SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT

MANUELA DE JESUS SOUSA

DISSERTAÇÃO DE MESTRADO
EM ENGENHARIA ELÉTRICA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT

MANUELA DE JESUS SOUSA

ORIENTADOR: PAULO ROBERTO DE LIRA GONDIM

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE.DM - 830/25

BRASÍLIA/DF: ABRIL – 2025

Universidade de Brasília
Faculdade de Tecnologia
Departamento de Engenharia Elétrica

SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT

Manuela de Jesus Sousa

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

Paulo Roberto de Lira Gondim, PhD (ENE/UnB)
(Orientador)

Renato Mariz de Moraes, PhD (CIN/UFPE)
(Examinador Externo)

Hugerles Sales Silva, PhD (ENE/UnB)
(Examinador Interno)

Brasília/DF, abril de 25.

FICHA CATALOGRÁFICA

SOUSA, MANUELA DE JESUS
SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT. [Brasília/DF] 25.
xi, 141p., 210 x 297 mm (ENE/FT/UnB, Mestre, Dissertação de Mestrado, 25).
Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica.
Departamento de Engenharia Elétrica
1. Internet of Drones (IoD) 2. Authentication
3. Security 4. Unmanned aerial vehicle (UAV)
I. ENE/FT/UnB II. Mestre

REFERÊNCIA BIBLIOGRÁFICA

SOUSA, MANUELA DE JESUS (25). SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT. Dissertação de Mestrado, Publicação PPGEE.DM-830/25, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 141p.

CESSÃO DE DIREITOS

AUTOR: Manuela de Jesus Sousa
TÍTULO: SECURE AND EFFICIENT AUTHENTICATION PROTOCOLS FOR THE INTERNET OF DRONES ENVIRONMENT.
GRAU: Mestre ANO: 25

Manuela de Jesus Sousa
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
Faculdade de Tecnologia - FT
Departamento de Engenharia Elétrica(ENE)
Brasília - DF CEP 70919-970

Dedico este trabalho à minha mãe (in memoriam), que sempre me incentivou a seguir meus estudos, seja por meio de seus conselhos ou pelo exemplo que deu. Também dedico a todos os amigos e à minha família, que me apoiaram ao longo dessa jornada. Sem eles, com certeza, eu não teria chegado até aqui.

AGRADECIMENTOS

Este trabalho é fruto de muito esforço, dedicação e, acima de tudo, do apoio incondicional de pessoas especiais que estiveram ao meu lado durante esta jornada. Aos meus irmãos, Mirele e Marcos, sou imensamente grata pelo carinho, paciência e incentivo constantes. Aos meus pais, que sempre acreditaram no meu potencial, meu mais sincero agradecimento, e, em especial, à minha mãe (in memoriam), que me ensinou o valor do conhecimento.

Ao meu orientador, Prof. Paulo Roberto de Lira Gondim, cuja paciência, dedicação e vasto conhecimento foram fundamentais para a construção deste trabalho, expresso minha profunda gratidão. Suas orientações precisas e seu compromisso com a excelência foram essenciais para o meu crescimento acadêmico e profissional. Aos meus amigos, e em especial Ana Luiza, José Ricardo e Elpídio, companheiros incansáveis de estudo, que estiveram ao meu lado nos desafios e conquistas, obrigado por serem meu apoio e inspiração.

Ao Fabinho, pelo amor, apoio e incentivo inabaláveis em cada etapa desta trajetória. Sua confiança em mim foi essencial para que eu seguisse em frente, mesmo nos momentos mais difíceis. A todos que, de alguma forma, contribuíram para a realização deste sonho, meu mais sincero agradecimento.

RESUMO

"Protocolos de Autenticação Seguros e Eficientes para o Ambiente da Internet dos Drones"

A Internet dos Drones (IoD, do inglês *Internet of Drones*) é uma extensão especializada da Internet das Coisas (IoT), que oferece soluções inovadoras em uma ampla gama de aplicações, incluindo monitoramento ambiental, segurança pública e logística urbana, e que tem se destacado como uma das tecnologias de crescimento mais rápido no mundo, com capacidade de operar em ambientes remotos ou desafiadores, tornando os drones valiosos em situações críticas, como entrega rápida de suprimentos, vigilância de áreas de alta segurança e monitoramento de desastres ambientais.

A natureza sensível dos dados coletados e transmitidos por drones, incluindo informações geográficas detalhadas, imagens de alta resolução e dados ambientais críticos, apresenta desafios significativos de segurança e eficiência. Adicionalmente, as limitações de recursos desses dispositivos, como restrições de processamento, largura de banda e energia, devem ser equilibradas com as necessidades de segurança robusta para proteger contra acesso não autorizado e uso indevido de dados.

A segurança na IoD é crucial, e sua proteção envolve protocolos de autenticação e acordo de chaves (AKA, do inglês *Authentication and Key Agreement*), essenciais para garantir integridade, confidencialidade e disponibilidade das comunicações. Contudo, os protocolos usados em redes tradicionais não estão adaptados ao ambiente IoD, que apresenta desafios únicos devido à dinâmica dos drones e suas limitações. O uso desses protocolos em larga escala na IoD implicaria elevado consumo de banda, processamento computacional e energia.

Este trabalho apresenta o projeto e a avaliação de dois novos protocolos de autenticação para o ambiente IoD, desenvolvidos para cenários distintos, considerando infraestruturas ar-terra: i) um protocolo de autenticação multifator, para um cenário genérico, que utiliza biometria e criptografia de curva elíptica, visando aprimorar a verificação de identidade do

usuário e assegurar uma segurança robusta; ii) um segundo protocolo, em um cenário de inventário florestal, que integra computação em névoa na infraestrutura de rede e emprega assinaturas agregadas para autenticar grupos de drones simultaneamente, melhorando a escalabilidade do sistema, aumentando a sua segurança e evitando a exposição de dados confidenciais.

A metodologia adotada incluiu uma revisão abrangente da literatura, definição de arquiteturas específicas para cada cenário, propriedades de segurança a serem alcançadas e possíveis ataques contra os quais oferecer proteção. Ambos os protocolos tiveram sua segurança e desempenho avaliados e comparados com outras propostas publicadas na literatura. A avaliação de segurança e a comparação consideraram o atendimento a propriedades como confidencialidade, integridade, privacidade e anonimidade, além da resistência a diversos ataques como *man-in-the-middle*, personificação e *message replay*, entre outros. As duas propostas demonstraram ser mais robustas que as outras propostas consideradas na comparação.

A avaliação de desempenho dos protocolos foi realizada considerando, inicialmente, os custos computacionais, avaliados com base no tempo de processamento das operações necessárias para executar cada sessão de autenticação do protocolo. Os custos de comunicação, relativos ao transporte de mensagens, foram medidos em bits, considerando os tamanhos de todos os campos referentes a parâmetros presentes nas mensagens trocadas entre as entidades durante uma sessão de autenticação. O custo energético, por sua vez, foi calculado para o segundo protocolo, sendo determinado pelo consumo total de energia, representado pela soma dos gastos energéticos referentes às operações computacionais e de comunicação. Adicionalmente, os protocolos propostos foram validados pela ferramenta AVISPA, que comprovou sua segurança para uso prático. Os resultados obtidos demonstram que os protocolos desenvolvidos oferecem um equilíbrio eficaz entre segurança robusta e eficiência operacional, atendendo às demandas específicas dos ambientes IoD.

Este trabalho contribui para o campo da segurança em IoD, oferecendo soluções práticas e eficientes para os desafios de autenticação neste ambiente dinâmico e restrito em recursos. Os protocolos propostos não apenas melhoram a segurança das comunicações em IoD, mas também consideram as limitações de processamento e energia dos drones, tornando-os adequados para implementação em cenários reais.

Palavras-chave: Internet of Drones (IoD), autenticação, segurança, Veículo aéreo não tripulado (UAV).

ABSTRACT

The Internet of Drones (IoD), a critical extension of the Internet of Things (IoT), provides innovative solutions across a wide range of applications, including environmental monitoring, public security, and urban logistics. The IoD has emerged as one of the fastest-growing technologies worldwide, with its ability to operate in remote or challenging environments, making drones valuable in critical situations such as rapid supply delivery, high-security area surveillance, aand environmental disaster monitoring.

The sensitive nature of the data collected and transmitted by drones including detailed geographic information, high-resolution images, and critical environmental data poses significant security and efficiency challenges. Additionally, the resource constraints of these devices, such as processing, bandwidth limitations and energy, must be balanced with the need for robust security to prevent unauthorized access and data misuse.

Security in the IoD is crucial, and its protection includes authentication and key agreement (AKA) protocols, which are fundamental to ensuring the integrity, confidentiality, and availability of communications. However, authentication protocols used in traditional networks are not adapted to the IoD environment, which presents unique challenges due to the dynamic nature of drones and their resource limitations. The large-scale deployment of these protocols in the IoD would result in high bandwidth, computational processing, and energy consumption.

This work presents the design and evaluation of two novel authentication protocols for the Internet of Drones (IoD) environment, developed for distinct scenarios while considering air-to-ground infrastructures: i) a multifactor authentication protocol, designed for a generic scenario, which employs biometrics and elliptic curve cryptography to enhance user identity verification and ensure robust security; ii) a second protocol, designed for a forest inventory scenario, which integrates fog computing into the network infrastructure and utilizes aggregate signatures to authenticate groups of drones simultaneously, thereby improving system scalability, enhancing security, and preventing the exposure of confiden-

tial data.

The adopted methodology included a comprehensive literature review, the definition of specific architectures for each scenario, the identification of security properties to be achieved, and the analysis of potential attacks against which protection is required. The security and performance of both protocols were evaluated and compared with other proposals in the literature. The security evaluation and comparison considered properties such as confidentiality, integrity, privacy, and anonymity, as well as resistance to various attacks, including man-in-the-middle, impersonation, and message replay, among others. The two proposed protocols demonstrated greater robustness compared to other approaches analyzed in the comparison.

The performance evaluation of the protocols was initially conducted by considering the computational costs, assessed based on the processing time required to execute each authentication session of the protocol. The communication costs, related to message transmission, were measured in bits, taking into account the sizes of all fields corresponding to parameters included in the messages exchanged between entities during an authentication session. The energy cost, in turn, was calculated for the second protocol and determined by the total energy consumption, represented by the sum of the energy expenditures associated with computational and communication operations. Additionally, the proposed protocols were validated using the AVISPA tool, which confirmed their security for practical use. The obtained results demonstrate that the developed protocols achieve an effective balance between strong security and operational efficiency, meeting the specific demands of IoD environments.

This work contributes to the field of IoD security by providing practical and efficient solutions to authentication challenges in this dynamic and resource-constrained environment. The proposed protocols not only enhance the security of IoD communications but also account for the processing and energy limitations of drones, making them suitable for real-world implementation.

Keywords: Internet of Drones (IoD), authentication, security, drone and unmanned aerial vehicle (UAV).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

λ	Security parameter
ΔT	Maximum transmission delay
GF	Galois Function
U_i	i^{th} User, i = 1,2,3,. . . , n
RD_j	j^{th} Remote Drone, j = 1,2,3,. . . , m
C_k	k^{th} Fly Zone (Cluster), k = 1,2,3,. . . , l
$params$	System parameters
CK_k	Group key
MD_{U_i}	Mobile Device U_i
T	Current timestamp
A	Adversary
ID	Tdentity
TID	Temporary identity
PW_{U_i}	Password of i^{th} User (U_i)
E/D	Encryption/Decryption operation
SK	Session key
RTS	Timestamp
Gen ($\cdot$)	Generation process in fuzzy extractor
Rep ($\cdot$)	Reproduction process in fuzzy extractor

Bio_{U_i}	Biometric template of U_i
σ_i	Biometric secret key of U_i for Bio_{U_i}
τ_i	Public reproduction parameter of U_i for Bio_{U_i}
$\|\|$	Concatenation operation
$\oplus$	Bitwise XOR operation

GLOSSARY

5G	Fifth Generation Mobile Network
6G	Sixth Generation Mobile Network
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AVISPA	Automated Validation of Internet Security Protocols and Applications
BS/FS	Backward Secrecy and Forward Secrecy
CAGR	Compound Annual Growth
CIA	Confidentiality, Integrity and Availability
CL-AtSe	Constraint Logic-based Attack Searcher
DDoS	Distributed Denial of Service
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ESL	Ephemeral Secrets Leakage
GPS	Global Positioning System
GSS	Ground Station Server
GCS	Ground Control Station
HLPSL	High-Level Protocol Specification Language
HMAC	Hash-based Message Authentication Code

IoD	Internet of Drones
IoT	Internet of Things
KGC	Key Generation Centre
MAC	Message Authentication Code
OFMC	On-the-Fly Model Checker
P2P	Peer-to-Peer
PUF	Physically unclonable functions
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm 256-bit
UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 INITIAL CONSIDERATIONS

The Internet of Things (IoT) has been driving digital transformation across various sectors, enabling the autonomous and real-time connection and communication between heterogeneous devices. This integrated environment facilitates the collection and sharing of large volumes of data, creating new opportunities for applications in security, monitoring, and logistics in areas such as public safety, emergency management, and urban infrastructure [1] [2]. Within this context, the Internet of Drones (IoD) emerges as an extension of the IoT, leveraging unmanned aerial vehicles (UAVs), commonly referred to as drones, to perform tasks that require high mobility and precise data collection. With applications spanning infrastructure inspection, surveillance, disaster response, and forest inventory management, the IoD expands IoT capabilities by exploring the advantages of interconnected drone networks [3] [4].

The IoD architecture consists of drones operating in designated flight areas, collecting and transmitting data to ground control stations or directly to users. Equipped with advanced sensors, such as high-resolution cameras, accelerometers, and GPS, these drones can monitor environmental conditions and parameters of critical infrastructure [5]. This capability enables the IoD to be utilized in a wide range of applications, from monitoring weather conditions to gathering public safety data in smart cities [6]. However, this dynamic and highly interconnected infrastructure also introduces significant security challenges, particularly due to the decentralized nature and wireless communication of drones, which make them vulnerable to data interception, identity spoofing, and unauthorized access [7].

The increasing adoption of IoD in various application areas underscores the urgent need for robust security solutions, particularly authentication protocols. Effective authentication

stands out as one of the primary measures to safeguard the IoD against a variety of threats, including data interception and identity spoofing, which could compromise information security and the physical integrity of drones [8]. The IoD environment demands authentication protocols that are scalable and adaptable, allowing new drones to be seamlessly integrated or removed from the network without compromising security. Furthermore, authentication is fundamental to protecting data privacy and confidentiality, as drones often capture detailed and sensitive information, such as high-resolution images and location data. Without appropriate authentication and encryption protocols, such data could be exposed and misused, posing significant risks, especially in critical applications like public safety and emergency response [9].

In this context, authentication protocols allow only authorized devices and users to access and control the drones, securing communications against malicious access and preventing cyberattacks [5]. However, many existing protocols were designed for traditional networks that do not share the same resource constraints as drones, such as limited processing power and communication links. These limitations necessitate lightweight and efficient solutions capable of maintaining a high level of security without impairing the operational capacity of the devices [10].

Emerging technologies such as biometrics, fuzzy extractors, cloud computing, fog computing, and blockchain have shown promise in addressing the needs of new IoD authentication protocols [9]. Biometric solutions and Fuzzy Extractors enable robust multifactor authentication by combining biometric characteristics with algorithms that generate unique and secure keys from fuzzy data, significantly reducing the possibility of identity spoofing and enhancing operational reliability [11]. Cloud computing, in turn, provides a centralized and secure infrastructure for storing and managing authentication data at scale, enabling real-time identity verification and updates [12]. Fog computing complements this infrastructure by facilitating data processing closer to the network edge, enhancing security by minimizing the exposure of sensitive data during transmission to distant servers and reducing latency [13]. This is particularly advantageous in scenarios requiring rapid response and continuous communication, such as forest inventory operations and urban monitoring.

This dissertation proposes two authentication protocols designed to address the unique

security challenges in the Internet of Drones (IoD) environment, leveraging emerging technologies in different application scenarios. The first protocol employs a multifactor approach using biometrics to enhance identity verification and prevent spoofing attacks. The second protocol integrates fog computing to enable real-time data processing near the network edge, reducing latency, and improving security in resource-constrained environments, such as forest inventory management.

1.2 MOTIVATION

The motivation for this work stems from the need for new authentication protocols specifically designed to meet the unique requirements of the Internet of Drones (IoD). The conventional authentication protocols, widely employed in fixed or centralized communication networks, face challenges when adapting to the IoD scenario due to their performance limitations in resource-constrained devices, such as drones, which possess limited processing and communication capabilities [13].

Furthermore, the use of drones in critical applications, such as public safety, environmental monitoring, and smart city operations, necessitates the protection of sensitive data against interception and unauthorized access [14]. The absence of IoD-specific protocols leaves such data vulnerable to cyberattacks, jeopardizing both the privacy of the information and the physical integrity of the drones. The authenticity of communications between drones and ground control stations is essential to prevent unauthorized entities from manipulating or capturing critical data, which could compromise the safety of operations in highly critical areas [15].

Another limitation relates to the scalability and flexibility of authentication protocols within the IoD. In drone networks, the ability to securely and continuously incorporate new devices or remove compromised or inactive ones is essential for maintaining system integrity. Traditional authentication protocols lack adaptability to address this dynamic environment, which becomes even more problematic when considering the resource constraints of drones, making it difficult to implement robust protocols without overburdening the devices [9].

Additionally, the decentralized infrastructure of the IoD, where drones communicate directly with each other and with control stations, demands authentication solutions that balance security and efficiency. The application of traditional cryptographic techniques, such as RSA, often entails high energy consumption and computational demands [16], rendering their large-scale use within the IoD infeasible. Therefore, the development of lightweight yet robust protocols becomes a necessity to ensure security without compromising the operational efficiency of the drones.

Consequently, there is a pressing need to develop new authentication protocols that not only ensure the integrity and privacy of IoD communications but also operate efficiently in resource-constrained devices, guaranteeing scalability, resilience against attacks, and trust in operations conducted in critical scenarios.

1.3 OBJECTIVES

The general objective of this work is to develop and evaluate authentication protocols for the Internet of Drones (IoD), focusing on security, efficiency, and scalability in different application scenarios.

The specific objectives include:

1. Developing two novel authentication protocols for the IoD scenario, each designed for a specific application scenario: one for a generic environment and another for forest inventory operations.

2. Applying advanced security concepts, such as confidentiality, integrity, anonymity, and resistance to cyberattacks, including man-in-the-middle, identity spoofing, and replay attacks.

3. Evaluating the security and performance of the proposed protocols in comparison to other protocols in the literature, considering computational, communication, and energy costs in IoD environments.

4. Validating the proposed protocols through formal verification tools, such as AVISPA, to confirm their robustness against known attacks.

1.4 METHODOLOGY

The methodology adopted for this dissertation is structured in phases, detailed below:

- Phase 1: Comprehensive literature review on topics relevant to developing authentication protocols for the IoD environment. The review explored security requirements for secure communications in drone networks, identifying specific vulnerabilities and authentication challenges in the IoD context. Existing authentication protocols for IoT and IoD networks were also analyzed, focusing on multifactor authentication and fog computing solutions.

- Phase 2: Study of multifactor authentication in the IoD context, emphasizing techniques combining biometrics and elliptic curve cryptography. Based on this study, A network architecture and an attack model have been defined, and a multifactor authentication protocol was developed for the IoD, considering data security, anonymity, and efficient integration with the drone control system. This ensured secure communication and resistance to interception and identity spoofing attacks.

- Phase 3: Study of fog computing applications in the IoD, particularly in forest inventory scenarios, where continuous and real-time communication is essential. A network architecture incorporating fog computing and an attack model have been defined, and a second protocol has been developed to enhance scalability. An aggregated signature strategy was also developed to authenticate drone groups efficiently, considering the dynamic addition and removal of drones.

- Phase 4: Performance and security analyses of the two proposed authentication protocols. This phase evaluated aspects such as communication bandwidth consumption and the processing time for each operation involved in the authentication procedure. For the second protocol, energy consumption during the process was additionally assessed. Security analyses were also conducted to validate the protocols' resilience against various attacks, including data interception, identity spoofing, and session desynchronization.

- Phase 5: Formal validation of the developed protocols using the Automated Validation

of Internet Security Protocols and Applications (AVISPA) tool, widely recognized for verifying the security of authentication protocols. This analysis aimed to confirm the robustness of the protocols against a range of attacks and their compliance with IoD security requirements.

- Phase 6: Development of scientific articles describing and evaluating the proposed protocols in comparison with other solutions in literature. The articles highlighted the merits and limitations of each protocol, alongside potential improvements for future applications.

- Phase 7: Writing and defense of the dissertation, consolidating all the knowledge gained during protocol development, the literature review, validation, and comparison with other proposals. This phase included organizing results and conclusions.

1.5 CONTRIBUTIONS

The main contributions of this work are:

- Discussion on Authentication Protocols for the IoD Environment: An in-depth examination of existing authentication mechanisms and their application to the Internet of Drones (IoD).

- Proposal of a Multifactor Authentication Protocol: Development of a secure protocol for the IoD utilizing biometrics and elliptic curve cryptography to enhance identity verification and ensure robust security.

- Proposal of an Authentication Protocol for Forest Inventory Using Fog Computing: Design of a scalable and efficient solution incorporating aggregated signatures to support dynamic drone operations in a resource-constrained environment (forest) for inventory-related tasks.

- Evaluation of Security and Performance of the Proposed Protocols: Comprehensive analysis of the security properties, computational and communication costs of the protocols.

- Formal Validation Using AVISPA: A semi-formal verification of the security properties of the protocols was conducted using the AVISPA tool to confirm their robustness against various types of attacks.

1.6 PUBLICATIONS

During this research, one article was published in a JCR-ranked international journal:

Manuela de Jesus Sousa, Paulo Roberto L. Gondim, "A multi-factor user authentication protocol for the internet of drones environment. Peer-to-Peer Networking and Applications", v. 18, n. 2, p. 1-22, 2025, https://doi.org/10.1007/s12083-024-01862-0, as presented in Appendix A.

A second article, accepted for publication at the technical-scientific event IEEE SmartNets 2025, can be found in Appendix B.

1.7 ORGANIZATION

The remainder of this dissertation is organized as follows: Chapter 2 presents relevant concepts on authentication and security considered during the development of the two proposed protocols for the Internet of Drones (IoD). It also addresses the main security threats and specific challenges faced in IoD environments.

Chapter 3 describes the development of a multifactor authentication protocol for the IoD environment. This protocol uses biometrics and elliptic curve cryptography to enhance communication security while reducing computational and communication resource consumption compared to other protocols in the literature. Elliptic Curve Cryptography (ECC) was selected due to its ability to provide high levels of security with smaller key sizes, significantly reducing processing time and energy consumption—making it ideal for resource-constrained drone environments. Security analyses, performance evaluation and formal validation of the protocol are presented.

Chapter 4 proposes an authentication protocol for forest inventory operations using fog computing. This protocol aims to improve scalability and efficiency by employing aggre-

gated signatures to authenticate groups of drones. The chapter includes security analysis, performance evaluation, and formal validation of the protocol.

Finally, Chapter 5 concludes the dissertation by presenting the final considerations, synthesis of contributions of the work, and suggestions for future research in the field of IoD security.

CHAPTER 2

BACKGROUND

Abstract. *This chapter addresses the fundamental concepts necessary for understanding the proposed protocols for the Internet of Drones (IoD). It begins by presenting a definition and description of the IoD architecture, followed by its primary applications and use case scenarios, as well as specific security challenges within this environment. Subsequently, the chapter discusses various technologies applied to authentication in the IoD, such as Elliptic Curve Cryptography (ECC), biometric verification using fuzzy extractor and fog computing. It concludes with an overview of the AVISPA tool used to validate the security of the proposed protocols.*

2.1 INTERNET OF DRONES

With the continuous advancement of Internet of Things (IoT) technology, the connectivity of various devices or "things" via the Internet has become increasingly accessible and effective. These devices cooperate to collect vast amounts of data, enabling real-time applications in fields such as smart agriculture, environmental monitoring, public health, disaster management, and both civilian and military operations, where precise and timely responses are critical [17] [18] [19]. For instance, IoT supports real-time monitoring of urban infrastructure, logistics asset tracking, and search and rescue operations by analyzing collected data to facilitate immediate decision-making [20].

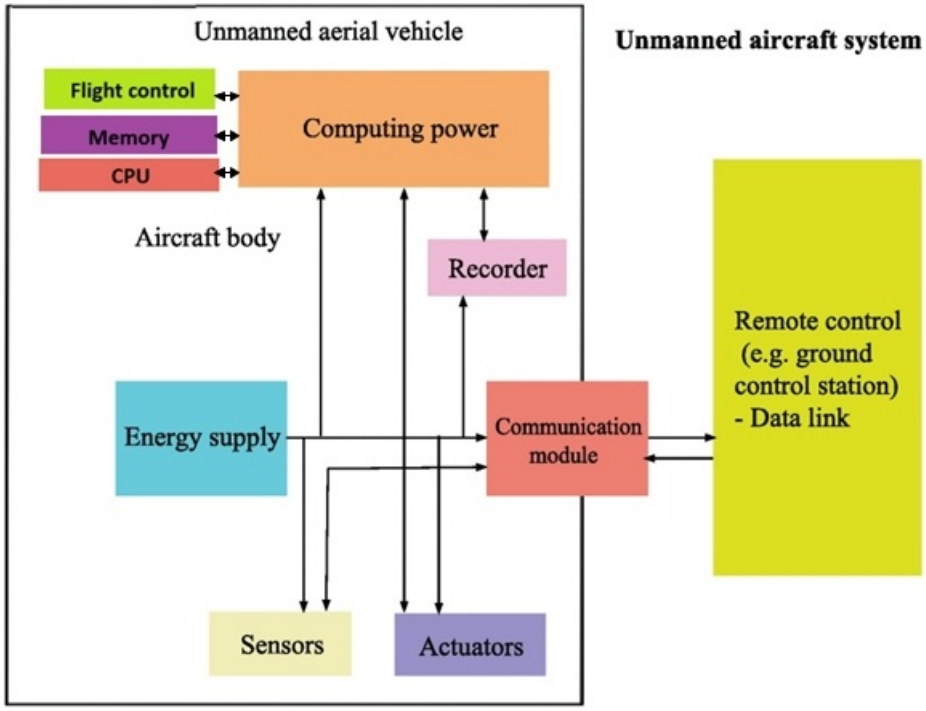
A key advantage of IoT is its ability to enable autonomous, real-time decision-making by interconnected devices, often without human intervention. This capability, combined with advancements in high-speed, low-latency networks like 5G, and the development of cost-efficient sensors and miniaturized electronics, has expanded IoT applications across industries ranging from agriculture to healthcare, improving operational efficiency and responsiveness [17] [21] [22].

The Internet of Drones (IoD) represents an advanced extension of the Internet of Things (IoT), focusing on the interconnection and cooperation of Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, within a dynamic and distributed network. According to Gharibi et al. [23], IoD is defined as an architecture designed to provide coordinated access to UAV-controlled airspace.

Through IoD, drones can execute complex missions autonomously and collaboratively, exchanging data and instructions in real-time with each other, ground stations, or cloud servers. This network enables drones to carry out strategic tasks such as surveillance, environmental monitoring, and long-distance deliveries while adapting dynamically to environmental changes and mission requirements [24].

The IoD relies on a communication and control infrastructure consisting of drones e, ground control stations, control rooms, and, in some cases, cloud servers. These elements facilitate the collection, processing, and storage of large data volumes. Modern drones in this context are equipped with high-resolution cameras, GPS, accelerometers, and environmental sensors capable of gathering detailed information, such as temperature, humidity, traffic conditions, and air quality [5]. Figure 2.1 illustrates bacic structure of a UAV.

Figure 2.1. Basic structure of a UAV



Source: adapted from [25] and [26].

To enable communication between drones and remote user access, the IoD utilizes a versatile network infrastructure that supports various communication technologies, including mobile networks, satellites, and wireless sensor networks (WSN). The choice of communication technology largely depends on the use case and specific application. For instance, in long-range missions or densely populated urban areas, drones may connect via mobile networks or satellites to ensure continuous and uninterrupted communication. Conversely, in enclosed environments or regions with low network coverage, such as dense forests, WSNs and mesh networks are often used [27] [28].

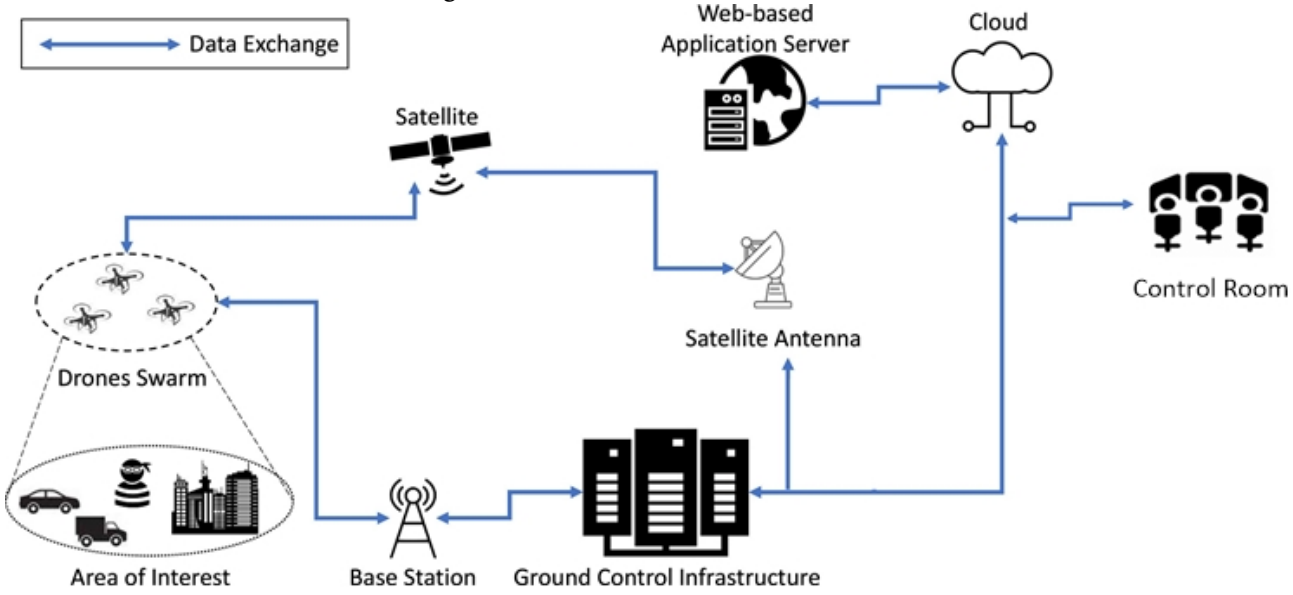
The ground control station (GCS) plays a critical role in facilitating communication between drones and the control room. It enables telemetry data exchange and command transmission, ensuring route tracking and maintaining connections with drones in critical missions, even in challenging conditions. Additionally, the GCS can be configured for specific tasks, such as energy management and security monitoring against physical and cyber threats [29].

The control room functions as the command center where operators monitor and control drones in real-time. It processes telemetry data and information gathered by drones, ensuring secure operation and handling essential flight data. This environment is vital for maintaining flight and mission safety, enabling rapid responses to changing conditions [30].

The IoD can also integrates cloud servers to facilitate data storage and processing collected by drones. Cloud processing capabilities allow complex data, such as high-resolution images and videos, to be analyzed in real-time or near real-time, providing operators with valuable insights for quick decision-making. Moreover, cloud systems enable IoD to store large amounts of historical data, which can be used for predictive analyses and continuous operational improvements [22] [7].

Finally, the IoD architecture must be scalable and resilient, allowing the addition or removal of drones without compromising network stability. This characteristic is especially important in dynamic operations where new drones may be added to expand coverage areas or replace out-of-service drones. IoD supports flexible and continuous expansion, aligned with application needs and technological advancements in the drone sector. This flexibility also extends to communication approaches and authentication protocols, which must evolve alongside the network to ensure security and efficiency in increasingly complex scenarios [5]. Figure 2.2 illustrates reference IoD architecture.

Figure 2.2. Reference IoD architecture

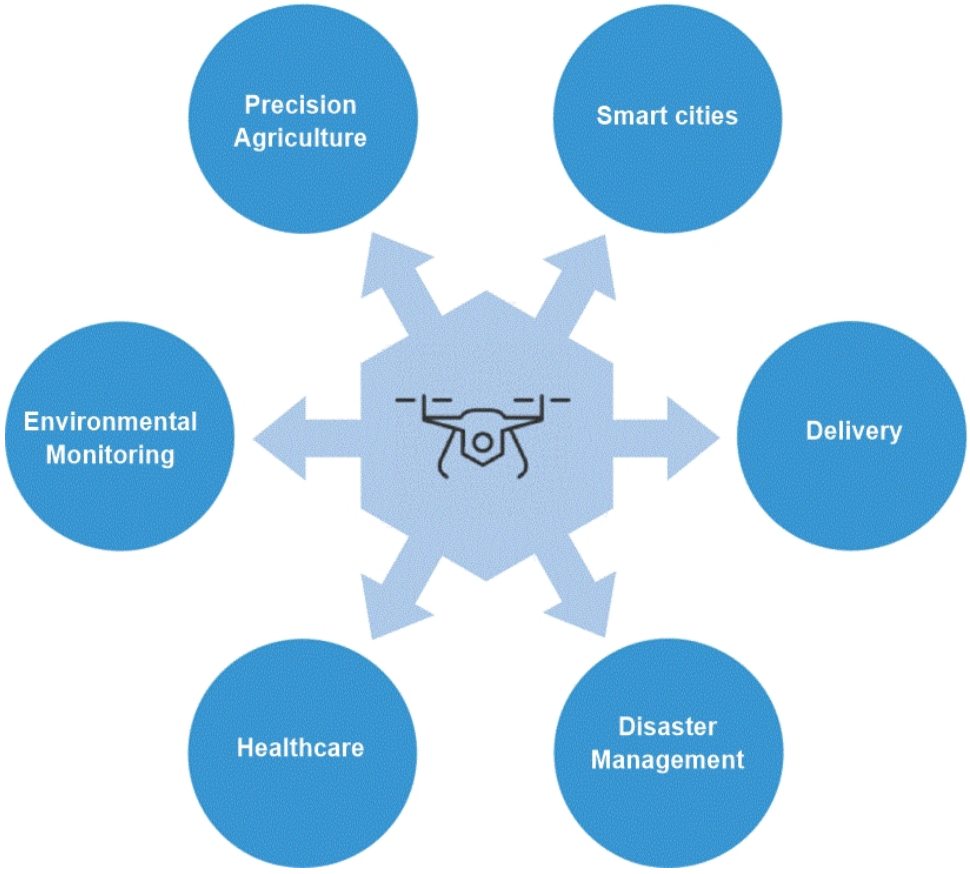


Source: adapted from [22].

2.1.1 IoD Application Scenarios

The IoD is rapidly expanding, with the drone market projected to generate revenues exceeding $500 billion by 2030 and drone operations expected to double from 15 million to 28 million globally by 2029 [31] [32]. This growth reflects a compound annual growth rate (CAGR) of 14.4%, positioning the drone industry as one of the fastest-growing sectors globally. Drones have become critical in a variety of fields, including environmental monitoring, precision agriculture, civil construction, and public safety. These technologies have revolutionized conventional methods, offering faster, safer, and more efficient alternatives. Their ability to operate in remote or challenging environments makes them particularly valuable in critical situations, such as rapid supply delivery and surveillance of high-security areas. These advancements improve existing operations and create opportunities for new applications where human presence is limited or unfeasible [31]. Figure 2.3 shows the different potential applications of drones.

Figure 2.3. IoD application areas



Source: adapted from [33].

In environmental monitoring, drones collect data in inaccessible regions with minimal ecological impact, aiding biodiversity conservation and ecosystem health monitoring. Continuous surveillance enables swift responses to anomalies, allowing preventive actions to mitigate irreversible environmental damage [34] [4].

Precision agriculture employs drones equipped with advanced imaging technologies to enhance planting, irrigation, and pesticide application efficiency [35]. The agricultural drone market is anticipated to reach $32.4 billion in the near future [36].

In smart cities, drones play a vital role in urban planning, infrastructure development, and real-time traffic monitoring. Their adaptability enables efficient data collection for metro systems, bike paths, and congestion management, significantly enhancing urban mobility through continuous aerial surveillance [20] [4] [37] [38].

Delivery logistics benefit significantly from drones, offering rapid and efficient last-mile delivery services, including the transportation of emergency supplies Companies like Amazon and DHL have showcased the potential of drone deliveries, emphasizing their capacity to enhance logistics while reducing emissions, fuel consumption, and urban congestion [39] [40] [41].

In healthcare, drones address logistical challenges by delivering critical medical supplies, such as blood and vaccines, especially in remote areas. During the COVID-19 pandemic, drones demonstrated their value by rapidly transporting medicines and collecting biological samples [42] [43].

For disaster management, drones equipped with high-resolution cameras and sensors provide aerial views of affected areas, aiding rescue teams and facilitating rapid disaster assessments. They are invaluable for prevention, intervention, and recovery efforts in emergencies [44] [45].

In military applications, the IoD supports real-time surveillance, logistics, and precision strikes. Drones enhance mobility, responsiveness, and operational efficiency in conflict zones, offering strategic advantages through swarm technology and automated logistics [23] [3] [46].

In addition to these, the IoD can be applied in various other areas, such as entertainment

and event coverage, water resource management, inspection of wind and solar farms, aerial photography for the film industry, and the fishing industry, further expanding its possibilities and solidifying its role in both critical situations and everyday activities.

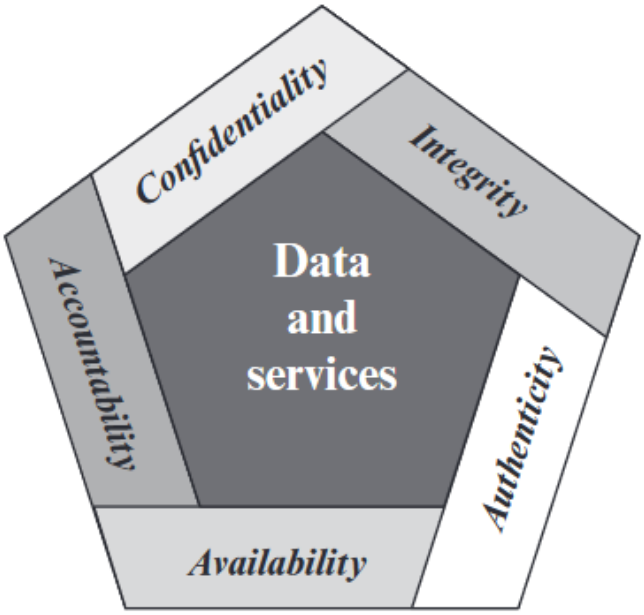
2.2 SECURITY CHALLENGES

System security is based on three core objectives - confidentiality, integrity, and availability, collectively known as the CIA triad. These principles, as defined by Stallings [47] and NIST FIPS 199, address risks such as unauthorized disclosure, data tampering, and disruptions to system access [47].

While these foundational objectives provide a solid framework for understanding security needs, they are insufficient on their own to address the complexities of modern systems, particularly dynamic and decentralized networks like the Internet of Drones (IoD).

Building upon these foundational concepts, additional principles such as authenticity and accountability have been introduced to address emerging security demands. Authenticity ensures that an entity or piece of information is genuine, verifiable, and trustworthy, confirming that users are who they claim to be. Accountability, in turn, enables traceability of actions, supporting non-repudiation, failure detection, and legal proceedings. Together, these principles form the basis for addressing the advanced security challenges posed by IoD environments, Figure 2.4.

Figure 2.4. Essential Network and Computer Security



Source: [47].

2.2.1 Security Challenges in IoD

In the IoD environment, information plays a crucial role in data analysis and overall system performance. However, the network faces significant security challenges, as most data is confidential and private. Protecting this information is particularly critical given the bandwidth limitations of IoD, which can facilitate real-time attacks on sensory data. Such attacks threaten the drones and ground control stations, users, servers, and other network participants, potentially compromising the integrity, availability, and confidentiality of transmitted information. The consequences include loss of critical data, communication disruptions, and malicious actions that could jeopardize the safe operation of drones [22] [7] [8]. To address these challenges, it is essential to focus on key aspects of security and privacy in IoD, which can be categorized as follows:

- **Confidentiality:** Ensures that information is accessible only to authorized drones, users, and gateways, preventing unauthorized access or manipulation. This protection is fundamental to maintaining the security of communications between connected entities in IoD.

- **Integrity:** Protects transmitted information from tampering, modification, or destruction, ensuring the data remains unaltered throughout its transfer.
- **Availability:** Guarantees uninterrupted access to essential IoD services for authorized users, ensuring the network operates efficiently even under adverse conditions.
- **Authentication:** Facilitates mutual authentication among drones, users, and gateways by using unique identities and parameters to verify the legitimacy of all entities involved in the network.
- **Scalability:** As the number of connected drones grows, the IoD infrastructure must handle increased demand without compromising efficiency or security.
- **Non-repudiation:** Ensures that transmitting drones are accountable for their messages, particularly in critical situations like emergencies. This accountability prevents entities from denying message transmission, enabling traceability and swift incident response.
- **Anonymity:** Protects the true identities of drones, users, and other entities, safeguarding them from exposure and impersonation attacks by malicious actors.
- **Privacy:** Prevents unauthorized access to sensitive information, such as geolocation data or personally identifiable details, ensuring that this data is not misused to profile individuals [48].
- **Backward Secrecy and Forward Secrecy (BS/FS):** Maintains communications privacy in the dynamic IoD network. Backward secrecy ensures that newly added drones cannot access previous communications, while forward secrecy prevents drones leaving the network from accessing future communications, preserving the security of the entire communication chain.

These interconnected security aspects form the foundation for addressing IoD's unique challenges. While confidentiality, integrity, and availability remain central to secure operations, the dynamic nature of IoD requires solutions that adapt to its scalability, mobility, and diverse applications.

2.2.2 Security Attacks

Ensuring IoD security is challenging due to the diversity of communication standards and the wide range of applications involved. These vulnerabilities manifest in various forms, ranging from direct interception of communications to resource exhaustion attacks. Below are some of the most common threats targeting the IoD environment [7] [49].

- **Replay Attack:** In this type of attack, adversary A repeatedly sends previously transmitted messages to the recipient to gain unauthorized access to services within the IoD environment. The goal is to deceive the system into recognizing old communications as current. Such attacks exploit the IoD's reliance on time-sensitive data, making them particularly damaging in operational scenarios

- **Man-in-the-Middle Attack:** Besides replaying old messages, adversaries can intercept communications directly, as seen in Man-in-the-Middle attacks. Here, the adversary intercepts communication between the sender and recipient, inserting themselves into the message exchange while pretending to be the sender. This real-time attack allows the adversary to transmit an apparently legitimate message to the recipient while monitoring or altering the ongoing communication.

- **Privileged Insider Attack:** IoD systems are also vulnerable to threats from within. In this case, the adversary acts as a privileged user, appearing to be a legitimate entity within the IoD network. Exploiting their internal access, the adversary seeks to establish communication with authorized participants to extract sensitive information or compromise system security.

- **Ephemeral Secrets Leakage (ESL) Attack:** Beyond impersonation, an adversary may compromise session credentials directly. In this attack, the adversary captures the state of a session, exposing short and long-term secret credentials. With this information, the adversary can compute the secret session key used by legitimate entities in the IoD, gaining access to the information exchanged during the session.

- **Drone Physical Capture Attack:** While many attacks target digital vulnerabilities, physical security is also a concern. The adversary may physically capture a drone

and use power analysis techniques [50] to extract stored information from the device's memory. The extracted data can then be exploited for impersonation attacks, enabling the adversary to operate within the IoD network like the original drone.

- **Denial-of-Service (DoS) Attack:** While the attacks described above primarily target data and credentials, others focus on exhausting system resources. In the IoD, where communication is predominantly wireless, drones face limited bandwidth, battery capacity, and storage constraints. In a DoS attack, the adversary aims to deplete network resources and disrupt services by overwhelming the target with excessive traffic or sending malicious data to cause system failures.

2.3 AUTHENTICATION - PRINCIPLES AND SOLUTIONS

In the IoD implementations, network architectures are typically divided into two main types: those based on air-ground infrastructures and ad hoc configurations composed exclusively of aerial nodes. In the first case, networks include drones organized into groups, operators or users, and a trusted GCS. This station has high computational capacity and an adequate energy supply [3]. In the second type, networks consist of aerial nodes operating in a decentralized manner, utilizing drone-to-drone communication links.

It is important to note that user-to-drone and drone-to-GCS communications often occur over public channels, which are inherently insecure and vulnerable to attacks. On the other hand, drone-to-drone links are frequently modeled as Peer-to-Peer (P2P) connections, which have specific vulnerabilities, including Distributed Denial-of-Service (DDoS) attacks [51].

As noted by Michailidis et al. [5], the authentication procedure in IoD encompasses both node and message authentication. Node authentication aims to verify the identity of each node in the network, granting access to resources and establishing connections between registered and trusted nodes. By correctly authenticating legitimate nodes, unauthorized nodes are blocked, ensuring the security and privacy of the network.

Message authentication requires verifying the integrity of the data and its origin and detecting possible anomalies in the transmitted message patterns. Figure 2.5 illustrates that the authentication process typically occurs in multiple phases, involving the exchange

of cryptographic keys among network entities.

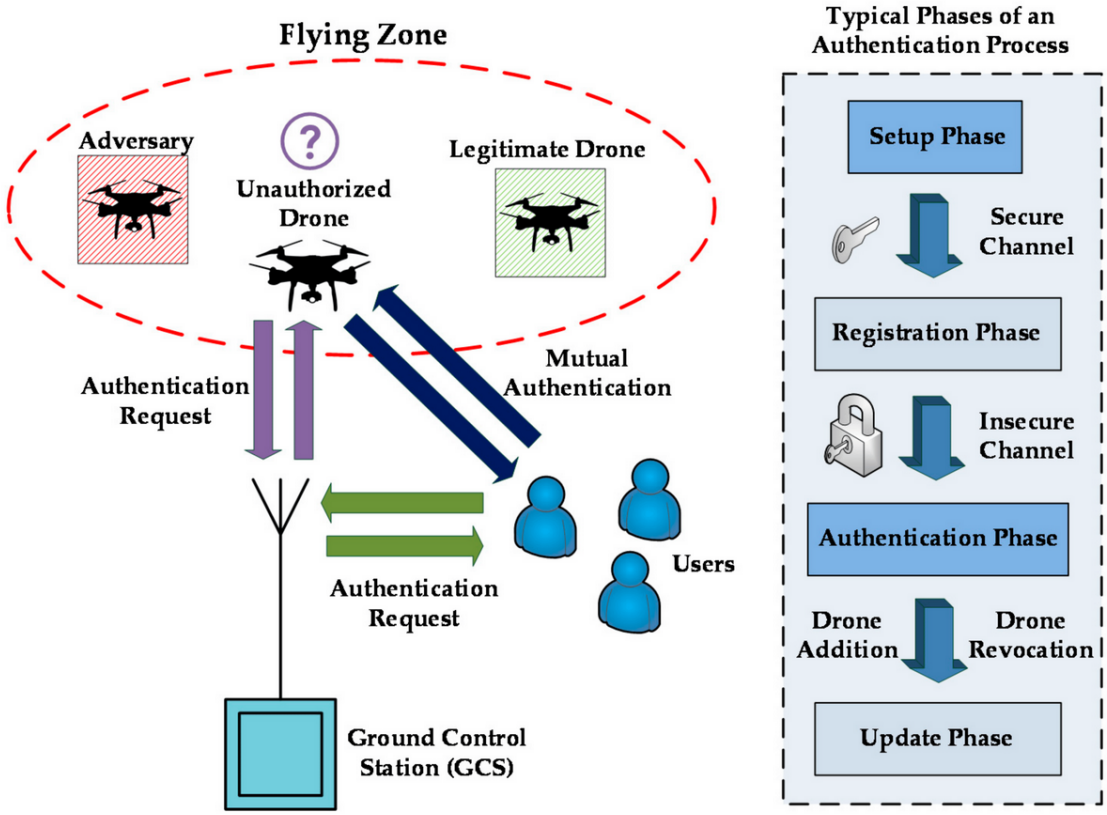
- **Initialization Phase:** This is the first step, during which the GCS initializes and locally stores security parameters such as the protocol, the secret key, and the public-private key pairs.

- **Registration Phase:** Users and partially trusted drones wishing to join the IoD network register with the trusted GCS via secure channels, enabling initial identification. Registration data is stored in the GCS database for future reference.

- **Authentication and Key Agreement Phase:** A shared secret key is generated and negotiated among the involved parties through an insecure channel.

- **Update Phase:** This phase dynamically manages the addition of new drones to the network or the revocation of drones that no longer meet trust criteria.

Figure 2.5. Simple representation of an authentication process in an IoD



Source: [9].

Software-based authentication schemes utilize mathematical algorithms, secret keys, and cryptographic methods like RSA and AES to secure communication. One-way hash functions, essential in digital signatures, ensure data integrity by transforming information into fixed-size representations. Message Authentication Codes (MACs) validate both message integrity and authenticity, while Elliptic Curve Cryptography (ECC) delivers RSA-equivalent security with smaller keys and enhanced efficiency in resource-limited environments. Identity-based security integrates traditional logins with biometric methods, such as fingerprints and facial recognition, providing a robust and efficient authentication solution [9].

2.4 GEOTECHNOLOGIES, SATELLITES AND DRONES APPLIED TO FOREST INVENTORY

Using geospatial technologies has played a crucial role in environmental monitoring, enabling the collection and analysis of data on changes in vegetation cover, biodiversity, and environmental impacts [52]. Geotechnologies encompass a set of tools and techniques, including remote sensing systems, geographic information systems (GIS), and satellite positioning, which are widely employed in the biodiversity conservation of forest ecosystems [53] In the context of the IoD, these technologies enhance the accuracy and efficiency of environmental surveys, providing critical support for decision-making [54].

2.4.1 Geotechnologies and Remote Sensing

Remote sensing is a technique that enables the acquisition of information about the Earth's surface without direct physical contact using sensors mounted on satellites, manned aircraft, or drones [55]. This technology is widely used for monitoring forest areas, providing data on biomass, vegetation cover, soil moisture, and environmental degradation [56].

- Among the main techniques used, the following stand out:

- Optical images: Capture vegetation reflectance at different wavelengths, enabling land use and land cover classification [57].

- Synthetic aperture radar (SAR): Uses microwaves to map vegetation structure, being effective even in cloudy or low-light conditions [54].

- LiDAR (Light Detection and Ranging): An active sensor that uses laser pulses to create three-dimensional models of vegetation and soil, providing precise estimates of tree height and biomass volume [53] .

2.4.2 Satellites for Forest Monitoring

Using satellites in forest monitoring has been fundamental for analyzing large areas, allowing the detection of deforestation, vegetation cover changes, and carbon stock estimates [57]. Some of the most commonly used satellites include:

- Landsat (NASA/USGS - National Aeronautics and Space Administration/United States Geological Survey): Provides medium spatial resolution images (30 m) with a long time series since 1972, being widely used in environmental change studies [58].

- Sentinel-2 (ESA - European Satellite Agency): Offers high-resolution multispectral images (10 m) with frequent revisits, making it ideal for continuous forest monitoring [58].

- CBERS (China-Brazil Earth Resources Satellite): Developed in partnership between Brazil and China, it provides free data for environmental and agricultural applications [59].

Each of these satellites has specific characteristics that influence their applicability in forest inventory, such as spatial, spectral, and temporal resolution. Combining these images allows for the generation of high-precision maps for landscape dynamics analysis and sustainable planning.

2.4.3 Integration of Drones and Satellites in Forest Inventory

The fusion of data obtained from drones and satellites has proven to be an effective strategy for improving the accuracy and scalability of environmental studies. While satellites

provide periodic information on large territorial extensions, drones enable detailed surveys in specific areas, allowing the collection of high-resolution data in real-time[54]. The main advantages of this integration include:

- Spatial and temporal complementarity: Satellites cover vast regions but with lower resolution and longer revisit times, while drones offer precise details in smaller areas [60].
- Improvement in data validation: Information collected by drones can be used to calibrate and validate models generated from satellite images [54].
- Monitoring environmental changes: Allows the rapid detection of illegal deforestation and other adverse events that impact the environment [61].

The challenges of this integration include the need for efficient processing of the large volumes of generated data, interoperability among different sensors, and the security of sensitive information transmissions.

2.4.4 Integration of Geotechnology and Drones in Forest Inventory

The growing adoption of geotechnologies in forest monitoring requires robust security measures to ensure the integrity and authenticity of the collected data. In the IoD context, transmitting sensitive geospatial information, such as drone flight coordinates and captured images, must be protected against cyberattacks, including interception and data falsification [13]. The authentication protocol proposed in this dissertation significantly contributes to the protection of these data by offering mechanisms that ensure:

- Authenticity of images and metadata: Preventing unauthorized manipulation of the collected information [62].
- Protection against interception attacks: Only authorized entities can access transmitted data [19].
- Resistance to location spoofing: Preventing spoofing attacks that could compromise the accuracy of environmental surveys [19].

Thus, integrating geotechnologies and secure authentication protocols is essential to strengthen the reliability of environmental studies and promote sustainability in ecosystem monitoring.

2.5 CRYPTOGRAPHIC TECHNOLOGIES

2.5.1 Hash Function

Hash functions are algorithms that transform an input of any size into a fixed-size output, known as a hash value or digest. A critical characteristic of cryptographic hash functions is that, for a specific input, they always produce the same hash value; however, any change to the input results in a completely different hash value. Additionally, these functions are designed to be one-way, meaning it is practically impossible to deduce the original input from the hash value [47].

Beyond ensuring data integrity, hash functions enhance system efficiency by reducing the volume of data processed. Instead of transmitting an entire message for validation, only the hash value needs to be sent and compared, saving bandwidth and processing time. In this way, hash functions not only strengthen the security and integrity of transmitted data but also optimize communication [63].

Hash functions can be categorized into two main types: keyed and non-keyed. In keyed hash functions, a secret key is used during the computation of the hash value, whereas non-keyed hash functions operate without such a key.

A common example of a keyed hash function is the HMAC (Hash-based Message Authentication Code), which is widely applied to ensure message integrity and authentication in secure communications. In contrast, traditional cryptographic hash functions, such as SHA-256 (Secure Hash Algorithm 256-bit), are non-keyed and extensively used in digital signatures, blockchain, and data verification [64].

From a computational perspective, hash functions are implemented using mathematical transformations—such as bitwise operations, modular arithmetic, and compression functions to convert input data into a fixed-size output. These functions are optimized for per-

formance and collision resistance, making them suitable for real-time applications.

2.5.1.1 Security Properties of Cryptographic Hash Functions

A cryptographic one-way hash function can be formally defined as a deterministic function $h : X \rightarrow Y$, where $X = \{0,1\}^*$ is the set of binary strings of arbitrary length, and $Y = \{0,1\}^m$ is the set of binary strings of fixed length m, representing the message digest or hash [47] [65].

To be considered secure, a hash function must satisfy the following properties[47]:

- **Efficient Computation:** For any input $x \in X$, the hash value $h(x)$ must be computable in polynomial time.
- **Preimage Resistance:** Given a hash output $h(x)$, it is computationally infeasible to determine the original input x.
- **Second Preimage Resistance:** Given an input x_1, it is computationally infeasible to find another input $x_2 \neq x_1$ such that $h(x_1) = h(x_2)$.
- **Collision Resistance:** It is computationally difficult to find any two distinct inputs $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$.

According to the birthday paradox, finding a collision requires about $2^{n/2}$ operations for a hash output of n bits, while reversing a hash (preimage attack) would require around 2^n operations [66].

2.5.1.2 Common Cryptographic Hash Functions

The Secure Hash Algorithm (SHA) family includes several widely used cryptographic hash functions such as SHA-1, SHA-2, and SHA-3. SHA-2 consists of variants like SHA-224, SHA-256, SHA-384, and SHA-512, while SHA-3 includes SHA3-224, SHA3-256, SHA3-384, and SHA3-512.

SHA-1, introduced in 1995 by the U.S. National Security Agency (NSA), produces a

160-bit hash output from input blocks of 512 bits. It was initially published by the National Institute of Standards and Technology (NIST) in the Secure Hash Standard (FIPS PUB 180). Over time, newer variants have replaced it due to vulnerabilities. Today, SHA-256 is widely adopted in security-critical applications such as digital signatures (e.g., ECDSA) and blockchain technology.

Table 2.1. Comparison of Common Hash Functions

Hash Function	Output Size (bits)	Speed	Collision Resistance	Type
SHA-1	160	Fast	Moderate (deprecated)	Non-keyed
SHA-256	256	Moderate	Strong	Non-keyed
SHA-3	224–512	Moderate	Very Strong	Non-keyed
HMAC-SHA256	256	Moderate	Strong (with key)	Keyed

Source: adapted from [67].

2.5.2 Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is an asymmetric cryptographic approach that leverages the mathematical properties of elliptic curves over finite fields to implement high-security, resource-efficient cryptographic algorithms. Compared to traditional RSA cryptography, ECC offers the same level of security with significantly smaller key sizes [47].

The efficiency of ECC arises from the computational complexity of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is considered infeasible for sufficiently large keys. Consequently, ECC enables the implementation of security mechanisms that consume less energy and require lower processing capacity [65].

2.5.3 Elliptic Curve Diffie-Hellman (ECDH)

Elliptic Curve Diffie-Hellman (ECDH) is a variation of the Diffie-Hellman key exchange protocol that utilizes Elliptic Curve Cryptography (ECC) to provide a secure means of establishing a shared key between two parties over a public channel [47].

ECDH enables two parties, each with a private key and corresponding public key, to compute a shared key using their private key and the other party's public key. This process generates an identical shared key for both parties without transmitting it directly, minimiz-

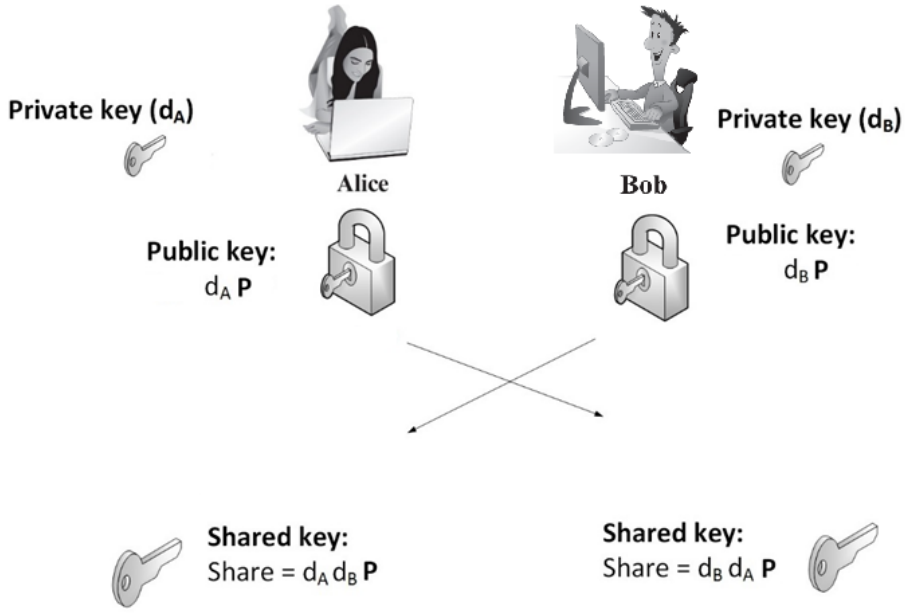
ing interception risks and ensuring a secure, efficient key exchange[47].

Here is an example of an ECDH key exchange between two entities, Alice and Bob:

- Some system parameters are established, such as a large prime number p , an elliptic curve E over a large finite field F_p and a point P on that curve, which serves as a public value.
- Alice and Bob each generate a secret by choosing random numbers: d_A for Alice and d_B for Bob. They perform scalar multiplication over the elliptic curve, producing $d_A P$ and $d_B P$, which are their respective public keys.
- Alice sends to Bob $d_A P$ and Bob sends to Alice $d_B P$.
- Both calculate $d_B P$ and agree on it as the shared key. They can now use $d_A d_B P$ as an encryption key for secure data exchange.

In the scenario described above, the system's security relies on the difficulty for an intruder to derive d_A or d_B when given $d_A P$, $d_B P$, and P . The discrete logarithm problem ensures that it is computationally infeasible to recover these values. Figure 2.6 illustrates the message exchange.

Figure 2.6. ECDH example



Source: adapted from [47].

2.5.4 Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature method based on ECC, widely used to authenticate and ensure the integrity of messages in environments requiring high security and computational efficiency. Leveraging the mathematical properties of elliptic curves, ECDSA enables the generation of compact and robust digital signatures, providing a security level equivalent to algorithms like RSA but with a significantly smaller key size [68].

The applications of ECDSA utilize prime curves over Z_p and binary curves over $GF(2^m)$. For ECDSA, prime curves are employed. The global domain parameters required for the operation of ECDSA are as follows:

- q : A prime number defining the finite field Z_p .
- a, b : Integers specifying the elliptic curve equation defined over Z_p, given by the formula $y^2 = x^3 + ax + b$.
- G : A base point on the elliptic curve, represented as G=(x_g,y_g), used as the starting point for public key computations.
- n : The order of the point G , defined as the smallest positive integer such that $nG = O$, where O is the point at infinity. This value also corresponds to the number of points on the curve.

The ECDSA process is divided into three main stages: key generation, signature generation, and signature verification. Below are the details of each phase [68]:

Key generation: Each signer must generate a pair of keys, one private and one public. The signer, let us call him Bob, generates the two keys using the following steps:

1. Select a random integer $d, d \in [1, n-1]$.
2. Compute $Q = dG$. This is a point in E_q(a,b).
3. Bob's public key is Q, and the private key is d.

Signature generation: Using the public domain parameters and his private key, Bob generates a 320-byte digital signature for message mm by following these steps:

1. Select a random or pseudorandom integer $k, k \in [1, n-1]$.
2. Compute point $P = (x,y) = kG$ and $r = x \bmod n$. If $r = 0$, then go to step 1.
3. Compute $t = k^{-1} \bmod n$.
4. Compute $e = H(m)$, where H is one of the SHA-2 or SHA-3 hash functions.
5. Compute $s = k^{-1}(e + dr) \bmod n$. If $s = O$, then go to step 1.

Signature verification: Alice, knowing the public domain parameters and Bob's public key, verifies Bob's digital signature for the presented message by following these steps:

1. Verify that r and s are integers in the range 1 through $n-1$.
2. Using SHA, compute the 160-bit hash value $e = H(m)$.
3. Compute $w = s^{-1} \bmod n$.
4. Compute $u_1 = ew$ and $u_2 = rw$.
5. Compute the point $X = (x_1,y_1) = u_1 G + u_2 Q$.
6. If $X = O$, reject the signature else compute $v = x_1 \bmod n$.
7. Accept Bob's signature if and only if $v = r$.

We can confirm the validity of this process as follows: if the message received by Alice was indeed signed by Bob, the calculations performed during the verification process will hold true. Here's how:

$$s = k^{-1}(e + dr) \bmod n$$

Then

$$k = s^{-1}(e + dr) \bmod n$$

$$k = (s^{-1}e + s^{-1}dr) \bmod n$$

$$k = (we + wdr) \bmod n$$

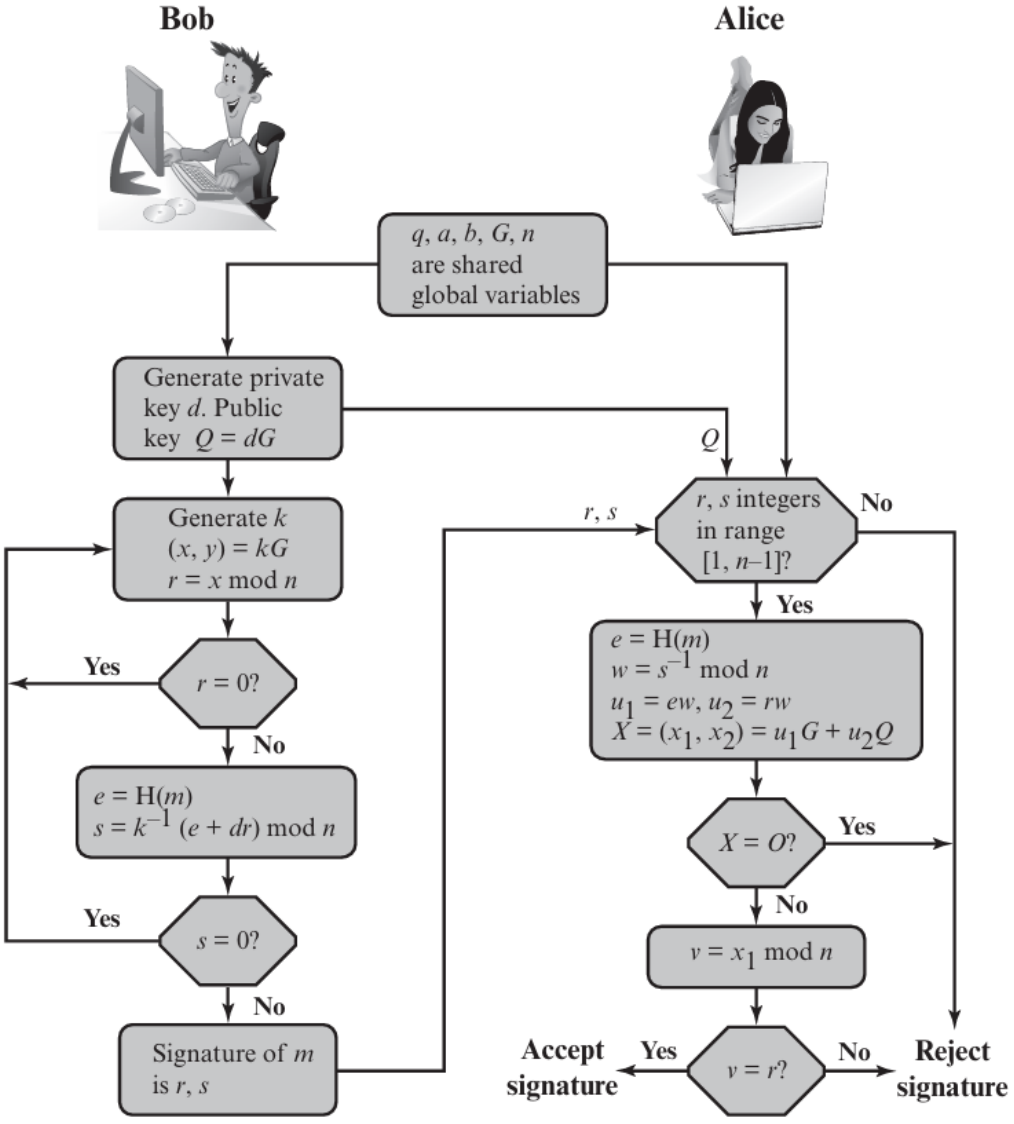
$$k = (u_1 + u_2 d) \bmod n$$

Now consider that

$$u_1 G + u_2 Q = u_1 G + u_2 dG = (u_1 + u_2 d)G = kG.$$

In step 6 of the verification process, we have $v = x_1 \bmod n$, where point $X = (x_1, y_1) = u_1 G + u_2 Q$. Thus we see that $v = r$ since $r = x \bmod n$ and x is the x coordinate of the point kG and we have already seen that $u_1 G + u_2 Q = kG$.

Figure 2.7. ECDSA



Source: adapted from [47].

2.5.5 Aggregate Signatures with ECDSA

Aggregate signatures are a cryptographic technique that allows multiple digital signatures to be combined into a single signature while preserving the ability to authenticate and verify the integrity of all the original messages. When implemented using the Elliptic Curve Digital Signature Algorithm (ECDSA), aggregate signatures provide a lightweight and efficient solution for network environments with bandwidth and processing constraints.

This method enables multiple messages, each containing data and an ECDSA-generated signature, to be combined into a single aggregate signature before transmission to the server. This approach significantly reduces latency and bandwidth requirements by replacing multiple individual signatures with a single aggregated one, optimizing communication and computational efficiency.

2.6 EMERGING TECHNOLOGIES

In recent years, a variety of studies have explored the integration of emerging technologies such as cloud computing and fog computing, to enhance authentication and security in the IoD environment. The integration of IoD with cloud computing, combined with the storage of sensitive information, not only improves network security but also offers greater scalability, data accessibility, and computational efficiency for real-time drone operations and decision-making processes. Fog computing, on the other hand, supports drone mobility and reduces associated computational costs [13].

2.6.1 Biometric Verification Using Fuzzy Extractor

The combination of biometrics and passwords is a common foundation for two-factor authentication systems, leveraging the unique characteristics of biometrics, such as fingerprints, irises, or facial features, for secure identity validation [69]. These keys offer significant advantages: they cannot be forgotten or lost, are extremely difficult to replicate or share, and exhibit high resistance to fraud and unauthorized access. Moreover, biometrics provides greater security than traditional methods like passwords, reducing the risk of au-

thentication data compromise.

However, biometric data is sensitive to noise during capture, such as slight variations in positioning or reading quality, which can hinder exact reproduction. To address these limitations, a fuzzy extractor is employed [70], which generates stable and reproducible cryptographic keys from noisy biometric inputs by applying error correction and randomness extraction techniques [68], ensuring both security and reliability in authentication processes.

Fuzzy extractors operate in two phases: key generation and reproduction. During generation, the user's biometric data (Bio_i) is processed to produce two outputs: a secret key (σ_i), a random, uniform sequence used as confidential data, and an auxiliary public key (τ_i) which aids in future key reproduction. This process is defined as $Gen(Bio_i) =< \sigma_i, \tau_i >$.

In the reproduction phase, the user provides new biometric data (Bio_i'), that may contain noise or variations. The fuzzy extractor uses τ_i to correct these differences and recreate the original secret key, σ_i . Reproduction is successful if the difference between Bio_i and Bio_i' is within a tolerable threshold (e_t). This is represented as $Rep(Bio_i', \tau_i) = \sigma_i$, where Bio_i' is the noisy biometric data, τ_i is the auxiliary public key, and σ_i is the recreated secret key [69].

Fuzzy extractors enhance the reliability of biometric authentication by ensuring consistent key generation and reproduction, even with slight data variations. They produce highly secure keys (σ_i) with a minimal probability of being guessed, strengthening authentication systems.

2.6.2 Fog Computing

Fog computing is an extension of cloud computing that brings storage and processing resources closer to the network edge, where data is generated. Instead of sending all collected data to a centralized cloud server, fog computing enables this data to be processed and stored on local servers, known as fog nodes. This approach reduces latency, improves scalability, and provides faster response times for applications requiring real-time processing.

Fog computing is particularly valuable for applications demanding high performance

and low latency. Additionally, it offers scalability, allowing systems to handle increasing data volumes and workloads efficiently. This decentralized model also enhances security, as data remains at the network edge, reducing the exposure of sensitive information to attacks during transmission to distant servers.

2.7 AVISPA TOOLS

Formal security verification using automated tools has gained significant traction among researchers in the security domain. These tools enable the validation of security protocols, ensuring their robustness against attacks such as replay and man-in-the-middle attacks. Under the Dolev-Yao (*DY*) model [71]. several verification tools have been developed for protocols involving access control, authentication, and key agreement. Among these is the Automated Validation of Internet Security Protocols and Applications (AVISPA) [72].

The AVISPA tool, developed by the AVISPA project, is a widely used framework for validating security-sensitive protocols. Its primary purpose is to formalize protocols, define security objectives, and model threats to enable automated vulnerability detection. Protocol validation is achieved by specifying message exchanges in the High-Level Protocol Specification Language (HLPSL), which organizes interactions in a sender/receiver format [72].

AVISPA supports various cryptographic functionalities, including asymmetric and symmetric encryption, hash functions, non-atomic keys, and exponentiation operations [73]. The protocol's structure is defined by specific roles assigned to agents or entities involved in the authentication process [50].

To verify security, AVISPA provides four back-ends, two of which were employed to validate the protocols proposed in this work: the On-the-Fly Model Checker (OFMC) and the Constraint-Logic-based Attack Searcher (CL-AtSe). These back-ends analyze the security of message exchanges and produce clear assessments: "SAFE" if security properties are preserved or "UNSAFE" if vulnerabilities are detected [13].

The OFMC back-end generates a binary tree to represent potential decisions within the protocol. It provides detailed outputs, including the time required for analysis, the duration

of attack searches, the number of nodes visited, and the depth reached during processing. Conversely, the CL-AtSe back-end models each protocol step by applying constraints on the adversary's knowledge, limiting the analysis to a predefined number of cycles. It translates HLPSL code into constraints, facilitating the identification of vulnerabilities. Results include metrics such as the number of analyzed cycles, steps reached, translation time, and total protocol analysis time [50].

2.8 CHAPTER CONCLUSIONS

This chapter presented the fundamental concepts necessary for understanding the proposed authentication protocols for the IoD. Initially, the IoD architecture, its main applications, and specific security challenges were described. Key cyber threats that could compromise the integrity, confidentiality, and availability of communications were discussed, emphasizing the need for robust and efficient authentication protocols.

Additionally, geoprocessing and remote sensing technologies, including satellites and drones, were explored, highlighting their crucial role in environmental monitoring, particularly in forest inventory. The integration of satellite imagery with drone-collected data was identified as an effective approach to improving the accuracy of environmental analyses. However, this data fusion also introduces challenges in terms of security and privacy, reinforcing the need for reliable authentication mechanisms.

The chapter also examined cryptographic technologies relevant to authentication mechanisms, such as ECC, ECDH, ECDSA, and aggregate signatures. These approaches were selected to balance security and computational efficiency, enabling resource-constrained devices, such as drones, to operate with low energy consumption and reduced processing time. Additionally, emerging solutions, including biometric authentication based on Fuzzy Extractors and fog computing, were analyzed as methods to enhance security and scalability in IoD networks.

Finally, the use of the AVISPA tool for the formal verification of authentication protocols was highlighted as an essential strategy to ensure resistance against known attacks and compliance with established security requirements.

The concepts discussed in this chapter provide the theoretical foundation for the development of the authentication protocols proposed in the subsequent chapters. Building on this theoretical framework, the next chapter introduces a multi-factor authentication protocol for IoD, integrating elliptic curve cryptography and biometric authentication to enhance the security of communications between users and drones.

CHAPTER 3

A MULTI-FACTOR USER AUTHENTICATION PROTOCOL FOR THE INTERNET OF DRONES ENVIRONMENT

Abstract. *Due to the popularization of unmanned aerial vehicles (UAVs), many of which are known as drones, the Internet of Drones (IoD) has gained significant importance over the past years in several areas. It has been implemented in various fields (e.g., military, rescue, agriculture, and entertainment). It is enabled by implementing several drones in different flight zones for undertaking specific tasks, commonly collecting data in real-time and providing them to users who communicate with them through their mobile devices. However, owing to the critical nature of information and the utilization of public communication channels, privacy and security issues must be considered. Authentication protocols can be adopted for reliable and secure communication, enabling data exchange between the user and the drone and resisting attacks such as man-in-the-middle and replay. On the other hand, developing an efficient protocol for meeting security properties while considering resource consumption requirements is challenging due to the peculiarities of IoD environments. This chapter proposes a user authentication scheme for IoD based on biometry and elliptic curve cryptography, to be used in a set of scenarios, such as logistics, public safety, and emergency rescue operations. Its robustness was evaluated by a security analysis and a semi-automatized verification by the AVISPA tool, which confirmed that the scheme resists several known attacks against passive/active adversaries and meets security properties such as anonymity, authenticity, and nontraceability. Moreover, it shows better communication and computational performance in comparison to other authentication protocols from the literature.*

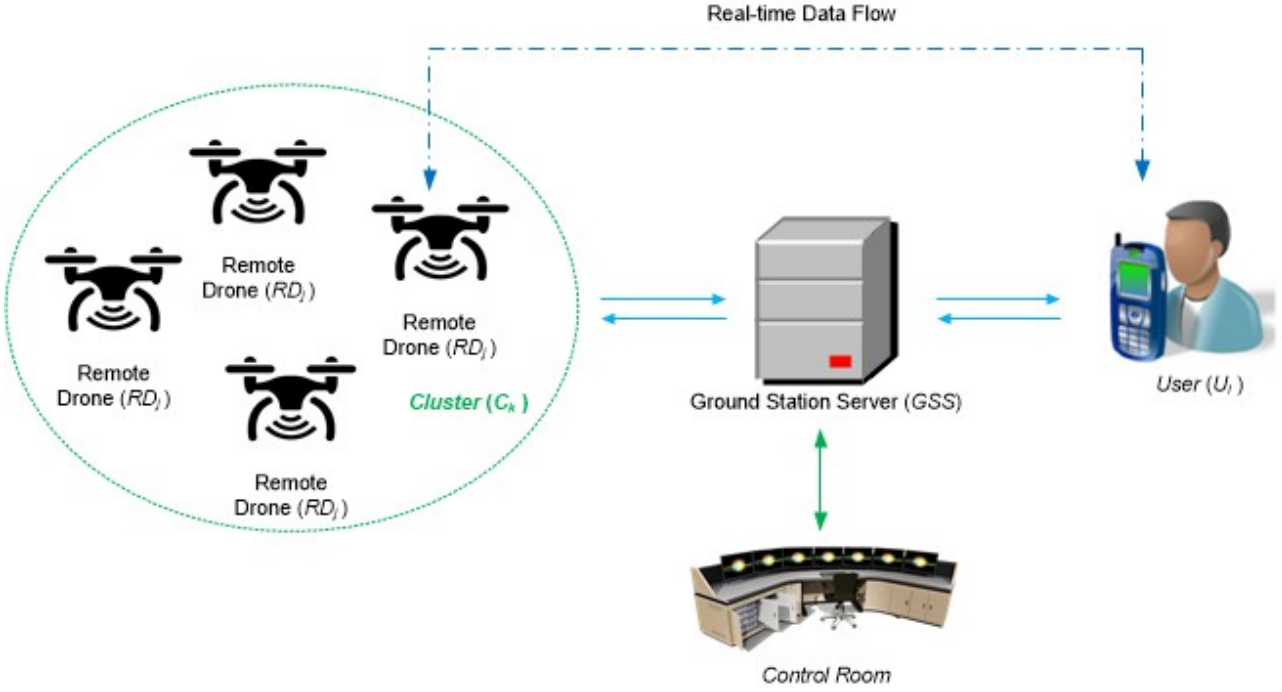
3.1 INTRODUCTION

Due to the continuous miniaturization of processors and sensors, wireless connectivity, and the advent of 5G and 6G networks, the number of drone solutions has increased toward improving lifestyles [74]. This has led to the successful adoption of IoD to support different

applications, such as pack delivery, medicine delivery in areas affected by the pandemic, traffic surveillance, and search and rescue operations. Its use has significantly increased in several fields, from agriculture to industry, government to private organizations, and rural areas to smart cities [75]. In 2022, the giant retailer Amazon officially started offering its Lockeford customers in California a pack-delivery service via drones [76]. AT&T has also implemented drones for automating its inspections of cellular towers and Dubai (UAE) recently introduced drones in transport, launching its flying taxi service [77].

The Internet of Drones (IoD) involves a network control architecture that provides coordinated access to a controlled aerial space to unmanned aerial vehicles (UAVs), generally called drones [3]. Drones play a fundamental role in IoD networks and have been incorporated as units of communication, computation, energy, and control, as well as board advanced actuators and sensors (e.g., cameras, accelerometers, and gyroscopes) for data collection and measurements of altitude, speed, and location, among other tasks. As shown in Figure 3.1, architecture usually includes remote drones, users, and a ground station server (*GSS*). Remote drones collect/monitor information on the environment, whereas users aim to access such data in real-time [9]. *GSS* in an element connected to the control room, which controls the information collected by the drones and the frequency of their collection through wireless channels.

Figure 3.1. Architecture of the IoD



Source: Own authorship.

Drones frequently collect data on geographical location, high-resolution images and videos, environmental data such as air quality and weather conditions, and information on critical infrastructure like power grids and transportation systems [78] [79]. These data are sensitive because they can reveal personal details, compromise individuals' privacy, or expose vulnerabilities in essential infrastructures. The collection of such data necessitates robust security and privacy mechanisms to protect against unauthorized access and misuse [80] since remote malicious users may have access to restricted information available on a drone.

In this sense, secure information exchange among elements in an IoD environment represents a critical requirement for realizing the benefits of IoD and its applications [33], where node authentication is a primary necessity for securing an IoD network. Since authentication verifies the identity of IoD elements, only authorized and legitimate users should be granted access to sensitive information [25].

Such data collection necessitates robust security and privacy mechanisms to protect against unauthorized access and misuse [80]. These mechanisms include advanced encryption, strict access control, and authentication. Encryption ensures that transmitted and

stored data are inaccessible to unauthorized individuals, while strict access control guarantees that only users with proper permissions can interact with drone systems [81]. Authentication plays a crucial role in verifying the identity of users and devices and ensuring that only legitimate entities can access and manipulate sensitive data [82]. It is imperative in the IoD context due to the high mobility and diverse usage scenarios of drones, where rapid and secure identity verification is necessary to maintain the integrity and reliability of operations [5]. Without effective authentication, the entire IoD system is vulnerable to attacks by intruders who can compromise critical data, threatening the privacy and security of the collected information.

Existing solutions for authentication in the IoD environment often fail to balance lightweight attributes, efficiency, and robust security adequately. Many current protocols either focus on enhancing security at the expense of computational and communication efficiency or prioritize lightweight operations that compromise security robustness [33]. For instance, some protocols use traditional cryptographic methods such as RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) that are too resource-intensive for drones, which have limited processing power and battery life [83]. These traditional methods, while providing robust security, often require significant computational resources, making them unsuitable for the constrained environments in which drones operate.

Moreover, the dynamic nature of IoD networks and the high computational demand of current authentication protocols pose significant challenges. These protocols often require extensive computational resources, increasing energy consumption and inefficiencies in resource-constrained environments such as drones [84]. The heavy computational and communication overheads of these protocols result in significant resource depletion, making them less effective in maintaining seamless and secure communication [85]. Thus, developing lightweight and efficient authentication mechanisms is critical to optimize resource utilization without compromising security [80].

To meet the aforementioned requirements, this chapter proposes a novel authentication protocol based on biometrics, passwords, and elliptic curve cryptography (ECC). It ensures secure communication between remote drones and users and efficiently balances the need for robust security with lightweight attributes and operational efficiency. By employing

cryptographic operations, such as XOR and hash functions in combination with ECC, the protocol offers a lightweight and secure method that is feasible for drones with limited resources.

3.1.1 Main contributions

The main contributions of this research include:

1. A safe and efficient user authentication protocol based on biometrics, passwords, ECC and lightweight cryptographic operations is proposed to increase efficiency in an IoD environment.

2. Evaluation of the protocol's security through analyzing its robustness against several known attacks and the essential functionalities required for an IoD environment.

3. Formal security verification by semi-automatized tool Automated Validation of Internet Security Protocols and Applications (AVISPA).

4. Performance analysis of the protocol through an evaluation of the communication and computational costs and comparison to other schemes available in the literature.

3.1.2 Structure of the chapter

The remainder of the chapter is structured as follows: Section 2 focuses on related work, with brief discussions on the characteristics and limitations of each work; Sections 3 and 4 describe the model of the system and the threat model, respectively; Section 5 introduces the protocol; Section 6 reports a security analysis; Section 7 is devoted to evaluating the computational and communication costs of the scheme, in comparison to those of other protocols; and finally, Section 8 provides the conclusions and outlines future work.

3.2 RELATED WORK

This section provides an overview of several proposals published in the past few years, aiming to solve issues related to security and, more specifically, user authentication in the IoD environment.

Initially, some references involving overviews about security in IoD are presented. Among the recent surveys on the security challenges related to IoD environments are those developed by Abdelmaboud et al. [10], Yang et al. [8], Michailidis et al. [9], and Omolara et al. [46]. Abdelmaboud et al. [10] discussed the requirements, recent advances, and challenges in IoD research, mainly focusing on privacy and authentication. They highlighted the necessity of prioritizing authentication to protect real-time information from intruders who could alter original messages during operations.

Building on these concepts, Yang et al. [8] reviewed the latest developments in IoD security research, emphasizing authentication techniques and blockchain-based schemes. They highlighted the high-security vulnerabilities associated with direct access to drone data without proper authentication and that advanced, cost-effective biometric sensors integrated into drones, along with lightweight feature extraction and matching algorithms, will make biometric authentication for IoD increasingly attractive to researchers and industry professionals. Also mentioned that although balancing security and design complexity simultaneously is challenging, this is an approach worth exploring.

Michailidis et al. [9] further expanded on the topic by reviewing both software and hardware-based authentication mechanisms for UAV networks. They explored conventional technologies such as hash functions and public key infrastructure (PKI), alongside emerging technologies like elliptic curve cryptography (ECC), to enhance the security of IoD environments. Their work outlines critical aspects for developing future authentication schemes, particularly considering the mobility of drones during secure data exchanges.

Omolara et al. [46] recently conducted an exhaustive survey on drone security and privacy issues. The security concerns were thoroughly analyzed, with a special focus on cybersecurity, and emphasizing that the development of protocols and the deployment of drones in practice require a balance between security and performance, considering computational

costs. Furthermore, the authors mention that using traditional cryptographic methods to implement authentication schemes for drones can increase computational costs, and the development of strategic solutions that balance costs and security remains an unresolved research issue.

On the other hand, several researchers have proposed authentication protocols for the IoD environment, specifically designed to optimize drone resource consumption and provide efficient security. Among them, Srinivas et al. [5] developed a lightweight authentication protocol called TCALAS (Temporal Credential-Based Anonymous Lightweight Authentication Scheme) using lightweight symmetrical hash functions, suitable for drones with limited resources. However, it fails to resist traceability and impersonation attacks due to the immutable pseudo-identity used between sessions.

Chen et al.[86] introduced a privacy-preserving authentication protocol based on digital signatures, ECC, and cryptographic hash functions for UAV communication control systems. The authors claimed the protocol is secure against malicious attacks and efficiently provides anonymity, confidentiality, and data integrity. However, the protocol fails to incorporate a signature, timestamp, or any means to identify alteration of the first message transferred via an insecure channel. Therefore, if the message is intercepted, altered, and sent to a legitimate entity, it will not be possible to verify if the received message was altered, making the scheme susceptible to replay attacks.

Wazid et al.[87] developed an authentication protocol for industrial environments utilizing ECC and hash functions that can be adapted for IoD. However, due to its reliance on precise synchronization between the involved devices, this can become a critical issue in an IoD environment. In an IoD scenario, communication delays or packet loss can occur due to mobility and variability of network conditions. Lack of synchronization can lead to authentication or key management failures, allowing attackers to exploit these flaws to compromise the system's security. These attacks can interfere with key exchange or manipulate exchanged messages, making the system susceptible to desynchronization attacks.

Tanveer et al. [11] developed the Robust Authenticated Key Management Protocol (RAMP-IoD), using ECC and hash functions. Although it has proven to be secure and addresses the mobility of drones with the addition phase of drones, it does not handle revoking drone

credentials in the system in case of long-term inactivity, which can pose a threat. If an adversary captures a drone, it could return to the system without needing new registration and communication and computing expenses are somewhat high.

Nikooghadam et al. [16] designed a user authentication protocol for IoD based on ECC for smart city surveillance. Despite its stability and resistance to known attacks under the random oracle model, it lacks anonymity and traceability properties due to the use of a constant pseudo-identity in all sessions. In response to this, Alzahrani et al. [88] proposed an enhanced security scheme using lightweight symmetric key primitives and ECC, which avoids plaintext identity disclosure and constant session parameters, but fails to withstand offline password guessing attacks and have a significant processing and communication cost, which could adversely affect the drone's computational capabilities.

Bhattarai et al. [89] proposed *liteA4*, a lightweight and anonymous authentication and key agreement protocol for the Internet of Drones (IoD). To mitigate inconsistencies in Physical Unclonable Function (PUF) outputs, the authors incorporated a fuzzy extractor in conjunction with error correction codes. Although the protocol supports the generation of data-type–specific session keys, it remains vulnerable to denial-of-service (DoS) attacks and does not offer user untraceability within the drone communication framework.

Tanveer et al. [90] recently introduced SEAF-IoD, an authentication framework designed for user-drone interaction within the IoD environment. The framework incorporates PUFs, Fuzzy Extractors, and the XOR operation to ensure lightweight security. Although considered secure, the scheme lacks discussion regarding the revocation and reissue mechanisms, as well as protection against scenarios involving stolen smart devices.In the same year, Tanveer et al. [89] proposed PAF-IoD, which incorporates SHA, authenticated encryption with associative data (AEAD), XOR, and Fuzzy Extractor techniques. However, this scheme also lacks a discussion on the revocation and reissuance phase, as well as strategies to mitigate attacks involving stolen smart devices.

These studies, though diverse in their approaches, demonstrate a logical progression in addressing authentication issues in the IoD environment. Each protocol aims to tackle security aspects using cryptographic techniques and authentication methods. Yet, they still face specific limitations that underscore the need for continued research to develop more

comprehensive and robust solutions.

Table 3.1 compares these studies, presenting the limitations of the discussed proposals in the last column, which will be addressed as potential improvements in our proposed protocol, to be described in Section 3.5.

Table 3.1. Authentication Protocols Summary — Security Features and Functionality

Protocols	Year	Techniques applied	Formal Verification Tool	Limitations
Srinivas et al. [5]	2019	Three-factor (smart card, user password, and biometrics). ECC and one-way cryptographic hash function; based on temporal credentials	AVISPA	Nonanonymity and nonuntraceability. No resistance to personification attacks based on stolen verifier counterattacks. Nonexistence of a Revocation remote drone phase.
Chen et al. [86]	2020	Two-factor (smart card, user password); ECC and one-way cryptographic hash function.	BAN Logic	Nonanonymity and nonuntraceability. No Forward/Backward Secrecy. No resistance to Denial of Service (DoS) attack. Nonexistence of user password update, dynamic Remote drone addition, and revocation of drone phases.
Nikooghadam et al. [16]	2021	Two-factor (smart card, user password); ECC and one-way cryptographic hash function	Scyther Tool	Nonanonymity and nonuntraceability. Exposes secret parameters.
Wazid et al. [87]	2021	Three-factor (smart card, user password, and biometrics). ECC, XOR, and one-way cryptographic hash function	AVISPA	No resistance to desynchronization attack. Nonexistence of a Revocation remote drone phase.
Alzahrani et al. [88]	2021	Two-factor (smart card, user password); ECC and one-way cryptographic hash function	Scyther Tool	Nonexistence of a Revocation remote drone phase. No resistance to offline password-guessing attacks.
Tanveer et al. [11]	2022	Three-factor (smart card, user password, and biometrics). ECC, AES-CBC-256 encryption, XOR, and one-way cryptographic hash function	Scyther Tool	Nonexistence of a revocation remote drone phase.
Bhattarai et al. [89]	2024	Physical unclonable function, hash function, and bitwise XOR	AVISPA	Vulnerable to DoS attack and lack of untraceability. Nonexistence of a revocation remote drone phase.
Tanveer et al. [90]	2024	PUF, Fuzzy Extractor, XOR, and one-way cryptographic hash function	Scyther Tool	Nonexistence of a revocation remote drone phase. No discussion about reissue stage and smart device stolen attack.

Source: Own authorship.

The next section presents the System Model considered for the proposal.

3.3 MODEL OF THE SYSTEM

Fig. 2 illustrates the system model, which is composed of three main elements, namely, Remote Drone(RD_j), User(U_i), and Ground Station Server(GSS), as in [5], [16] and [33]:

- Remote Drone (RD_j): an element controlled by remote or autonomous controls using software and incorporated sensors.

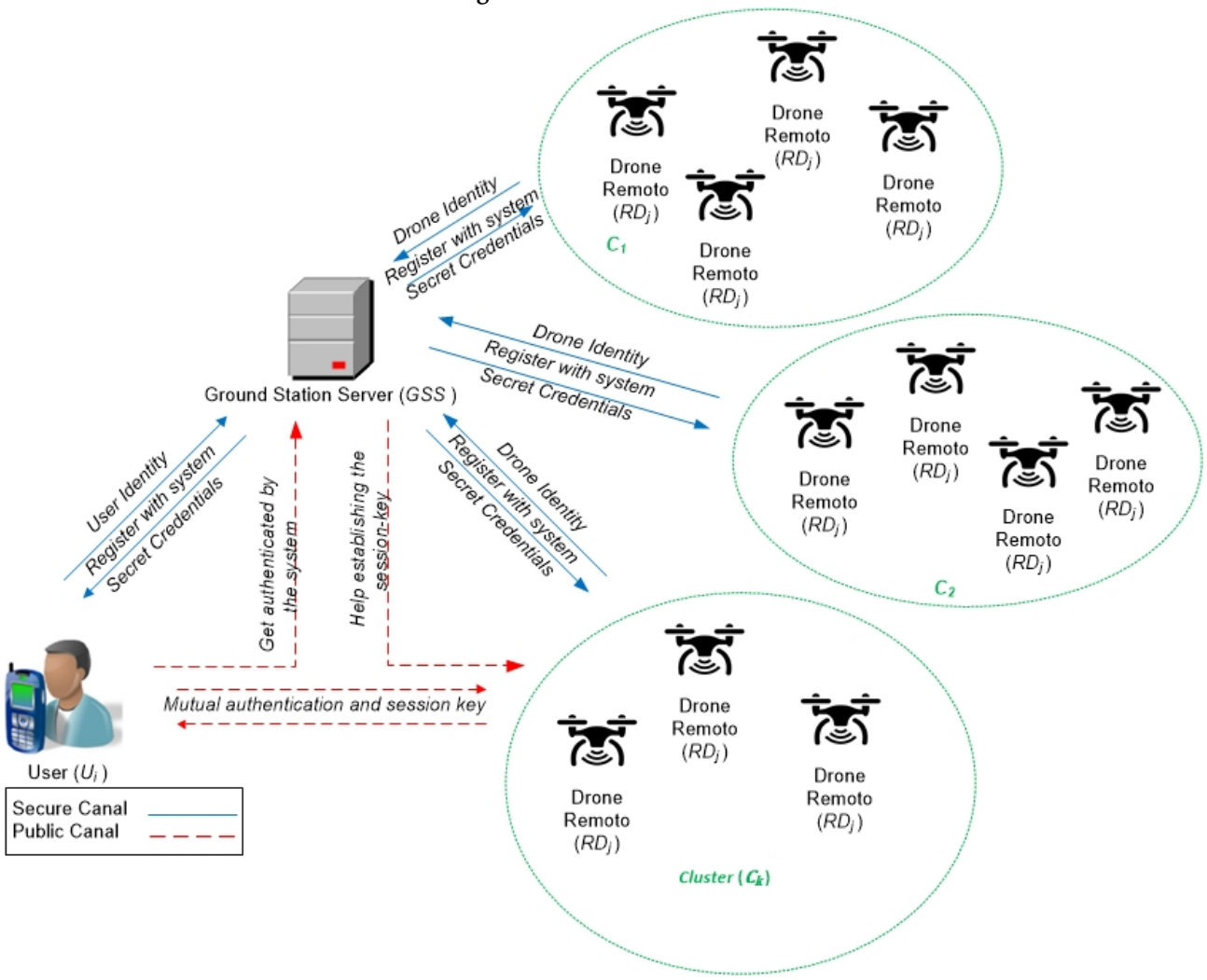
- User (U_i): an element interested in accessing data from designated remote drones in real-time in a specific flight zone in IoD implementation.

- Ground Station Server (GSS): the only reliable entity of the system and an element that enables users to authenticate in one or more drones.

The flight area is divided into several flight zones in which several RD_j are implemented, forming clusters(C_k). Traditional wireless networks and promising technologies such as 5G/6G cellular networks can provide wireless connectivity in a specific cluster [91]. U_i can monitor/access remote drones implemented in a specific flight zone with their mobile device.

Both U_i and RD_j forward their ID credentials and registration requests to GSS, which registers them and sends them and the system's secret credentials to be used in the authentication process and establishment of the session key. U_i and RD_j are subsequently mutually aided by GSS. After a successful authentication, a session key is established between the user U_i and remote drones RD_j, thus, enabling a secure data exchange.

Figure 3.2. Network Model



Source: Own authorship.

3.4 THREAT MODELS

The development of the protocol considered Dolev-Yao (DY), a threat model commonly adopted in authentication scenarios in implementations for IoD was considered in the development of the protocol [79] [80] [87]. Therefore, it is assumed that:

- Adversary A can capture exchanged messages, exclude or modify their content, or even insert malicious content in all communications established through public channels. A exerts no control over the communication established through a secure channel.

- A can represent an authentic node (drone or user) in some region and start commu-

nication with *GSS*; however, it cannot access *GSS* to obtain its private key without permission.

- *A* can be a malicious user or a user outside the system.

The Canetti and Krawczyk threat model (*CK*) [92] was also considered for the development of the scheme since it has been adopted in authentication protocol projects [5] [87] [93]. According to the model, A can alter messages, as in the DY model, but also compromise session keys, private keys, and other session states through session sequestration attacks.

Despite session states and secret information being compromised in a specific session, such information must not jeopardize the secrecy of credentials of other parts involved in communication [5]. A user authentication protocol projected on the CK must preserve forward and backward secrecy.

Below are the possible threat models for the system model proposed for IoD:

- Physical capture threat: An adversary can physically capture a drone or access a user's mobile device. It attacks a drone/mobile device to obtain access to the information stored in the memory through energy analysis attacks [94]. It then exposes such information and starts authentication with *GSS* with either a user or a drone.

- Traffic analysis threat: The packets exchanged among drones, users, and the GSS compose the traffic. A can analyze the traffic exchanged between system elements to extract valuable data from devices.

- Access control threat: An intruder can understand all rules and policies and how a legitimate entity can communicate, thus, obtaining access for controlling and altering privileges, permissions, authorizations, and authentication, which may lead to substantial damage.

- Identity-falsification threat: An adversary can successfully masquerade a legitimate identity using the false identity of an actual drone or user, thus, obtaining access to and controlling the public communication channel.

3.5 PROPOSED SCHEME

This section introduces a novel user authentication protocol that uses biometry and passwords for the Internet of Drones and involves six phases, namely, system initialization and registration, authentication, password update, mobile device replacement, dynamic addition of drones, and revocation of drones.

- System initialization phase: *GSS* selects the system's public parameters and registers remote drones (RD_j) and users U_i. The calculated and distributed parameters are further used in the authentication stage.

- Authentication phase: U_i and RD_j mutually authenticate with the aid of *GSS* and establish a common session key so that RD_j can securely transmit data to U_i.

- User password update phase: U_i can update the current password. This functionality was designed due to security issues related to the system, which requires a periodic update of the user's passwords.

- Mobile device replacement phase: This phase is performed if a registered user's authorized mobile device MD_i has been stolen or lost. U_i can obtain a new mobile device, $MD_{U_i}^{new}$, and enable it to access the network.

- Dynamic remote drone addition phase: This phase is performed if a new drone must be dynamically implemented due to either arbitrary physical damage to a drone caused by an adversary or accidental reasons such as lack of battery and internal circuit problems.

- Remote drone revocation phase: This phase is performed when the authorized RD_j is inoperative for a period longer than the one allowed by the system. This phase is necessary since the RD_j connection can be lost due to a fall or a failure or captured by an adversary.

The notations in Table 3.2 have been adopted for discussion and analyses of the scheme.

Table 3.2. Notations Used

Symbol	Definition
U_i	i^{th} User, i = 1,2,3,. . . , n
RD_j	j^{th} Remote Drone, j = 1,2,3,. . . , m
C_k	k^{th} Fly Zone (Cluster), k = 1,2,3,. . . , l
GSS	Ground Station Server
MD_{U_i}	Mobile Device U_i
p	a k bit prime
Z_p	a prime field of order p
$E_p(a,b)$	A nonsingular elliptic curve of the form: $y^2 = x^3 + ax + b$ with $4a^3 + 27b^2 \neq 0$.
P	Generator point
$h(\cdot)$	Collision-Resistant One-Way Hash Function, $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$, where $l \geq 256$ bits
s_{GSS}	Private key GSS
s_{RD_j}	Private key RD_j
T	Current timestamp
ΔT	Maximum transmission delay
A	Adversary
ID_{RD_j}	RD_j identity
ID_{U_i}	U_i identity
CID_k	C_k identity
TID_{RD_j}	RD_j temporary identity
TID_{U_i}	U_i temporary identity
PW_{U_i}	Password of i^{th} User (U_i)
Sec_{RD_j}	secret between GSS and RD_j
Sec_{U_i}	secret between GSS and U_i
E_{Sec_x}/D_{Sec_x}	Encryption/Decryption operation that uses the secret between x and *GSS*
SK	Session key
RTS_j	Timestamp of RD_j record
b_{U_i} , f_{U_i},q_{U_i},y_{RD_j}	Random numbers $\in$ Z_p
Gen ($\cdot$)	Generation process in fuzzy extractor [70]
Rep ($\cdot$)	Reproduction process in fuzzy extractor [70]
σ_i	Biometric secret key of U_i for Bio_{U_i}
τ_i	Public reproduction parameter of U_i for Bio_{U_i}
Bio_{U_i}	Biometric template of U_i
$\|\|, \oplus$	Concatenation, bitwise XOR operations

Source: Own authorship.

3.5.1 System initialization phase

GSS selects the system's parameters and registers drones RD_j and users U_i so that can proceed to the offline authentication phase, i.e., the adversary cannot alter messages sent during this phase. *GSS* selects a large prime number p, an elliptical curve $E_p(a,b)$, a generator point $P \in E_p(a,b)$ of order p, a hash function $h(\cdot)$ (e.g., SHA-256), and a random number $s_{GSS} \in Z_p$ as its private key. It attributes an identity to each cluster of drones CID_k , stores parameters $\{E_p(a,b), p, P, h(\cdot), s_{GSS} \in Z_p, \text{CID}_k | 1 \leq k \leq n_c\}$ in its memory, and publishes $\{E_p(a,b), p, P, h(\cdot)\}$, as the public parameters of the system. The registration of RD_j, starts with the remote drone sending its identity ID_{RD_j} and the registration request to *GSS*, which then checks in its database whether the drone can register in the system. If so, *GSS* chooses a random number $s_{RD_j} \in Z_p$ to be used as a private key for the calculation of the temporary identity of RD_j and the secret between it and RD_j, as follows:

$$\text{TID}_{\text{RD}_j} = h\left(\text{ID}_{\text{RD}_j} \| s_{\text{RD}_j}\right), \tag{3.1}$$

$$\text{Sec}_{\text{RD}_j} = h\left(\text{TID}_{\text{RD}_j} \| s_{\text{GSS}} \| s_{\text{RD}_j} \| \text{CID}_k\right). \tag{3.2}$$

It then selects a timestamp RTS_{RD_j} to register the registration time of the drone, stores parameters $\{ID_{RD_j}, TID_{RD_j}, Sec_{RD_j}, RTS_{RD_j}\}$ in its database, and sends $\{TID_{RD_j}, CID_k, Sec_{RD_j}, s_{RD_j}, h(\cdot)\}$, to RD_j, which stores them in its memory.

Toward registering in *GSS* through a secure channel and receiving secret credentials from the environment, U_i chooses its user's identity ID_{U_i} and password PW_{U_i}. It then prints its biometric Bio_{U_i} in MD_{U_i} , selects a random number $b_{U_i} \in Z_p$, and calculates

$$\text{Gen}(\text{Bio}_{U_i}) = (\sigma_i, \tau_i), \tag{3.3}$$

$$\text{HPW}_{U_i} = h\left(\text{PW}_{U_i} \| \sigma_i\right), \tag{3.4}$$

$$\text{TID}_{U_i} = h\left(\text{ID}_{U_i} \| b_{U_i}\right). \tag{3.5}$$

U_i is supposed to have a list of identities ID_{RD_j} of remote drones RD_j to which it wishes to access data in real time, as in [5] and [95]. When requesting registration by sending credentials $\{ID_{U_i}, TID_{U_i}, HPW_{U_i}, ID_{RD_j}\}$ to *GSS* , the user also requires the temporary identities of the remote drones he/she can access. After receiving the registration request from U_i,

GSS checks whether ID_{U_i} is in its database and whether the user can request registration in the system. In the case of a negative response, the registration request is denied. However, if U_i can be registered, GSS selects a random number $f_{U_i} \in Z_p$ and calculates

$$\mathrm{Sec}_{U_i} = h(\mathrm{TID}_{U_i} \| f_{U_i} \| s_{\mathrm{GSS}}), \tag{3.6}$$

$$C_{U_i} = \mathrm{HPW}_{U_i} \oplus \mathrm{Sec}_{U_i}. \tag{3.7}$$

It then stores $\{ ID_{U_i}, Sec_{U_i}, TID_{U_i}, f_{U_i} \}$ in its database and sends $\{ C_{U_i}, TID_{RD_j} \}$ to mobile device U_i , which calculates

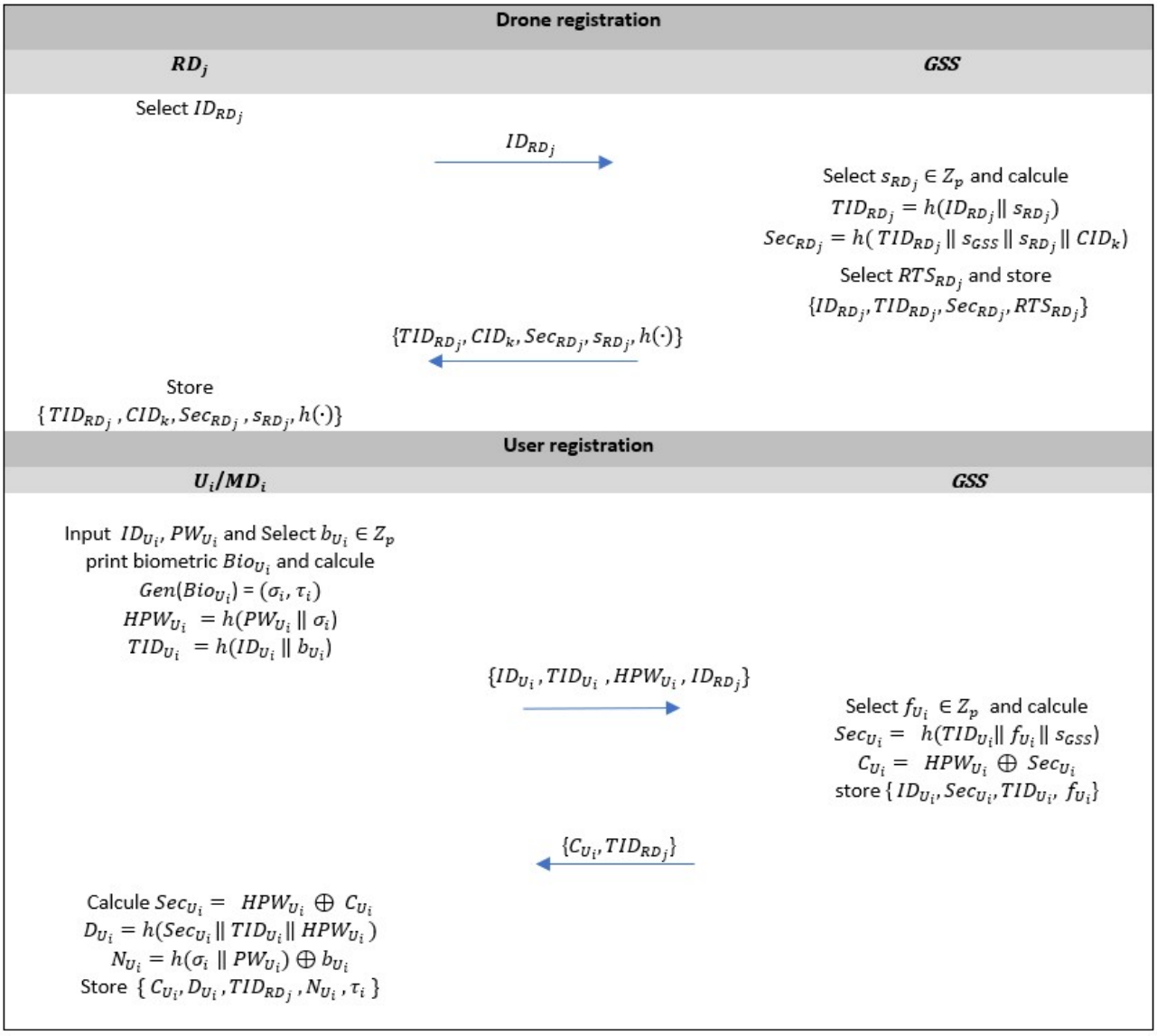
$$\mathrm{Sec}_{U_i} = \mathrm{HPW}_{U_i} \oplus C_{U_i}, \tag{3.8}$$

$$D_{U_i} = h(\mathrm{Sec}_{U_i} \| \mathrm{TID}_{U_i} \| \mathrm{HPW}_{U_i}), \tag{3.9}$$

$$N_{U_i} = h(\sigma_i \| \mathrm{PW}_{U_i}) \oplus b_{U_i}. \tag{3.10}$$

Finally, U_i stores credentials $\{C_{U_i}, D_{U_i}, TID_{RD_j}, N_{U_i}, \tau_i\}$ in MD_{U_i} to complete the registration process. The complete procedure is shown in Figure 3.3.

Figure 3.3. Registration phase



Source: Own authorship.

3.5.2 Authentication phase

U_i and RD_j usually authenticate aided by GSS and establish a common session key. RD_j can then securely send data to U_i through a public channel. The stages for the execution of the phase are detailed in what follows. The complete procedure is shown in Figure 3.4.

U_i inserts its ID_{U_i}, PW_{U_i} and prints its biometry Bio'_{U_i} in its mobile device MD_{U_i}, which calculates

$$\sigma'_i = \text{Rep}(\text{Bio}'_{U_i}, \tau_i), \tag{3.11}$$

$$b_{U_i} = N_{U_i} \oplus h(\sigma_i' \| \mathrm{PW}'_{U_i}), \tag{3.12}$$

$$\mathrm{TID}_{U_i} = h(\mathrm{ID}_{U_i} \| b_{U_i}), \tag{3.13}$$

$$\mathrm{HPW}'_{U_i} = h(\mathrm{PW}_{U_i} \| \sigma_i'), \tag{3.14}$$

$$\mathrm{Sec}_{U_i} = C_{U_i} \oplus \mathrm{HPW}'_{U_i}, \tag{3.15}$$

$$D'_{U_i} = h(\mathrm{Sec}_{U_i} \| \mathrm{TID}_{U_i} \| \mathrm{HPW}'_{U_i}). \tag{3.16}$$

MD_{U_i} checks if $D'_{U_i} \stackrel{?}{=} D_{U_i}$. In case of a negative correspondence, the authentication phase is immediately terminated; otherwise, MD_{U_i} validates the authenticity of U_i locally, generates a timestamp T_1, selects a random number $q_{U_i} \in Z_p$, and performs the following operations, similarly to [96], as follows:

$$H_1 = h(\mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_1), \tag{3.17}$$

$$E_{U_i} = E_{\mathrm{Sec}_{U_i}}(H_1, q_{U_i}, \mathrm{TID}_{\mathrm{RD}_j}). \tag{3.18}$$

GSS receives message M_1 at T_2 and checks whether timestamp T_1 is within the transmission time limit $| T_2 - T_1 | \leq \Delta\mathrm{T}$. In the case of a negative response, it terminates the session; otherwise, it recovers (TID_{U_i}, Sec_{U_i}) from the database and calculates

$$(H_1, g_{U_i}, \mathrm{TID}_{\mathrm{RD}_j}) = D_{\mathrm{Sec}_{U_i}}(E_{U_i}), \tag{3.19}$$

$$H_1' = h(\mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_1). \tag{3.20}$$

If $H_1' \stackrel{?}{=} H_1$ results in a negative correspondence, the authentication phase is immediately terminated; otherwise, *GSS* validates the authenticity of U_i, recovers Sec_{RD_j} from the database, and calculates

$$H_2 = h(\mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_2), \tag{3.21}$$

$$E_{\mathrm{GSS}} = E_{\mathrm{Sec}_{\mathrm{RD}_j}}(H_2, q_{U_i}, \mathrm{TID}_{U_i}), \tag{3.22}$$

$$M_2 = \{T_2, E_{\mathrm{GSS}}\}. \tag{3.23}$$

GSS sends message $M_2 = \{T_2, E_{GSS}\}$ to RD_j, which receives it at moment T_3 and checks if the timestamp T_2 is within the transmission time limit $| T_3 - T_2 | \leq \Delta\mathrm{T}$. In case of a negative

response, it terminates the session; otherwise, if RD_j is positive, it recovers Sec_{RD_j} from the database and calculates

$$(H_2, q_{U_i}, \mathrm{TID}_{U_i}) = D_{\mathrm{Sec}_{\mathrm{RD}_j}}(E_{\mathrm{GSS}}), \tag{3.24}$$

$$H_2' = h(\mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_2). \tag{3.25}$$

RD_j checks $H_2^{'} \stackrel{?}{=} H_2$ and the authentication phase is immediately terminated if there is a negative correspondence. Otherwise RD_j validates the authenticity of GSS, selects a random number $y_{RD_j} \in Z_p$, and calculates

$$\mathrm{SK}_{\mathrm{RD}_j} = h(\mathrm{TID}_{\mathrm{RD}_j} \| y_{\mathrm{RD}_j} q_{U_i} P \| \mathrm{TID}_{U_i}), \tag{3.26}$$

$$H_3 = h(\mathrm{SK}_{\mathrm{RD}_j} \| \mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_3), \tag{3.27}$$

$$M_3 = \{T_3, y_{\mathrm{RD}_j} P, H_3\}. \tag{3.28}$$

RD_j sends a message to U_i. After receiving $M_3 = \{T_3, y_{RD_j}P, H_3\}$ at T_3, U_i checks if it is within the limit of transmission time $| T_4 - T_3 | \leq \Delta \mathrm{T}$. In case of a negative response, it terminates the session; otherwise, it calculates

$$\mathrm{SK}_{U_i} = h(\mathrm{TID}_{\mathrm{RD}_j} \| q_{U_i} y_{\mathrm{RD}_j} P \| \mathrm{TID}_{U_i}), \tag{3.29}$$

$$H_3' = h(\mathrm{SK}_{U_i} \| \mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_3). \tag{3.30}$$

The mobile device of U_i checks if $H_3 \stackrel{?}{=} H_3^{'}$. In the case of a negative correspondence, the authentication phase is immediately terminated; otherwise, U_i validates the authenticity of RD_j and U_i and RD_j establish a common session key, given by:

$$\mathrm{SK} = \mathrm{SK}_{U_i} = \mathrm{SK}_{\mathrm{RD}_j} = h(\mathrm{TID}_{\mathrm{RD}_j} \| y_{\mathrm{RD}_j} q_{U_i} P \| \mathrm{TID}_{U_i}). \tag{3.31}$$

Figure 3.4. Authentication phase

Source: Own authorship.

3.5.3 User password update phase

This phase describes the way the proposed scheme treats the registered user who must replace the current password with a new one password with no assistance of *GSS*. U_i inserts

his/her ID_{U_i}, PW_{U_i} and $Bio^{'}_{U_i}$ in the mobile device MD_{U_i}, which calculates

$$\sigma_i' = \mathrm{Rep}(\mathrm{Bio}'_{U_i}, \tau_i), \tag{3.32}$$

$$\mathrm{HPW}'_{U_i} = h(\mathrm{PW}_{U_i} \,\|\, \sigma_i), \tag{3.33}$$

$$\mathrm{Sec}_{U_i} = \mathrm{C}_{U_i} \oplus \mathrm{HPW}'_{U_i}, \tag{3.34}$$

$$\mathrm{D}'_{U_i} = h(\mathrm{Sec}_{U_i} \,\|\, \mathrm{HPW}'_{U_i} \,\|\, \mathrm{TID}_{U_i}). \tag{3.35}$$

MD_{U_i} checks the authenticity of $\mathrm{D}'_{U_i} \stackrel{?}{=} D_{U_i}$. In case of a negative response, the password change request is aborted; otherwise, MD_{U_i} informs U_i that it must provide a new password. U_i chooses a new password PW_i^{new} and MD_{U_i} calculates

$$\mathrm{HPW}^{\mathrm{new}}_{U_i} = h(\mathrm{PW}^{\mathrm{new}}_{U_i} \,\|\, \sigma_i), \tag{3.36}$$

$$\mathrm{N}^{\mathrm{new}}_{U_i} = h(\sigma_i \,\|\, \mathrm{PW}^{\mathrm{new}}_{U_i}) \oplus b_{U_i}, \tag{3.37}$$

$$\mathrm{C}^{\mathrm{new}}_{U_i} = \mathrm{Sec}_{U_i} \oplus \mathrm{HPW}^{\mathrm{new}}_{U_i}, \tag{3.38}$$

$$\mathrm{D}^{\mathrm{new}}_{U_i} = h(\mathrm{Sec}_{U_i} \,\|\, \mathrm{HPW}^{\mathrm{new}}_{U_i} \,\|\, \mathrm{TID}_{U_i}). \tag{3.39}$$

Finally, MD_{U_i} replaces parameters $\{N_{U_i}, C_{U_i}, D_{U_i}\}$ by $\{\mathrm{N}^{new}_{U_i}, C^{new}_{U_i}, D^{new}_{U_i}\}$.

3.5.4 MD_{U_i} mobile device replacement phase

This phase is performed if the mobile device MD_{U_i} of an authorized registered user has been stolen or lost. U_i can obtain a new $MD^{new}_{U_i}$ and enable it. The stages to be performed are detailed in what follows.

U_i keeps identity ID_{U_i}, but chooses a new password PW_i^{new}. He/she must enter again with their biometry Bio_{U_i}, which can be the same however, the system will evaluate it with a new one. ID_{U_i} then creates a random number $b^{'}_{U_i}$ to calculate $Gen\ (Bio^{new}_{U_i}) = (\ \sigma^{new}_i, \tau_i)$, $TID'_{U_i} = h(\mathrm{ID}_{U_i} \,\|\, b'_{U_i})$ and $HPW^{\mathrm{new}}_{U_i} = h(\mathrm{PW}^{\mathrm{new}}_{U_i} \,\|\, \sigma^{\mathrm{new}}_i)$ and sends $TID^{'}_{U_i}$ and $HPW^{new}_{U_i}$ to GSS through a secure channel, which checks if user ID_{U_i} can request a new registration in the system. In case of a negative response, it refuses the $MD^{new}_{U_i}$ registration; otherwise, it calculates

$$\mathrm{Sec}^{\mathrm{new}}_{U_i} = h\Big(\mathrm{TID}'_{U_i} \,\|\, f_{U_i} \,\|\, s_{GSS}\Big), \tag{3.40}$$

$$C_{U_i}^{\text{new}} = \text{Sec}_{U_i}^{\text{new}} \oplus \text{HPW}_{U_i}^{\text{new}}. \tag{3.41}$$

It replaces credentials $\{TID_{U_i}, Sec_{U_i}\}$ by $\{TID_{U_i}^{'}, Sec_{U_i}^{new}\}$ in the database and sends $\{C_{U_i}^{new}, TID_{RD_j}\}$ to $MD_{U_i}^{new}$, which then calculates

$$D_{U_i}^{\text{new}} = h\Big(\text{Sec}_{U_i} \,\|\, \text{HPW}_{U_i}^{\text{new}} \,\|\, \text{TID}_{U_i}^{\prime}\Big), \tag{3.42}$$

$$N_{U_i}^{\text{new}} = h\Big(\sigma_i^{\text{new}} \,\|\, \text{PW}_{U_i}^{\text{new}}\Big) \oplus b_{U_i}^{\prime}. \tag{3.43}$$

Finally, MD_{U_i} stores credentials $\{C_{U_i}^{new}, D_{U_i}^{new}, TID_{RD_j}, N_{U_i}^{new}, \tau_i, Gen(\cdot), Rep(\cdot), h(\cdot)\}$.

3.5.5 Dynamic Remote Drone Addition Phase

This phase is performed if a new drone must be dynamically reimplemented due to either physical damage caused by an adversary or accidental reasons such as lack of battery or internal circuit problems, among others. The phase is based on Srinivas et al. [5]. The stages below must be followed for the implementation of a new drone.

A new drone RD_j^{new} sends a registration request to GSS selecting an exclusive identity $ID_{RD_j}^{new}$ and transmitting it through a secure channel. GSS checks the $ID_{RD_j}^{new}$ exclusivity by comparing it to the identities stored in the database. If $ID_{RD_j}^{new}$ corresponds to any identity registered, the registration is aborted; otherwise, GSS selects a random number $s_{RD_j}^{new} \in Z_p$ and calculates

$$\text{TID}_{RD_j}^{\text{new}} = h\Big(s_{RD_j}^{\text{new}} \,\|\, \text{ID}_{RD_j}^{\text{new}}\Big), \tag{3.44}$$

$$\text{Sec}_{RD_j}^{\text{new}} = h\Big(\text{TID}_{RD_j}^{\text{new}} \,\|\, s_{GSS} \,\|\, s_{RD_j}^{\text{new}} \,\|\, \text{CID}_k\Big). \tag{3.45}$$

GSS selects a timestamp $RTS_{RD_j}^{new}$, stores ($ID_{RD_j}^{new}$, $TID_{RD_j}^{new}$, $Sec_{RD_j}^{new}$, $RTS_{RD_j}^{new}$) in its database and sends $\{TID_{RD_j}^{new}, Sec_{RD_j}^{new}, CID_k, h(.), E_p(a,b), p, P, s_{RD_j}^{new}\}$ through a secure channel. RD_j^{new} receives the parameters and stores them in its memory.

3.5.6 Remote Drone Revocation Phase

This phase is performed when the authorized RD_j remains inoperative for a period longer than the one allowed by the system. The phase is necessary, since the RD_j connection

may have been lost due to a fall, failure, or capture by an adversary or even controlled by an undesirable entity. If data on the credentials of RD_j remain in GSS , the drone may represent a threat. The registered and revoked identities of drones ID_{RD_j} are stored in the GSS' database on a list called ReL, as in Jan et al. [95]. The database is periodically consulted by the system since it contains the dates of registration time of drones RTS_{RD_j}. If the inoperability time of a drone is longer than the one allowed by the system, a revocation procedure is conducted. GSS inserts the ID_{RD_j} of RD_j on ReL as a revoked drone, searches for credentials $\{Sec_{RD_j}, TID_{RD_j}, S_{RD_j}\}$ in its database, and excludes them. If the remote drone wishes to return to the system, it must forward a new registration request to GSS, which checks in its database if RD_j can request a new registration or if it has been registered as dropped, captured, or compromised.

3.6 SECURITY ANALYSIS

This section is devoted to an informal security analysis and a simulation verification by AVISPA to demonstrate the scheme's security.

3.6.1 Informal security analysis

This section addresses an informal security analysis for evaluating the security of the proposed scheme, which has been shown to resist security attacks and to meet the requirements of mutual authentication, anonymity, and session key agreement.

3.6.1.1 Mutual authentication

The participants involved (U_i, GSS, and RD_j) must authenticate themselves mutually. GSS authenticates U_i after receiving parameters H_1, q_{U_i}, TID_{RD_j} in message $M_1=\{T_1,E_{U_i}\}$ from U_i , calculates $H_1' = h\left(\mathrm{TID}_{U_i} \| \mathrm{TID}_{RD_j} \| T_1\right)$ and checks if $H_1' \stackrel{?}{=} H_1$. In case of a positive correspondence, it authenticates U_i. RD_j authenticates GSS after receiving parameters H_2, q_{U_i}, TID_{U_i} from GSS in message $M_2 = \{T_2,E_{GSS}\}$, calculates $H_2' = h\left(\mathrm{TID}_{U_i} \| \mathrm{TID}_{RD_j} \| T_2\right)$ and checks if $H_2' \stackrel{?}{=} H_2$. In the case of a positive correspondence, RD_j authenticates GSS. U_i

authenticates RD_j after receiving message $\mathrm{M}_3 = \{T_3, y_{\mathrm{RD}_j}P, M_{\mathrm{RD}_j}\}$, calculates $\mathrm{H}_3 = h\left(\mathrm{SK}_{U_i} \parallel \mathrm{TID}_{U_i} \parallel \mathrm{TID}_{\mathrm{RD}_j} \parallel T_3\right)$, and checks if $H_3 \stackrel{?}{=} \mathrm{H}_3'$. In case of a positive correspondence, U_i authenticates RD_j. Therefore, the protocol provides mutual authentication. In case of a positive correspondence, U_i authenticates RD_j. Therefore, the protocol provides mutual authentication.

3.6.1.2 Anonymity and Untraceability

The real identities of U_i and RD_j are never exchanged through an insecure channel. Moreover, temporary identities used $TID_{\mathrm{RD}_j} = h\left(\mathrm{ID}_{\mathrm{RD}_j} \parallel s_{\mathrm{RD}_j}\right)$ and $TID_{U_i} = h\left(\mathrm{ID}_{U_i} \parallel f_{U_i}\right)$ are calculated with the use of different random numbers in the registration phase, in which all information exchange is performed through a secure channel, i.e., saved from A. According to threat model *DY*, if *A* intercepts the messages exchanged through a public channel, it cannot recognize a device connecting new and old messages. M_1 , $M_{2,}$ and M_2 demonstrate the scheme's security.

3.6.1.3 Resistance to Denial of Service (DoS) attack

In M_1 , $M_{2,}$ and M_3 exchanged in the authentication phase, the element that receives a message checks if the timestamp is valid before conducting complex calculations. Random numbers are also used in the authentication phase to avoid generating repetitive messages. Moreover, authentication is checked before the operation involving an elliptic curve, which is considered costly compared to others. As a result, the proposed scheme is secure against such types of denial-of-service attacks.

3.6.1.4 Forward/backward secrecy

The protocol guarantees forward/backward secrecy by using random values recently generated in each authentication session during the session key calculation. Session key SK includes $q_{U_i}y_{RD_j}P$, where q_{U_i} and y_{RD_j} are randomly selected numbers that cannot be easily calculated or guessed. If A discovers old system keys, it cannot use them in future

authentication sessions (backward secrecy). On the other hand, if it discovers future session keys, it cannot use them in past authentication sessions (forward secrecy). Therefore, A cannot determine the keys of past and future sessions even if the current session key is compromised.

3.6.1.5 Ephemeral Secret Leakage Attack

Under model CK, adversary A can obtain random numbers generated in each session. Let us suppose q_{U_i} and y_{RD_j} are short-term ephemeral secrets known by A. A can try to calculate current session key $SK = h\left(\mathrm{TID}_{\mathrm{RD}_j} \| q_{U_i} y_{\mathrm{RD}_j} P \| \mathrm{TID}_{U_i}\right)$ based on those short-term secrets; however, it cannot calculate TID_{RD_j} and TID_{U_i} without long-term secrets. Let us now assume TID_{RD_j} and TID_{U_i} are ephemeral long-term secrets known by A. It still cannot construct session key SK since it does not know short-term secrets q_{U_i} and y_{RD_j}. Therefore, the protocol avoids ephemeral secret leakage and attacks because the construction of its session key uses long-term and short-term keys.

3.6.1.6 Session key agreement

U_i and RD_j calculate a common session key $SK = SK_{U_i} = SK_{RDj} = h(TID_{RDj} \| q_{U_i}, y_{RDj} \| \mathrm{TID}_{U_i})$ and do not transmit it through a public channel, thus, guaranteeing session key agreement and security.

3.6.1.7 Resistance to stolen verifier attack

A can steal information from a legally registered user $U_{i.}$ However, TID_{U_i}, C_{U_i}, and D_{U_i} are updated every session, and even if they are compromised, A cannot obtain the session key since it would require y_{RD_j} and q_{U_i} calculate it. Such numbers are inaccessible and randomly selected. The same occurs if A accesses the memory of an $RD_{j,}$ hence, the information stored there. TID_{RD_j} and Sec_{RD_j} are also updated in each session, and the adversary cannot obtain the session key, which is calculated as in U_i, thus, proving that the protocol resists stolen verifier attack.

3.6.1.8 Resistance to offline password guessing attack

Let us suppose an attacker A has lost/stolen MD_{U_i} and tries to extract information from its memory using power analysis methods [94]. Having the extracted credentials from lost or stolen MD_{U_i} of U_i, A fails to guess HPW_{U_i} from extracted parameters correctly C_{U_i},D_{U_i},TID_{RD_j},N_{U_i}, τ_i since he/she needs secret parameters σ_i, Sec_{U_i}, D_{U_i} and ID_{U_i}. Therefore, the protocol also resists offline password-guessing attacks.

3.6.1.9 Resistance to capture of remote drone attacks

According to adversary model CK , if A can capture RD_j and access the information stored in the memory, it can obtain $\{ID_{RD_j}$,TID_{RD_j},CID_k,Sec_{RD_j},s_{RD_j},$h(\cdot)\}$. However, it cannot calculate session key $SK_{\mathrm{RD}_j} = h\left(\mathrm{TID}_{\mathrm{RD}_j} \| y_{\mathrm{RD}_j} q_{U_i} P \| \mathrm{TID}_{U_i}\right)$, since it cannot calculate $y_{RD_j} g_{U_i} P$ due to the CDHP. Moreover, the session key established between a user and a drone in the system is different for each remote drone in the environment because of the unique credentials of each drone $\{ ID_{RD_j}$,TID_{RD_j},Sec_{RD_j},$s_{RD_j}\}$. Consequently, a compromised RD_j leads to no consequence on the session keys among U_i and the noncompromised remaining drones, proving the protocol resists the capture of remote drone attacks.

3.6.1.10 Resistance to drone-personification attack

If A attempts to impersonate RD_j, it must create a message $M_3 = \{ T_3$,$y_{RD_j} P$, $H_3 \}$ for U_i to authenticate it and calculate $H_3 = h\left(\mathrm{SK}_{\mathrm{RD}_j} \| \mathrm{TID}_{U_i} \| \mathrm{TID}_{\mathrm{RD}_j} \| T_3\right)$. Due to the lack of knowledge on secret parameters SK_{RD_j},TID_{U_i},TID_{RD_j} , A cannot calculate H_3, thus, failing to impersonate RD_j, which proves the protocol is robust to drone personification attacks.

3.6.1.11 Resistance to privileged insider attack

The user managing GSS can act as a privileged insider and access parameters received and stored. However, as discussed in the user's registration phase, secret credentials PW_{U_i} and the biometry of U_i are not sent to GSS . Therefore, the privileged insider of GSS cannot obtain the secret credentials of U_i, i.e., the protocol resists such an attack.

3.6.1.12 Resistance to man-in-the-middle attack

According to the threat models adopted, A can intercept messages exchanged through a public channel and try to perform an MITM attack. In the proposed scheme, the authentication phase includes a timestamp and the creation of hash functions in each phase. Messages M_1 and M_2 are encrypted with hash functions calculated in the registration phase; therefore, A cannot generate authentication messages, and the authentication process fails for the intruder. The technique suggested protects against such an attack.

3.6.1.13 Resistance to desynchronization attack

The credentials of U_i,RD_j, and GSS are not altered during the authentication stage, and neither U_i nor RD_j need to synchronize the credentials with GSS in that phase. Therefore, even if A intercepts M_1,M_2, or M_3 who controls the public channel according to the CK model adopted, it creates no hurdle for SK in the upcoming session key between U_i and RD_j participants, proving the scheme is safe against desynchronization attack.

3.6.1.14 Resistance to replay attack

The protocol uses timestamps T_x ($1 \leq x \leq 4$) after message exchange to verify the freshness of the messages transmitted. Therefore, if A reproduces an old message, the receiver can detect it by checking the date/time stamp update. In addition, all participants of the protocol adopt different recently calculated random values in each authentication process, i.e., the protocol resists replay attack.

The protocol accomplishes all security objectives analyzed and is resistant to all attacks considered in this IoD environment, thus, showing robustness regarding security. Table 3.3 shows a comparison among the proposed scheme and those of [88] and [11].

Table 3.3. Security Properties

Attributes	Alzahrani et al.[88]	Tanveer et al. [11]	Protocol Proposed
Mutual authentication	Yes	Yes	Yes
Anonymity and Untraceability	Yes	Yes	Yes
Resistance to Denial of Service (DoS) attack	Yes	Yes	Yes
Forward/Backward Secrecy	Yes	Yes	Yes
Ephemeral Secret Leakage Attack	No	Yes	Yes
Session key agreement	Yes	Yes	Yes
Resistance to stolen verifier attack	Yes	Yes	Yes
Resistance to offline password guessing attack	No	Yes	Yes
Resistance to drone-capture attack	Yes	Yes	Yes
Resistance to drone-personification attack	Yes	Yes	Yes
Resistance to privileged insider attack	Yes	Yes	Yes
Resistance to man-in-the-middle attack	Yes	Yes	Yes
Resistance to desynchronization attack	Yes	Yes	Yes
Resistance to replay attack	Yes	Yes	Yes
User password update phase	No	Yes	Yes
Mobile device replacement phase	No	Yes	Yes
Dynamic Remote Drone addition phase	No	Yes	Yes
Drone revocation phase	No	No	Yes

Source: Own authorship.

3.6.2 Formal security verification by AVISPA

Complementing the results obtained through the previously conducted informal analysis, this section addresses the formal security verification by employing a semi-automated tool. The proposed scheme was simulated for a formal security verification using the broadly accepted Automated Validation of Internet Security Protocols and Applications (AVISPA), a semi-automated validation tool that verifies the security robustness of authentication protocols by checking the secrecy of key parameters and vulnerability to intruders.

AVISPA examines network security protocols and applications codified by High-Level

Protocol Specification Language (HLPSL), which is composed of basic roles that define several candidates and configurations of characters that describe situations of essential roles. The roles do not depend on each other, thus, obtaining some preliminary data per parameter and interacting with other roles via channels [72]. The AVISPA output format is accessed by one of the four back ends, namely., "On-the-Fly Model Checker (OFMC)", “Constraint Logic-based Attack Searcher (CL-AtSe)", “SAT-based Model Checker (SATMC)”, and “Tree automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP)”[68]. The input is converted in a format called “Intermediate Format (IF)” and output in a format called “Output format (OF)”. OF shows the security analysis results of the protocol.

To validate the proposed scheme, we employed software tools such as SPAN (version: SPAN-Ubuntu-10.10-light) and Oracle VM Virtual Box (version: 7.0.6 r155176). The HLPSL source code of the proposed scheme contains five roles, namely, User, GSS, Drone , session and environment, as shown in Figures 3.5, 3.6, 3.7 and 3.8, respectively. AVISPA uses a special identifier i for the intruder. OFMC and CL-ASTE, two back ends of AVISPA tool, were used to validate the scheme. The simulation result of the protocol with the use of ATSE and OFMC back ends of AVISPA shows the protocol is safe (see Figures 3.9 and 3.10, respectively).

Figure 3.5. User Role (HLPSL source code)

```
%%%%%%%%%%%%  User  %%%%%%%%%%%%%%
role user(Ui, GSS, RDj : agent, SecureChannel1: symmetric_key, P,H: hash_func, SND, RCV : channel(dy))
played_by Ui
def=
local State: nat,
   IDui, PWui,TIDj, TIDui, HPWui, Bui, Taui, BIOi, Sigmai, Fui, Sgss, Secui, Cui, Dui, IDrdj, CIDk, Nui, T1, T2, T3: text,
   Qui, Yrdj, H1, H2, H3, Eui, Egss, SKij, Srdj,RTSrdj, Secrdj: text
const sp1,sp2,sp3,sp4,sp5,sp6,sp7,sp8, ui_gss_qui, ui_gss_t1, gss_ui_t3, gss_rdj_t2, gss_ui_Yrdj, rdj_gss_ng, rdj_ui_yrdj, rdj_ui_t3: protocol_id
init State :=0
transition

%%%Registration phase
1. State = 0 /\ RCV(start) =|>
State':= 1 /\ Bui' := new() /\ Sigmai' := new() /\ Taui' := new()
      /\ HPWui' := H(PWui.Sigmai') /\ TIDui' := H(IDui.Bui')
      /\ SND({IDui.TIDui'.HPWui'}_SecureChannel1)
      /\ secret({PWui}, sp1, {Ui}) /\ secret({IDui,HPWui',TIDui'}, sp2, {Ui,GSS})
2. State = 1 /\ RCV ({(xor(H(PWui.Sigmai').H(H(IDui.Bui').Fui'.Sgss'))).H(IDrdj.Srdj')}_SecureChannel1)=|>
State' := 2  /\ Secui':= xor(H(Sigmai'.PWui).(xor(H(PWui.Sigmai').H(H(IDui.Bui').Fui'.Sgss'))))
   /\ Dui' := H((xor(H(H(IDui.Bui').Sgss'.Fui').H(PWui.Sigmai')).H(IDrdj.Srdj')).H(PWui.Sigmai').H(IDui.Bui'))
   /\ Nui' := xor(H(Sigmai'.PWui).Bui')
   /\ secret({Secui', Dui',Nui'}, sp3, {Ui})

%%%Login & Authentication phase
   /\ Qui' := new() /\ T1' := new()
   /\ H1' := H(H(IDui.Bui').H(IDrdj.Srdj').T1')
   /\ Eui' := ({H1'.Qui'.H(IDrdj.Srdj')}_Secui')
   /\ SND(Eui'.T1')
   %Ui has freshly generated the values Qui and T1 for GWN
   /\ witness(Ui,GSS,ui_gss_qui,Qui')  /\ witness(Ui,GSS,ui_gss_t1,T1')
3. State = 2 /\ RCV(T3.P(Yrdj').H(H(H(IDrdj.Srdj').P(Yrdj'.Qui').H(IDui.Bui').H(IDrdj.Srdj').T3'))) =|>
   %Ui acceptance of T3 and Yrdj generated for Ui by Rdj
State' := 3 /\ request(RDj,Ui,rdj_ui_yrdj,Yrdj')  /\ request(RDj,Ui,rdj_ui_t3,T3')
end role
```

Source: Own authorship.

Figure 3.6. *GSS* Role (HLPSL source code)

```
%%%%%%%%%%%%%%  GSS  %%%%%%%%%%%%%%%%%%
role gss(Ui, GSS, RDj : agent, SecureChannel1, SecureChannel2: symmetric_key, P,H: hash_func, SND, RCV : channel(dy))
played_by GSS
def=
local State: nat,
   IDui, PWui,TIDj, TIDui, HPWui, Bui, Taui, BIOi, Sigmai, Fui, Sgss, Secui, Cui, Dui, IDrdj, CIDk, Nui, T1, T2, T3: text,
   Qui, Yrdj, H1, H2, H3, Eui, Egss, SKij, Srdj, RTSrdj, Secrdj: text
const sp1,sp2,sp3,sp4,sp5,sp6,sp7,sp8, ui_gss_qui, ui_gss_t1, gss_ui_t3, gss_rdj_t2, gss_ui_Yrdj, rdj_gss_ng, rdj_ui_yrdj, rdj_ui_t3: protocol_id
init State := 0
transition

%%%Registration phase
1. State = 0 /\ RCV({IDui.H(IDui.Bui).H(PWui.Sigmai)}_SecureChannel1) =|>
State' :=1 /\ Fui' := new()
   /\ Secui' := H(H(IDui.Bui).Fui'.Sgss)
   /\ Cui':= xor(H(PWui.Sigmai).Secui')
   /\ SND({Cui'.H(IDrdj.Srdj)}_SecureChannel1)
   /\ secret({Fui,Secui},sp5,{Ui,GSS})
2.State = 1 /\ RCV(start) =|>
State' := 2 /\ Srdj' := new() /\TIDj' := H(IDrdj.Srdj')
   /\ Secrdj':= H(TIDj'.Sgss.Srdj'.CIDk)
   /\ SND({TIDj.Secrdj}_SecureChannel2)
   /\ secret({TIDj,Secrdj},sp5,{RDj,GSS})

 %%Login & Authentication phase
3. State = 2
   /\ RCV(T1'.({H1'.Qui'.H(IDrdj.Srdj')}_Secui')) =|>
State' := 3 /\ T2' := new()
   /\ H2' := H(H(IDui.Bui).TIDj.T2')
   /\ Egss' := ({(H(IDui.Bui).TIDj.T2').Qui'.(H(IDui.Bui))}_Secrdj)
   /\ SND(T2'.Egss')
   /\ witness(GSS, RDj, gss_rdj_t2, T2')
   /\ witness(GSS,RDj, gss_rdj_srdj,Srdj')
end role
```

Source: Own authorship.

Figure 3.7. Drone Role (HLPSL source code)

```
%%%%%%%%%%%%%%Drone%%%%%%%%%%%%%%
role drone(Ui, GSS, RDj : agent, SecureChannel1,SecureChannel2 : symmetric_key, P,H:hash_func, SND, RCV : channel(dy))

played_by RDj
def=
local State: nat,
   IDui, PWui,TIDj, TIDui, HPWui, Bui, Taui, BIOi, Sigmai, Fui, Sgss, Secui, Cui, Dui, IDrdj, Nui, CIDk, T1, T2, T3: text,
   Qui, Yrdj, H1, H2, H3, Eui, Egss, SKij, Srdj, RTSrdj, Secrdj: text
const sp1,sp2,sp3,sp4,sp5,sp6,sp7,sp8, ui_gss_qui, ui_gss_t1, gss_ui_t3, gss_rdj_t2, gss_ui_Yrdj, rdj_gss_ng, rdj_ui_yrdj, rdj_ui_t3: protocol_id
init State := 0
transition

%%%Registration phase
1. State = 0 /\ RCV(start)=|>
%Send registration request to the GSS securely
State':= 1 /\ SND({IDrdj}_SecureChannel2)
   /\ secret({IDrdj},sp7,{Ui,GSS})
%Receive RDj from the GSS securely
2. State = 1 /\ RCV({H(IDrdj.Srdj').CIDk.Secrdj'}_SecureChannel2) =|>
  State':= 2 /\ secret({Srdj,Sgss,Secrdj},sp8,{GSS})

%%Login & Authentication phase
3.State = 2 /\ RCV(T2.({(H(IDui.Bui').H(IDrdj.Srdj').T2').Qui'.(H(IDui.Bui'))}_Secrdj')) =|>
    State':= 3 /\ secret({Qui'},sp9,{GSS})
   /\ T3' := new() /\ Yrdj' := new()
   /\ SKij' :=(H(IDrdj.Srdj').P(Yrdj.Qui).H(IDui.Bui'))
   /\ H3' := (SKij'.H(IDui.Bui').H(IDrdj.Srdj').T3')
   %Send request to the UI via open channel
   /\ SND(T3'.P(Yrdj).H3')
   %Rdj has freshly generated the values T3 and Yrdj for the Ui
   /\ witness(RDj,GSS,rdj_ui_t3,T3') /\ witness(RDj,GSS,rdj_ui_yrdj,Yrdj')
end role
```

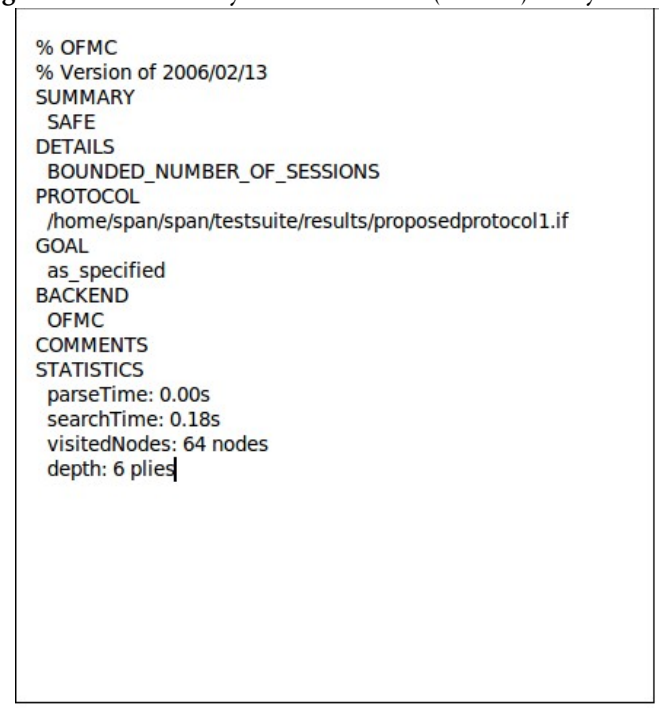
Source: Own authorship.

Figure 3.8. Session and Environment Roles (HLPSL source code)

```
%%%Role for the session
role session(Ui, GSS, RDj : agent, SecureChannel1,  SecureChannel2 : symmetric_key, P,H:hash_func)
def=
local SN1, SN2, SN3, RV1, RV2, RV3: channel(dy)
composition
user(Ui, GSS, RDj, SecureChannel1, P,H, SN1, RV1)
/\ gss(Ui, GSS, RDj, SecureChannel1, SecureChannel2, P,H, SN2, RV2)
/\ drone(Ui, GSS, RDj, SecureChannel1, SecureChannel2, P, H, SN3, RV3)
end role

role environment()
def=
const ui, gss, rdj : agent,
securechannel1, securechannel2: symmetric_key,
p,h: hash_func,
idrdj, tidui, idui: text,
ui_gss_qui, ui_gss_t1, gss_rdj_t2, rdj_ui_yrdj, gss_rdj_srdj: protocol_id,
sp1,sp2,sp3,sp4,sp5,sp6,sp7,sp8,sp8,sp9: protocol_id

intruder_knowledge = {ui,gss,rdj,idrdj,tidui,idui,h}
composition
session(ui,gss,rdj,securechannel1, securechannel2,p,h)
/\ session(i,gss,rdj,securechannel1, securechannel2,p,h)
/\ session(ui,i,rdj,securechannel1, securechannel2,p,h)
/\ session(ui,gss,i,securechannel1, securechannel2,p,h)

end role

goal
secrecy_of sp1, sp2, sp3, sp4, sp5 ,sp6, sp7, sp8, sp9
authentication_on ui_gss_qui, ui_gss_t1
authentication_on gss_rdj_t2 , gss_rdj_srdj
authentication_on rdj_ui_yrdj , rdj_ui_t3
end goal

environment()
```

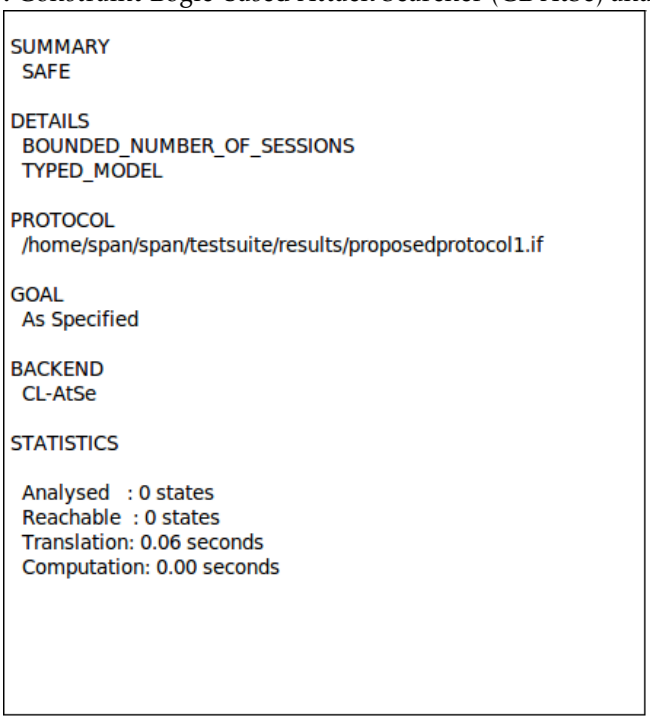
Source: Own authorship.

Figure 3.9. On-the-Fly Model-checker (OFMC) analysis result



Source: Own authorship.

Figure 3.10. Constraint Logic-based Attack Searcher (CL-AtSe) analysis results



Source: Own authorship.

3.7 PERFORMANCE ANALYSIS

This section addresses a comparative performance analysis of the protocol.

3.7.1 Analysis of computational costs

One of the primary objectives in developing an authentication protocol for the Internet of Drones (IoD) is to minimize computational overhead without compromising security. This section presents the computational cost of the proposed authentication scheme and compares it with other protocols that utilize similar network models [88] [11].

The selection of protocols for comparison was based on similarity in terms of network architecture, and metrics used in the selected articles, allowing for a fair comparison with the proposed protocol. Additionally, previous performance analyses of the chosen articles have demonstrated that they have lower computational costs compared to other protocols, raising interest in their proposals. For instance, Alzahrani et al. [88] protocol proved to be more efficient than Srinivas et al. [5] and Nikooghadam et al.[16]; Tanveer et al. [11] protocol was more efficient than Wazid et al. [87]. The selection is also based on their influence within the scientific community, as evidenced by the Scopus database: for instance, Tanveer et a. [11] has 60 citations to date. Moreover, such schemes aim to promote a tradeoff between efficiency, security and lightweight attributes.

In terms of computational costs, Table 3.4 presents the unit costs and descriptions of each operation in milliseconds (ms), with the values adopted according to the configurations described in [93], where:

- A desktop with "Intel(R) Core (TM) i7-6700 3.40 GHz CPU, 8 GB RAM, and Ubuntu 16.04 LTS, 64-bit OS" simulated *GSS* ;
- Raspberry PI with "Raspberry Pi (RP-3) Quad-core@1.2 GHz (64 bits) CPU, 1 GB RAM, and Ubuntu 16.04 LTS (64-bit) OS simulated RD_j and MD_{U_i} .

Operations conducted in the authentication phase – except XOR operation, since it is negligible in comparison to others – were analyzed. Table 5 shows the computational costs

Table 3.4. Cost of each operation

Notation	Description	Raspberry PI	Desktop
T_{mul}	ECC point multiplication	2.92ms	0.605ms
$T_{fe} \approx T_{mul}$	Biometric-fuzzy extractor	2.92ms	0.605ms
T_{add}	ECC point addition	0.154ms	0.004ms
T_{hash}	Hash Function	0.311ms	0.029ms
T_{ac}	Encryption scheme	0.425ms	0.036ms

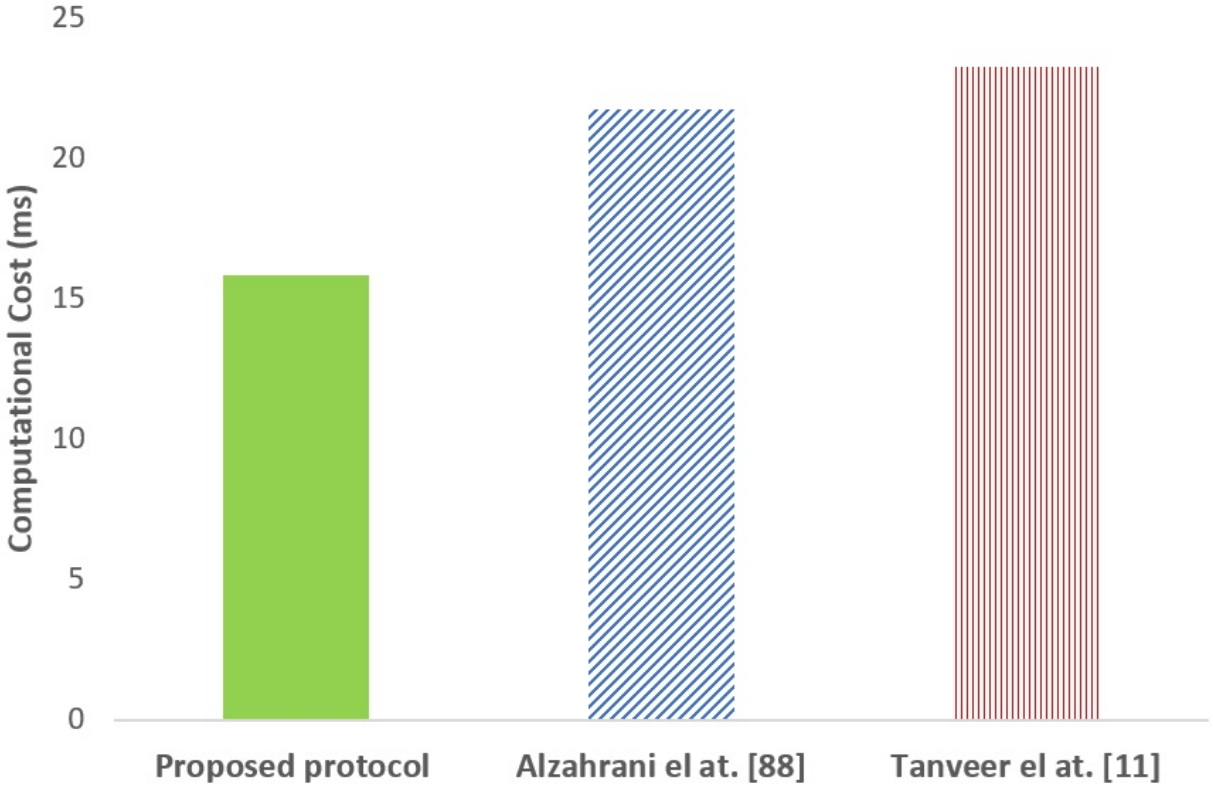
of the proposed scheme and those of the protocols of Alzahrani et al. [88] and Tanveer et al.[11]. According to the results, the computational costs of [88] and [11] are higher. The proposed scheme requires the lowest computational cost due to the use of scalar multiplication in elliptic curves only for calculating the session key, which incurs higher costs. The schemes of Alzahrani et al. [88] and Tanveer et al.[11] adopted scalar multiplication in elliptic curves for calculating not only SK , but also other credentials involved in the authentication phase.

According to the proposed protocol, user U_i performs $T_{fe} + 1T_{mul} + 7T_{hash} \approx 8.442$ms, RD_j performs $2T_{mul} + 3T_{hash} + 1T_{ac} \approx 7.198$ ms, and GSS performs $2T_{hash} + 1T_{ac} \approx 0.179$ ms, leading to a total cost of $T_{fe} + 3T_{mul} + 12T_{hash} + 4T_{ac} \approx 15.819$ ms, whereas that of [88] is $6T_{mul} + 13T_{ac} + 20T_{hash} \approx 21.689$ms and that of [11] is $T_{fe} + 6T_{mul} + 8T_{ac} + 11T_{hash} \approx 23.215$ms. Table 3.5 shows of the costs, and Figure 3.11 displays a graphic representation of the costs, confirming the better performance of the proposed scheme regarding computational costs.

Table 3.5. Comparison of computational costs

Protocol	U_i/MD_{U_i}	RD_j	**GSS**	**Total**
Proposed protocol	$T_{fe} + 1T_{mul} + 7T_{hash} + 1T_{ac} \approx$ 8.442ms	$2T_{mul} + 3T_{hash} + 1T_{ac}$ $\approx$7.198ms	$2T_{hash} + 2T_{ac}$ $\approx$0.179ms	$T_{fe} + 3T_{mul} + 12T_{hash} + 4T_{ac}$ $\approx$15.819ms
Alzahrani et al. [88]	$3T_{mul} + 3T_{ac} + 6T_{hash}$ $\approx$11.901ms	$2T_{mul} + 3T_{ac} + 5T_{hash} \approx$ 8.670ms	$1T_{mul} + 7T_{ac} + 9T_{hash} \approx$ 1.118ms	$6T_{mul} + 13T_{ac} + 20T_{hash}$ $\approx$21.689ms
Tanveer et al. [11]	$T_{fe} + 3T_{mul} + 3T_{ac} + 6T_{hash}$ $\approx$14.821ms	$2T_{mul} + 2T_{ac} + 3T_{hash} \approx$ 7.623ms	$1T_{mul} + 3T_{ac} + 2T_{hash}$ $\approx$0.771ms	$T_{fe} + 6T_{mul} + 8T_{ac} + 11T_{hash}$ $\approx$23.215ms

Figure 3.11. Comparison of computational costs



Source: Own authorship.

3.7.2 Analysis of communication costs

This subsection addresses a comparison of the communication costs of the proposed scheme and those of [88] and [11].

The methodology for the calculation of communication costs takes into account the number of bits necessary for the transmission of the set of messages required for the operation of a given protocol. In this sense, the contents of each message to be transmitted for a protocol are considered, with the size in bits of the different parameters/fields that compose such a message.

To ensure a fair comparison, the sizes of the most common message parameters used in protocols from references [11] and [88] , as well as in our proposed scheme, were standardized. The bit values adopted for each parameter were defined based on the specifications

presented in [11] and [88], as detailed in Table 3.6.

Table 3.6. Size of each parameter

PARAMETERS	VALUES IN BITS
Identity	160
Timestamp	32
Encrypt/decrypt	128
Eliptic curve point	320
Nonce	32
Hash function	256

Table 3.7 shows the results of the communication cost analysis and the respective comparisons. The proposed scheme provided better communication cost in comparison to those of [88] and [11].

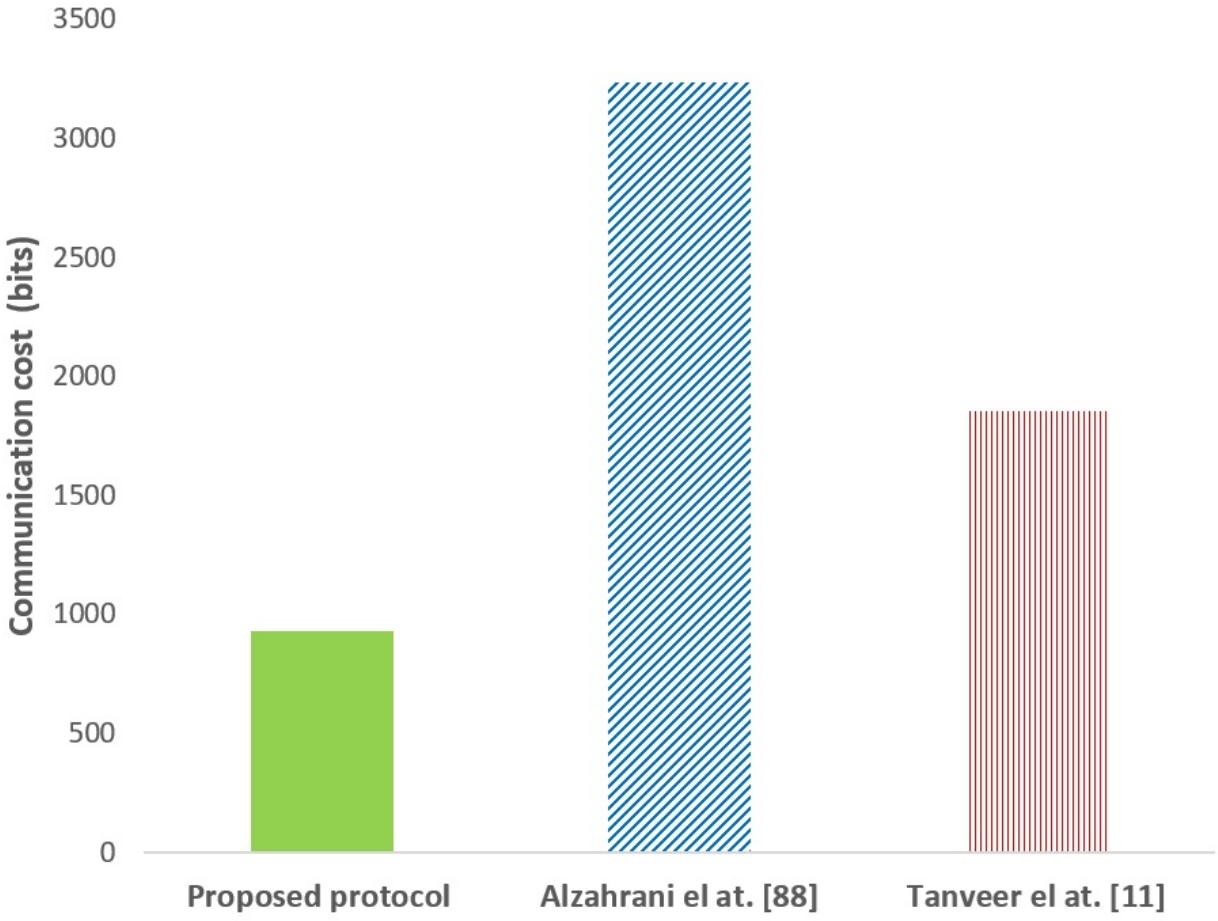
Table 3.7. Comparison of communication costs

Protocol	U_i/MD_{U_i}	RD_j	GSS	**Total (bits)**
Proposed protocol	160	160	608	928
Alzahrani et al. [88]	992	1120	1120	3232
Tanveer et al. [11]	704	672	480	1856

According to the protocol, cost per user U_i generates $M_1 = \{T_1, E_{U_i}\}$ and sends it to GSS. Therefore, the communication cost of U_i is $32 + 128 = 160$ bits. GSS generates $M_2 = \{T_2, E_{GSS}\}$ and sends it to RD_j – its communication cost is $32 + 128 = 160$ bits. Finally, RD_j generates and transmits $M_3 = \{T_3, z_{RD_j}P, H_3\}$ so that its communication cost is 32+320+256 = 608 bits. Therefore, the communication cost of the protocol is $160 + 160 + 608 = 928$ bits.

The total costs of the schemes of [88] and [11] are $992 + 1120 + 1120 = 3232$ bits and $704 + 672 + 480 = 1856$ bits, respectively. Figure 3.12 displays a graphic representation of the communication costs, confirming the better performance of the proposed scheme.

Figure 3.12. Comparison of communication costs



Source: Own authorship.

3.8 CHAPTER CONCLUSIONS

Due to the sensitivity of the information exchanged between users and drones, the delivery of secure and light communication is highly required. This chapter has proposed an efficient and secure protocol for the IoD environment, which provides confidentiality and integrity to the information exchanged between a drone and a user in such an environment. It has shown efficiency regarding resources, checks the user's authenticity, and configures a session key between the user and a drone specific for indecipherable communications. Both formal and informal security analyses revealed the scheme is secure against several known attacks.

The performance evaluation involved the computational and communication overloads

of the scheme and compared them to those of other authentication protocols based on ECC developed for drones and IoT, revealing the proposed scheme outperformed the others. Moreover, it is well protected against known attacks compared to the other protocols and the results from AVISPA formal analysis demonstrated its security. Future studies will include designing and evaluating other mutual authentication protocols for the Internet of Drones integrated with the cloud and fog environment.

CHAPTER 4

AUTHENTICATION PROTOCOL FOR THE INTERNET OF DRONES WITH FOG COMPUTING BASED ON AGGREGATE SIGNATURES FOR FOREST INVENTORY

Abstract *The Internet of Drones (IoD) has gained importance in areas such as forest inventory, utilizing advanced sensors and Internet connectivity for efficient data collection and surpassing traditional methods in cost-effectiveness. However, it faces security and privacy challenges due to public channel communications, unreliable connectivity, and a dynamic environment. Protecting forest inventory data is crucial to ensuring accuracy, preventing unauthorized access, and avoiding data manipulation, which might lead to poor management decisions. An authentication protocol secures IoD communication and must be lightweight, consider network bandwidth limitations and scalability, and integrate emerging technologies. This chapter presents a novel Authentication and Key Agreement (AKA) protocol that uses asymmetric cryptography and aggregate signatures for IoD in forest inventories with fog computing. Its robustness was confirmed through informal and formal security analyses by the AVISPA tool, demonstrating resistance to known attacks and superior communication computational and energy performance compared to existing protocols.*

4.1 INTRODUCTION

Forest inventory constitutes a crucial phase in forest management, which assesses the composition of the forest and its suitability for silvicultural management [97]. The process enables the understanding of the forest biological diversity, monitoring of tree vitality, and tracking vegetation development, which are indispensable in the context of progressive deforestation. Furthermore, knowledge and preservation of forest cover are essential for the ecological balance of the planet [98].

An accurate forest inventory requires the collection of representative data. Traditional field surveys, however, may be inaccurate, especially in expansive forests, and tend to be costly, complex, and prone to errors. The variability in forest structure, tree height, diameter, and density across regions and the logistical challenges of data collection in extensive, remote, and difficult-to-access areas hamper the acquisition of precise and representative forest data [34] [99].

Recent technological advancements have enhanced the quality and efficiency of forest inventory activities by applying geotechnologies. Satellites have revolutionized data collection and analyses from the Earth's surface, covering large areas at regular intervals [100] [101]. However, whereas some satellite data are freely available (e.g., Landsat and Sentinel), high-resolution imagery comes at a significant cost [102]. Spatial resolution may be inadequate for studies focused on the canopy, leaves, or individual trees [103] and the acquisition of satellite data can be hampered by challenges such as cloud coverage and viewing angles, potentially limiting the effectiveness of those technologies in specific contexts [104].

Given the aforementioned limitations, the use of drones for forest inventories has emerged as an innovative solution, offering effectiveness and multiple benefits [34] [105] [106] [107] [108]. Drones can acquire high spatial and temporal resolution images, enabling flights close to tree canopies and capture of high-resolution orthophotos, thus leading to a more efficient and cost-effective alternative to satellites. Moreover, the versatility of onboard sensors enables the collection of valuable information on vegetation cover, forest structure, and relevant parameters across various environmental conditions and ecosystems. The operational flexibility of those devices is evident, since they can navigate cloud cover, adapt flights according to local weather conditions, and adjust the data acquisition frequency as necessary [103] [109] [4].

The Internet of Things (IoT) has emerged as one of the preeminent research domains in recent years due to its increasing applicability across diverse emerging fields. Novel areas such as pollution monitoring, disaster management, industrial IoT, and smart agriculture have arisen as prominent themes revolutionizing the application of IoT in everyday life [110]. In this context, the integration of drones with the Internet has inaugurated a new paradigm known as the Internet of Drones (IoD), expanding upon the principles of the IoT

[7].

This technological advancement has enabled drones to operate with enhanced intelligence, self-organize into clusters, establish interconnections, and collaborate on various tasks[23]. Furthermore, it has facilitated the exchange of critical information with ground stations, optimizing their operations efficiently [111]. Such advancement has empowered drones to operate with heightened intelligence, organize into clusters, establish interconnections, collaborate on diverse tasks [23], and exchange crucial information with ground stations to streamline operations efficiently [111]. In the domain of forest inventories, the IoD enhances data collection by enabling rapid coverage of extensive areas and acquisition of accurate data.

The drones seamlessly integrate with networks of sensors and smart devices, such as soil sensors and cameras, facilitating a comprehensive accumulation of data, which can subsequently be stored and analyzed on cloud computing platforms by artificial intelligence algorithms and machine learning techniques for generating meaningful insights [112].

However, the environment in which forest inventories occur is generally complex and dynamic, with a wide diversity of tree species, shrubs, lianas, herbs, and other vegetal components. Since they are often situated in remote and inaccessible regions with rugged terrain and adverse weather conditions, implementing communication infrastructures such as antennas, ground stations, and energy resources can prove challenging [101]. Such obstacles can impede the seamless transmission of data collected by drones to ground stations, mainly because broadband wireless networks are not uniformly available throughout the environment, thus, exposing vulnerabilities in terms of security and privacy due to the lack of robust safeguards in the communication channels between drones and ground stations [7].

In response to those challenges, specifically coverage of large-scale areas and overcoming connectivity hurdles, the strategy of using multiple drones that operate in coordination to form groups has been adopted. The approach requires sophisticated management techniques since the direct control of each drone via ground station becomes impractical with increasing number of drones involved in a single mission [113].

Another approach, namely, the use of fog computing in the IoD architecture, has been

explored for large-scale areas such as forests to address that challenge [114] [113] [115]. According to Yahuza et al. [7], the application of fog computing to IoD architectures is one of the most significant developments. Gupta et al. [114] also emphasize the benefits of integrating fog-enabled drones in the IoD, particularly in enhancing responsiveness and decentralizing processing. Drones can be equipped with computational and storage capabilities to act as fog nodes. They process and store data locally before transmitting them to the cloud, reducing the volume of data sent, and can also implement local security mechanisms, such as assistance to the network in the authentication process of its elements, improving the security of the IoD environment while also providing more robust support for low latency, scalability, and effective integration with emerging IoD technologies [111] [116] [117]. Additionally, they can expand the coverage area and enhance data transmission in remote regions with no Internet connectivity [114].

However, significant concerns arise regarding privacy and security in IoD and drone-based data transmission systems. Drones typically operate in open and untrusted environments, making them vulnerable to cyber threats [118]. These include potential hijacking through cyber-attacks, data breaches, payload theft, and authentication threats. Additionally, there are risks of leaking sensitive information such as identity, location, and flight routes [7] [64] [6]. This vulnerability is particularly critical in applications like forest inventories, where the collected data often includes sensitive information about forest resources and locations. Protecting such data is essential to prevent unauthorized access and potential misuse of natural resources. The open nature of drone operations also makes identity authentication extremely challenging, further complicating the task of securing drone networks against malicious users. These multifaceted challenges underscore the complexity of ensuring information security and privacy protection in drone-based transmission systems, especially when handling sensitive environmental data [119].

One of the measures adopted to protect the IoD environment is the implementation of authentication protocols, which prevent malicious nodes from entering and accessing the network [120], allowing only authorized elements to access the collected data. Additionally, authentication helps ensure such data are accurate and reliable, which is essential for the success of forest inventories. However, due to the computational limitations inherent

to drones, the demands for scalability in the IoD scenario and the complexity of integration with fog computing, designing authentication protocols faces complex and nontrivial challenges.

Some studies have highlighted the importance and necessity of developing authentication protocols. Gupta et al. [114] claimed one of the most critical requirements in an IoD environment with fog computing is the authentication of devices connected to the network and the implementation of security and device authentication mechanisms still faces challenges that must be addressed. Michailidis et al. [9] emphasize that the evolution of IoD networks has required the development of models that mitigate various security and privacy threats; however, some questions on the authentication of IoD networks are still open.

Although several researchers have proposed authentication schemes for the IoD environment [121] [91] [88], authentication protocols tailored to the IoD network that address mobility for dynamic addition and revocation of drones after initial deployment [9] and protocols that adapt to the environment of drones with emerging technologies, such as fog computing, still have open issues [114]. Jan et al. [95] designed an authentication protocol considering the high mobility features of drones; however, they did not anticipate its implementation in an IoD environment with fog computing. Yahuza et al. [80] introduced a protocol that could be adapted for implementation in an IoD environment with fog computing; however, they did not consider the high mobility of drones. To date, no authentication protocol specifically developed for IoD environments aimed at forest inventories has been identified.

This chapter presents the design and evaluation of a secure and reliable Authentication and Key Agreement (AKA) protocol tailored for the IoD environment, specifically aimed at forest inventory activities utilizing fog computing. The scheme incorporates a security and privacy model for group authentication, facilitating mutual authentication among drones and fog drones within the same cluster, as well as between fog drones and the ground station, thereby establishing secure sessions among those entities.

4.1.1 Main contributions

In what follows are the main contributions of the chapter:

- Development of a novel AKA protocol for IoD with fog computing, employing asymmetric cryptography and the elliptic curve digital signature algorithm (ECDSA) for application in forest inventory environments.
- Implementation of aggregate signatures to enhance mutual authentication within drone clusters and integration of binary trees and databases towards an efficient management of drone dynamics, enabling seamless addition and removal of drones from the network.
- An informal security analysis validating the scheme's resilience against multiple known attacks, demonstrating its ability to meet essential IoD functionalities.
- A formal security assessment by AVISPA (Automated Validation of Internet Security Protocols and Applications) tool, a semi-automated system that verifies internet security protocols, confirming the protocol's compliance with established security standards.
- A performance analysis of the protocol through evaluating its computational, communication and energy costs, comparing it with other schemes available in the literature. According to the results, the scheme has lower costs and is, therefore, suitable for IoD environments.

4.1.2 Structure of the chapter

The remainder of the chapter is structured as follows: Section 2 discusses some related work; Section 3 describes the system model; Section 4 introduces the protocol; Sections 5 and 6, report on a security analysis and a performance analysis comparing the communication and computational costs of the protocol with other schemes from the literature, respectively; finally, Section 7 discusses the main conclusions and suggests some future work.

4.2 RELATED WORK

This section provides an overview of various authentication protocols published in recent years, aimed at enhancing security in the Internet of Drones (IoD) environment while optimizing resource efficiency. Though they still face specific limitations, they demonstrate a logical progression in discussions on authentication challenges in the IoD environment.

Semal et al. [122] developed a certificate-free authenticated group key agreement protocol for IoD network communications over insecure channels. It enables parties to agree on an authenticated group-shared key without requiring authentication certificates, using bilinear pairing for shorter signatures, which, however, results in high computational costs, particularly when a fog drone must authenticate multiple edge drones within a cluster. Moreover, the authors did not consider the functionality of adding and revoking drones.

Hong et al.[77] proposed an identity-based aggregate signature authentication protocol for a drone cluster network. The scheme employs elliptic curve cryptography, but is susceptible to privileged insider attacks, indicating although it enhances efficiency, it compromises security. The protocol does not address the revocation of drones.

Li et al. [123] improved the scheme of [77] by adding an authentication mechanism based on an identity-based aggregate signature method that uses bilinear pairing and asymmetric cryptography. According to the security analysis, the authors claim their scheme is secure. However, it is computationally costly and does not address the revocation of drones from the cluster.

Ever et al. [124] introduced a protocol that authenticates multiple drones using bilinear pairing. Drones are considered mobile sinks in a hierarchical architecture of wireless sensor networks that helps to provide unique user authentication for sensor nodes, cluster heads, and mobile sinks (UAVs). However, the scheme is neither resistant to ESL attack under Canetti and Krawczyk adversary model nor maintains anonymity or untraceability, critical for privacy in drone operations.

Han et al. [113] proposed a mutual authentication protocol between fog drones and remote drones in multi-drone environments that enables authentication without a ground station. The protocol is resistant to man-in-the-middle and replay attacks and handles the

revocation of authentication keys after mission completion. However, it lacks mechanisms for an individual revocation of a remote drone from the cluster, which might lead to security breaches if a drone is compromised.

Subramani et al. [125] proposed a blockchain-based anonymous authentication scheme for IoD. The protocol employs physically unclonable functions (PUFs) and reverse fuzzy extractors. The approach provides physical security and privacy and facilitates handover authentication. It demonstrates resistance to various attacks and reduced overhead compared to related works. The scheme advances IoD security and supports dynamic drone addition, but lacks explicit support for dynamic drone revocation.

Although those protocols illustrate various approaches to enhancing security and efficiency in the IoD environment none of them offer a comprehensive solution that addresses all security challenges, such as high computational costs, lack of anonymity, susceptibility to various attacks, and limitations in key revocation. Our protocol aims to bridge those gaps, providing a more robust and holistic approach to IoD security. Table 4.1 shows a general comparison among the protocols.

Table 4.1. Authentication Protocols Summary — Security Features and Functionality

Protocols	**Year**	**Techniques applied**	**Formal Verification Tool**	**Limitations**
Semal et al. [122]	2018	Bilinear pairing. Hash functions	Scyther tool	High computational costs. Does not support dynamic drone addition/revocation.
Hong el at. [77]	2020	Bilinear pairing. Elliptic curve cryptosystem	Random Oracle Model (ROM)	Privileged Insider Attack Does not support dynamic drone addition/revocation.
Li el at. [123]	2020	Bilinear pairing. One-way hash functions Elliptic curve cryptosystem	No formal security verification	High computational costs. Does not support dynamic drone addition/revocation
Ever et at. [124]	2020	Elliptic curve cryptosystem. One-way hash functions Bilinear pairing.	No formal security verification	Does not support dynamic drone addition/revocation. Does not achieve user anonymity/untraceability. Vulnerable to ephemeral key leakage attack.
Han et al. [113]	2022	Hash-Based Message Authentication Code One-way hash functions Group key	ProVerif tool	Does not support dynamic drone addition. Does not support individual revocation of a cluster drone.
Subramani et al. [125]	2024	Blockchain PUFs Reverse Fuzzy Extractors One-way hash functions	BAN Logic	Does not support dynamic drone revocation.

Source: Own authorship.

4.3 NETWORK AND THREAT MODELS

This section presents the system model considered for the proposal. The following subsections explain the network and threat models employed to demonstrate the applicability

of the protocol.

4.3.1 Network Model

The network model adopted for the authentication protocol in the Internet of Drones (IoD) with fog computing, specifically for forest inventory applications, consists of four main elements, namely, Cloud Data Center (CDC), Ground Station (GS), fog drones, and remote drones. The roles of each element are detailed in what follows.

- CDC: provides rapid processing capabilities, advanced computing tools, and substantial storage capacity and serves as the trusted entity (Trust Authority - TA) responsible for system initialization and drone network registration. It also includes the Key Generation Centre (KGC), which generates partial and cluster private keys, and hosts the database server that stores confidential information about drones, airspace, and control room operations.

- GS: manages one or more drone clusters and acts as a relay, receiving data from fog drones and transmitting them to the CDC. It can process requests from multiple fog drones simultaneously.

- Fog Drone: integrates the functions of a remote drone and a fog node, serving as a portal between the drones and the GS for data transmission.

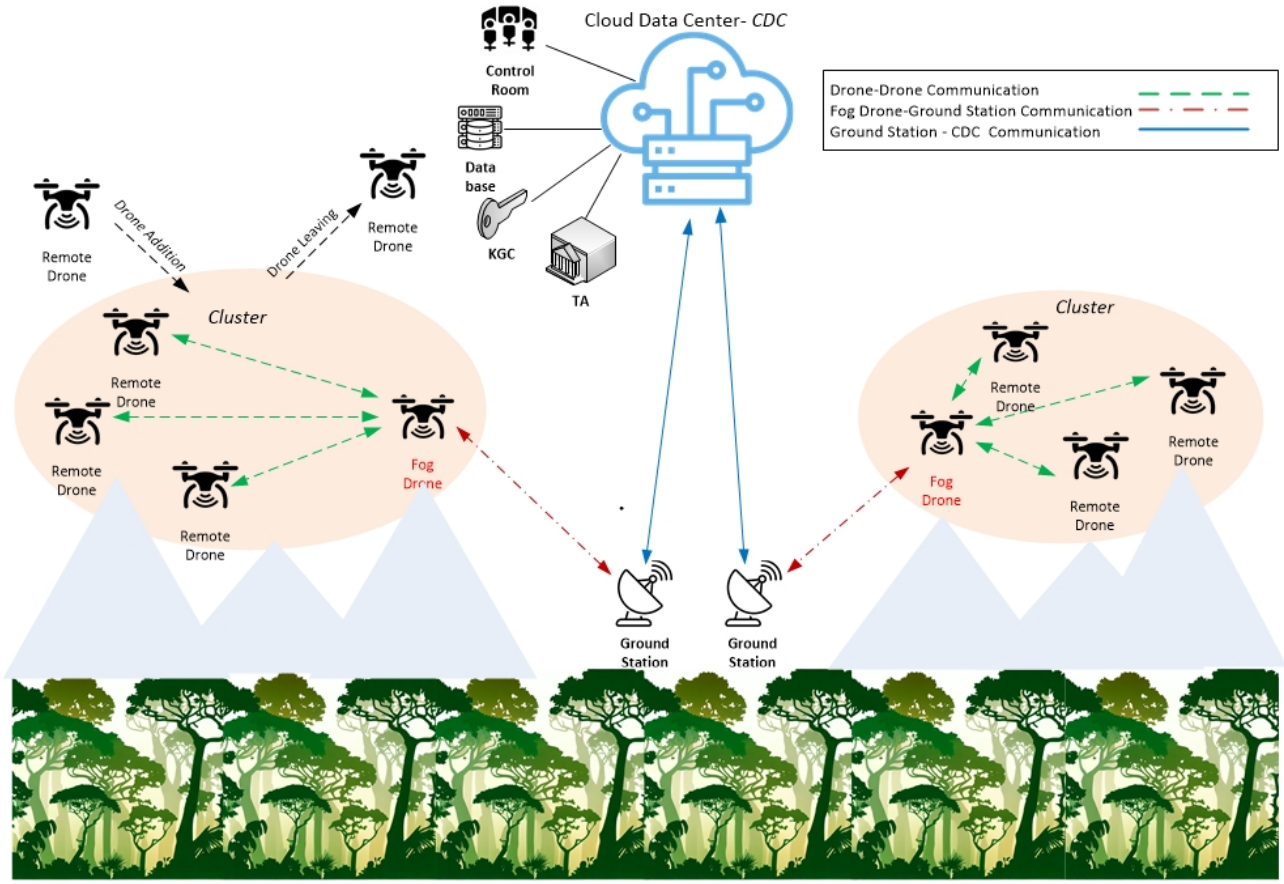
- Remote Drone (RD_{j-k}): collects environmental data and transmits them to the fog drones.

As illustrated in Figure 4.1, the flight area is divided into zones where remote drones gather in clusters to collect environmental data according to their flight plans. Within each cluster, a specific remote drone is selected as a fog node based on algorithms that consider factors such as position, energy levels, and mobility [126] [127] [128] [129]. The fog node receives data from the remote drones and forwards them to the ground station, which then transmits them to the CDC. All remote drones in a cluster must be within the communication range of the fog node. Communication between CDC and GS occurs through secure

channels, whereas communication among fog drones, $RD_{j-k,}$ and GS occurs over insecure channels.

The protocol supports scalability through a dynamic addition and revocation phase, enabling inclusion or exclusion of drones at any time. However, before initiating data exchange, RD_{j-k} must complete an AKA procedure.

Figure 4.1. Network Model



Source: Own authorship.

4.3.2 Threat Model

The security of the protocol was analyzed under the following two models:

- Dolev–Yao threat model (DY) [71], in which an adversary (A) can intercept, modify, delete, or inject malicious data into any message exchanged over a public network. The adversary can impersonate a legitimate node, such as a Remote Drone or a Fog Drone.

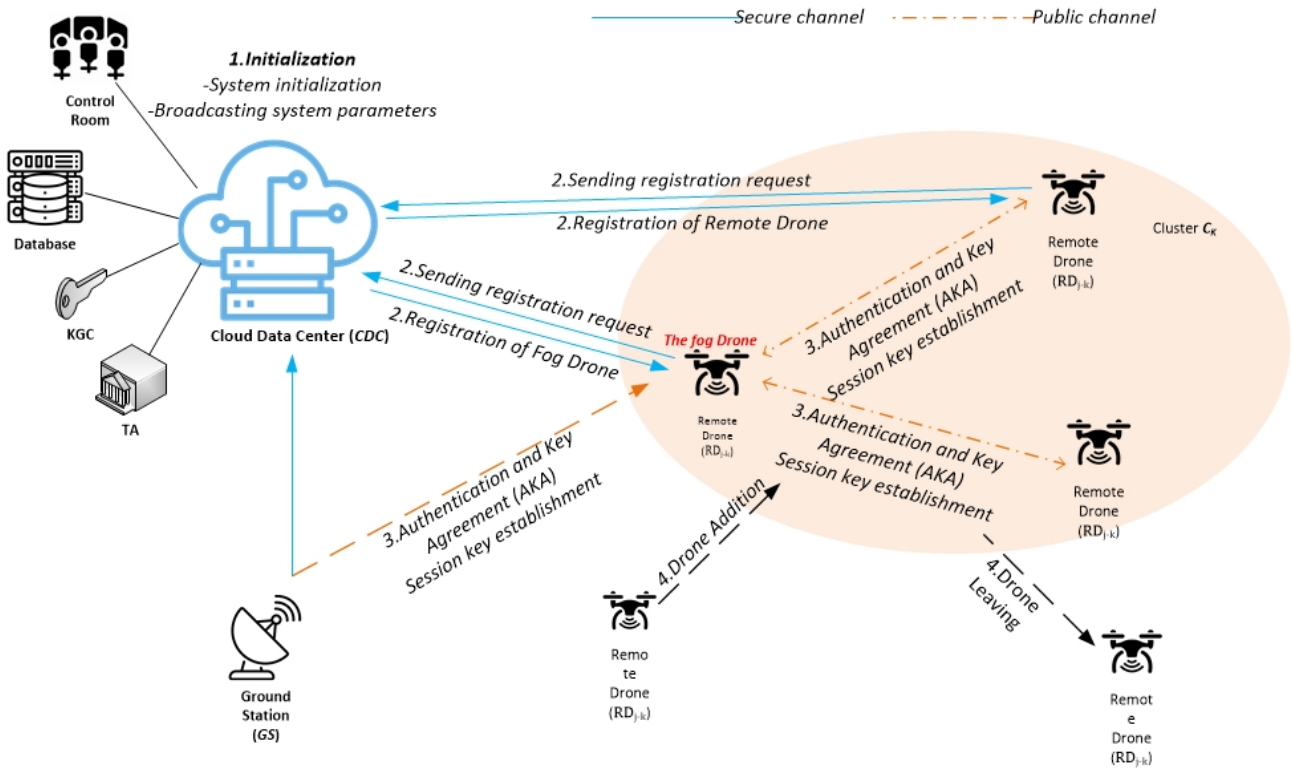
- Canetti and Krawczyk threat model (CK) [92], which addresses recent advances in attack techniques, requiring enhanced assumptions about adversary capabilities. Therefore, it has been integrated into the design of authentication protocols [80] [96] [130]. Beyond the capabilities described in DY, CK enables adversary A to compromise both long-term keys, which include the secret keys of network elements and random session numbers generated during the authentication process [5].

The security analysis section reports on an analysis of the protocol that used the two aforementioned adversary models.

4.4 PROPOSED PROTOCOL

As shown in Figure 4.2, the protocol comprises four phases, namely, initialization, registration, authentication, and drone addition and revocation. The flowchart of the proposed protocol is shown in Figure 4.3 . All notations of the system parameters used and their descriptions are provided in Table 4.2.

Figure 4.2. Proposed protocol



Source: Own authorship.

Table 4.2. System parameters

Symbol	Definition
λ	security parameter
$params$	system parameters
p	a k bit prime
Z_p	a prime field of order p
$E_p(a,b)$	a nonsingular elliptic curve of the form: "$y^2 = x^3 + ax + b\ (mod p)$, where $a, b \in Z_p^*$ with $4a^3 + 27b^2 \neq 0 (mod p)$"
P	generator point
j	index of drones
k	index of cluster
x	index of ground station
CID_k	k^{th}Cluster, k = 1,2,3,..., l
GID_x	x^{th}Ground station, x = 1,2,3,..., q
RD_{j-k}	j^{th}Remote Drone, j = 1,2,3,..., m of cluster k^{th}, k = 1,2,3,...,l
$h_1(\cdot), h_2(\cdot), h_3(\cdot), h_4(\cdot)$	Collision-Resistant, One-Way Hash Function,$h(\cdot)$: $\{0,1\}^* \rightarrow Z_p^*$
Pub_{CDC}	system public key
Pub_{GID_x}	public key of RD_{j-k}
s_{CDC}	system private key
$s_{RD_{j-k}}$,	private key of RD_{j-k}
$TID_{RD_{j-k}}$	temporary identity of RD_{j-k}
$RTS_{RD_{j-k}}$	timestamp of $TID_{RD_{j-k}}$
$SEC_{RD_{j-k}}$	secret between drone i of cluster k and CDC
$PS_{RD_{j-k}}$	partial private key of RD_{j-k}
$y_{RD_{j-k}}$	secret of RD_{j-k}
$Pub_{RD_{j-k}}$	public key of RD_{j-k}
$Pri_{RD_{j-k}}$	private key of RD_{j-k}
$r_c, b_{RD_{j-k}}, r_{RD_{j-k}}, x_{RD_{j-k}}, y_{RD_{j-k}}, u_{RD_{j-k}} d$	random numbers $\in Z_p^*$
CK_k	group key
T	current timestamp
$U_{RD_{j-k}}$	first signature element of RD_{j-k}
$\delta_{RD_{j-k}}$	second signature element of RD_{j-k}
$\sigma_{RD_{j-k}}$	signature element of RD_{j-k}
ΔT	maximum transmission delay
A	Adversary
SK	session key
$\|\|$, $\oplus$	concatenation, bitwise XOR operations

Source: Own authorship.

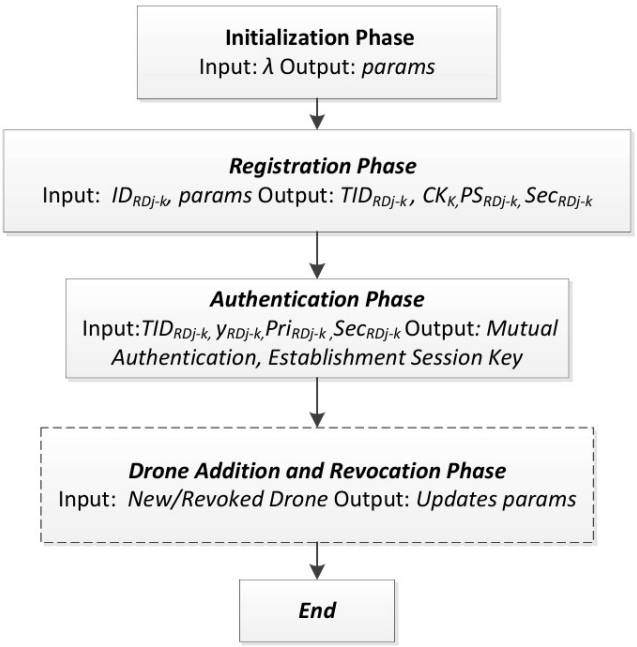
1. Initialization Phase: consists of the generation and distribution of system parameters and authentication information. Communications among the network elements are assumed to occur through secure channels.

2. Registration Phase: involves registering drones with the CDC to obtain their individual credentials, system credentials, and a group key for the drone cluster. The process is conducted offline and through secure channels.

3. Authentication and Session Key Phase: involves mutual authentication among the GS, fog drones, and remote drones, followed by generating a session key. The process is essential for preventing internal attacks and ensuring both confidentiality and privacy of communications across the network elements.

4. Drone Addition and Revocation Phase: addresses the dynamic addition of new drones due to adversarial physical damage or accidental issues such as battery depletion or internal circuit failures. It also includes the removal of authorized drones that remain inactive beyond the permitted time due to crashes, technical failures, capture by an adversary, or upon task completion.

Figure 4.3. Flowchart of the proposed protocol



Source: Own authorship.

4.4.1 Initialization Phase

To generate security parameters λ, CDC first selects a large prime number p and an elliptic curve $E_p(a,b)$. It also chooses a generator point $P \in E_p(a,b)$ on the elliptic curve of order p and four hash functions from a finite domain (SHA-256), called $h_1(\cdot)$, $h_2(\cdot)$, $h_3(\cdot)$ and $h_4(\cdot) : \{0,1\}^* \rightarrow Z_p^*$. Subsequently, it selects a random number $s_{CDC} \in Z_p^*$ as its private key, and the system public key is calculated as $Pub_{CDC} = s_{CDC}P$.

Next, CDC generates a random number $r_c \in Z_p^*$, calculates an identity for each drone cluster in the flight area as $CID_k = h_1(r_c)$, and assigns an identity GID_x to each ground station. Finally, it stores system parameters $params = \{p, E_p(a,b), P, h_1(\cdot), h_2(\cdot), h_3(\cdot), s_{CDC}, Pub_{CDC}, CID_k | 1 \leq k \leq n_c, GID_x\}$ in its memory and publishes parameters $\{p, E_p(a,b), P, h_2(\cdot), h_3(\cdot), h_4(\cdot), Pub_{CDC}, CID_k, GID_x\}$.

4.4.2 Registration Phase

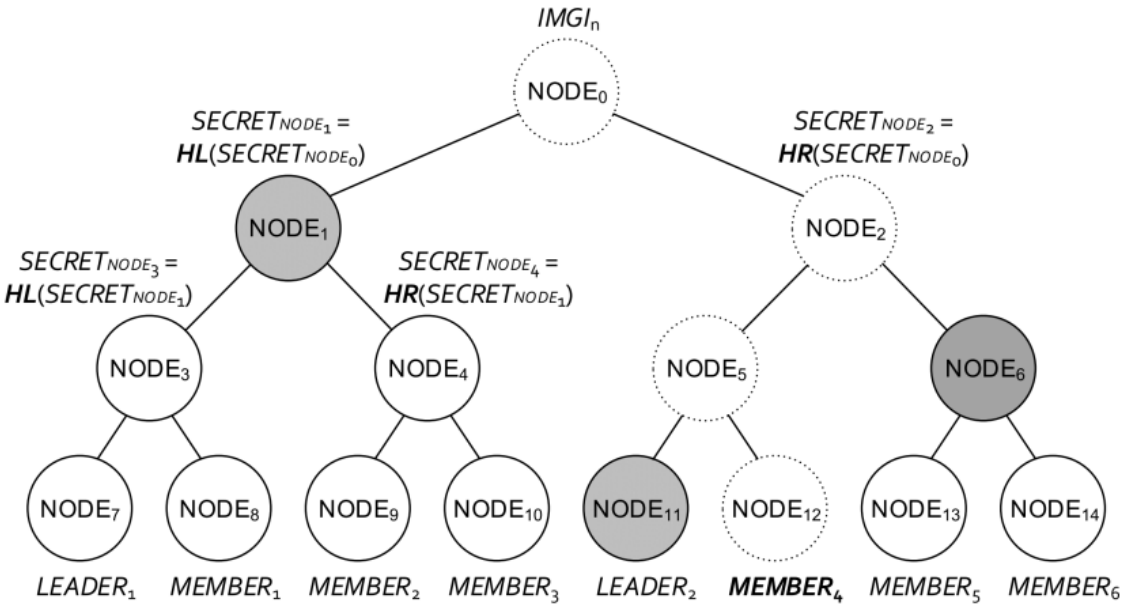
The registration phase begins with RD_{j-k} sending their identities $ID_{RD_{j-k}}$ and a registration request to the CDC. The CDC then checks its database, which contains a list of all valid and revoked drone identities. If the identity is not valid, the CDC rejects the registration request. If the identity is valid, the CDC generates a random number $s_{RD_{j-k}} \in Z_p^*$ as the private key and calculates a temporary identity for each drone, as follows:

$$TID_{RD_{j-k}} = h_1(ID_{RD_{j-k}} \| s_{RD_{j-k}}.P). \tag{4.1}$$

It then generates a timestamp $RTS_{RD_{j-k}}$ for each drone to define the validity period of its registration in the system and stores the data in its memory. Next, it organizes the RD_{j-k} and GID_x of a cluster into a binary tree structure for group key generation, following the methodology proposed in [52], [53], [54]. Each drone and the CDC are represented as leaves in the tree, each having an associated secret, $SEC_{RD_{j-k}}$, SEC_{CDC}, derived from the secret values of their parent nodes. Two hash functions, namely, H_R and H_L, are defined for calculating their secrets. H_R is used for nodes located on the right side of their parent, whereas H_L is used for nodes on the left side of their parent, as shown in Figure 4.4. Therefore, all the secret values of the descendant nodes can be derived as long as the secret value

of the nodes is known. A member located at the leaf node knows all the secret values in the tree except for the restricted ones situated on the ascending path toward the root direction of their own node.

Figure 4.4. Binary tree for group organization



Source: [52]

CDC then calculates the group key for each cluster in the following manner:

$$CK_k = h_3\left(SEC_{RD_{1-k}} \oplus SEC_{RD_{2-k}} \oplus \ldots \oplus SEC_{RD_{j-k}} \oplus SEC_{GID_x} \| s_{CDC} \| CID_k\right). \tag{4.2}$$

Next, it calculates the partial private key of the remote drones, selecting the GID_k of ground stations the fog drone of the cluster can use to send data to *CDC* to prevent remote drones from being deceived by a fake *GS*. It then generates a random number $r_{RD_{j-k}} \in Z_p^*$ and calculates

$$R_{RD_{j-k}} = r_{RD_{j-k}} P, \tag{4.3}$$

$$H_1 = h_2(PID_{RD_{j-k}} \| GID_k \| Pub_{CDC} \| R_{RD_{j-k}}), \tag{4.4}$$

$$PS_{RD_{j-k}} = \left(r_{RD_{j-k}} + s_{CDC} H_1\right) mod\ p. \tag{4.5}$$

It stores parameters $\left\{s_{RD_{j-k}}, TID_{RD_{j-k}}, SEC_{RD_{j-k}}, SEC_{GID_x}, CK_k, r_{RD_{j-k}}, R_{RD_{j-k}}, H_1, PS_{RD_{j-k}}\right\}$ in its memory and sends parameters $\{s_{RD_{j-k}}, TID_{RD_{j-k}}, SEC_{RD_{j-k}}, CK_k, r_{RD_{j-k}}, R_{RD_{j-k}},$

$PS_{RD_{j-k}}\}$ to the remote drones . Upon receiving them, RD_{j-k} chooses a random number $y_{RD_{j-k}} \in Z_p^*$ as their secret and calculates their partial public and private keys, as follows:

$$X_{RD_{j-k}} = y_{RD_{j-k}}.P, \tag{4.6}$$

$$H_2 = h_3(TID_{RD_{j-k}} \| X_{RD_{j-k}}), \tag{4.7}$$

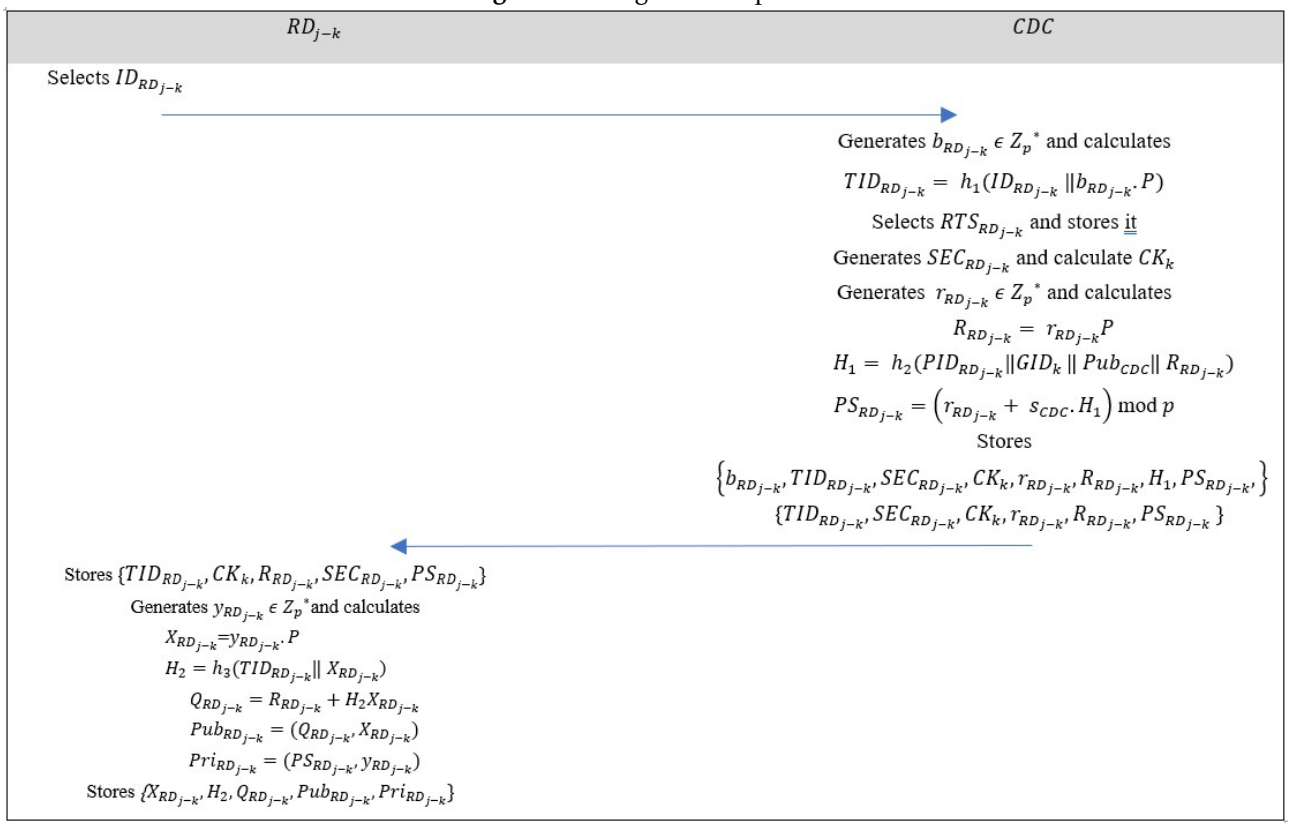
$$Q_{RD_{j-k}} = R_{RD_{j-k}} + H_2 X_{RD_{j-k}}, \tag{4.8}$$

$$Pub_{RD_{j-k}} = (Q_{RD_{j-k}}, X_{RD_{j-k}}), \tag{4.9}$$

$$Pri_{RD_{j-k}} = (PS_{RD_{j-k}}, y_{RD_{j-k}}). \tag{4.10}$$

Finally, it stores in its memory the following parameters $\{X_{RD_{j-k}}, H_2, Q_{RD_{j-k}}, Pub_{RD_{j-k}}, Pri_{RD_{j-k}}\}$. The complete procedure is shown in Figure 4.5.

Figure 4.5. Registration phase



Source: Own authorship.

4.4.3 Authentication and Session Key Phase

In this phase, network elements authenticate each other to create secure channels and generate a unique session key for communication. The process is performed online through insecure channels. Towards ensuring security and integrity, each remote drone RD_{j-k} sets a timestamp $T_{1RD_{j-k}}$ and generates a random number $u_{RD_{j-k}} \in Z_p^*$. Then, it produces a signature as follows:

$$U_{RD_{j-k}} = u_{RD_{j-k}}.SEC_{RD_{i-k}}.P, \tag{4.11}$$

$$H_2 = h_4(TID_{RD_{j-k}} \| X_{RD_{j-k}}), \tag{4.12}$$

$$H_3 = h_4(TID_{RD_{j-k}} \| Pub_{RD_{j-k}} \| U_{RD_{j-k}} \| T_{1RD_{j-k}}), \tag{4.13}$$

$$\delta_{RD_{j-k}} = [u_{RD_{j-k}} + H_3(PS_{RD_{j-k}} + H_2.SEC_{RD_{j-k}}.y_{RD_{j-k}})]modp. \tag{4.14}$$

The signature is given by:

$$\sigma_{RD_{j-k}} = (U_{RD_{j-k}}, \delta_{RD_{j-k}}). \tag{4.15}$$

Next, RD_{j-k} sends parameters $\left\{TID_{RD_{j-k}}, Pub_{RD_{j-k}}, \sigma_{RD_{j-k}}, T_{1RD_{j-k}}\right\}$to the fog drone chosen by the *CDC*. After receiving the signature, the fog drone verifies whether the timestamp $T_{1RD_{j-k}}$ is within the allowed transmission time limit $|T_2 - T_{1RD_{j-k}}| \leq \Delta T$. If it is not within the limit, the session is terminated. Otherwise, the for drone it verifies signature $\sigma_{RD_{j-k}} = (U_{RD_{j-k}}, \delta_{RD_{j-k}})$ by calculating

$$H_1^{'} = h_2(TID_{RD_{j-k}} \| GID_k \| Pub_{CDC} \| R_{RD_{j-k}}), \tag{4.16}$$

$$H_3^{'} = h_4(TID_{RD_{j-k}} \| Pub_{RD_{j-k}} \| U_{RD_{j-k}} \| T_1). \tag{4.17}$$

and checks whether the following equation has been established:

$$
\begin{aligned}
&\delta_{RD_{j-k}}.P \stackrel{?}{=} \\
&\delta_{RD_{j-k}}.P \stackrel{?}{=} \left(u_{RD_{j-k}} SEC_{RD_{i-k}} + H_3^{'}\left(PS_{RD_{j-k}} + H_2 \cdot SEC_{RD_{i-k}} \cdot y_{RD_{j-k}}\right)\right).P \\
&= U_{RD_{j-k}} + H_3^{'}\left(PS_{RD_{j-k}} + H_2 \cdot SEC_{RD_{i-k}} \cdot y_{RD_{j-k}}\right).P \\
&= U_{RD_{j-k}} + H_3^{'}\left(\left(r_{RD_{j-k}} + S_{CDC} \cdot H_1^{'}\right) + H_2 \cdot SEC_{RD_{i-k}} \cdot y_{RD_{j-k}}\right).P \\
&= U_{RD_{j-k}} + H_3\left(r_{RD_{j-k}} + H_1^{'} \cdot Pub_{CDC} + H_2 \cdot SEC_{RD_{i-k}} \cdot y_{RD_{j-k}}\right).P \\
&= U_{RD_{j-k}} + H_3^{'}\left(R_{RD_{j-k}} + H_1^{'} \cdot Pub_{CDC} + H_2 \cdot SEC_{RD_{i-k}} \cdot X_{RD_{j-k}}\right) \\
&= U_{RD_{j-k}} + H_3^{'}\left(Q_{RD_{j-k}} \cdot SEC_{RD_{i-k}} + H_1^{'} \cdot Pub_{CDC}\right).
\end{aligned} \tag{4.18}
$$

If the verification is successful, the fog drone aggregates the signatures by calculating

$$
U_{RD_{j-k}} = \sum_{k=1}^{n} U_{RD_{j-k}} \delta_{RD_{j-k}} = \sum_{k=1}^{n} \delta_{RD_{j-k}}, \tag{4.19}
$$

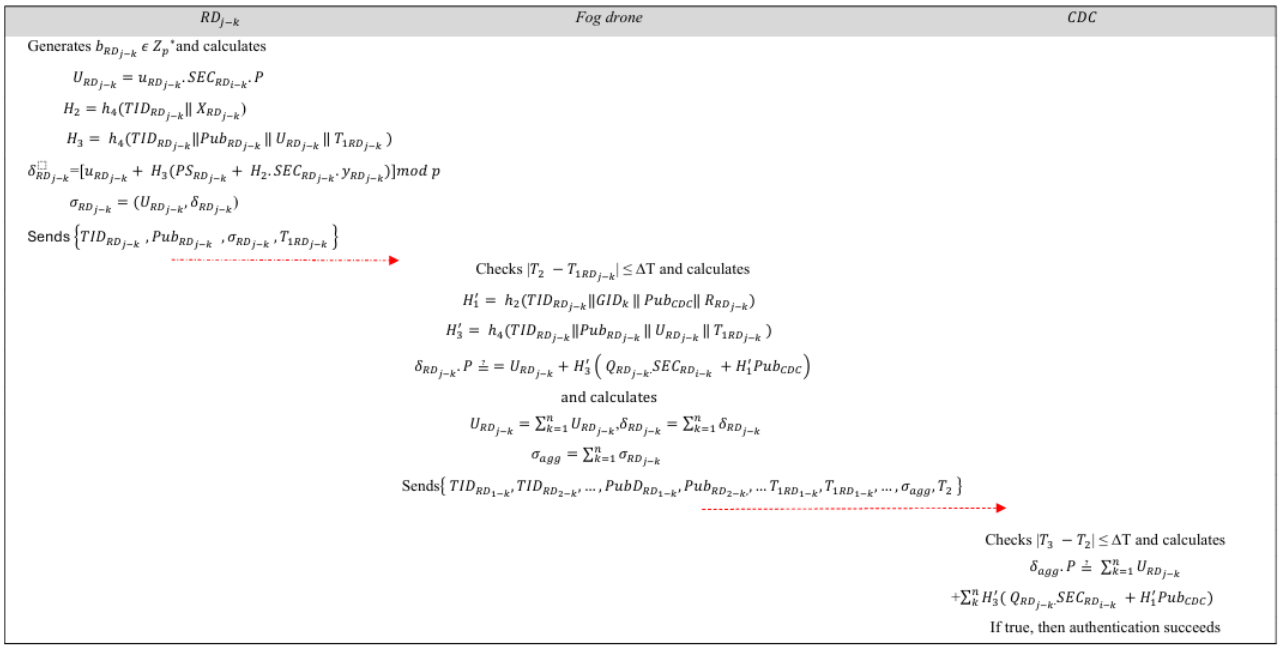
$$
\sigma_{\text{agg}} = \sum_{k=1}^{n} \sigma_{RD_{j-k}}. \tag{4.20}
$$

Next, it sends parameters $\{TID_{RD_{1-k}}, TID_{RD_{2-k}}, \ldots, PubD_{RD_{1-k}}, Pub_{RD_{2-k}}, \ldots, T_{1RD_{1-k}}, T_{1RD_{2-k}}, \ldots, \sigma_{\text{agg}}, T_2\}$ received from RD_{j-k} to the *CDC*. The *CDC* then checks whether T_2 is within the transmission time limit $|T_3 - T_2| \leq \Delta T$. If the response is negative, it terminates the session; otherwise, it checks if the signature has met the following condition:

$$
\begin{aligned}
\delta_{\text{agg}} \cdot P &\stackrel{?}{=} \sum_{k=1}^{n} \delta_{RD_i} \cdot P \sum_{k=1}^{n}\left(U_i + H_3^{'}\left(Q_{RD_{j-k}} SEC_{RD_{i-k}} + H_1^{'} Pub_{CDC}\right)\right) \\
&\stackrel{?}{=} \sum_{k=1}^{n} U_{RD_{j-k}} + \sum_{k=1}^{n} H_3^{'}\left(Q_{RD_{j-k}} SEC_{RD_{i-k}} + H_1^{'} Pub_{CDC}\right).
\end{aligned} \tag{4.21}
$$

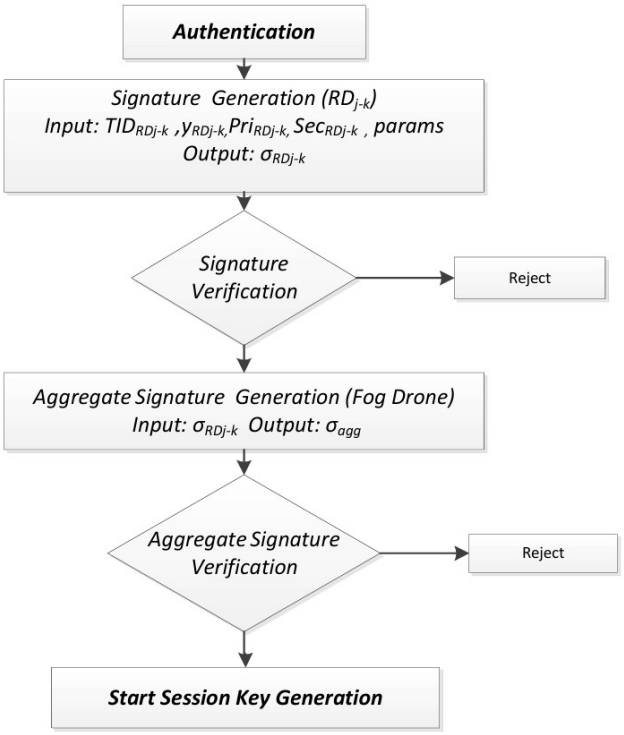
If it holds, all drones are authenticated and accepted as legitimate. The complete procedure is shown in Figure 4.6 and the flowchart of the authentication procedure is shown in Figure 4.7.

Figure 4.6. Authentication procedure



Source: Own authorship.

Figure 4.7. Flowchart of the authentication procedure



Source: Own authorship.

After a successful mutual authentication, a session key is created to ensure a secure

data exchange. The session key is calculated from pre-distributed secrets in the registration phase. First, the fog drone and the remote drone compare their known secrets, identify shared secrets, and exchange variables to create the session key. After that identification, the session keys between RD_{j-K} and the fog drone are calculated as follows:

$$SK_{RD_{j-k}} = \left(Sec_{RD_{1-k}} \oplus Sec_{RD_{2-k}} \oplus \ldots \oplus Sec_{CDC}\right).U_{RD_{j-K}}.U_{RD_{j-k}}, \tag{4.22}$$

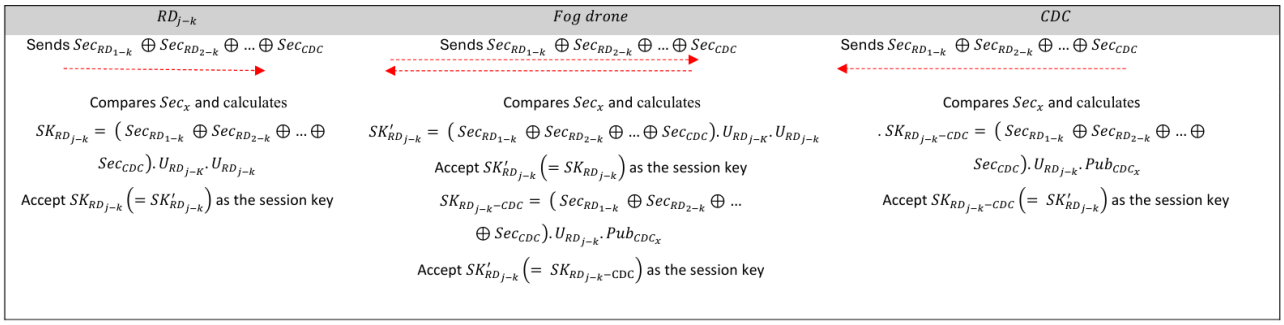
$$SK^{'}_{RD_{j-k}} = \left(Sec_{RD_{1-k}} \oplus Sec_{RD_{2-k}} \oplus \ldots \oplus Sec_{CDC}\right).U_{RD_{j-K}}.U_{RD_{j-k}}. \tag{4.23}$$

The session key between the CDC and the fog drone is similarly determined by:

$$SK_{RD_{j-k}-CDC} = \left(Sec_{RD_{1-k}} \oplus Sec_{RD_{2-k}} \oplus \ldots \oplus Sec_{CDC}\right).U_{RD_{RD-k}}.Pub_{CDC}. \tag{4.24}$$

Where $Sec_{RD_{1-k}} \oplus Sec_{RD_{2-k}} \oplus \ldots \oplus Sec_{CDC}$ represents the secret values shared between RD_{j-K} and CDC. This session key model is based on the approach proposed by Choi et al. [131] and demonstrates its effectiveness for secure communication between drones and support infrastructure. The complete procedure is shown in Figure 4.8.

Figure 4.8. Generation of session key



Source: Own authorship.

4.4.4 Drone Addition and Revocation Phase

When a new drone is deployed in the flight area, it is assigned to a specific flight zone and integrated into the corresponding cluster. The drone registers with the CDC and receives all parameters distributed during the registration/authentication phase, along with a free leaf from the binary tree that contains a secret key Sec_{NODE_x}.

A new group key for the cluster, which includes the secret from the joining drone's leaf, is computed with a new group identity. The newly generated parameters are then encrypted

with the old cluster key CK_{OLD_k} and transmitted to the cluster drones as follows:

$$CKnew_k = h_3\left(SEC_{RD_{1-k}} \oplus SEC_{RD_{2-k}} \oplus \ldots \oplus SEC_{RD_{j-k}} \oplus SEC_{CDC} \parallel s_{CDC} \parallel CID_k\right), \tag{4.25}$$

$$NewCK_k = CK_{old}(TID_{RD_{i-k}} \parallel CID_k \parallel CKnew_k). \tag{4.26}$$

The new drone also undergoes an authentication process to establish a session key with the cluster's fog drone. This process mirrors the one described in the mutual authentication section, but it is executed between multiple devices and a single device. Upon successful completion of this process, a session key is generated.

If the authorized RD_{j-k} has completed its tasks or has been inactive for a period longer than the one allowed by the system, it must be removed, since it may pose a threat. The registered and revoked identities of drones $ID_{RD_{j-k}}$are stored in the *CDC*'s database in a list called *Re*l, similarly to what was proposed by Jan et al. [95]. The system periodically consults the database to check the timestamps of drone records $RTS_{RD_{j-k}}$. If a drone's downtime exceeds the system's allowed limit, or if a drone has completed its tasks, the revocation procedure is executed as described below.

The fog drone forwards $TID_{RD_{j-k}}$ and an exit request of the revoked remote drone, encrypted with the current cluster's key CK_k, to *CDC* as follows:

$$Out_{RD_{j-k}} = CK_k(TID_{RD_{j-k}} \parallel CID_k). \tag{4.27}$$

The *CDC* receives the request, decrypts the message, and obtains the $TID_{RD_{j-k}}$of the drone that is leaving. The *CDC* then checks the $ID_{RD_{j-k}}$ in the database, marks it as a revoked drone in *ReL*, and searches for its credentials in the database, including CK_k and all parameters associated with the drone. Those keys are revoked and the drone is disassociated from its leaf in the binary tree. Next, the *CDC* selects a new random number $R_c \in Z_p^*$ and calculates a new CK_k, using equations 4.25 and 4.27, with secrets $Sec_{RD_{j-K}}$ of the remaining drones in the cluster. The CDC sends the new key group to the drones in the cluster.

If a remote drone wishes to return to the system, it must submit a new registration request to the *CDC*, which checks its database to determine whether RD_{j-k} can request a new registration or if it has been marked as discarded, captured, or compromised.

4.5 SECURITY ANALYSIS

This section is dedicated to analyses and discussions on the security objectives achieved by the protocol concerning the adversary models, namely, DY and CK attacks. It also includes a verification using AVISPA to substantiate the protocol's security.

4.5.1 Informal security analysis

This subsection presents an informal security analysis of the protocol, demonstrating its resilience against various security attacks while fulfilling the security properties for mutual authentication, anonymity, non-repudiation, confidentiality, forward/backward secrecy and session key agreement.

4.5.1.1 Mutual Authentication

Mutual authentication is achieved with the use of elliptic curve operations. The message shared by the remote drones includes $\left\{TID_{RD_{j-k}}, Pub_{RD_{j-k}}, \sigma_{RD_{j-k}}, T_{1RD_{j-k}}\right\}$, where $\sigma_{RD_{j-k}}$ is the remote drone's signature. Before accepting the signature, the fog drone verifies it using equation 4.20 and the CDC checks the aggregate signature of the cluster's drones using equation 4.21 to detect any message modifications. If the verification is successful, all drones in the cluster are authenticated through a single mutual authentication procedure, thus ensuring both authentication and integrity.

4.5.1.2 Anonymity

The protocol maintains the anonymity of the drones by ensuring only the CDC knows the drone's real identity and associated secret $Sec_{RD_{j-k}}$. Communication occurs over an insecure channel using temporary identities $TID_{RD_{j-k}}$, which prevents tracking of the drone's trajectory by an adversary or other drones. Therefore, the drone's anonymity is preserved.

4.5.1.3 Non-Repudiation

Since the *CDC* can link the drones' real identities to their temporary identities, no drone can deny its signature. The transmissions made by the drones are their responsibility. If a drone denies sending a message, its true identity is exposed. Equation $TID_{RD_{j-k}} = h_1(ID_{RD_{j-k}} \| b_{RD_{j-k}}.P)$ reveals the real identity of the drones. Therefore, the protocol ensures no drone can repudiate its transmissions.

4.5.1.4 Confidentiality

Confidentiality is ensured through session keys generated at the end of the mutual authentication phase. Each session key is calculated by both entities involved, and any message containing drone data is encrypted with the corresponding session key before being transmitted through an insecure channel. Therefore, only entities with the session key can access the drone data.

4.5.1.5 Session key agreement

The protocol elements involved in exchanging messages calculate a common session key, as described in the authentication phase, thus, guaranteeing a secure session key agreement.

4.5.1.6 Forward/Backward Secrecy

The proposed model guarantees forward and backward secrecy using dynamic group keys. The generation of new group keys in each authentication session ensures new drones cannot access previous communications, forthe latest key is not valid for old messages. Similarly, drones leaving the cluster cannot access future messages, since the group key has been updated, ensuring both forward and backward secrecies.

4.5.1.7 Resistance to Denial of Service (DoS) Attack

Denial of service (DoS) DoS attacks are mitigated by verifying the integrity of timestamps before any complex computations are performed during the authentication phase, Figure 4.6, thus preventing an adversary from overloading the system and ensuring uninterrupted service.

4.5.1.8 Ephemeral Secret Leakage Attack

The first part of the drone signature generation involves the calculation of $U_{RD_{j-k}} = u_{RD_{j-k}}.SEC_{RD_{j-k}}.P$, which includes long-term secret $SEC_{RD_{j-k}}$ and short-term secret $u_{RD_{j-k}}$. An adversary must compromise both $SEC_{RD_{j-k}}$and $u_{RD_{j-k}}$. According to the CK adversary model, even if short-term secret $u_{RD_{j-k}}$ is compromised, $U_{RD_{j-k}}$ remains secure because of long-term secret $SEC_{RD_{j-k.}}$ is not obtained. Therefore, the protocol resists ephemeral secret leakage attacks.

4.5.1.9 Resistance to Replay Attack

In the protocol, the drone includes a current timestamp $T_{1RD_{j-k}}$ in its signature, ensuring the timeliness of the message. Therefore, the fog drone can detect replay attacks before aggregating signatures. If a message is retransmitted, the fog drone identifies it as an attack and takes appropriate measures, ensuring both security and integrity of communications.

4.5.1.10 Resistance to Man-in-the-Middle Attack

Upon registration, a drone receives a temporary identity and partial private key from the CDC through a secure channel. Only legitimate drones with such information can communicate securely, which prevents an adversary from performing a man-in-the-middle attack. Additionally, session keys are based on secret values from the binary tree and Elliptic Curve Diffie-Hellman ($ECDH$) techniques, making them secure against interception. Group keys (CK) are also protected and cannot be derived from intercepted messages.

4.5.1.11 Resistance to Attack Inside the Group

The protocol prevents insider attacks by using distinct session keys for each connection, along with unique parameters such as identities, random values, and generated signatures, which ensures malicious drones cannot impersonate legitimate ones or use their session keys to access unauthorized information, thereby enhancing system security and preventing unauthorized data access.

Table 4.3 shows a comparison among the protocol proposed in this chapter and those of [123]and [124].

Table 4.3. Security Properties

PROPERTIES	LI EL AT. [123]	EVER ET AL. [124]	PROPOSED PROTOCOL
Mutual authentication	Yes	Yes	Yes
Anonymity	No	No	Yes
Non-Repudiation	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes
Session key agreement	No	Yes	Yes
Forward/Backward Secrecy	Yes	Yes	Yes
Resistance to Denial of Service (DoS) attack	No	Yes	Yes
Ephemeral Secret Leakage attack	Yes	No	Yes
Resistance to replay attack	Yes	Yes	Yes
Resistance to man-in-the-middle attack	Yes	Yes	Yes
Resistance to attack inside the group	No	Yes	Yes
Drone addition and revocation phase	No	No	Yes
Formal security verification by tool	No	No	Yes

Source: Own authorship.

4.5.2 Formal Security Verification by AVISPA

The protocol underwent a formal security verification through simulations and using the widely recognized Automated Validation of Internet Security Protocols and Applications (AVISPA). This semi-automated tool assesses the security integrity of authentication

protocols by evaluating the confidentiality of key parameters and their susceptibility to unauthorized access.

AVISPA analyzes network security protocols and applications encoded in High-Level Protocol Specification Language (HLPSL). HLPSL utilizes fundamental roles to define various potential configurations and characteristics representing critical role scenarios. Such roles operate independently, facilitating the acquisition of initial data for each parameter and enabling interaction with other roles through channels [72]. The output from AVISPA is processed via one of four back-ends, namely, On-the-Fly Model Checker (OFMC), Constraint Logic-based Attack Searcher (CL-AtSe), SAT-based Model Checker (SATMC), and Tree Automata based on Automatic Approximations for Analysis of Security Protocols (TA3SP) [56]. Inputs are transformed into an Intermediate Format (IF), and results are presented in an Output Format (OF), which details the security analysis findings of the examined protocol.

To validate the proposed scheme, we employed software tools such as SPAN (version: SPAN-Ubuntu-10.10-light) and Oracle VM Virtual Box (version: 7.0.6 r155176). The HLPSL source code of the proposed scheme contains five roles, namely, drone, fog drone, CDC, session, and environment, as shown in Figures 4.9, 4.10, 4.11 and 4.12. AVISPA uses a special identifier **i** for the intruder, as displayed in Figure 4.12.

The protocol was validated using OFMC and CL-AtSe back-ends of AVISPA. Both tools confirmed the security of the protocol. As shown in Figure 4.13, the simulation results indicated the protocol had met all security requirements. Figures 4.14 and 4.15 display the detailed simulation results, where both tools (OFMC and CL-AtSe) validated the security of the protocol.

Figure 4.9. Remote Drone Role

```
%%%%%%%%%%%  Drone %%%%%%%%%%%%
role drone(RD, FG, CDC : agent, SecureChannel1, SecureChannel2: symmetric key,
Abst modp,Aggregate signatures,Verify signature,P, H,Sum: hash func,
 SND, RCV : channel(dy))
played by RD
def=
local State: nat,
    IDrd, TIDrd, IDrdfg,CIDk,Urd,UUrd, T1, T2, T3,Secrd, Deltard,Sigmard : text,
    CKk, Rrd, RRrd, Scdc, Publcdc,GIDk, Qrd, Yrd, Xrd, H1, H2, H3, Eui: text,
    Egss, SKij, RTSrdj, Secrdj, Secrdfg, Seccdc, PSrd, Publrd,Prird, Rc, Brd: text,
    SKcdcfg,SKrdj_fog,SKfog_cdc: text,
    Check equation, Sigma agg: text
 const sp1,sp2,sp3,sp4,sp5,sp6: protocol id,
rd_fog_t1,rd_fog_sigmard,fg_cdc_t2,fg_cdc_sigma_agg,fg_cdc_sk,fog_cdc_sk : protocol_id
init State :=0
transition

%%%Registration phase
1. State = 0 /\ RCV(start) =|>
State':= 2
    /\ SND({IDrd}_SecureChannel1)
    /\ secret({IDrd}, sp3, {RD,CDC,FG})
2. State = 1 /\ RCV ({TIDrd.CKk.RRrd.H1. Secrd. PSrd} SecureChannel2) =|>
 State':= 4
    /\ Yrd' := new()  /\ Xrd' := (Yrd.P)
    /\ H2':= H(TIDrd.Xrd) /\ Qrd' := Sum(RRrd.H2).Xrd
    /\ Publrd' := (Qrd.Xrd)  /\ Prird' := (PSrd.Yrd)
    /\ secret({Yrd,H2',Qrd,Publrd,Prird'},sp6,{RD,FG})

%%%Login & Authentication phase
3. State = 5 /\ RCV(start) =|>
 State':= 3
    /\ T1' := new() /\ Urd' := new()
    /\ UUrd' := (Urd.Secrd.P)   /\ H2':= H(TIDrd.Xrd)
    /\ H3' := H(TIDrd.Publrd.UUrd.T1)
    /\ Deltard' := Abst_modp(Sum(Urd, H(Sum(PSrd, H2.Secrdj.Yrd))))
    /\ Sigmard' := (UUrd.Deltard)
    /\ SND ({TIDrd.Publrd.Sigmard.T1})
    /\ witness(RD, FG, rd_fog_t1, T1)  /\ witness(RD, FG, rd_fog_sigmard, Sigmard)
4.State = 3 /\ RCV ((Secrdj'. Secrdfg'.Seccdc'))=|>
State' := 8
    /\ SKrdj_fog':= {(Secrdj'. Secrdfg'. Seccdc').UUrd.Publcdc}
    /\ witness(RD, CDC, rd_fog_sk, SKrdj_fog')
end role
```

Source: Own authorship.

Figure 4.10. Fog Drone Role

```
%%%%%%%%%%  FOGDRONE %%%%%%%%%%%
role fogdrone(RD, FG, CDC : agent, SecureChannel1, SecureChannel2: symmetric key,
Abst_modp,Collectedallsignatures, Aggregate_signatures,Verify_signature,P, H,Sum:
hash_func,
 SND, RCV : channel(dy))
played_by FG
def=
local State: nat,
    IDrd, TIDrd, IDrdfg,CIDk,Urd,UUrd, T1, T2, T3,Secrd, Deltard,Sigmard : text,
    CKk, Rrd, RRrd, Scdc, Publcdc,GIDk, Qrd, Yrd, Xrd, H1, H2, H3, Eui: text,
    Egss, SKij, RTSrdj, Secrdj, Secrdfg, Seccdc,Csig, PSrd, Publrd,Prird, Rc, Brd:
    text,
    SKcdcfg,SKrdj fog,SKfog cdc: text,
    Check_equation, Sigma_agg: text
 const sp1,sp2,sp3,sp4,sp5,sp6: protocol_id,
rd fog t1,rd fog sigmard,fg cdc t2,fg cdc sigma agg,fg cdc sk,fog cdc sk : protocol id
init State :=0
transition

1. State = 0  /\ RCV ((TIDrd'. Publrd'. Sigmard'. T1'))=|>
State' := 6
    /\ T2' := new()    /\ H1' := H(TIDrd'.GIDk.Publcdc.Rrd)
    /\ H2':= H(TIDrd'.Xrd)
    /\ Check equation' := Verify signature(Sigmard'. TIDrd'. Publrd'. T1')
    /\ Csig' := Collectedallsignatures(Sigmard')
    /\ Sigma_agg' := Aggregate_signatures(Sigmard')
    /\ SND({TIDrd'. Publrd'. Sigma agg'. T2'} CDC)
    /\ witness(FG, CDC, fg_cdc_t2, T2')  /\ witness(FG, CDC, fg_cdc_sigma_agg,
    Sigma_agg')
2.State = 6 /\ RCV ((Secrdj'. Secrdfg'.Seccdc'))=|>
State' := 8
    /\ SKfog_cdc':= {(Secrdj'. Secrdfg'. Seccdc').UUrd.Publcdc}
    /\ witness(FG, CDC, fog_cdc_sk, SKfog_cdc)
end role
```

Source: Own authorship.

Figure 4.11. CDC Role

```
%%%%%%%%%%%  CDC %%%%%%%%%%%%
role cdc(RD, FG, CDC : agent, SecureChannel1, SecureChannel2: symmetric key,
Abst modp,Aggregate signatures,Verify signature,P, H,Sum: hash func,
 SND, RCV : channel(dy))
played_by CDC
def=
local State: nat,
    IDrd, TIDrd, IDrdfg,CIDk,Urd,UUrd, T1, T2, T3,Secrd, Deltard,Sigmard : text,
    CKk, Rrd, RRrd, Scdc, Publcdc,GIDk, Qrd, Yrd, Xrd, H1, H2, H3, Eui: text,
    Egss, SKij, RTSrdj, Secrdj, Secrdfg, Seccdc, PSrd, Publrd,Prird, Rc, Brd: text,
    SKcdcfg,SKrdj_fog,SKfog_cdc: text,
    Check_equation, Sigma_agg: text
 const sp1,sp2,sp3,sp4,sp5,sp6: protocol id,
rd fog t1,rd fog sigmard,fg cdc t2,fg cdc sigma agg,fg cdc sk,fog cdc sk : protocol id
init State :=0
transition

%%% Initialization phase
1. State = 0 /\ RCV(start) =|>
State' := 1  /\ Scdc' := new()  /\ Publcdc' := (Scdc'.P)
    /\ Rc' := new()     /\ CIDk' := H(Rc')
    /\ SND({Publcdc'.CIDk'.GIDk}_SecureChannel1)
    /\ secret({Scdc',Publcdc',Rc',CIDk'},sp1,{CDC})
    /\ secret({Publcdc',CIDk',GIDk},sp2,{CDC,RD,FG})

%%%Registration phase%%%
1. State = 2 /\ RCV({IDrd}_SecureChannel1)=|>
State' := 3
    /\ Rrd' := new()  /\ Brd' := new()
    /\ TIDrd' :=  H(IDrd.Brd'.P)
    /\ Secrd':= new() /\ Secrdfg' := new()
        /\ CKk' := H(xor(Secrd'.Secrdfg').Rc.CIDk)
        /\ RRrd' := (Rrd'.P)
        /\ H1' := H(TIDrd'.GIDk.Publcdc.RRrd')
        /\ PSrd' := Abst modp(Sum(Rrd'.Scdc).H1)
        /\ SND({TIDrd'.CKk'.RRrd'.H1'.Secrd'.Secrdfg'.PSrd'} SecureChannel2)
        /\ secret({Brd',TIDrd',CKk',Rrd',RRrd',H1', Secrd',PSrd'}, sp4, {CDC})
        /\ secret({TIDrd,CKk',RRrd',H1', Secrd',PSrd'}, sp5, {FG,RD})

%%%Login & Authentication phase
2.State = 2 /\ RCV ((TIDrd'. Publrd'. Sigma_agg'. T2'))=|>
State' := 7
    /\ T3' := new()
    /\ Check_equation':= Verify_signature(Sigma_agg'. TIDrd'. Publrd'. T2')
    /\ witness(FG, CDC, fg_cdc_sigma_agg, Sigma_agg')
3.State = 2 /\ RCV ((Secrdj'. Secrdfg'.Seccdc'))=|>
State' := 8
    /\ SKcdcfg':= {(Secrdj'. Secrdfg'. Seccdc').UUrd.Publcdc}
    /\ witness(FG, CDC, fog cdc sk, SKcdcfg')
end role
```

Source: Own authorship.

Figure 4.12. Session and Environment Roles

```
%%%%%%%%%%% Session %%%%%%%%%%%%
role session(RD, FG, CDC: agent, SecureChannel1, SecureChannel2: symmetric_key,
Abst modp,Collectedallsignatures, Aggregate signatures, Verify signature, P, H, Sum:
hash func) def=
    local SN1, SN2, SN3, RV1, RV2, RV3: channel(dy)
composition
    cdc(RD, FG, CDC, SecureChannel1, SecureChannel2, Abst modp, Aggregate signatures,
     Verify_signature, P, H, Sum, SN1, RV1)
    /\ drone(RD, FG, CDC, SecureChannel1, SecureChannel2, Abst_modp,
    Aggregate signatures,
     Verify signature, P, H, Sum, SN2, RV2 )
    /\ fogdrone(RD, FG, CDC, SecureChannel1, SecureChannel2, Abst_modp,
     Aggregate_signatures, Collectedallsignatures,Verify_signature, P, H, Sum, SN3,
     RV3 )
end role

role environment()
def=
const rd, fg, cdc : agent,
securechannel1, securechannel2: symmetric_key,
abst modp, aggregate signatures, verify signature, collectedallsignatures, p, h, sum:
hash func,
idrd, tidrd, sigma_agg,sigmard : text,

sp1,sp2,sp3,sp4,sp5,sp6: protocol id,
rd fog t1,rd fog sigmard,fg cdc t2,fg cdc sigma agg,fg cdc sk,rd fog sk,fog cdc sk  :
protocol_id

intruder knowledge = {rd,fg,idrd,tidrd,h,sigma agg,sigmard}
composition
session(rd, fg, cdc, securechannel1, securechannel2, abst_modp, aggregate_signatures,
verify signature,  collectedallsignatures, p, h, sum)
/\ session(i, cdc, rd, securechannel1, securechannel2, abst modp,
aggregate_signatures, verify_signature,  collectedallsignatures, p, h, sum)
/\ session(rd, i, fg,  securechannel1, securechannel2, abst_modp,
aggregate signatures, verify signature,  collectedallsignatures, p, h, sum)
/\ session(rd, cdc, i, securechannel1, securechannel2, abst modp,
aggregate_signatures, verify_signature,  collectedallsignatures, p, h, sum)

end role
```

Source: Own authorship.

Figure 4.13. Simulation goals

```
goal
secrecy of sp1, sp2, sp3, sp4, sp5, sp6
authentication on rd fog sigmard, rd fog t1, rd fog sk
authentication_on fg_cdc_sigma_agg, fg_cdc_t2, fog_cdc_sk
end goal
environment()
```

Source: Own authorship.

Figure 4.14. OFMC backend result

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/proposedprotocol2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 3.11s
  visitedNodes: 960 nodes
  depth: 9 plies
```

Source: Own authorship.

Figure 4.15. CL-AtSe backend result

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/proposedprotocol2.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 4 states
  Reachable  : 4 states
  Translation: 0.04 seconds
  Computation: 0.00 seconds
```

Source: Own authorship.

4.6 PERFORMANCE ANALYSIS

This section presents a performance analysis of the protocol, comparing it with those described in Li et al. [123] and Ever et al. [124]. The selection of protocols was based on similarity regarding network architecture and metrics used in the selected articles, enabling a fair comparison with the proposed scheme. Previous performance analyses of the chosen schemes demonstrated their lower computational costs, thus, raising our interest in choosing them. The selection was also based on their influence within the scientific community,

as evidenced by the Scopus database, for instance, according to which Ever et at. [124], has 66 citations to date. Moreover, such schemes aim to promote a tradeoff among efficiency, security, and lightweight attributes. In what follows are analyses of computational and communication costs.

4.6.1 Computational Costs

One of the main objectives of a protocol design is to minimize computational load without compromising security properties. Therefore, the computational costs involved in the authentication phase were assessed through comparisons with recent ones from the literature to evaluate the proposed protocol [123] and [124].

The experimental setup costs cited in [132] were adopted for our measurement of the computational cost and MIRACL library was used on two corresponding devices. An HP EliteBook 6360P with an Intel Core i7-2620 M processor at 2.7 GHz and 3 GB of RAM running Ubuntu 16.03 LTS operating system simulated the CDC and a Raspberry Pi 3 Model B+ with a 1.3GHz processor (Cortex-A53 - ARMv6) and 1 GB of RAM simulated the drone.

The methodology adopted for the performance evaluation considers the cost of each unitary operation multiplied by the number of times each operation is executed, encompassing the various messages that include one or more of those unitary operations, as required by the different authentication protocols. The execution times of the calculation operations are provided in Table 4.4.

A more recent reference was adopted in this chapter, using a device with a slightly higher clock frequency, which led to lower execution times for operations such as elliptic curve point addition, hash functions, and symmetric encryption when compared to the results of the previous chapter, which used the Raspberry Pi 3 model (1.2 GHz, 1 GB RAM). This difference can be attributed to incremental hardware improvements and optimizations in the execution environment, highlighting the influence of technological evolution and experimental setup on performance results.

Table 4.4. Execution Time of Different Cryptographic Operations

Notation	Description	Drone	CDC/Server
$\mathbf{T_B}$	Bilinear pairing	12.52 ms	3.036 ms
$\mathbf{T_{mul}}$	ECC point multiplication	3.107ms	0.926ms
$\mathbf{T_{add}}$	ECC point addition	0.016ms	0.006ms
$\mathbf{T_{hash}}$	Hash Function	0.006ms	0.003ms
$\mathbf{T_{sym}}$	Encryption scheme	0.013ms	0.006ms

Source: Own authorship.

Consider n as the number of remote drones participating in the authentication process in the evaluated protocols. In the protocol of Li et al. [123], RD_{j-k} performs $2nT_{hash} + 2nT_{mul} + 2nT_{add} + 4nT_B$. The aggregator drone ($AGT$) executes $(n+2)T_{hash} + 3T_{mul} + (n+4)T_{add} + 5T_B$ for request forwarding and aggregation operations, while the server performs $(2n+1)T_{hash}+3T_b$, resulting in a total computational cost of $\approx 58{,}374n + 87{,}111$ms.

In the scheme of Ever et al. [124], RD_{j-k} executes $10nT_{hash} + 2nT_B$, resulting in an execution time of $\approx 25{,}1n$. The cluster head executes $3nT_{hash} + 2nT_B$, leading to an execution time of $\approx 25{,}063n$, and the Control Server (CS) performs $7nT_{hash} + 2nT_B + 3nT_{mul}$, leading to a total execution time of $\approx 61{,}972n$ms..

In the proposed protocol, the authentication procedure involves the costs of signature generation, individual signature verification, aggregate signature verification, and session key establishment. Unlike the schemes of [123] and [124], bilinear pairing is not used; instead, elliptic curve digital signature algorithm (ECDSA) is adopted.

At the beginning of the authentication phase, RD_{j-k} calculates the parameters for generating its signature, resulting in a computational cost of $3nT_{hash} + 2nT_{mul} + 2nT_{add}$, hence, an execution time of $\approx 8{,}268n$ms.

Subsequently, the fog drone performs operations to verify the individual signatures of RD_{j-k} and aggregate them, resulting in a $2nT_{hash} + 3nT_{mul} + 3nT_{add} \approx 12{,}387n$m cost. The CDC verifies the aggregate signature, resulting in a $2nT_{mul}+2nT_{add} \approx 1{,}864n$ms cost. Finally, the remote drones establish a session key with the fog drones in the cluster, and fog drone with CDC, resulting in a computational cost of $2nT_{mul} + T_{mul} \approx 8{,}214n + 4{,}107$, and the CDC establishes a session key with the remote drones resulting in a computational cost

of $nT_{mul} \approx 0{,}926n$ms. Consequently, the cost incurred by the drones was $5nT_{hash} + 6nT_{mul} + T_{mul} + 5nT_{add} \approx 28{,}869n + 4{,}107$, which, added to that of CDC $3nT_{mul} + 2nT_{add} \approx 2{,}79n$, results in the computational cost of the protocol, expressed as $\approx 31{,}659n + 4{,}107$.

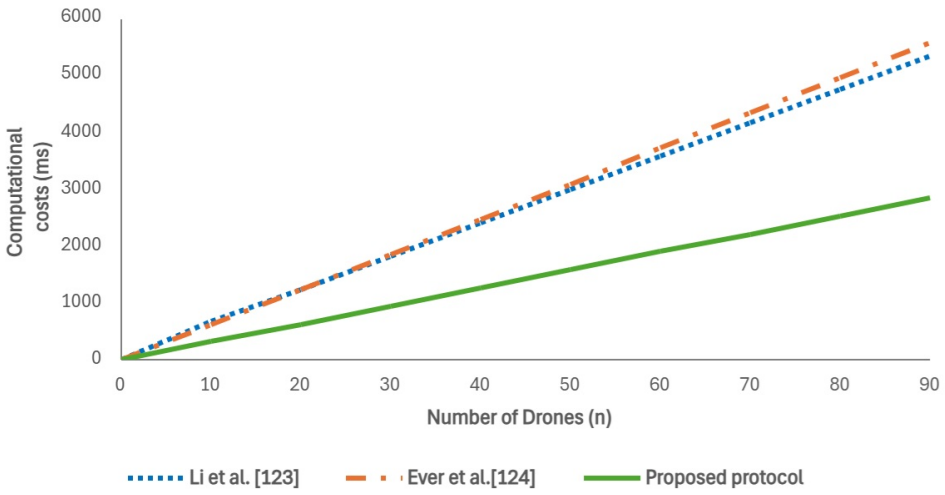
Details of the operations performed at each phase and the total computational cost, measured in milliseconds (ms), in Table 4.5 shows the computational costs of the proposed scheme and those of the protocols of Li et al. [123] and Ever et al. [124]. Figure 4.16 displays a graphic representation of the costs, varying linearly as a function of the number of drones, and confirms the proposed scheme's better performance regarding computational costs.

Table 4.5. Comparison of computational costs

PROTOCOLS (ms)	DRONES (ms)	CDC/SERVER	TOTAL (ms)
Li et al. [123]	$(3n + 2)T_{hash} + (3n + 4)T_{add} + (2n + 3)T_{mul} + (4n + 5)T_B \approx 58{,}366n + 74{,}933$	$(2n+1)T_{hash} + 3T_B \approx 0{,}008n + 12{,}118$	$\approx 58{,}3743n + 87{,}111$
Ever et al. [124]	$13nT_{hash} + 4nT_b \approx 50{,}164n$	$7nT_{hash} + 3nT_{mul} + 2nT_b \approx 11{,}808n$	$\approx 61{,}972n$
Proposed protocol	$5nT_{hash} + 6nT_{mul} + T_{mul} + 5nT_{add} \approx 28{,}869n + 4{,}107$	$3nT_{mul} + 2nT_{add} \approx 2{,}79n$	$\approx 31{,}659n + 4{,}107$

Source: Own authorship.

Figure 4.16. Comparison of computational costs



Source: Own authorship.

4.6.2 Communication Costs

Another objective of protocol design is to minimize communication costs without compromising security properties. To quantify these costs, we employed a methodology that involved identifying all exchanged messages, analyzing their structure, and computing the total number of bits transmitted during the authentication process. Specifically, the evaluation was based on the summation of the bit-length of cryptographic elements exchanged, such as public keys, nonces, hash outputs and digital signatures.

The communication costs involved in the authentication phase were evaluated through a comparison with two recent protocols proposed by Li et al. [123] and Ever et al. [124]. The following parameter sizes [132] were assumed according to the considerations provided in Table 4.6 for comparison:

Table 4.6. Size of each parameter

PARAMETERS	VALUES IN BITS
Identity	160
Timestamp	32
Encrypt/decrypt	126
ECC	160+160 =320
Bilinear Pairing	1023
Nonce	32
Hash function	256

Source: Own authorship.

The authentication procedure of the protocol of Li et al. [123] involves the exchange of 3 messages, totaling $640n + 640n + 832 + (640n + 640)$ and leading to a communication cost of $2752n + 630bits$. In the scheme of Ever et al [124], the authentication phase involves the exchange of five messages, totaling $992n + 512n + 160n + 1312n + 1260n$ and resulting in a communication cost of $3256nbits$.

In the proposed protocol, RD_{j-k} sends a message $\left\{TID_{RD_{j-k}}, Pub_{RD_{j-k}}, \sigma_{RD_{j-k}}, T_{1RD_{1-k}}\right\}$ to the fog drone for verification and subsequent aggregation of its signature with those of other RD_{j-k}in the cluster. This first message has a communication cost of approximately $256n + (320 + 320)\,n + 320n + 32n \approx 1236n$.

Next, the fog drone of the cluster transmits message $\{TID_{RD_{1-k}}, TID_{RD_{2-k}}, \ldots, PubD_{RD_{1-k}}$, $\text{Pub}_{RD_{2-k}}, \ldots T_{1RD_{1-k}}, T_{1RD_{1-k}}, \ldots, \sigma_{agg}, T_2$ to the *CDC*, which checks the aggregate signature and performs a mutual authentication of the drones. This second message has a communication cost of approximately $256n+320n+32n+(320+320)+32bits \approx 606n+672bits$.

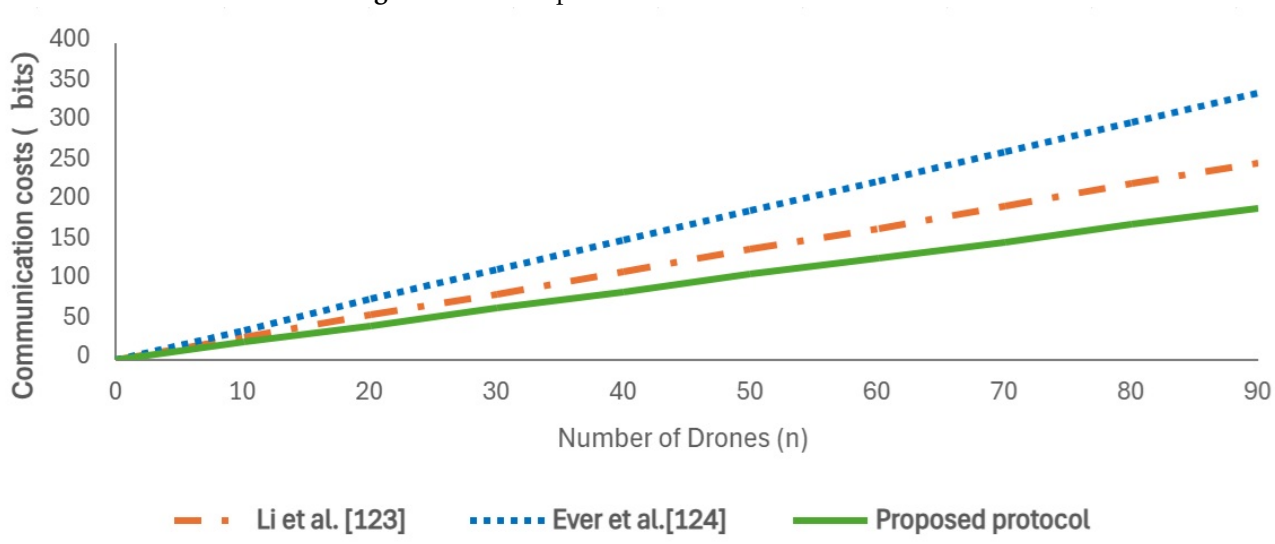
Finally, the session secret and key $Sec_{RD_{1-k}} \oplus Sec_{RD_{2-k}} \oplus \ldots \oplus Sec_{CDC}$ are sent, resulting in a communication cost of $256nbits$ Therefore, the protocol involves the exchange of fewer messages, providing better performance in terms of communication cost and totaling approximately $\approx 2112n+672bits$. Table 4.7 shows the communication costs of the proposed scheme and those of the protocols of Li et al. [123] and Ever et al. [124]. Figure 4.17 displays a graphic representation of the costs, varying linearly as a function of the number of drones. The proposed protocol demonstrates better performance, with communication costs lower and comparable to those of Li et al. [123].

Table 4.7. Comparison of communication costs

PROTOCOLS	MESSAGES	TOTAL (*bits*)
Li et al. [123]	3	$2752n+630$
Ever et al. [124]	5	$3256n$
Proposed protocol	2	$2112n+672$

Source: Own authorship.

Figure 4.17. Comparison of communication costs



Source: Own authorship.

4.6.3 Energy Costs

In IoD authentication protocols, energy efficiency is crucial for drone operation. The total energy consumption (E_{total}) combines computational (E_C) and communication (E_t), energy, both influenced by cryptographic complexity and communication design. This study analyzes the protocols by Li et al.[123], Ever et al.[124], and the proposed one under a unified framework, assuming a 100 mW (0.1W) processor—typical of ARM Cortex-M, widely used in drones.

The computational energy is given by:

$$E_c = P_{\text{CPU}} \times T_{\text{cpu}}. \tag{4.28}$$

Where P_{CPU} is the processor's power consumption and T_{cpu} is the total execution time of cryptographic operations such as ECDSA, hashing, and bilinear pairings.

The communication energy is calculated as:

$$E_t = P_t \times \frac{S}{R}. \tag{4.29}$$

where P_t is the transmission power, S is the message size in bits, and R is the data transmission rate.

Thus, the total energy consumption is given by:

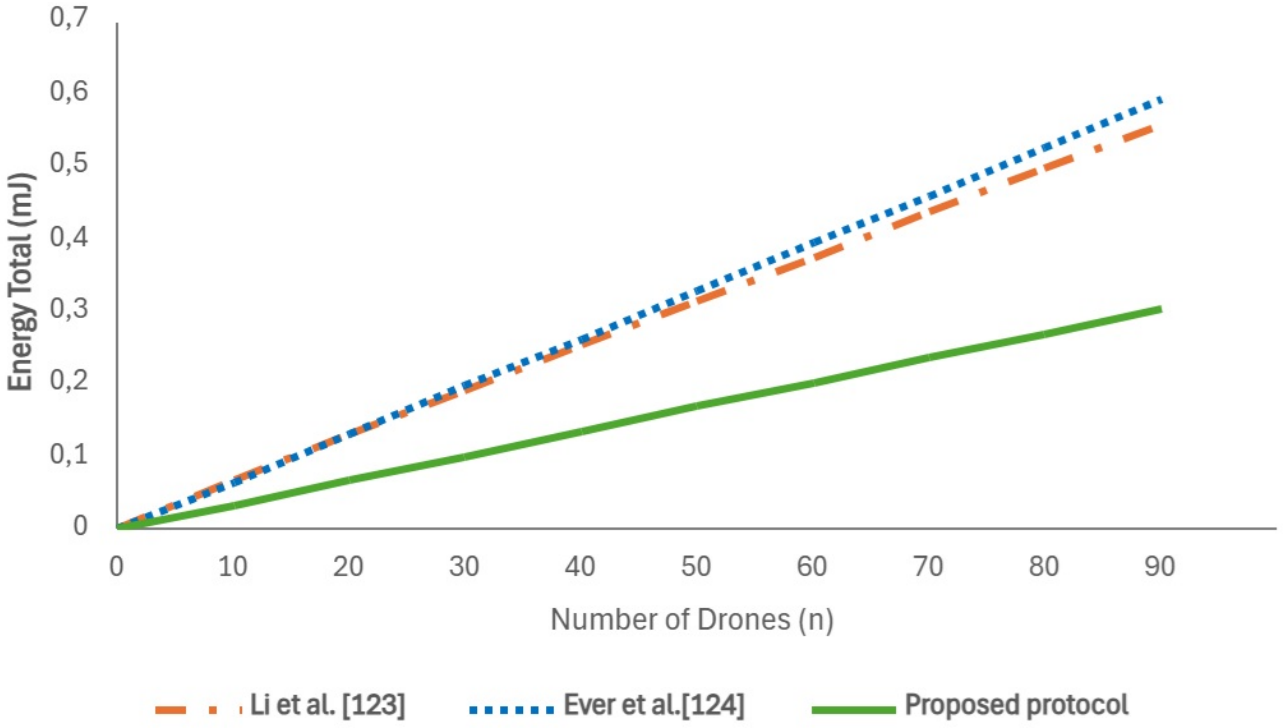
$$E_{\text{total}} = E_c + E_t. \tag{4.30}$$

This formulation allows for a precise comparison of energy performance across different authentication schemes under varying network sizes.

Figure 4.18 displays a graphic representation of the costs, varying linearly as a function of the number of drones. By analyzing the figure, it is evident that the proposed protocol consumes less energy than the schemes in [123] and [124], significantly as the number of drones increases. This reduction is primarily attributed to its lightweight cryptographic design and optimized message transmission, which minimize computational overhead. As

a result, the protocol demonstrates better scalability and efficiency in resource-constrained IoD environments.

Figure 4.18. Comparison of energy costs



Source: Own authorship.

4.7 CHAPTER CONCLUSIONS

This chapter presented an authentication protocol for the Internet of Drones (IoD) specifically tailored for use in forest inventories with fog computing. By utilizing asymmetric cryptography and aggregate signatures, the scheme offers a secure and efficient solution to the inherent challenges of IoD, such as communication on public channels, unstable connectivity, and a highly dynamic environment.

A security analysis conducted both informally and formally by AVISPA tool confirmed the robustness of the protocol against known attacks and its effectiveness in terms of communication, computational and energy performance in comparison to other authentication protocols from the literature.

Since this study focused on the applicability of the protocol to forest inventories, its

implications can be extended, opening doors for a variety of applications in other fields that use IoD. Additionally, integrating emerging technologies, such as blockchain, which was not explored here, is a promising path for future research.

CHAPTER 5

CONCLUSIONS

The primary objective of this dissertation was to develop novel authentication protocols for the IoD environment. Two protocols were proposed, targeting different application scenarios of IoD while considering the resource limitations and specific security challenges inherent to this environment. These protocols were designed to address the critical need for secure communication in IoD systems, where the sensitivity of collected data and the potential for malicious attacks necessitates robust security measures.

The first protocol focused on creating a multi-factor authentication scheme for IoD, utilizing biometrics and elliptic curve cryptography. It considers mutual authentication between users, remote drones, and the ground station server. The protocol was designed to provide confidentiality, privacy, and anonymity and to prevent attacks such as denial of service, impersonation, and data interception. This approach significantly enhances the security of IoD communications by leveraging multiple authentication factors, making it substantially more difficult for unauthorized entities to access the system. This protocol was developed for a generic IoD environment, in which users and drones interact with a centralized infrastructure and perform a variety of missions. The architecture reflects traditional IoD networks without intermediate computing nodes. Consequently, the design prioritizes strong user identity verification and session security, while ensuring lightweight cryptographic operations suitable for resource-constrained devices.

The second protocol, developed for forest inventory scenarios, integrates fog computing and aggregate signatures to authenticate groups of drones simultaneously. This approach enhances scalability and reduces communication latency and processing costs, addressing the challenges of large-scale IoD deployments. Fog computing not only accelerates processing and decision-making but also increases system security by reducing sensitive data exposure and enabling the implementation of more robust and contextualized security measures.

Due to this architectural distinction and its application context, the protocol design also includes energy cost modeling—an aspect not addressed in the first protocol—reflecting the unique operational demands of large-scale and energy-aware deployments.

Both protocols underwent rigorous security and performance evaluations and were compared to other proposals published in the literature. The security evaluation and comparison considered the fulfillment of properties such as confidentiality, integrity, privacy, and anonymity, as well as resistance to various attacks including man-in-the-middle, impersonation, and replay, among others. The two proposals demonstrated greater robustness compared to other proposals in the comparison, highlighting their effectiveness in addressing the complex security landscape of IoD environments.

The performance evaluation comprised the measurement of two main costs: computational and communication. Computational costs were evaluated based on the processing time of operations necessary to execute each protocol authentication session. Communication costs were measured in bits, considering all parameters in the messages exchanged between entities during an authentication session. In the case of the forest inventory protocol, a third metric—energy cost—was included, capturing the total consumption associated with computation and transmission activities, further emphasizing its suitability for constrained environments. This comprehensive evaluation approach ensures that the protocols provide strong security and remain efficient and practical for implementation in resource-constrained IoD environments.

Additionally, the proposed protocols were validated using the AVISPA tool, proving their practical security. The results obtained demonstrate that the developed protocols offer an effective balance between robust security and operational efficiency, meeting the specific demands of IoD environments. This validation provides confidence in the protocols' ability to withstand various security threats while maintaining the performance requirements necessary for real-world IoD applications.

This research contributes significantly to the field of IoD security, offering practical and efficient solutions to authentication challenges in this dynamic and resource-constrained environment. The proposed protocols enhance the security of communications in IoD and consider the processing and energy limitations of drones, making them suitable for imple-

mentation in real-world scenarios. By addressingsecurity and efficiency concerns, this work paves the way for more secure and reliable IoD deployments across various industries and applications.

Future work may explore the integration of these protocols with other emerging technologies, such as artificial intelligence and machine learning, to develop even more adaptive and resilient authentication systems. Furthermore, the application of these protocols in other IoD scenarios, such as package delivery and urban monitoring, could be investigated to expand their scope of utilization. Additionally, exploring the potential of blockchain technology in IoD authentication could provide new avenues for enhancing security and trust in distributed drone networks. Blockchain's decentralized and immutable nature could offer innovative solutions for secure data sharing, identity management, and transaction verification in IoD ecosystems, potentially revolutionizing the way drones interact and authenticate in complex, multi-stakeholder environments.

REFERENCES

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, dec 2017. doi: 10.1109/ACCESS.2017.2779844 .

[2] Y. Hajjaji, W. Boulila, I. R. Farah, I. Romdhani, and A. Hussain, "Big data and IoT-based applications in smart environments: A systematic review," *Computer Science Review*, vol. 39, p. 100318, feb 2021. doi: 10.1016/J.COSREV.2020.100318 .

[3] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, Deployments, and Integration of Internet of Drones (IoD): A Review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25 532–25 546, nov 2021. doi: 10.1109/JSEN.2021.3114266 .

[4] R. P. M. NETO and F. M. BREUNIG, "Drones nas Ciências Florestais," *Drones E Ciência*, p. 68, 2019.

[5] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019. doi: 10.1109/TVT.2019.2911672 .

[6] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *Journal of Information Security and Applications*, vol. 48, p. 102354, oct 2019. doi: 10.1016/J.JISA.2019.06.010 .

[7] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges," *IEEE Access*, vol. 9, pp. 57 243–57 270, 2021. doi: 10.1109/ACCESS.2021.3072030 .

[8] W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A Review on Security Issues and Solutions of the Internet of Drones," *IEEE Open Journal of the Computer Society*, vol. 3, no. June, pp. 96–110, 2022. doi: 10.1109/ojcs.2022.3183003 .

[9] E. T. Michailidis and D. Vouyioukas, "A Review on Software-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones," *Drones*, vol. 6, no. 2, pp. 1–26, 2022. doi: 10.3390/drones6020041 .

[10] A. Abdelmaboud, "The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends," *Sensors*, vol. 21, no. 17, 2021. doi: 10.3390/s21175718 .

[11] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A Robust Authenticated Key Management Protocol for the Internet of Drones," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1339–1353, jan 2022. doi: 10.1109/JIOT.2021.3084946 .

[12] A. K. Mishra, M. Wazid, D. P. Singh, A. K. Das, J. Singh, and A. V. Vasilakos, "Secure Blockchain-Enabled Authentication Key Management Framework with Big Data Analytics for Drones in Networks Beyond 5G Applications," *Drones 2023, Vol. 7, Page 508*, no. 8, p. 508, aug. doi: 10.3390/DRONES7080508 .

[13] A. Gupta, S. K. Gupta, C. Sachin, and K. Gupta, "A survey on green unmanned aerial vehicles-based fog computing: Challenges and future perspective," *Transactions on Emerging Telecommunications Technologies*, no. 11, p. e4603, nov. doi: 10.1002/ETT.4603 .

[14] S. Samanth, P. K V, and M. Balachandra, "Security in Internet of Drones: A Comprehensive Review," *Cogent Engineering*, no. 1, dec. doi: 10.1080/23311916.2022.2029080 .

[15] A. Vangala, A. K. Das, A. K. Das, S. K. Das, and Y. Park, "Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 904–919, 2023. doi: 10.1109/TIFS.2022.3231121 .

[16] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *Journal of Systems Architecture*, vol. 115, no. October 2020, p. 101955, 2021. doi: 10.1016/j.sysarc.2020.101955 .

[17] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, aug 2020. doi: 10.1109/TVT.2020.3000576 .

[18] K. Kethineni and P. Gera, "Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture," *Systems 2023, Vol. 11, Page 304*, no. 6, p. 304, jun. doi: 10.3390/SYSTEMS11060304 .

[19] S. U. Jan and H. U. Khan, "Identity and Aggregate Signature-Based Authentication Protocol for IoD Deployment Military Drone," *IEEE Access*, vol. 9, pp. 130 247–130 263, 2021. doi: 10.1109/ACCESS.2021.3110804 .

[20] S. Yu, A. K. Das, Y. Park, and P. Lorenz, "SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10 374–10 388, oct 2022. doi: 10.1109/TVT.2022.3188769 .

[21] D. Yu and L. Zhang, "Centralized and Distributed Consensus in Wireless Network: An Analytical Comparison," *Proceedings - 2022 IEEE 20th International Conference on Embedded and Ubiquitous Computing, EUC 2022*, pp. 81–89, 2022. doi: 10.1109/EUC57774.2022.00022 .

[22] P. Boccadoro, D. Striccoli, and L. A. Grieco, "An extensive survey on the Internet of Drones," *Ad Hoc Networks*, vol. 122, p. 102600, nov 2021. doi: 10.1016/J.ADHOC.2021.102600 .

[23] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," *IEEE Access*, pp. 1148–1162. doi: 10.1109/ACCESS.2016.2537208 .

[24] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of Drones (IoD): Threats, Vulnerability, and Security Perspectives," *Research Briefs on Information and Communication Technology Evolution*, vol. 4, pp. 64–77, aug 2018. doi: 10.56801/rebicte.v4i.67 .

[25] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, apr 2019. doi: 10.1109/JIOT.2018.2888821 .

[26] D. Joshi, D. Deb, and S. M. Muyeen, "Comprehensive Review on Electric Propulsion System of Unmanned Aerial Vehicles," *Frontiers in Energy Research*, vol. 10, p. 752012, may 2022. doi: 10.3389/FENRG.2022.752012/XML/NLM .

[27] Z. Xu, "UAV surveying and mapping information collection method based on Internet of Things," *Internet of Things and Cyber-Physical Systems*, vol. 2, pp. 138–144, jan 2022. doi: 10.1016/J.IOTCPS.2022.07.002 .

[28] S. A. R. Naqvi, S. A. Hassan, H. Pervaiz, and Q. Ni, "Drone-Aided Communication as a Key Enabler for 5G and Resilient Public Safety Networks," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 36–42, jan 2018. doi: 10.1109/MCOM.2017.1700451 .

[29] S. R. Haque, R. Kormokar, and A. U. Zaman, "Drone ground control station with enhanced safety features," *2017 2nd International Conference for Convergence in Technology, I2CT 2017*, vol. 2017-January, pp. 1207–1210, dec 2017. doi: 10.1109/I2CT.2017.8226318 .

[30] L. Garbarino, N. Genito, G. Di Capua, and R. Rocchio, "Innovative Low-Cost Design of a Ground Control Station for Unmanned Aerial Systems Experimentation," *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, 2023. doi: 10.1109/DASC58513.2023.10311145 .

[31] "Top 10 Applications of Drone Technology." [Online]. Available: https://blog.aonic.com/my/blogs-drone-technology/top-10-applications-of-drone-technology

[32] "PwC report highlights financial challenges and opportunities in the global UTM market - Unmanned airspace." [Online]. Available: https://www.pwc.com/c1/en/pdf-nf/PwC_DPS_Global_UTM_Report.pdf

[33] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles," *IEEE Access*, vol. 8, pp. 43 711–43 724, 2020. doi: 10.1109/ACCESS.2020.2977817 .

[34] C. A. N. dos Santos, D. d. A. Papa, L. d. S. Prado, E. O. Figueiredo, and E. J. L. Ferreira, "Uso de drone para mapeamento de açaizeiros na Amazônia Ocidental," 2021. [Online]. Available: http://www.alice.cnptia.embrapa.br/handle/doc/1139346

[35] E. Salamí, C. Barrado, E. Pastor, A. Lucieer, P. J. Zarco-Tejada, U. Rascher, G. Bareth, Y. Inoue, and P. S. Thenkabail, "UAV Flight Experiments Applied to the Remote Sensing of Vegetated Areas," *Remote Sensing 2014, Vol. 6, Pages 11051-11081*, vol. 6, no. 11, pp. 11 051–11 081, nov 2014. doi: 10.3390/RS61111051 .

[36] Dulifski, "Pwc global report on the commercial applications of drone technology, 2016." [Online]. Available: https://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf

[37] A. Gohari, A. B. Ahmad, R. B. A. Rahim, A. S. Supa'at, S. A. Razak, and M. S. M. Gismalla, "Involvement of Surveillance Drones in Smart Cities: A Systematic Review," *IEEE Access*, vol. 10, pp. 56 611–56 628, 2022. doi: 10.1109/ACCESS.2022.3177904 .

[38] S. H. Alsamhi, O. Ma, M. Samar Ansari, and S. K. Gupta, "Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization," *Drones 2019, Vol. 3, Page 13*, vol. 3, no. 1, p. 13, jan 2019. doi: 10.3390/DRONES3010013 .

[39] A. Gehlot, R. Singh, and D. Singh, "Modular attachments for several applications with the aid of an aerial drone," *International Interdisciplinary Humanitarian Conference for Sustainability, IIHC 2022 - Proceedings*, pp. 794–798, 2022. doi: 10.1109/IIHC55949.2022.10060339 .

[40] B. E. Balassa, R. Koteczki, B. Lukács, and L. Buics, "Sustainability Aspects of Drone-Assisted Last-Mile Delivery Systems—A Discrete Event Simulation Ap-

proach," *Energies 2023, Vol. 16, Page 4656*, vol. 16, no. 12, p. 4656, jun 2023. doi: 10.3390/EN16124656 .

[41] R. R. Beck, A. Vijeev, and V. Ganapathy, "Privaros: A Framework for Privacy-Compliant Delivery Drones," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 181–194, oct 2020. doi: 10.1145/3372297.3417858/SUPPL$_F$*ILE/COPY* .

[42] S. Vermani, "Smart Healthcare: Future Applications Challenges," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 131–135.

[43] N. Koshta, Y. Devi, and C. Chauhan, "Evaluating Barriers to the Adoption of Delivery Drones in Rural Healthcare Supply Chains: Preparing the Healthcare System for the Future," *IEEE Transactions on Engineering Management*, vol. 71, pp. 13 096–13 108, 2024. doi: 10.1109/TEM.2022.3210121 .

[44] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities," *IEEE Access*, vol. 7, pp. 128 125–128 152, 2019. doi: 10.1109/ACCESS.2019.2934998 .

[45] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the Sky: Leveraging UAVs for Disaster Management," *IEEE Pervasive Computing*, vol. 16, no. 1, pp. 24–32, jan 2017. doi: 10.1109/MPRV.2017.11 .

[46] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey," *Neural Computing and Applications*, vol. 35, no. 31, pp. 23 063–23 101, nov 2023. doi: 10.1007/S00521-023-08857-7/METRICS .

[47] W. Stallings, *Cryptography and network security: principles and practice*, 7th ed. Boston: Pearson, 2017.

[48] C. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel, and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, jan 2018. doi: 10.1109/MCOM.2017.1700390 .

[49] M. Adil, M. A. Jan, Y. Liu, H. Abulkasim, A. Farouk, and H. Song, "A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements with Future Research Directions," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1437–1455, feb 2023. doi: 10.1109/TITS.2022.3220043 .

[50] D. Basin, S. Mödersheim, and L. Viganò, "OFMC: A symbolic model checker for security protocols," *International Journal of Information Security*, vol. 4, no. 3, pp. 181–208, 2005. doi: 10.1007/s10207-004-0055-7 .

[51] J. P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, sep 2020. doi: 10.1016/J.IOT.2020.100218 .

[52] Z. Li, Z. Gui, B. Hofer, Y. Li, S. Scheider, and S. Shekhar, "Geospatial information processing technologies," *Manual of digital earth*, pp. 197–227, 2020. doi: 10.1007/978-981-32-9915-3$_6$.

[53] S. Sofia, F. G. Maetzke, M. Crescimanno, A. Coticchio, D. S. La Mela Veca, and A. Galati, "The efficiency of LiDAR HMLS scanning in monitoring forest structure parameters: implications for sustainable forest management," *EuroMed Journal of Business*, vol. 17, no. 3, pp. 350–373, 2022. doi: 10.1108/EMJB-01-2022-0017 .

[54] M. Vishweshwaran and E. R. Sujatha, "A Review on Applications of Drones in Geotechnical Engineering," *Indian Geotechnical Journal*, 2024. doi: 10.1007/s40098-024-01071-9 .

[55] F. E. Fassnacht, J. C. White, M. A. Wulder, and E. Næsset, "Remote sensing in forestry: current challenges, considerations and directions," *Forestry: An International Journal of Forest Research*, vol. 97, no. 1, pp. 11–37, 2024. doi: 10.1093/forestry/cpad024 .

[56] Y. Gao, M. Skutsch, J. Paneque-Gálvez, and A. Ghilardi, "Remote sensing of forest degradation: a review," *Environmental Research Letters*, no. 10, p. 103001, sep. doi: 10.1088/1748-9326/ABAAD7 .

[57] E. Chuvieco, *Fundamentals of satellite remote sensing: an environmental approach*, 2nd ed. Boca Raton: CRC Press, 2016.

[58] M. Drusch, U. Del Bello, S. Carlier, O. Colin, V. Fernandez, F. Gascon, B. Hoersch, C. Isola, P. Laberinti, P. Martimort, A. Meygret, F. Spoto, O. Sy, F. Marchese, and P. Bargellini, "Sentinel-2: ESA's Optical High-Resolution Mission for GMES Operational Services," *Remote Sensing of Environment*, vol. 120, pp. 25–36, 2012. doi: https://doi.org/10.1016/j.rse.2011.11.026 .

[59] L. M. G. Fonseca, J. C. N. Epiphanio, D. M. Valeriano, J. V. Soares, J. C. L. Dalge, and M. A. Alvarenga, "Earth observation applications in Brazil with focus on the CBERS program," *IEEE Geoscience and Remote Sensing Magazine*, vol. 2, no. 2, pp. 53–55, 2014.

[60] H. Ren, Y. Zhao, W. Xiao, and Z. Hu, "A review of UAV monitoring in mining areas: current status and future perspectives," *International Journal of Coal Science and Technology*, vol. 6, no. 3, pp. 320–333, sep 2019. doi: 10.1007/S40789-019-00264-5/FIGURES/6 .

[61] M. B. Nuwantha, C. N. Jayalath, M. P. Rathnayaka, D. C. Fernando, L. Rupasinghe, and M. Chethana, "A Drone-Based Approach for Deforestation Monitoring," in *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2022, pp. 1–6. doi: 10.1109/ICCCNT54827.2022.9984404 .

[62] A. Qureshi and D. Megías Jiménez, "Blockchain-Based Multimedia Content Protection: Review and Open Challenges," *Applied Sciences*, vol. 11, no. 1, 2021. doi: 10.3390/app11010001 .

[63] E. de Suporte SSL, "O que é uma função criptográfica de hash? - SSL.com." [Online]. Available: https://www.ssl.com/pt/artigo/o-que-{é}-uma-fun{ç}{~{a}}o-de-hash-criptogr{á}fico/

[64] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Computer Communications*, vol. 153, pp. 229–249, mar 2020. doi: 10.1016/J.COMCOM.2020.02.011 .

[65] A. J. MENEZES, P. C. VAN OORSCHOT, and S. A. VANSTONE, *Handbook of applied cryptography*, 1st ed. Boca Raton: CRC Press, 1996.

[66] P. Rogaway and T. Shrimpton, "Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance," in *Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers 11*. Springer, 2004, pp. 371–388.

[67] NIST, "Hash functions | csrc," Nist.gov, 01 2017. [Online]. Available: https://csrc.nist.gov/projects/hash-functions

[68] J. Lee, S. Yu, M. Kim, Y. Park, and A. Kumar Das, "On the Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks," *IEEE Access*, vol. 8, pp. 107 046–107 062, 2020. doi: 10.1109/ACCESS.2020.3000790 .

[69] V. Odelu, A. K. Das, and A. Goswami, "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, sep 2015. doi: 10.1109/TIFS.2015.2439964 .

[70] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 523–540. doi: 10.1007/978-3-540-24676-$3_3$1 .

[71] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983. doi: 10.1109/TIT.1983.1056650 .

[72] "AVISPA v1.1 User Manual The AVISPA Team," 2006. [Online]. Available: https://people.irisa.fr/Thomas.Genet/Crypt/AVISPA_manual.pdf

[73] "Analysing cryptographic protocols with AVISPA | AVISPA Project | Results in brief | FP5 | CORDIS | European Commission." [Online]. Available: https://cordis.europa.eu/article/id/83181-analysing-cryptographic-protocols-with-avispa

[74] A. Gumaei, M. Al-Rakhami, M. M. Hassan, P. Pace, G. Aloi, K. Lin, and G. Fortino, "Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Mode Detection," *IEEE Network*, vol. 35, no. 1, pp. 94–100, mar 2021. doi: 10.1109/MNET.011.2000204 .

[75] A. K. Das, B. Bera, M. Wazid, S. S. Jamal, and Y. Park, "IGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment," *IEEE Access*, vol. 9, pp. 87 024–87 048, 2021. doi: 10.1109/ACCESS.2021.3089871 .

[76] "Amazon Prime Air prepares for drone deliveries." [Online]. Available: https://www.aboutamazon.com/news/transportation/amazon-prime-air-prepares-for-drone-deliveries

[77] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 53–63, jan 2020. doi: 10.1007/S12083-019-0718-9/TABLES/3 .

[78] V. O. Nyangaresi and M. A. Morsy, "Towards Privacy Preservation in Internet of Drones," *6th International Forum on Research and Technology for Society and Industry, RTSI 2021 - Proceedings*, pp. 306–311, 2021. doi: 10.1109/RTSI50628.2021.9597324 .

[79] M. Zhang and X. Li, "Drone-Enabled Internet-of-Things Relay for Environmental Monitoring in Remote Areas Without Public Networks," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7648–7662, aug 2020. doi: 10.1109/JIOT.2020.2988249 .

[80] M. Yahuza, M. Y. I. Idris, A. W. A. Wahab, T. Nandy, I. B. Ahmedy, and R. Ramli, "An edge assisted secure lightweight authentication technique for safe communication on the internet of drones network," *IEEE Access*, vol. 9, pp. 31 420–31 440, 2021. doi: 10.1109/ACCESS.2021.3060420 .

[81] J. H. Cheon, K. Han, S. M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song, "Toward a Secure Drone System: Flying with Real-Time Homomorphic Authenticated Encryption," *IEEE Access*, vol. 6, pp. 24 325–24 339, mar 2018. doi: 10.1109/ACCESS.2018.2819189 .

[82] Y. Park, D. Ryu, D. Kwon, and Y. Park, "Provably Secure Mutual Authentication and Key Agreement Scheme Using PUF in Internet of Drones Deployments," *Sensors 2023, Vol. 23, Page 2034*, no. 4, p. 2034, feb. doi: 10.3390/S23042034 .

[83] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones," *arXiv.org*, apr 2019.

[84] Y. Lei, L. Zeng, Y. X. Li, M. X. Wang, and H. Qin, "A Lightweight Authentication Protocol for UAV Networks Based on Security and Computational Resource Optimization," *IEEE Access*, vol. 9, pp. 53 769–53 785, 2021. doi: 10.1109/ACCESS.2021.3070683 .

[85] V. O. Nyangaresi and N. Petrovic, "Efficient PUF Based Authentication Protocol for Internet of Drones," *2021 International Telecommunications Conference, ITC-Egypt 2021 - Proceedings*, pp. 1–4, jul 2021. doi: 10.1109/ITC-EGYPT52936.2021.9513902 .

[86] C. L. Chen, Y. Y. Deng, W. Weng, C. H. Chen, Y. J. Chiu, and C. M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics (Switzerland)*, vol. 9, no. 1, pp. 1–31, 2020. doi: 10.3390/electronics9010062 .

[87] M. Wazid, A. K. Das, N. Kumar, and M. Alazab, "Designing Authenticated Key Management Scheme in 6G-Enabled Network in a Box Deployed for Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7174–7184, 2021. doi: 10.1109/TII.2020.3020303 .

[88] B. A. Alzahrani, A. Barnawi, and S. A. Chaudhry, "A Resource-Friendly Authentication Protocol for UAV-Based Massive Crowd Management Systems," *Security and Communication Networks*, vol. 2021, 2021. doi: 10.1155/2021/3437373 .

[89] I. Bhattarai, C. Pu, K. K. Raymond Choo, and D. Korac, "A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Inter-

net of Drones," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19 790–19 803, jun 2024. doi: 10.1109/JIOT.2024.3367799 .

[90] M. Tanveer, A. Aldosary, N. Kumar, and S. A. Aldossari, "SEAF-IoD: Secure and efficient user authentication framework for the Internet of Drones," 2024. doi: 10.1016/j.comnet.2024.110449 .

[91] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Applied Sciences (Switzerland)*, vol. 10, no. 9, 2020. doi: 10.3390/app10093149 .

[92] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, I. C. o. t. T. EUROCRYPT2002 and A. of Cryptographic Techniques, Eds., vol. 2332. Amsterdam: Springer Verlag, 2002, pp. 337–351. doi: 10.1007/3-540-46035-$7_2$2 .

[93] M. Tanveer, A. Alkhayyat, A. Naushad, A. U. Khan, N. Kumar, and A. G. Alharbi, "RUAM-IoD: A Robust User Authentication Mechanism for the Internet of Drones," *IEEE Access*, vol. 10, pp. 19 836–19 851, 2022. doi: 10.1109/ACCESS.2022.3149376 .

[94] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002. doi: 10.1109/TC.2002.1004593 .

[95] S. U. Jan, F. Qayum, and H. U. Khan, "Design and Analysis of Lightweight Authentication Protocol for Securing IoD," *IEEE Access*, vol. 9, pp. 69 287–69 306, 2021. doi: 10.1109/ACCESS.2021.3076692 .

[96] V. Kumar, A. Mohammed Ali Al-Tameemi, A. Kumari, M. Ahmad, M. W. Falah, and A. A. Abd El-Latif, "PSEBVC: Provably Secure ECC and Biometric Based Authentication Framework Using Smartphone for Vehicular Cloud Environment," *IEEE Access*, vol. 10, no. July, pp. 84 776–84 789, 2022. doi: 10.1109/ACCESS.2022.3195807 .

[97] H. J. B. d. Araujo, "Inventário florestal a 100% em pequenas áreas sob manejo florestal madeireiro," *Acta Amazônica*, vol. 36, pp. 447–464, 2006. doi: 10.1590/S0044-59672006000400007 .

[98] E. Tomppo, K. Schadauer, R. E. McRoberts, T. Gschwantner, K. Gabler, and G. Ståhl, *Introduction*. Dordrecht: Springer Netherlands, 2010, pp. 1–18. doi: 10.1007/978-90-481-3233-1$_1$.

[99] E. Lopatin and P. Poikonen, "Cost-Effective Aerial Inventory of Spruce Seedlings Using Consumer Drones and Deep Learning Techniques with Two-Stage UAV Flight Patterns," *Forests 2023, Vol. 14, Page 973*, no. 5, p. 973, may. doi: 10.3390/F14050973 .

[100] "Satélites de Monitoramento - Portal Embrapa," 2020. [Online]. Available: https://www.embrapa.br/en/satelites-de-monitoramento

[101] M. A. et al NALON, "Drones mapeiam matas brasileiras.[Depoimento a Tiago Jokura]," *Pesquisa FAPESP*, vol. 300, pp. 76–79, 2021. [Online]. Available: https://repositorio.usp.br/bitstreams/d733e08c-530c-4683-b660-92dd1f0657d9

[102] M. Ruwaimana, B. Satyanarayana, V. Otero, A. M. Muslim, A. Muhammad Syafiq, S. Ibrahim, D. Raymaekers, N. Koedam, and F. Dahdouh-Guebas, "The advantages of using drones over space-borne imagery in the mapping of mangrove forests," *PLOS ONE*, no. 7, p. e0200288, jul. doi: 10.1371/JOURNAL.PONE.0200288 .

[103] T. P. Banu, G. F. Borlea, and C. Banu, "The use of drones in forestry," *Journal of Environmental Science and Engineering B*, vol. 5, no. 11, pp. 557–562, 2016. doi: 10.17265/2162-5263/2016.11.007 .

[104] E. Alvarez-Vanhard, T. Corpetti, and T. Houet, "UAV satellite synergies for optical remote sensing applications: A literature review," *Science of Remote Sensing*, vol. 3, p. 100019, jun 2021. doi: 10.1016/J.SRS.2021.100019 .

[105] J. McGlade, L. Wallace, B. Hally, K. Reinke, and S. Jones, "The Effect of Surrounding Vegetation on Basal Stem Measurements Acquired Using Low-Cost Depth Sensors in Urban and Native Forest Environments," *Sensors 2023, Vol. 23, Page 3933*, vol. 23, no. 8, p. 3933, apr 2023. doi: 10.3390/S23083933 .

[106] K. Kuželka, R. Marušák, and P. Surový, "Inventory of close-to-nature forest stands using terrestrial mobile laser scanning," *International Journal of Applied Earth Observation and Geoinformation*, vol. 115, p. 103104, dec 2022. doi: 10.1016/J.JAG.2022.103104 .

[107] M. V. N. D'Oliveira, E. O. Figueiredo, D. R. A. de Almeida, L. C. Oliveira, C. A. Silva, B. W. Nelson, R. M. da Cunha, D. de Almeida Papa, S. C. Stark, and R. Valbuena, "Impacts of selective logging on Amazon forest canopy structure and biomass with a LiDAR and photogrammetric survey sequence," *Forest Ecology and Management*, vol. 500, p. 119648, nov 2021. doi: 10.1016/J.FORECO.2021.119648 .

[108] S. K. Srivastava, K. P. Seng, L. M. Ang, A. A. Pachas, and T. Lewis, "Drone-Based Environmental Monitoring and Image Processing Approaches for Resource Estimates of Private Native Forest," *Sensors 2022, Vol. 22, Page 7872*, no. 20, p. 7872, oct. doi: 10.3390/S22207872 .

[109] L. Calisto, "Obtenção e utilização de imagens de alta resolução (espacial, espectral e temporal) na Gestão Florestal, obtidas por Sistemas Aéreos Não Tripulados," *Simpósio Brasileiro De Sensoriamento Remoto*, vol. 16, pp. 3199–3206, 2013.

[110] K. Kumar, S. Kumar, O. Kaiwartya, P. K. Kashyap, J. Lloret, and H. Song, "Drone assisted Flying Ad-Hoc Networks: Mobility and Service oriented modeling using Neuro-fuzzy," *Ad Hoc Networks*, vol. 106, p. 102242, sep 2020. doi: 10.1016/J.ADHOC.2020.102242 .

[111] A. Derhab, O. Cheikhrouhou, A. Allouch, A. Koubaa, B. Qureshi, M. A. Ferrag, L. Maglaras, and F. A. Khan, "Internet of drones security: Taxonomies, open issues, and future directions," *Vehicular Communications*, vol. 39, p. 100552, feb 2023. doi: 10.1016/J.VEHCOM.2022.100552 .

[112] A. Solanki, S. Tarar, S. P. Singh, and A. Tayal, *The internet of drones: AI applications for smart solutions*. CRC Press, 2022.

[113] K. Han, E. A. Nuaimi, S. A. Blooshi, R. Psiakis, and C. Y. Yeun, *A New Scalable Mutual Authentication in Fog-Edge Drone Swarm Environment*. Springer International Publishing. doi: 10.1007/978-3-031-21280-2$_1$0 .

[114] A. Gupta, . Sachin, K. Gupta, and C. Sachin, "Flying through the secure fog: A complete study on UAV-Fog in heterogeneous networks," *International Journal of Communication Systems*, no. 13, p. e5237, sep. doi: 10.1002/DAC.5237 .

[115] Y. Luo, Q. Hu, Y. Wang, J. Wang, O. Alfarraj, and A. Tolba, "Revenue Optimization of a UAV-Fog Collaborative Framework for Remote Data Collection Services," *IEEE Access*, vol. 8, pp. 150 599–150 610, 2020. doi: 10.1109/ACCESS.2020.3016779 .

[116] A. Sharma, P. Vanjani, N. Paliwal, C. M. Basnayaka, D. N. K. Jayakody, H. C. Wang, and P. Muthuchidambaranathan, "Communication and networking technologies for UAVs: A survey," *Journal of Network and Computer Applications*, vol. 168, p. 102739, oct 2020. doi: 10.1016/J.JNCA.2020.102739 .

[117] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1123–1152, apr 2016. doi: 10.1109/COMST.2015.2495297 .

[118] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," *IEEE Network*, vol. 35, no. 1, pp. 130–137, mar 2021. doi: 10.1109/MNET.011.2000223 .

[119] "Remote Sensing and Image Processing: Examining Privacy and Data Protection Issues | Free Essay Example." [Online]. Available: https://studycorgi.com/remote-sensing-and-image-processing-examining-privacy-and-data-protection-issues/

[120] E. T. Michailidis, K. Maliatsos, D. N. Skoutas, D. Vouyioukas, and C. Skianis, "Secure UAV-Aided Mobile Edge Computing for IoT: A Review," *IEEE Access*, vol. 10, pp. 86 353–86 383, 2022. doi: 10.1109/ACCESS.2022.3199408 .

[121] P. Mall, R. Amin, M. S. Obaidat, and K. F. Hsiao, "CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN," *Computer Networks*, vol. 199, p. 108476, nov 2021. doi: 10.1016/J.COMNET.2021.108476 .

[122] B. Semal, K. Markantonakis, and R. N. Akram, "A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks," *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*, vol. 2018-September, dec 2018. doi: 10.1109/DASC.2018.8569730 .

[123] J. Li, M. Zhao, Y. Ding, D. Y. Liu, Y. Wang, and H. Liang, "An aggregate authentication framework for unmanned aerial vehicle cluster network," *Proceedings - 2020 IEEE International Symposium on Parallel and Distributed Processing with Applications, 2020 IEEE International Conference on Big Data and Cloud Computing, 2020 IEEE International Symposium on Social Computing and Networking and 2020 IEE*, pp. 1249–1256, 2020. doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom51426.2020.00185 .

[124] Y. Kirsal Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Computer Communications*, vol. 155, pp. 143–149, apr 2020. doi: 10.1016/J.COMCOM.2020.03.009 .

[125] J. Subramani, A. Maria, A. S. Rajasekaran, and J. Lloret, "Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones," *Security and Privacy*, vol. 7, no. 3, p. e364, may 2024. doi: 10.1002/SPY2.364 .

[126] R. A. Da Silva, N. L. Da Fonseca, and R. Boutaba, "Evaluation of the Employment of UAVs as Fog Nodes," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 20–27, oct 2021. doi: 10.1109/MWC.101.2100018 .

[127] R. Ganesan, X. M. Raajini, A. Nayyar, P. Sanjeevikumar, E. Hossain, and A. H. Ertas, "BOLD: Bio-Inspired Optimized Leader Election for Multiple Drones," *Sensors 2020, Vol. 20, Page 3134*, vol. 20, no. 11, p. 3134, jun 2020. doi: 10.3390/S20113134 .

[128] L. Ye, Y. Zhang, Y. Li, and S. Han, "A Dynamic Cluster Head Selecting Algorithm for UAV Ad Hoc Networks," *2020 International Wireless Commu-*

nications and Mobile Computing, IWCMC 2020, pp. 225–228, jun 2020. doi: 10.1109/IWCMC48107.2020.9148458 .

[129] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and A. Alsewari, "Chebyshev Polynomial-Based Fog Computing Scheme Supporting Pseudonym Revocation for 5G-Enabled Vehicular Networks," *Electronics 2023, Vol. 12, Page 872*, no. 4, p. 872, feb. doi: 10.3390/ELECTRONICS12040872 .

[130] D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "A robust provable-secure privacy-preserving authentication protocol for Industrial Internet of Things," *Peer-to-Peer Networking and Applications*, no. 3, pp. 1548–1571, may. doi: 10.1007/S12083-020-01063-5/TABLES/10 .

[131] D. Choi, S. Hong, and H. K. Choi, "A group-based security protocol for machine type communications in LTE-advanced," *Proceedings - IEEE INFOCOM*, pp. 161–162, 2014. doi: 10.1109/INFCOMW.2014.6849205 .

[132] S. Hussain, M. Farooq, B. A. Alzahrani, A. Albeshri, K. Alsubhi, and S. A. Chaudhry, "An Efficient and Reliable User Access Protocol for Internet of Drones," *IEEE Access*, vol. 11, pp. 59 688–59 700, 2023. doi: 10.1109/ACCESS.2023.3284832 .

APPENDIX A

PUBLICATION IN THE PEER-TO-PEER NETWORKING AND APPLICATIONS JOURNAL- HTTPS://DOI.ORG/10.1007/S12083-024-01862-0

Peer-to-Peer Networking and Applications (2025) 18:69
https://doi.org/10.1007/s12083-024-01862-0

A multi-factor user authentication protocol for the internet of drones environment

Manuela de Jesus Sousa[1] · Paulo Roberto L. Gondim[1]

Received: 27 December 2023 / Accepted: 18 September 2024

Abstract
Due to the popularization of unmanned aerial vehicles (UAVs), many of which are known as drones, the Internet of Drones (IoD) has gained significant importance over the past years in several areas and has been implemented in a wide range of fields (e.g., military, rescue, agriculture, and entertainment). It is enabled by the implementation of several drones in different flight zones for undertaking specific tasks, commonly collecting data in real time and providing them to users who communicate with them through their mobile devices. However, owing to the critical nature of information and the utilization of public communication channels, privacy and security issues must be considered. Authentication protocols can be adopted for reliable and secure communication, enabling data exchange between the user and the drone and resisting attacks such as man-in-the-middle and replay. On the other hand, due to the peculiarities of IoD environments, the development of an efficient protocol in terms of resource consumption that meets security properties is challenging. This article proposes a user authentication scheme based on biometry and elliptic curve cryptography for IoD. Its robustness was evaluated by a security analysis and a semi-automatized verification by AVISPA tool, which confirmed the scheme resists several known attacks against passive/active adversaries and meets security properties such as anonymity, authenticity, and nontraceability. Moreover, it shows better communication and computational performance in comparison to other authentication protocols from the literature.

Keywords Internet of drones (IoD) · UAVs · Authentication · Security

1 Introduction

Due to the continuous miniaturization of processors and sensors, wireless connectivity, and the advent of 5G and 6G networks, the number of solutions using drones has increased toward improving lifestyles [1]. This has led to a successful adoption of IoD to support different applications, such as pack delivery, delivery of medicine in areas affected by the pandemic, traffic surveillance, and search and rescue operations. Its use has significantly increased in several fields, from agriculture to industry, from government to private organizations, and from rural areas to smart cities [2]. In 2022, Amazon, the giant retailer, officially started offering its Lockeford customers in California a pack-delivery service via drones [3]. AT&T has also implemented drones for automating its inspections of cellular towers and Dubai (UAE) recently introduced drones in transport, launching its flying taxi service [4].

The Internet of Drones (IoD) involves a network control architecture that provides coordinated access to a controlled aerial space to unmanned aerial vehicles (UAVs), generally called drones [5]. Drones play a fundamental role in IoD networks and have been incorporated as units of communication, computation, energy, and control, as well as board advanced actuators and sensors (e.g., cameras, accelerometers, and gyroscopes) for data collection and measurements of altitude, speed, and location, among other tasks. As shown in Fig. 1, the IoD architecture usually includes remote drones, users, and a ground station server (GSS) Remote drones collect/monitor information on the environment, whereas users aim to access such data in real

This article is part of the Topical Collection: *Track on Security and Privacy*
Guest Editor: Rongxing Lu

✉ Manuela de Jesus Sousa
sousamanuela@gmail.com

Paulo Roberto L. Gondim
pgondim@unb.br

[1] Department of Electrical Engineering, Faculty of Technology, University of Brasilia, Brasilia 70910-900, DF, Brazil

Published online: 14 January 2025

APPENDIX B

ARTICLE ACCEPTED FOR PUBLICATION AT THE IEEE SMARTNETS 2025 EVENT

Secure and Energy-Efficient Authentication Protocol for the Internet of drones in Forest Inventory

1st MANUELA DE JESUS SOUSA
Dept. of Electrical Engineering
Universidade de Brasília (UNB)
Brasília, Brazil
sousamanuela@gmail.com

2nd PAULO ROBERTO L. GONDIM
Dept. of Electrical Engineering
Universidade de Brasília (UNB)
Brasília, Brazil
pgondim@unb.br

3rd JAIME LLORET
IMCZ Research Institute
Universitat Politècnica de València (UPV)
Valencia, Spain
jlloret@dcom.upv.es

***Abstract*—The Internet of Drones (IoD) has gained importance in the area of forest inventory, utilizing advanced sensors and Internet connectivity for efficient data collection and surpassing traditional methods in cost-effectiveness. However, it faces security and privacy challenges due to public channel communications, unreliable connectivity, and a dynamic environment. Protecting forest inventory data is crucial to ensuring accuracy, preventing unauthorized access, and avoiding data manipulation, which might lead to inadequate management decisions. An authentication protocol secures IoD communication and must offer mutual authentication among entities, be resistant to attacks and lightweight regarding resource consumption. This paper presents a novel Authentication and Key Agreement (AKA) protocol that uses asymmetric cryptography and aggregate signatures with IoD in forest inventories for fog computing. Its robustness was confirmed through security analyses, demonstrating resistance to known attacks. In comparison with other protocols, a superior computational and energy efficiency has been proven.**

***Index Terms*—Internet of Drones (IoD), fog computing, authentication, security, drone swarm, aggregated signatures, forest inventory.**

I. Introduction

Forest inventory is vital for forest management, aiding in the understanding of biodiversity, monitoring tree vitality, and tracking vegetation development, which is crucial amidst progressive deforestation. Additionally, maintaining forest cover is essential for ecological balance and assessments of composition and suitability for silvicultural purposes [1]. Traditional methods for data collection are often costly, error-prone, and impractical for expansive and remote forests [2].

Technological advancements, such as geotechnology and satellite communication, have improved forest inventory processes. However, geotechnology can have limitations in updating data and detecting changes in land use or vegetation. Although satellites provide regular large-scale coverage, challenges that include high costs, inadequate spatial resolution for tree-level studies, and cloud interference limit their utility in specific contexts. Towards overcoming those limitations, drones have emerged as a cost-effective alternative, offering high-resolution images and operational flexibility [2].

Equipped with versatile sensors, they enable the collection of detailed vegetation data and integration with Internet of Things (IoT) devices for a comprehensive monitoring [3]. In this context, the integration of drones with the Internet has introduced a new paradigm known as the Internet of Drones (IoD), which extends the principles of the IoT. IoD enhances drone operations by enabling interconnectivity, self-organization, and collaboration [6].

The environment in which forest inventories are conducted is inherently complex and dynamic, characterized by a diverse range of species and vegetation components. These inventories can occur in remote and inaccessible areas, where rugged terrain and adverse weather conditions pose significant challenges to deploying communication infrastructures such as antennas, ground stations, and energy resources [4].

A promising approach to mitigating these limitations is the application of fog computing in IoD architectures [3]. In this model, drones can be equipped with computational and storage resources to function as fog nodes. This enables local data processing and storage before transmission to the cloud, significantly reducing data traffic, optimizing bandwidth usage, and improving energy efficiency. Furthermore, this approach expands the coverage area and enhances data transmission in remote regions without direct Internet connectivity [5].

Despite such advancements, IoD environments face significant security challenges, including vulnerabilities to cyber threats, data breaches, and authentication issues [3] [4]. Ensuring secure communication channels and reliable authentication is critical to protecting sensitive forest data from misuse. Authentication protocols prevent unauthorized access and ensure data integrity, addressing the unique challenges of IoD systems in dynamic and resource-constrained environments. Several studies have proposed IoD authentication protocols; however, the existing schemes often lack adaptability to IoD environments [6].

Our literature review identified no authentication protocol specifically designed for IoD environments with applications in forest inventories.

This manuscript introduces a secure Authentication and Key Agreement (AKA) protocol for IoD environments in forest inventory, incorporating asymmetric cryptography and an elliptic curve digital signature algorithm (ECDSA). The proposed protocol enables mutual authentication and ensures secure sessions among drones, fog nodes, and ground stations.

The main contributions of the manuscript are:

Acceptance e-mail:

Manuela de Jesus Sousa <manuela.sousa@embrapa.br>

[SmartNets 2025 - SCitiesIoE] Your paper #1571126168 ('Secure and Energy-Efficient Authentication Protocol for the Internet of Drones in Forest Inventory')

1 mensagem

smartnets2025-scitiesioe-chairs@edas.info <smartnets2025-scitiesioe-chairs@edas.info> 27 de abril de 2025 às 05:02
Para: Manuela de Jesus Sousa <manuela.sousa@embrapa.br>, Paulo Roberto de Lira Gondim <pgondim@ene.unb.br>, Jaime Lloret <jlloret@dcom.upv.es>

Dear Ms. Manuela Sousa:

Congratulations!- your paper #1571126168 ('Secure and Energy-Efficient Authentication Protocol for the Internet of Drones in Forest Inventory') for SmartNets 2025 - SCitiesIoE has been accepted for presentation in the SmartNets 2025 conference, and will be published in the conference proceedings and submitted to the IEEE Xplore.

Please prepare your final manuscript while taking into consideration the following guidelines and then submit your paper via EDAS. :

consider the reviewers' comments follow the IEEE Templates when formating your final manuscripts

o All hypertext links - email addresses + Reference Links
- should be disabled,

o the numbering of pages is not allowed

_ the paper should be checked with PDF eXpress as required in "Registration" (PDF Instructions) on the website,

Authors who are not going to attend physically the conference should submit through EDAS the recorded video presentation(s) of their paper(s), (in mp4 format and lasting 10 min) by ***June 29, 2025*** . More instructions are provided in the following: https://smartnets.ieee.tn/video-instructions/

The Early Bird Registration Deadline is ***May 18*** , and the deadline for the camera-ready paper submission and for authors' Final registration is ***June 08, 2025*** .

At least one of the authors of each accepted paper must register for the conference.

The reviews are below or can be found at 1571126168.

Best Regards,

SmartNets 2025 Technical Program Committee Chairs

Review 1

Reviewer Familiarity?: Please assess your familiarity with the subject matter of the paper.

Working in this area of research (1)

Relevance and Timeliness: Rate the importance of the topic addressed in the paper and its timeliness within its area of research.

Excellent (5)

Technical content and correctness: Rate the technical contribution of the paper, its soundness and scientific rigour.

Solid work of some importance (4)

Novelty and originality: Rate the novelty and originality of the work presented in the paper.

Some novel results on a subject well investigated (3)

Quality of presentation: Rate the paper organization, the clearness of text and figures, the completeness and accuracy of references.

Well written (4)

Recommended Changes: Comments to the author: Please indicate any changes that should be made to the paper if it is accepted.

In this paper, authors introduce an Authentication and Key Agreement (AKA) protocol for the Internet of Drones in forest inventory applications. The topic is timely and the paper technically sounds. A good overview on related work and background is provided. The system model along with the proposed protocol are well explained. This protocol uses asymmetric cryptography and aggregate signatures to secure communication and ensure data integrity. Its robustness is confirmed through security analyses, demonstrating resistance to known attacks. The protocol also shows superior computational and energy efficiency compared to existing protocols. However, to further improve the quality of the paper, the authors are suggest to consider the following issues: _the protocol implementation complexity should be discussed as it requires significant computations resources *while the protocol is designed to be scalable, its performance validation in large scale IoD networks should be discussed* the protocol effectiveness validation in real world testing considering practical scenarios are required to provide meaningful recommendations

Review 2

Reviewer Familiarity?: Please assess your familiarity with the subject matter of the paper.

Working in this area of research (1)

Relevance and Timeliness: Rate the importance of the topic addressed in the paper and its timeliness within its area of research.

Excellent (5)

Technical content and correctness: Rate the technical contribution of the paper, its soundness and scientific rigour.

Solid work of some importance (4)

Novelty and originality: Rate the novelty and originality of the work presented in the paper.

Some novel results on a subject well investigated (3)

Quality of presentation: Rate the paper organization, the clearness of text and figures, the completeness and accuracy of references.

Well written (4)

Recommended Changes: Comments to the author: Please indicate any changes that should be made to the paper if it is accepted.

This paper presents an Authentication and Key Agreement-AKA- protocol. It aims to address the unique security challenges of IoD in forest inventory applications while maintaining efficiency and scalability. The proposed mechanism uses asymmetric cryptography and aggregate signatures to secure data transmission between drones, fog nodes and ground stations. The proposed protocol is designed to ensure mutual authentication among all entities involved in the IoD network to prevent unauthorized access and data manipulation. A performance analysis is performed showing that its lightweight design minimizes energy consumption. This protocol is however compared with only two existing protocols, limiting the scope of its performance evaluation. Its integration with existing IoD infrastructures should be also discussed. Anyway, the paper is well written and organized. Its conclusions and potential impacts are made clear.

Review 3

Reviewer Familiarity?: Please assess your familiarity with the subject matter of the paper.

Working in this area of research (1)

Relevance and Timeliness: Rate the importance of the topic addressed in the paper and its timeliness within its area of research.

Excellent (5)

Technical content and correctness: Rate the technical contribution of the paper, its soundness and scientific rigour.

Valid work but marginal or incremental contribution (3)

Novelty and originality: Rate the novelty and originality of the work presented in the paper.

Some novel results on a subject well investigated (3)

Quality of presentation: Rate the paper organization, the clearness of text and figures, the completeness and accuracy of references.

Well written (4)

Recommended Changes: Comments to the author: Please indicate any changes that should be made to the paper if it is accepted.

Authors introduce a novel AKA protocol that uses asymmetric cryptography and aggregate signatures to secure IoD communications in forest inventory applications. They demonstrate that the proposed protocol ensures mutual authentication among entities, preventing unauthorized access and data manipulation. It maintains drone anonymity and ensures non-repudiation, enhancing security and accountability. The paper provides a detailed performance evaluation, demonstrating the protocol's superior computational and energy efficiency. However, the authors do not explicitly mention if the presented results are derived from simulations or the analytical model. It is indeed not mentioned how simulations are performed while comparing the proposed mechanism with two other protocols. Overall, the paper is concise. Its findings will certainly generate discussions.