electronics

MDPI

Article

A Traceable and Privacy-Preserving Authentication for UAV Communication Control System

Chin-Ling Chen [1,2,3], Yong-Yuan Deng [3,*], Wei Weng [1,*], Chi-Hua Chen [4,*], Yi-Jui Chiu [5] and Chih-Ming Wu [6]

1 College of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China; clc@mail.cyut.edu.tw
2 School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
3 Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan
4 College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350116, China
5 School of Mechanical and Automotive Engineering, Xiamen University of Technology, Xiamen 361024, China; chiuyijui@xmut.edu.cn
6 School of Civil Engineering and Architecture, Xiamen University of Technology, Xiamen 361024, China; chihmingwu@xmut.edu.cn
* Correspondence: allen.nubi@gmail.com (Y.-Y.D.); wwweng@xmut.edu.cn (W.W.); chihua0826@gmail.com (C.-H.C.)

Received: 15 November 2019; Accepted: 20 December 2019; Published: 1 January 2020

Abstract: In recent years, the concept of the Internet of Things has been introduced. Information, communication, and network technology can be integrated, so that the unmanned aerial vehicle (UAV) from consumer leisure and entertainment toys can be utilized in high value commercial, agricultural, and defense field applications, and become a killer product. In this paper, a traceable and privacy-preserving authentication is proposed to integrate the elliptic curve cryptography (ECC), digital signature, hash function, and other cryptography mechanisms for UAV application. For sensitive areas, players must obtain flight approval from the ground control station before they can control the UAV in these areas. The traditional cryptography services such as integrity, confidentiality, anonymity, availability, privacy, non-repudiation, defense against DoS (Denial-of-Service) attack, and spoofing attack can be ensured. The feasibility of mutual authentication was proved by BAN logic. In addition, the computation cost and the communication cost of the proposed scheme were analyzed. The proposed scheme provides a novel application field.

Keywords: UAV; Mutual authentication; Privacy; Traceable; BAN logic

1. Introduction

With the development of battery power, sensing systems, artificial intelligence and other technologies, small commercial unmanned aerial vehicles (UAVs) combining these technologies have, in recent years, become a very popular product. Small UAVs have tremendous potential in different fields and tasks, and have great flexibility in application. In addition to personal aerial photography, entertainment, and commercial markets, they can be used in various monitoring work such as disaster relief [1], in various environments involving animals and plants, coasts and borders [2,3], in freight transportation, military and police law enforcement tasks, and even agricultural and industrial applications [4–8]. Nader et al. [9] pointed out that UAVs could be employed in different ways to achieve smart city services. For example, using UAVs for traffic monitoring and management, merchandise delivery, health and emergency services, and air taxi services can enhance these services in terms of quality, productivity, timeliness, reliability, and performance and could help reduce the

costs of offering these services. However, small UAVs also can pose a variety of security threats under improper use.

Although every case of an unmanned aerial vehicle being improperly used has complex security implications, it is difficult to sum this up as a single security threat; for example, in the protection of important persons, unmanned aerial vehicles may violate their privacy, launch attacks, threaten their lives, or destroy their facilities. Different threats in several different cases are examined below.

(1) Personal safety of specific persons and military and police officers: The small UAVs used by the fighters of the Organization of Islamic States could, for example, be used to attack enemy soldiers on the battlefield in the Middle East. This situation can be described as the future personal safety protection work for important persons and law enforcement officers. It is necessary to take precautions against small UAVs.
(2) Protection of key infrastructure: In July 2018, Greenpeace posted a video on the Internet showing the small UAVs operated by members of Greenpeace, painted superhuman, hitting a spent fuel facility near Lyon, France. This incident still reminds us of the importance of UAV protection for key infrastructure or the environment (for example, forest fire detection).
(3) Flight safety: In late December 2018 and early January 2019, London's Gatwick and Heathrow airports were disrupted by UAVs, causing chaos in takeoff, landing, and scheduling. The former even closed for 33 h and cancelled hundreds of flights, causing losses of more than 50 million pounds.
(4) Privacy and confidentiality protection: UAVs can be used to steal important confidential information, such as in Northern Ireland in August 2016, when UAVs were used to take pictures of people entering passwords in ATMs. Small UAVs can even be used as hackers' tools to further steal business secrets. According to the reports of The Times on 21 January 2019, in recent years, secrets have been stolen by eavesdropping, or even masquerading as wireless network connections to obtain employee passwords, etc. More and more companies are seeking anti-UAV technology to ensure against commercial benefits by stealing secrets by disguising wireless network connections to obtain employee passwords and other information.
(5) Other criminal behaviors: In addition to the use of military and police personnel to monitor and assist in law enforcement, small UAVs may also operate in the hands of criminals. The surveillance functions provided by UAVs also enable criminal groups to detect and monitor their targets before committing crimes.
(6) Security loopholes become a hidden concern: In addition to the improper use by the users themselves, UAVs may also be attacked by intentional hackers. By means of security loopholes including GPS and control signals, wireless networks and so on, "hijacking" may take control of a UAV. Vulnerabilities in the UAV manufacturer's security may also become another type of drone-derived security problem. A well-known software technology website Check Point reported in November 2018 that the world's largest manufacturer, China's Dajiang, has a security vulnerability in its identity authentication process. If it is attacked by a hacker, it may leak the location of the operator and the captured image, etc. Even the possibility of intercepting the carried goods also highlights the security problems of drones.

To sum up, in spite of UAVs being widely used in civilian, commercial, and military applications in recent years, because they use wireless networks for information exchange, there are many security issues that are faced.

Firstly, "privacy" refers to the part of an individual that he does not want to be known by others, and that he has the right to protect. In English, "to be let alone" means to "not be disturbed by others", which is the basic spirit of privacy. Privacy also means "secret". In general, what we call privacy refers to information privacy. Privacy and freedom are related to individual behavior rather than inappropriate observation and interference by others. The interests of privacy include sexual activities, religious practices, and political activities. What is the importance of privacy? Privacy is about human

dignity, personal subjectivity, and personality development. If some of a person's own information is exposed, he will feel uncomfortable, embarrassed, or harassed by others, and it will be difficult to live comfortably. Compared with personal privacy, sensitive information of the state or government has a greater impact.

Secondly, the malicious attacker can perform passive eavesdropping, active interfering, leaking of secret information, data tampering, denial of service, message misuse, message replay, and impersonation attack between sender and receiver. This will cause the resource collapse attack, and even disturb the operations of routing protocol for UAVs [10]. UAVs are conducted in flying ad hoc networks (FANETs) which should provide defense against various known attacks under wireless environment.

Thirdly, because of the specific properties of FANET (wireless links, collaborative characteristics, uncontrollable environment, and lack of a fixed infrastructure) securing the network is difficult. The traditional security issues are availability, authentication, integrity, and confidentiality, which have become targets that the attacker wants to break. [11]. Legitimate UAVs suffer from malicious UAVs by implanting the incorrect information into their sensors. Therefore, it causes these compromised UAVs to transmit the wrong messages for the base station, and thereby endangering the data integrity [10].

In order to legalize and guarantee the privacy of the broadcasted messages, much literature is focused on this issues. For example, Strohmeier et al. [12] surveyed an automatic dependent surveillance-broadcast protocol (ADS-B), and that is an on-board component part of the UAV system, and discussed and listed the vulnerabilities in ADS-B protocol. Wesson et al. [13] further analyzed and evaluated the cryptographic strategies of ADS-B based on their effectiveness and practicality in the cost-averse, technologically-complex, and interoperability-focused aviation community. The purpose of these works was to find a suitable mechanism to ensure the security of the UAVs system for sensitive control areas.

In past literature, some articles [10,14–16] refer to malicious attacks on UAV applications, such as intrusion detection, enhancing security against the lethal cyber-attacks for UAV networks. Therefore, a Q-learning-based UAV power allocation strategy combining Q-learning and deep learning to accelerate the learning speed for attack modes was proposed by Xiao et al. [17]. García-Magariño et al. [16] used a secure asymmetric encryption with a pre-shared list of official UAVs and an agent-based approach to detect if an official UAV is physically hijacked. However, these articles only focus on the intrusion detection or the problem of UAVs being physical hijacked. It is a fact that to prevent all intrusions from being attacked by hackers, the fundamental solution is to propose an effective and comprehensive security protocol. Such a secure mechanism should comprehensively detect and provide information and identity authentication to achieve the purposes of availability, privacy, and non-repudiation and to defend against known attacks for the UAV's environment.

Recently, some literature [18–21] has used specific cryptographic algorithms to implement security mechanisms in UAVs. In 2017, Yoon et al. [18] used the Raspberry Pi to present a design of a second channel security system that can regain control of a UAV when there is an attack on the UAV. In this scheme, the authors only used flow charts to describe the scenario. The authors claimed that they can provide authentication with the ground station and defense against the DoS attack. However, this scheme does not present the detail cryptography scenario and no performance analysis.

Later, Chen et al. [19] proposed a mutual authentication improvement in security. In order to achieve higher efficiency and reduce the computational cost, thus the proposed scheme conformed to the network-connected UAV communication systems, and that satisfied the requirements of the limited bandwidth and computation resources. However, the authors used the asymmetric bilinear pairings mechanism and the cost of this was high and it was not supported by formal proof. Wazid et al. [20] also presented a lightweight remote user authentication and key agreement scheme to solve security issues between the user and the accessed drone in Internet of Drones (IoD) applications.

Recently, Tian et al. [21] proposed an efficient privacy-preserving authentication framework for the edge-assisted Internet of Drones. They followed a predictive UAV authentication approach. The

authors considered that location, identity, and flying routes of each legitimate UAV are sensitive information in the IoD network. Therefore, they proposed a secure authentication and privacy protection for an efficient MEC-assisted (mobile edge computing) framework. But this scheme did not consider mutual authentication for ensuring the communication entity.

In fact, due to the UAV's characteristics, it is hard to prevent a privacy leak. Therefore, this study aims to focus on sensitive areas (for example: airports and military areas) to set up this management system and use ECC (elliptic curve cryptography) technology [22,23] to ensure data integrity and nonrepudiation. It is a fact that any intruders can break through the defense function of the system if the security mechanism of the system is not perfect and the user's identity is not authenticated accurately. This study also intends to employ the proof mode of BAN logic mechanism for mutual authentication to eliminate the intrusive chances of malicious attackers.

The paper is organized as follows. The applied mechanisms and security mechanisms are reviewed and discussed in Section 2. The designs and flows of the proposed scheme are presented in Section 3. Security analyses and comparisons are discussed in Section 4. Finally, in Section 5, conclusions are offered.

2. Preliminary and Security Requirements

This section includes two subsections: (1) the elliptic curve cryptography and Diffie–Hellman key exchange are presented in Section 2.1 and (2) security requirements are defined in Section 2.2.

2.1. Elliptic Curve Cryptography and Diffie–Hellman Key Exchange

Elliptic curve cryptography [22,23] was proposed in 1995. Digital signature schemes can be used to provide the following basic cryptographic services: data integrity, data origin authentication, and non-repudiation.

The Diffie–Hellman key exchange [24] is a method for securely exchanging cryptographic keys over a public channel. It is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications by using a symmetric key cipher.

The following problems exist for the Elliptic Curve Diffie-Hellman method:

Computational Diffie–Hellman (CDH) Problem: Given aP and bP, where $a, b \in R$, $Z * q$, and P are the generator of G, compute abP.
Decisional Diffie–Hellman (DDH) Problem: Given aP, bP, and cP, where $a, b, c \in R$, $Z * q$, and P are the generators of G, confirm whether or not $cP = abP$, which is equal to confirming whether or not $c = ab \bmod q$.

2.2. Security Requirements

A UAV communication control system has the following main security requirements and known attacks [11,13–15,19,20,25]:

- Mutual authentication: this ensures that only legitimate parties are allowed to participate in the UAV network. There are two types of authentication services: node authentication and message authentication [11,19,20,25]. In order to ensure the communication security. The communication entity should perform mutual authentication before communication. As long as the mutual authentication is implemented, some known attacks can be excluded.
- Integrity: preventing the altering GPS coordinates or disseminating of false information [25], thus ensuring the consistent and uncompromising adherence of data message over their whole passage through the flying networks [11,19,20]
- Confidentiality: Only the authorized UAVs are allowed to access the data packets [11,13,19,20,25].

- Identity anonymity: The UAV communication control system should keep identity anonymity from the attacker to ensure the users real identity is not obtained from eavesdropped or captured messages [11].
- Availability: The UAV communication control system should be always available to provide all services in any time and in any conditions [11,25].
- Privacy: By tracking the messages sent out by the same UAV at different locations, adversaries can disclosure the UAVs' identities and perform further analysis to get other information from the UAVs [11,18,20].
- Non-repudiation: Repudiation threat comes from the UAVs denying their behaviors in the IoD. For example, malicious UAVs abuse their valid identities to broadcast fake information in the IoD [18,20,25].
- DoS attack: DoS attack means that a malicious node attempts to exhaust energy resources of UAVs or disturb the network and routing protocol [15,20,25].
- Spoofing attack: The attacker could generate a spoofed message such that the receiver gets the incorrect message [15,25].

3. The Proposed Scheme

This section includes nine subsections: (1) system architecture is designed and described in Section 3.1, (2) the used notations in this study are defined in Section 3.2, (3) the manufacturer (UAV) registration phase of the proposed scheme is illustrated in Section 3.3, (4) the player (mobile device) registration phase of the proposed scheme is presented in Section 3.4, (5) the ground control station registration phase of the proposed scheme is described in Section 3.5, (6) the player and manufacturer authentication and communication phase of the proposed scheme is shown in Section 3.6, (7) the player and ground control station authentication and communication phase of the proposed scheme is designed in Section 3.7, (8) the player, UAV, and ground control station authentication and communication phase of the proposed scheme is discussed in Section 3.8, and (9) the ground control station and UAV authentication and communication phase of the proposed scheme is illustrated in Section 3.9.

3.1. System Architecture

Figure 1 is the system framework of the proposed scheme in this study.

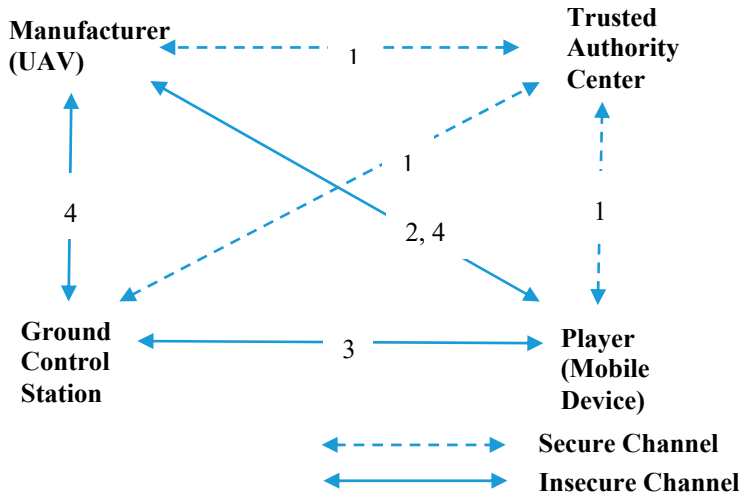

Figure 1. The framework of a traceable and privacy-preserving authentication for UAV ad hoc communication.

There are four parties in the scheme:

(1) Trusted authority center: a trusted third party agency which provides a public key and private key to the registrant.
(2) Manufacturer (UAV): a UAV manufacturing company. The company has jurisdiction over all manufactured UAVs.
(3) Player (mobile device): a person who intends to control a UAV. He/she must first buy or rent a UAV from the manufacturer, then obtain the flight permit before he/she can control the UAV.
(4) Ground control station (GCS): a control center that provides the facilities for human control of the UAV. A GCS reviews the flight path proposed by the player, and decides whether to agree to the flight request.

1. All UAVs manufactured, all mobile devices carried by players, and all ground control stations must be registered to the trusted authority center through a secure channel. The manufacturer (UAV), player (with mobile device), and ground control station sends their universally unique IDs to the trusted authority center. The trusted authority center returns parameters calculated by elliptic curve group technology.
2. When a player wants to control UAVs, the player carries his/her mobile device to buy or rent a UAV from the manufacturer. After mutual authentication between the player and the manufacturer, the manufacturer will transfer the purchase or rental certificate of the UAV to the player, and store the certificate to the UAV.
3. After the player has the right to use the UAV, then he/she must submit flight information and a purpose to the ground control station for review. After mutual authentication between the player and the ground control station, the ground control station will transfer the decision of the flight plan to the player, and keep the relevant flight information.
4. The player transfers the purchase or rental certificate of the UAV, and the flight path agreed by the ground control station to the UAV. After mutual authentication between the player and the UAV and mutual authentication between the UAV and the ground control station, the ground control station will confirm the legality of the UAV flight path. Once the legality of the relevant identity and flight path have been confirmed, the player can control the UAV through his/her mobile device.

3.2. Notations

q:	A k-bit prime
F_q:	A prime finite field
E/F_q:	An elliptic curve E over F_q
G:	A cyclic additive group of composite order q
P:	A generator for the group G
s:	A secret key of the trusted authority center
PK_{TAC}:	A public key of the trusted authority center, $PK_{TAC} = sP$
$H_i(\ )$:	ith one-way hash function
ID_x:	x's identity, like a universal unique ID code
r_x, a, b, c, d, e, f:	A random numbers of elliptic curve group
S_x:	x's elliptic curve group signature
SEK_{xy}:	A session key established by x and y
$E_x(m)$:	Use a session key x to encrypt the message m
$D_x(m)$:	Use a session key x to decrypt the message m
Sig_{xy}:	The signed message for parties x and y
SK_x/PK_x:	x's private key SK_x/x's public key PK_x
$S_{SK_x}(m)$:	Use x's private key SK_x to sign the message m

$V_{PK_x}(m)$:	Use x's public key PK_x to verify the message m
CHK_x:	x's verified message
$A \stackrel{?}{=} B$:	Determines if A is equal to B
$M_{payment}$:	The payment message between the player and the manufacturer (UAV)
$M_{request}$:	The flight plan proposed by the player
$M_{confirm}$:	The flight permission issued by ground control station to UAV
M_{GPS}:	The GPS message reported by the UAV
c_i:	The session key encrypted sensitive information
$Cert_{UAV}$:	The purchase or rental certificate of the UAV held by the player

3.3. Manufacturer (UAV) Registration Phase

The manufacturer must take the UAV to register with the trusted authority center. The manufacturer (UAV) registration phase of the proposed scheme is shown in Figure 2.

Step 1: The manufacturer selects an identity ID_{UAV}, and transmits it to the trusted authority center.

Step 2: The trusted authority center selects a random number r_{UAV}, calculates

$$\begin{aligned} R_{UAV} &= r_{UAV}P, \\ h_{UAV} &= H_1(ID_{UAV}, R_{UAV}), \\ S_{UAV} &= r_{UAV} + h_{UAV}s, \end{aligned}$$

and then sends $(R_{UAV}, S_{UAV}, PK_{UAV}, SK_{UAV})$ to the manufacturer.

Step 3: The manufacturer verifies

$$S_{UAV}P \stackrel{?}{=} R_{UAV} + H_1(ID_{UAV}, R_{UAV})PK_{TAC}.$$

If the verification is passed, the manufacturer stores $(R_{UAV}, S_{UAV}, PK_{UAV}, SK_{UAV})$ to the UAV.

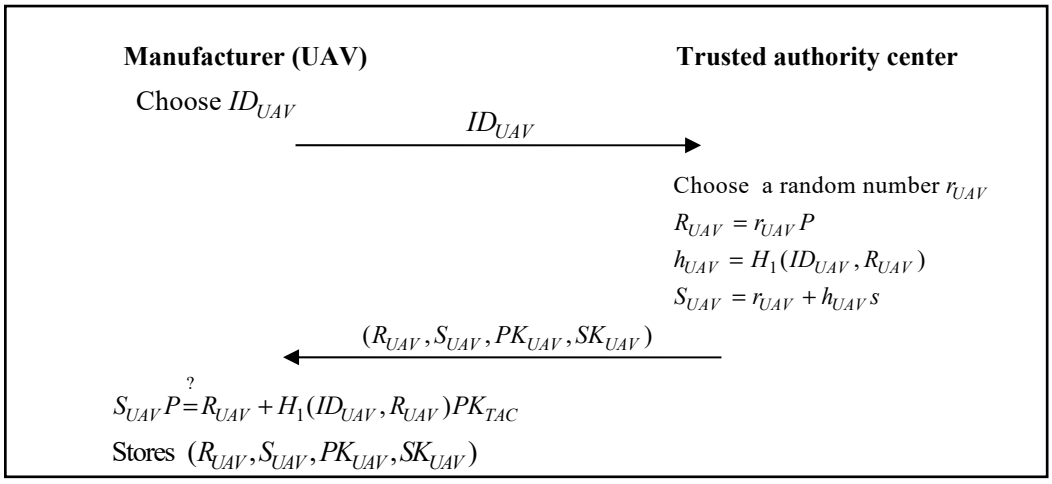

Figure 2. Manufacturer (UAV) registration phase of the proposed scheme.

3.4. Player (Mobile Device) Registration Phase

The player must take the mobile device to register with the trusted authority center. The scenarios of player (mobile device) registration phase is shown in Figure 3.

Step 1: The player selects an identity ID_{PMD}, and transmits it to the trusted authority center.

Step 2: The trusted authority center selects a random number r_{PMD}, calculates

$$\begin{aligned} R_{PMD} &= r_{PMD}P, \\ h_{PMD} &= H_1(ID_{PMD}, R_{PMD}), \\ S_{PMD} &= r_{PMD} + h_{PMD}s, \end{aligned}$$

and then sends $(R_{PMD}, S_{PMD}, PK_{PMD}, SK_{PMD})$ to the player.

Step 3: The player verifies

$$S_{PMD}P \stackrel{?}{=} R_{PMD} + H_1(ID_{PMD}, R_{PMD})PK_{TAC}.$$

If the verification is passed, the player stores $(R_{PMD}, S_{PMD}, PK_{PMD}, SK_{PMD})$ to the mobile device.

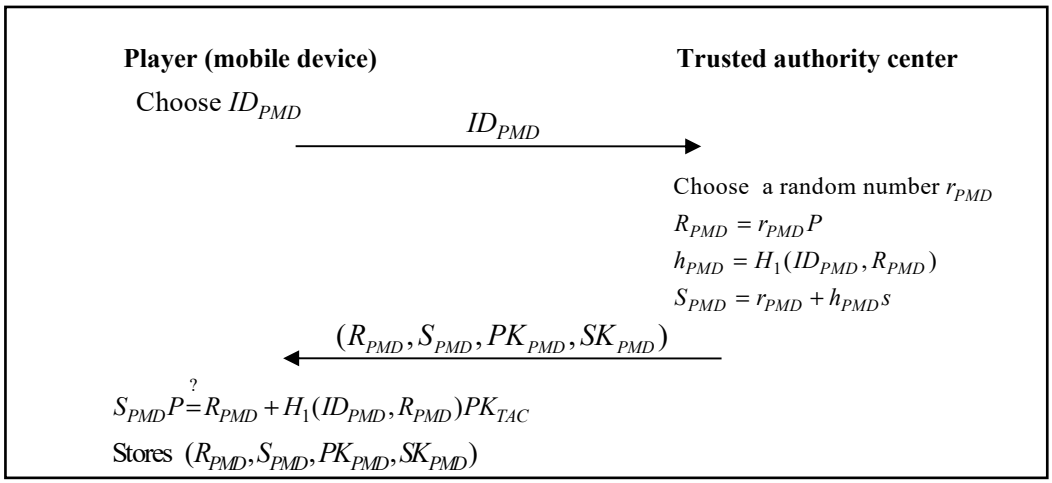

Figure 3. Player (mobile device) registration phase of the proposed scheme.

3.5. Ground Control Station Registration Phase

The ground control station must also register with the trusted authority center. The ground control station registration phase of the proposed scheme is shown in Figure 4.

Step 1: The ground control station selects an identity ID_{GCS}, and transmits it to the trusted authority center.

Step 2: The trusted authority center selects a random number r_{GCS}, calculates

$$\begin{aligned} R_{GCS} &= r_{GCS}P, \\ h_{GCS} &= H_1(ID_{GCS}, R_{GCS}), \\ S_{GCS} &= r_{GCS} + h_{GCS}s, \end{aligned}$$

and then sends $(R_{GCS}, S_{GCS}, PK_{GCS}, SK_{GCS})$ to the ground control station.

Step 3: The ground control station verifies

$$S_{GCS}P \stackrel{?}{=} R_{GCS} + H_1(ID_{GCS}, R_{GCS})PK_{TAC}.$$

If the verification is passed, the ground control station stores $(R_{GCS}, S_{GCS}, PK_{GCS}, SK_{GCS})$.

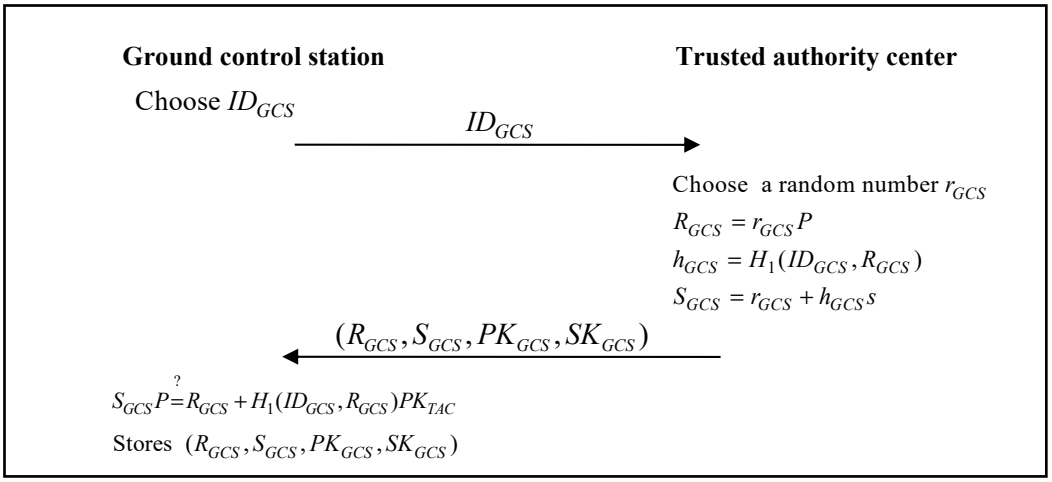

Figure 4. Ground control station registration phase of the proposed scheme.

3.6. Player and Manufacturer Authentication and Communication Phase

When a player wants to control UAVs, the player carries his/her mobile device to buy or rent a UAV from the manufacturer. After mutual authentication between the player and the manufacturer, the manufacturer will transfer the purchase or rental certificate of the UAV to the player, and store the certificate of the UAV. The player and manufacturer authentication and communication phase is shown in Figure 5.

Step 1: The player selects a random number a, computes

$$T_{PMD} = aP,$$

and then transmits $(ID_{PMD}, R_{PMD}, T_{PMD})$ to the manufacturer.

Step 2: The manufacturer selects a random number b, calculates

$$\begin{gathered} T_{UAV} = bP, \\ PK_{PMD} = R_{PMD} + H_1(ID_{PMD}, R_{PMD})PK_{TAC}, \\ K_{UP1} = S_{UAV}T_{PMD} + bPK_{PMD}, \\ K_{UP2} = bT_{PMD}, \end{gathered}$$

and the session key

$$SEK_{UP} = H_2(K_{UP1}, K_{UP2}).$$

The manufacturer then calculates

$$CHK_{PU} = H_3(SEK_{UP}, T_{PMD})$$

and transmits $(ID_{UAV}, R_{UAV}, T_{UAV}, CHK_{PU})$ to the player.

Step 3: The player calculates

$$\begin{gathered} PK_{UAV} = R_{UAV} + H_1(ID_{UAV}, R_{UAV})PK_{TAC}, \\ K_{PU1} = S_{PMD}T_{UAV} + aPK_{UAV}, \\ K_{PU2} = aT_{UAV}, \end{gathered}$$

and the session key

$$SEK_{UP} = H_2(K_{PU1}, K_{PU2}),$$

The player verifies

$$CHK_{PU} \stackrel{?}{=} H_3(SEK_{UP}, T_{PMD})$$

to check the legality of the manufacturer. If the verification is passed, the player computes

$$c_{PMD} = E_{SEK_{UP}}(M_{payment}),$$
$$CHK_{UP} = H_3(SEK_{UP}, T_{UAV}),$$

and transmits $(ID_{PMD}, c_{PMD}, CHK_{UP})$ to the manufacturer.

Step 4: The manufacturer verifies

$$CHK_{UP} \stackrel{?}{=} H_3(SEK_{UP}, T_{UAV})$$

to check the legality of the player. If the verification is passed, the session key SEK_{UP} between the player and the manufacturer is established successfully. The manufacturer calculates

$$M_{payment} = D_{SEK_{UP}}(c_{PMD})$$

to get the payment information of the player. After the payment, the manufacturer generates the encrypted purchase or rental certificate of the UAV

$$c_{UAV} = E_{SEK_{UP}}(M_{payment}, Cert_{UAV}),$$
$$Sig_{UAV} = S_{SK_{UAV}}(M_{payment}, Cert_{UAV}),$$

and transmits $(ID_{UAV}, c_{UAV}, Sig_{UAV})$ to the player.

Step 5: The player decrypts the received message

$$(M_{payment}, Cert_{UAV}) = D_{SEK_{UP}}(c_{UAV}),$$

verifies the signature

$$(M_{payment}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV}),$$

and obtains the purchase or rental certificate of the UAV from the manufacturer.

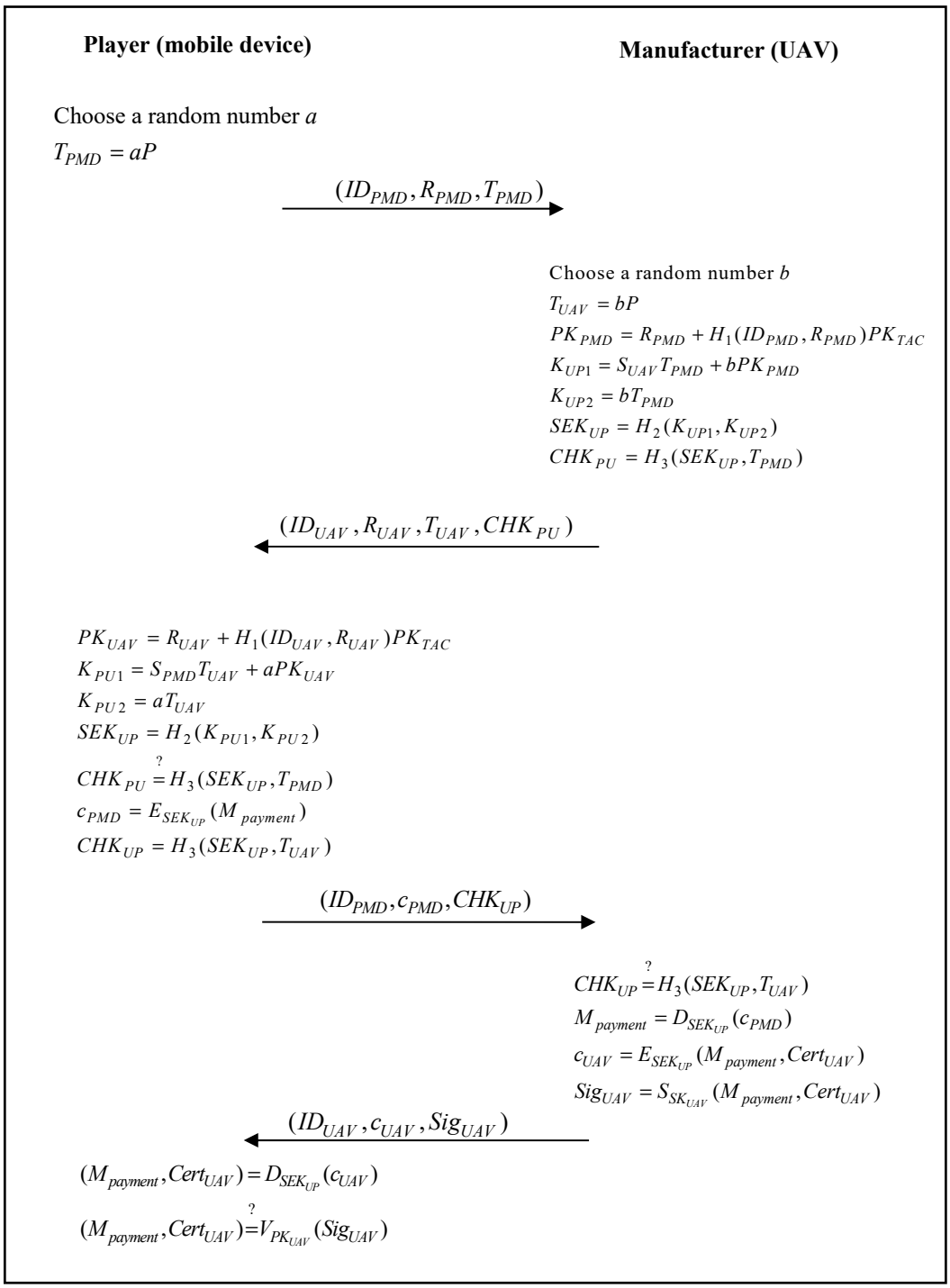

Figure 5. Player and manufacturer authentication and communication phase of the proposed scheme.

3.7. Player and Ground Control Station Authentication and Communication Phase

After the player has the right to use the UAV, then he/she must submit a flight path and purpose to the ground control station for review. After mutual authentication between the player and the ground control station, the ground control station will transfer the decision of the flight plan to the player, and keeps the relevant flight information. The player and ground control station authentication and communication phase of the proposed scheme is shown in Figure 6.

Step 1: The player selects a random number c, computes

$$T_{PMD2} = cP,$$

and then transmits $(ID_{PMD}, R_{PMD}, T_{PMD2})$ to the ground control station.

Step 2: The ground control station selects a random number d, calculates

$$\begin{gathered} T_{GCS} = dP, \\ PK_{PMD} = R_{PMD} + H_1(ID_{PMD}, R_{PMD})PK_{TAC}, \\ K_{GP1} = S_{GCS}T_{PMD2} + dPK_{PMD}, \\ K_{GP2} = dT_{PMD2}, \end{gathered}$$

and the session key

$$SEK_{GP} = H_2(K_{GP1}, K_{GP2}).$$

The ground control station then calculates

$$CHK_{PG} = H_3(SEK_{GP}, T_{PMD2})$$

and transmits $(ID_{GCS}, R_{GCS}, T_{GCS}, CHK_{PG})$ to the player.

Step 3: The player calculates

$$\begin{gathered} PK_{GCS} = R_{GCS} + H_1(ID_{GCS}, R_{GCS})PK_{TAC}, \\ K_{PG1} = S_{PMD}T_{GCS} + cPK_{GCS}, \\ K_{PG2} = cT_{GCS}, \end{gathered}$$

and the session key

$$SEK_{GP} = H_2(K_{PG1}, K_{PG2}).$$

The player verifies

$$CHK_{PG} \stackrel{?}{=} H_3(SEK_{GP}, T_{PMD2})$$

to check the legality of the ground control station. If the verification is passed, the player calculates

$$\begin{gathered} c_{PMD2} = E_{SEK_{GP}}(M_{request}, Cert_{UAV}), \\ CHK_{GP} = H_3(SEK_{GP}, T_{GCS}), \end{gathered}$$

and transmits $(ID_{PMD}, c_{PMD2}, CHK_{GP})$ to the ground control station.

Step 4: The ground control station verifies

$$CHK_{GP} \stackrel{?}{=} H_3(SEK_{GP}, T_{GCS})$$

to check the legality of the player. If the verification is passed, the session key SEK_{GP} between the player and the ground control station is established successfully. The ground control station calculates

$$(M_{request}, Cert_{UAV}) = D_{SEK_{GP}}(c_{PMD2})$$

to get the flight path information of the player. After the review, the ground control station generates the encrypted decision of the flight plan

$$\begin{gathered} c_{GCS} = E_{SEK_{GP}}(ID_{PMD}, M_{request}, Cert_{UAV}), \\ Sig_{GCS} = S_{SK_{GCS}}(ID_{PMD}, M_{request}, Cert_{UAV}), \end{gathered}$$

and transmits $(ID_{GCS}, c_{GCS}, Sig_{GCS})$ to the player.

Step 5: The player decrypts the received message

$$(ID_{PMD}, M_{request}, Cert_{UAV}) = D_{SEK_{GP}}(c_{GCS}),$$

verifies the signature

$$(ID_{PMD}, M_{request}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS}),$$

and obtains the decision of the flight plan from the ground control station.

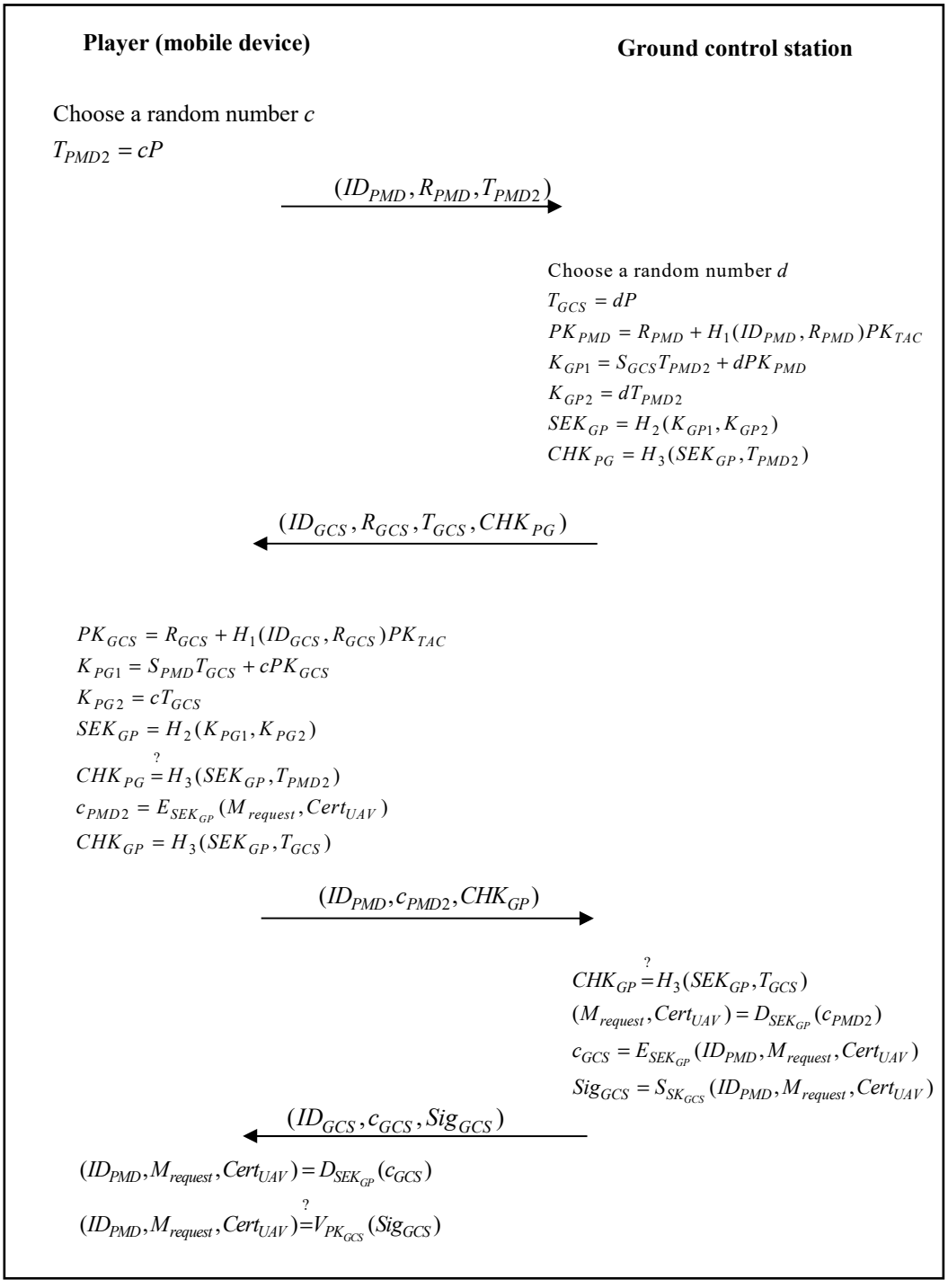

Figure 6. Player and ground control station authentication and communication phase of the proposed scheme.

3.8. Player, UAV and Ground Control Station Authentication and Communication Phase

The player transfers the purchase or rental certificate of the UAV, and the flight path agreed by the ground control station to the UAV. After mutual authentication between the player and the UAV, and mutual authentication between the UAV and the ground control station, the UAV will confirm the legality of the flight path again from the ground control station. After confirming the legality of the relevant identity and flight path, the player can control the UAV through his/her mobile device. The player, UAV and ground control station authentication and communication phase of the proposed scheme is shown in Figure 7.

Step 1: The player calculates

$$c_{PMD3} = E_{SEK_{UP}}(M_{request}, Cert_{UAV}),$$
$$Sig_{PMD3} = S_{SK_{PMD}}(M_{request}, Cert_{UAV}),$$

and transmits $(ID_{PMD}, c_{PMD3}, Sig_{PMD3})$ to the UAV.

Step 2: The UAV decrypts the received message

$$(M_{request}, Cert_{UAV}) = D_{SEK_{UP}}(c_{PMD3}),$$

verifies the signature

$$(M_{request}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{PMD}}(Sig_{PMD3}),$$

and obtains the purchase or rental certificate of the UAV, and the flight path agreed by the ground control station.

The UAV then chooses a random number e, calculates

$$T_{UAV2} = eP,$$

and then transmits $(ID_{UAV}, R_{UAV}, T_{UAV2})$ to the ground control station.

Step 3: The ground control station chooses a random number f, computes

$$T_{GCS2} = fP,$$
$$PK_{UAV} = R_{UAV} + H_1(ID_{UAV}, R_{UAV})PK_{TAC},$$
$$K_{GU1} = S_{GCS}T_{UAV2} + fPK_{UAV},$$
$$K_{GU2} = fT_{UAV2},$$

and the session key

$$SEK_{GU} = H_2(K_{GU1}, K_{GU2}).$$

The ground control station then calculates

$$CHK_{UG} = H_3(SEK_{GU}, T_{UAV2}),$$

and transmits $(ID_{GCS}, R_{GCS}, T_{GCS2}, CHK_{UG})$ to the UAV.

Step 4: The UAV calculates

$$PK_{GCS} = R_{GCS} + H_1(ID_{GCS}, R_{GCS})PK_{TAC},$$
$$K_{UG1} = S_{UAV}T_{GCS2} + ePK_{GCS},$$
$$K_{UG2} = eT_{GCS2},$$

and the session key

$$SEK_{GU} = H_2(K_{UG1}, K_{UG2}).$$

The UAV verifies

$$CHK_{UG} \stackrel{?}{=} H_3(SEK_{GU}, T_{UAV2})$$

to check the legality of the ground control station. If the verification is passed, the UAV calculates

$$c_{UAV2} = E_{SEK_{GU}}(ID_{PMD}, M_{request}, Cert_{UAV}),$$
$$CHK_{GU} = H_3(SEK_{GU}, T_{GCS2}),$$

and transmits $(ID_{UAV}, c_{UAV2}, CHK_{GU})$ to the ground control station.

Step 5: The ground control station verifies

$$CHK_{UG} \stackrel{?}{=} H_3(SEK_{GU}, T_{GCS2})$$

to check the legality of the UAV. If the verification is passed, the session key SEK_{GU} between the UAV and the ground control station is established successfully. The ground control station calculates

$$(ID_{PMD}, M_{request}, Cert_{UAV}) = D_{SEK_{GU}}(c_{UAV2})$$

to get the flight path information of the UAV. After the review, the ground control station generates the encrypted confirm message of the flight plan

$$c_{GCS2} = E_{SEK_{GU}}(ID_{PMD}, M_{confirm}, Cert_{UAV}),$$
$$Sig_{GCS2} = S_{SK_{GCS}}(ID_{PMD}, M_{confirm}, Cert_{UAV}),$$

and transmits $(ID_{GCS}, c_{GCS2}, Sig_{GCS2})$ to the UAV.

Step 6: The UAV decrypts the received message

$$(ID_{PMD}, M_{confirm}, Cert_{UAV}) = D_{SEK_{GU}}(c_{GCS2}),$$

verifies the signature

$$(ID_{PMD}, M_{confirm}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS2}),$$

and obtains the confirm message of the flight plan from the ground control station. Then, the UAV generates the encrypted confirm message of the flight plan and GPS information

$$c_{UAV3} = E_{SEK_{UP}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}),$$
$$Sig_{UAV3} = S_{SK_{UAV}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}),$$

and transmits $(ID_{UAV}, c_{UAV3}, Sig_{UAV3})$ to the player.

Step 7: The player decrypts the received message

$$(ID_{PMD}, M_{request}, M_{GPS}, Cert_{UAV}) = D_{SEK_{UP}}(c_{UAV3}),$$

verifies the signature

$$(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV3}),$$

then obtains the confirm message of the flight plan and GPS information.

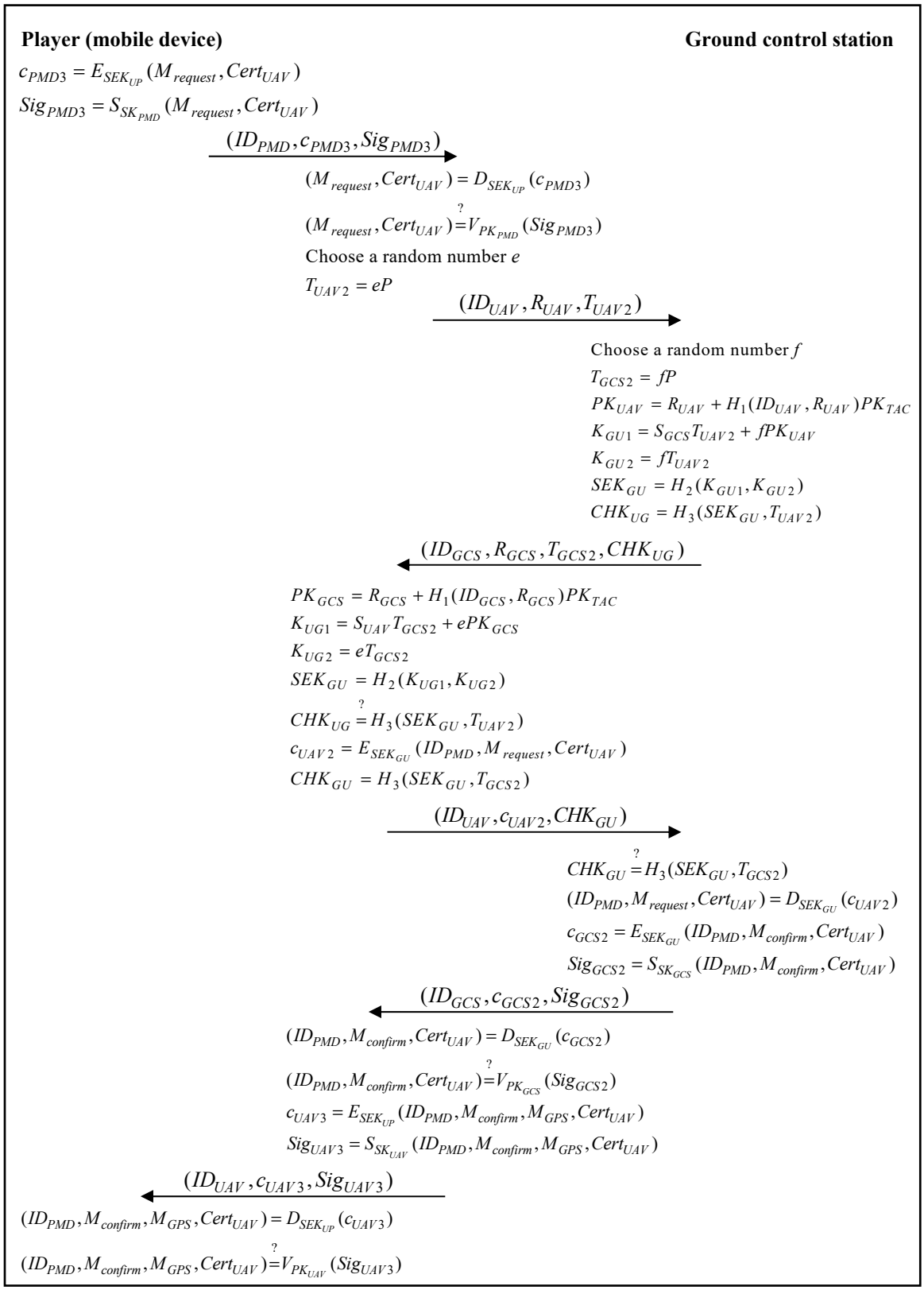

Figure 7. Player, UAV, and ground control station authentication and communication phase of the proposed scheme.

3.9. Ground Control Station and UAV Authentication and Communication Phase

When the ground control station wants to know whether the scope of the regulation has been applied to the UAV, the ground control station can ask the UAV to provide relevant proof. After mutual authentication between the ground control station and the UAV, the UAV will respond and confirm the message of the flight plan from the ground control station and GPS information to the ground control station. The ground control station and UAV authentication and communication phase of the proposed scheme is shown in Figure 8.

Step 1: The ground control station calculates

$$c_{GCS3} = E_{SEK_{GU}}(ID_{UAV}, M_{request}),$$
$$Sig_{GCS3} = S_{SK_{GCS}}(ID_{UAV}, M_{request}),$$

and transmits $(ID_{UAV}, M_{request}) = D_{SEK_{GU}}(c_{GCS3})$ to the UAV.

Step 2: The UAV decrypts the received message

$$(ID_{UAV}, M_{request}) = D_{SEK_{GU}}(c_{GCS3}),$$

verifies the signature

$$(ID_{UAV}, M_{request}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS3}),$$

and obtains the legality check request from the ground control station. Then, the UAV generates the encrypted confirmation message of the flight plan and GPS information

$$C_{UAV4} = E_{SEK_{GU}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}),$$
$$Sig_{UAV4} = S_{SK_{UAV}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}),$$

and transmits $(ID_{UAV}, c_{UAV4}, Sig_{UAV4})$ to the ground control station.

Step 3: The ground control station decrypts the received message

$$(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}) = D_{SEK_{GU}}(c_{UAV4}),$$

verifies the signature

$$(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV4}),$$

then obtains the response of the UAV and GPS information.

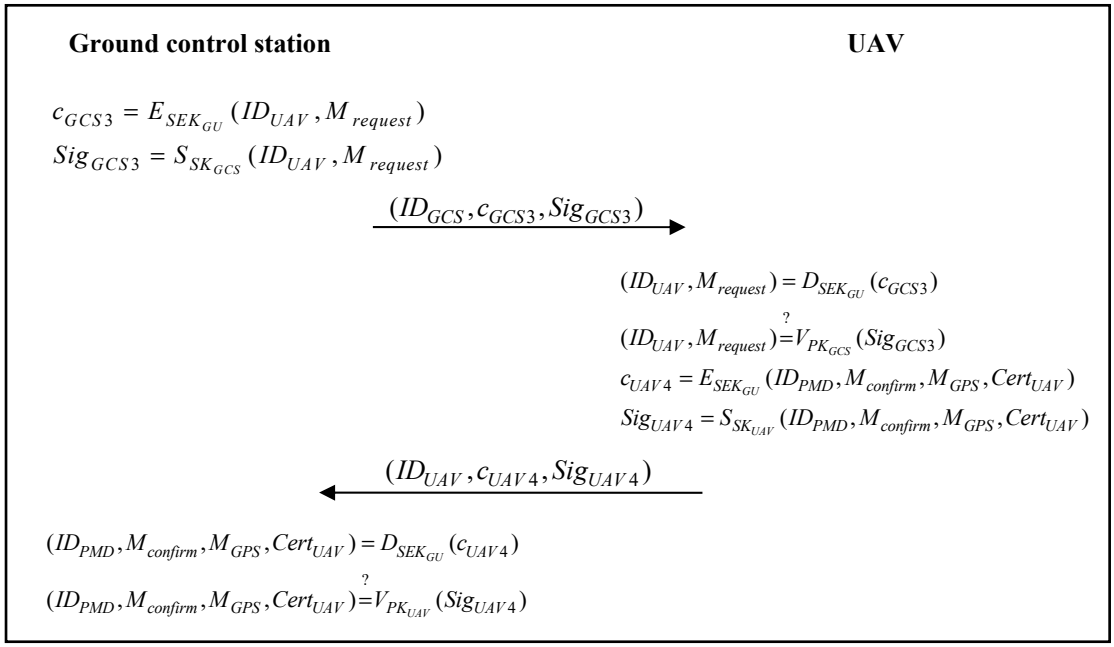

Figure 8. Ground control station and UAV authentication and communication phase of the proposed scheme.

4. Security Analysis

This section includes nine subsections: (1) the mutual authentication of the proposed scheme is analyzed in Section 4.1, (2) the integrity and confidentiality of the proposed scheme are evaluated in Section 4.2, (3) the identity anonymity and privacy of the proposed scheme are proved in Section 4.3, (4) availability and prevention of DoS attack are discussed in Section 4.4, (5) prevention of spoofing attack is discussed in Section 4.5, (6) the non-repudiation of the proposed scheme is analyzed in Section 4.6, (7) security issues are compared in Section 4.7, (8) the computation cost of the proposed scheme is compared with other schemes in Section 4.8, and (9) the communication cost of the proposed scheme is compared with other schemes in Section 4.9.

4.1. Mutual Authentication

BAN logic [26] is used to prove that the proposed scheme achieves mutual authentication between different parties in each phase.

In the player and manufacturer authentication and communication phase, the main goal of the scheme is to make sure whether the legality is authenticated by the player P and the manufacturer M.

$G1: \; P| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$

$G2: \; P| \equiv M| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$

$G3: \; M| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$

$G4: \; M| \equiv P| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$

$G5: \; P| \equiv ID_{UAV}$

$G6: \; P| \equiv M| \equiv ID_{UAV}$

$G7: \; M| \equiv ID_{PMD}$

$G8: \; M| \equiv P| \equiv ID_{PMD}$

According to the player and manufacturer authentication and communication phase, BAN logic is used to produce an idealized form as follows.

$M1:\ (< ID_{PMD}, R_{PMD}, T_{PMD} >_{PK_{UAV}}, < H(SEK_{UP}, T_{UAV}) >_{CHK_{UP}})$
$M2:\ (< ID_{UAV}, R_{UAV}, T_{UAV} >_{PK_{PMD}}, < H(SEK_{UP}, T_{PMD}) >_{CHK_{PU}})$

To analyze the proposed scheme, the following assumptions are made.

$A1:\ P| \equiv \#(T_{PMD})$
$A2:\ M| \equiv \#(T_{PMD})$
$A3:\ P| \equiv \#(T_{UAV})$
$A4:\ M| \equiv \#(T_{UAV})$
$A5:\ P| \equiv M| \Rightarrow P \overset{SEK_{UP}}{\leftrightarrow} M$
$A6:\ M| \equiv P| \Rightarrow P \overset{SEK_{UP}}{\leftrightarrow} M$
$A7:\ P| \equiv M| \Rightarrow ID_{UAV}$
$A8:\ M| \equiv P| \Rightarrow ID_{PMD}$

According to these assumptions and goals of BAN logic, the main proof of the player and manufacturer authentication and communication phase is as follows.

a. The manufacturer M authenticates the player P.

By *M1* and the *seeing rule*, *Statement 1* can be derived.
$M \triangleleft (< ID_{PMD}, R_{PMD}, T_{PMD} >_{PK_{UAV}}, < H(SEK_{UP}, T_{UAV}) >_{CHK_{UP}})$. (*Statement 1*)
By *A2* and the *freshness rule*, *Statement 2* can be derived.
$M| \equiv \#(< ID_{PMD}, R_{PMD}, T_{PMD} >_{PK_{UAV}}, < H(SEK_{UP}, T_{UAV}) >_{CHK_{UP}})$. (*Statement 2*)
By (*Statement 1*), *A4*, and the *message meaning rule*, *Statement 3* can be derived.
$M| \equiv P| \sim (< ID_{PMD}, R_{PMD}, T_{PMD} >_{PK_{UAV}}, < H(SEK_{UP}, T_{UAV}) >_{CHK_{UP}})$. (*Statement 3*)
By (*Statement 2*), (*Statement 3*), and the *nonce verification rule*, *Statement 4* can be derived.
$M| \equiv \#(< ID_{PMD}, R_{PMD}, T_{PMD} >_{PK_{UAV}}, < H(SEK_{UP}, T_{UAV}) >_{CHK_{UP}})$. (*Statement 4*)
By (*Statement 4*) and the *belief rule*, *Statement 5* can be derived.
$M| \equiv P| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$. (*Statement 5*)
By (*Statement 5*), *A6*, and the *jurisdiction rule*, *Statement 6* can be derived.
$M| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$. (*Statement 6*)
By (*Statement 6*) and the *belief rule*, *Statement 7* can be derived.
$M| \equiv P| \equiv ID_{PMD}$. (*Statement 7*)
By (*Statement 7*), *A8*, and the *jurisdiction rule*, *Statement 8* can be derived.
$M| \equiv ID_{PMD}$. (*Statement 8*)

b. The player P authenticates the manufacturer M.

By *M2* and the *seeing rule*, *Statement 9* can be derived.
$P \triangleleft (< ID_{UAV}, R_{UAV}, T_{UAV} >_{PK_{PMD}}, < H(SEK_{UP}, T_{PMD}) >_{CHK_{PU}})$. (*Statement 9*)
By *A1* and the *freshness rule*, *Statement 10* can be derived.
$P| \equiv \#(< ID_{UAV}, R_{UAV}, T_{UAV} >_{PK_{PMD}}, < H(SEK_{UP}, T_{PMD}) >_{CHK_{PU}})$. (*Statement 10*)
By (*Statement 9*), *A3*, and the *message meaning rule*, *Statement 11* can be derived.
$P| \equiv M| \sim (< ID_{UAV}, R_{UAV}, T_{UAV} >_{PK_{PMD}}, < H(SEK_{UP}, T_{PMD}) >_{CHK_{PU}})$. (*Statement 11*)

By (*Statement 10*), (*Statement 11*), and the *nonce verification rule*, *Statement 12* can be derived.

$P| \equiv M| \equiv (< ID_{UAV}, R_{UAV}, T_{UAV} >_{PK_{PMD}}, <$
$H(SEK_{UP}, T_{PMD}) >_{CHK_{PU}})$. (*Statement 12*)

By (*Statement 12*) and the *belief rule*, *Statement 13* can be derived.

$P| \equiv M| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$. (*Statement 13*)

By (*Statement 13*), *A5*, and the *jurisdiction rule*, *Statement 14* can be derived.

$P| \equiv P \overset{SEK_{UP}}{\leftrightarrow} M$. (*Statement 14*)

By (*Statement 14*) and the *belief rule*, *Statement 15* can be derived.

$P| \equiv M| \equiv ID_{UAV}$. (*Statement 15*)

By (*Statement 15*), A7, and the *jurisdiction rule*, *Statement 16* can be derived.

$P| \equiv ID_{UAV}$. (*Statement 16*)

By (*Statement 6*), (*Statement 8*), (*Statement 14*), and (*Statement 16*), it can be proved that the player P and the manufacturer M authenticate each other in the proposed scheme. Moreover, it can also be proved that the proposed scheme can establish a session key between the player P and the manufacturer M.

In the proposed scheme, the manufacturer authenticates the player by

$$CHK_{UP} \overset{?}{=} H_3(SEK_{UP}, T_{UAV}).$$

If it passes the verification, the manufacturer authenticates the legality of the player. The player authenticates the manufacturer by

$$CHK_{PU} \overset{?}{=} H_3(SEK_{UP}, T_{PMD}).$$

If it passes the verification, the player authenticates the legality of the manufacturer. The player and manufacturer authentication and communication phase of the proposed scheme thus guarantees mutual authentication between the player and the manufacturer.

In the player and ground control station authentication and communication phase, the main goal of the scheme is to make sure whether the legality is authenticated by the player P and the ground control station G.

$G9$: $P| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$
$G10$: $P| \equiv G| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$
$G11$: $G| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$
$G12$: $G| \equiv P| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$
$G13$: $P| \equiv ID_{GCS}$
$G14$: $P| \equiv G| \equiv ID_{GCS}$
$G15$: $G| \equiv ID_{PMD}$
$G16$: $G| \equiv P| \equiv ID_{PMD}$

According to the player and ground control station authentication and communication phase, BAN logic is used to produce an idealized form as follows.

$M3$: $(< ID_{PMD}, R_{PMD}, T_{PMD2} >_{PK_{GCS}}, < H(SEK_{GP}, T_{GCS}) >_{CHK_{GP}})$
$M4$: $(< ID_{GCS}, R_{GCS}, T_{GCS} >_{PK_{PMD}}, < H(SEK_{GP}, T_{PMD2}) >_{CHK_{PG}})$

To analyze the proposed scheme, the following assumptions are made.

$A9$: $P| \equiv \#(T_{PMD2})$
$A10$: $G| \equiv \#(T_{PMD2})$
$A11$: $P| \equiv \#(T_{GCS})$

$A12: G| \equiv \#(T_{GCS})$

$A13: P| \equiv G| \Rightarrow P \overset{SEK_{GP}}{\leftrightarrow} G$

$A14: G| \equiv P| \Rightarrow P \overset{SEK_{GP}}{\leftrightarrow} G$

$A15: P| \equiv G| \Rightarrow ID_{GCS}$

$A16: G| \equiv P| \Rightarrow ID_{PMD}$

According to these assumptions and goals of BAN logic, the main proof of the player and ground control station authentication and communication phase is as follows.

c. The ground control station G authenticates the player P.

By *M3* and the *seeing rule*, *Statement 17* can be derived.
$G \lhd (< ID_{PMD}, R_{PMD}, T_{PMD2} >_{PK_{GCS}}, < H(SEK_{GP}, T_{GCS}) >_{CHK_{GP}})$. (*Statement 17*)

By *A10* and the *freshness rule*, *Statement 18* can be derived.
$G| \equiv \#(< ID_{PMD}, R_{PMD}, T_{PMD2} >_{PK_{GCS}}, < H(SEK_{GP}, T_{GCS}) >_{CHK_{GP}})$. (*Statement 18*)

By (*Statement 17*), *A12*, and the *message meaning rule*, *Statement 19* can be derived.
$G| \equiv P| \sim (< ID_{PMD}, R_{PMD}, T_{PMD2} >_{PK_{GCS}}, < H(SEK_{GP}, T_{GCS}) >_{CHK_{GP}})$. (*Statement 19*)

By (*Statement 18*), (*Statement 19*), and the *nonce verification rule*, *Statement 20* can be derived.
$G| \equiv P| \equiv (< ID_{PMD}, R_{PMD}, T_{PMD2} >_{PK_{GCS}}, < H(SEK_{GP}, T_{GCS}) >_{CHK_{GP}})$. (*Statement 20*)

By (*Statement 20*) and the *belief rule*, *Statement 21* can be derived.
$G| \equiv P| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$. (*Statement 21*)

By (*Statement 21*), *A14*, and the *jurisdiction rule*, *Statement 22* can be derived.
$G| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$. (*Statement 22*)

By (*Statement 22*) and the *belief rule*, *Statement 23* can be derived.
$G| \equiv P| \equiv ID_{PMD}$. (*Statement 23*)

By (*Statement 23*), *A16*, and the *jurisdiction rule*, *Statement 24* can be derived.
$G| \equiv ID_{PMD}$. (*Statement 24*)

d. The player P authenticates the ground control station G.

By *M4* and the *seeing rule*, *Statement 25* can be derived.
$P \lhd (< ID_{GCS}, R_{GCS}, T_{GCS} >_{PK_{PMD}}, < H(SEK_{GP}, T_{PMD2}) >_{CHK_{PG}})$. (*Statement 25*)

By *A9* and the *freshness rule*, *Statement 26* can be derived.
$P| \equiv \#(< ID_{GCS}, R_{GCS}, T_{GCS} >_{PK_{PMD}}, < H(SEK_{GP}, T_{PMD2}) >_{CHK_{PG}})$. (*Statement 26*)

By (*Statement 25*), *A11*, and the *message meaning rule*, *Statement 27* can be derived.
$P| \equiv G| \sim (< ID_{GCS}, R_{GCS}, T_{GCS} >_{PK_{PMD}}, < H(SEK_{GP}, T_{PMD2}) >_{CHK_{PG}})$. (*Statement 27*)

By (*Statement 26*), (*Statement 27*), and the *nonce verification rule*, *Statement 28* can be derived.
$P| \equiv G| \equiv (< ID_{GCS}, R_{GCS}, T_{GCS} >_{PK_{PMD}}, < H(SEK_{GP}, T_{PMD2}) >_{CHK_{PG}})$. (*Statement 28*)

By (*Statement 28*) and the *belief rule*, *Statement 29* can be derived.
$P| \equiv G| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$. (*Statement 29*)

By (*Statement 29*), *A13*, and the *jurisdiction rule*, *Statement 30* can be derived.
$P| \equiv P \overset{SEK_{GP}}{\leftrightarrow} G$. (*Statement 30*)

By (*Statement 30*) and the *belief rule*, *Statement 31* can be derived.
$P| \equiv G| \equiv ID_{GCS}$. (*Statement 31*)

By (*Statement 31*), *A15*, and the *jurisdiction rule*, *Statement 32* can be derived.
$P| \equiv ID_{GCS}$. (*Statement 32*)

By (*Statement 22*), (*Statement 24*), (*Statement 30*), and (*Statement 32*), it can be proved that the player P and the ground control station G authenticate each other in the proposed scheme. Moreover, it can

also be proved that the proposed scheme can establish a session key between the player P and the ground control station G.

In the proposed scheme, the ground control station authenticates the player by

$$CHK_{GP} \stackrel{?}{=} H_3(SEK_{GP}, T_{GCS}).$$

If it passes the verification, the manufacturer authenticates the legality of the player. The player authenticates the ground control station by

$$CHK_{PG} \stackrel{?}{=} H_3(SEK_{GP}, T_{PMD2}).$$

If it passes the verification, the player authenticates the legality of the ground control station. The player and ground control station authentication and communication phase of the proposed scheme thus guarantees mutual authentication between the player and the ground control station.

In the player, UAV, and ground control station authentication and communication phase, the main goal of the scheme is to make sure whether the legality is authenticated by the UAV U and the ground control station G.

$G17: U| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$
$G18: U| \equiv G| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$
$G19: G| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$
$G20: G| \equiv U| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$
$G21: U| \equiv ID_{GCS}$
$G22: U| \equiv G| \equiv ID_{GCS}$
$G23: G| \equiv ID_{UAV}$
$G24: G| \equiv U| \equiv ID_{UAV}$

According to the player, UAV, and ground control station authentication and communication phase, BAN logic is used to produce an idealized form as follows:

$M5: \ (< ID_{UAV}, R_{UAV}, T_{UAV2} >_{PK_{GCS}}, < H(SEK_{GU}, T_{GCS2}) >_{CHK_{GU}})$
$M6: \ (< ID_{GCS}, R_{GCS}, T_{GCS2} >_{PK_{UAV}}, < H(SEK_{GU}, T_{UAV2}) >_{CHK_{UG}})$

To analyze the proposed scheme, the following assumptions are made.

$A17: U| \equiv \#(T_{UAV2})$
$A18: G| \equiv \#(T_{UAV2})$
$A19: U| \equiv \#(T_{GCS2})$
$A20: G| \equiv \#(T_{GCS2})$
$A21: \ U| \equiv G| \Rightarrow U \overset{SEK_{GU}}{\leftrightarrow} G$
$A22: \ G| \equiv U| \Rightarrow U \overset{SEK_{GU}}{\leftrightarrow} G$
$A23: \ U| \equiv G| \Rightarrow ID_{GCS}$
$A24: \ G| \equiv U| \Rightarrow ID_{UAV}$

According to these assumptions and goals of BAN logic, the main proof of the player, UAV, and ground control station authentication and communication phase is as follows.

e The ground control station G authenticates the UAV U.

By *M5* and the *seeing rule*, *Statement 33* can be derived.
$G \triangleleft (< ID_{UAV}, R_{UAV}, T_{UAV2} >_{PK_{GCS}}, <$
$H(SEK_{GU}, T_{GCS2}) >_{CHK_{GU}})$. (*Statement 33*)
By *A18* and the *freshness rule*, *Statement 34* can be derived.
$G| \equiv \#(< ID_{UAV}, R_{UAV}, T_{UAV2} >_{PK_{GCS}}, <$
$H(SEK_{GU}, T_{GCS2}) >_{CHK_{GU}})$. (*Statement 34*)
By (*Statement 33*), *A20*, and the *message meaning rule*, *Statement 35* can be derived.
$G| \equiv U| \sim (< ID_{UAV}, R_{UAV}, T_{UAV2} >_{PK_{GCS}}, <$
$H(SEK_{GU}, T_{GCS2}) >_{CHK_{GU}})$. (*Statement 35*)
By (*Statement 34*), (*Statement 35*), and the *nonce verification rule*, *Statement 36* can be derived.
$G| \equiv U| \equiv (< ID_{UAV}, R_{UAV}, T_{UAV2} >_{PK_{GCS}}, <$
$H(SEK_{GU}, T_{GCS2}) >_{CHK_{GU}})$. (*Statement 36*)
By (*Statement 36*) and the *belief rule*, *Statement 37* can be derived.
$G| \equiv U| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$. (*Statement 37*)
By (*Statement 37*), *A22*, and the *jurisdiction rule*, *Statement 38* can be derived.
$G| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$. (*Statement 38*)
By (*Statement 38*) and the *belief rule*, *Statement 39* can be derived.
$G| \equiv U| \equiv ID_{UAV}$. (*Statement 39*)
By (*Statement 39*), *A24*, and the *jurisdiction rule*, *Statement 40* can be derived.
$G| \equiv ID_{UAV}$. (*Statement 40*)

f The UAV U authenticates the ground control station G.

By *M6* and the *seeing rule*, *Statement 41* can be derived.
$U \triangleleft (< ID_{GCS}, R_{GCS}, T_{GCS2} >_{PK_{UAV}}, <$
$H(SEK_{GU}, T_{UAV2}) >_{CHK_{UG}})$. (*Statement 41*)
By *A17* and the *freshness rule*, *Statement 42* can be derived.
$U| \equiv \#(< ID_{GCS}, R_{GCS}, T_{GCS2} >_{PK_{UAV}}, <$
$H(SEK_{GU}, T_{UAV2}) >_{CHK_{UG}})$. (*Statement 42*)
By (*Statement 41*), *A19*, and the *message meaning rule*, *Statement 43* can be derived.
$U| \equiv G| \sim (< ID_{GCS}, R_{GCS}, T_{GCS2} >_{PK_{UAV}}, <$
$H(SEK_{GU}, T_{UAV2}) >_{CHK_{UG}})$. (*Statement 43*)
By (*Statement 42*), (*Statement 43*), and the *nonce verification rule*, *Statement 44* can be derived.
$U| \equiv G| \equiv (< ID_{GCS}, R_{GCS}, T_{GCS2} >_{PK_{UAV}}, <$
$H(SEK_{GU}, T_{UAV2}) >_{CHK_{UG}})$. (*Statement 44*)
By (*Statement 44*) and the *belief rule*, *Statement 45* can be derived.
$U| \equiv G| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$. (*Statement 45*)
By (*Statement 45*), *A21*, and the *jurisdiction rule*, *Statement 46* can be derived.
$U| \equiv U \overset{SEK_{GU}}{\leftrightarrow} G$. (*Statement 46*)
By (*Statement 46*) and the *belief rule*, *Statement 47* can be derived.
$U| \equiv G| \equiv ID_{GCS}$. (*Statement 47*)
By (*Statement 47*), *A23*, and the *jurisdiction rule*, *Statement 48* can be derived.
$U| \equiv ID_{GCS}$. (*Statement 48*)

By (*Statement 38*), (*Statement 40*), (*Statement 46*), and (*Statement 48*), it can be proved that the UAV U and the ground control station G authenticate each other in the proposed scheme. Moreover, it can also be proved that the proposed scheme can establish a session key between the UAV U and the ground control station G.

In the proposed scheme, the ground control station authenticates the UAV by

$$CHK_{GU} \stackrel{?}{=} H_3(SEK_{GU}, T_{GCS2}).$$

If it passes the verification, the ground control station authenticates the legality of the UAV. The UAV authenticates the ground control station by

$$CHK_{UG} \stackrel{?}{=} H_3(SEK_{GU}, T_{UAV2}).$$

If it passes the verification, the UAV authenticates the legality of the ground control station. The player, UAV, and ground control station authentication and communication phase of the proposed scheme thus guarantees mutual authentication between the UAV and the ground control station.

Scenario: A malicious attacker uses an illegal mobile reader to control an UAV.
Analysis: The attacker will not succeed because the illegal mobile reader has not been registered to the trusted authority center and thus cannot calculate the correct session key SEK_{UP}. Thus, the attack will fail when the legal UAV attempts to authenticate the illegal mobile device. In the proposed scheme, the attacker cannot achieve their purpose using an illegal mobile device. In the same scenario, the proposed scheme can also defend against a malicious attack using an illegal ground control station to send a fake message to a legal UAV, because the illegal ground control station has not been registered to the trusted authority center and thus cannot calculate the correct session key SEK_{GU}. Thus, the attack will fail when the legal UAV attempts to authenticate the illegal ground control station.

4.2. Integrity and Confidentiality

To ensure the integrity and confidentiality of the transaction data, this study uses elliptic curve cryptography and Diffie–Hellman key exchange algorithm to calculate the session key SEK_{UP}, SEK_{GP} and SEK_{GU}, and also to protect the integrity and confidentiality. The malicious attacker cannot use the signatures (K_{UP1}, K_{UP2}), (K_{PU1}, K_{PU2}), (K_{GP1}, K_{GP2}), (K_{PG1}, K_{PG2}), (K_{GU1}, K_{GU2}), and (K_{UG1}, K_{UG2}) to calculate the correct session key SEK_{UP}, SEK_{GP}, and SEK_{GU}.

Only a legal mobile device or UAV can calculate the correct session key SEK_{UP}. The legal UAV calculates the session key

$$SEK_{UP} = H_2(K_{UP1}, K_{UP2})$$

and the legal mobile device calculates the session key

$$\begin{aligned} SEK_{UP} &= H_2(K_{PU1}, K_{PU2}). \\ K_{PU1} &= S_{PMD}T_{UAV} + aPK_{UAV} \\ &= S_{PMD}bP + aS_{UAV}P \\ &= bS_{PMD}P + S_{UAV}aP \\ &= bPK_{PMD} + S_{UAV}T_{PMD} = K_{UP1} \\ K_{PU2} = aT_{UAV} &= abP = baP = bT_{PMD} = K_{UP2} \end{aligned}$$

Only a legal mobile device or ground control station can calculate the correct session key SEK_{GP}. The legal ground control station calculates the session key

$$SEK_{GP} = H_2(K_{GP1}, K_{GP2})$$

and the legal mobile device calculates the session key

$$\begin{aligned} SEK_{UP} &= H_2(K_{PU1}, K_{PU2}). \\ K_{PG1} &= S_{PMD}T_{GCS} + cPK_{GCS} \\ &= S_{PMD}dP + cS_{GCS}P \\ &= dS_{PMD}P + S_{GCS}cP \\ &= dPK_{PMD} + S_{GCS}T_{PMD2} = K_{GP1} \\ K_{PG2} = cT_{GCS} &= cdP = dcP = dT_{PMD2} = K_{GP2} \end{aligned}$$

Only a legal UAV or ground control station can compute the correct session key SEK_{GU}. The legal ground control station computes the session key

$$SEK_{GU} = H_2(K_{GU1}, K_{GU2})$$

and the legal UAV calculates the session key

$$\begin{aligned} SEK_{GU} &= H_2(K_{UG1}, K_{UG2}). \\ K_{UG1} &= S_{UAV}T_{GCS2} + ePK_{GCS} \\ &= S_{UAV}fP + eS_{GCS}P \\ &= fS_{UAV}P + S_{GCS}eP \\ &= fPK_{UAV} + S_{GCS}T_{UAV2} = K_{GU1} \\ K_{UG2} = eT_{GCS2} = efP = feP = fT_{UAV2} &= K_{GU2} \end{aligned}$$

Only the correct session key will allow successful communication. Thus, attackers cannot decrypt or modify the transmitted message. Therefore, the proposed scheme achieves the integrity and confidentiality.

Scenario: A malicious attacker intercepts the transmitted message from the ground control station to the player and decrypts the message or sends a modified message to the player.
Analysis: The attacker will not succeed because the legal player will use

$$CHK_{PG} \stackrel{?}{=} H_3(SEK_{GP} \| T_{PMD2})$$

to check the integrity. The attacker cannot calculate the correct session key SEK_{GP}. Thus, the attack will fail when the legal player authenticates the received message. In the proposed scheme, the attacker cannot achieve his/her purpose by sending a modified message to the player, and he/she also cannot decrypt the intercepted message. For the same reason, the attack will fail when the legal ground control station uses

$$CHK_{GP} \stackrel{?}{=} H_3(SEK_{GP} \| T_{GCS})$$

to check the integrity. Therefore, attackers cannot achieve their purpose by sending a modified message to the ground control station or decrypt the intercepted message.

4.3. Identity Anonymity and Privacy

Another form of privacy attack involves attempting to obtain a player's real name or physical location by tracing his/her mobile device. If the mobile device sends the same message continuously, an attacker can trace its location. In the proposed scheme, the session key SEK_{UP} and SEK_{GP} is changed for every communication round in order to avoid location tracing. Besides, the pseudonym identity is used instead of real name in the proposed scheme. Thus, location privacy is protected and identity anonymity is achieved.

4.4. Availability and Prevention of DoS Attack

An attacker may impersonate a legal sender and then send the same message again to the intended receiver, trying to make the system unable to provide services properly. However, this attack will fail in the proposed scheme, as all messages between the sender and the receiver are protected with the session key SEK_{UP}, SEK_{GP}, and SEK_{GU}, and the attacker cannot calculate the correct session key. Because the transmitted messages are changed every round, the same message cannot be sent twice. Thus, the DoS attack is prevented and system availability is achieved.

4.5. Prevention of Spoofing Attack

In the proposed scheme, the GPS message is obtained by the UAV then transmitted to the ground control station or the player. The GPS message M_{GPS} is protected by the session key SEK_{UP} and SEK_{GU}. The attacker cannot compute the correct session key SEK_{UP} or SEK_{GU} and he/she cannot impersonate a legal UAV and send a fake message. Therefore, the spoofing attack is prevented.

Scenario: A malicious attacker pretends a legal UAV and sends a fake message to the legal ground control station.
Analysis: The attacker will not succeed because the illegal UAV has not been registered to the trusted authority center and thus cannot calculate the correct session key SEK_{GU}. Thus, the attack will fail when the legal ground control station attempts to authenticate the illegal UAV. In the proposed scheme, the attacker cannot achieve the purpose of pretending to be a legal UAV and sending a fake message. In the same scenario, the proposed scheme can also defend against a malicious attacker pretending to be a legal UAV and sending a fake message to the legal player, because the illegal UAV has not been registered to the trusted authority center and thus cannot calculate the correct session key SEK_{UP}. Thus, the attack will fail when the legal player attempts to authenticate the illegal UAV.

4.6. Non-Repudiation

In the proposed scheme, the digital signature is used to achieve non-repudiation between the parties in each phase. The sender uses his/her private key to sign the transmitted message, and the receiver uses the public key of the sender to verify the received message. Thus, the non-repudiation is achieved. Table 1 shows the non-repudiation of the proposed scheme.

Table 1. Non-repudiation of the proposed scheme.

Item / Phase	Proof	Issuer	Holder	Verification
Player and manufacturer authentication and communication phase	(C_{UAV}, Sig_{UAV})	M	P	$Sig_{UAV} = S_{SK_{UAV}}(M_{payment}, Cert_{UAV})$ $(M_{payment}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV})$
Player and ground control station authentication and communication phase	(C_{GCS}, Sig_{GCS})	G	P	$Sig_{GCS} = S_{SK_{GCS}}(ID_{PMD}, M_{payment}, Cert_{UAV})$ $(ID_{PMD}, M_{payment}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS})$
Player, UAV, and ground control station authentication and communication phase	(C_{PMD3}, Sig_{PMD3})	P	U	$Sig_{PMD3} = S_{SK_{PMD}}(M_{request}, Cert_{UAV})$ $(M_{request}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{PMD}}(Sig_{PMD3})$
	(C_{GCS2}, Sig_{GCS2})	G	U	$Sig_{GCS2} = S_{SK_{GCS}}(ID_{PMD}, M_{confirm}, Cert_{UAV})$ $(ID_{PMD}, M_{confirm}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS2})$
	(C_{UAV3}, Sig_{UAV3})	U	P	$Sig_{UAV3} = S_{SK_{UAV}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV})$ $(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV3})$
Ground control station and UAV authentication and communication phase	(C_{GCS3}, Sig_{GCS3})	G	U	$Sig_{GCS3} = S_{SK_{GCS}}(ID_{UAV}, M_{request})$ $(ID_{UAV}, M_{request}) \stackrel{?}{=} V_{PK_{GCS}}(Sig_{GCS3})$
	(C_{UAV4}, Sig_{UAV4})	U	G	$Sig_{UAV4} = S_{SK_{UAV}}(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV})$ $(ID_{PMD}, M_{confirm}, M_{GPS}, Cert_{UAV}) \stackrel{?}{=} V_{PK_{UAV}}(Sig_{UAV4})$

4.7. Comparison of Security Issues

Table 2 shows a comparison of security issues of related works.

Table 2. Comparison of security issues.

	Yoon et al. [18]	**Chen et al. [19]**	**Wazid et al. [20]**	**Tian et al. [21]**	**The Proposed Scheme**
Mutual authentication	Unidirectional authentication	Yes	Yes	Unidirectional authentication	Yes
Integrity	N/A	Yes	No	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Identity anonymity	N/A	N/A	Yes	Yes	Yes
Availability	No	N/A	N/A	N/A	Yes
Privacy	N/A	N/A	Yes	Yes	Yes
Non-repudiation	No	Yes	No	Yes	Yes
DoS attack	Yes	N/A	Yes	N/A	Yes
Spoofing attack	N/A	N/A	Yes	N/A	Yes

4.8. Computation Cost

Table 3 shows the computation cost of the proposed scheme and Wazid et al.'s scheme [20].

T_P: Polynomial function operation
T_{Mul}: Multiplication operation
T_H: Hash function operation
T_{Cmp}: Comparison operation
T_{Enc}: Symmetric encryption operation
T_{Sig}: Signature operation
T_{Xor}: Exclusive-or operation

Table 3. Computation cost of the proposed scheme and Wazid et al.'s scheme [21].

		Wazid et al. [20]	**The Proposed Scheme**
Manufacturer (UAV) registration phase	Manufacturer (UAV)	N/A	$2T_{Mul} + 1T_H + 1T_{Cmp}$
	Trusted authority center	$1T_P + 2T_H$	$2T_{Mul} + 1T_H$
Player (mobile device) registration phase	Player (mobile device)	$1T_P + 8T_H + 6T_{Xor}$	$2T_{Mul} + 1T_H + 1T_{Cmp}$
	Trusted authority center	$4T_H$	$2T_{Mul} + 1T_H$
Ground control station registration phase	Ground control station	N/A	$2T_{Mul} + 1T_H + 1T_{Cmp}$
	Trusted authority center	N/A	$2T_{Mul} + 1T_H$
Player and manufacturer authentication and communication phase	Player (mobile device)	N/A	$5T_{Mul} + 4T_H + 2T_{Cmp} + 2T_{Enc} + 1T_{Sig}$
	Manufacturer (UAV)	N/A	$5T_{Mul} + 4T_H + 1T_{Cmp} + 2T_{Enc} + 1T_{Sig}$
Player and ground control station authentication and communication phase	Player (mobile device)	N/A	$5T_{Mul} + 4T_H + 2T_{Cmp} + 2T_{Enc} + 1T_{Sig}$
	Ground control station	N/A	$5T_{Mul} + 4T_H + 1T_{Cmp} + 2T_{Enc} + 1T_{Sig}$
Player, UAV, and ground control station authentication and communication phase	Player (mobile device)	$1T_P + 16T_H + 3T_{Cmp} + 11T_{Xor}$	$1T_{Cmp} + 2T_{Enc} + 2T_{Sig}$
	Manufacturer (UAV)	$7T_H + 2T_{Cmp} + 4T_{Xor}$	$5T_{Mul} + 4T_H + 3T_{Cmp} + 4T_{Enc} + 3T_{Sig}$
	Ground control station	N/A	$5T_{Mul} + 4T_H + 1T_{Cmp} + 2T_{Enc} + 1T_{Sig}$
	Trusted authority center	$8T_H + 2T_{Cmp} + 5T_{Xor}$	N/A
Ground control station and UAV authentication and communication phase	Ground control station	N/A	$1T_{Cmp} + 2T_{Enc} + 2T_{Sig}$
	Manufacturer (UAV)	N/A	$1T_{Cmp} + 2T_{Enc} + 2T_{Sig}$

In Table 3, computation costs of the proposed scheme and Wazid et al.'s for the trusted authority center, manufacturer (UAV), player (mobile device), and ground control station in each phase are analyzed. For the highest computation cost in the player, UAV, and ground control station authentication and communication phase, a UAV needs five multiplication operations, four hash function operations, three comparison operations, four symmetric encryption operations, and three signature operations. A player needs one comparison operation, two symmetric encryption operations, and two signature operations. A ground control station needs five multiplication operations, four hash function operations, one comparison operation, two symmetric encryption operations, and one signature operation. The computation cost is acceptable in the proposed scheme.

4.9. Communication Cost

The communication cost of the proposed scheme and Wazid et al.'s scheme [20] is shown in Table 4.

Table 4. Communication cost of the proposed scheme and Wazid et al.'s scheme [21].

		Wazid et al. [20]	**The Proposed Scheme**
Manufacturer (UAV) registration phase	Message length	560 bits	2528 bits
	Round	1	2
	3.5G (14 Mbps)	0.040 ms	0.181 ms
	4G (100 Mbps)	0.006 ms	0.025 ms
Player (mobile device) registration phase	Message length	880 bits	2528 bits
	Round	2	2
	3.5G (14 Mbps)	0.063 ms	0.181 ms
	4G (100 Mbps)	0.009 ms	0.025 ms
Ground control station registration phase	Message length	N/A	2528 bits
	Round	N/A	2
	3.5G (14 Mbps)	N/A	0.181 ms
	4G (100 Mbps)	N/A	0.025 ms
Player and manufacturer authentication and communication phase	Message length	N/A	2816 bits
	Round	N/A	4
	3.5G (14 Mbps)	N/A	0.201 ms
	4G (100 Mbps)	N/A	0.028 ms
Player and ground control station authentication and communication phase	Message length	N/A	2816 bits
	Round	N/A	4
	3.5G (14 Mbps)	N/A	0.201 ms
	4G (100 Mbps)	N/A	0.028 ms
Player, UAV, and ground control station authentication and communication phase	Message length	1840 bits	5536 bits
	Round	3	6
	3.5G (14 Mbps)	0.131 ms	0.395 ms
	4G (100 Mbps)	0.018 ms	0.055 ms
Ground control station and UAV authentication and communication phase	Message length	N/A	2720 bits
	Round	N/A	2
	3.5G (14 Mbps)	N/A	0.194 ms
	4G (100 Mbps)	N/A	0.027 ms

The communication efficiency of the proposed scheme and Wazid et al.'s scheme during the transaction process of each phase was also analyzed. It was assumed that an elliptic curve modular operation required 160 bits, a hash operation required 160 bits, an AES operation required 256 bits, a signature operation required 1024 bits, and other messages, such as id, pid, and random number, required 80 bits. For example, the player, UAV and ground control station authentication and communication phase of the proposed scheme requires four elliptic curve modular messages, two hash messages, four AES messages, three signature operation messages, and six other messages. It thus requires $160 \times 4 + 160 \times 2 + 256 \times 4 + 1024 \times 3 + 80 \times 6 = 5536$ bits. In a 3.5G environment, the maximum transmission speed is 14 Mbps. This study also considered the player, UAV, and ground control station authentication and communication phase of the proposed scheme, which only takes 0.395 ms to transfer all messages. In a 4G environment, the maximum transmission speed is 100 Mbps and the transmission time is reduced to 0.055 ms.

Basically, Wazid et al.'s scheme provides a lightweight user authentication scheme in which a user in the IoD environment needs to access data. This appeals as it aims at providing a fast authorization mechanism. However, the integrity, non-reputation, and availability issues are excluded. However, compared to Wazid et al.'s scheme, the proposed scheme used the public key cryptography to design a UAV application field which was applied in a sensitive field such that the integrity, non-reputation and availability issues needed to be considered and should be ensured [20]. The proposed scheme is a different application field to Wazid et al.'s scheme. The players must pass necessary procedures to obtain the flight authority in a sensitive area. It needs more scenarios and overloads. As shown in Table 4, the communication cost sounds good. The proposed scheme provides a novel solution in the UAV application field.

Compared to the Wazid et al.'s scheme, the proposed scheme achieves the following advantages: firstly, the proposed scheme uses a signature mechanism, thus it can ensure data integrity and achieve non-repudiation and secondly, the proposed architecture involves the role of the ground control station to effectively grasp the UAVs' flying status in a sensitive area. The ground control station can also confirm whether the flying UAV is authorized. Although the proposed architecture has higher computing and communication costs than the Wazid et al.'s scheme, it also achieves higher security and availability.

5. Conclusions

At present, UAVs are mainly used for small package delivery and leisure entertainment. In the future, they will have thousands of uses that could even be widely extended to agricultural, land protection surveillance, emergency relief, military reconnaissance, space exploration, and other applications. UAVs will also create new jobs, while also addressing population ageing and manpower shortages. Advanced technology can bring a better and convenient living environment for mankind, but UAVs can also be maliciously used, and even endanger national security.

In this paper, a traceable and privacy protection protocol was designed to conduct the UAVs' application in sensitive control area. The proposed scheme creates a feasible and secure management platform in a sensitive area surveillance for UAVs' application. For sensitive military areas, players must obtain flight approval from a ground control station before they can control the UAV in these sensitive areas. The proposed scheme achieves mutual authentication, integrity and confidentiality, anonymity and privacy, non-repudiation, availability and protection against DoS attack, while also preventing spoofing attack. This study also analyzed the computation cost and the communication cost in the proposed scheme to prove the proposed scheme is practical in the real world.

Author Contributions: Conceptualization, Y.-Y.D. and C.-L.C.; methodology, Y.-Y.D. and C.-L.C.; validation, W.W., C.-H.C., Y.-J.C., and C.-M.W.; investigation, W.W. and C.-H.C.; data analysis, C.-H.C., Y.-J.C., and C.-M.W.; writing—original draft preparation, Y.-Y.D.; writing—review and editing, C.-L.C.; supervision, C.-L.C. and C.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 61906043, Grant 61877010, Grant 11501114, and Grant 11901100, in part by the Fujian Natural Science Funds under Grant 2019J01243, and in part by Fuzhou University under Grant 510730/XRC-18075, Grant 510809/GXRC-19037, Grant 510649/XRC-18049, and Grant 510650/XRC-18050.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Maza, I.I.; Caballero, F.F.; Capitán, J.; Martínez-de-Dios, J.R.; Ollero, A. Experimental results in multi-UAV coordination for disaster management and civil security applications. *J. Intell. Robot. Syst.* **2011**, *61*, 563–585. [CrossRef]
2. Meng, X.; Wang, W.; Leong, B. SkyStitch: A cooperative Multi-UAV-based real-time video surveillance system with stitching. In Proceedings of the 23rd Annual ACM Conference on Multimedia Conference, Brisbane, Australia, 26–30 October 2015; pp. 261–270.
3. Sun, Z.; Wang, P.; Vuran, M.C.; Al-Rodhaan, M.A.; Al-Dhelaan, A.M.; Akyildiz, I.F. BorderSense: Border patrol through advanced wireless sensor networks. *Ad Hoc Netw.* **2011**, *9*, 468–477. [CrossRef]
4. Vollgger, S.A.; Cruden, A.R. Mapping folds and fractures in basement and cover rocks using UAV photogrammetry, cape liptrap and cape Paterson, Victoria, Australia. *J. Struct. Geol.* **2016**, *85*, 168–187. [CrossRef]
5. Cho, J.; Lim, G.; Biobaku, T.; Kim, S.; Parsaei, H. Safety and security management with unmanned aerial vehicle (UAV) in oil and gas industry. *Proc. Manuf.* **2015**, *3*, 1343–1349. [CrossRef]
6. Zaouche, L.; Natalizio, E.; Bouabdallah, A. ETTAF: Efficient target tracking and filming with a flying ad hoc network. In Proceedings of the 1st ACM International Workshop on Experiences with the Design and Implementation of Smart Objects, Paris, France, 7 September 2015; pp. 49–54.
7. Danoy, G.; Brust, M.R.; Bouvry, P. Connectivity stability in autonomous multi-level UAV swarms for wide area monitoring. In Proceedings of the 5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, Cancun, Mexico, 2–6 November 2015; pp. 1–8.
8. Ben-Asher, Y.; Feldman, S.; Gurfil, P.; Feldman, M. Distributed decision and control for cooperative UAVs using ad hoc communication. *IEEE Trans. Control Syst. Technol.* **2008**, *16*, 511–516. [CrossRef]
9. Nader, M.; Jameela, A.J.; Imad, J. Unmanned aerial vehicles applications in future smart cities. *Technol. Forecast. Soc. Chang.* **2018**, in press. [CrossRef]
10. Sedjelmaci, H.; Senouci, S.M.; Messous, M. How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network? In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6. [CrossRef]
11. Chriki, A.; Touati, H.; Snoussi, H.; Kamoun, F. FANET: Communication, mobility models and security issues. *Comput. Netw.* **2019**, *163*, 106877. [CrossRef]
12. Strohmeier, M.; Lenders, V.; Martinovic, I. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1066–1087. [CrossRef]
13. Wesson, K.D.; Humphreys, T.E.; Evans, B.L. Can Cryptography Secure Next Generation Air Traffic Surveillance? Technical Report. Available online: https://radionavlab.ae.utexas.edu/images/stories/files/papers/adsb_for_submission.pdf (accessed on 21 December 2019).
14. Sedjelmaci, H.; Senouci, S.M.; Ansari, N. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A Bayesian game-theoretic methodology. *IEEE Trans. Intell. Transp. Syst.* **2016**, *18*, 1143–1153. [CrossRef]
15. Sedjelmaci, H.; Senouci, S.M.; Ansari, N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. *IEEE Trans. Syst. Man Cybern. Syst.* **2017**, *48*, 1594–1606. [CrossRef]
16. García-Magariño, I.; Lacuesta, R.; Rajarajan, M.; Lloret, J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Netw.* **2019**, *86*, 72–82. [CrossRef]
17. Xiao, L.; Xie, C.; Min, M.; Zhuang, W. User-centric view of unmanned aerial vehicle transmission against smart attacks. *IEEE Trans. Veh. Technol.* **2017**, *67*, 3420–3430. [CrossRef]

18. Yoon, K.; Park, D.; Yim, Y.; Kim, K.; Yang, S.K.; Robinson, M. Security authentication system using encrypted channel on UAV network. In Proceedings of the 2017 First IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan, 10–12 April 2017; pp. 393–398.
19. Chen, L.; Qian, S.; Lim, M.; Wang, S. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems. *China Commun.* **2018**, *15*, 61–76. [CrossRef]
20. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J.P.C. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet Things J.* **2018**, *6*, 3572–3584. [CrossRef]
21. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. *J. Inf. Secur. Appl.* **2019**, *48*, 102354. [CrossRef]
22. Han, W.; Zhu, Z. An ID-based mutual authentication with key agreement protocol for multiserver environment on elliptic curve cryptosystem. *Int. J. Commun. Syst.* **2014**, *27*, 1173–1185. [CrossRef]
23. Sarath, G.; Jinwala, D.C.; Patel, S. A Survey on Elliptic Curve Digital Signature Algorithm and its Variants. *Comput. Sci. Inf. Technol. (CSIT)–CSCP* **2014**, 121–136. [CrossRef]
24. Chen, L.; Morrissey, P.; Smart, N.P. Pairings in Trusted Computing. *LNCS* **2008**, *5209*, 1–17.
25. He, D.; Chan, S.; Guizani, M. Communication security of unmanned aerial vehicles. *IEEE Wirel. Commun.* **2017**, *24*, 134–139. [CrossRef]
26. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).