Design and Development of Secure Communication in IoT-based UAV Networks

A THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

DOCTOR OF PHILOSOPHY

Submitted by

JATIN SHARMA
(2K22/PHD/CO/02)

Under the supervision of

DR. PAWAN SINGH MEHRA

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi 110042

SEPTEMBER, 2025

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Jatin Sharma (2K22/PHDCO/02) Research Scholar (Department of Computer Science and Engineering), hereby declare that the thesis titled **"Design and Development of Secure Communication in IoT-based UAV Networks"**, which is submitted by me to the Department of Computer Science and Engineering, Delhi Technological University, in partial fulfilment of the requirement for the award of Doctorate of Philosophy is original and not copied from any source without proper citation. This work has not previously formed the basis for awarding any Degree, Diploma, Associateship, Fellowship or other title or recognition.

Place: Delhi Jatin Sharma

Date:

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

This is to certify that the work entitled **"Design and Development of Secure Communication in IoT-based UAV Networks"**, which is being submitted by **Mr. Jatin Sharma, Roll No. 2K22/PHD/CO/02** to the Department of Computer Science Engineering, Delhi Technological University for the award of the degree of Doctor of Philosophy is a record bonafide research work carried out by him under my supervision and guidance. He has fulfilled the requirements for the submission of this thesis. The contents of this thesis, in whole or in parts, have not been submitted for any other degree or diploma.

Place: Delhi　　　　Dr. Pawan Singh Mehra

Date:　　　　**SUPERVISOR**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

Be grateful when things go good and graceful when they go bad; as it is said, I feel immensely grateful when it comes to acknowledging my thanks to those who helped me complete my thesis successfully. At the onset, I bowed my head to the almighty God, who led me on this path, as everything has been possible with his blessings.

I take great pleasure in expressing my gratitude with profound respect to my revered supervisor, **Dr. Pawan Singh Mehra**, Assistant Professor, Department of Computer Science and Engineering, Delhi Technological University, New Delhi, for his invaluable guidance, close supervision, untiring ever, ready help and discussions throughout my Ph.D. work. I am indebted to him for his constructive criticism, exemplary patience, perseverance, motivation, and immense knowledge, which have gone a long way towards completing this thesis. His constant inspiration gave me considerable impetus to achieve this milestone. I could not have imagined having a better supervisor and mentor for my Ph.D. study.

I extend my gratitude to **Prof.(Dr.) Manoj Kumar**, Head, Department of Computer Science and Engineering, Delhi Technological University, New Delhi, for his support and guidance in carrying out this research work.

I also extend my heartiest thanks to the **Departmental Research Committee** for monitoring the progress and providing priceless suggestions encouraging me to widen my research from various perspectives.

I am also deeply grateful to all the members of the Department of Computer Science and Engineering, Delhi Technological University, for their constant help and providing all the necessary research resources.

I am also thankful to all academic, administrative and technical staff of Delhi Technological University for providing me with the university's resources and the necessary laboratory and research facilities for carrying out this work throughout my candidature.

A special thanks to my family members for their love, encouragement, patience and trust. With God's grace, this work allows me to make my parents, **Mr. Pawan Sharma** and **Mrs. Suman Sharma**, feel proud. I am also thankful to my brother, **Mr. Hitesh Sharma**. Their prayer for me was what sustained me in reaching this milestone.

Place: Delhi

Jatin Sharma
2K22/PHD/CO/02

Abstract

IoT (Internet of Things) has revolutionised the world with applications like home automation, transportation, agriculture, etc. IoT-based Unmanned Aerial Vehicle (UAV) networks are an emerging field that introduces the UAV network with the power of the Internet.

IoT-based UAV networks are networks of External Users (EU) and interconnected UAVs equipped with sensors, flight controllers, and other components to exchange collected data with each other via GCS (Ground Control Station) over the Internet. IoT-based UAV network system is used for surveillance, monitoring, and payload delivery in smart city environments, which generate a plethora of sensitive information, such as traffic situations on the road and high-definition images of properties and survivors during natural calamities, which can be obtained by adversaries in the middle for there bad intentions.

Communication between the External EU, UAVs, and GCS is vulnerable to security threats, such as eavesdropping replay attacks and location and physical capture attacks. The message between these entities is not enciphered, which makes them error-prone. Moreover, UAVs are resource-constrained devices with limited storage and computational capabilities to complete the assigned mission and task. Therefore, robust and lightweight authentication schemes are required for secure data transmission in IoT-based UAV networks. Thus, we aim to identify modern cryptographic techniques with provable security based on mathematics to overcome the current security challenges in IoT-based UAV networks.

To achieve the abovementioned framework, we have examined peer-reviewed literature that discusses previous six-year established papers with existing attacks, such as physical and logical attacks with suggested solutions such as trajectory planning, lightweight schemes, solutions based on blockchain, quantum cryptography, etc. This survey analyses the secure communication network between UAVs by systematically answering research questions based on the research methodology for the relevant study. Finally, the survey addresses several issues and guidelines for future research.

One of the modern cryptography techniques, such as Hyperelliptic Curve Cryptography (HCC) utilising Genus-2 curve and Fuzzy Extractor (FE)-based cryptosystem, is proposed to protect sensitive information during communication in IoT-based UAV networks. The scheme is designed with lightweight operations such as XOR, hash functions, random nonces, and timestamps. HCCs maximum key size is 80 bits, differing from the 160-bit requirement of the elliptic curve, making it apt for UAVs with limited resources. The proposed scheme utilises biometrics traits of users to avoid exposing data from stealing smart devices using FE. This protocol facilitates the mutual authentication of users and UAVs, allowing them to exchange a session key for secure communication. The Hyperelliptic Curve (HC) scalar multiplication protects the users private key from attackers, even in public channels. The obfuscation identity of the user and UAVs generated through the hash function and timestamp makes the external user and UAV anonymous. The efficacy of this proposed framework is examined using the Scyther verification tool and Random oracle model-based formal analysis, and informal analysis is also discussed, which validates its robustness against well-known potential physical and logical attacks. The performance analysis shows that the HC-based scheme has lower computation, communication, and storage costs than existing schemes.

Keywords: Internet of Things (IoT), Unmanned aerial vehicle (UAV), Authentication, Fuzzy Extractor(FE), Hyperelliptic Curve Cryptography(HCC), Secure communication.

Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

Abbreviation	**Description**	**Abbreviation**	**Description**
IoT	Internet of Things	UAV	Unmanned Aerial Vehicles
GCS	Ground Control Station	EU	External Users
UAS	Unmanned Aircraft System	5G NR	5G New Radio
WiFi	Wireless Fidelity	VTOL	Vertical Takeoff and Landing
ESC	Electronic Speed Controllers	FC	Flight Controller
VT	Video Transmitter	SHA	Secure Hash Algorithm
RC	Remote Controller	IR	Infrared
IEEE	Institute of Electrical and Electronics Engineers	HAP	High altitude platform
LAP	Low altitude platform	MALE	Medium Altitude Long Endurance
HALE	High Altitude Long Endurance	NATO	North Atlantic Treaty Organization
FANET	Flying Adhoc Network	MANET	Mobile Adhoc Network
VANET	Vehicle Adhoc Network	GPS	Global Positioning System
A2A	Air to Air Communication	S2A	Space-to-Air
A2G	Air to Ground	MITM	Man-in-the-Middle
DoS	Denial of Service	ECC	Elliptic Curve Cryptography
HCC	Hyperelliptic Curve Cryptography	RSA	Rivest-Shamir-Adleman
HCDLP	Hyperelliptic Curve Discrete logarithm problem	WSNs	Wireless Sensor Networks
RO	Research Objectives	RQ	Research Questions
GSM	Global System for Mobile Communications	WEP	Wired Equivalent Privacy
WPA2	Wi-Fi Protected Access 2	BLE	Bluetooth Low Energy
RMS	Remote management server	ADS-B	Automatic Dependent Surveillance-Broadcast
IMU	Inertial Measurement Unit	mmWave	Millimeter Wave
NOMA	Non-Orthogonal Multiple Access	MIMO	multiple-input multiple-output
AVISPA	Automated Validation of Internet Security Protocols and Applications	IoD	Internet of Drones

List of Abbreviations and Symbols

Abbreviation	**Description**	**Abbreviation**	**Description**
AES	Advanced Encryption Standard	ARM	Advanced RISC Machine
AVR	Advanced Virtual RISC	SENTINEL	A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles
TCALAS	Temporal Credential-Based Anonymous Lightweight Authentication Scheme	SDN	Software Defined Networking
PARTH	PUF based Authentication for Remote Hovering Devices	LinHAE	Linearly homomorphic authenticated encryption
BPV	Boyko-Peinado-Venkatesan	RAMP	Robust Authentication key management protocol
FL	Federated Learning	PoS	Proof-of-Stake
ICN	Information-centric networking	MEC	Mobile Edge Computing
GNSS	Global Navigation Satel- lite System	PBFT	Practical Byzantine Fault Tolerance
DDG	Data Delivery and Gathering	IDS	Intrusion Detection System
SVM	Support Vector Machine	PCA	Principal Component Analysis
MAVIDS	Micro Aerial Vehicle IDS	DDoS	Distributed Denial of Service
CSV	Comma Separated Value	DROP	Drone open-source parser
ESCALB	An effective slave controller allocation-based load balancing	PRM	Probabilistic Roadmap
DDRRT	Dynamic Domain RRT	RNN	Recurrent Neural Network
Q	Rational number	PUF	Physical Unclonable Function
CRPs	Challenge-response pairings	SPDL	Security Protocol Description Language
DY	Dolev and Yao	CK	CanettiKrawczyk
AVISPA	Automated Validation of Internet Security Protocols and Applications	Proverif	Protocol Verifier

List of Abbreviations and Symbols

Symbol	**Description**	**Symbol**	**Description**
ID_{EU}	EU original identity	$PASS_{EU}$	EU original password
PRK_{GCS}	GCS private key	PBK_{GCS}	GCS public key
PRK_{UAV}	UAV private key	D	Divisor of Genus-2 curve
ID_{UAV}	UAV original identity	OID_{UAV}	UAV obfuscation identity
$h(.)$	Hash operation	$\|\|$	Concatenation operation
$\oplus$	XOR operation	TS_1, TS_2, TS_3, $TS_4, T_a, T_b, T_c, T_d, T_e, T_f$	Timestamps
TS_{pr}	Present timestamp	ΔT	Message receive threshold time
RT_1, RT_2, RT_3, η, λ	Random tokens	MSG_1, MSG_2, MSG_3	Messages among entities
K_{EU}, K_{GCS}	Secret key of EU and GCS	$SK_{EU->UAV/UAV->EU}$	Shared session key
Y_{EU}^S	Secret variable comprises message digest of confidential ID, password and random number	OID_{EU}^S	UAV obfuscation identity during authentication stage
AUT_N/AUT_N*	Secret values to check whether authentication among EU and UAV is valid or not	(CH_{UAV}, RES_{UAV})	Challenge-Response pair of PUF at UAV
BT_{EU}	Biometric Traits of external user	hd	Helper data to get biometric secret key
γ_{EU}	Biometric secret key	τ	Threshold time for message reception
R_1, R_2, $R_a \dots R_d$	Arbitrary numbers	α	Random number
AL_{UAV}	Identity Alias of UAV	SK_{EO}	Session key of EO

Chapter 1

INTRODUCTION

1.1 Internet of Things based Unmanned Aerial Networks (IoT-based UAV Networks)

Drones, also known as unmanned aerial vehicles or UAVs, were initially created for military use. A drone is a flying object that has remote control independence and self-piloting capabilities. Among the various applications of drones are disaster rescue, battlefield communication, photography, aerial delivery and device-to-device communication. The essential elements of drones are batteries, propellers and motors, flight controller, IMU and magnetometer. There are various type of drones such as quadrotor, multirotor drones, fixed wing UAV, fixed wing hybrid UAV. The drones are dynamic and fast, so maintaining communication reliability is essential which can be achieved through the Mavlink protocol by bridging the gap between UAV and GCS (Ground Control Station).

IoT-based UAV networks are the networks of EU (External User), GCS, and interconnected UAV nodes with the power of the Internet and equipped with embedded sensors and flight-controller. In these networks, UAVs collect data and send it to a GCS. The GCS then sends out commands to control and watch over the drones through wireless connections. IoT-based UAV networks are ubiquitously deployed across diverse sectors, with notable prominence in civil and military spheres. UAVs play crucial roles in studying the earths structure, spraying crops, surveillance and monitoring during natural disasters.

Despite the merits, there are some significant concerns regarding security breaches in smart city environments as external users like traffic management authorities and emergency vehicles such as firefighters and ambulances need sensitive data from UAVs through GCS over the public channel, which can be captured by the adversary to perform replay, man-in-the-middle, session key attacks. Moreover, the UAVs can be captured by adversaries to tamper with the credentials stored in UAV storage. The IoT-based UAV Networks have several other challenges, such as high computation, communication and storage overheads. Therefore, securing communication and resource constrained challenges in these networks is the focus for industries, academicians and researchers.

1.2 Internet of Things

The Internet of Things (IoT) refers to the network of physical objects embedded with sensors, software, and other technologies, with the aim of connecting and exchanging data with other devices and systems over the internet [1]. These “things” vary from ordinary domestic items to sophisticated industrial tools, each outfitted with the capability to communicate and interact with other connected devices. The core concept behind IoT is to introduce a higher level of intelligence and automation to our daily lives by leveraging data collected from the physical world [2]. IoT network is made of three separate components such as person to person, person to things/objects and things/objects to things/objects over the Internet connectivity. IoT spans a wide array of domains, such as smart cities, healthcare, industries, agriculture, and connected vehicles, as shown in Figure 1.1. The smart city is an infrastructure that utilizes cutting-edge technology to facilitate efficient data management, resulting in improved citizen satisfaction, increased economic growth, and a more sustainable environment [1].

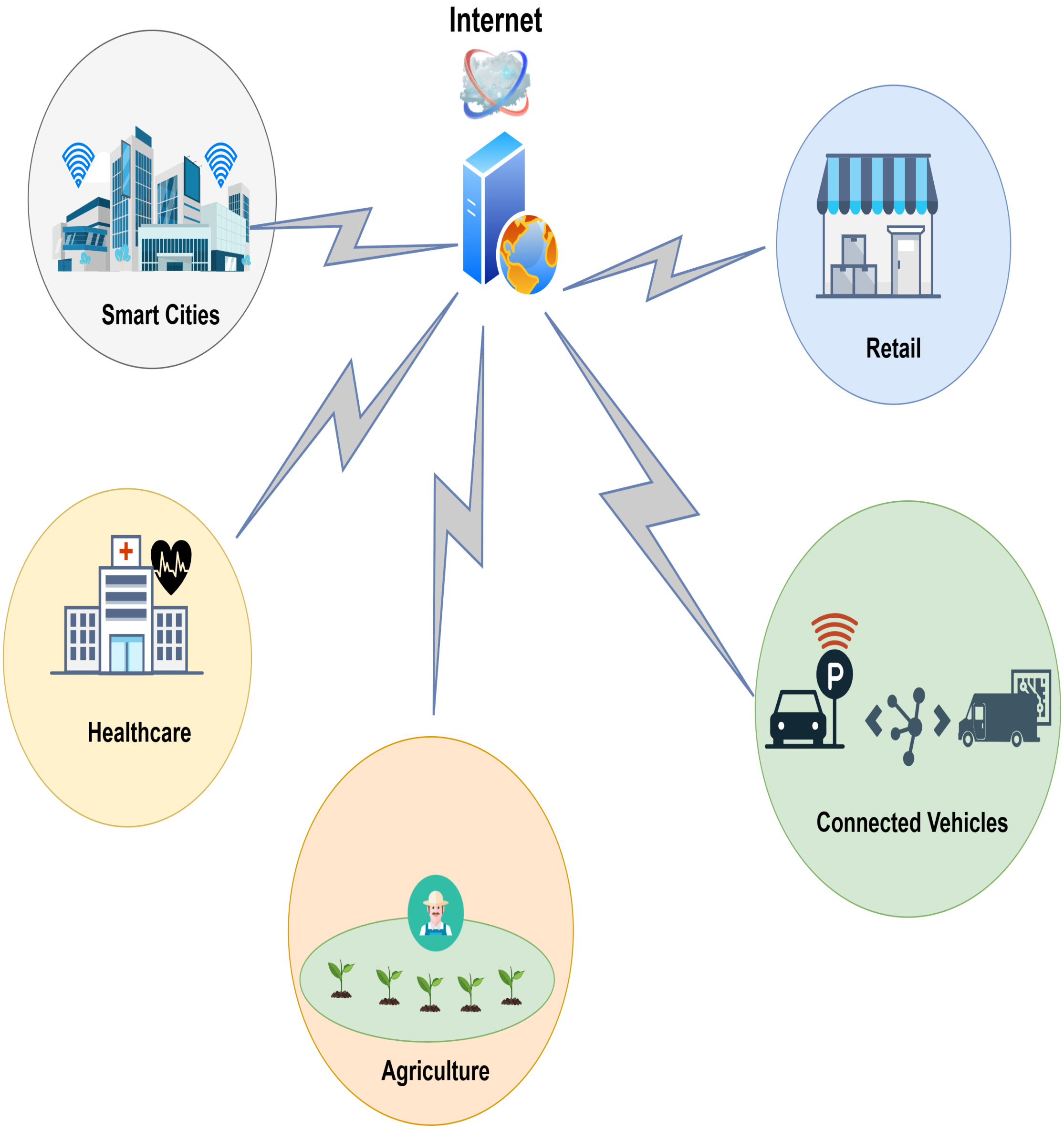


Figure 1.1: Domains of IoT

1.3 IoT-based Unmanned Aerial Vehicles System

1.3.1 UAV

UAV is an unmanned aircraft or vehicle which can be operated autonomously as well as independently. UAVs are famous for their role in reconnaissance and rescue and battlefield. The UAVs network covers various domains like wireless hotspot services, smart cities, remote sensing, agriculture, etc. The UAV and its components are presented in Figure 1.2:

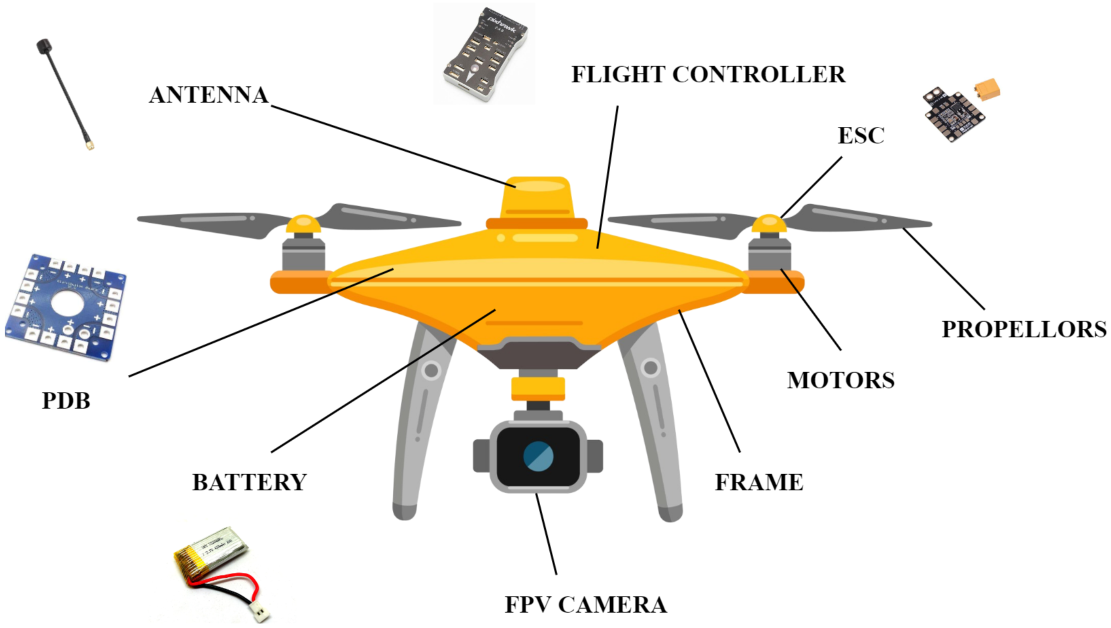


Figure 1.2: UAV

The main components of UAVs are:

- **Frame**: Frame is the skeleton of a UAV, which is made from lightweight but strong materials like carbon fibre or aluminium to keep it durable with a capacity of carrying motors, propellers, etc.

- **Motors**: Motors is a power component that produces the thrust necessary for propelling UAVs.

- **Electronic Speed Controllers**: An Electronic Speed Controller (ESC) is a vital component in a UAV that manages the speed, direction, and braking of the drone motors. It is an interface between the flight controller and the motors, converting electrical information into accurate motor motions.

- **Flight Controller**: The flight controller (FC) functions as the "brain" of the drone. It's a small computer that handles everything, from stabilizing the UAV to performing intricate flying patterns. It accepts input from the pilot or a pre-programmed plan and changes the motors and other components to ensure the drone performs as intended.

- **Power Distribution Board**: A Power Distribution Board (PDB) is an essential element of UAVs that regulates the allocation of electrical power from the battery to many onboard systems. It guarantees that the motors, ESCs, FC, and other ancillary equipment get the requisite voltage and current.

- **Radio Receiver**: A radio receiver in a UAV receives signals from the remote controller and relays them to the flight controller. It enables the operator to direct the drone's motions and functionalities. It operates on specified frequency bands, ensuring steady communication and accurate control.

- **Battery** : The battery of a UAV powers the motors, flight controller, and other components. Because of its lightweight design and great energy density, lithium-polymer (LiPo) batteries are used in the majority of drones. The battery capacity influences the drone's flying length and performance, with bigger batteries providing longer durations but adding weight.

- **Propellers**: Propellers in a UAV generate thrust by spinning rapidly and pushing air downward, creating lift. Their size, shape, and number affect the drone's stability, speed, and maneuverability. Proper matching with the motors ensures efficient flight performance and energy use.

- **FPV Camera**: An FPV (First-Person View) camera takes real-time video from the drones viewpoint, enabling the operator to see what the drone sees. It is often used for racing and aerial photography, offering a live feed of the surroundings. The camera delivers the video signal to goggles or a screen for immersive control.

- **Video Transmitter**: A video transmitter (VT) provides the real-time video feed from the FPV camera to the receiver or goggles. It transforms the camera's visual signal into a radio frequency signal for wireless transmission. The transmitter's power and frequency impact the range and quality of the video stream

- **Antenna**: An antenna sends and receives radio signals that enable communication between the UAV and its controller or video receiver. It is critical in maintaining a reliable link for control instructions and video feeds. The antenna's design and direction affect the signal's range and power.

1.3.2 IoT-based UAV Networks Model

In this framework, GCS is the trustworthy registration authority for drones and users. A UAV collects data from its surroundings in a specified airspace. The IoT-based UAV Networks System Model includes EU, a trustworthy entity GCS, and UAVs as presented in Figure 1.3 and mentioned below:

- **External User:** The external user holds the smartphone device and obtains the confidential credentials during the registration stage. The secure session key is established between the EU and UAVs, ensuring mutual authentication.

- **Ground Control Station:** The Ground Control Station is the recognised entity which maintains the communication between UAVs and external users and allows only registered users and UAVs in the network.

- **Unmanned Aerial Vehicle:** Unmanned Aerial Vehicle gets its confidential data from GCS after registration. These vehicles collect the required data via sensors for smart cities and transfer it to authorised GCS and EU.

- **Control Channels:** From a technical standpoint, there is a wide range of communication technologies that can be employed to regulate a UAV. The essential requirement is transmitting data from the RC to the UAV and vice versa, which can be accomplished through various types of electromagnetic radiation.
  - **Infrared:** In households, Infrared (IR) technology is commonly used for TV and peripheral device remote controls, mainly because it is simple and inexpensive. However, its use for controlling Unmanned Aerial Vehicles (UAVs) is greatly limited due to the technology's physical constraints. The transmitter (light source) and the receiver (light detector) must have a line of sight, and any obstruction between them can cause reception issues. Utilizing Infrared light-based remote controls for UAVs can be difficult, given that they are usually operated at distances exceeding 10 meters from the remote control, and it is not always possible to avoid obstacles that may come between the remote control and the UAV. Additionally, IR communication can be affected by environmental factors such as rain and sunlight, further limiting its practical use in a typical outdoor Unmanned Aircraft System (UAS) setting.
  - **Radiowaves:** Radiowaves are a type of electromagnetic radiation that has a longer wavelength than Infrared light. They are classified into various frequency bands based on their wavelength characteristics, and their usage is regulated by the National Telecommunications and Information Administration in the United States and the European Committee of the Regions in Europe. Table [3] displays the IEEE-defined frequency bands and Specific frequency bands, which are prohibited for use due to regulatory restrictions, and certain frequencies are assigned solely to private entities through licensing. However, there are unlicensed frequency ranges that can be utilized to control Unmanned Aerial Vehicles (UAVs). The authors have provided an overview of the various frequency bands utilized in the European Union and their applications.
  - **Bluetooth and WiFi :** UAVs are commonly operated through standardized technologies like WiFi or Bluetooth that function on unregulated frequencies. These technologies are typically employed to link a personal computer with drones to program the UAV's flight computer in advance. These technologies have a limited range due to their wavelength, making them suitable for controlling UAVs with restricted ranges, particularly Micro/Mini UAVs. The cost-effective method is advantageous because it allows customers to use their smartphones remotely, eliminating the need for additional RC.

1.4 Types of UAVs

UAVs are categorized based on the functional area of wings, weight, altitude and range:

1.4.1 According to Wings :

The different UAVs lies under this category are following [4]:

- **Fixed wing:** This is a small version of aircraft without a pilot having fixed wings that need a runway to fly and land. They have long range and endurance. fixed

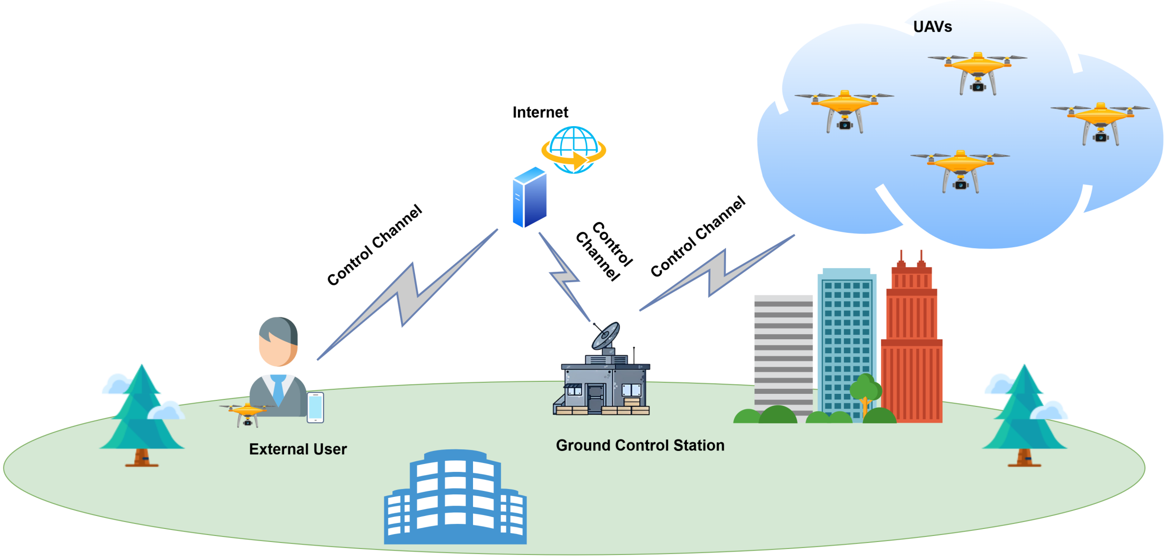


Figure 1.3: IoT-based UAVs Network model

wings to generate lift, enabling efficient and long-duration flights. These UAVs are often employed for purposes such as aerial surveillance, mapping, and environmental monitoring because to their capacity to cover enormous regions. Unlike rotary-wing drones, fixed-wing UAVs need a runway or catapult for takeoff and landing. Their aerodynamic efficiency makes them excellent for applications demanding prolonged flying periods and greater speeds.

- **Rotatory wing:** The rotatory wing craft can be single as well as multirotor or vertical takeoff and landing (VTOL) UAVs. This type of wing has high maneuverability. It is easy to take off with precise control. This UAV employs revolving blades to provide lift, enabling vertical takeoff, landing, and hovering capabilities. Unlike fixed-wing UAVs, they can fly in limited locations and do not need a runway. Their adaptability makes them a popular option for both commercial and military purposes.

- **Hybrid wing:** Hybrid-wing Unmanned Aerial Vehicles integrate characteristics from both fixed-wing and rotary-wing designs, providing a balance of efficiency and adaptability. These UAVs generally employ rotary mechanics for VTOL before transitioning to fixed-wing flight for greater range and endurance. This design is suited for applications that need agility in limited locations as well as long-distance mobility. Hybrid-wing UAVs are rapidly being utilized for mapping, surveillance, and logistics because of their agility and operational flexibility.

The category of UAVs based on wings is shown in Figure 1.4 :

1.4.2 According to Weight

The various UAVs in this category are mentioned below: [5]:

- **Nano:** Nano UAVs are very miniature UAVs, often weighing around 250 grams, suitable for operations in limited or indoor areas.

- **Micro:** Micro Air Vehicles (MAVs) are a kind of micro drone intended for low-altitude, close-in support missions with a weight greater than 250 g and less than 2 Kg. These UAVs are often tiny enough to be carried by one person, with some measuring as little as 5 cm. Their small size and agility make them suitable for tasks like surveillance, reconnaissance, and environmental monitoring, particularly in areas where bigger UAVs cannot operate efficiently.

- **Small:** Small UAVs are aircrafts weighing between 2 and 25 kilograms and intended for a variety of professional applications. They are widely used for aerial photography, surveying, precision agriculture, and environmental monitoring. These UAVs establish a balance between portability and capability, allowing for longer flight times and modest cargo capacities. Their versatility makes them suitable for a variety of industries, including construction, media, and public safety.

- **Medium:** Medium UAVs weigh between 25 and 150 kilograms and are intended for missions with increased range, endurance, and payload capacity. They are commonly utilized in fields such as border monitoring, disaster relief, and scientific study. Medium UAVs may carry modern sensors, cameras, and technology, making them appropriate for civilian and military tasks. When compared to smaller UAVs, their expanded capabilities enable for more efficient observation of greater regions.

- **Large:** Large UAVs generally weigh above 150 kg and are built for long-duration, high-performance missions. These UAVs are commonly utilized for military, commercial, and industrial purposes, such as freight delivery, surveillance, and environmental monitoring. Their increased size enables them to carry bigger payloads, like improved sensors, cameras, or even supplies for isolated places. With longer flight periods and wider ranges, big UAVs are suited for activities that demand great endurance and high operating capacity.

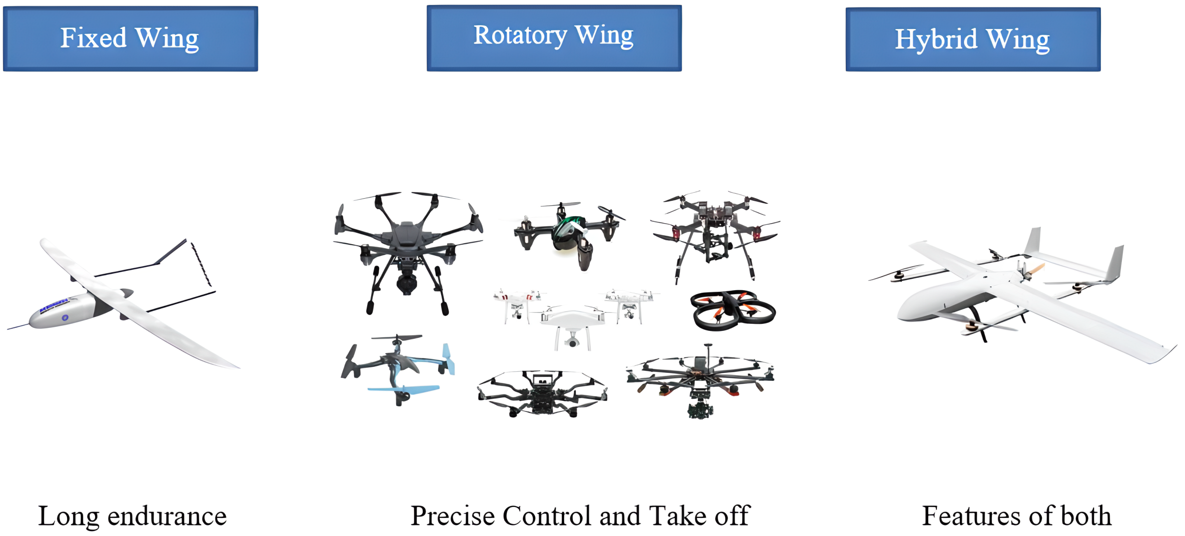


Figure 1.4: Aircraft based on wings

1.4.3 According to Altitude

This category comprises the following types of UAVs [4]:

- **High altitude platform(HAP):** High Altitude Platform (HAP) UAVs are meant to operate in the stratosphere, at altitudes ranging from 20 to 50 kilometres above the Earth's surface. This operating range enables HAP UAVs to offer continuous surveillance, communication relays, and environmental monitoring over large regions, effectively linking the terrestrial and satellite systems. Their capacity to stay aloft for lengthy periods makes them useful for both civilian and military uses.

- **Low altitude platform(LAP):** Low Altitude Platform (LAP) UAVs are intended to operate at altitudes up to 10 kilometres (about 33,000 feet). These UAVs are outfitted with powerful sensors and navigation systems, allowing them to undertake activities such as atmospheric research, surveillance, and environmental monitoring. VTOL aircraft belong to this category.

1.4.4 According to Range

: The UAVs included in this category are as follows [4] :

- **Close Range:** Close-range UAVs are intended to operate over short distances, usually up to 10 km. These UAVs are often utilized for duties such as surveillance, reconnaissance, and environmental monitoring in limited or urban environments. Their tiny size and agility make them perfect for applications that need precision control and real-time data collecting.

- **NATO:** NATO has progressively incorporated Unmanned Aerial Systems (UAS) into its operations to increase surveillance, reconnaissance, and information-collecting capabilities. The alliance has created a strategic concept for the deployment of UAS, offering key direction for their usage across multiple combat activities with a range of up to 50 km.

- **Tactical:** Tactical UAVs are intended for short-range operations and often operate within line-of-sight distances. These UAVs are used for surveillance, reconnaissance, and target acquisition, delivering real-time information to ground forces. Their small size and agility make them suitable for usage in limited or urban environments, providing precise control and real-time data transfer with a range of up to 50 km.

- **Medium Altitude Long Endurance (MALE):** Medium Altitude Long Endurance (MALE) UAVs are intended to operate at 200 km. These unmanned aerial vehicles are generally used for surveillance, reconnaissance, intelligence collecting, and target monitoring over wide regions, providing real-time data to assist military and civilian activities.

- **High Altitude Long Endurance(HALE):** High Altitude Long Endurance (HALE) UAVs are intended to operate unlimited range. for lengthy periods of time, frequently more than 24 hours. These UAVs are generally used for surveillance, reconnaissance, and communication relay missions, which provide continuous coverage over large regions.

- **Hypersonic:** Hypersonic UAVs are unmanned aerial vehicles that operate with a range of more than 200 km, allowing them to traverse long distances swiftly. These UAVs use sophisticated propulsion systems, such as scramjets, to maintain high speeds. They are mainly utilized for fast reconnaissance, surveillance, and striking operations, with unparalleled speed and agility .

1.5 FANET

FANET (Flying Adhoc Network) is the subset of MANET where the UAV nodes are connecting in an ad-hoc manner. Every UAV operates at a higher speed in comparison with MANET or VANET and Underwater ad-hoc networks. Each UAV consists of physical devices such as sensors, GPS, and a flight controller. FANETs are utilized in defense organizations or military and civilian applications because of their dynamic nature, self-operatable, self-configured, etc. Figure 1.5 presents the FANET architecture.

1.5.1 Commmunication in FANET

In a FANET, UAVs can communicate by exchanging data among themselves without any infrastructure and can be coordinated with GCS (Global Positioning System). There are four types of communication [6].

- **A2A (Air to Air Communication):** In A2A communication, one UAV can exchange data with another UAV and act as a relay node to extend the connectivity range.
- **A2G (Air to Ground Communication):** In this type of communication, one UAV can exchange essential data with the ground control station. The Ground

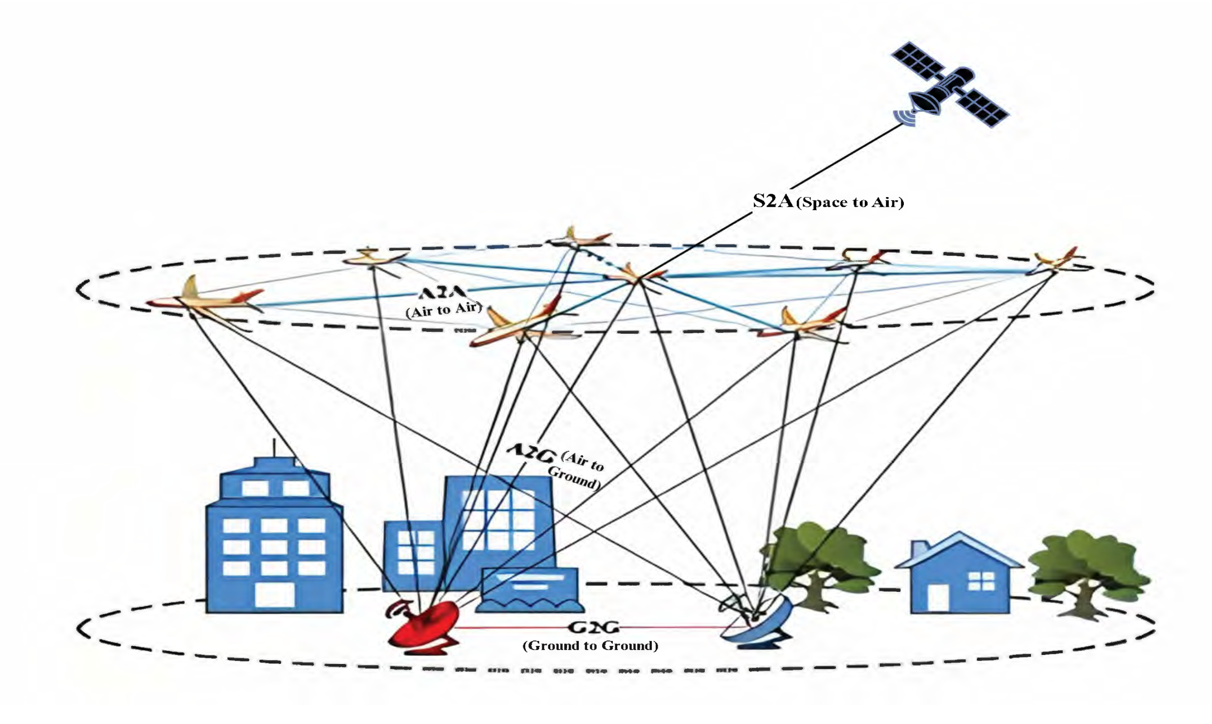


Figure 1.5: FANET Architecture

control station can send control commands to the UAVs to perform a specific task.

- **S2A (Space/Satellite to Air Communication):** Space-to-Air (S2A) communication is the exchange of data between a UAV and satellites or space-based technologies. This sort of communication may be used in a variety of UAV tasks, including navigation, control, data transfer, and remote sensing.

- **Hybrid communication:** This kind of communication is the integration of the above three communications, i.e. S2A, A2A, and A2G, which is required for higher coverage and data rate.

1.5.2 Features of FANET

The are many features of FANET, which are the following [6]:

- **Cost:** The cost of small UAVs in FANET is low because of their lower operating expenditure.

- **Survivability:** Multi UAVs in FANET are survivable in the case of one UAV node failure in a mission.

- **Speedup:** UAVs in FANET can accomplish the mission at a faster rate due to more in number.

- **Scalability:** The multi-UAVs network is scalable as more UAVs can participate in FANET, and thus coverage area in the mission can be expanded.

- **Reliability:** Due to bad atmospheric conditions, the A2G communication is adversely affected and in that case, the A2A condition can resolve the connectivity issues to ensure network reliability.

1.5.3 Communication Protocols in FANET

Communication protocols in FANETs are essential for facilitating reliable and efficient data sharing among UAVs inside dynamic, decentralized networks. These protocols tackle distinct issues, including high mobility, frequent topological changes, and constrained resources, by facilitating seamless coordination and connection. The various protocols based on two layers are following :

1.5.3.1 Based on Physical Layer:

- **FANET communication characterization:** Propagation model based on radio waves of FANET node-to-node links are identical to the 2-ray ground schema.

- **Channel modelling** The 2-state Markov model based on Rician fading is used to make the channel infrastructure-less among UAVs.

- **Nakagami-based FANET radio propagation model:** In this model, the Nakagami-m fading channel was derived, and a mathematical theorem evolved as output for link disconnection.

- **General link outage model:** In this model, the FANET node-to-node and UAV node-to-ground link disconnection over the defined fading channel was provided with the formula.
- **Many transmitters and receivers:** The packet transfer rate was improved in many receivers and transmitters for a longer time.

1.5.3.2 Based on Network Layer/Routing Protocols:

- **Proactive type:** For a limited time, routing information is modified and kept in a 2D format such as DOLSR, in which the directed antenna concept is used so as to reduce latency and enhance packet delivery ratio.
- **Reactive type:** In this type of protocol, routing information is modified and kept only when the point or device finds a change in the network, such as on-demand routing based on a time slot, which is used to eliminate collisions.
- **Hybrid Protocols:**In this type, the functionality of two protocols reactive and proactive is joined together to achieve routing, for example, zone routing protocols.
- **Geographic type:** It predicts the movement of UAVs with the GaussMarkov mobility model and uses this information to determine the next hop.
- **Position-based protocol:** This protocol determines the position of the particular UAV in the network. They are divided into two strategies: single path and multipath.
- **Swarm-based protocol:** This protocol is based on the behaviour of animals.

1.6 Security Attacks

Multiple security vulnerabilities can exploit UAV communications. Two kinds of attacks are possible as follows.

1.6.1 Physical Attacks

Physical attacks provide significant risks to both individual drones and the entire network architecture. The attacks may include direct physical harm to drones, including shooting them down or seizing them to retrieve important information or manipulate hardware elements. Furthermore, opponents may use jamming devices to interfere with communication signals, resulting in loss of control or crashes. Hijacking incidents, in which unauthorized individuals take control of a drone's navigation system, represent a significant threat, possibly diverting drones for malicious objectives. These attacks will be further discussed in Chapter 2.

1.6.2 Logical Attacks

Logical attacks aim to target the software and communication protocols of drone systems. A common concern is the Man-in-the-Middle (MITM) assault, in which attackers intercept and perhaps modify communications between drones and control stations, resulting in illegal data access or command manipulation. A notable concern is the Denial of Service (DoS) attack, which inundates a drone's communication channels or processing capacity, resulting in unresponsiveness or system failures. Additionally, spoofing attacks entail altering data or signals to trick drones into accepting wrong information, possibly leading to misnavigation or unlawful actions. These logical assaults exploit flaws in the IoT-based UAVs communication and software infrastructure, presenting serious concerns about the security and dependability of drone operations. These attacks will be further discussed in Chapter 2.

1.7 Security Objectives of IoT-based UAV Networks

Security objectives of IoT-based UAV Networks are essential for guaranteeing safe, dependable, and trustworthy drone operations across linked networks. These goals include safeguarding sensitive data, preserving system integrity, and thwarting unwanted access or control of drones.

1.7.1 Mutual authentication

Mutual authentication in these networks guarantees that both the users and UAVs validate each other's identities before communicating. This prohibits unauthorized organizations from taking control of drones or obtaining important information. Mutual authentication requires strong cryptographic techniques to prevent impersonation and man-in-the-middle attacks. It is crucial for ensuring safe operations in UAV networks, particularly in sensitive applications such as surveillance logistics and traffic monitoring in smart cities.

1.7.2 Privacy Protection

Privacy protection in UAV networks protects sensitive data, such as flight routes, surveillance videos, and personal information, against unwanted access or use. Robust encryption, access restrictions, and anonymization measures prevent data breaches and illegal drone monitoring. This protection is critical for preserving user confidence and adhering to privacy requirements in applications such as delivery, monitoring, and surveillance. Effective privacy safeguards also reduce the danger of disclosing essential information in sensitive circumstances.

1.7.3 Untraceability

Untraceability in IoT-based UAV networks assures that UAV identities, locations, and activities are not traced or observed by unauthorized organizations. It is accomplished by using methods like encryption, anonymization, and dynamic routing to obscure communication and operating information. This is especially crucial in sensitive applications such as military operations and private surveillance to prevent enemies from obtaining information. Untraceability improves operational security by preventing unwanted tracking or hostile intervention.

1.7.4 Anonymity

Anonymity guarantees that the identities of drones, operators, or users remain hidden throughout communication or activities. It is accomplished via methods such as pseudonymization, encrypted transmission, and identity masking. This prevents illegal identification and safeguards sensitive data in privacy-critical and security-sensitive drone applications.

1.7.5 Session Key Establishment

It guarantees that the cryptographic key used for safe communication between drones and control systems stays secret. Robust encryption techniques, secure key exchange protocols like Diffie-Hellman, and key management systems are employed to safeguard the session key from eavesdropping or leaking. This stops unauthorized actors from decrypting conversations or obtaining access to sensitive data. Maintaining the secrecy of the session key is crucial for ensuring the integrity and security of UAV activities.

1.7.6 Safeguarding Against Recognized Attacks

It ensures the system is resilient against typical cyber threats such as eavesdropping, man-in-the-middle (MITM) attacks, replay attacks, and denial-of-service (DoS) attacks. This uses secure communication protocols, real-time intrusion detection systems, and robust encryption standards. Regular upgrades and vulnerability assessments are crucial to tackling emerging threat vectors. Ensuring resilience to known assaults strengthens the overall security and dependability of UAV networks, preserving critical activities and data.

1.8 Applications of IoT-based UAV Networks

The IoT-based UAV Networks have revolutionized how drones are utilized across various industries, transforming traditional processes with their interconnected capabilities. By enabling real-time communication, data sharing, and automation, IoT-based UAV networks open up diverse applications that improve efficiency, reduce costs, and enhance decision-making. From precision agriculture to military operations, UAVs integrate advanced technologies like IoT to address complex challenges. Its versatility and scalability make it an essential tool for innovation in today's rapidly evolving world.

- **Agriculture:** Agriculture benefits from real-time monitoring and data collecting on the UAV network to enhance agricultural techniques. IoT-based UAV networks help with precision farming by monitoring crop health, soil conditions, and water levels, resulting in more effective resource usage. They can carry out automated duties like crop spraying and pest management with little human interaction. This technology increases production, lowers expenses, and encourages sustainable agriculture practices.

- **Smart cities:** IoT-based UAV network improves urban infrastructure and public services by collecting and monitoring data in real time. UAVs help with traffic control, environmental monitoring, and infrastructure inspections, increasing efficiency and sustainability. They also play an important role in emergency response, giving immediate situational awareness during disasters. IoT-based UAV network integration promotes the creation of safer, more connected, and environmentally responsible urban areas.

- **Environmental monitoring:** This network requires UAV to gather real-time data on air quality, water pollution, and deforestation. UAVs equipped with modern sensors can follow animals, identify forest fires in their early stages, and monitor environmental changes in distant regions. UAV systems provide seamless data exchange for analysis and decision-making in order to solve environmental problems. This technology improves sustainability by allowing for proactive and accurate environmental control.

- **Healthcare:** Healthcare applications use drones to improve access and reaction times. UAVs effectively transport important medical supplies, such as vaccinations, blood, and organs, to distant or disaster-affected regions. They also help in crises by getting Automated External Defibrillators (AEDs) and first-aid supplies to patients quicker than conventional means. This technology makes healthcare more accessible, saves lives, and lowers logistical problems.

- **Disaster management:** IoT-based UAVs deliver real-time aerial data for quick reaction and decision-making. UAVs outfitted with cameras and sensors analyze damage, find trapped people, and distribute emergency supplies to remote locations. They help to map catastrophe zones, which allows for more effective resource allocation and rescue operations. UAVs network increases the speed and efficacy of disaster relief activities, lowering hazards and saving lives.

- **Delivery and logistics:** The UAVs network transforms delivery and logistics by allowing quick, efficient, and seamless transfer of products. Drone networks provide last-mile delivery by transporting goods, medical supplies, or food straight to clients. They use real-time data to improve delivery routes, resulting in reduced delays and operating expenses. IoD improves logistical efficiency, especially in urban and distant regions, resulting in fast and dependable service.

- **Military and defense applications:** UAV networks include the use of drones for reconnaissance, surveillance, and tactical support. IoT-enabled UAVs give real-time intelligence in dangerous environments, reducing crew risk. They may also carry out targeted attacks, border patrol, and continuous surveillance of critical locations. This integration improves situation awareness, operational efficiency, and national security.

- **Infrastructure inspection:** IoT-based UAV network advances infrastructure inspection by allowing drones to evaluate and monitor essential assets such as bridges, electricity lines, pipelines, and buildings. Drones, outfitted with high-resolution cameras and sensors, gather real-time data to detect possible damages or risks while ensuring human safety is not compromised. These systems provide expedited, precise, and economical examinations, particularly in inaccessible or dangerous locations. This improves the efficacy and dependability of maintenance and infrastructure management.

1.9 Hyperelliptic Curve Cryptography

Hyperelliptic Curve Cryptography (HCC) is a public-key cryptography framework based on the mathematical principles of hyperelliptic curves, which serve as extensions of elliptic curves [7]. HCC is especially useful in lightweight or resource-constrained contexts owing to its ability to give high levels of security with reduced key sizes compared to classic cryptographic techniques like RSA or ECC (Elliptic Curve Cryptography).

1.9.1 HCC's key features and strength

HCC's key features and strengths are the following:

- **Compact key sizes**. Hyperelliptic curves provide the same degree of security as standard cryptosystems (RSA or ECC) but with much lower key sizes. For example: A 60-bit HCC key offers the same level of security as a 160-bit ECC key or a 1024-bit RSA key. This reduces memory use and processing needs.

- **Low Computational Overhead:** HCC is appropriate for resource-constrained devices, such as IoT sensors and mobile devices, due to its low computational overhead and speedier encryption, decryption, and signature verification with reduced key sizes.

- **Enhanced Security:** The HECDLP is more complicated and difficult to solve than other cryptosystems, resulting in higher cryptographic strength even with lower parameters.

- **Storage Efficient:** HCC is ideal for devices with limited storage overhead because of its low computational and communication requirements. This makes it especially useful in storage-sensitive systems like wireless sensor networks (WSNs).

1.9.2 Comparison of HCC with ECC and RSA

Hyperelliptic Curve Cryptography (HCC) provides a considerable benefit over RSA and ECC by delivering the same degree of security with lower key sizes, making it very efficient for resource-constrained applications as mentioned in Table 1.1. While ECC also provides tiny key sizes, HCC beats it in terms of energy economy and computational simplicity. RSA, yet extensively used, lags behind because of its huge key sizes and considerable computational cost, restricting its usefulness for lightweight applications.

1.10 Applications of HCC

The various applications of HCC are outlined below:

- **Wireless sensor networks:** HCC finds substantial uses in Wireless sensor networks (WSNs), where resource efficiency is crucial. In these networks, HCC enables secure communication between sensor nodes while reducing computational overhead and energy usage. The lightweight operations of HCC assist increase the battery life of sensors and allow large-scale deployment, making it perfect for environmental monitoring, industrial automation, and smart cities.

Table 1.1: Comparison of HCC, ECC, and RSA

Features	**HCC**	**ECC**	**RSA**
Key Size	Smallest	Small	Largest
Security Basis	HECDLP	ECDLP	Integer Factorization Problem
Computational Overhead	Low	Moderate	High
Energy Efficiency	High	Moderate	Low
Memory/Bandwidth Use	Low	Low	High
Best Use Cases	IoT, WSNs, lightweight systems	General-purpose cryptography	Traditional cryptography

- **Internet of Things:** HCC solves security concerns caused by billions of networked devices. It enables secure device authentication, encrypted data transfer, and safe firmware upgrades, ensuring user privacy and preventing unwanted control. IoT devices, typically resource-constrained, benefit from the lower key sizes and decreased computing needs of HCC, making it a trustworthy option for applications in healthcare, smart homes, and autonomous systems.

- **Digital signatures and authentication:** HCC plays a vital role in digital signatures and authentication, giving compact and safe techniques for confirming the integrity and validity of data. Lightweight HCC-based digital signature techniques are especially beneficial in blockchain systems, providing rapid transaction validation and smart contract security. These qualities make HCC a powerful tool for financial systems, e-commerce, and decentralized applications.

1.11 Motivation

Despite the obvious advantages of UAV networks, their implementation is constrained by security concerns. In 2011, Unmanned aerial vehicle security was raised when Iranian troops captured an American RQ-170 [8]. The risk of enemies initiating network assaults exists whenever UAV networks are used for tasks like combat communication and scouting in dangerous circumstances. During the Russia-Ukraine war in 2022 [9], the army of Ukraine formed small teams to physically attack Russian drones with the help of laser weapons. The author [10] explains how attackers can take advantage of tampering with the communication between UAVs and their remote counterparts, rendering them vulnerable. With recent perusal, it is clear that IoT-based UAV Communication is not secured. UAVs with sensitive information on military missions can be compromised. As far as security is concerned, high-end missions like military applications, viz. reconnaissance, search and rescue, and power line inspection, require more safety, and existing studies provide us with brief assessments or surveys restricted to only a few security attacks or counter-measures. Since no systematic study in the field of IoT-based UAV Networks was released, so this is a recent study. Moreover, the communication between the EU, UAVs, and GCS is vulnerable to security threats such as eavesdropping, replay attacks and location and physical capture attacks. This motivated us to carry out this study to fulfil the gaps and design secure mutual authentication schemes for security needs in the high-end application of UAVs.

1.12 Research Gaps

This section highlights the research gaps found in the available literature.

1. **RG1-** The current research work does not consider a systematic survey for physical, logical attacks and their countermeasures in IoT-based UAV Networks with taxonomy [4, 6, 11].

2. **RG2-** Existing studies of UAV security, privacy, and communication designs have mostly focused on cryptographic techniques, which are computationally expensive strategies [11–16].

3. **RG3-** The research work does not consider formal security analysis for security vulnerabilities. [17, 18]

4. **RG4-** There is a lack of study on modern cryptographic techniques [4, 6].

5. **RG5-** Do not balance security with efficiency regarding communication, storage, and computational costs [12–16].

1.13 Research Objectives

The objective of the thesis is to identify lightweight and robust authentication mechanisms for secure communication in IoT-based UAV networks. This objective can be achieved on several levels as follows:

1. **RO1-** To conduct a systematic literature survey on secure communication in IoT-based UAV Networks.

2. **RO2-** To design a mutual authentication scheme for IoT-based UAV Networks.

3. **RO3-** To design a secure cryptosystem for secure data transmission by considering major attacks in IoT-based UAV Networks.

1.14 Contributions

The main contributions towards this thesis have been summarized in the following subsections.

1. **Secure Communication in IOT-based UAV Networks: A Systematic Survey**
   This work analyses how the secure communication method shifts from classical cryptography to lightweight cryptography, elliptic curve cryptography, blockchain, and quantum cryptography between UAVs by systematically answering the research questions mentioned based on the previous six years existing surveys along with existing attacks, such as physical and logical attacks. This survey also discusses the current research issues and future directions for researchers to work on.

2. **G2CAIUN: A Novel Genus-2 Curve-based Authentication for Secure Data Transmission in IoT-based UAV Networks**
   The novel G2CAIUN mutual authentication scheme is designed which is based on the Genus-2 Curve for IoT-based UAV networks. The proposed work provides separate session keys for each session between EU and UAVs through distinct timestamps and enigmatic identities. This work provides PUF primitive to protect UAVs from physical capture attacks in each communication environment, such as EU-GCS-UAV, UAV-GCS and UAV-UAV. This work employs a Genus-2 hyperelliptic curve point multiplication with a reduced key size of 80-bit, providing a similar level of robust security as an elliptic curve of genus-1 with a half-field size. Currently, no such subexponential fast algorithm exists for the Genus-2 curve to solve discrete logarithmic problems, which motivates us to design a robust and lightweight mutual authentication scheme.

3. **HCFAIUN: A Novel Hyperelliptic Curve and Fuzzy Extractor-based Authentication for Secure Data Transmission in IoT-based UAV Networks**

   We have developed a novel lightweight and safe authentication method called Hyperelliptic Curve and Fuzzy Extractor-based authentication in IoT-based UAV networks (HCFAIUN) employing HC, XOR operations and SHA-1 (Secure Hash Algorithm) hash functions. The maximum key size for HCC is 80 bits, as opposed to the elliptic curves need of 160 bits, making it suitable for UAVs with limited resources. This protocol supports the mutual authentication of users and UAVs by allowing them to share a session key for safe interactions and prevent malicious activity of exposing sensitive data by generating biometric traits through FE. The proposed protocol adopts HC scalar multiplication to protect the private key from well-known assaults and identity obfuscation to keep the external user, GCS, and UAVs anonymous. This work excludes the requirement of Physical Unclonable Functions (PUF), which are hardware modules for physical UAV attack prevention because the private key of a UAV is securely stored using a hash function, obfuscation identity, timestamp and random numbers, which prevent attackers from predicting session key between EU and UAVs. HCFAIUN scheme generates separate sessions by creating a unique obfuscation identity of EU and UAVs.

4. **A Secure Cryptosystem for Secure Data Transmission in IoT-based UAV Networks**

   We proposed a secure cryptosystem for secure data transmission in IoT-based UAV Networks, which employs the hyperelliptic curve of genus greater than one, providing better performance in terms of computation, communication, and storage costs. The cryptosystem secures the users private key while transmitting sensitive information using a hyperelliptic curve discrete logarithmic problem (HCDLP). It achieves security features such as anonymity, untraceability, forward secrecy and others using a secure hash function, random number and separate timestamps to prevent physical and logical attacks, which are analysed using formal verification Scyther tool and informal method. The proposed cryptosystem performance is compared with benchmark schemes, and the result shows lower computation, communication and storage costs with no trade-off between security and performance.

1.15 Outline of the Thesis

The organization of this thesis is as follows.

Chapter 1 provides a thorough review of IoT-based UAV network systems along with security issues and motivation behind using modern cryptography concepts such as Hyperelliptic Curve Cryptography for secure communication among this network.

Chapter 2 offers a systematic study of recent attacks, different security vulnerabilities and their solutions by covering the previous six years' papers (2017-2022) and provides the preliminaries of authentication schemes.

Chapter 3 presents a novel Genus-2 curve-based authentication for secure data transmission in IoT-based UAV Networks along with UAV-UAV and UAV-GCS authentication. This work provides analyses of protocol with the DY-threat model and CK-adversary model.

Chapter 4 discusses the novel hyperelliptic curve and fuzzy extractor-based authentication in IoT-based UAV networks (HCFAIUN) for secure data transmission with formal and informal security validation.

Chapter 5 A secure cryptosystem based on the hyperelliptic curve for secure data transmission in IoT-based UAV Networks is presented with a comparative analysis among benchmark schemes.

Chapter 6 summarizes the thesis by highlighting the contributions, and it also discusses some future research directions and social impact.

Chapter 2

LITERATURE REVIEW AND PRELIMINARIES

2.1 Introduction

This chapter presents a literature review on secure communication in IoT-based UAV Networks by providing a research methodology and comparison with an existing survey using parameters like novel hierarchy, attacks, secure communication methodologies, etc., in a tabular layout. This chapter gives the recent countermeasures such as lightweight cryptography, elliptic curve cryptography, blockchain, and quantum cryptography to address the formulated research queries. The outline of each recent secure communication methodology covers its pros and cons through a tabular format. It also covers open research problems related to malware detection and future guidelines for the researchers, like advancement in quantum cryptography techniques, chaotic cryptology, Software-defined networking, etc. We also present the Hyper-elliptic curve cryptography-based preliminaries at the end of this chapter.

2.2 Research Aim and Research Questions

This segment furnishes details regarding the research aim & queries through a thorough review of Unmanned Aerial Systems attacks and solutions. The Research aims and questions are defined as:

2.2.1 Research Aim:

To study the security vulnerabilities and solutions in communication in IOT-based UAV networks to raise awareness among researchers and the general community.

2.2.2 Research Questions:

Research Questions to meet our objectives are as follows:

- **RQ1** *What are the various security vulnerabilities or attacks through which communication in IoT-based UAV networks is compromised?*
  To answer this question, the most recent research articles are analyzed in section 2.3 to figure out various security breaches in UAV networks.

- **RQ2** *What is the cutting-edge status in terms of high-end UAV security?*
  The preliminary study and analysis of recent UAV attacks in section 2.3.3 responds

to the query. Consequently, it is necessary to carefully observe the recent assaults and research findings and assess their relevance to this study.

- **RQ3** *What makes this survey different from the existing survey?*
  To answer this question, the analogy is mentioned with the existing study based on parameters defined in the tabular layout, and section 2.4 will address this query.

- **RQ4** *What are the current defense strategies available for ensuring secure communication in IoT-based UAV networks?*
  The research question is answered based on previous research question one(**RQ1**) about security vulnerabilities. section 2.6 discusses the related work based on recent defense strategies and provides a comparison table with existing research.

2.3 Preliminary study of attacks on UAV

This section discusses the related studies about security vulnerabilities and explains query RQ1. Multiple security vulnerabilities can exploit UAV communications. Two kinds of attacks are possible as follows.

2.3.1 Physical Attacks

The control of a UAV can be taken by another drone called an interceptor drone. A UAV's task could be jeopardized if it collides with moving or immovable objects, as well as with other aircraft. An idea proposed is to equip the second unmanned aerial vehicle with a spear, which could be used to aim at the intrusive UAV. Alternatively, a mesh could be thrown over it [19], or a wire could be released into its propellers [20] to pull it away and eliminate the threat. Other types of physical attacks are directed energy weapons like lasers and microwaves[9]. The physical attack demonstration is shown in Figure 2.1.

2.3.2 Logical Attacks

As UAVs are unmanned vehicles so they are operated using commands forward by the GCS to control flight speed and altitude etc. The various type of logical attacks is discussed below:

- **GPS Jamming :** A jamming attempt stops a receiver from picking up the real GPS signals. This can be done by transmitting higher-powered interference signals in the same frequency band [8].

- **Meaconing :** Meaconing is the practice of recording real GPS signals and relaying them to the receiver with an additional delay [8].

- **Spoofing Attack :** In this kind of attack, the attacker sends a signal that is malicious and more powerful than the real signal, tricking the receiver into using the fake signal. It is a more destructive attack as UAV control can be taken by adversaries. Interestingly, US RQ 170 Sentinel was captured by Iranian forces after a recent security attack against UAVs [8].

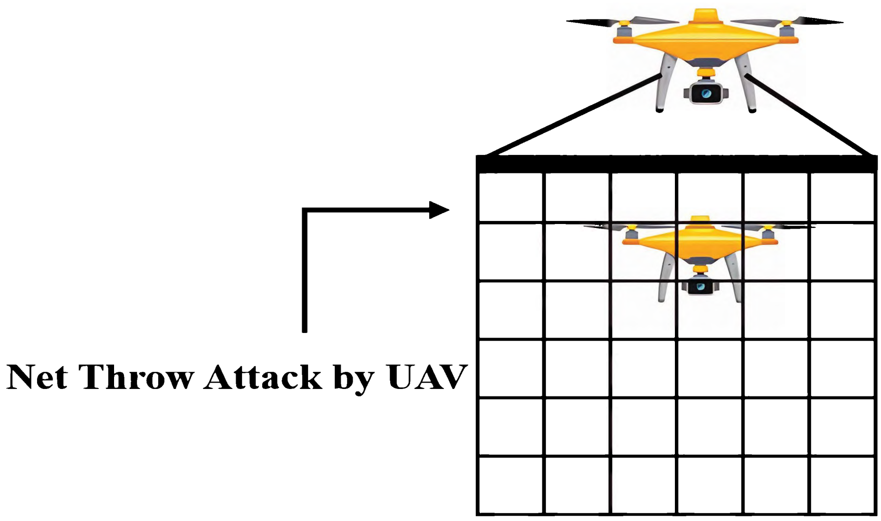


Figure 2.1: Physical attack

- **Eavesdropping :** The adversary can directly access the exchanged UAV data in the open environment due to the absence of encryption and other security measures [21].
- **Code injection attack :** It is an active attack in which the adversary injects fake information and instructions by masquerading as a legitimate entity [22].
- **Virus :** A virus is a passive attack and self-replicate program which spread from computer to computer. In [23], a virus known as a keylogger has infected a group of U.S. military drones stationed at an Air Force base in Nevada, enabling it to monitor every key and button pressed by their pilots.
- **Man in the Middle attack :**This is a type of active attack in which the communication link between the multi-UAV system is intervened and a malicious drone acquires the control by modifying and dropping the content [21].
- **Replay attack :** The malicious UAV can pose as a valid sender after a surveillance attempt and transfer the encrypted data to another UAV. In [24], the replay attack was performed on the E010 drone by acquiring four channels with 20 MHZ bandwidth radio signal and by replaying it through HackRF hardware.
- **De-authentication attack :** In this kind of attack, the adversary sends the deauthentication frames to interrupt the target UAV connection. In [8] the Aircracking was used to de-authenticate or disconnect a genuine client and gain control over the system.
- **Denial of Services (DoS) attack :** In this type of attack, the adversary makes the UAV network unavailable. The adversary obstructs the UAV network by flooding it with data [8]. The types of DoS attacks are the following:
  - **Black Hole Attack:** In this type of denial-of-service attack obtains vicious UAV packets but does not transfer them to the target UAV and discards them [25].

  - **Grey Hole Attack:** It is the type of DoS attack that obtains vicious UAV packets and chooses the packets and transfers the chosen packets to the target UAV or neighboring UAV and obliterates the rest of the packets [25].

Some other types of attacks:

- **Wormhole attack** In this type of attack, the adversary makes a tunnel with the help of one or more malicious nodes and then they use tunnels to forward packets to other networks [21].

- **Sinkhole attack** In this kind of attack the adversary tries to gather network traffic by broadcasting on the fake path with altering routing information[25].

- **Sybil attack:** When a malevolent unmanned aerial vehicle infiltrates an existing network, it generates a digital resemblance. such I1,I2,I3 [21].

The logical attack demonstration is shown in Figure 2.2. The hierarchy of attacks is shown in Figure 2.3 and a related study of attacks is shown in Table 2.1 with Yes and No values Yes means Attack is discussed in respective work and No means Attack is not discussed.

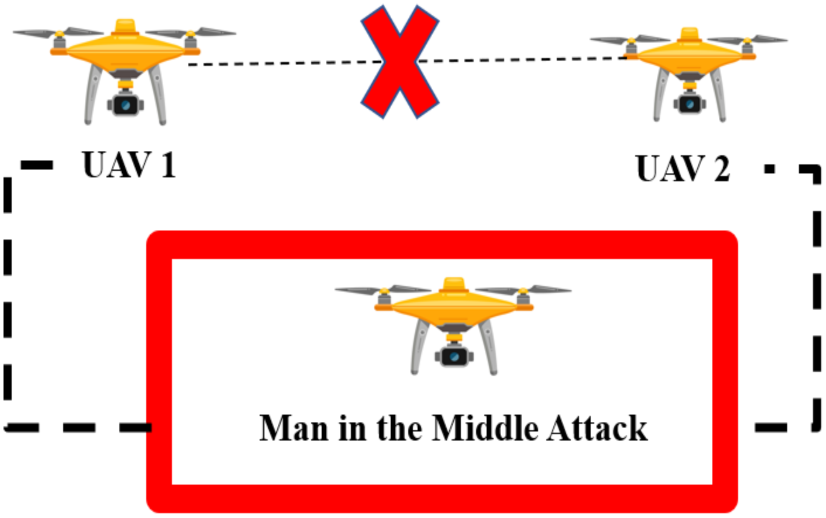


Figure 2.2: Logical attack

2.3.3 Recent drone attacks

This section elucidates the current state of the art regarding high security and addresses Query RQ2.

- **SkyJack:** SkyJack takes advantage of an open WiFi communication channel that exists between the Parrot AR drone 2, which controls the UAV, and the smart phone. An attacker may introduce de-authentication packets into the system and cut off the authorized operator from the UAV [29].

- **ProtoX:** A ProtoX is a small quadcopter drone that could be reversed engineered with equipment like a logical analyzer and development board. To control the small

Table 2.1: Type of attacks

Sno.	Type of attacks discussed	[8]	[26]	[27]	[25]	[28]	[10]	[21]	[22]	This survey
1	GPS Jamming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	GPS Spoofing	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes
3	Meaconing	Yes	No	No	No	No	No	No	No	Yes
4	Eavesdropping	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5	Injection Attack	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
6	Virus	No	No	No	No	No	No	No	Yes	Yes
7	Active Eavesdropping	No	No	No	No	No	Yes	Yes	Yes	Yes
8	Replay Attack	Yes	No	Yes	No	No	No	Yes	Yes	Yes
9	De-authentication attack	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes
10	Black Hole	No	No	No	Yes	Yes	No	Yes	Yes	Yes
11	Grey Hole	No	No	No	Yes	No	No	Yes	No	Yes
12	Worm Hole	No	No	No	No	No	No	No	Yes	Yes
13	Sink Hole	No	No	No	Yes	No	No	No	No	Yes
14	Sybil Attack	No	No	No	No	No	No	Yes	Yes	Yes

quadcopter, the adversary removes the microcontroller of the remote control with joysticks and connects it to the output pins of a development board. This allows them to write program scripts to transmit control signals to the quadcopter. Thus, reverse engineering can be possible [29].

- **MalDrone:** A drone can be compromised if malware is installed on the device in case the communication channel is not encrypted. One restriction is that the malware can be installed on Parrot AR.2 Drone. The malware can attack the flight controller, and it allows the attacker to connect back to control[29].

- **War Flying:** By attaching wireless communication devices to the UAVs, which allows the adversary to spy on objects or targets. Bluetooth, WiFi, and GSM (IMSI Catcher) are used for privacy invasion[30].

- **WiFi and Bluetooth Cracking:** In 1997, WiFi was introduced, and it utilized a cryptographic protocol known as WEP(Wired Equivalent Privacy). However, this had certain limitations in terms of security and was susceptible to attacks. To address these issues, a new encryption standard called WiFi Protected Access 2 (WPA2) was developed, which provides a high level of security. Nonetheless, depending on certain conditions, this standard can still be compromised [8]. Bluetooth technology is often used for exchanging data between aircraft, micro UAVs, and remote controls. However, this technology can be susceptible to various security attacks [31], including the newer Bluetooth Low-Energy (BLE) standard.

2.4 Related Work

This section presents the related studies on secure communication in IoT-based networks. There are fewer publications in this field but this paper tries to cover the most relevant paper of the last six years with the comparison table as shown in Table 2.2 and address the query RQ3.

He et al. (2017) [11] have discussed secure communication techniques, i.e., hierarchical identity-based broadcast encryption and pseudonym technique, but have not covered each attack and their countermeasures. Moreover, According to the abstract, the author has mentioned that there is no usage of a third-party central server, but the methodology has mentioned the usage of a third-party Remote Management Server (RMS). As per the computational assumption, the author has implemented his scheme in bilinear groups, which is hard to break, but the cost of implementing the bilinear groups is high, which is not feasible to implement. The Performance analysis was also performed in which less number of figures and tables were used for better understanding. The category of UAVs is also missing in this paper. A preliminary study of UAVs is also missing in this paper. The proposed scheme in this paper has not gone through formal security analysis approaches like AVISPA, ProVerif, etc.

Sedjelmaci and Senouci (2018) [32] have provided cyber attack countermeasures using machine learning algorithms like Neural networks, but due to power-constrained UAV, the execution of complex operations is difficult. The authors have also spoken about cyber-attacks, i.e. active and passive attacks such as modification and Denial of service attacks. Further, the author has described the detection schemes like rule-based specification and Bio-inspired detection schemes. The author has presented only one security frame architecture which is based on an intrusion detection system. The author has not described any lightweight encryption and cutting-edge countermeasures for IoT-based UAV networks. The author has not mentioned what type of security analysis has been done for the verification of the proposed framework.

Riahi Manesh and Kaabouch (2019) [33] described the scenario of attacks on GPS, ADS-B(Automatic Dependent Surveillance-Broadcast) system and GCS only without any focus on the security of sensors data. The author has not provided any privacy-preserving authentication scheme, which is present in our paper. The logical attacks and their taxonomy, like data interception, data manipulation, and DoS attacks, cannot discuss physical attacks[19]. The author has covered cryptographic-based defense methods like some lightweight cryptography methods but does not cover all kinds of the latest encryption techniques like ECC(Elliptic curve cryptography), which is a form of public-key cryptography that utilizes the mathematical properties of elliptic curves over finite fields to ensure security. ECC offers the advantage of using smaller keys compared to other forms of cryptography while still maintaining an equivalent level of security. Moreover, the author has not provided any efficient detection mechanism for the intrusion but our paper has provided a different intrusion detection mechanism. There are a lot of cutting-edge technologies which need to be mentioned by the author and which are covered in this paper.

Yaacoub et al. (2020) [34] focused on the vulnerabilities of UAVs belonging to specific domains such as military, civilian, and terrorism. Still, the authors failed to describe the physical and logical attack hierarchy and the specific frequency range and wavelength for different bands. Also, the discussed defense strategies for secure communications in IoT-based UAV networks are limited, i.e., IDS and some of the encryption schemes like traceable and privacy-preserving authentication. The author does not describe many limitations, such as lightweight authentication schemes and the latest encryption strategies for resource-constrained IoT-based UAVs.The author of this paper has not categorized the secure communication methodologies based on authentication and encryption strategies for a clear understanding, which is covered by our paper.

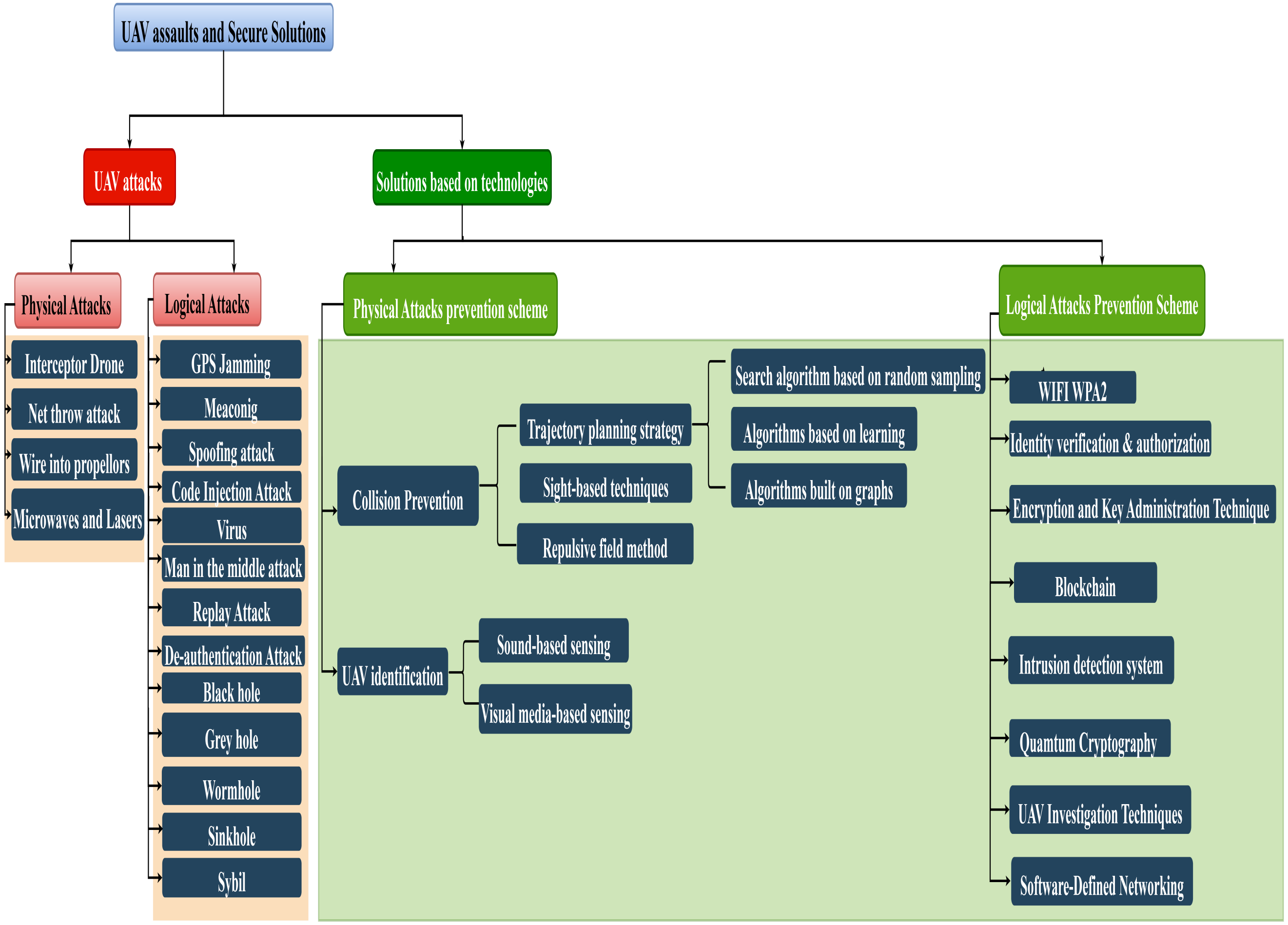

UAV assaults and Secure Solutions
UAV attacks
Solutions based on technologies
Physical Attacks
Logical Attacks
Physical Attacks prevention scheme
Logical Attacks Prevention Scheme
Interceptor Drone
Net throw attack
Wire into propellors
Microwaves and Lasers
GPS Jamming
Meaconig
Spoofing attack
Code Injection Attack
Virus
Man in the middle attack
Replay Attack
De-authentication Attack
Black hole
Grey hole
Wormhole
Sinkhole
Sybil
Collision Prevention
Trajectory planning strategy
Sight-based techniques
Repulsive field method
Search algorithm based on random sampling
Algorithms based on learning
Algorithms built on graphs
UAV identification
Sound-based sensing
Visual media-based sensing
WIFI WPA2
Identity verification & authorization
Encryption and Key Administration Technique
Blockchain
Intrusion detection system
Quamtum Cryptography
UAV Investigation Techniques
Software-Defined Networking

Figure 2.3: Hierarchy of UAV attacks and Solutions

Chamola et al. (2021) [4] have described the usage of UAVs in civilian, military, and industry with a detailed description of UAVs and their types. The paper covers the recent scenario about UAV attacks, like attacks based on terrorist activities such as the Abqaiq- khurais attack, the Caracas drone attack, and military attacks, but fails to explain the taxonomy of all existing threats in IoT-based UAV networks. The paper provides the preliminary of wireless communication but has not given any frequency range and wavelength description. The recent attacks case studies were provided by the author but there was no discussion about existing state of art countermeasures and future directions provided by the authors.

Pandey et al. (2022) [22] have described the comprehensive survey on security vulnerabilities and provided a descriptive taxonomy of security threats. There is no discussion about the preliminary of UAVs, their types, and wireless communication which does not give ground understanding to the researchers and first-time readers. The author has talked about the various security vulnerabilities related to physical attacks only but has not covered logical attacks. The author has focused only on physical security and cellular communication technologies like mmWave, NOMA, massive MIMO, etc. The authors have covered some recent drone attacks but not covered war flying and Bluetooth and WiFi-related attacks. Similarly, the author has covered only the last four years' papers, but this paper has covered the last six years' papers. The authors have discussed the mitigation technique for physical attacks [19] like collision, i.e. trajectory planning, but have not discussed any trajectory planning strategy like algorithms based on random sampling, graph and learning, which is covered in this paper. The author has not provided solutions with lightweight authentication techniques as well as quantum-based cryptography, which is mentioned in this paper. The taxonomy of all threats is not picturized in one place in previous work. The AI-based Intrusion detection system & lightweight authentication schemes are presented in this paper, which was not covered in previous work done by the author.

2.5 Research Methodology

This section covers the search strategies and their criteria to systematically carry out the study. The systematic literature review's objective is to assess, look into, and synthesize all of the existing research on this topic. To give a response to the formulated research question, we follow the guidelines of Kitchenham and Charters[35]. The number of steps required to conduct a systematic literature survey are: (1) Identify the research question (2) Determine the Database (3) Locate Keyword (4) Inclusion and Exclusion Criteria (5) Search Results and research gaps. The flow chart of a systematic literature survey is shown in Figure 2.4, and the survey methodology is shown in Table 2.3.

2.5.1 Identify the research questions.

In this section, the key concerns and difficulties in the IoT-based UAV network security sector are noted, such as attacks and vulnerabilities with recent assaults in UAV networks, communication technologies, and existing surveys. Also, the state of art defense strategies. The Research aims and questions are presented in Section 2.2.

Table 2.2: Related work

Reference	Year	Hierarchy	Physical attacks	Logical attacks	Security Assessment	Secure communication methodology	Current research issues and Future Scope	Description
[11]	2017	×	×	∂	✓	⋆	×	proposed only one methodology based on identity-based encryption
[32]	2018	×	×	∂	✓	⋆	×	proposed security framework to protect an aircraft with a short review
[33]	2019	✓	×	∂	×	∂	✓	covers few logical attacks defense strategies
[34]	2020	✓	✓	✓	×	∂	✓	covers few prevention scheme based on IDS only
[4]	2021	✓	✓	∂	×	×	×	describes only current perspective of security of UAVs
[22]	2022	✓	×	∂	∂	∂	✓	covers few security threats and defense techniques
This survey	2023	✓	✓	✓	✓	✓	✓	This survey covers major security assaults and their defense strategies

✓- Mentioned × - not mentioned ∂ - partial information ⋆ - limited to one

2.5.2 Determine the database

In this section, several internet databases, including IEEE Xplore(https://ieeexplore.ieee.org/Xplore/home.jsp), Springer(https://www.springer.com), MDPI(https://www.mdpi.com), Wiley Online Library(https://onlinelibrary.wiley.com), Engineering Village(https://www.engineeringvillage.com), and Google Scholar(https://scholar.google.com) may be used to find published academic research papers and journals.

2.5.3 Locate keyword

In this section, Keywords used to locate the interested paper/article are "UAV security", "Secure communication in UAV", "security threats and countermeasures in UAV", "Encryption and Key management schemes", "authentication schemes or framework in UAV", "Blockchain in drones security", "Intrusion Detection System Scheme in drones security", "Quantum cryptography in secure communication of UAV", "UAV Forensics" An example of one of the expert search queries is :((((UAV security OR Secure communication in UAV OR security threats and countermeasures in uav) WN ALL)) AND ((2022 OR 2021 OR 2020 OR 2019 OR 2018 OR 2017) WN YR)) where WN stands for "within".

2.5.4 Inclusion and Exclusion Criteria

Papers must be written in English. Papers are limited to the duration between 2017-2022. This paper is based on security threats and their prevention schemes. This work considers journal papers, transaction papers, and conference papers based on secure UAV communication, including a comprehensive survey on security attacks and solutions, whereas this work does not include white papers, low-quality papers, non-English papers, and articles with similar content and short reviews. We applied the inclusion and exclusion criteria on the title and abstract screening, and at last whole text has gone through screening.

2.5.5 Search Results and Research Gaps

This section denotes the filtered six papers from the previous six years based on inclusion and exclusion criteria, and the comparative analysis with gaps is presented in Table 2.2 based on the following parameters:

1. **Hierarchy:** Hierarchy classifies and organizes the data into different categories. Some of the filtered papers were found with the hierarchy of attacks and countermeasures. Hierarchy provides a clear view of the research topic to the researchers for better acquisition of knowledge.

2. **Physical Attacks:** The IoT-based UAV networks are vulnerable to physical attacks such as net throw attacks, and Only a few papers were found with these kinds of attacks.

3. **Logical Attacks:**The IoT-based UAV networks are also vulnerable to logical attacks such as Jamming and wormhole attacks, and Most of the papers with partial information are found for logical attacks.

4. **Security Assessment:** Security analysis is required for the proposed method or scheme, whether the scheme prevents attacks or not. Few papers were found with formal and informal security analysis such as AVISPA(Automated Validation of Internet Security Protocols and Applications), ProVerif, etc.

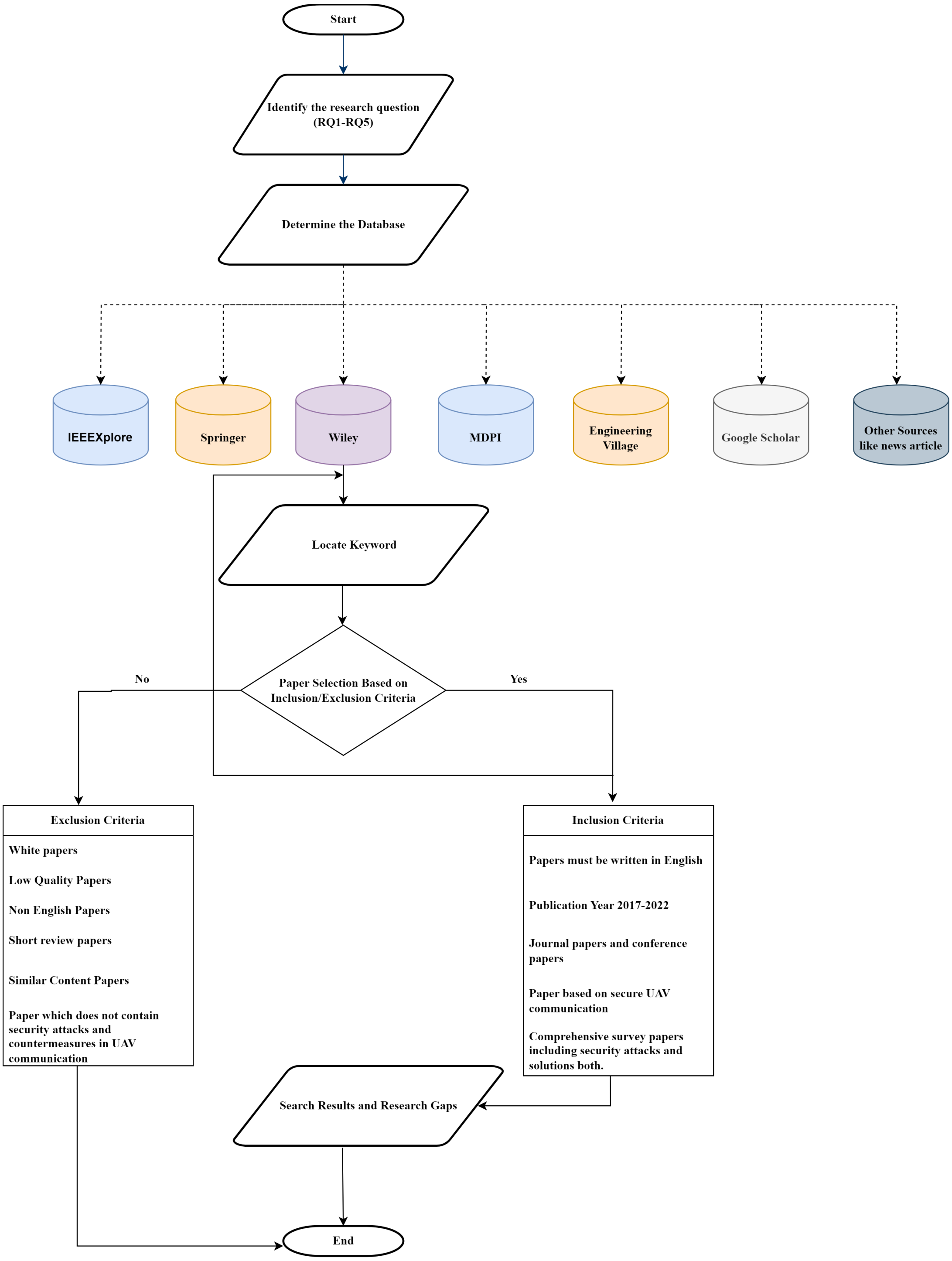

Start
Identify the research question (RQ1-RQ5)
Determine the Database
IEEEXplore
Springer
Wiley
MDPI
Engineering Village
Google Scholar
Other Sources like news article
Locate Keyword
Paper Selection Based on Inclusion/Exclusion Criteria
No
Yes
Exclusion Criteria
White papers
Low Quality Papers
Non English Papers
Short review papers
Similar Content Papers
Paper which does not contain security attacks and countermeasures in UAV communication
Inclusion Criteria
Papers must be written in English
Publication Year 2017-2022
Journal papers and conference papers
Paper based on secure UAV communication
Comprehensive survey papers including security attacks and solutions both.
Search Results and Research Gaps
End

Figure 2.4: Systematic Literature Approach

Table 2.3: Research Methodology

Property	Category
Research Questions	• **RQ1** What are the various security vulnerabilities or attacks through which communication in IoT-based UAV networks is compromised? • **RQ2** What is the cutting-edge status in terms of high-end UAV security? • **RQ3** What makes this survey different from the existing survey? • **RQ4** What are the current defense strategies available for ensuring secure communication in IoT-based UAV networks?
Databases	• **IEEE Xplore**: `https://ieeexplore.ieee.org/Xplore/home.jsp` • **Springer**: `https://www.springer.com/` • **MDPI**: `https://www.mdpi.com/` • **Wiley Online Library**: `https://onlinelibrary.wiley.com/` • **Engineering Village**: `https://www.engineeringvillage.com/` • **Google Scholar**: `https://scholar.google.com/`
Search String	• UAV security • Secure communication in UAV • security threats and countermeasures in UAV
Inclusion Criteria	• Papers must be written in English vehicles • Publication Year 2017-2022 • Journal papers and conference papers • Paper based on secure UAV communication • Comprehensive survey papers including security attacks and solutions.
Exclusion Criteria	• White papers • Low-Quality Papers • Non-English Papers • Short review papers • Similar Content Papers • Paper which does not contain security attacks and countermeasures in UAV communication

5. **Secure Communication methodology or countermeasures :** The countermeasures were limited to one or partial information provided in the filtered papers i.e. lack of cutting edge solution.

6. **Current research issues and future scope:**Some of the papers have no information for current research issues and future directions which are essential for researchers to work upon.

2.6 Secure Communication Methodology

This section covers existing countermeasures for secure UAV communication and answers query RQ4. There are many secure communication standards for protection from attacks:

2.6.1 Logical Attacks Prevention Scheme:

2.6.1.1 WIFI WPA2:

To defend against attacks like de-authentication, GPS spoofing, and jamming attacks, WPA2 is the best encryption technique. WPA2 is 2nd generation wireless protected access protocol that is defined as a standard in IEEE 802.11i-2004. According to this standard, a key with at least 20 characters is advised. Large-size keys are hard to crack.

2.6.1.2 Encryption and key administration:

As we know, IoT-based UAV systems are vulnerable to eavesdropping and de-authentication attacks, so to mitigate these vulnerabilities, a UAV system should have cryptographic and key management techniques such as:

1. **Lightweight self-certified cryptographic system:** The technique introduced is named IoD-Crypt, which is the countermeasure for authentication and confidentiality of communication [36].

2. **Identity-based encryption:** It is the better encryption technique with no overhead of certificates to use in public key architecture. It is a selection-based encipher algorithm that selectively enciphers the content and provides a data-hiding feature for confidentiality [18].

3. **Transfer key control:** The proposed approach uses cellular-based networks for drone control and provides identity verification and key control among a drone and GCS. A functional layer key is created between a drone and the new GCS when the drone switches from one GCS to the next. The AS key is not revealed based on the study of this method [37].

4. **OTP technology:** According to the author, in the One-time pad encryption scheme, the replicated key was provided and used with the message to obtain the cypher context using the EX-OR operation before being used with the cypher text to obtain the plain text and the replicated key to destroying the duplicated keys once the message was successfully decrypted. When compared to AES128, the performance was the best [38].

5. **Protected lightweight network coding alias:** In this author developed the client-server coding technique to combine the catchphrase with the personality, which produces two keys: one for anonymization and the other for certification [39].

6. **Elliptic Curve Cryptography-Based El Gamal encryption technique:** In this technique, the optimal key is generated along with the artificial gorilla troops optimizer technique [40].

Table 2.4 represents encryption key and administration schemes.

2.6.1.3 Identity verification and authorization:

As messages are unauthenticated and their validity cannot be verified, fake signals can be injected. Deploying authentication systems that guarantee the legitimacy of only legal systems in the IoT-based UAV networks is crucial to resolving this problem.

1. **Message Authentication Code Scheme:**This type of solution uses two phases:
   (a) **Data Verification:**The cluster head node filters using the data verification step.
   (b) **Cluster watermark authentication:** At the sink node, this cluster verification phase is used to confirm the accuracy and integrity of the data. This scheme is vulnerable to 5 attacks, i.e. propagation delay, forging of packets, data altering, replay, and grey hole attack [41].
2. **Mutual Authentication model:** The scheme is generated to solve the issue of de-authentication packets in hijacked UAVs. This scheme consists of the ground station, middleware, and UAVs.The theme is to utilize encoded channels between the above-mentioned segments [42].
3. **Continuous authentication model:** In this type of scheme, the UAV flight operators behavior is authenticated by the flight commands sent from the UAV operator. By assuming that each operator has a distinct pattern of behavior, it's feasible to detect authorized operators who are attempting to take control of the UAVs [43].
4. **SENTINEL Framework:** The primary aim of the SENTINEL framework, a secure and efficient authentication system for unmanned aerial vehicles, is to establish mutual authenticity between UAVs and ground stations. To achieve this, the UAV must send a flight plan request to the ground station, which then decides whether to approve or reject it. If the request is approved, the ground station stores the UAV identity and flight session key in the flight information database, which can be accessed by all ground stations [44].
5. **TCALAS authentication:** The proposed authentication framework for IoT-based UAV networks is based on temporal credentials and enables anonymous lightweight user authentication. It provides mutual authentication between the user and the network. The framework utilizes a three-factor authentication scheme, including cellular device, biometrics, and password.[45].
6. **Secure authentication framework:** This framework proposed was based on elliptic curve cryptosystems[17].
7. **Detectable and Privacy protecting authentication:** This technique is used for drone applications comprised of the utilization of hash function, asymmetric cryptosystems [46].
8. **Identity-based Signcryption:** The authors propose a 3-factor user access control technique based on signcryption for IoT. This technique makes use of 3 authentication factors such as password, portable device, and biometrics [47].

Table 2.4: Encryption and Key Administration Techniques

Reference	Year	Name of Technique	Security Assessment	Outline
[36]	2019	Lightweight Cryptographic Framework	Analysis on 2 common UAV processors,i.e. ARM(32 bit) AVR(8 bit)	• Protected from the ability to create fraudulent messages even when the attacker has access to chosen messages • Reduces energy consumption by up to 48 times compared to conventional methods.
[18]	2018	Lightweight Cryptographic Framework	Identity-based selective encryption technique	• Future and past protection of data confidentiality. • Resistance to node hijacking. • Diminish resource usage, information camouflage procedure
[37]	2017	Transfer Key control technique	Ad hoc security encryption analysis	• single-hop key isolation. • method ensures secure storage of communication keys.
[38]	2019	One Time pad technique	A binary additive stream cipher security analysis with C++ code	• Better security level and encryption speed. • Better accuracy than DES and AES encryption algorithm
[39]	2018	Protected lightweight network coding alias	A binary additive stream cipher security analysis with C++ code	• Better security level and encryption speed.
[40]	2022	ECC- Based El-Gamal encryption	formal security analysis with a random oracle model security analysis with C++ code	• Better image encryption with optimal key generation

9. **Privacy-preserving authentication framework:** This scheme was based on mobile edge computing. The key elements involved in this scheme are credible authority, UAVs, and mobile edge computing devices. This framework provides an online and offline signature design with extremely efficient signature key generation and updation. This scheme helps in detecting replay attacks and repudiation threats [48].

10. **Covert channels-based lightweight authentication:**Under this scheme, the author utilizes the covert channels in physical layers. The various attacks like message replay and Impersonation, eavesdropping, and MITM attacks are conquered using this scheme [49].

11. **Key agreement and lightweight verification scheme:** The proposed scheme utilizes the Diffie-Hellman key exchange protocol and incorporates a symmetric key encryption algorithm to ensure message confidentiality and integrity. The authentication process between end users and UAVs is achieved through a bitwise XOR operation and a one-way hash function. Both parties mutually authenticate each other within this scheme [50].

12. **Lightweight remote user authentication with key agreement:** The author proposed this scheme when a ground user wants to gain control over the data activities from UAV directly [51].

13. **2-stage lightweight mutual authentication scheme:** The proposed scheme is designed for a multi-UAV network based on SDN. The authentication process is divided into two stages: the first stage involves the authentication between the leader drone and the ground station, while the second stage involves the authentication between the mini drone and the leader drone. The protocol, named PARTH, ensures mutual authentication, integrity, and session key security [52]

14. **Data aggregate Authentication scheme:** The proposed approach by the author suggests the utilization of ID-based encryption and elliptic curve-based technique for data aggregate authentication to achieve data security, as well as to reduce computation and communication costs. [53].

15. **Homomorphic encryption scheme:**The proposed technique by the author is called advanced linearly homomorphic authenticated encryption, which is designed to provide security against forgery and eavesdropping attacks by adversaries. Unlike other encryption techniques, LinHAE does not store the secret keys within the controller but is instead intended for use by the GCS [54].

16. **UAV-UAV and UAV-GCS security protocol based on mutual authentication:**The author proposed two secured protocols for military application [55].

    (a) **UAV-UAV security protocol:**In this protocol, secure communication among the UAVs is provided with key exchange and mutual authentication.

    (b) **UAV- GCS security protocol:**According to this protocol, secure communication is required between the UAV and the GCS. The telemetry data and status findings are exchanged securely over the link between UAV and GCS. The protocol's security analysis was conducted using both the Scyther tool and BAN logic.

17. **Secure hash algorithm/Hash message authentication scheme:**The author has proposed the authenticated scheme based on hash message authentication. This scheme provides security against various attacks such as privileged-insider attacks, DDoS attacks, Stolen verifier attacks, replay, and spoofing attacks. The storage and calculation are less overhead under this scheme [56].

18. **3-factor authentication and key agreement protocol:** The 3-factor authentication and key agreement protocol has been proposed by the author, which utilizes the Boyko-Peinado-Venkatesan (BPV) pre-calculation and FourQ. The security of this protocol is verified through detailed analysis, ensuring the protection of forward secrecy. Furthermore, experimental findings conducted on Raspberry Pi reveal that 4Q curve-based methods are between four to five times more efficient than conventional EC curve [57].

19. **Robust Authentication key management protocol (RAMP):** The RAMP protocol is based on two types of cryptography techniques: one is based on authenticated encryption primitives, and the other is EC cryptography. This protocol is validated using the Scyther tool and random oracle model. This protocol provides protection against active eavesdropping and replay attacks. The verification results prove that the RAMP protocol ensures security against various covert security attacks. This security protocol delivers a protected mechanism with less overhead of calculation and storage [16].

20. **2-factor lightweight verification scheme:** The author has suggested this strategy which is built on an asymmetric cryptographic technique. The previously proposed scheme was prone to lose access to IoT-based UAV networks because of corruption in key management systems. The proposed technique has proven to be a more secure system than other schemes. This scheme is secured against many attacks, such as phishing and replay attacks [58].

21. **ECC and symmetric encryption scheme:** The security of UAVs and users is ensured by utilizing Elliptic Curve Cryptography(ECC) and Symmetric Encryption in this scheme. This scheme provides anonymity and security against offline password guessing and various kinds of security attacks like impersonation [59].

Identity verification authorization techniques are shown in Table 2.5.

2.6.1.4 Solution based on Blockchain:

Blockchain technology is an emerging field in the era of the digital World. It applies to all domains apart from computer science, such as energy, supply chain, and healthcare. A significant advancement in distributed ledger technology is blockchain technology. Since Satoshi Nakamoto released Bitcoin, a peer-to-peer computerized cash transaction system, its reputation has been steadily rising [60]. Blockchain technology has enormous promise in other fields where reciprocal reliance between parties is necessary. In addition to allowing safe communication between autonomous swarm systems and smart financial markets, its usefulness extends beyond electronic currency exchange systems like Bitcoin, Litecoin, etc. Blockchain provides many advantages over centralized record-keeping methods, including complete data openness and faultless operation. Blockchain offers security and privacy while doing away with the need for an intermediary or third party. Blockchain technology offers a workable and highly promising answer to the security flaws in IoT-based UAV networks. [61].

Table 2.5: Identity verification and authorization

Reference	**Year**	**Name of Technique**	**Security Assessment**	**Outline**
[41]	2017	Message Authentication Code Technique	Analysis based on the watermarking scheme	• Protection against data transmission delay, packet forging selective forwarding, data replay, data tampering • Minimizes the network burden and conserves power resources. • No discussion about Brute force attack.
[42]	2017	Mutual Authentication model	Security analysis by Raspberry Pi	• solve the issue of deauthentication packets in hijacked UAVs Resistance to node hijacking. • Diminish resource usage, information camouflage procedure • Prone to replay assault.
[43]	2017	Continuous authentication model	Machine learning used to train random forest classifier	• Protection against malicious commands. • Recognize authorized users. • Prone to replay assault. • Protection of privacy is not taken into account.
[44]	2020	SENTINEL Framework technique	Analysis by Proverif tool	• Offers the ability to revoke and use pseudonyms. • Vulnerable to session key attack. • No solution of geolocation confidentiality.
[45]	2019	TCALAS authentication	Analysis conducted with the help of AVISPA tool(Automated Validation of Internet Security-sensitive Protocols and Applications)	• Unrestricted modification of password or biometric data • Protection against DoS attack. • Susceptible to spoofing assault

Table 2.5: Identity verification and authorization(Continued)

Reference	Year	Name of Technique	Security Assessment	Outline
[17]	2020	Secure authentication framework	Spontaneous security evaluation.	• Capable of withstanding sensor node takeover attack • No spoofing assaults. • No solution for geolocation confidentiality.
[46]	2020	Detectable and Privacy protecting authentication	BAN logic.	• Ensures confidentiality, integrity, and availability • Vulnerable to a session key assault.
[47]	2020	Identity-based Signcryption	Analysis done by the AVISPA tool Spontaneous security evaluation.	• Ensure prevention against sensor node capture attacks and spoofing attacks. • No solution for geolocation confidentiality.
[48]	2019	Privacy-preserving authentication framework	Security supposition.	• Identify replay assaults. • Protection against repudiation threats. • Known key attack and De synchronization attack are not discussed.
[49]	2019	ECC-Based Covert channel-based lightweight authentication	Raspberry Pi 3	• Offers adaptable networking. • Does not require traditional methods of key distribution or creation. • It does not ensure security against spoofing attacks.
[50]	2020	Key agreement and lightweight verification scheme	Ideal cipher model.	• Offers untraceable anonymity. • Protect against UAV capture attack. • No consideration of Non-repudiation.
[51]	2019	Remote user authentication with key agreement	Analysis by AVISPA tool.	• Protection against attempts to guess your password offline and unauthorized access. • No consideration for mobile edge computing devices.

Table 2.5: Identity verification and authorization(Continued)

Reference	Year	Name of Technique	Security Assessment	Outline
[52]	2020	2-stage lightweight mutual verification scheme	Mao and Boyd Logic	• Ensures the security of both physical and session keys • Spoofing attack can be possible.
[53]	2020	Data aggregate Authentication	Ideal cipher model	• Coalition attack prevention. • Provide minimum cost and computation for UAVCN. • No protection against known key attack.
[54]	2018	Data Homomorphic encryption technique	Ideal cipher model	• Protection against forgery and eavesdropping attacks. • No consideration of Non-Repudiation.
[55]	2021	Drone secure communication protocol (UAV-UAV and UAV-GCS security protocol based on mutual authentication)	Ideal cipher model	• Protection against forgery and eavesdropping attacks. • No consideration of Non-Repudiation.
[56]	2021	Hash message authentication technique	Ideal cipher model,ProVerif2 tool	• Protection against DoS, replay attack, stolen verifier attack, spoofing attack.
[57]	2021	3-factor authentication and key agreement protocol	Real-or-Random model.	• Secure against various known attacks like online and offline password attacks. • Attain user anonymity and untraceability. • No protection against spoofing attack.
[16]	2021	Robust Authentication key management protocol	Ideal cipher model, Scyther tool.	• Password estimation, Man in the middle, replay attack can be eliminated. • No protection against Known key attacks.

Table 2.5: Identity verification and authorization(Continued)

Reference	Year	Name of Technique	Security Assessment	Outline
[58]	2021	2-factor lightweight verification scheme	Ad hoc security review.	• Secured against many attacks, such as phishing and replay attacks. • No adoption of proper security analysis technique.
[59]	2021	ECC and symmetric encryption scheme	Ideal cipher model	• provides anonymity and security against offline password guessing and various kinds of security attacks like impersonation. • No protection against key known attacks.

The proposed security solutions based on blockchain by different authors are the following:

1. **Neural blockchain-based Ultra reliable caching scheme:** For edge-enabled Drone networks, In [62] neural-blockchain combo was suggested. Distributed ledgers are used for trustworthy communication on the blockchain network, which can help consolidate services on the IoT-based UAV network. A hybrid neural model is suggested to keep the blockchain network's reliability criteria. The drone caching system uses the blocks to set up the operational drones in the specified network.

2. **Delivery coin-based blockchain delivery framework:** The author proposed a Delivery coin framework based on blockchain and an intrusion detection system. The blockchain uses hash functions and short signatures to achieve anonymity protection, and the identification of intrusions is done using machine learning techniques. The pBFTF protocol is a UAV-assisted forwarding technique used to achieve an accord within the blockchain-based delivery network [63].

3. **Blockchain-based Federate learning in UAVs:**The authors of [22] have examined nano UAV-edge computing for decentralization administration and safety, driven by the advantages of FL and blockchain. They have talked about basic technological structures, issues, and issues like the scalability of blockchain-assisted apps, energy economy, and transaction capacity.

4. **Key management for IoT-based UAVs using blockchain:**The authors of [64] have proposed a distributed blockchain-aided scheme for safe key management in UAV-assisted apps with a focus on the heterogeneous IoT-based UAV network. The system allows UAVs to travel between clusters on their own, spread cluster keys, and update key pairs while thwarting malicious UAVs both inside and outside the system.

5. **Blockchain-Enabled-Data Gathering Method in IoT-based UAV network:**The author [65] suggested using blockchain technology to acquire info. Blockchain technology and drone groups are proposed as data-gathering strategies to offer safety as well as accuracy. To keep contact before starting data collection, the IoT devices and the autonomous aerial vehicle swarm specifically share a common key. Hash filters and electronic signatures are used to fight and thwart man-in-the-middle attacks that aim to manipulate and eavesdrop on users.

6. **Blockchain-based UAV system:**The author [66] proposed a system that uses both drones and blockchain technology for the industry. Inventory data is collected using drones, while smart contracts are enabled through the implementation of blockchain technology.

7. **Secure data propagation technique based on blockchain:**The author [67] developed a secure data distribution system for the IoT-based UAV network that utilizes game theory and blockchain technology. The system ensures the safe transmission of data by leveraging the security features of blockchain technology and the strategic decision-making principles of game theory. Blocks are verified and validated using the Proof-of-Stake (PoS) method and a forger node selection technique.

8. **Secure blockchain-based access control technique:**The author [68] outlined a secure communication system for UAVs and ground station computers, which is based on blockchain technology. This system utilizes transactions created from sensitive data gathered by GCS for block creation, which are combined with the blockchain via the ripple protocol consensus method. A Cloud-based machine communicates with GCS to facilitate this process.

9. **Blockchain-Based and ICN-Based UAS Ad Hoc Network Security** The author put forth a sophisticated and methodical approach that makes use of blockchain technology to effectively spot harmful material. This method combines interest key-content binding, on-demand authentication, and a transmitting technique. The authors created a flexible and extensible distributed consensus approach over specified network data for unmanned aerial vehicle ad hoc networks that are essential for critical operations to enable dispersed concern key-content attaching preservation to detect internal assailants [69].

10. **Smart City UAV-Based Blockchain-Based Environmental Health Tracking Program:**The authors proposed a safe method for tracking health in outdoor environments that integrates blockchain technology, Mobile Edge Computing, and drones. Under this proposed system, users' devices collect their health data, which are then transmitted to a Mobile Edge Computing server by a UAV. The health information is safeguarded from cyberattacks before being sent to the MEC [70].

11. **Agent-based security inspired by blockchain:**To ensure the monitoring and security of UAV networks and to identify corrupted UAVs, The author developed a multi-agent approach built on trust rules and blockchain technology [71].

12. **Spoofing Detection in IoT-based UAVs using Blockchain:**Blockchain technology was employed by the author [72] to identify GNSS(Global Navigation Satellite System) signal assaults on IoT-based UAVs.

13. **Security infrastructure for UAV-aided wildlife monitoring based on blockchain:**The author [73] established a testbed using a public blockchain for tracking animals with the assistance of drones. The drones employ IoT devices that are linked to the animals to collect relevant data, which is transmitted to the ground control station (GCS) associated with each flying zone. The Practical Byzantine Fault Tolerance (PBFT) consensus mechanism is used by the Ground Control Station (GCS) to create and validate blocks. This consensus mechanism includes transmitting the block from the GCS to the point-to-point network of GCS nodes.

14. **Blockchain-based data delivery and gathering approach:**To ensure differentiation between drones and the ground control systems that operate them, a blockchain-based Data Delivery and Gathering system was proposed by author [74]. The DDG creates the system nodes with secret blocks and keeps track of all interactions among them.

15. **An innovative search and rescue system architecture built on blockchain:**The author [75] suggested an IoT-based blockchain architecture for performing search and rescue operations. The design uses edge computers and both small and large drones to conduct offloading tasks.

16. **Traffic management for Unmanned aerial system using blockchain:**The author [76] proposed a Lightweight blockchain-based security solution for low-altitude Drones using hyper ledger fabric that satisfies the processing and storage resource constraints of UAVs. Between the UAVs and their ground control centres, This proposed chain technique also offers secure and impermeable traffic data.

2.6.1.5 Solution based on Intrusion Detection System (IDS) Scheme:

To prevent intruder attacks such as Denial of service attacks, the Intrusion detection system is required. The intrusion detection system is a monitoring system to detect any uncertain activity and make an alert for any breach by an alarm system. When an IDS is implemented in a system as complex as the FANET system, the generated alerts need to be both extremely precise and minimal to optimize the efficiency of the security system and avoid interfering with the proper operation of control applications that use the medium. The different types of security approaches carried out by IDS:

1. **Network IDS for IoT-based UAV network:**To validate the efficacy of their proposed safeguard mechanism, the author [68] utilized a paparazzi UAV, an open-source drone hardware and software project for simulated and emulated testing to accurately depict realistic scenarios. They generated three-dimensional digital signatures for denial of service (DoS) attacks by analyzing network traffic datasets that contained anomalies. The proposed technique was assessed in simple settings with a limited number of legitimate nodes and a single attack to detect both continual and progressive flash crowds.

2. **Detection of attacks using Lightweight IDS:**The author [77] described a small, energy-efficient system that may be included in contemporary UAVs to accurately detect GPS spoofing and denial-of-service attacks. To find the attacker, the IDS combines autodidactic with a multiclass SVM(Support vector machine). The results

are valuable since they were evaluated in a real-world setting with 20 UAVs and 4 Ground Control Station.

3. **Intrusion detection and response scheme:**The author [78] developed and tried several IDSs that can handle a wide range of assaults, getting excellent precision with few false positives to safeguard drones that conduct excursions in remote locations and to gather and transmit vital information about the conditions of these areas. The cyber-attacks like jamming, spoofing, gray hole, and black hole attacks are prevented under this scheme.

4. **IDS inspired by the human immune system:**The author [79] suggested an improved IDS that can protect drones from a variety of threats but at the expense of significant transmission overhead between nodes to find safe paths. Additionally, in highly mobile settings like Drones, the suggested IDS makes the unreal assumption that this safe path won't alter during the subsequent communication try.

5. **Secure communication with improved network IDS:**The author [80] proposed an IDS for making traffic fingerprints based on Wavelet Leader Multifractal analysis and assessed their approach in a mixed experimental system using actual traces. Although no comparison with other techniques is provided, the method works admirably under a denial of service attack.

6. **IoT-UAV network IDS based on deep learning:**The author suggested [81] a dispersed IDS that is installed on the GCS and drones. Each UAV employs the Long short-term memory access-recurrent neural networks algorithm to identify UAV assaults. To validate the observed attack and alert the other drones, the GCS also utilizes the Long short-term memory access-recurrent neural networks model. On various datasets, including CICIDS2017, and TON IoT, the authors tried their model.

7. **AI-based IDS for IoT-based UAVs:**Under this scheme, the author [82] merged one-class classifiers with principal component analysis (PCA) to identify assaults so that the IDS could be trained with only regular data. Every UAV can be equipped with the suggested MAVIDS (Micro aerial vehicle IDS), which enables quick discovery and possible mitigation of cyberattacks even when there are GCS communication problems. Solution based on IDS is shown in Table 2.6.

2.6.1.6 Solution based on quantum cryptography:

As per the prior study of attacks, there are a bunch of attacks like active eavesdropping, denial of service attacks, GPS jamming, and spoofing through which IoT-based UAV networks can be compromised. So to overcome the possible assaults, the researchers came to provide a solution based on quantum cryptography. Quantum cryptography is based on the principle of quantum physics. Quantum physics utilizes two main properties, which are the following :

1. **Quantum Superposition:** Quantum superposition means combining the two valid quantum states to produce the other authorized quantum state. The quantum state can be represented in the form of a qubit in the case of quantum computers, whereas traditional computer uses the concept of binary state, either 0 or 1 at a particular point in time. In the case of a quantum computer, the qubit may be both states 0

or 1 simultaneously. So, due to its varying state, the output of computers can never remain the same, and that property is utilized by quantum computers to solve the calculations at a high rate.

2. **Quantum entanglement:**Quantum entanglement is a property of quantum physics in which quantum particles share information and interact with each other at some distance. This property plays an important role in quantum computing in securing communication with quantum cryptography.

The quantum computer utilizes the above properties to provide secure communication in an IoT-based UAV network. The author [10] proposed a solution based on quantum cryptography to ensure security. The author of this paper discusses the layered architecture, which consists of many layers such as a monitoring layer, UAV layer, quantum security layer (BB84 protocol), Internet layer, and control layer.

In the monitor layer, the UAVs with cameras monitor and capture data from various desired positions like cities, forests, etc. This layer works on mathematical expression.

In the UAV layer, UAVs appear physically in any location. To collect further information from the ground, the UAV layer forms the swarm of UAVs to achieve this purpose. This layer is vulnerable to various known attacks. So, to address these problems the next quantum layer was proposed by the author.

In the Quantum layer, the data is transferred to this layer right from the monitor layer and provides security to the sensitive information using the quantum key distribution protocol. BB84 protocol. BB84 protocol is used for key transfer, which produces a nonce private key between two entities. The BB84 protocol uses the concept of photon polarization for secure transmission.

In the Internet layer, beyond 5G, mobile communication technology is used due to low latency and scalability, which gives flexibility to UAV swarms for quick data transmission. 5G networks provide secure and fast communication using two communication channels such as quantum as well as the classical state.

In the last control layer, the ground control station(GCS) is responsible for centralized data control for UAVs to keep and obtain real-time data given by the above layers. The quantum key distribution between UAVs can be applied among quantum computers at GCS.

2.6.1.7 UAV Forensics:

A new area of digital forensics called ”drone forensics” seeks to gather and examine data from drone and their parts to detect assailants and malevolent intent. As UAVs travel the above-inhabited region and can be used by progressive groups and criminals to carry out unlawful activities, drone forensics is crucial. Even though forensics inquiry is well established in conventional fields, the IoT-based UAV network field lacks standards for the processes for gathering and analyzing evidence for a security event [83]. The IoT-based UAV environment presents several difficulties that prevent the standardization of forensics practices. It is challenging to develop a standard procedure that can be used with all of the different drone platforms and architectures, to start with. The investigation is also made more difficult by the drone’s multiple components and devices because forensics analysis must deal with the supporting devices as well as locate and connect the evidence gathered from these various devices. The IoT-based UAV nodes are typically connected to the cloud to offload resource-intensive duties. This feature expands the scope of the incident inquiry by moving data processing and management from the drone to the cloud. Additionally, cloud service companies rarely collaborate with investigators, and even when they do, the data may be spread across various servers and nations. This calls for authorization to be given to various organizations and agencies. The relevant methods proposed for UAV forensics are the following:

1. **Micro aerial vehicle forensic framework:**The author [84] suggested an investigative structure that was more thorough. The first division made by the authors was between hardware/physical car forensics and digital forensics for drones. Drone network data system records, sensor readings, file storage systems, and video recordings are all subject to analysis in digital forensics. Hardware forensics covers drone model identification, testing for modification, cargo carrying, fingerprint analysis, and position. The authors suggested using an investigation structure to determine the UAVs structural elements. The JAVA program was created to examine and display the drones' flying records. The only record files that can be used for this task are CSV files, though.

2. **Drone examination and analysis:**The author [85] analyzed a Parrot Bebop 2 drone to gather flying information, retrieve media from the drone, and determine ownership. They only operate with small-scale drones, though.

3. **Investigation procedure of UAV:** The efficacy of current forensic standards for forensic investigations involving UAVs and drones is evaluated by the author. The author has gone over a list of recommendations for UAV/drone inquiries. Finally, the usage of DJI Phantom 3 UAV as an intensive report to present how the suggested principles can be applied to direct a drone forensic inquiry [86].

4. **Evaluation of UAV Forensic data:**Based on the investigation that was done and the science that contributed to this work, the author suggests the UAV Death Chain and classifies the significance and difficulty of all tasks mentioned. To the best of our knowledge, no addition has evaluated UAV-related studies in cybersecurity and digital forensics using ”Purple-Teaming” techniques. Additionally, this study suggests a classification structure that creates groups of UAVs with static and lives digital evidence problems according to how difficult and significant they are [87]

5. **Evaluation of UAV Forensic data:** By suggesting a digital forensic inquiry into drone technological processes, this paper develops a standardized method to carry out a digital forensic analysis of the Yuneec Typhoon H drone [88].

6. **Forensics investigation of DJI drone:**The author of this paper discusses the collection, examination, modification, and evaluation of important artifacts from the recorded flight data. To investigate and assess the relationship between the drone, the mobile phone, and the SD card, the criminal reconstruction for temporal analysis and relational artifacts is given [89].

7. **Boarded media investigation of UAV:** It's crucial to perform investigations on the drone's onboard storage media to gather forensic proof. The analysis of this storage medium, which includes various artifacts like images, movies, log files, etc., is done to compile the digital proof needed to solve a crime. This study presents the data collected from the drone storing device [90].

Table 2.6: Solution based on IDS

Reference	Year	Name of Technique	Security Assessment	Outline
[91]	2019	Network IDS for IoT-based UAV networks.	Attack signature with Wavelet Leader Multi-fractal	• detects both continual and progressive surges in the number of users • There is a lack of precision or exact measurements.
[77]	2019	Lightweight IDS	Analysis by anomaly based .	• Detect spoofing and Jamming attacks. • Variable selection.
[78]	2017	Intrusion detection and response technique	Signal strength intensity, JITTER	• Protection against various attacks like GPS spoofing, jamming, and false information dissemination. • Delay Tolerant network is a challenge
[79]	2020	IDS is inspired by the human immune system	Human immune system.	• Protection against wormhole, grayhole, blackhole attacks, and Fake information dissemination attacks. • High overhead of communication.
[80]	2018	Secure communication with improved network IDS	Bayesian Nash equilibrium game theory	• Protection against distributed denial of service attack. • No discussion and comparison with other techniques.
[81]	2021	IoT-UAV IDS based on deep learning	Recurrent neural networks	• Protection against well-known attacks like DDoS. • No discussion and comparison with other techniques.
[82]	2022	AI-based IDS for IoT-based UAV network	Principal component analysis	• Mitigate attacks like jamming and spoofing. • The count of UAVs is one only.

8. **Evaluation of UAV Forensic Analysis Software:**In [92], the author thoroughly examined the state-of-the-art UAV forensic research methods from various angles.

This article also makes the following contributions:

(a) The discovery of personally identifiable information

(b) The testing and evaluation of forensic software tools currently in use.

(c) A review of the methods for storing data and the layout of the proof in two DJI drones (such as Phantom 4 and Matrices 210).

(d) The use of a three-dimensional visualization tool to examine flying paths that were retrieved from UAVs.

9. **DJI Phantom 3 UAV forensic investigation:**The author [93] provides the first comprehensive forensic examination of a DJI Phantom III drone and the first report of any proprietary file structures the drone under examination may have saved. DRone Open-source Parser (DROP), an open-source utility that analyzes private DAT files extracted from the drone's nonvolatile internal storage, is also presented. This DAT data is compressed and secured. The study also includes a preliminary analysis of written documents that were found on the mobile device that was controlling the drone and that were private, secret, and coded. These folders contained a wealth of information, including GPS coordinates, battery life, flight duration, etc. The UAV investigation scheme is presented in Table 2.7.

2.6.1.8 Solution based on SDN(Software-Defined Networking):

SDN(Software-defined Networking) is a revolutionary form of network architecture and administration that attempts to simplify and improve network operations. It adds a centralized control plane, which enables more adaptable and dynamic network administration by isolating the network's control logic from the underlying hardware architecture. Through the centralized controller's global perspective, SDN in IoT decreases the complexity of distributed IoT architectures and improves resource utilization. The different methods for SDN-based UAV networks are the following:

1. **optiML algorithm:** The authors of this paper [94] have introduced a secure machine learning-based strategy named the ”optiML algorithm” to enhance the throughput of an SDN controller and improve UAV communications and security. The proposed approach comprises three main steps. Firstly, it involves the optimal positioning and user association of UAVs using a Genetic algorithm. Secondly, it determines the placement of the SDN controller using the shortest path in a single connected graph. Finally, it includes the creation and detection of DDoS attacks using a Feedforward neural network classifier.

2. **ESCALB(Efficient slave controller allocation-based load balancing) Scheme:** This work [95] offers ESCALB, a novel load balancing strategy for SDN-enabled IoT in a multi-domain scenario such as UAV networks, intending to resolve quality of service (QoS) and denial of service concerns utilizing a distributed control plan that employs SDN controllers. To do this, the ESCALB model continuously analyses the control plan's load information, allowing for the ranking of slave controllers and the efficient movement of switches within the network.

2.6.2 Physical attacks prevention scheme:

2.6.2.1 Techniques for preventing collisions:

1. **Trajectory planning strategy:** The objective is to locate a concise and obstacle-free flight path to the intended destination, where the obstacles are stationary and well-defined. Trajectory planning methods can be further broken down into the three types of algorithms to prevent physical attacks [19], which are listed below [96]:

   (a) **Search algorithm based on random sampling:** In this group, a collection of nodes that sample the surroundings randomly look for a route that will prevent collisions. PRM(Probabilistic Roadmap), RRBT(Rapid Exploring Random Belief Tree), RRT(Rapidly Exploring Random Tree), and DDRRT (Dynamic Domain RRT) are examples of algorithms that fall under the category of arbitrarily selecting search algorithms and have been applied to the UAV industry[97–99].

   (b) **Algorithms based on learning** The fundamental principle of learning-based algorithms is to direct the UAV in a specific condition using a training procedure. The benefit of using learning-based approaches is being able to solve complicated, multi-objective issues. The problem of UAV route planning has been solved using some evolutionary techniques. Single and multiple UAV trajectory planning is utilized by genetic algorithms [100]. Neural networks are also used in planning a UAV trajectory, such as RNN (recurrent neural network) [101]. Reinforcement learning is also used in trajectory planning of UAV [102].

   (c) **Algorithms built on graphs:** Way planning has seen a rise in the use of graph-based search tools. With this approach, the search area is divided into a grid, and the grid is represented by a collection of squares. Many algorithms are utilized for the route planning of UAVs, such as Bellman-Ford, A^*, Kinematic A^*, Lazy theta star(θ), D^* Lite. These types of algorithms are the fastest in terms of search, but due to not having straightforward routes and being suitable for small areas, these algorithms are not a perfect fit [103].

2. **Sight-based techniques:** To address the impact avoidance issue, a variety of vision-based object recognition techniques have been suggested. To address the collision avoidance issue in an indoor setting, many experts used pictures taken by cameras placed on UAVs [104, 105]. To estimate how near objects would be to the UAV, the researchers used a method based on stereo cameras. This approach has a high computational expense, making it unsuitable for dealing with circumstances that arise in real-time [106]. A straightforward sight-based collision avoidance strategy was suggested because it employs a monocular camera to create a collision-free route while off-board processing of heavyweight calculations [107].

3. **Repulsive field method:**The repulsive field technique is one of the effective methods used in collision prevention. It is used by many academics to address the obstacle and UAV collision avoidance issue. This method considers each UAV as a charged particle, and collision avoidance moves are produced by the repelling forces between the aircraft. The potential field technique is a viable option for real-time application

because of its straightforward execution and minimal processing complexity.[108–110]. Due to the dynamic nature of UAVs, the repulsive field method is not suitable.

Table 2.7: UAV Investigation Schemes

Reference	Year	Name of Technique	Outline
[84]	2019	Micro aerial vehicle forensic framework	• created a Java-based program to examine and display the drones' flying records. • This framework makes use of digital and physical frameworks.
[85]	2019	Drone examination and analysis	• Obtain information related to a flight, retrieve media from UAV, and determine ownership.
[86]	2018	Investigation procedure of UAV	• Illustrate the utilization of the suggested principles in directing a drone forensic examination with the DJI Phantom 3 drone.
[87]	2021	Evaluation of UAV Forensic data	• Consider static and live digital evidence problems. • Discuss the anti-forensics techniques.
[88]	2019	Forensic validation Analysis Process	• Develop a standard method to carry out a digital forensics analysis of the Yuneec Typhoon H drone.
[89]	2019	Forensics investigation of DJI drone	• Discuss the collection, examination, modification, and evaluation of important artifacts from the recorded flight data
[111]	2022	Boarded media investigation of UAV	• Examine flying route data that has been stored.
[92]	2021	Evaluation of UAV Forensic Analysis Software	• Testing and evaluation of forensic software tools currently in use

2.6.2.2 UAV identification techniques:

The two broad categories of UAV identification techniques are the following:

1. **Sound-based sensing:**Sound sensors have been suggested in several works as an effective tool to find drones. Some studies contrast the sound signatures produced by drone engines and rotating blades with other sound signatures that have been

gathered. Acoustic characteristics are taken after sound analysis. However, the precision of detection is impacted by noise and temperature. Additionally, the sensing area is constrained [90, 112, 113].

2. **Visual media-based sensing:** It is important to note that the majority of the research on drone identification has looked at image data and video feeds obtained from cameras [114, 115]. Other literature studies have mentioned shape analysis for UAV identification [116].

   UAV Investigation schemes are shown in Table 2.7

The hierarchy of secure communication is shown in Figure 2.3

2.7 Current Research Issues and Future Directions

While there have been various proposed solutions aimed at enhancing the security of IoT-based UAV networks, there are still some unresolved concerns that necessitate the collaboration of researchers and industry experts.

- **Identification and avoidance of malicious software of UAV:** Research has demonstrated that malware has the potential to infect drones [117]. To the best of our knowledge, there is currently no research available that deals with the identification of malware specifically designed for drones. Despite the absence of a malware dataset specifically designed for drones, a malware classification model is recommended for ground control centres [118]. The topic of detecting malware is not new and has received extensive attention from both academic and industrial sectors. Detection of malicious software relies on operating systems and necessitates the incorporation of specific detection capabilities. To identify harmful drones, the anti-malware system must take into account certain characteristics unique to the drone's operating system, including its use of navigational state in terms of height, place, speed, and direction. Hence, a suggestion has been made for the research community to explore the subject of detecting malware in drones.

- **Unique Intrusion detection system** Many of the Intrusion detection systems will work on UAV to GCS but do not include any additional intrusions associated with the drone, GCS, or any efforts to tamper with stored data without using the cloud system. The UAV dataset is not used for IDS instead of network simulators. So, by considering the UAV dataset, the IDS system can be trained.

- **Amalgamation of UAVs with different types of Networks:** To improve the secure communication between UAVs and ground stations then there is a requirement for the amalgamation of UAVs with IoT, Vehicle networks, and 5G. However, the combination of these networks can be vulnerable to attacks, so an integration framework & authentication protocols should be developed by the research community to ensure secure communication.

- **Lightweight encryption algorithms:** The GCS and UAVs constantly transfer the signals in IoT-based UAV networks, resulting in a significant transmission overhead. Therefore, UAVs need a lightweight encryption protocol to protect transmission because they run on batteries and can travel great distances. The researchers can work on lightweight quantum cryptography due to the dynamic nature of UAVs.

- **Fleet system for UAV security:** In an IoT-based UAV network system, the UAVs should collaborate to complete the task, but with better security, and for this purpose, a fleet system is the answer to maintain secure communication among UAVs. The fleet system must include reliable node identification and collaborative learning for privacy.

- **Post Quantum cryptography:** BB84 protocol discussed in section 2.6.1.6 can be vulnerable to active eavesdropping, and also quantum computers can break the product of large prime numbers in the RSA algorithm using faster calculation. To protect these cons, the lattice-based cryptographic technique can be the future scope for the researchers.

- **Chaos-based cryptology:** The chaos-based cryptology technique is used for image encryption that can also be used for encrypting messages between UAVs and UAV to GCS communication. Therefore, the chances of active eavesdropping by adversaries can be eliminated by using the chaotic map.

- **Secure UAVs communication based on SDN:** Software-defined networking can help IoT-based UAV networks eliminate security vulnerabilities with the help of controllers that can manage the whole network using the flexibility of programming rather than self-configuration. With the usage of a centralized SDN controller, the whole UAV network system can be compromised using the centre point of failure. So, the researchers should come up with a solution to overcome the single point of failure.

- **Rules and guidelines:** The administration should be made to limit the unauthorized usage of UAVs for harming the population. The stringent regulations must be there by allowing only authorized people with proper licenses to operate UAVs. The government should provide a security training session to companies and UAV operators like [86].

2.8 Preliminaries of Authentication schemes

This section provides prior knowledge on the authentication schemes.

2.8.1 Genus-2 Curve

Hyperelliptic curves encompass a range of algebraic curves with various degrees of complexity, including elliptic curves [119–122]. Consequently, it is possible to perceive an elliptic curve as a hyperelliptic curve with a genus of 2 [123, 124]. The hyperelliptic curve (HC) of genus g is given by the equation 2.1 as mentioned below:

$$y^2 + h(x)y = f(x) \tag{2.1}$$

where f(x) denotes the polynomial with a degree of $\phi = 2g+1$ or $\phi = 2g+2$, where $n > 4$ and has ϕ distinct roots. Also, let h(x) be a polynomial with a degree less than $g+2$. For example, Consider the hyperelliptic curve G2C, defined as in equation 2.2:

$$G2C : y^2 = x^5 - 5x^3 - 4x - 1 \tag{2.2}$$

This curve is situated over the rational numbers (Q), and it possesses a genus of g = 2, as shown in Figure 2.5.

The genus of a curve is a topological invariant representing the count of non-intersecting, single-closed curves that can be traced on the surface without dividing it. In other words, it corresponds to the number of topological handles present on the surface. The genus is always greater than or equal to 1 for hyperelliptic curves.

Let Z be the finite field with order p and p$\approx 2^{80}$.

- **Divisor**
  A divisor, denoted as D, is a formal summation of points P within the set G2C as in equation 2.3.
  $$D = \sum_{P \in G2C} j_p P \tag{2.3}$$
  where j$\in$ Z.

  The degree of D is the integer deg(D)=$\sum_{P \in G2C} j_p P$
  The order of D at P is the integer ord p (D)= j_p

  The divisors collectively constitute a mathematical group when operated upon by addition. This group, representing the divisor of hyperelliptic curve G2C, is formally denoted as 'D(G2C)'. The addition operation for combining two divisors can be executed in the following manner as in the equation 2.4 :
  $$D = \sum_{P \in G2C} j_p P + \sum_{P \in G2C} k_p P = \sum_{P \in G2C} (j_p P + k_p P) \tag{2.4}$$

2.8.1.1 Computational Hypotheses

- **Hypothesis Underlying the Genus 2 Curve Discrete Logarithm Problem (G2CDLP)**

  In the context of G2CDLP, we have adopted the following assumptions:

  - Let's denote a variable as "α", and it takes on values from the set {j — j is a positive integer greater than or equal to 1}

  - The likelihood of successfully computing "α" from the equation $K = \alpha \cdot D$ is deemed to be exceedingly small.

- **Computational Assumption for the Diffie-Hellman Problem in Genus 2 Curves (G2CDHP)**

  In the context of G2CDHP (Genus 2 Curve Diffie-Hellman Problem), we establish the following assumptions:

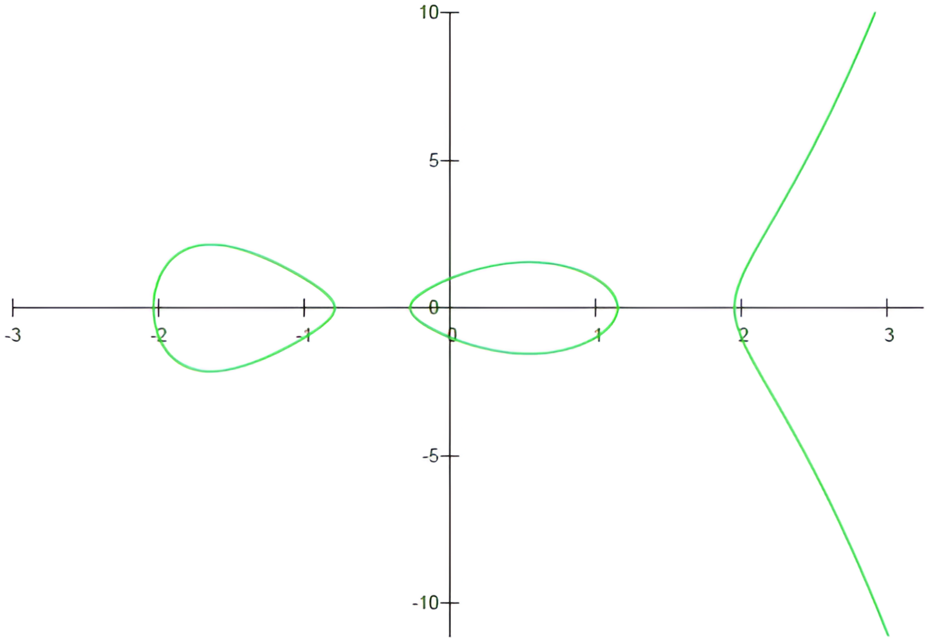


Figure 2.5: Genus-2 hyperelliptic curve

- We introduce two variables, ρ and Ω, and both are drawn from the set {j — j is a positive integer greater than or equal to 1}.
- To predict the variables ρ and Ω from the equation $K = \rho \cdot \Omega \cdot D$ is considered to be of negligible significance.

2.8.2 Physical Unclonable Function

PUF is a cryptographic primitive that acts as a distinctive electronic fingerprint [125, 126] encoded in a device's hardware, formed by unforeseen differences in production. Each PUF installed on the UAV is distinct, making it nearly hard to clone. For instance, the tiny variances in microchip circuits yield unique reactions when given the identical input challenge, generally described mathematically as $R = PUF(C)$, where C is the input challenge and R is the consequent response, thus forming (C, R) pair [127]. This innate uniqueness makes PUFs suitable for secure authentication and encryption applications, delivering a natural layer of protection thats impossible to imitate.

2.8.2.1 Properties of Physical Unclonable Function

Physically Unclonable Functions (PUFs) possess several essential properties that make them attractive for hardware security applications:

- **Unclonability** The inherent unpredictability generated during production renders it virtually hard to duplicate the precise structure of a PUF, even by the original producer. This mitigates redundancy and enhances security.
- **Unpredictability** The outputs of a PUF are indeterminate without prior familiarity with the individual challenge-response pairings (CRPs). This guarantees that adversaries cannot deduce answers from observable patterns.

- **Tamper Resistance** Any attempt to physically probe, manipulate, or tamper with a PUF modifies its physical properties, causing it to generate inaccurate or no replies. The tamper-evident characteristic augments its security.
- **Entropy** PUF answers display high entropy, indicating they contain a considerable amount of randomness. This attribute is critical for secure key generation and ensuring robust cryptographic performance.
- **Uniqueness** Each PUF demonstrates a unique response to the same problem due to intrinsic manufacturing variances. This ensures that every device with a PUF is recognizable from others, making it an effective hardware fingerprint.

2.8.3 Fuzzy Extractor

A fuzzy extractor is a cryptographic technology that is commonly applied in scenarios where biometric data, such as fingerprints or voiceprints, are used for user identification purposes [128]. It includes two operations:

- The generation operation ($Gen(\cdot)$) receives biometrtic traits (BT_{EU}) as inputs and produces a secret biometric key γ_{EU} and helper data (hd). The equation for the generator function is $Gen(BT_{EU}) = (\gamma_{EU}, hd)$
- The reproduction operation, ($Rep(\cdot)$), accepts Biometric traits (BT^*_{EU}) and hd as inputs. It reproduces the biometric key on verifying the condition $HamD(BT^*_{EU}, BT_{EU})$ $\leq t$, where $HamD$ signifies the Hamming distance $HamD$, and t denotes the threshold. The equation for the Reproduction function is $Rep(BT^*_{EU}, hd) = \gamma_{EU}$.

2.8.4 Security Validation Tool

2.8.4.1 Scyther

Scyther is a protocol verification tool which comes with Security Protocol Description Language (SPDL) syntax. This simulation tool is used to validate the security aspects related to authentication, confidentiality, and integrity. Scyther tool characterizes the entities involved as roles within the proposed protocol. Scyther is instrumental in verifying, falsifying, and comprehensively analysing the security features of the protocol. Scyther serves as a mechanism for assessing the core security properties based on the assumption of perfect cryptography [129]. It's worth noting that when using the Scyther tool, potential attackers cannot execute security attacks on encrypted messages unless they possess the decryption key. Contrasting with the DY model presented by Dolev and Yao in 1983, where attackers had absolute control over communication entities, in the scenario involving the Scyther tool, adversaries are constrained from capturing, altering, or deleting transmissions across the network unless they can derive new information from their existing knowledge. Understanding these mathematical foundations is crucial for designing and evaluating PUFs in secure hardware applications. The Scyther tool employs claims to articulate and define the security requisites. These claims encompass a range of criteria, including Nisynch, Secret, Niagree, Alive, and Weakagree.

- **Secret:** The objective is to establish confidentiality measures that facilitate secure communication between the two participating parties, and the written syntax for the claim is claim(I, Secret, H) where I is the role or entity and H is considered a secret value.

- **Niagree:** The establishment of a non-injective agreement with a role concerning a set of data items can be achieved through the inclusion of the relevant signal claims and syntax for this claim is claim(I, Niagree)

- **Nisynch:** All processes related to data transmission and network sessions involving the entities must adhere rigorously to the security regulations delineated within the proposed protocol. It is paramount that all participating entities diligently uphold synchronization with their current operational states. claim(I, Nisynch) is the syntax in SPDL.

- **Alive:** The aim of claim(GCS, Alive) is to ensure a robust authentication process between the designated parties, focusing on enabling the execution of specific tasks by an intended communication partner.

- **Weakagree:** In professional terminology, one can assert that a protocol provides a form of weak agreement to an initiating party denoted as 'A' concerning another party, referred to as 'B,' when it ensures that whenever 'A' assumes the role of the initiator and successfully concludes a protocol session, ostensibly involving 'B' as the responder, it is implied that 'B' had been engaged in a prior execution of the same protocol, seemingly with 'A' as the initiator. In the domain of SPDL programming, which facilitates input provision to the Scyther tool, security assertions are appended to the conclusion of each role. These assertions serve as essential criteria enabling entities to assess whether the protocol has successfully passed the verification process as intended and whether the predefined security goals have been achieved. The syntax for this claim is claim(I, Weakagree).

2.8.5 Random oracle model

This method is a mathematical model that responds to distinct queries with arbitrary responses by validating shared session keys from adversaries. The Random Oracle Model (ROM) is a theoretical framework in cryptography where hash functions are idealized as random oracles. In this model, a hash function functions as a black box that gives really random outputs for each unique input, while ensuring consistency for repeated requests. This abstraction facilitates the study and design of cryptographic protocols by allowing them to assume the availability of a perfect hash function [13].

2.8.6 Principle terms in Random oracle model

- **Oracle:** The oracle in ROM is a theoretical entity that resembles a perfect hash function. It accepts an input (query) and returns a really random response while maintaining consistencyreturning the same output for subsequent requests with the same input. The oracle is essential to the ROM because it provides an idealized abstraction of cryptographic hash functions, enabling easier security proofs.

- **Participants:** Participants are the entities entailed in the cryptographic protocol under investigation in the ROM. These can include humans, devices, or systems that interact with the Oracle and one another. Participants send queries to the

Oracle and use the replies to perform protocol processes such as key generation, authentication, and data verification.

- **Partnership:** Partnership refers to the interaction between protocol participants who work together to achieve a certain cryptographic purpose, such as creating a shared secret or authenticating one another. Partners are often characterized by their common knowledge of specific parameters (for example, a session key or pre-shared secrets) and their agreement to complete protocol stages together.

- **Freshness:** Freshness guarantees that cryptographic elements, such as session keys or nonces, are fresh and not repeated from earlier protocol sessions. This characteristic is critical for mitigating replay attacks when adversaries reuse legitimate data from old sessions. Freshness is sometimes achieved by integrating nonces (unique random numbers), timestamps, or sequence numbers into protocol messages.

- **Adversary:** The adversary in ROM symbolizes a theoretical attacker seeking to compromise the protocol's security. The adversary can engage with the oracle by sending queries and observing responses, imitating real-world assaults like guessing, interception, or message tampering. In security proofs, the adversary's success is quantified to demonstrate the protocol's resilience under the assumed paradigm.

2.8.7 ROM Queries

This method contains various queries that are necessary for the assessment of adversary attacks as follows:

- **Send:** Send Query allows an attacker to send messages to protocol participants and observe their answers, imitating active assaults like impersonation or message manipulation.

- **Execute:** Execute query enables the adversary to passively watch the communication between honest parties without interference, indicating passive eavesdropping attacks.

- **Corrupt:** Corrupt query allows an attacker to compromise a participant in order to acquire access to their long-term secret keys, making it easier to assess the protocol's robustness to insider threats and key compromise scenarios.

- **Reveal:** The Reveal query allows the attacker to collect session-specific secrets, such as session keys, in order to assess the protocol's security regarding session key disclosure and attributes, such as forward secrecy.

- **Test:** Test query evaluates the indistinguishability of a session key from a random value, which is critical for demonstrating the protocol's security against chosen-ciphertext or chosen-plaintext attacks.

2.9 Summary

In this chapter, we have provided a thorough analysis of secure communication methods in IoT-based UAV networks, outlining the progression from traditional methods to lightweight, elliptic curve encryption, blockchain, and quantum cryptography. This study focuses on significant research questions and covers literature from 2017 to 2022. Current physical and logical attacks against UAVs are categorized in this chapter. It examines past malicious attempts and suggests a systematic research approach. Future directions and current research challenges are discussed for additional analysis. The chapter also introduces foundational concepts related to authentication schemes.

Chapter 3

G2CAIUN: A Novel Genus-2 Curve-based Authentication for Secure Data Transmission in IoT-based UAV Networks

In this chapter, we have proposed a novel Genus-2 curve-based authentication and key agreement scheme which provides resilient communication in IoT-based UAV networks. The proposed work applies the hyperelliptic curve discrete logarithm hardness, cryptographic hash function, XOR operation, random tokens and unique timestamps, and PUF to prevent adversary attempts such as session key disclosure in the smart city environment.

3.1 Introduction

The Internet of Things is a rapidly growing domain with the advancement of miniature technologies and provides a network of a more significant number of devices through the Internet. Every device, such as appliances, industry machines, and vehicles in an IoT environment, is equipped with sensors, integrated circuits and embedded hardware. There are numerous applications like healthcare to monitor patient health, track weather conditions and soil moisture efficiency, and crop management [130]. IoT-based UAV networks comprise a GCS, UAVs, and EU. In this network, UAVs gather data from their surroundings and transmit it to the designated server located at the GCS. The GCS, in turn, exercises control and oversight over the UAVs by dispatching control commands through wireless channels [16]. The use of UAV innovation[41] has altered the manner in which the community gathers information for a variety of purposes, including but not limited to disaster response, healthcare, public safety, delivery, agriculture, security, and military [8, 131]. Additionally, unmanned aerial vehicle applications extend to smart cities, which have played a significant part in the improvement of urban management and public services [22, 132, 133].

Despite the merits, there are some significant concerns regarding security breaches in smart city environments as external users like traffic management authorities and emergency vehicles such as firefighters and ambulances need sensitive data from UAVs through GCS over the public channel, which can be captured by the adversary to perform replay, man-in-the-middle, session key attacks. Moreover, the UAVs can be captured by adversaries to tamper with the credentials stored in UAV storage [134]. Therefore, the proposed G2CAIUN protocol provides a mutual authentication scheme based on the Genus-2 curve. This authentication and key agreement scheme utilises hyperelliptic curve point multiplication, ensuring high security with formal and informal security analysis, and the performance of the proposed scheme shows lower computation and communication overhead.

3.1.1 Motivation

Although IoT-based UAV Networks offer significant advantages and facilitate several potentially beneficial applications and its general design needs new data protection measures and secure authentication protocols. In smart city environments, external users need sensitive updated information from the deployed UAVs to make the perfect decisions in certain circumstances, such as current traffic conditions required by the traffic police to prevent vehicle crash incidents and healthcare ambulance vehicles for patients in emergencies. When UAVs provide data to third-party users, protecting the identity of the UAVs becomes critical [16, 135]. This is because an opponent might theoretically track a UAV and determine its geographical location. The existing study employs bilinear pair cryptography, symmetric encryption, and authenticated encryption with associative data (AEAD), elliptic curve cryptography (ECC) with high computation and communication overhead, and their work provides secure communication within EU and UAV entities through GCS without including UAV-GCS and UAV-UAV environment. Thus, to mitigate these challenges, the proposed G2CAIUN mutual authentication scheme is designed which is based on the Genus-2 Curve for IoT-based UAV networks. The proposed work provides separate session keys for each session between EU and UAVs through distinct timestamps and enigmatic identities. This work provides PUF primitive to protect UAVs from physical capture attacks in each communication environment, such as EU-GCS-UAV, UAV-GCS and UAV-UAV. This work employs a Genus-2 hyperelliptic curve point multiplication with a reduced key size of 80-bit, providing a similar level of robust security as an elliptic curve of genus-1 with a half-field size. Currently, no such subexponential fast algorithm exists for the Genus-2 curve to solve discrete logarithmic problems, which motivates us to design a robust and lightweight mutual authentication scheme.

3.1.2 Novel Contributions

This section mentions all the novel contributions of the proposed scheme as follows:

- Demonstrates a Genus-2 curve-based authentication scheme for robust communication in IoT-based UAV networks.
- Leverages the hyperelliptic curve discrete logarithm problem and anonymous identity to ensure the communication is encrypted and anonymous from adversary attacks.
- The proposed work applies the cryptographic hash function, XOR operation, random tokens and unique timestamps to prevent session key disclosure and maintain forward secrecy.
- Adopts Physical Unclonable Function (PUF) technique to keep the scheme lightweight and resistant to physical tampering attacks.
- This work provides mutual authentication and key agreement among EU, GCS and UAV with UAV-GCS and UAV-UAV authentication mechanisms.

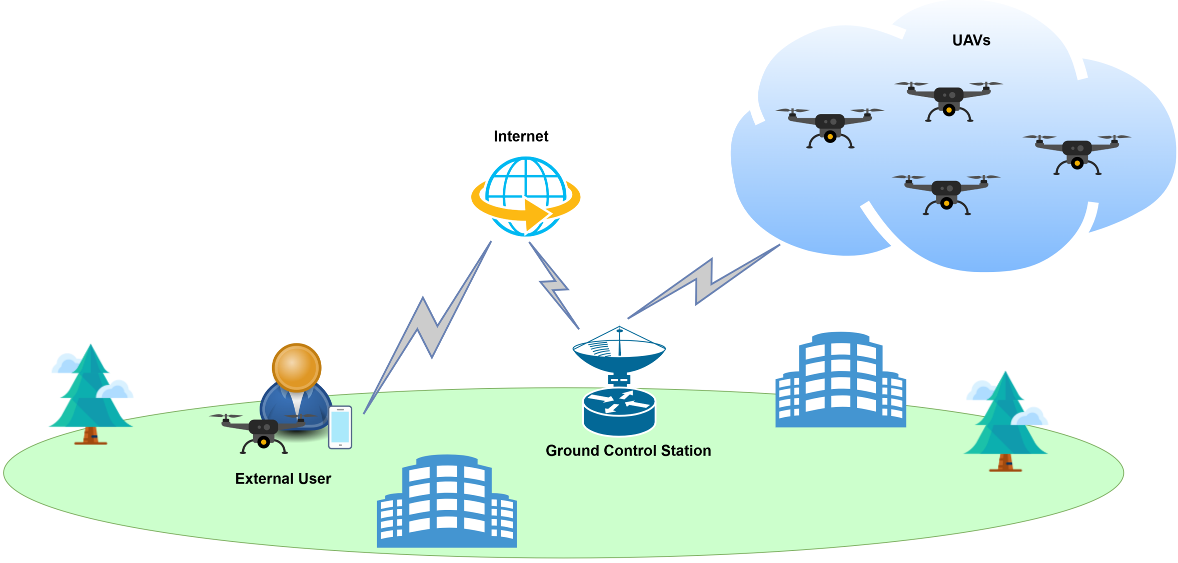


Figure 3.1: Network model

- Comparative analysis of the proposed scheme is presented regarding security attributes, communication and computation overhead.

- The proposed work is analysed with formal and informal methods such as the Random Oracle Model and Scyther tool under the DY and CK-adversary model.

3.2 System Model

This section discusses the network model for IoT-based UAV networks along with the adversary model as described below:

3.2.1 Network Model

This model demonstrates the network model for IoT-enabled UAV networks in smart city scenarios. The suggested network model includes three entities such as EU, UAV and recognised entity GCS. which is illustrated in Figure 3.1 and described below:

- EU : The external user holds the smartphone device and obtains the confidential credentials during the registration stage. The secure session key is established between the EU and UAVs, ensuring mutual authentication.

- GCS : The Ground Control Station is the recognised entity which maintains the communication between UAVs and external users and allows only registered users and UAVs in the network.

- $UAVs$: Unmanned Aerial Vehicle gets its confidential data from GCS after registration. These vehicles collect the required data via sensors for smart cities and transfer it to authorised GCS and EU.

3.2.2 Adversary Model

The following adversary models are assumed for the IoT-based UAV network.

- **DY-Adversary Model** We assumed the DY adversary model [136] for IoT-based UAV networks. Under this model, an attacker (A) can take complete control over an insecure channel. The attacker may delete, block, replay and modify any message content transferred on the channel, thus obtaining sensitive information by known attacks such as “eavesdropping”, “denial of service”, “replay”, “modification” and “man in the middle” attacks.

- **CK-Adversary Model** We also consider the complete CK adversary model [137] in which it is assumed that confidential credentials such as session temporary information can be obtained by the attacker thus, perform the unauthorised activity such as “impersonation”, “known-session key” attacks using the credentials and may capture the UAVs physically.

3.2.3 Design Goals

The various design goals are required to achieve the robustness of the proposed scheme, as mentioned below [50, 138–141]:

- **Mutual authentication:** Authentication is required at both entities’ ends, i.e. between EU and UAV and among UAVs, to ensure trustworthiness.

- **Untraceability:** The communicated messages or confidential information, such as the UAV’s actual location, must not be traceable among entities such as EU, GCS and UAVs.

- **Anonymity:** The attacker must not reveal the original identity of the enrolled entities such as EU, UAV and GCS.

- **Non disclosure of session key:** The current session key must be kept secret between the EU and UAV. If this is not the case, then predicting the previous session key by the attacker must remain intact.

- **Resistance to known attacks:** The communicating entities must ensure resistance against well-known attacks such as “eavesdropping”, “denial of service”, “replay”, “modification” and “man in the middle” and “impersonation ”attacks.

- **Physical capture resiliance:** If the smartphone device and UAVs are captured by the attacker, then the designed scheme must ensure the safety of these devices without revealing the sensitive data stored in their respective memories.

3.3 Proposed Scheme

This section covers the design and development stages of the proposed scheme.

3.3.1 Setup Stage

The main task in this stage is performed by GCS to publish parameters that will be employed during enrollment, authentication and key agreement stages as described below:

- **Step-1:** Perform amalgamation of PUF hardware from reliable sources into UAVs to publish parameters such as PUF challenge (CH_{UAV}) and store them in UAV storage.
- **Step-2:** GCS choose the private key,$PRK_{GCS} \in Z$ i.e. set of positive integers.
- **Step-3:** The GCS then selects HC and picks a divisor (D) to calculate the public key as mentioned in equation 3.1:

$$PBK_{GCS} = PRK_{GCS}.D \tag{3.1}$$

- **Step-4:** The GCS selects hash function '$h(.)$' and publish the parameters $\{CH_{UAV}, PBK_{GCS}, D, h(.)\}$ in IoT-based UAV environment.

3.3.2 Enrollment Stage

External users and UAVs register themselves to get confidential credentials from a trusted authority, GCS, as described below:

3.3.2.1 External User Enrollment

The sensitive data is required for the monitoring purposes from UAVs under smart city environments, which can be accomplished when the External User (EU) is enrolled with GCS securely as mentioned below:

- **Step-1:** In first step EU choose an original identity 'ID_{EU}' and a corresponding password '$PASS_{EU}$' along with random number 'λ' to perform computation as specified in equation (3.2):

$$Y_{EU} = h(ID_{EU} \oplus PASS_{EU} \oplus \lambda) \tag{3.2}$$

- **Step-2:** GCS perform computation OID_{EU} and Z_{EU} on receiving request message, as in equations (3.3) and (3.4):

$$OID_{EU} = ID_{EU}.D \tag{3.3}$$

$$Z_{EU} = h(Y_{EU} \parallel OID_{EU}) \tag{3.4}$$

Subsequently, GCS records (ID_{EU}, OID_{EU}, Z_{EU}) within its database, and the message (OID_{EU},Z_{EU}) is transferred to user via secure channel and then EU completes the registration stage by storing the (OID_{EU},Z_{EU}, λ) in its memory after receiving the parameters from GCS as shown in Figure 3.2.

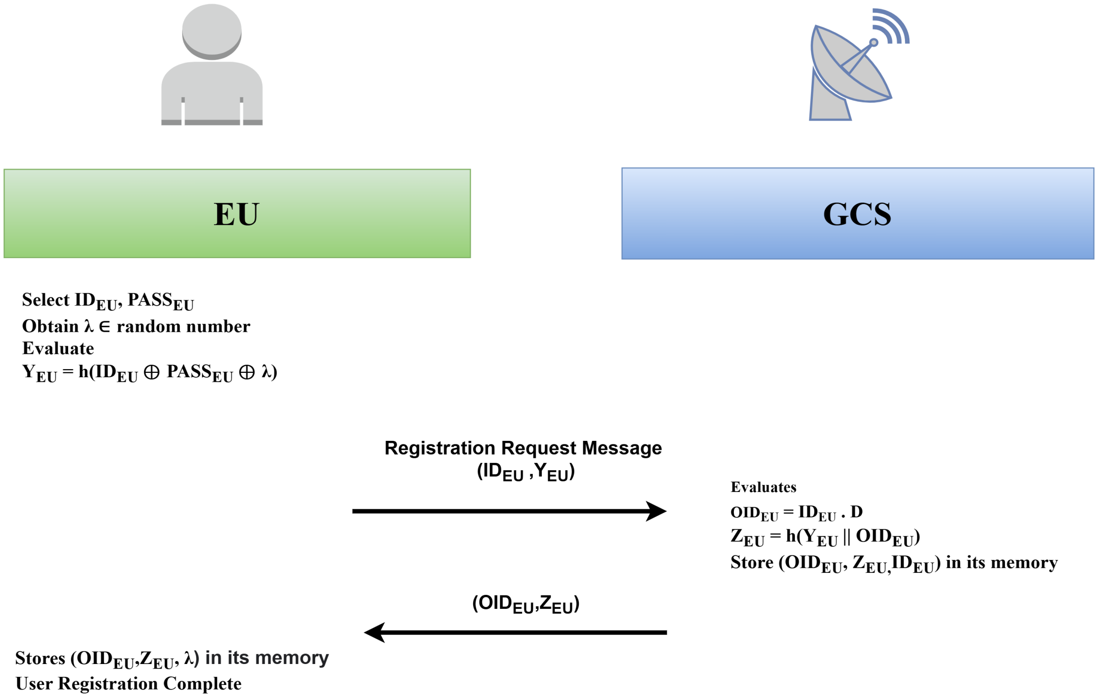

EU
GCS
Select ID$_{EU}$, PASS$_{EU}$
Obtain λ ∈ random number
Evaluate
$Y_{EU} = h(ID_{EU} \oplus PASS_{EU} \oplus \lambda)$
Registration Request Message
(ID_{EU}, Y_{EU})
Evaluates
$OID_{EU} = ID_{EU} . D$
$Z_{EU} = h(Y_{EU} \| OID_{EU})$
Store $(OID_{EU}, Z_{EU}, ID_{EU})$ in its memory
(OID_{EU}, Z_{EU})
Stores $(OID_{EU}, Z_{EU}, \lambda)$ in its memory
User Registration Complete

Figure 3.2: External user enrollment

3.3.2.2 UAV Enrollment

All the UAVs carry the bulk of information from the environments like smart cities, which can be required by the external user through GCS, which is presented in Figure 3.3 and described below:

- **Step-1:** Each UAVs selects there original identity 'ID_{UAV}' and forward the request message to GCS, which then utilise PUF hardware installed on UAVs and picks a random number 'η' and evaluates intermediate hash value IH_{UAV} along with OID_{UAV} as in equations (3.5)–(3.7) :

$$RES_{UAV} = PUF(CH_{UAV}) \tag{3.5}$$

$$IH_{UAV} = h(ID_{UAV} \parallel \eta \parallel RES_{UAV}) \tag{3.6}$$

$$OID_{UAV} = h(h(ID_{UAV} \parallel PRK_{GCS}) \oplus IH_{UAV}) \tag{3.7}$$

- **Step-2:** On successfully evaluating OID_{UAV}, GCS then transmit and store the obfuscation and original ID pair (OID_{UAV}, ID_{UAV}) to UAV for its respective memory to complete the enrollment.

3.3.3 Authentication and Key Agreement Stage

In this stage, both entities, EU and UAV, perform mutual authentication with each other to generate a session key for the secure transmission of data as presented in Figure 3.4.

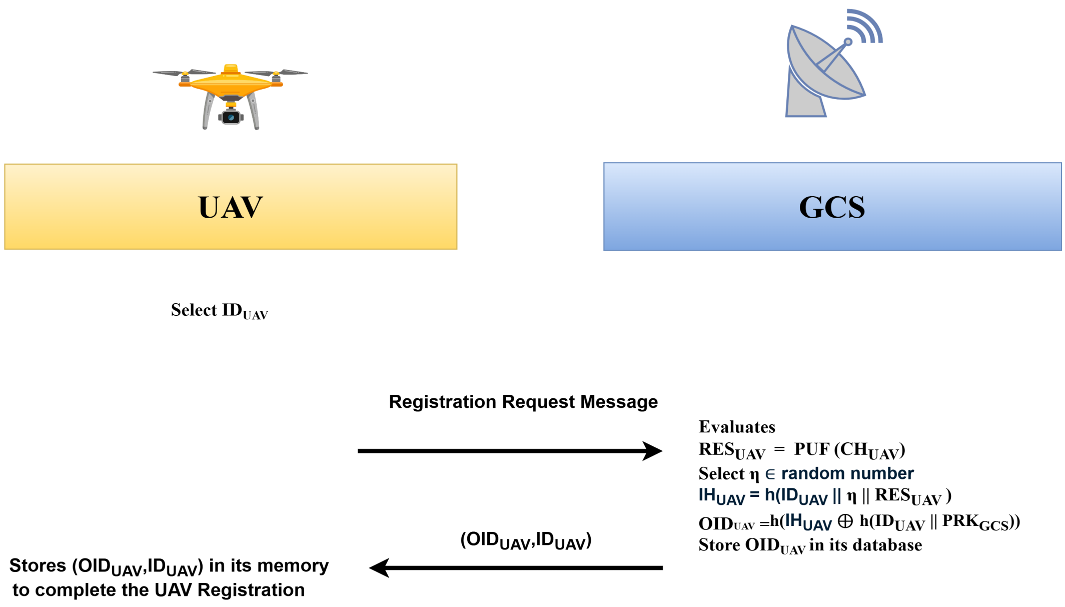

UAV
GCS
Select $\mathrm{ID}_{\mathrm{UAV}}$
Registration Request Message
Evaluates
$\mathrm{RES}_{\mathrm{UAV}} = \mathrm{PUF}\,(\mathrm{CH}_{\mathrm{UAV}})$
Select $\eta \in$ random number
$\mathrm{IH}_{\mathrm{UAV}} = h(\mathrm{ID}_{\mathrm{UAV}} \,||\, \eta \,||\, \mathrm{RES}_{\mathrm{UAV}})$
$\mathrm{OID}_{\mathrm{UAV}} = h(\mathrm{IH}_{\mathrm{UAV}} \oplus h(\mathrm{ID}_{\mathrm{UAV}} \,||\, \mathrm{PRK}_{\mathrm{GCS}}))$
Store $\mathrm{OID}_{\mathrm{UAV}}$ in its database
$(\mathrm{OID}_{\mathrm{UAV}},\mathrm{ID}_{\mathrm{UAV}})$
Stores $(\mathrm{OID}_{\mathrm{UAV}},\mathrm{ID}_{\mathrm{UAV}})$ in its memory
to complete the UAV Registration

Figure 3.3: UAV enrollment

- **Step-1:** External user enters ID_{EU} and password $PASS_{EU}$ in smartphone device to perform the computation as in equations (3.8)–(3.10).

$$Y^S_{EU} = h(ID_{EU} \oplus PASS_{EU} \oplus \lambda) \tag{3.8}$$

$$OID^S_{EU} = ID_{EU}.D \tag{3.9}$$

$$Z^S_{EU} = h(Y^S_{EU} \parallel OID^S_{EU}). \tag{3.10}$$

and checks (Z^S_{EU} ?= Z_{EU}).If validation is successful,then EU selects a timestamp TS_1 and evaluate the following equations (3.11)–(3.15):

$$PBK_{GCS} = PRK_{EU}.D \tag{3.11}$$

$$K_{EU} = PRK_{EU}.PBK_{GCS} \tag{3.12}$$

$$M_1 = h(OID_{GCS} \,||\, TS_1) \oplus OID_{EU} \tag{3.13}$$

$$M_2 = h(OID_{GCS} \parallel TS_1 \parallel K_{EU}) \oplus OID_{UAV} \tag{3.14}$$

$$M_3 = h(OID_{EU} \parallel OID_{GCS} \parallel OID_{UAV} \parallel K_{EU} \parallel TS_1) \tag{3.15}$$

After performing calculations, EU transmit the message $MSG_1 = (M_1, M_2, M_3, PBK_{EU}, TS_1)$ to GCS over the public channel.

- **Step-2:** GCS receives the request the MSG_1 and perform the validation ($|TS_{pr} - TS_1| \leq \Delta T$) , where ΔT depicts the maximum time for acquiring the message, and If the validation is successful, the GCS calculates the following as in equations (3.16)–(3.19).

$$K_{GCS} = PBK_{EU}.PRK_{GCS} \tag{3.16}$$

$$OID_{EU}* = h(OID_{GCS} \parallel TS_1) \oplus M_1 \tag{3.17}$$

$$OID_{UAV}* = h(OID_{EU}* \parallel TS_1 \parallel K_{GCS}) \oplus M_2 \tag{3.18}$$

$$M_3* = h(OID_{EU}* \parallel OID_{UAV}* \parallel OID_{GCS}* \parallel K_{GCS} \parallel TS_1) \tag{3.19}$$

GCS checks ($M_3? = M_3*$). If the condition is not valid, then GCS terminates the session; otherwise evaluates the following equations (3.20)–(3.22).

$$M_4 = h(OID_{UAV}* \parallel TS_2) \oplus RT_1 \tag{3.20}$$

$$M_5 = OID_{EU}* \oplus h(OID_{UAV}* \parallel OID_{GCS}* \parallel TS_2 \parallel RT_1) \tag{3.21}$$

$$M_6 = h(OID_{UAV}* \parallel OID_{GCS} \parallel OID_{EU}* \parallel TS_2 \parallel RT_1 \parallel RES_{UAV}) \tag{3.22}$$

Ultimately, GCS transmits message MSG_2 with contents such as M_4, M_5, M_6 along with TS_2 to the UAV.

- **Step-3:** UAV proceeds to validate $|TS_{pr} - TS_2| <= \Delta T$ on acquiring MSG_2, and If this validation is successful, then UAV performs the following equations (3.23)–(3.26) computations:

$$RT_1* = h(OID_{UAV} \parallel TS_2) \oplus M_4 \tag{3.23}$$

$$OID_{UAV}* = h(OID_{UAV} \parallel OID_{GCS} \parallel TS_2 \parallel RT_1*) \oplus M_5 \tag{3.24}$$

$$RES_{UAV}* = PUF(CH_{UAV}*) \tag{3.25}$$

$$M_6* = h(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}* \parallel TS_2 \parallel RT_1* \parallel RES_{UAV}*) \tag{3.26}$$

then check if ($M_6? = M_6*$). On successful verification, a new random token RT_2 and TS_3, is produced followed by equations (3.27)–(3.29).

$$M_7 = h(OID'_{UAV}* \parallel OID_{UAV} \parallel TS_3) \oplus RT_2 \tag{3.27}$$

$$SK_{UAV->EU} = h(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}{}^{*} \parallel TS_3 \parallel RT_2) \tag{3.28}$$

$$AUT_N = h(SK_{UAV->EU} \parallel TS_3) \tag{3.29}$$

After performing all the computations, the UAV transfers message $MSG_3 = (M_7, AUT_N, TS_3)$ to the EU over a public channel.

- **Step-4:** EU receives the message M_7 and validate the condition $|TS_{pr} - TS_3| <= \Delta T$. If the condition is valid, EU performs computation $RT_2{}^{*}, AUT_N{}^{*}$, the session key, denoted as $(SK_{EU->UAV})$, in the following equations (3.30)–(3.32):

$$RT_2{}^{*} = h(OID_{EU} \parallel OID_{GCS} \parallel TS_3) \oplus M_7 \tag{3.30}$$

$$SK_{EU->UAV} = h(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU} \parallel TS_3 \parallel RT_2{}^{*}) \tag{3.31}$$

$$AUT_N{}^{*} = h(SK_{EU->UAV} \parallel TS_3) \tag{3.32}$$

At last, EU validates $AUT_N{}^{*}$ and AUT_N. If the condition is satisfied, then the calculated session key is considered to be valid for secure data transmission. Otherwise, the session between the EU and UAV will terminate.

3.3.4 UAV-GCS Authentication Stage

This stage is responsible for establishing the session key between UAV and GCS as shown in Figure 3.5 and given as:

- **Step-1:** UAV initiates the process by producing timestamps TS_4 and random token (RT_3) followed by the equations (3.33)–(3.36) :

$$RES_{UAV_1} = PUF(CH_{UAV_1}) \tag{3.33}$$

$$MRES_{UAV} = h(RES_{UAV_1} \parallel CH_{UAV_1}) \tag{3.34}$$

$$RES_{UAV} = h(OID_{UAV} \parallel ID_{UAV} \parallel TS_4 \parallel MRES_{UAV} \parallel RT_3) \tag{3.35}$$

$$N = h(OID_{UAV} \parallel MRES_{UAV} \parallel TS_4 \parallel RT_3) \tag{3.36}$$

and forwards the message $(OID_{UAV}, RES_{UAV}, N, TS_4, RT_3)$ to GCS.

- **Step-2:** After collecting messages from UAV then, GCS will check the condition $|TS_{pr} - TS_4| <= \Delta T$. If validation is successful, then GCS recovers $MRES_{UAV}$ by knowing OID_{UAV} followed by equation (3.37):

$$N^{*} = h(OID_{UAV} \parallel MRES_{UAV} \parallel TS_4 \parallel RT_3) \tag{3.37}$$

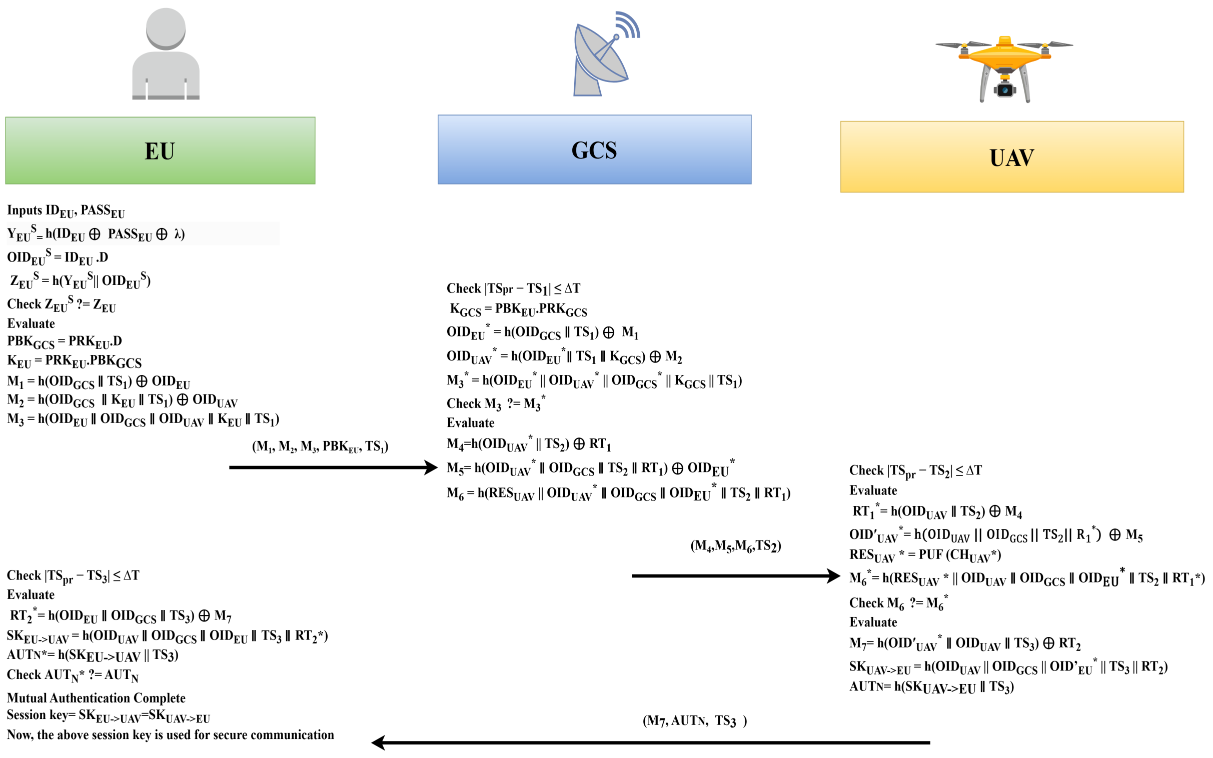

EU
GCS
UAV
Inputs ID_{EU}, $PASS_{EU}$
$Y_{EU}{}^{S} = h(ID_{EU} \oplus PASS_{EU} \oplus \lambda)$
$OID_{EU}{}^{S} = ID_{EU}.D$
$Z_{EU}{}^{S} = h(Y_{EU}{}^{S} \| OID_{EU}{}^{S})$
Check $Z_{EU}{}^{S}$?= Z_{EU}
Evaluate
$PBK_{GCS} = PRK_{EU}.D$
$K_{EU} = PRK_{EU}.PBK_{GCS}$
$M_1 = h(OID_{GCS} \| TS_1) \oplus OID_{EU}$
$M_2 = h(OID_{GCS} \| K_{EU} \| TS_1) \oplus OID_{UAV}$
$M_3 = h(OID_{EU} \| OID_{GCS} \| OID_{UAV} \| K_{EU} \| TS_1)$
$(M_1, M_2, M_3, PBK_{EU}, TS_1)$
Check $|TSpr - TS_1| \leq \Delta T$
$K_{GCS} = PBK_{EU}.PRK_{GCS}$
$OID_{EU}{}^{*} = h(OID_{GCS} \| TS_1) \oplus M_1$
$OID_{UAV}{}^{*} = h(OID_{EU}{}^{*} \| TS_1 \| K_{GCS}) \oplus M_2$
$M_3{}^{*} = h(OID_{EU}{}^{*} \| OID_{UAV}{}^{*} \| OID_{GCS}{}^{*} \| K_{GCS} \| TS_1)$
Check M_3 ?= $M_3{}^{*}$
Evaluate
$M_4 = h(OID_{UAV}{}^{*} \| TS_2) \oplus RT_1$
$M_5 = h(OID_{UAV}{}^{*} \| OID_{GCS} \| TS_2 \| RT_1) \oplus OID_{EU}{}^{*}$
$M_6 = h(RES_{UAV} \| OID_{UAV}{}^{*} \| OID_{GCS} \| OID_{EU}{}^{*} \| TS_2 \| RT_1)$
(M_4, M_5, M_6, TS_2)
Check $|TS_{pr} - TS_2| \leq \Delta T$
Evaluate
$RT_1{}^{*} = h(OID_{UAV} \| TS_2) \oplus M_4$
$OID'_{UAV}{}^{*} = h(OID_{UAV} \| OID_{GCS} \| TS_2 \| R_1{}^{*}) \oplus M_5$
$RES_{UAV}{}^{*} = PUF(CH_{UAV}{}^{*})$
$M_6{}^{*} = h(RES_{UAV}{}^{*} \| OID_{UAV} \| OID_{GCS} \| OID_{EU}{}^{*} \| TS_2 \| RT_1{}^{*})$
Check M_6 ?= $M_6{}^{*}$
Evaluate
$M_7 = h(OID'_{UAV}{}^{*} \| OID_{UAV} \| TS_3) \oplus RT_2$
$SK_{UAV\text{->}EU} = h(OID_{UAV} \| OID_{GCS} \| OID'_{EU}{}^{*} \| TS_3 \| RT_2)$
$AUT_N = h(SK_{UAV\text{->}EU} \| TS_3)$
(M_7, AUT_N, TS_3)
Check $|TS_{pr} - TS_3| \leq \Delta T$
Evaluate
$RT_2{}^{*} = h(OID_{EU} \| OID_{GCS} \| TS_3) \oplus M_7$
$SK_{EU\text{->}UAV} = h(OID_{UAV} \| OID_{GCS} \| OID_{EU} \| TS_3 \| RT_2{}^{*})$
$AUT_N{}^{*} = h(SK_{EU\text{->}UAV} \| TS_3)$
Check $AUT_N{}^{*}$?= AUT_N
Mutual Authentication Complete
Session key= $SK_{EU\text{->}UAV} = SK_{UAV\text{->}EU}$
Now, the above session key is used for secure communication

Figure 3.4: Authentication and Key Agreement Stage

Then, GCS perform validation $N? = N^*$. If the validation is unsuccessful, then the session is terminated; otherwise, GCS will generate a new challenge CH_{GCS} and a random number RT_3^* followed by equations (3.38)–(3.41):

$$OID_{GCS} = h(ID_{GCS} \parallel CH_{GCS}) \tag{3.38}$$

$$G_1 = h(OID_{UAV} \parallel TS_4 \parallel RT_3^* \parallel MRES_{UAV}) \oplus OID_{GCS} \tag{3.39}$$

$$SK_{GCS \to UAV} = h(OID_{UAV} \parallel TS_4 \parallel RT_3^* \parallel MRES_{UAV}) \tag{3.40}$$

$$G_2 = h(G_1 \parallel SK_{GCS \to UAV} \parallel RT_3^*) \tag{3.41}$$

At last, GCS forwards (G_1, G_2, RT_3^*) to UAV after computation.

- **Step-3:** On receiving (G_1, G_2, RT_3^*) from GCS, UAV evaluates the following equations (3.42) and (3.43):

$$SK_{UAV \to GCS} = h(OID_{UAV} \parallel TS_4 \parallel RT_3^* \parallel MRES_{UAV}) \tag{3.42}$$

$$G_2^* = h(G_1 \parallel SK_1 \parallel RT_3^*) \tag{3.43}$$

UAV will check for the validation of $G_2^* ?= G_2$. If the validation is successful, then SK_1 is treated as a valid session key for the UAV−GCS authentication stage.

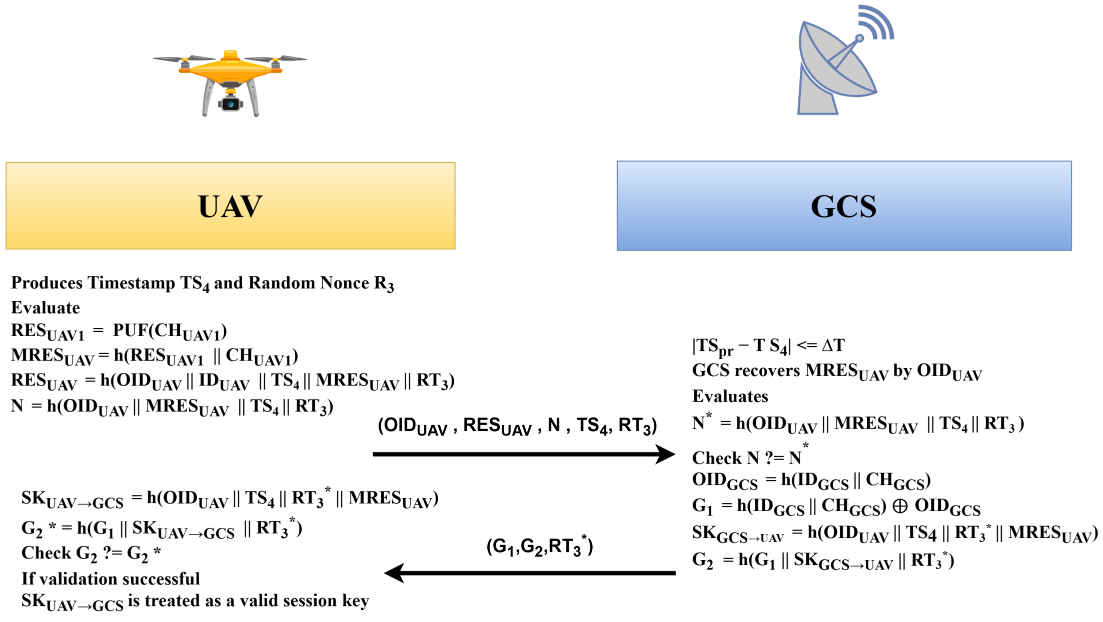

UAV
GCS
Produces Timestamp TS_4 and Random Nonce R_3
Evaluate
$RES_{UAV1} = PUF(CH_{UAV1})$
$MRES_{UAV} = h(RES_{UAV1} || CH_{UAV1})$
$RES_{UAV} = h(OID_{UAV} || ID_{UAV} || TS_4 || MRES_{UAV} || RT_3)$
$N = h(OID_{UAV} || MRES_{UAV} || TS_4 || RT_3)$
$(OID_{UAV}, RES_{UAV}, N, TS_4, RT_3)$
$|TS_{pr} - T S_4| <= \Delta T$
GCS recovers $MRES_{UAV}$ by OID_{UAV}
Evaluates
$N^* = h(OID_{UAV} || MRES_{UAV} || TS_4 || RT_3)$
Check $N ?= N^*$
$OID_{GCS} = h(ID_{GCS} || CH_{GCS})$
$G_1 = h(ID_{GCS} || CH_{GCS}) \oplus OID_{GCS}$
$SK_{GCS \to UAV} = h(OID_{UAV} || TS4 || RT_3^* || MRES_{UAV})$
$G_2 = h(G_1 || SK_{GCS \to UAV} || RT_3^*)$
(G_1, G_2, RT_3^*)
$SK_{UAV \to GCS} = h(OID_{UAV} || TS_4 || RT_3^* || MRES_{UAV})$
$G_2{}^* = h(G_1 || SK_{UAV \to GCS} || RT_3^*)$
Check $G_2 ?= G_2{}^*$
If validation successful
$SK_{UAV \to GCS}$ is treated as a valid session key

Figure 3.5: UAV-GCS Authentication

3.3.5 UAV-UAV Authentication Stage

In this stage, the UAV loaded with sensitive information needs to be disseminated to other UAVs by using authentication as shown in Figure 3.6 and given as:

- **Step-1:** UAV_1 sends the request to GCS for generating secure session key $SK_{UAV_1 \leftrightarrow UAV_2}$ to transfer the sensitive information to UAV_2 and session key between UAV_1 and GCS is generated before the send request.

- **Step-2:** On receiving the request by UAV_1, the GCS redirect this authentication request (REQ) along with $h(SK_{UAV_1 \to GCS}||OID_{GCS}||REQ)$ to UAV_2. UAV_2 then verifies the hash value and generates a session key $SK_{UAV_2 \to GCS}$ between UAV_2 and GCS.

- **Step-3:** Each session key $SK_{UAV_1 \to GCS}$ and $SK_{UAV_2 \to GCS}$ is utilised by UAV-GCS authentication stage to generate session key $SK_{UAV_1 \leftrightarrow UAV_2}$ which will be disseminated to UAV_1 and UAV_2 the for secure communication.

3.3.6 Password Update Stage

Each user can update their password credentials from time to time to keep the communication safe, and the following procedure is required to achieve this task:

- **Step-1:** EU with smartphone device enters its original identity ID_{EU} and password $PASS_{EU}$ and selects the random token λ to proceed with computations as in equations (3.44)–(3.46).

$$Y_{EU}^S = h(ID_{EU} \oplus PASS_{EU} \oplus \lambda) \tag{3.44}$$

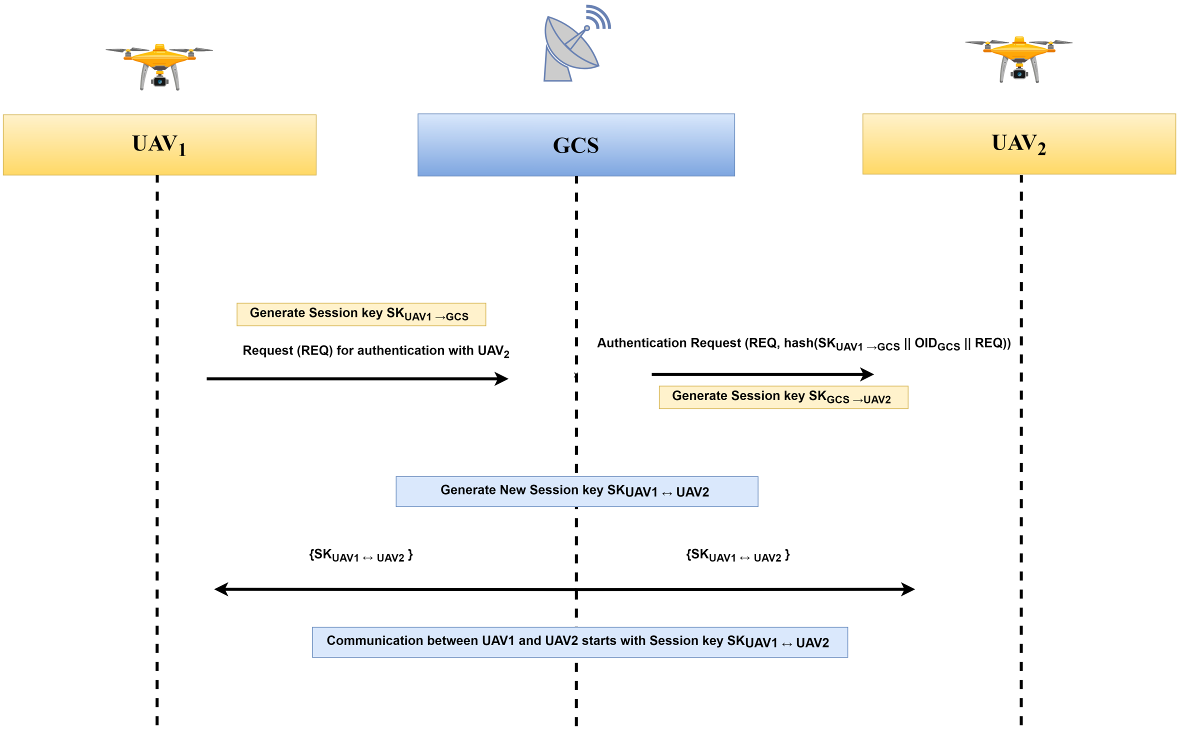

UAV1
GCS
UAV2
Generate Session key SKUAV1 →GCS
Request (REQ) for authentication with UAV2
Authentication Request (REQ, hash(SKUAV1 →GCS || OIDGCS || REQ))
Generate Session key SKGCS →UAV2
Generate New Session key SKUAV1 ↔ UAV2
{SKUAV1 ↔ UAV2 }
{SKUAV1 ↔ UAV2 }
Communication between UAV1 and UAV2 starts with Session key SKUAV1 ↔ UAV2

Figure 3.6: UAV-UAV Authentication

$$OID_{EU}^{S} = ID_{EU}.D \tag{3.45}$$

$$Z_{EU}^{S} = h(Y_{EU}^{S} \parallel OID_{EU}^{S}) \tag{3.46}$$

and if the condition $(Z_{EU}^{S}? = Z_{EU})$ is valid then EU can provide its fresh password credential for the updation. On the other hand, the session terminates automatically in case it is not valid.

- **Step-2:** On validation, EU provides $PASS_{EU}^{N}$ to the smartphone device, followed by the calculations in equations (3.47)–(3.49).

$$Y_{EU}^{N} = h(ID_{EU} \oplus PASS_{EU}^{N} \oplus \lambda) \tag{3.47}$$

$$OID_{EU} = ID_{EU}.D \tag{3.48}$$

$$Z_{EU}^{N} = h(Y_{EU}^{N} \parallel OID_{EU}) \tag{3.49}$$

- **Step-3:** At last, EU with smartphone device replaces the fresh Z_{EU}^{N} secret the EU substitutes Z_{EU}^{N} in place of Z_{EU}^{S} to maintain the robust system.

3.3.7 Termination and Reissuance Stage

EU smartphone devices can be lost or stolen due to any unforeseen situation, which can be overcome by replacement of the device as mentioned :

- **Step-1:** EU with smartphone device enters its original identity ID_{EU} and new password $PASS^{N}_{EU}$ and selects the random token λ' to proceed with computations as in equation (3.50).

$$Y^{N}_{EU} = h(ID_{EU} \oplus PASS^{N}_{EU} \oplus \lambda') \tag{3.50}$$

  then forward ID_{EU} and Y^{N}_{EU} for GCS storage over secure channel.

- **Step-2:** On getting a message from EU, GCS perform the following computation as given in equations (3.51) and (3.52).

$$OID_{EU} = ID_{EU}.D \tag{3.51}$$

$$Z^{N}_{EU} = h(Y^{N}_{EU} \parallel OID_{EU}) \tag{3.52}$$

  Subsequently, the GCS stores OID_{EU} and Z^{N}_{EU} in its memory and forwards these secret values to the EU over a secure medium.

- **Step-3:** EU performs computation on receiving data from GCS, and calculation is provided in equations (3.53) and (3.54)

$$Z^{N}_{EU}{}^{*} = h(OID_{EU} \parallel Y^{\mathrm{N}}_{EU}) \oplus Z^{\mathrm{N}}_{EU} \tag{3.53}$$

$$OID_{EU}{}^{*} = h(OID_{EU} \parallel PASS^{\mathrm{N}}_{EU}) \oplus OID_{EU} \tag{3.54}$$

At last EU replaces Z_{EU} with $Z^{N}_{EU}{}^{*}$ and stores $OID_{EU}{}^{*}$, $Z^{N}_{EU}{}^{*}$ in its memory.

3.3.8 UAV Augmentation Stage

The UAVs are resource-constrained devices due to which they can be easily exhausted from the network, so the replacement of UAVs is required to accomplish the task, and the process of augmentation is given as follows:

- **Step-1:** The latest UAV^{N} provides its ID as ID^{N}_{UAV} to the GCS and after receiving ID^{N}_{UAV} , GCS calculates new challenge-response $(CH^{N}_{UAV}, RES^{N}_{UAV})$ pair and intermediate hash value (IH^{N}_{UAV}) to calculate anonymous ID as in equations (3.55)–(3.57):

$$RES^{N}_{UAV} = PUF(CH^{N}_{UAV}) \tag{3.55}$$

$$IH^{N}_{UAV} = h(ID^{N}_{UAV} \parallel \eta \parallel RES^{N}_{UAV}) \tag{3.56}$$

$$OID^{N}_{UAV} = h(h(ID^{N}_{UAV} \parallel PRK^{N}_{GCS}) \oplus IH^{N}_{UAV}) \tag{3.57}$$

- **Step-2:** The GCS archives ID^{N}_{UAV}, OID^{N}_{UAV} within the drone's memory before its deployment in the operational field, along with ID^{N}_{UAV} in storage.

3.4 Security Evaluation

The G2CAIUN scheme is verified and analysed for resistance to security attacks using formal and informal verification through ROM and Scyther tools.

3.4.1 Formal evaluation

There are two formal verification strategies of the G2CAIUN protocol, which are mentioned below:

3.4.1.1 Ramdom Oracle Model-based evaluation

This evaluation provides the formal proof of session key ($SK_{EU \to UAV/UAV \to EU}$) during the authentication and key agreement stage of G2CAIUN. According to Table 3.1, the attacker can run different queries like *Corrupt*, *Test*, *Reveal* and *Execute* to perform the unauthorised activity. The fundamental ROM elements are given as:

- **Participants:** Our protocols include the following entities: EU, GCS, and UAV, all of which are considered participants in the communication. Each of the participant such as EU has the instance I_1 with oracle $\xi_{EU}^{I_1}$, UAV has the instance I_2 with oracle $\xi_{GCS}^{I_2}$ and UAV has the instance I_3 with oracle $\xi_{UAV}^{I_3}$.
- **Random Oracle:** Two random oracles, namely, $PUF(\cdot)$ and hash function $h(\cdot)$ will be selected for analysis.
- **Partnerships:** If the EU oracle $\xi_{EU}^{I_1}$ and UAV oracle $\xi_{UAV}^{I_3}$ continue to share a secure session key, they will become partners.
- **Adversary**: The adversary or attacker (A) can compromise the communication between entities as mentioned in the adversary model.
- **Freshness:** If attacker (A) does not reveal shared key information then $\xi_{EU}^{INS_1}$, $\xi_{UAV}^{INS_3}$ is fresh.

***Definition* (*Semantic Security*)**: Determining the actual SK created from a random number by an adversary A serves as the basis for the confidentiality of the session key communicated between the EU and UAV. By leaking SK information, A has a chance of violating the semantic security of the G2CAIUN protocol by winning the game $b' = b$ where b is real bit and b' is imagined bit, which leads to success probability denotes as sc, and advantage is described as:

$$Adv_A^{G2CAIUN} = |2.Pr[sc] - 1| \tag{3.58}$$

***Theorm* 1**: Let an attacker (A) working in polynomial time ($Poly_T$) to capture the session key $SK_{UAV \to EU}/SK_{EU \to UAV}$ during authentication and key agreement stage, then the advantage of A is given as:

$$Adv_A^{G2CAIUN}(poly_T) \leq \frac{Hash_Q^2}{|Hash|} + \frac{PUF_Q^2}{|PUF|} + 2Adv_A^{G2CDLP}(Poly_T) \tag{3.59}$$

Where terms like $|Hash|$, $|PUF|$, $Hash_Q$, PUF_Q, and $Adv_A^{G2CDLP}(poly_T)$ represent hash function length without collision, PUF length, hash queries frequencies, PUF query

Table 3.1: Query Details

Query	**Description**
$Corrupt(\xi^{I_1})$	Confidential information of EU can be obtained by the attacker A after running a Corrupt query
$Execute(\xi^{I_1}_{EU}, \xi^{I_2}_{GCS}, \xi^{I_3}_{UAV})$	The message content can be gathered after execution of this query by attacker A
$Test(\xi^{I_1})$	The original or arbitrary session key decision is done by performing this query by the attacker A
$Reveal(\xi^{I_1}, MSG)$	The session key generated among UAV and EU can be revealed by the attacker A by performing this query.

frequencies and attacker advantage to break Genus-2 discrete logarithm problem (G2CDLP), respectively.

$Proof$: The following four games ($G_i^A | i = 0, 1, 2, 3$) are utilised by the attacker for the Theorem 1 proof as discussed below.

G_0^A : The real attack in this game is carried out by A against G2CAIUN in the ROM by selecting bit b then the semantic security of G2CAIUN provides the following.:

$$Adv_A^{G2CAIUN}(Poly_T) = |2Adv_{A,G_i}^{G2CAIUN} - 1| \tag{3.60}$$

G_1^A : Attacker A plays this game to perform eavesdropping attacks with $Execute$ query during authentication and key agreement stage, Attacker A can obtain all of the information of messages like $MSG_1 = (M_1, M_2, M_3, PBK_{EU}, TS_1), MSG_2 = (M_4, M_5, M_6, TS_2)$, and $MSG_3 = (M_7, AUT_N, TS_3)$. $SK_{UAV \to EU} = h(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}* \parallel TS_3 \parallel RT_2) = SK_{EU \to UAV}$, created among EU and UAV, is obtained by Attacker A with the $Test$, $Reveal$ queries to acquire the shared secret key along with a timestamp and random token, RT_2*, the G2CAIUN protocol employs hash function without collision that protects anonymous ids like OID_{UAV}, OID_{GCS}, and OID'_{EU}. As a result, the shared session key leak is unaffected by an eavesdropping attack, making G_0^A and G_1^A identical, as seen below:

$$Adv_{A,G_0}^{G2CAIUN} = Adv_{A,G_1}^{G2CAIUN} \tag{3.61}$$

G_2^A : In this game, attacker A carries out malevolent actions to get EU secret credentials, including ID_{EU} and $PASS_{EU}$ using a $Corrupt$ query. Furthermore, the G2CDLP math problem and cryptographic hash function difficulty make it impossible to anticipate PRK_{EU} if the attacker manages to get the concealed credentials stored in memory. Furthermore, if hash queries and computational G2CDLP are disregarded, it is difficult to discern between G_2^A and G_2^A. The benefits of calculating G2CDLP and using the birthday paradox to identify hash collisions are as follows:

$$|Adv_{A,G_1}^{G2CAIUN} - Adv_{A,G_2}^{G2CAIUN}| \leq \frac{Hash_Q^2}{2|Hash|} + 2Adv_A^{G2CDLP}(poly_T) \tag{3.62}$$

G_3^A : In this Game , the difference between G_2^A and G_3^A is calculated for the simulation of $PUF(.)$ oracle. Adversary (A) can try to obtain the session key ($SK_{UAV \to EU}$) on verifying M_6* which is calculated by knowing $RES_{UAV}*$ specifically. The adversary repeatedly queries for PUF oracles in order to find $RES_{UAV}*$ and the probability of finding this response is impossible for the adversary, which is shown as:

$$|Adv_{A,G_2}^{G2CAIUN} - Adv_{A,G_3}^{G2CAIUN}| \leq \frac{PUF_Q^2}{2|PUF|} \tag{3.63}$$

Attacker A must imagine bit b' to win the game after completing the $Test$ and all other queries. Then, it becomes clear that,

$$|Adv_{A,G_3}^{G2CAIUN}| \leq \frac{1}{2} \tag{3.64}$$

From equation 3.60 and 3.61, we get

$$\frac{1}{2}Adv_{A}^{G2CAIUN}(poly_T) = |Adv_{A,G_0}^{G2CAIUN} - \frac{1}{2}| \tag{3.65}$$

From equations (3.60)–(3.63),and utilizing triangular inequality, we get

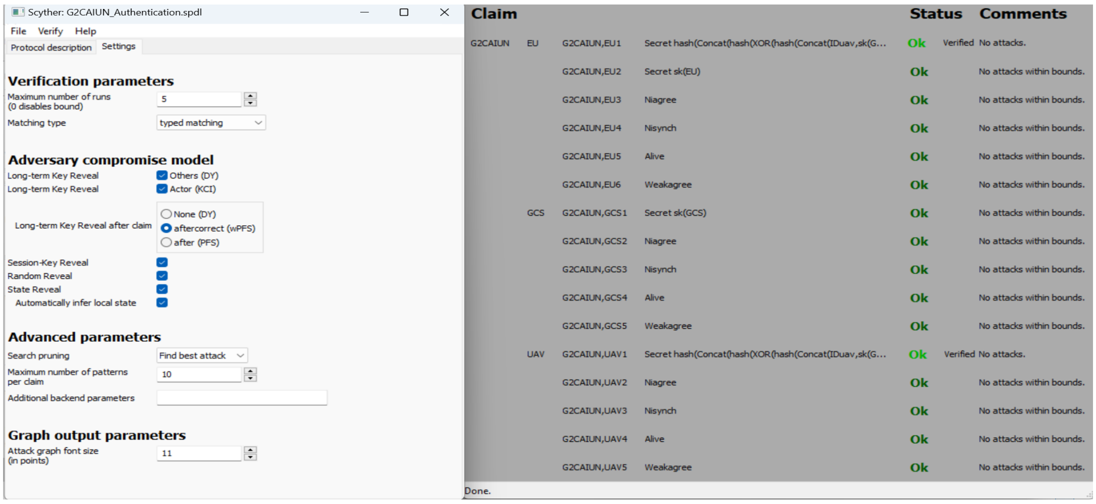
$$\begin{aligned}\frac{1}{2}Adv_{A}^{G2CAIUN}(T_{poly}) &= |Adv_{A,G_0}^{G2CAIUN} - Adv_{A,G_3}^{G2CAIUN}| \\ &= |Adv_{A,G_1}^{G2CAIUN} - Adv_{A,G_2}^{G2CAIUN}| \\ &= |Adv_{A,G_2}^{G2CAIUN} - Adv_{A,G_3}^{G2CAIUN}| \\ &\leq \frac{Hash_Q^2}{2|Hash|} + \frac{PUF_Q^2}{2|PUF|} + Adv_{A}^{G2CDLP}(Poly_T)\end{aligned} \tag{3.66}$$

From equation (3.66), we obtain

$$Adv_{A}^{G2CAIUN}(Poly_T) \leq \frac{Hash_Q^2}{|Hash|} + \frac{PUF_Q^2}{|PUF|} + 2Adv_{A}^{G2CDLP}(Poly_T) \tag{3.67}$$

3.4.1.2 Scyther formal evaluation

The proposed protocol G2CAIUN has been tested using the Scyther tool, which is written in the “Security Protocol Description Language (SPDL)” as described in works [142, 143]. Scyther is crucial in thoroughly analyzing, validating, and faking the protocol’s security characteristics. Scyther, as defined by [143], serves as a mechanism for assessing the core security properties based on the assumption of perfect cryptography. Scyther is utilized widely to show the security viewpoints of any security mechanism in an automated manner. Compared to other security protocol validation tools, such as AVISPA and Proverif, Scyther is more typically adopted by the researcher to verify the security of the suggested authentication and key agreement schemes. There are three roles established in the SPDL script: EU, GCS, and UAV. In addition, there are different claims in SPDL, such as Secret, Niagree, Alive, Nisynch and Weakagree. Secret claim checks for confidentiality; in our case, $claim(EU, Secret, SKeuuav)$ and $claim(EU, Secret, SKuaveu)$ are verified successfully for mutual authentication. Nisynch claim ensures the communicated messages are transferred and received in a synchronised manner to prevent MITM and replay attacks, so $claim(EU, Nisynch), claim(GCS, Nisynch), claim(UAV, Nisynch)$ are analysed with no attacks. Alive claim denotes whether the entity has completed some tasks; thus, $claim(EU, Alive), claim(GCS, Alive), claim(UAV, Alive)$ ensures trustworthiness. Similarly, the Weakagree claim ensures resistance to impersonation attacks, and all these claims ensure better security of G2CAIUN under the DY and CK adversary model settings (Scyther Adversary compromise model), as shown in Figures 3.7 and 3.8, respectively.



Verification parameters

Maximum number of runs (0 disables bound): 5

Matching type: typed matching

Adversary compromise model

Long-term Key Reveal: ☑ Others (DY)

Long-term Key Reveal: ☑ Actor (KCI)

Long-term Key Reveal after claim: ○ None (DY) ● aftercorrect (wPFS) ○ after (PFS)

Session-Key Reveal: ☑

Random Reveal: ☑

State Reveal: ☑

Automatically infer local state: ☑

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

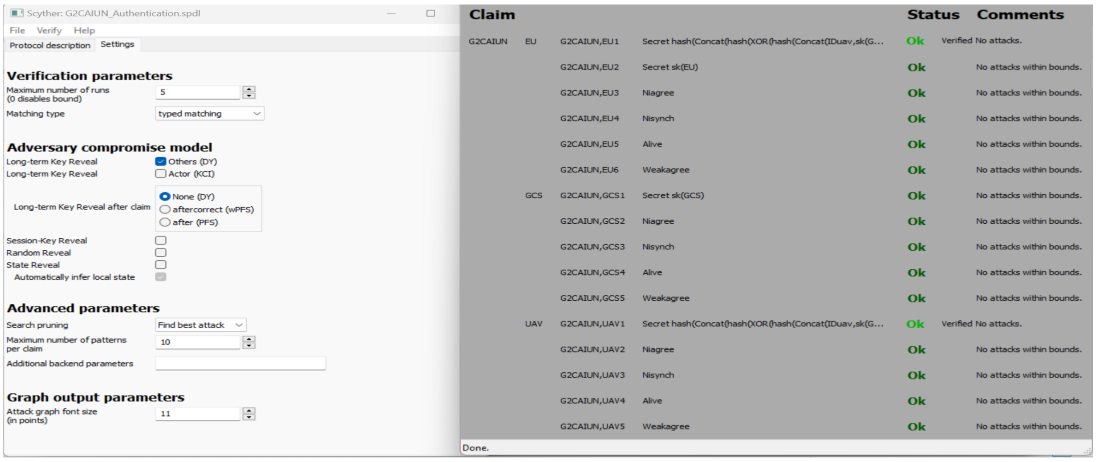
Graph output parameters

Attack graph font size (in points): 11

Claim				Status		Comments
G2CAIUN	EU	G2CAIUN,EU1	Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...	Ok	Verified	No attacks.
		G2CAIUN,EU2	Secret sk(EU)	Ok		No attacks within bounds.
		G2CAIUN,EU3	Niagree	Ok		No attacks within bounds.
		G2CAIUN,EU4	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,EU5	Alive	Ok		No attacks within bounds.
		G2CAIUN,EU6	Weakagree	Ok		No attacks within bounds.
	GCS	G2CAIUN,GCS1	Secret sk(GCS)	Ok		No attacks within bounds.
		G2CAIUN,GCS2	Niagree	Ok		No attacks within bounds.
		G2CAIUN,GCS3	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,GCS4	Alive	Ok		No attacks within bounds.
		G2CAIUN,GCS5	Weakagree	Ok		No attacks within bounds.
	UAV	G2CAIUN,UAV1	Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...	Ok	Verified	No attacks.
		G2CAIUN,UAV2	Niagree	Ok		No attacks within bounds.
		G2CAIUN,UAV3	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,UAV4	Alive	Ok		No attacks within bounds.
		G2CAIUN,UAV5	Weakagree	Ok		No attacks within bounds.

Done.

Figure 3.7: Scyther tool result based on DY model



Verification parameters

Maximum number of runs (0 disables bound): 5

Matching type: typed matching

Adversary compromise model

Long-term Key Reveal: ☑ Others (DY)

Long-term Key Reveal: □ Actor (KCI)

Long-term Key Reveal after claim: ● None (DY) ○ aftercorrect (wPFS) ○ after (PFS)

Session-Key Reveal: □

Random Reveal: □

State Reveal: □

Automatically infer local state: ☑

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 11

Claim				Status		Comments
G2CAIUN	EU	G2CAIUN,EU1	Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...	Ok	Verified	No attacks.
		G2CAIUN,EU2	Secret sk(EU)	Ok		No attacks within bounds.
		G2CAIUN,EU3	Niagree	Ok		No attacks within bounds.
		G2CAIUN,EU4	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,EU5	Alive	Ok		No attacks within bounds.
		G2CAIUN,EU6	Weakagree	Ok		No attacks within bounds.
	GCS	G2CAIUN,GCS1	Secret sk(GCS)	Ok		No attacks within bounds.
		G2CAIUN,GCS2	Niagree	Ok		No attacks within bounds.
		G2CAIUN,GCS3	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,GCS4	Alive	Ok		No attacks within bounds.
		G2CAIUN,GCS5	Weakagree	Ok		No attacks within bounds.
	UAV	G2CAIUN,UAV1	Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...	Ok	Verified	No attacks.
		G2CAIUN,UAV2	Niagree	Ok		No attacks within bounds.
		G2CAIUN,UAV3	Nisynch	Ok		No attacks within bounds.
		G2CAIUN,UAV4	Alive	Ok		No attacks within bounds.
		G2CAIUN,UAV5	Weakagree	Ok		No attacks within bounds.

Done.

Figure 3.8: Scyther tool result based on CK model

3.4.2 Informal Evaluation

It is customary to assess the protocol's safekeeping by informally scrutinizing it for vulnerabilities against a range of potential attacks, affirming its robustness. In this section, we undertake a comprehensive security evaluation of G2CAIUN, specifically focusing on well-established attack scenarios to underscore its security resilience.

3.4.2.1 Replay attack

Attacker A can intercept the messages MSG_1, MSG_2, and MSG_3 by listening to the conversation among entities, which can be prevented by introducing the timestamps such as TS_1, TS_2 and TS_3 and tokens such as RT_1 and RT_2 present in the transmitted messages. The present timestamp T_{pr} is compared with each timestamp received by the entities for its freshness, which ensures resistance against replay attack.

3.4.2.2 Man in the middle attack

Incorporating a hash function denoted as '$h(.)$' and utilising time windows for authentication tokens effectively neutralizes the MITM attack. The adversary wants to capture the communication messages such as MSG_1, MSG_2,
and MSG_3 transferred among entities which are secured using a non-invertible hash function, G2C scalar multiplication. Additionally, $SK_{UAV \to EU}$ is difficult to predict without knowing PUF response $RES_{UAV}*$ and random tokens (RT_1, RT_2). Therefore, the G2CAIUN scheme is protected from MITM attack.

3.4.2.3 Smartphone device attack

During stolen or lost device condition, if somehow an adversary can extract all the stored information Z_{EU}, OID_{EU} in the smartphone device memory due to a power analysis attack, then the adversary cannot be able to calculate actual identity of the user due to the challenging Genus-2 curve scalar multiplication and cryptographic hash digest function.

3.4.2.4 Impersonation attack

The adversary can perform an impersonation attack among EU, GCS and UAV and prevention of these attacks is given as follows:

- UAV impersonation attack prevention
  UAV authentication requests such as $MSG_3 = (M_7, AUT_N, TS_3)$ can be captured by malevolent users to carry out this attack, but it is not feasible for attacker to calculate AUT_N without knowing OIDs, random token and PUF response which makes G2CAIUN scheme to resist UAV impersonation attack.

- EU impersonation attack prevention
  The malevolent user who pretends to be a real user is not able to calculate M_1, M_2, M_3 in the authentication request $MSG_1 = (M_1, M_2, M_3, PBK_{EU}, TS_1)$ due to anonymous OIDs such as OID_{EU}, OID_{GCS} and OID_{UAV}. Additionally, it is not possible for an attacker to guess (PRK_{EU}) to calculate K_{EU} as per G2CDLP. Thus, the G2CAIUN scheme prevents EU impersonation attacks.

- GCS impersonation attack prevention
  The adversary may capture $MSG_2 = (M_4, M_5, M_6, TS_2)$ to carry out this attack by guessing random token RT_1 and timestamp TS_2. Still, it is not possible for the adversary to calculate M_4, M_5 and M_6 due to OIDs such as OID_{GCS}, OID_{UAV}, OID_{EU} and PUF generated response, RES_{UAV}. Therefore, the G2CAUN scheme can resist GCS impersonation attacks.

3.4.2.5 Session key attack

The session key comprises of parameters such as $OID_{UAV}, OID_{GCS}, OID_{EU}*, TS_3$
and RT_2 which are secured with a cryptographic hash algorithm, anonymous identities, random tokens and PUF response which is unclonable and resist attackers to perform session key attack.

3.4.2.6 UAV capture and tampering attack

In the case of a UAV capture attack, an adversary can obtain all the stored information in the local storage such as (OID_{UAV}, ID_{UAV}). Despite this, it is impossible for an attacker to get into the network and calculate OID_{UAV} due to the hash digest and PUF's unique response to challenge and tampering attempt alters unique physical properties, thus making it non-functional.

3.4.2.7 Denial of service attack

In this attack, the adversary sends unlimited illegitimate requests to flood the network, but this attempt fails when each time malevolent users have to log in with incorrect login and password, which leads to an invalid verification $Z^S_{EU}? = Z_{EU}$ due to different Y_{EU} of actual user.

3.4.2.8 Untraceability

The G2CAIUN scheme offers untraceability as it is impractical for an adversary to acquire the original identity of the user from the communicated messages such as MSG_1, MSG_2 and MSG_3. Moreover, to ensure that the message of every participant is unique, the fresh timestamps TS_{pr} and random nonce,RT_1, RT_2, for each session are chosen this way at the authentication, different for each run. It is also difficult to trace the sender. Also, a secure cryptographic hash function hides the true identities of entities.

3.4.2.9 Anonymity preservation

All the communicated messages $(MSG_1, MSG_2$ and $MSG_3)$ during the authentication and key agreement stage are secured with anonymous entity IDs such as OID_{UAV}, OID_{GCS} and OID_{EU} which make it infeasible for an attacker to guess actual identities.

3.4.2.10 Data alteration and integrity

During the authentication and key agreement stage, data alteration cannot be possible by the attacker because there is a strict validation of messages such as $M_3? = M_3^*$, and $M_6? = M_6^*$ at the GCS and UAV side, respectively. Moreover, the prediction of the session key $(SK_{UAV->EU/EU->UAV})$ is not possible due to PUF's unique response and hash digest functionality, which ensures the data integrity of the G2CAIUN scheme.

3.4.2.11 Perfect forward secrecy

As per the forward secrecy, if the current session key becomes compromised, the confidentiality of the previous secret session key must hold, which is achieved by the G2CAIUN scheme due to the unique session key $SK_{UAV->EU/EU->UAV}$ generated for each session with random tokens and PUF unclonable response. Moreover, the freshness of timestamps on the entity side ensures previous sessions stay preserved.

3.4.2.12 Mutual authentication

To achieve mutual authentication, the verification of condition such as $AUT_N? = AUT_N^*$ is applied then session-key $SK_{UAV->EU/EU->UAV} = h(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}{}^* \parallel TS_3 \parallel RT_2)$ is generated which is shared with EU and UAV to securely transmit the data.

3.4.2.13 Eavesdropping attack

The attacker can gain sensitive information like encryption keys by performing an eavesdropping attack. The messages among EU, GCS and UAVs such as $MSG_1 = (M_1, M_2, M_3, PBK_{EU}, TS_1)$, $MSG_2 = (M_4, M_5, M_6, TS_2)$, and $MSG_3 = (M_7, AUT_N, TS_3)$ can be compromised by attacker through eavesdropping but despite of this attempt the session key cannot be obtained by the attacker due to message digest function along with obfuscation identities and random tokens ($OID_{UAV}, OID_{GCS}, OID_{EU}, RT_2$*) and they are not transferred directly. Thus, the proposed protocol is robust against eavesdropping attacks.

3.5 Performance Analysis

G2CAIUN scheme performance is evaluated in the authentication and key agreement stage, and comparative analysis is presented in terms of computation and communication cost with the existing schemes.

3.5.1 Computation Cost

The computation cost of the proposed scheme is evaluated based on the system specification mentioned in the previous literatures [12, 129, 144–146] during the authentication and key agreement stage. We utilise testbed experiment results of previous schemes [12, 129, 144–147], i.e. execution time of different cryptographic primitives such as $T_{ENC/DEC}, T_{PUF}, T_{ECM}, T_{ECA}, T_H, T_{G2CM}, T_{FE}, T_{AE}$ indicates encryption/decryption time $\approx$ 0.036 ms, physical unclonable function time $\approx$ 0.0004 ms, elliptic curve multiplication $\approx$ 0.605 ms, the elliptic curve addition $\approx$ 0.16 ms, one-way hash function $\approx$ 0.029 ms, G2C multiplication $\approx$ 0.48 ms, fuzzy extractor $\approx$ 0.605 ms, authenticated encryption-ASCON time $\approx$ 0.370 ms, respectively. The computation results of the G2CAIUN scheme show a low computation cost (2.55 ms) compared to existing schemes, which is best suited for resource-constrained UAVs and smartphone device users without compromising communication security. Figure 3.9 and Table 3.2 presents the computation analysis comparison.

Table 3.2: Computation cost comparative summary

Schemes	**Yu et al.** [144]	**Tanveer et al.** [145]	**Zhang et al.**[146]	**Tanveer et al.** [129]	**Badshah et al.**[12]	**Proposed G2CAIUN**
EU Side	$4T_{FE} + 12T_H + T_{PUF}(2.768)$	$8T_H + 4T_{ENC} + 3T_{ECM} + T_{FE}(2.796)$	$T_{FE} + 10T_H + 4T_{ECM} + 2T_{ECA}(3.635)$	$5T_{ENC} + 7T_H + 2T_{FE} + T_{PUF}(1.5934)$	$4T_H + 3T_{AE} + T_{PUF}(1.2264)$	$8T_H + 3T_{G2CM}(1.672)$
GCS Side	$9T_H(0.261)$	$5T_H + 3T_{ENC} + T_{ECM}(0.858)$	$5T_H(0.145)$	$4T_{ENC} + 3T_H + T_{FE} + T_{PUF}(0.8364)$	$T_H + 4T_{AE}(1.509)$	$6T_H + 1T_{G2CM}(0.654)$
UAV Side	$T_{FE} + 8T_H + T_{PUF}(0.837)$	$6T_H + 2T_{ENC} + 2T_{ECM}(1.456)$	$4T_H + T_{PUF}(0.116)$	$3T_{ENC} + 5T_H + T_{FE} + T_{PUF}(0.8584)$	$4T_H + 3T_{AE} + T_{PUF}(1.2264)$	$6T_H + T_{PUF}(0.1744)$
Total (ms)	3.605 ms	5.11 ms	3.896 ms	3.288 ms	3.961 ms	2.500 ms

3.5.2 Communication Cost

The communication overhead of the G2CAIUN scheme is calculated based on the size and number of messages shared among the entities such as EU, GCS and UAV in the authentication and key agreement stage. The size of messages such as timestamp,

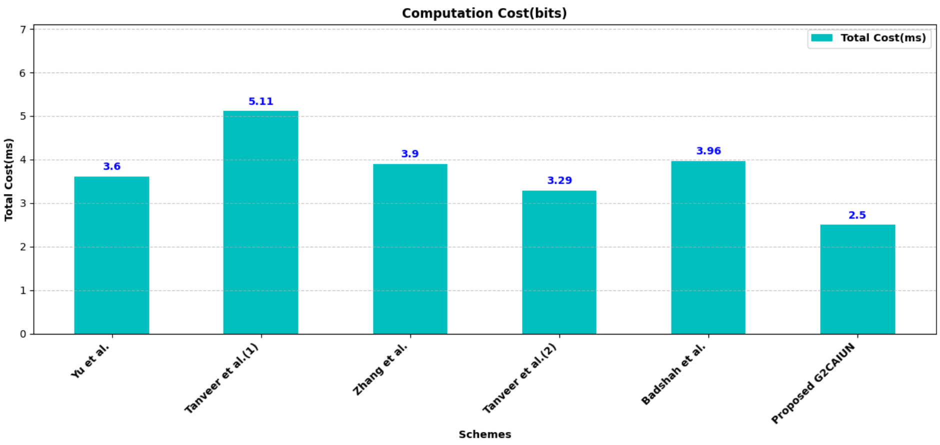


Figure 3.9: Computation cost analysis chart

identity, elliptic curve point, Genus-2 hyperelliptic curve, secure hash function (SHA-1) and a random token is considered 32 bits, 160 bits, 320 bits, 80 bits, 160 bits and 160 bits, respectively. In the G2CAIUN scheme, EU creates and forwards message $MSG_1 = (M_1, M_2, M_3, PBK_{EU}, TS_1)$ to GCS, which leads to the cost of 592 bits. GCS provides message $MSG_2 = (M_4, M_5, M_6, TS_2)$ to UAV, resulting in a cost of 512 bits. UAV generates and forwards the message $MSG_3 = (M_7, AUT_N, TS_3)$ to EU, which leads to a cost of 352 bits. The total communication overhead for G2CAIUN scheme results in 1456 bits which is minimum as compared to recent benchmark schemes [12, 129, 144–146] which is demonstrated in Figures 3.10,3.11 and Table 3.3

Table 3.3: Communication cost comparative summary

Schemes	**Yu et al.** [144]	**Tanveer et al.** [145]	**Zhang et al.**[146]	**Tanveer et al.** [129]	**Badshah et al.**[12]	**Proposed G2CAIUN**
Total Cost (bits)	2048	2240	2816	2272	1696	1456
Messages	4	3	3	3	3	3

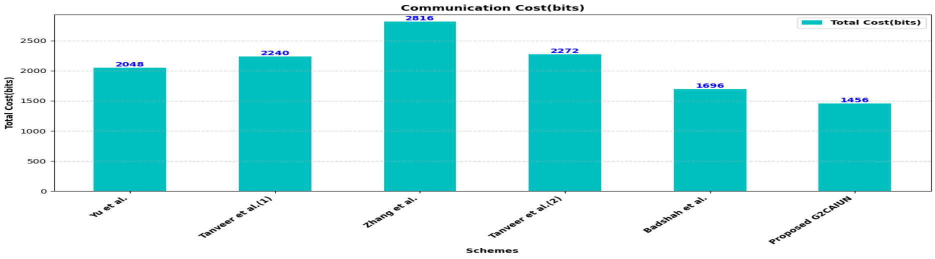


Figure 3.10: Communication cost analysis chart

3.5.3 Security Attributes Comparative Study

Security attributes in protocols are essential for safeguarding data and communication. Key features such as confidentiality, authentication and integrity are required for the robust protocol. Additionally, numerous attacks and other features measure the enhanced security of the G2CAIUN scheme, such as ‘Session key attack’,‘ Denial of service attack’,‘

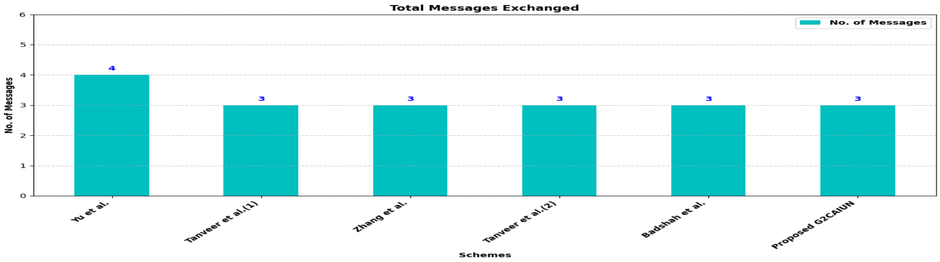


Figure 3.11: Communicated messages count chart

EU, GCS and UAV impersonation attacks', 'Alteration and integrity', 'Dynamic device addition', 'UAV capture and tampering attack', 'Anonymity preservation', 'Smartphone device attack', 'Replay attack', 'Forward secrecy', 'Man in the middle attack', 'Mutual authentication and key agreement', 'Untraceability', 'Formal security evaluation', 'Informal security evaluation'. All the mentioned attributes are analysed in comparison with relevant pertinent schemes [12, 129, 144–146] and described in Table 3.4.

Table 3.4: Security attributes comparative analysis

Attributes	**Yu et al. [144]**	**Tanveer et al. [145]**	**Zhang et al.[146]**	**Tanveer et al. [129]**	**Badshah et al.[12]**	**Proposed G2CAIUN**
ATR_1	○	●	○	●	●	●
ATR_2	· · ·	· · ·	●	●	●	●
ATR_3	○	○	●	●	●	●
ATR_4	●	○	●	●	●	●
ATR_5	○	●	○	○	○	●
ATR_6	○	●	○	○	●	●
ATR_7	●	●	●	●	●	●
ATR_8	●	○	●	●	●	●
ATR_9	●	●	●	●	●	●
ATR_{10}	●	●	○	●	●	●
ATR_{11}	●	○	●	○	○	●
ATR_{12}	●	●	●	●	●	●
ATR_{13}	●	●	●	●	●	●
ATR_{14}	●	●	○	●	●	●
ATR_{15}	●	●	· · ·	· · ·	· · ·	●
ATR_{16}	●	●	●	●	●	●

ATR_1-' Denial of Service attack', ATR_2-'EU, GCS, UAV impersonation attacks', ATR_3-'Integrity',ATR_4-'Session key attack', ATR_5-'Dynamic device addition', ATR_6-'Smartphone device attack', ATR_7-'UAV capture attack', ATR_8-'Tampering attack', ATR_9- 'Anonymity preservation', ATR_{10}-'Replay attack', ATR_{11}-'Perfect forward secrecy', ATR_{12}-'Man in the middle attack', ATR_{13}-'Mutual Authentication and key agreement', ATR_{14}-'Untraceability', ATR_{15}-'Formal security evaluation', ATR_{16}-'Informal security evaluation'. (●) - 'Attribute included', (○)- 'Attribute is not included', (· · ·) - 'partial information'

3.6 Summary

We have proposed the G2CAIUN scheme in this chapter, which employs Genus-2 hyperelliptic curve cryptography, cryptographic hash, XOR, random tokens, and fresh timestamps to protect from well-known attacks along with PUF features to withstand UAV capture and tampering attacks. The proposed scheme uses a Genus-2 curve, which resists the index calculus attack and makes discrete logarithm problems complex and unsolvable. The password update stage, termination and re-issuance stage are discussed to keep the credentials up-to-date for safe communication and resistance against lost devices scenarios. Moreover, an authentic UAV can be part of UAV networks using the UAV augmentation stage. This scheme also offers UAV-GCS and UAV-UAV authentication to disseminate gathered data securely to UAV and authentic users. The performance analysis provides better security and performance with less computation (2.5 ms) and communication cost (1456 bits) compared to related benchmark schemes based on authenticated encryption and elliptic curves and other PUF-based schemes. The formal scyther and informal evaluation results prove the scheme's authenticity under the DY and CK-adversary model to resist attacks like MITM, perfect forward secrecy.

Chapter 4

HCFAIUN: A Novel Hyperelliptic Curve and Fuzzy Extractor-based Authentication for Secure Data Transmission in IoT-based UAV Networks

In this chapter, we have designed a novel lightweight mutual authentication protocol, HCFAIUN, for secure communication in IoT-based UAV Networks using a Hyperelliptic curve (HC) and Fuzzy Extractor (FE), which provides resilient communication in IoT-based UAV networks.

4.1 Introduction

IoT provides unprecedented benefits while introducing new concerns, particularly privacy and security. The word “things” in the context of IoT refers to intelligent objects connected over the Internet with computational, sensory, and actuation capabilities [148]. These intelligent gadgets are pervasive in many aspects of our lives, including typical IT-centric tools like smartphones and laptops and more lifestyle-oriented entities like smart lighting, linked appliances, and electronic personal assistants. A UAV is an unmanned aircraft that can be controlled remotely via a radio communication interface and has an inbuilt programme control unit [149]. With their versatility and simplicity of operation, IoT-based UAV networks eliminate the inherent risks of personal damage or loss.

IoT-based UAV network architecture has three entities: external users (EU), Ground Control Station (GCS) and UAVs. In these networks, UAVs collect data and send it to a GCS. The GCS then sends out commands to control and watch over the drones through wireless connections [16]. IoT-based UAV networks are ubiquitously deployed across diverse sectors, with notable prominence in civil and military spheres. UAVs play crucial roles in studying the earth’s structure, spraying crops, surveillance and monitoring during natural disasters [8, 132, 150]. The fifth-generation (5G) networks are the latest cellular technology with the major benefits in IoT. UAVs can support the network in various ways, such as 5G network slicing [151], acting as base stations or relays during emergencies, or collecting data from IoT devices using various data collection schemes such as graph and AI-based methods [152]. Thus, the UAV-assisted paradigm provides better coordination or fosters connectivity between the EU and GCS in case of network infrastructure flaws.

EU, acting as data consumers, seek real-time access to the information the UAVs acquire via the public Internet. Using public wireless channels for data exchange between the GCS and users introduces vulnerabilities and security risks, including the potential for unauthorised information disclosure. Given the sensitive and critical nature of the information being collected and exchanged between UAVs and the GCS, ensuring information security emerges as a pivotal and intricate challenge in IoT-based UAV networks. Unlike the previous studies that relied on protocols which are not lightweight for resource-constraints UAVs as they use pairing-based cryptography and chaotic maps. Therefore, we have developed a lightweight and safe authentication method called Hyperelliptic Curve and Fuzzy Extractor-based authentication in IoT-based UAV networks (HCFAIUN) employing HC, XOR operations and SHA-1 (Secure Hash Algorithm) hash functions. The maximum key size for HCC is 80 bits, as opposed to the elliptic curve's need of 160 bits, making it suitable for UAVs with limited resources.

This protocol supports the mutual authentication of users and UAVs by allowing them to share a session key for safe interactions and prevent malicious activity of exposing sensitive data by generating biometric traits through FE. The proposed protocol adopts HC scalar multiplication to protect the private key from well-known assaults and identity obfuscation to keep the external user, GCS, and UAVs anonymous. This work excludes the requirement of Physical Unclonable Functions (PUF) [129], which are hardware modules for physical UAV attack prevention because the private key of a UAV is securely stored using a hash function, obfuscation identity, timestamp and random numbers, which prevent attackers from predicting session key between EU and UAVs. HCFAIUN scheme generates separate sessions by creating a unique obfuscation identity of EU and UAVs. The storage overhead of the UAV is also minimised to 160 bits in the authentication stage as compared to existing schemes, thus eliminating its resource limitations. This paper analyses existing authentication systems in a tabular and graphical format utilising security characteristics followed by formal and informal security assessments using the recent Scyther verification tool, Random oracle model and cryptographic primitives, resulting in less computation, communication and storage overheads.

4.1.1 Motivation

In an IoT-based UAV network environment, consider the usual circumstance where the EU want quick access to real-time data directly from a specific UAV. This makes the situation pivotal for protecting the sensitive data and identity of the UAV from adversaries, as this can help them track a UAV by determining its geographical location. There are various security concerns like tampering attacks, replay attacks, man-in-the-middle (MITM) attacks, etc., while communicating among EU, UAVs and GCS. The impact of these security concerns can be seen in various scenarios like smart city environments, including search and rescue, package deliveries, ensuring safety and locating people in emergencies [129]. IoT-based UAVs use a lot of sensors like thermal and imaging sensors, which collect vital data during natural calamities and accidents [152, 153]. This data aids in locating missing individuals and injured victims in adverse conditions, which can be intercepted by adversaries in between public channels instead of transferring the crucial information to the rescue team, resulting in delaying the monitoring scenario. In 2015, Nepal faced a natural disaster, an earthquake that put the lives of 2.8 million people in danger with physical property destruction, and UAVs played a crucial role in transferring the analysed destruction data to GCS. The rough landscape and damaged properties made it hard for UAVs to operate, resulting in frequent interruptions to the precision and reliable data transmitted to GCS. These disruptions stemmed from unauthorised data tampering and natural barriers, which affected the rescue operations by the Nepal army [154]. Therefore, the proposed work endeavours to bridge the existing discrepancies and address the security requirements for securing communication in IoT-based UAV networks. So, we have proposed the HCFAIUN protocol, a lightweight and secure authentication protocol based on the HC for IoT-based UAV networks.

4.1.2 Contribution

In this segment, we elaborate on the proposed HCFAIUN's primary research contributions, which are outlined subsequently.

- Presents a novel lightweight mutual authentication protocol, HCFAIUN, for secure communication in IoT-based UAV Networks by utilising HC.
- Utilises the HC with a maximum key size of 80 bits rather than the elliptic curve key size, i.e., 160 bits, which is useful for resource-constrained UAVs.
- Employs the FE mechanism to generate biometric traits of the user, such as a key which can be reproducible to prevent exposing data from stealing smart devices.
- Employs the HC scalar multiplication to make the private key secure and obfuscation identity to maintain the anonymity of the EU, GCS, and UAVs.
- Comparison with existing authentication methods using security parameters like mutual authentication, un-traceability, etc., in a tabular layout.
- Excludes the requirement of PUF hardware module on UAVs by utilising secure hash function, obfuscation identity, timestamp and random numbers time to prevent the physical attacks.
- The storage overhead of resource-constrained UAVs is reduced to 160 bits compared to established benchmark schemes during the login and authentication stage.
- The security of the HCFAIUN scheme was formally verified using the Scyther tool and Random Oracle Model, ensuring its resistance to various attacks. Informal security analyses have been conducted to underscore the scheme's resilience against potential attacks.
- According to a comparative study, HCFAIUN produces lower computational, communication and storage overheads than existing schemes.

4.2 System Model

This section elucidates two essential models, namely the threat and network model, which are integral to elucidating the functionality and applicability of the devised scheme.

4.2.1 Network Model

Within this architectural framework, the GCS serves as the trusted registration authority responsible for enrolling both drones and users. A drone operates within a designated airspace, collecting data from its immediate surroundings. The network architecture of the formulated framework is depicted in Figure 4.1, featuring three key entities: the GCS, the EU, and the UAVs.

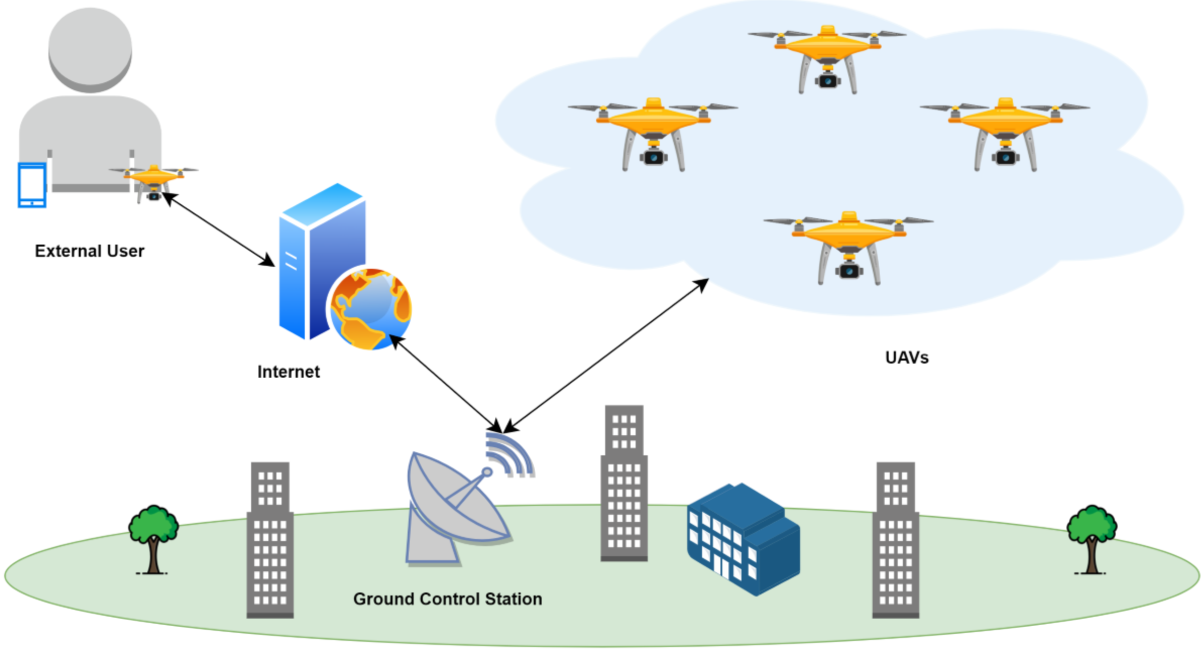


Figure 4.1: Network model

- **GCS:** It is established as a trusted entity responsible for registering all users and drones. The GCS generates long-term secret keys for both EU and UAVs based on their respective identities.
- **EU:** The user having a smart device gets his/her secret key from GCS in the registration phase. Before accessing and communicating with drones on the mission, he/she should be verified.
- **UAVs:** Drones, during the registration phase, receive their secret keys from the GCS as well. Once the validity of the EU is confirmed, the UAV and EU establish a session key to ensure the security of their communication.

4.2.2 Threat Model

Within the scope of this document, we examine two distinct threat models and a concise overview of each is presented herein:

4.2.2.1 DY Threat Model

In the IoT-based UAV Networks environment, we operate under the widely recognized DY (Dolev-Yao) threat model [13]. This model posits that any communication transmitted or received through vulnerable channels can be eavesdropped upon by an adversary denoted as 'A'. Furthermore, A can tamper with the messages by deleting, modifying, or introducing spurious content into the communication stream. It is imperative to note that, following this model, the communication endpoints, in this case, UAVs, do not automatically command dependability on this connection.

4.2.2.2 CK - Adversary Model

We apply the complete CK adversary framework [13] to improve the resilience of our user identification approach, which outperforms the efficacy of the DY threat model typically used in current literature for user authentication techniques. Following the CK-adversary model, adversary 'A' can gain session states and sensitive information, including secret keys and capabilities. It is also believed that this enemy will physically seize selected drones. A may acquire access to all private information on the seized UAVs by using power analysis attacks. UAV capture attacks highlight the concern under the circumstances.

4.2.3 Security Objectives

Given the inherent properties of the authentication mechanism for IoT-based UAV networks. Our suggested scheme must meet the following security requirements to provide reliable and resilient communication. [50, 139, 155–157]

4.2.3.1 Mutual Authentication

This pertains to the process where both users and drones mutually authenticate themselves before transmitting messages through the network channel, thereby verifying their respective identities, which are conveyed alongside the messages.

4.2.3.2 Privacy Protection

Our proposed plan or scheme safeguards users' privacy by ensuring their identities remain confidential. Only authorized counterparts with whom the user has registered possess access to this information. In the event of an adversarial attempt to obtain such information, only encrypted data will be revealed.

4.2.3.3 Un-Traceability

Our scheme guarantees the security of users and drones by providing un-traceability. Should an adversary endeavour to ascertain the locations of drones or users by intercepting the network channel, the untraceability feature will thwart such efforts.

4.2.3.4 Session Key Establishment

Following the effective implementation of the scheme, a session key is generated to facilitate further secure communication between users and drones. For other legitimate users not part of the ongoing session, even if they possess the session key, the adversary cannot access any information.

4.2.3.5 Resilience Against Diverse Threats

To prevent data loss or unauthorized disclosure of user information, our scheme is designed to withstand various attacks, including impersonation attacks, MITM attacks, drone capture attempts, server impersonation, password and biometric modification, message modification, replay attacks, and known session key attacks.

4.3 Proposed Protocol

The proposed protocol encompasses six stages under this section.

4.3.1 Initialization Stage

In this phase, the GCS, operating as a certificate authority, is responsible for generating the public parameters of this scheme along with the confidential key. GCS perform the following steps as mentioned below:

- **Step-1:** Selects a randomly generated numerical value private key, $Pri\_Key_{GCS} \in \{j \mid j \text{ is a positive integer greater than or equal to } 1\}$.
- **Step-2:** The GCS Public Key is calculated as in the equation 4.1:

$$Pub\_Key_{GCS} = Pri\_Key_{GCS}.D \tag{4.1}$$

as D denotes the divisor on a HC.

- **Step-3:** The GCS uses the unidirectional cryptographic hash function '$hash(\cdot)$'. Finally, the ensemble of parameters $\{Pub\_Key_{GCS}, D, n = 280, hash(\cdot)\}$ is made public.

4.3.2 Registration Stage

The GCS performs a complete offline registration process for all UAVs before deployment during this phase and is considered to be storage efficient for credentials. Furthermore, the GCS ensures that users' registrations are safe. The following explanation delves into the registration step.

4.3.2.1 UAV Registration

The GCS enrols all UAVs before being deployed in a certain geographic region. The UAV enrollment process is explained in detail, and Figure 4.2 represents the UAV registration process.

- **Step-1:** The GCS selects a unique identification known as 'ID_{UAV}' for each drone, after which a random number 'α' is chosen from the set of natural numbers 'N' to facilitate computation, and then proceeds to ascertain the corresponding obfuscation identity (OID_{UAV}) using the message digest MD_{UAV} and Pri_Key_{GCS} as in equations (4.2) and (4.3) :

$$MD_{UAV} = hash(ID_{UAV} \parallel \ \alpha) \tag{4.2}$$

$$OID_{UAV} = hash(hash(ID_{UAV} \parallel Pri\_Key_{GCS}) \oplus MD_{UAV})) \tag{4.3}$$

- **Step-2:** The GCS securely retains the identity 'OID_{UAV}' within its proprietary database, establishing a permanent association of the pair (ID_{UAV}, OID_{UAV}) in the memory of the respective UAV.

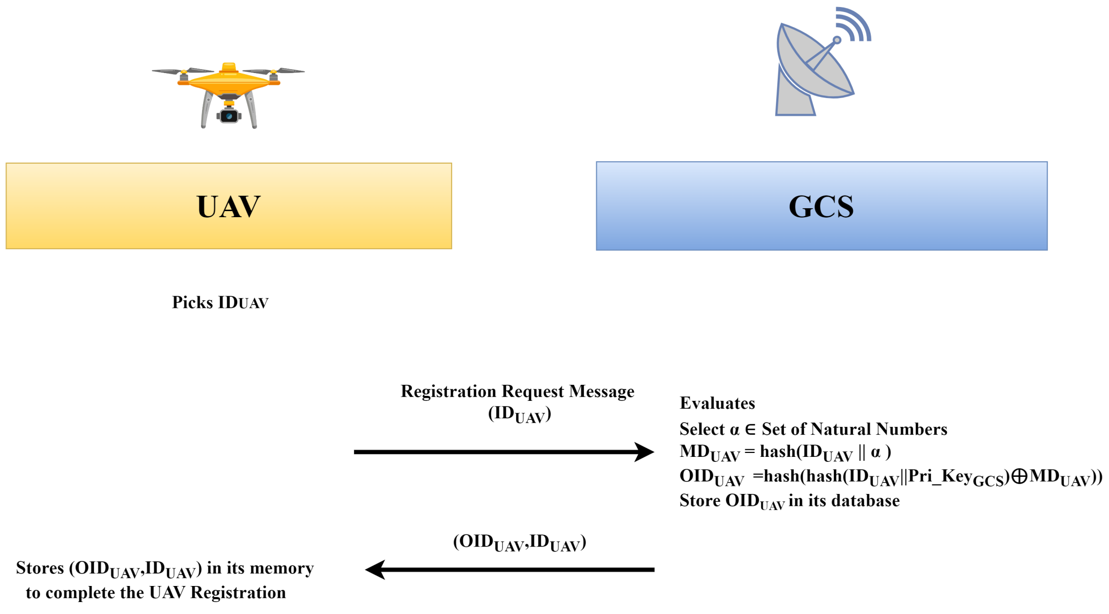

UAV
GCS
Picks IDUAV
Registration Request Message
(ID_{UAV})
Evaluates
Select α ∈ Set of Natural Numbers
MD_{UAV} = hash(ID_{UAV} || α)
OID_{UAV} =hash(hash(ID_{UAV}||Pri_Key_{GCS})⊕MD_{UAV}))
Store OID_{UAV} in its database
(OID_{UAV},ID_{UAV})
Stores (OID_{UAV},ID_{UAV}) in its memory
to complete the UAV Registration

Figure 4.2: UAV registration

4.3.2.2 External User Registration

An EU is enrolled through a secure registration process with the GCS at this stage. The EU can access instantaneous data by a specified UAV flying inside a particular aerial zone upon completing the enrollment. The GCS and EU performs the following operations as mentioned below:

- **Step-1:** EU selects an exclusive identifier ID_{EU}’ and a corresponding password $PASS_{EU}$’, after which EU engraves his/her biometric traits (BT_{EU}) such as iris and fingerprint into a sensor of smart device and a random number ‘μ’ is chosen from the set of natural numbers ‘N’ to facilitate the computation as given in equations (4.4) and (4.5):

$$Gen(BT_{EU}) = (\gamma_{EU}, hd) \tag{4.4}$$

$$Y_{EU} = hash(ID_{EU} \parallel PASS_{EU} \parallel \mu \parallel \gamma_{EU}) \tag{4.5}$$

- **Step-2:** Upon the reception of the message, GCS proceeds to calculate OID_{EU} and Z_{EU}, as in equations (4.6) and (4.7):

$$OID_{EU} = hash(ID_{EU} \parallel Pri\_Key_{GCS}) \tag{4.6}$$

$$Z_{EU} = hash(OID_{EU} \parallel Y_{EU}) \tag{4.7}$$

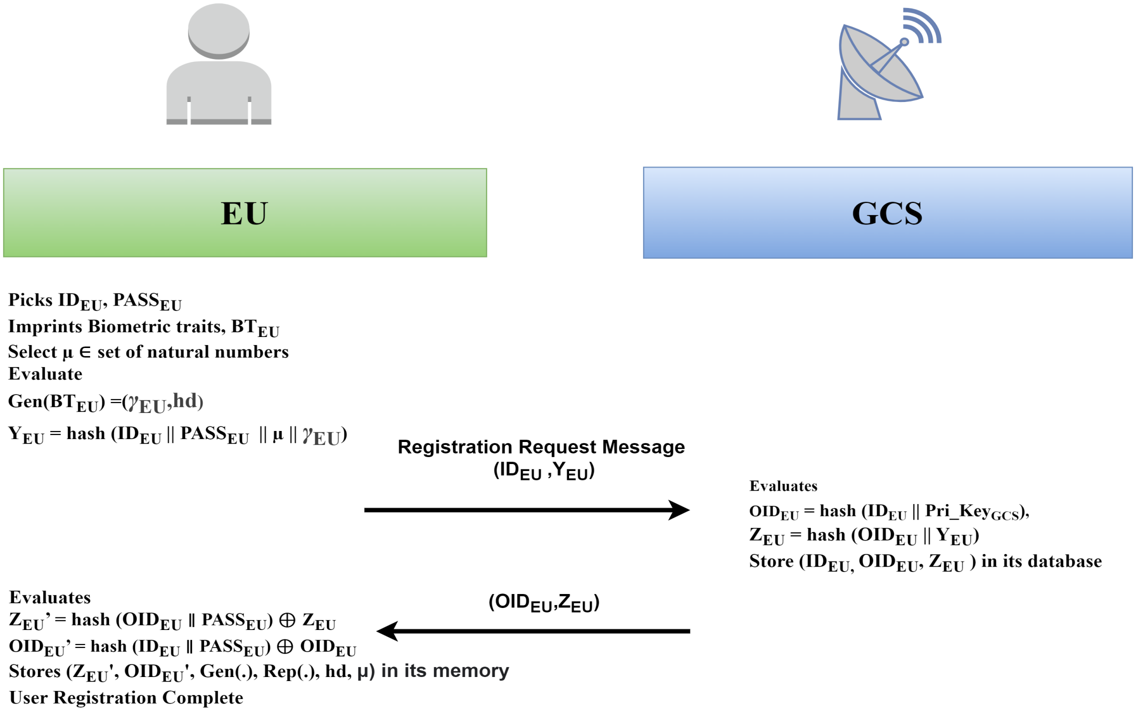
Subsequently, GCS records (ID_{EU}, OID_{EU}, Z_{EU}) within its database, and securely transmits (OID_{EU}, Z_{EU}) to EU via a protected communication channel.

- **Step-3:** Upon receiving the information from GCS, EU performs the computation as in equations (4.8) and (4.9)

$$Z_{EU}' = hash(OID_{EU} \parallel PASS_{EU} \parallel \gamma_{EU}) \oplus Z_{EU} \tag{4.8}$$

$$OID_{EU}' = hash(ID_{EU}||PASS_{EU}) \oplus OID_{EU} \tag{4.9}$$

  In conclusion, EU archives the information μ, Z_{EU}', OID_{EU}' in its device's local memory, marking the completion of the enrolment phases and Figure 4.3 represents the external user enrollment steps.



EU
GCS
Picks ID_{EU}, $PASS_{EU}$
Imprints Biometric traits, BT_{EU}
Select $\mu \in$ set of natural numbers
Evaluate
$Gen(BT_{EU}) = (\gamma_{EU}, hd)$
$Y_{EU} = hash(ID_{EU} \parallel PASS_{EU} \parallel \mu \parallel \gamma_{EU})$
Registration Request Message
(ID_{EU}, Y_{EU})
Evaluates
$OID_{EU} = hash(ID_{EU} \parallel Pri\_Key_{GCS})$,
$Z_{EU} = hash(OID_{EU} \parallel Y_{EU})$
Store $(ID_{EU}, OID_{EU}, Z_{EU})$ in its database
(OID_{EU}, Z_{EU})
Evaluates
$Z_{EU}' = hash(OID_{EU} \parallel PASS_{EU}) \oplus Z_{EU}$
$OID_{EU}' = hash(ID_{EU} \parallel PASS_{EU}) \oplus OID_{EU}$
Stores $(Z_{EU}', OID_{EU}', Gen(.), Rep(.), hd, \mu)$ in its memory
User Registration Complete

Figure 4.3: External user registration

4.3.3 Login and Authentication Stage

An External user, denoted as EU, initiates the access and verification phase within the proposed approach to establish a secure communication channel and obtain authorization. This section offers a comprehensive elaboration on the intricacies of this particular stage.

- **Step-1:** EU is obligated to furnish their identification, denoted as ID_{EU}, and their respective password indicated as $PASS_{EU}$ with biometric traits as BT_{EU}* into smart device prior to initiate the computation as in equations (4.10)–(4.13),

$$\gamma_{EU}{}^* = Rep(BT_{EU}{}^*, hd) \tag{4.10}$$

$$Y_{EU}^S = hash(hash(ID_{EU} \parallel \mu \parallel \gamma_{EU}{}^*) \oplus hash(PASS_{EU} \parallel \mu \parallel \gamma_{EU}{}^*)) \tag{4.11}$$

$$OID_{EU}\text{S} = hash(ID_{EU} \parallel Pub\_Key_{GCS}) \tag{4.12}$$

$$Z_{EU}^{S} = hash(OID_{EU}^{S} \parallel Y_{EU}^{S}). \tag{4.13}$$

Now prove ($Z_{EU}^{S}? = Z_{EU}$). In the event of unsuccessful verification, the procedure is promptly terminated. Otherwise, EU generates Pub_Key_{GCS} and a timestamp TS_1 to calculate the following equations (4.14)–(4.18):

$$Pub\_Key_{GCS} = Pri\_Key_{EU}.D \tag{4.14}$$

$$K_{EU} = Pri\_Key_{EU}.Pub\_Key_{GCS} \tag{4.15}$$

$$EU_1 = OID_{EU} \oplus hash(OID_{GCS} \,||\, TS_1) \tag{4.16}$$

$$EU_2 = OID_{UAV} \oplus hash(OID_{GCS} \;\parallel\; TS_1 \;\parallel\; K_{EU}) \tag{4.17}$$

$$EU_3 = hash(OID_{EU} \;\parallel\; OID_{GCS} \;\parallel\; OID_{UAV} \;\parallel\; K_{EU} \;\parallel\; TS_1) \tag{4.18}$$

Subsequently, the authentication message request, denoted as $M_1 = (EU_1, EU_2, EU_3, Pub\_Key_{EU}, TS_1)$ is transmitted over a public channel and is subject to subsequent analysis by the GCS.

- **Step-2:** Upon receipt of the authentication request message by the GCS, i.e. $M_1 = (EU_1, EU_2, EU_3, Pub\_Key_{EU}, TS_1)$, GCS initially assesses the validity of TS_1 through verification. ($|TS_{cur} - TS_1| \leq \tau$), where τ represents the threshold time receiving the information, and on successful verification, the GCS will calculate the following based on the current message time (TS_{cur}) as in equation (4.19).

$$K_{GCS} = Pub\_Key_{EU}.Pri\_Key_{GCS} \tag{4.19}$$

With this value as a starting point, GCS proceeds to perform the subsequent calculations as in equations (4.20)–(4.22) :

$$OID_{EU}{*} = EU_1 \oplus hash(OID_{GCS} \parallel TS_1) \tag{4.20}$$

$$OID_{UAV}{*} = EU_2 \oplus hash(OID_{EU}{*} \parallel TS_1 \parallel K_{GCS}) \tag{4.21}$$

$$EU_3{*} = hash(OID_{EU}{*} \parallel OID_{UAV}{*} \parallel OID_{GCS}{*} \parallel K_{GCS} \parallel TS_1) \tag{4.22}$$

GCS checks if the condition ($EU_3? = EU_3{*}$) is valid. In the event of an invalid request, the GCS will decline the authentication request. If the request is valid, GCS can proceed with the EU authentication and subsequently execute the following equations (4.23)–(4.25).

$$B_1 = hash(OID_{UAV}{*} \parallel TS_2) \oplus R_1 \tag{4.23}$$

$$B_2 = OID_{EU}{*} \oplus hash(OID_{UAV}{*} \parallel OID_{GCS}{*} \parallel TS_2 \parallel R_1) \tag{4.24}$$

$$B_3 = hash(OID_{UAV}{*} \parallel OID_{GCS} \parallel OID_{EU}{*} \parallel TS_2 \parallel R_1) \tag{4.25}$$

Ultimately, GCS transmits message M_2 to the UAV via a publicly accessible communication channel, comprising elements B_1, B_2, B_3 and TS_2

- **Step-3:** UAV validates recent content by confirming that the $|TS_{cur} - TS_2| \leq \tau$ after receiving and If this validation is successful, the drone, denoted as a UAV, proceeds to initiate the following equations (4.26)–(4.28) computations:

$$R_1{*} = B_1 \oplus hash(OID_{UAV} \parallel TS_2) \tag{4.26}$$

$$OID_{UAV}{*} = B_2 \oplus hash(OID_{UAV} \parallel OID_{GCS} \parallel TS_2 \parallel R_1{*}) \tag{4.27}$$

$$B_3{*} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}{*} \parallel TS_2 \parallel R_1{*}) \tag{4.28}$$

It additionally verifies if $(B_3? = B_3{*})$ to establish the authenticity of GCS. In the event of failure, the session is promptly terminated. However, if the verification is successful, it generates a random number, denoted as R_2, based on the current timestamp, TS_3, before advancing to the subsequent stages as in equations (4.29)–(4.31).

$$U_1 = hash(OID'_{UAV}{*} \parallel OID_{UAV} \parallel TS_3) \oplus R_2 \tag{4.29}$$

$$Sess\_Key_{UAV \to EU} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID'_{EU}{*} \parallel TS_3 \parallel R_2) \tag{4.30}$$

$$AUT_N = hash(Sess\_Key_{UAV \to EU} \parallel TS_3) \tag{4.31}$$

Conclusively, the UAV directly transmits message M_3, comprising elements U_1, AUT_N, and TS_3, to the EU via a publicly accessible communication channel.

- **Step-4:** Following the reception of a message M_3, EU initiates the process by verifying the recent time through decision $|TS_{cur} - TS_3| <= \tau$. If the decision proves to be legitimate, EU proceeds to compute $R_2{*}, AUT_N{*}$, the session key, denoted as $(Sess\_Key_{EU \to UAV})$, in the following equations (4.32)–(4.34):

$$R_2{*} = U_1 \oplus hash(OID_{EU} \parallel OID_{GCS} \parallel TS_3) \tag{4.32}$$

$$Sess\_Key_{EU \to UAV} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU} \parallel TS_3 \parallel R_2{*}) \tag{4.33}$$

$$AUT_N{*} = hash(Sess\_Key_{EU \to UAV} \parallel TS_3) \tag{4.34}$$

The EU performs an additional check to confirm the equivalence of AUT_N* and AUT_N. When these values match, it signifies the successful mutual authentication of the user EU and the UAV, and the calculated session key is stored for subsequent secure communication. Conversely, if (AUT_N*) and (AUT_N) do not match, EU promptly terminates the session. Figure 4.4 shows the steps involved in the login and authentication stage.

4.3.4 Password Modification Stage

In a secure authentication framework, a procedure for password modification should be accessible. This allows an authorized user, denoted as EU, utilizing a smart device, to replace the existing password $PASS_{EU}$ with a new one, referred to as $PASS_{EU}^N$ and biometric traits as BT_{EU}^N. To effect this change, the EU is required to carry out the following actions:

- **Step-1:** EU initiates the process by entering their login credentials, comprising identity ID_{EU}, password $PASS_{EU}$ and biometric traits as $BT_{EU}*$. Subsequently, the smartphone device performs the ensuing computational tasks
as in equations (4.35), (4.37) and (4.38).

$$\gamma_{EU} = Rep(BT_{EU}*, hd) \tag{4.35}$$

$$Y_{EU}^S = hash(hash(ID_{EU} \parallel \mu \parallel \gamma_{EU}) \oplus hash(PASS_{EU} \parallel \mu \parallel \gamma_{EU})) \tag{4.36}$$

$$OID_{EU}^S = hash(ID_{EU} \parallel Pub\_Key_{GCS}) \tag{4.37}$$

$$Z_{EU}^S = hash(OID_{EU}^S \parallel Y_{EU}^S) \tag{4.38}$$

The smart device subsequently verifies the validity of the condition ($Z_{EU}^S == Z_{EU}$), and if it proves invalid, the procedure is terminated. In contrast, when the condition proves valid, the device prompts the EU to furnish a fresh password as a requisite step in finalizing the process.

- **Step-2:** EU opts for a fresh password denoted as $PASS_{EU}^N$ with biometric traits as BT_{EU}^N and transmits it. Subsequently, the smart device performs the subsequent computations as in equations (4.40)–(4.42).

$$Gen(BT_{EU}^N) = (\gamma_{EU}^N, hd^N) \tag{4.39}$$

$$Y_{EU}^N = hash(hash(ID_{EU} \parallel \mu \parallel \gamma_{EU}^N) \oplus hash(PASS_{EU}^N \parallel \mu \parallel \gamma_{EU}^N)) \tag{4.40}$$

$$OID_{EU} = hash(ID_{EU}^N, Pri\_Key_{GCS}) \tag{4.41}$$

$$Z_{EU}^N = hash(OID_{EU} \parallel Y_{EU}^N) \tag{4.42}$$

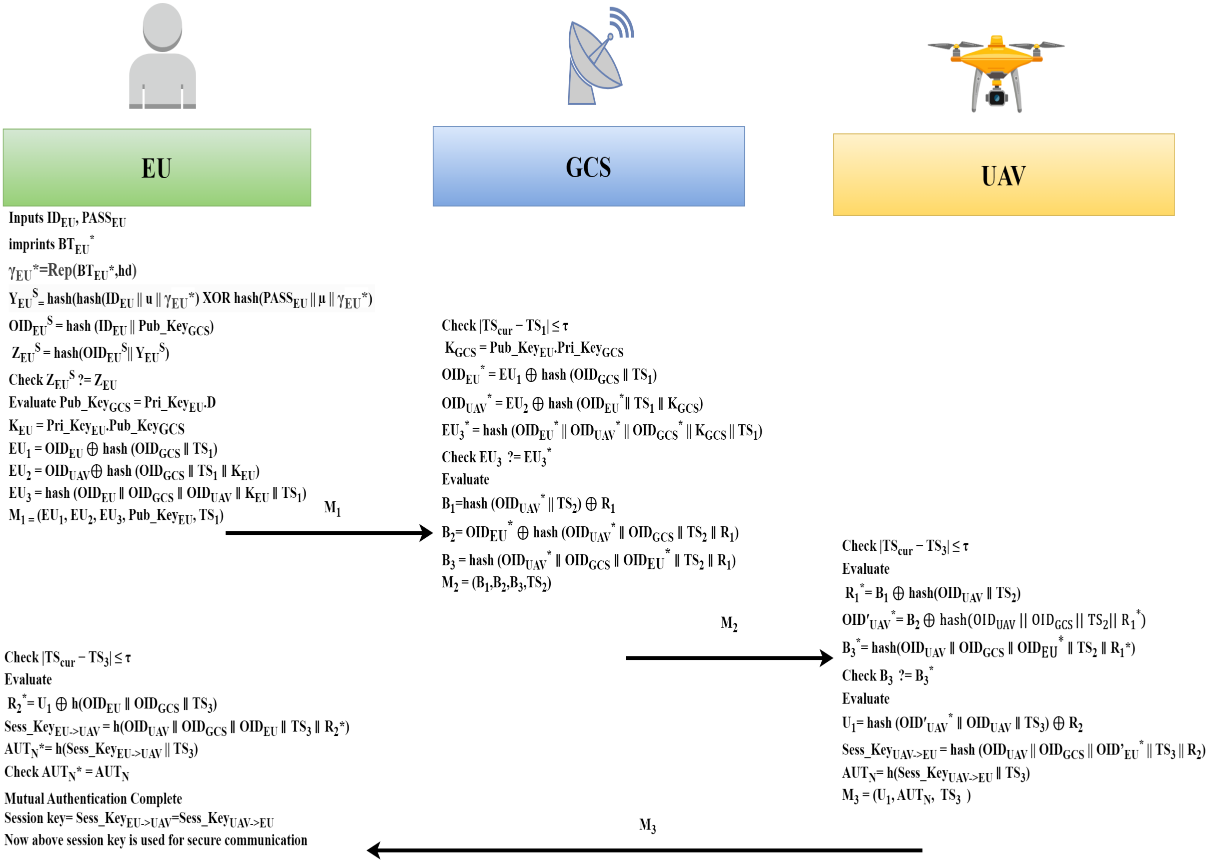

EU
GCS
UAV
Inputs ID_{EU}, $PASS_{EU}$
imprints BT_{EU}^{*}
γ_{EU}^{*}=Rep(BT_{EU}^{*},hd)
Y_{EU}^{S}= hash(hash(ID_{EU} || u || γ_{EU}^{*}) XOR hash($PASS_{EU}$ || μ || γ_{EU}^{*})
OID_{EU}^{S} = hash (ID_{EU} || Pub_Key_{GCS})
Z_{EU}^{S} = hash(OID_{EU}^{S}|| Y_{EU}^{S})
Check Z_{EU}^{S} ?= Z_{EU}
Evaluate Pub_Key_{GCS} = Pri_Key_{EU}.D
K_{EU} = Pri_Key_{EU}.Pub_Key_{GCS}
EU_1 = OID_{EU} ⊕ hash (OID_{GCS} ‖ TS_1)
EU_2 = OID_{UAV}⊕ hash (OID_{GCS} ‖ TS_1 ‖ K_{EU})
EU_3 = hash (OID_{EU} ‖ OID_{GCS} ‖ OID_{UAV} ‖ K_{EU} ‖ TS_1)
M_1 = (EU_1, EU_2, EU_3, Pub_Key_{EU}, TS_1)
M_1
Check $|TS_{cur} - TS_1| \leq \tau$
K_{GCS} = Pub_Key_{EU}.Pri_Key_{GCS}
OID_{EU}^{*} = EU_1 ⊕ hash (OID_{GCS} ‖ TS_1)
OID_{UAV}^{*} = EU_2 ⊕ hash (OID_{EU}^{*}‖ TS_1 ‖ K_{GCS})
EU_3^{*} = hash (OID_{EU}^{*} || OID_{UAV}^{*} || OID_{GCS}^{*} || K_{GCS} || TS_1)
Check EU_3 ?= EU_3^{*}
Evaluate
B_1=hash (OID_{UAV}^{*} || TS_2) ⊕ R_1
B_2= OID_{EU}^{*} ⊕ hash (OID_{UAV}^{*} ‖ OID_{GCS} ‖ TS_2 ‖ R_1)
B_3 = hash (OID_{UAV}^{*} ‖ OID_{GCS} ‖ OID_{EU}^{*} ‖ TS_2 ‖ R_1)
M_2 = (B_1,B_2,B_3,TS_2)
M_2
Check $|TS_{cur} - TS_3| \leq \tau$
Evaluate
R_1^{*}= B_1 ⊕ hash(OID_{UAV} ‖ TS_2)
$OID'_{UAV}{}^{*}$= B_2 ⊕ hash(OID_{UAV} || OID_{GCS} || TS_2|| R_1^{*})
B_3^{*}= hash(OID_{UAV} ‖ OID_{GCS} ‖ OID_{EU}^{*} ‖ TS_2 ‖ R_1*)
Check B_3 ?= B_3^{*}
Evaluate
U_1= hash ($OID'_{UAV}{}^{*}$ ‖ OID_{UAV} ‖ TS_3) ⊕ R_2
$Sess\_Key_{UAV\text{->}EU}$ = hash (OID_{UAV} || OID_{GCS} || $OID'_{EU}{}^{*}$ || TS_3 || R_2)
AUT_N= h($Sess\_Key_{UAV\text{->}EU}$ ‖ TS_3)
M_3 = (U_1, AUT_N, TS_3)
M_3
Check $|TS_{cur} - TS_3| \leq \tau$
Evaluate
R_2^{*}= U_1 ⊕ h(OID_{EU} ‖ OID_{GCS} ‖ TS_3)
$Sess\_Key_{EU\text{->}UAV}$ = h(OID_{UAV} ‖ OID_{GCS} ‖ OID_{EU} ‖ TS_3 ‖ R_2*)
AUT_N*= h($Sess\_Key_{EU\text{->}UAV}$ || TS_3)
Check AUT_N* = AUT_N
Mutual Authentication Complete
Session key= $Sess\_Key_{EU\text{->}UAV}$=$Sess\_Key_{UAV\text{->}EU}$
Now above session key is used for secure communication

Figure 4.4: Login and Authentication Stage

- **Step-3:** Ultimately, the EU substitutes Z_{EU}^{N} with Z_{EU} using a smart device. Finally, it is essential to remember that EU credentials may be subject to periodic revisions to improve the safety mechanism.

4.3.5 Withdrawal and Renewal Stage

The external user, denoted as EU, encounters the unfortunate circumstance of their smart device being lost or stolen, EU retains the capability to initiate a replacement procedure and diligently adhere to the prescribed instructions outlined below:

- **Step-1:** EU maintains his ID_{EU} identity while opting for $PASS_{EU}^{N}$ as his updated password with biometric traits (BT_{EU}^{N}). Subsequently, employing a randomly generated number μ', EU proceeds with the computation as in equations (4.43) and (4.44).

$$Gen(BT_{EU}^{N}) = (\gamma_{EU}^{N}, hd^{N}) \tag{4.43}$$

$$Y_{EU}^{N} = hash(hash(ID_{EU} \parallel \mu' \parallel BT_{EU}^{N}) \oplus hash(PASS_{EU}^{N} \parallel \mu' \parallel BT_{EU}^{N})) \tag{4.44}$$

and conveys ID_{EU} and Y_{EU}^{N} to the GCS through a secure communication medium.

- **Step-2:** The GCS calculates OID_{EU} and Z^N_{EU} upon reception of the message in the manner as given in equations (4.45) and (4.46).

$$OID_{EU} = hash(ID_{EU} \parallel Pri\_Key_{GCS}) \tag{4.45}$$

$$Z^N_{EU} = hash(OID_{EU} \parallel Y^S_{EU}) \tag{4.46}$$

Subsequently, the GCS archives OID_{EU} and Z^N_{EU} within its storage and securely transmits the same data to the EU via a protected communication channel.

- **Step-3:** After receiving the data from the GCS, EU engages in the computation process as in equations (4.47) and (4.48)

$$Z^N_{EU}{}^* = hash(OID_{EU} \parallel Y^N_{EU}) \oplus Z^N_{EU} \tag{4.47}$$

$$OID_{EU}{}^* = hash(OID_{EU} \parallel PASS^N_{EU}) \oplus OID_{EU} \tag{4.48}$$

In conclusion, EU substitute Z_{EU} with Z^N_{EU} and archives $Z^N_{EU}{}^*$, $OID_{EU}{}^*$ in its local device's memory. Furthermore, EU expunges Z'_{EU} from the device's memory, finalizing the revocation and re-issuance procedure.

4.3.6 Scalable UAV Stage

In unforeseen incidents, such as situations involving depleted battery levels or UAV capture by a potential adversary, the prompt deployment of an alternative drone within the same operational airspace becomes paramount. In this regard, the proposal enables the inclusion of the latest aircraft into the infrastructure. This process closely mirrors the drone registration phase, and a more comprehensive delineation of this particular phase is presented below.

- **Step-1:** To enable the utilization of a new UAV, which has not yet been registered, within a specific airspace, the GCS selects an individualized identity, ID^N_{UAV} and subsequently calculates the associated obfuscated identity as in equation (4.49):

$$OID^N_{UAV} = hash(ID^N_{UAV} \parallel Pri\_Key_{GCS}) \tag{4.49}$$

- **Step-2:** The GCS archives ID^N_{UAV}, OID^N_{UAV} within the UAV storage before its deployment in the operational field, while also retaining ID^N_{UAV} in its current record.

4.4 Security Assessment

This section examines the security aspects of the HCFAIUN scheme. To begin with, we demonstrate HCFAIUN 's security by utilising the Scyther tool. Following this, we assess the security characteristics to confirm that HCFAIUN is strongly resistant to various potential attacks.

4.4.1 Formal Security Assessment

The proposed protocol HCFAIUN has been tested using the Scyther tool and Random Oracle model, which are the following:

4.4.1.1 Scyther tool-based Security Assessment

The proposed protocol HCFAIUN has been tested using the Scyther tool, which is written in the "Security Protocol Description Language (SPDL)" as described in works [142]. The primary aim of the simulation is to validate the security aspects related to authentication, confidentiality, and integrity. In this context, the Scyther tool characterizes the entities involved as roles within the proposed protocol. Scyther is instrumental in verifying, falsifying, and comprehensively analysing the security features of the protocol. Scyther serves as a mechanism for assessing the core security properties based on the assumption of perfect cryptography [129]. It's worth noting that when using the Scyther tool, potential attackers cannot execute security attacks on encrypted messages unless they possess the decryption key. Contrasting with the DY model presented by Dolev and Yao in 1983, where attackers had absolute control over communication entities, in the scenario involving the Scyther tool, adversaries are constrained from capturing, altering, or deleting transmissions across the network unless they can derive new information from their existing knowledge. The protocol was analyzed on a system configuring 12th Gen Intel(R) Core(TM) i5-1240P 1.70 GHz, 8 GB RAM, and a 64-bit Windows 11 operating system. The Scyther tool employs claims to articulate and define the security requisites. These claims encompass a range of criteria, including Nisynch, Secret, Niagree, Alive, and Weakagree.

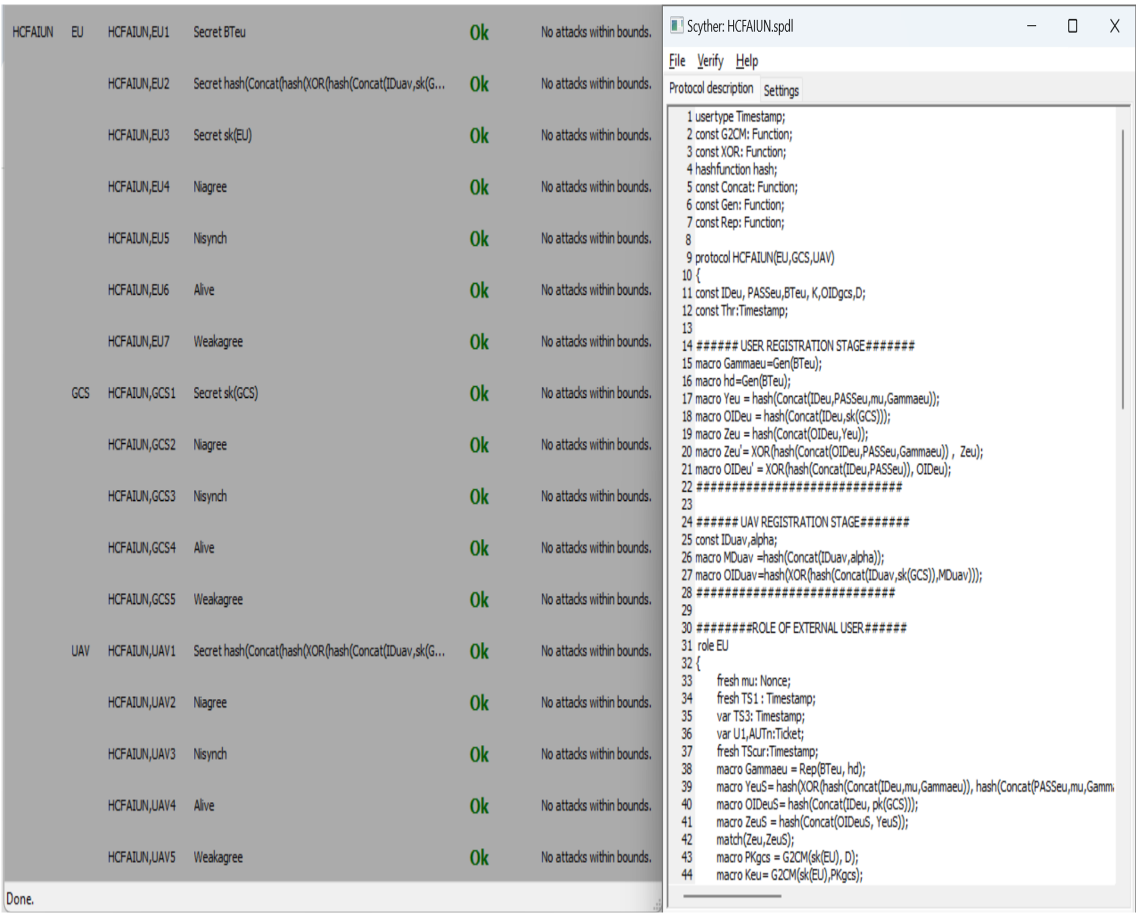
- **Secret:** The objective is to establish confidentiality measures that facilitate secure communication between the two participating parties. From the figure, it is clear that claim(EU, Secret, Keuuav), claim(GCS, Secret,sk(GCS)), and claim(UAV, Secret, Kuaveu) represent the shared session key, which is confidential for secure communication, helps prevent session key attacks, and helps achieve mutual authentication.

- **Niagree:** The establishment of a non-injective agreement with a role concerning a set of data items can be achieved through the inclusion of the relevant signal claims like claim(EU, Niagree), claim(GCS, Niagree), and claim(UAV, Niagree), which prevents from tampering, smart device attack and provides mutual authentication.

- **Nisynch:** All processes related to data transmission and network sessions involving the entities must adhere rigorously to the security regulations delineated within the proposed protocol. It is paramount that all participating entities diligently uphold synchronization with their current operational states. From the figure, it is clear that claim(EU, Nisynch), claim(GCS, Nisynch), and claim(UAV, Nisynch) represent all entities that can send and receive all messages which will prevent replay and MITM attacks.

- **Alive:** The aim is to ensure a robust authentication process between the designated parties, focusing on enabling the execution of specific tasks by an intended communication partner. From the simulation results, it was found that claim(EU, Alive), claim(GCS, Alive), and claim(UAV, Alive) represent the trust among the entities, and each entity talks to the intended communicating partner.

- **Weakagree:** In professional terminology, one can assert that a protocol provides a form of weak agreement to an initiating party denoted as 'A' concerning another party, referred to as 'B', when it ensures that whenever 'A' assumes the role of the initiator and successfully concludes a protocol session, ostensibly involving 'B' as the responder, it is implied that 'B' had been engaged in a prior execution of the same protocol, seemingly with 'A' as the initiator. In the domain of SPDL programming, which facilitates input provision to the Scyther tool, security assertions are appended to the conclusion of each role. These assertions serve as essential criteria enabling entities to assess whether the protocol has successfully passed the verification process as intended and whether the predefined security goals have been achieved. From the simulation result, it is clear that the claim(EU, Weakagree), claim(UAV, Weakagree), and claim(GCS, Weakagree) represent an impersonation attack that an adversary cannot perform. Scyther conducts a comprehensive assessment of security claims within the protocol. In identifying any security vulnerabilities or attacks, it presents a graphical representation of the security breach. To elaborate, Scyther specifically scrutinises secrecy and authentication aspects in the context of security protocols. The proposed framework has been implemented, encompassing three fundamental roles: EU, GCS, and UAVs. The system model of mutual authentication in IoT-based UAV Networks will satisfy the above-mentioned claims for security requirements using the simulation of the proposed protocol, as shown in Figure 4.5.



```
HCFAIUN  EU   HCFAIUN,EU1    Secret BTeu                                           Ok   No attacks within bounds.
              HCFAIUN,EU2    Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...  Ok   No attacks within bounds.
              HCFAIUN,EU3    Secret sk(EU)                                         Ok   No attacks within bounds.
              HCFAIUN,EU4    Niagree                                               Ok   No attacks within bounds.
              HCFAIUN,EU5    Nisynch                                               Ok   No attacks within bounds.
              HCFAIUN,EU6    Alive                                                 Ok   No attacks within bounds.
              HCFAIUN,EU7    Weakagree                                             Ok   No attacks within bounds.
         GCS  HCFAIUN,GCS1   Secret sk(GCS)                                        Ok   No attacks within bounds.
              HCFAIUN,GCS2   Niagree                                               Ok   No attacks within bounds.
              HCFAIUN,GCS3   Nisynch                                               Ok   No attacks within bounds.
              HCFAIUN,GCS4   Alive                                                 Ok   No attacks within bounds.
              HCFAIUN,GCS5   Weakagree                                             Ok   No attacks within bounds.
         UAV  HCFAIUN,UAV1   Secret hash(Concat(hash(XOR(hash(Concat(IDuav,sk(G...  Ok   No attacks within bounds.
              HCFAIUN,UAV2   Niagree                                               Ok   No attacks within bounds.
              HCFAIUN,UAV3   Nisynch                                               Ok   No attacks within bounds.
              HCFAIUN,UAV4   Alive                                                 Ok   No attacks within bounds.
              HCFAIUN,UAV5   Weakagree                                             Ok   No attacks within bounds.
Done.
```

```
usertype Timestamp;
const G2CM: Function;
const XOR: Function;
hashfunction hash;
const Concat: Function;
const Gen: Function;
const Rep: Function;

protocol HCFAIUN(EU,GCS,UAV)
{
const IDeu, PASSeu,BTeu, K,OIDgcs,D;
const Thr:Timestamp;

###### USER REGISTRATION STAGE#######
macro Gammaeu=Gen(BTeu);
macro hd=Gen(BTeu);
macro Yeu = hash(Concat(IDeu,PASSeu,mu,Gammaeu));
macro OIDeu = hash(Concat(IDeu,sk(GCS)));
macro Zeu = hash(Concat(OIDeu,Yeu));
macro Zeu'= XOR(hash(Concat(OIDeu,PASSeu,Gammaeu)) ,  Zeu);
macro OIDeu' = XOR(hash(Concat(IDeu,PASSeu)), OIDeu);
#############################

###### UAV REGISTRATION STAGE#######
const IDuav,alpha;
macro MDuav =hash(Concat(IDuav,alpha));
macro OIDuav=hash(XOR(hash(Concat(IDuav,sk(GCS)),MDuav)));
############################

#######ROLE OF EXTERNAL USER######
 role EU
{
    fresh mu: Nonce;
    fresh TS1 : Timestamp;
    var TS3: Timestamp;
    var U1,AUTn:Ticket;
    fresh TScur:Timestamp;
    macro Gammaeu = Rep(BTeu, hd);
    macro YeuS= hash(XOR(hash(Concat(IDeu,mu,Gammaeu)), hash(Concat(PASSeu,mu,Gamm
    macro OIDeuS= hash(Concat(IDeu, pk(GCS)));
    macro ZeuS = hash(Concat(OIDeuS, YeuS));
    match(Zeu,ZeuS);
    macro PKgcs = G2CM(sk(EU), D);
    macro Keu= G2CM(sk(EU),PKgcs);
```

Figure 4.5: Scyther tool results

According to verification findings, all roles satisfy the requirements for being alive, Niagree, and Nisynch. Moreover, no attacks within the bounds were found, which means EU and UAV parameters, i.e. $Sess\_Key_{EU/UAV}$, Pri_Key_{EU}, and Pri_Key_{GCS} are secured from the attacker.

4.4.1.2 ROM based Security Assessment

The ROM model is a formal provable security analysis that validates the session key ($Sess\_Key_{EU \rightarrow UAV/UAV \rightarrow EU}$) security from Attacker A. This builds the groundwork for integrating the HCFAIUN with ROM. The model posits various queries such as Execute, Corrupt, Reveal and Test, which are required for adversary attack analysis. The core terms associated with ROM are the following:

- **Random Oracle:** The selected one-way cryptographic function acts as a random oracle $hash(\cdot)$.
- **Participants:** Participants are the entities indulging in the communication, and the entities present in our protocols are EU, GCS and UAV. We denote the instances INS_1, INS_2, and INS_3 of EU, GCS, and UAV as $\chi_{EU}^{INS_1}$, $\chi_{GCS}^{INS_2}$, $\chi_{UAV}^{INS_3}$ which act as oracles.
- **Partnerships:** EU and UAV will become partners if they retain a securely shared session key. The two instances $\chi_{EU}^{INS_1}$, $\chi_{UAV}^{INS_3}$ during the acceptance state can become partners if they own a common session key($Sess\_Key_{EU/UAV}$).
- **Freshness:** Freshness is achieved when Attacker (A) cannot leak the session key details maintained between $\chi_{EU}^{INS_1}$, $\chi_{UAV}^{INS_3}$
- **Attacker**: The adversary or attacker (A) model is mentioned in Section 4.2.2

Definition (Semantic Security of Sess_Key): The foundation for the secrecy of $Sess\_Key$ shared between EU and UAV is the difficulty in discovering the real session key generated from an arbitrary number through an attacker (A). A has the advantage of violating the semantic security of HCFAIUN protocol by leakage of $Sess_{Key}$ information, which is described as:

$$Adv_{A}^{HCFAIUN} = |2.Pr[b' = b] - 1| \tag{4.50}$$

where b and b denote correct bits and guess bits, respectively, and Pr[b=b] denotes the success probability.

Theorem 1: Suppose a polynomial time (T_{poly}) in which attacker A attempts to gain $Sess\_Key$ information $Sess\_Key_{UAV \rightarrow EU} = Sess\_Key_{EU \rightarrow UAV}$ in login and authentication stage of HCFAIUN then the advantage is mentioned as:

$$Adv_{A}^{HCFAIUN}(T_{poly}) \leq \frac{Hash_{Q}^{2}}{|Hash|} + 2Adv_{A}^{HCDLP}(T_{poly}) \tag{4.51}$$

Where terms like $Hash\_Q$ and $|Hash|$ denote the number of hash queries and the length of the one-way hash function with collision resistance, respectively. Moreover, $Adv_{A}^{HCDLP}(T_{poly})$ represents the advantage of attacker A to compromise the HCDLP security in T_{poly}.

Proof: We illustrate the proof of Theorm by the following three games such as $(Game_k^A | k = 0, 1, 2)$, which are played by Attacker A such that in each game, if A can predict the random bit b in $Game_k^A$ correctly, then it wins the game with event $Success_{Game_k}^A$. The probability of attacker A winning the $Game_k^A$ is given by the $Adv_{A,Game_k}^{HCFAIUN} = Pr[Success_{Game_k}^A]$. The demonstration of the three games played by attacker A is as follows:

$Game_0^A$: Attacker A plays the game and performs an actual attack by taking a random bit b ;then from the definition of semantic security, it is given as:

$$Adv_A^{HCFAIUN}(T_{poly}) = |2Adv_{A,Game_k}^{HCFAIUN} - 1| \tag{4.52}$$

$Game_1^A$: In this Game, Attacker A can gain the complete information of messages such as $M_1 = (EU_1, EU_2, EU_3, Pub\_Key_{EU}, TS_1), M_2 = (B_1, B_2, B_3, TS_2)$ and $M_3 = (U_1, AUT_N, TS_3)$ from eavesdropping attack by queries like Execute query during Login and Authentication Stage. Attacker A runs the reveal() and test() query to obtain Session key, $Sess\_Key_{UAV \to EU} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID'_{EU}{}^* \parallel TS_3 \parallel R_2) = Sess\_Key_{EU \to UAV}$ which is generated between the UAV and the user. The HCFAIUN protocol uses a one-way collision-resistant hash function which protects anonymous id such as $OID_{UAV}, OID_{GCS}, OID'_{EU}$ along with a timestamp and random nonce, R2*. Thus, an eavesdropping attack does not impact the leakage of the shared session key, which makes $Game_0^A$ and $Game_1^A$ identical, which is shown below:

$$Adv_{A,Game_0}^{HCFAIUN} = Adv_{A,Game_1}^{HCFAIUN} \tag{4.53}$$

$Game_2^A$: In this scenario, Attacker A performs malicious activity by executing a Corrupt query to gather secret credentials of EU such as ID_{EU} and $PASS_{EU}$. Moreover, if the attacker gains the secrete credentials stored in memory, then predicting $M_1 = (EU_1, EU_2, EU_3, Pub\_Key_{EU}, TS_1)$ is difficult due to the one-way hash function with collision resistance and HCDLP computation hardness to predict Pri_Key_{EU}. Additionally, $Game_1^A$ and $Game_2^A$ are hard to distinguish if hash queries and computational HCDLP are ignored. Utilizing the birthday paradox to find the hash collision along with the advantage of computing HCDLP is given as:

$$|Adv_{A,Game_1}^{HCFAIUN} - Adv_{A,Game_2}^{HCFAIUN}| \leq \frac{Hash_Q^2}{2|Hash|} + 2Adv_A^{HCDLP}(T_{poly}) \tag{4.54}$$

Attacker A, on completing all games $(Game_k^A | k = 0, 1, 2)$, does not gain any valid bit to win the game. Thus, we obtain the equation:

$$|Adv_{A,Game_2}^{HCFAIUN}| \leq \frac{1}{2} \tag{4.55}$$

From equation 4.52 and 4.53, we get

$$\frac{1}{2}Adv_A^{HCFAIUN}(T_{poly}) = |Adv_{A,Game_0}^{HCFAIUN} - \frac{1}{2}| \tag{4.56}$$

From the triangular inequality result and equations (4.52)–(4.54), we get,

$$\begin{aligned} \frac{1}{2}Adv_A^{HCFAIUN}(T_{poly}) &= |Adv_{A,Game_0}^{HCFAIUN} - Adv_{A,Game_2}^{HCFAIUN}| \\ &= |Adv_{A,Game_1}^{HCFAIUN} - Adv_{A,Game_2}^{HCFAIUN}| \\ &\leq \frac{Hash_Q^2}{2|Hash|} + Adv_A^{HCDLP}(T_{poly}) \end{aligned} \tag{4.57}$$

The final equation can be obtained by multiplying the equation (4.57) on both sides by 2.

$$Adv_{A}^{HCFAIUN}(T_{poly}) \leq \frac{Hash_{Q}^{2}}{|Hash|} + 2Adv_{A}^{HCDLP}(T_{poly}) \tag{4.58}$$

4.4.2 Informal Security Assessment:

The protocols safety management is commonly subjected to informal validation by analyzing it for vulnerability to numerous kinds of attacks. Its effectiveness and security assuredness are guaranteed. This section is aimed at conducting a complete security assessment of HCFAIUN, where well-known attacks are selected to showcase the defense capabilities of the system.

4.4.2.1 Replay Attack

In the login and authentication stage, all of the messages M_1, M_2, and M_3 contain some enciphered messages such as (EU_1) in M_1 and M_1 carries timestamp TS_1. The entity GCS will verify the timestamp TS_1 with the timestamp contained in the enciphered message (EU_1) on receiving the message from the EU. If the matching fails, the recipient will quickly learn that the message has undergone unauthorized modifications by the attacker A. The same scenario is followed for message M_2. Therefore, our protocol remains resilient in the face of replay attacks.

4.4.2.2 Man in the Middle Attack

If the hacker (A) tries to intercept and modify the contents of messages such as M_1, M_2, and M_3 to generate a false breach by disguising himself as a real participant. This illicit activity will be pointless because the attacker cannot emit authentication tokens or validate them. They cannot delay or forge messages due to fresh timestamps and unidirectional cryptographic $hash(\cdot)$, which guarantees the authenticity and validity of messages. As a result, the suggested strategy displays resistance against MITM assaults.

4.4.2.3 Impersonation Attack

4.4.2.3.1 Protection for UAV

If a malicious entity attempts to assume the identity of a registered UAV, denoted as UAV, they must generate authentic messages denoted as $AUT_N = hash(Sess\_Key_{UAV} \parallel TS_3)$ and successfully transmit them to the intended recipient, EU. However, it's important to note that AUT_N encapsulates the session key $Sess\_Key_{UAV}$, which remains beyond the attacker's reach and Upon receipt of the message AUT_N, EU proceeds to compute $AUT_N{*}$ and subsequently compares it with AUT_N to assess their validity. Consequently, the EU can distinguish between an attacker posing as a drone and a genuine registered drone. This capability underscores the security of the proposed scheme against drone impersonation attacks.

4.4.2.3.2 Protection for User

Under the information provided during the 2nd stage of the access and verification process, the GCS verifies the identity of user EU by calculating $EU_3{*}$ and subsequently comparing it to the EU_3 value received from EU. In an attempt to impersonate U_i, one method available to an attacker involves the creation of legitimate messages in the form of $EU_3 = hash(OID_{EU} \parallel OID_{GCS} \parallel OID_{UAV} \parallel K_{EU} \parallel TS_1)$, which are then transmitted to the GCS. It is important to note that the attacker can generate their timestamp (TSattacker), but they lack access to the confidential parameters, which encompass K_{EU} and GCS's private key (Pri_Key_{GCS}). These confidential parameters remain beyond the reach of the adversary. Consequently, the adversary cannot generate a legal EU_3, thereby enabling GCS to discern the impostor from the legitimate user.

4.4.2.3.3 Protection for GCS

In this assault, the attacker A acts as an authentic enrolled GCS and intercepts the authentication message M_2 between the GCS and the UAV. The attacker may construct modified or fraudulent communications by obtaining crucial data from the GCS to demonstrate his legitimacy. The attacker constructs legitimate information M_2 by generating slot TS_2 & a new arbitrary numeral R1. Due to a lack of knowledge regarding OID_{UAV}, OID_{GCS}, and OID_{EU}, the attacker cannot compute B_1, B_2, B_3,or alter M_3. As a result, it ensures that the attacker cannot fabricate or alter the confidential message of the GCS in polynomial time. Thus, the HCFAIUN protocol remains resilient to GCS impersonation attempts.

4.4.2.4 Session Key Attack

The session key derived as $Sess\_Key_{UAV \to EU} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID_{EU}^{'}{}^{*} \parallel TS_3 \parallel R_2)$ incorporates unique random numbers specific to the ongoing session. Including the trapdoor hash function ensures that the intruder (A) cannot extract arbitrary numerals such as R_2 from the session key. Consequently, even if an attacker gains possession of a previous session key, they are precluded from obtaining access to the current session key. This characteristic underscores the HCFAIUN protocol resilience against known session key attacks.

4.4.2.5 DoS Attack

During the access phase or a password update operation, if an enrolled EU provides an incorrect ID_{EU} and $PASS_{EU}$, a local validation process is employed, which includes verifying the condition $Y_{prev} = Y_{updated}$. Once this validation is completed, the external user EU login request is relayed to the GCS. Additionally, password updates are exclusively allowed when the old password is verified successfully during the update procedure. As a result, the HCFAIUN protocol exhibits resilience against DoS attacks of this nature.

4.4.2.6 Smart Device Attack

If an attacker A steals or loses the smart device belonging to a registered user EU. It is possible to extract all information $Z_{EU}^{'}$, $OID_{EU}^{'}$ stored in the device's memory through power analysis attacks. Where $Z_{EU}^{'} = hash(OID_{EU} \parallel Y_{EU}) \oplus Z_{EU}$ and $OID_{EU}^{'} = hash(ID_{EU} \parallel PASS_{EU}) \oplus OID_{EU}$. Despite this knowledge, the attacker is unable to reliably deduce OID_{EU} and $PASS_{EU}$ from the collected data without the safe factor Y_{EU}. Moreover, applying a unidirectional trapdoor hashing (SHA-1) averts the intruder from concurrently recovering the confidential details. Nevertheless, the assailant remains incapable of obtaining the secret parameters of the EU. As a result, the HCFAIUN protocol is resilient against assaults involving the theft of mobile devices.

4.4.2.7 Physical UAV Attack

As previously mentioned, a potential attacker's physical seizure of a UAV is a legitimate concern. Let us consider a scenario in which an attacker has successfully taken control of a UAV and gained access to all stored credentials and communication data, specifically $\{ID_{UAV}, OID_{UAV}\}$. It is important to note that the Pri_Key_{GCS} is securely stored within a unidirectional hash (SHA-1), effectively protecting any malicious actor by calculating the subsequently shared key without requisite information of the arbitrary value (R_1*) and obfuscation identity (OID_{GCS}, OID_{EU}). The confidential information differs for each individual deployed UAV, so attacker A cannot produce shared keys for UAVs and the EU. Consequently, the HCFAIUN demonstrates robustness against physical drone capture attacks.

4.4.2.8 Tampering Attack

An intruder A may manipulate the authentication and response details. We employ a unidirectional trapdoor hash method (SHA-1) to mitigate this risk and safeguard against unauthorized alterations. It is important to note that the transmitted message EU_3 includes the recipient's (sender's) secret key K_{EU}. The GCS can distinguish any modifications to the message with the help of equation $EU_3 = EU_3$*. Additionally, the user EU can detect any changes to the authentication component by verifying the equation $AUT = AUT_N$*. Consequently, the HCFAIUN protocol maintains its resilience against tampering attacks.

4.4.2.9 Password and Biometric Modification Attack

In this attack, attacker A can gather sensitive credentials of EU such as $Z^{'}_{EU}$, $OID^{'}_{EU}$, $Gen(\cdot)$, $Rep(\cdot)$, hd, μ by capturing the smart device. The purpose of A in this attack is to modify or update the $PASS_{EU}$ and biometric traits (BT_{EU}) of EU. To achieve this, A randomly chooses sensitive credentials such as ID^{A}_{EU}, $PASS^{A}_{EU}$ and BT^{A}_{EU}, and evaluate the following computations: $Gen(BT^{A}_{EU}) = (\gamma^{A}_{EU}, hd)$, $Y^{A}_{EU} = hash(ID^{A}_{EU} \parallel PASS^{A}_{EU} \parallel \mu \parallel \gamma^{A}_{EU})$, Z^{A}_{EU}' $= hash(OID_{EU} \parallel PASS_{EU} \parallel \gamma^{\mathrm{A}}_{EU}) \oplus Z_{EU}$, OID^{A}_{EU}' $= hash(ID^{\mathrm{A}}_{EU} \parallel PASS^{\mathrm{A}}_{EU}) \oplus OID_{EU}$. To complete the evaluation of the above parameters, it is difficult for attacker A to guess secret credentials of EU like OID_{EU}, Z_{EU}, ID_{EU}, $PASS_{EU}$ and BT_{EU}. Thus, guessing the password and modifying the smart device's information is impossible for the attacker.

4.4.2.10 Un-Traceability

To guarantee that every participant's message is unique, at the authentication step, the random nonce, R_1, R_2, and the current timestamp TS_{cur} for each session are selected at random. The enemy adversary cannot connect the communications the GCS, UAV, and EU sent. Likewise, it's hard to track down the sender. In addition, a secure unidirectional hash function contains or conceals genuine identities. (ID, OID). Thus, the HCFAIUN approach may be used to create un-traceability.

4.4.2.11 Privacy Preserving

To safeguard privacy and anonymity, the proposed protocol must ensure that an attacker cannot retrieve actual identities once our system is operational. Our protocol can safeguard the confidentiality of all sent and received communications, including M_1, M_2, and M_3. Moreover, these messages are generated using new periods and random integers. This provides a significant benefit in that it is harder for attackers to obtain sensitive information and actual identities from users, GCS, and drones. The HCFAIUN system, as a result, guarantees anonymity and privacy.

4.4.2.12 Accuracy and Validity

Data Accuracy and Validity are the assurance that no attacker may alter the information that is sent, and if they do, the system will detect and report the alteration. First of all, attacker A find it difficult to infer the matching session key ($Sess\_Key_{UAV/EU}$) based on the HCDLP. Second, nodes use the one-way hash function to conduct an integrity check following each phase's message exchange. As a result, the HCFAIUN system has significantly more integrity maintenance security.

4.4.2.13 Forward Secrecy

The Forward secrecy attribute ensures that the session key from the prior communication does not leak due to the compromised persistent key. Under the HCFAIUN method, participants must generate a new key ($Sess\_Key$) for every session. This new session key ($Sess\_Key$) must contain a random number that makes it difficult for attacker A to calculate or predict. Furthermore, the protocol incorporates a timestamp TS that checks current sessions. Therefore, the gathered secret key is irrelevant to the attacker in case of attempting to breach earlier sessions, indicating that our protocol guarantees absolute forward secrecy.

4.4.2.14 Authentication and Key Agreement

The common session key $Sess\_Key_{UAV \to EU} = hash(OID_{UAV} \parallel OID_{GCS} \parallel OID'_{EU}{}^{*} \parallel TS_3 \parallel R_2) = Sess\_Key_{EU \to UAV}$ is calculated among UAV and EU for secure communication which will be possible when mutual authentication is done.

4.5 Performance Evaluation

This section conducts an exhaustive performance analysis, comparing HCFAIUN with other pertinent schemes.

4.5.1 Computation Cost

In the mutual authentication phase, we evaluate the computing costs of the suggested method and previous work [13, 15–17]. According to [13, 16, 17], $T_H, T_{ECM}, T_{HCM}, T_{FE}, T_P, T_{CM}, T_{AC}, T_{ENC/DEC}, T_E$ denote the hash function with 0.027 ms time for GCS and 0.06 ms for EU and UAV, ECC multiplication with 0.56 ms duration for GCS and 1.27 ms for EU and UAV, HC multiplication with 0.48 ms time, FE with 1.27 ms time for EU and UAV, Bilinear pairing with 5.6 ms operation time for EU and UAV and 3.61 ms operation time for GCS, chaotic map with 0.512 ms for GCS and 0.98 ms operation time for EU and UAV, AEGIS authenticated encryption algorithm with computation time of 0.415 ms, encryption operation time of 0.5 ms for EU and UAV and 0.19 ms for GCS. Compared with previous work, our proposed work shows less computation cost, i.e. 3.832 ms, with high security against logical and physical attacks in IoT-based UAV networks, illustrated in Table 4.1 and Figure 4.6.

Table 4.1: Comparative study of computation costs

Schemes	**Ever [17]**	**Tanveer et al. [16]**	**Rajasekaran et al.[15]**	**Tanveer et al.[13]**	**Proposed HCFAIUN**
EU Side	$3T_H + 2T_P(11.38)$	$6T_H + 3T_{AC} + 3T_{ECM} + T_{FE}(6.685)$	$4T_E + T_P + T_H(8.06)$	$6T_H + 3T_{CM} + T_{FE}(6.57)$	$10T_H + 2T_{HCM} + T_{FE}(2.83)$
GCS Side	$9T_H + 2T_P + 4T_{ECM}(13.683)$	$2T_H + T_{ECM} + 3T_{AC}(0.824)$	-	$2T_H + T_{CM} + T_{ENC}(0.756)$	$6T_H + T_{HCM}(0.642)$
UAV Side	$5T_H + 2T_P(11.335)$	$3T_H + 2T_{ECM} + 2T_{AC}(3.451)$	$3T_E + 2T_P + T_H(13.06)$	$4T_H + T_{CM} + 2T_E(2.22)$	$6T_H(0.36)$
Total (ms)	36.398 ms	10.96 ms	21.12 ms	9.54 ms	3.832 ms

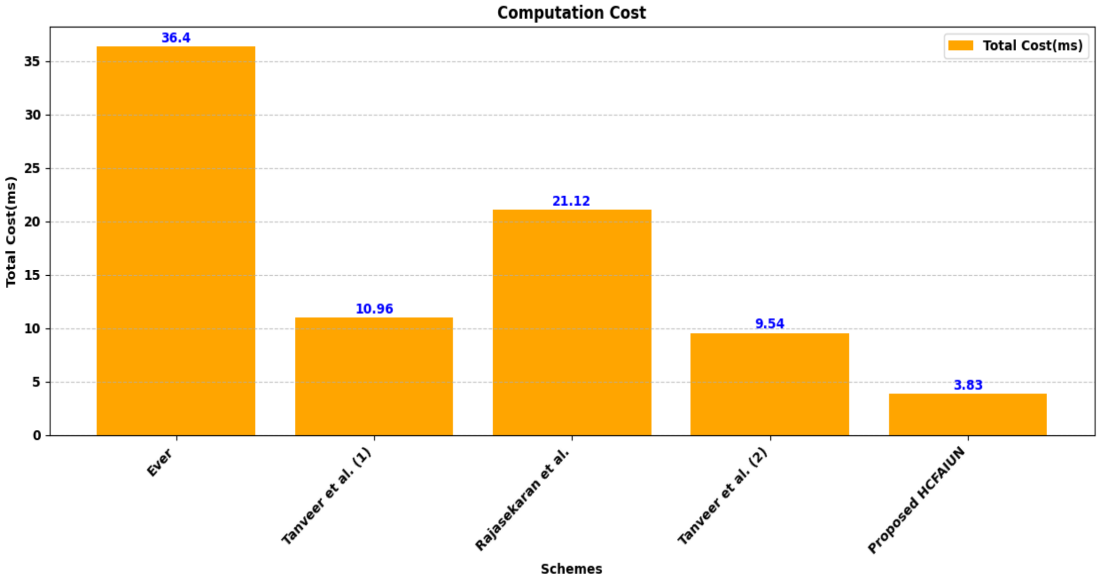


Figure 4.6: Comparison of computation costs

4.5.2 Communication Cost

To showcase the efficacy compared to prevailing methodologies [13, 15–17], we assess the communication expenditures incurred by diverse entities involved in the login and authentication phases. This analysis focuses on transmitting messages among the participants during these stages. To gauge communication expenses, we posit that the sizes for the the hash function (SHA-1), timestamp, HC, elliptic curve point, identity, and random number are 160, 32, 80, 160, 160, and 160 bits, respectively. To transmit message, $M_1 = (EU_1, EU_2, EU_3, Pub\_Key_{EU}, TS_1)$ the cost will be (160+160+160+80+32=592 bits). Similarly for $M_2 = (B_1, B_2, B_3, TS_2)$, cost will be (160+160+160+32=512) and to transmit $M_3 = (U_1, AUT_N, TS_3)$, the cost will be (160+160+32=352 bits). Therefore, the total cost will be 1456 bits, which is less than the existing ones with three messages exchanged as illustrated in Table 4.2 and Figures 4.7-4.8.

Table 4.2: Comparitive study of communication cost

Schemes	**Ever[17]**	**Tanveer et al.[16]**	**Rajasekaran et al.[15]**	**Tanveer et al.[13]**	**Proposed HCFAIUN**
Total Cost (bits)	1920	1856	1184	1664	1456
Messages	3	3	2	3	3

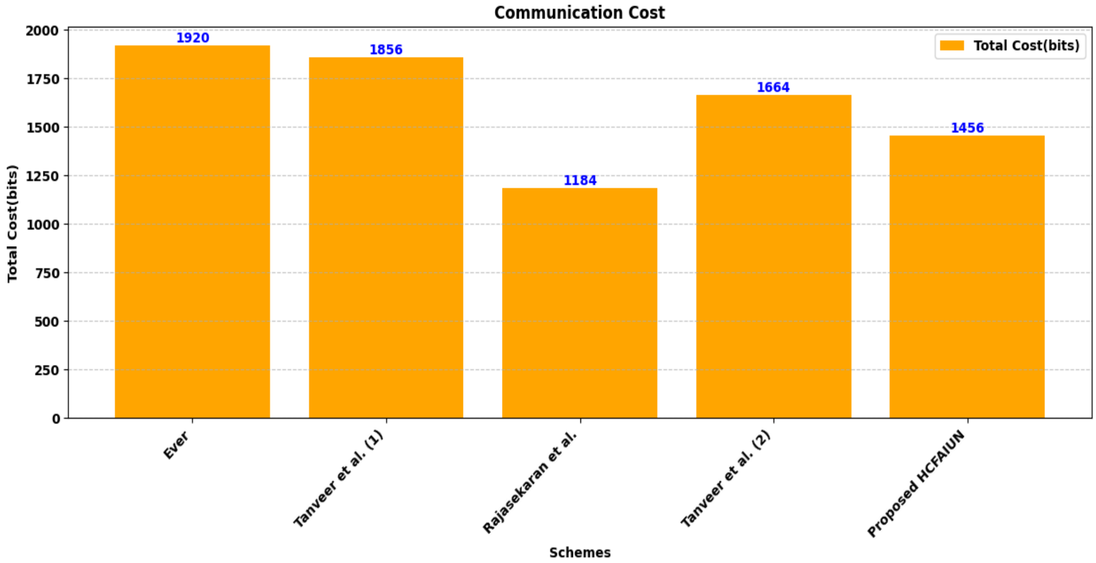


Figure 4.7: Comparison of communication costs

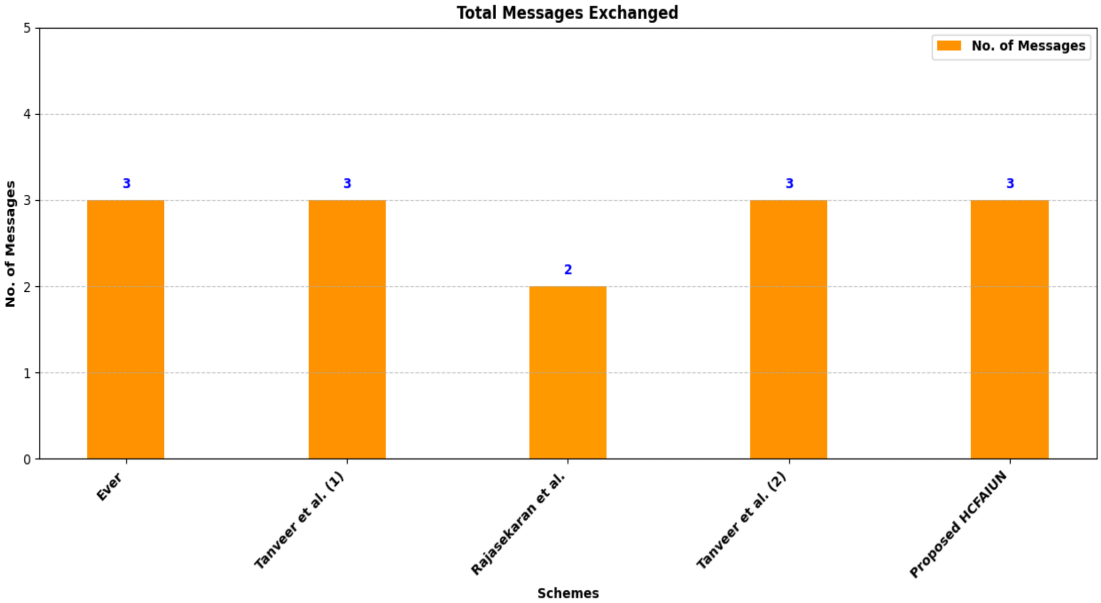


Figure 4.8: Comparison of total messages exchanged

4.5.3 Storage Cost

The proposed protocol provides insights into storage overhead complexities and demonstrates a comparison with existing schemes [13, 15–17] during the login and authentication stage, as shown in Table 4.3 and Figure 4.9. As UAVs are resource-constrained devices which often carry limited storage on board. Therefore, a reduction of storage costs is necessary. In the HCFAIUN protocol, the cost required to store the information $\{Z_{EU}, OID_{EU}, Gen(\cdot), Rep(\cdot), hd, \mu\}$,$\{OID_{UAV}\}$ and $\{OID_{EU}, OID_{UAV}\}$ at EU, UAV and GCS are {160+160+160+8+160}=648 bits, 160 bits and {160+160}=320 bits, respectively. Therefore, the total storage overhead in this scheme is 1128 bits, which is lower than existing schemes.

Table 4.3: Comparative study of storage costs

Schemes	**Ever [17]**	**Tanveer et al. [16]**	**Rajasekaran et al.[15]**	**Tanveer et al.[13]**	**Proposed HCFAIUN**
EU Side	160 bits	536 bits	1152 bits	824 bits	648 bits
GCS Side	128 bits	592 bits	-	608 bits	320 bits
UAV Side	1184 bits	256 bits	1046 bits	416 bits	160 bits
Total (bits)	1472 bits	1384 bits	2198 bits	1848 bits	1128 bits

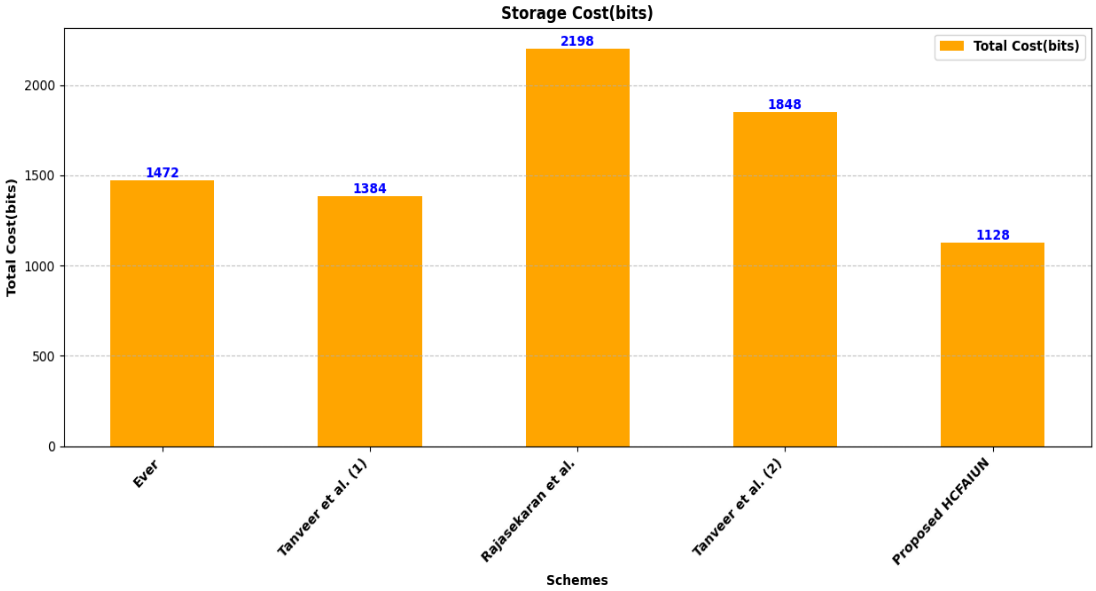


Figure 4.9: Comparison of storage costs

4.5.4 Comparative Analysis of Security Features

The proposed HCFAIUN scheme is provably secure and lightweight as compared to the previous schemes [13, 15–17] and the security features comparison is shown in Table 4.4. In the case of Tanveer et al. [16], the scheme is prone to various attacks, such as session key attacks, physical UAV attacks and tampering attacks with the lack of integrity and forward secrecy. This proposed scheme is secured against user and device impersonation attacks without discussing its effect on UAVs and GCS. Regarding Rajasekran [15], the scheme is vulnerable to session key attacks, DoS attacks, smart device attacks, physical UAV attacks, tampering attacks and biometric modification attacks. Additionally, this scheme lacks forward secrecy and dynamic device addition and no formal security analysis is provided for the session key. As per Ever [17], the discussed scheme is prone to an MITM attack, impersonation attack at the user and GCS side, DoS attack, smart device attack, tampering attack, password and biometric modification with weakness against untraceability, privacy-preserving, integrity, forward secrecy, dynamic device addition and no formal security assessment. In the case of Tanveer et al., [13], the scheme offers protection against various attacks such as replay and MITM attacks, but it is weak against DoS attacks, Smart Device attacks, physical UAV attacks, tampering attacks, privacy-preserving and dynamic device addition. Most of the schemes are based on a high-cost chaotic map, bilinear pairing cryptography, and a genus-1 elliptic curve without a strong key generation strategy. Consequently, our proposed scheme demonstrates enhanced security and functional attributes compared to previous schemes by utilising an HC scalar multiplication and FE to keep the private key secure and generate strong keys.

Table 4.4: Comparative study of security features

Features	**Tanveer et al.[16]**	**Rajasekaran et al. [15]**	**Ever et al. [17]**	**Tanveer et al. [13]**	**Proposed HCFAIUN**
SF1	✓	✓	✓	✓	✓
SF2	✓	✓	×	✓	✓
SF3	∂	✓	∂	✓	✓
SF4	×	×	×	✓	✓
SF5	✓	×	×	×	✓
SF6	✓	×	×	×	✓
SF7	×	×	✓	×	✓
SF8	×	×	×	×	✓
SF9	✓	×	×	✓	✓
SF10	✓	✓	×	✓	✓
SF11	✓	✓	×	×	✓
SF12	×	✓	×	✓	✓
SF13	×	×	×	✓	✓
SF14	✓	✓	✓	✓	✓
SF15	✓	×	×	×	✓
SF16	✓	×	×	✓	✓
SF17	✓	✓	✓	✓	✓

Note: ✓ - Discussion on security features, **x**- Not discussed ∂-partial information, SF1-Replay Attack, SF2-MITM attack, SF3-Impersonation attack (EU, GCS, UAV), SF4-Session Key Attack, SF5-DoS Attack, SF6-Smart Device Attack, SF7-Physical UAV Attack, SF8-Tampering Attack, SF9-Password and Biometric Modification Attack, SF10-Un-traceability, SF11- Privacy preserving, SF12-Integrity, SF13-Forward secrecy, SF14-Mutual Authentication and key agreement, SF15-dynamic device addition, SF16-formal security analysis, SF17-informal security analysis.

4.6 Summary

This chapter offers a Hyperelliptic curve and Fuzzy extractor-based authentication in IoT-based UAV networks that is effective and safe as per security requirements, leveraging HCC to satisfy the criterion of decreased computation, communication and storage cost, such as 3.82 ms, 1456 bits and 1128 bits, respectively, as compared to previous protocols. The proposed protocol improves the elliptic curve using lower parameters and key sizes.

Unlike typical bilinear pairing-based cryptography with exponential operations and elliptic curves, which require a 160-bit key size, HCC only requires a maximum of 80 bits, making it ideal for resource-constrained UAVs. This protocol also employs an FE mechanism to generate biometric traits of the user, such as a key which can be reproducible to prevent exposing data from stealing smart devices. The lower storage overhead in HCFAIUN eliminates the resource limitation of UAVs. Security and performance evaluations using Scyther formal and informal analyses, including comparative analyses, show that our proposed solution is secure. The real-world application of this protocol is to assist smart cities in rescue, package deliveries, and predicting traffic behaviour by firefighting service vehicles and ambulance drivers without any large computation and communication delay. HCFAIUN protocol can protect sensitive information like property destruction of people during natural disasters from physical and logical attacks on UAVs. Besides its advantages, the HCFAIUN scheme is based on fixed UAV topology in smart city scenarios. It can be vulnerable to quantum-based attacks, as quantum computers can solve complex HCDLP in seconds. In the future, our objective is to evaluate the effectiveness of our methodology in real-world conditions with dynamic UAV topologies consideration. This work can be enhanced by utilising a post-quantum-based cryptosystem.

Chapter 5

A Secure Cryptosystem for Secure Data Transmission in IoT-based UAV Networks

This chapter covers the design and development of the proposed secure cryptosystem with key operations such as HC of genus-2, secure hashing, XOR, random nonce and timestamps to generate shared session keys for further communication in IoT-based UAV networks.

5.1 Introduction

Wireless communication networks have facilitated the growing integration of IoT into our daily lives. Globally, the number of connected devices is outpacing human population growth. This situation leads to an increase in the average number of devices and connections per household and person. New gadgets with enhanced intelligence are launched and adopted annually. IoT-based UAV Networks link Unmanned Aerial Vehicles (UAVs), generally known as drones, with the IoT. This technology is utilized for inspection, surveillance, package delivery, military operations, and many other purposes, creating an enormous amount of sensitive information [158]. IoT-based UAV networks provide internet connectivity between users and UAVs to securely transmit data in smart cities, military, agriculture and healthcare environments [159]. IoT-based UAV networks provide connections among external operators (EO), UAVs and GCS. UAVs acquire data from their environment and relay it to the designated server located at the GCS in this system. In the same way, by sending control directives over wireless channels, the GCS monitors and manages the UAVs.

The UAVs carry traffic information on roads in smart cities, which is crucial for traffic authorities to track and prevent road accidents [160, 161]. Moreover, the UAVs capture aerial views through cameras to provide real-time information about survivors of natural calamities or disasters [162]. The collected traffic or disaster data transmission in this type of network is vulnerable to different kinds of attacks, such as impersonation and physical capture attacks by adversaries [163–165]. Moreover, UAVs are resource-constrained devices, i.e., they have limited computation capabilities, batteries, and storage on board. There are several other challenges, such as security and performance trade-offs. In most of the existing research studies [13, 15–17, 166], the proposed cryptosystems are based on pairing-based cryptography, chaotic maps and genus-1 elliptic curves with large key sizes and having high communication, computation and storage costs with a lack of security features such as untraceability, anonymity, forward secrecy and physical UAV attacks. Thus, to address these challenges, we propose a secure and lightweight cryptosystem based on a hyperelliptic curve (HC), which provides mutual authentication among users and UAVs by generating session keys for secure data transmission. The proposed cryptosystem overcomes the large key size problem by employing HC small key size of 80 bits suitable for a resource-constrained UAV network. The cryptosystem is secured with HC scalar multiplication, an anonymous alias of UAV and its operator, a secure hash algorithm, random nonces and unique timestamps for each session. The major contributions of the proposed cryptosystem are:

1. This paper introduces a unique and computationally efficient cryptosystem leveraging the hyperelliptic curve of a genus greater than one.

2. Employs the hyperelliptic curve discrete logarithm problem (HCDLP) using concealment ID for identity preservation.

3. Assessment of the cryptosystem is done through formal verification tools such as Scyther and ROM.

4. Performance evaluation is done with a comparative analysis of computation, communication and storage costs.

5.2 Summary of Recent Cryptosystems

This section provides a relevant study of authentication and key agreement techniques in existing cryptosystems.
Ever [17] discussed a cryptosystem based on pairing-based cryptography and elliptic curve cryptography (ECC) in order to facilitate mutual authentication among external operators and UAVs. Nevertheless, it is important to note that the system requires significant computational resources and lacks provisions for ensuring robust defense, untraceability and privacy. In [16], Tanveer et al. proposed an authentication scheme that employs several cryptographic primitives to accomplish its aims, including the use of hash functions and elliptic curve cryptography, but their scheme lacks verification of a session key and is vulnerable to man-in-the-middle and physical UAV attack. Rajasekaran et al. [15] presented a method for establishing a safe mutual authentication among users and UAVs using bilinear pairing. However, this scheme has a high computation overhead. In [166], the robust and reliable mutual authentication scheme was designed for UAV networks leveraging hash functions and chaotic maps, which mitigate masquerade and physical attack, but it is not suited for UAVs owing to high computation and communication costs. In addition, Tanveer et al. [13] discussed an authentication and key agreement method utilizing Chebyshev polynomial and symmetric key encryption. This scheme is prone to physical UAV attacks, denial of service attacks, and smartphone attacks with high computation, communication, and storage overhead.

5.3 System Model

This section provides the relevant background of the threat and network model.

5.3.1 Adversary model

The prominent Dolev-Yao (DY) threat model is applied in the proposed cryptosystem. In the DY Model [14, 129, 136], an attacker with malicious intent may inject fake information, edit, erase, manipulate, steal and carry out other unlawful actions on the information communicated by the two communicating parties in the public channel. This study also presents the Canetti-Krawczyk (CK) adversary model. In the CK model [137], an attacker can implement all the attack techniques of the DY model, and the attacker can additionally access and reveal secret credentials, session state, and session keys throughout the session. Therefore, the cryptosystem suggested in this work has to guarantee that the leaking of temporary session secrets and temporary session keys does not compromise the genuine credentials of the communicating entities. Thus, our suggested cryptosystem assumes that the registration and authentication service is trustworthy, while the external operator and UAV communication are not trusted.

5.3.2 Network model

The proposed cryptosystem consists of three entities, i.e., EO, GCS, and UAV, which are presented in Figure 5.1 and discussed below:

- **GCS:** A trusted identity that provides registration among external operators and UAVs. Based on this, the GCS creates long-term secret keys for UAVs and the EO based on their unique identities.

- **EO:** GCS provides the private key to the smart mobile user upon registration. The external operators prove their identity before communicating with UAVs.

- **UAVs:** At the registering stage, they get their secret keys from the GCS, too. Once EU legitimacy is verified, the UAV and EU set a session key that guarantees communication security.

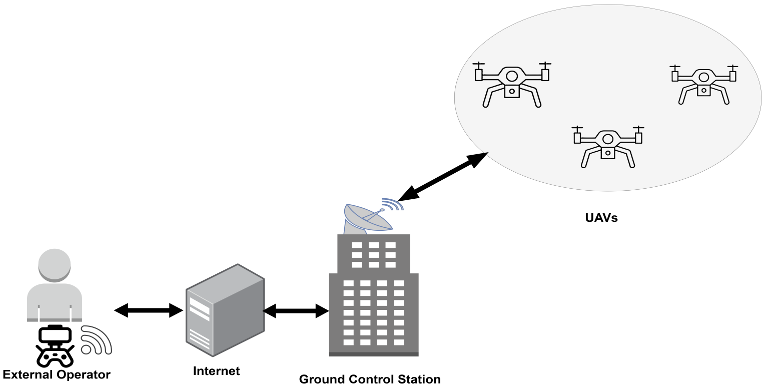


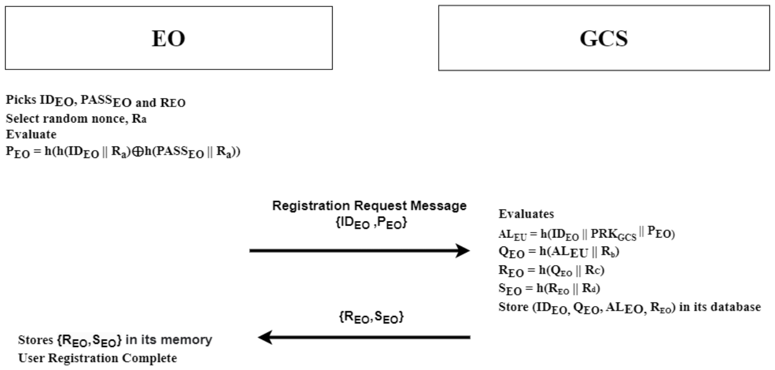
Figure 5.1: Network model of Cryptosystem

5.4 Proposed Cryptosystem

The proposed system contains four stages, which are briefly discussed in this section.

5.4.1 External Operator Enrollment Stage

An EO is required to register through GCS. The EO chooses one identity as ID_{EO} and password as $PASS_{EO}$ along with a random number R_a and evaluates $P_{EO} = h(h\,(ID_{EO} \parallel R_a) \oplus\; h\,(PASS_{EO} \parallel R_a))$, which is then sent to GCS via a private channel. GCS on receiving P_{EO}, evaluates anonymous alias $Al_{EO} = h(ID_{EO} \parallel PRK_{GCS} \parallel P_{EO})$, $Q_{EO}{=}h\,(Al_{EO} \parallel R_b)\,, R_{EO}{=}h(Q_{EO} \parallel R_c)$, $S_{EO}{=}h(R_{EO} \parallel R_d)$ and keeps $\{ID_{EO}$, Q_{EO}, $Al_{EO}, R_{EO}\}$ in its storage and forward $\{R_{EO},\; S_{EO}\}$ for external operator device storage over a private channel as presented in Figure 5.2.

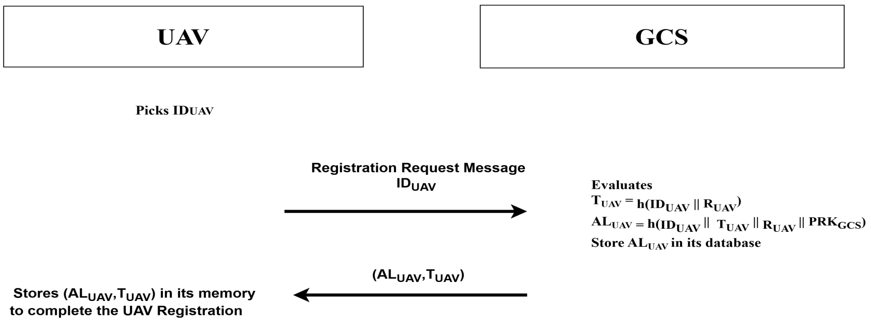


EO
GCS
Picks ID_{EO}, $PASS_{EO}$ and REO
Select random nonce, Ra
Evaluate
P_{EO} = h(h(ID_{EO} || R_a)⊕h($PASS_{EO}$ || R_a))
Registration Request Message
{ID_{EO} ,P_{EO}}
Evaluates
AL_{EU} = h(ID_{EO} || PRK_{GCS} || P_{EO})
Q_{EO} = h(ALEU || R_b)
R_{EO} = h(Q_{EO} || Rc)
S_{EO} = h(R_{EO} || Rd)
Store (ID_{EO}, Q_{EO}, ALEO, R_{EO}) in its database
{R_{EO},S_{EO}}
Stores {R_{EO},S_{EO}} in its memory
User Registration Complete

Figure 5.2: External Operator Registration Stage

5.4.2 UAV Enrollment Stage

A UAV sends its original identity, ID_{UAV}, over the private channel to GCS. GCS then selects a random number R_{UAV} and evaluates $T_{UAV} = h(ID_{UAV} \parallel R_{UAV})$ and anonymous alias, $AL_{UAV} = h(ID_{UAV} \parallel T_{UAV} \parallel R_{UAV} \parallel PRK_{GCS})$ and keeps AL_{UAV} in its memory and forwards $\{AL_{UAV},\, T_{UAV}\}$ to UAV over a private channel. The UAV receives and stores the parameters in its memory for subsequent use, as shown in Figure 5.3.



UAV
GCS
Picks IDUAV
Registration Request Message
ID_{UAV}
Evaluates
T_{UAV} = h(ID_{UAV} || R_{UAV})
AL_{UAV} = h(ID_{UAV} || T_{UAV} || R_{UAV} || PRK_{GCS})
Store AL_{UAV} in its database
(AL_{UAV},T_{UAV})
Stores (AL_{UAV},T_{UAV}) in its memory
to complete the UAV Registration

Figure 5.3: UAV Registration Stage

5.4.3 Authentication Stage

The various steps included in this stage are represented in Figure 5.4 and explained below:

1. **Step-1:** EO provides input credentials such as ID_{EO} and password as $PASS_{EO}$ which evaluate $P^{\$}_{EO} = h(h\,(ID_{EO} \parallel\ R_a) \oplus\ h\,(PASS_{EO} \parallel R_a))$,$AL^{\$}_{EO} = h(ID_{EO} \parallel PRK_{GCS} \parallel P_{EO})$ and $Q^{\$}_{EO}{=}h\left(AL^{\$}_{EO} \parallel R_b\right)$, $R^{\$}_{EO}{=}h(Q^{\$}_{EO} \parallel R_c)$, $S^{\$}_{EO}{=}h(R^{\$}_{EO} \parallel R_d)$ if $S_{EO}?{=}S^{\$}_{EO}$ validates successfully, then $PUK_{GCS} = PRK_{EO}.D$ and $TK_{EO} = PRK_{EO}.PUK_{GCS}$ and EO chooses a timestamp, T_a to evaluate $T_{EO} = h(Q_{EO} \,||\, AL_{EO} \,||\, TK_{EO} \,||\, T_a)$ which then sends a message $\{T_{EO}$, TK_{EO},PUK_{EO}, Q_{EO}, $T_a\}$ to GCS over the public channel.

2. **Step-2:** On receiving the first message, GCS will check for the freshness of the message by validating $|T_b{-}T_a| \leq \delta(T)$,then, $T^{\$}_{EO} = h(Q_{EO} \,||\, AL_{EO} \,||\, TK_{EO} \,||\, T_a)$, verify $T^{\$}_{EO}$?= T_{EO} and if verified successfully, then evaluate $K_{GCS} = PUK_{EO} * PRK_{GCS}$, $U_{UAV} = R_{EO} \oplus K_{GCS}$, $V_{EO} = h(U_{UAV}||K_{GCS}||T_b||R_b)$ and forward $\{K_{GCS}$, Q_{EO}, U_{UAV}, V_{EO}, $T_b\}$ to UAV end over insecure channel.

3. **Step-3:** On verifying timestamp , $|T_c - T_b| \leq \delta(T)$ UAV computes $R_{EO} = U_{UAV} \oplus K_{GCS}$ and $V^{\$}_{EO} = h(U_{UAV}||K_{GCS}||T_b||R_b)$ then confirms $V^{\$}_{EO} = V_{EO}$, if valid $SK_{UAV} = h(AL_{UAV} \,||\, R_{EO}||\, T_b)$ and $Auth_{UAV}$ is calculated as $Auth_{UAV} = h(SK_{UAV}||\, Q_{EO}||R_{EO}||T_b)$ and $\{\ Auth_{UAV}$, $T_d\}$ is forwarded to EO over an insecure medium.

4. **Step-4:** EO will check $|T_e - T_d| \leq \delta(T)$, if verification is successful, then evaluate $SK_{EO} = h(AL_{UAV} \,||\, R_{EO}||\, T_b)$, $Auth_{EO} = h\,(SK_{EO}||Q_{EO}\,||R_{EO}||\, T_d)$, confirm $Auth_{UAV}$?= $Auth_{EO}$ if verification fails, then the session is terminated; otherwise, mutual authentication is completed with the result as a shared session key, SK= SK_{UAV}= SK_{EO}.

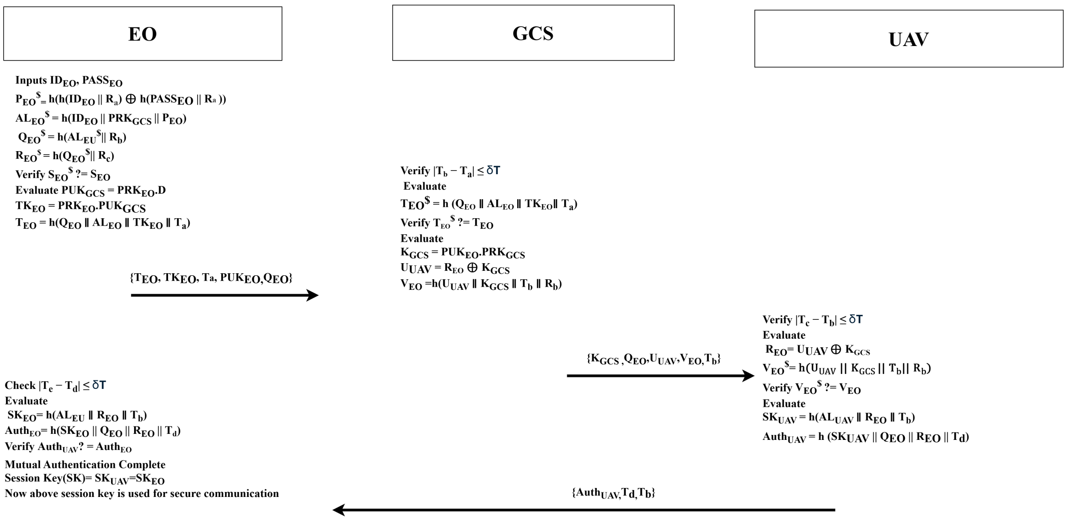

EO
GCS
UAV
Inputs ID_{EO}, $PASS_{EO}$
$P_{EO}{}^{\$} = h(h(ID_{EO} \,||\, R_a) \oplus h(PASS_{EO} \,||\, R_a))$
$AL_{EO}{}^{\$} = h(ID_{EO} \,||\, PRK_{GCS} \,||\, P_{EO})$
$Q_{EO}{}^{\$} = h(AL_{EU}{}^{\$} || R_b)$
$R_{EO}{}^{\$} = h(Q_{EO}{}^{\$} || R_c)$
Verify $S_{EO}{}^{\$}$?= S_{EO}
Evaluate $PUK_{GCS} = PRK_{EO}.D$
$TK_{EO} = PRK_{EO}.PUK_{GCS}$
$T_{EO} = h(Q_{EO} \parallel AL_{EO} \parallel TK_{EO} \parallel T_a)$
$\{T_{EO}, TK_{EO}, Ta, PUK_{EO}, Q_{EO}\}$
Verify $|T_b - T_a| \leq \delta T$
Evaluate
$TEO^{\$} = h\ (Q_{EO} \parallel AL_{EO} \parallel TK_{EO} \parallel T_a)$
Verify $T_{EO}{}^{\$}$?= T_{EO}
Evaluate
$K_{GCS} = PUK_{EO}.PRK_{GCS}$
$U_{UAV} = R_{EO} \oplus K_{GCS}$
$V_{EO} = h(U_{UAV} \parallel K_{GCS} \parallel T_b \parallel R_b)$
$\{K_{GCS}, Q_{EO}, U_{UAV}, V_{EO}, T_b\}$
Verify $|T_c - T_b| \leq \delta T$
Evaluate
$R_{EO} = U_{UAV} \oplus K_{GCS}$
$V_{EO}{}^{\$} = h(U_{UAV} \,||\, K_{GCS} \,||\, T_b \,||\, R_b)$
Verify $V_{EO}{}^{\$}$?= V_{EO}
Evaluate
$SK_{UAV} = h(AL_{UAV} \parallel R_{EO} \parallel T_b)$
$Auth_{UAV} = h\ (SK_{UAV} \,||\, Q_{EO} \,||\, R_{EO} \,||\, T_d)$
Check $|T_e - T_d| \leq \delta T$
Evaluate
$SK_{EO} = h(AL_{EU} \parallel R_{EO} \parallel T_b)$
$Auth_{EO} = h(SK_{EO} \,||\, Q_{EO} \,||\, R_{EO} \,||\, T_d)$
Verify $Auth_{UAV}$? = $Auth_{EO}$
Mutual Authentication Complete
Session Key(SK)= SK_{UAV}=SK_{EO}
Now above session key is used for secure communication
$\{Auth_{UAV}, T_d, T_b\}$

Figure 5.4: Authentication Stage

5.4.4 Password Alteration stage

In this stage, EO enters their ID_{EO} and $PASS_{EO}$ in the smart device and evaluates $P^{\$}_{EO} = h(h\,(ID_{EO} \parallel\ R_a) \oplus\ h\,(PASS_{EO} \parallel R_a))$, $AL^{\$}_{EO} = h(ID_{EO} \parallel PRK_{GCS} \parallel\ P_{EO})$ and $Q^{\$}_{EO}{=}h\left(AL^{\$}_{EO} \parallel R_b\right)$, $R^{\$}_{EO}{=}h(Q^{\$}_{EO} \parallel R_c)$, $S^{\$}_{EO}{=}h(R^{\$}_{EO} \parallel R_d)$ confirm $S_{EO}?{=}S^{\$}_{EO}$, Then, EO provides an alternate password to update $PASS^{N}_{EO}$ followed by evaluation, $P^{N}_{EO} = h(h\,(ID_{EO} \parallel\ R_a) \oplus\ h\left(PASS^{N}_{EO} \parallel R_a\right))$, $AL^{N}_{EO} = h(ID_{EO} \parallel PRK_{GCS} \parallel\ P_{EO})$ and $Q^{N}_{EO}{=}h\left(AL^{N}_{EO} \parallel R_b\right)$, $R^{N}_{EO}{=}h(Q^{N}_{EO} \parallel R_c)$, $S^{N}_{EO}{=}h(R^{N}_{EO} \parallel R_d)$, EO substitutes $P^{\$}_{EO}$, $AL^{\$}_{EO}$, $Q^{\$}_{EO}$, $R^{\$}_{EO}$, $S^{\$}_{EO}$ with P^{N}_{EO}, AL^{N}_{EO}, Q^{N}_{EO}, R^{N}_{EO}, S^{N}_{EO} respectively.

5.5 Security Assessment

This section covers the security assessment of the proposed cryptosystem with formal and informal analysis methods.

5.5.1 Formal Analysis

Formal analysis of the cryptosystem is carried out using the Random Oracle Model (ROM) and Scyther tool.

1. **ROM method:** This method is a mathematical model that responds to distinct queries with arbitrary responses by validating shared session keys from adversaries. The principle terms for this model are the following:

   - **Oracle:** The one-way hash function h(.) acts as an oracle.
   - **Participants:** In the proposed cryptosystem, there are three participants involved in secure data transmission, namely GCS, EO, and UAV, with instances as i1,i2, i3, and oracles as I^{i1}_{GCS}, I^{i2}_{EO}, I^{i3}_{UAV} respectively.
   - **Partnership:** If the session key is shared among all the oracles I^{i1}_{GCS}, I^{i2}_{EO}, I^{i3}_{UAV} then they form a partnership during the acceptance state.
   - **Freshness:** Freshness is achieved when Adv cannot disclose the shared session key among I^{i2}_{EO} and I^{i3}_{UAV}.

   This method contains various queries that are necessary for the assessment of Adv attacks as follows:

   (a) Send(I^{i}, M): Adv can execute this query to transfer message M to I^{i} and obtain the response.

   (b) Execute(I^{i1}_{GCS}, I^{i2}_{EO}, I^{i3}_{UAV}): Adv can obtain the information by performing an eavesdropping attack with this query.

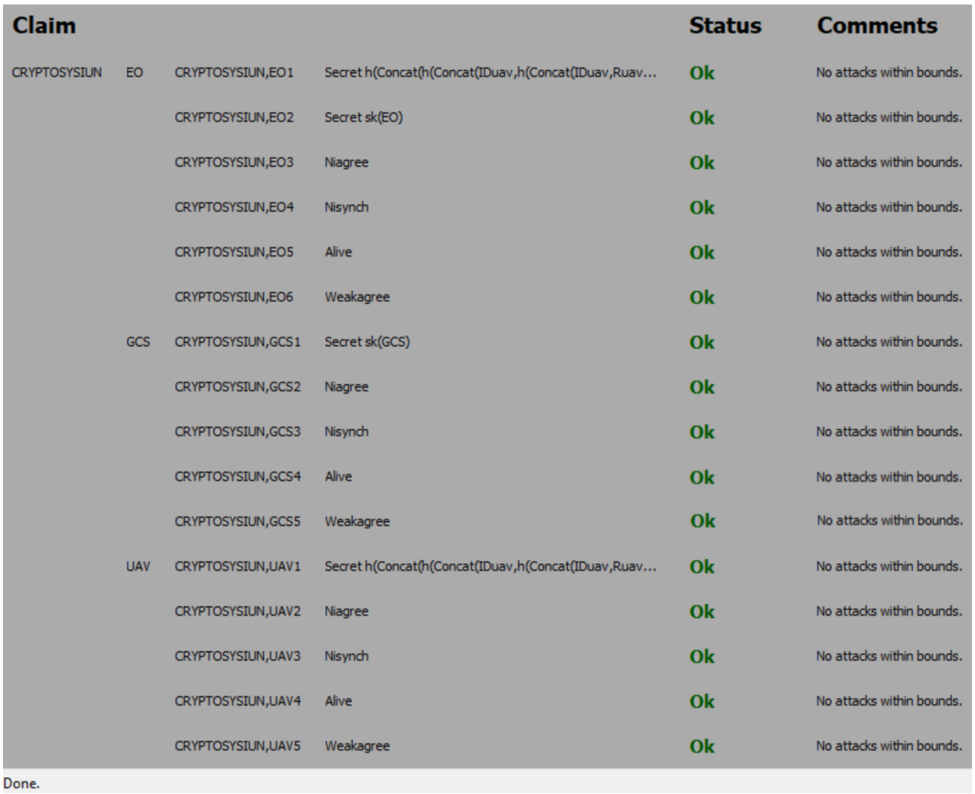
   (c) Corrupt(I^{i}): Adv runs this query to gather the privileges of an external operator.

   (d) Reveal(I^{i}): The session key shared among EO and UAV can be revealed by the Adv by executing Reveal query.

   (e) Test(I^{i}): The attacker can run this query to obtain the session key from I^{i} which in turn responds with random outcome C from the unbiased coin.

2. **Scyther verification:**

   The proposed cryptosystem is verified using the Scyther verification tool [143, 167], which validates all security principles such as Integrity, Confidentiality, and Authentication. The proposed cryptosystem follows SPDL (Security Protocol Description Language) for the writing syntax. The output shows no attacks on the proposed cryptosystem with identities and session key protection from adversaries, as shown in Figure 5.5.



Claim				Status	Comments
CRYPTOSYSIUN	EO	CRYPTOSYSIUN,EO1	Secret h(Concat(h(Concat(IDuav,h(Concat(IDuav,Ruav...	Ok	No attacks within bounds.
		CRYPTOSYSIUN,EO2	Secret sk(EO)	Ok	No attacks within bounds.
		CRYPTOSYSIUN,EO3	Niagree	Ok	No attacks within bounds.
		CRYPTOSYSIUN,EO4	Nisynch	Ok	No attacks within bounds.
		CRYPTOSYSIUN,EO5	Alive	Ok	No attacks within bounds.
		CRYPTOSYSIUN,EO6	Weakagree	Ok	No attacks within bounds.
	GCS	CRYPTOSYSIUN,GCS1	Secret sk(GCS)	Ok	No attacks within bounds.
		CRYPTOSYSIUN,GCS2	Niagree	Ok	No attacks within bounds.
		CRYPTOSYSIUN,GCS3	Nisynch	Ok	No attacks within bounds.
		CRYPTOSYSIUN,GCS4	Alive	Ok	No attacks within bounds.
		CRYPTOSYSIUN,GCS5	Weakagree	Ok	No attacks within bounds.
	UAV	CRYPTOSYSIUN,UAV1	Secret h(Concat(h(Concat(IDuav,h(Concat(IDuav,Ruav...	Ok	No attacks within bounds.
		CRYPTOSYSIUN,UAV2	Niagree	Ok	No attacks within bounds.
		CRYPTOSYSIUN,UAV3	Nisynch	Ok	No attacks within bounds.
		CRYPTOSYSIUN,UAV4	Alive	Ok	No attacks within bounds.
		CRYPTOSYSIUN,UAV5	Weakagree	Ok	No attacks within bounds.

Done.

Figure 5.5: Scyther Verification

5.5.2 Informal Analysis

This section provides a provably secure analysis of the proposed cryptosystem.

- **External operator device attack:** If adversary tries to attempt this attack and wants to gather information $\{ID_{EO}, Q_{EO}, Al_{EO}, R_{EO}\}$ from the memory of the device then it is difficult for Adv to do so as it is unable to deduce message digest P_{EO} which rely on the one-way hash function SHA-1.

- **Man-in-the-middle attack:** The proposed cryptosystem is secured from man-in-the-middle attack. If the adversary tries to capture messages such as $\{T_{EO}$, TK_{EO},PUK_{EO}, Q_{EO}, $T_a\}$, $\{K_{GCS}$, Q_{EO}, U_{UAV}, V_{EO}, $T_b\}$and $\{$ $Auth_{UAV}$, $T_d\}$ by delete, update and eavesdrop, then it will not possible for an attacker as each message is acquired with a timestamp and unidirectional hash function.

- **DoS attack:** If the attacker tries to flood the network with bulk requests with incorrect login credentials, then multiple validation is required, such as $S_{EO}?{=}S^{\$}_{EO}$, $T_{EO}?{=}T^{\$}_{EO}$ and $V_{EO}?{=}V^{\$}_{EO}$. Each validation is required to be done at a particular timestamp, which will be hard to guess for adversaries; therefore, this cryptosystem is secured against DoS attack.

- **Impersonation attack:** If the attacker tries to impersonate the system, then there will be the requirement of original identity credentials such as ID_{EO} and ID_{UAV} which are secure using alias identities of EO and UAV such as $AL_{EO} = h(ID_{EO} \parallel PRK_{GCS} \parallel P_{EO})$ and $AL_{UAV} = h(ID_{UAV} \parallel T_{UAV} \parallel R_{UAV} \parallel PRK_{GCS})$. Therefore, the proposed cryptosystem is secured against impersonation attacks.

- **Replay attack:** The messages such as $\{T_{EO}$, TK_{EO},PUK_{EO}, Q_{EO}, $T_a\}$, $\{K_{GCS}$, $Q_{EO}, U_{UAV}, V_{EO}, T_b\}$and $\{$ $Auth_{UAV}\}$ are involved in the communication are secured with timestamps such as $\{T_a, T_b, T_c, T_d$ $\}$ and random nonce $\{R_a, R_b, R_c,$ $, R_d\}$ which will prevent replay attacks.

- **Session key attack:** The session key generated between UAV and EO, such as $SK_{EO} = SK_{UAV} = h(AL_{UAV} \mid\mid R_{EO} \mid\mid T_d)$ are equipped with an alias of UAV, R_{EO} and a unique timestamp for each session. Moreover, the attacker cannot extract these parameters from the one-way hash function. Thus, our cryptosystem is secured against session key attacks.

- **Untraceability:** The message communicated between EO, GCS, and UAV are secured with random nonces such as R_a, R_b and the specific timestamp T_b, T_c and T_e are provided for the current session which prevents an attacker from performing malicious activity in between the communication.

- **Forward secrecy:** The session key shared by the entities EO and UAV, SK_{EO} and SK_{UAV} are generated for each session, which holds timestamp and random numbers and makes the scenario difficult for the attacker if somehow the attacker predicts the current timestamp for the current session then it is hard for them to predict earlier session key due to random nonce which guarantees the security of the proposed cryptosystem.

- **UAV capture attack:** Any adversary can physically capture the drone by the laser or net throw attack and take control of the whole UAV storage component such as $\{AL_{UAV}$, $T_{UAV}\}$ but despite the control, the attacker cannot extract actual credentials of UAV such as ID_{UAV} and PRK_{GCS} due to SHA-1 one-way hash function.

- **Tampering attack:** An internal user may try to intercept the network by altering the message communicated between the entities. The EO entity has the content TK_{EO} which is generated with the help of PUK_{GCS} and calculated with hyperelliptic curve discrete logarithm (HCDLP), which is difficult for the internal adversary to evaluate. Similarly, the verification $T^{\$}_{EO}$?= T_{EO} at the GCS end ensures the security of the proposed cryptosystem.

5.6 Performance Evaluation

This section covers the performance of the proposed cryptosystem by evaluating the computation, communication and storage overhead.

5.6.1 Computation Overhead

The computation overhead of the proposed cryptosystem is evaluated based on the time taken by the different operations evaluation while transferring the message content among different entities EO, GCS and UAV. The computation time standard values utilized by the proposed protocol are defined in [13, 15–17, 166]. The computation time of various operations such as hash function (T_h), HC scalar multiplication (T_{hc}), EC scalar multiplication (T_{ec}), bilinear pair (T_{bp}), chaotic map (T_{cm}) and physical unclonable function (T_{puf}), encryption/decryption ($T_{enc/dec}$) and fuzzy extractor (T_{fe}) is are 0.55 ms, 0.48ms, 0.98 ms, 2.31 ms, 0.66 ms, 0.22 ms, 0.71 ms and 1.27 ms respectively. The calculation of computation cost at each entity end denotes that our cryptosystem has a minimum cost of 10.33 ms as compared with the previous cryptosystem, which is shown in Figure 5.6 and Table 5.1.

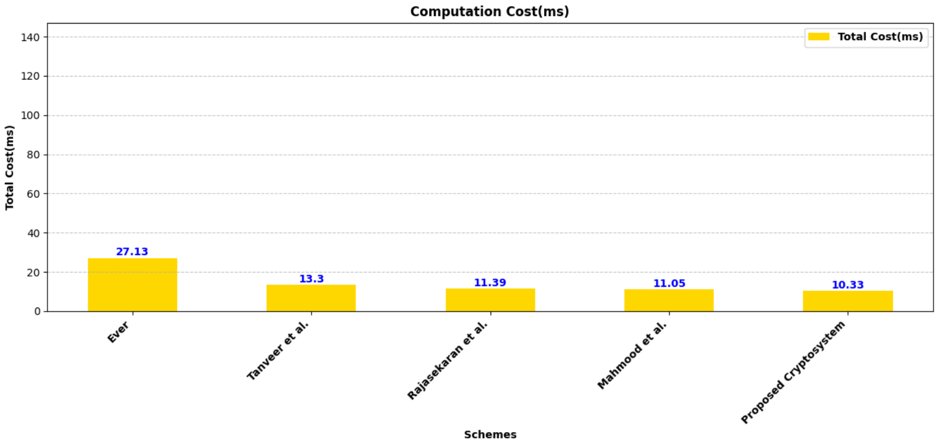


Figure 5.6: Computation Cost Comparative Analysis

Table 5.1: Computation cost of proposed cryptosystem

Entities	**Operations**	**Computation Overhead(ms)**
EO	$10T_h$+$2T_{hc}$	6.46
GCS	$3T_h$+T_{hc}	2.13
UAV	$3T_h$	1.74
		Total Cost 10.33 ms

5.6.2 Communication Overhead

All the entities EO, GCS and UAV involved in the communication carry messages in bits or bytes. The size considered for the hash function, identity, timestamp, concatenation, xor and the random number is 160, 160, 32, 160, 160 and 160 bits, respectively. The first message $\{T_{EO}, TK_{EO}, PUK_{EO}, Q_{EO}, T_a\}$ which consumes 160+160+160+80+32}=592 bits. Similarly, the second message $\{K_{GCS}$, Q_{EO}, U_{UAV}, V_{EO}, $T_b\}$ has overhead {160+160+160+160+32}=672 bits and third message $\{Auth_{UAV}$

, $T_d\}$ consumes {160+32}=192 bits. The final computed value for communication overhead is 1456 bits, which is less than that of other schemes as represented in Table 5.2 and Figure 5.7.

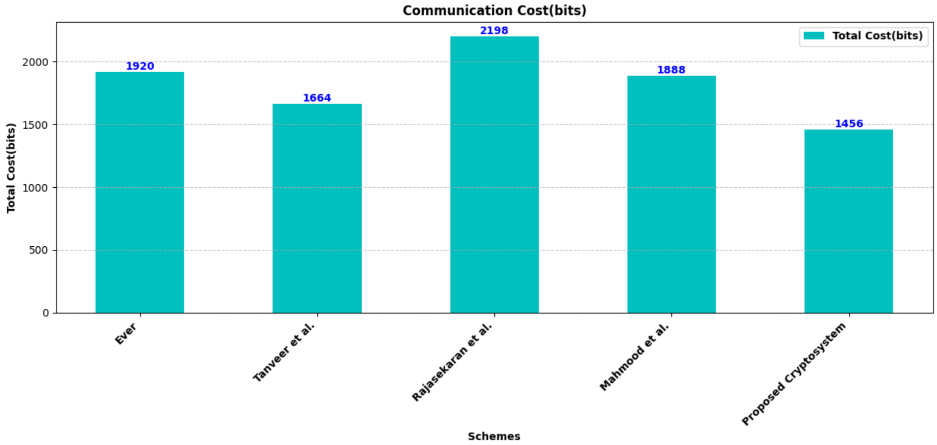


Figure 5.7: Communication Cost Comparative Analysis

Table 5.2: Communication cost of proposed cryptosystem

Communication Entities	Messages	Communication Overhead (bits)
$EO \rightarrow GCS$	$\{T_{EO}, TK_{EO}, PUK_{EO}, Q_{EO}, T_a\}$	592
$GCS \rightarrow UAV$	$\{K_{GCS}, Q_{EO}, U_{UAV}, V_{EO}, T_b\}$	672
$UAV \rightarrow EO$	$\{Auth_{UAV}, T_d\}$	192
		Total Cost 1456 bits

5.6.3 Storage Overhead

The local memory space utilized by the entities is known as storage overhead. In the proposed cryptosystem, memory space utilized by entities EO, GCS, and UAV for storing message contents $\{ID_{EO}, Q_{EO}, AL_{EO}, R_{EO}\}$, $\{AL_{UAV}, AL_{EO}\}$ and $\{AL_{UAV}, T_{UAV}\}$are {160+160+160+160=640 bits},{160+160=320 bits} and {160+160=320 bits} respectively. Therefore, the proposed cryptosystem has minimum storage overhead as compared to other schemes, which gives an advantage to resource-constrained UAVs as represented in Figure 5.8 and Table 5.3.

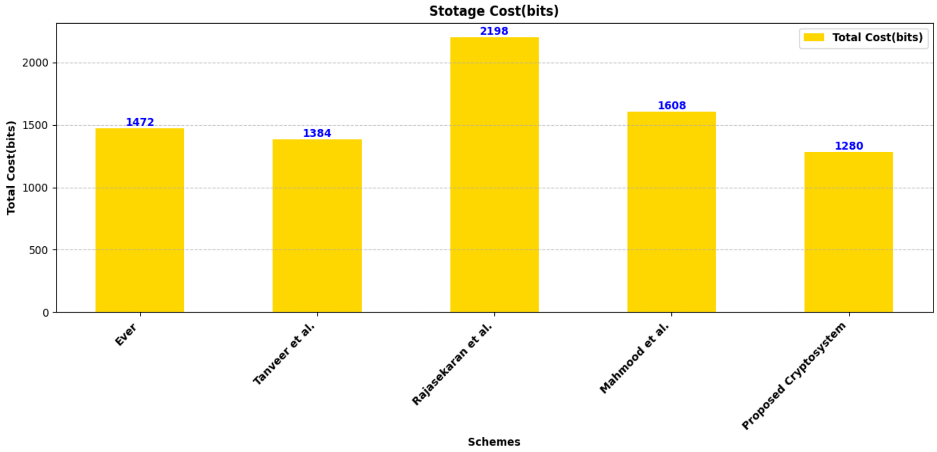


Figure 5.8: Storage Cost Comparative Analysis

Table 5.3: Storage cost of proposed cryptosystem

Entities	**Message Stored**	**Storage Overhead (bits)**
EO	$\{ID_{EO}, Q_{EO}, AL_{EO}, R_{EO}\}$	640
GCS	$\{AL_{UAV}, AL_{EO}\}$	320
UAV	$\{AL_{UAV}, T_{UAV}\}$	320
		Total Cost 1280 bits

5.7 Summary

This chapter discussed the cryptosystem based on the hyperelliptic curve, which utilizes the HCDLP, secure hash function, random nonce, alias identity, and XOR function. The results of formal scyther verification and ROM show that the proposed cryptosystem is secured from adversaries' attacks, and informal analysis shows provable security. The comparative study of different cryptosystems is described with computation, communication, and storage overhead charts, and the proposed system shows minimum computation, communication and storage overhead as 10.33 ms, 1456 bits and 1280 bits, respectively, making it suitable for resource-constrained UAVs. The cryptosystem can be implemented for real-world UAV operations with enhanced security.

Chapter 6

CONCLUSION, FUTURE SCOPE AND SOCIAL IMPACT

6.1 Conclusion

The integration of IoT with UAV networks has revolutionised various applications such as surveillance, traffic monitoring and payload delivery in smart city scenarios. However, there are significant security concerns in transmitting plenty of sensitive data within the entities from external users to UAVs and among UAVs via GCS. In the smart cities., IoT-based UAV networks are susceptible to various physical and logical attacks, such as net throw attacks, DoS, and impersonation attacks. The use of UAVs in smart cities raises privacy issues, such as disclosure of UAVs' position through latitude and longitudinal coordinates and captured images in the UAV's memory. Ensuring the privacy of citizens and sensitive data is a critical challenge. UAVs often have limited computational, communication and storage resources, which requires lightweight and efficient security protocols. The open-access communication landscape of IoT-based UAV networks makes them vulnerable to authentication vulnerabilities. Unauthorised access to this network can lead to data breaches and other security incidents. The recently proposed schemes rely on pairing-based cryptography, elliptic curve cryptography, and chaotic crypto methods, which have intensive computation, communication and storage costs and fail to provide a balance between security and performance. Given numerous attempts of adversary attacks in smart cities and other gaps, we have contributed through the design and development of novel mutual authentication schemes in our thesis work. We proposed three novel mutual authentication schemes as described below:

1. G2CAIUN: A Novel Genus-2 Curve-based Authentication for Secure Data Transmission in IoT-based UAV Networks

2. HCFAIUN: A Novel Hyperelliptic Curve and Fuzzy Extractor-based Authentication for Secure Data Transmission in IoT-based UAV networks

3. A Secure Cryptosystem for Secure Data Transmission in IoT-based UAV Networks

In Chapter 2, we systematically surveyed the existing literature on secure communication in IoT-based UAV networks. It covers a wide range of security vulnerabilities, including physical and logical attacks such as jamming, spoofing, eavesdropping and code injection. Our work evaluates existing countermeasures based on different technologies, such as encryption and key management techniques, authentication mechanisms, blockchain-based solutions, quantum cryptography and intrusion detection systems. We provide a well-defined research methodology, including research questions, databases, inclusion and exclusion criteria and a systematic approach to selecting relevant papers. This ensures a thorough and unbiased review of the literature. We also discussed a comparison of existing searches with our findings, highlighting the limitations of previous research and providing a more detailed analysis of security challenges and solutions in IoT-based UAV networks. We also examined recent case studies on drone attacks. This work covers a hierarchal approach that provides a clear and organised view of attacks and their countermeasures. At last, we have provided the mathematical foundation of HCC and its advantages over traditional cryptographic schemes, along with the background of formal validation techniques and tools.

In Chapter 3, we have proposed a novel mutual authentication scheme (G2CAIUN) for robust communication in IoT-based UAV networks for smart city scenarios. The proposed protocol utilises the Genus-2 hyperelliptic curve discrete logarithm problem and anonymous identity to ensure the communication is encrypted and anonymous from adversary attacks. We adopt PUF functionality, which protects the physical capture attack or tampering. The protocol considered the network model and threat model, such as the DY-threat and CK adversary model for malicious attempts. We have provided the number of steps to design the protocol, starting from the Setup stage and enrollment stage, followed by the EU-GCS-UAV, UAV-UAV and UAV-GCS authentication stage. This scheme offers termination and re-issuance stage in case of device loss. The security evaluation of the G2CAIUN scheme is done with formal validation of the Scyther tool and ROM model. Moreover, the informal analysis provides valid proof against a number of logical and physical attacks. We have offered a comparative study of security attributes in tabular format. The performance evaluation of our protocol depicts the low computation (2.5 ms) and communication (1456 bits) overhead with existing schemes without compromising security.

In Chapter 4, we have presented a novel authentication protocol (HCFAIUN) for secure data transmission in IoT-based UAV networks. This protocol leverages Hyperelliptic curve cryptography and fuzzy extractor mechanisms to address the security challenges that occur in smart city scenarios. We achieve a significant reduction in key size, making it suitable for UAVs with limited computational and storage resources. The fuzzy extractor enhances security by generating biometric traits to protect from unauthorised access. We have facilitated the mutual authentication between users and UAVs, allowing them to securely exchange session keys for encrypted communication. The use of HC scalar multiplication and identity obfuscation techniques further strengthens the protocol's resilience against various physical and logical attacks, including GPS spoofing, jamming, eavesdropping and code injection. We have validated our protocol's robustness through formal security assessments using the Scyther verification tool and ROM model, as well as informal analysis. Our performance evaluations demonstrate that the HCFAIUN protocol incurs lower computational, communication and storage costs compared to benchmark schemes, making it an efficient solution for secure UAV communication.

In Chapter 5, we provided a discussion on a secure cryptosystem for secure data transmission in IoT-based UAV networks. We presented a hyperelliptic curve-based cryptosystem which is carried out with three main stages. In the first registration stage, both EO and UAVs enrol with GCS to obtain an anonymous identity, followed by the secure mutual authentication of EO and UAVs for data transmission. The system is designed and developed with key operations such as HC of genus-2, secure hashing, XOR, random nonce and timestamps to generate shared session keys for further communication in IoT-based

UAV networks. The timestamp validation during the transmission of messages provides the session key freshness. The lightweight operations utilized in the cryptosystem are not only efficient in terms of high-level security but also provide lower computation(10.33 ms), communication and storage overhead in comparison with benchmark schemes. The system provides formal analysis using ROM and scyther tools rather than the existing AVISPA (Automated Validation of Internet Security Protocols and Applications) tool due to the attack graph feature. The cryptosystem successfully prevents the attempts of adversaries such as man-in-the-middle, forward secrecy, UAV capture and other known attacks by provable security, as mentioned in the informal analysis section.

6.2 Future Scope

This section provides enhancement of our proposed work through the following future directions:

1. **Quantum-resistant Cryptography**
   The emergence of quantum computing could cause conventional cryptography techniques susceptible. Thus, The post-quantum cryptography-based authentication can further enhance the security of IoT-based UAV networks. Lattice-based cryptosystems can be utilised to further enhance the robustness of proposed G2CAIUN, HCFAIUN and secure cryptosystem with the hardness of the shortest vector in multidimensional space.

2. **Dynamic UAV Topologies**
   A primary objective is to create protocols and algorithms capable of adapting to these constantly evolving topologies. This requires building systems that can handle the continual movement and reconfiguration of drones without sacrificing security or performance. For example, traffic authorities may employ these advanced UAV networks to monitor traffic flow, detect accidents, and manage congestion in real-time. The drones would need to interact quickly with one another and with ground control centres, ensuring that the data they collect is accurate and up-to-date.

3. **Application-aware Authentication Mechanism:**

   Application-aware authentication systems can be designed to adjust security measures based on the individual requirements and features of distinct apps. In the context of UAV networks, this entails building authentication protocols that can adapt to the particular needs of various use cases, such as traffic management, emergency response, and environmental monitoring. UAVs may need to interact with several ground control stations and other UAVs to monitor traffic flow, detect accidents, and manage congestion. An application-aware authentication strategy can prioritize low-latency communication and real-time data exchange, ensuring that traffic authorities receive timely and correct information. This technique can also contain context-aware security features, such as altering the amount of encryption based on the sensitivity of the data being transmitted.

4. **Aggregate Authentication Mechanism:**

   Aggregate authentication systems can simplify the authentication process and lessen the overall network load in a smart city where many UAVs are deployed for different purposes. Several UAVs can combine their authentication requests and carry out a single, group authentication procedure rather than each UAV authenticating with a central server separately. This results in speedier and more effective authentication by lowering the transmission overhead and the computational load. In a smart city, where several UAVs are deployed for diverse applications, aggregate authentication systems can expedite the authentication process, decreasing the overall stress on the network. For example, instead of each UAV separately authenticating with a central server, many UAVs can aggregate their authentication requests and complete a single, collective authentication procedure. This not only decreases the computational strain but also minimizes the communication overhead, resulting in faster and more efficient authentication.

5. **Formal Security analysis through Proverif**
   The proposed work can be further analysed using the Proverif tool, which employs the applied pi-calculus to convert protocols into Horn clauses for automated reasoning over security characteristics, facilitating unbounded session verification. Despite the generation of attack graphs, Poverif comes with a command line interface and facilitates an extensive range of cryptographic primitives, encompassing symmetric and asymmetric encryption, digital signatures, and hash functions.

6.3 Social Impact

This section provides the impact of our proposed work on people and communities:

- The secure communication protocol can significantly improve public safety by ensuring reliable and secure data transmission in emergency situations. UAVs can be used for search and rescue operations, monitoring natural disasters, and providing real-time data to emergency responders.

- This research can lead to cost savings in various industries, such as logistics, agriculture, and public safety. This can drive economic growth and create new opportunities for businesses and entrepreneurs.

- Mutual authentication prevents unauthorized access, reducing the risks of malicious drone takeovers, smuggling, and terrorism.

- Secure authentication helps prevent drone collisions, airspace violations, and interference with emergency services.

Appendix A

List of Publications

International Journals

1. J. Sharma and P. S. Mehra, Secure communication in IOT-based UAV networks: A systematic survey, Internet of Things, vol. 23, p. 100883, Jul. 2023, doi: 10.1016/j.iot.2023.100883.(SCIE- 7.6)

2. J. Sharma and P. S. Mehra, HCFAIUN: A novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in IoT-based UAV networks, Vehicular Communications, Elsevier, vol. 49, p. 100834, Oct. 2024, doi: 10.1016/j.vehcom.2024.100834. (SCIE- 6.5)

3. J. Sharma and P. S. Mehra, G2CAIUN: A novel Genus-2 curve-based authentication for secure data transmission in IoT-based UAV networks, Physical Communication, vol. 71, p. 102647, Aug. 2025, doi: 10.1016/j.phycom.2025.102647 (SCIE- 2.2)

4. J. Sharma and P. S. Mehra, A Survey on Quantum Resistant Cryptography for Secure Communication in IoT-based UAV networks [Communicated].

5. J. Sharma and P. S. Mehra, Quantum-Resistant Lattice and Hyperelliptic Curve based Hybrid Cryptosystem for Secure Data Transmission in IoT-based UAV networks [Communicated].

International Conferences

1. J. Sharma and P. S. Mehra, A Survey of Security Challenges and Existing Prevention Methods in FANET, in Intelligent Data Analytics, IoT, and Blockchain, 1st ed., Boca Raton: Auerbach Publications, 2023, pp. 252262. doi: 10.1201/9781003371380-24.

2. J. Sharma and P. S. Mehra, A Secure Cryptosystem for Secure Data Transmission in IoT-based UAV Networks, in 2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC), Ghaziabad, India: IEEE, Nov. 2024, pp. 16. doi: 10.1109/AKGEC62572.2024.10868597.

Patent

1. J. Sharma and P. S. Mehra, Secure Quantum Cryptography System and Method for Safe Communication and Storage of IoT-Based Data Published(2024), Application Number: 202311064981, Indian Patent Office.

Book Chapter

1. J. Sharma and P.S. Mehra, Secure Communication and Authentication in IoT-Based UAV Networks, in Network Optimization in Intelligent Internet of Things Applications, 1st ed., Boca Raton: Chapman and Hall/CRC, 2024, pp. 257273. doi: 10.1201/9781003405535-20.

References

[1] E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, “Internet of Things in Smart Cities: Comprehensive Review, Open Issues, and Challenges,” *IEEE Internet Things J.*, vol. 11, pp. 34941–34952, Nov. 2024.

[2] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, “Internet of Things: Security and Solutions Survey,” *Sensors*, vol. 22, p. 7433, Sept. 2022.

[3] *521-2019 - IEEE Standard Letter Designations for Radar-Frequency Bands.* Place of publication not identified: IEEE, 2020. OCLC: 1156377734.

[4] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, “A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques,” vol. 111, p. 102324.

[5] DGCA, “Know about UAS types.”

[6] S. Zaidi, M. Atiquzzaman, and C. T. Calafate, “Internet of Flying Things (IoFT): A Survey,” *Computer Communications*, vol. 165, pp. 53–74, Jan. 2021.

[7] S. Ullah, Z. Jiangbin, M. T. Hussain, N. Din, F. Ullah, and M. U. Farooq, “A perspective trend of hyperelliptic curve cryptosystem for lighted weighted environments,” *Journal of Information Security and Applications*, vol. 70, p. 103346, Nov. 2022.

[8] D. He, S. Chan, and M. Guizani, “Communication Security of Unmanned Aerial Vehicles,” *IEEE Wireless Communications*, vol. 24, pp. 134–139, Aug. 2017.

[9] S. Tiwari, “Ukraine Shoots Laser Weapons At Russian Suicide Drones,” Dec. 2022.

[10] V. K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, G. Sharma, and I. E. Davidson, “Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study,” *IEEE Access*, vol. 10, pp. 1475–1492, 2022.

[11] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y.-N. Li, “Secure communications in unmanned aerial vehicle network,” in *Information Security Practice and Experience* (J. K. Liu and P. Samarati, eds.), vol. 10701, pp. 601–620, Springer International Publishing. Series Title: Lecture Notes in Computer Science.

[12] A. Badshah, G. Abbas, M. Waqas, S. Tu, Z. H. Abbas, F. Muhammad, and S. Chen, “USAF-IoD: Ultralightweight and Secure Authenticated Key Agreement Framework for Internet of Drones Environment,” *IEEE Trans. Veh. Technol.*, vol. 73, pp. 10963–10977, Aug. 2024.

[13] M. Tanveer, H. Alasmary, N. Kumar, and A. Nayak, “SAAF-IoD: Secure and Anonymous Authentication Framework for the Internet of Drones,” *IEEE Transactions on Vehicular Technology*, vol. 73, pp. 232–244, Jan. 2024.

[14] V. O. Nyangaresi, “Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles,” *High-Confidence Computing*, vol. 3, p. 100154, Dec. 2023.

[15] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, “Anonymous Mutual and Batch Authentication with Location Privacy of UAV in FANET,” *Drones*, vol. 6, p. 14, Jan. 2022.

[16] 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, pp. 1339–1353, Jan. 2022.

[17] 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.

[18] M. S. Haque and M. U. Chowdhury, “A New Cyber Security Framework Towards Secure Data Communication for Unmanned Aerial Vehicle (UAV),” in *Security and Privacy in Communication Networks* (X. Lin, A. Ghorbani, K. Ren, S. Zhu, and A. Zhang, eds.), vol. 239, pp. 113–122, Cham: Springer International Publishing, 2018. Series Title: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.

[19] D. Alexander, “Drone Hunters: 9 of the Most Effective Anti-Drone Technologies for Shooting Drones out of the Sky,” Nov. 2021.

[20] A. Liszewski, “Parachuting Quadcopter Shoots Off Its Own Propellers to Take Out Other Drones,” Apr. 2022.

[21] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, “A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks,” *Ad Hoc Networks*, vol. 133, p. 102894, Aug. 2022.

[22] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, “Security threats and mitigation techniques in UAV communications: A comprehensive survey,” vol. 10, pp. 112858–112897.

[23] P. Chiaramonte, “U.S. Military Drones Infected With Mysterious Computer Virus,” Jan. 2017.

[24] A. K. Somani, R. S. Shekhawat, A. Mundra, S. Srivastava, and V. K. Verma, eds., *Smart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019*, vol. 141 of *Smart Innovation, Systems and Technologies*. Singapore: Springer Singapore, 2020.

[25] M. Faraji-Biregani and R. Fotohi, “Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles,” *The Journal of Supercomputing*, vol. 77, pp. 5076–5103, May 2021.

[26] C. Li, Y. Xu, J. Xia, and J. Zhao, "Protecting Secure Communication Under UAV Smart Attack With Imperfect Channel Estimation," *IEEE Access*, vol. 6, pp. 76395–76401, 2018.

[27] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Computer Networks*, vol. 163, p. 106877, Nov. 2019.

[28] L. Wang, Y. Chen, P. Wang, and Z. Yan, "Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications," *IEEE Communications Standards Magazine*, vol. 5, pp. 41–47, Dec. 2021.

[29] K. Best, J. Schmid, S. Tierney, J. Awan, N. Beyene, M. Holliday, R. Khan, and K. Lee, *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools.* RAND Corporation, 2020.

[30] H. Alrashede and R. A. Shaikh, "IMSI Catcher Detection Method for Cellular Networks," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, (Riyadh, Saudi Arabia), pp. 1–6, IEEE, May 2019.

[31] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022.

[32] H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution," vol. 74, no. 10, pp. 4928–4944.

[33] M. Riahi Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," vol. 85, pp. 386–401.

[34] 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, Sept. 2020.

[35] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering,"

[36] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones," Apr. 2019. arXiv:1904.06829 [cs].

[37] G. Wang, K. Lim, B.-S. Lee, and J. Y. Ahn, "Handover Key Management in an LTE-based Unmanned Aerial Vehicle Control Network," in *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, (Prague), pp. 200–205, IEEE, Aug. 2017.

[38] S. Atoev, O.-J. Kwon, C.-Y. Kim, S.-H. Lee, Y.-R. Choi, and K.-R. Kwon, "The Secure UAV Communication Link Based on OTP Encryption Technique," in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, (Zagreb, Croatia), pp. 1–3, IEEE, July 2019.

[39] Y.-J. Chen and L.-C. Wang, “Privacy Protection for Internet of Drones: A Network Coding Approach,” *IEEE Internet of Things Journal*, vol. 6, pp. 1719–1730, Apr. 2019.

[40] F. S. Alrayes, S. S. Alotaibi, K. A. Alissa, M. Maashi, A. Alhogail, N. Alotaibi, H. Mohsen, and A. Motwakel, “Artificial Intelligence-Based Secure Communication and Classification for Drone-Enabled Emergency Monitoring Systems,” *Drones*, vol. 6, p. 222, Aug. 2022.

[41] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, “A data authentication scheme for UAV ad hoc network communication,” *The Journal of Supercomputing*, vol. 76, pp. 4041–4056, June 2020.

[42] K. Yoon, D. Park, Y. Yim, K. Kim, S. K. Yang, and M. Robinson, “Security Authentication System Using Encrypted Channel on UAV Network,” in *2017 First IEEE International Conference on Robotic Computing (IRC)*, (Taichung, Taiwan), pp. 393–398, IEEE, Apr. 2017.

[43] A. Shoufan, “Continuous authentication of UAV flight command data using behaviometrics,” in *2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, (Abu Dhabi), pp. 1–6, IEEE, Oct. 2017.

[44] G. Cho, J. Cho, S. Hyun, and H. Kim, “SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles,” *Applied Sciences*, vol. 10, p. 3149, Apr. 2020.

[45] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, “TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment,” *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 6903–6916, July 2019.

[46] 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*, vol. 9, p. 62, Jan. 2020.

[47] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K. R. Choo, and Y. Park, “Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment,” *IEEE Internet of Things Journal*, vol. 7, pp. 3184–3197, Apr. 2020.

[48] 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.

[49] X. H. Cao, X. Du, and E. P. Ratazzi, “A Light-Weight Authentication Scheme for Air Force Internet of Things,” in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, (Shanghai, China), pp. 1–6, IEEE, May 2019.

[50] Y. Zhang, D. He, L. Li, and B. Chen, “A lightweight authentication and key agreement scheme for Internet of Drones,” *Computer Communications*, vol. 154, pp. 455–464, Mar. 2020.

[51] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment," *IEEE Internet Things J.*, vol. 6, pp. 3572–3584, Apr. 2019.

[52] T. Alladi, V. Chamola, Naren, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Computer Communications*, vol. 160, pp. 81–90, July 2020.

[53] 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, pp. 53–63, Jan. 2020.

[54] 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. 24325–24339, 2018.

[55] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, "Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone," *Sensors*, vol. 21, p. 2057, Mar. 2021.

[56] S. U. Jan, F. Qayum, and H. U. Khan, "Design and Analysis of Lightweight Authentication Protocol for Securing IoD," *IEEE Access*, vol. 9, pp. 69287–69306, 2021.

[57] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 3319–3332, Sept. 2021.

[58] H. Khalid, S. J. Hashim, S. Mumtazah Syed Ahamed, F. Hashim, and M. A. Chaudhary, "Secure Real-time Data Access Using Two-Factor Authentication Scheme for the Internet of Drones," in *2021 IEEE 19th Student Conference on Research and Development (SCOReD)*, (Kota Kinabalu, Malaysia), pp. 168–173, IEEE, Nov. 2021.

[59] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," *IEEE Systems Journal*, vol. 15, pp. 4431–4438, Sept. 2021.

[60] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Vehicular Communications*, vol. 23, p. 100249, June 2020.

[61] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518–538, Feb. 2020.

[62] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-Blockchain-Based Ultrareliable Caching for Edge-Enabled UAV Networks," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 5723–5736, Oct. 2019.

[63] M. A. Ferrag and L. Maglaras, "DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services," *Computers*, vol. 8, p. 58, Aug. 2019.

[64] Y. Tan, J. Liu, and N. Kato, "Blockchain-Based Key Management for Heterogeneous Flying Ad Hoc Network," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 7629–7638, Nov. 2021.

[65] A. Islam and S. Y. Shin, "BUS: A Blockchain-Enabled Data Acquisition Scheme With the Assistance of UAV Swarm in Internet of Things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019.

[66] T. Fernndez-Carams, O. Blanco-Novoa, M. Surez-Albela, and P. Fraga-Lamas, "A UAV and Blockchain-Based System for Industry 4.0 Inventory and Traceability Applications," in *5th International Electronic Conference on Sensors and Applications*, p. 26, MDPI, Nov. 2018.

[67] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A New Secure Data Dissemination Model in Internet of Drones," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, (Shanghai, China), pp. 1–6, IEEE, May 2019.

[68] 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.

[69] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu, "Securing ICN-Based UAV Ad Hoc Networks with Blockchain," *IEEE Communications Magazine*, vol. 57, pp. 26–32, June 2019.

[70] A. Islam and S. Y. Shin, "BHMUS: Blockchain Based Secure Outdoor Health Monitoring Scheme Using UAV in Smart City," in *2019 7th International Conference on Information and Communication Technology (ICoICT)*, (Kuala Lumpur, Malaysia), pp. 1–6, IEEE, July 2019.

[71] I. Garca-Magario, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Networks*, vol. 86, pp. 72–82, Apr. 2019.

[72] R. Han, L. Bai, J. Liu, and P. Chen, "Blockchain-Based GNSS Spoofing Detection for Multiple UAV Systems," *Journal of Communications and Information Networks*, vol. 4, pp. 81–88, June 2019.

[73] A. Mitra, B. Bera, and A. K. Das, "Design and Testbed Experiments of Public Blockchain-Based Security Framework for IoT-Enabled Drone-Assisted Wildlife Monitoring," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, (Vancouver, BC, Canada), pp. 1–6, IEEE, May 2021.

[74] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment," *Computer Networks*, vol. 195, p. 108219, Aug. 2021.

[75] T. Nguyen, R. Katila, and T. N. Gia, "A Novel Internet-of-Drones and Blockchain-based System Architecture for Search and Rescue," in *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, (Denver, CO, USA), pp. 278–288, IEEE, Oct. 2021.

[76] A. Allouch, O. Cheikhrouhou, A. Kouba, K. Toumi, M. Khalgui, and T. Nguyen Gia, "UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones," *Sensors*, vol. 21, p. 3049, Apr. 2021.

[77] M. P. Arthur, "Detecting Signal Spoofing and Jamming Attacks in UAV Networks using a Lightweight IDS," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, (Beijing, China), pp. 1–5, IEEE, Aug. 2019.

[78] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, pp. 1594–1606, Sept. 2018.

[79] R. Fotohi, "Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system," *Reliability Engineering & System Safety*, vol. 193, p. 106675, Jan. 2020.

[80] R. Zhang, J.-P. Condomines, N. Larrieu, and R. Chemali, "Design of a novel network intrusion detection system for drone communications," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, (London), pp. 1–10, IEEE, Sept. 2018.

[81] R. A. Ramadan, A.-H. Emara, M. Al-Sarem, and M. Elhamahmy, "Internet of Drones Intrusion Detection Using Deep Learning," *Electronics*, vol. 10, p. 2633, Oct. 2021.

[82] J. Whelan, A. Almehmadi, and K. El-Khatib, "Artificial intelligence for intrusion detection systems in Unmanned Aerial Vehicles," *Computers and Electrical Engineering*, vol. 99, p. 107784, Apr. 2022.

[83] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," *Array*, vol. 14, p. 100135, July 2022.

[84] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," *Digital Investigation*, vol. 30, pp. 52–72, Sept. 2019.

[85] F. Iqbal, B. Yankson, M. A. AlYammahi, N. AlMansoori, S. M. Qayed, and B. Shah, "Drone forensics: examination and analysis,"

[86] "The Drone Rules, 2021," Jan. 2022.

[87] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges," *Drones*, vol. 5, p. 42, May 2021.

[88] F. E. Salamh, U. Karabiyik, and M. K. Rogers, "RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H," *Sensors*, vol. 19, p. 3246, July 2019.

[89] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen, and F. Tsai, "Drone Forensic Investigation: DJI Spark Drone as A Case Study," *Procedia Computer Science*, vol. 159, pp. 1890–1899, 2019.

[90] Z. Shi, X. Chang, C. Yang, Z. Wu, and J. Wu, "An Acoustic-Based Surveillance System for Amateur Drones Detection and Localization," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 2731–2739, Mar. 2020.

[91] J.-P. Condomines, R. Zhang, and N. Larrieu, "Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation," *Ad Hoc Networks*, vol. 90, p. 101759, July 2019.

[92] F. E. Salamh, M. M. Mirza, and U. Karabiyik, "UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies," *Electronics*, vol. 10, p. 733, Mar. 2021.

[93] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," *Digital Investigation*, vol. 22, pp. S3–S14, Aug. 2017.

[94] S. Safavat and D. B. Rawat, "OptiML: An enhanced ML approach towards design of SDN based UAV networks," in *ICC 2022 - IEEE International Conference on Communications*, pp. 1–6, IEEE.

[95] J. Ali, R. H. Jhaveri, M. Alswailim, and B.-h. Roh, "ESCALB: An effective slave controller allocation-based load balancing scheme for multi-domain SDN-enabled-IoT networks," vol. 35, no. 6, p. 101566.

[96] Y. Zhao, Z. Zheng, and Y. Liu, "Survey on computational-intelligence-based UAV path planning," *Knowledge-Based Systems*, vol. 158, pp. 54–64, Oct. 2018.

[97] A. Saravanakumar, A. Kaviyarasu, and R. Ashly Jasmine, "Sampling based path planning algorithm for UAV collision avoidance," *Sdhan*, vol. 46, p. 112, Sept. 2021.

[98] R. DuToit, M. Holt, M. Lyle, and S. Biaz, "UAV Collision Avoidance Using RRT* and LOS Maximization Technical Report #CSSE12 - 03,"

[99] S. Huang and R. S. H. Teo, "Computationally Efficient Visibility Graph-Based Generation Of 3D Shortest Collision-Free Path Among Polyhedral Obstacles For Unmanned Aerial Vehicles," in *2019 International Conference on Unmanned Aircraft Systems (ICUAS)*, (Atlanta, GA, USA), pp. 1218–1223, IEEE, June 2019.

[100] A. Sonmez, E. Kocyigit, and E. Kugu, "Optimal path planning for UAVs using Genetic Algorithm," in *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*, (Denver, CO, USA), pp. 50–55, IEEE, June 2015.

[101] K. Kelchtermans and T. Tuytelaars, "How hard is it to cross the room? – Training (Recurrent) Neural Networks to steer a UAV," Feb. 2017. arXiv:1702.07600 [cs].

[102] L. Wang, K. Wang, C. Pan, and N. Aslam, "Joint Trajectory and Passive Beamforming Design for Intelligent Reflecting Surface-Aided UAV Communications: A Deep Reinforcement Learning Approach," *IEEE Transactions on Mobile Computing*, pp. 1–11, 2022.

[103] M. Radmanesh, M. Kumar, P. H. Guentert, and M. Sarim, “Overview of Path-Planning and Obstacle Avoidance Algorithms for UAVs: A Comparative Study,” *Unmanned Systems*, vol. 06, pp. 95–118, Apr. 2018.

[104] K. McGuire, G. de Croon, C. De Wagter, K. Tuyls, and H. Kappen, “Efficient Optical Flow and Stereo Vision for Velocity Estimation and Obstacle Avoidance on an Autonomous Pocket Drone,” *IEEE Robotics and Automation Letters*, vol. 2, pp. 1070–1076, Apr. 2017.

[105] P. Ramon Soria, B. Arrue, and A. Ollero, “Detection, Location and Grasping Objects Using a Stereo Sensor on UAV in Outdoor Environments,” *Sensors*, vol. 17, p. 103, Jan. 2017.

[106] A. Al-Kaff, F. Garca, D. Martn, A. De La Escalera, and J. Armingol, “Obstacle Detection and Avoidance System Based on Monocular Camera and Size Expansion Algorithm for UAVs,” *Sensors*, vol. 17, p. 1061, May 2017.

[107] J. Hu, H. Zhang, Z. Li, C. Zhao, Z. Xu, and Q. Pan, “Object traversing by monocular UAV in outdoor environment,” *Asian Journal of Control*, vol. 23, pp. 2766–2775, Nov. 2021.

[108] H. V. Abeywickrama, B. A. Jayawickrama, Y. He, and E. Dutkiewicz, “Potential Field Based Inter-UAV Collision Avoidance Using Virtual Target Relocation,” in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, (Porto), pp. 1–5, IEEE, June 2018.

[109] P. K. Selvam, G. Raja, V. Rajagopal, K. Dev, and S. Knorr, “Collision-free Path Planning for UAVs using Efficient Artificial Potential Field Algorithm,” in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, (Helsinki, Finland), pp. 1–5, IEEE, Apr. 2021.

[110] J. Sun, J. Tang, and S. Lao, “Collision Avoidance for Cooperative UAVs With Optimized Artificial Potential Field Algorithm,” *IEEE Access*, vol. 5, pp. 18382–18390, 2017.

[111] P. Parghi, R. Dhamija, and A. K. Agrawal, “Innovative Approach to Onboard Media Forensic of a Drone,” *IOT with Smart Systems*, pp. 307–314, 2022.

[112] M. Z. Anwar, Z. Kaleem, and A. Jamalipour, “Machine Learning Inspired Sound-Based Amateur Drone Detection for Public Safety Applications,” *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 2526–2534, Mar. 2019.

[113] X. Chang, C. Yang, J. Wu, X. Shi, and Z. Shi, “A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays,” in *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, (Sheffield), pp. 573–577, IEEE, July 2018.

[114] H. Liu, F. Qu, Y. Liu, W. Zhao, and Y. Chen, “A drone detection with aircraft classification based on a camera array,” *IOP Conference Series: Materials Science and Engineering*, vol. 322, p. 052005, Mar. 2018.

[115] B. Taha and A. Shoufan, “Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research,” *IEEE Access*, vol. 7, pp. 138669–138682, 2019.

[116] E. Unlu, E. Zenou, and N. Riviere, “Using Shape Descriptors for UAV Detection,” *Electronic Imaging*, vol. 30, pp. 128–1–128–5, Jan. 2018.

[117] S. Khandelwal, “MalDrone First Ever Backdoor Malware for Drones,” Jan. 2015.

[118] Y. Sung, S. Jang, Y.-S. Jeong, and J. H. J. J. Park, “Malware classification algorithm using advanced Word2vec-based Bi-LSTM for ground control stations,” *Computer Communications*, vol. 153, pp. 342–348, Mar. 2020.

[119] D. R. Hankerson, A. J. Menezes, S. A. Vanstone, D. Hankerson, A. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography.* Springer professional computing, New York, NY: Springer, 2004.

[120] L. C. Washington, *Elliptic curves: number theory and cryptography.* Discrete mathematics and its applications, Boca Raton, FL: Chapman & Hall/CRC, 2nd ed ed., 2008. OCLC: ocn192045762.

[121] S. Zhang, Y. Liu, Z. Han, and Z. Yang, “A Lightweight Authentication Protocol for UAVs Based on ECC Scheme,” *Drones*, vol. 7, p. 315, May 2023.

[122] G. Bansal and B. Sikdar, “S-MAPS: Scalable Mutual Authentication Protocol for Dynamic UAV Swarms,” *IEEE Trans. Veh. Technol.*, vol. 70, pp. 12088–12100, Nov. 2021.

[123] S. Hussain, I. Ullah, H. Khattak, M. Adnan, S. Kumari, S. S. Ullah, M. A. Khan, and S. J. Khattak, “A Lightweight and Formally Secure Certificate Based Signcryption With Proxy Re-Encryption (CBSRE) for Internet of Things Enabled Smart Grid,” *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[124] R. Alimoradi, “A Study of Hyperelliptic Curves in Cryptography,” *International Journal of Computer Network and Information Security*, vol. 8, pp. 67–72, Aug. 2016.

[125] Y. Gao, S. F. Al-Sarawi, and D. Abbott, “Physical unclonable functions,” *Nature Electronics*, vol. 3, pp. 81–91, 2 2020.

[126] A. Yadav, S. Kumar, and J. Singh, “A review of Physical Unclonable Functions (PUFs) and its applications in IoT environment,” *Lecture notes in networks and systems*, pp. 1–13, 1 2022.

[127] H. Ning, F. Farha, A. Ullah, and L. Mao, “Physical unclonable function: architectures, applications and challenges for dependable security,” *IET Circuits Devices & Systems*, vol. 14, pp. 407–424, 2 2020.

[128] H. Y. Tran, J. Hu, and W. Hu, “Biometrics-Based Authenticated Key Exchange with Multi-Factor Fuzzy Extractor,” May 2024. arXiv:2405.11456 [cs].

[129] M. Tanveer, A. Aldosary, N. Kumar, and S. A. Aldossari, “SEAF-IoD: Secure and efficient user authentication framework for the Internet of Drones,” *Computer Networks*, vol. 247, p. 110449, June 2024.

[130] A. F. S. Pino, P. H. Ruiz, A. Mon, and C. A. Collazos, “Systematic literature review on mechanisms to measure the technological maturity of the Internet of Things in enterprises,” *Internet of Things*, vol. 25, p. 101082, 1 2024.

[131] J. Sharma and P. S. Mehra, *A Survey of Security Challenges and Existing Prevention Methods in FANET*. Boca Raton: Auerbach Publications, 1 ed., Sept. 2023.

[132] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, “Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends,” *Intel Serv Robotics*, Jan. 2023.

[133] . Bekmezci, O. K. Sahingoz, and . Temel, “Flying Ad-Hoc Networks (FANETs): A survey,” *Ad Hoc Networks*, vol. 11, pp. 1254–1270, May 2013.

[134] J. Sharma and P. S. Mehra, “Secure communication in IOT-based UAV networks: A systematic survey,” *Internet of Things*, vol. 23, p. 100883, Oct. 2023.

[135] B. Deebak and F. Al-Turjman, “A smart lightweight privacy preservation scheme for IoT-based UAV communication systems,” *Computer Communications*, vol. 162, pp. 102–117, Oct. 2020.

[136] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, pp. 198–208, Mar. 1983.

[137] R. Canetti and H. Krawczyk, “Universally Composable Notions of Key Exchange and Secure Channels,” in *Advances in Cryptology EUROCRYPT 2002* (G. Goos, J. Hartmanis, J. Van Leeuwen, and L. R. Knudsen, eds.), vol. 2332, pp. 337–351, Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

[138] W. Stallings, *Cryptography and network security: principles and practice*. Boston: Pearson, seventh edition ed., 2017.

[139] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, “A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment,” *IEEE Internet Things J.*, vol. 9, pp. 9918–9933, June 2022.

[140] J. Sharma and P. S. Mehra, “HCFAIUN: A novel hyperelliptic curve and fuzzy extractor-based authentication for secure data transmission in IoT-based UAV networks,” *Vehicular Communications*, vol. 49, p. 100834, Oct. 2024.

[141] J. Sharma, P. Singh Mehra, D. Chawla, D. Dabas, and A. Jamshed, *Secure Communication and Authentication in IoT-Based UAV Networks*. Boca Raton: Chapman and Hall/CRC, 1 ed., Aug. 2024.

[142] C. Cremers, “Scyther tool,” 2014.

[143] C. J. F. Cremers, “The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols,” in *Computer Aided Verification* (A. Gupta and S. Malik, eds.), vol. 5123, pp. 414–418, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. ISSN: 0302-9743, 1611-3349 Series Title: Lecture Notes in Computer Science.

[144] 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 Trans. Veh. Technol.*, vol. 71, pp. 10374–10388, Oct. 2022.

[145] 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. 19836–19851, 2022.

[146] Y. Zhang, L. Meng, M. Zhang, and W. Meng, "A secure and lightweight batch authentication scheme for Internet of Drones environment," *Vehicular Communications*, vol. 44, p. 100680, Dec. 2023.

[147] 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*, vol. 23, p. 2034, Feb. 2023.

[148] R. Randhawa and M. Verma, "A Comprehensive Review on Recent Advancements in the Field of Internet of Things, Its Challenges and Future Scope," *Optoelectron.Instrument.Proc.*, vol. 59, pp. 137–147, Feb. 2023.

[149] J. Sharma and P. S. Mehra, "Secure communication in iot-based uav networks: A systematic survey," *Internet of Things*, vol. 23, p. 100883, 2023.

[150] D. Chawla and P. S. Mehra, "A survey on quantum computing for internet of things security," *Procedia Computer Science*, vol. 218, pp. 2191–2200, 2023. International Conference on Machine Learning and Data Engineering.

[151] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5g-enabled iot: Challenges, opportunities and solutions," *Internet of Things*, vol. 24, p. 100950, 2023.

[152] K. Messaoudi, O. S. Oubbati, A. Rachedi, A. Lakas, T. Bendouma, and N. Chaib, "A survey of UAV-based data collection: Challenges, solutions and future perspectives," *Journal of Network and Computer Applications*, vol. 216, p. 103670, July 2023.

[153] A. Khan, M. M. A. Khan, M. A. Javeed, M. U. Farooq, A. Akram, and C. Wang, "Multilevel Privacy Controlling Scheme to Protect Behavior Pattern in Smart IoT Environment," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–17, July 2021.

[154] S. Ogunbunmi, Y. Chen, E. Blasch, and G. Chen, "A Survey on Reputation Systems for UAV Networks," *Drones*, vol. 8, p. 253, June 2024.

[155] M. U. F. Qaisar, W. Yuan, P. Bellavista, S. A. Chaudhry, A. Ahmed, and M. Imran, "Reliable and Resilient Communication in Duty Cycled Software Defined Wireless Sensor Networks," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, (Rome, Italy), pp. 397–402, IEEE, May 2023.

[156] D. Chawla and P. S. Mehra, "Qaka: A novel quantum authentication and key agreement (qaka) protocol using quantum entanglement for secure communication among iot devices," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 3, p. e4957, 2024.

[157] D. Chawla and P. S. Mehra, “Qsmah: A novel quantum-based secure cryptosystem using mutual authentication for healthcare in the internet of things,” *Internet of Things*, vol. 24, p. 100949, 2023.

[158] S. M. Gilani, A. Anjum, A. Khan, M. H. Syed, S. A. Moqurrab, and G. Srivastava, “A robust Internet of Drones security surveillance communication network based on IOTA,” *Internet of Things*, vol. 25, p. 101066, Apr. 2024.

[159] M. K. Banafaa, . Pepeolu, I. Shayea, A. Alhammadi, Z. A. Shamsan, M. A. Razaz, M. Alsagabi, and S. Al-Sowayan, “A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges,” *IEEE Access*, vol. 12, pp. 7786–7826, 2024.

[160] M. Tanveer, A. Aldosary, S.-u.-d. Khokhar, A. K. Das, S. A. Aldossari, and S. A. Chaudhry, “PAF-IoD: PUF-Enabled Authentication Framework for the Internet of Drones,” *IEEE Trans. Veh. Technol.*, pp. 1–15, 2024.

[161] S. O. Ajakwe, D.-S. Kim, and J.-M. Lee, “Drone Transportation System: Systematic Review of Security Dynamics for Smart Mobility,” *IEEE Internet Things J.*, vol. 10, pp. 14462–14482, Aug. 2023.

[162] I. Chandran and K. Vipin, “A PUF secured lightweight mutual authentication protocol for multi-UAV networks,” *Computer Networks*, vol. 253, p. 110717, Nov. 2024.

[163] Z. Zhang, C. Hsu, M. H. Au, L. Harn, J. Cui, Z. Xia, and Z. Zhao, “PRLAP-IOD: a PUF-based robust and lightweight authentication protocol for internet of drones,” *Computer Networks*, vol. 238, p. 110118, 11 2023.

[164] S. Javed, A. Hassan, R. Ahmad, W. Ahmed, R. Ahmed, A. Saadat, and M. Guizani, “State-of-the-Art and Future Research Challenges in UAV Swarms,” *IEEE Internet Things J.*, vol. 11, pp. 19023–19045, June 2024.

[165] G. S. Ilgi and Y. K. Ever, *Critical analysis of security and privacy challenges for the Internet of drones: a survey.* 1 2020.

[166] K. Mahmood, Z. Ghaffar, M. Farooq, K. Yahya, A. K. Das, and S. A. Chaudhry, “A Security Enhanced Chaotic-Map-Based Authentication Protocol for Internet of Drones,” *IEEE Internet Things J.*, vol. 11, pp. 22301–22309, June 2024.

[167] M. Saqib and A. H. Moon, “A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication,” *Computers & Security*, vol. 125, p. 103053, Feb. 2023.

Author Biography

Jatin Sharma is currently serving as an Assistant Professor in the Department of Computer Engineering at the Faculty of Technology, University of Delhi. He is pursuing his Ph.D. from Delhi Technological University in the Department of CSE. He received his M.Tech. in Computer Applications from Thapar Institute of Engineering and Technology, Patiala. He has completed his B.Tech. in Information Technology from JCDM College of Engineering, Sirsa. He has three years of Software Development experience at ITG Telematics Pvt Ltd, New Delhi. His research interests include the Internet of Things, Post-Quantum Cryptography, Unmanned Aerial Vehicles, Wireless ad hoc networks, Cryptography, and network security.