People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of 8 May 1945 Guelma

Faculty of Mathematics, Computer Science and Sciences of Matter
Department of Computer Science
Laboratory of Science and Technology of Information and Communication

DISSERTATION

In Partial Fulfillment of the Requirements for The Doctorate degree in 3rd cycle

Domain: Mathematics and Computer Science. **Field**: Computer Science
Specialty: Computer Science Systems

Presented by:

BERINI Aymen Dia Eddine

Entitled

Management of Surveillance Drones in an IoT Environment

Defended: **14/10/2023** Before the board of examiners composed of:

Mr.Nemissi Mohamed	**Professor**	Univ. of 8 May 1945, Guelma	Chairman
Mr.Mohamed Amine Ferrag	**MCA**	Univ. of 8 May 1945, Guelma	Supervisor
Mr.Seridi Hamid	**Professor**	Univ. of 8 May 1945, Guelma	Co-supervisor
Mr.Kouahla Zineddine	**Professor**	Univ. of 8 May 1945, Guelma	Examiner
Mr. Smaine Mazouzi	**Professor**	Univ. of 20 august 1955, Skikda	Examiner
Mr.Farou Brahim	**Professor**	Univ. of 8 May 1945, Guelma	Invited

Academic Year: 2022-2023

Many thanks to each and every single one of you. This dissertation is dedicated to my parents (including my in-laws), wife, sisters, brother and his wife.

Acknowledgements

This dissertation marks the end of a long journey. Without God's help, first and foremost, and the support of many people, it would not have been possible to finish it. Research is not something you do by yourself, as some people think. Instead, you work with others. One needs much support and guidance from colleagues, family, and friends.

To my dear parents, without you, I would not be standing here today, you supported me back when I was young, and you were always there for me when I needed you the most.

My sincere appreciation goes to my supervisor **Dr Mohamed Amine FERRAG**, for his professional advice and academic support.

I would like to thank **Prof. Hamid SERIDI** for the benefit of his immense experience and for encouraging me to advance in my work. I really thank him for his help and express my deepest gratitude.

I owe a lot to **Prof. Brahim FAROU** has helped, encouraged and guided me for the past few years. On this special occasion, I would like to express my deep gratitude to him for his numerous remarks and appreciation of his extreme relevance.

I would like to express my heartfelt gratitude to **Prof. Mohamed NEMISSI**, **Dr Zineddine KOUAHLA**, **Prof.Brahim FAROU** of the University of Guelma, and **Prof.Smaine MAZOUZI** of the University of SKIKDA for the honor of examining this work and participating in the defense jury.

I want to express my special thanks to all **my teachers**, past and present, for helping me reach this level.

I am immensely grateful to my beloved wife, who has been not only my partner but also my unwavering support throughout this journey. Her patience, encouragement, support and unconditional love that gave me confidence and allowed me to complete this thesis. This thesis is hers too.

Last but not least, I am grateful to God for my time spent at the **LabSTIC Laboratory**. Without exception, I'd want to thank each and every one of the LabSTIC team members for their time, effort, and the wealth of knowledge they shared with me.

ملخص

تركز أطروحة الدكتوراه هذه على معالجة التحديات التي تواجه تخطيط مسار التغطية الثابتة (CPP) وأمن المعلومات في سياق إنترنت الطائرات بدون طيار(IoD). توفر الأطروحة نظرة عامة شاملة على ماهو متداول في مجال CPP و أمن IoD ، كما تغطي مواضيع مثل محاكيات الدرون ، وحلول الأمان ، والتقنيات الحديثة ، واتجاهات البحث المستقبلية المحتملة. الهدف الأساسي من هذه الأطروحة هو معالجة جانبين أساسيين، الجانب الأول هو اقتراح استراتيجية جديدة لتخطيط مسار الطائرات بدون طيار و التي تقلل من استهلاك الطاقة ، وتقلل من عدد انعطافات الدرون ، كما توفر أهمية متساوية للمنطقة بأكملها. تهدف هذه الاستراتيجية الجديدة إلى تحسين أداء الطائرات بدون طيار مع تحقيق أقصى قدر من الكفاءة في تشغيلها. تم تقييم المسار المقترح ، وقد تفوق على المسارات الحالية ، مما أدى إلى تحسينات كبيرة في وقت إنجاز المهمة ، والمسافة المقطوعة ، واستهلاك الطاقة. الجانب الثاني من هذه الرسالة يتعلق بأمن المعلومات والذي أصبح أكثر أهمية في تكنولوجيا الطائرات بدون طيار.

في الواقع ، يفرض استخدام الطائرات بدون طيار في بيئة إنترنت الأشياء IoT العديد من التحديات ، حيث تقوم الدرون بجمع ونقل البيانات الحساسة آنياً. يعد نظام المصادقة الآمن والفعال أمرا بالغ الأهمية لضمان اتصال موثوق بين الطائرة بدون طيار والمستخدمين الخارجيين ، لا سيما بالنظر إلى سعة البطارية والذاكرة المحدودة للطائرات بدون طيار. يمكن أن يؤدي الفشل في تنفيذ نظام مصادقة إلى اختراق البيانات الحساسة من خلال الوصول غير المصرح به والاعتراض والتلاعب والتحكم بها. تقترح هذه الأطروحة أيضا نظام قليل التكلفة للمصادقة و الاتفاق على المفاتيح يسمى HCALA لتأمين اتصال المستخدم بدون طيار في بيئة الطائرات بدون طيار، يستخدم البروتوكول المقترح وظيفة تجزئة ، Exclusive-OR ، تشفير منحنى Hyperelliptic (HECC) ، كما يدعم تقنية البلوكشين . يوفر HCALA حلاً فعالاً لمرحلتي الغاء الدخول وإعادة الدخول ، بالإضافة إلى تحديثات كلمة المرور. يأخذ البروتوكول بعين الاعتبار نموذج التهديد Yao (DY) - Dolev و Krawczyk Canetti(CK) ، والذي يتيح للخصم قدرة كبيرة للمساومة على أمن النظام المقترح.

لتقييم التطبيق العملي والفعالية لـ HCALA ، نستخدم نموذج Oracle العشوائي (ROM) والتحقق الأمني الرسمي من خلال أداة برمجية تسمى AVISPA ، والتي تستخدم عادة للتحقق من بروتوكولات أمان الإنترنت. بالإضافة إلى ذلك ، نقوم بتقييم

HCALAباستخدام أساليب تحليل الأمان غير الرسمية ، مما يدل على قدرته على مقاومة هجمات العدو المختلفة ، سواء النشطة أو السلبية. علاوة على ذلك ، تشير مقارنة الأداء إلى أن HCALA أكثر كفاءة من حيث المؤشرات المختلفة بالمقارنة مع المخططات المماثلة في السنوات الأخيرة. يُظهر HCALA أمانا ووظائف محسّنة ، مع تقليل الحساب وتكاليف الاتصال واستهلاك الطاقة. يساهم هذا البحث في تقدم تكنولوجيا الطائرات بدون طيار وتطبيقاتها في تطوير شبكات IoD آمنة وفعالة.

الكلمات المفتاحية: تخطيط مسار التغطية، إنترنت الطائرات بدون طيار، استهلاك الطاقة، إنترنت الأشياء، نظام مصادقة.

Résumé

Cette thèse de doctorat se concentre sur les défis rencontrés dans la planification statique de couverture de chemin (PCC) et la sécurité dans le contexte de l'Internet des drones (IdD). La thèse offre un aperçu complet de l'état actuel de la PCC et de la sécurité IdD, couvrant des sujets tels que les simulateurs de drones, les solutions de sécurité, les technologies émergentes et les orientations futures potentielles. Le premier aspect de cette thèse est de proposer une nouvelle stratégie de planification de trajectoire de drone qui réduit la consommation d'énergie, minimise le nombre de virages et donne une importance égale à l'ensemble de la zone. Cette stratégie vise à optimiser les performances des drones tout en atteignant une efficacité maximale dans leur fonctionnement. La solution proposée a été évaluée et a surpassé les trajectoires existantes, entraînant des améliorations significatives du temps d'achèvement de la mission, de la distance parcourue et de la consommation d'énergie. Le deuxième aspect de cette thèse concerne la sécurité, qui est devenue de plus en plus critique dans la technologie des drones.

En effet, l'utilisation de drones dans l'environnement d'IdO pose plusieurs défis, car ils collectent et transmettent des données sensibles en temps réel. Un schéma d'authentification sûr et efficace est crucial pour assurer une communication fiable et sûre entre le drone et les utilisateurs externes, surtout compte tenu de la capacité de batterie et de mémoire limitée des drones. Cette thèse propose également un schéma d'authentification et d'accord de clé léger appelé HCALA pour sécuriser la communication utilisateur-drone dans IdD. Le schéma proposé utilise une fonction de hachage, une opération OU-exclusive et une cryptographie de courbe hyperelliptique (CCHE), et est pris en charge par la blockchain. HCALA offre une solution efficace aux phases de révocation et de réémission, ainsi qu'aux mises à jour de mot de passe. Le protocole prend en compte le modèle de menace Dolev-Yao (DY) et l'adversaire Canetti et Krawczyk (CK), qui offre la plus grande capacité à un adversaire tentant de compromettre la sécurité du schéma proposé.

Pour évaluer la praticabilité et l'efficacité de HCALA, nous utilisons le modèle d'oracle aléatoire et la vérification de sécurité formelle grâce à un outil logiciel nommé AVISPA, qui est couramment utilisé pour vérifier les protocoles de sécurité Internet. De plus, nous évaluons HCALA en utilisant des méthodes d'analyse de sécurité informelle, démontrant sa capacité à résister à diverses attaques d'adversaires, à la fois actives et passives. En outre, la comparaison des performances indique que HCALA est plus efficace en termes de différents paramètres. Par rapport à des schémas similaires ces dernières années, HCALA montre une sécurité et une fonctionnalité améliorées, tout en réduisant les coûts de calcul, de communication et de consommation d'énergie. Cette recherche contribue à l'avancement de la technologie des drones et de ses applications dans le développement de réseaux sécurisés et efficaces d'IdD.

Mots Clée : PPC, IdD, Sécurité, Consommation d'énergie, IdO, Schéma d'authentification.

Abstract

This Ph.D. dissertation focuses on addressing the challenges encountered in static coverage path planning (CPP) and security in the context of the Internet of Drones (IoD). The dissertation provides a comprehensive overview of the current state of CPP and IoD security, covering topics such as drone simulators, security solutions, emerging technologies, and potential future research directions. The primary objective of this dissertation is to address two fundamental aspects. The first aspect is to propose a novel strategy for UAV path planning that reduces energy consumption, minimizes the number of turns, and provides equal importance to the entire area. This novel strategy aims to optimize the performance of UAVs while achieving maximum efficiency in their operation. The proposed solution has been evaluated, and it has outperformed existing paths, resulting in significant improvements in mission completion time, distance traveled, and energy consumption. The second aspect of this dissertation concerns security, which is becoming increasingly critical in UAV technology.

Indeed, the use of drones in the Internet of Things (IoT) environment poses several challenges, as they collect and transmit sensitive data in real time. A secure and efficient authentication scheme is crucial to ensure dependable and safe communication between the drone and external users, especially considering the limited battery and memory capacity of drones. Failure to implement an efficient authentication scheme can lead to the compromise of sensitive data through unauthorized access, interception, manipulation, and control. This dissertation also proposes a lightweight authentication and key agreement (AKA) scheme called HCALA to secure user-drone communication in IoD. The proposed scheme utilizes a hash function, Exclusive-OR operation, and a Hyperelliptic Curve Cryptography (HECC), and is supported by blockchain. HCALA provides an efficient solution to the revocation and reissue phases, as well as password updates. The protocol considers the Dolev–Yao (DY) threat model and Canetti and Krawczyk (CK) adversary, which provides the most capability to an opponent attempting to compromise the proposed scheme's security.

To assess the practicality and effectiveness of HCALA, we utilize the Random Oracle

Model (ROM) and formal security verification through a software tool named AVISPA, which is commonly utilized to verify internet security protocols. In addition, we evaluate HCALA using informal security analysis methods, demonstrating its ability to resist various adversary attacks, both active and passive. Furthermore, performance comparison indicates that HCALA is more efficient in terms of different parameters. Compared to similar schemes in recent years, HCALA shows improved security and functionality, while reducing computation, communication costs, and energy consumption. This research contributes to the advancement of drone technology and its applications in the development of secure and efficient IoD networks.

Keywords : CPP, IoD, Security, Energy consumption, IoT, Authentication scheme.

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Meaning
AES	Advanced Encryption Standard
AirSim	Aerial Informatics and Robotics simulator
AVENS	Aerial Vehicle Network Simulator
AI	Artificial Intelligence
AVISPA	Automated Validation of Internet Security Protocols and Applications
BF	back-and-forth
BS	Base Station
GPA	Bayesian Learning Approach
BC	Blockchain
BAN	Burrows-Abadi-Needham
BFT	Byzantine Fault Tolerance
CA	Certificate Authority
CLDA	Certificate-Less Data Aggregation
CL-MRES	Certificate-Less Multi-Recipient Encryption
CLSC-TKEM	Certificate-Less Signcryption Tag Key Encapsulation Mechanism
CL-GAKA	Certificateless-Group Authenticated Key Agreement
CPP	Coverage Path Planning
DPoS	Delegated Proof of Stake
DoS	Denial of Service
DH	Diffie-Hellman
DAA	Direct Anonymous Attestation
DGCA	Directorate General of Civil Aviation
ECC	Elliptic Curve Cryptography
EPSRC	Engineering and Physical Sciences Research Council

Continued on next (↓) page

Continued from previous (↑) page

Abbreviation	**Meaning**
ESL	Ephemeral Secret Leakage
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FoV	Field of View
FANET	Flying Ad-Hoc Network
GPS	Global Positioning System
GUI	Graphical User Interface
GSS	Ground Station Server
HMAC	Hash-Based Message Authentication Code Function
HLPSL	High-Level Protocol Specification Language
HTOL	Horizontal Take-Off and Landing
HECC	Hyperelliptic Curve Cryptography
HECDLP	Hyperelliptic Curve Discrete Logarithm Problem
HCALA	Hyperelliptic Curve-Based Anonymous Lightweight Authentication
IMU	Inertial Measurement Unit
IF	Intermediate Format
IoD	Internet of Drones
IoT	Internet of Things
KNN	K-Nearest Neighbor
LAKE-IoD	Lightweight AKE Protocol for IoD Environment
LMAT	Localization Algorithm with a Mobile Anchor Node Based on Trilateration
LR	Logistic Regression
MTM	Man-in-the-Middle
MAC	Message Authentication Code
MAVLink	Micro Air Vehicle Link
MEMS	Micro-Electro Mechanical Systems
MP	Mission Planner Simulator
MA-DAA	Mutual Authentication DAA
NFZ	No-Flight Zones
OSRF	Open Source Robotics Foundation
OF	Output Format

Continued on next (↓) page

Continued from previous (↑) page

Abbreviation	**Meaning**
PFS	Perfect Forward Secrecy
PUFs	Physical Unclonable Functions
PBFT	Practical Byzantine Fault Tolerance
PoS	Proof of Stake
PoW	Proof of Work
PID	Proportional-Integral-Derivative
PARTH	PUF-Based Authentication for Remote Hovering Devices
RFID	Radio Frequency Identification
ROM	Random Oracle Model
RP-3	Raspberry Pi
ROR	Real-or-Random
RMC	Remote Management Centre
RPCA	Ripple Protocol Consensus Algorithm
ROS	Robot Operating System
SAR	Search and Rescue
SENTINEL	Secure and Efficient AutheNTIcation for uNmanned aErial vehicLes
SPAN	Security Protocol ANimator
SUAAVE	Sensing Unmanned Autonomous Aerial Vehicles
SBC	Single-Board Computer
SDN	Software-Defined Networking
SPP	Spiral Path Planning
SVM	Support Vector Machines
TCALAS	Temporal Credential-Based Anonymous Lightweight Authentication Scheme
TPM	Trusted Platform Module
TPMs	Trusted Platform Modules
USC	University of Southern California
UAVs	Unmanned Aerial Vehicles
UAS	Unmanned Aircraft/Aerial System
VTOL	Vertical Take-Off and Landing
WSNs	Wireless Sensor Networks

Introduction

General context and Issues

Over the past decade, Unmanned Aerial Vehicles (UAVs), commonly known as drones, have become increasingly prevalent in various fields, such as surveillance, agriculture, mapping, and package delivery. These unmanned vehicles are widely used in various applications such as surveillance, monitoring, and search and rescue operations. However, the use of drones also presents several challenges and issues, particularly with respect to their operation, security, and efficiency.

One significant challenge in drone operations is the need for efficient and effective coverage path planning (CPP) algorithms. CPP plays a vital role in the success of drone operations, as it determines the drone's flight path and coverage area, affecting the efficiency of data collection and surveillance. Moreover, designing and implementing an appropriate CPP algorithm for drones can be challenging due to the complex nature of the tasks involved.

Another major issue in the use of drones is their security vulnerabilities. The Internet of Drones (IoD) involves the collection and transmission of sensitive data in real-time, which is vulnerable to several security issues, including unauthorized access, interception, manipulation, and control. Ensuring secure and reliable communication between drones and external users is crucial to prevent these security threats.

Additionally, drones typically have limited battery and memory capacity, which poses a significant challenge in the use of security mechanisms. Lightweight and efficient security techniques are necessary to address these challenges while ensuring the security and reliability of IoD networks.

Given these challenges and issues, researchers have focused on developing new technologies and solutions to address the limitations and enhance the performance of drone operations and security. This thesis aims to contribute to this research field by exploring new solutions and techniques for CPP and IoD security, with a focus on the use of simulators and blockchain-based authentication schemes.

Through this research, we aim to address the current limitations and challenges of CPP and IoD security, contributing to the efficient and secure use of drones in various fields.

Objectives and research questions

The main objective of this thesis is to address the challenges faced in CPP and security in IoD environments. Specifically, the thesis aims to :

- Provide a comprehensive overview of the current state of static CPP for drones and IoD security, including drone simulators and security solutions for the IoD network, the challenges of emerging technologies, and potential future research directions in these fields.
- Develop and propose novel algorithms for UAV path planning that significantly reduce energy consumption and minimize the number of turns while providing the whole area with the same level of importance.
- Evaluate the effectiveness and efficiency of the proposed algorithms and security scheme and compare them with existing state-of-the-art methods.
- Analyze the security of IoD networks, identify the most probable attacks that could be executed, and propose an efficient and secure blockchain-based authentication scheme to enable secure and reliable communications between drones and external users.

The research questions that will guide this thesis are as follows :

- What are the challenges of emerging technologies in CPP for drones and IoD security, and what are the potential future research directions in these fields ?
- How can we develop a novel UAV path planning algorithm that reduces energy consumption and minimizes the number of turns while providing the whole area with the same level of importance ?
- How effective and efficient are the proposed algorithms and security scheme compared with existing state-of-the-art methods ?
- What are the vulnerabilities of IoD networks, and how can we propose an efficient and secure blockchain-based authentication scheme to ensure secure and reliable communications between drones and external users ?

By answering these research questions, this thesis aims to contribute to the advancement of CPP for drones and IoD security, addressing the challenges faced by these fields and proposing novel solutions to improve their efficiency, security, and reliability.

Scientific Contributions

This thesis employs a combination of simulation-based experimentation and theoretical analysis.

- Firstly, simulators for drones are used to test and evaluate CPP algorithms in a controlled environment. The proposed novel CPP algorithm is evaluated against four static paths : Back and forth (BF), Spiral, LMAT, and Zamboni.
- Secondly, the proposed blockchain-based authentication scheme for the IoD network is developed and evaluated using ROM and formal security verification using a software tool called AVISPA. Informal security analysis techniques are also used to demonstrate the protocol's effectiveness against well-known active and passive adversary attacks.

Structure of the thesis

The thesis is organized into two primary sections. The first section comprises three state-of-the-art chapters, and the second section consists of two contribution chapters. The thesis culminates with a general conclusion.

❖ Part I : Backgrounds, Preliminaries and Basic Concepts

❏ *Chapter 01 : « Internet of Drones (IoD) »*

This chapter provides an introduction to the topic of drones in IoT and their potential applications. It outlines the research problem and significance, research objectives, scope, and limitations, and the methodology and approach used in the thesis.

❏ *Chapter 02 : « Drone Path Management »*

This chapter delves into the topic of (CPP) for drones, which is a crucial aspect of UAV operations. It explores the current simulators for drones, including their objectives, strengths, and shortcomings. It also discusses the challenges of CPP for drones and potential future directions for research in this field.

- ❑ *Chapter 03 : « Security of IoD »*

This chapter provides a comprehensive study of the security of IoD networks. It summarizes the causes of vulnerability of the IoD network, followed by a thorough risk analysis to identify the most probable attacks that could be executed on the network. It details the network's security needs by emphasizing the functions and the protected data conveyed in the network. The last part presents the security solutions and discusses the security challenges of emerging technologies and protocols of IoD networks.

❖ Part II : Novel Approaches to UAV Path Planning and Security in IoD Networks

- ❑ *Chapter 04 : « An Efficient Static CPP Strategy for Drones »*

This chapter presents a novel UAV coverage path planning for the monitoring task that reduces energy consumption considerably and minimizes the number of turns. The proposed path prioritizes the entire area equally and is compared to four existing static paths, including back and forth, spiral, LMAT, and Zamboni. The findings demonstrate that the proposed path provides better coverage with lower energy consumption compared to the state-of-the-art strategy.

- ❑ *Chapter 05 « Securing the IoD : A Lightweight Blockchain-Based User-Drone Authentication Scheme »*

The main focus of this chapter is to create an authentication system based on blockchain technology, called HCALA, that uses Hyperelliptic Curve Cryptography (HECC) to secure the communication between an external user and a drone. The effectiveness and feasibility of HCALA are analyzed through informal security analysis techniques, which demonstrate that the proposed protocol is capable of withstanding various active and passive adversary attacks

Part I

Backgrounds, Preliminaries, and Basic Concepts

Chapter 1

Internet of Drones (IoD)

Chapter contents

1.1 Introduction

A drone or UAV (Unmanned Aerial Vehicle) is an aircraft that replaces the aircrew with a computer system and a radio link. The level of autonomy can vary from remote-controlled to fully autonomous, and the type of mission determines the military payloads that can be carried [6]. The size and weight of the drone affect the capacities required for each mission. These vehicles are equipped with various sensors and payloads, such as cameras, video cameras, and thermal sensors, to gather information during a mission. Additionally, they are equipped with GPS to determine their location and path during the mission [7].

The Internet of Drones (IoD) is a concept that has emerged in recent years with the advancement of drone technology and the growth of the Internet of Things (IoT). IoD involves the integration of drones into IoT networks to enhance the capabilities of both systems. By combining the real-time data acquisition and processing capabilities of drones with the ubiquitous connectivity of IoT networks, IoD enables the creation of intelligent, autonomous and responsive aerial systems that can perform various tasks efficiently and effectively.

IoD has the potential to support many industrial applications, including agriculture, infrastructure inspection, search and rescue operations, environmental monitoring, and many more. Using drones equipped with sensors and cameras, IoD can provide accurate and detailed data on various parameters, such as temperature, humidity, air quality, and structural integrity of buildings and bridges.

However, IoD poses several challenges, including energy consumption, security, privacy, and managing large numbers of drones in a single network. Researchers and engineers are actively working to address these challenges by developing new algorithms, mechanisms, and technologies that enable efficient and secure communication, management, and operation of drones in IoT environments.

This chapter provides a comprehensive overview of the fundamental concepts of IoD, starting with the definition of IoD and delving into the classification of UAVs, their potential applications, and the communication architecture that enables their operation. In addition, we highlight the challenges of implementing IoD, such as energy consumption, security, and privacy, as well as the solutions proposed to address these challenges. We also explore the future of IoD, including the potential for new technological advancements and its impact on various industries.

1.2 Internet of Things (IoT)

The term Internet of Things (IoT) refers to a constantly expanding network of ordinary physical objects that are linked to the internet. This technology enables internet-enabled devices to connect to a network, creating a web of digital data that can be accessed from anywhere and at any time [8–10]. These physical objects can be small or large machines that can interact with each other through the Internet without human involvement [9,11]. Figure 1.1 illustrates how the IoT is evolving, with devices interconnected and data being exchanged over the Internet.

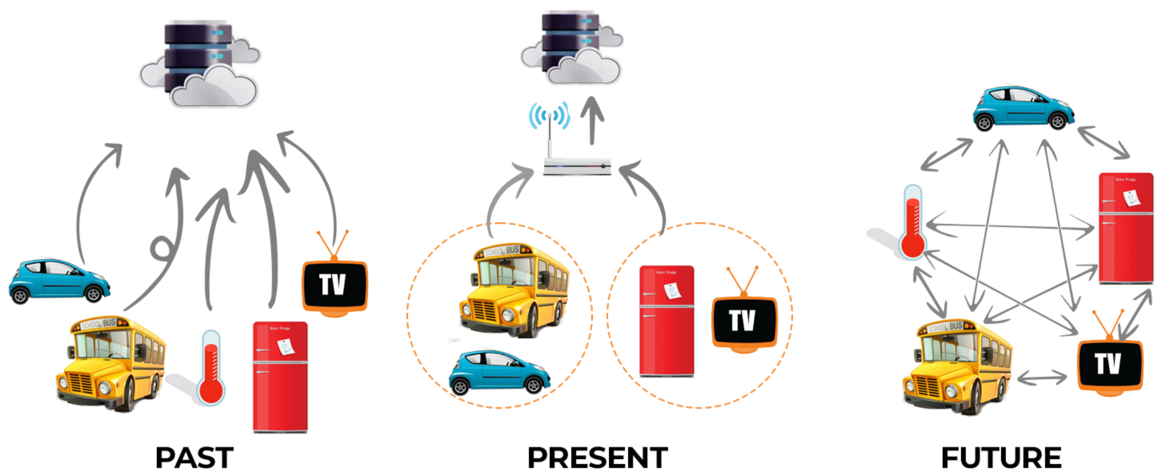


Figure 1.1 : Evolution of IoT.

Cisco estimates that there are currently about 50 billion devices connected to the Internet [12]. By 2025, more than 75 billion devices are predicted to be deployed and connected to the Internet, according to statistics published by the Statistics Research

Department [13, 14]. These IoT devices are designed with sensors that allow them to perceive their surroundings intelligently and actuators that allow them to perform actions independently [15]. Figure 1.2 provides examples of various IoT devices. These devices are typically resource-constrained, which means that they have limited memory space, low processing capabilities, and limited computational power.

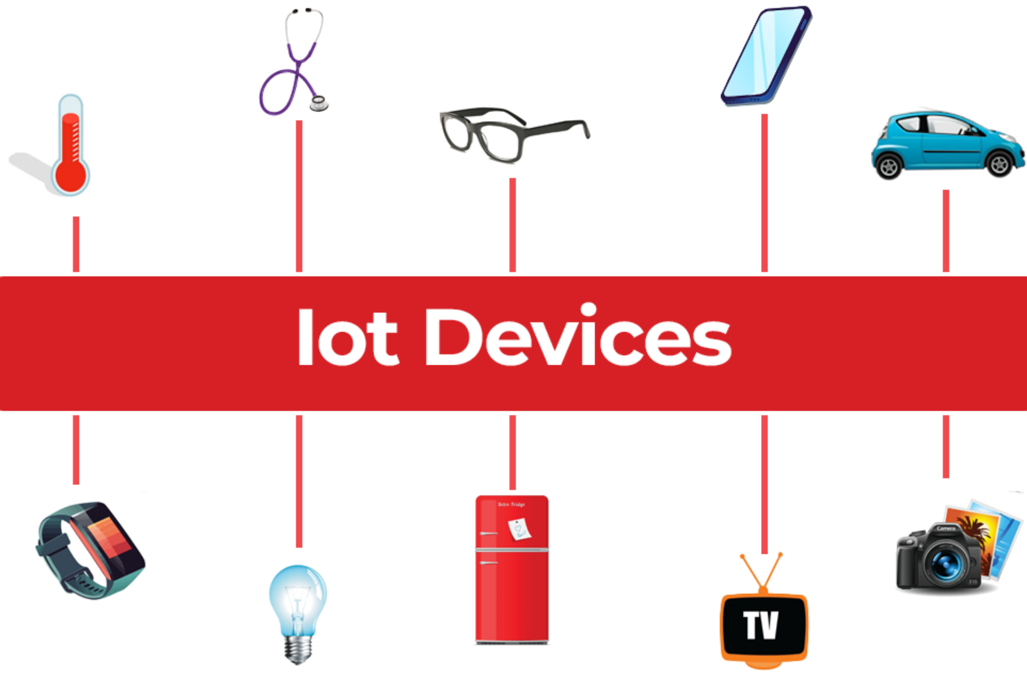


FIGURE 1.2 : Examples of IoT devices.

The emergence of IoT technology is made possible by various enabling technologies, including wireless sensor networks (WSNs), radio frequency identification (RFID), and cloud computing, which serve as essential components [16].

1.3 From IoT To IoD

While IoT technology has been widely applied in various industries, it has limitations in the context of drone technology. To address these limitations, IoD has emerged, which involves integrating drones into the IoT ecosystem to create a more efficient and autonomous system.

The switch from IoT to IoD technology has enabled drones to operate autonomously, making decisions based on real-time data. IoD technology uses on-board processors and sensors to process and analyze data, allowing drones to operate independently without relying on a central server for data processing. This enables drones to make immediate decisions based on real-time data and respond to changing conditions quickly and efficiently.

In addition, IoD technology enables drones to communicate directly with other drones, forming a network of interconnected devices. This enables joint drone operations, such as swarming, where multiple drones can work together to complete a task. IoD technology also enables drones to operate in areas where traditional wireless networks are not available, such as remote or rural locations, expanding the potential applications of drone technology.

In general, the limitations of IoT technology in the context of drone technology have been addressed by the emergence of IoD technology, which allows drones to operate more efficiently and autonomously.

1.4 Unmanned Aerial Systems and their Architecture

1.4.1 Unmanned Aircraft System

The Federal Aviation Administration (FAA) introduced the term Unmanned Aircraft/Aerial System (UAS) to refer to a system consisting of UAVs, various communication and data transfer links, one or more ground stations (GS), and additional systems to ensure the success of the mission and compliance with regulations and certification requirements. It is important to note that both FAA and European Aviation Safety Agency (EASA), through the Directorate General of Civil Aviation (DGCA), advocate for permanent control of the UAS system by a ground system, which limits the deployment of a fleet of UAVs. To address this, a dedicated GS is required to control each drone in the network. Figure 1.3 shows an example of UAS.

The UAVs in the system receive control and command data from the GS at a specific frequency while sending configuration information back to the GS regarding their flight conditions (position, speed, etc.) and the data acquired by the payload. These data enable the operator on the ground to monitor the flight and intervene in the UAV by sending commands if necessary.

1.4.2 UAS architecture

The UAS is a control system consisting of three main components : (i) the UAV or drone [17], (ii) the Ground Station Server (GSS), and (iii) communication links [18]. The GSS is responsible for the operation of the UAS system, while the UAV has a flight controller, which acts as its central processing unit, while the UAV performs a specific

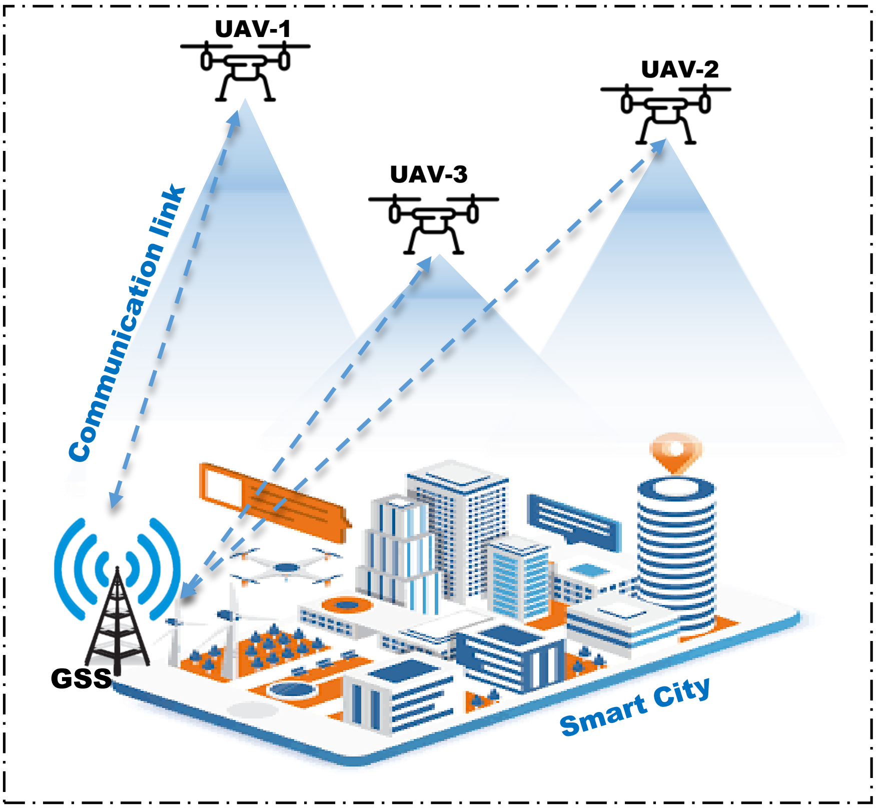


FIGURE 1.3 : An example of Unmanned Aircraft System

operation mission in the flight area. Moreover, the UAV's communication interface enables it to exchange commands and data with the GSS. The different components of the UAS are described below.

- **Unmanned Aerial Vehicle :** UAV is the primary element of the UAS that can acquire, retain, process, and share sensory data with other UAVs and the GSS. UAVs can have a variety of sizes, shapes, components, configurations, and objectives. Figure 1.4 shows that the UAV consists primarily of the following parts :
  - **Airframe :** UAV airframe is the platform that is responsible for carrying the various components of the UAV, and is designed to be lightweight, stable, and with limited space.
  - **Flight controller :** This component measures and monitors the UAV's stability and navigation. In addition, the flight controller generates control signals for the different states of the UAV to provide users with manual control of the UAV.

- **Sensors :** UAVs use sensors to collect data on various environmental factors such as temperature, humidity, pressure, and gas, which can be processed either partially by the UAV itself or transmitted to the GS for further analysis and processing [19].
- **The Global Position System (GPS) :** The GPS provides location, speed, and direction information for the UAV at specific intervals.
- **Radio Frequency IDentification (RFID) reading system :** The RFID reader collects data from RFID tags using a single antenna. It also performs tasks such as searching for tags in the area, downloading tags data, and localizing tags [20].
- **Single-Board Computer (SBC) :** The SBC receives and processes the data collected by the RFID reading system and sends them to the GSS through the UAV communication interface.
- **Communication interface :** An omnidirectional antenna or similar communication device is necessary for wireless communication with other UAVs and the GSS.
- **Battery :** The UAV relies on a battery to power its devices, but the battery life is limited and therefore efficient energy management algorithms are required.

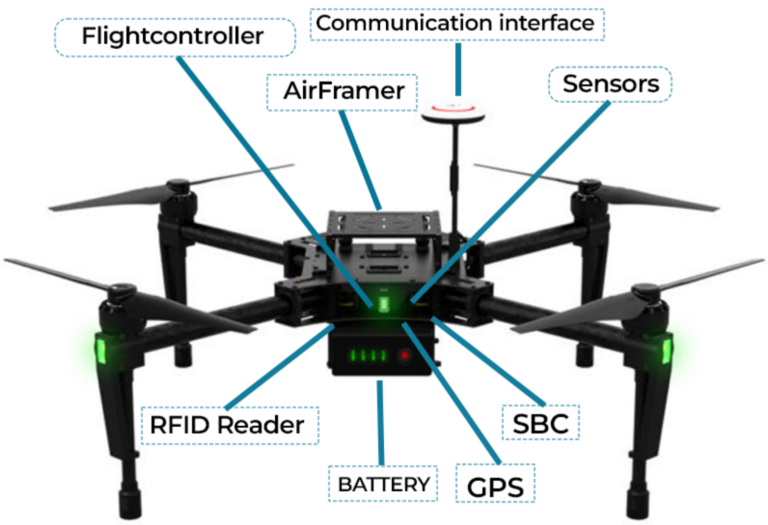


FIGURE 1.4 : UAV Components

- **Ground Station (GS) :** The GS, as shown in Figure 1.3, is a sophisticated system that consists of physical components and software that allow precise control of

UAV movement. Depending on the GS type, it may include a user-friendly human-machine interface that empowers the ground operator to track the UAV's real-time position using a topographic map overlaid with the UAV's trajectory. Additionally, the operator can customize various parameters, including altitude and payload settings, to ensure optimal UAV performance [21].

- **Communication links :** The communication links play a crucial role in UAS by facilitating the secure and reliable exchange of control messages and data between UAV and GSS. There are two communication links in UAS : control and data communication links [22]. The former is responsible for transmitting control messages between the GSS and UAVs, including commands, status reports, and control information between UAVs. The latter ensures the transmission of data captured by UAVs to the GSS, which user applications can utilize. Both types of links require high reliability, low latency, and bi-directional communication to ensure safe and efficient UAS operation.

1.5 Classification of UAVs

The categorization of UAVs varies across different countries and even among different military branches within a country [5, 23], as observed in the United States. The classification is based on various factors, including but not limited to the drone's size, endurance, flight altitude, function, mass, and payload. One of the most common ways to classify drones is based on size, weight, wing span, wing loading, range, maximum altitude, speed, endurance, and production costs. These design parameters are critical factors that differentiate various types of drone and facilitate useful classification systems.

1.5.1 Based on Aerodynamics

Numerous types of UAV systems have been developed and are currently in various stages of development. These include fixed-wing aircraft [24,25], helicopters [26,27], multicopters [28], motor parachutes and gliders [29–31], vertical takeoff and landing UAVs [32–34], drones assembled from pre-made parts [35], and commercialized UAVs [36, 37]. Each UAV is tailored to suit a specific mission and has advantages and disadvantages.

- **Fixed-wing drones :** are straightforward in their design and manufacturing process due to the widespread use of larger fixed-wing planes with minor enhancements and adjustments. The primary source of lift in fixed-wing drones is the fixed wings, which generate lift in response to forward acceleration. The amount of lift generated is regulated by the velocity and angle of air flowing over the fixed wings.

- **Flapping wing drones :** are primarily inspired by insects such as tiny hummingbirds to large dragonflies [38, 39]. Insects and birds have lightweight and flexible wings, the primary design features integrated into flapping wing drones. However, these flapping wings are complex because of their complicated aerodynamics. Unlike fixed-wing drones, flapping drones can support stable flights in windy conditions. Light, flexible, and flapper wings provide flapper motion with an actuation mechanism.

- **Fixed/flapping-wing :** A combination of fixed and flapping mechanisms is utilized, where the fixed wings generate lift, while the flapping wings generate propulsion [40]. The design of these drones is inspired by dragonflies, which use two pairs of wings to increase lift and thrust forces. By incorporating both fixed and flapping wings, these drones achieve increased efficiency and aerodynamic balance [40].

- **Multi-rotor :** The primary means of generating lift and propulsion for multi-rotor UAVs is through the forceful thrust produced by the main rotor blades. Unlike fixed-wing aircraft, multirotors can have vertical take-off and landing (VTOL) and hover in place [41,42]. The multi-rotor design is determined by the number and placement of motors and propellers on the frame. Their ability to hover and maintain a stable position makes them well suited for surveillance and monitoring applications. However, the main limitation of multi-rotors is their high power consumption, which restricts their endurance.

  The categorization of multicopters is based on the number and arrangement of motors, with each category designed for a specific type of mission. Depending on the mission's requirements, multicopters are classified into various configurations, including monocopter, tricopter, quadcopter, hexacopter, and ocopter.

1.5.2 Based on Landing

Drones can be further classified according to their take-off and landing mechanisms, which fall into horizontal take-off and landing (HTOL) and vertical take-off and landing (VTOL). HTOL drones have several benefits, such as the ability to fly longer distances and capture high-quality photos and videos for aerial photography and filming, which makes them popular among professionals. However, they also pose particular challenges, particularly during take-off and landing. In contrast, VTOL drones have limitations in angle, stability, and coverage, affecting the quality of the photos and videos they capture. As a result, they may not be as well-suited for professional use as their HTOL counterparts [3].

UAVs are defined and differentiated according to the flight mechanism and altitude, as shown in Figure 1.5

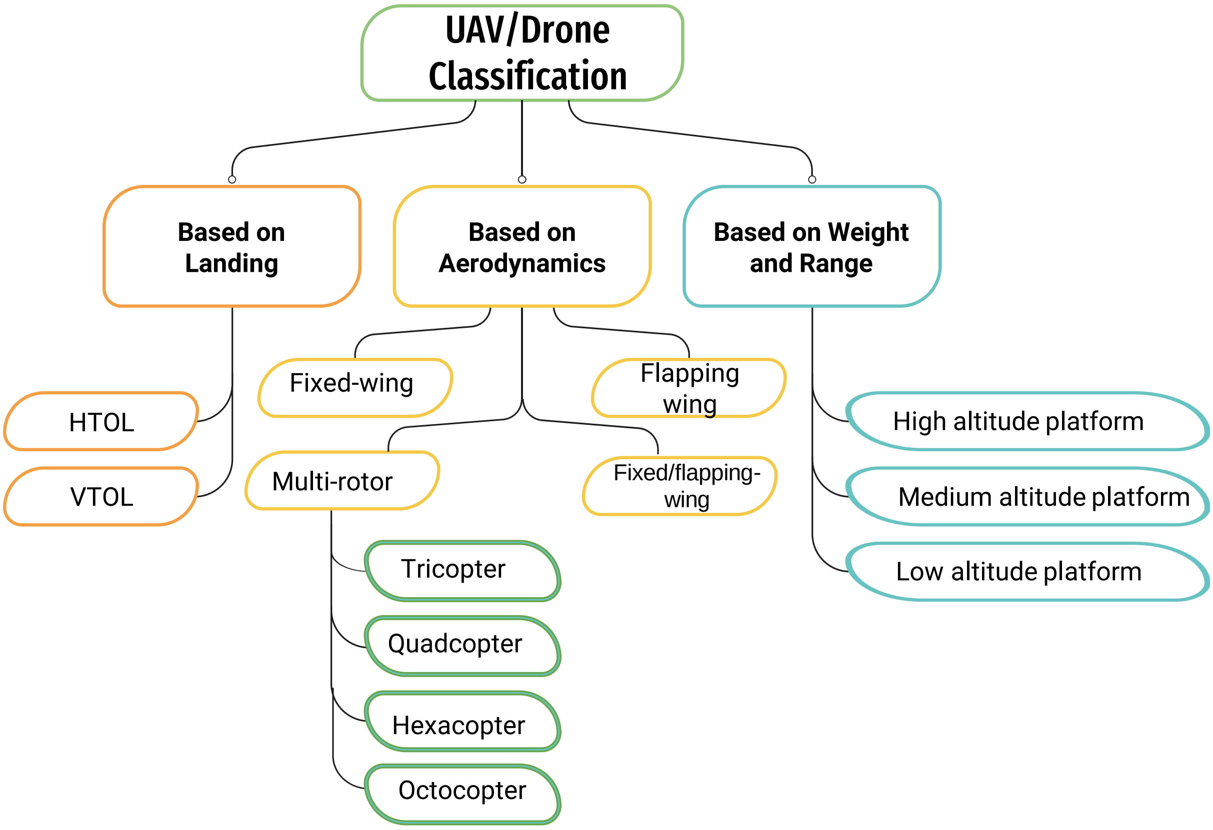


FIGURE 1.5 : Classification of UAV based on landing, aerodynamics and altitude

1.5.3 Based on Weight and Range

Drones have been classified by weight and range by certain researchers and organizations. A tabulated list of UAVs sorted by size, weight, altitude, and endurance is presented in Table 1.1.

1.6 Communication Architectures for IOD

An architecture of communication defines how data are transmitted between the ground crew and UAVs or among UAVs. In fast-moving multi-UAV systems, communication is a crucial factor. Based on the data flow, the communication structures of UAVs

Type	**Size (cm)**	**Weight (g)**	**Maximum Altitude (m)**	**Endurance (min)**
Nano	Up to 15	$W \leq 50$	$h \leq 100$	$E \leq 10$
Micro	$15 \leq S \leq 30$	$15 \leq W \leq 30$	$100 \leq h \leq 500$	$30 \leq E \leq 60$
Mini	$30 \leq S \leq 60$	$250 \leq W \leq 1000$	$500 \leq h \leq 1000$	$30 \leq E \leq 60$
Medium	$60 \leq S \leq 150$	$1000 \leq W \leq 5000$	$1000 \leq h \leq 5000$	$60 \leq E \leq 120$
MALE	$150 \leq S \leq 300$	$5000 \leq W \leq 20000$	$5000 \leq h \leq 10000$	$120 \leq E \leq 240$
HALE	$S > 300$	$W > 2000$	$h > 10000$	$E > 240$

Table 1.1 : UAVs classification [3–5]

can be classified as either centralized or decentralized. This categorization is illustrated in Figure 1.6 and is explained in the following.

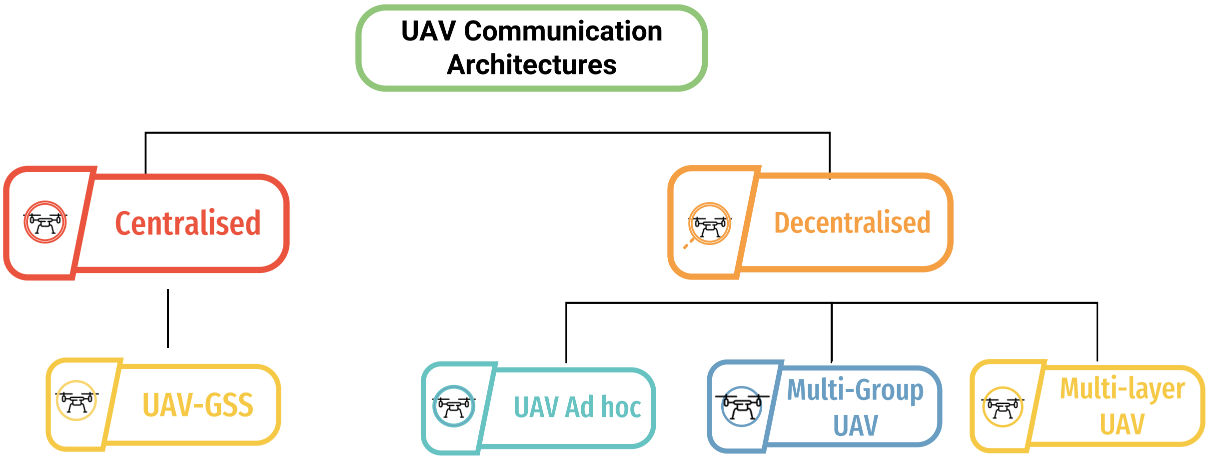


Figure 1.6 : UAV communication architectures

1.6.1 Centralized Communication Architecture

A centralized UAV communication architecture is shown in Figure 1.7, which has a central node (that is, the GS) to which all UAVs are connected. This widely used architecture involves direct connections between each UAV and the GS to transmit and receive command and control data. At the same time, UAVs are not connected to each other. The entire network is centered on the GS, and data communication between two UAVs is transmitted through the GS. Command and control data transmitted between the ground crew and a UAV have a short information delay, since all UAVs are directly connected to the GS. However, data transmitted between two UAVs are expected to experience a longer delay as it needs to be routed through the GS. This architecture requires advanced radio transmission devices with high transmission power to facilitate long-distance communications between the GS and UAVs, which may need to be more practical for smaller UAVs due to their size and payload constraints. In addition, the GS represents a single point of failure, rendering the entire UAV network vulnerable in the event of GS failure. Therefore, this communication architecture lacks robustness.

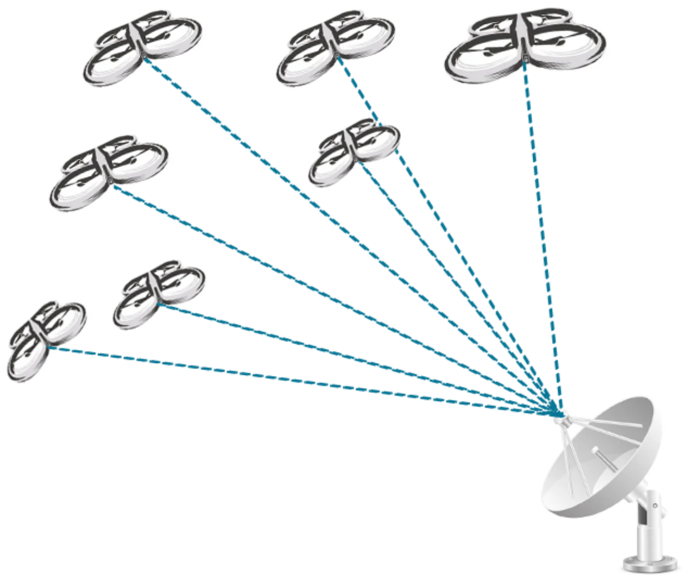


Figure 1.7 : Centralized UAV Network

1.6.2 Decentralized Communication Architecture

In contrast to the centralized architecture, the decentralized architecture does not require a central node, and two UAVs can communicate with each other directly or indirectly. This allows information data not intended for the GS to be routed via the UAV rather than the GS [43]. Three different types of decentralized communication architectures are described below.

1.6.2.1 UAV Ad hoc Network

A UAV ad hoc network is shown in Figure 1.8, a popular type of multi-UAV system called the UAANET (UAV Ad hoc Network). It comprises a swarm of UAVs, each with one or several base stations. These drones exchange information, with a leader UAV acting as a gateway that relays data between the GS and the other drones. This architecture requires two radio transmissions. Since drones fly near each other, they can use lightweight, cost-effective transceivers. Each node in the network can act as a relay to transmit information from the source to the destination. In the UAANET, nodes can enter or exit the network at any time, and the group of UAVs is homogeneous. Reliable protocols are needed to maintain network topology and reconstruction. Additionally, suppose different types of UAVs are used in the network. In that case, it can be divided into two distinct communication architectures : multi-layer UAV ad hoc network and multi-group UAV network.

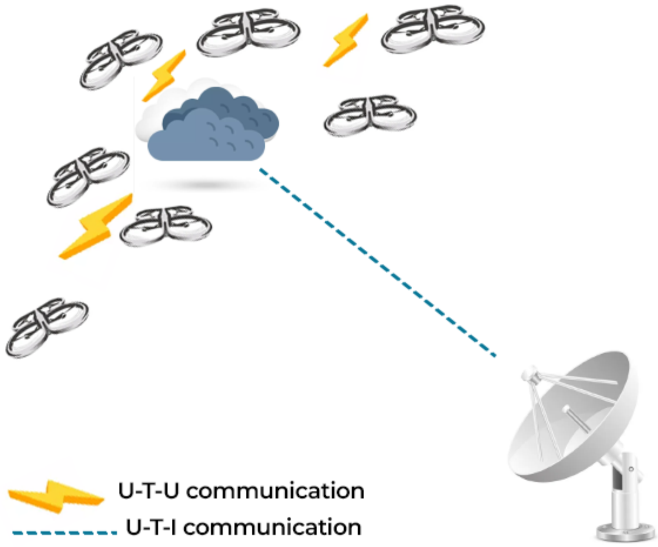


Figure 1.8 : UAV Ad Hoc Network

1.6.2.2 Multi-Group UAV Ad hoc Network

A multi-group UAV network is depicted in Figure 1.9. In this architecture, UAVs form a network within their respective groups, with a backbone UAV serving as a gateway to the ground station. Intragroup communication occurs within the UAV ad hoc network, while intergroup communication occurs through the backbone UAVs and the GS. This architecture is a combination of centralized and UAV ad hoc networks, making it suitable for missions involving many UAVs with different communication and flight characteristics. However, it is essential to note that this semi-centralized architecture is still not entirely robust.

1.6.2.3 Multi-layer UAV Ad hoc Network

The multi-layer UAV ad hoc network is a communication architecture designed to network multiple groups of different UAVs. An example of this architecture is depicted in Figure 1.10. In this architecture, the UAVs within each group form a UAV ad hoc network that constitutes the lower layer of the multi-layer UAV ad hoc network. The backbone

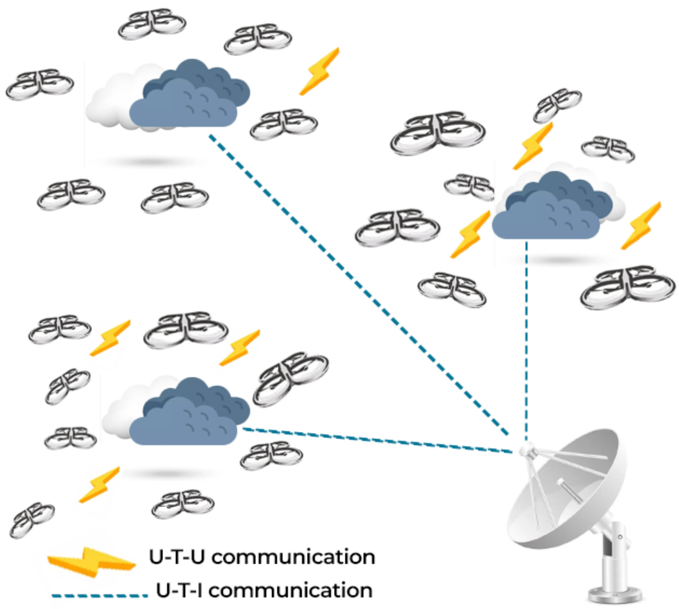


FIGURE 1.9 : Multi-Group UAV Ad hoc Network

UAVs of all groups form the upper layer. Only one backbone UAV in the multi-layer UAV ad hoc network is directly connected to the GS, and information exchange between any two UAV groups does not necessarily require routing through the GS. This architecture reduces the computational and communication load on the GS because it only processes information data that are destined for it. The multi-layer UAV ad hoc network architecture is beneficial for one-to-many UAV operation modes. It is also robust, since it does not have a single point of failure.

The technology for UAV swarm communication architecture has made significant advancements. There are various communication architectures available for different mission scenarios. The advantages and disadvantages of the four architectures mentioned earlier are summarized in Table 1.2.

1.7 Applications of IoD

In this section, we explore the potential uses of the IoD networking architecture, examining all proposed application fields in detail. [44–53]. Additionally, we will delve deeper into the subject by analyzing how drones can be used in various applications that can reap the benefits of their adoption from an economic standpoint. The primary objective of UAVs is to perform various missions that can be military, scientific, economic,

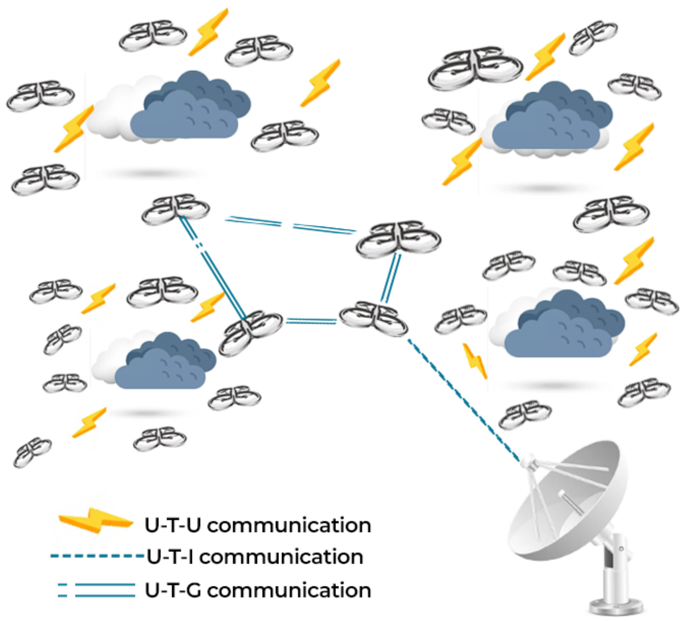


FIGURE 1.10 : Multi-layer UAV Ad hoc network

or commercial. UAVs gained significant attention due to their ability to operate in hazardous environments [54]. Initially, UAVs were developed for military purposes to carry out missions considered (3D) "Dull, Dirty, and Dangerous" for human pilots. During the First World War, aircraft without radio-controlled pilots were introduced to decrease the number of pilot diseases [55]. However, military drones were not widely used until the wars in Korea and Vietnam, when they were used for stealth surveillance. In the 1990s, the concept of 'zero death' emerged, which led to the development and use of drones in all military conflicts from the early 2000s. The increasing popularity of these machines is attributed to the miniaturization of avionics and their long-distance communication capabilities.

It is suitable to list some military applications that involve the utilization of UAVs.

- **Military applications :**
  - Combat aircraft ;
  - Surveillance at border ;
  - Bomb detection ;
  - Spying ;
  - Missile launching.

Features	Centralized	**Decentralized**		
		Single-Group	Multi-Group	Multi-Layer
Communication through multiple hops	×	✓	✓	✓
Relay of traffic by UAVs	×	✓	✓	✓
Various categories of UAVs	×	×	✓	✓
Self-configuration	×	✓	×	✓
Coverage constraints	✓	✓	✓	×
Single Point of Failure	✓	×	✓	×
Resilience	✓	×	×	✓

Table 1.2 : The advantages and disadvantages of the mentioned architectures

In the 90s, after the emergence of UAVs in the military domain and the rapid development of this technology, they emerged in the civilian domain [56] and have been known for a new role in environmental monitoring. Their applications have grown significantly in recent years, with examples including :

- **Civil applications :**
  - Aerial cartography for geographic studies ;
  - Construction and infrastructure inspection ;
  - Remote sensing ;
  - Disaster management ;
  - Search and rescue (SAR) ;
  - Crowd management ;
  - Monitoring of road traffic ;
  - Provide wireless coverage ;
  - Pipelines and Power line inspection ;
  - Delivering.
- **Environmental applications :**
  - Firefighting and forest fire detection ;
  - Precision agriculture ;
  - Soil monitoring ;
  - Pollution studies and land monitoring ;

- Mountain inspection ;
- Meteorological measurements.

To provide more clarity, Table 1.3 lists some primary sources of this present work, categorizing the application areas and the specific functions that drones perform [45].

Application area	Activity	Open challenges	References
Law enforcement	Ensuring the safety of the public Crowd control	Use of multiple sensory units Extended duration of missions Uninterrupted connectivity	[45, 47–52, 57–59]
Civil engineering	Aerial photogrammetry Creation of Maps for (Gis) Development of land Advancement of science and research.	Multiple sensing units High quality video imaging	[46, 53]
Logistics tracking	Unmanned cargo Enhancing Processes Proactive maintenance	Utilization of multiple sensors Interaction with surrounding environment	[47, 48, 51–53, 58–61]
Military applications	Search and rescue Protection border from above	Extended duration of missions Multiple sensing units Uninterrupted connectivity Autonomous decision-making	[45, 47–51, 58]
Air traffic controlling	Traffic control Security Weather forecast Intelligent Transportation Systems Science and research	Multiple sensing units Uninterrupted connectivity Near Real-Time	[45,47,48,50–53, 57, 59, 60]
Public safety	Search and rescue Disaster Management	Real-time monitoring High quality video capture	[44,45,47,51–53, 59, 60, 62, 63]
Entertainment	TV series and films Live streaming concerts and events Flight clubs and associations Self-Portrait photography	High-quality video recording Artificial Vision Objects and Pattern Tracking	[46–48,59,60,63, 64]
Industrial monitoring	Smart Agriculture and Pharming	Utilization of various sensing units	[46–48,59,60,63, 64]
Processes enhancement	Monitoring Power lines and grids Oil and Gas	High-resolution video capturing Interaction with the environment	[65–69]

Table 1.3 : A summary of the main applications of drones

1.8 Challenges and future of IoD

Integrating IoD and IoT technologies offer flexible support for IoT services, such as surveillance, monitoring, emergency management, and SAR scenarios. However, IoD faces several challenges, such as UAV control and management, deployment, selection, collisions, and interference, path planning, data rate, and coverage, energy consumption, security, and privacy. This section discusses the various IoD challenges that require comprehensive studies. Furthermore, we present future perspectives for IoD to address these challenges, aiming to promote the creation of innovative solutions that enhance IoD's reliability, efficiency, and security.

1.8.1 UAV control and management

As the number of UAVs increases, remotely controlling and managing them from an Internet location can become complicated due to the frequent data transmissions between the UAVs and IoT ground devices. While some studies on the IoD have tackled this concern [70, 71], it is still necessary to develop effective algorithms that can enable UAV management and control features, including subscription and notification, data handling, localization of UAVs, and management of groups.

1.8.2 UAV deployment

Some IoD studies have addressed the issue of deploying UAVs in critical locations to reduce wireless latency for IoT ground users and ease traffic congestion [72, 73]. When UAVs are placed in high-density user areas, channel conditions can be favorable, but congestion can increase due to limited wireless channel capacity. In contrast, placing UAVs over areas with low user density can limit traffic offloading and affect wireless latency. An optimal UAV deployment strategy can maximize coverage and throughput, but this is an NP-hard optimization problem. However, different optimization heuristics such as the ant colony, particle swarm, and genetic algorithms can be used to solve this problem with low complexity.

1.8.3 UAV selection

One of the challenges in IoD is selecting the most suitable UAV for a particular task to minimize energy consumption and operation time. Factors such as remaining UAV energy, task energy requirements, distance to the task location, UAV speed, and time required for task transmission and processing must be considered to make this selection. Researchers have proposed various algorithms and mechanisms to address this challenge [74, 75].

1.8.4 Collision and interference

When multiple UAVs offload large amounts of data, such as real-time video streams, to a GS with high IoD connectivity, it can lead to collisions and interference between the UAVs and the GS [71, 76–79]. Numerous studies on IoD have focused on managing the challenges of collisions and interference. Several parameters must be optimized to reduce interference, including the UAV trajectory, path planning, resource allocation, and control of altitude and mobility.

1.8.5 UAV path planning

Another significant challenge in IoD is developing an optimal UAV path planning mechanism, which has been discussed in multiple studies [80–84]. The goal of UAV path planning is to maximize data collection rate while minimizing the cost of flying time, energy consumption, and flying risk level. To address this challenge, various types of information can be used, including geographic topology, static sensor node locations, flying risk levels, and airspace restrictions.

1.8.6 Energy consumption

Despite IoD's goal of lowering the energy consumption of UAVs and IoT ground devices by merging the resource capabilities of FANET and IoT networks, energy usage still presents a considerable obstacle for IoD. Energy consumption is utilized for various IoD activities, including data processing and storage, routing, querying, and data transmission. Some IoD studies have addressed this issue, but there is still room for improvement [85–90]. In the future, researchers could explore using the wireless medium to recharge UAV and IoT device batteries.

1.8.7 Data rate and coverage

Providing seamless, wide-area coverage with high data rates anywhere and anytime is another significant challenge of IoD. Integrating UAVs with satellite communication networks can create an integrated space-air-ground network with higher data rates and coverage. Numerous research studies have been suggested on communication between

UAVs and satellites [91–94]. In these studies, the UAV functions as a relay that establishes a connection between the terrestrial network through the satellite link and the user terminals via a ground link [91].

1.8.8 Security and privacy

Since the wireless medium is broadcasted, security and privacy issues can affect UAVs. Malicious eavesdropping can compromise the security of data transmitted between UAVs and GS. To address this, the physical layer can incorporate measures such as relay selection, friendly jamming, and multiple-antenna arrays, to ensure the security of the data exchanged. Although most of the IoD research that deals with security and privacy challenges focuses on the physical layer [95, 96], future IoD research in this area could explore addressing security and privacy issues in other layers, such as the transportation and application layers.

IoD challenge (s)	Recommended IoD references	Future IoD research directions
UAV control and management	[70, 71]	Suggested efficient algorithms for UAVs managing and controlling UAVs, offering various functionalities, including but not limited to subscription and notification, data management, UAV localization, and swarm management.
UAV selection	[74, 75]	Take into account various variables, such as the UAV's energy capacity, the energy demand for the mission, the distance to the mission location, the UAV's velocity, and the time needed for task transmission and processing.
UAV deployment	[72, 73]	Application of optimization heuristics, such as the Particle swarm, genetic algorithms, and ant colony optimization, to the deployment of UAVs.
Collision and interference	[72, 76–79]	The optimization of various IoD parameters are necessary, including UAV trajectories and the planning of paths, allocation of resources for UAV and IoT, and management of UAV altitude and mobility.
UAV path planning	[80–85]	The flight path of UAVs can be planned using various categories of data, such as geographical topology, the locations of static sensor nodes, airspace constraints, and flight risk levels.
Data rate and coverage	[91–94]	Incorporating UAVs into satellite communication networks.
Energy consumption	[85–90]	Wireless charging of batteries for UAVs and IoT devices.
Security and privacy	[95, 96]	Improving the security and privacy of IoD at three levels : Application layer, transport layer, and physical layer

Table 1.4 : Literature summary

1.9 Conclusion

In conclusion, integrating drones into the IoT environment has paved the way for developing IoD, which enables the creation of intelligent, autonomous, and responsive aerial systems. IoD has the potential to revolutionize the applications of various industries, providing accurate and detailed data on various parameters. However, the implementation of IoD poses several challenges, such as energy consumption, security, and managing large numbers of drones in a single network.

In this chapter, we have provided a comprehensive understanding of the fundamental concepts of IoD. We began with a clear definition of IoD and moved on to explore the classification of UAVs, their potential applications, and the communication architecture that enables their operation. Finally, we have highlighted the various challenges that need to be addressed to successfully implement IoD, including energy consumption, security, and privacy concerns. It is evident that IoD has significant potential and that new technological advances will continue to shape its development. Overall, this chapter lays the groundwork for the subsequent chapters, in which we will delve deeper into specific aspects of IoD and examine the current state-of-the-art in more detail.

The next chapter will delve into the current state of CPP for drones, with a specific focus on static path planning patterns. This will include a thorough examination of existing simulators for drones, highlighting their strengths, weaknesses, and overall objectives.

Chapter 2

Drone Path Management

Chapter contents

2.1 Introduction

CPP is a crucial aspect of UAV operations. Drones have been increasing rapidly in recent years, and they are being employed for a wide range of applications, such as search and rescue, surveillance, mapping, and environmental monitoring. The success of these operations depends on the effectiveness of the CPP algorithm employed. However, designing and implementing a CPP algorithm for drones can be challenging due to the complex nature of the tasks involved.

One way to address this challenge is by using simulator platforms for drones. Simulators provide a safe and cost-effective environment for testing and evaluating CPP algorithms for drones. They offer the ability to simulate real-world scenarios and test various CPP algorithms in different environments. Furthermore, simulators can provide a controlled environment to evaluate the drone's performance regarding coverage efficiency, endurance, and battery life.

In recent years, there has been an increase in the development of simulator platforms for drones, which has led to the emergence of various commercial and open-source platforms. These simulators offer different features and capabilities, such as environmental modelling, and sensor simulation. However, choosing the appropriate simulator platform for CPP testing can be challenging due to the varying features and capabilities of the simulators.

In this chapter, we will provide an overview of the current state of CPP for drones, focusing on static path planning patterns. We will explore the current simulators for drones, including their objectives, strengths, and shortcomings. We will also discuss the challenges of CPP for drones and potential future directions for research in this field.

2.2 Coverage Path Planing (CPP)

2.2.1 What is Coverage Path Planning ?

Drone CPP is a vital aspect of UAV operations that involves finding the optimal path for a drone to cover a designated area while avoiding obstacles. In the context of aerial operations, the obstacles within the workspace can act as no-flight zones (NFZs), which are areas that the UAV must exclude from its planning phases, such as locations close to airports or irrelevant buildings. The goal is to ensure that the entire area is visited while minimizing the distance traveled by the UAV, taking into account the limited flight time, payload capacity, and other constraints of the UAV. The specific constraints of the UAV may include the altitude, speed, field of view (FoV) and sensor range. This can be used in a variety of applications, such as aerial photography, surveying, mapping, search and rescue, and monitoring of natural resources.

Usually, a decomposition technique divides the target environment into non-overlapping regions called cells. Depending on the decomposition type, the cells' size and resolution may vary, and a specific strategy must be implemented to ensure complete coverage. These cells are proportional to the range of the UAV's camera (aerial coverage) and represent the footprint of the UAV. The following subsection will introduce key considerations for selecting a CPP strategy for a particular use case.

2.2.2 Importance of CPP for Drones

CPP is critical for drones in various applications, including agriculture, forestry, search and rescue operations, and infrastructure inspection. In agriculture, drones can be used to monitor crop health, detect pests and diseases, and identify irrigation problems. In forestry, drones can help identify areas affected by wildfires, monitor tree health, and assess the growth of new trees. In infrastructure inspection, drones can inspect buildings, bridges, and other structures for damage and wear, reducing the need for manual inspections that can be dangerous and time-consuming. In search and rescue operations, drones can be used to search for missing persons, map out terrain, and deliver emergency supplies.

CPP algorithms allow drones to cover large areas quickly and efficiently, providing valuable data and insights that can be used for decision-making. By using CPP algorithms, drones can perform tasks that would be difficult or impossible for humans, making them an essential tool in various industries.

2.2.2.1 Variation of Goals in CPP

One common goal in CPP for drones is surveilling a specific location or object. The drone must fly around the location or object and capture images or videos from different angles. This type of goal is common in applications such as security surveillance, traffic monitoring, and industrial inspections.

Another goal in CPP for drones is the coverage of a specific area. The drone must fly over and cover the area to achieve the goal. This type of goal is common in applications such as mapping, environmental monitoring, and search and rescue. The CPP algorithm for this goal must ensure that the drone covers the entire area with minimal overlap or uncovered zones.

In some cases, the goal in CPP for drones can be dynamic and change during the mission. For example, in a search and rescue operation, the goal can change from covering a specific area to locating and rescuing a person. The CPP algorithm for this type of goal needs to be flexible and adaptable to changes in the mission objective.

Moreover, in some applications, the goal in CPP for drones can be a combination of different objectives. For example, in an environmental monitoring mission, the goal can be to cover a specific area while collecting data from different sensors. The CPP algorithm for this type of goal needs to consider multiple objectives and optimize the drone's path to achieve all objectives efficiently.

In summary, the variations of goals for CPP drones depend on the application and can affect the CPP algorithm employed. The algorithm needs to be tailored to the specific goal, whether it is coverage of an area, surveillance of a location or object, dynamic goal, or a combination of objectives.

2.2.2.2 Collision-free vs. Optimal Planning

Path planners that return optimal paths typically employ optimization, which requires initializing a cost function. During path generation, the cost functions may consider different properties/metrics based on the conditions imposed by the objective, environment, and other application-related factors. The cost function may include variables such as path length, altitude change, proximity, flight time, battery consumption, etc. Minimizing the cost function yields the optimal path concerning the specified criterion.

2.2.3 Environment Variations

When selecting a path planning approach for a drone, it is crucial to take into account the environment in which the drone will be operating. There are several critical factors to consider when choosing a path planner approach, and we will discuss some of the most important considerations below.

2.2.3.1 The Distinction of 2D and 3D Path Planning

It is important to understand whether a path planner is designed for 3D or 2D space when choosing a planner for a drone. While many of the same approaches can be used in both cases, 3D space presents additional complexity that can make path planning more difficult and computationally expensive.

Offline path planning is a more practical option for drones when compared to online path planning, since the path can be calculated on a more powerful computer and then uploaded to the UAV. However, it is still essential to evaluate whether the environment is 3D or 2D since long computation times can be undesirable, regardless of the path planning approach used. By assessing the environment and selecting a path planner that is suitable for it, drone operators can optimize the path planning process, ensuring that the drone follows a safe and efficient path. It is important to minimize computation times to ensure that the drone is able to achieve its mission quickly and effectively.

2.2.3.2 Static vs. Dynamic

Another important consideration when selecting a path planner for a drone is whether the environment is static or dynamic. In a static environment, an offline path planning approach can be used since the environment is assumed to remain the same over time. A path generated before the UAV's flight will remain valid.

In a static environment, the path can be tested and evaluated in a simulator to ensure that it avoids all obstacles. This can be especially helpful if the planner does not initially consider the dynamics of the UAV. A similar approach can be used for dynamic environments, but the path may need to be updated in real-time as the environment changes.

Online path planning is necessary for dynamic environments since the environment is continuously changing. This requires a fast search algorithm that can generate a new path quickly based on sensor data. Stopping the drone mid-flight to generate a new path can be inefficient, as a lot of energy will be wasted. Although fast planning may result in lower accuracy, appropriate safety features can be put in place to mitigate any potential issues.

2.2.4 Area of Interest (AoI)

One important aspect of drone CPP is identifying the AoI that needs to be covered. The AoI can vary depending on the application, but it is typically a specific geographical location that needs to be surveyed or monitored.

The AoI is the region that a drone needs to cover. This region can be represented by a shape with a set of points called vertices $\{v_1, v_2, \cdots, v_p\}$, which can be identified by their coordinates $(V_x(i), V_y(i))$. Each vertex has an internal angle referred by γ_i. The sequence of vertices is called a polygon, and it can be closed or open. The edges between two adjacent vertices V_i and are referred by e_i, and their length can be calculated using the distance formula $l_i = ||V_i - V_{next(i)}||$. The AoI interest may also include No-Fly Zones (NFZ) that can be represented by obstacle-points $\{u_1, u_2, \ldots, u_p\}$. Figure 2.1 shows three examples of such areas.

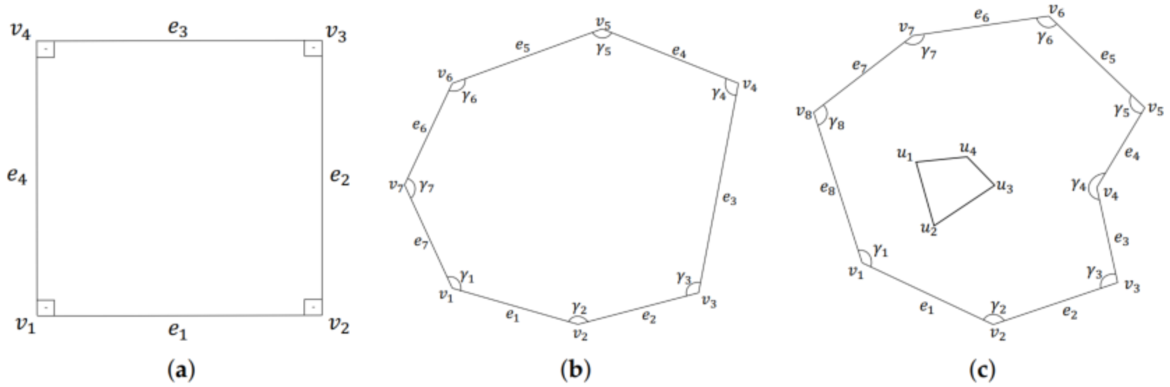


Figure 2.1 : Exploring various AoI during CPP missions : (a) Rectangular ; (b) Convex Polygon ; (c) Concave Polygon with NFZ. [1]

During coverage path planning, it's important to consider the shape of the area being covered. Some planning methods may only work with rectangular areas or simplify the shape to a rectangle, while others can handle more complex shapes like concave and convex polygons that represent irregular areas. In some cases, the area may also contain NFZs that must be avoided during coverage. These zones could be areas where coverage is unnecessary or places where drones are not permitted to fly. To make the coverage task easier, different techniques can be used to break down the complex shapes of areas, such as reducing their concavities or dividing the area into smaller cells.

2.2.5 Field of View

One of the key factors in the CPP of drones is the drone's field of view (FoV). The FoV, or the UAV footprint, refers to the area visible to the drone's cameras while flying.

The FoV is determined by the drone's height (h), and camera lens. The FoV is essential in determining the coverage efficiency of the drone and optimizing the CPP algorithm.

Moreover, the FoV is also affected by the drone's orientation and movement. As the drone moves along the CPP path, its orientation changes, and its FoV shifts. Therefore, the CPP algorithm should account for the drone's movement and adjust the path planning accordingly.

The projected area of a camera's field of view (FoV), illustrated in Figure 2.2, is dependent on the camera's height (h) and its angle of view. To calculate the dimensions (F_w, F_l) of the projected area, the following equations can be utilized :

$$F_w = 2h \times \tan(\frac{\alpha}{2}) \tag{2.1}$$

$$F_l = 2h \times \tan(\frac{\beta}{2}) \tag{2.2}$$

Where F_w is the width of FoV, F_l is the length of FoV, (h) is the altitude of the UAV, α is the vertical degree of camera, and β is the horizontal degree of camera.

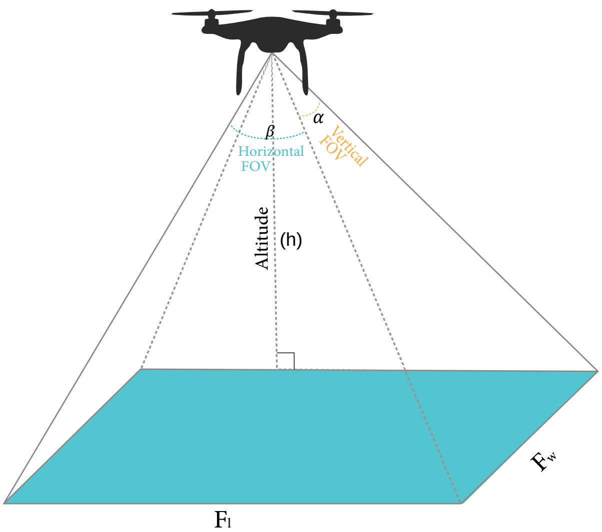


FIGURE 2.2 : UAV footprint representation

2.2.6 Performance Metrics for CPP Algorithms

Performance metrics are critical for evaluating the effectiveness and efficiency of CPP algorithms. The evaluation criteria vary depending on the application domain, but most of them share some common metrics. In this section, we will discuss some key performance metrics used for CPP algorithms.

2.2.6.1 Coverage Quality

The coverage quality metric measures the completeness of coverage achieved by the algorithm. It calculates the percentage of the total area that has been covered by the UAV. It is essential to maximize the coverage quality, especially when the mission involves tasks such as surveying, monitoring, and inspection.

2.2.6.2 Path Length

The path length metric is used to evaluate the efficiency of the algorithm. It measures the total length of the path followed by the UAV to cover the AoI. The shorter the path length, the more efficient the algorithm.

2.2.6.3 Execution Time

The time of execution for a drone mission refers to how long it takes for the drone to finish its task, from takeoff to landing. This time includes flying to the area it needs to cover, doing the task, and coming back. The duration of a drone mission is important because it affects how efficient the operation is and how many resources are needed. It's an essential factor to consider when planning a drone mission, especially when time is a critical aspect of the mission.

2.2.6.4 Number of turns

The number of turning maneuvers is a crucial factor in the performance evaluation of coverage path planning (CPP) algorithms for drones. During a turning maneuver, the drone slows down, rotates, and then accelerates again. This process takes time and requires energy. Hence, reducing the number of turning maneuvers is often considered to be an effective way to save energy and prolong the mission time.

2.3 Mobility Patterns for Surveillance

Choset [97] categorized CPP algorithms based on the decomposition employed. The majority of CPP algorithms decompose the AoI into cells. This is the preferred method for irregular areas. In contrast, when the AOI has a regular shape, no decomposition is necessary for a single UAV coverage. In this section, five search patterns are described.

2.3.1 Back-and-forth Search Pattern

The back-and-forth or scan technique is a straightforward and useful way for drones to plan their paths over an area. The drone moves back and forth along one axis (either horizontal or vertical) over the AoI, with the distance between each segment along that axis determining the resolution in the trajectory(R). This scanning method can also be adapted for regions with straight sides, called convex polygonal regions [98]. We can calculate the total length of this path using a formula [99] :

$$D_{scan} = \left(\frac{L}{R} + 2\right) L \tag{2.3}$$

Figure 2.3 illustrates a scan path that is aligned with the x-axis, where $L = 7$ represents the length of the AoI and $R = 1$ is the resolution of the trajectory.

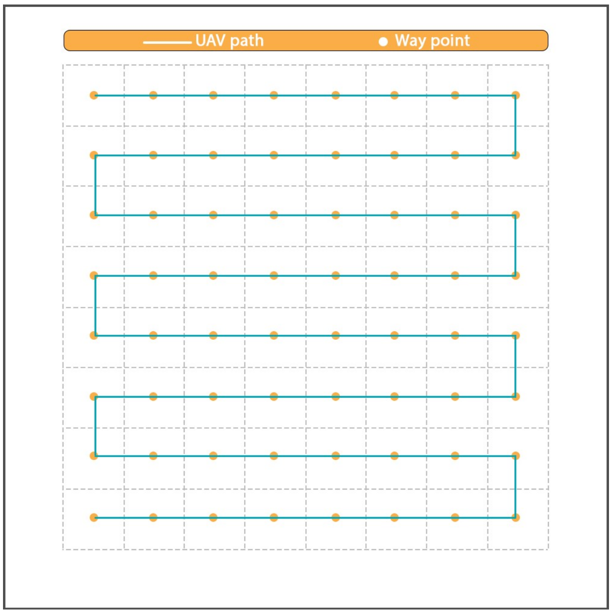


FIGURE 2.3 : Back-and-forth Path

2.3.2 Rectangular Spiral Search Pattern

Rectangular spiral is a common flight pattern for UAVs or drones conducting a systematic search of an area. A rectangular spiral pattern covers the area along the x and y axes, ensuring thorough and systematic coverage of the target area.

The pattern starts from the center of the target area and moves parallel to one side while flying. After that, the drone turns 90 degrees and flies parallel to the next side of the rectangle while gradually increasing the length of each line segment. This pattern continues until the entire area is covered. Alternatively, the pattern can begin outside the area and move inward, with decreasing line segments. This approach ensures that no area is missed, and the entire region is covered with minimal overlap. The total length of the spiral path can be computed using the formula :

$$D_{scan} = \left(\frac{L}{R} + 2\right) L \tag{2.4}$$

Figure 2.4 depicts the rectangular spiral path that covers a square of side $L = 7$ with a resolution of $R = 1$.

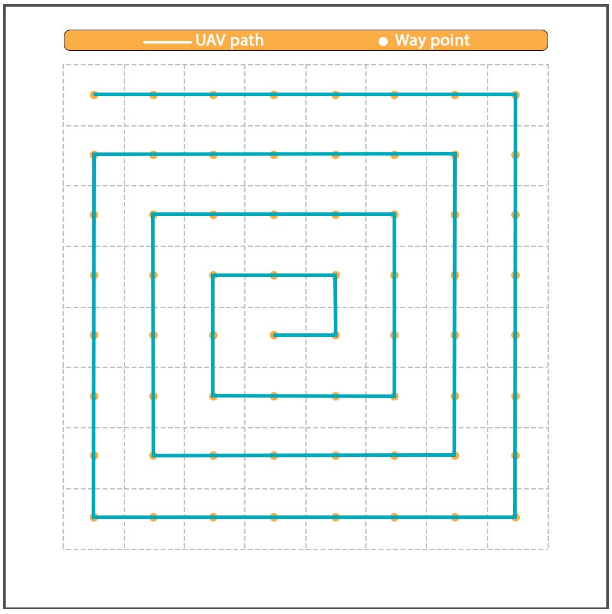


Figure 2.4 : Rectangular spiral path

2.3.3 Hilbert Search Pattern

The Hilbert pattern, also known as the Hilbert curve or the space-filling curve, is a flight pattern used by drones to conduct a systematic search of an area. This pattern involves flying along a continuous curve that passes through every point of a two-dimensional space, covering the entire target area in a single flight. The Hilbert trajectory architecture divides the AoI into square grids of 4^n where n indicates the trajectory level. This trajectory is illustrated in Figure 2.5 and traced by linearly following the centers of the square grid, as explained in [100]. A higher level of n corresponds to a longer path for the trajectory and an increased number of turns to navigate. The trajectory's length is calculated using the following equation, as expressed in [101, 102] :

$$L = \frac{D^2}{R} - R = (4^n - 1)R \tag{2.5}$$

Where the level n for a given resolution R can be determined for a given AoI $D \times D$ by :

$$n = \frac{log(\frac{D^2}{R^2})}{log(4)}$$

The distance between the centers of two square cells at a specific level, denoted as R, is called the resolution. Knowing the value of n is crucial in determining a key feature of the HILBERT trajectory, which is the number of turns N_{turns}, represented as follows :

$$N_{turns} = \begin{cases} 12(\frac{\sqrt{4^n}}{4})^2 + 2 & , \quad n \geq 3 \\ ((3\sqrt{4^n} + 2) \times \sqrt{4^{n-2}}) - 2 & , \quad n \leq 2 \end{cases} \tag{2.6}$$

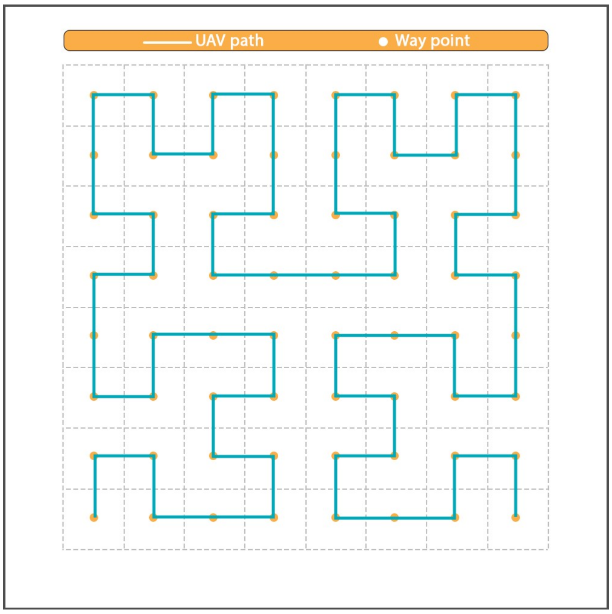


FIGURE 2.5 : Hilbert Path

2.4 UAVs Simulation Platforms

In the study of UAV motion planning, simulation is important. It allows evaluating algorithms in a safe and inexpensive manner, without worrying about dealing with real-world hardware. The ideal simulator needs to be fast, physically accurate, and photo-realistic.

2.4.1 Popular UAV Simulator Software

2.4.1.1 Aerial Informatics and Robotics simulator (AirSim)

Microsoft developed the Aerial Informatics and Robotics simulator (AirSim), a drone simulator based on Unreal Engine. AirSim is cross-platform, open-source, and supports hardware-in-the-loop with popular flight controllers like PX4 for physically and visually realistic simulations. Its purpose is to facilitate the creation and evaluation of algorithms for use in autonomous vehicles, including deep learning, computer vision, and reinforcement learning algorithms. The first simulations for this concept were confined to quadcopters. However, the AIR intends to integrate further airborne robotic models. With the help of this simulator, data for ML model training might be produced. This simulator's compatibility for protocols such as Micro Air Vehicle Link (MAVLink) allows for more realistic simulations to be created [103].

2.4.1.2 X-Plane Simulator

X-Plane is a commercially available flight simulator developed by Lamina Research. It is compatible with various platforms, including Windows, Linux macOS, and mobile platforms, including Android, iOS, and WebOS [104]. It allows users to design aircraft using additional software such as Plane Maker and Airfoil Maker, and is therefore utilized by a few aircraft manufacturers. Additionally, X-Plane may construct a network of its instances and connect with UDP or TCP networks. This simulator enables the visualization of various forces acting on UAVs, the path followed by drones, and the determination of flight failures [105].

2.4.1.3 The Aerial Vehicle Network Simulator (AVENS)

The Aerial Vehicle Network Simulator (AVENS) combines X-Plane and the OMNeT++ simulator with the LARISSA (Layered Architecture Model for Interconnection of Systems in UAS) [106]. The drones in this scenario utilize well-known communication protocols for FANETs (Flying Ad-hoc Networks). AVENS uses X-Plane for flight control and OMNeT++ for monitoring network performance metrics, including throughput and packet loss. XML files are used for communication between the simulators. Before the simulation ends, there is a constant flow of communication. Unlike other contributions, AVENS prioritizes accurately simulating key components of actual flying conditions [107].

2.4.1.4 RotorS Simulator

Eidgenössische Technische Hochschule Zürich developed an open-source MAV simulator called RotorS [108]. (ETH Zurich, i.e., Swiss Federal Institute of Technology in Zurich). It has numerous multi-copter versions designed for scientific study, including the AscTec Hummingbird, Pelican, and Firefly. It also supports adding sensors such as a camera and an inertial measurement unit (IMU) to the UAV payload.

The RotorS simulation framework was developed to reduce field-testing times and separate testing problems, make debugging easier, reduce crashes of real MAVs, and solve complicated tasks such as path planning. In addition to the model, RotorS also has a position controller and a state estimator. The different parts of a genuine MAV are simulated using the Gazebo plugins and the Gazebo physics engine.

2.4.1.5 UAVSim Simulator

The University of Toledo researchers created UAVSim, a testbed based on OMNeT++. With its simple graphical user interface (GUI), users can readily simulate UAV networks by adjusting settings like the number of hosts and attackers, the degree of mobility, and the nature of radio transmission. Some options may be adjusted to make these simulations more faithful to the actual world. Various forms of attack, UAV models, and analysis data are all handled in their sections. Users can simulate and examine the results of DoS and jamming assaults on UAVNets. The communication behavior in a UAV-Network can also be validated using this testbed [109–111]. The original simulator was enhanced to contain a GNSS simulator named GNSSim [112]. The authors integrated GNSSim and UAVSim to design and simulate GPS-related threats, like jamming and spoofing, against drones [113].

2.4.1.6 Sensing Unmanned Autonomous Aerial Vehicles (SUAAVE) Simulator

The Engineering and Physical Sciences Research Council (EPSRC) funded SUAAVE as part of the WINES wireless networking program, with participation from University of Ulster, University College London, and University of Oxford. Focusing on how to manage swarms of autonomous UAVs is the primary goal of this research. These groups of light payload quadcopters work together to gather data about their surroundings, deal with failed nodes, and relay that information to a base station. Though the setup is not limited to any situation, it can be used in search and rescue operations, the military, and emergency management [114, 115].

Following are some main ideas explored in this project, there are two processes to a conversation within a swarm of drones. Ad hoc and mesh networks are used after 802.11's feasibility has been verified. Second, a coordinated strategy is needed for control, with each UAV considering the availability of resources and the condition of its neighbors. Third, using drones equipped with sophisticated means of communication, management, and command to solve a practical search problem is a prime example of how Artificial Intelligence (AI) is being put to practical use. Fourth, to assemble and show reliable information for situational awareness, data fusion, and image processing, use various airborne sensors and cameras.

2.4.1.7 HEXAGON Simulator

This simulator comprises three primary parts : the mathematical model software, the LabVIEW-based GUI, and the rendering engine. The first two parts operate on separate workstations and interact with one another. Three LCD screens are involved here to show the flight, the virtual cockpit, and the live update of flight parameters. The graphics engine is developed in C/C++, providing a wide variety of camera angles that let you spin your virtual vehicle around as you drive.

HEXAGON is equipped with a joystick and a radio controller, as MAVs' complex agility necessitates an operator who can manage the platform (RC). A realistic and usable RC simulator interface has been enhanced to allow this functionality. In addition, the training provided by the simulator makes it possible for pilots to grasp advanced concepts related to the MP2028 autopilot system. The pilot can analyze several autopilot parameters, such as the proportional –integral-derivative (PID) gains, beforehand to improve the platform's performance in realistic scenarios [116].

2.4.1.8 Gazebo Simulator

In 2002, researchers at the University of Southern California (USC) developed Gazebo and later Open Source Robotics Foundation (OSRF) [3]. Gazebo is the default simulator that comes with ROS ; it has a large and active user base and is considered a top 3D dynamics multi-robot simulator. Gazebo facilitates the simple building of 3D worlds and the use of a variety of physics engines and sensor models, which in turn enables the testing of robot designs and algorithms, regression testing, and the training of AI systems using realistic situations.

Drones can be simulated in Gazebo with the help of Robot Operating System (ROS) framework. The framework offers a Gazebo ROS package called Hector Quadrotor[1] that

[1] http://wiki.ros.org/hectorquadrotor

tries to simulate several drone characteristics, including flight dynamics, onboard sensors, external imaging sensors, and complicated environments.

2.4.1.9 UE4SIM Simulator

2017 marks the development of the UE4Sim simulator at the King Abdullah University of Science and Technology [117]. UE4Sim was developed on Unreal Engine 4 of Epic Games. It is utilized in several areas of computer vision, including object tracking, object detection, autonomous navigation, multi-agent collaboration, etc. UE4Sim is a sophisticated physics' engine that makes it possible to construct complicated drone motions.

Human control and input and motion capture may be synced with the visually and physically generated environment thanks to the inclusion of flying joysticks and RGB-D sensors. New blueprints can be made in UE4Sim, and the engine comes with several framework classes that each have its own set of objects, obstacles, functions, etc. UE4SIM uses the Matlab Socket Interface (TCP/UDP) to transmit video frames and data between the tracker script and the UAV.

Table 2.1 compares existing drone simulators based on their implementation language, supported operating system, and whether they are commercial or free. In addition, any missing information is indicated by (N/A).

Simulator	Open Source	Implementation language	Support operating system	Free or commercial
AirSim	Yes	C++	Windows, Linux	Free
X-Plane	Yes	N/A	Windows, Linux and MacOs	N/A
AVENS	Yes	C++	Windows, Linux and MacOs	Free
RotorS	Yes	C++	Linux	Free
UAVSim	Yes	Python and C++	Windows, Linux and MacOs	Free
SUAAVE	Yes	Python	N/A	Free
HEXA-GON	Yes	C/C++	N/A	Free
Gazebo	Yes	C++	Linux and MacOs	Free
UE4SIM	Yes	C++	N/A	Free

Table 2.1 : Comparative analysis of existing drone simulators

2.5 Challenges and Future Directions

CPP for drones has seen significant advancements in recent years. However, there are still several challenges that need to be addressed to further improve the effectiveness and efficiency of CPP algorithms. In this section, we will discuss the major challenges faced in CPP for drones and suggest some future research directions.

2.5.1 Limited Battery Life

One of the major challenges in CPP for drones is limited battery life. Drones can only stay in the air for a limited amount of time, and this limits the area that can be covered in a single flight. Researchers have proposed several solutions to this problem, such as designing energy-efficient CPP algorithms, using renewable energy sources, and developing better batteries.

2.5.2 Dynamic Environments

CPP algorithms are designed to work in static environments, where the obstacles and targets are stationary. However, in real-world scenarios, the environment can be dynamic, with moving obstacles and targets. Developing CPP algorithms that can handle dynamic environments is a challenging task that requires a deep understanding of the environment and the ability to make quick decisions.

2.5.3 Scalability

Another challenge in CPP for drones is scalability. CPP algorithms should be able to handle large-scale areas, with hundreds or thousands of targets and obstacles. As the number of targets and obstacles increases, the computation time required to generate an optimal path also increases, which can make the CPP algorithm impractical.

2.5.4 Accurate simulator

One of the challenges is developing a simulator for UAVs that accurately models the complex dynamics of a real-world environment. The simulator should include a variety of environmental conditions, such as wind, rain, and snow, to test the performance of the UAVs in different scenarios accurately. Furthermore, the simulator should be capable of simulating different types of UAVs, including multi-rotor, fixed-wing, and hybrid UAVs, or testing various CPP algorithms on different platforms.

Future research directions in CPP for drones can focus on developing more efficient and scalable algorithms that can handle dynamic environments and robustly navigate drones towards their targets. Researchers can also investigate the use of machine learning and AI techniques to improve the effectiveness and efficiency of CPP algorithms. Finally, more attention can be paid to the safety and privacy issues associated with the use of drones, with the development of ethical guidelines and regulations.

2.6 Conclusion

In conclusion, CPP is a critical aspect of UAV operations that has become increasingly important due to the growing use of drones in various applications. The effectiveness of CPP algorithms employed is crucial for the success of these operations. However, designing and implementing a CPP algorithm for drones can be challenging due to the complex nature of the tasks involved.

Simulator platforms for drones provide a safe and cost-effective environment for testing and evaluating CPP algorithms. They offer the ability to simulate real-world scenarios and test various CPP algorithms in different environments. Furthermore, simulators can provide a controlled environment to evaluate the drone's performance regarding coverage efficiency, endurance, and battery life.

This chapter has provided an overview of the current state of CPP for drones, focusing on static path planning patterns. We have explored the current simulators for drones, including their objectives, strengths, and shortcomings. We have also discussed the challenges of CPP for drones and potential future directions for research in this field.

Overall, it is clear that CPP is a crucial aspect of UAV operations that requires careful consideration when designing and implementing algorithms. The use of simulator platforms provides an effective means of testing and evaluating these algorithms in a safe and controlled environment. As such, it is likely that we will see continued growth in this area as more researchers explore the potential of CPP for drones.

Chapter 3

Security of IoD

Chapter contents

3.1 Introduction

The emergence of drones has opened up exciting possibilities for various industries, offering new services and improving human lives. However, the IoD is vulnerable to several security issues, compromising the system's integrity and confidentiality. Adversaries can disrupt the radio communication of drones, intercept valuable information such as command and control signals, and even manipulate the data to take control of the drone. Moreover, attackers can exploit vulnerabilities in drone software to remotely hijack the drone or control its GPS signals for malicious purposes [45].

Given these security risks, researchers have focused on analyzing IoD vulnerabilities and developing security mechanisms to address them [118, 119]. Several security requirements and properties, such as authentication, integrity, confidentiality, and so on, must be ensured to secure the IoD network.

This chapter presents a comprehensive study of the security of IoD networks. First, it summarizes the causes of vulnerability of the IoD network, followed by a thorough risk analysis to identify the most probable attacks that could be executed on the network. Then, it details the network's security needs by emphasizing the functions and the protected data conveyed in the network. The last part presents the security solutions in the family of IoD networks. Finally, it discusses the security challenges of emerging technologies and protocols.

3.2 Vulnerability of IoD Network

The weaknesses, limitations, or flaws in a network that allow attackers to infiltrate and compromise the system are known as network vulnerabilities. Attackers can exploit these vulnerabilities to alter, delete, or block data on the network, potentially resulting in drone damage, unsafe landings, collisions with other drones or buildings, and even loss of life. Various vulnerabilities have been identified in UAV networks, including wireless connectivity issues, physical access to drones, dynamic network topology, fleet communication problems, unencrypted GPS data, limited resources, and hardware vulnerabilities. Each of these vulnerabilities presents numerous attack vectors that must be addressed to secure the network.

As the use of drones continues to increase, securing the IoD network against cyberattacks has become an important and rapidly developing area of research. Security techniques implemented should be resilient to attacks while also being lightweight regarding memory, energy consumption, communication, and computation overhead to accommodate the resource constraints of drone networks.

3.3 Attacks on the IoD Network

As the use of drones continues to grow, it becomes increasingly important to ensure their security against various types of threats and attacks. The security of IoD network is crucial as any compromise can result in the loss of valuable resources, trust, and availability [120,121]. IoD components, including devices, networks, and communication links, are all potential targets for attackers looking to exploit vulnerabilities [122]. To understand the nature of these threats, they can be classified into five main domains, as shown in Figure 3.1. By identifying and understanding these domains, appropriate security measures can be put in place to mitigate the risks and protect IoD against potential attacks.

3.3.1 Attacks on Integrity

The concept of integrity in IoD refers to the necessity of having consistent, accurate, and trustworthy data that remains unchanged during transmission and is not subject to any malicious alterations by unauthorized users or attackers [45]. If the integrity is compromised, it may affect the performance of the UAV system and result in mission failure. Therefore, it is crucial to protect and verify any communication. Common mechanisms used to protect data integrity include hash functions, checksums, and other similar methods. The following attacks can affect the integrity of IoD :

3.3.1.1 Data Alteration

Data alteration refers to manipulating information by adding false or incorrect details to change its original meaning. This practice can take different forms, including modification, fabrication, substitutions, and data injections. In the IoD context, these alterations

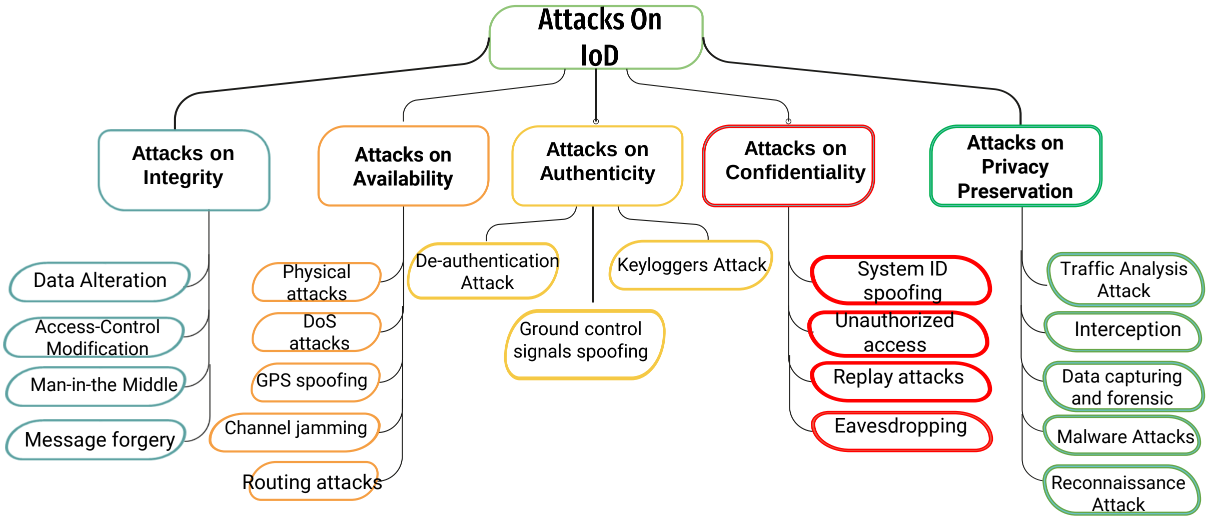


Figure 3.1 : The proposed taxonomy of attacks on the IoD.

can significantly impact the data used in communications. Misrepresenting information can confuse or deceive users by providing them with fabricated information.

3.3.1.2 Access-Control Modification

Access controls are sets of guidelines and regulations that govern the ways in which other entities within the IoD interact with one another, as well as how users gain access to information. In a sense, access control can be thought of as the brain of the IoD, instructing it on how to operate. If an unauthorized party manages to access these controls, they can modify permissions, privileges, and authorizations as they see fit, leading to potentially significant losses.

3.3.1.3 Man-in-the Middle Attacks

One of the most notorious attacks involves an adversary intercepting data transmitted between entities within the IoD [123]. This type of attack is commonly referred to as a "Man-in-the-Middle" attack, where the attacker uses a Rogue Access Point to establish a wireless access point and deceive nearby devices into connecting to it as part of IoD communications. By doing so, the attacker gains the ability to manipulate network traffic.

3.3.1.4 Message forgery

During a message forging attack on the IoD, an attacker forges a login request message from a previous session that was transmitted over a public or open channel while the authentication protocol is being executed. The attacker can then impersonate a legitimate entity and alter the message before retransmitting it to the user

3.3.2 Attacks on Availability

The term "availability" refers to the ability of services to start immediately when necessary in order to maintain proper functioning. In the context of information, availability is the assurance that authorized users can access the required information. Since the IoD operates in mission-critical fields or environments, ensuring its availability is a significant security concern [122]. Several attacks can affect the availability of IoD, including :

3.3.2.1 Physical attacks

Hardware-based attacks are carried out on the physical components of a device, with the primary goal of causing damage or destruction. Since IoD devices are costly, safeguarding them against physical attacks is a significant concern.

3.3.2.2 Denial of Service Attacks (DoS)

The most straightforward and prevalent form of attack, known as DoS, can be utilized by adversaries to disrupt the normal functioning of IoD. The act of DoS involves denying access to resources or hindering legitimate users from accessing designated resources. Communication channels are essential for transmitting data in IoD, making them vulnerable to DoS attacks [124]. Flooded requests to these channels by attackers restrict the access of shared resources to authorized users, leading to system overloading and the possible denial of some or all legitimate demands. During this attack, the network connection between the drone and the ground controller is de-authenticated due to the adversary's transmission of numerous data packets to the drone. Consequently, the computational power of the drone is weakened, leading to failure [125].

3.3.2.3 GPS spoofing

The GPS determines the IoD's location and guides the intended destination. An attacker can manipulate the received GPS signals or create counterfeit signals by using GPS signal generators [126]. The delay in GPS signals can also result in a significant loss to IoD, as it can disrupt coordination, leading to collisions. If a drone's chipboard lacks encryption, a hacker can easily track it and deceive the drone controller by transmitting false location data using a directional antenna with a narrow beam width, targeting the drone [122]. The spoofer can redirect the drone to an undesired path by sending fake coordinates at regular intervals without alerting the controller. This tactic can be used to slow down the drone's speed, making it less effective. Military drones are more difficult to spoof because of their advanced encryption mechanisms.

3.3.2.4 Channel jamming

The main aim of jamming is to deliberately interrupt IoD's communication channel [127]. It operates by utilizing a transmitter that is set to the same frequency as the target. If a jammer has sufficient power, it can disrupt frequency signals and prevent the target from configuring any signal. Low-power jammers can easily disrupt Wi-Fi and Bluetooth signals. An attacker can use a UAV to send a jamming signal from their end to the base station, matching the frequency of the signal with the deployed drone, which results in the blocking of the signals between the drone and the backup serving base station [128]. Consequently, no data or commands can reach the server, rendering the deployed drone non-responsive. After losing contact with the control station, some drones have an auto-pilot mode that gets activated. The attacker can take advantage of this mode to launch a GPS-spoofing attack and force the drone to land away from the original destination by sending fake GPS signals [129].

3.3.2.5 Routing attacks

Routing attacks aim to disrupt or redirect the routing process to compromise the network's security and privacy. These attacks are critical and can lead to severe consequences such as data loss, denial of service, or unauthorized access to the network. Examples of routing attacks include node isolation, flooding, location discloser attacks, etc [122].

3.3.3 Attacks on Authenticity

The authentication procedure is vital in establishing secure communication among various entities in IoD. It is necessary to authenticate these entities and the origins of information. This helps each node confirm the transmitted data's source, ensuring that the message is genuinely from an authentic source. Authenticating the unmanned system by the ground station is crucial in ensuring that the ground station controls an authorized drone, not a fake one. Additionally, it is essential to authenticate the ground station to prevent an unmanned system from sending its state or accepting commands from a hacked or fake ground station. Thus, both ends must be authenticated to ensure reliable data sources. Furthermore, authentication safeguards the UAV network from adversaries spoofing legitimate nodes.

3.3.3.1 Ground control signals spoofing

The drone uses wireless links to communicate with the ground station, exchange data, and control signals. However, the wireless environment is open, making it vulnerable to attackers who can easily spoof communication commands. In other words, the drone is directed to a specific location through deceptive ground control signals sent by an unauthorized third party.

3.3.3.2 De-authentication Attack

The attacker disrupts the original connection of the target genuine entity from the IoD network by sending de-authentication packets, allowing them to take over the infected entity.

3.3.3.3 Keyloggers Attack

Internal threats in IoD include using keyloggers, which can be embedded in the software during the development and deployment stages. These keyloggers capture sensitive information and send it to the attacker.

3.3.4 Attacks on Confidentiality

The confidentiality in IoD ensures that only authorized nodes can access real-time and critical data [130]. As IoD can gather a considerable amount of sensitive and personally identifiable data, such as drone owners, travel paths, geographical locations, and drone identities, it is crucial to protect the true identity of the drone. However, relevant authorities like the FAA or CAA should be able to track and identify individual drones if necessary. Malicious IoD drones can collaborate and record target positions while monitoring to obtain their actual identity [131].

3.3.4.1 System ID spoofing

Per the FAA's guidelines [132], UAVs must disclose their System ID and location to third parties like law enforcement and federal agencies when demanded. Nonetheless, due to the lack of encryption mechanisms in most UAVs, an attacker can launch an identity spoofing attack by impersonating a third party, which could compromise the communication link and result in the theft of the UAV's System ID [45]. To avoid such attacks, encrypted IDs or one-time use pseudo IDs could be an effective solution.

3.3.4.2 Unauthorized access

Unauthorized access occurs when an individual gains entry into the IoD server or services without proper authorization, either by using someone else's account or creating duplicate IDs. This type of attack poses a significant threat as it can result in the unauthorized disclosure of sensitive information from the IoD.

3.3.4.3 Replay attacks

A replay attack occurs when a third party intercepts and modifies messages sent by genuine IoD entities, and then sends them to the target entity as if the original sender sent them. Unlike the MTM attack, where the attacker can manipulate the intercepted messages, in the replay attack, the attacker always changes the intercepted message before forwarding it. To prevent this attack, authentication mechanisms in IoD networks should securely use fresh message requests to obtain data and start communications.

3.3.4.4 Eavesdropping

Passive eavesdropping is a serious threat, as it enables an attacker to secretly listen to network communications and obtain crucial information without modifying any data [133]. This information could include an encryption key sent during authentication [134] or sensitive messages transmitted between UAVs. The absence of authentication and encryption in communication channels exposes them to such attacks.

3.3.5 Attacks on Privacy Preservation

Ensuring privacy is a crucial aspect of data-centric security in IoD. The data collected and processed by IoD increases the potential for threats and vulnerabilities, making it a significant concern [135]. This data breach leads to privacy concerns and risks identity- and location-related information. Attackers target IoD to gain access to sensitive information through various means. The privacy of IoD is affected by the following attacks.

3.3.5.1 Traffic Analysis Attack

Within IoD, the traffic analysis attack is a significant risk to users' privacy. This attack is passive in nature, where the attacker intercepts and listens to the network traffic to extract valuable information for their gain [136]. The network traffic includes packets exchanged between IoD and GSS. By analyzing these packets, the attacker can extract sensitive information such as location data, sensor connectivity, and captured sensor data. Such information can be used to violate users' privacy and cause harm.

3.3.5.2 Interception

During an interception, an intruder may monitor network traffic regularly. It can be challenging to detect an intruder who is passively monitoring the network. In critical missions, IoD may contain sensitive information. As a result, tracking and monitoring IoD can pose a threat to the agencies responsible for these missions.

3.3.5.3 Data capturing and forensic

IoD can provide a wealth of data that can be gathered through traffic analysis. Although encrypted data may not disclose valuable information, data forensics can extract sensitive information from the collected data. Therefore, it is important to develop strategies that can prevent information breaches in the event that forensics-based mechanisms are utilized to attack IoD.

3.3.5.4 Malware Attacks

The insertion of spying software by intruders is considered one of the most significant threats to the security of IoD. This type of software is specifically designed to monitor the activities of targeted IoD entities and collect sensitive information, including location data and sensor data. Because this type of attack is intended to operate without alerting the user or system, it can be challenging to detect and prevent. Additionally, once the software has been inserted, it can continue to collect data over an extended period of time, posing a persistent threat to the privacy and security of IoD.

3.3.5.5 Reconnaissance Attack

The malicious party uses a combination of social engineering tactics and automated tools to gather critical information about the target IoD network. This information includes the IP addresses of the genuine entities involved in the network. Automated tools may include network scanning and port scanning tools that can identify and map out the network topology, as well as vulnerability scanning tools that can identify weaknesses that can be exploited to gain access to the network. By gathering this information, the malicious party can develop a targeted attack that exploits specific vulnerabilities in the network to gain unauthorized access and carry out their objectives.

3.4 Security Mechanisms and Solutions

Security issues may occur in the IoD due to the lack of security measures on communication channels and entities, making it vulnerable to various adversarial attacks [137]. Hence, to prevent such security threats, there is a need to establish protective measures such as real-time strategies, anti-attack mechanisms, and easily updatable security solutions. This study analyses the current state-of-the-art security solutions, including authentication techniques, blockchain-powered schemes, and software-defined networking (SDN), focusing on authentication techniques and blockchain-powered schemes.

3.4.1 Cryptographic techniques

Cryptography is a widely-used technique in both wired and wireless networks to ensure secure communication between entities, even over an insecure channel. The primary goal of cryptography is to protect the information exchanged from being interpreted by attackers. To achieve this, encryption algorithms are applied to the message content to make it incomprehensible, and decryption algorithms are used to reconstruct the original message. There are two main cryptography techniques : symmetric cryptography, which uses a secret key, and asymmetric cryptography, which uses a public key.

3.4.1.1 Symmetric cryptography

Assumes that each entity knows the only shared secret key to encrypt and decrypt messages. This identical key is previously shared securely. Symmetric encryption is generally simple, fast, and efficient, providing a malicious node cannot discover the secret key. However, before they can communicate with each other, the two nodes must agree on the key. This initial exchange is the main weak point of symmetric encryption.

3.4.1.2 Asymmetric cryptography

Asymmetric crypto-systems provide a secure key distribution and management solution that eliminates the need for a shared secret key in symmetric cryptography. Each party has a unique pair of keys ; a private key that is kept secret and a public key that is shared with others. As a result, asymmetric cryptography is more flexible and scalable than symmetric cryptography. However, a major concern with asymmetric cryptography is the larger key sizes required to achieve the same level of security as symmetric algorithms. Despite their benefits, asymmetric cryptography solutions can impose significant computational, memory, and energy overhead, particularly on resource-constrained devices.

3.4.1.3 Digital signatures

A digital signature is a digital code associated with a message so that recipient nodes can authenticate its origin and verify its integrity. It is implemented using hash functions and the signer's private key. A public key verification algorithm can verify digital signatures.

Many categories of algorithms can be used to perform digital signatures. For example, the RSA algorithm [138]is known to be robust. We can also mention the algorithms of Schnorr [139] and ElGamal [140], which are based on discrete logarithms. Although all these algorithms have different architectures, they all provide roughly the same user interface. Therefore, in this manuscript, we will apply the hypothesis of perfect encryption, according to which an encrypted text has no property other than being able to be decrypted with the corresponding key.

On the other hand, it is essential to note that using a digital signature in an IoD requires using a small signature size to maintain a reasonable communication overhead.

3.4.1.4 Message authentication

Message authentication protects the message's integrity and verifies that an attacker has not modified the information. It also allows verifying the sender's identity and the latter's non-repudiation. To perform the operation of authentication, a signature, or a Message Authentication Code (MAC) is required. These digests must be sent with the message. The MAC is generated through an algorithm that depends on both the message and a particular key that can be private or public and is known only to the sender and the receiver. The size of the message can be variable, but in most cases a MAC has a fixed size.

3.4.1.5 Hash functions

A cryptographic hash function is a fundamental technique in the field of cryptography, used for a wide range of applications. It takes an input of variable length and outputs a fixed-length string of bits, known as the hash value or message digest. This hash function is one-way, which means it is computationally infeasible to invert or reverse the process to obtain the original input from the hash value. The primary purpose of a one-way hash function is to provide data integrity by detecting any changes or modifications to the message during transmission. The hash technique is lightweight and has fast execution times, making it an attractive option for many cryptography applications. To put it simply, the one-way hash function $h : \{0,1\}^* \Rightarrow \{0,1\}^l$ takes any input $x \in \{0,1\}^*$ and produces a fixed-length (l-bits) output $h(x) \in \{0,1\}^l$. A hash function has several important properties [141–144] :

- It can be applied to data blocks of any size.
- It is easy to compute the message digest $h(x)$ for any given input x.
- The output length of the message digest $h(x)$ is fixed.
- It is computationally infeasible to derive the original input x from its message digest (one-way property).
- It is computationally infeasible to find another input with the same message digest as a given input (weak-collision resistance).
- It is computationally infeasible to find two different inputs (x, y) with the same message digest, $h(x) = h(y)$ (strong-collision resistance).

3.4.1.6 Certificate

A certificate is a digital document that verifies the identity of a user, drone, or other entity in the network. It is issued by a trusted third-party entity known as a Certificate Authority (CA) and contains the entity's public key, identifying information, and the CA's digital signature. Certificates establish trust between drones, users, and other entities in the network. When a drone or user wants to communicate with another entity, it first verifies the entity's certificate to ensure that it is valid and has been issued by a trusted CA.

Certificates are also used with encryption to ensure the confidentiality and integrity of data transmitted between drones and users. When two entities communicate, they use each other's public key to encrypt and decrypt the data. This process ensures that only the intended recipient can access the data and that the data has not been tampered with during transmission.

In IoD, certificates are critical for establishing trust and ensuring secure communication. As the number of drones and users in the network continues to grow, the management of certificates becomes increasingly complex. Therefore, it is essential to have a robust certificate management system to ensure that certificates are issued, renewed, and revoked in a timely and secure manner.

3.4.1.7 Public Key Infrastructure

PKI is a system of techniques providing a streamlined approach to managing keys and certificates. This infrastructure is responsible for overseeing the creation of keys and certificates, safeguarding private keys, managing situations where a node's private Key is compromised, storing and recovering keys, updating keys and certificates, managing key histories, and controlling access to certificates.

3.4.2 Node authentication

To ensure the authenticity of data collected from various drone applications, proper security measures must be in place to prevent any corrupted node from compromising the entire IoD. This means that authenticated entities should only be granted access [145]. Two methods can be utilized to verify the identity of nodes in the IoD network. Firstly, the Key agreement protocol can be implemented to authenticate all communication entities before exchanging sensitive data. This protocol generates shared session keys between drones and users to encrypt transmitted information. One example of such a protocol is the Diffie-Hellman (DH) model [146]. Secondly, biometric-based authentication methods such as face [147], fingerprint [148], and iris recognition [149] can be employed in the context of the IoD. This can enhance the security of drone operations and restrict access to authorized personnel only, preventing unauthorized access and ensuring that only registered and legitimate users can access the drone's data.

3.4.3 Blockchain-based solutions

Blockchain is a groundbreaking technology that has disrupted the world of cryptocurrency. A distributed database stores transactions between nodes in a peer-to-peer network [150]. Transactions are grouped into blocks and validated through a consensus algorithm in a distributed manner. These blocks are then chained together to form a blockchain, as illustrated in Figure 3.2. Each block contains validated transactions, block timestamp, nonce value, a hash of the block, and the previous block's hash.

Miners execute the consensus process, nodes in the network. Consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are commonly used to ensure that miners agree on adding new blocks to the blockchain [150].

Two types of blockchain exist : public (permissionless) and private (permissioned) [150]. Any node can join the network in a public blockchain, whereas a private blockchain includes only specified nodes. The selection of blockchain type and consensus algorithm

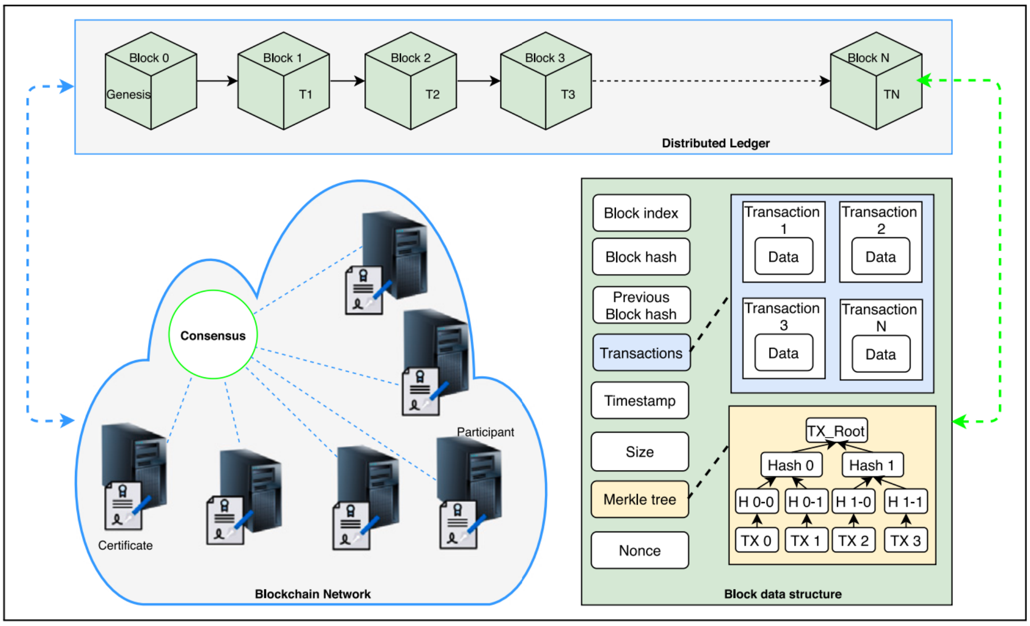


FIGURE 3.2 : Structure of the blockchain. [2]

depends on the nature and requirements of the IoD application.

Blockchain technology has several advantages, such as decentralization, immutability, and transparency, which make it suitable for various IoD applications, such as authentication [151–154], access control [155], and trust management [156, 157].

3.4.4 Software defined networking-based solutions

Software-Defined Networking, or SDN, refers to a networking approach that involves separating a computer network's data plane or forwarding plane and the application layer from the control plane. The main objective of SDN is to create agile and flexible networks. This is achieved by virtualizing the network by separating the control plane, which handles network management, and the data plane, where traffic flows. By decoupling network control from packet forwarding, SDN enables independent network control without affecting traffic flow, keeping network services and traffic abstracted from the network control. These SDN features can play a vital role in enhancing the security of drone communications [128].

3.5 Analysis of IoD Authentication Schemes

Authentication plays a crucial role in maintaining the security of the IoD, and it has been extensively addressed in recent years [158–162]. This section presents a comprehensive survey of the most prominent authentication schemes for IoD proposed in the literature. We have divided these schemes into three main categories : 1) user authentication, 2) mutual authentication between two entities, and 3) drone authentication. To facilitate the understanding of these schemes, we have created a taxonomy of the authentication protocols, which is illustrated in Figure 3.3. We also provide a comparison of various lightweight authentication techniques in Table 3.1.

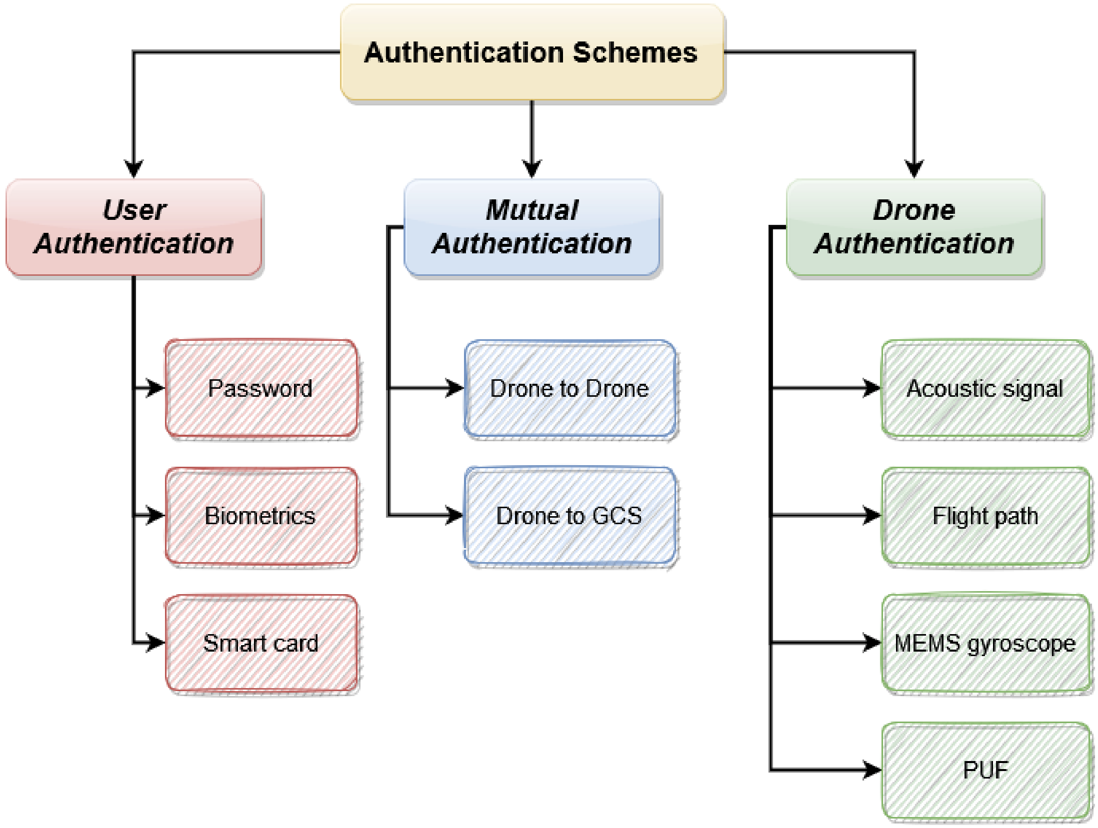


FIGURE 3.3 : A taxonomy of the authentication schemes.

3.5.1 User authentication

Most of the applications in the IoD environment are based on real-time information. As a result, it's understandable that users (third parties) are interested in getting real-time sensing data from drones flying in specific areas. A remote user at a different location may need to connect with drones in an IoD. Only an authenticated user has the ability to do so. Passwords, smart cards, and personal biometrics are all used to authenticate users. Secret keys can be shared between the drone and the user for future conversations after the user has been validated. Several studies have been conducted in the domains of IoT and Wireless Sensors networks (WSNs), but only a few have been conducted in the specific domain of IoD. To confirm the identity of the remote user requesting services from the drone network, two-factor schemes employ two user credentials, whereas three-factor schemes use three user credentials. After successfully completing the key agreement procedure with the Ground Center Station (GCS), the user must register with the GCS before initiating data transfer.

In an IoD environment, the works in [163] and [164] are based on three-factor user authentication. The key agreement protocol, described in [163], has seven phases, including secure communication and key establishment between two communicating drones. The method is resistant to man-in-the-middle attacks, replay attacks, secret leakage attacks, drone capture attacks, and password update attacks since it employs cryptographic hash functions and a biometric fuzzy extractor. It employs the Dolev-Yao (DY) threat model, and security is validated using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. In [164], the authors proposed a lightweight three-factor user authentication protocol based on a cryptographic hash function, fuzzy extractor, and bit-wise XOR operation. The drone-to-drone key management described in [163] is not taken into account here. The communication cost is 1536 bits, the computing cost is 0.026 seconds, and there is no consideration for storage overhead. For confirming the security of the session keys, the Real-or-Random (ROR) model is used for security analysis. A formal security check was also performed using the AVISPA tool.

3.5.2 Mutual Authentication Between Two Entities

One of the most essential security services utilised in the IoD environment is mutual authentication which is a process in which the participants in a network check each other's identities and authenticate each other in order to transfer secret keys and establish a secure communication channel. It might be a battle between drone and GCS, or between drone and drone. The majority of the applications in the IoD environment are based on real-time information. As a result, it's understandable that users (third parties) are interested in getting real-time sensing data from drones flying in specific areas. This is achievable if users are allowed to obtain real-time data from flying drones within the IoD environment directly rather than through the server.

Authors in [165] describe a mutual authentication scheme between the drone and the end device, in which both entities may mutually authenticate their identities via signatures. A group of drones, a set of end devices, and a remote management centre (RMC) that manages and generates private keys for the end devices and drones based on their identities make up the system. A member of the end device group must authenticate their identity with the drone and get the drone's broadcast key in order to communicate with other end devices. To produce the master key, the RMC runs system setup, and all network entities must first register with the RMC in order to generate their private keys. The identification of the end device and the drone are used to register the drone via signcryption. If the end devices wish to connect to the network, drones are responsible for authenticating them. Denial-of-service attacks are not really a problem for this system. For analysing the protocol's security, game strategy is employed. A pseudonym or a temporary identity is used to mask the devices.

A certificateless mutual authentication scheme between a smart object and a drone is proposed by the authors in [166]. The first case involves communication between a smart object and a drone ; the second case involves a drone sharing data with a large number of smart objects ; and the third case involves several smart objects communicating their data to a drone. They propose three protocols for this : a Certificate-Less Signcryption Tag Key Encapsulation Mechanism (eCLSC-TKEM) for one-to-one communication, a Certificate-Less Multi-Recipient Encryption(CL-MRES) Scheme for one-to-many communication, and a Certificate-Less Data Aggregation (CLDA) protocol for many-to-one communication. The first scheme makes use of a partial private key that expires after a specific time period, whereas CLDA employs ElGamal homomorphic encryption with an efficient batch verification technique, CL-MRES is a hybrid scheme. However, the computational cost of this approach is high.

For mutual authentication between network connected UAVs and the GCS, Chen et al. [167] employ asymmetric bi-linear pairing. In a cellular-connected UAV scenario, authenticating the trusted platform module (TPM) via platform identity authentication is expensive, and no security analysis is performed. Authors in [166] discusse a certificateless group authenticated key agreement scheme for secure UAV-UAV communication. The scheme is divided into two stages : initialization and group key agreement. The server generates the user's partial private key and public key during the initialization step. This scheme is only feasible for static groups ; a dynamic addition of UAVs is not taken into account. The protocol's security is tested using the Scyther tool. Mutual key agreement, key escrow elimination, joint key control, key freshness, known key security, entity revocation, conditional privacy, non-repudiation, entity revocation, and known key security are just a several of the benefits of this method.

A system for mutual authentication based on elliptic curve cryptography (ECC) is proposed in [168] and consists of a trusted authority, UAV manufacturer, the GCS, and drone operator. In this paper, mutual authentication between a drone operator or player and the UAV manufacturer is considered, followed by mutual authentication between the operator and the GCS, mutual authentication between the drone operator and the UAV, and finally mutual authentication between the GCS and the UAV. The system is resistant to spoofing and denial of service (DoS) assaults. Burrows–Abadi–Needham (BAN) logic is used to prove security. However, this method comes with a considerable expense in terms of computation and communication.

3.5.3 Drone Authentication

Because malicious drones can be deployed by an attacker, a deployed drone may not necessarily be a legitimate drone, and it is difficult to identify malicious new drone from existing legitimate drone in the network. [169] discusses a drone authentication and tracking scheme based on radio-frequency identification (RFID)-based signcryption. The system is made up of six components : the base station (BS), the BS controller, the civilian cloud, the database, the identity server, and the routers. Each drone has an RFID tag that allows it to connect to a network. Every drone in the network has an RFID tag, which is read by the BS's RFID reader. The drone must be in close proximity to or within range of the BS. When a drone enters the range of a BS, the drone's RFID is read by the BS and relayed to the BS controller, who then requests a temporary identification from the cloud that expires after a certain period of time. The drone identities are used to produce private keys, which are then used to generate signatures. The algorithms for drone to drone and drone to multi-drone communication are discussed. There are no security proofs or performance analysis provided. Mutual authentication and communication between drones are not taken into account, therefore the scheme's efficiency is not evaluated using this method.

The specific properties of the gyroscope sensor on drones are used to fingerprint them in [170]. Micro-electro mechanical systems (MEMS) gyroscopes are used to measure the drones' orientation and rotation, and each sensor's output is different from the outputs of other sensors given identical inputs. This disparity arises as a result of differences in production techniques. As a result, this trait may be utilised as a unique identity or fingerprint for a legitimate drone. However, as the number of drones in a system grows, the findings become more limited and are better suited to small networks. In [171], variances in the drones' noise characteristics (due to manufacturing defects in the drone motors) are utilised to identify and authenticate the drone. The goal of this acoustic drone fingerprinting is to prevent drone impersonation attacks. It is a two-factor authentication scheme, with the first factor being a digital signature and the second being an acoustic fingerprint. Support Vector Machines (SVM) classifier using radial basis function as the kernel is used to extract and train the electromagnetic and mechanical noise properties of the valid drone motors. The motors' acoustic signals are recorded using a microphone and then preprocessed to eliminate noise and normalise the data. The characteristics are extracted and trained before being utilised as an authentication database. By capturing and analysing the drone's motor sound, it may be utilised to predict its authenticity.

Another study [172] employs machine learning algorithms such as K-Nearest Neighbor (KNN), SVM, and Logistic Regression (LR) to predict and validate the drone flight path using flight traces. The flight path of a drone is used to authenticate it. It's a drone hijack if authentication fails. The algorithms are trained with both actual and fake data and may be used to predict whether or not new drone tracks are legitimate. The Euclidean distance function is utilised in the KNN model to discover the incorrect data. The Ardu-Pilot simulator is used for simulations. SVM identifies changes in the original data, while LR looks for a relationship between the features. The experiments show that the KNN classifier is the best for validating the flight path, although the process is time consuming.

Authors in [173] proposes a real-time behavior-based UAV identification scheme. They discuss a UAV identification technique that predicts the real-time UAV path and identifies illegal users attempting to modify the flight path. To investigate the behaviour of the drones, real-time data from the drones is collected, mostly location and sensor data, and a model is constructed that can predict the drone's trajectory in the future and validate the flight path, therefore authenticating the UAV. Longitude, latitude, and speed, as well as drone attributes like weight and maximum speed, are all taken into account in real-time sensor data. The authentication is known as Gaussian-Processes based authentication, and these data are learned using a Kalman filter online Bayesian learning approach (GPA). A server processes the data, which is then saved in a database management system. A serial number and a QR code are used to identify UAVs, the operator must also enter their identity credentials, after which the server will issue a licence. This research, however, is limited to a single UAV system. Physical Unclonable Functions (PUFs) and Trusted Platform Modules (TPMs) might be used on drones in the future to generate device specific keys and authenticate device hardware.

TABLE 3.1 : Summary of existing authentication schemes in IoD environment.

Scheme	**Year**	**Short Description**	**Authentication Category**	**Security Analysis**	**Tools Used**	**Drawbacks and limitations**
[165]	2017	Mutual authentication scheme between UAVs and end devices using an identity-based signcryption.	Mutual authentication	Game strategy	NS3	More computations needed.
[167]	2018	Authors employ asymmetric bi-linear pairing for mutual authentication of UAVs and GCS over a network. In a UAV with cellular connectivity, the trusted platform module (TPM) must be authenticated utilizing platform identity authentication.	Mutual authentication	No security analysis	TPM emulator	Incurs high cost and no security analysis is performed. Computationally expensive.
[166]	2018	This study investigates certificateless-group authenticated key agreement (CL-GAKA) as a means of securing inter-UAV communication. The protocol comprises two main phases : the setup phase and the group key agreement phase. In the setup phase, the user's partial private key and public key are generated by the server.	Mutual authentication	Scyther tool	Raspberry Pi 3 Model B+	Only for static groups, and dynamic addition of UAVs is not considered
[163]	2018	The research relies on three-factor user authentication in IoD environment. In this work there are seven steps in the key agreement protocol which also includes the secure communication and key establishment between two communicating drones. It uses cryptographic hash functions and biometric fuzzy extractor.	User Authentication	Automated Validation of Internet Security Protocols and Applications (AVISPA)	NS-2 with 50 drones	Throughput is less and slightly higher packet loss rate.

Table 3.1 – continued from previous page

Scheme	Year	Short Description	Authentication Category	Security Analysis	Tools Used	Drawbacks and limitations
[169]	2018	To ensure the authentication procedure and privacy, this research presented a new architecture based on ID-based Signcryption. The UAV carries an RFID tag for identifying purposes. To protect confidentiality throughout the permission procedure, a temporary UAV ID is issued, and both IDs are used to create the cryptographic keys.	Drone Authentication	No security analysis	RFID (Simulation with 100 drones)	Mutual authentication and communication between the drones are not considered. Efficiency of the scheme is not evaluated in this method.
[170]	2018	In this study, the unique qualities of the drone's gyroscope sensor are utilized to create a unique fingerprint for each drone. Micro-electro mechanical systems (MEMS) gyroscopes are used for measuring the orientation and rotation of the drones, and the output of each sensor is distinct from the outputs of other sensors for identical inputs. This difference occurs due to the variations in the manufacturing processes. Hence, this feature can be used as an identifier or a fingerprint of an authentic drone.	Drone Authentication	No security analysis	MEMS gyroscope	Suitable for small networks.

Table 3.1 – continued from previous page

Scheme	**Year**	**Short Description**	**Authentication Category**	**Security Analysis**	**Tools Used**	**Drawbacks and limitations**
[174]	2019	A blockchain-based approach for the mutually-healing distribution of group keys. First, the GCS made a private blockchain (BC) database to store all the group keys that were given out and to keep track of when UAVs joined and left the network. At the same time, the blockchain is used to keep track of a continually updating database of UAANET membership verification documents. With the help of its neighbors, a node can recover its lost group keys via a basic mutual-healing protocol or an improved one based on the Longest-Lost-Chain mechanism, depending on the attack model it is subjected to.	Mutual authentication	ProVerif	OPNETModeler 14.5, BC : Hyperledger Fabric 2.0 -open-source BC development platform	Not effective for a large drone network. More computation.
[164]	2019	TCALAS is a lightweight three-factor user authentication protocol using a combination of cryptographic hash function, fuzzy extractor method, and bit-wise XOR operation.	User Authentication	Real or random (ROR) model and AVISPA	Simulation study not done	Slightly higher computation cost. The drone to drone key management is not considered here.

Table 3.1 – continued from previous page

Scheme	Year	Short Description	Authentication Category	Security Analysis	Tools Used	Drawbacks and limitations
[171]	2019	Differences between the drones' noise characteristics (due to manufacturing defects of the drone motors) are used for identifying the drone and authenticating it. Acoustic drone fingerprinting is an attempt to counter drone imitation attacks. It is a two-factor authentication technique in which the first component of authentication is a digital signature, and the second factor is an acoustic fingerprint. The legitimate drone motors' electromagnetic and mechanical noise characteristics are extracted and trained with the help of a Support Vector Machines (SVM) classifier that uses radial basis function as the kernel.	Drone Authentication	No security analysis	Arduino UNO, Blue Yeti Pro microphone	Not suitable for large number of drones, and manufacturing defects in propellers are not considered
[172]	2019	This work uses K-Nearest Neighbor (KNN), SVM, and Logistic Regression (LR) machine learning methods to predict and validate the drone flight path from the flight traces. The models are trained using both real and false data and can be used for predicting the new drone paths as authentic or not. In KNN model, Euclidean distance function is used for finding the wrong data. SVM detects the changes from the original data, whereas LR finds a relation between the features.	Drone Authentication	No security analysis	ArduPilot	More computations.

Table 3.1 – continued from previous page

Scheme	**Year**	**Short Description**	**Authentication Category**	**Security Analysis**	**Tools Used**	**Drawbacks and limitations**
[168]	2020	The authors propose an ECC based method for mutual authentication consisting of a trusted authority, UAV manufacturer, drone operator, and the GCS.This study examines mutual authentication in four different contexts : first, between a drone operator and the UAV manufacturer ; second, between the operator and the GCS ; third, between the drone operator and the UAV ; and fourth, between the ground station and the UAV.	Mutual authentication	Burrows Abadi Needham (BAN) logic proof	Simulation study not done	High computational and communication costs.
[175]	2021	The authors used blockchain technology to create an authentication and key management system (AKMS-AgriIoT). Data is gathered from Internet of Things (IoT) intelligent devices in a specific area by drones, which are then safely transmitted to the GSS. The GSS generates encrypted transactions and signatures, which are then used by the cloud server to build blocks. After the consensus process verifies the blocks, they are added to the blockchain.	Mutual authentication	ROM, BAN logic proof and Avispa	Raspberry PI 3 B+	Problems with managing certificates arise when the number of concurrent users exceeds the limit. Very expensive computation and communication.
[176]	2022	The RUAM-IoD protocol utilizes AES-CBC-256 encryption, ECC, a hash function (SHA-256), and the XOR operation to create an AKA scheme that can establish encrypted connections between drones and external users. According to the authors, their protocol is resilient to multiple security threats, such as biometric and password changes, stolen smart devices, MTM attacks, drone capture, and replay attacks.	User authentication	Scyther tool and ROM	Raspberry Pi (RP-3)	The costs related to communication and computing are relatively high. The use of blockchain technology is incompatible.

3.6 IoD Authentication Challenges and Open Issues

3.6.1 Reliable and comprehensive security analysis

Conduct sound and thorough security analyses for authentication schemes proposed in the literature. While many schemes offer heuristic security analysis and assert security under security analysis models like Burrows-Abadi-Needham (BAN) logic, they are still vulnerable to known attacks. To address this, it would be necessary to utilize automated formal security verification software tools to examine security against various attacks.

3.6.2 Evaluation in a real-world application setting

Conducting evaluations of authentication schemes in a real-world application setting : While many existing authentication schemes have been evaluated using simulators, these evaluations may not accurately reflect the system's actual performance in real-world scenarios. To achieve satisfactory outcomes in terms of security and authentication performance, there is a need for testing and assessing authentication protocols in real-world environments, which will provide researchers with a more realistic view and allow them to modify or fine-tune their work accordingly.

3.6.3 Expanding the size of blockchains

The scalability of a blockchain is an essential factor that determines its throughput (i.e., the rate at which transactions are processed) and the size of the system (i.e., the number of peers in the blockchain network). As the scale of the blockchain increases with the IoD and the amount of data continues to grow, the storage and computational load of the blockchain will become increasingly burdensome. This will result in longer synchronization times, making it difficult for the blockchain to operate efficiently in the IoD.

3.6.4 Privacy-related Regulation Issues

The deployment of drones in the IoD introduces new privacy concerns for individuals and organizations. Drones can capture data from people and objects within their view range, leading to privacy breaches when used for monitoring purposes [177]. Furthermore, drones used in search scenarios may collect large amounts of personal data without individuals having the opportunity to provide consent [178], thus weakening privacy control policies. As a result, it is crucial for authorities to be aware of these privacy issues and to develop regulations and policies that align with the development of IoD technologies.

3.6.5 Balances between Security and Lightweight Features

The IoD involves collaborative data collection by many drones, which generates massive amounts of unstructured data to be processed by big data clustering and mining techniques in real time [179]. However, the security of sensitive data in the IoD is at risk without proper security measures, such as authentication and blockchain-powered schemes. This can be costly due to the substantial computational and communication overheads they create. Smart drones with limited computing capacity pose challenges such as weak cryptography and data insecurity [145]. Achieving high levels of security would require increased design complexity and more computational load and power consumption, making it difficult to balance between robust security measures and maintaining lightweight features in the IoD system. [180].

3.7 Conclusion

IoD is an emerging technology that connects drones and analyses data from various sources to create real-life applications. However, attacks on IoD can have serious implications for the operational use of networked drones. Security threats and vulnerabilities can compromise IoD's confidentiality, integrity, authenticity, and availability. Cryptographic mechanisms are used to ensure message security and control signal protection. However, security issues, such as unauthorized access, malicious control, illegal connections, and other attacks, require strategic solutions without affecting performance. Identifying and mitigating threats in IoD presents various research challenges that require secure and efficient approaches.

This chapter provides an overview of the security context in IoD, with a specific focus on the authentication aspect. It highlights the security mechanisms, challenges, and issues that need to be addressed for secure IoD operations. Through an extensive review of the literature, it identifies the key research works in this area and the existing gaps that need to be filled. The review revealed several open issues that require further attention and investigation.

The next chapter presents the first contribution of the thesis, which is a new static path planning strategy for drones.

Part II

Novel Approaches to UAV Path Planning and Security in IoD Networks

Chapter 4

An Efficient Static CPP Strategy for Drones

Chapter contents

4.1 Introduction

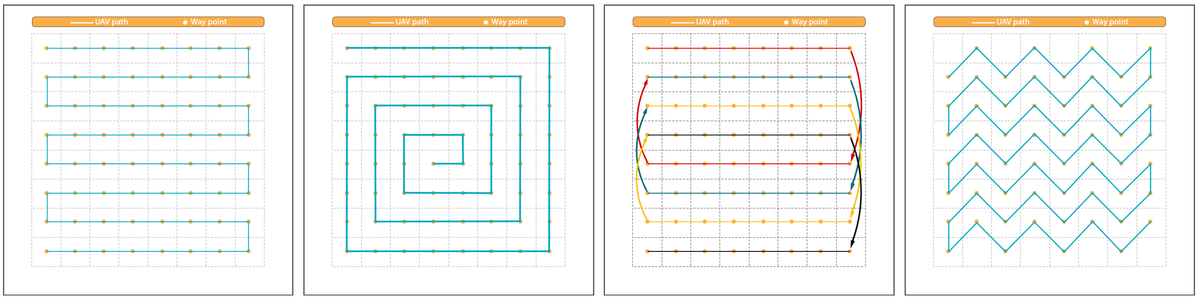
The use of drones in civil applications has recently gained popularity and has been employed in various sectors such as surveillance [181], disaster management [182,183], search and rescue (SAR) operations [184], shooting missions [185], smart agriculture [186, 187], data collection [188], and many more, as evidenced by previous studies. Among these applications, reconnaissance missions are considered essential drone operations where drones search for a target in an open area. There are two methods for exploring with drones : random mobility and path planning [189]. The random mobility method does not follow pre-planned paths, allowing drones to react to unexpected events such as equipment failure and to approach targets unpredictably. The path planning method, on the other hand, involves each drone following a predetermined path to cover its designated region.

In this chapter, we introduce a novel UAV path planning to monitor an area. This method is designed to decrease energy consumption and minimize the number of turns while ensuring that the entire area is given equal importance. To evaluate the effectiveness of this approach, we compared it with four static paths, namely back and forth, spiral, LMAT, and Zamboni (Figure 4.1). Our results indicate that the proposed path provides better coverage and consumes less energy than the existing state-of-the-art methods.

4.2 Related work

CPP for drones has recently become a popular research topic. Many drones now use CPP-based methods for their reconnaissance missions, relying on simple geometric flight models. [98].

In the literature, there has been considerable discussion on the topic of CPP using UAVs. A recent comprehensive survey of CPP algorithms and their performance was



(a) Back and Forth **(b)** Spiral path **(c)** Zamboni path **(d)** LMAT path

Figure 4.1 : Basic coverage path planning paths

conducted by Cabreira et al. [1]. The survey included various approaches such as back-and-forth movement, spiral, barrier patrol, sector scan, energy-aware spiral, gradient-based, Hilbert curves, harmony search, and wavefront algorithm. The authors categorized the current methods based on the adopted cellular decomposition technique, using Choset's [97] classic taxonomy. Geometric patterns for path planning were summarized in [190], including spiral or spiral-like, Dubins path, Lawnmower model, Zamboni, and a modified Lawnmower/Zamboni path planning strategy that considers different mission features.

The back-and-forth (BF) model, also known as the lawnmower model, is commonly used for missions in rectangular environments. Several studies have presented and analyzed different flight patterns for this model. For instance, Andersen et al. [98] evaluated five flight patterns, including two versions of back-and-forth, sector search, spiral, and barrier patrol, based on the US National Search and Rescue Manual. Valente et al. [191] and Nam et al. [192] employed a grid-based technique to divide the environment into square cells and assign occupancy information to each corresponding region. The cells are explored using a single drone that moves back and forth, as reported in [193] and [98]. In [194], a grid-based approach with approximate cellular decomposition was used to cover an obstacle-free area of interest with a single UAV in an offline mode. On the other hand, some studies such as [190, 195, 196] employed multiple UAVs with BF movements to cover the area in an offline mode with minimal turns. To cover an area in offline mode with shorter distances and less time to complete the mission, the authors of [197] presented a path planning algorithm known as Spiral Path Planning (SPP), based on spiral decomposition, which employs a single drone. Artemenko et al. [198] found that turning a drone consumes a significant amount of time and energy because the drone must decelerate, rotate, and accelerate each time it performs a turn. Thus, using the principle of Bézier curves, the algorithms smooth maneuvers along a given path to adjust conventional trajectories such as BF, LMAT (Localization algorithm with a Mobile Anchor node based on Trilateration), and HILBERT. A solution for CPP with energy optimization for a single multi-rotor was proposed by Di Franco et al. [199]. They formulated energy models based on real measurements to estimate the energy consumption of the UAV under different conditions. However, their formulation only considered distance and did not take turns into account. On the other hand, Torres et al. [200] proposed a CPP strategy for 3D terrain reconstruction using a single UAV. They divided the region into one or more polygons and used a raster scan to cover each polygon. They calculated the ideal line sweep direction in order to reduce the number of rotations.

4.3 The suggested CPP approach

In this chapter, we adopt the same assumptions as those used in the related work, including the use of a single drone for each path, an offline mode, and an area without obstacles or non-flying zones. Our analysis of state-of-the-art methods shows that UAVs spend a considerable amount of time making turns, which results in a significant waste of energy due to the three-step process involved in making a turn : deceleration, rotation, and acceleration.

To address these challenges, We suggest a new strategy with a unique flight path planning method that could potentially cover the desired area in the shortest path possible. Additionally, it aims to decrease computational time, minimize the number of turns, and reduce energy consumption.

4.3.1 Decomposition of the area

Once the geographical specifications of the coverage area are obtained, they are transformed into a regular shape (square), such as a square. Then, an approximate cellular decomposition technique is used to divide the area of interest into smaller segments. This technique involves dividing the operational area into uniformly sized cells. $C = \{c_1, c_2 ... c_n\}$in such a way,

$$E = \bigcup_{c \in C} c \tag{4.1}$$

It is important to note that the number of cells on each side must be an odd number, such as $3 \times 3, 5 \times 5, 7 \times 7$, and so on. One of the main advantages of using a grid-based decomposition technique is that it allows for the transformation of the area of interest into a unit distance graph called a grid graph, denoted as $G_{(V,E)}$ (depicted in Figure 4.2). The vertices, denoted by V, correspond to the center of each cell, and the edges, denoted by E, represent the path connecting two adjacent cells. The proposed path is designed to traverse through the center of each cell, represented by waypoints.

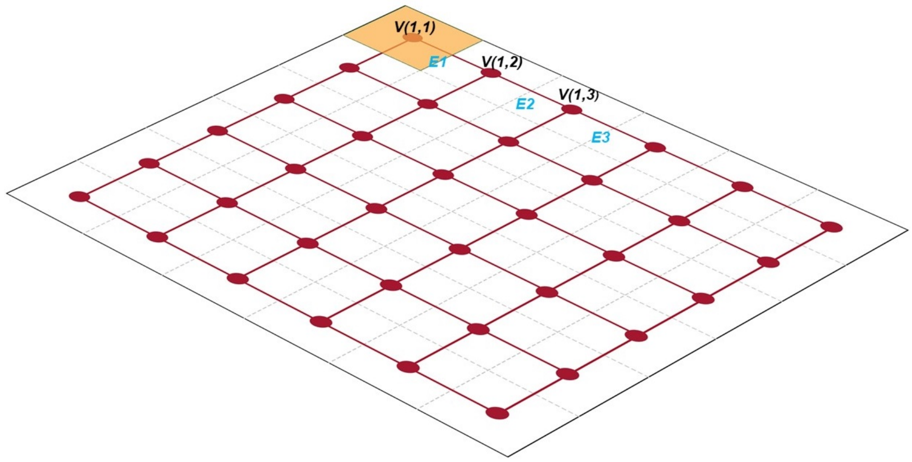


FIGURE 4.2 : Projected Area to Grid

4.3.2 Navigation strategy

As previously stated, the coverage area is divided into sub-squares of size $(n \times n)$, where $(n \mod 2 = 1)$, and a single drone is used to cover the entire workspace. The planning phase is done offline, and the proposed path is loaded onto the drone as a waypoint list. The path follows a zigzag pattern, with the drone moving diagonally across the deployment area. The drone follows the waypoints to determine the direction it needs to move in the environment. Because the area is modeled as a square, the drone can start at the nearest corner to the main station and move horizontally at a distance of 2α (where $\alpha = c_i$) towards $(V_{1,3})$. Once it reaches vertex $(V_{1,3})$, it turns 135° clockwise and continues to move to the next cell until it reaches the side boundary of the area. When the drone reaches vertex $(V_{3,1})$, it turns 45° counterclockwise and moves 2α towards vertex $(V_{1,5})$. Then it turns 135° again and moves back to the starting point. When the drone reaches the top boundary of the area, it executes a return action in the same way as in the previous phases. The resolution of the proposed trajectory is determined by the distance between two diagonal lines and denoted as $s = \alpha\sqrt{2}$. The movement of the drone is illustrated in Figure 4.3

The primary stages of the suggested mobility strategy are outlined in the diagram depicted in Figure 4.4.

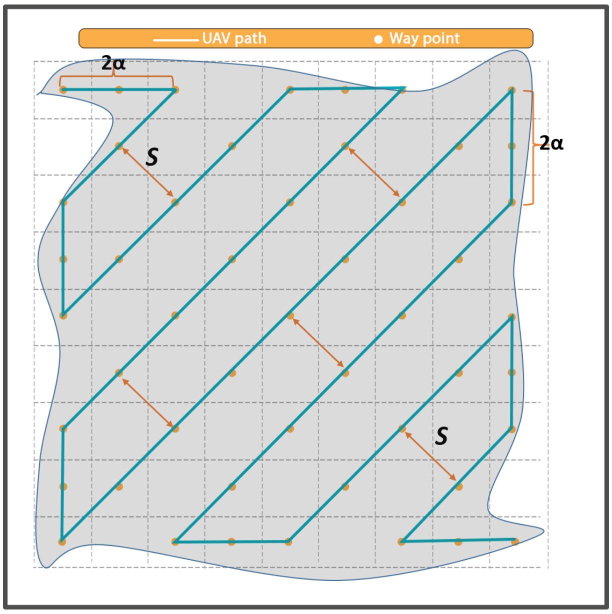


FIGURE 4.3 : The proposed path

4.4 Evaluation Metrics

To evaluate the effectiveness of the proposed method, it is necessary to measure its performance using established metrics. The proposed path was compared against existing methods using four metrics : mission time, path length, number of turns, and energy consumption.

4.4.1 Time required for the mission

In order to assess the effectiveness of a UAV in a mission, it is essential to optimize the trajectory duration and the time taken to complete the mission. These metrics are crucial for evaluating the performance of UAVs. [198, 201, 202].

The equation from [192] was utilized to compute the completion time represented by T, which takes into account the path length denoted by S, the speed of UAV movement represented by V, and the number of turns represented by k along with the angle of each turn represented by ϑ and the UAV rotation rate represented by ρ.

$$T = \frac{S}{V} + \sum_{i=1}^{k} \frac{\vartheta}{\rho} \tag{4.2}$$

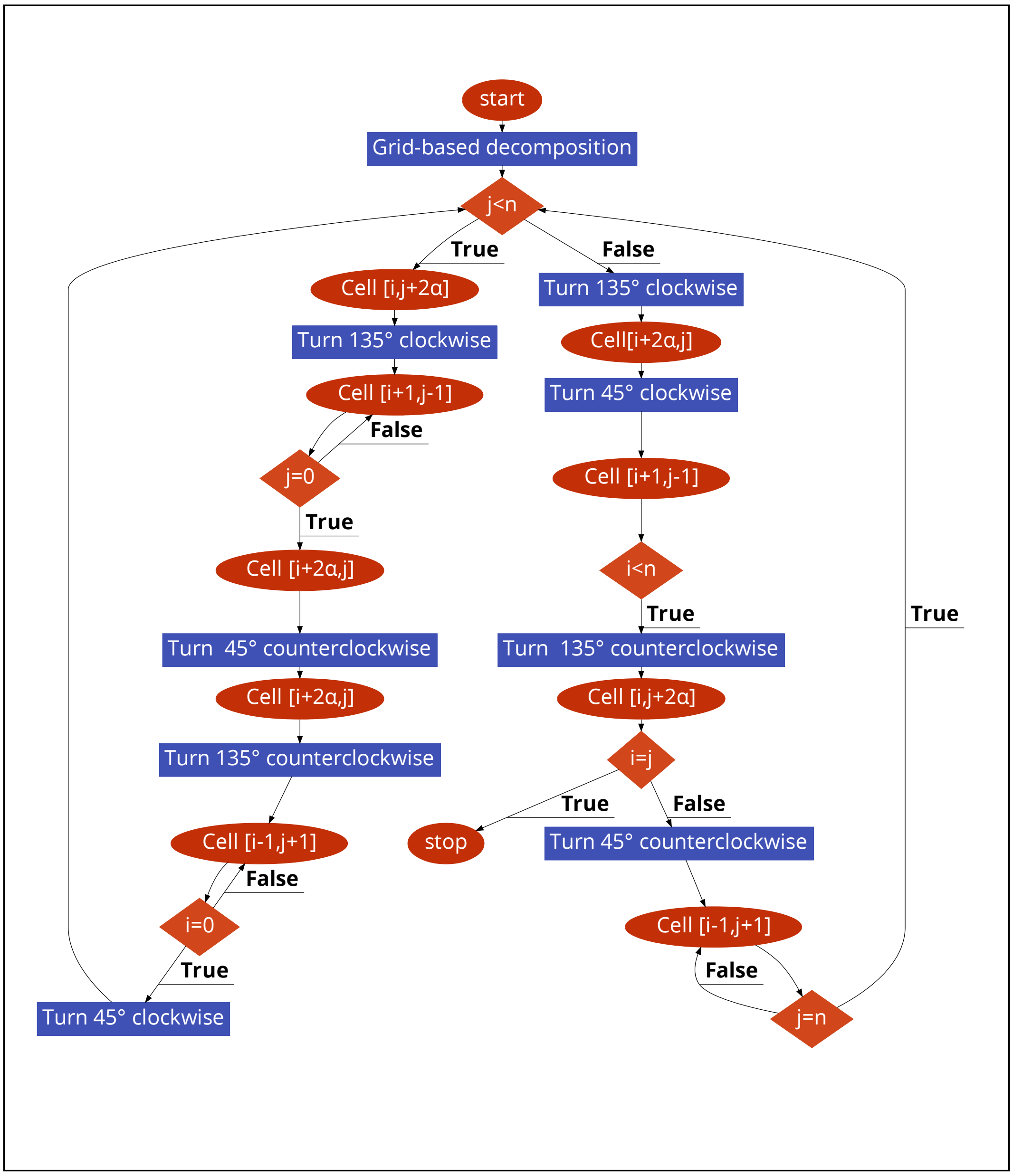


Figure 4.4 : Flowchart of the proposed Path

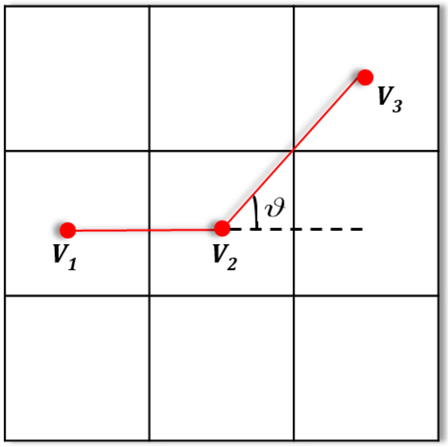


FIGURE 4.5 : The external angle for three vertices of the trajectory

4.4.2 Turning Angle

The power consumption is significantly affected by the turn rate. One crucial factor to consider is the number of turns needed to complete the mission. Returning to Figure 4.5, the external angle between vertices V_1, V_2, and V_3 at point V_2 is the turn angle. It can be calculated from the internal angle $\widehat{V_2V_1V_3}$ as follows :

$$\vartheta = \pi - \cos^{-1}(\widehat{V_2V_1V_3}) \tag{4.3}$$

The calculation of $\cos^{-1}$ involves the application of the law of cosines within the triangle $V_2V_1V_3$.

$$\vartheta = \pi - \cos^{-1}\left[\frac{(d(V_2,V_1)^2 + (d(V_1,V_3)^2 - (d(V_3,V_2)^2)}{2d(V_2,V_1)d(V_1,V_3)}\right] \tag{4.4}$$

4.4.3 Consumption of Energy

To assess the proposed path, an energy model was employed, expressed as the sum of energy consumed to travel the entire distance and to perform the turns. The former is denoted by E_t, and the latter by E_{Turn}.

$$E_{Total} = E_t + E_{Turn} \tag{4.5}$$

E_t is calculated as :

$$E_t = \lambda D_t \tag{4.6}$$

Where λ represents the energy consumption per unit length, and D_t is the total distance traveled.

E_{Turn} is obtained as :

$$E_{Turn} = \gamma \frac{180}{\pi} \vartheta_t \tag{4.7}$$

where γ represents the energy consumption per unit angle, and ϑ_t represents the sum of turning angles. This study sets λ and γ to 0.1164 KJ/m and 0.0173 KJ/degree, respectively.

The total energy consumption, denoted as E_{Total}, is calculated by considering two factors : distance covered and the sum of turning angles, which are weighted accordingly.

4.5 Simulations and Results

In this section, we will run simulations to show how our single-drone solution to the CPP problem can be beneficial. Mission Planner version 1.3.74 was used to run the simulations, and the host machine, which ran Windows 10 and included an Intel Core i7 processor running at 2.9 GHz and 16 GB of RAM, was equipped accordingly.

The Mission Planner Simulator (MPS) [203] is an open-source tool developed by Michael Oborne for the APM autopilot project, and it is only compatible with Windows operating systems. MPS offers an intuitive interface that shows details about the UAV, such as GPS status, airspeed, battery life, and video. It also permits users to download and examine mission log files.

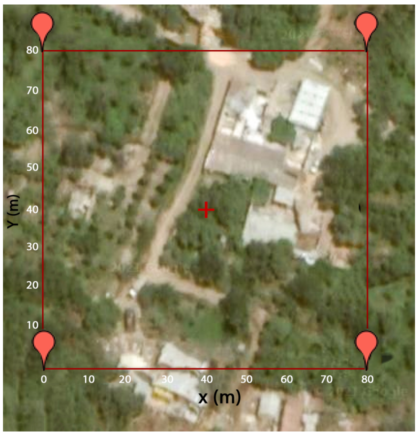
Four implemented paths, namely BF, Spiral, Zamboni, and LMAT path, were evaluated to showcase the efficacy of the proposed path in relation to other strategies, which were all implemented using the same simulator and area (as shown in Figure 4.6).

To ensure a fair comparison of different approaches in all scenarios, we assume the following :

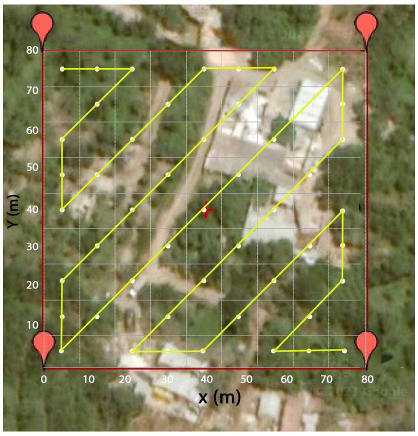
- UAVs are homogeneous.
- UAVs move at a constant velocity (UAV speed = 5 m/s).
- UAV rotation rate is $\theta = 30 degree/sec$.
- The distance between two waypoints is 10 meters.

The proposed strategy was implemented in an area near the 8 May 1945 University in Guelma, Algeria. The area of interest is a square measuring $180 \times 180\ m^2$. The initial map of the area was obtained from a satellite image, which can be seen in Figure 4.6a.

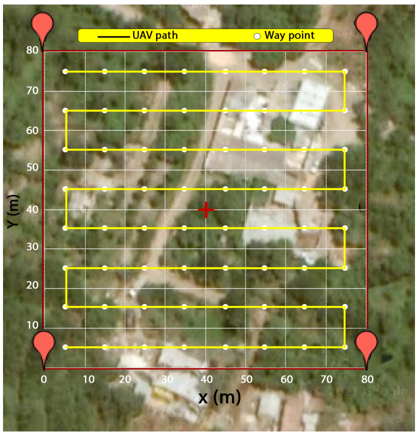
In order to demonstrate how the selected paths perform in variously sized areas, the simulation was conducted on three areas divided into grids of 5x5, 9x9, and 15x15. The



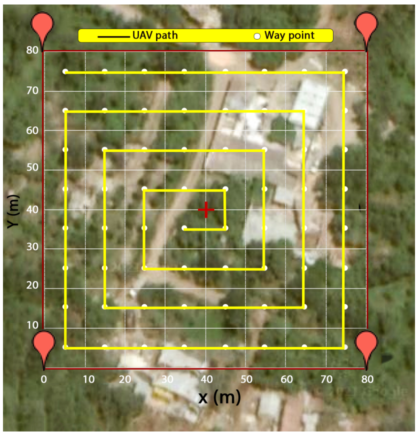
(a) Workplace



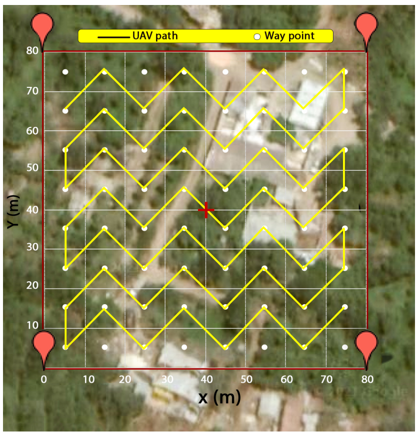
(b) Proposed Path



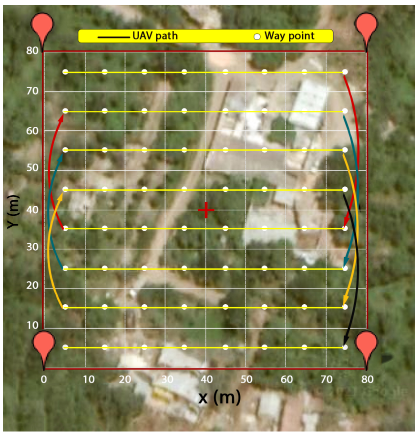
(c) Back and Forth Path



(d) Spiral Path



(e) LMAT path



(f) Zamboni Path

Figure 4.6 : Workplace and the simulated paths.

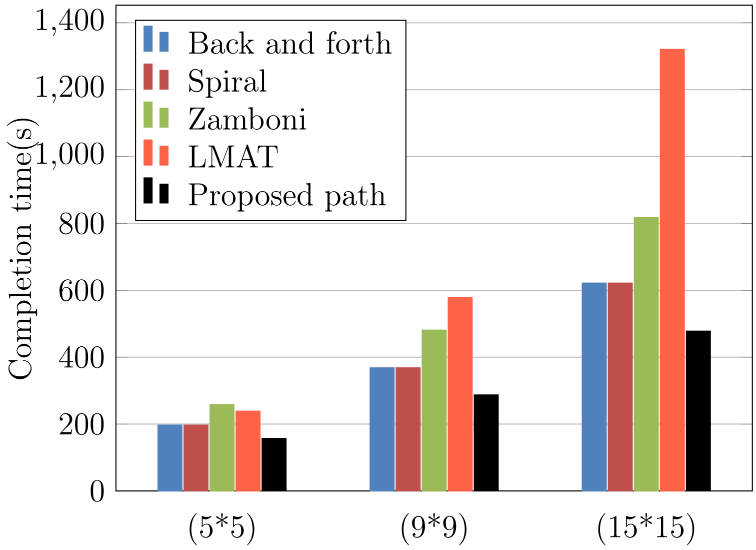


FIGURE 4.7 : Completion Time comparison of paths with 5x5, 9x9, and 15x15 Grids

effectiveness of each path was assessed by comparing the time taken by the drone to complete the mission and the total energy consumption. Figure 4.7 shows the calculation time for all tested paths in the three areas, while Figure 4.8 shows the corresponding energy consumption.

Table 4.1 presents a summary of the results achieved for the selected paths, including information on the number of turns, the total degree of turns, the length of the path, the time required for computation, and the amount of energy consumed.

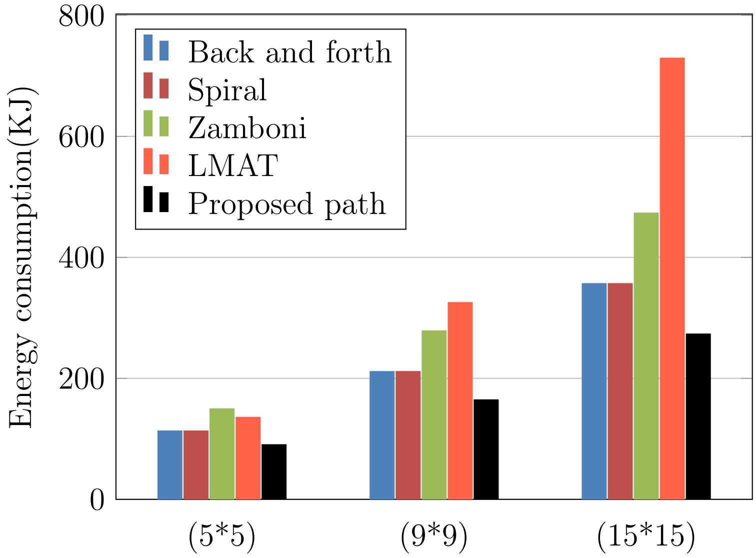


Figure 4.8 : Performance comparison of paths with 5×5, 9×9, and 15×15 Grids

Table 4.1 : Comparison of the obtained results

Paths	**(1) Back and Forth Path**	**(2) Spiral Path**	**(3) Zamboni Path**	**(4) Lmat Path**	**(5) Proposed Path**
			Area 1 (5×5)		
Number of Turns	8	8	4	18	6
Total degree of turns (°)	720	720	355.96	1620	540
Path length (m)	864	864	835	922.59	695.29
Completion-time (s)	196.8	196.8	178.87	238.52	157.058
Energy consumption (KJ)	113.0256	113.0256	103.0256	135.4155	90.27376
			Area 2 (9*9)		
Number of Turns	16	16	8	70	14
Total degree of turns (°)	1440	1440	699.68	5670	1260
Path length (m)	1600	1600	1555	1950.18	1225.09
Completion-time (s)	368	368	334.3227	579.036	287.018
Energy consumption (KJ)	211.152	211.152	193.1065	325.092	164.3985
			Area 3 (15*15)		
Number of Turns (KJ)	28	28	14	208	26
Total degree of turns (°)	2520	2520	1231.58	18720	2340
Path length (m)	2688	2688	3489	3482.23	1999.1
Completion-time (s)	362	368	334.3227	579.036	287.018
Energy consumption (KJ)	356.4792	356.4792	427.4259 9	729.1876	273.1772

Table 4.1 displays the comparison of the proposed path with other models, indicating thatThe proposed path is capable of achieving a remarkable improvement of 9.61% to 57.16% in terms of the time taken to complete the mission, indicating a significant reduction. Additionally, it covers less distance than other paths, with a reduction ranging from 13.72% to 51.83%. The proposed strategy also eliminates over 36.94% of the unnecessary turns compared to other paths, resulting in less energy consumption. In fact, all four tested paths consume more energy than the proposed path, with energy loss varying from 10.86% to 56%. This can be attributed to the overlap problem created by the repetitive passage of the drone over the same surface. Overall, the proposed path outperforms all the tested paths in terms of energy consumption, mission completion time, and traveled distance, demonstrating its effectiveness compared to state-of-the-art methods.

4.6 Conclusion

In this chapter, a new technique for static path planning for single drone reconnaissance missions was presented. The method involves dividing the AoI into cells using a grid-based approach. The key objectives of this proposed strategy are to efficiently cover the area in offline mode, reduce computational time, and minimize path length, number of turns, and energy consumption during missions. The evaluation results demonstrated that the proposed path outperforms existing paths in terms of performance, achieving significant improvements ranging from 9.61% to 57.16% in mission completion time, and 13.72% to 51.83% in distance traveled. Moreover, the proposed path eliminates unnecessary turns by more than 36.94% compared to other paths, resulting in less energy consumption.
Overall, the proposed approach can contribute to enhancing the efficiency and effectiveness of reconnaissance missions, and it can serve as a starting point for future research in the field of path planning for UAVs.

Chapter 5

Securing the IoD : A Lightweight Blockchain-Based User-Drone Authentication Scheme

Chapter contents

5.1 Introduction

Drones have become increasingly popular in a variety of civilian and military applications, including agriculture, surveillance and package delivery. The IoD involves drones collecting sensitive data and transmitting it to an external user (U_i) in real time via a GSS. In order to establish a session key and allow users and drones to authenticate each other securely and efficiently, it is essential to implement a reliable and effective authentication scheme for communication. Furthermore, due to the limited memory and battery capacity of drones, it is crucial to implement lightweight and effective security mechanisms. Although various solutions have been proposed to secure the IoD scenarios, neither has been effective or had a negative impact on efficiency.

This chapter focuses on HCALA, a novel authentication scheme that uses blockchain technology and Hyperelliptic Curve Cryptography (HECC) to secure user-drone communication. In order to evaluate the effectiveness and feasibility of the proposed scheme, we used the Random Oracle Model (ROM) and the AVISPA software tool, which are commonly used to verify the Internet protocol security. In addition to formal verification techniques, we also employed informal security analysis methods to assess HCALA's resistance against both active and passive attacks by adversaries. These various evaluations demonstrated that HCALA is a secure and robust authentication scheme for drones.

5.2 Related work

Recent research efforts have been devoted to developing secure and efficient communication methods for drones. In an IoD context, the transmission of sensitive data between drones is often done through unsafe wireless networks, making them vulnerable to various security threats. The first approach presented in [204] used an AKA-based method to establish a key agreement between user-nodes without using a gateway node, as reported by [205]. This method was considered lightweight because it only used bit-wise XOR and hash functions. However, Farash et al. [206] argued that this scheme was susceptible to multiple attacks such as man-in-the-middle (MTM) attacks, node anonymity and traceability, and node impersonation attacks. To overcome these security concerns, Farash et al. proposed an improved protocol, which addressed the weaknesses of the Turkanovic et al. scheme [204]. Despite these enhancements, the scheme proposed by Farash et al. still has vulnerabilities, such as offline password guessing, user impersonation, and smart card loss attacks, and it fails to provide secure session key secrecy or user anonymity against gateway nodes. To address these limitations, [207] suggested an efficient AKA scheme based on smart cards that can adapt to multiple gateway scenarios, addressing the deficiencies of the protocol described in [206]. Although the scheme has several advantages, it does not address the potential risks of Denial-of-Service (DoS) attacks or smart card theft, and it does not guarantee user anonymity. Challa et al. [208] suggested a user authentication protocol that was based on ECC. However, the scheme was found to have significant weaknesses by Jia et al. [209], making it susceptible to impersonation attacks. Additionally, the computational and communication costs associated with [208] were deemed excessively high, rendering it infeasible for deployment in various real-world scenarios.

Numerous security protocols have been proposed by researchers in the IoD network to ensure secure communication. Wazid [159] classified these protocols into several categories, including key management, access control, user authentication, identity privacy, and intrusion detection. In 2018, Wazid et al. [163] developed a lightweight AKA protocol for authenticating users and drones, which supports mutual authentication. The scheme's simplicity is attributed to the use of hash functions and fuzzy extractors, which results in minimal memory overhead, as well as low computational and communication costs. Although the authors addressed various security concerns, they failed to highlight the importance of forward and backward perfect secrecy, as well as non-repudiation, which are crucial requirements for sensitive drone operations.

Chen et al. [167] presented an improved Direct Anonymous Attestation (DAA) cryptographic scheme called Mutual Authentication DAA (MA-DAA) in which asymmetric bi-linear pairing is used for mutual authentication between network-connected UAVs and the GSS. Their approach is particularly suitable for UAV networks with low bandwidth and computational capabilities. However, their method relies on the use of specialized and costly security coprocessors called Trusted Platform Modules (TPMs), which must be integrated into systems, resulting in increased costs. Moreover, the security of the scheme has not been formally proven.

In contrast, Tanveer et al. [210] proposed a Lightweight AKE Protocol for IoD Environment (LAKE-IoD) that uses the AEGIS authenticated encryption algorithm, bit-wise XOR, and SHA256 hash function. Their protocol has various phases for revocation or reissue, dynamic drone deployment, and password update. They analyzed the security of their scheme using the Burrows-Abadi-Needham (BAN) logic for formal analysis, the Scyther toolkit for simulation, and mathematical assumptions for informal analysis. Their study shows that their scheme is secure against various security threats such as replay and man-in-the-middle (MTM) attacks.

The PARTH scheme enables mutual authentication between three entities in a software-defined UAV network through PUF-based authentication [211]. The system generates two session keys to ensure high security in sensitive data transmission and authentication. The authors claim that their scheme can withstand various attacks such as MTM, node capture, and replay attacks. On the other hand, TCALAS is a temporal credential-based anonymous lightweight authentication scheme that combines cryptographic, fuzzy extractor, bit-wise XOR, and hash function methods [164]. However, according to analysis, the scheme is limited to a single flying zone and vulnerable to stolen verifier attacks, which compromises untraceability. Ali et al. [212] proposed an enhanced version of the scheme called "iTCALAS" that addresses these issues and provides scalability for the IoD environment.

Cho et al. [213] proposed the SENTINEL (Secure and Efficient autheNTIcation for uNmanned aErial vehicLes) authentication framework to address security issues related to unauthorized drones in the IoD environment. The scheme provides mutual authentication between drones and GSS, but it is susceptible to "ESL attack under the CK-adversary model", and it does not preserve untraceability and anonymity. On the other hand, Ever [214] presented a secure authentication framework based on ECC, which provides one-time user authentication for drones in a hierarchical wireless sensor network architecture. However, their scheme is also vulnerable to the ESL attack under the CK-adversary model and does not provide anonymity and untraceability features like the SENTINEL authentication framework proposed by Cho et al. [213].

In their paper [215], Bera et al. proposed a blockchain-based access control protocol for the IoD environment that uses an ECC-based Diffie-Hellman key exchange for two authentication mechanisms : drone-to-drone and drone-to-GSS. In a later paper, Bera et al. [216] designed a secure data delivery and collecting scheme called BSD2C-IoD that uses blockchain to enable authentication between drones and their associated GSS. The authors claim that their framework is secure against many IoD attacks, but it has a high computational cost. Nikooghadam et al. [217] proposed a lightweight authentication protocol for the IoD, which they claim is secure against many threats. However, their scheme is vulnerable to several attacks, including control server impersonation, user impersonation, privileged insider attacks, and drone impersonation, and it does not provide user anonymity. Hussain et al. [218] suggested a three-party authentication scheme in an IoD environment that uses symmetric encryption and a one-way hash function. However, their scheme is susceptible to privileged insider attacks, drone capture attacks, and impersonation attacks

In order to secure communication in an IoD system, Tanveer et al. [219] proposed a security scheme that employs ECC, a hash function and an authenticated encryption algorithm. The scheme validates the user's identity across seven steps and then establishes a secret key for subsequent communications between the user and the drone. The authors claim that their proposed security scheme offers better performance and satisfies the security requirements. However, the scheme does not provide dynamic privacy protection. To address security concerns in communication between a remote user and a drone, Tanveer et al. [176] developed the RUAM-IoD authentication scheme using AES-CBC-256 encryption, a hash function (SHA-256), ECC, and XOR operation. The authors claimed that the scheme is resistant to several security threats, including stolen smart devices, biometric and password change, drone capture, replay, and MTM attacks. However, the scheme has high communication and computing expenses.

In recent work, Javed et al. [220] abandon the blockchain-based authentication protocol and HEC for IoT drones. Instead, the blockchain serves as a certification authority, with transactions defined as certificates to reduce maintenance costs while still ensuring high communication security. The authors claimed that their protocol provides protection against common attacks in drone IoT networks while being more efficient than other solutions in terms of computational and communication overheads.

Based on previous research, we aim to address various security vulnerabilities in existing IoD authentication protocols. Our proposed solution is HCALA, a new lightweight and secure user authentication scheme that is suitable for the IoD environment. The scheme is blockchain-based and employs hyperelliptic curve cryptography, which is more efficient and secure than other solutions. One notable feature is the small key size of 80 bits, which is half the size of the elliptic curve key (160 bits). Table 5.1 summarizes the cryptographic techniques, advantages, and properties of existing authentication/access control schemes and the proposed HCALA scheme for the IoD environment.

Table 5.1 : continued from previous page

Scheme	**Year**	**Cryptography Techniques**	**Limitations & Characteristics**
Challa et al. [208]	2017	• ECC • Bit-wise XOR operation • Hash function(SHA160)	• Exposed to privilege insider and stolen device.
Wizid et al. [162]	2018	• Bit-wise XOR operation • Hash function(SHA160)	• It is vulnerable to stolen-verifier attacks, user impersonation, and drone impersonation. • Exposed to session key leakage attack, server broadcasting and traceability issues.
Srinivas et al. [163]	2019	• Hash function • Biometric fuzzy extractor	• Vulnerable to user impersonation, identity guessing, and device impersonation attacks. • The cost of computation is slightly more expensive.
Tanveer et al. [210]	2020	• The authenticated encryption scheme (AEGIS) • Bit-wise XOR operation • Hash function (SHA256)	• The cost of computation is a little high. • Their scheme lacks support for blockchain solutions.
Ali et al. [212]	2020	• Advanced encryption standard (AES) • Bit-wise XOR operation • Hash function(SHA160)	• Exposed to forgery, Privilege Insider, Stolen Smart Device, Server Impersonation, and Denial-of-Service (DoS) attacks. • Perfect Forward Secrecy and key freshness features are not rendered.

Table 5.1 : continued from previous page

Scheme	**Year**	**Cryptography Techniques**	**Limitations & Characteristics**
Cho et al. [213]	2020	• ECC • Hash-based message authentication code function (HMAC) • One-way hash functions • Public key encryption	• Does not maintain untraceability and anonymity • Susceptible to ephemeral secret leakage (ESL) attack under the CK-adversary model • Does not allow for the dynamic deployment of drones.
Ever et al. [214]	2020	• One-way hash functions. • Bilinear pairings. • ECC. • Symmetric key encryption	• Susceptible to ESL attack under the CK-adversary model. • Absence of untraceability and anonymity preservation properties. • High costs of communication and computing.
Bera et al. [215]	2020	• ECC • Hash function(SHA256) • Symmetric key encryption • Blockchain consensus algorithms	• Vulnerable to user anonymity attack. • Computation is high.
Bera et al. [216]	2020	• ECC • Hash function(SHA256)	• Cannot provide user/drone anonymity. • High communication cost.

Table 5.1 : continued from previous page

Scheme	Year	Cryptography Techniques	Limitations & Characteristics
Nikooghadam et al. [217]	2021	• One-way hash functions • Bit-wise XOR operations • ECC	• Vulnerable to control server impersonation, drone impersonation, user impersonation attack, privileged insider attack. • Does not offer user anonymity and untraceability.
Hussain et al. [218]	2021	• One-way hash functions • Symmetric key encryption	• Exposed to privileged insider attacks. • Vulnerable to impersonation attacks. • Not able to fend off drone capture attempts.
Tanveer et al. [219]	2021	• ECC • One-way hash functions • AEGIS • Bit-wise XOR operations	• Does not ensure dynamic privacy protection. • The use of blockchain technology is not endorsed.
Tanveer et al. [175]	2022	• Hash function (SHA-256) • Bit-wise XOR operations • ECC • AES-CBC-256 encryption	• Communication and computing expenses are somewhat high. • The blockchain solution is not supported.

TABLE 5.1 : continued from previous page

Scheme	**Year**	**Cryptography Techniques**	**Limitations & Characteristics**
HCALA scheme	2023	• HEC • One-way hash functions • Bit-wise XOR operation • Symmetric key encryption • Blockchain consensus algorithms	• It provides protection against various known attacks. • It provides formal security analysis and communication cost is very low.

5.3 Preliminaries

5.3.1 HEC : Hyperelliptic Curve

HEC, a class of algebraic curves [221], was proposed by [222] as a generalized version of elliptic curves (EC). However, unlike EC points, HEC points cannot be obtained through a group. Instead, the additive Abelian group is obtained through a divisor or calculated using HEC. One advantage of HEC over RSA, EC, and bilinear pairing is that it can maintain the same security level while using smaller parameter sizes [223].

An elliptic curve (EC) is defined as a curve with a genus value of 1. On the other hand, Figure 5.1 illustrates an HEC with a genus value greater than 1. For a genus value of $D = 1$, the finite field group order (Fq) required 160-bit long operands, necessitating at minimum $g.\log_2(q) = 2^{160}$ bits. Likewise, with a genus value of 2, curves required operands of 80-bit long, while with a genus value of 3, curves required operands of 54-bit long.

A HEC "C" of genus g $(g > 1)$ over F is a set of solutions $(x, y) \in F \times F$ to the following equation :

$$C : y^2 + h(x)y = f(x) \tag{5.1}$$

The divisor (D) of an HEC is a finite sum of points, and it is written as :

$$D = \sum_{p_i \in C} m_i p_i, m_i \in Z \tag{5.2}$$

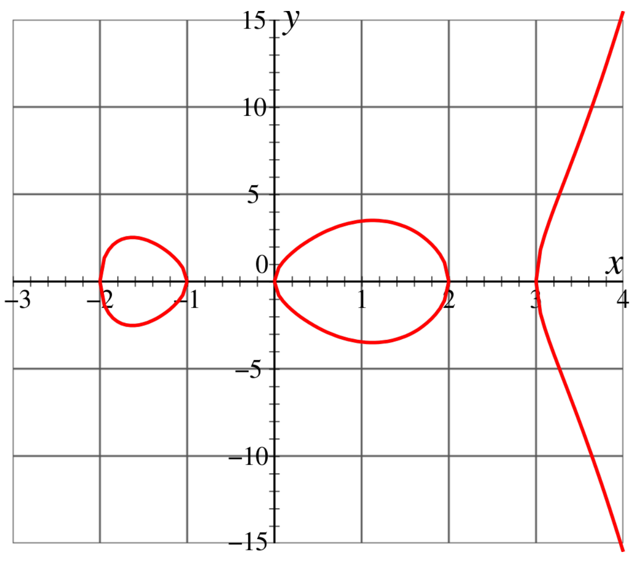


FIGURE 5.1 : Hyperelliptic curve of genus 2 (from wikipedia)

5.3.2 Complexity assumptions

5.3.2.1 Assumptions Of Hyperelliptic Curve Discrete Logarithm Problem (HECDLP)

The following assumptions are made for the HECDLP :

- $\eta \in \{1, 2, 3, \ldots, q-1\}$.
- The probability calculation η from $R = \eta.D$ is negligible.

5.3.2.2 Computational Diffie-Hellman Assumption Of Hyperelliptic Curve (HCCDHP)

We assume :

- η and $\vartheta \in \{1, 2, 3, \ldots, q-1\}$.
- The probability computation of η and ϑ from $\Gamma = \eta.\vartheta.D$ is negligible.

5.3.3 Consensus algorithms

In a Peer-to-Peer network, a consensus algorithm is needed to add a block to the blockchain. A consensus algorithm is a mechanism for making decisions in an environment where nodes cannot be trusted. It refers to a state where all nodes in a distributed network agree on a specific matter. Due to the distributed nature of blockchain networks, achieving consensus is difficult. Since there is no central node responsible for validating all the distributed nodes' trustworthiness, certain consensus mechanisms are required to maintain consistency in the ledgers across different nodes. Several consensus mechanisms are available in blockchain technology, some of which are outlined in Figure 5.2.

5.4 System models

To comprehend the functionality and usability of the HCALA protocol, two crucial models must be understood : the network model and the threat model.

5.4.1 Network model

Figure 5.3 illustrates the HCALA network model designed for the IoD environment. The registration authority (GSS) assumes the responsibility of registering all drones and users and is deemed trustworthy. Drones are dispatched to a designated flying zone to

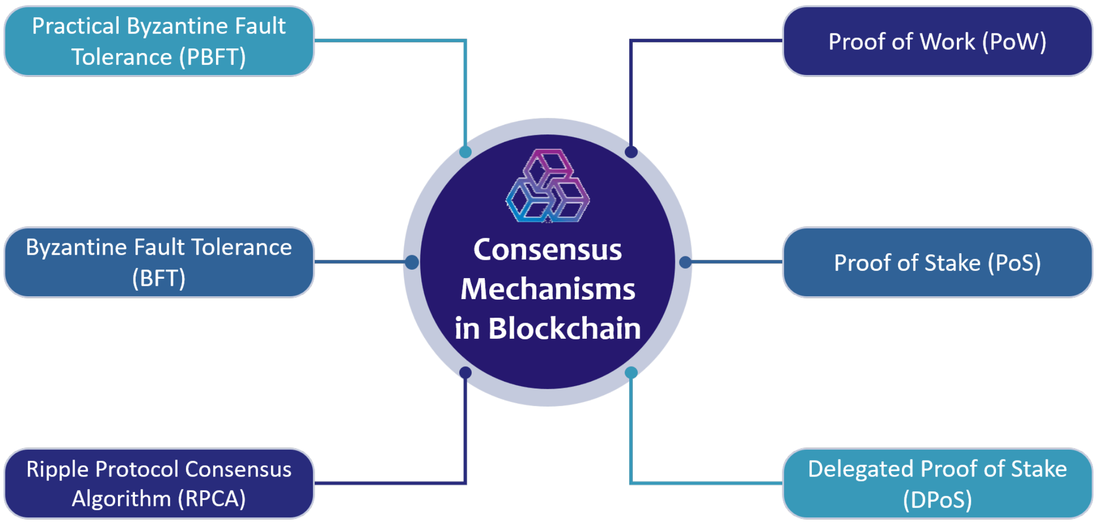


FIGURE 5.2 : Consensus mechanisms in blockchain

collect information or data from the surrounding area. Typically, an internal user seated in the (CR) is assigned to monitor an IoD environment. Suppose an external registered user (U_i), such as an ambulance driver, wants to obtain traffic information from a specific flying zone quickly. In that case, the user needs to connect to the GSS via the Internet and use it to request data from the drone deployed in that region. Both the U_i and the drone use the GSS to authenticate each other. After authentication, they can establish a session key (secret key) and securely communicate in the future.

5.4.2 Threat model

Below, we provide a brief explanation of the two threat models we have considered :

5.4.2.1 Dolev–Yao threat model (DY)

In IoD, it is assumed, according to the commonly known Dolev-Yao threat model [224], that an adversary A can intercept all messages transmitted via untrusted communication channels and also has the ability to modify or add erroneous information into the communication channel. Moreover, in the DY model, communication end-points, e.g., drones, are considered untrusted in the network.

5.4.2.2 Canetti and Krawczyk (CK)-adversary model

To strengthen the security of our user authentication technique, we incorporate the (CK)-adversary model [225], which offers higher robustness than the DY threat model used in other user authentication protocols. As per the CK-adversary model, besides the

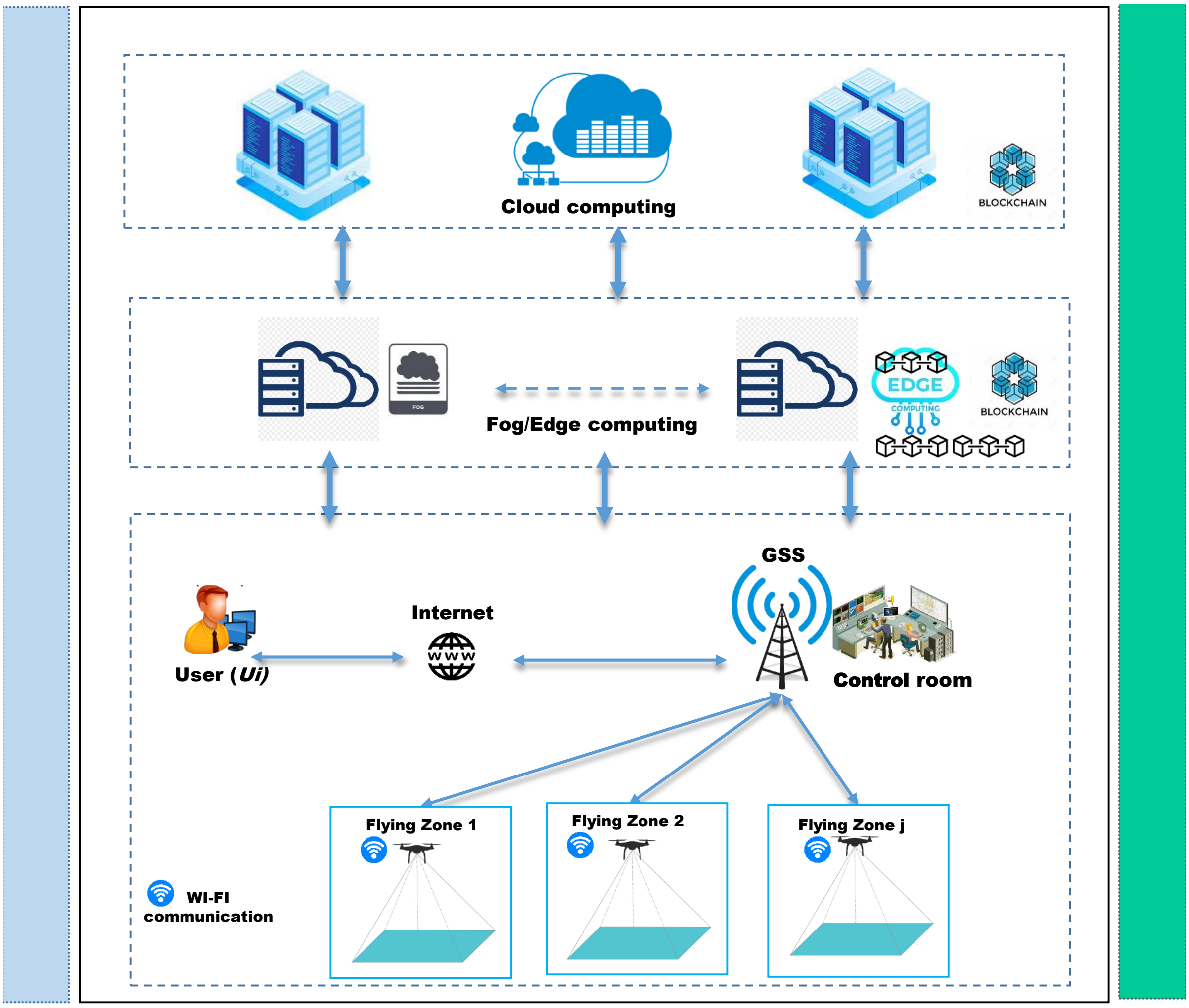


FIGURE 5.3 : Network Model

abilities mentioned in the DY threat model, the adversary "A" can also gain access to secret session states and confidential information, such as secret keys. In addition, there is a possibility that A may conduct power analysis attacks and physically capture some drones to obtain all the secret credentials stored on them, leading to the risk of ESL and physical drone capture attacks. We assume that the registration authority, GSS, is a trusted entity that offers registration services to other communication entities and that servers responsible for blockchain mining are reliable.

5.5 Proposed scheme

Figure 5.4 illustrates the phases of the proposed HCALA protocol, while the following table (Table 5.2) summarizes the symbols used in the scheme.

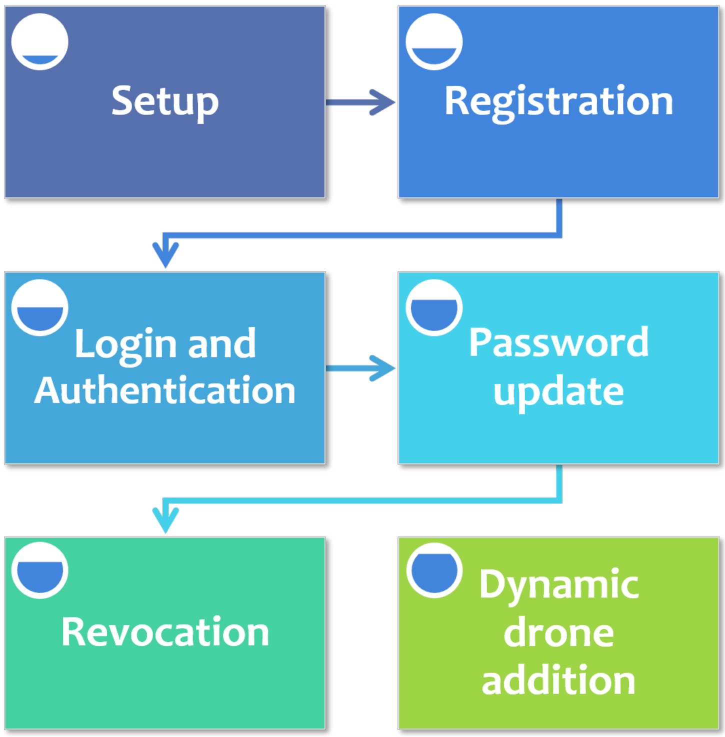


FIGURE 5.4 : HCALA protocol phases

5.5.1 Setup phase

In this phase, the certificate authority (GSS) generates the public parameters of the HCALA scheme and its private key. This process involves the following steps taken by GSS :

- **Step 1 :** Chooses a random number $PR_{GSS} \in \{1, 2, \ldots, n-1\}$ as his private key.
- **Step 2 :** The GSS calculates the public key in the following way : $PK_{GSS} = PR_{GSS}.D$, where D is the divisor on a hyperelliptic curve.
- **Step 3 :** The GSS selects $h(.)$ as a secure one-way cryptographic hash function. Finally, the parameter set $\{PK_{GSS}, D, n = 2^{80}, h(.)\}$ are published publicity.

5.5.2 Registration phase

This phase involves the secure registration of all drones (Dr) and users (U_i) by the (GSS) in offline mode before they are deployed. The registration process is described in detail below for each drone and user.

Table 5.2 : Symbols and their descriptions

Symbol	Descriptions
ID_x	Real identity of x
PR_x	Private key of x
PK_x	Public key of x
MID_x	Masked identity of x
$h(.)$	hash function
Tw_x	Time window generated by X
$\oplus$	Bitwise XOR operation
ΔT	Threshold value for the timestamp
$\|$	Concatenation operation
Rn_2, Rn_3	Random numbers
$SK_{Dr,i}$	Session key between user and drone
$SK_{i,Dr}$	Session key between drone and user
D	Divisor of hyperelliptic curve

5.5.2.1 Drone registration

The procedure for registering drones prior to deployment in a specific area is conducted by the GSS. The following is a detailed explanation of the steps involved in registering each drone.

- **Step 1 :** For each drone, GSS selects a unique identity ID_{Dr} and computes the corresponding masked-identity as : $MID_{Dr} = h(ID_{Dr} \parallel PR_{GSS})$.
- **Step 2 :** GSS saves the identity MID_{Dr} in its own database and engraves $\{ID_{Dr_j}$, $MID_{Dr}\}$ in the memory of the respective drone (Dr).

5.5.2.2 User registration

To access real-time data from a specific drone in an IoD environment, an external user (U_i) needs to register securely with the GSS either in person or over a secure channel. The following steps are carried out by the GSS and U_i to complete the registration process.

- Step 1 : To begin with, U_i selects a distinct identifier, referred to as ID_i, and a password, denoted as PW_i. Then, U_i chooses a random value $\beta \in n$ to computes

  $$A_i = h(h(ID_i \parallel \beta) \oplus h(PW_i \parallel \beta))$$

  Finally, U_i securely transfers the registration request message to GSS.

- Step 2 :After receiving the message, GSS calculates the value of MID_i And B_i as

$$MID_i = h(ID_i \parallel PR_{GSS})$$

$$B_i = h(MID_i \parallel A_i)$$

Next, GSS stores $\{ID_i, MID_i, B_i\}$ in its database, and sends $\{MID_i, B_i\}$ to U_i across a secure channel.

- Step 3 : Upon receipt from GSS, U_i calculates

$$B_i{}' = h(MID_i \parallel PW_i) \oplus B_i$$

$$MID_i^{'} = h(ID_i \parallel PW_i) \oplus MID_i$$

Finally, U_i stores $\{\beta, B_i{}', MID_i{}'\}$ in its own memory of the device to complete the registration process.

5.5.3 Login and authentication phase

This section presents a detailed description of the login and authentication phase of the proposed scheme, which is initiated by a registered user U_i to establish a secure channel and obtain authorization by sharing a secret key with a drone deployed in a specific area.

- **Step 1 :** Before the mobile device performs the computation $A_i^m = h(h(ID_i \parallel \beta) \oplus h(PW_i \parallel \beta))$ $MID_i^m = h(ID_i, PK_{GSS})$ and $B_i^m = h(MID_i^m \parallel A_i^m)$, U_i must provide their identification ID_i and password PW_i. Then verifies ($B_i^m \stackrel{?}{=} B_i$). If the verification process fails, it is terminated immediately. However, if the verification is successful, U_i proceeds to generate PR_u and a current time window Tw_1 to perform the following computation :

$$PK_{GSS} = PR_u.D$$

$$E_i = PR_u.PK_{GSS}$$

$$U_1 = MID_i \oplus h(MID_{GSS} \parallel Tw_1)$$

$$U_2 = MID_{Dr} \oplus h(MID_{GSS} \parallel Tw_1 \parallel E_i)$$

$$U_3 = h(MID_i \parallel MID_{GSS} \parallel MID_{Dr} \parallel E_i \parallel Tw_1)$$

Finally, the authentication request message $MSG1 = (U_1, U_2, U_3, PK_u, Tw_1)$ is sent to GSS over a public channel to be analysed later.

- **Step 2 :** Upon receiving the authentication request message$MSG1(U_1, U_2, U_3, PK_u, Tw_1)$, the GSS performs the following validation steps. Firstly, it checks whether the time window Tw_1 is valid by verifying whether the difference between Tw_c (the time at which the message was received) and Tw_1 is less than or equal to ΔT, which is the maximum time threshold for message reception. If the validation is successful, the GSS computes $E_{GSS} = PK_u.PR_{GSS}$ using the public key of the user (PK_u) and its own private key (PR_{GSS}). With this value, the GSS can then compute the following :

  $MID_i^* = U_1 \oplus h(MID_{GSS} \parallel Tw_1)$

  $MID_{Dr} = U_2 \oplus h(MID_i^* \parallel Tw_1 \parallel E_{GSS})$

  $U_3^* = h(MID_i^* \parallel MID_{Dr}^* \parallel MID_{GSS}^* \parallel E_{GSS} \parallel Tw_1)$

  GSS verifies whether the equation ($U_3 \stackrel{?}{=} U_3^*$) holds true. If this equation is false, GSS declines the authentication request. If true, GSS can authenticate U_i and move on to the next steps.

  $$G_1 = h(MID_{Dr}^* \parallel Tw_2) \oplus Rn_2$$

  $$G_2 = MID_i^* \oplus h(MID_{Dr}^* \parallel MID_{GSS} \parallel Tw_2 \parallel Rn_2)$$

  $$G_3 = h(MID_{Dr}^* \parallel MID_{GSS} \parallel MID_i^* \parallel Tw_2 \parallel Rn_2)$$

  Finally, GSS sends message $MSG_2 = (G_1, G_2, G_3, TW_2)$ to drone through a public channel.

- **Step 3 :** When the drone receives the message, it verifies its freshness by checking if Tw_c and Tw_2 satisfy the condition $|Tw_c - Tw_2| \leq \Delta T$. If the condition is satisfied, the drone can perform the following calculations :

  $$Rn_2^* = G_1 \oplus h(MID_{Dr} \parallel Tw_2)$$

  $$MID_i^{'*} = G_2 \oplus h(MID_{Dr} \parallel MID_{GSS} \parallel Tw_2 \parallel Rn_2^*)$$

  $$G_3^* = h(MID_{Dr} \parallel MID_{GSS} \parallel MID_i^* \parallel Tw_2 \parallel Rn_2^*)$$

  If the condition ($G_3 \stackrel{?}{=} G_3^*$) to authenticate GSS fails, the session will end immediately. However, if it succeeds, the drone generates a random number Rn_3 based on the current time window Tw_3 and then moves on to the next steps.

  $$D_1 = h(MID_i^{'*} \parallel MID_{Dr} \parallel Tw_3) \oplus Rn_3$$

$$SK_{Dr,i} = h(MID_{Dr} \parallel MID_{GSS} \parallel MID_i^{*'} \parallel Tw_3 \parallel Rn_3)$$

$$Auth = h(SK_{Dr,i} \parallel Tw_3)$$

Finally, Dr sends the message MSG_3=$(D_1, Auth, Tw_3)$ directly to user U_i through a public channel.

- **Step 4 :** After getting the message MSG_3=$(D_1, Auth, Tw_3)$, U_i first checks time freshness by the condition $|Tw_c - Tw_3| \leq \Delta T$. If the condition is valid, U_i calculates Rn_3^*, session key and authentication value ($Sk_{i,Dr}$) as :

$$Rn_3^* = D_1 \oplus h(MID_i \parallel MID_{Dr} \parallel Tw_3)$$

$$SK_{i,Dr} = h(MID_{Dr} \parallel MID_{GSS} \parallel MID_i \parallel Tw_3 \parallel Rn_3^*)$$

$$Auth^* = h(SK_{i,Dr} \parallel Tw_3)$$

U_i checks if $Auth^*$ matches with $Auth$ for authentication of the drone Dr and then saves the session key for future secure communication. However, if $Auth^*$ and $Auth$ do not match, the session is immediately terminated by U_i. A detailed representation of the authentication phase is provided in Figure 5.5.

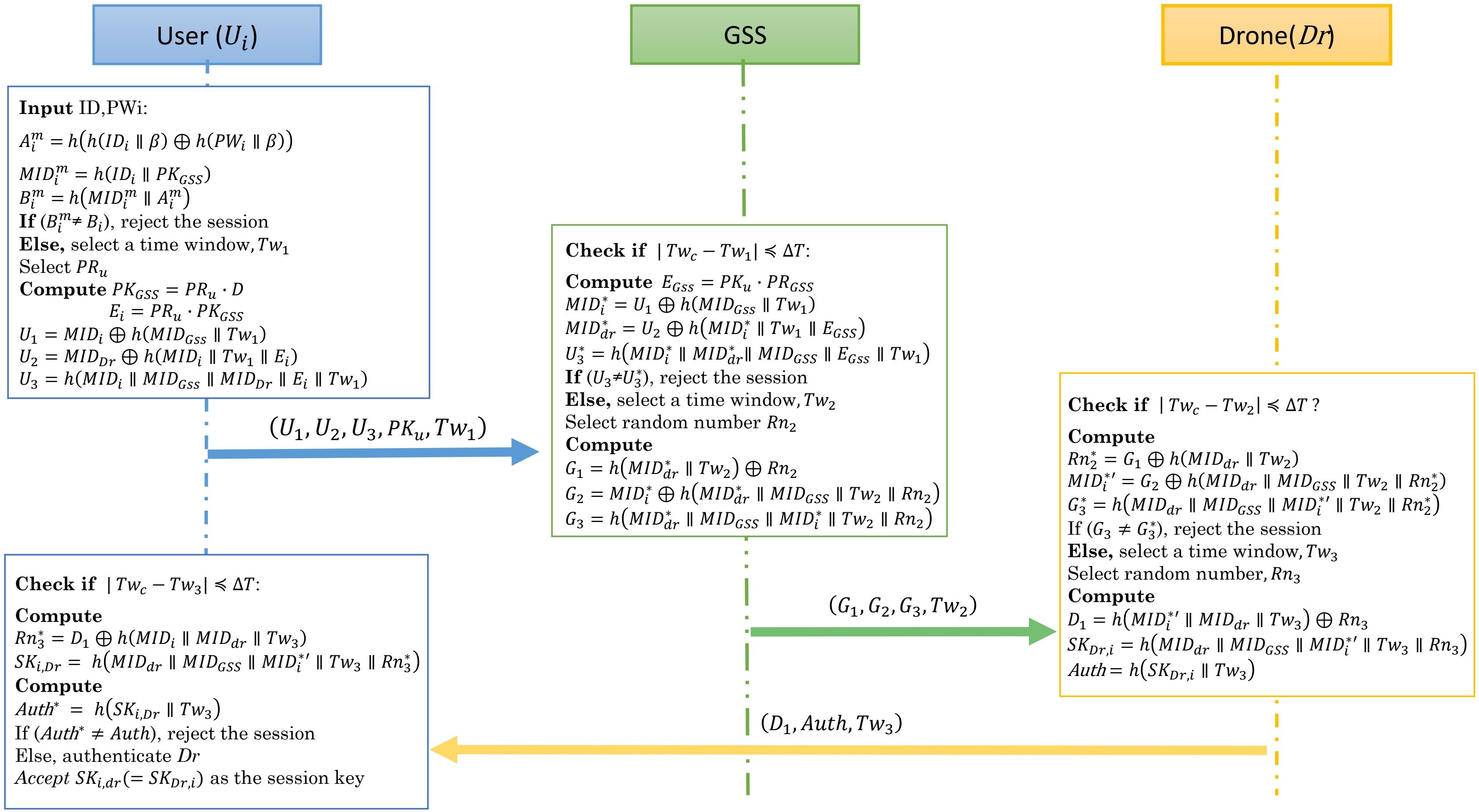


Figure 5.5 : Authentication process of the HCALA scheme

5.5.4 Password update phase

To ensure a secure authentication scheme, a password updating process must be available. An authorized user, U_i, can change their current password, PW_i, to a new password, PW_i^{new}, using their mobile device. The following steps must be completed by U_i :

- **Step 1 :** U_i enters his or her login information, including the identity ID_i and password Pw_i, and the mobile device performs the following computations :

$$A_i^m = h(h(ID_i \parallel \beta) \oplus h(PW_i \parallel \beta))$$

$$MID_i^m = h(ID_i, PK_{GSS})$$

$$B_i^m = h(MID_i^m \parallel A_i^m)$$

  Next, the mobile device verifies the condition ($B_i^m \stackrel{?}{=} B_i$) and aborts the process if it is invalid. If the condition is satisfied, the mobile device prompts U_i to provide a new password to complete the process.

- **Step 2 :** U_i selects a new password PW_i^{new} and sends it. The mobile device computes the following :

$$A_i^{new} = h(h(ID_i \parallel \beta) \oplus h(PW_i^{new} \parallel \beta))$$

$$MID_i = h(ID_i^{new}, PK_{GSS})$$

$$B_i^{new} = h(MID_i \parallel A_i^{new})$$

- **Step 3 :** Finally, U_i replaces B_i^{new} with B_i in the mobile device.

To enhance the security of the system, it is crucial to consider that the password of the user U_i should be changed at regular intervals.

5.5.5 Revocation and reissue phase

If an authorized user's (U_i) mobile device is lost or stolen, they can obtain a replacement device and follow the instructions given below.

- **Step 1 :** U_i keeps his ID_i identity but chooses PW_i^{new} as his new password. Then, using a random number β', U_i computes

$$A_i^{new} = h(h(ID_i \parallel \beta') \oplus h(PW_i^{new} \parallel \beta'))$$

  and sends$\{ID_i, A_i^{new}\}$ to the GSS across secure channel.

- **Step 2 :** GSS computes MID_i and B_i after receiving the message, as follows :

$$MID_i = h(ID_i \parallel PR_{GSS})$$

$$B_i^{new} = h(MID_i \parallel A_i^{new})$$

Next, GSS stores $\{MID_i, B_i^{new}\}$ in its database, and sends $\{MID_i, B_i^{new}\}$ to U_i through a safe channel.

- **Step 3 :** Following receipt from GSS, U_i computes

$$B_i^{new^*} = h(MID_i \parallel A_i^{new}) \oplus B_i^{new}$$

$$MID_i^* = h(ID_i \parallel PW_i^{new}) \oplus MID_i$$

Finally, U_i replaces B_i with $B_i^{new^*}$, and stores $\{B_i^{new^*}, MID_i^*\}$ in its own memory of device. U_i also deletes $B_i^{'}$ from the memory of the device to complete the revocation and reissue process.

5.5.6 Dynamic drone addition phase

In scenarios where a drone's battery is low, or the drone is physically seized by an attacker, it is crucial to promptly deploy another drone in the same AoI. The HCALA protocol facilitates this by allowing for the addition of new drones to the network at any time. This phase is comparable to the drone registration phase and involves similar steps. The following section provides a more detailed description of this phase.

- **Step 1 :** The GSS generates a unique identity ID_{Dr}^{new} for a new drone that is not registered yet and then computes the corresponding masked-identity as :

$$MID_{Dr}^{new} = h(ID_{Dr}^{new} \parallel PR_{GSS})$$

- **Step2 :** The GSS stores $\{ID_{Dr}^{new}, MID_{Dr_j}^{new}\}$ in the drone's memory before deploying it in the field, GSS also keep $\{ID_{Dr}^{new}\}$ in its own database.

5.5.7 Block creation and addition in blockchain

The HCALA scheme considers the data gathered by drones to be confidential and private. Thus, it is desired to store this information on a private blockchain managed by the P2P CS network. However, drones have limited computing power, and assigning

Block Header	
Block Sequence Number	BS_n
Timestamp	TS
Last Block Hash	BH_l
Merkle Tree Root	MTR
Proposer public key	PK_{pcs}
Block Payload (Encrypted Transactions)	
List of Encrypted Transactions #i (Tx_i)	$\{(Tx_i^{id}, Tx_i^{makerid}, E_{pk\_GSS}(Tx_i), Tx_i^{hash}, Tx_i^{ES})\} \mid i=1,2,\ldots,t_n \mid$
Current Block Hash	BH_c
ECDSA signature on BH_c	$ES.BH_c$
Commit Message Pool	MSG_{cp}

FIGURE 5.6 : Structure of a block $Block_m$

them the responsibility of creating transactions for the blockchain could be challenging. To address this issue, the GSS is allowed to construct the transactions of the collected data to be added to the blockchain, which is more computationally efficient. When a cloud server CS receives a block $Block_m$ from the GSS, and the number of transactions in the transaction pool reaches a certain threshold ($Tran_{sh}$), CS creates a transaction pool containing the securely received transactions. The transactions $Tx_1, Tx_2, Tx_3, \ldots$ are then included in the formation of $Block_m$, as illustrated in Figure 5.6. Using a voting-based consensus mechanism, such as the "PBFT" algorithm, CS adds the transactions to the blockchain. The detailed process is given in Algorithm 5.1.

5.6 Security analysis

In this section, we examine the security features of the HCALA scheme, and demonstrate its security using the "ROM" and the AVISPA tool [226]. We also evaluate the scheme's security features to ensure that it can withstand various types of attacks. Table 5.4 provides a comparison of the security and functionality properties of HCALA with those of other existing schemes.

5.6.1 Formal security verification using (ROM)

This section aims to evaluate the security properties of the HCALA scheme using the (ROM). The ROM involves a scenario where an attacker, A, interacts with the i^{th} instance of a participant that runs the protocol, represented as Π^i. In our proposed scheme, the

Algorithme 5.1 : Consensus for block validation and addition

Input : $Tans_p$: A pool of transactions, N : number of P2P nodes, $Tans_sh$: transaction threshold, App_t : approval threshold, where $App_t = 2 * (N - 1)/3 + 1$

Output : After successful validation, the block $Block_m$ is committed and added to the blockchain.

if $(|Tans_p| = Tans_{sh})$ **then**

  A leader CS_l is chosen in a round-robin manner from the P2P CS network for voting requests.

  (CS_l) constructs a block $Block_m$ depicted in Figure 5.6, sets $MSG_{cp} \leftarrow \emptyset$ (empty) and broadcasts $Block_m$ to the P2P network for voting request

  The follower receives $Block_m$ and validates it with the transaction pool

  for *"each follower"* CS_j **do**

    Verify $Tx_i^{hash}, Tx_i^{ES}, MTR, BH_c, ES.BH_c$

    If all are validated successfully, CS_j puts a valid vote reply to MSG_{cp}

  Let VT_{count} denotes the number of valid votes in the pool, MSG_{cp}

  Set $VT_{count} \leftarrow 0$

  for *"each valid vote reply in* MSG_{cp}*"* **do**

    Set $VT_{count} = VT_{count} + 1$

  if $(App_t \leq VT_{count})$ **then**

    Add block $Block_m$ to the blockchain

    Broadcast commitment response to all followers

participant can be a legitimate user denoted as U_i, a drone represented by DR_j, or the GSS. The ROM model assumes that various queries, such as $Extract(.)$, $Execute(.)$, $Test(.)$, and $Reveal(.)$, are utilized to simulate an actual attack, as indicated in Table 5.3. Moreover, each entity's instances, including A, have access to a collision-resistant one-way hash function $h(.)$.

Definition 5.1. (Semantic Security) : The security of the shared key SK between U_i and DR_j under the ROM is based on the indistinguishability of the real SK from a random number guessed by an attacker A. The attacker has a probability of breaking the security of the HCALA scheme and obtaining the SK. The security is tested through a game where A tries to guess the correct bits of SK, represented by Ω, and their guess is represented by Ω'. If Ω=Ω', then A wins the game. The advantage of A is a measure of how successful they are in breaking the security :

$$Adv_A^{protocol} = |2.Prob[\Omega = \Omega'] - 1|.$$

Where $Prob[\Omega = \Omega']$ denotes the probability of success. If $Adv_A^{protocol}$ is negligible under the ROM, then HCALA scheme is secure.

Table 5.3 : Queries and their purposes.

Query	Purpose
$Corrupt(\Pi^t, U_i)$	Applying this query, the adversary A can utilize a power analysis attack to corrupt a legitimate user and obtain the sensitive credentials.
$Send(\Pi^t, msg)$	This means that A can initiate an active attack by sending the message msg to Π^t and receiving message in return from Π^t. A can start a new instance of Π^t by sending Send(Π^t, start) to the oracle.
$Reveal(\Pi^t)$	Applying this query, A can reveal a session key Sk between Π^t and its partner.
$Execute(U_i, V_j)$	This query enables A to launch passive attacks. This query has the potential to eavesdrop on any messages sent over the public channel. It outputs the exchanged messages among participants.
$Test(\Pi^t)$	By executing this query, A may confirm if the established SK is actual or a probabilistic random result of a coin flip. This query can only be executed once by A. if $b = 1$, C returns a valid SK to A; else, $(b = 0)$ returns a random, equal-sized secret key.

Theorem 5.1. *Suppose that attacker A tries to compromise a secret key's security in polynomial time T. If Q_{Hash}, $|Hash|$, and $Adv_A^{HECDLP}(P_t)$, denotes the number of hash queries, the size of the one-way collision-resistant hash function $h(.)$, and the advantage of breaking the (HECDLP) for A, respectively. The estimated advantage that A has in breaking HCALA's security to acquire SK between U_i and Dr is expressed as :*

$$Adv_A^{HCALA}(P_t) \leq \frac{Q^2_{Hash}}{2|Hash|} + Adv_A^{HECDLP}(P_t).$$

Proof. The security of SK is demonstrated proved in the following three games, namely $Game_i^A (i = 1, 2, 3)$, using the queries provided in Table 5.3. In the game $Game_i^A$, let $Success_{game_i}^A$ be an event in which A successfully guesses a random bit Ω . Thus, the advantage (success probability) of A to win the game $Game_i^A$ is $Adv_{A,Game_i}^{HCALA} = Prob[success_{Game_i}^A]$. The following is a detailed description of each game.

$Game_1^A$: In this game under ROM, A engages in an actual attack against the proposed scheme. At the start of $Game_1^A$, A is required to make a prediction on the bit Ω. Thus, we have :

$$Adv_{A}^{HCALA}(P_t) = |2.Adv_{A,Game_1}^{HCALA} - 1|. \tag{5.3}$$

$Game_2^A$: This game involves a simulated eavesdropping attack, where A is capable of intercepting all messages being transmitted $MSG1 = \{U_1, U_2, U_3, PK_u, TW_1\}$, $MSG2 = \{G_1, G_2, G_3, TW_2\}$, and $MSG3 = \{D1, Auth, TW_3\}$ during the login and authentication phase by utilizing the *Execute* query provided in Table 5.3 to execute the proposed scheme. A uses the *Reveal* and *Test* queries to verify if the SK generated is legitimate or random during the game. The session key established between the user U_i and the drone DR_j is represented by $SK_{i,Dr} = h(MID_{Dr} \parallel MID_{GSS} \parallel MID_i \parallel Tw_3 \parallel Rn_3^*)$. Since the attacker A does not have access to the temporal secrets (Rn_3^*) and long-term secrets ($MID_{Dr}, MID_{GSS}, MID_i$) that are protected by the one-way collision-resistant hash function $h(.)$, the probability of successfully obtaining the session key $SK_{i,Dr}(= SK_{Dr,i})$ will not increase by intercepting the messages $MSG1, MSG2$ and $MSG3$. Consequently, in the event of an eavesdropping attack, $Game_2^A$ and $Game_1^A$ become indistinguishable. This results in the subsequent :

$$Adv_{Game_2,A}^{HCALA} = Adv_{Game_1,A}^{HCALA}. \tag{5.4}$$

$Game_3^A$: In this scenario, the adversary A executes a $Corrupt(\Pi^t, U_i)$ query to extract the data stored in the memory of U_i (i.e., B_i', MID_i') by employing a power analysis attack [224]. The hash function provides protection for variables such as ID_i, PW_i, and A_i. It should be noted that the task of generating the authentication message $MSG1 = (U_1, U_2, U_3, PK_u, Tw_1)$ would be difficult for the attacker, even if they were able to capture ID_i, PW_i, and A_i. There are two reasons for this difficulty :

- Calculating the values of related variables like PK_u and E_i requires complicated HECDLP computations.
- The hash function property prevents the attacker from determining the values of MID_{GSS} and MID_{Dr} using U_1, U_2, and U_3.

Even if the attacker A makes hash queries, no collision occurs. Moreover, distinguishing between $Game_2^A$ and $Game_3^A$ is challenging. As a result of the HECDLP and the concept of the birthday paradox, the following outcome is achieved :

$$|Adv_{A,Game_2}^{HCALA} - Adv_{A,Game_3}^{HCALA}| \leq \frac{Q_{Hash}^2}{2|Hash|} + Adv_{A}^{HECDLP}(P_t). \tag{5.5}$$

Once the *Test* query has been executed, it is only necessary to correctly guess the bit

c to win the *Game*. This leads to the following result :

$$Adv_{A,Game_3}^{HCALA} = \frac{1}{2}. \tag{5.6}$$

Eq.(5.3) gives :

$$\frac{1}{2}Adv_{A}^{HCALA}(p_t) = |Adv_{A,Game_1}^{HCALA} - \frac{1}{2}|. \tag{5.7}$$

Simplifying the Eqs.(5.3-5.5), and using the result of triangular inequality, we can derive the following equation from Eq.(5.7)

$$\frac{1}{2}Adv_{A}^{HCALA}(p_t) = |Adv_{A,Game_1}^{HCALA} - Adv_{A,Game_3}^{HCALA}| \tag{5.8}$$

$$= |Adv_{A,Game_2}^{HCALA} - Adv_{A,Game_3}^{HCALA}| \tag{5.9}$$

$$\leq \frac{Q_{Hash}^2}{2|Hash|} + Adv_{A}^{HECDLP}(p_t).$$

The final result is obtained by multiplying both sides of the equation Eq.(5.9) by "2" as follows :

$$Adv_{A}^{HCALA}(P_t) \leq \frac{Q_{Hash}^2}{|Hash|} + 2Adv_{A}^{HECDLP}(P_t)$$

■

5.6.2 Formal security verification

This section discusses the security validation process for HCALA protocol, which involved the use of the AVISPA tool for formal security verification [226]. Automated software for formal security verification has become increasingly popular among security researchers in recent years. AVISPA [226], ProVerif [227], Casper/FDR [228], and Scyther [229] are some of the available formal security verification techniques. AVISPA provides advanced methods for automatically analyzing the security of a security scheme. It integrates with four back-ends, which are CL-AtSe, SATMC, OFMC, and TA4SP [226]. The High-Level Protocol Specification Language (HLPSL) is the modular language used to implement the protocols to be tested, which simplifies the modeling of complex security properties. The HLPSL code is converted to an intermediate format (IF), and then fed into one of the four available back-ends to create the output format (OF).

The HCALA protocol has been implemented for three primary roles, including User (U_i), GSS, and Dr_j. It also defines mandatory roles for the session, as well as composite roles for the session, goal, and environment. The protocol uses the OFMC and CL-AtSe

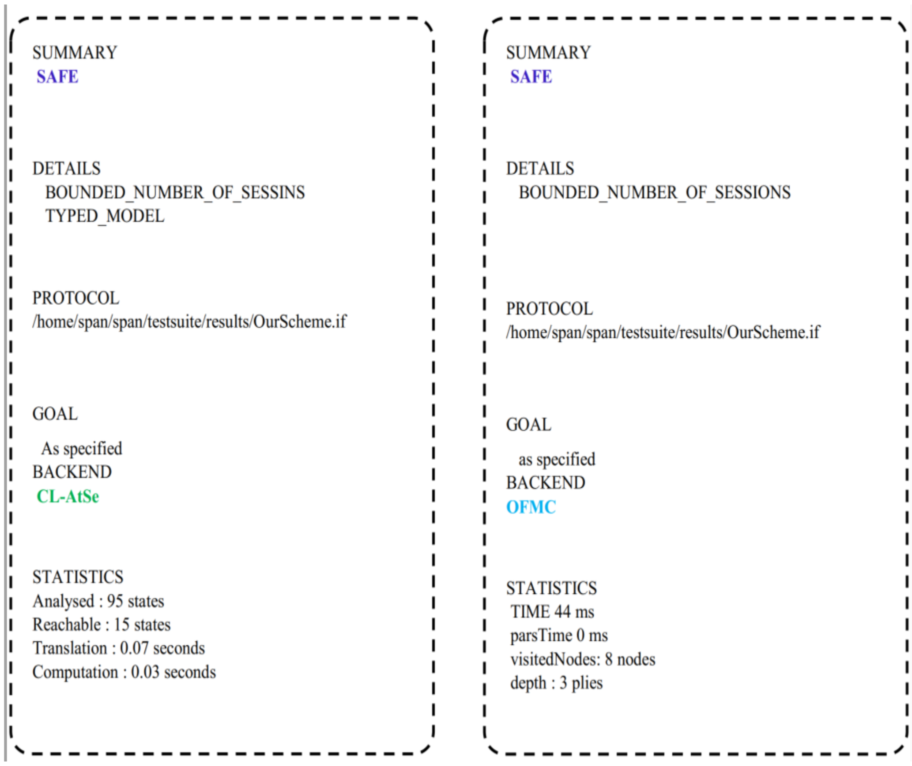


FIGURE 5.7 : Results from the AVISPA simulation utilizing the CL-AtSe and OFMC backends.

back-ends for formal security verification, while the TA4SP and SATMC back-ends are not considered due to their inability to perform bitwise XOR operations. The back-ends are used to determine whether the protocol is susceptible to a replay attack by approved agents who can identify a passive adversary. Information regarding authorized agents' normal sessions is provided to the intruder by the back-ends.

The performance of the suggested scheme was evaluated through a simulation using the Security Protocol ANimator for AVISPA (SPAN) tool [226]. Figure 5.7 illustrates a detailed representation of the simulation results.

5.6.3 Informal security analysis

5.6.3.1 Privacy and anonymity

To ensure privacy and anonymity, it is important that the proposed scheme guarantees that no attacker can extract real identities once the system is deployed. As previously mentioned, our system can provide privacy protection for all sent and received messages, including MSG_1, MSG_2, and MSG_3, by using fresh time windows and random numbers to generate these messages. This makes it challenging for attackers to obtain private data or real identities of users, drones, or GSS, which is a significant advantage. Therefore, the

HCALA scheme provides a strong level of privacy and anonymity.

5.6.3.2 Un-traceability

The HCALA protocol ensures un-traceability by selecting unique random nonces (Rn_2, Rn_3) and current time windows during authentication for each session. This results in unique messages sent by each participant, which the opponent (A) cannot correlate. Additionally, the sender cannot be traced. A hash function is used to store real or masked identities (ID_x, MID_x), which further ensures un-traceability.

5.6.3.3 Session Key Agreement

Once the registered user U_i and drone Dr_j mutually authenticate during the login and authentication phase, they both generate a common session key denoted as $SK_{Dr,i}$ (also equal to $SK_{i,Dr}$) by utilizing the following calculation : $SK_{Dr,i} = h(MID_{Dr} \parallel MID_{GSS} \parallel MID_i^{*'} \parallel Tw_3 \parallel Rn_3)$. This session key is then used for subsequent communication between the user and drone, ensuring session key agreement in the HCALA scheme.

5.6.3.4 Perfect Forward Secrecy (PFS)

In the HCALA scheme, PFS is guaranteed because each participant creates a new session key (Sk) for each session. The session key contains a random number (Rn) that an adversary does not easily guess or calculate. This property ensures that even if a long-term key is compromised, previous session keys used in earlier communications remain secure. Additionally, the protocol uses a time window (TW) to authenticate recent sessions, which means that even if an attacker gains access to a secret component key, the security of previous sessions will not be compromised. Hence, the suggested scheme provides PFS.

5.6.3.5 Integrity

The HCALA scheme provides assurance of message integrity, which means that it prevents any unauthorized modifications to the messages transmitted between the nodes. The security of the scheme is based on the hardness of the HECDLP problem, which makes it difficult for opponents to deduce the corresponding Sk_x. Moreover, nodes perform an integrity check after exchanging messages in each phase using a one-way hash function. As a result, the proposed scheme provides better security in terms of maintaining message integrity.

5.6.4 Resistance against potential attacks

5.6.4.1 Replay attacks

Based on the mechanism of TW_s and nonces (random numbers) used in the messages transmitted in the HCALA scheme to protect against replay attacks. When a message is received, the first step is to extract the time window associated with it and compare it to the TW encrypted within it. If the values match, the receiver will consider the message valid ; otherwise, the receiver will reject the message as old or tampered with. This feature of the HCALA scheme ensures its resilience against replay attacks.

5.6.4.2 DoS attack

During the login or password update phase, if the registered user U_i provides incorrect credentials such as ID_i and/or PW_i, the HCALA scheme performs a local check by verifying if $A1 = A$ or $A_{old} = A_{new}$. Once the verification is successful, the user's login request is forwarded to the GSS. Moreover, in the password update process, the old password is only updated if it has been verified successfully. This way, the HCALA scheme is designed to withstand DoS attacks of such nature.

5.6.4.3 MTM attacks

Using the time windows, authentication tokens, and the hash function $h(.)$ makes the MTM attack futile. In this type of attack, an adversary tries to intercept and manipulate the messages, such as MSG_1, MSG_2, MSG_3, in order to make the participants believe that they are communicating with legitimate parties. However, the MTM attack fails because the attacker is unable to create or authenticate the required authentication tokens. Additionally, the attacker cannot modify or delay the communicated messages due to the use of the hash function for both message integrity and freshness. Therefore, the suggested HCALA scheme can effectively resist MTM attacks.

5.6.4.4 Drone Impersonation attack

To impersonate a registered drone Dr_j, an attacker needs to generate valid messages $Auth = h(sk_{Dr_j} \parallel TW_3)$ and transmit them to U_i in a way that passes the verification process. However, the authentication token $Auth_j$ includes the session key SK_{Dr_j} that the attacker cannot obtain. Upon receiving the message $Auth$, U_i computes $Auth^*$ and compares it to $Auth$ to determine whether they are the same. Thus, U_i can differentiate between a legitimate drone and an impersonated drone, indicating that the proposed scheme is resistant to drone impersonation attacks.

5.6.4.5 User Impersonation attack

Based on the information provided in the second step, the GSS authenticates a user U_i in the login and authentication phase, the GSS calculates U_3^* and compares it with U_3 received from U_i. To impersonate U_i, an attacker can generate a message that looks valid to the GSS. This message includes MID_i, MID_{GSS}, MID_{Dr}, E_i, and Tw_1, and is hashed to produce $U_3 = h(MID_i \parallel MID_{GSS} \parallel MID_{Dr} \parallel E_i \parallel Tw_1)$. However, the attacker cannot access the secret parameters such as E_i and the private key PR_{GSS} of the GSS, which are necessary to generate a valid U_3. Although the adversary can construct its time window TW_A, it cannot produce a valid U_3. Therefore, the GSS can differentiate between impersonated and legitimate users. Our scheme is resistant to user impersonation attacks.

5.6.4.6 GSS impersonation attack

In this attack, the attacker is playing the role of a legitimate register GSS, and he is intercepting the authentication message MSG_2 between the GSS and the drone Dr_j. The adversary can attempt to prove his legitimacy by creating modified or fake messages based on the sensitive data extracted from the GSS. To do so, the attacker must generate a valid message MSG_2 in polynomial time by creating a timestamp TW_2 and a fresh random number Rn_2. However, the attacker cannot compute G_1, G_2, or G_3, nor modify MSG_3 due to a lack of information about MID_{dr}, MID_{GSS}, and MID_i. Therefore, the attacker cannot forge or tamper with the $GSS's$ deceived message in polynomial time. The HCALA scheme can resist GSS impersonation attacks.

5.6.4.7 Stolen Smart Device attack

Suppose that a registered user U_i loses their smart device or has it stolen by an attacker. The attacker can use power analysis attacks to extract all information B_i', MID_i' from the device's memory, where $B_i' = h(MID_i \parallel A_i) \oplus B_i$ and $MID_i' = h(ID_i \parallel PW_i) \oplus MID_i$. Despite this, the attacker cannot guess ID_i and PW_i correctly from the extracted information because they do not have access to the secret parameter A_i. Moreover, because of the one-way hash function used, the attacker cannot retrieve both the identity and password at the same time. However, the attacker cannot access U_i's secret parameters. Therefore, our protocol is protected against attacks in which a mobile device is lost or stolen.

5.6.4.8 Known Session Key attack

The session key $SK_{Dr,i} = h(MID_{Dr} \parallel MID_{GSS} \parallel MID'_{i^*} \parallel Tw_3 \parallel Rn_3)$ contains the random numbers unique to the current session. As the hash function used in the scheme is one-way and collision-resistant, it is not possible for an attacker to extract the random numbers from the session key. Hence, if an attacker somehow manages to obtain an old session key, they will not be able to use it to access the present session key. Therefore, the HCALA protocol is secure against known session key attacks.

5.6.4.9 Physical Drone Capture attack

As previously mentioned, it is possible for an attacker to physically capture a drone. If a drone Dr_j is captured, an attacker can access all of its stored credentials and communication information, including ID_{Dr_j}, MID_{Dr_j}. The private key PR_{GSS} is protected by a one-way hash function, which means that the attacker cannot compute the next communication session key without knowledge of the masked identity and random numbers. Since the secret information for each deployed drone and the GSS is unique and distinct, an attacker cannot produce session keys for non-compromised drones and the GSS using information obtained from a captured drone. Therefore, the suggested scheme can prevent physical drone capture attacks.

5.6.4.10 Modification attack

To prevent an adversary from modifying authentication and reply packets, hash function is utilized to confirm that the information is not tampered with. The message sent, $U_3(G_3)$, includes the sender's secret key, E_i, and the $GSS(Dr_j)$ can easily detect if the message has been altered by verifying the equation $U_3 = U_3^*(G_3 = G_3^*)$. Similarly, U_i can identify any modification to $Auth$ by checking the equation $Auth = Auth^*$. As a result, the HCALA scheme is resistant to attacks involving modification of packets.

5.7 Performance evaluation

In this section, the performance of the proposed HCALA scheme is evaluated in terms of computation and communication overheads as well as energy consumption. These metrics are important indicators of the practicality and efficiency of the HCALA scheme in real-world scenarios. To assess the effectiveness of the HCALA scheme, a comparison is made with several existing schemes, namely Tanveer et al.'s [219], Ever et al. [214], Challa et al.'s [208], Wazid et al.'s [163], and Hussain et al.'s [218] scheme. This comparative analysis enables an evaluation of the strengths and weaknesses of the proposed scheme and highlights its advantages over other existing schemes.

Table 5.4 : Comparison of functionality features between HCALA scheme and related authentication schemes.

		[219]	**[214]**	**[208]**	**[163]**	**[218]**	**HCALA**
Security goals	▪ Privacy and anonymity	●	●	●	●	●	●
	▪ Un-traceability	○	○	●	●	●	●
	▪ Mutual Authentication	●	●	●	●	●	●
	▪ Session Key Agreement	●	●	●	●	●	●
	▪ Integrity	○	○	○	○	○	●
Resistance to	▪ Replay Attacks	●	●	●	●	●	●
	▪ Denial-of-Service Attack	○	○	●	●	●	●
	▪ MTM Attack	●	●	●	●	●	●
	▪ Modification Attack	○	○	○	○	○	●
	▪ Physical Drone Capture Attack	○	●	●	●	●	●
	▪ Known session key Attack	○	○	●	○	●	●
	▪ Stolen Smart Device Attack	●	●	●	●	●	●
	▪ GSS impersonation Attack	○	●	○	○	○	●
	▪ User Impersonation Attack	○	●	●	●	●	●
	▪ Drone Impersonation Attack	●	○	○	●	○	●
Network components	▪ Cloud computing	○	○	○	○	○	●
	▪ Blockchain	○	○	○	○	○	●
Security analysis	▪ Formal: ROM	●	○	○	○	○	●
	▪ Formal: AVISPA tool	○	○	●	●	○	●
	▪ Informal analysis	●	●	●	●	●	●

Notes: ●: indicates that the feature is available; ○: indicates that the feature is not available.

5.7.1 Computational overhead

The registration phase includes necessary operations such as XOR operations, hash functions, comparisons, ECC and HEC multiplicative operations, and concatenation operations. In comparison with other operations and functions, concatenation, XOR operation, and comparison are negligible. Let T_h, T_{ecm}, T_{hcm}, T_{fe}, T_{sym}, and T_{ag} denote the time required to execute a secure hash function, HEC divisor multiplication, ECC point multiplication, fuzzy extractor function (Gen(·)/Rep(·)), symmetric encryption/decryption, and AEGIS (AEAD scheme), respectively. Using the results utilized in [164, 230–232], we have $T_h \approx 0.0023ms$, $T_{ecm} \approx 2.226ms$, $T_{hcm} \approx 0.48ms$, $T_{fe} \approx T_{ecm} \approx 2.226ms$, $T_{sym} \approx 0.0046ms$, and $T_{ag} \approx 0.415ms$.

The comparative results of computing overheads among various related authentication schemes [163, 208, 214, 218, 219] reported in Table 5.5 as well as in Figure 5.8 . Table 5.5 and Figure 5.5 clearly show that the HCALA scheme achieves significantly better performance than other related schemes [208, 214, 219], but incurs a higher computation cost than comparable schemes [163,218], However, the HCALA scheme provides enhanced security and functionality.

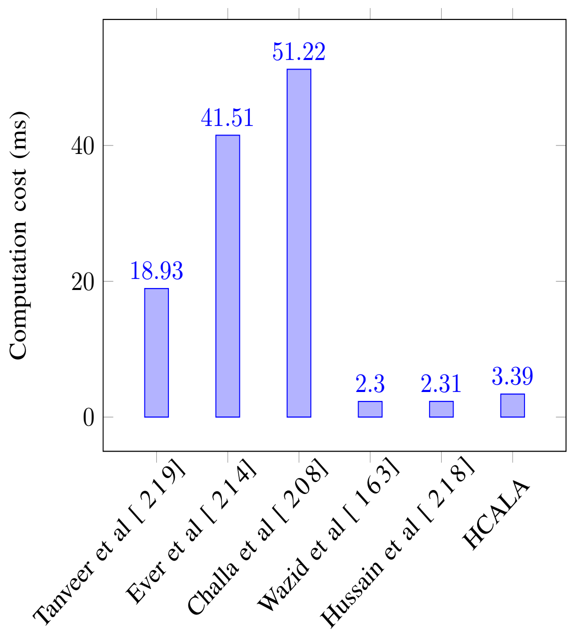


FIGURE 5.8 : Comparison of computation costs

Table 5.5 : Comparison of computation cost

Scheme	User side	Server side	Drone side/ Sensing device side	Total(ms)
[219]	$6T_h + 3T_{ag} + 3T_{ecm} + T_{fe}(10.1628)$	$2T_h + 3T_{ecm} + T_{ag}(3.4756)$	$3T_h + 2T_{ecm} + 2T_{ag}(5.2889)$	18.9273
[214]	$5T_h + 2T_b(10.8655)$	$3T_h + 2T_b(10.8609)$	$9T_h + 2T_b + 4T_{ecm}(19.7787)$	41.5051
[208]	$5T_h + 5T_{ecm} + T_{fe}(13.3675)$	$4T_h + 5T_{ecm}(11.1392)$	$3T_h + 4T_{ecm}(26.712)$	51.2187
[163]	$T_{fe} + 16T_h(2.2605)$	$8T_h(0.0184)$	$7T_h(0.0161)$	2.2973
[218]	$15T_h + T_{fe}(2.2605)$	$9T_h + 2T_{sym}(0.0299)$	$7T_h(0.0161)$	2.3065
HCALA	$9T_h + 2T_{Hec}(2.2467)$	$6T_h + T_{Hec}(1.1268)$	$6T_h(0.0138)$	3.3873

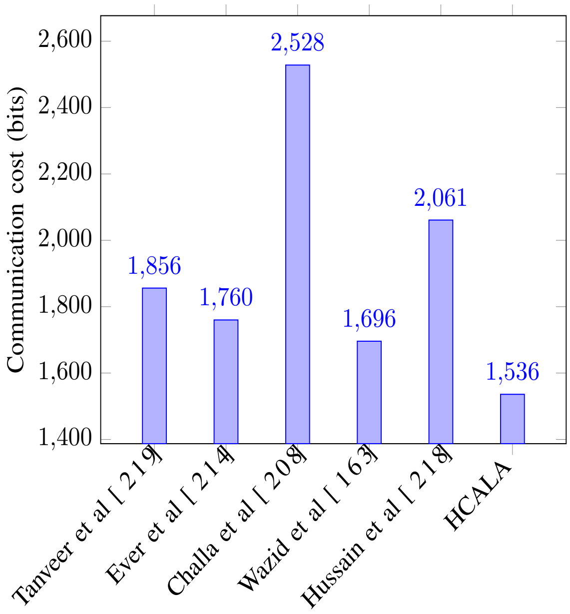


FIGURE 5.9 : Comparison of communication costs

5.7.2 Communication overheads

Figure 5.9 provides a comparison of the communication costs of some related authentication schemes [163, 208, 214, 218, 219] and HCALA scheme during the login and authentication phases. To estimate communication costs, we assume the bit-sizes of the identity, random number, timestamp, elliptic curve point, hyperelliptic curve and the digest of a hash function using Secure Hash Standard "SHA-1" are 160, 32, 128,160, 80, and 160 bits, respectively. As shown in Figure 5.9, our protocol requires less communication cost than the related protocols [163, 208, 214, 218, 219] in terms of bits needed to transmit the messages.

5.7.3 Energy consumption

Energy consumption refers to the total amount of energy used to complete all algorithm operations [233]. The measurement of energy consumption during the communication procedure is expressed in Joules and is based on the number of messages transmitted [234].

Table 5.6 provides a comparison of the energy consumption of the HCALA scheme with several relevant schemes [163, 208, 214, 218, 219], during the authentication process. The HCALA scheme and [163, 208, 218] demonstrate similar energy consumption levels of (3.38×10^{-4}) and consume less energy than other schemes (6.76×10^{-4}) [214, 219]. These results indicate that the HCALA scheme is more energy-efficient.

Table 5.6 : Comparative Analysis of Communication Energy Consumption

Scheme	No. of messages	Energy Consumption(Joule)
[219]	6	6.76×10^{-4}
[214]	6	6.76×10^{-4}
[208]	3	3.38×10^{-4}
[163]	3	3.38×10^{-4}
[218]	3	3.38×10^{-4}
HCALA	3	3.38×10^{-4}

5.8 Conclusion

This chapter presents the design of an anonymous lightweight authentication scheme called HCALA for secure communication between users and drones, utilizing hyperelliptic curve cryptography (HECC), hash functions, XOR operation, and blockchain technology. The HCALA scheme encompasses various phases : setup, registration, login and authentication, password update, revocation and reissue, and dynamic drone addition. The scheme provides privacy, anonymity, un-traceability, mutual authentication, session key agreement, integrity, and confidentiality while being resistant to various attacks such as replay, DoS, MTM, physical drone capture, impersonation, known session key, stolen smart device, and modification attacks. The security of HCALA is analyzed informally and formally using "ROM" and the AVISPA tool. The comparison study indicates that our scheme provides a better balance between efficiency and security for drones while outperforming existing schemes in terms of security.

Conclusion and Perspectives

In recent years, there has been a rapid increase in the use of drones for various applications, from aerial photography to delivery services. Drones have proven to be highly effective in tasks that are either too dangerous or difficult for humans to perform. They are capable of providing real-time data and information, which has enabled professionals to make informed decisions and take appropriate actions quickly.

Coverage path planning (CPP) is one of the critical factors that determine the effectiveness of drones, particularly in situations where human access is limited or hazardous. CPP involves generating optimal flight paths for drones to ensure maximum coverage of an area of interest. The goal of CPP is to minimize flight time and energy consumption while maximizing the coverage area. However, the challenges associated with generating optimal flight paths for drones require further research and development to enable them to operate optimally in different environments and situations. One of the significant challenges is the need to optimize flight paths while accounting for factors such as drone weight, battery life, and payload. This can be particularly challenging when dealing with larger drones that require more energy to operate and are less maneuverable than smaller drones.

As the usage of drones continues to increase, it is becoming increasingly essential to ensure their security in operations. With drones operating on the Internet of Drones (IoD) network, security has become a critical factor that needs to be considered during drone operations. Hackers can exploit vulnerabilities in drone systems and take control of drones, leading to unauthorized access, theft, or damage to property or lives.

Blockchain-based authentication schemes offer promising solutions for ensuring the security of drone operations on the IoD network. However, there are challenges that must be addressed, such as interoperability and standardization, and the need for continuous updates and maintenance. Addressing these challenges requires ongoing research and development to develop effective security solutions that can keep pace with the growing usage of drones.

The aim of this thesis was to develop new solutions for CPP and security in drone operations. The research problem was to address the challenges of designing and implementing CPP algorithms for drones, as well as the security threats and vulnerabilities associated with the Internet of Drones (IoD).

To achieve these objectives, a comprehensive literature review was conducted to identify the state-of-the-art approaches in CPP and security for drones. A new static path planning strategy was proposed, which was designed to reduce computational time, path length, number of turns, and energy consumption during missions. Additionally, a hyper-elliptic curve-based anonymous lightweight authentication (HCALA) scheme was developed to ensure privacy and anonymity, un-traceability, mutual authentication, session key agreement, integrity, and confidentiality in drone operations.

The structure of the thesis comprised five chapters, each addressing a specific research question. The first chapter provided an introduction to the research problem, objectives, and research questions. The second chapter reviewed the current state of CPP for drones, focusing on static path planning patterns. The third chapter presented an overview of the security context in IoD, with a specific focus on authentication. The fourth chapter proposed a new static path for reconnaissance with a single drone, while the fifth chapter developed the HCALA scheme for user-drone authentication.

The contribution of this thesis was the development of new solutions for CPP and security in drone operations. The proposed static path planning strategy and HCALA scheme provide more efficient and secure ways of operating drones. The impact of this research is significant, as it can lead to the development of more efficient and secure drone operations, with implications for several fields, such as emergency services, surveillance, and environmental monitoring.

In conclusion, the contribution of this thesis lies in six points :

- Investigating the current state of CPP for drones and exploring the existing simulators for evaluating CPP algorithms.
- Exploring the security challenges and vulnerabilities of IoD-based communication between users and drones.
- Proposing a new static path planning strategy for drones that can optimize coverage efficiency, reduce computational time, path length, and energy consumption.
- Designing a secure and lightweight anonymous authentication scheme between users and drones that can provide privacy, mutual authentication, session key agreement, integrity, confidentiality, and resistance to various security attacks.

- Evaluating the proposed CPP strategy and authentication scheme using simulation experiments and security analysis, respectively.

The research presented in this thesis opens up several avenues for future work in the field of drone operations and security. The following are some potential directions for future research :

- *Dynamic Coverage Path Planning :* The proposed static path planning strategies can be extended to dynamic scenarios, where the environment is changing, and drones need to adapt their paths in real-time. Future research can explore dynamic coverage path planning techniques that take into account changing environmental conditions, such as wind, weather, and traffic.
- *Obstacle Detection and Avoidance :* While the proposed path planning strategies consider the Area of Interest as a grid without obstacles, real-world environments are often cluttered with obstacles such as trees, buildings, and power lines. Future research can explore techniques for obstacle detection and avoidance to ensure safe and efficient drone operations in cluttered environments.
- *Multi-Drone Coordination :* The proposed path planning strategies assume a single drone operating in the Area of Interest. Future research can explore techniques for coordinating multiple drones to perform coverage tasks in parallel, improving efficiency and reducing mission time.
- *Advanced Security Techniques :* While the HCALA scheme presented in this thesis provides strong security guarantees, future research can explore advanced security techniques such as homomorphic encryption and zero-knowledge proofs to further enhance the security and privacy of drone operations.
- *Incorporate IA, machine learning, and federated learning techniques in security :* One possible area for future research is the integration of artificial intelligence (AI) and machine learning (ML) techniques into the security of drones. Specifically, the use of federated learning can be explored to improve the efficiency and privacy of data processing in IoD. Furthermore, the development of intelligent security mechanisms that can detect and respond to new types of attacks can also be an interesting direction for future research. This may include the use of deep learning algorithms to identify anomalous behavior patterns and generate timely alerts to prevent potential security breaches.

- *Real-world Implementations :* The proposed strategies and schemes need to be tested and validated in real-world scenarios to demonstrate their effectiveness and feasibility. Future research can explore the implementation of the proposed techniques and schemes on real drones and test their performance in various environments.

References

[1] Tauã M Cabreira, Lisane B Brisolara, and Paulo R Ferreira Jr. Survey on coverage path planning with unmanned aerial vehicles. *Drones*, 3(1) :4, 2019.

[2] Merzougui Salah Eddine, Mohamed Amine Ferrag, Othmane Friha, and Leandros Maglaras. Easbf : An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *Journal of Information Security and Applications*, 59 :102802, 2021.

[3] Faezeh Pasandideh, João Paulo J da Costa, Rafael Kunst, Nahina Islam, Wibowo Hardjawana, and Edison Pignaton de Freitas. A review of flying ad hoc networks : Key characteristics, applications, and wireless technologies. *Remote Sensing*, 14(18) :4459, 2022.

[4] Louisa Brooke-Holland. Unmanned aerial vehicles (drones) : an introduction. *House of Commons Library : London, UK*, 2012.

[5] Gaurav Singhal, Babankumar Bansod, and Lini Mathew. Unmanned aerial vehicle classification, applications and challenges : A review. 2018.

[6] AS Danilov, Ur D Smirnov, and MA Pashkevich. The system of the ecological monitoring of environment which is based on the usage of uav. *Russian journal of ecology*, 46(1) :14–19, 2015.

[7] Camille Alain Rabbath and Nicolas Léchevin. *Safety and reliability in cooperating unmanned aerial systems*. World Scientific, 2010.

[8] Zineddine Kouahla, Ala-Eddine Benrazek, Mohamed Amine Ferrag, Brahim Farou, Hamid Seridi, Muhammet Kurulay, Adeel Anjum, and Alia Asheralieva. A survey on big iot data indexing : Potential solutions, recent advancements, and open issues. *Future Internet*, 14(1) :19, 2022.

[9] Ala-Eddine Benrazek. *Internet of Things : Analysis of suspicious behaviour in a surveillance camera network*. PhD thesis, 2021.

[10] Ala-Eddine Benrazek, Zineddine Kouahla, Brahim Farou, Mohamed Amine Ferrag, Hamid Seridi, and Muhammet Kurulay. An efficient indexing for internet of things massive data based on cloud-fog computing. *Transactions on Emerging Telecommunications Technologies*, 31(3) :e3868, 2020.

[11] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42 :120–134, 2014.

[12] Dave Evans. The internet of things : How the next evolution of the internet is changing everything. *CISCO white paper*, 1(2011) :1–11, 2011.

[13] Statista Research Department. Internet of things – number of connected devices worldwide 2015-2025, November 2016. Accessed : 2023-01-30.

[14] Ibtissem Kemouguette, Zineddine Kouahla, Ala-Eddine Benrazek, Brahim Farou, and Hamid Seridi. Cost-effective space partitioning approach for iot data indexing and retrieval. In *2021 International Conference on Networking and Advanced Systems (ICNAS)*, pages 1–6. IEEE, 2021.

[15] Irfan Saif, Sean Peasley, and Arun Perinkolam. Safeguarding the internet of things. *Deloitte Review*, 2015.

[16] Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer networks*, 57(10) :2266–2279, 2013.

[17] Fumie Ono, Hideki Ochiai, and Ryu Miura. A wireless relay network based on unmanned aircraft system with rate optimization. *IEEE Transactions on Wireless Communications*, 15(11) :7699–7708, 2016.

[18] R Kurt Barnhart, Douglas M Marshall, and Eric Shappee. *Introduction to unmanned aircraft systems*. Crc Press, 2021.

[19] Enric Pastor, Juan Lopez, and Pablo Royo. Uav payload and mission control hardware/software architecture. *IEEE Aerospace and Electronic Systems Magazine*, 22(6) :3–8, 2007.

[20] G Greco, C Lucianaz, S Bertoldo, and M Allegretti. Localization of rfid tags for environmental monitoring using uav. In *2015 IEEE 1st International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, pages 480–483. IEEE, 2015.

[21] Riham Altawy and Amr M Youssef. Security, privacy, and safety aspects of civilian drones : A survey. *ACM Transactions on Cyber-Physical Systems*, 1(2) :1–25, 2016.

[22] Yong Zeng, Rui Zhang, and Teng Joon Lim. Wireless communications with unmanned aerial vehicles : Opportunities and challenges. *IEEE Communications magazine*, 54(5) :36–42, 2016.

[23] Mithra Sivakumar and Naga Malleswari TYJ. A literature survey of unmanned aerial vehicle usage for civil applications. *Journal of Aerospace Technology and Management*, 13, 2021.

[24] Randal Beard, Derek Kingston, Morgan Quigley, Deryl Snyder, Reed Christiansen, Walt Johnson, Timothy McLain, and Michael Goodrich. Autonomous vehicle technologies for small fixed-wing uavs. *Journal of Aerospace Computing, Information, and Communication*, 2(1) :92–108, 2005.

[25] Jurgen Everaerts et al. The use of unmanned aerial vehicles (uavs) for remote sensing and mapping. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 37(2008) :1187–1192, 2008.

[26] E Ben-Dor. Quantitative remote sensing of soil properties. 2002.

[27] Sebastian Candiago, Fabio Remondino, Michaela De Giglio, Marco Dubbini, and Mario Gattelli. Evaluating multispectral images and vegetation indices for precision farming applications from uav images. *Remote sensing*, 7(4) :4026–4047, 2015.

[28] R Ehsani, S Sankaran, JM Maja, and J Camargo Neto. Affordable multi-rotor remote sensing platform for applications in precision horticulture. In *th International Conference on Precision Agriculture*, 2014.

[29] Ross Bryant, M Susan Moran, Stephen A McElroy, Chandra Holifield, Kurtis J Thome, Tomoaki Miura, and Stuart F Biggar. Data continuity of earth observing 1 (eo-1) advanced land i satellite imager (ali) and landsat tm and etm+. *IEEE transactions on geoscience and remote sensing*, 41(6) :1204–1214, 2003.

[30] Camille CD Lelong, Philippe Burger, Guillaume Jubelin, Bruno Roux, Sylvain Labbé, and Frédéric Baret. Assessment of unmanned aerial vehicles imagery for quantitative monitoring of wheat crop in small plots. *Sensors*, 8(5) :3557–3585, 2008.

[31] Rafael Coronel B Sampaio, André C Hernandes, Marcelo Becker, Fernando M Catalano, Fabio Zanini, Joao LEM Nobrega, and Caio Martins. Novel hybrid electric motor glider-quadrotor mav for in-flight/v-stol launching. In *2014 IEEE Aerospace Conference*, pages 1–12. IEEE, 2014.

[32] Ugur Ozdemir, Yucel Orkut Aktas, Aslihan Vuruskan, Yasin Dereli, Ahmed Farabi Tarhan, Karaca Demirbag, Ahmet Erdem, Ganime Duygu Kalaycioglu, Ibrahim Ozkol, and Gokhan Inalhan. Design of a commercial hybrid vtol uav system. *Journal of Intelligent & Robotic Systems*, 74 :371–393, 2014.

[33] Jacopo Primicerio, Salvatore Filippo Di Gennaro, Edoardo Fiorillo, Lorenzo Genesio, Emanuele Lugato, Alessandro Matese, and Francesco Primo Vaccari. A flexible unmanned aerial vehicle for precision agriculture. *Precision Agriculture*, 13(4) :517–523, 2012.

[34] P Spanoudakis, L Doitsidis, N Tsourveloudis, and K Valavanis. Vertical takeoff and landing vehicle market overview. *KOREA*, 1(4), 2003.

[35] Yanbo Huang, Steven J Thomson, W Clint Hoffmann, Yubin Lan, and Bradley K Fritz. Development and prospect of unmanned aerial vehicle technologies for agricultural production management. *International Journal of Agricultural and Biological Engineering*, 6(3) :1–10, 2013.

[36] Kimberly M Fornace, Chris J Drakeley, Timothy William, Fe Espino, and Jonathan Cox. Mapping infectious disease landscapes : unmanned aerial vehicles and epidemiology. *Trends in parasitology*, 30(11) :514–519, 2014.

[37] Hrvoje KUTNJAK, Josip LETO, Marina VRANIĆ, Krešimir BOŠNJAK, and Goran PERČULIJA. Potential of aerial robotics in crop production : high resolution nir/vis imagery obtained by automated unmanned aerial vehicle (uav) in estimation of botanical composition of alfalfa-grass. In *Proceedings. 50th Croatian and 10th International Symposium on Agriculture. Opatija. Croatia*, volume 349, page 353, 2015.

[38] Michael AA Fenelon and Tomonari Furukawa. Design of an active flapping wing mechanism and a micro aerial vehicle using a rotary actuator. *Mechanism and Machine Theory*, 45(2) :137–146, 2010.

[39] Wei Shyy, Yongsheng Lian, Jian Tang, Dragos Viieru, and Hao Liu. *Aerodynamics of low Reynolds number flyers*. 2008.

[40] KD Jones, CJ Bradshaw, J Papadopoulos, and MF Platzer. Bio-inspired design of flapping-wing micro air vehicles. *The Aeronautical Journal*, 109(1098) :385–393, 2005.

[41] Purvi M Joshi. wing analysis of a flapping wing unmanned aerial vehicle using cfd. *Development*, 2(5), 2015.

[42] Konstantin Schauwecker, Nan Rosemary Ke, Sebastian Andreas Scherer, and Andreas Zell. Markerless visual control of a quad-rotor micro aerial vehicle by means of on-board stereo processing. In *Autonomous Mobile Systems 2012 : 22. Fachgespräch Stuttgart, 26. bis 28. September 2012*, pages 11–20. Springer, 2012.

[43] Muhammad Asghar Khan, Ijaz Mansoor Qureshi, and Fahimullah Khanzada. A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (fanet). *Drones*, 3(1) :16, 2019.

[44] Mirmojtaba Gharibi, Raouf Boutaba, and Steven L Waslander. Internet of drones. *IEEE Access*, 4 :1148–1162, 2016.

[45] Gaurav Choudhary, Vishal Sharma, Takshi Gupta, Jiyoon Kim, and Ilsun You. Internet of drones (iod) : threats, vulnerability, and security perspectives. *arXiv preprint arXiv :1808.00203*, 2018.

[46] Giovanni Iacovelli, Pietro Boccadoro, and Luigi Alfredo Grieco. An iterative stochastic approach to constrained drones' communications. In *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, pages 1–8. IEEE, 2020.

[47] Danil Vasiliev, Andrei Chunaev, Albert Abilov, Irina Kaysina, and Daniil Meitis. Application layer arq and network coding for qos improving in uav-assisted networks. In *2019 25th Conference of Open Innovations Association (FRUCT)*, pages 353–360. IEEE, 2019.

[48] Bertold Van den Bergh, Alessandro Chiumento, and Sofie Pollin. Ultra-reliable ieee 802.11 for uav video streaming : from network to application. In *Advances in Ubiquitous Networking 2 : Proceedings of the UNet'16 2*, pages 637–647. Springer, 2017.

[49] Theodore Zahariadis, Artemis Voulkidis, Panagiotis Karkazis, and Panagiotis Trakadas. Preventive maintenance of critical infrastructures using 5g networks & drones.

In *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 1–4. IEEE, 2017.

[50] Emad Ebeid, Martin Skriver, Kristian Husum Terkildsen, Kjeld Jensen, and Ulrik Pagh Schultz. A survey of open-source uav flight controllers and flight simulators. *Microprocessors and Microsystems*, 61 :11–20, 2018.

[51] Ali Alnoman and Alagan Anpalagan. On d2d communications for public safety applications. In *2017 IEEE Canada international humanitarian technology conference (IHTC)*, pages 124–127. IEEE, 2017.

[52] Anis Koubâa, Basit Qureshi, Mohamed-Foued Sriti, Yasir Javed, and Eduardo Tovar. A service-oriented cloud-based management system for the internet-of-drones. In *2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, pages 329–335. IEEE, 2017.

[53] Hamid Menouar, Ismail Guvenc, Kemal Akkaya, A Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer. Uav-enabled intelligent transportation systems for the smart city : Applications and challenges. *IEEE Communications Magazine*, 55(3) :22–28, 2017.

[54] Aníbal Ollero and Iván Maza. *Multiple heterogeneous unmanned aerial vehicles*, volume 37. Springer, 2007.

[55] Rodolphe Jobard. *Les drones : La nouvelle révolution.* Editions Eyrolles, 2014.

[56] Phuoc Luong. Securing embedded systems for autonomous aerial vehicles. *Worcester Polytechnic Institute*, 2013.

[57] Mohamed Alzenad, Muhammad Z Shakir, Halim Yanikomeroglu, and Mohamed-Slim Alouini. Fso-based vertical backhaul/fronthaul framework for 5g+ wireless networks. *IEEE Communications Magazine*, 56(1) :218–224, 2018.

[58] Ahmed Bader and Mohamed-Slim Alouini. An ultra-low-latency geo-routing scheme for team-based unmanned vehicular applications. In *2015 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2015.

[59] Ludovico Ferranti, Francesca Cuomo, Stefania Colonnese, and Tommaso Melodia. Duplicate : Drone cellular networks : Enhancing the quality of experience of video streaming applications. *Ad hoc networks*, 80 :130–141, 2018.

[60] Walid Saad, Mehdi Bennis, and Mingzhe Chen. A vision of 6g wireless systems : Applications, trends, technologies, and open research problems. *IEEE network*, 34(3) :134–142, 2019.

[61] Daniele Giovanni Cileo, Navuday Sharma, and Maurizio Magarini. Coverage, capacity and interference analysis for an aerial base station in different environments. In *2017 International Symposium on Wireless Communication Systems (ISWCS)*, pages 281–286. IEEE, 2017.

[62] Hamid Shoja, Hossein Nahid, and Reza Azizi. A comparative survey on load balancing algorithms in cloud computing. In *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, pages 1–5. IEEE, 2014.

[63] Stefania Colonnese, Andrea Carlesimo, Lorenzo Brigato, and Francesca Cuomo. Qoe-aware uav flight path design for mobile video streaming in hetnet. In *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, pages 301–305. IEEE, 2018.

[64] Xiaoli Wang, Aakanksha Chowdhery, and Mung Chiang. Networked drone cameras for sports streaming. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 308–318. IEEE, 2017.

[65] Javier Irizarry, Masoud Gheisari, and Bruce N Walker. Usability assessment of drone technology as safety inspection tools. *Journal of Information Technology in Construction (ITcon)*, 17(12) :194–212, 2012.

[66] Jiyoon Park, Solhee Kim, and Kyo Suh. A comparative analysis of the environmental benefits of drone-based delivery services in urban and rural areas. *Sustainability*, 10(3) :888, 2018.

[67] Konstantin A Vytovtov, Elizaveta A Barabanova, Tatiana Ya Gladkikh, Anastasia L Kulina, and Georgii K Vytovtov. Remote monitoring of water pollution with oil products in the visible range by using uav multispectral camera. In *2022 International Conference on Information, Control, and Communication Technologies (ICCT)*, pages 1–5. IEEE, 2022.

[68] Scott Lobermeier, Matthew Moldenhauer, Christopher M Peter, Luke Slominski, Richard A Tedesco, Marcus Ver Meer, James F Dwyer, Richard E Harness, and Andrew H Stewart. Mitigating avian collision with power lines : a proof of concept

for installation of line markers via unmanned aerial vehicle. *Journal of Unmanned Vehicle Systems*, 3(4) :252–258, 2015.

[69] Lucila Dunnington and Masami Nakagawa. Fast and safe gas detection from underground coal fire by drone fly over. *Environmental Pollution*, 229 :139–145, 2017.

[70] Sung-Chan Choi, Nak-Myung Sung, Jong-Hong Park, Il-Yeop Ahn, and Jaeho Kim. Enabling drone as a service : Onem2m-based uav/drone management system. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 18–20. IEEE, 2017.

[71] Hamed Hellaoui, Oussama Bekkouche, Miloud Bagaa, and Tarik Taleb. Aerial control system for spectrum efficiency in uav-to-cellular communications. *IEEE Communications Magazine*, 56(10) :108–113, 2018.

[72] Qiang Fan and Nirwan Ansari. Towards traffic load balancing in drone-assisted communications for iot. *IEEE Internet of Things Journal*, 6(2) :3633–3640, 2018.

[73] Bin Jiang, Jiachen Yang, Huifang Xu, Houbing Song, and Gan Zheng. Multimedia data throughput maximization in internet-of-things system based on optimization of cache-enabled uav. *IEEE Internet of Things Journal*, 6(2) :3525–3532, 2018.

[74] Naser Hossein Motlagh, Miloud Bagaa, and Tarik Taleb. Uav selection for a uav-based integrative iot platform. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[75] Shi Yan, Mugen Peng, and Xueyan Cao. A game theory approach for joint access selection and resource allocation in uav assisted iot communication networks. *IEEE Internet of Things Journal*, 6(2) :1663–1674, 2018.

[76] Hyunbum Kim and Jalel Ben-Othman. A collision-free surveillance system using smart uavs in multi domain iot. *IEEE communications letters*, 22(12) :2587–2590, 2018.

[77] Vijaya Yajnanarayana, Y-P Eric Wang, Shiwei Gao, Siva Muruganathan, and Xingqin Lin Ericsson. Interference mitigation methods for unmanned aerial vehicles served by cellular networks. In *2018 IEEE 5G World Forum (5GWF)*, pages 118–122. IEEE, 2018.

[78] Rafhael Amorim, Huan Nguyen, Jeroen Wigard, István Z Kovács, Troels B Sørensen, David Z Biro, Mads Sørensen, and Preben Mogensen. Measured uplink interference

caused by aerial vehicles in lte cellular networks. *IEEE Wireless Communications Letters*, 7(6) :958–961, 2018.

[79] Ursula Challita, Walid Saad, and Christian Bettstetter. Deep reinforcement learning for interference-aware path planning of cellular-connected uavs. In *2018 IEEE international conference on communications (ICC)*, pages 1–7. IEEE, 2018.

[80] Qin Yang and Sang-Jo Yoo. Optimal uav path planning : Sensing data acquisition over iot sensor networks using multi-objective bio-inspired algorithms. *IEEE access*, 6 :13671–13684, 2018.

[81] Sang-Jo Yoo, Jae-hyun Park, Su-hee Kim, and Anish Shrestha. Flying path optimization in uav-assisted iot sensor networks. *ICT Express*, 2(3) :140–144, 2016.

[82] Mohamed A Abd-Elmagid and Harpreet S Dhillon. Average peak age-of-information minimization in uav-assisted iot networks. *IEEE Transactions on Vehicular Technology*, 68(2) :2003–2008, 2018.

[83] Sherin Abdelhamid. Uav path planning for emergency management in iot. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2018.

[84] Shuowen Zhang, Yong Zeng, and Rui Zhang. Cellular-enabled uav communication : A connectivity-constrained trajectory optimization perspective. *IEEE Transactions on Communications*, 67(3) :2580–2604, 2018.

[85] Vishal Sharma, Fei Song, Ilsun You, and Mohammed Atiquzzaman. Energy efficient device discovery for reliable communication in 5g-based iot and bsns using unmanned aerial vehicles. *Journal of Network and Computer Applications*, 97 :79–95, 2017.

[86] Sara Handouf, Essaid Sabir, and Mohammed Sadik. Energy-throughput tradeoffs in ubiquitous flying radio access network for iot. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 320–325. IEEE, 2018.

[87] Dimitrios Sikeridis, Eirini Eleni Tsiropoulou, Michael Devetsikiotis, and Symeon Papavassiliou. Wireless powered public safety iot : A uav-assisted adaptive-learning approach towards energy efficiency. *Journal of Network and Computer Applications*, 123 :69–79, 2018.

[88] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Mérouane Debbah. Mobile internet of things : Can uavs provide an energy-efficient mobile architecture ? In

2016 IEEE global communications conference (GLOBECOM), pages 1–6. IEEE, 2016.

[89] Jacob Chakareski, Syed Naqvi, Nicholas Mastronarde, Jie Xu, Fatemeh Afghah, and Abolfazl Razi. An energy efficient framework for uav-assisted millimeter wave 5g heterogeneous cellular networks. *IEEE Transactions on Green Communications and Networking*, 3(1) :37–44, 2019.

[90] Abdullah M Almasoud and Ahmed E Kamal. Data dissemination in iot using a cognitive uav. *IEEE Transactions on Cognitive Communications and Networking*, 5(4) :849–862, 2019.

[91] Jianwei Zhao, Feifei Gao, Qihui Wu, Shi Jin, Yi Wu, and Weimin Jia. Beam tracking for uav mounted satcom on-the-move with massive antenna array. *IEEE Journal on Selected Areas in Communications*, 36(2) :363–375, 2018.

[92] Mi Li, Yifeng Hong, Cheng Zeng, Yuejiang Song, and Xuping Zhang. Investigation on the uav-to-satellite optical communication systems. *IEEE Journal on Selected Areas in Communications*, 36(9) :2128–2138, 2018.

[93] Meng Hua, Yi Wang, Min Lin, Chunguo Li, Yongming Huang, and Luxi Yang. Joint comp transmission for uav-aided cognitive satellite terrestrial networks. *IEEE Access*, 7 :14959–14968, 2019.

[94] Mario Marchese, Aya Moheddine, and Fabio Patrone. Iot and uav integration in 5g hybrid terrestrial-satellite networks. *Sensors*, 19(17) :3704, 2019.

[95] Bin Li, Zesong Fei, Yan Zhang, and Mohsen Guizani. Secure uav communication networks over 5g. *IEEE Wireless Communications*, 26(5) :114–120, 2019.

[96] Hyunbum Kim, Jalel Ben-Othman, Lynda Mokdad, Sungrae Cho, and Paolo Bellavista. On collision-free reinforced barriers for multi domain iot with heterogeneous uavs. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pages 466–471. IEEE, 2017.

[97] Howie Choset. Coverage for robotics–a survey of recent results. *Annals of mathematics and artificial intelligence*, 31 :113–126, 2001.

[98] Håvard Lægreid Andersen. Path planning for search and rescue mission using multicopters. Master's thesis, Institutt for teknisk kybernetikk, 2014.

[99] Dimitrios Koutsonikolas, Saumitra M Das, and Y Charlie Hu. Path planning of mobile landmarks for localization in wireless sensor networks. *Computer Communications*, 30(13) :2577–2592, 2007.

[100] David Hilbert. Analysis, grundlagen der mathematik, physik verschiedenes, nebst einer lebensgeschichte. *(No Title)*.

[101] Farhanda Javed, Samiullah Khan, Asfandyar Khan, Alweena Javed, Rohi Tariq, Matiullah, and Faheem Khan. On precise path planning algorithm in wireless sensor network. *International journal of distributed sensor networks*, 14(7) :1550147718783385, 2018.

[102] Hans Sagan. *Space-filling curves*. Springer Science & Business Media, 2012.

[103] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor. Airsim : High-fidelity visual and physical simulation for autonomous vehicles. In *Field and Service Robotics : Results of the 11th International Conference*, pages 621–635. Springer, 2018.

[104] Chia-Chang Chuang, Jiann-Yeou Rau, Meng-Kuan Lai, and Chung-Liang Shih. Combining unmanned aerial vehicles, and internet protocol cameras to reconstruct 3-d disaster scenes during rescue operations. *Prehospital Emergency Care*, 2018.

[105] Lucio R Ribeiro and Neusa Maria F Oliveira. Uav autopilot controllers test platform using matlab/simulink and x-plane. In *2010 IEEE Frontiers in Education Conference (FIE)*, pages S2H–1. IEEE, 2010.

[106] Emerson A Marconato, Daniel F Pigatto, Kalinka RLJC Branco, and Luiz Henrique C Branco. Larissa : Layered architecture model for interconnection of systems in uas. In *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 20–31. IEEE, 2014.

[107] Emerson Alberto Marconato, Mariana Rodrigues, Rayner de Melo Pires, Daniel Fernando Pigatto, Alex Roschildt Pinto, Kalinka RLJC Branco, et al. Avens-a novel flying ad hoc network simulator with automatic code generation for unmanned aircraft system. 2017.

[108] Fadri Furrer, Michael Burri, Markus Achtelik, and Roland Siegwart. Rotors—a modular gazebo mav simulator framework. *Robot Operating System (ROS) The Complete Reference (Volume 1)*, pages 595–625, 2016.

[109] Ahmad Javaid, Weiqing Sun, and Mansoor Alam. Uavnet simulation in uavsim : A performance evaluation and enhancement. In *Testbeds and Research Infrastructure : Development of Networks and Communities : 9th International ICST Conference, TridentCom 2014, Guangzhou, China, May 5-7, 2014, Revised Selected Papers 9*, pages 107–115. Springer, 2014.

[110] Ahmad Yazdan Javaid. *Cyber security threat analysis and attack simulation for unmanned aerial vehicle network*. PhD thesis, University of Toledo, 2015.

[111] Ahmad Y Javaid, Weiqing Sun, and Mansoor Alam. Uavsim : A simulation testbed for unmanned aerial vehicle network cyber security analysis. In *2013 ieee globecom workshops (gc wkshps)*, pages 1432–1436. IEEE, 2013.

[112] Farha Jahan. *Implementation of GNSS/GPS navigation and its attacks in UAVSim Testbed*. The University of Toledo, 2015.

[113] Ahmad Y Javaid, Farha Jahan, and Weiqing Sun. Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation. *Simulation*, 93(5) :427–441, 2017.

[114] Stephen Cameron, Stephen Hailes, Simon Julier, Sally McClean, Gerard Parr, Niki Trigoni, Mohamed Ahmed, Graeme McPhillips, Renzo De Nardi, Julia Nie, et al. Suaave : Combining aerial robots and wireless networking. 2010.

[115] Ilker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. Flying ad-hoc networks (fanets) : A survey. *Ad Hoc Networks*, 11(3) :1254–1270, 2013.

[116] Elisa Capello, Giorgio Guglieri, and Fulvia B Quagliotti. Uavs and simulation : an experience on mavs. *Aircraft Engineering and Aerospace Technology*, 81(1) :38–50, 2009.

[117] Matthias Mueller, Vincent Casser, Jean Lahoud, Neil Smith, and Bernard Ghanem. Ue4sim : A photo-realistic simulator for computer vision applications. 2017.

[118] Matthew Leccadito, Tim Bakker, Robert Klenke, and Carl Elks. A survey on securing uas cyber physical systems. *IEEE Aerospace and Electronic Systems Magazine*, 33(10) :22–32, 2018.

[119] Chao Lin, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, Alexey Vinel, and Xinyi Huang. Security and privacy for the internet of drones : Challenges and solutions. *IEEE Communications Magazine*, 56(1) :64–69, 2018.

[120] Katrina Mansfield, Timothy Eveleigh, Thomas H Holzer, and Shahryar Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, pages 722–728. IEEE, 2013.

[121] Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, and Mansoor Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 585–590. IEEE, 2012.

[122] Mark Yampolskiy, Peter Horvath, Xenofon D Koutsoukos, Yuan Xue, and Janos Sztipanovits. Taxonomy for description of cross-domain attacks on cps. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, pages 135–142, 2013.

[123] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18(3) :2027–2051, 2016.

[124] Nils Miro Rodday, Ricardo de O Schmidt, and Aiko Pras. Exploring security vulnerabilities of unmanned aerial vehicles. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*, pages 993–994. IEEE, 2016.

[125] Vishal Sharma, Gaurav Choudhary, Ilsun You, Jae Deok Lim, and Jeong Nyeo Kim. Self-enforcing game theory-based resource allocation for lorawan assisted public safety communications. *arXiv preprint arXiv :1804.07204*, 2018.

[126] Sait Murat Giray. Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In *2013 6th International Conference on Recent Advances in Space Technologies (RAST)*, pages 795–800. IEEE, 2013.

[127] Sourabh Bhattacharya and Tamer Başar. Game-theoretic analysis of an aerial jamming attack on a uav communication network. In *proceedings of the 2010 American control conference*, pages 818–823. IEEE, 2010.

[128] Vikas Hassija, Vinay Chamola, Adhar Agrawal, Adit Goyal, Nguyen Cong Luong, Dusit Niyato, Fei Richard Yu, and Mohsen Guizani. Fast, reliable, and secure drone communication : A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(4) :2802–2832, 2021.

[129] Menaka Pushpa Arthur. Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids. In *2019 international conference on computer, information and telecommunication systems (CITS)*, pages 1–5. IEEE, 2019.

[130] Benjamin Tan, Ramesh Karri, Nimisha Limaye, Abhrajit Sengupta, Ozgur Sinanoglu, Md Moshiur Rahman, Swarup Bhunia, Danielle Duvalsaint, Amin Rezaei, Yuanqi Shen, et al. Benchmarking at the frontier of hardware security : Lessons from logic locking. *arXiv preprint arXiv :2006.06806*, 2020.

[131] Raja Naeem Akram, Konstantinos Markantonakis, Keith Mayes, Oussama Habachi, Damien Sauveron, Andreas Steyven, and Serge Chaumette. Security, privacy and safety evaluation of dynamic and static fleets of drones. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, pages 1–12. IEEE, 2017.

[132] Abdulhadi Shoufan, Chan Yeob Yeun, and Bilal Taha. esim-based authentication protocol for uav remote identification. *Security and Privacy in the Internet of Things : Architectures, Techniques, and Applications*, pages 91–122, 2021.

[133] Sajal K Das, Krishna Kant, and Nan Zhang. *Handbook on securing cyber-physical critical infrastructure*. Elsevier, 2012.

[134] Umut Can Cabuk, Gokhan Dalkilic, and Orhan Dagdeviren. Comad : Context-aware mutual authentication protocol for drone networks. *IEEE Access*, 9 :78400–78414, 2021.

[135] Cristina Pauner, Irene Kamara, and Jorge Viguri. Drones. current challenges and standardisation solutions in the field of privacy and data protection. In *2015 ITU Kaleidoscope : Trust in the Information Society (K-2015)*, pages 1–7. IEEE, 2015.

[136] Dimitrios Konstantinidis, Vasileios Argyriou, Tania Stathaki, and Nikolaos Grammalidis. A modular cnn-based building detector for remote sensing images. *Computer networks*, 168 :107034, 2020.

[137] Muktar Yahuza, Mohd Yamani Idna Idris, Ismail Bin Ahmedy, Ainuddin Wahid Abdul Wahab, Tarak Nandy, Noorzaily Mohamed Noor, and Abubakar Bala. Internet of drones security and privacy issues : Taxonomy and open challenges. *IEEE Access*, 9 :57243–57270, 2021.

[138] Hanae Nozaki, Masahiko Motoyama, Atsushi Shimbo, and Shinichi Kawamura. Implementation of rsa algorithm based on rns montgomery multiplication. In *Cryptographic Hardware and Embedded Systems—CHES 2001 : Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*, pages 364–376. Springer, 2001.

[139] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4 :161–174, 1991.

[140] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4) :469–472, 1985.

[141] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *Advances in Cryptology—CRYPTO'96 : 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, pages 1–15. Springer, 1996.

[142] Robert R Jueneman, Stephen M Matyas, and Carl H Meyer. Message authentication with manipulation detection code. In *1983 IEEE Symposium on Security and Privacy*, pages 33–33. IEEE, 1983.

[143] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 33–43, 1989.

[144] Ralph C Merkle. One way hash functions and des. In *Advances in Cryptology—CRYPTO'89 Proceedings*, pages 428–446. Springer, 2001.

[145] Saeed H Alsamhi, Ou Ma, Mohammad Samar Ansari, and Faris A Almalki. Survey on collaborative smart drones and internet of things for improving smartness of smart cities. *Ieee Access*, 7 :128125–128152, 2019.

[146] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval. Provably authenticated group diffie-hellman key exchange—the dynamic case. In *Advances in Cryptology—ASIACRYPT 2001 : 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings*, pages 290–309. Springer, 2001.

[147] Guangcan Mai, Kai Cao, Xiangyuan Lan, and Pong C Yuen. Secureface : Face template protection. *IEEE Transactions on Information Forensics and security*, 16 :262–277, 2020.

[148] Wencheng Yang, Song Wang, Guanglou Zheng, Junaid Chaudhry, and Craig Valli. Ecb4ci : An enhanced cancelable biometric system for securing critical infrastructures. *The Journal of Supercomputing*, 74 :4893–4909, 2018.

[149] Wencheng Yang, Song Wang, Jiankun Hu, Ahmed Ibrahim, Guanglou Zheng, Marcelo Jose Macedo, Michael N Johnstone, and Craig Valli. A cancelable iris-and steganography-based user authentication system for the internet of things. *Sensors*, 19(13) :2985, 2019.

[150] Axel Moinet, Benoît Darties, and Jean-Luc Baril. Blockchain based trust & authentication for decentralized sensor networks. *arXiv preprint arXiv :1706.01730*, 2017.

[151] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of trust : A decentralized blockchain-based authentication system for iot. *Computers & Security*, 78 :126–142, 2018.

[152] Chao Lin, Debiao He, Neeraj Kumar, Xinyi Huang, Pandi Vijayakumar, and Kim-Kwang Raymond Choo. Homechain : A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 7(2) :818–829, 2019.

[153] Sunghyuck Hong. P2p networking based internet of things (iot) sensor node authentication by blockchain. *Peer-to-Peer Networking and Applications*, 13(2) :579–589, 2020.

[154] Umair Khalid, Muhammad Asim, Thar Baker, Patrick CK Hung, Muhammad Adnan Tariq, and Laura Rafferty. A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Cluster Computing*, 23(3) :2067–2087, 2020.

[155] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec : Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)*, pages 25–30. IEEE, 2016.

[156] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. Blockchain-based decentralized trust management in vehicular networks. *IEEE internet of things journal*, 6(2) :1495–1505, 2018.

[157] Vishal Sharma, Ilsun You, and Gökhan Kul. Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain. In *Proceedings of the 2017 international workshop on managing insider security threats*, pages 81–84, 2017.

[158] Emmanouel T Michailidis and Demosthenes Vouyioukas. A review on software-based and hardware-based authentication mechanisms for the internet of drones. *Drones*, 6(2) :41, 2022.

[159] Mohammad Wazid, Ashok Kumar Das, and Jong-Hyouk Lee. Authentication protocols for the internet of drones : taxonomy, analysis and future directions. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–10, 2018.

[160] Laith Abualigah, Ali Diabat, Putra Sumari, and Amir H Gandomi. Applications, deployments, and integration of internet of drones (iod) : a review. *IEEE Sensors Journal*, 21(22) :25532–25546, 2021.

[161] Abdelouahid Derhab, Mohamed Guerroumi, Abdu Gumaei, Leandros Maglaras, Mohamed Amine Ferrag, Mithun Mukherjee, and Farrukh Aslam Khan. Blockchain and random subspace learning-based ids for sdn-enabled industrial iot security. *Sensors*, 19(14) :3119, 2019.

[162] Adnan Shahid Khan, Muhammad Ali Sattar, Kashif Nisar, Ag Asri Ag Ibrahim, Noralifah Binti Annuar, Johari bin Abdullah, and Shuaib Karim Memon. A survey on 6g enabled light weight authentication protocol for uavs, security, open research issues and future directions. *Applied Sciences*, 13(1) :277, 2023.

[163] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V Vasilakos, and Joel JPC Rodrigues. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet of Things Journal*, 6(2) :3572–3584, 2018.

[164] Jangirala Srinivas, Ashok Kumar Das, Neeraj Kumar, and Joel JPC Rodrigues. Tcalas : Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. *IEEE Transactions on Vehicular Technology*, 68(7) :6903–6916, 2019.

[165] Shuangyu He, Qianhong Wu, Jingwen Liu, Wei Hu, Bo Qin, and Ya-Nan Li. Secure communications in unmanned aerial vehicle network. In *International Conference on Information Security Practice and Experience*, pages 601–620. Springer, 2017.

[166] Benjamin Semal, Konstantinos Markantonakis, and Raja Naeem Akram. A certificateless group authenticated key agreement protocol for secure communication in untrusted uav networks. In *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pages 1–8. IEEE, 2018.

[167] Liquan Chen, Sijie Qian, Ming Lim, and Shihui Wang. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems. *China Communications*, 15(5) :61–76, 2018.

[168] Chin-Ling Chen, Yong-Yuan Deng, Wei Weng, Chi-Hua Chen, Yi-Jui Chiu, and Chih-Ming Wu. A traceable and privacy-preserving authentication for uav communication control system. *Electronics*, 9(1) :62, 2020.

[169] Sana Benzarti, Bayrem Triki, and Ouajdi Korbaa. Privacy preservation and drone authentication using id-based signcryption. In *SoMeT*, pages 226–239, 2018.

[170] Yunmok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. Gyrosfinger : Fingerprinting drones for location tracking based on the outputs of mems gyroscopes. *ACM Transactions on Privacy and Security (TOPS)*, 21(2) :1–25, 2018.

[171] Soundarya Ramesh, Thomas Pathier, and Jun Han. Sounduav : Towards delivery drone authentication via acoustic noise fingerprinting. In *Proceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, pages 27–32, 2019.

[172] Mehdi Karimibiuki, Michal Aibin, Yuyu Lai, Raziq Khan, Ryan Norfield, and Aaron Hunter. Drones' face off : Authentication by machine learning in autonomous iot systems. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0329–0333. IEEE, 2019.

[173] Changjun Jiang, Yu Fang, Peihai Zhao, and John Panneerselvam. Intelligent uav identity authentication and safety supervision based on behavior modeling and prediction. *IEEE Transactions on Industrial Informatics*, 16(10) :6652–6662, 2020.

[174] Xinghua Li, Yunwei Wang, Pandi Vijayakumar, Debiao He, Neeraj Kumar, and Jianfeng Ma. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. *IEEE Transactions on Vehicular Technology*, 68(11) :11309–11322, 2019.

[175] Basudeb Bera, Anusha Vangala, Ashok Kumar Das, Pascal Lorenz, and Muhammad Khurram Khan. Private blockchain-envisioned drones-assisted authentication scheme in iot-enabled agricultural environment. *Computer Standards & Interfaces*, 80 :103567, 2022.

[176] Muhammad Tanveer, Ahmed Alkhayyat, Alamgir Naushad, Neeraj Kumar, Abdullah G Alharbi, et al. Ruam-iod : A robust user authentication mechanism for the internet of drones. *IEEE Access*, 10 :19836–19851, 2022.

[177] Azade Fotouhi, Haoran Qiang, Ming Ding, Mahbub Hassan, Lorenzo Galati Giordano, Adrian Garcia-Rodriguez, and Jinhong Yuan. Survey on uav cellular communications : Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications surveys & tutorials*, 21(4) :3417–3442, 2019.

[178] Sven Mayer, Lars Lischke, and Paweł W Woźniak. Drones for search and rescue. In *1st International Workshop on Human-Drone Interaction*, 2019.

[179] Abdelzahir Abdelmaboud. The internet of drones : Requirements, taxonomy, recent advances, and challenges of research trends. *Sensors*, 21(17) :5718, 2021.

[180] Wencheng Yang, Song Wang, Jiankun HuHu, and Nickson M Karie. Multimedia security and privacy protection in the internet of things : research developments and challenges. *International Journal of Multimedia Intelligence and Security*, 4(1) :20–46, 2022.

[181] Ala-Eddine Benrazek, Farou Brahim, and Kurulay Muhammet. Efficient camera clustering method based on overlapping fovs for wmsns. *International Journal of Informatics and Applied Mathematics*, 1(1) :10–23, 2019.

[182] Milan Erdelj, Michał Król, and Enrico Natalizio. Wireless sensor networks and multi-uav systems for natural disaster management. *Computer Networks*, 124 :72–86, 2017.

[183] Milan Erdelj, Enrico Natalizio, Kaushik R Chowdhury, and Ian F Akyildiz. Help from the sky : Leveraging uavs for disaster management. *IEEE Pervasive Computing*, 16(1) :24–32, 2017.

[184] David C Schedl, Indrajit Kurmi, and Oliver Bimber. An autonomous drone for search and rescue in forests using airborne optical sectioning. *Science Robotics*, 6(55) :eabg1188, 2021.

[185] Nicola Basilico and Stefano Carpin. Deploying teams of heterogeneous uavs in cooperative two-level surveillance missions. In *2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 610–615. IEEE, 2015.

[186] N Padmapriya, R Aswini, and P Kanimozhi. Using drones in smart farming. In *Artificial Intelligence and IoT-Based Technologies for Sustainable Farming and Smart Agriculture*, pages 255–272. IGI Global, 2021.

[187] Mohamed Amine Ferrag, Lei Shu, Xing Yang, Abdelouahid Derhab, and Leandros Maglaras. Security and privacy for green iot-based agriculture : Review, blockchain solutions, and challenges. *IEEE access*, 8 :32031–32053, 2020.

[188] Shidrokh Goudarzi, Nazri Kama, Mohammad Hossein Anisi, Sherali Zeadally, and Shahid Mumtaz. Data collection using unmanned aerial vehicles for internet of things platforms. *Computers & Electrical Engineering*, 75 :1–15, 2019.

[189] Emmanuel Kieffer, Grégoire Danoy, Pascal Bouvry, and Anass Nagih. Hybrid mobility model with pheromones for uav detection task. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1–8. IEEE, 2016.

[190] JF Araujo, PB Sujit, and João B Sousa. Multiple uav area decomposition and coverage. In *2013 IEEE symposium on computational intelligence for security and defense applications (CISDA)*, pages 30–37. IEEE, 2013.

[191] Joao Valente, David Sanz, Jaime Del Cerro, Antonio Barrientos, and Miguel Ángel de Frutos. Near-optimal coverage trajectories for image mosaicing using a mini quad-rotor over irregular-shaped fields. *Precision agriculture*, 14(1) :115–132, 2013.

[192] LH Nam, Loulin Huang, Xue Jun Li, and JF Xu. An approach for coverage path planning for uavs. In *2016 IEEE 14th international workshop on advanced motion control (AMC)*, pages 411–416. IEEE, 2016.

[193] Taua M Cabreira, Carmelo Di Franco, Paulo R Ferreira, and Giorgio C Buttazzo. Energy-aware spiral coverage path planning for uav photogrammetric applications. *IEEE Robotics and Automation Letters*, 3(4) :3662–3668, 2018.

[194] Alia Ghaddar and Ahmad Merei. Energy-aware grid based coverage path planning for uavs. In *Proceedings of the Thirteenth International Conference on Sensor Technologies and Applications SENSORCOMM, Nice, France*, pages 27–31, 2019.

[195] Jose Joaquin Acevedo, Begoña C Arrue, Ivan Maza, and Anibal Ollero. Distributed approach for coverage and patrolling missions with a team of heterogeneous aerial robots under communication constraints. *International Journal of Advanced Robotic Systems*, 10(1) :28, 2013.

[196] Gustav Öst. Search path generation with uav applications using approximate convex decomposition, 2012.

[197] Wu Yue and Zhu Jiang. Path planning for uav to collect sensors data based on spiral decomposition. *Procedia computer science*, 131 :873–879, 2018.

[198] Oleksandr Artemenko, Omachonu Joshua Dominic, Oleksandr Andryeyev, and Andreas Mitschele-Thiel. Energy-aware trajectory planning for the localization of mobile devices using an unmanned aerial vehicle. In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–9. IEEE, 2016.

[199] Carmelo Di Franco and Giorgio Buttazzo. Energy-aware coverage path planning of uavs. In *2015 IEEE international conference on autonomous robot systems and competitions*, pages 111–117. IEEE, 2015.

[200] Marina Torres, David A Pelta, José L Verdegay, and Juan C Torres. Coverage path planning with unmanned aerial vehicles for 3d terrain reconstruction. *Expert Systems with Applications*, 55 :441–451, 2016.

[201] Deshi Li, Xiaoliang Wang, and Tao Sun. Energy-optimal coverage path planning on topographic map for environment survey with unmanned aerial vehicles. *Electronics Letters*, 52(9) :699–701, 2016.

[202] C Nattero, CT Recchiuto, A Sgorbissa, and F Wanderlingh. Coverage algorithms for search and rescue with uav drones. In *Workshop of the XIII AIIA Symposium on Artificial Intelligence, Pisa*, 2014.

[203] Aicha Idriss Hentati, Lobna Krichen, Mohamed Fourati, and Lamia Chaari Fourati. Simulation tools, environments and frameworks for uav systems performance analysis. In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 1495–1500. IEEE, 2018.

[204] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. *Ad Hoc Networks*, 20 :96–112, 2014.

[205] Yunru Zhang, Debiao He, Li Li, and Biwen Chen. A lightweight authentication and key agreement scheme for internet of drones. *Computer Communications*, 154 :455–464, 2020.

[206] Mohammad Sabzinejad Farash, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Networks*, 36 :152–176, 2016.

[207] Ruhul Amin, SK Hafizul Islam, GP Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, 101 :42–62, 2016.

[208] Sravani Challa, Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Alavalapati Goutham Reddy, Eun-Jun Yoon, and Kee-Young Yoo. Secure signature-based

authenticated key establishment scheme for future iot applications. *Ieee Access*, 5 :3028–3043, 2017.

[209] Xiaoying Jia, Debiao He, Li Li, and Kim-Kwang Raymond Choo. Signature-based three-factor authenticated key exchange for internet of things applications. *Multimedia Tools and Applications*, 77 :18355–18382, 2018.

[210] Muhammad Tanveer, Amjad Hussain Zahid, Musheer Ahmad, Abdullah Baz, and Hosam Alhakami. Lake-iod : Lightweight authenticated key exchange protocol for the internet of drone environment. *IEEE Access*, 8 :155645–155659, 2020.

[211] Tejasvi Alladi, Vinay Chamola, Neeraj Kumar, et al. Parth : A two-stage lightweight mutual authentication protocol for uav surveillance networks. *Computer Communications*, 160 :81–90, 2020.

[212] Zeeshan Ali, Shehzad Ashraf Chaudhry, Muhammad Sher Ramzan, and Fadi Al-Turjman. Securing smart city surveillance : A lightweight authentication mechanism for unmanned vehicles. *IEEE Access*, 8 :43711–43724, 2020.

[213] Geumhwan Cho, Junsung Cho, Sangwon Hyun, and Hyoungshick Kim. Sentinel : A secure and efficient authentication framework for unmanned aerial vehicles. *Applied Sciences*, 10(9) :3149, 2020.

[214] Yoney Kirsal Ever. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Computer Communications*, 155 :143–149, 2020.

[215] Basudeb Bera, Durbadal Chattaraj, and Ashok Kumar Das. Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment. *Computer Communications*, 153 :229–249, 2020.

[216] Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, 69(8) :9097–9111, 2020.

[217] Mahdi Nikooghadam, Haleh Amintoosi, SK Hafizul Islam, and Mostafa Farhadi Moghadam. A provably secure and lightweight authentication scheme for internet of drones for smart city surveillance. *Journal of Systems Architecture*, 115 :101955, 2021.

[218] Sajid Hussain, Khalid Mahmood, Muhammad Khurram Khan, Chien-Ming Chen, Bander A Alzahrani, and Shehzad Ashraf Chaudhry. Designing secure and lightweight user access to drone for smart city surveillance. *Computer Standards & Interfaces*, 80 :103566, 2022.

[219] Muhammad Tanveer, Neeraj Kumar, Mohammad Mehedi Hassan, et al. Ramp-iod : A robust authenticated key management protocol for the internet of drones. *IEEE Internet of Things Journal*, 9(2) :1339–1353, 2021.

[220] Sana Javed, Muhammad Asghar Khan, Ako Muhammad Abdullah, Amjad Alsirhani, Abdullah Alomari, Fazal Noor, and Insaf Ullah. An efficient authentication scheme using blockchain as a certificate authority for the internet of drones. *Drones*, 6(10) :264, 2022.

[221] Thomas Wollinger, Jan Pelzl, and Christof Paar. Cantor versus harley : optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems. *IEEE Transactions on Computers*, 54(7) :861–872, 2005.

[222] Thomas Wollinger, Jan Pelzl, Volker Wittelsberger, Christof Paar, Gökay Saldamli, and Çetin K Koç. Elliptic and hyperelliptic curves on embedded μp. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3) :509–533, 2004.

[223] Insaf Ullah, Noor Ul Amin, Mahdi Zareei, Asim Zeb, Hizbullah Khattak, Ajab Khan, and Shidrokh Goudarzi. A lightweight and provable secured certificateless signcryption approach for crowdsourced iiot applications. *Symmetry*, 11(11) :1386, 2019.

[224] Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on information theory*, 29(2) :198–208, 1983.

[225] Ran Canetti and Hugo Krawczyk. Universally composable notions of key exchange and secure channels. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 337–351. Springer, 2002.

[226] Luca Vigano. Automated security protocol analysis with the avispa tool. *Electronic Notes in Theoretical Computer Science*, 155 :61–86, 2006.

[227] Bruno Blanchet. Modeling and verifying security protocols with the applied pi calculus and proverif. *Foundations and Trends® in Privacy and Security*, 1(1-2) :1–135, 2016.

[228] Gavin Lowe, Philippa Broadfoot, and Mei Lin Hui. Casper : a compiler for the analysis of security. In *Protocols Proceedings of the 1997, IEEE. Computer society symposium on Research in security and Privasy*, pages 18–30, 1997.

[229] Cas JF Cremers. The scyther tool : Verification, falsification, and analysis of security protocols. In *International conference on computer aided verification*, pages 414–418. Springer, 2008.

[230] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami. An efficient biometric-based privacy-preserving three-party authentication with key agreement protocol using smart cards. *Security and Communication Networks*, 8(18) :4136–4156, 2015.

[231] H Hakan Kilinc and Tugrul Yanik. A survey of sip authentication and key agreement schemes. *IEEE communications surveys & tutorials*, 16(2) :1005–1023, 2013.

[232] Muhammad Asghar Khan, Insaf Ullah, Shibli Nisar, Fazal Noor, Ijaz Mansoor Qureshi, Fahim Ullah Khanzada, and Noor Ul Amin. An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network. *IEEE Access*, 8 :36807–36828, 2020.

[233] Aymen Dia Eddine Berini, Brahim Farou, Mohamed Amine Ferrag, Hamid Seridi, and Herman Akdag. A new static path planning strategy for drones. *Internet Technology Letters*, 5(6) :e386, 2022.

[234] Cong Pu, Andrew Wall, Imtiaz Ahmed, and Kim-Kwang Raymond Choo. Secureiod : A secure data collection and storage mechanism for internet of drones. In *2022 23rd IEEE International Conference on Mobile Data Management (MDM)*, pages 83–92. IEEE, 2022.

Author's publication

❖ International publications

[J1] **Tilte :** A new static path planning strategy for drones.

Authors : Aymen Dia Eddine Berini, Farou Brahim, Mohamed Amine Ferrag, Seridi Hamid and Herman Akdag.

Journal : Internet Technology Letters.

Year : 2022.

[J2] **Tilte :** HCALA : Hyperelliptic Curve-based Anonymous Lightweight Authentication Scheme for Internet of Drones.

Authors : Aymen Dia Eddine Berini, Mohamed Amine Ferrag, and Seridi Hamid.

Journal : Pervasive and Mobile Computing.

Year : 2023.

❖ International Communications

[C1] **Tilte :** Survey on Unmanned Aerial Vehicle Applications : Challenges Trends and Prospects.

Authors : Aymen Dia Eddine Berini, Brahim Farou, Mohamed Amine Ferrag, and Seridi Hamid.

Confernece : 3^{rd} **conference on Informatics and Applied Mathematics** $IAM'20$.

Location :Guelma university,Algeria

Year : 2020

Status :Published

[C2] **Tilte :** Taxonomy, Threat models and future research directions for Authentication schemes in IoD.

Authors : Aymen Dia Eddine Berini, Mohamed Amine Ferrag, Brahim Farou and Seridi Hamid.

Confernece : 4^{th} conference on Informatics and Applied Mathematics $IAM'21$.

Location : Guelma university,Algeria

Year : 2021

Status :Published

[C3] **Tilte :** Drone simulators : Features Highlights and Performance Comparison

Authors : Aymen Dia Eddine Berini, Mohamed Amine Ferrag, Brahim Farou, and Seridi Hamid.

Confernece : 5^{th} conference on Informatics and Applied Mathematics $IAM'22$

Location : Guelma university,Algeria

Year : 2022

Status : Published

[C4] **Tilte :** Authentication schemes for internet of drones : Taxonomy, threat models and future research directions

Authors : Aymen Dia Eddine Berini, Mohamed Amine Ferrag, Brahim Farou, and Seridi Hamid.

Confernece : 3^{rd} International Conference on Computing and Information Technology ($ICCIT$).

Location : University of Tabuk, Kingdom of Saudi Arabia.

Year : 2023

Status : Published