Design of Secure Handover Authentication Scheme for Urban Air Mobility Environments

DEOKKYU KWON1, SEUNGHWAN SON1, YOHAN PARK2, HYUNGPYO KIM1,3, YOUNGHO PARK1,4, (Member, IEEE), SANGWOO LEE5, AND YONGSUNG JEON5

1School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
2School of Computer Engineering, Keimyung University, Daegu 42601, South Korea
3Department of Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea
4School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea
5Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant by the Korean Government through Ministry of Science and ICT (MSIT) (Study on Wireless Covert Channel Risk Verification) under Grant 2020-0-00913.

ABSTRACT Urban air mobility (UAM) is a future air transportation system to solve the air pollution and movement efficiency problems of the traditional mobility system. In UAM environments, unmanned aerial vehicles (UAVs) are used to transport passengers and goods providing various convenient services such as package delivery, air bus, and air taxi. However, UAVs communicate with ground infrastructures through open channels that can be exposed to various security attacks. Therefore, a secure mutual authentication scheme is necessary for UAM environments. Moreover, a handover authentication is also necessary to ensure seamless communication when the service location is changed. In this paper, we design a secure and efficient handover authentication scheme for UAM environments considering various security vulnerabilities and efficiency using elliptic curve cryptography (ECC). We utilize informal security analysis, Real-or-Random (RoR), Burrows–Abadi–Needham (BAN) logic, and Automated Validation of Internet Security Protocols and Applications (AVISPA) to prove the security of the proposed scheme. Furthermore, we compare the computation and communication cost comparisons of the proposed scheme with the other related schemes. The results show that the proposed scheme is secure and efficient for UAM environments.

INDEX TERMS Urban air mobility, handover, authentication, BAN logic, RoR model, AVISPA.

I. INTRODUCTION
Urban air mobility (UAM) [1], [2] is a future air transportation system that uses a low-altitude airspace as a path of movement. This transportation system can overcome problems of traditional urban traffic systems such as vehicles and railroads. With the rapid increase in vehicles and logistics, the movement efficiency of the urban transportation system has been decreasing due to urban concentration. In addition, there has been a high increase in urban air pollution problems because traditional vehicles use fossil fuels [3]. These existing problems of traditional urban transportation systems can be solved in UAM environments as follows. First, 3D airspace is used as a movement path in UAM environments, increasing the amount of traffic in the same space compared to existing transportation systems. Thus, the movement efficiency can be increased in UAM environments. Second, UAM environments use “electric Vertical Take-Off and Landing (eVTOL)” technology that performs a flight mission only with electric motors [4]. Compared with traditional vehicles that use fossil fuels, eVTOL technology can provide low emission and noise. Therefore, the urban air pollution problem can be solved in UAM environments. Accordingly, UAM environments are expected to change the paradigm of the mobility industry, and research for this future transportation system has been proposed [5], [6].

To use the airspace as a path, an unmanned aerial vehicle (UAV) is used for transportation in UAM environments. A UAV, i.e. drone, is an aircraft that does not have a pilot on board. In a UAV, there are various modules including communication, sensor, actuator, computing power, energy supply and recorder [7]. The UAV uses these modules to collect the surrounding information and communicates with the ground controller to receive navigation and environment
broadcasting services. Recently, UAV technology has improved due to the development of eVTOL and battery technologies. Moreover, autonomous flight for UAVs has been researched due to the development of information and communication technologies (ICT) [8]. Figure 1 indicates the general structure of a UAV.

In UAM environments, it is necessary to control many UAVs and support seamless communications simultaneously. “Internet of Drones (IoD)” [9] is an architecture designed to provide controlled airspace with coordinated access. In the IoD environments, there are two entities: UAVs and zone service providers (ZSPs). To join in the network, both UAVs and ZSPs register to the central ground station server (GSS). ZSPs act as base stations managing specific areas and providing UAVs with information of navigation and surrounding environment. If a UAV enters a ZSP zone, the ZSP provides the UAV with flight information including identity and navigation services. With the information, UAVs can perform flight missions to people such as package delivery, air bus, and air taxi. Figure 2 shows the proposed system model for UAM environments.

Although UAM environments can provide people with convenient services, there are still several issues. In UAM environments, UAVs communicate with ZSPs using wireless channels which can be exposed to various security vulnerabilities. If an adversary hijacks and replays messages to another UAV, it can confuse the entire transportation system. If an adversary obtains the verification table of the server, the adversary can try to communicate with UAVs using this information. Moreover, handover authentication is necessary to overcome each ZSP’s geographical coverage limit and support a seamless communication service for UAVs. If there is no handover authentication in UAM environments, each UAV must perform a new authentication process every time when it enters in the service area of another ZSP. This can cause inefficiency of the entire network and it is necessary to manage the information securely in authentication process. Thus, we design a mutual authentication and handover authentication scheme for UAM environments to ensure security and efficiency.

### A. CONTRIBUTION

Contributions of this paper are as below.

- We design a mutual authentication and handover authentication scheme for UAM environments. To ensure a secure key agreement process, we use elliptic curve cryptography (ECC) in our scheme. The handover authentication phase of our proposed scheme provides lower computation costs than the initial mutual authentication phase. Moreover, the proposed scheme supports a UAV revocation process when a ZSP detects a malicious or misbehaving UAV.
- We analyze the security of the proposed scheme using formal and informal analyses in Section V and Section VI. Then, we propose a handover authentication scheme in Section IV. To prove the security and estimate the performance of the proposed scheme, we utilized digital signatures to verify each other’s certificate. However, Jan et al.’s scheme, various UAV authentication schemes have been proposed for IoD environments. Lin et al. [13] presented security and privacy challenges in IoD such as denial of service (DoS), spoofing, and data injection attacks. They also proposed a solution to provide privacy using identity-based encryption (IBE). Cho et al. [14] suggested an authentication scheme for UAV in IoD environments. Cho et al. utilized digital signatures to verify each other’s certificate. However, Jan et al. [15] found that Cho et al.’s scheme can be vulnerable to privileged insider and verification table leakage attacks, and does not provide dynamic UAV addition and revocation phases. Jan et al. [15] proposed an authentication scheme considering these vulnerabilities using symmetric encryption. The above schemes [13]–[15] can provide convenient services such as weather forecasting and

### B. ORGANIZATION

We introduce the existing authentication schemes for IoD environments and handover schemes in Section II. The system model, adversary model, and basic concept of ECC are described in Section III. Then, we propose a handover authentication scheme in Section IV. To prove the security and estimate the performance of the proposed scheme, we utilized formal and informal analyses in Section V and Section VI. Finally, we conclude and summarize the proposed scheme in Section VII.

### II. RELATED WORKS

The basic concept of IoD was firstly proposed by Gharibi et al. [9]. They presented the conceptual layered network architecture for UAVs. With this network model, UAVs can provide users with various services such as package delivery, traffic surveillance, and rescue. Moreover, Gharibi et al. demonstrated that IoD environments can be exposed to jammed broadcast messages and airspace clogging. From Gharibi et al.’s scheme, various UAV authentication schemes have been proposed for IoD environments. Lin et al. [13] presented security and privacy challenges in IoD such as denial of service (DoS), spoofing, and data injection attacks. They also proposed a solution to provide privacy using identity-based encryption (IBE). Cho et al. [14] suggested an authentication scheme for UAV in IoD environments. Cho et al. utilized digital signatures to verify each other’s certificate. However, Jan et al. [15] found that Cho et al.’s scheme can be vulnerable to privileged insider and verification table leakage attacks, and does not provide dynamic UAV addition and revocation phases. Jan et al. [15] proposed an authentication scheme considering these vulnerabilities using symmetric encryption. The above schemes [13]–[15] can provide convenient services such as weather forecasting and
target tracking, but they are limited in long-distance flights because they did not consider handover processes.

To provide users with secure and seamless communications, handover authentication schemes have been proposed for smart cities and vehicular network environments. Kumar and Om [16] suggested an authentication scheme for 5G-WLAN networks to achieve a handover process between small cell base stations and mobile devices. They used bilinear pairings to provide secure device-to-device communication and privacy to users. However, Kumar et al.’s scheme requires high computation resources due to using bilinear pairings. Wang et al. [17] proposed a V2I authentication scheme in vehicular ad hoc network (VANET). In Wang et al.’s scheme, blockchain was utilized to record the attribute and trustworthiness of each vehicles. Zhou et al. [18] proposed an authentication and key agreement scheme in VANET environments to ensure user privacy and data confidentiality. They claimed that their scheme can provide a secure seamless communication and service in large-scale service-oriented VANET using ECC and XOR operations. However, ZakeriKia et al. [19] discovered that Zhou et al. [18]’s scheme can be vulnerable to impersonation, man-in-the-middle attacks and have an inefficient searching method. Therefore, ZakeriKia et al. proposed an enhanced handover authentication scheme to be suitable for vehicular sensor network environments. However, ZakeriKia et al.’s scheme [19] can be vulnerable to DoS attacks because several messages does not use fresh timestamps in authentication scheme. Considering the above schemes [16]–[19], we design a handover authentication scheme which is secure and efficient for UAM environments.

III. PRELIMINARIES
In this section, we introduce the system model of the proposed protocol and describe the basic concept of ECC and security challenges for UAM environments.

A. SYSTEM MODEL
The system model of the proposed scheme consists of ground station server (GSS), control room (CR), ZSPs, and UAVs, which are represented in Figure 2. Details are as below.

- GSS: The GSS is a main server that manages the identity information of UAVs and ZSPs. Therefore, the GSS can make a revocation list of misbehaving UAVs. The GSS has a high computation power and storage capacity. We define that the GSS is a trusted entity.
- CR: CR has the whole authority of this networks and manages the GSS.
- ZSPs: A ZSP is deployed in a specific zone and provides UAVs with useful services such as surrounding information and navigation services. Furthermore, the ZSP supports a handover service when the UAV moves to a service area of another ZSP. The ZSP is a trusted entity and has enough computation and storage capacities.
- UAVs: A UAV is an aircraft capable of autonomous flight. After authentication with ZSP, the UAV performs various convenient services for people such as package
delivery, air taxi, and air subway. The UAV has restricted computation and storage capacities.

B. ADVERSARY MODEL

In this paper, we follow the well-known adversary model named “Dolev-Yao threat model” [20]. In this model, an adversary can control all messages exchanged via an open channel such as eavesdropping, modifying, intercepting, and deleting messages. In addition, the adversary can obtain ephemeral parameters or the master key of the GSS using the “Canetti-Krawczyk threat model” [21]. Therefore, an adversary can try various security attacks as follows.

- An adversary attempts to obtain and threaten the UAV’s privacy and traceability.
- An adversary tries to impersonate as a legitimate UAV and communicate with the nearby ZSP.
- An adversary can execute various security attacks such as man-in-the-middle, privileged insider, verification table leakage, and replay attacks [22].

C. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is a public key cryptosystem using an elliptic curve [23]. Over a large finite field \( \mathbb{F}_p \), an elliptic curve \( E_p(c, d) \) is defined as \( y^2 = x^3 + cx + d \), where \( p \) and \( q \) are large prime integers and \( 4c^3 + 27d^2 \neq 0 \). Then, we select a subgroup \( G \), a base point \( P \in G \), and an integer \( k \in \mathbb{Z}_q \). The point multiplication \( k \cdot P \) and mathematical security of ECC are represented as below.

\[
k \cdot P = P + P + \ldots + P \text{(times)}
\]

- Elliptic curve discrete logarithm (ECDL) problem: It is difficult to calculate and obtain the integer \( k \) from \( k \cdot P \), where \( k \in \mathbb{Z}_q \).
- Elliptic curve decisional Diffie-Hellman (ECDDH) problem: It is difficult to decide \( k \cdot m \cdot P = n \cdot P \) when \( k \cdot P, m \cdot P, \) and \( n \cdot P \) are given (\( k, m, n \in \mathbb{Z}_q \)).
- Elliptic curve computational Diffie-Hellman (ECCDH) problem: It is difficult to calculate \( k \cdot m \cdot P \) if \( k \cdot P \) and \( m \cdot P \) are given, where \( k, m \in \mathbb{Z}_q \).

IV. PROPOSED SCHEME

The proposed scheme consists of initialization, UAV registration, initial authentication, handover authentication, dynamic UAV addition, and UAV revocation phases. Table 1 defines the notations used in our scheme.

A. INITIALIZATION PHASE

To construct the whole network system, GSS initializes UAM environments and publishes public parameters. Therefore, GSS selects an elliptic curve \( E(a, b) \): \( y^2 = x^3 + ax + b \), a base point \( P \), hash function \( h(.) \) and a master key \( k \). Then, GSS publishes the public parameters \( h(.) \), \( E(a, b) \), \( P \). Moreover, GSS registers ZSP and deploys it in specific zones. Firstly, GSS selects an identity \( ID_i \) and generates a random number \( r_{s_i} \). Then, GSS computes \( S_j = h(ID_j||r_{s_j}||k) \) and stores \( \{ID_j, r_{s_j}\} \) in its secure database. To provide secure handover process, GSS also computes \( k_{12} = h(ID_j||ID_{ZSP}||k) \) as a shared secret of ZSP and ZSP2 which is located near the ZSP. GSS sends \( \{ID_j, k_{12}\} \) to the ZSP via a secure channel. The ZSP selects a secret key \( k_j \) and computes its public key \( Pub_j = h(S_j||k_j) \cdot P \) and stores \( \{S_j\} \) in its database. Finally, the ZSP broadcasts \( \{Pub_j, ID_j\} \) in its management area.

B. UAV REGISTRATION PHASE

A UAV must register in GSS to join in UAM network system. Figure 3 indicates the UAV registration phase and details are as below.

Step 1: The UAV selects an identity \( ID_i \), a random number \( dr_i \) and sends \( \{ID_i, dr_i\} \) to GSS through a secure channel.

Step 2: After receiving the message \( \{ID_i, dr_i\} \) from the UAV, GSS generates a random number \( r_i \) and computes \( DID_i = h(ID_i||dr_i||k) \). Then, the ZSP selects a secret key \( S_j \) and computes its public key \( Pub_j = h(S_j||k_j) \cdot P \) and stores \( \{S_j\} \) in its database. Finally, the ZSP broadcasts \( \{Pub_j, ID_j\} \) in its management area.

C. INITIAL AUTHENTICATION PHASE

To perform various services such as package delivery, air taxi, and air bus, the UAV initially authenticates with a ZSP to prove its identity and establish a session key. Therefore, the UAV sends a request message to ZSP. We represent the initial authentication phase in Figure 4 and details are as below.

Step 1: The UAV generates a random nonce \( r_1 \) and a timestamp \( T_1 \). Then, the UAV computes \( D_1 = r_1 \cdot P, PD_1 = r_1 \cdot Pub_j, z_{ij} = d_i \cdot Pub_i \), a temporary identity \( TID_i = DID_i \oplus h(ID_i||PD_1||T_1) \), and \( V_1 = h(PD_1||ID_i||z_{ij}|| DID_i || T_1) \). The UAV sends a authentication request message \( MSG_1 = \{TID_i, ID_i, D_1, V_1, T_1\} \) to the ZSP through an open channel.

Step 2: When the ZSP receives the message \( MSG_1 \) from the UAV, the ZSP firstly checks \( |T_e - T_1| < \Delta T \)
FIGURE 3. UAV registration phase of the proposed scheme.

FIGURE 4. Initial authentication phase of the proposed scheme.

D. Handover Authentication Phase

If the UAV leaves the current ZSP(ZSP1) region, ZSP1 must support the handover service to the UAV and the next ZSP(ZSP2). Figure 5 indicates the handover authentication phase of the proposed scheme and presents the details below.

Step 1: The UAV generates a random nonce \( r_3 \) and a timestamp \( T_3 \). Then, the UAV computes \( D_2 = r_3 \cdot P \), \( HS_1 = h(SK||E_1) \), a temporary handover identity \( HID_1 = DID_1 \oplus h(HS_1||ID_j) \), and \( V_3 = h(D_2||ID_j||DID_1||Pub_j||SK||ID_3) \) and sends a handover request message \( MSG_3 = \{HID_1, ID_j, D_2, V_3, T_3\} \) to the ZSP2 via an open channel.

Step 2: The ZSP2 checks the timestamp \( |T_e - T_3| < \Delta T \) and generates \( T_4 \). Then, the ZSP2 computes \( V_4 = h(V_3||ID_j||ID_2||Pub_j) \) and sends a message \( MSG_4 = \{HID_1, ID_j, D_2, V_4, T_4\} \) to the ZSP1 through an open channel.

Step 3: Here, the ZSP1 firstly checks \( |T_e - T_4| < \Delta T \) and computes \( HS_2 = h(SK||E_2) \), \( HID_2 = DID_2 \oplus h(HS_2||ID_j) \) and \( V_4 = h(D_2||ID_j||DID_1^t||Pub_1) \) in the memory.
In this section, we analyze our scheme using RoR computes $E^r_i = E'_{i \text{new}} \oplus h(SK_{\text{new}}(||ID_{\text{ID}}||))$, and $V_6^r = h(DZ_2||SK_{\text{new}}||HID_{i \text{new}}||ID_{\text{ID}}||ID_{\text{ID}}||E'_{i \text{new}}||T_6)$ and stores $E'_{i \text{new}}$ in the memory. When $V_6^r = V_6$ is correct, the handover phase is successful.

E. DYNAMIC UAV ADDITION PHASE

The proposed scheme supports an additional UAV service. Details are presented below.

Step 1: The UAV selects an identity $ID_i$, a random number $dr_i$, and sends $\{ID_i, dr_i\}$ to GSS through a secure channel.

Step 2: Upon receiving the message $\{ID_i, dr_i\}$ from the UAV, GSS generates a random number $r_i$ and computes $\text{CID}_{i} = h(ID_i||dr_i||k)$, $d_i = h(dr_i||k)$, $\text{RID}_{i} = ID_i \oplus h(\text{CID}_{i})$ and a public key $\text{Pub}_{i} = d_i \cdot P$ for the UAV. Then, GSS stores $\{ID_i, d_i, \text{CID}_{i}, \text{RID}_{i}\}$ and returns a message $\{ID_{\text{ID}}, \text{Pub}_{i}, d_i\}$ to the UAV via a secure channel.

Step 3: The UAV stores $\{ID_{\text{ID}}, d_i, \text{RID}_{i}\}$ in its memory.

F. UAV REVOCATION PHASE

When a ZSP detects a malicious/misbehaving UAV, the ZSP firstly retrieves $\{HID_a, d_a\}$ and computes $\text{DID}_a = HID_a \oplus h(SK_a||E_{a}(ID_a))$. Then, the ZSP sends $\text{DID}_a$ to GSS. GSS searches and retrieves $\{\text{DID}_a, d_a, \text{RID}_a\}$ and computes $d_a = \text{RID}_a \oplus h(\text{DID}_a)||h(d_a||k)||$. Finally, GSS updates the revocation list and broadcasts $\{HID_a, \text{DID}_a\}$ to all ZSPs.

V. SECURITY ANALYSIS

In this section, we analyze our scheme using informal analysis. The proposed scheme can prevent various security attacks such as replay, man-in-the-middle, session key disclosure, impersonation, privileged insider, verification table leakage, DoS, known session-specific temporary information attacks. Moreover, the proposed scheme can also ensure anonymity, untraceability, perfect forward secrecy, and mutual authentication.

A. INFORMAL ANALYSIS

we analyze the security of our scheme using informal analysis. The proposed scheme can prevent various security attacks such as replay, man-in-the-middle, session key disclosure, impersonation, privileged insider, verification table leakage, DoS, known session-specific temporary information attacks. Moreover, the proposed scheme can also ensure anonymity, untraceability, perfect forward secrecy, and mutual authentication.

1) REPLAY AND MAN-IN-THE-MIDDLE ATTACKS

Suppose that an adversary intercepts messages $MSG_1, MSG_2, MSG_3, MSG_4, MSG_5,$ and $MSG_6$ and replays them in another session. However, these messages include timestamp $T_1, T_2, T_3, T_4, T_5, T_6$ and each entity checks the freshness of the messages. Moreover, ZSPs can verify the freshness of request messages $MSG_1$ and $MSG_3$ using the expiration time $E_i$. Thus, the proposed scheme can prevent replay and man-in-the-middle attacks.

2) IMPERSONATION ATTACK

An adversary intercepts all messages and tries to impersonate as a UAV $D_U$. To act as $D_U$, the adversary must calculate the secret parameter $\text{CID}_{i} = h(ID_i||r_i||k)$. However, the adversary cannot obtain $\text{CID}_{i}$ because $r_i$ and $k$ are random numbers and the master key of GSS, respectively. Therefore, the adversary cannot impersonate a UAV $D_U$.

3) PRIVILEGED INSIDER ATTACK

Suppose that an privileged insider obtains the registration request message $\{ID_i, dr_i\}$ of a UAV $D_U$. However, the adversary cannot calculate the session key $SK = h(DZ_1||T_2||z_j||\text{DID}_i||ID_{\text{ID}})$ because $z_j$ is composed of $D_U$ and secret keys of ZSP. In the handover authentication phase, the adversary must calculate $DZ_2 = r_3 \cdot r_4 \cdot P$, which is under the ECDL problem. Therefore, the proposed scheme is resistant to privileged insider attacks.

4) VERIFICATION TABLE LEAKAGE ATTACK

If an adversary obtains the verification table $\{ID_i, r_j\}$, $\{ID_i, d_i\}$ stored in GSS, the adversary can attempt to calculate the session key $SK = h(DZ_1||T_2||z_j||\text{DID}_i||ID_{\text{ID}})$ without knowing the secret key of $D_U$ and ZSP because $z_j$ is composed of $r_j$ and $d_i$. Moreover, the adversary cannot obtain the session key $SK_{\text{new}} = h(DZ_2||T_6||\text{DID}_i||ID_{\text{ID}})$ in the handover authentication phase without knowing $\text{CID}_i$. Therefore, the proposed scheme is secure against verification table leakage attacks.

5) DOS ATTACK

We can assume that an adversary intercepts all of authentication request messages and sends them to the ZSPs...
concurrently. Recall, there is a timestamp to check the freshness of each message. Moreover, each message includes the real identity of the ZSP and the ZSP can filter the invalid message out. Therefore, the proposed scheme can prevent DoS attacks.

6) SESSION-SPECIFIC RANDOM NUMBER LEAKAGE ATTACK
Assume that an adversary obtains random nonces $r_1, r_2, r_3$, and $r_4$. However, the adversary cannot calculate the session key $SK = h(DZ_1[|T_2|]|DID_1||ID_2)$ because the adversary cannot reveal $z_{ij}$ and $DID_2$. Therefore, the proposed scheme defends session specific random number leakage attacks.

7) ANONYMITY AND UNTRACEABILITY
In our scheme, each message utilizes temporary identity $TID_i$ and $HID_i$, which change dynamically every session. This makes that the adversary cannot identify the real identity of the UAV $ID_i$ during initial and handover authentication phases. Therefore, the proposed scheme can ensure anonymity and untraceability.

8) PERFECT FORWARD SECRECY
If an adversary obtains the master key $k$ of GSS and messages $MSG_m (m = 1, 2, 3, 4, 5, 6)$ of the previous session, the adversary can try to calculate the session key $SK$ of UAV $D_U$. However, the adversary cannot calculate $SK$ because $DZ_1$ and $DZ_2$ are based on the ECDL problem. Furthermore, the secret keys of $D_U$ and ZSP are necessary to calculate $z_{ij} = d_i \cdot k_j \cdot P$. Therefore, the adversary has no advantage and this means that the proposed scheme provides perfect forward secrecy.

9) MUTUAL AUTHENTICATION
In our scheme, each entity sends message including timestamp $T_m$ ($m = 1, 2, 3, 4, 5, 6$) to check the freshness and verification parameter $v_m$ and the correctness of each parameter. If the verification parameter is clear, it means that the entity authenticates to the target entity. Therefore, the proposed scheme provides mutual authentication.

B. RoR MODEL
This section analyzes the session key security of the proposed handover authentication scheme using RoR model [10]. In RoR model, we define participants, adversary, and queries to reflect our scheme. Participants in our scheme consist of three elements: $Pa^{i-1}_{UAV}$, $Pa^{i-1}_{ZSP_1}$, and $Pa^{i-1}_{ZSP_2}$. Each participant $Pa^{i-1}_{UAV}$, $Pa^{i-1}_{ZSP_1}$, and $Pa^{i-1}_{ZSP_2}$ indicates $UAV$, $ZSP_1$, and $ZSP_2$ and $i_m$ is the instance of the participant. Adversary in RoR model can inject, rerun, intercept, and delete messages exchanged via open channels. With this ability, the adversary can perform security attacks using $Execute$, $CorruptUAV$, $Send$, and $Test$ queries:

- $Execute(Pa^{i-1}_{UAV}, Pa^{i-1}_{ZSP_1}, Pa^{i-1}_{ZSP_2})$: If an adversary performs this query, the adversary can eavesdrop messages transmitted through public channel. Thus, $Execute$ query is a passive attack.

| UAV ($D_U$) | ZSP$_1$ | ZSP$_2$ |
|-------------|---------|---------|
| Generates $r_1, r_2$ | Computes $D_2 = r_2 \cdot P, H_2 = h(SK_{i-1}||E_{i-1})$ | Generates $T_2$ |
| $HID_2 = D_2 \oplus h(H_2||ID_2)$ | Computes $V_2 = h(D_2||ID_2||T_2||ID_2)$ | Computes $V_4 = h(V_4||ID_2||T_2)$ |
| $(HID_2,ID_2,T_2)$ | Checks $(T_1 - T_2) < \Delta T$ | Checks $(T_1 - T_2) < \Delta T$ |
| $V_2 = h(V_2||ID_2||T_2||ID_2)$ | $(HID_1,ID_1,T_1,V_3,T_2)$ | $(HID_1,ID_1,T_1,V_3,T_2)$ |

FIGURE 5. Handover authentication phase of the proposed scheme.
• **CorruptUAV(Pa,V,UAV):** It is an active attack, where an adversary obtains secret parameters stored in a UAV Pa,V,UAV.

• **Send(Pa,m, MSG):** Using this query, an adversary can transmit a message MSG to the other entities Pa,V,UAV, Pa,V,ZSP, and Pa,ZSP. Moreover, the adversary can receive a return message from these entities. Thus, the query Send have an attribute of active attack.

• **Test(Pa,m):** An unbiased coin uc is flipped when a Test query is conducted. The flipping result of uc can be 0 or 1, where uc = 1 and uc = 0 means the session key is fresh and not fresh, respectively. Otherwise, the adversary gets NULL (⊥) value.

**Theorem 1:** We define Adver,M(L) as the possibility of breaking the session key security in polynomial time. We also make a definition of Hash and qHASH that are the range space of the hash function h(.) and the number of hash queries, respectively. Moreover, Adver,ECDDH,M(L) is the possibility of breaking ECDDH problem.

\[
\text{Adver}_M(L) = \frac{q^2_{\text{Hash}}}{|\text{Hash}|} + 2\text{Adver}_{ECDDH,M}(L) \tag{1}
\]

**Proof:** Following the RoR security proof in [24]–[26], we conduct four games GA_n (n = 0, 1, 2, 3). We define the winning probability of the adversary as SuccGA_n. We also denote the advantage of SuccGA_n as PR[SuccGA_n].

• **GA_0:** In GA_0, the adversary has no information to calculate the session key SK. Therefore, the adversary picks the random bit b. As a result, we obtain the following equation.

\[
\text{Adver}_M(L) = |2\text{PR}[\text{SuccGA}_0] - 1| \tag{2}
\]

• **GA_1:** The adversary conducts Execute query to obtain messages transmitted through open channels. With the messages MSG_3 = \{HID_1, ID_1, D_2, V_3, T_3\}, MSG_4 = \{HID_1, ID_2, D_2, V_4, T_3, T_1\}, MSG_5 = \{M_1, V_5, T_3\}, and MSG_6 = \{Z_2, V_6, E_i, T_6\}, the adversary performs Test query to distinguish whether the result value is the session key or not. However, the session key SK = h(DZ_2||T_6||ID_1||ID_2) is composed of DZ_2 and DID_1. To calculate DZ_2, the adversary must obtain random nonces r_3 and r_4. Moreover, DID_1 is the secret parameter of UAV. Therefore, we can obtain the following equation.

\[
\text{PR}[\text{SuccGA}_1] = \text{PR}[\text{SuccGA}_1] \tag{3}
\]

• **GA_2:** In GA_2, the adversary attempts to attack the network using Send and Hash queries. In our scheme, parameters are masked by random nonces and hash functions which have resistance against hash collision. Therefore, the adversary has not any advantage using Hash query. Thus, we can obtain the following equation using the birthday paradox [27].

\[
|\text{PR}[\text{SuccGA}_2] - \text{PR}[\text{SuccGA}_1]| \leq \frac{q^2_{\text{Hash}}}{|\text{Hash}|} \tag{4}
\]

• **GA_3:** In the final game GA_3, the adversary obtains secret parameters of UAV \{DID_i, d_i\} using CorruptUAV query. However, the adversary cannot calculate the session key SK = h(DZ_2||T_6||ID_1||ID_2) because DZ_2 = r_3 \cdot r_4 \cdot P is based on ECDDH problem. Thus, we can obtain the following result.

\[
|\text{PR}[\text{SuccGA}_3] - \text{PR}[\text{SuccGA}_2]| \leq \text{Adver}_{ECDH,M}(L) \tag{5}
\]

The adversary executes Test query and obtains a guessed bit b. Thus, we can get the following equation.

\[
\text{PR}[\text{SuccGA}_1] = \frac{1}{2} \tag{6}
\]

Using (2) and (3), we can calculate and get the equation.

\[
\frac{1}{2}\text{Adver}_M(L) = |\text{PR}[\text{SuccGA}_0] - \frac{1}{2}|
\]

\[
= |\text{PR}[\text{SuccGA}_1] - \frac{1}{2}| \tag{7}
\]

We can obtain the following equation using (6) and (7).

\[
\frac{1}{2}\text{Adver}_M(L) = |\text{PR}[\text{SuccGA}_1] - \text{PR}[\text{SuccGA}_2]| \tag{8}
\]

Applying the triangular inequality and simplifying the equation (8), we can obtain the following.

\[
\frac{1}{2}\text{Adver}_M(L) \leq |\text{PR}[\text{SuccGA}_1] - \text{PR}[\text{SuccGA}_3]| + |\text{PR}[\text{SuccGA}_3] - \text{PR}[\text{SuccGA}_2]|
\]

\[
\leq \frac{q^2_{\text{Hash}}}{2|\text{Hash}|} + \text{Adver}_{ECDH,M}(L) \tag{9}
\]

Multiplying (9) by 2, we can get the following result.

\[
\text{Adver}_M(L) \leq \frac{q^2_{\text{Hash}}}{|\text{Hash}|} + 2\text{Adver}_{ECDH,M}(L) \tag{10}
\]

Therefore, the **Theorem 1** is proved.

**C. BAN LOGIC**

To prove the mutual authentication of our handover authentication scheme, we utilize a well-known formal proof named BAN logic [11]. Many researchers have proved the mutual authentication of their scheme using BAN logic [28]–[30]. To apply our scheme into BAN logic, we introduce notations and descriptions as follows.

1) **RULES**

In BAN logic, there are five basic logical rules shown as follows.

1. **Message meaning rule (MMR):**

\[
\text{Pr}_i \leftarrow \text{Pr}_j \Rightarrow \text{Pr}_i \leftarrow [\text{MSG}_1]_S
\]

\[
\text{Pr}_j \leftarrow \text{MSG}_1 \sim \text{Pr}_i
\]
The assumptions in our scheme are as below.

4) ASSUMPTIONS

There are four messages in our handover authentication scheme. The idealized forms of the messages are as below.

| Message | Description |
|---------|-------------|
| $D_U$ | The NVR can be obtained from $D_U$ using $BP_1$ and $A_5$. |
| $D_U \rightarrow Z_2$ | The MMR can be obtained from $D_U$ using $BP_4$ and $A_5$. |
| $Z_2 \rightarrow Z_1$ | The FR can be obtained from $Z_2$ using $BP_7$ and $A_6$. |
| $D_U \rightarrow [D_2, DID_i, T_3]_{HS_1}, T_4$ | The NVR can be obtained from $D_U$ using $BP_4$ and $A_5$. |
| $D_U \rightarrow [D_2, DID_i, T_3]_{HS_1}, T_4$ | The FR can be obtained from $D_U$ using $BP_7$ and $A_6$. |

5) BAN LOGIC PROOF

Step 1: $BP_1$ is obtained from the message $MSG_2$.

$BP_1 : Z_1 \leftarrow \{D_U \rightarrow \{D_2, DID_i, T_3\}_{HS_1}, T_4\}_{k_{12}}$

Step 2: $BP_2$ is obtained from the MMR using $BP_1$ and $A_5$.

$BP_2 : Z_1 \leftarrow \{D_U \rightarrow \{D_2, DID_i, T_3\}_{HS_1}, T_4\}_{k_{12}}$

Step 3: $BP_3$ can be obtained from $MSG_1$ because $Z_1$ believes that $\{D_2, DID_i, T_3\}_{HS_1}$ is sent from $D_U$ in $BP_2$.

$BP_3 : Z_1 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 4: $BP_4$ can be obtained from the MMR using $BP_3$ and $A_8$.

$BP_4 : Z_1 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 5: $BP_5$ is obtained from the FR using $A_2$ and $BP_4$.

$BP_5 : Z_1 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 6: $BP_6$ is obtained from the NVR using $BP_4$ and $BP_5$.

$BP_6 : Z_2 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 7: From the message $MSG_3$, $BP_7$ can be obtained.

$BP_7 : Z_2 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 8: $BP_8$ can be obtained from the MMR using $BP_7$ and $A_6$.

$BP_8 : Z_2 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 9: $BP_9$ can be obtained from the FR using $BP_8$ and $A_4$.

$BP_9 : Z_2 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 10: $BP_{10}$ can be obtained from the NVR using $BP_8$ and $BP_9$.

$BP_{10} : Z_2 \leftarrow \{D_2, DID_i, T_3\}_{HS_1}$

Step 11: $BP_{11}$ can be obtained from the message $MSG_4$.

$BP_{11} : D_U \leftarrow \{Z_2, T_6\}_{DID_i}$

TABLE 2. Notations of BAN logic.

| Notation | Description |
|----------|-------------|
| $Pr_i, Pr_j$ | Principals of the UA, $ZSP_1$, and $ZSP_2$, respectively. |
| $MSG_1, MSG_2$ | $Pr_i$ believes $MSG_1$. |
| $SK$ | $Pr_i$ once said $MSG_1$. |
| $Pr_i \equiv MSG_1$ | $Pr_i$ controls $MSG_1$. |
| $Pr_i \equiv MSG_1$ | $Pr_i$ receives $MSG_1$. |
| $\#MSG_1$ | $MSG_1$ is fresh. |
| $(MSG_1)_S$ | $MSG_1$ is encrypted with $S$. |
| $Pr_i \rightarrow Pr_j$ | $Pr_i$ and $Pr_j$ have shared key $S$. |
| $Pr_i \equiv (MSG_1, MSG_2)$ | $Pr_i \equiv MSG_1$. |
| $Pr_i \equiv \#(MSG_1, MSG_2)$ | $Pr_i \equiv \#(MSG_1, MSG_2)$. |

2) GOALS

We denote that principals of the UAV, $ZSP_1$, and $ZSP_2$ are $D_U$, $Z_1$, and $Z_2$, respectively. Thus, goals of our scheme are as below.

Goal 1: $D_U \equiv D_U \leftrightarrow Z_2$

Goal 2: $D_U \equiv Z_2 \equiv D_U \leftrightarrow Z_2$

Goal 3: $Z_2 \equiv D_U \leftrightarrow Z_2$

Goal 4: $Z_2 \equiv D_U \equiv D_U \leftrightarrow Z_2$

3) IDEALIZED FORMS

There are four messages in our handover authentication scheme. The idealized forms of the messages are as below.

- $MSG_1 : D_U \rightarrow Z_2 : \{D_2, DID_i, T_3\}_{HS_1}$
- $MSG_2 : Z_2 \rightarrow Z_1 : \{D_U \rightarrow \{D_2, DID_i, T_3\}_{HS_1}, T_4\}_{k_{12}}$
- $MSG_3 : Z_1 \rightarrow Z_2 : \{DID_i, T_3\}_{k_{12}}$
- $MSG_4 : Z_2 \rightarrow D_U : \{Z_2, T_6\}_{DID_i}$

4) ASSUMPTIONS

The assumptions in our scheme are as below.

$A_1 : D_U \equiv \#(T_6)$

$A_2 : Z_1 \equiv \#(T_3)$
Step 12: $BP_{12}$ can be obtained from the MMR using the assumption $A_{11}$.

$$BP_{12} : D_U \equiv Z_2 \sim (Z_2, T_6)$$

Step 13: $BP_{13}$ can be obtained from the FR using the assumption $A_1$.

$$BP_{13} : D_U \equiv \#(Z_2, T_6)$$

Step 14: $BP_{14}$ can be obtained from the NVR using $BP_{12}$ and $BP_{13}$.

$$BP_{14} : D_U \equiv Z_2 \equiv (Z_2, T_6)$$

Step 15: $D_U$ compute the session key $SK = h(DZ_2||T_6||DID_2||ID_2)$. Therefore, we can obtain $BP_{15}$ and $BP_{16}$ from $BP_{14}$ and $BP_{10}$.

$$BP_{15} : D_U \equiv Z_2 \equiv (D_U \leftrightarrow Z_2) \quad \text{(Goal2)}$$

$$BP_{16} : Z_2 \equiv D_U \equiv (D_U \leftrightarrow Z_2) \quad \text{(Goal4)}$$

Step 16: $BP_{17}$ and $BP_{18}$ can be obtained from the JR using $BP_{15}$, $BP_{16}$, $A_9$, and $A_{10}$, respectively.

$$BP_{17} : D_U \equiv (D_U \leftrightarrow Z_2) \quad \text{(Goal1)}$$

$$BP_{18} : Z_2 \equiv (D_U \leftrightarrow Z_2) \quad \text{(Goal3)}$$

**D. AVISPA SIMULATION**

AVISPA [12] simulation tool has been widely used to prove the security features, i.e., replay and man-in-middle attacks, of various schemes [31]–[33]. Therefore, we simulate and demonstrate the security against replay and man-in-the-middle attacks of the proposed scheme using AVISPA.

To apply our scheme into AVISPA, we complete a code design written in “High-Level Protocol Specification Language (HLPSL)”. After that, the HLPSL code is converted to “Intermediate Format (IF)” by the translator and the IF enters in four backends to perform security analysis named On-the-Fly Model Checker (OFMC), Tree Automata based on Automatic Approximations for Analysis of Security Protocol (TA4SP), Constraint Logic based Attack Searcher (CL-AtSe), and SAT-based Model Checker (SATMC). In this paper, we use OFMC and CL-AtSe backends because they can support exclusive-OR ($\oplus$) operators.

**VI. PERFORMANCE ANALYSIS**

In this section, we compare the security features, communication, and computation costs of proposed scheme with the other related schemes.

**A. COMPUTATION COSTS COMPARISON**

In this section, computation costs of the proposed scheme and the related schemes [16]–[19] are estimated to prove the efficiency of our scheme. Therefore, we simulate and estimate handover authentication in state 4. Figure 7 indicates the session, environment, and goal of our scheme and Figure 8 shows the OF of our scheme. Since the summary of the result displays “SAFE”, we can demonstrate that the proposed scheme can prevent replay and man-in-the-middle attacks.

**TABLE 3. Simulation result using MIRACL**

| Notations | Descriptions | Desktop | Raspberry PI |
|-----------|--------------|---------|--------------|
| $E_{val}$ | ECC multiplication | 2.598 ms | 2.862 ms |
| $E_{add}$ | ECC addition | 0.012 ms | 0.017 ms |
| $S_e$ | AES encryption | 0.001 ms | 0.013 ms |
| $S_d$ | AES decryption | 0.001 ms | 0.014 ms |
| $M_{exp}$ | Modular exponentiation | 0.196 ms | 0.311 ms |
| $B$ | Bilinear pairing (BP) | 6.490 ms | 9.244 ms |
| $B_{mul}$ | BP multiplication | 0.813 ms | 1.014 ms |
| $H$ | Hash function | 0.003 ms | 0.006 ms |
TABLE 4. Computation costs comparison.

| Schemes       | Device | Infrastructure 1 | Infrastructure 2 | Total Costs (ms) |
|---------------|--------|------------------|------------------|------------------|
| Kumar et al. [16] | $4E_{mul} + 4B + 1B$ | $1E_{mul} + 1B$ | $2E_{mul} + 1B + 2H$ | 41.502          |
| Wang et al. [17]   | $1Mexp + 1B_{mul} + 1B$ | $3Mexp + 1B_{mul} + 1B$ | $2Mexp$ | 19.197          |
| Zhou et al. [18]    | $6E_{mul} + 2E_{add} + 3H$ | $7E_{mul} + 2E_{add} + 5H$ | $3E_{mul} + 2E_{add} + 4H$ | 43.279          |
| ZakeriKia et al. [19] | $4E_{mul} + 4E_{add} + 7H$ | $4E_{mul} + 3E_{add} + 6H$ | $5E_{mul} + 3E_{add} + 9H$ | 35.057          |
| Proposed         | $2E_{mul} + 7H$ | $2E_{mul} + 8H$ | $5H$ | 11.001          |

TABLE 5. Communication costs comparison.

| Schemes       | Total Communication Costs | Messages |
|---------------|---------------------------|----------|
| Kumar et al. [16] | 3300 bits                 | 4        |
| Wang et al. [17]    | 3072 bits                 | 3        |
| Zhou et al. [18]    | 2880 bits                 | 4        |
| ZakeriKia et al. [19] | 2944 bits              | 4        |
| Proposed         | 2560 bits                 | 4        |

We compare communication costs of our scheme with the related schemes [16]–[19]. From [35], we define that the identity, hash function, random number, ECC point, timestamp and modular exponentiation are 160 bits, 160 bits, 160 bits, 320 bits, 64 bits, and 1024 bits, respectively. By applying them, we obtain the communication cost of the proposed scheme for each message as follows: $(\{\text{HID}_i, \text{ID}_j, D_2, V_3, T_3\}: 864$ bits, $\{\text{HID}_i, \text{ID}_j^2, D_2, V_4, T_3, T_4\}: 928$ bits, $\{\text{M}_1, V_5, T_3\}: 384$ bits, $\{Z_2, V_6, E_i^o, T_6\}: 704$ bits). Therefore, the total communication costs of proposed scheme requires $864 + 928 + 384 + 704 = 2880$ bits. We also compare the communication costs of the proposed protocol with the other related schemes [16]–[19] in Table 5. The result represents that the proposed scheme has a lower communication costs compared with the existing schemes.

C. SECURITY AND FUNCTIONALITY FEATURES COMPARISON

We compare security and functionality features of the proposed scheme and those of the existing schemes [16]–[19]. Table 6 shows the comparison of each scheme, and the descriptions of security features are as follows: SFC1:“replay attack”, SFC2:“man-in-the-middle attack”, SFC3:“impersonation attack”, SFC4:“privileged insider attack”, SFC5:“verification table leakage attack”, SFC6:“DoS attack”, SFC7:“session-specific random number leakage attack”, SFC8:“anonymity”, SFC9:“untraceability”, SFC10:“perfect forward secrecy”, SFC11:“mutual authentication”, SFC12:“provide a computationally efficient communication”. The result shows that the proposed scheme can provide a secure and efficient communication for UAM environments.

FIGURE 7. Role of session, environment, and goal.

FIGURE 8. Result of the AVSIPA simulation.
In this paper, we designed a secure handover authentication scheme for UAM environments which are expected as a future air mobility system. In the proposed scheme, the handover authentication process can provide a lower computation cost than the initial authentication because the previous ZSP supports the handover authentication. We conducted an informal security analysis to demonstrate that our scheme can prevent various security attacks. We also conducted RoR model and BAN logic to prove that the proposed scheme can provide session key security and mutual authentication, respectively. Moreover, we executed AVISPA simulation tool to show the robustness of our scheme against man-in-the-middle and replay attacks. To estimate the efficiency of our scheme, we compared computation and communication costs of our scheme with other related schemes. Therefore, the proposed scheme can provide a secure and efficient communication for UAM environments. In the future study, we will design an enhanced scheme for implementation in practical environments and contribute to secure UAM environments.

VII. CONCLUSION

In this paper, we designed a secure handover authentication scheme for UAM environments which are expected as a future air mobility system. In the proposed scheme, the handover authentication process can provide a lower computation cost than the initial authentication because the previous ZSP supports the handover authentication. We conducted an informal security analysis to demonstrate that our scheme can prevent various security attacks. We also conducted RoR model and BAN logic to prove that the proposed scheme can provide session key security and mutual authentication, respectively. Moreover, we executed AVISPA simulation tool to show the robustness of our scheme against man-in-the-middle and replay attacks. To estimate the efficiency of our scheme, we compared computation and communication costs of our scheme with other related schemes. Therefore, the proposed scheme can provide a secure and efficient communication for UAM environments. In the future study, we will design an enhanced scheme for implementation in practical environments and contribute to secure UAM environments.

REFERENCES

[1] D. P. Thipphavong, R. Apaza, B. Barmore, V. Battiste, B. Burian, Q. Dao, M. Feary, S. Go, K. H. Goodrich, J. Homola, H. R. Idris, P. H. Kopardekar, J. B. Lachter, N. A. Neogi, H. K. Ng, R. M. Oseguera-Lohr, M. D. Patterson, and S. A. Verma, "Urban air mobility airspace integration concepts and considerations," in *Proc. Aviation Technol., Integ., Oper. Conf.*, Atlanta, GA, USA, Jun. 2018, pp. 3676–3687.

[2] N. Kim and Y. Yoon, "Regionalization for urban air mobility application with analyses of 3D urban space and geodemography in San Francisco and New York," *Proc. Comput. Sci.*, vol. 184, pp. 388–395, Jan. 2021.

[3] H. Eisfeldt, "Sustainable urban air mobility supported with participatory noise sensing," *Sustainability*, vol. 12, no. 8, pp. 3320–3331, 2020.

[4] A. Bandyopadhyay, N. S. Raj, and J. T. Varghese, "Coexisting in a world with urban air mobility: A revolutionary transportation system," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, Abu Dhabi, United Arab Emirates, Feb. 2018, pp. 1–6.

[5] A. P. Cohen, S. A. Shaheen, and E. M. Farrar, "Urban air mobility: History, ecosystem, market potential, and challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 6074–6087, Sep. 2021.

[6] K. Song and H. Yeo, "Development of optimal scheduling strategy and approach control model of multicopter VTOL aircraft for urban air mobility (UAM) operation," *Transp. Res. C, Emerg. Technol.*, vol. 128, pp. 103181–103198, Jul. 2021.

[7] M. Waidz, A. K. Das, and J.-H. Lee, "Authorization protocols for the Internet of Drones: Taxonomy, analysis and future directions," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Aug. 2018, doi: 10.1007/s12652-018-1000-x.

[8] J. Ivosevic, E. Ganic, A. Petosic, and T. Radisic, “Comparative UAV noise-impact assessments through survey and noise measurements,” *Int. J. Environ. Res. Public Health*, vol. 18, no. 12, pp. 6602–6622, 2021.

[9] M. Gharibi, R. Boutaba, and S. L. Waslander, “Internet of Drones,” *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[10] M. Abdalla, P. A. Fouque, and D. Pointcheval, “Password-based authenticated key exchange in the three-party setting,” in *Proc. Int. Workshop Theory Pract. Public Key Cryptogr.*, in Lecture Notes in Computer Science, Les Diablerets, Switzerland, Jan. 2005, pp. 65–84.

[11] M. Burrows, A. Abadi, and R. Needham, “A logic of authentication,” *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[12] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Heim, O. Kouchcarenok, J. Mantovani, S. Módersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turaní, L. Viganò, and L. Vigneron, “The AVISPA tool for the automated validation of internet security protocols and applications,” in *Proc. Int. Conf. Comput. Aided Verification*, Scotland, U.K., Jul. 2005, pp. 281–285.

[13] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, “Security and privacy for the Internet of Drones: Challenges and solutions,” *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[14] G. Cho, J. Cho, S. Hyun, and H. Kim, “SEN TinEL: A secure and efficient authentication framework for unmanned aerial vehicles,” *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.

[15] S. U. Jan, F. Qayum, and H. U. Khan, “Design and analysis of lightweight authentication protocol for securing IoT,” *IEEE Access*, vol. 9, pp. 69287–69306, 2021.

[16] A. Kumar and H. Oin, “Handover authentication scheme for device-to-device outband communication in 5G-WLAN next generation heterogeneous networks,” *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7961–7977, Dec. 2018.

[17] C. Wang, J. Shen, J. F. Lai, and J. Liu, “B-TSCA: Blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs,” *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1386–1396, Sep. 2020.

[18] Y. Zhou, X. Long, L. Chen, and Z. Yang, “Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETS,” *J. Inf. Secur. Appl.*, vol. 47, pp. 295–305, Aug. 2019.

[19] S. ZakeriKia, R. Hajian, S. H. Erfani, and A. M. Rahmani, “Robust and anonymous handover authentication scheme without key escrow problem in vehicular sensor networks,” *Wireless Netw.*, vol. 27, no. 7, pp. 4997–5028, Oct. 2021.

[20] D. Dolev and A. C. Yao, “On the security of public key protocols,” *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[21] R. Canetti and H. Krawczyk, “Universally composable notions of key exchange and secure channels,” in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Amsterdam, The Netherlands, May 2002, pp. 337–351.

[22] D. Kwon, S. Yu, J. Lee, S. Son, and Y. Park, “WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks,” *Sensors*, vol. 21, no. 3, pp. 936–959, 2021.

[23] N. Koblitz, “Elliptic curve cryptosystems,” *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[24] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, and Y. Park, “Secure ECC-based three-factor mutual authentication protocol for telecare medical information system,” *IEEE Access*, vol. 10, pp. 11511–11526, 2022.

[25] A. K. Das, M. Waidz, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, “Provably secure ECC-based device access control and key agreement protocol for IoT environment,” *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[26] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, “Design of blockchain-based lightweight V2I handover authentication protocol for VANET,” *IEEE Trans. Netw. Sci. Eng.*, early access, Jan. 13, 2022, doi: 10.1109/TNSE.2022.3142287.

[27] V. Boyko, P. MacKenzie, and S. Patel, “Provably secure password-authorized key exchange using Diffie-Hellman,” in *Proc. Int. Conf. Theor. Appl. Cryptograph. Techn.*, Bruges, Belgium, May 2000, pp. 156–171.

[28] J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, “A secure and lightweight authentication protocol for IoT-based smart homes,” *Sensors*, vol. 21, no. 4, pp. 1488–1512, 2021.

[29] J. Lee, M. Kim, J. Oh, Y. Park, K. Park, and S. Noh, “A secure key aggregate searchable encryption with multi delegation in cloud data sharing service,” *Appl. Sci.*, vol. 11, no. 19, pp. 8841–8861, 2021.

[30] M. Kim, J. Lee, K. Park, Y. Park, K. H. Park, and Y. Park, “Design of secure decentralized car-sharing system using blockchain,” *IEEE Access*, vol. 9, pp. 54796–54810, 2021.
S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, “IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment,” IEEE Access, vol. 8, pp. 167875–167886, 2020.

J. Lee, G. Kim, A. K. Das, and Y. Park, “Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks,” IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2412–2425, Jul. 2021.

S. Son, Y. Park, and Y. Park, “A secure, lightweight, and anonymous user authentication protocol for IoT environments,” Sustainability, vol. 13, no. 16, pp. 9241–9262, 2021.

MIRACL Cryptographic SDK: Multiprecision Integer and Rational Arithmetic Cryptographic Library. Accessed: Feb. 20, 2022. [Online]. Available: https://github.com/miracl/MIRACL

J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, “Cloud centric authentication for wearable healthcare monitoring system,” IEEE Trans. Dependable Secure Comput., vol. 17, no. 5, pp. 942–956, Sep. 2020.

DEOKKYU KWON received the B.S. degree in electronics engineering and the M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2020 and 2022, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include the Internet of Drones, wireless sensor networks, mutual authentication, and information security.

SEUNGHWAN SON received the B.S. degree in mathematics and the M.S. degree in electronic and electrical engineering from Kyungpook National University, Daegu, South Korea, in 2019 and 2021, respectively, where he is currently pursuing the Ph.D. degree with the School of Electronic and Electrical Engineering. His research interests include authentication, blockchain, cryptography, and information security.

YOHAN PARK received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 2006, 2008, and 2013, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, Keimyung University, Daegu. His research interests include computer networks, mobile security, blockchain, and the IoT.

HYUNGPYO KIM received the B.S., M.S., and Ph.D. degrees in electrical engineering from Kyungpook National University, Daegu, South Korea, in 1992, 1994, and 1998, respectively. In 1998, he joined Kyungpook National University, where he is currently a Professor with the Department of Electrical Engineering. His research interests include sensor devices and sensor security and systems.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sungju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronic and Electrical Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.

SANGWOO LEE received the B.S., M.S., and Ph.D. degrees in electronics from Kyungpook National University, Daegu, Republic of Korea, in 1999, 2001, and 2009, respectively. Since 2001, he has been a Principal Engineering Staff with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. He was a Visiting Research Fellow in WMG at the University of Warwick, U.K., from 2016 to 2017. He is currently a Rapporteur of Q13, security aspects on ITS, in ITU-T SG17. He is also the editor of X.1371, X.1372, X.1374, X.1375 for ITS security. His research interests include information security based on cryptography, hardware architectures for cryptographic algorithms, and ITS security.

YONGSUNG JEON received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University, in 1986, 1990, and 2010, respectively. He was with the Agency for Defense and Development (ADD), Daejeon, South Korea, from 1992 to 1999. He has been with the Electronics and Telecommunications Research Institute (ETRI), Daejeon, since 1999, where he is currently a Principal Research Engineer. His research interests include wireless covert channel, information security, and cryptography.

***