

## RESEARCH ARTICLE

# An Efficient Authentication and Access Control Protocol for Securing UAV Networks Against Anomaly-Based Intrusion

KHAISTA RAHMAN<sup>1</sup>, MUHAMMAD ASGHAR KHAN<sup>2</sup>, (Member, IEEE),  
FATEMEH AFGHAH<sup>3</sup>, (Senior Member, IEEE), GORDANA BARB<sup>4</sup>, NISREEN INNAB<sup>5</sup>,  
AND TANVEER AHMED CHEEMA<sup>1</sup>

<sup>1</sup>Department of Electronic Engineering, School of Engineering and Applied Sciences, Isra University, Islamabad 44000, Pakistan

<sup>2</sup>Faculty of Engineering Sciences and Technology, Hamdard University, Islamabad 44000, Pakistan

<sup>3</sup>Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA

<sup>4</sup>Department of Communications, Politehnica University of Timisoara, 300006 Timisoara, Romania

<sup>5</sup>Department of Computer Science and Information Systems, College of Applied Sciences, Almaarefa University, Riyadh 11597, Saudi Arabia

Corresponding author: Muhammad Asghar Khan (m.asghar@hamdard.edu.pk)

**ABSTRACT** UAV networks have gained widespread recognition across multiple industries due to their remarkable adaptability, prompting a fundamental transformation in operational procedures. However, utilizing the open wireless communication channel has consistently brought about significant privacy concerns as a prominent aspect within these networks. Moreover, UAVs are typically equipped with limited computing capabilities that hinder their ability to execute complex cryptographic algorithms. In light of these considerations, this paper proposes a security protocol for UAV networks that uses an authentication and access control mechanism to eliminate the possibility of any security breaches. The proposed scheme is based on hyperelliptic curve cryptography (HECC), which employs a smaller key size of 80 bits instead of the 160 bits required by elliptic curve cryptography (ECC). Remarkably, HECC offers equivalent security to other methods such as RSA, ECC, bilinear pairing, etc., and is, therefore, suitable for UAV networks. The proposed protocol is evaluated for security using the well-known Real-Or-Random (ROR) Oracle model. The AVISPA tool is employed to illustrate the security of the proposed protocol against adversarial scenarios in the on-the-fly model-checker (OFMC) and constraint-logic-based attack searcher (Cl-AtSe) models. Furthermore, the informal security analysis guarantees that the proposed protocol withstands possible attacks based on the Canetti-Krawczyk (CK) and Dolev–yao (DY) adversarial models. The comparative analysis of the proposed protocol's performance with other existing methods demonstrates the proposed protocol's viability in terms of computation and communication costs.

**INDEX TERMS** UAVs, security, authentication, access control, intrusion detection, hyperelliptic curve cryptography, AVISPA.

## I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), also known as drones, have acquired popularity over the past decade due to their extensive spectrum of industry-specific applications [1]. UAVs typically come in various sizes and configurations to facilitate autonomous or remote task execution without

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu<sup>1</sup>.

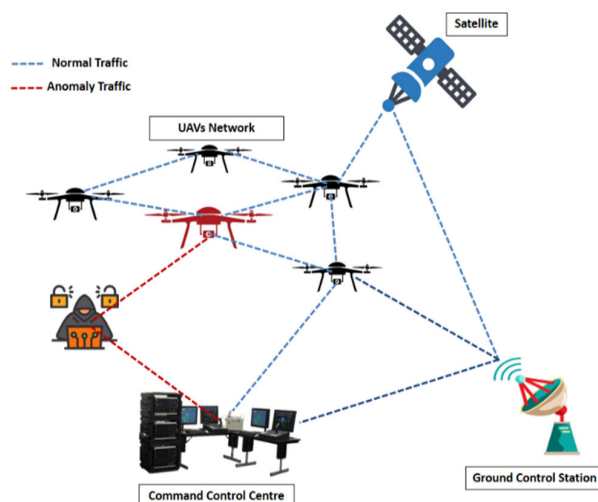
any manual intervention by the human operator. They are capable of transporting lethal or nonlethal payloads [2]. UAVs are typically outfitted with components that are essential to their operational capabilities. These components include data storage, rechargeable batteries for power supply, inertial measurement units (IMUs) for stability and control, and communication modules for real-time data exchange with ground control and operators. A UAV has various sensors, including radio detection and ranging sensors,

sonar-pulse distance sensors (ultrasonic), thermo-sensors, orientation sensors, light-pulse distance sensors (laser), and magnetic-field change sensors. Moreover, complemented by navigation aids, control units, and safety features, these essential components enable UAVs to perform various tasks across various applications, including aerial imaging and mapping, environmental monitoring and surveillance, and more [3]. Nevertheless, when a UAV operates independently, it may have restricted capabilities. However, when integrated into a network, these systems can effectively handle complex situations with significantly improved efficiency and reliability [4].

While adopting UAV networks unquestionably yields substantial advantages and simplifies numerous facets of our everyday existence, it's essential to consider the flip side, where these networks face cybersecurity obstacles due to constraints arising from operating on open wireless channels [5]. Primary cybersecurity concerns within UAV networks encompass issues related to data privacy and confidentiality, the potential for remote hijacking and unauthorized control, weaknesses in communication channels, the presence of threats such as jamming and global positioning system (GPS) spoofing, susceptibilities to malware and software-based threats, the risk of denial-of-service (DoS) attacks, challenges about physical security, supply chain vulnerabilities, adherence to regulatory standards, and the critical significance of implementing data transmission encryption [6], [7], [8]. Figure 1 provides an overview of the main entities within the UAV network and presents a potential cyber-attack scenario. Addressing these cybersecurity concerns necessitates a comprehensive strategy that combines encryption, intrusion detection systems, regular updates, and strict adherence to cybersecurity best practices [9]. Nonetheless, emphasizing the cybersecurity of UAV networks is crucial to ensure their reliable and secure operation in a diverse array of applications.

To address the challenges above effectively, implementing an authentication and access control protocol is imperative for detecting unauthorized UAVs [10]. Nevertheless, the development of such protocols encounters significant hindrances due to the limitations posed by UAVs' insufficient onboard computational capabilities. Consequently, these limitations render UAVs unable to undertake intricate cryptographic operations. Hence, the critical need arises to implement efficient security mechanisms to reduce the burdens associated with computation and communication costs [11]. Similarly, we analyze several proposed key agreements and authentication protocols [12], [13] for the UAV networks from the literature. However, most protocols have security flaws and scalability issues [18].

The security and efficiency of the authentication and access control protocols for UAV networks are based on computationally challenging problems such as Rivest-Shamir-Adleman (RSA) cryptography, bilinear pairing (BP), and elliptic curve cryptography (ECC) [14]. RSA cryptography, for instance, relies on solving significant factorization



**FIGURE 1.** An overview of the main entities within the UAV network and a potential cyber-attack scenario.

problems with keys, parameters, certificates, and identities that can be as long as 1024 bits [15]. However, this cryptographic approach could be better suited for resource-constrained networks, particularly for small UAVs, as these devices typically lack the onboard processing resources required to handle such complex computations effectively. Additionally, BP is considerably less efficient than RSA, slower due to the extensive pairing and map-to-point function computations it requires. A newer cryptographic approach, ECC, was introduced to address the limitations of RSA and bilinear pairing in resource-constrained environments [16], [17]. In ECC [19], key components like parameters, public keys, private keys, identities, and certificates are smaller, making them more suitable for such scenarios. In addition, the scheme's security and efficiency are based on using short 160-bit keys, unlike BP and RSA. However, the 160-bit key size must be more appropriate and cost-effective for resource-intensive devices. Consequently, a new cryptographic approach, HECC [20], a generalized form of ECC, was introduced. The HECC provides comparable security to BP and RSA but with smaller 80-bit keys, identities, and certificates, which is a more feasible option for UAVs. Additionally, its resistance to quantum attacks ensures long-term security in an evolving threat landscape. HECC's versatility allows for its implementation across various security applications, ensuring comprehensive UAV communications and data protection. Moreover, despite being less widespread, HECC is standardized and supported, facilitating integration into existing UAV networks. The HECC relies on the hash function, which is post-quantum resilient and efficient cryptographic operations, safeguarding UAVs against emerging cyber threats, including those posed by quantum computing technologies.

To mitigate the challenges above, we have formulated an authenticated access control protocol for detecting and mitigating unauthorized UAVs. Wireless communication over

public channels is susceptible to a spectrum of threats, including Denial-of-Service, Man-in-the-Middle, impersonation, and ESL attacks, which can disrupt public, administrative, and corporate sectors. To address these security concerns, our proposed scheme has been meticulously crafted with a primary focus on security and rigorously tested through the ROR oracle mode. The RoR Oracle model is a widely adopted tool for formal security verifications. It is used to verify the authenticity and integrity of data transmitted over insecure channels, such as those found in UAV networks. Also, the AVISPA tool is employed to illustrate the security of the proposed scheme against adversarial scenarios in the OFMC and CI-AtSe models. It significantly enhances overall security by providing formal verification and analysis of security protocols used in UAV networks. From a performance standpoint, the scheme is constructed utilizing the HECC, an advanced variant of ECC. The main contributions of this article are as follows:

- 1) This work introduces an authentication and access control protocol for UAV networks, utilizing hyperelliptic curve cryptography (HECC) and incorporating lightweight cryptographic primitives like hash operations.
- 2) The proposed scheme demonstrates robust resilience against well-known attacks, validated through a combination of informal security analysis and formal security analysis employing the ROR oracle mode.
- 3) The viability of the proposed scheme is verified through formal security validations conducted using the AVISPA tool.
- 4) Our findings also include a comprehensive efficiency analysis considering computation and communication costs. The findings indicate that the proposed scheme presents significant efficiency advantages, especially in computation and communication costs, compared to existing schemes.

The rest of the article is organized as follows: Section II discusses related work. Section III covers the network model. Construction of the proposed scheme is provided in Section IV. A security analysis of the proposed scheme is presented in Section V. In Section VI, we provide the performance analysis. Finally, Section VII comprises the conclusion.

## II. RELATED WORK

Within a UAV network, ensuring secure communication is of paramount importance as the communication predominantly occurs over an open and vulnerable wireless channel. The key challenges to be tackled encompass issues of authenticity, anonymity, and data integrity. Consequently, implementing a robust authentication scheme becomes imperative in the UAV environment to provide a clear defence against intrusions. Srinivas et al. [21] proposed a user authentication system for drones that incorporates many authentication elements, such as mobile devices, biometrics, and passwords, to address

these security concerns. The proposed approach employs ephemeral credentials to safeguard user privacy and mitigate the risk of illegitimate drone access. The proposed scheme primarily relied on reliable ground stations as gateways and remote control centres. However, the scheme [21] does not provide a failover authentication function [22]. Subsequently, Ali et al. [23] introduced an improved authentication protocol for IoD networks to enhance the existing approach [21]. In the study by Ali et al. [23], an AKA protocol was developed to facilitate continuous communication between the user and the drone. The technique uses the SHA-160 cryptographic hash algorithm and the XOR logical operation. However, the proposed method [23] is susceptible to several security threats, including user impersonation, privileged insider attacks, forgeries, and denial-of-service (DoS) attacks.

In their study, Tian et al. [24] introduced a certificate-based authentication technique explicitly designed for the IoD environment. The proposed security protocol has a two-tier structure. Within the first layer, UAVs have the capability to both broadcast and receive messages. Subsequently, in the subsequent tier, these vehicles can transmit real-time data. Nevertheless, the computing requirements of the proposed protocol [24] are significantly high, and it does not provide enough safeguards against “Ephemeral Secret Leakage (ESL)” attacks within the framework of “Canetti and Krawczyk’s model (CK-adversary model)”. Likewise, Nikooghadam et al. [25] proposed an authentication strategy that utilizes ECC to enhance the security of smart city surveillance systems, including drones. The proposed protocol [25] is secured in the random oracle model (ROM), fulfilling the necessary security criteria while maintaining minimal computational and communication requirements. Rupa Ch et al. [26] proposed a method to enhance the security of UAVs and drone applications. Their approach included the implementation of ECC and secure hash algorithm (SHA) to safeguard the privacy of data stored in these systems. The research paper suggested the use of a digital signature as a means of safeguarding data against both plain-text and cypher-text assaults. While the proposed scheme successfully attained the necessary level of security, there is potential for future enhancement by doing performance analysis on several devices simultaneously.

Bera et al. [27] introduced a blockchain-based access control mechanism for IoT-enabled IoD systems to ensure that their scheme can effectively withstand a spectrum of potential attacks. For this, they conducted a formal security analysis under the ROM model, informal security assessment, and simulation-based formal security verification. However, Bera et al.’s scheme lacks support for anonymity and is vulnerable to threats such as drone impersonation, man-in-the-middle, and replay attacks [27]. On the other hand, Chaudhry et al. [28] developed a certificate-based access-control scheme to facilitate inter-drone authentication and access control within the IoD domain and offer anonymity. Nevertheless, Chaudhry et al.’s [24] scheme does reveal vulnerabilities to ESL attacks under the CK-adversary model,

does not provide anonymity, and is susceptible to drone and GSS impersonation attacks. In the context of an IoD environment, Cho et al. [29] introduced a methodology to mitigate several security risks from unauthorized drones. However, it is essential to note that this protocol lacks untraceability and anonymity while also exhibiting vulnerabilities to ESL attacks.

Shin and Kwon [30] presented a key agreement scheme relying on ECC. In this protocol, they introduced an improved version of the access control and authentication protocol initially developed by Adavoudi-Jolfaei et al. [31]. As part of the cryptanalysis, it was revealed that the scheme by Adavoudi-Jolfaei et al. exhibited several security shortcomings. These weaknesses encompassed susceptibility to user collusion attacks and issues related to sensor node anonymity. Consequently, the scheme by Shin and Kwon [30] is exposed to ESL attacks. Mahmood et al. [32] introduced an access control protocol for AI-driven aerial vehicles, employing neural computing to mitigate potential security threats comprehensively. A thorough security assessment of this protocol was conducted formally, employing the well-established Real-Or-Random (ROR) oracle model. Informal security analysis further affirmed the resilience of our approach against a spectrum of potential attacks, considering CK and DY adversarial models. Additionally, compared with various existing schemes, an in-depth performance evaluation of the proposed protocol demonstrated superior computational efficiency, communication overhead, and security attributes. In the work by Bera et al. [33], a novel blockchain-based framework (BSD2C-IoD) is introduced for the secure management of data among communication entities in IoD environments. Their approach demonstrates resilience against various potential attacks, and the formal security analysis of BSD2C-IoD is conducted using the ROR oracle model. Additionally, formal security verification is performed with the AVISPA tool. This solution leverages blockchain technology for the storage and validation of data. Drones' communication and registration processes occur through a secure channel with the control room and are authenticated by a registered authority acting as a trusted third party. Since drones are resource-constrained devices, using certificate-based cryptography to secure the channel may pose inefficiencies.

Similarly, Bera et al. [34] proposed an access control mechanism designed to detect and mitigate unauthorized UAVs in another article. In this mechanism, the authors aimed to safeguard data transmitted from a UAV to the ground station server and identify abnormal data indicative of unauthorized UAVs. The outcomes of this proposed mechanism demonstrated the feasibility of conducting big data analytics on authenticated transactional data recorded on the blockchain. Nevertheless, the study lacks coverage of privacy protection and potential attack issues during the data transfer from the UAV to the server. Rodrigues et al. [35] introduced two authentication protocols initially designed for Wireless Sensor Networks (WSNs) and subsequently adapted for use in UAVs. The authors conducted tests to analyze

**TABLE 1. Description of symbols used in the proposed scheme.**

S. No	Symbol	Descriptions
1	$hec$	This symbol represents the hyperelliptic curve
2	$\rho$	This symbol represents the order of finite field ( $FID_{\rho}$ )
3	$FID_{\rho}$	This symbol represents the finite field on which the hyperelliptic curve is constructed.
4	$D$	This symbol represents the divisor of the hyperelliptic curve.
5	$MPS$	This symbol represents the published master parameter set.
6	$C$	This symbol represents the private key of the ground station server.
7	$\mathcal{V}$	This symbol represents the public key of the ground station server.
8	$hf$	This symbol represents an irreversible and collision-resistant hash function.
9	$UAV_r$	This symbol represents the UAV device.
10	$GSS$	This symbol represents the ground station server.
11	$id_{gss}$	This symbol represents the identity of the ground station server.
12	$id_{UAV_r}$	This symbol represents the identity of the UAV device.
13	$C_{UAV_r}$	This symbol represents the certificate of the UAV device.
14	$PK_{UAV_r}$	This symbol represents the private key of the UAV device.
15	$PBK_{UAV_r}$	This symbol represents the public key of the UAV device.
16	$K_{Dr}, K_{gss}$	These symbols represent the secret shared key between the UAV device and the ground station server.

the execution time and CPU usage, explicitly focusing on security-related operations such as hash tables and ECC operations. However, ECC is a computationally costly operation for UAVs. In response to the challenges identified in the existing schemes [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35] outlined in the literature, we have developed an authenticated access control protocol to detect and mitigate unauthorized UAVs. To address these security concerns, our proposed scheme has been meticulously designed with a primary emphasis on security and rigorously tested using the ROR oracle mode. From a performance perspective, the scheme is constructed using the HECC, an advanced iteration of ECC.

### III. NETWORK MODEL

The network model of the proposed scheme is shown in Fig. 2, which involves “n” UAVs, where  $n \geq 2$ . The UAVs are equipped with all the essential components required for their operational capabilities to perform various tasks across various applications, including aerial imaging and mapping, environmental monitoring and surveillance, and more. These components include data storage, rechargeable batteries for power supply, inertial measurement units (IMUs) for stability and control, and communication modules for real-time data



exchange with ground control and operators. A UAV has various sensors, including radio detection and ranging sensors, sonar-pulse distance sensors (ultrasonic), thermo-sensors, orientation sensors, light-pulse distance sensors (laser), and magnetic-field change sensors. We considered a Raspberry Pi wireless module onboard UAVs in the proposed scheme. Each UAV, equipped with a Raspberry Pi, operates as a node within a mesh network topology, establishing interconnected links with adjacent UAVs and the ground station. The Raspberry Pi boards are generally more affordable, lightweight, have low power consumption, and are easier to troubleshoot, making them a good option for small UAVs. In addition, the Raspberry Pi's computational capabilities help deploy an authentication mechanism and access control to fortify communication channels and prevent unauthorized access.

In the proposed network model, the UAVs are grouped into different geographical clusters that comprise the mission area. Each UAVs are assigned a unique ID. A cluster has a fixed number of UAVs connected and can communicate with the ground station. The UAVs are fed information about the neighbour's zone ID, location, altitude, speed, etc. Further, the information includes the height sensors, IMU, GPS unit, flight controller, etc. The associated UAVs are interlinked using the discovery function, which uses the beacon signals. Raspberry Pi wireless module supports a range of Wi-Fi standards to provide flexibility and compatibility with various networks and devices. In the proposed network model, the wireless connectivity of the network includes 802.11ac Wi-Fi that supports all the IEEE 802.11 standards, Bluetooth 4.0, and some USB 3.0 and Thunderbolt 2.0 ports to connect with the other UAVs, ground station server (GSS) and all the relevant sensors and components. The built-in rechargeable battery facilitates the UAV to use its battery for the maximum time during the flight, while its low weight makes it easy to mount on the accessory bay part of the UAV. By proactively addressing security threats through anomaly-based intrusion detection, this network model ensures the integrity, confidentiality, and resilience of the UAV network, enhancing mission success and operational effectiveness in dynamic and challenging environments.

#### IV. PROPOSED SCHEME

This section provides the primary steps in constructing the proposed authentication and access control protocol. Table 1 displays most symbols employed in the proposed scheme to enhance clarity and facilitate a better understanding of the proposed algorithm. The main steps are as follows:

##### A. INITIALIZATION

This phase is executed by the ground station server (GSS), performing the following steps.

- GSS choose the security parameter and hyperelliptic curve ( $hec$ ) with an equation like  $A^2 + h(B)A = F(B)$ ; note that this equation is constructed over a finite field ( $FID_\rho$ ), where  $\rho$  is the order of  $FID_\rho$ .

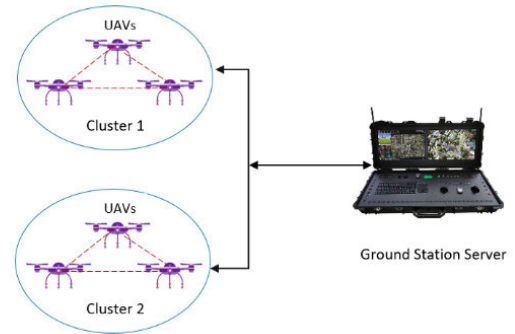


FIGURE 2. A sample network model of the proposed scheme.

- It chooses  $D$  form  $hec$  as a divisor with a length of 80 bits
- Choose the hash function ( $hf$ ) that has properties like one-way and collision-resistant
- Choose  $C \in FID_\rho$  randomly as the master private key and compute  $V = C.D$  as a master public key
- GSS produces the master parameter set  $MPS = \{V, D, FID_\rho, hec, hf\}$  and published it to the network.

##### B. REGISTRATION

In this phase, each UAV ( $UAV_r$ ) register himself with GSS, and we can see the registration process in Fig.3 and the following computations:

- $UAV_r$  chooses his unique identity ( $id_{UAV_r}$ ) and a random number  $\Omega_{UAV_r} \in FID_\rho$
- $UAV_r$  compute  $\beta_{UAV_r} = \Omega_{UAV_r}.D$  and send ( $id_{UAV_r}, \beta_{UAV_r}$ ) to GSS using secure network
- GSS then chose  $P_{UAV_r} \in FID_\rho$  and compute  $U_{UAV_r} = P_{UAV_r}.D$
- Compute  $C_{UAV_r} = U_{UAV_r} + \beta_{UAV_r}$  and  $H_{UAV_r} = P_{UAV_r}.hf(C_{UAV_r}, id_{UAV_r}) + C$
- GSS Sends ( $C_{UAV_r}, H_{UAV_r}$ ) to  $UAV_r$  using an insecure network.
- $UAV_r$  then compute his private key as:  $PK_{UAV_r} = P_{UAV_r}.hf(C_{UAV_r}, id_{UAV_r}) + C$
- And his public key is  $PBK_{UAV_r} = PK_{UAV_r}.D$ .

##### C. LOGIN AND AUTHENTICATION PHASE

In this phase, by using Fig. 4 and the following steps,  $UAV_r$  and GSS can make authentication and key management between each other:

- $UAV_r$  compute  $H = hf(C_{UAV_r}, id_{UAV_r}, PBK_{UAV_r}, N_{UAV_r})$  and sends ( $H, T_X$ ) to GSS using open networks, where  $T_X$  represents timestamp.
- GSS, then by using the message arrival time  $T_X^*$ , it validates the timestamp  $T_X$  as:  $|T_X^* - T_X| < \Delta T$ , if it is true, then compute  $H' = hf(C_{UAV_r}, id_{UAV_r}, PBK_{UAV_r}, N_{UAV_r})$
- GSS compare if  $H' = H$  is true, then chose  $G_{gss} \in FID_\rho$  and compute  $N_{gss} = G_{gss}.D$
- GSS compute  $X = hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$  and  $S_{gss} = G_{gss} + X.C$

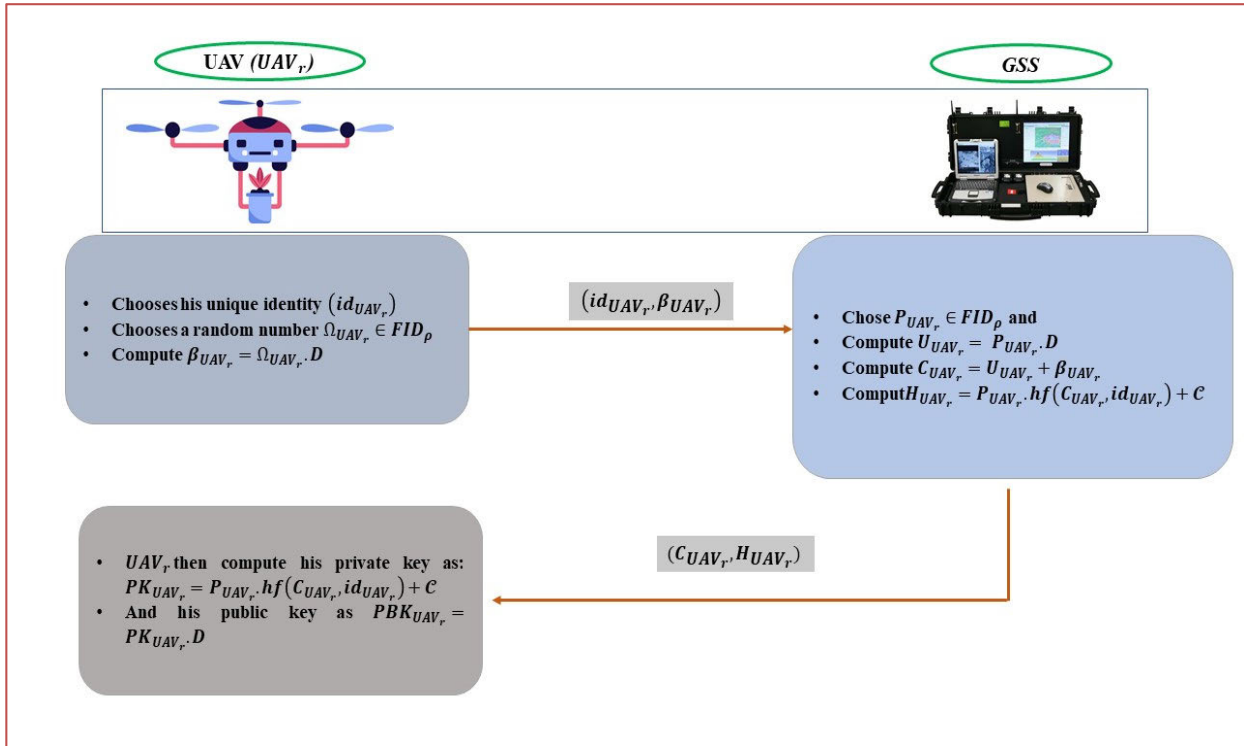


FIGURE 3. Registration phase of the proposed scheme.

- GSS compute  $K_{gss} = G_{gss} \cdot PBK_{UAV_r}$  and sends  $(S_{gss}, X, N_{gss}, T_y)$  to  $UAV_r$  using open networks, where  $T_y$  represents the timestamp.
- $UAV_r$  then by using the message arrival time  $T_y^*$ , it validates the timestamp  $T_y$  as:  $|T_y^* - T_y| < \Delta T$ , if it is true, then compute  $X' = hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$
- $UAV_r$  compare if  $X' = X$  is true, then it validates the signature as:  $N_{gss} = S_{gss} \cdot D - \mathcal{V} \cdot X$
- $UAV_r$  computes the secret key as  $K_{UAV_r} = PK_{UAV_r} \cdot N_{gss}$ , so  $K_{UAV_r} = K_{gss}$  must satisfy.

#### D. NEW UAV ADDING PHASE

In this phase, we explained that the proposed scheme is scalable, and we can add a new UAV ( $UAV_{new}$ ) in real-time using the following steps.

- $UAV_{new}$  chooses his unique identity ( $id_{UAV_{new}}$ ) and a random number  $\Omega_{UAV_{new}} \in FID_\rho$
- $UAV_{new}$  computes  $\beta_{UAV_{new}} = \Omega_{UAV_{new}} \cdot D$  and sends  $(id_{UAV_{new}}, \beta_{UAV_{new}})$  to GSS using secure network.
- GSS then chooses  $P_{UAV_{new}} \in FID_\rho$  and computes  $U_{UAV_{new}} = P_{UAV_{new}} \cdot D$
- Computes  $C_{UAV_{new}} = U_{UAV_{new}} + \beta_{UAV_{new}}$  and  $H_{UAV_{new}} = P_{UAV_{new}} \cdot hf(C_{UAV_{new}}, id_{UAV_{new}}) + C$
- GSS sends  $(C_{UAV_{new}}, H_{UAV_{new}})$  to  $UAV_{new}$  using an insecure network.
- $UAV_{new}$  then computes his private key as:  $PK_{UAV_{new}} = P_{UAV_{new}} \cdot hf(C_{UAV_{new}}, id_{UAV_{new}}) + C$
- And the public key is as follows:  $PBK_{UAV_{new}} = PK_{UAV_{new}} \cdot D$ .

#### E. CORRECTNESS

$UAV_r$  can validate the signature ( $S_{gss}$ ) as follows:  $S_{gss} \cdot D - \mathcal{V} \cdot X = (G_{gss} + X \cdot C) \cdot D - \mathcal{V} \cdot X = (G_{gss} \cdot D + X \cdot C \cdot D) - \mathcal{V} \cdot X = (G_{gss} \cdot D + X \cdot C \cdot D) - C \cdot D \cdot X = G_{gss} \cdot D + X \cdot C \cdot D - C \cdot D \cdot X = G_{gss} \cdot D = N_{gss}$  hence proved.

$UAV_r$  can compute the secret key  $K_{UAV_r} = PK_{UAV_r} \cdot N_{gss}$ , so  $K_{UAV_r} = K_{gss}$  must satisfy by using the following computations:

$$K_{UAV_r} = PK_{UAV_r} \cdot N_{gss} = PK_{UAV_r} \cdot N_{gss} = PK_{UAV_r} \cdot (G_{gss} \cdot D) = PK_{UAV_r} \cdot D \cdot (G_{gss}) = PBK_{UAV_r} \cdot (G_{gss}) = G_{gss} \cdot PBK_{UAV_r} \text{ hence proved.}$$

#### V. SECURITY ANALYSIS

This section presents three forms of security proofs for the proposed scheme: informal analysis, proofs using a Random-Or-Real (ROR) model, and validation using the AVISPA Tool. Firstly, we will provide definitions for the terms ‘‘hard problem’’ and ‘‘hash function,’’ which are fundamental to the security of the proposed scheme. Subsequently, we will elaborate on each security proof, providing comprehensive explanations.

**Hash Function:** The hash function is the mathematically deterministic approach with qualities like irreversible and collision resistance. In reality, it accepts a string of any length and produces a constant value of size  $k$ , which may be written as  $hf(\cdot) : \{0, 1\}^* \rightarrow \{0, 1\}^k$ .

**Hyperelliptic Curve Discrete Logarithmic Problem (HCDLP):** According to HCDLP, the malicious opponent ( $M_{opn}$ ) can try to extract the value  $l$  from  $L = l \cdot D$ , where  $l \in FID_\rho$ , but it is hard for him.

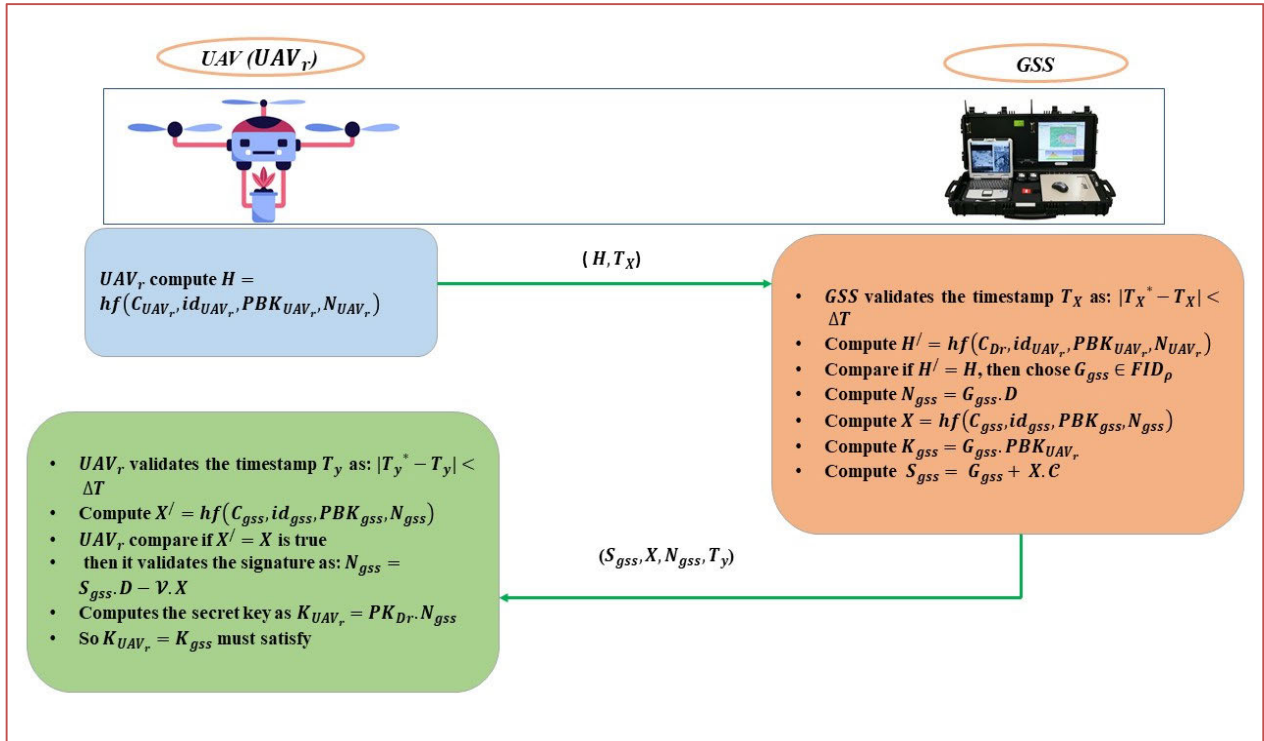


FIGURE 4. Login and authentication phase of the proposed scheme.

### A. INFORMAL SECURITY ANALYSIS

In this section, we prove that the proposed scheme provides the security requirements like authentication, unforgeability, resistance against reply attacks, confidentiality, non-repudiations, resistance against impersonation attacks, secret key security, resistance against privileged insider attacks, and man-in-the-middle attacks.

#### 1) CONFIDENTIALITY

In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to decrypt any ciphertext that is communicated between the UAV and GSS, it must need the secret key  $K_{gss} = G_{gss} \cdot PBK_{Dr}$ . To compute  $K_{gss}$ ,  $M_{opn}$  needs  $G_{gss}$  from  $N_{gss} = G_{gss} \cdot D$ , however, it is not feasible because it is equal to solving HCDLP. That's why we can say that our scheme meets the confidentiality requirement.

#### 2) AUTHENTICATIONS

In our scheme,  $UAV_r$  compute  $H = hf(C_{UAV_r}, id_{UAV_r}, PBK_{UAV_r}, N_{UAV_r})$  and sends  $(H, T_X)$  to  $GSS$  using open networks, where  $T_X$  represents timestamp.  $GSS$ , then by using the message arrival time  $T_X^*$ , it validates the timestamp  $T_X$  as:  $|T_X^* - T_X| < \Delta T$ , if it is true, then compute  $H' = hf(C_{UAV_r}, id_{UAV_r}, PBK_{UAV_r}, N_{UAV_r})$ , compare if  $H' = H$  is true, then chose  $G_{gss} \in FID_\rho$ , compute  $N_{gss} = G_{gss} \cdot D$ ,  $X = hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$ ,  $S_{gss} = G_{gss} + X \cdot C$ ,  $K_{gss} = G_{gss} \cdot PBK_{Dr}$  and sends  $(S_{gss}, X, N_{gss}, T_y)$  to  $UAV_r$ .  $UAV_r$  then by using the message arrival time  $T_y^*$ , it validates the timestamp  $T_y$  as:  $|T_y^* - T_y| < \Delta T$ , if it is true, then compute

$X' = hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$ , compare if  $X' = X$  is true, then it validates the signature as:  $N_{gss} = S_{gss} \cdot D - \mathcal{V} \cdot X$  and computes the secret key as  $K_{UAV_r} = PK_{UAV_r} \cdot N_{gss}$ , so  $K_{UAV_r} = K_{gss}$  must satisfy. If the above computations are successful, then we can say that our scheme meets the authentication requirement.

#### 3) UNFORGEABILITY

In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to generate a valid signature as  $S_{gss} = G_{gss} + X \cdot C$ . for this purpose,  $M_{opn}$  needs  $G_{gss}$  and  $C$ , which is not feasible because finding two unknown values from the single equation is not possible. So, we can say that our scheme meets the requirement of unforgeability.

#### 4) RESISTANT AGAINST REPLY ATTACK

Our scheme,  $UAV_r$  sends  $(H, T_X)$  to  $GSS$  using open networks, where  $T_X$  represents timestamp.  $GSS$ , then by using the message arrival time  $T_X^*$ , validates the timestamp  $T_X$  as:  $|T_X^* - T_X| < \Delta T$ , if it is true, then  $(H, T_X)$  will be acceptable. Further,  $GSS$  sends  $(S_{gss}, X, N_{gss}, T_y)$  to  $UAV_r$ .  $UAV_r$  then by using the message arrival time  $T_y^*$ , it validates the timestamp  $T_y$  as:  $|T_y^* - T_y| < \Delta T$ , if it is true, then  $(S_{gss}, X, N_{gss}, T_y)$  will be acceptable. So, we can say that our scheme meets the resistance against the reply attack requirement.

#### 5) NON-REPUDIATIONS

In our scheme,  $GSS$  compute  $S_{gss} = G_{gss} + X \cdot C$  and sends  $(S_{gss}, X, N_{gss}, T_y)$  to  $UAV_r$ , where  $N_{gss} = G_{gss} \cdot D$ ,  $X =$

TABLE 2. Security requirement comparison.

Requirement	Mahmood et al. [32]	Bera et al. [33]	Bera et al. [34]	Rodrigues et al. [35]	Bera et al. [27]	Our Scheme
Confidentiality	√	×	√	√	√	√
Authentication	√	×	√	√	√	√
Unforgeability	×	×	×	×	×	√
Resistant against reply attack	√	√	√	√	√	√
Non-repudiations	×	×	×	×	×	√
Resistant against GSS impersonation attack	√	×	×	√	×	√
Resistant against $UAV_r$ impersonation attack	√	×	×	×	√	√
Secret key security	√	×	√	×	√	√
Resistant against privileged insider attack	√	√	√	√	√	√
Man-in-the-middle attack	√	√	√	×	√	√

$hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$ , and  $T_y$  is the timestamp.  $UAV_r$  compute  $X' = hf(C_{UAV_r}, id_{gss}, PBK_{gss}, N_{gss})$  and validates the signature as:  $N_{gss} = S_{gss} \cdot D - \mathcal{V} \cdot X$  must satisfy. If this equation is satisfied, then our scheme meets the requirement of non-repudiations because  $S_{gss}$  is the public key of  $GSS$ , and he cannot deny from his signature.

#### 6) RESISTANT AGAINST GSS IMPERSONATION ATTACK

In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to impersonate  $GSS$ , then it must generate a valid signature as  $S_{gss} = G_{gss} + X \cdot C$ . for this purpose,  $M_{opn}$  needs  $G_{gss}$  and  $C$ , which is not feasible because finding two unknown values from single equation is not possible. So, we can say that our scheme meets the requirement of resistance against impersonation attacks.

#### 7) RESISTANT AGAINST

$UAV_r$  impersonation attack: In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to impersonate  $UAV_r$ , then it must generate  $K_{UAV_r} = PK_{UAV_r} \cdot N_{gss}$ . For this purpose,  $M_{opn}$  needs  $PK_{UAV_r}$  from  $PBK_{UAV_r} = PK_{UAV_r} \cdot D$  which is equal to solving HCDLP. We can say that our scheme meets the resistance requirement against  $UAV_r$  impersonation attack.

#### 8) SECRET KEY SECURITY

In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to get the secret key  $K_{gss} = G_{gss} \cdot PBK_{Dr}$  or  $K_{UAV_r} = PK_{UAV_r} \cdot N_{gss}$ . To compute  $K_{gss}$  or  $K_{UAV_r}$ ,  $M_{opn}$  needs  $G_{gss}$  from  $N_{gss} = G_{gss} \cdot D$  and  $PK_{UAV_r}$  from  $PBK_{UAV_r} = PK_{UAV_r} \cdot D$ , however, it is not feasible because it is equal to solving HCDLP for two times. That's why we can say that our scheme meets the requirement of secret key security.

#### 9) RESISTANT AGAINST PRIVILEGED INSIDER ATTACK

In our scheme,  $GSS$  registers all the UAVs before deployment in the flying zone without storing any secrets in their memories. So the attacker will not be able to assume the secret key.

#### 10) MAN-IN-THE-MIDDLE ATTACK

In our scheme, when a malicious opponent ( $M_{opn}$ ) wants to perform a man-in-the-middle attack, then it generates a valid signature as  $S_{gss} = G_{gss} + X \cdot C$ . for this purpose,  $M_{opn}$  needs  $G_{gss}$  and  $C$ , which is not feasible because finding two unknown values from the single equation is not possible. We can say that our scheme meets the requirement of resisting a man-in-the-middle attack.

In Table 2, we have given the security requirements comparison between our scheme and the existing counterparts by Mahmood et al. [32], Bera et al. [33], Bera et al. [34], Rodrigues et al. [35] and Bera et al. [27], in which the symbol  $\checkmark$  and  $\times$  represents to satisfied and dissatisfied the security requirement. The proposed scheme meets more security requirements as compared to those proposed by Mahmood et al. [32], Bera et al. [33], Bera et al. [34], Rodrigues et al. [35] and Bera et al. [27].

### B. SECURITY ANALYSIS USING THE ROR MODEL

The ROR model serves as a formal security framework that may be used to evaluate the security of the proposed scheme. The primary advantage of this model is that it can demonstrate the security of the UAV communication system. It does this by evaluating the system's ability to distinguish between actual and random data. It also demonstrates the system's capacity to protect against malicious actors. Based on this theoretical framework, a malicious opponent ( $M_{opn}$ ) seeks to disrupt the communication among the interconnected nodes in the UAV communication system by simulating authentic attacks using a planned set of queries to accomplish this goal. The planned set of queries can be defined as follows:

#### 1) EXECUTE QUERY

Using this specific query, a malicious opponent ( $M_{opn}$ ) can intercept or covertly see all messages sent and received between the UAV and  $GSS$ .



2) SEND QUERY

Through this query, an assailant acquires the capacity to transmit a message to either the Drone or GSS and obtain a corresponding response from the targeted entity.

3) REVEAL QUERY

By employing this query, a malicious opponent ( $M_{opn}$ ) seeks to acquire the secret key between the UAV and GSS.

4) TEST QUERY

Through this particular query, a malicious opponent ( $M_{opn}$ ) can initiate a request to both the UAV and GSS to obtain the secret key. This action subsequently leads to the extraction of a random bit  $u$ .

Moreover, in the model, the hash function is represented as a random oracle and is available to all the devices involved, including malicious opponents ( $M_{opn}$ ). The participants in the proposed scheme are designated as the  $i^{th}$ -device and  $j^{th}$ -device and are represented by their respective instances, indicated as  $I_{ns} = \{I_{nsi} \text{ and } I_{nsj}\}$ . The malicious opponent ( $M_{opn}$ ) is supposed to interact with  $I_{ns} = \{I_{nsi} \text{ and } I_{nsj}\}$ , where  $I_{ns}$  is an instance of an executing participant (UAV and GSS). Theorem 1 can be used to demonstrate that the proposed access control scheme provides session key security, also known as semantic security.

*Theorem 1:* Theorem 1 states that when a malicious opponent ( $M_{opn}$ ) operates within a polynomial time frame, denoted as  $p_{tm}$ , and seeks to undermine the security of the session key between  $I_{nsi}$  and  $I_{nsj}$ , the advantage of  $M_{opn}$  in compromising the session key security is as follows:

$$ADV^{our\ scheme}_{M_{opn}}(p_{tm}) \leq \frac{Q_{hf}^2}{|Hash|} + 2 \cdot ADV^{HCDLP}_{M_{opn}}(p_{tm}) \quad (1)$$

where  $p_{tm}$ ,  $ADV^{HCDLP}_{M_{opn}}(p_{tm})$ ,  $|Hash|$ , and  $Q_{hf}^2$  denotes the polynomial time, the winning advantage of breaching HCDLP, space for hash  $hf(\cdot)$ , and the queries to hash, respectively.

*Proof of Theorem 1.* In our security analysis, we have observed three separate Games  $G_i$ , where  $i = \{1, 2, 3\}$ . In each of these games,  $M_{opn}$  endeavours to predict the value of the bit  $c$  by employing the Test query. Let  $Success_{M_{opn}}^{G_i}$  represent the event in which  $M_{opn}$  successfully anticipates the bit  $u$ . In this case, the advantage of  $M_{opn}$  in winning the game can be mathematically stated as follows:

$$ADV^{ourscheme}_{M_{opn}, G_i}(p_{tm}) = \Pr[Success_{M_{opn}}^{G_i}] \quad (2)$$

Game 1 ( $G_1$ ) : The outcome of  $G_1$  corresponds to the behaviour exhibited by the real system functioning under the ROR model. So, we have the following result:

$$ADV^{our\ scheme}_{M_{opn}}(p_{tm}) = |2ADV^{our\ scheme}_{M_{opn}, G_1}(p_{tm}) - 1| \quad (3)$$

Game 2 ( $G_2$ ) : In  $G_2$ ,  $M_{opn}$  makes use of the *Execute Query* to eavesdrop on  $I_{nsi}$  and  $I_{nsj}$  communication. Intercepted

communications include the following messages:  $(H, T_X)$  and  $(S_{gss}, X, N_{gss}, T_Y)$ . Following the execution of the *Reveal Query*,  $M_{opn}$  obtains the secret key and then uses the *Test Query* to validate the secret key's authenticity. The proposed access control scheme uses the following method for generating the session key:  $K_{gss} = G_{gss}.PBK_{Dr}$ ,  $K_{Dr} = PK_{Dr}.N_{gss}$ , and  $K_{gss} = K_{Dr}$ . If  $M_{opn}$  wants to access  $K_{gss} = G_{gss}.PBK_{Dr}$ , then he/she must extract  $G_{gss}$  from  $N_{gss} = G_{gss}.D$  which is not feasible due to HCDLP hardness. Also, If  $M_{opn}$  wants to access  $K_{gss} = G_{gss}.PBK_{Dr}$ , then he/she must extract  $PK_{Dr}$  from  $PBK_{Dr} = PK_{Dr}.D$  which is not feasible due to HCDLP hardness. This implies that merely eavesdropping on all messages will not enhance the chances of success. Therefore, both games, Game 1 ( $G_1$ ) and Game 2 ( $G_2$ ), are equivalent, as indicated by the equation below:

$$ADV^{our\ scheme}_{M_{opn}, G_2}(p_{tm}) = ADV^{our\ scheme}_{M_{opn}, G_1}(p_{tm}) \quad (4)$$

Game 3 ( $G_3$ ) : The Hash and Send Queries are employed throughout this game. In the context of  $G_2$ , it has been ascertained that monitoring all communications does not result in hash collisions. This is due to the protective nature of the hash function and HCDLP, which ensures the security of these messages. Both  $K_{gss} = G_{gss}.PBK_{Dr}$  and  $K_{Dr} = PK_{Dr}.N_{gss}$  are protected through a hash function and HCDLP. So, in this game, if  $M_{opn}$  can break the security of HCDLP with the advantage of  $ADV^{HCDLP}_{M_{opn}}(p_{tm})$  and the hash function with advantage of  $\frac{Q_{hf}^2}{2|Hash|}$ . The following result can be obtained:

$$ADV^{our\ scheme}_{M_{opn}, G_2}(p_{tm}) - ADV^{our\ scheme}_{M_{opn}, G_3}(p_{tm}) \leq \frac{Q_{hf}^2}{2|Hash|} + ADV^{HCDLP}_{M_{opn}}(p_{tm}) \quad (5)$$

To guess the bit  $u$ ,  $M_{opn}$  perform all the queries, and we can get the following result:

$$ADV^{our\ scheme}_{M_{opn}, G_3}(p_{tm}) = \frac{1}{2} \quad (6)$$

From  $ADV^{our\ scheme}_{M_{opn}}(p_{tm}) = |2ADV^{our\ scheme}_{M_{opn}, G_1}(p_{tm}) - 1|$  and  $ADV^{our\ scheme}_{M_{opn}, G_2}(p_{tm}) = ADV^{ourscheme}_{M_{opn}, G_1}(p_{tm})$  we can get the following result:

$$\begin{aligned} & \frac{1}{2} ADV^{our\ scheme}_{M_{opn}}(p_{tm}) \\ &= \left| ADV^{our\ scheme}_{M_{opn}, G_1}(p_{tm}) - \frac{1}{2} \right| \\ &= ADV^{our\ scheme}_{M_{opn}, G_2}(p_{tm}) - \frac{1}{2} \end{aligned} \quad (7)$$

From  $ADV^{our\ scheme}_{M_{opn}, G_3}(p_{tm}) = \frac{1}{2}$  and  $\frac{1}{2} ADV^{our\ scheme}_{M_{opn}}(p_{tm}) = \left| ADV^{our\ scheme}_{M_{opn}, G_1}(p_{tm}) - \frac{1}{2} \right|$ , we can get the following result:

$$\frac{1}{2} ADV^{our\ scheme}_{M_{opn}}(p_{tm})$$

TABLE 3. HLPSP role for GSS.

<b>role</b>
role_Gss(Gss:agent,Uavr:agent,Pkuavr:public_key,Vgss:public_key,SND,RCV:channel(dy)) played_by Gss
<b>def=</b>
local
<b>State:</b> nat,G:text,X:text,Kgss:symmetric_key,M:text
init
State := 0
transition
1. <b>State=0</b>
∧ RCV(Uavr.Gss) = >
2. <b>State:=1</b>
∧ X':=new() ∧ secret(X',sec_4,{Uavr}) ∧
witness(Gss,Uavr,auth_3,X') ∧ G':=new() ∧
secret(G',sec_2,{Uavr}) ∧
witness(Gss,Uavr,auth_1,G') ∧
SND(Gss.{G'.X'}_inv(Vgss)) ∧ Kgss':=new() ∧
M':=new() ∧ witness(Gss,Uavr,auth_5,M') ∧
SND(Gss.{M'}_Kgss')
<b>end role</b>

TABLE 4. HLPSP role for UAV.

<b>role</b>
role_Uavr(Gss:agent,Uavr:agent,Pkuavr:public_key,Vgss:public_key,SND,RCV:channel(dy)) played_by Uavr
<b>def=</b>
local
<b>State:</b> nat,G:text,X:text,Kgss:symmetric_key,M:text
init
State := 0
transition
1. <b>State=0</b>
∧ RCV(start) = > State':=1 ∧
SND(Uavr.Gss)
2. <b>State=1</b>
∧ RCV(Gss.{G'.X'}_inv(Vgss)) = >
State':=2 ∧ secret(X',sec_4,{Uavr})
∧ request(Uavr,Gss,auth_1,G') ∧
secret(G',sec_2,{Uavr})
3. <b>State=2</b>
∧ RCV(Gss.{M'}_Kgss') = >
State':=3
<b>end role</b>

$$= \left| ADV_{M_{opn}, \mathcal{G}_1}^{our\ scheme}(p_{tm}) - ADV_{M_{opn}, \mathcal{G}_2}^{our\ scheme}(p_{tm}) \right| \quad (8)$$

Using  $ADV_{M_{opn}, \mathcal{G}_2}^{our\ scheme}(p_{tm}) - ADV_{M_{opn}, \mathcal{G}_3}^{our\ scheme}(p_{tm}) \leq \frac{Q_{hf}^2}{2|Hash|} + ADV_{M_{opn}}^{HCDLP}(p_{tm})$  and  $\frac{1}{2}ADV_{M_{opn}}^{our\ scheme}(p_{tm}) = \left| ADV_{M_{opn}, \mathcal{G}_1}^{our\ scheme}(p_{tm}) - ADV_{M_{opn}, \mathcal{G}_2}^{our\ scheme}(p_{tm}) \right|$ , we can get the following outcomes:

$$\frac{1}{2}ADV_{M_{opn}}^{our\ scheme}(p_{tm}) = \frac{Q_{hf}^2}{2|Hash|} + ADV_{M_{opn}}^{HCDLP}(p_{tm}) \quad (9)$$

By multiplying 2 by both sides of equation (9), we can get the following result:  $ADV_{M_{opn}}^{our\ scheme}(p_{tm}) = \frac{Q_{hf}^2}{|Hash|} + 2ADV_{M_{opn}}^{HCDLP}(p_{tm})$  hence proved.

### C. SECURITY ANALYSIS USING THE AVISPA

In this subsection, we present the outcomes derived from the simulation results using the AVISPA tool [36] with the primary objective being to assess the effectiveness of the proposed scheme in mitigating replay and man-in-the-middle attacks. AVISPA is an automated tool offering a sophisticated and modular formal language for simulating protocols and evaluating their security properties. The specific protocol animator for AVISPA (SPAN) [37], designed as a security animator, aids protocol developers in composing HLPSP specifications [38]. These HLPSP specifications undergo interpretation into IF through the HLPSP/IF trans-

lator. Subsequently, the IF is transformed into the OF using tools such as OFMC [39], CL-based AtSe [40], SATMC, or TA4SP. These integrated tools analyze the security assertions of the IF code, focusing on two specific types of attacks—replay and man-in-the-middle attacks. The IF code operates within two validation states: SAFE, indicating the cryptographic scheme's capability to guard against man-in-the-middle attacks, and UNSAFE, signifying scenarios where the IF code lacks protection against man-in-the-middle attacks. Formal security verification employing the AVISPA tool has been extensively documented in various studies to assess the security posture of numerous authentication protocols concerning replay and man-in-the-middle attacks [41], [42], [43], [44], [45], [46]. The codes for HLPSP for GSS, UAVs, sessions and environments are provided in Tab. 3, Tab. 4, Tab. 5 and Tab. 6 respectively. The simulations results for OFMC and AtSe are shown in Fig. 5 and Fig. 6, respectively and It is evident that the proposed protocol is safe against replay and man-in-the-middle attack.

## VI. PERFORMANCE COMPARISON

This section compares the performance of the proposed scheme in terms of computational cost and communication cost with the existing counterparts by Mahmood et al. [32], Bera et al. [33], Bera et al. [34], Rodrigues et al. [35] and Bera et al. [27].

### A. COMPUTATIONAL COST

In the context of computational cost analysis, the primary operations considered are elliptic curve point multiplication

TABLE 5. HLPSSL role for session.

```

role
session1(Gss:agent,Uavr:agent,Pkuavr:public_key,Vgss:publ
ic_key)

def=
    local
        SND2,RCV2,SND1,RCV1:channel(dy)
    composition
        role_Gss(Gss,Uavr,Pkuavr,Vgss,SND2,RCV2) ∧
        role_Uavr(Gss,Uavr,Pkuavr,Vgss,SND1,RCV1)

end role

role
session2(Gss:agent,Uavr:agent,Pkuavr:public_key,Vgss:publ
ic_key)

def=
    local
        SND1,RCV1:channel(dy)
    composition
        role_Uavr(Gss,Uavr,Pkuavr,Vgss,SND1,RCV1)

end role
    
```

TABLE 6. HLPSSL role for environment.

```

role environment()
def=
    const
        hash_0:hash_func,pkuavr:public_key,alice:agent,b
        ob:agent,vgss:public_key,const_1:agent,const_2:public_key,
        const_3:public_key,auth_1:protocol_id,sec_2:protocol_id,au
        th_3:protocol_id,sec_4:protocol_id,auth_5:protocol_id,sec_6
        :protocol_id
        intruder_knowledge = {alice,bob}
    composition

session1(const_1,i,const_2,const_3)
session2(alice,bob,pkuavr,vgss)

end role

goal
    authentication_on auth_1
    secrecy_of sec_2
    authentication_on auth_3
    secrecy_of sec_4
    authentication_on auth_5
    secrecy_of sec_6

end goal
    
```

(TEMP), elliptic curve addition (TEA), hash function (THF), hyperelliptic curve divisor multiplication (THDP), and

TABLE 7. Computational cost based on major operations.

Schemes	UAV	GSS
Mahmood et al. [32]	2TEMP+2TEA+6THF	2TEMP +2TEA+7THF
Bera et al. [33]	5TEMP+2TEA+6THF	6TEMP +2TEA+6THF
Bera et al. [34]	2TEMP+1TEA+6THF	2TEMP +1TEA+7THF
Rodrigues et al. [35]	6TEMP+9THF	2TEMP +9THF
Bera et al. [27]	4TEMP+5THF+1TEA	4TEMP +5THF+1TEA
Our scheme	3THDP+2THF	3THDP+2THF

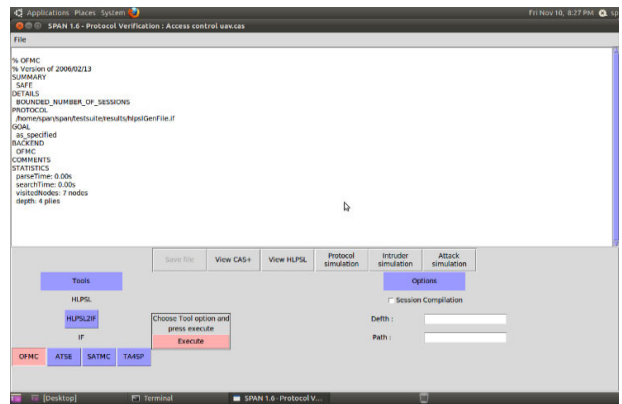


FIGURE 5. Simulation results for OFMC.

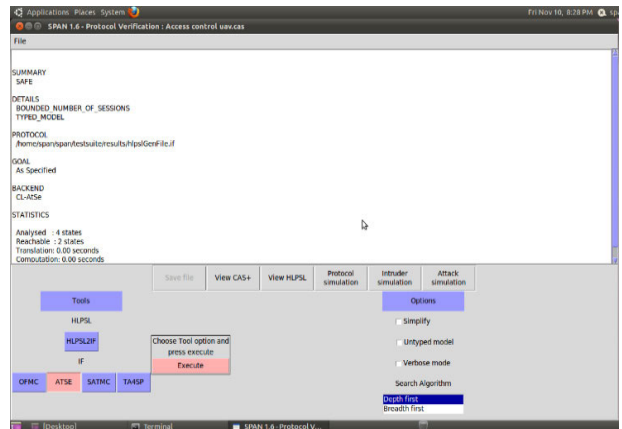


FIGURE 6. Simulation results for ATSE.

hyperelliptic curve addition (THA). These operations are examined in terms of the time (milliseconds) required for their execution. The primary operations such as TEMP, TEA, and THF are determined by analyzing the execution time of cryptographic functions on two distinct devices [47]: to support UAV a Pi3 B+ with Cortex-A53(ARMv8) 64-bit SoC @ 1.4 GHz processor, 1 GB LPDDR2 SDRAM RAM is used. By using Pi3, TEMP, TEA, and THF need processing times of 4.107 milliseconds (ms), 0.018 ms, and 0.006 ms, respectively. We suppose hyperelliptic curve divisor multiplication (THDP) will need 2.0535 ms and hyperelliptic curve addition (THA) will require 0.009 ms because hyperelliptic curves need half the time compared to elliptic curves. For

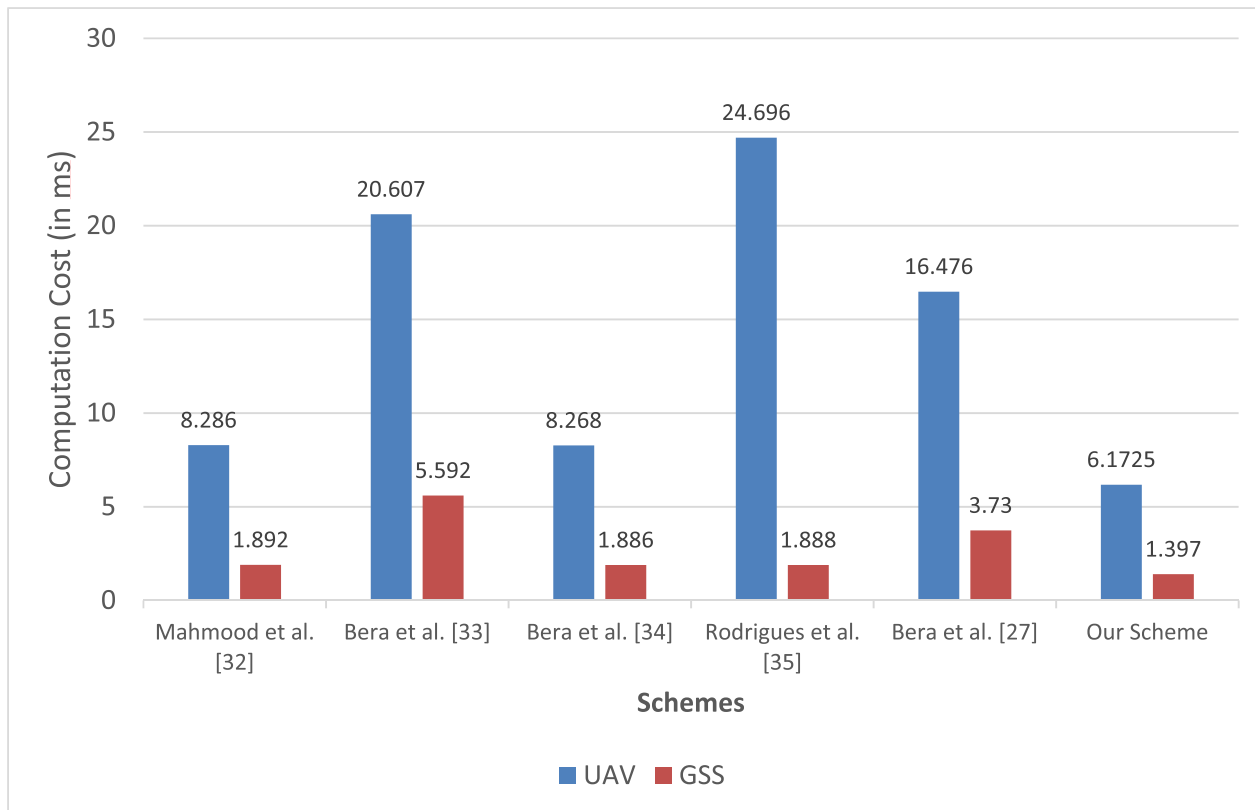


FIGURE 7. Comparison of computation cost (in ms).

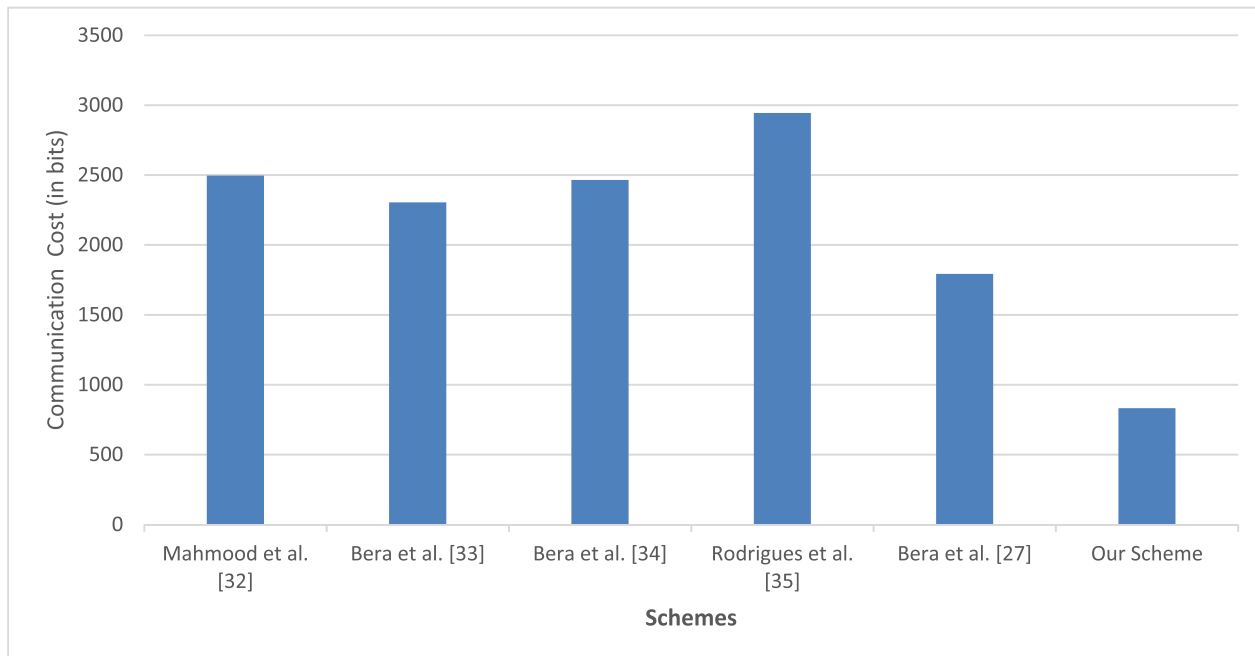


FIGURE 8. Comparison of communication cost (in bits).

GSS, the HP EliteBook 8460P with Intel Core i7-2620 M 2.7 GHz Processor and 4 GB RAM over Ubuntu 16.0 LTS operating system is used. By using HP EliteBook, TEMP, TEA, and THF need processing times of 0.926 milliseconds (ms), 0.006 ms, and 0.004 ms, respectively. We suppose

hyperelliptic curve divisor multiplication (THDP) will need 0.463 ms and hyperelliptic curve addition (THA) will require 0.003 ms because hyperelliptic curves need half the time compared to elliptic curves [48], [49], [50]. The computational cost for each entity, namely the UAV and GSS, has been



**TABLE 8.** Computational cost based on milliseconds.

Schemes	UAV	GSS
Mahmood et al. [32]	$2*4.107 + 2*0.018 + 6*0.006 = 8.286$	$2*0.926 + 2*0.006 + 7*0.004 = 1.892$
Bera et al. [33]	$5*4.107 + 2*0.018 + 6*0.006 = 20.607$	$6*0.926 + 2*0.006 + 6*0.004 = 5.592$
Bera et al. [34]	$2*4.107 + 1*0.018 + 6*0.006 = 8.268$	$2*0.926 + 1*0.006 + 7*0.004 = 1.886$
Rodrigues et al. [35]	$6*4.107 + 9*0.006 = 24.696$	$2*0.926 + 9*0.004 = 1.888$
Bera et al. [27]	$4*4.107 + 5*0.006 + 1*0.018 = 16.476$	$4*0.926 + 5*0.004 + 1*0.006 = 3.73$
Our scheme	$3*2.0535 + 2*0.006 = 6.1725$	$3*0.463 + 2*0.004 = 1.397$

**TABLE 9.** Communication cost based on transmitted bits.

Schemes	Communication Cost	Communication Cost in bits
Mahmood et al. [32]	$6 q +6 H $	$6* 160 +6* 256 =2496$
Bera et al. [33]	$8 q +4 H $	$8* 160 +4* 256 =2304$
Bera et al. [34]	$9 q +4 H $	$9* 160 +4* 256 =2464$
Rodrigues et al. [35]	$12 q +4 H $	$12* 160 +4* 256 =2944$
Bera et al. [27]	$8 q +2 H $	$8* 160 +2* 256 =1792$
Our scheme	$4 n +2 H $	$4* 80 +2* 256 =832$

computed. Similar calculations are performed on the computational costs of all relevant existing algorithms, detailed in Table 7 (major operations) and Table 8 (milliseconds). The computation cost of the proposed scheme is comparatively lower than that of existing algorithms, as illustrated in Fig. 7.

## B. COMMUNICATION COST

This subsection compares the proposed scheme's communication cost results and existing schemes. In terms of communication costs, we evaluate the proposed scheme against similar approaches put forth by Mahmood et al. [32], Bera et al. [33], Bera et al. [34], Rodrigues et al. [35], and Bera et al. [27]. The variables for the comparative analysis and their respective values are outlined in Table 9. As depicted in Fig. 8 and Table 9, it is evident that the proposed scheme proves to be more efficient in terms of communication cost than existing comparable solutions.

## VII. CONCLUSION

In this article, we introduced an authentication and access control protocol designed to address security concerns in UAV networks. The proposed scheme is based on HECC, utilizing a smaller key size of 80 bits compared to the 160 bits used in ECC. HECC maintains the same security standards as other methods like RSA, ECC, and bilinear pairing while employing a significantly smaller key size, making it well-suited for UAV networks. We assessed the security of the proposed protocol using the well-known ROR model and the formal security validations through the AVISPA tool. Simulation results from AVISPA demonstrate the protocol's security against adversarial scenarios in the OFMC and CI-AtSe models. Additionally, informal security analysis ensured the robustness of the proposed scheme against

potential attacks based on the CK and DY adversarial models. A comparative analysis of the protocol's performance against existing methods highlights its computational and communication efficiency. In the future, we are intended to perform the security analysis using the ROM.

## REFERENCES

- [1] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones*, vol. 6, no. 6, p. 147, Jun. 2022.
- [2] T. Elmokadem and A. V. Savkin, "Towards fully autonomous UAVs: A survey," *Sensors*, vol. 21, no. 18, p. 6223, Sep. 2021.
- [3] G. Pajares, "Overview and current status of remote sensing applications based on unmanned aerial vehicles (UAVs)," *Photogrammetric Eng. Remote Sens.*, vol. 81, no. 4, pp. 281–330, Apr. 2015.
- [4] M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywolek, and I. Ullah, "Swarm of UAVs for network management in 6G: A technical review," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 1, pp. 741–761, Mar. 2023.
- [5] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 134–139, Aug. 2017.
- [6] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the security: An enhanced authentication protocol for drone communications over 5G networks," *Drones*, vol. 6, no. 1, p. 10, Dec. 2021.
- [7] L. Meng, L. Yang, W. Yang, and L. Zhang, "A survey of GNSS spoofing and anti-spoofing technology," *Remote Sens.*, vol. 14, no. 19, p. 4826, Sep. 2022.
- [8] J. Zhang, S. Peng, Y. Gao, Z. Zhang, and Q. Hong, "APMSA: Adversarial perturbation against model stealing attacks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1667–1679, 2023.
- [9] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR)*, Shanghai, China, Oct. 2017, pp. 194–199.
- [10] M. A. Khan, B. A. Alzahrani, A. Barnawi, A. Al-Barakati, A. Irshad, and S. A. Chaudhry, "A resource friendly authentication scheme for space-air-ground-sea integrated maritime communication network," *Ocean Eng.*, vol. 250, Apr. 2022, Art. no. 110894.
- [11] J. Hu, C. Chen, L. Cai, M. R. Khosravi, Q. Pei, and S. Wan, "UAV-assisted vehicular edge computing for the 6G Internet of Vehicles: Architecture, intelligence, and challenges," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 12–18, Jun. 2021.
- [12] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.
- [13] M. Tanveer, A. U. Khan, H. Shah, S. A. Chaudhry, and A. Naushad, "PASKE-IoD: privacy-protecting authenticated key establishment for Internet of Drones," *IEEE Access*, vol. 9, pp. 145683–145698, 2021.
- [14] B. Hassan, A. A. AlSanad, I. Ullah, N. U. Amin, M. A. Khan, M. I. Uddin, and J. M.-T. Wu, "A cost effective identity-based authentication scheme for Internet of Things-enabled agriculture," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Apr. 2022.
- [15] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 3156, M. Joye, J. J. Quisquater, Eds. Berlin, Germany: Springer, 2004.

- [16] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *Proc. Int. Conf. Electron., Commun. Comput. Eng. (ICECCE)*, Hosur, India, Nov. 2014, pp. 83–93.
- [17] F. Maqsood, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A comparative analysis for modern techniques," *Int. J. Adv. Comput. Sci.*, vol. 8, pp. 442–448, Apr. 2017.
- [18] M. G. Yaseen, M. Naemullah, and I. A. Mansoor, "Parallel generalized Hebbian algorithm for large scale data analytics," *Mesopotamian J. Big Data*, pp. 14–21, Mar. 2021.
- [19] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2014, pp. 157–175.
- [20] A. Yadav, P. Sharma, and Y. Gigras, "Image encryption using hyper elliptic curve and phase truncate transformation," in *Proc. 5th Int. Conf. Comput. Intell. Commun. Technol. (CCICT)*, Jul. 2022, pp. 576–583.
- [21] 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 Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
- [22] S. Banerjee, A. K. Das, S. Chattopadhyay, S. S. Jamal, J. J. P. C. Rodrigues, and Y. Park, "Lightweight failover authentication mechanism for IoT-based fog computing environment," *Electronics*, vol. 10, no. 12, p. 1417, Jun. 2021.
- [23] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.
- [24] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354.
- [25] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.
- [26] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102670.
- [27] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020.
- [28] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria, "GCACS-IoD: A certificate based generic access control scheme for Internet of Drones," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107999.
- [29] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.
- [30] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things," *IEEE Access*, vol. 8, pp. 67555–67571, 2020.
- [31] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 43–59, Jan. 2019.
- [32] K. Mahmood, T. Tariq, A. K. Sangaiah, Z. Ghaffar, M. A. Saleem, and S. Shamsad, "A neural computing-based access control protocol for AI-driven intelligent flying vehicles in industry 5.0-assisted consumer electronics," *IEEE Trans. Consum. Electron.*, p. 1, 2023, doi: 10.1109/TCE.2023.3276066.
- [33] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.
- [34] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, Jan. 2021.
- [35] M. Rodrigues, J. Amaro, F. S. Osório, and B. Kalinka, "Authentication methods for UAV communication," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Barcelona, Spain, 2019, pp. 1210–1215.
- [36] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. Accessed: Oct. 25, 2023. [Online]. Available: <http://www.avispa-project.org/>
- [37] AVISPA. (2019). *SPAN: A Security Protocol Animator for AVISPA*. Accessed: Oct. 25, 2023. [Online]. Available: <http://www.avispa-project.org/>
- [38] D. V. Oheimb, "The high-level protocol specification language HLPSSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, Tallinn, Finland, Sep. 2005, pp. 1–2.
- [39] D. Basin, S. Mödersheim, and L. Viganó, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, Jun. 2005.
- [40] M. Turuani, "The CL-Atse porotocol analyser," in *Proc. Int. Conf. Rewriting Techn. Appl. (RTA)*, Seattle, WA, USA, Aug. 2006, pp. 227–286.
- [41] S. Yu, J. Lee, K. Lee, K. Park, and Y. Park, "Secure authentication protocol for wireless sensor network in vehicular communications," *Sensors*, vol. 18, p. 3191, Jul. 2018.
- [42] K. Park, Y. Park, Y. Park, A. Goutham Reddy, and A. K. Das, "Provably secure and efficient authentication protocol for roaming service in global mobility networks," *IEEE Access*, vol. 5, pp. 25110–25125, 2017.
- [43] V. Odelu, A. K. Das, K. R. Choo, N. Kumar, and Y. Park, "Efficient and secure time-key based single sign-on authentication for mobile devices," *IEEE Access*, vol. 5, pp. 27707–27721, 2017.
- [44] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Gener. Comput. Syst.*, vol. 68, pp. 74–88, Mar. 2017.
- [45] K. Park, Y. Park, Y. Park, and A. K. Das, "2PAKEP: Provably secure and efficient two-party authenticated key exchange protocol for mobile environment," *IEEE Access*, vol. 6, pp. 30225–30241, 2018.
- [46] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, N. Kumar, Y. Park, and S. Tanwar, "Design of an anonymity-preserving group formation based authentication protocol in global mobility networks," *IEEE Access*, vol. 6, pp. 20673–20693, 2018.
- [47] 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 Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.
- [48] I. Ullah, S. Zeadally, N. U. Amin, M. Asghar Khan, and H. Khattak, "Lightweight and provable secure cross-domain access control scheme for Internet of Things (IoT) based wireless body area networks (WBAN)," *Microprocessors Microsystems*, vol. 81, Mar. 2021, Art. no. 103477.
- [49] M. A. Khan, H. Alhakami, W. Alhakami, A. V. Shvetsov, and I. Ullah, "A smart card-based two-factor mutual authentication scheme for efficient deployment of an IoT-based telecare medical information system," *Sensors*, vol. 23, no. 12, p. 5419, Jun. 2023.
- [50] S. Javed, M. A. Khan, A. M. Abdullah, A. Alsirhani, A. Alomari, F. Noor, and I. Ullah, "An efficient authentication scheme using blockchain as a certificate authority for the Internet of Drones," *Drones*, vol. 6, no. 10, p. 264, Sep. 2022.



**KHAISTA RAHMAN** received the M.Sc. degree in electronics from Preston University, Islamabad, in 2010, and the M.S. degree in electronics from International Islamic University, Islamabad, Pakistan, in 2017. He is currently pursuing the Ph.D. degree in electronic engineering with the School of Engineering and Applied Sciences, Isra University, Pakistan. He is the Director of a private establishment and serves as a Consultant to prominent companies in Islamabad. His research interests include unmanned aerial vehicles (UAVs), cybersecurity, satellite communication, and digital fault diagnosis of electronic printed circuit boards (PCBs).



**MUHAMMAD ASGHAR KHAN** (Member, IEEE) received the Ph.D. degree in electronic engineering from the School of Engineering and Applied Sciences, Isra University, Islamabad, Pakistan. He is currently an Associate Professor and heads the Electrical Engineering Department, Hamdard University, Islamabad. He is also a Research Fellow with the Smart Systems Engineering Laboratory, Prince Sultan University, Riyadh, Saudi Arabia. With an extensive publication history, he has authored or coauthored over 100 technical and review articles, prominently featured in reputable journals, such as IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE INTERNET OF THINGS JOURNAL. His research interests include drones/UAVs, specifically focusing on networks, platforms, security, and applications and services. He has presented his research findings at numerous national and international conferences. Actively engaged in academia, he contributes as a Reviewer for distinguished journals published by IEEE, Elsevier, and Springer. He has also served as the guest editor for various international journals. In recognition of his outstanding scholarly contributions, Stanford University acknowledged him as one of the top 2% of highly cited scientists globally, in 2023.



**FATEMEH AFGHAH** (Senior Member, IEEE) received the B.Sc. and M.Sc. (Hons.) degrees in electrical engineering from the Khajeh Nasir Toosi University of Technology (KNTU), Tehran, in 2005 and 2008, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Maine, in 2013. She was an affiliated faculty with the Partnership for Native American Cancer Prevention between Arizona Cancer Center and NAU. She was a Visiting Graduate Student

with the ECE Department, University of Maryland, College Park, MD, USA, from 2012 to 2013. She is currently a tenured Associate Professor with the Department of Electrical and Computer Engineering, Clemson University. Before joining Northern Arizona University (NAU), she was an Associate Professor (with tenure) with the School of Informatics, Computing and Cyber Systems, NAU. She is also the Director of the Intelligent Systems and Wireless Networking (IS-WiN) Laboratory. She was a recipient of the NSF CAREER Award, in 2020, the AFOSR Young Investigator Award, in 2019, the NAU's Most Promising New Scholar Award, in 2020, the NSF CISE Research Initiative Initiation (CRII) Award, in 2017, and the AFRL Visiting Research Faculty Award, in 2016 and 2017. She was the Chair and an Organizer of the IEEE Communications and Signal Processing Chapter at the IEEE Central North Carolina Section. She serves as an Associate Editor for *Computer Networks* (Elsevier), *Journal of Network and Computer Applications* (Elsevier), *Ad Hoc Journal* (Elsevier), *ACM Transactions on Computing for Healthcare*, *Neural Processing Letters* (Springer), *IET Wireless Sensor Systems*, and *Frontiers Aerial and Space Networks*. She was a Representative of IEEE Regions R1–6 on the Membership Board Standing Committee for the IEEE Signal Processing Society, from 2016 to 2018.



**GORDANA BARB** received the M.Sc. degree in electronics and telecommunications from the University of Aveiro, in 2017, and the Ph.D. degree in electronics and telecommunications from the Politehnica University of Timisoara, in 2021. She is currently a University Lecturer with the Communications Department, Politehnica University of Timisoara, and also an RF Engineer. Her research interests include 5G communication systems, cybersecurity, UAVs, massive MIMO, V2X, and millimeter-wave communications. She has contributed to various international journals with her research publications and has also presented her work in international conference proceedings.



**NISREEN INNAB** received the Ph.D. degree in computer information systems, in 2008. She is currently an Associate Professor with the Department of Computer Science and Information Systems, College of Applied Sciences, Almaarefa University, Riyadh, Saudi Arabia. She is also a Program Director of the Information Systems Program. She supervised many theses for the Master of Information Security. Furthermore, she also supervised many graduation projects for computer science, information systems, and health information systems. She has published many scientific research in international high-prestigious journals indexed in Web of Science and Scopus. Her research interests include information security, cyber security, machine learning, artificial intelligence, and the IoT.

information systems, and health information systems. She has published many scientific research in international high-prestigious journals indexed in Web of Science and Scopus. Her research interests include information security, cyber security, machine learning, artificial intelligence, and the IoT.



**TANVEER AHMED CHEEMA** received the M.Phil. degree in electronics from Quaid-e-Azam University, in 1999, and the Ph.D. degree in electrical engineering from Mohammad Ali Jinnah University, in 2005. He is currently the Chairperson of the Department of Electrical Engineering, Isra University, Islamabad Campus. He is also a Consultant for several prominent companies in Islamabad. His contributions to the field are evident through the publication of around 25 papers in various journals and conferences. His research interests include digital communications, information security, digital image processing, and optimization techniques.