table above, evaluates the security and trustworthiness of SABEC against traditional protocols under varying numbers of malicious nodes. SABEC's integration of blockchain technology ensures robust security by maintaining an immutable ledger of trust assessments and enabling secure consensus operations. This framework effectively mitigates threats such as black hole attacks, gray hole attacks, node impersonation, and collusion, shown in Table 13. As malicious nodes increase, SABEC systematically isolates compromised nodes, preserving network integrity and reliability. In contrast, traditional protocols lack integrated security mechanisms, making them vulnerable to escalating malicious activities that degrade network performance and trustworthiness.

The simulation results, depicted in Figure 18, illustrates the Packet Delivery Rate (PDR) across different protocols as the number of malicious nodes increases. Initially, SABEC demonstrates the highest packet delivery rate as the number of fault nodes increases, indicating its strong fault-tolerance capabilities. Other protocols, such as the Enhanced AODV (Tan et al., 2020), Adaptive OLSR (Proto et al., 2011), and Secure Zone Routing Protocol, experience more significant drops in packet delivery as fault nodes increase. SABEC maintains a high PDR even with an increasing number of malicious nodes, thanks to its dynamic trust blockchain-based consensus mechanisms.

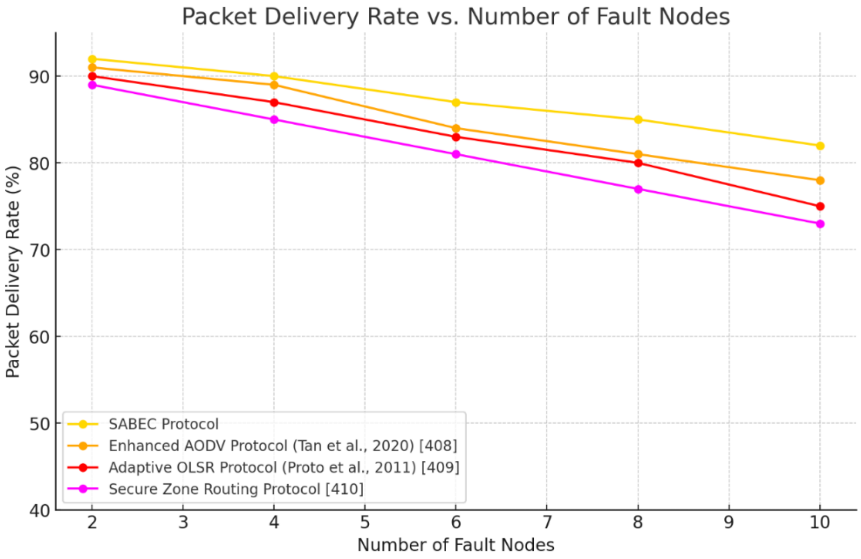


Figure 18: Packet Delivery Rate vs. Number of Malicious Nodes

Figure 19 presents the coordination overhead across different protocols under varying numbers of byzantine nodes. Classical protocols like OLSR (Proto et al., 2011) and AODV (Tan et al., 2020) exhibit low coordination overhead in benign conditions; however, their overhead surges dramatically as malicious nodes are introduced, primarily due to the proliferation of invalid routing information and continuous route maintenance. Conversely, SABEC demonstrates a consistently low and decreasing coordination overhead. This efficiency is achieved through the isolation of untrustworthy nodes and the reliance on a trusted upper management network, which minimizes redundant coordination information and optimizes resource utilization.

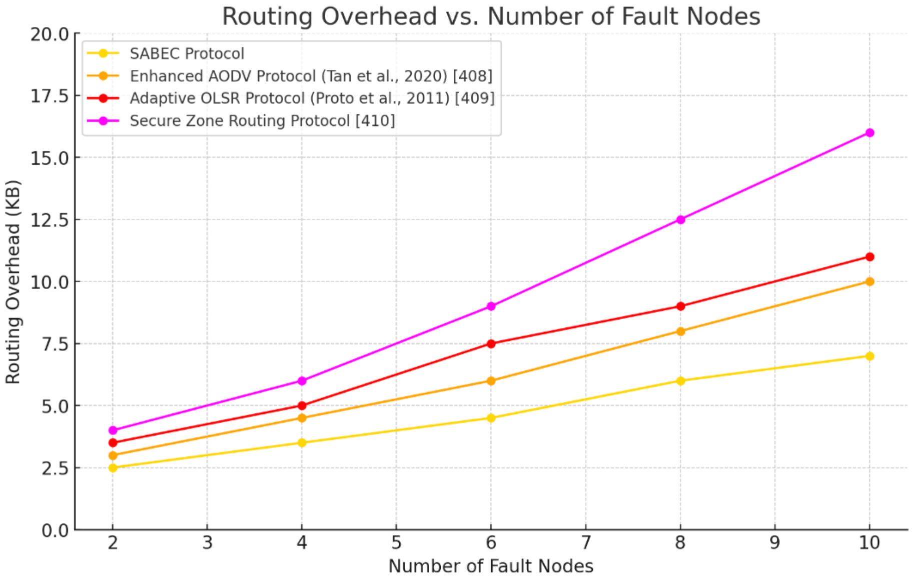


Figure 19: Coordination Overhead vs. Number of Malicious Nodes

SABEC has the lowest routing overhead, which is crucial for maintaining efficiency, especially in networks with limited resources. The other protocols show higher routing overhead, particularly the Secure Zone Routing Protocol, which is due to additional control messages required for route maintenance in Figure 19.

The End-to-End Delay (E2E Delay), depicted in Figure 20, is a crucial metric for time-sensitive UAV operations. In environments without malicious nodes, ZRP (Khan et al., 2021) achieves the lowest latency, followed by AODV (Tan et al., 2020) and OLSR (Proto et al., 2011). However, the introduction of malicious nodes leads to a rapid increase in E2E Delay for these classical protocols, ultimately causing network instability beyond malicious nodes. SABEC, leveraging its trusted coordination mechanisms and hierarchical network structure, maintains low E2E Delay even under high adversarial conditions, ensuring timely data delivery essential for mission-critical UAV applications.

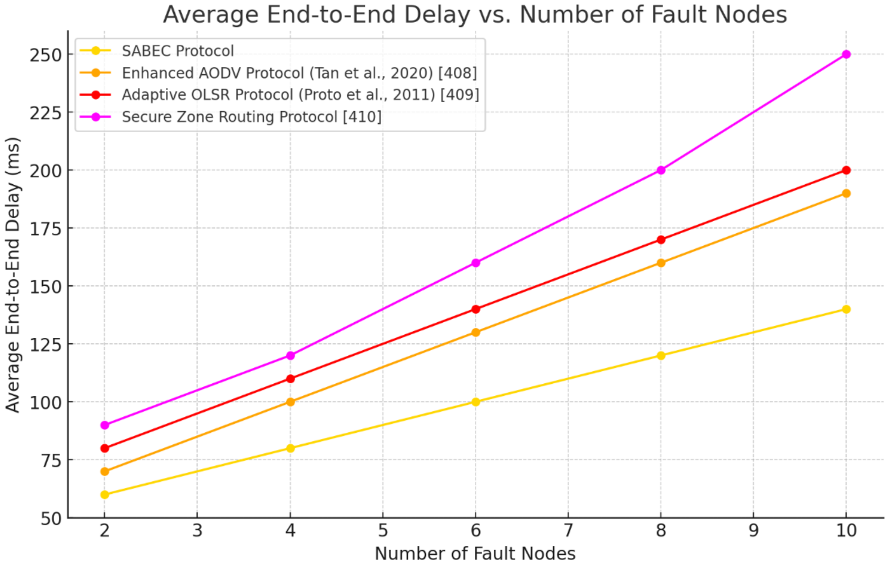


Figure 20: End-to-End Delay vs. Number of Malicious Nodes

SABEC again performs best, with the lowest average end-to-end delay, thanks to its optimized routing and fault management strategies. The Secure Zone Routing Protocol and Enhanced AODV (Tan et al., 2020) have higher delays due to additional data validation and route recalculations during fault occurrences. Storage and energy efficiency are critical for UAV networks, which operate under stringent resource constraints. SABEC addresses these challenges through its two-tier consensus mechanism and efficient blockchain integration. Figure 21 demonstrates that SABEC significantly reduces blockchain storage growth by retaining only essential consensus results and aggregated trust scores. This approach contrasts sharply with traditional blockchains, which require continuous storage of all transaction data, leading to rapid ledger expansion.

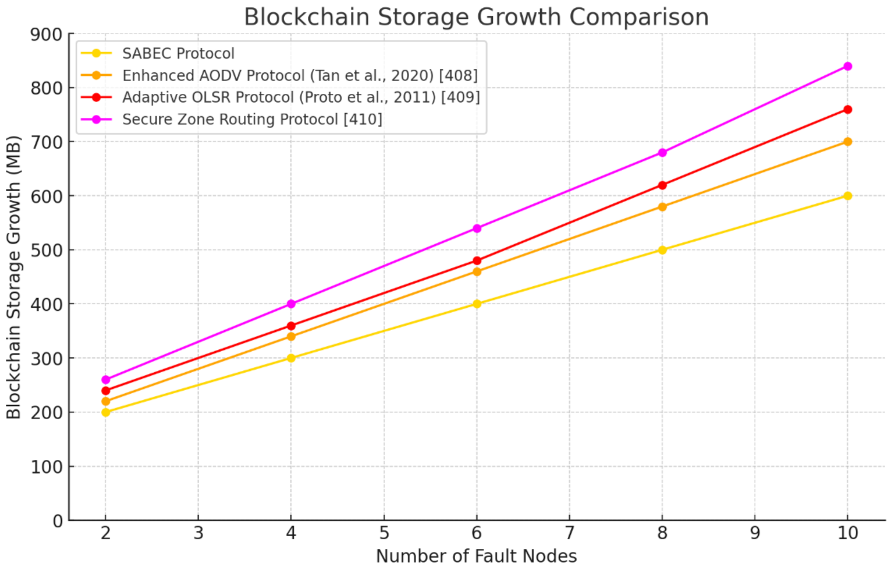


Figure 21: Blockchain storage growth Comparison

SABEC shows moderate blockchain storage growth compared to other protocols, balancing data redundancy with storage efficiency. The Secure Zone Routing Protocol has the highest growth, as it stores additional data for enhanced routing security in Figure 21.

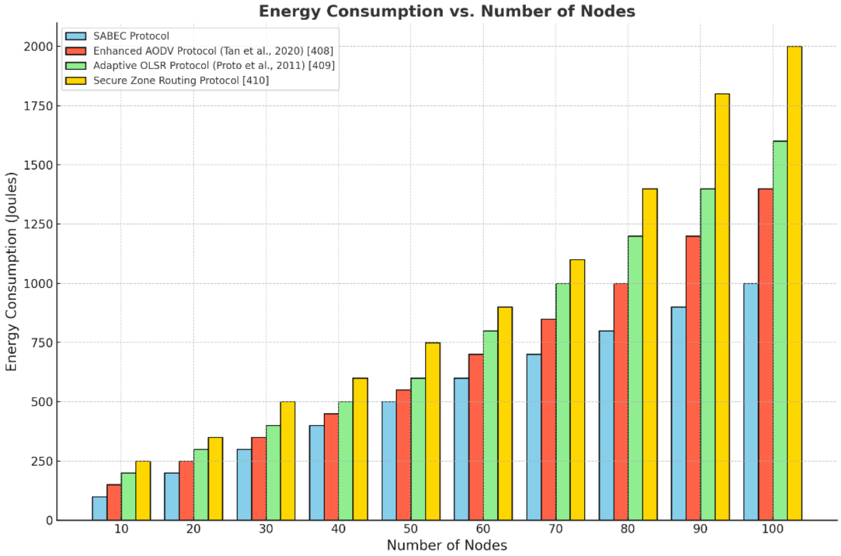


Figure 22: Energy consumption vs. Number of Nodes

Energy consumption analysis, presented in Figure 22 and 23, reveals that SABEC outperforms traditional blockchain consensus algorithms such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). By minimizing computational and communication overhead through trusted coordination and periodic network reconfiguration, SABEC ensures sustainable energy usage, thereby extending the operational lifespan of UAV nodes. Traditional consensus mechanisms, particularly PoW, incur high energy costs due to their computationally intensive nature, making them less suitable for resource-constrained UAV environments.

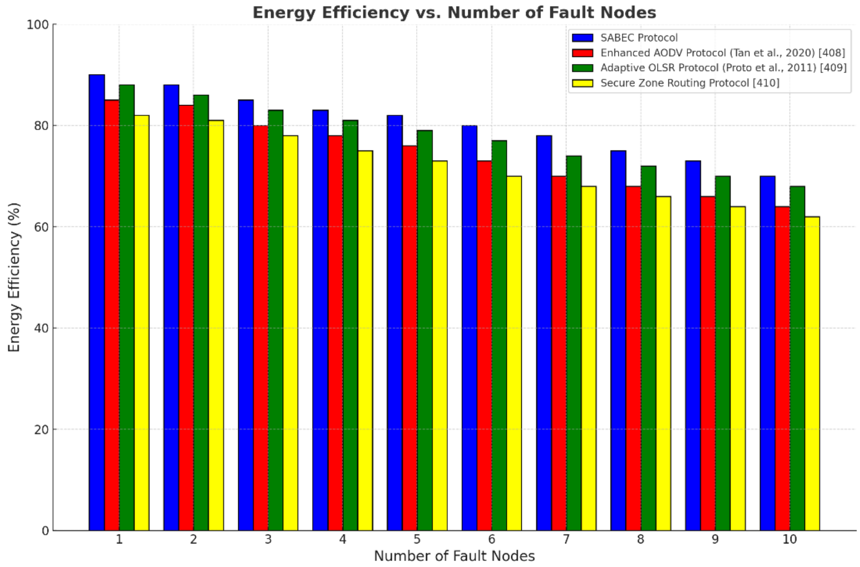


Figure 23: Energy efficiency vs. Number of Fault Nodes

7.7 Conclusion

The implementation and evaluation of the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) demonstrate its efficacy in enhancing the performance, scalability, and security of UAV networks. By integrating blockchain technology with advanced coordination protocols, SABEC effectively mitigates coordination overhead, ensures high packet delivery rates, maintains low end-to-end delays, and optimizes energy consumption. The framework's ability to dynamically reconfigure the network in response to changing node states and malicious activities further underscores its suitability for mission-critical UAV applications.

Simulation results validate SABEC's superior performance compared to traditional coordination protocols, highlighting its resilience and efficiency in complex operational environments. The adoption of a two-tier consensus mechanism and hierarchical network structure ensures that SABEC can scale effectively while maintaining robust security and trust management.

Future work may explore the integration of machine learning algorithms for predictive trust assessments, further optimization of the consensus mechanism for enhanced energy efficiency, and real-world deployment of SABEC in diverse UAV mission scenarios to validate its performance in practical applications. Additionally, expanding SABEC’s capabilities to support heterogeneous UAV networks and incorporating adaptive security measures can further enhance its robustness and versatility, ensuring its continued relevance in the evolving landscape of UAV communications.

Chapter 8

Case Studies and Real-World Deployment

To rigorously evaluate the practical applicability and robustness of the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC), it is imperative to test the system in real-world scenarios that encapsulate the complexities inherent in Unmanned Aerial Vehicle (UAV) networks. The selection of case studies was guided by the need to demonstrate the framework's effectiveness in scenarios involving drone selection, leader drone election, and the operation of consensus protocols under realistic conditions. The chosen case study is designed to reflect diverse operational environments and challenges:

- ***Case Study:*** Swarm-Based Environmental Monitoring with Dynamic Leader Election

The scenario provides a comprehensive examination of the SABEC's capabilities, highlighting its potential to enhance UAV network performance in critical applications such as environmental surveillance and emergency response.

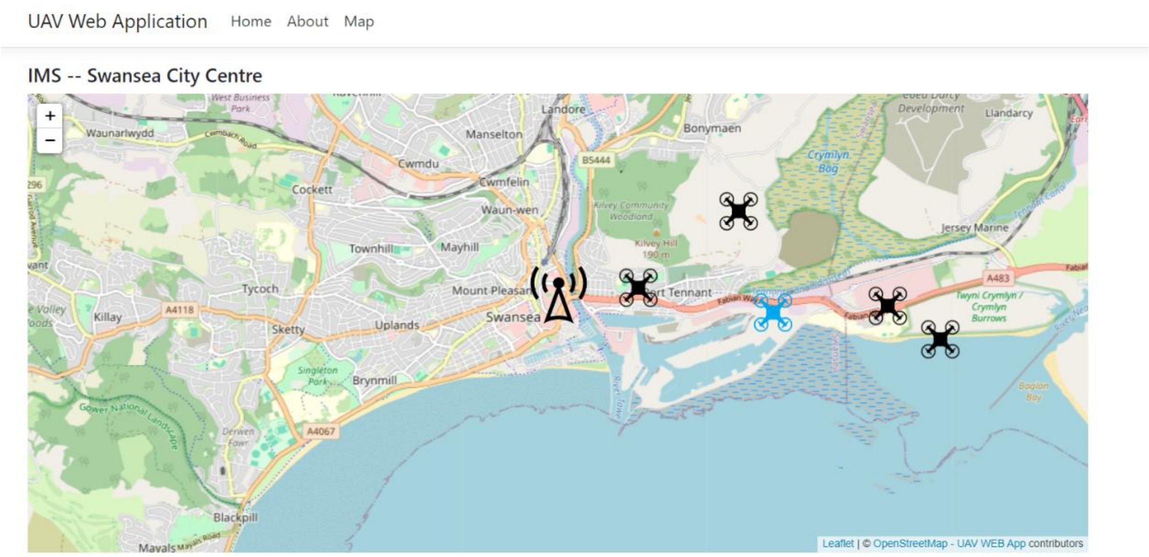


Figure 24: Real case study of the proposed Identity Management System

Clarification Note: This section is based on a conceptual scenario and does not reflect an evaluation conducted in a real-world deployment. The scenario is structured to demonstrate how the SABEC protocol would operate according to its design principles and how its performance could be measured through specific metrics. Real-world implementation tests are planned as the next step in this line of research.

8.1 Description of Case Study: Simulation of a Fire Monitoring Scenario and Byzantine Drone Detection in Swansea

The case study presented in this section is designed to evaluate the SABEC protocol within a simulation scenario that emulates real-world conditions. The scenario models a large-scale fire incident spreading across an extensive area in the city of Swansea and aims to test the protocol's capabilities in dynamic leader election, trust evaluation, consensus mechanisms, and Byzantine drone detection. This study was not conducted in a real environment; rather, it represents a conceptual case analysis intended to assess the protocol's performance and resilience in alignment with its design principles.

In the scenario, 150 unmanned aerial vehicles (UAVs) were simulated to support fire response and environmental monitoring over an area of 20 square kilometres. The swarm consists of drones with varying capabilities: high-endurance drones equipped with advanced sensors, agile drones with enhanced manoeuvrability for narrow spaces, and standard drones designed for balanced tasks. The UAVs were virtually launched from three ground control stations positioned around the city and assigned to designated operational sectors. Initially, the drones formed clusters based on their geographic locations and signal quality; these clusters were dynamically reconfigured as the fire spread, and communication conditions changed.

Two primary tasks were defined in the scenario, as shown in Figure 25. First, each cluster leader was expected to collect and process temperature and smoke data from cluster members at 5-second intervals and relay this information to the control stations. Second, the network aimed to detect and isolate drones exhibiting Byzantine behaviour. For this purpose, 10% of the swarm (15 drones) were designated as Byzantine drones, transmitting falsified temperature data deviating by more than ±50% from the cluster average (e.g., reporting below 100°C or above 800°C, while the normal temperature range was between 300°C and 600°C).

During the protocol's evaluation, SABEC's trust computation and consensus mechanisms operated concurrently with data exchange cycles. The dynamic trust threshold $\tau(t)$ was initially set as the mean trust score plus 1.5 standard deviations and was adapted during the simulation according to the rate of change in trust scores. Drones that remained below the threshold for three consecutive evaluation cycles were marked as Byzantine. Simulation outputs showed that 90% of Byzantine drones were successfully detected and isolated within the first 30 seconds, while the remaining were isolated within 60 seconds. Leader change processes were completed in an average of 2.2 seconds, and the integrity of the mission was maintained during re-clustering and leader reassignment. The key metrics obtained from the scenario included a packet delivery rate (PDR) of approximately 94%, an average end-to-end delay of 120 ms for transmissions from leaders to control stations, and a consensus validation rate of 97%. These metrics demonstrate the protocol's resilience in a simulated complex environment designed according to its architectural principles. However, it is important to emphasise that these results are not derived from a real-world deployment but from a simulation of a scenario constructed to evaluate the protocol's design performance; no actual flights or fire conditions were involved.

This case study offers a proof-of-concept that illustrates the potential applicability of the SABEC protocol in real-world operations and supports the scientific contribution of this research by demonstrating that the protocol's dynamic leader election, Byzantine detection, and adaptive consensus mechanisms function as intended. It confirms that SABEC is capable of ensuring data security and mission continuity in complex and adversarial environments. Future work should include real-world field tests to validate these findings further.

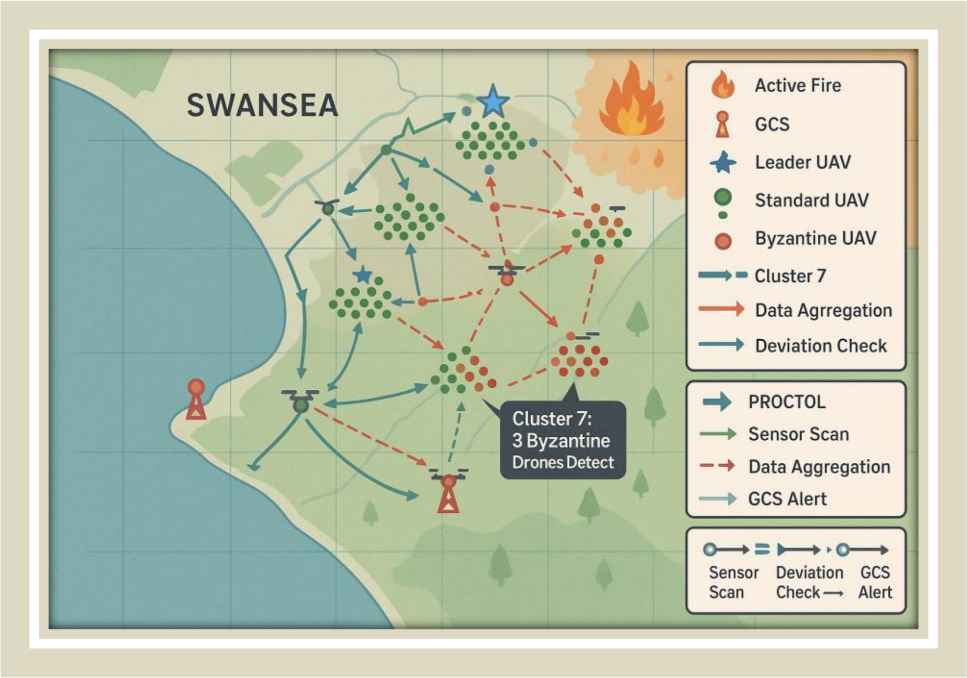


Figure 25: Fire Monitoring Scenario

Chapter 9

Discussion and Conclusions

9.1 Summary of the Research Findings

The advent of Unmanned Aerial Vehicle (UAV) networks has opened new horizons in various sectors, including surveillance, environmental monitoring, disaster management, and delivery services. This research has delved into the development and evaluation of a novel protocol aimed at enhancing the reliability, security, and efficiency of UAV networks. The proposed the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC) integrates blockchain technology with advanced coordination protocols to address the inherent challenges faced by UAV networks, such as high mobility, dynamic topology changes, and susceptibility to malicious activities.

Through comprehensive simulations and analyses, the study demonstrated that SABEC significantly improves network performance metrics, including packet delivery rate, coordination overhead, end-to-end delay, scalability, energy consumption, and security robustness. The framework effectively isolates malicious nodes, maintains high data delivery rates even in the presence of adversarial conditions, and optimizes resource utilization through hierarchical structuring and dynamic trust management.

9.2 Contributions of the Study

This thesis makes several noteworthy contributions to the field of UAV network communications. Introduced an innovative cross-tier framework that seamlessly integrates blockchain technology into UAV networks, enhancing trust management and coordination efficiency. Devised a lightweight consensus algorithm tailored for resource-constrained UAV environments, ensuring rapid and secure agreement on network trust assessments without incurring significant computational overhead. Implemented a mechanism for the real-time reconfiguration of the network topology based on trust evaluations, which effectively isolates compromised nodes and adapts to changing network conditions. Employed advanced clustering algorithms to create a scalable and efficient hierarchical network architecture, reducing coordination complexity and improving overall network performance. Conducted extensive simulations using realistic UAV network scenarios to validate the effectiveness of SABEC, comparing its performance against traditional routing protocols across multiple critical metrics.

9.3 Implications for Identity Management in UAV Networks

The integration of blockchain technology within the SABEC framework has significant implications for identity management in UAV networks. By assigning each UAV node a unique cryptographic identity and maintaining an immutable ledger of trust assessments, the framework ensures robust authentication and authorization mechanisms. This approach mitigates risks associated with identity spoofing, unauthorized access, and malicious node infiltration. Furthermore, the dynamic trust management system enables real-time monitoring and evaluation of node behaviours, allowing for prompt detection and isolation of compromised nodes. This enhances the overall security posture of the network and fosters a trustworthy environment for coordination and data exchange. The decentralized nature of blockchain also eliminates single points of failure and reduces reliance on centralized authorities, which is particularly advantageous in distributed and dynamic UAV networks.

The implications extend to regulatory compliance and interoperability, as the framework can be adapted to meet various standards and protocols required for UAV operations. By providing a secure and scalable identity management solution, SABEC facilitates the integration of UAV networks into broader communication infrastructures and supports the advancement of autonomous aerial operations.

9.4 Recommendations for Future Research

While the SABEC framework has demonstrated significant improvements over traditional protocols, several areas warrant further investigation to enhance its applicability and performance. Future research could explore incorporating machine learning algorithms for predictive trust assessments and anomaly detection. This would enable the framework to anticipate potential security threats and adapt more proactively to network changes. Investigating energy harvesting techniques and energy-aware algorithms could further reduce the energy consumption of UAV nodes, extending their operational lifespan and sustainability. Expanding the framework to support heterogeneous UAV networks, including varying UAV types and capabilities, would enhance its versatility and applicability in diverse operational contexts. Implementing the SABEC framework in real-world UAV deployments would provide valuable insights into its practical performance, scalability, and resilience under actual operational conditions. Developing adaptive security protocols that respond to evolving threats and environmental factors could strengthen the framework's ability to maintain network integrity in the face of sophisticated attacks. Exploring seamless integration with ground-based communication networks and infrastructure could enable more comprehensive coverage and coordination between aerial and terrestrial systems.

9.5 Conclusion

The research presented in this study addresses critical challenges in UAV network communications by introducing the Secure and Adaptive Blockchain-Enabled Coordination Protocol (SABEC). By leveraging blockchain technology and advanced coordination protocols, the framework enhances trust management, security, and coordination efficiency within UAV networks. The comprehensive simulations and performance evaluations demonstrate that SABEC outperforms traditional routing protocols across key metrics, particularly in environments with high node mobility and adversarial conditions. SABEC's ability to dynamically reconfigure the network in response to trust evaluations and environmental changes ensures robust and reliable operations, which are essential for mission-critical UAV applications. The framework's scalability and resource optimization make it suitable for large-scale deployments, and its security enhancements address the growing concerns of malicious activities in autonomous networks.

In conclusion, the SABEC framework represents a significant advancement in UAV network communications, offering a robust solution that meets the demands of modern applications. By addressing the limitations of existing protocols and incorporating innovative technologies, this research contributes valuable knowledge to the field and sets the stage for future developments that will further enhance the capabilities and security of UAV networks.

Bibliography

Abbas, S. M., Khan, M. A., & Boulila, W. (2024). UAVs and blockchain synergy: Enabling secure reputation-based federated learning in smart cities. IEEE Access, vol. 12, pp. 154035-154053. https://ieeexplore.ieee.org/abstract/document/10608113.

Abdulazeez, Z. Q., & Shakir, W. M. R. (2024). On the performance of the UAV-based multi-source FSO communications. International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1-5. https://ieeexplore.ieee.org/abstract/document/10721795.

Abegaz, M. S., Abishu, H. N., Yacob, Y. H., Ayall, T. A., Erbad, A., & Guizani, M. (2023). Blockchain-Based Resource Trading in Multi-UAV-Assisted Industrial IoT Networks: A Multi-Agent DRL Approach. IEEE Transactions on Network and Service Management, 20(1), 166–181. https://ieeexplore.ieee.org/document/9852754.

Abishu, H. N., Sun, G., & Yacob, Y. H. (2024). Multi-agent DRL-based consensus mechanism for blockchain-based collaborative computing in UAV-assisted 6G networks. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10726599.

Abreu, R., Simão, E., Serôdio, C., Branco, F., & Valente, A. (2024). Enhancing IoT security in vehicles: A comprehensive review of AI-driven solutions for cyber-threat detection. AI, 5(4), 2279-2299. https://doi.org/10.3390/ai5040112.

Abubakar, M. A. (2023). Blockchain-based authentication and access control mechanism for Internet of Things (IoT). (Thesis). Available at Edinburgh Napier University Repository. http://researchrepository.napier.ac.uk/Output/3406748.

Abubakar-Sadiq, M. S. (2023). Establishing secure and privacy-preserving digital identity with self-sovereign identity. (PhD Thesis). Universidade do Porto. https://repositorio-aberto.up.pt/bitstream/10216/156847/2/657403.pdf.

Achuthan, K., Hay, N., Aliyari, M., & Ayele, Y. Z. (2021). A digital information model framework for UAS-enabled bridge inspection. Energies, 14(19), 6017. https://doi.org/10.3390/en14196017.

Aditya, U. S. P. S., Singh, R., Singh, P. K., & Kalla, A. (2021). A survey on blockchain in robotics: Issues, opportunities, challenges and future directions. Journal of Network and Computer Applications, vol. 196, 103245. Retrieved from https://www.sciencedirect.com/science/article/pii/S1084804521002435.

Akram, J., & Anaissi, A. (2024). Decentralized PKI framework for data integrity in spatial crowdsourcing drone services. IEEE International Conference on Web Services (ICWS), pp. 643-653. https://ieeexplore.ieee.org/abstract/document/10707566.

Aldossri, R., Aljughaiman, A., & Albuali, A. (2024). Advancing drone operations through lightweight blockchain and fog computing integration: A systematic review. Drones, 8(4), 153. https://doi.org/10.3390/drones8040153.

Algarni, F., & Jan, S. U. (2024). PSLAPS-IoD: A Provable Secure and Lightweight Authentication Protocol for Securing Internet-of-Drones (IoD) Environment. IEEE Access, vol. 12, pp. 45948-45960. https://ieeexplore.ieee.org/abstract/document/10480416.

Al-Hamadi, H., Chen, R., Wang, D. C., & Almashan, M. (2020). Attack and defense strategies for intrusion detection in autonomous distributed IoT systems. IEEE Access, vol. 8, pp. 168994-169009. https://ieeexplore.ieee.org/abstract/document/9194704.

Ali, Z., Alzahrani, B. A., Barnawi, A., Al-Barakati, A., Vijayakumar, P., & Chaudhry, S. A. (2021). TC-PSLAP: Temporal Credential-Based Provably Secure and Lightweight Authentication Protocol for IoT-Enabled Drone Environments. Computational Technologies for Malicious Traffic Identification in IoT Networks. https://onlinelibrary.wiley.com/doi/full/10.1155/2021/9919460.

Aljohani, M., & Mukkamala, R. (2024). Information-based infrastructure in support of autonomous UAV reconnaissance missions. Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-10. https://ieeexplore.ieee.org/abstract/document/10550489.

Alkadi, R., Al-Ameri, S., & Shoufan, A. (2021). Identifying drone operator by deep learning and ensemble learning of IMU and control data. IEEE Transactions on Human-Machine Systems, vol. 51, no. 5, pp. 451-462. https://ieeexplore.ieee.org/abstract/document/9527245.

Alkanhal, M., Alali, A., & Younis, M. (2023). A distributed lightweight PUF-based mutual authentication protocol for IoV. IoT, 5(1), 1-19. https://doi.org/10.3390/iot5010001.

Alkatheiri, M. S., Saleem, S., Alqarni, M. A., & Aseeri, A. O. (2022). A lightweight authentication scheme for a network of unmanned aerial vehicles (UAVs) by using physical unclonable functions. Electronics, 11(18), 2921. https://doi.org/10.3390/electronics11182921.

Alladi, T., Bansal, G., & Chamola, V. (2020). SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15068-15077. https://ieeexplore.ieee.org/abstract/document/9237145.

Alladi, T., Chamola, V., & Kumar, N. (2020). PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. Computer Communications, vol. 160, pp. 81-90. https://www.sciencedirect.com/science/article/abs/pii/S0140366419318456.

Aloqaily, M., Bouachir, O., & Boukerche, A. (2021). Design guidelines for blockchain-assisted 5G-UAV networks. IEEE Network, vol. 35, no. 1, pp. 64-71. https://ieeexplore.ieee.org/abstract/document/9354921.

Alotaibi, S. S., Sayed, A., & Abd Elhameed, E. S. (2024). Enhancing security in IoT-assisted UAV networks using adaptive mongoose optimization algorithm with deep learning. IEEE Access, vol. 12, pp. 63768-63776. https://ieeexplore.ieee.org/abstract/document/10506908.

Alsamhi, S. H., Shvetsov, A. V., & Shvetsova, S. V. (2022). Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. IEEE Transactions on Green Communications and Networking, vol. 7, no. 1, pp. 328-338. https://ieeexplore.ieee.org/abstract/document/9852392.

Alserhani, F. (2024). Analysis of Encrypted Network Traffic for Enhancing Cyber-security in Dynamic Environments. Applied Artificial Intelligence, 38(1). https://doi.org/10.1080/08839514.2024.2381882.

Alsoliman, A., Rabiah, A. B., & Levorato, M. (2020). Privacy-preserving authentication framework for UAS traffic management systems. 4th Cyber Security in Networking Conference (CSNet), pp. 1-8. https://ieeexplore.ieee.org/abstract/document/9265534.

Al-Syouf, R. A., Bani-Hani, R. M., & Al-Jarrah, O. Y. (2024). Machine learning approaches to intrusion detection in unmanned aerial vehicles (UAVs). Neural Computing and Applications, 36, 18009–18041. https://doi.org/10.1007/s00521-024-10306-y.

Alva, A., Moreno, L. M., Asif, M., & Khalil, A. A. (2024). Secured UAV navigation: A novel intrusion detection system based on PWM signal analysis. 11th IEEE Swiss Conference on Data Science (SDS), pp. 174-180. https://ieeexplore.ieee.org/abstract/document/10675865.

Alzahrani, A. A. (2024). VSKAP-IoD: A Verifiably Secure Key Agreement Protocol for Securing IoD Environment. IEEE Access, vol. 12, pp. 58039-58056. https://ieeexplore.ieee.org/abstract/document/10499258.

Amarcha, F. A., Chehri, A., & Jakimi, A. (2024). Drones optimization for public transportation safety: Enhancing surveillance and efficiency in smart cities. IEEE World Forum on Public Safety Technology (WFPST), pp. 153-158. https://ieeexplore.ieee.org/abstract/document/10607062.

Arafat, M. Y., & Moh, S. (2019). Routing protocols for unmanned aerial vehicle networks: A survey. IEEE Access, vol. 7, pp. 99694-99720. https://ieeexplore.ieee.org/abstract/document/8772093.

Arthur, M. P. (2019). Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDS. International Conference on Computer, Information and Telecommunication Systems (CITS, pp. 1-5. https://ieeexplore.ieee.org/abstract/document/8862148.

Arun, S. L., & Tatipatri, N. (2024). A Comprehensive Review on Cyber-attacks in Power Systems: Impact Analysis, Detection and Cybersecurity. IEEE Access, vol. 12, pp. 18147-18167. https://ieeexplore.ieee.org/abstract/document/10418207.

Asilian, A., Shahinzadeh, H., & Zanjani, S. M. (2023). The role of microelectronics for smart cities, smart grids, and Industry 5.0: Challenges, solutions, and opportunities. 13th Smart Grid Conference (SGC), Tehran, Iran, Islamic Republic of, 2023, pp. 1-12. https://ieeexplore.ieee.org/abstract/document/10459310.

Badshah, A., Abbas, G., Waqas, M., & Tu, S. (2024). USAF-IoD: Ultralightweight and secure authenticated key agreement framework for Internet of Drones environment. IEEE Transactions on Vehicular Technology, vol. 73, no. 8, pp. 10963-10977. https://ieeexplore.ieee.org/abstract/document/10465668.

Badshah, A., Abbas, G., Waqas, M., & Tu, S. (2024). USAF-IoD: Ultralightweight and secure authenticated key agreement framework for Internet of Drones environment. IEEE Transactions on Vehicular Technology, vol. 73, no. 8, pp. 10963-10977. https://ieeexplore.ieee.org/abstract/document/10465668.

Bai, J., Zhu, S., & Chen, Y. (2024). The joint optimization of caching and content delivery in air-ground cooperation environment. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10742096.

Bansal, G., & Sikdar, B. (2021). Location aware clustering: Scalable authentication protocol for UAV swarms. IEEE Networking Letters, vol. 3, no. 4, pp. 177-180. https://ieeexplore.ieee.org/abstract/document/9551300.

Bansal, G., & Sikdar, B. (2021). S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms. IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12088-12100. https://ieeexplore.ieee.org/abstract/document/9551779.

Bansal, G., & Sikdar, B. (2024). Achieving secure and reliable UAV authentication: A Shamir's secret sharing based approach. IEEE Transactions on Network Science and Engineering, vol. 11, no. 4, pp. 3598-3610. https://ieeexplore.ieee.org/abstract/document/10487794.

Bansal, G., Chamola, V., & Sikdar, B. (2022). SHOTS: Scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms. IEEE Transactions on Vehicular Technology, vol. 71, no. 6, pp. 5827-5836. https://ieeexplore.ieee.org/abstract/document/9743804.

Bashlykova, A. A., & Oleinikov, A. Y. (2021). A Solution to the Problem of Interoperability for Aviation Unmanned Aerial Vehicles in the Russian Federation. 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), pp. 849-852. https://ieeexplore.ieee.org/abstract/document/9632226.

Bera, B., Bisht, A., Das, A. K., & Bhargava, B. (2024). BioKA-ASVN: Biometric-Based Key Agreement Scheme for Air Smart Vehicular Networks Using Blockchain Service. IEEE Transactions on Vehicular Technology, vol. 73, no. 7, pp. 9478-9494. https://ieeexplore.ieee.org/abstract/document/10477615.

Bera, B., Chattaraj, D., & Das, A.K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. Comput. Commun., 153, 229-249. https://www.sciencedirect.com/science/article/abs/pii/S0140366419318377.

Bertrand, S., Raballand, N., & Lala, S. (2024). Handling ground risks for road networks in UAS specific operations risk assessment (SORA). International Conference on Unmanned Aircraft Systems (ICUAS), pp. 850-857. https://ieeexplore.ieee.org/abstract/document/10556970.

Bhanurangarao, M. (2024). Enhancing hybrid object identification for instantaneous healthcare through Lorentz force. Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud), pp. 1365-1368. https://ieeexplore.ieee.org/abstract/document/10714704.

Bharany, S., Sharma, S., Badotra, S., Khalaf, O. I., Alotaibi, Y., Alghamdi, S., & Alassery, F. (2021). Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol. Energies, 14(19), 6016. https://doi.org/10.3390/en14196016.

BinSaeedan, W., Aldawsari, A., Alhussain, L., Alrushud, L., Alfawzan, L. (2023). Security Challenges for UAV Systems Communications: Potential Attacks and Countermeasures. In: Abdelkader, M., Koubaa, A. (eds) Unmanned Aerial Vehicles Applications: Challenges and Trends. Synthesis Lectures on Intelligent Technologies. Springer, Cham. https://doi.org/10.1007/978-3-031-32037-8_9.

Birtolo, C., & Ronca, D. (2013). Advances in clustering collaborative filtering by means of fuzzy C-means and trust. Expert Systems with Applications, vol. 40, iss. 17, pp. 6997-7009. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0957417413004028.

Blika, A., Palmos, S., & Doukas, G. (2024). Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: A comprehensive survey. IEEE Open Journal of the Communications Society. https://ieeexplore.ieee.org/abstract/document/10647114.

Boi, B., De Santis, M., & Esposito, C. (2024). Decentralized identity management and privacy-enhanced federated learning for automotive systems: A novel framework. IEEE 27th International Symposium on Real-Time Distributed Computing (ISORC), pp. 1-6. https://www.computer.org/csdl/proceedings-article/isorc/2024/10551371/1XIre1NnOVO.

Bozorgchenani, A., Zarakovitis, C. C., & Chien, S. F. (2022). Joint security-vs-qos framework: Optimizing the selection of intrusion detection mechanisms in 5G networks. ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security, no. 67, pp. 1 – 6. https://doi.org/10.1145/3538969.3544480.

Butt, R., Rehman, T., Tariq, N., Ashraf, M., & Humayun, M. (2024). Security of unmanned aerial vehicles. In Cybersecurity Issues and Challenges in the Drone Industry, pp. 19. IGI Global. https://www.igi-global.com/chapter/security-of-unmanned-aerial-vehicles/340080.

Cabuk, U. C., Dalkilic, G., & Dagdeviren, O. (2021). CoMAD: Context-aware mutual authentication protocol for drone networks. IEEE Access, vol. 9, pp. 78400-78414. https://ieeexplore.ieee.org/abstract/document/9440478.

Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer network simulation with ns-3: A systematic literature review. Electronics, 9(2), 272. https://doi.org/10.3390/electronics9020272.

Cecchinato, N., Toma, A., Drioli, C., Oliva, G., Sechi, G., & Foresti, G. L. (2023). Secure real-time multimedia data transmission from low-cost UAVs with a lightweight AES encryption. IEEE Communications Magazine, 61(5), 160–165. https://ieeexplore.ieee.org/abstract/document/10129046.

Chatterjee, B., Cao, N., & Raychowdhury, A. (2019). Context-aware intelligence in resource-constrained IoT nodes: Opportunities and challenges. IEEE Design & Test, vol. 36, no. 2, pp. 7-40. https://ieeexplore.ieee.org/abstract/document/8641375.

Chelloug, S. A., Alkanhel, R., Aziz, A., Muthanna, M. S. A., & Muthanna, A. (2023). Secured Reliable Communication Through Authentication and Optimal Relay Selection in Blockchain Enabled Cellular IoT Networks. IEEE Access, vol. 11, pp. 122368-122386. https://ieeexplore.ieee.org/abstract/document/10304116.

Chen, H., Zhou, R., Chan, Y. H., Jiang, Z., Chen, X., & Ngai, E. C. H. (2024). LiteChain: A lightweight blockchain for verifiable and scalable federated learning in massive edge networks. IEEE Transactions on Mobile Computing. https://ieeexplore.ieee.org/abstract/document/10740312.

Chen, K., Zhang, L., & Zhong, J. (2024). Vertical handover strategy in satellite-aerial based emergency communication networks. 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10657700.

Chen, P., Luo, L., Guo, D., Zhang, Q., & Luo, X. (2024). Frisbee: An efficient data sharing framework for UAV swarms. IEEE Transactions on Network Science and Engineering. https://ieeexplore.ieee.org/abstract/document/10716497.

Chen, R., Tseng, H.-W., Lien, J.-L., & Liao, W. (2022). Blockchain-empowered identity management with a dual identity model for UAVs in 5G networks. IEEE Internet of Things Magazine, vol. 5, no. 2, pp. 69-73. https://ieeexplore.ieee.org/abstract/document/9889266.

Chen, W., Liu, J., & Guo, H. (2020). Achieving robust and efficient consensus for large-scale drone swarm. IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15867-15879. https://ieeexplore.ieee.org/abstract/document/9254156.

Chen, X., Xiao, Z., Cheng, Y., & Hsia, C. C. (2024). FireHunter: Toward proactive and adaptive wildfire suppression via multi-UAV collaborative scheduling. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2024, pp. 1-2. https://ieeexplore.ieee.org/abstract/document/10620862.

Chen, Z., Xiong, X., Wang, W., Xiao, Y., & Alfarraj, O. (2023). A blockchain-based multi-unmanned aerial vehicle task processing system for situation awareness and real-time decision. Sustainability, 15(18), 13790. https://www.mdpi.com/2071-1050/15/18/13790.

Cheng, C. F., Srivastava, G., Lin, J. C. W., & Lin, Y. C. (2022). A consensus protocol for unmanned aerial vehicle networks in the presence of byzantine faults. Computers and Electrical Engineering, 99, 107774. https://www.sciencedirect.com/science/article/pii/S0045790622000763.

Cheng, J., Mahmud, S., & Mohammed, M. (2024). Design of a novice-friendly drone control system. IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0184-0190. https://ieeexplore.ieee.org/abstract/document/10427804.

Cheval, V., Cortier, V., & Turuani, M. (2018). A little more conversation, a little less action, a lot more satisfaction: Global states in ProVerif. 2018 IEEE 31st Computer Security Foundations Symposium (CSF), 344–358. https://ieeexplore.ieee.org/document/8429316.

Cho, G., Cho, J., Hyun, S., & Kim, H. (2020). SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles. Applied Sciences, 10(9), 3149. Retrieved from https://www.mdpi.com/2076-3417/10/9/3149.

Chung, S. J., Paranjape, A. A., & Dames, P. (2018). A survey on aerial swarm robotics. IEEE Transactions on Robotics. IEEE Transactions on Robotics, vol. 34, no. 4, pp. 837-855. https://ieeexplore.ieee.org/abstract/document/8424838.

Cirillo, F., Solmaz, G., Berz, E. L., & Bauer, M. (2019). A standard-based open source IoT platform: FIWARE. IEEE Internet of Things Magazine, vol. 2, no. 3, pp. 12-18. https://ieeexplore.ieee.org/abstract/document/8950963.

Consul, P., Budhiraja, I., & Garg, D. (2024). Task offloading in AIoT-enabled UAV-assisted MEC network: A digital twin-empowered approach with FedRL. IEEE Transactions on Consumer Electronics. https://ieeexplore.ieee.org/abstract/document/10705107.

Cook, A., & Vigano, L. (2020). A Game Of Drones: Extending the Dolev-Yao Attacker Model With Movement. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 280-292. https://ieeexplore.ieee.org/abstract/document/9229681.

Cox, J., Hanheide, M., & Polvara, R. (2024). AGRIDS: An advanced multi-modal mapping architecture for robotics and agriculture. IEEE 20th International Conference on Automation Science and Engineering (CASE), pp. 2531-2536. https://ieeexplore.ieee.org/abstract/document/10711678.

Cremonezi, B., Vieira, A. B., Nacif, J., & Silva, E. F. (2024). Identity management for Internet of Things: Concepts, challenges and opportunities. Elsevier Computer Communications, vol. 224, pp. 72-94. https://doi.org/10.1016/j.comcom.2024.05.014.

Cui, X., Tian, Y., Zhang, X., Lin, H. W., & Li, M. (2024). A lightweight certificateless edge-assisted encryption for IoT devices: Enhancing security and performance. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10736996.

Cui, Y., Liang, Y., Luo, Q., Shu, Z., & Huang, T. (2024). Resilient consensus control of heterogeneous multi-UAV systems with leader of unknown input against Byzantine attacks. IEEE Transactions on Automation Science and Engineering. https://ieeexplore.ieee.org/abstract/document/10584430.

Cumino, P., Maciel, K., Tavares, T., Oliveira, H., Rosário, D., & Cerqueira, E. (2019). Cluster-Based Control Plane Messages Management in Software-Defined Flying Ad-Hoc Network. Sensors (Basel), 20(1), 67. https://pmc.ncbi.nlm.nih.gov/articles/PMC6983144/.

Damaj, I., Kasbah, S. (2019). Integrated Mobile Solutions in an Internet-of-Things Development Model. In: Paiva, S. (eds) Mobile Solutions and Their Usefulness in Everyday Life. EAI/Springer Innovations in Communication and

Computing. Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-93491-4_1.

Das, A. K., Bera, B., Wazid, M., Jamal, S. S., & Park, Y. (2021). iGCACS-IoD: An improved certificate-enabled generic access control scheme for Internet of Drones deployment. IEEE Access, 9, 87024-87048. https://doi.org/10.1109/ACCESS.2021.3089871.

Day, M. A., Clement, M. R., & Russo, J. D. (2015). Multi-UAV software systems and simulation architecture. International Conference on Unmanned Aircraft Systems (ICUAS), pp. 426-435. https://ieeexplore.ieee.org/abstract/document/7152319.

Deebak, B. D., & Hwang, S. O. (2023). Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era. Computer Networks, vol. 225, 109664. Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S1389128623001093.

Din, N., Waheed, A., Zareei, M., & Alanazi, F. (2021). An improved identity-based generalized signcryption scheme for secure multi-access edge computing empowered flying ad hoc networks. IEEE Access, 9, 120704–120714. https://ieeexplore.ieee.org/document/9523850.

Ding, Y., Yang, Z., Pham, Q. V., & Hu, Y. (2023). Distributed machine learning for UAV swarms: Computing, sensing, and semantics. IEEE Internet of Things Journal, vol. 11, no. 5, pp. 7447-7473. https://ieeexplore.ieee.org/abstract/document/10353003.

Dogan, H. (2023). Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme. 2023 7th International Conference on Cryptography, Security and Privacy (CSP), Tianjin, China, 2023, pp. 13-21. https://ieeexplore.ieee.org/document/10235922.

Dong, C., Jiang, F., Chen, S., & Liu, X. (2022). Continuous authentication for UAV delivery systems under zero-trust security framework. IEEE International Conference on Edge Computing and Communications (EDGE), pp. 123-132. https://ieeexplore.ieee.org/abstract/document/9860313.

Dong, C., Jiang, F., Li, X., Yao, A., & Li, G. (2021). A blockchain-aided self-sovereign identity framework for edge-based UAV delivery system. IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid), pp. 622-624. https://ieeexplore.ieee.org/abstract/document/9499580.

Dong, C., Zhou, J., An, Q., Jiang, F., Chen, S., Pan, L., & Liu, X. (2023). Optimizing Performance in Federated Person Re-identification Through Benchmark Evaluation for Blockchain-Integrated Smart UAV Delivery Systems. Drones 2023, 7(7), 413. https://doi.org/10.3390/drones7070413.

Du, P., Xiao, T., Cao, H., & Zhai, D. (2024). AI-based UAVs 3D coverage deployment in 6G-enabled IoV networks for Industry 5.0. IEEE Transactions on Consumer Electronics. https://ieeexplore.ieee.org/abstract/document/10716736.

Duan, X., Zhao, Y., Tian, D., Zhou, J., & Ma, L. (2023). Joint communication and control optimization of a UAV-assisted multi-vehicle platooning system in uncertain communication environment. IEEE Transactions on Vehicular

Technology, vol. 73, no. 3, pp. 3177-3190. https://ieeexplore.ieee.org/abstract/document/10304322.

Ejiyeh, A. M. (2024). Secure, robust, and energy-efficient authenticated data sharing in drone to vehicles communications. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 380-389. https://ieeexplore.ieee.org/abstract/document/10628700.

Erdelj, M., Król, M., & Natalizio, E. (2017). Wireless sensor networks and multi-UAV systems for natural disaster management. Computer Networks, vol. 124, pp. 72-86. https://www.sciencedirect.com/science/article/abs/pii/S1389128617302220.

F. Cunico, F., Aldegheri, S., Avogaro, A., & Boldo, M. (2024). Enhancing safety and privacy in Industry 4.0: The ICE Laboratory case study.12, pp. 154570-154599, 2024. https://ieeexplore.ieee.org/abstract/document/10716394.

Fagin, R. (1982). Horn clauses and database dependencies. Journal of the ACM (JACM), 29(4), 952–985. https://dl.acm.org/doi/abs/10.1145/322344.322347.

Fan, X., Wu, P., Sun, T., Zhao, J., & Xia, M. (2024). UAV-based coverage hole detection and recovery for large-scale IoT networks. In 2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops), pp. 317–322. https://ieeexplore.ieee.org/abstract/document/10693829.

Fang, H., Wang, X., Xiao, Z., & Hanzo, L. (2022). Autonomous collaborative authentication with privacy preservation in 6G: From homogeneity to heterogeneity. IEEE Network, vol. 36, no. 6, pp. 28-36. https://ieeexplore.ieee.org/abstract/document/9839653.

Faraji, M., Kang, J. M., Bannazadeh, H., & Leon-Garcia, A. (2014). Identity access management for Multi-tier cloud infrastructures. IEEE Network Operations and Management Symposium (NOMS), pp. 1-9. https://ieeexplore.ieee.org/document/6838229.

Farithkhan, A., Ruby, E. D. K., & Prabha, M. (2024). Improving FANET communication with a QoS optimized location-aided routing protocol. 5th International Conference on Smart Electronics and Communication (ICOSEC), pp. 630-635. https://ieeexplore.ieee.org/abstract/document/10722211.

Finn, R. L., Wright, D., Jacques, L., & De Hert, P. (2014). Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations. Luxembourg: Final Report. https://www.politico.eu/wp-content/uploads/2019/08/Study-on-privacy-data-protection-and-ethical-risks-in-civil-RPAS-operations-1.pdf.

Ganesan, T., Jayarajan, N., & Shri Varun, B. G. (2024). Dynamic control, architecture, and communication protocol for swarm unmanned aerial vehicles. In Naganathan, A., Jayarajan, N., & Bin Ibne Reaz, M. (Eds.), Computing in intelligent transportation systems. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-031-38669-5_3.

Garg, S., Singh, A., Batra, S., Kumar, N., & Yang, L. T. (2018). UAV-empowered edge computing environment for cyber-threat detection in smart vehicles. IEEE

Network, vol. 32, no. 3, pp. 42-51. https://ieeexplore.ieee.org/abstract/document/8370877.

Garzon, S. R., Yildiz, H., & Küpper, A. (2022). Decentralized identifiers and self-sovereign identity in 6G. IEEE Network, vol. 36, no. 4, pp. 142-148. https://ieeexplore.ieee.org/abstract/document/9919761.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), 3–16. Association for Computing Machinery. https://doi.org/10.1145/2976749.2978341.

Ghourab, E. M., Jaafar, W., Bariah, L., Muhaidat, S., Yanikomeroglu, H., & Naser, S. (2023). Interplay between physical layer security and blockchain technology for 5G and beyond: A comprehensive survey. TechRxiv. https://www.techrxiv.org/doi/full/10.36227/techrxiv.21601848.v2.

Giambene, G., Addo, E. O., & Chen, Q. (2024). Design and analysis of low-power IoT in remote areas with NTN opportunistic connectivity. IEEE Transactions on Aerospace and Electronic Systems. https://ieeexplore.ieee.org/abstract/document/10702435.

Giuliari, G., Sonnino, A., Frei, M., Streun, F., Kokoris-Kogias, L., & Perrig, A. (2024). An empirical study of consensus protocols' DoS resilience. In Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), pp. 1345–1360. Association for Computing Machinery. https://doi.org/10.1145/3634737.3656997.

González, C. C., Pupo, E. F., & Montalban, J. (2024). Federated learning-based unicast/multicast service delivery over 6G O-RAN framework. IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10608261.

Granieri, F. (2024). Navigating the skies: A cross-country exploration of drone policies in Europe, USA, and China, unveiling privacy and cybersecurity challenges. Journal of Law, Market & Innovation, vol. 3 no. 2. Retrieved from https://doi.org/10.13135/2785-7867/10740.

Guo, K., Wu, M., Li, X., & Lin, Z. (2024). Joint trajectory and beamforming optimization for federated DRL-aided space-aerial-terrestrial relay networks with RIS and RSMA. IEEE Transactions on Wireless Communications. https://ieeexplore.ieee.org/abstract/document/10719633.

Guo, Z., Cao, J., Wang, X., Zhang, Y., Niu, B., & Li, H. (2024). UAV-assisted vehicular authentication scheme in edge computing networks. IEEE Internet of Things Journal, vol. 11, no. 12, pp. 22091-22106. https://ieeexplore.ieee.org/abstract/document/10478495.

Gupta, R., Patel, M. M., & Tanwar, S. (2021). Blockchain-based data dissemination scheme for 5G-enabled softwarized UAV networks. IEEE Transactions on Green Communications and Networking, vol. 5, no. 4, pp. 1712-1721. https://ieeexplore.ieee.org/document/9531961.

Gupta, S., Maple, C., & Passerone, R. (2023). An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles. IEEE Access, 11, 90641–90669. https://ieeexplore.ieee.org/abstract/document/10226207.

Hadi, H. J., Cao, Y., Li, S., Hu, Y., Wang, J., & Wang, S. (2024). Real-time collaborative intrusion detection system in UAV networks using deep learning. IEEE Internet of Things Journal, 11(20), 33371–33391. https://ieeexplore.ieee.org/abstract/document/10594772.

Hafeez, S. (2024). Blockchain-based secure Unmanned Aerial Vehicles (UAV) in network design and optimization (Doctoral dissertation). University of Glasgow. Available at https://theses.gla.ac.uk/84460/.

Haider, S. K., Jiang, A., Almogren, A., Rehman, A. U., Ahmed, A., Khan, W. U., & Hamam, H. (2021). Energy efficient UAV flight path model for cluster head selection in next-generation wireless sensor networks. Sensors, 21(24), 8445. https://www.mdpi.com/1424-8220/21/24/8445.

Han, L., Xun, Y., Liu, J., Benslimane, A., & Zhang, Y. (2023). DP-Authentication: A novel deep learning based drone pilot authentication scheme. Ad Hoc Networks, vol. 147, 103180. Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S1570870523001002.

Hansen, K. S., Bruun, F. M., & Sermsar, F. (2024). Comparative analysis of SSD and Faster R-CNN in UAV-based vehicle detection. 8th International Artificial Intelligence and Data Processing Symposium (IDAP), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10711057.

Hawashin, D., Nemer, M., Gebreab, S. A., & Salah, K. (2024). Blockchain applications in UAV industry: Review, opportunities, and challenges. Journal of Network and Computer Applications, vol 230, pp.103932. https://doi.org/10.1016/j.jnca.2024.103932.

Hawashin, D., Nemer, M., Gebreab, S. A., Salah, K., Jayaraman, R., Khan, M. K., & Damiani, E. (2024). Blockchain applications in UAV industry: Review, opportunities, and challenges. Journal of Network and Computer Applications, vol. 230, 103932, ISSN 1084-8045. https://doi.org/10.1016/j.jnca.2024.103932.

Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2624-2661. https://ieeexplore.ieee.org/document/7463007.

Hazra, A., Adhikari, M., & Amgoth, T. (2021). A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. ACM Computing Surveys (CSUR), vol. 55, Issue 1, no. 9, pp. 1 – 35. https://dl.acm.org/doi/abs/10.1145/3485130.

He, D., Yang, G., Li, H., Chan, S., & Cheng, Y. (2020). An effective countermeasure against UAV swarm attack. IEEE Network, vol. 35, no. 1, pp. 380-385. https://ieeexplore.ieee.org/abstract/document/9183792.

Hildmann, H., & Kovacs, E. (2019). Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security, and public safety. Drones, 3(3), 59. https://doi.org/10.3390/drones3030059.

Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661. https://www.sciencedirect.com/science/article/abs/pii/S0167404823005710.

Hosseini, S. M., Ferreira, J., & Bartolomeu, P. C. (2023). Blockchain-based decentralized identification in IoT: An overview of existing frameworks and their limitations. Electronics 2023, 12(6), 1283. https://doi.org/10.3390/electronics12061283.

Hu, S., Wu, Q., & Wang, X. (2020). Energy management and trajectory optimization for UAV-enabled legitimate monitoring systems. IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 142-155. https://ieeexplore.ieee.org/abstract/document/9201322.

Hughes, I., Pupo, A., Wynd, J., & Thurlow, Z. (2024). Securing the unprotected: Enhancing heartbeat messaging for MAVLink UAV communications. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10690216.

Ibrahim, A. G., Awad, M. I., & Shehata, O. M. (2024). Blockchain-Based Framework for Secure Robotics Communication. Intelligent Methods, Systems, and Applications (IMSA), pp. 348-354. https://ieeexplore.ieee.org/abstract/document/10652730.

Ihekoronye, V. U., Nwakanma, C. I., & Kim, D. S. (2024). ASR-Fed: Agnostic straggler-resilient semi-asynchronous federated learning technique for secured drone network. International Journal of Machine Learning and Cybernetics, 15, 5303–5319. https://doi.org/10.1007/s13042-024-02238-9.

Ihekoronye, V., Nwakanma, C. I., Kim, D.-S., & Lee, J. M. (2023). DATA-FedAVG: Delay-aware truncated accuracy-based federated averaging for intrusion detection in UAV network. The Journal of Korean Institute of Communications and Information Sciences, 48(6), 648–668. https://www.researchgate.net/publication/370953371_DATA-FedAVG_Delay-Aware_Truncated_Accuracy-Based_Federated_Averaging_for_Intrusion_Detection_in_UAV_Network.

Islam, A., & Shin, S. Y. (2019). Bus: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in Internet of Things. IEEE Access, vol. 7, pp. 103231-103249. https://ieeexplore.ieee.org/abstract/document/8771158.

Jacobsen, R. H., & Marandi, A. (2021). Security threats analysis of the unmanned aerial vehicle system. MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), 316–322. https://ieeexplore.ieee.org/abstract/document/9652900.

Jadhav, P., Misbahuddin, M., Chippalkatti , S. S., & Sudarsan, S. D. (2024). PKI-enabled authentication and encryption for enhanced drone communication. IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), pp. 1-10. https://ieeexplore.ieee.org/abstract/document/10727500.

Jain, A., Barke, S., Garg, M., Gupta, A., Narwal, B., & Mohapatra, A. K. (2024). A Walkthrough of Blockchain-Based Internet of Drones Architectures. IEEE

Internet of Things Journal, vol. 11, no. 21, pp. 34924-34940. https://ieeexplore.ieee.org/abstract/document/10643145.

Jaiswal, A., Shivateja, S., & Hazra, A. (2024). UAV-enabled mobile RAN and RF-energy transfer protocol for enabling sustainable IoT in energy-constrained networks. IEEE Transactions on Green Communications and Networking, vol. 8, no. 3, pp. 1118-1127. https://ieeexplore.ieee.org/abstract/document/10536022.

Jan, S. U., Abbasi, I. A., & Algarni, F. (2022). A mutual authentication and cross verification protocol for securing Internet-of-Drones (IoD). Computers, Materials & Continua, 72(3), pp. 5845-5869. https://www.researchgate.net/publication/360106330_A_Mutual_Authentication_and_Cross_Verification_Protocol_for_Securing_Internet-of-Drones_IoD.

Jan, S. U., Abbasi, I. A., Algarni, F., & Khan, A. S. (2022). A verifiably secure ECC based authentication scheme for securing IoD using FANET. IEEE Access, 10, 95321–95343. https://ieeexplore.ieee.org/abstract/document/9877803.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. 2012 IEEE Conference on Technologies for Homeland Security (HST), 585–590. https://ieeexplore.ieee.org/abstract/document/6459914.

Javed, S., Hassan, A., Ahmad, R., & Ahmed, W. (2024). State-of-the-art and future research challenges in UAV swarms. IEEE Internet of Things Journal, vol. 11, no. 11, pp. 19023-19045. https://ieeexplore.ieee.org/abstract/document/10430396.

Jensen, I. J., & Selvaraj, D. F. (2019). Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs). IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 1-7. https://ieeexplore.ieee.org/abstract/document/8793027.

Jia, K., Yang, D., Wang, Y., Shui, T., & Liu, C. (2024). Energy Efficient and Balanced Task Assignment Strategy for Multi-UAV Patrol Inspection System in Mobile Edge Computing Network. IEEE Transactions on Network Science and Engineering. https://ieeexplore.ieee.org/abstract/document/10739907.

Jiang, C., Fang, Y., & Zhao, P. (2020). Intelligent UAV identity authentication and safety supervision based on behavior modeling and prediction. IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6652-6662. https://ieeexplore.ieee.org/abstract/document/8960477.

Jiang, H., Li, N., & Yi, P. (2024). PUBA: A physical undirected backdoor attack in vision-based UAV detection and tracking systems. International Joint Conference on Neural Networks (IJCNN), pp. 1-8. https://ieeexplore.ieee.org/abstract/document/10650950.

Jin, C., Yao, H., Mai, T., Xu, J., & Zhang, Q. (2024). A resource-efficient content sharing mechanism in large-scale UAV named data networking. IEEE/ACM Transactions on Networking. https://ieeexplore.ieee.org/abstract/document/10716865.

Jin, Y., Minai, A. A., & Polycarpou, M. M. (2003). Cooperative real-time search and task allocation in UAV teams. 42nd IEEE International Conference on

Decision and Control, pp. 7-12 Vol.1. https://ieeexplore.ieee.org/abstract/document/1272527.

Juárez, R., & Bordel, B. (2023). Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. Electronics, 12(23), 4794. https://doi.org/10.3390/electronics12234794.

Kafetzis, D., Vassilaras, S., Vardoulias, G., & Koutsopoulos, I. (2022). Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions. IEEE Access, 10, 9989–10014. https://ieeexplore.ieee.org/abstract/document/9684421.

Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A Systematic Literature Review on Wireless Security Testbeds in the Cyber-Physical Realm. Computers & Security, vol. 133, 103383. https://www.sciencedirect.com/science/article/pii/S0167404823002936.

Karmakar, R., & Kaddoum, G. (2023). A blockchain-based distributed and intelligent clustering-enabled authentication protocol for UAV swarms. IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 6178-6195. https://ieeexplore.ieee.org/abstract/document/10264210.

Karuppaiah, J., Aarthi, C., Girirajan, M., Jananai, M., & P. B., D. (2022). Secure Smart Healthcare Surveillance Framework Using Fuzzy C-Means Clustering with Effective Ant Colony Optimization in Internet of Things. Proceedings of the 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), 1–5. https://ieeexplore.ieee.org/document/10060099.

Kayalvizhi, M., & Ramamoorthy, S. (2022). Meta-heuristic optimal path planning in blockchain-aided UAV swarm network. Futuristic Trends in Networks and Computing Technologies. Lecture Notes in Electrical Engineering, vol 936. Springer, Singapore. https://doi.org/10.1007/978-981-19-5037-7_13.

Keshavarz, M., Gharib, M., Afghah, F., & Ashdown, J. D. (2020). UASTrustChain: A decentralized blockchain-based trust monitoring framework for autonomous unmanned aerial systems. IEEE Access, vol. 8, pp. 226074-226088. https://ieeexplore.ieee.org/abstract/document/9293278.

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., & Tariq, M. A. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computing, 23(3), 2067–2087. https://doi.org/10.1007/s10586-020-03058-6.

Khan, A. A., Laghari, A. A., Gadekallu, T. R., Shaikh, Z. A., Javed, A. R., Rashid, M., Estrela, V. V., & Mikhaylov, A. (2022). A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment. Computers and Electrical Engineering, 102, 108234. https://www.sciencedirect.com/science/article/abs/pii/S0045790622004700.

Khan, A. S., Sattar, M. A., Nisar, K., Ibrahim, A. A. A., & Annuar, N. B. (2022). A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues, and future directions. Applied Sciences, 13(1), 277. https://www.mdpi.com/2076-3417/13/1/277.

Khan, I. U., Shah, S. B. H., Wang, L., Aziz, M. A., Stephan, T., & Kumar, N. (2021). Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. International Journal of Communication Systems, 34(9), e4885. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4885.

Khan, M. A., Alsamhi, S. H., & Barb, G. (2024). Security and privacy issues and solutions for UAVs in B5G networks: A review. IEEE Transactions on Network and Service Management. https://ieeexplore.ieee.org/abstract/document/10737101.

Khan, M. A., Javaid, S., & Mohsan, S. A. H. (2024). Future-proofing security for UAVs with post-quantum cryptography: A review. IEEE Open Journal of the Communications Society. https://ieeexplore.ieee.org/abstract/document/10737027.

Khan, M. A., Kumar, N., & Mohsan, S. A. H. (2022). Swarm of UAVs for network management in 6G: A technical review. IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 741-761. https://ieeexplore.ieee.org/abstract/document/9915455.

Khan, M. A., Kumar, N., Alsamhi, S. H., & Barb, G. (2024). Security and privacy issues and solutions for UAVs in B5G networks: A review. IEEE Transactions on Network and Service Management. https://ieeexplore.ieee.org/abstract/document/10737101.

Khan, M. J., Fang, B., Cimino, G., & Cirillo, S. (2024). Privacy-preserving artificial intelligence on edge devices: A homomorphic encryption approach. IEEE International Conference on Web Services (ICWS), pp. 395-405. https://ieeexplore.ieee.org/abstract/document/10707429.

Khanh, Q. V., Chehri, A., & Nam, V. H. (2024). Performance evaluation of routing protocol for 6G UAV communication networks. IEEE 99th Vehicular Technology Conference (VTC2024-Spring), pp. 1-5. https://ieeexplore.ieee.org/abstract/document/10683157.

Khor, J. H., Sidorov, M., Law, S. Z., Tan, S. Y., & Woon, P. Y. (2023). Public blockchain-based data integrity protection for federated learning in UAV networks using MAVLink protocol. International Conference on Green Energy, Computing and Intelligent Technology, Electrical Engineering (LNEE), vol. 1142, pp. 321–333. https://link.springer.com/chapter/10.1007/978-981-99-9833-3_23.

Khowaja, S. A., Khuwaja, P., Dev, K., Lee, I. H., Khan, W. U., & Wang, W. (2022). A secure data sharing scheme in community segmented vehicular social networks for 6G. IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 890-899. https://ieeexplore.ieee.org/document/9816030.

Kobeissi, N., Bhargavan, K., & Blanchet, B. (2017). Automated verification for secure messaging protocols and their implementations: A symbolic and computational approach. IEEE European Symposium on Security and Privacy (EuroS&P), pp. 435-450. https://ieeexplore.ieee.org/document/7961995.

Kong, L., Chen, B., & Hu, F. (2022). LAP-BFT: Lightweight asynchronous provable Byzantine fault-tolerant consensus mechanism for UAV network. Drones, 6(8), 187. https://doi.org/10.3390/drones6080187.

Kourtis, M. A., Xilouris, G., & Oikonomakis, A. (2023). Integration of drone connectivity in 5G: An examination of the OASEES framework. IEEE Future Networks World Forum (FNWF), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10520379.

Kumar, L., Pham, V. Q., Khan, F., Piran, J., & Dev, K. (2021). Blockchain for securing aerial communications: Potentials, solutions, and research directions. Physical Communication, 47(9), 10139. https://www.researchgate.net/publication/352058069_Blockchain_for_securing_aerial_communications_Potentials_solutions_and_research_directions.

Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). A taxonomy of blockchain-enabled softwarization for secure UAV network. Computer Communications, vol. 161, pp. 304-323. Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S0140366420318545.

Kundu, J., Alam, S., Das, J. C., Dey, A., & De, D. (2024). Trust based Flying ad-hoc network: A survey. IEEE Access, vol. 12, pp. 99258-99281. https://ieeexplore.ieee.org/abstract/document/10574806.

Kurt, A., Saputro, N., Akkaya, K., & Uluagac, A. S. (2021). Distributed connectivity maintenance in swarm of drones during post-disaster transportation applications. IEEE Transactions on Intelligent Transportation Systems, 22(9), 6061–6073. https://ieeexplore.ieee.org/abstract/document/9385994.

Küsters, R., & Truderung, T. (2009). Using ProVerif to analyze protocols with Diffie-Hellman exponentiation. 22nd IEEE Computer Security Foundations Symposium, pp. 157-171. https://ieeexplore.ieee.org/abstract/document/5230620.

Kwon, D., Son, S., Kim, M. H., & Lee, J. Y. (2024). A secure self-certified broadcast authentication protocol for intelligent transportation systems in UAV-assisted mobile edge computing environments. IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 11, pp. 19004-19017. https://ieeexplore.ieee.org/abstract/document/10606320.

Labib, N. S., Brust, M. R., Danoy, G., & Bouvry P. (2019). Trustworthiness in IoT – A standards gap analysis on security, data protection and privacy. IEEE Conference on Standards for Communications and Networking (CSCN), pp. 1-7. https://ieeexplore.ieee.org/abstract/document/8931393.

Lakew, D. S., Sa'ad, U., Dao, N. N., Na, W., & Cho, S. (2020). Routing in Flying Ad Hoc Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 22(2), 1071–1120. https://ieeexplore.ieee.org/abstract/document/9044378.

Latif, Z., Lee, C., Sharif, K., & Helal, S. (2022). SDBlockEdge: SDN-blockchain enabled multihop task offloading in collaborative edge computing. IEEE Sensors Journal, vol. 22, no. 15, pp. 15537-15548. https://ieeexplore.ieee.org/abstract/document/9810819.

Lei, Y., Zeng, L., Li, Y. X., Wang, M. X., & Qin, H. (2021). A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access, vol. 9, pp. 53769-53785. https://ieeexplore.ieee.org/abstract/document/9393888.

Li, B., Fei, Z., & Zhang, Y. (2018). UAV communications for 5G and beyond: Recent advances and future trends. IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2241-2263. https://ieeexplore.ieee.org/abstract/document/8579209.

Li, B., Fei, Z., Zhang, Y., & Guizani, M. (2019). Secure UAV communication networks over 5G. IEEE Wireless Communications, vol. 26, no. 5, pp. 114-120. https://ieeexplore.ieee.org/abstract/document/8758975.

Li, M., & Zhang, N. (2022). Trajectory-Based Authenticated Key Establishment for Dynamic Internet of Things. IEEE Access, 10, 111419–111448. https://ieeexplore.ieee.org/abstract/document/9923764.

Li, T., Zhang, J., Obaidat, M. S., Lin, C., & Lin, Y. (2021). Energy-efficient and secure communication toward UAV networks. IEEE Internet of Things Journal, vol. 9, no. 12, pp. 10061-10076. https://ieeexplore.ieee.org/abstract/document/9560132.

Li, Y., Li, Q., Yu, H., & Li, L. (2024). TAAODV: TOPSIS-Aided AODV Routing Protocol to diffuse mass information in the unstable and high-density UAV ad hoc networks. IEEE Transactions on Intelligent Transportation Systems. https://ieeexplore.ieee.org/abstract/document/10706810.

Liang, Q., Hu, Y., Yan, Y., & Zhou, L. (2024). Drone target detection based on improved YOLOv5s algorithm. IEEE 43rd Chinese Control Conference, pp. 8357-8362. https://ieeexplore.ieee.org/abstract/document/10661446.

Liu, Y., Gao, J., Lu, Y., Cao, R., Yao, L., Xia, Y., & Han, D. (2024). Lightweight blockchain-enabled secure data sharing in dynamic and resource-limited UAV networks. IEEE Network, vol. 38, no. 4, pp. 25-31. https://ieeexplore.ieee.org/abstract/document/10485478.

Lou, T., Wang, Y., Yue, Z., & Zhao, L. (2024). Multi-UAV collaborative trajectory planning for 3D terrain based on CS-GJO algorithm. Complex System Modeling and Simulation, vol. 4, no. 3, pp. 274-291. https://ieeexplore.ieee.org/abstract/document/10737157.

Luo, Y., Tang, F., Zhang, H., & Yang, D. (2024). Synchronous position-attitude loop regulation-based distributed optimal trajectory tracking control for multi-UAVs formation with external disturbances. IEEE Transactions on Systems, Man, and Cybernetics: Systems. https://ieeexplore.ieee.org/abstract/document/10677375.

Ma, Z., & Zhang, J. (2023). Efficient, traceable and privacy-aware data access control in distributed cloud-based IoD systems. IEEE Access, vol. 11, pp. 45206-45221.

Maaloul, R., & Chaari, L. (2025). Authentication communication by using visualization cryptography for UAV networks. Computer Standards & Interfaces, vol. 92, 103918. https://www.sciencedirect.com/science/article/abs/pii/S0920548924000874.

Mabrek, Z. (2024). IoT Network Dynamic Clustering and Communication for Surveillance UAV's. (PhD Thesis). Université de Guelma. https://dspace.univ-guelma.dz/jspui/handle/123456789/15872.

Mahdoui, N., Natalizio, E., & Fremont, V. (2016). Multi-UAVs network communication study for distributed visual simultaneous localization and mapping. 2016 International Conference on Computing, Networking, and Communications (ICNC), 1-5. https://ieeexplore.ieee.org/abstract/document/7440564.

Manavadaria, M. S., & Sasikala, D. (2024). Automated detection and alerting system for wheat leaf diseases using the VGG16 deep learning model. International Conference on Data Science and Network Security (ICDSNS), pp. 1-5. https://ieeexplore.ieee.org/abstract/document/10690870.

Manikandan, K., & Sriramulu, R. (2023). ASMTP: Anonymous Secure Messaging Token-Based Protocol Assisted Data Security in Swarm of Unmanned Aerial Vehicles. International Journal of Network Management. Wiley Online Library. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/nem.2271.

Mao, H., Liu, Y., Xiao, Z., & Han, Z. (2024). Energy efficient defense against cooperative hostile detection and eavesdropping attacks for UAV-aided short-packet transmissions. IEEE Transactions on Vehicular Technology. https://ieeexplore.ieee.org/abstract/document/10721449.

Mbaya, E. B., Adetiba, E., Badejo, J. A., Wejin, J. S., Oshin, O., & Isife, O. (2023). SecFedIDM-V1: A Secure Federated Intrusion Detection Model With Blockchain and Deep Bidirectional Long Short-Term Memory Network. IEEE Access, vol. 11, pp. 116011-116025. https://ieeexplore.ieee.org/document/10287938.

Medhi, J. K., Liu, R., Wang, Q., & Chen, X. (2023). Robust Multiagent Reinforcement Learning for UAV Systems: Countering Byzantine Attacks. Information, 14(11), 623. https://www.mdpi.com/2078-2489/14/11/623.

Megala, G., Sevugan, P., & Swarnalatha, P. (2022). A review on blockchain-based device authentication schemes for IoT. (Book). In Blockchain for IoT. Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003188247-3/review-blockchain-based-device-authentication-schemes-iot-megala-prabu-sevugan-swarnalatha.

Mei, Z., Yuwen, Q., Cai, H., & Shi, L. (2024). A blockchain-assisted lightweight UAV network authentication mechanism via covert communication. Chinese Journal of Aeronautics. https://doi.org/10.1016/j.cja.2024.08.019.

Merah, M., Aliouat, Z., Harbi, Y., & Batta, M. S. (2023). Machine learning-based clustering protocols for Internet of Things networks: An overview. International Journal of Communication Systems, 36(10). Wiley. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.5487.

Michailidis, E. T., & Vouyioukas, D. (2022). A review on software-based and hardware-based authentication mechanisms for the internet of drones. Drones, 6(2), 41. https://doi.org/10.3390/drones6020041.

Mishra, S., & Palanisamy, P. (2023). Autonomous advanced aerial mobility—An end-to-end autonomy framework for UAVs and beyond. IEEE Access, vol. 11, pp. 136318-136349. https://ieeexplore.ieee.org/abstract/document/10343091.

Mohamed, M. A., Chaudhry, B. M., Chakraborty, J., & O’Sullivan, K. J. (2024). The Missing Piece in the Zero Trust Sphere: Knowledge Management Perspectives on Safeguarding Business Data. SSRN Electronic Journal. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4766980.

Mohammed, F., Jawhar, I., & Mohamed, N. (2016). Towards trusted and efficient UAV-based communication. IEEE Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 388-393. https://ieeexplore.ieee.org/abstract/document/7502321.

Mondal, M. S., Ramasamy, S., & Humann, J. D. (2024). A robust UAV-UGV collaborative framework for persistent surveillance in disaster management applications. International Conference on Unmanned Aircraft Systems (ICUAS), pp. 1239-1246. https://ieeexplore.ieee.org/abstract/document/10556900.

Mu, J., Zhang, X., Zhao, R., Wang, Q., Jing, P., & Feng, X. (2024). CAKA: Certificateless Authenticated Key Agreement Scheme for Satellite-assisted Unmanned-aerial-vehicle Network. International Conference on Networking and Network Applications (NaNA), pp. 28-34. https://ieeexplore.ieee.org/abstract/document/10679843.

Muthalagu, R., Malik, J., & Pawar, P. M. (2024). A Systematic Review of Adversarial Machine Learning Attacks, Defensive Controls and Technologies. IEEE Access, vol. 12, pp. 99382-99421. https://ieeexplore.ieee.org/abstract/document/10584534.

Nair, A. S., Thampi, S. M., & Jafeel, V. (2024). A post-quantum secure PUF based cross-domain authentication mechanism for Internet of drones. Vehicular Communications, vol. 47, 100780. https://www.sciencedirect.com/science/article/abs/pii/S221420962400055X.

Ngo, T. T. T., Dang, T. A., Huynh, V. V., & Le, T. C. (2023). A systematic literature mapping on using blockchain technology in identity management. IEEE Access, vol. 11, pp. 26004-26032. https://ieeexplore.ieee.org/abstract/document/10068205.

Nguyen, V. L., Lin, P. C., & Cheng, B. C. (2021). Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428. https://ieeexplore.ieee.org/abstract/document/9524814.

Nyangaresi, V. O., Ibrahim, A., & Others. (2021). Provably secure session key agreement protocol for unmanned aerial vehicles packet exchanges. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). https://ieeexplore.ieee.org/abstract/document/9698744.

Ogunbunmi, S., Chen, Y., Blasch, E., & Chen, G. (2024). A survey on reputation systems for UAV networks. Drones 2024, 8(6), 253. https://doi.org/10.3390/drones8060253.

Ometov, A., Petrov, V., Bezzateev, S., & Andreev, S. (2019). Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Network, vol. 33, no. 2, pp. 82-88. https://ieeexplore.ieee.org/abstract/document/8675176.

Onukak, P. (2024). Reputation-Enhanced Practical Byzantine Fault Tolerance for Node Capture Attacks on Unmanned Aerial Vehicle Networks in Adversarial Environments (Order No. 31555748). Available from ProQuest Dissertations & Theses Global. (3102275474). https://www.proquest.com/dissertations-theses/reputation-enhanced-practical-byzantine-fault/docview/3102275474/se-2.

Ouadah, M., & Merazka, F. (2024). Securing UAV Communication: Authentication and Integrity. 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), Leeds, United Kingdom, 1–7. https://ieeexplore.ieee.org/abstract/document/10656843.

Pajany, M., Venkatraman, S., Sakthi, U., & Sujatha, M. (2024). Optimal fuzzy deep neural networks-based plant disease detection and classification on UAV-based remote sensed data. IEEE Transactions, vol. 12, pp. 162131-162144. https://ieeexplore.ieee.org/abstract/document/10740292.

Pandey, G. K., Gurjar, D. S., Nguyen, H. H., & Yadav, S. (2022). Security threats and mitigation techniques in UAV communications: A comprehensive survey. IEEE Access, vol. 10, pp. 112858-112897. https://ieeexplore.ieee.org/abstract/document/9925214.

Pathé, P., Pannetier, B., & Bartheye, O. (2024). Advancing the detection of abnormal drone behaviors: A dynamic Bayesian network approach enhanced by the belief function machine. In 2024 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI) (pp. 1–6). https://ieeexplore.ieee.org/document/10705776.

Peddibhotla, U., Kumar, R., & Sobin, C. C. (2024). Securing agricultural communications: Blockchain integration in UAV networks for smart farming. IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1443-1449. https://ieeexplore.ieee.org/abstract/document/10615542.

Phadke, A., & Medrano, F. A. (2022). Towards resilient UAV swarms—A breakdown of resiliency requirements in UAV swarms. Drones 2022, 6(11), 340. https://doi.org/10.3390/drones6110340.

Phadke, A., & Medrano, F. A. (2023). Examining application-specific resiliency implementations in UAV swarm scenarios. Intelligence & Robotics, 3, 453-78. http://dx.doi.org/10.20517/ir.2023.27.

Poirrier, A., Cailleux, L., & Clausen, T. H. (2023). An interoperable zero trust federated architecture for tactical systems. IEEE Military Communications Conference (MILCOM), 405-410. https://ieeexplore.ieee.org/abstract/document/10356247.

Pokhrel, S. R. (2021). Blockchain brings trust to collaborative drones and LEO satellites: An intelligent decentralized learning in the space. IEEE Sensors Journal, vol. 21, no. 22, pp. 25331-25339. https://ieeexplore.ieee.org/abstract/document/9357330.

Proto, F. S., Detti, A., Pisa, C., & Bianchi, G. (2011). A framework for packet-droppers mitigation in OLSR wireless community networks. 2011 IEEE International Conference on Communications (ICC), 1–6. https://ieeexplore.ieee.org/document/5963001.

Psilias, D., Milidonis, A., & Lentaris, G. (2024). Secure video and telemetry FPGA architecture for UAVs. 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), pp. 69-74. https://ieeexplore.ieee.org/abstract/document/10734656.

Pu, C., & Choo, K.K.R. (2024). Chebyshev Polynomial and Private Blockchain Based Cross-Domain Authentication Protocol for IoD Networks. IEEE 21st Consumer Communications & Networking Conference (CCNC), pp. 931-936. https://ieeexplore.ieee.org/abstract/document/10454702.

Pu, C., Wall, A., Choo, K. K. R., & Ahmed, I. (2022). A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment. IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9918-9933. https://ieeexplore.ieee.org/abstract/document/9745033.

Qaqish, E., Aranki, A., Al-Haija, Q. A., & Qusef, A. (2023). Security Comparison of Blockchain and Cloud-based Identity Management: Considering the Scalability Problem. 2023 International Conference on Inventive Computation Technologies (ICICT), 1078-1085. https://ieeexplore.ieee.org/abstract/document/10134231.

Qian, Y., Cai, H., Shi, L., Mei, Z., Shao, Y., Shu, F., & Zhou, X. (2024). A blockchain-assisted lightweight UAV network authentication mechanism via covert communication. Chinese Journal of Aeronautics. https://www.sciencedirect.com/science/article/pii/S1000936124003200.

Queralta, J. P., Taipalmaa, J., Pullinen, B. C., & Sarker, V. K. (2020). Collaborative multi-robot search and rescue: Planning, coordination, perception, and active vision. IEEE Access, vol. 8, pp. 191617-191643. https://ieeexplore.ieee.org/abstract/document/9220149.

Qureshi, K. N., Nafea, H. O., Tariq, I., & Ghafoor, K. Z. (2024). Blockchain-based trust and authentication model for detecting and isolating malicious nodes in flying ad hoc networks. IEEE Access, vol. 12, pp. 95390-95401. https://ieeexplore.ieee.org/abstract/document/10589383.

Rafique, W., & Qadir, J. (2024). Internet of everything meets the metaverse: Bridging physical and virtual worlds with blockchain. Computer Science Review, vol. 54, 100678. https://www.sciencedirect.com/science/article/pii/S1574013724000625.

Rahbari, D., Ahmed, F., Jenihhin, M., & Alam, M. M. (2024). Reliability-Critical Computation Offloading in UAV Swarms. IEEE Systems Journal. https://ieeexplore.ieee.org/abstract/document/10616260.

Raj, G. P., Mehta, P. J., Parne, B. L., & Patel, S. J. (2023). PUF based Authentication and Key Agreement Framework for Internet of Drones. IEEE 20th India Council International Conference (INDICON), 491–496. https://ieeexplore.ieee.org/abstract/document/10440764.

Raja, G., & Anbalagan, S. (2021). Efficient and secured swarm pattern multi-UAV communication. IEEE Transactions on Vehicular Technology, vol. 70, no. 7, pp. 7050-7058. https://ieeexplore.ieee.org/abstract/document/9437802.

Rajesh, S.M., & Prabha, R. (2023). Lightweight cryptographic approach to address the security issues in intelligent applications: A survey. International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 122-128. https://ieeexplore.ieee.org/abstract/document/10053412.

Rajput, A., & Kumaravelu, V. B. (2021). FCM clustering and FLS based CH selection to enhance sustainability of wireless sensor networks for environmental monitoring applications. Journal of Ambient Intelligence and Humanized Computing, 12(2), 1139–1159. https://doi.org/10.1007/s12652-020-02159-9.

Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial attacks and defenses in deep learning. Engineering, vol. 6, issue 3, pp. 346-360. Elsevier. https://www.sciencedirect.com/science/article/pii/S209580991930503X.

Rifat, M. H., Ananna, A. I., Ahmed, T. I., Akter, S., & Mansoor, N. (2024). Blockchain-Based Controller Recovery and SDN Packet Filtering Scheme for Softwarized UAVs. International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS), pp. 1-5. https://ieeexplore.ieee.org/abstract/document/10499453.

Rigas, E. S., Kolios, P., & Ellinas, G. (2024). Scheduling aerial vehicles in large scale urban air mobility schemes with vehicle relocation. IEEE Transactions on Intelligent Vehicles. https://ieeexplore.ieee.org/abstract/document/10411091.

Rodionov, A. S., & Matkurbanov, T. A. (2023). Application of a genetic algorithm in planning the optimal route of unmanned aerial vehicles used for large area monitoring. IEEE XVI International Scientific and Technical Conference Actual Problems of Electronic Instrument Engineering (APEIE), 2023, pp. 1560-1564. https://ieeexplore.ieee.org/abstract/document/10347781.

Sabarishraj, K., Jayanthy, S., Kovilpillai, J. A., Santhosh, S. S., & Swathi, R. (2024). Efficient implementation of firmware over-the-air update using Raspberry Pi 4 and STM32F103C8T6. IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10677143.

Sabuwala, N. A., & Daruwala, R. D. (2024). An approach to enhance the security of unmanned aerial vehicles (UAVs). The Journal of Supercomputing, 80, 9609–9639. https://doi.org/10.1007/s11227-023-05811-1.

Sadique, K. M., Rahmani, R., & Johannesson, P. (2020). IMSC-EIoTD: Identity management and secure communication for edge IoT devices. Sensors, 20(22), 6546. https://doi.org/10.3390/s20226546.

Sahingoz, O. K. (2013). Mobile networking with UAVs: Opportunities and challenges. International Conference on Unmanned Aircraft Systems (ICUAS), pp. 933-941. https://ieeexplore.ieee.org/document/6564779.

Saleem, Z., Firdous, U., Afzal, M. K., & Ali, A. (2023). Blockchain-based privacy preservation using steganography in drone-enabled VANETs. IEEE Global Communications Conference, Kuala Lumpur, Malaysia, 2023, pp. 6862-6867. https://ieeexplore.ieee.org/abstract/document/10436933.

Saleh, A. M. S. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. Blockchain: Research and

Applications, vol. 5, issue 3, 100193. Elsevier. https://www.sciencedirect.com/science/article/pii/S209672092400006X.

Salim, N. (2024). A comprehensive review on the design and development of drones for diverse applications: Classifications, applications, and design challenges. SSRN. http://dx.doi.org/10.2139/ssrn.5002521.

Samuel, C. N. (2023). Connected Car Communication by DLT Technologies: Mobility Service Implementation by Adaptation of Consortium Blockchain Consensus Algorithms. HAL Archives. https://theses.hal.science/tel-04398183/.

Saraswat, D., Verma, A., Bhattacharya, P., & Tanwar, S. (2022). Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. IEEE Access, vol. 10, pp. 33154-33182. https://ieeexplore.ieee.org/abstract/document/9739009.

Sardar, M. U., Niemi, A., Tschofenig, H., & Fossati, T. (2024). Towards validation of TLS 1.3 formal model and vulnerabilities in Intel's RA-TLS protocol. ResearchGate. Available at https://www.researchgate.net/publication/385384309.

Saritha, E., & Sajesh Kumar, U. (2024). Data transmission via hybrid fuzzy time slot scheduling in long-range communication. International Journal of Electronics, 1–20. https://doi.org/10.1080/00207217.2024.2312567.

Saroopa, P., Poongodi, K., Saranya, V., & Subaash, S. (2024). Securing drones with blockchain-enabled privacy-preserving authentication. International Conference on Knowledge Engineering and Communication Systems (ICKECS), pp. 1–6. https://ieeexplore.ieee.org/abstract/document/10616927.

Sedjelmaci, H., & Senouci, S. M. (2017). A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 9, pp. 1594-1606. https://ieeexplore.ieee.org/abstract/document/7890467.

Selvam, P. K., & Lieb, T. J. (2024). How to implement U-space at an Airport–A general overview of an interaction and synchronization concept. Retrieved from https://elib.dlr.de/202982/.

Semal, B., Markantonakis, K., & Akram, R. N. (2018). A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), pp. 1-8. https://ieeexplore.ieee.org/abstract/document/8569730.

Serafimova, N., & Achkoski, J. (2023). Optimising early wildfire detection with wireless communication technologies. International Journal of Emergency Management, 18(4), 380-401. https://www.inderscienceonline.com/doi/abs/10.1504/IJEM.2023.141429.

Shafique, A., Mehmood, A., & Elhadef, M. (2021). Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access, 9, 46927–46948. https://ieeexplore.ieee.org/abstract/document/9380688.

Sharma, V., You, I., & Jayakody, D. N. K. (2019). Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks. IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5723-5736. https://ieeexplore.ieee.org/abstract/document/8734799.

Sikarwar, H., Vasudev, H., Das, D., & Conti, M. (2024). SECURE: Secure and Efficient ProtoCol Using Randomness and Edge-Computing for Drone-Assisted Internet of Vehicles. IEEE Transactions on Network and Service Management. https://ieeexplore.ieee.org/abstract/document/10681459.

Silva, F. A., Barbosa, V., Lima, L. N., Sabino, A., & Rego, P. (2024). Efficient strategies for unmanned aerial vehicle flights: Analyzing battery life and operational performance in delivery services using stochastic models. IEEE Access, vol. 12, pp. 144544-144564. https://ieeexplore.ieee.org/abstract/document/10646335.

Sindiramutty, S. R., Jhanjhi, N. Z., & Tan, C. E. (2024). Data Security and Privacy Concerns in Drone Operations. (Book). Cybersecurity Issues and Challenges in the Drone Industry, pp. 55. IGI Global. https://www.igi-global.com/chapter/data-security-and-privacy-concerns-in-drone-operations/340079.

Sisinni, S., Margaria, D., Pedone, I., Lioy, A., & Vesco, A. (2022). Integrity verification of distributed nodes in critical infrastructures. Sensors, 22(18), 6950. https://www.mdpi.com/1424-8220/22/18/6950.

Sodhro, A. H., Awad, A. I., van de Beek, J., & Nikolakopoulos, G. (2022). Intelligent authentication of 5G healthcare devices: A survey. Internet of Things, vol. 20, 100610. https://www.sciencedirect.com/science/article/pii/S2542660522000920.

Sohoni, P., Shrivastava, S. S., & others. (2024). A survey on QoS in flying ad hoc network based on fuzzy inference-based routing protocol. International Conference on Automation and Computation (AUTOCOM), pp. 534-539. https://ieeexplore.ieee.org/abstract/document/10486168.

Soliman, S., & Bendary, A. (2024). Scalable and secure cluster formation in Internet of drones using Hyperledger Fabric. 14th International Conference on Electrical Engineering (ICEENG), pp. 340-345. https://ieeexplore.ieee.org/abstract/document/10566407.

Son, S., Kwon, D., Lee, S., Jeon, Y., Das, A. K., & Park, Y. (2023). Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF. IEEE Access, vol. 11, pp. 60240-60253. https://ieeexplore.ieee.org/abstract/document/10151864.

Son, S., Kwon, D., Lee, S., Kwon, H., & Park, Y. (2024). A zero-trust authentication scheme with access control for 6G-enabled IoT environments. IEEE Access, vol. 12, pp. 154066-154079. https://ieeexplore.ieee.org/abstract/document/10729236.

Srinivas, J., Das, A. K., & Kumar, N. (2019). TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 6903-6916. https://ieeexplore.ieee.org/abstract/document/8693567.

Sudhina Kumar, G. K., Krishna Prakasha, K., Muniyal, B., Boiarkin, V., & Rajarajan, M. (2023). International Conference on Recent Advances in Information Technology for Sustainable Development (ICRAIS), pp. 112-117. https://ieeexplore.ieee.org/abstract/document/10367059.

Sullivan, J. M. (2006). Evolution or revolution? The rise of UAVs. IEEE Technology and Society Magazine, vol. 25, no. 3, pp. 43-49. https://ieeexplore.ieee.org/abstract/document/1700021.

Sun, A., Sun, C., Du, J., & Chen, C. (2024). AoI optimization for UAV-assisted wireless sensor networks. IEEE International Conference on Communications, pp. 1487-1492. https://ieeexplore.ieee.org/abstract/document/10615615.

Suomalainen, J., Julku, J., & Vehkaperä, M. (2021). Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. IEEE Open Journal of the Communications Society, vol. 2, pp. 1590-1615. https://ieeexplore.ieee.org/abstract/document/9471839.

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143-57179. https://ieeexplore.ieee.org/abstract/document/9773102.

Tan, X., Zuo, Z., Su, S., Guo, X., & Sun, X. (2020). Research of security routing protocol for UAV communication network based on AODV. Electronics, 9(8), 1185. https://www.mdpi.com/2079-9292/9/8/1185.

Tan, Y., Liu, J., & Kato, N. (2022). Blockchain-based lightweight authentication for resilient UAV communications: Architecture, scheme, and future directions. IEEE Wireless Communications, vol. 29, no. 3, pp. 24-31. https://ieeexplore.ieee.org/abstract/document/9857801.

Tang, Y., Tian, Y., Lin, Y., & Lv, C. (2024). Guest editorial enabling technologies and systems for Industry 5.0: From foundation models to foundation intelligence. IEEE Transactions on Industrial Informatics, vol. 54, no. 11, pp. 6496-6499. https://ieeexplore.ieee.org/abstract/document/10720572.

Tanveer, M., Zahid, A. H., Ahmad, M., Baz, A., & Alhakami, H. (2020). LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of Drone environment. IEEE Access, 8, 155645–155659. https://ieeexplore.ieee.org/abstract/document/9176990.

Tanzi, T., Apvrille, L., Dugelay, J. L. & Roudier Y. (2014). UAVs for humanitarian missions: Autonomy and reliability. IEEE Global Humanitarian Technology Conference (GHTC 2014), pp. 271-278. https://ieeexplore.ieee.org/document/6970292.

Tedeschi, P., Al Nuaimi, F. A., Awad, A. I., & Natalizio, E. (2023). Privacy-aware remote identification for unmanned aerial vehicles: Current solutions, potential threats, and future directions. IEEE Transactions on Industrial Informatics, vol. 20, no. 2, pp. 1069-1080. https://ieeexplore.ieee.org/abstract/document/10143727.

Teschner, G., Neményi, M., & Ambrus, B. (2023). Challenges of ecocentric sustainable development in agriculture with special regard to the internet of things (IoT), an ICT perspective. Progress in Agricultural Engineering Sciences, 19(1), 113–122. https://akjournals.com/view/journals/446/19/1/article-p113.xml.

Thakur, A., Sahoo, S., Mukherjee, A., & Halder, R. (2023). Making robotic swarms trustful: A blockchain-based perspective. ASME Journal of Computing and

Information Science in Engineering, 23(6), 060803. https://doi.org/10.1115/1.4062326.

Thangam, S., Gupta, P. K., & Kartthikeyan, N. (2024). Low-cost network jammer for Wi-Fi network in civilian areas. 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2024, pp. 666-672. https://ieeexplore.ieee.org/abstract/document/10722738.

Thomas, E., & Kumar, S. N. (2024). Fuzzy C Means Clustering Coupled with Firefly Optimization Algorithm for the Segmentation of Neurodisorder Magnetic Resonance Images. Procedia Computer Science, vol. 235, pp. 1577-1589. https://www.sciencedirect.com/science/article/pii/S1877050924008251.

Thompson, R. B., & Thulasiraman, P. (2016). Confidential and authenticated communications in a large fixed-wing UAV swarm. IEEE 15th International Symposium on Network Computing and Applications (NCA), pp. 375-382. https://ieeexplore.ieee.org/abstract/document/7778644.

Tian, D., Wang, C., Zhou, D., Yan, X., & Zeng, L. (2024). NFE-YOLO: A lightweight and efficient detection network for low, slow, and small drones. IEEE Access. https://ieeexplore.ieee.org/abstract/document/10744552.

Tian, X. H., Yang, R., Liu, H. Y., Fan, P., Zhang, J. N., & Gu, C. (2024). Experimental demonstration of drone-based quantum key distribution. Physical Review Letters, 133(20), 200801. Retrieved from https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.200801.

Tkachuk, R.-V., Ilie, D., Tutschku, K., & Robert, R. (2021). A survey on blockchain-based telecommunication services marketplaces. IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 228-255. https://ieeexplore.ieee.org/abstract/document/9592675.

Torens, C., Juenger, F., Schirmer, S., & Schopferer, S. (2022). Machine learning verification and safety for unmanned aircraft—a literature study. AIAA Scitech 2022 Forum. https://doi.org/10.2514/6.2022-1133.

Tufekci, B., Arslan, A., & Tunc, C. (2024). Enhancing the security of the MAVLink with symmetric authenticated encryption for drones. 11th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 58-65. https://ieeexplore.ieee.org/abstract/document/10710297.

Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight challenge-response authentication in SDN-based UAVs using elliptic curve cryptography. Electronics, 11(7), 1026. https://doi.org/10.3390/electronics11071026.

Vangala, A., Das, A. K., Mitra, A., Das, S. K., & Park, Y. (2022). Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks. IEEE Transactions on Information Forensics and Security, vol. 18, pp. 904-919. https://ieeexplore.ieee.org/abstract/document/9994772.

Verma, S., & Adhya, A. (2022). Routing in UAVs-assisted 5G Wireless Sensor Network: Recent advancements, challenges, research gaps, and future directions. In 2022 3rd International Conference on Intelligent Engineering and

Management (ICIEM), pp. 422–428. https://ieeexplore.ieee.org/abstract/document/9853082.

Wahab, O. A., Mourad, A., Otrok, H., & Taleb, T. (2021). Federated machine learning: Survey, multi-level classification, desirable criteria, and future directions in communication and networking systems. IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1342-1397. https://ieeexplore.ieee.org/abstract/document/9352033.

Wang, B., Xing, Y., & Wang, N. (2024). Monitoring waste from unmanned aerial vehicle and satellite imagery using deep learning techniques: A review. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing. https://ieeexplore.ieee.org/abstract/document/10738392.

Wang, D., Cao, Y., Lam, K. Y., Hu, Y., & Kaiwartya, O. (2024). Authentication and key agreement based on three factors and PUF for UAVs-assisted post-disaster emergency communication. IEEE Internet of Things Journal, vol. 11, no. 11, pp. 20457-20472. https://ieeexplore.ieee.org/abstract/document/10453335.

Wang, H., Wang, C., Zhou, K., & Liu, D. (2024). TEBChain: A trusted and efficient blockchain-based data sharing scheme in UAV-assisted IoV for disaster rescue. IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 4119-4130. https://ieeexplore.ieee.org/abstract/document/10509583.

Wang, J., Liu, Y., Niu, S., & Song, H. (2021). Lightweight blockchain assisted secure routing of swarm UAS networking. Computer Communications, vol. 165, pp. 131-140. https://doi.org/10.1016/j.comcom.2020.11.008.

Wang, J., Liu, Y., Niu, S., Song, H., Jing, W., & Yuan, J. (2021). Blockchain enabled verification for cellular-connected unmanned aircraft system networking. Future Generation Computer Systems, vol. 123, pp. 233-244. https://www.sciencedirect.com/science/article/abs/pii/S0167739X21001461.

Wang, J., Wang, R., Zheng, Z., & Lin, R. (2024). Physical layer security enhancement in UAV-assisted cooperative jamming for cognitive radio networks: A MAPPO-LSTM deep reinforcement learning approach. IEEE Transactions on Vehicular Technology. https://ieeexplore.ieee.org/abstract/document/10734220.

Wang, Y. (2024). Semantic communication networks empowered artificial intelligence of things. IEEE Annual Congress on Artificial Intelligence of Things (AIoT), pp. 189-193. https://ieeexplore.ieee.org/abstract/document/10677749.

Wang, Y., Hu, Q., Li, Z., Su, Z., Li, R., & Zou, X. (2024). Blockchain-envisioned UAV-aided disaster relief networks: Challenges and solutions. IEEE Communications Magazine. https://ieeexplore.ieee.org/abstract/document/10697415.

Wang, Y., Liu, H., Li, Z., Su, Z., & Li, J. (2024). Combating advanced persistent threats: Challenges and solutions. IEEE Network. https://ieeexplore.ieee.org/abstract/document/10507737.

Wang, Y., Su, Z., Ni, J., Zhang, N., & Shen, X. (2021). Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. IEEE

Communications Surveys & Tutorials, vol. 24, no. 1, pp. 160-209. https://ieeexplore.ieee.org/abstract/document/9631953.

Wani, A. R., Gupta, S. K., Khanam, Z., Rashid, M., Alshamrani, S. S., & Baz, M. (2023). A novel approach for securing data against adversary attacks in UAV embedded HetNet using identity-based authentication scheme. IET Intelligent Transport Systems. https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/itr2.12271.

Warrier, A., Aljaburi, L., Whitworth, H., & Al-Rubaye, S. (2024). Future 6G communications powering vertical handover in non-terrestrial networks. IEEE Access, vol. 12, pp. 33016-33034. https://ieeexplore.ieee.org/abstract/document/10453590.

Wei, X., Ma, J., & Sun, C. (2024). A survey on security of unmanned aerial vehicle systems: Attacks and countermeasures. IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34826-34847. https://ieeexplore.ieee.org/abstract/document/10599134.

Xiao, K., Zhao, J., He, Y., Li, C., & Cheng, W. (2019). Abnormal behavior detection scheme of UAV using recurrent neural networks. IEEE Access, vol. 7, pp. 110293-110305. https://ieeexplore.ieee.org/abstract/document/8793200.

Xiao, W., Hong, D., Jiang, S., & Li, W. (2024). MU-BISE: Multi-UAV collaborative mapping based on blockchain information security enhancement. 3rd International Conference on Robotics, Artificial Intelligence and Intelligent Control (RAIIC), pp. 241-244. https://ieeexplore.ieee.org/abstract/document/10670766.

Xiao, Z., Chen, Y., Jiang, H., Hu, Z., Lui, J. C. S., & Min, G. (2022). Resource management in UAV-assisted MEC: State-of-the-art and open challenges. Wireless Networks, 28(8), 3305–3322. https://doi.org/10.1007/s11276-022-03051-4.

Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2024). A blockchain-based ubiquitous entity authentication and management scheme with homomorphic encryption for FANET. Peer-to-Peer Networking and Applications, vol.17, pp. 569–584. https://doi.org/10.1007/s12083-024-01624-y.

Xiong, R., Xiao, Q., Wang, Z., Xu, Z., & Shan, F. (2024). Leveraging lightweight blockchain for secure collaborative computing in UAV Ad-Hoc Networks. Computer Networks, vol. 251, 110612. https://www.sciencedirect.com/science/article/abs/pii/S1389128624004444.

Xu, F., Ahmad, S., Khan, M. N., Ahmed, M., Raza, S., Khan, F., Ma, Y., & Khan, W. U. (2023). Beyond encryption: Exploring the potential of physical layer security in UAV networks. Journal of King Saud University - Computer and Information Sciences, vol. 35, issue 8, 101717. https://www.sciencedirect.com/science/article/pii/S1319157823002719.

Xu, Q., Yi, J., Wang, X., Niu, M., Miah, M. S., & Wang, L. (2024). Secure Unmanned Aerial Vehicle Communication in Dual-Function Radar Communication System by Exploiting Constructive Interference. Drones, 8(10), 581. https://www.mdpi.com/2504-446X/8/10/581.

Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). Blendcac: A blockchain-enabled decentralized capability-based access control for IoTs. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1027-1034. https://ieeexplore.ieee.org/abstract/document/8726680.

Xu, Y., Wu, X., Tang, Y., Shang, J., & Zheng, L. (2024). Joint resource allocation for V2X communications with multi-type mean-field reinforcement learning. IEEE Transactions on Intelligent Transportation Systems. https://ieeexplore.ieee.org/abstract/document/10740528.

Xu, Z., Qiao, H., Liang, W., Xu, Z., Xia, Q., Zhou, P., Rana, O. F., & Xu, W. (2024). Flow-time minimization for timely data stream processing in UAV-aided mobile edge computing. ACM Transactions on Sensor Networks, vol. 20, issue 3, no. 58, pp. 1 – 28. https://doi.org/10.1145/3643813.

Yadav, R., Kasim, M. M., & Srividhya, S. (2024). The techniques used for sustainable communication system FR 6-G type of network. 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 79-84. https://ieeexplore.ieee.org/abstract/document/10616452.

Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., & Wahab, A. W. A. (2021). Internet of drones security and privacy issues: Taxonomy and open challenges. IEEE Access, 9, 57243-57270. https://ieeexplore.ieee.org/abstract/document/9399464.

Yahya, M., Naeem, M., & Kaleem, Z. (2024). Robust multi-criterion offloading in digital twin-assisted UAVs networks. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/10684302.

Yang, H., & Lu, R. (2024). Frontiers in Cyber Security: 6th International Conference. (Book). FCS 2023, Chengdu, China, August 21–23, 2023, Revised Selected Papers. Springer. Available at https://link.springer.com/book/10.1007/978-981-99-9331-4.

Yang, J., Liu, X., Jiang, X., & Zhang, Y. (2023). Toward trusted unmanned aerial vehicle swarm networks: A blockchain-based approach. IEEE Vehicular Technology Magazine, vol. 18, no. 2, pp. 98-108. https://ieeexplore.ieee.org/abstract/document/10051720.

Yang, J., Sun, K., He, H., & Jiang, X. (2022). Dynamic virtual topology aided networking and routing for aeronautical ad-hoc networks. IEEE Transactions on Communications, vol. 70, no. 7, pp. 4702-4716. https://ieeexplore.ieee.org/abstract/document/9780352.

Yang, J., Wang, Y., Hang, X., & Delahaye, D. (2024). A review on airspace design and risk assessment for urban air mobility. IEEE Access, vol. 12, pp. 157599-157611. https://ieeexplore.ieee.org/abstract/document/10718279.

Yang, K. C., & Lin, P. C. (2023). Mutual authentication between aerial base stations and core network: A lightweight security scheme. 33rd International Telecommunication Networks and Applications Conference, pp. 11-18. https://ieeexplore.ieee.org/abstract/document/10368490.

Yanmaz, E., Yahyanejad, S., Rinner, B., Hellwagner, H., & Bettstetter, C. (2018). Drone networks: Communications, coordination, and sensing. Ad Hoc Networks, vol. 68, 1-15. https://www.sciencedirect.com/science/article/abs/pii/S1570870517301671.

Yazdinejad, A., Namakshenas, D., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2024). IP2FL: Interpretation-Based Privacy-Preserving Federated Learning for Industrial Cyber-Physical Systems. IEEE Transactions on Industrial Cyber-Physical Systems, vol. 2, pp. 321-330. https://ieeexplore.ieee.org/abstract/document/10614890.

Ye, N., Li, X., Yang, K., & An, J. (2024). Multiple access technology towards ubiquitous networks. (Book). Springer. https://link.springer.com/book/10.1007/978-981-19-4025-5.

Yu, J., Shvetsov, A. V., & Alsamhi, S. H. (2024). Leveraging machine learning for cybersecurity resilience in Industry 4.0: Challenges and future directions. IEEE Access, vol. 12, pp. 159579-159596. https://ieeexplore.ieee.org/abstract/document/10721279.

Yu, J., Xu, T., Zhu, X., & Wu, X. J. (2024). Local point matching for collaborative image registration and RGBT anti-UAV. Pattern Recognition and Computer Vision (PRCV). Springer, Lecture Notes in Computer Science, vol 15042. https://link.springer.com/chapter/10.1007/978-981-97-8858-3_29.

Yu, S., Das, A. K., & Park, Y. (2024). RLBA-UAV: A robust and lightweight blockchain-based authentication and key agreement scheme for PUF-enabled UAVs. IEEE Transactions on Intelligent Transportation Systems. https://ieeexplore.ieee.org/abstract/document/10734851.

Yu, S., Lee, J., Sutrala, A. K., Das, A. K., & Park, Y. (2023). LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks. Computer Networks , vol. 224, 109612. https://www.sciencedirect.com/science/article/abs/pii/S1389128623000579.

Yu, W., Xu, H., Nguyen, J., Blasch, E., & Hematian, A. (2018). Survey of public safety communications: User-side and network-side solutions and future directions. IEEE Access, vol. 6, pp. 70397-70425. https://ieeexplore.ieee.org/abstract/document/8523665.

Yu, Z., Wang, Z., Yu, J., Liu, D., & Song, H. H. (2023). Cybersecurity of unmanned aerial vehicles: A survey. IEEE Aerospace and Electronic Systems Magazine, vol. 39, no. 9, pp. 182-215. https://ieeexplore.ieee.org/abstract/document/10261240.

Yucesoy, Y. F., & Sahin, C. (2024). Object detection in infrared images with different spectra. 2024 International Congress on Human-Computer Interaction. Istanbul, Turkiye, 2024, pp. 1-6. https://ieeexplore.ieee.org/abstract/document/10550753.

Zadorozhnyi, Z. M., & Muravskyi, V. (2024). Aerial visual monitoring in accounting of smart construction. 14th International Conference on Advanced Computer Information Technologies (ACIT), pp. 465-470. https://ieeexplore.ieee.org/abstract/document/10712503.

Zanardo, E., Martini, B., & Bellisario, D. (2024). Tokenized intelligence: Redefine network optimization in softwarized networks. IEEE 10th International Conference on Network Softwarization (NetSoft), pp. 145-148. https://ieeexplore.ieee.org/abstract/document/10588949.

Zeng, R., Zhao, C., Liu, Z., & Lu, Y. (2024). UAV Anomaly Detection Model Based on Integrated Multi-Modal Neural Network and Neural Architecture Search. 5th International Conference on Information Science, Parallel and Distributed Systems (ISPDS), pp. 585-588. https://ieeexplore.ieee.org/abstract/document/10667484.

Zhang, J., Yang, L., Cao, W., & Wang, Q. (2020). Formal analysis of 5G EAP-TLS authentication protocol using ProVerif. IEEE Access, vol. 8, pp. 23674-23688. https://ieeexplore.ieee.org/abstract/document/8970242.

Zhang, K., Lee, C. K. M., & Tsang, Y. P. (2024). Stateless Blockchain-Based Lightweight Identity Management Architecture for Industrial IoT Applications. IEEE Transactions on Industrial Informatics, vol. 20, no. 6, pp. 8394-8405. https://ieeexplore.ieee.org/abstract/document/10468559.

Zhang, L., Zhang, B., & Li, C. (2024). An efficient and reliable Byzantine fault-tolerant blockchain consensus protocol for single-hop wireless networks. IEEE Transactions on Wireless Communications, 23(3), 1974–1987. https://ieeexplore.ieee.org/abstract/document/10184201.

Zhou, L., Leng, S., Wang, Q., & Quek, T. Q. S. (2024). Cooperative digital twins for UAV-based scenarios. IEEE Communications Magazine. https://ieeexplore.ieee.org/abstract/document/10742566.

Zhou, Y., Khuwaja, A. A., Li, X., & Zhao, N. (2024). Optimizing multi-UAV multi-user system through integrated sensing and communication for age of information (AoI) analysis. IEEE Open Journal of the Communications Society. https://ieeexplore.ieee.org/abstract/document/10741963.

Zhou, Y., Rao, B., & Wang, W. (2020). UAV swarm intelligence: Recent advances and future trends. IEEE Access, 8, 183856–183878. https://ieeexplore.ieee.org/abstract/document/9214446.

Zhou, Z., Luo, X., Mao, J., He, T., & Ji, X. (2024). Blockchain-assisted efficient data sharing scheme with accountability and privacy-preserving for Internet of Drones networks. IEEE Transactions on Vehicular Technology. https://ieeexplore.ieee.org/abstract/document/10711300.

Zhu, C., Zhu, X., Ren, J., & Qin, T. (2022). Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. IEEE Access, vol. 10, pp. 56591-56610. https://ieeexplore.ieee.org/document/9774400.

Zhuo, R., Song, S., & Xu, Y. (2022). UAV communication network modelling and energy consumption optimization based on routing algorithm. Computational and Mathematical Methods in Medicine. https://doi.org/10.1155/2022/4782850.

Zuo, J., Cao, R., Qi, J., Gao, P., Wang, Z., Li, J., Zhang, L., & Lu, Y. (2023). A hierarchical blockchain-based trust measurement method for drone cluster nodes. Drones, 7(10), 627. https://doi.org/10.3390/drones7100627.