IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 March 2024, accepted 15 May 2024, date of publication 23 May 2024, date of current version 6 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3404850

RESEARCH ARTICLE

Concurrent Two-Party Key Exchange With *Forward Unlinkability* in Internet of Drones

JAE YEOL JEONG[1], HYUNG WOO KANG[2], AND IK RAE JEONG[3]
[1]Department of Information Security, Soonchunhyang University, Asan, Chungcheongnam 31538, Republic of Korea
[2]Kim and Chang, Jongno, Seoul 03170, Republic of Korea
[3]School of Cybersecurity, Korea University, Seongbuk, Seoul 02841, Republic of Korea

Corresponding author: Ik Rae Jeong (irjeong@korea.ac.kr)

This work was supported in part by the Military Crypto Research Center funded by the Defense Acquisition Program Administration (DAPA) and Agency for Defense Development (ADD) under Grant UD210027XD, and in part by the Korea University Grant.

ABSTRACT By the drone capturing attacks, the adversaries can extract the long-term secret keys stored in the drones. Therefore, it is necessary to consider forward secrecy and forward unlinkability to minimize the damage by the drone capturing attacks. Forward secrecy protects the secrecy of the past sessions between users and drones, and forward unlinkability guarantees the strong anonymity of users and drones participated in the past sessions, even when the long-term secret keys are revealed to the attackers via the drone capturing attacks. In 2022 Jeong et el. suggested a three-party key agreement scheme for internet of drones which provides forward secrecy and forward unlikability. However, their scheme has some shortcomings. Especially, in their scheme a drone (or a user) cannot run concurrently multiple key exchange sessions with multiple users (or drones). And their scheme provides only weak forward secrecy, not standard forward secrecy. In this paper, we propose a key exchange protocol resolving all the shortcomings of the Jeong et al.'s scheme. That is, our key exchange protocol provides the standard forward secrecy and forward unlinkability. And a drone can run concurrently multiple sessions with users without communication with the server. We also suggest a formal model for the forward unlinkability, and prove the forward unlinkability of our scheme in the formal model.

INDEX TERMS Internet of drones, key agreement, anonymity, forward unlinkability, forward secrecy.

I. INTRODUCTION

Advancements in aviation, software, information and communication technology, and sensor technologies have catalyzed a surge in drone-based applications.

Innovative solutions based on the Internet of Drones (IoD) include aerial photography, smart agriculture, land management, infrastructure inspection, emergency response, smart city applications, and so on [1], [2].

Within the IoD context, securing communication through authenticated key exchange protocols is crucial for maintaining message integrity and confidentiality. Recent researches are increasingly focused on the light-weight key exchange protocols to provide user-drone authentication crucial for ensuring secure IoD communications [3], [4], [5], [6], [11].

The other pressing issue in an IoD environment is to protect the privacy of both users and drones. To provide anonymity, many authenticated key exchange schemes have used pseudonyms for users and drones. However, pseudonymity alone does not provide strong anonymity. For instance, should an adversary observe a repeated (and unchanging) pseudonym associated with a user or drone, it might know frequencies of activity or even trace the movements of the entities. Such surveillance could lead to the deanonymization of the parties involved. Specifically, within the context of military operations, the lack of strong anonymity, called unlinkability, could lead to catastrophic operation failures.

One of the most powerful attacks in IoD is a drone capturing attack [12]. By this capturing attack an adversary

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Abdur Razzaque.

could get a drone and analyze the drone. In the context of key exchange protocols, such drone capturing attacks make adversaries to uncover the drone's long-term secret key. The revealed long-term secret key is critical information in breaking the secrecy of session keys and unlinkability of the past sessions. Therefore, against the drone capturing attacks, it is important for key exchange protocols to provide forward secrecy and forward unlinkability.

Forward secrecy protects the secrecy of the past sessions between users and drones, and forward unlinkability guarantees the strong anonymity of users and drones participated in the past sessions, even when the long-term secret keys are revealed to the attackers via the drone capturing attacks.

A. RELATED WORKS

In 2018 Wazid et al. [4] proposed a novel and lightweight remote user authentication and key agreement scheme specifically tailored for IoD environments. This work was followed by an even more efficient scheme by Srinivas et al. [5], although these schemes in [4] and [5] were not secure against other authenticated users, who could potentially calculate session keys established by other parties. In 2020, Zhang et al. [6] offered a lightweight authenticated key agreement protocol using only a hash function and bitwise XOR operations. However, these schemes [4], [5], [6] only provided pseudonymity without unlinkability, because the same pseudonym of a party is used in different sessions.

Further advancements in drone-specific protocols have also been notable. For instance, Yazdinejad et al. [7], in 2020, proposed a drone authentication scheme using blockchain technology, allowing drones to be certified across multiple zones without re-certification. Sharma et al. [8] suggested a similar scheme that year, enabling drones to deploy sensor nodes for data collection. Also in 2020, Gope and Sikdar [9] were the first to consider the physical security of Unmanned Aerial Vehicles (UAVs), providing a system that outperformed existing methods in computational complexity while preserving privacy. In 2021, Jan et al. [10] attempted to design a key agreement scheme for civilian drone deployment in the IoD.

In 2022 Jeong et al. [11] introduced the first key agreement protocols that provides both forward secrecy and forward unlinkability. However, their scheme has some shortcomings. First, the forward secrecy provided by their scheme is a weak forward secrecy, not standard forward secrecy. Second, a drone (or a user) can not run concurrently multiple key exchange sessions with multiple users (or drones). Third, each session key establishment between a drone and a user involves communication with the server. That is, their scheme is a three-party key exchange protocol, not a two-party key exchange protocol. Fourth, the unlinkability analysis was done without the formal security model.

B. CONTRIBUTIONS

To overcome the shortcomings of the Jeong et al.'s scheme, we use an ID-based key exchange protocol and a MAC-based key exchange protocol. To make an authenticated key exchange scheme, we use the long-term key derivation protocol of the ID-based key exchange protocol suggested in [13] and modify the MAC-based key exchange protocol in [14] to make a session key. To provide anonymity and unlinkability, our scheme makes an ephemeral Diffie-Hellman key which is used to encrypt the messages necessary for authentication.

Our key exchange protocol provides the standard forward secrecy and forward unlinkability. And a drone can run concurrently multiple sessions with users without communication with the server. We also suggest a formal model for the forward unlinkbility, and prove the forward unlinkability of our scheme in the formal model.

We compare security and anonymity properties among related key exchange protocols in Table 1.

TABLE 1. Pseudonymity and unlinkability of related schemes.

Schemes	Forward secrecy	Pseudonymity of users	Pseudonymity of drones	Forward unlinkability	Concurrent execution	Two-Party key exchange
WDKVR [4]	X	O	O	X	O	X
SDKR [5]	X	O	X	X	O	X
ZHLC [6]	X	O	O	X	O	X
JBJ [11]	△	O	O	O	X	X
Our scheme	O	O	O	O	O	O

II. CRYPTOGRAPHIC PRIMITIVES

Definition 1: (RoR-CPA Security of Encryption Scheme [15]): We consider a symmetric encryption scheme $\mathsf{SE} = (\mathsf{Key}, \mathsf{E}, \mathsf{D})$. *We suppose that an adversary* $\mathcal{A}$ *can access encryption oracle* $\mathsf{E}_{sk}(RR(\cdot, b))$. *For a requested message* m, $RR(m, 0)$ *returns* m, *and* $RR(m, 1)$ *returns a random string* r.

The real-or-random chosen-plaintext attack (RoR-CPA) security for SE *is defined by the following experiment*:

$$
\begin{aligned}
&EXP^{RoR-b}_{\mathsf{SE},\mathcal{A}}(\theta)\\
&sk \leftarrow \mathsf{Key}(1^{\theta})\\
&b' \leftarrow \mathcal{A}^{\mathsf{E}_{sk}(RR(\cdot,b))}(\theta)
\end{aligned}
$$

The advantage of $\mathcal{A}$ *is defined as* $\mathsf{Adv}^{RoR}_{\mathcal{A}} = \Pr[EXP^{RoR-0}_{\mathsf{SE},\mathcal{A}}(\theta) = 1] - \Pr[EXP^{RoR-1}_{\mathsf{SE},\mathcal{A}}(\theta) = 1]$, *where* θ *is a security parameter.*

SE *is RoR-CPA secure if the advantage of any probabilistic polynomial-time adversary* $\mathcal{A}$ *is* $1/2 + \epsilon(\theta)$, *where* $\epsilon(\theta)$ *is a negligible function.*

Definition 2 (SUF security of MAC [16]): We consider a message authentication scheme (MAC) $\mathsf{Mac} = (\mathsf{KeyGen}, \mathsf{Mac}, \mathsf{Vrfy})$. *To define SUF security for* Mac, *we suppose an adversary* $\mathcal{F}$ *that can access MAC generation oracle* $\mathsf{Mac}_{mk}(\cdot)$ *and MAC verification oracle* $\mathsf{Vrfy}_{mk}(\cdot,\cdot)$. *Then, SUF security is defined by the following experiment*:

$$
\begin{aligned}
&EXP^{SUF}_{\mathsf{Mac},\mathcal{F}}(\theta)\\
&mk \leftarrow \mathsf{KeyGen}(1^{\theta})\\
&(m, \tau) \leftarrow \mathcal{F}^{\mathsf{Mac}_{mk}(\cdot),\mathsf{Vrfy}_{mk}(\cdot,\cdot)}(\theta)
\end{aligned}
$$

$\mathcal{F}$ can access oracles $\mathsf{Mac}_{mk}(\cdot)$ *and* $\mathsf{Vrfy}_{mk}(\cdot)$*, and we define an advantage of $\mathcal{F}$ as follows*:

$$\mathsf{Adv}_{\mathcal{F}}^{SUF} = \Pr[\mathsf{Vrfy}_{mk}(m,\tau) = 1 \text{ and } (m,\tau) \text{ is not in the set of query-response pairs}].$$

A Mac *is SUF secure if the advantage of any probabilistic polynomial-time adversary $\mathcal{F}$ is negligible in terms of the security parameter θ.*

In the following assumption, $\mathbb{G}$ is a cyclic multiplicative group of order q, where q is a θ-bit long prime. We assume that there are efficient algorithms to perform multiplication and membership tests in $\mathbb{G}$. Finally, we denote with g a generator of $\mathbb{G}$.

Assumption 1 (Decisional Diffie-Hellman [17]): For our study, we say that the Decisional Diffie-Hellman (DDH) Assumption (for $\mathbb{G}$ and g) holds, if for any probabilistic polynomial time adversary $\mathcal{A}$, $|\Pr[\mathcal{A}(\mathbb{G}, g, U_1, U_2, W) = 1| u_1, u_2 \leftarrow [1,q], U_1 = g^{u_1}, U_2 = g^{u_2}, W = g^{u_1u_2}] - \Pr[\mathcal{A}(\mathbb{G}, g, U_1, U_2, W) = 1 | u_1, u_2, w \leftarrow [1,q], U_1 = g^{u_1}, U_2 = g^{u_2}, W = g^{w}]|$ *is negligible in θ.*

III. SECURITY MODEL

In this section, we provide the formal security models for forward secrecy and forward unlinkability. Our formal security models are modeling various attacks including drone capturing attacks and compromised user device attacks.

Forward Secrecy [11]. The forward secrecy of a key exchange protocol is defined by an experiment. In the experiment, an adversary $\mathcal{A}$ asks Initiate, Execute, Send, Reveal, Corrupt, and Test queries, and it receives the messages according to the protocol description. We assume that U_i denotes users and D_j as drones, where $i \in [1,n]$ and $j \in [1,m]$. Each entity P_i, where $P_i \in \{U_i, D_j\}$, may have multiple instances.

- An $\mathsf{Initiate}(P_i,k)$ query is used to instigate a key agreement protocol, where $P_i \in \{U_i, D_j\}$. P_i returns the first message as its response according to the protocol description.
- A $\mathsf{Execute}(P_i,P_j)$ query is used to execute a key exchange protocol between party P_i and P_j, where $P_i, P_j \in \{U_i, D_j\}$. As the result of this query, the adversary receives the protocol messages between P_i and P_j. This query could be used to model the passive eavesdropping attacks.
- A $\mathsf{Send}(P_i,k,m)$ query is used to send message m to party P_i's k-th instance, where $P_i \in \{U_i, D_j\}$. After receiving m, P_i returns a message as its response according to the protocol description.
- A $\mathsf{Reveal}(P_i,k)$ query is used to get a session key made in party P_i's k-th instance, where $P_i \in \{U_i, D_j\}$.
- A $\mathsf{Corrupt}(P_i)$ query is used to get the long-term secret key of party P_i, where $P_i \in \{U_i, D_j\}$. P_i returns its long-term secret key as its response.
- A $\mathsf{Corrupt}(KGC)$ query is used to get the master secret key of KGC(Key Generation Center) in the ID-based key exchange scheme. KGC returns its master secret key as its response.
- A $\mathsf{Test}(P_i,k)$ query is used to define the advantage of an adversary, where $P_i \in \{U_i, D_j\}$. P_i flips a coin $\sigma \in \{0,1\}$. If $\sigma = 1$, P_i returns a real session key of the k-th instance. Otherwise, P_i returns a random value. We note that this query is valid only when the k-th instance of P_i is *fresh* (defined below).

The k-th session of party P_i, $P_i \in \{U_i, D_j\}$, is *fresh* if the following conditions hold:

1) $\mathsf{Corrupt}(P_i)$ and $\mathsf{Corrupt}(P_j)$ have not been asked if the k-th session of party P_i is communicating with P_j, where $P_j \in \{U_i, D_j\}$.
2) $\mathsf{Reveal}(P_i,k)$ has not been asked.
3) $\mathsf{Reveal}(P_j,k)$ has not been asked if P_i and P_j calculated the same session key, where $P_j \in \{U_i, D_j\}$.

To terminate the experiment, the adversary $\mathcal{A}$ outputs σ' to guess σ and stops. The advantage of $\mathcal{A}$ is defined by $\mathsf{Adv}_{\mathsf{KE},\mathcal{A}}^{FS} = Pr[\sigma = \sigma']$. A key agreement protocol is "forward secure" if the advantage of any probabilistic polynomial-time adversary $\mathcal{A}$ is $1/2 + \epsilon(\theta)$ in the security parameter θ, where $\epsilon(\theta)$ is a negligible function.

Forward Unlinkability. The forward unlinkability of a key exchange protocol is defined by the following experiment. In the experiment an adversary $\mathcal{A}$ can query a corrupt query to any party to get a long-term secret key.

$$\begin{aligned}
&EXP_{\mathsf{KE},\mathcal{A}}^{FU}(\theta)\\
&((P_i,P_j),(P_k,P_\ell)) \leftarrow \mathcal{A}^{\mathsf{Corrupt}(\cdot)}(\theta)\\
&t \leftarrow \mathsf{Execute}(P_i,P_j)\\
&t_0 \leftarrow \mathsf{Execute}(P_i,P_j)\\
&t_1 \leftarrow \mathsf{Execute}(P_k,P_\ell)\\
&\sigma \leftarrow \{0,1\}\\
&\sigma' \leftarrow \mathcal{A}^{\mathsf{Corrupt}(\cdot)}(t,t_b)
\end{aligned}$$

The advantage of $\mathcal{A}$ is defined as $\mathsf{Adv}_{\mathsf{KE},\mathcal{A}}^{FU} = \Pr[\sigma = \sigma']$.

KE provides "forward unlinkability", if the advantage of any probabilistic polynomial-time adversary $\mathcal{A}$ is $1/2+\epsilon(\theta)$, where $\epsilon(\theta)$ is a negligible function.

IV. OUR ID-BASED KEY EXCHANGE PROTOCOL

In this section, we outline our key exchange protocol, which requires a registration protocol.

All protocols throughout this paper are explained using the following common notations.

- U_i: a user
- D_i: a drone
- ID_i: ID_i denotes the identity of the i-th user U_i or drone D_i.
- PID_i: PID_i denotes a pseudonym for U_i or D_i.
- r_{ID_i}: This is the additional value necessary to prove the validity of ID_i.
- s_{ID_i}: This is the private key of U_i or D_i.
- $ek_{i,j}$: This is the ephemeral encryption key between U_i and D_j.

- $mk_{i,j}$: This is the ephemeral MAC key between U_i and D_j.
- $sk_{i,j}$: This is the session key between U_i and D_j.

A. PROTOCOL SETUP [13]

The Key Generation Center (KGC) chooses a group $\mathbb{G}$ of prime order q (where q is θ-bits long), a random generator $g \in \mathbb{G}$ and two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_2 : \{0,1\}^* \rightarrow \{0,1\}^\theta$. Then it picks a random $x \leftarrow \mathbb{Z}_q$ and sets $y = g^x$. Finally the KGC outputs the public parameters $MPK = (\mathbb{G}, g, y, H_1, H_2)$ and keeps the master secret key $MSK = x$ for itself.

B. KEY DERIVATION PROTOCOL [13]

In the key derivation protocols, the key generation center KGC creates r_{ID_i} and s_{ID_i} for U_i (or D_i). This protocol assumes that there is a secure channel between U_i (or D_i) and KGC.

U_i (or D_i) and KGC proceed as follows (see Fig. 1):

1) U_i (or D_i) selects an identity ID_i. U_i (or D_i) sends ID_i to KGC.
2) After receiving ID_i, KGC picks a random $k \leftarrow Z_q$ and sets $r_{ID_i} = g^k$. Then KGC uses the master secret key x to compute $s_{ID_i} = k + H_1(ID, r_{ID_i})x$. (r_{ID_i}, s_{ID_i}) is the secret key returned to U_i (or D_i).
3) U_i (or D_i) can verify the correctness of its secret key by using the public key $y = g^x$ and checking the equation $g^{s_{ID_i}} = r_{ID_i} y^{H_1(ID_i, r_{ID_i})}$.

C. OUR KEY EXCHANGE PROTOCOL

Our key exchange protocol makes a session key between U_i and D_j as shown in Fig. 2.

1) To being a protocol, U_i select a random $r_i \leftarrow Z_q$ and first sends $PID_i = g^{r_i}$ to D_j.
2) After receiving PID_i, D_j select a random $r_j \leftarrow Z_q$ and calculates $PID_j = g^{r_j}$. Then D_j calculates encryption key $ek_{i,j} = H_2(PID_i||PID_j||g^{r_i r_j}||0)$ and MAC key $mk_{i,j} = H_2(PID_i||PID_j||g^{r_i r_j}||1)$. D_j makes ciphertext $c_j = \mathsf{E}_{ek_{i,j}}(ID_j||r_{ID_j}||y_j)$ and MAC value $\tau_j = \mathsf{Mac}_{mk_{i,j}}(PID_j||PID_i||c_j)$. Then D_j sends $PID_j||PID_i||c_j||\tau_j$ to D_j.
3) After receiving $PID_j||PID_i||c_j||\tau_j$, U_i calculates encryption key $ek_{i,j} = H_2(PID_i||PID_j||g^{r_i r_j}||0)$ and MAC key $mk_{i,j} = H_2(PID_i||PID_j||g^{r_i r_j}||1)$. U_i makes ciphertext $c_i = \mathsf{E}_{ek_{i,j}}(ID_i||r_{ID_i}||y_i)$ and MAC value $\tau_i = \mathsf{Mac}_{mk_{i,j}}(PID_i||PID_j||c_i)$. Then U_i sends $PU_i||PU_j||c_i||\tau_i$ to D_j. And U_i decrypts c_j and obtains $ID_j||r_{ID_j}||y_j$. If $\mathsf{Vrfy}_{mk_{i,j}}(PID_j||PID_i||c_j, \tau_j) = 1$ and $y_j = r_{ID_j} y^{H_1(ID_j, r_{ID_j})}$, U_i calculates the session key $sk_{i,j} = H_2(PID_i||PID_j||g^{s_{ID_i} s_{ID_j}}||g^{r_i r_j})$.
4) After receiving $PU_i||PU_j||c_i||\tau_i$, D_j decrypts c_i and obtains $ID_i||r_{ID_i}||y_i$. If $\mathsf{Vrfy}_{mk_{i,j}}(PID_i||PID_j||c_i, \tau_i) = 1$ and $y_i = r_{ID_i} y^{H_1(ID_i, r_{ID_i})}$, D_j calculates the session key $sk_{i,j} = H_2(PID_i||PID_j||g^{s_{ID_i} s_{ID_j}}||g^{r_i r_j})$.

V. SECURITY AND EFFICIENCY ANALYSES

A. FORWARD SECRECY

Theorem 1. Our key exchange protocol is forward-secure in the random oracle model, if Mac is SUF-secure.

Proof: Let $\mathcal{A}$ be a polynomial-time adversary against the forward secrecy of the key exchange protocol. Then, we show that $\mathcal{A}$'s the advantage is bounded as follows:

$$\mathsf{Adv}^{FS}_{\mathsf{KE},\mathcal{A}}(\theta, q_s) \leq \frac{1}{2} + 2q_s \cdot \mathsf{Adv}^{DDH} + q_s \cdot \mathsf{Adv}^{SUF},$$

where q_s is the number of sessions, and θ is a security parameter.

$\mathcal{A}$'s advantage is from the following two cases:

Case 1. There are forged MACs with respect to τ made by $\mathcal{A}$.

Case 2. There is no forged MAC with respect to τ.

To make the upper bound of the advantage from the above cases, we define the following games:

- game_0: game_0 is the original game defined in the experiment for the key exchange protocol.
- game_1: game_1 is the same as game_0 except that in the first session $g^{r_i r_j}$ in $ek_{i,j}$, $mk_{i,j}$, and $sk_{i,j}$ is replaced by random g^{w_1}.

  ⋮
- game_k: game_k is the same as game_{k-1} except that in the k-th session $g^{r_i r_j}$ in $ek_{i,j}$, $mk_{i,j}$, and $sk_{i,j}$ is replaced by random g^{w_k}.

  ⋮
- game_{q_s}: game_{q_s} is the same as game_{q_s-1} except in the q_s-th session $g^{r_i r_j}$ in $ek_{i,j}$, $mk_{i,j}$, and $sk_{i,j}$ is replaced by random $g^{w_{q_s}}$.

We bound the advantage from each case in the following lemmas.

Lemma 1. The difference of advantage between the two adjacent games is bounded as $\mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_{k-1}} - \mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_k} \leq \mathsf{Adv}^{DDH}$.

Lemma 2. The advantage from Case 1 in game_{q_s} is bounded as $\mathsf{Adv}^{FS,Case\ 1}_{\mathcal{A},\mathsf{game}_{q_s}} \leq q_s \cdot \mathsf{Adv}^{SUF}$.

Lemma 3. The advantage from Case 2 in game_{q_s} is bounded as $\mathsf{Adv}^{FS,Case\ 2}_{\mathcal{A},\mathsf{game}_{q_s}} \leq \frac{1}{2}$.

Therefore, by the hybrid argument the advantage of $\mathcal{A}$ is bounded as follows:

$$\begin{aligned}\mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_0} &= q_s \cdot \mathsf{Adv}^{DDH} + \mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_{q_s}} \\ &= q_s \cdot \mathsf{Adv}^{DDH} + \mathsf{Adv}^{FS,Case\ 1}_{\mathcal{A},\mathsf{game}_{q_s}} + \mathsf{Adv}^{FS,Case\ 2}_{\mathcal{A},\mathsf{game}_{q_s}} \\ &\leq q_s \cdot (\mathsf{Adv}^{SUF} + \mathsf{Adv}^{DDH}) + \frac{1}{2}.\end{aligned}$$

Next, we prove the above three lemmas.

Proof of Lemma 1: Let game_{k-1} and game_k be two adjacent games. We can construct distinguisher $\mathcal{H}$ which breaks the DDH assumption with the advantage difference of $\mathcal{A}$ between game_{k-1} and game_k.

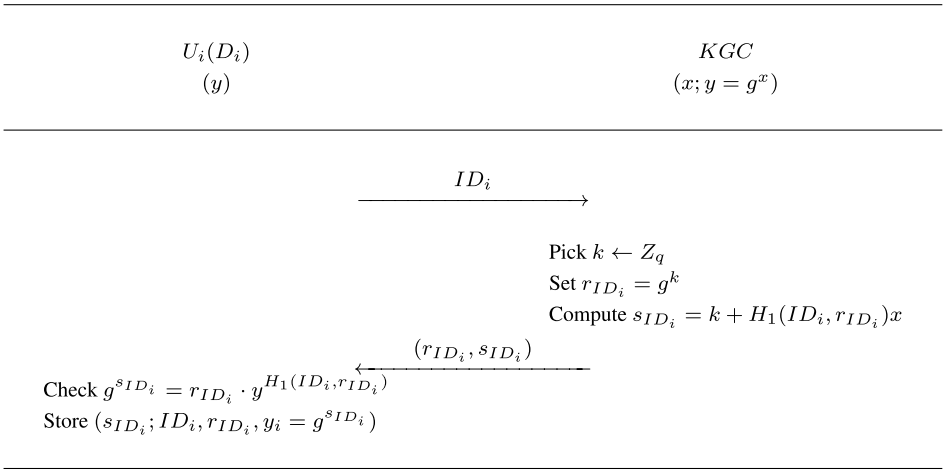

FIGURE 1. User(Drone) key derivation protocol for $U_i(D_i)$.

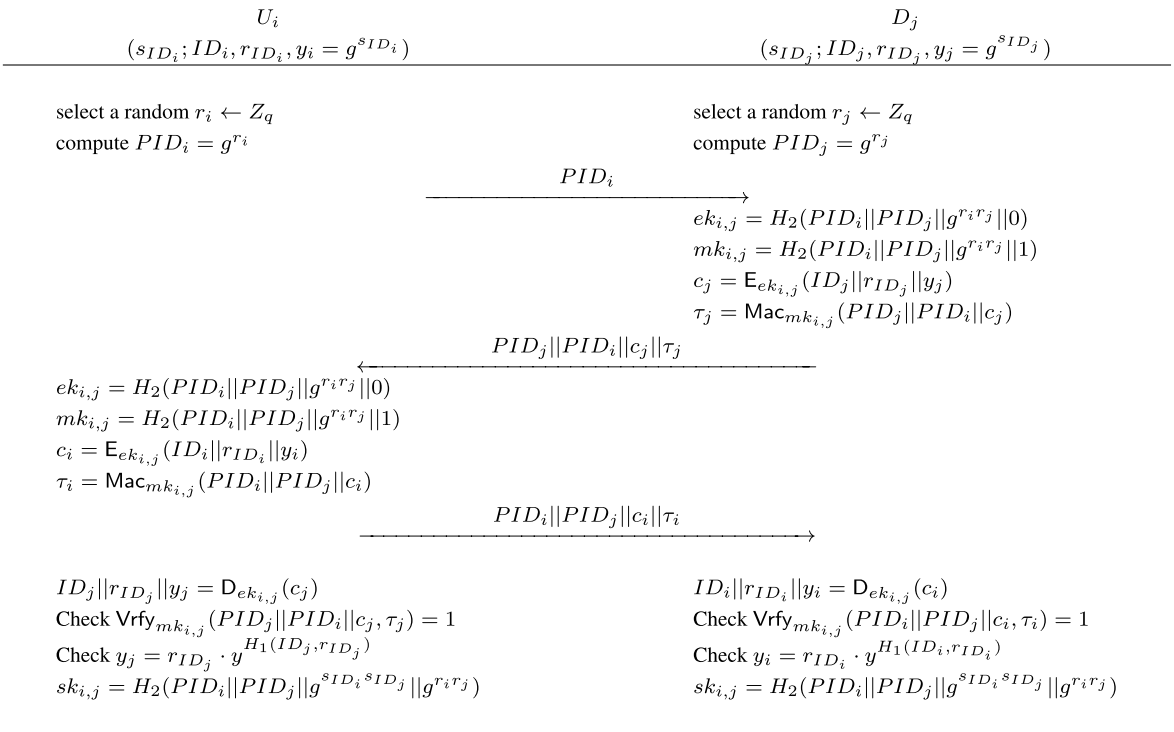

FIGURE 2. Key exchange protocol between user U_i and drone D_j.

$\mathcal{H}$ is given an input (G, q, g, U_1, U_2, W) in the experiment of the DDH problem, and inserts them as the protocol messages in simulating the key exchange protocol to $\mathcal{A}$. The more concrete description of $\mathcal{H}(G, q, g, U_1, U_2, W)$ is as follows:

1) $\mathcal{H}$ is given (G, q, g, U_1, U_2, W). In the k-th session $\mathcal{H}$ uses U_1 and U_2 as the PID_i and PID_j, respectively. $\mathcal{H}$ chooses r_i and r_j for all other sessions normally.
2) In the k-th session $\mathcal{H}$ makes $ek_{i,j} = H_2(PID_i||PID_j||W||0)$, $mk_{i,j} = H_2(PID_i||PID_j||W||1)$, and $sk_{i,j} = H_2(PID_i||PID_j||g^{s_{ID_i} s_{ID_j}}||W)$.
3) When $\mathcal{A}$ stops outputting σ, $\mathcal{H}$ stops outputting σ.

$\mathcal{H}$ simulates game_{k-1} and game_k depending on whether $W = g^{r_i r_j}$ or not, where $U_1 = PID_i$ and $U_2 = PID_j$. So the following inequality holds:

$$\begin{aligned}\mathsf{Adv}_{\mathcal{H}}^{DDH} \geq\ & \Pr[\mathcal{H}(U_1, U_2, W) = 1| \\ & U_1 = g_i^r, U_2 = g^{r_j}, W = g^{r_i r_j}] \\ & - \Pr[\mathcal{H}(U_1, U_2, W) = 1| \\ & U_1 = g^{r_i}, U_2 = g^{r_j}, W = g^w] \\ \geq\ & \Pr[\mathcal{A}() = 1 \text{ in } \mathsf{game}_{k-1}]\end{aligned}$$

$$- \Pr[\mathcal{A}() = 1 \text{ in } \mathsf{game}_k]$$
$$\geq \mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_{k-1}} - \mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_k}.$$

Proof of Lemma 2: If a forged MAC appears in game_{q_s}, we can construct an algorithm $\mathcal{F}$ that breaks the SUF security of the underlying MAC scheme Mac.

$\mathcal{F}$ is given oracles $\mathsf{Mac}_{sk}(\cdot)$ and $\mathsf{Vrfy}(\cdot,\cdot)$ in the MAC scheme experiment, and uses the oracles to make and verify MACs that are supposed to be generated and verified with $mk_{i,j}$, which is randomly selected. A more concrete description of $\mathcal{F}$ is as follows:

1) $\mathcal{F}$ is given oracles $\mathsf{Mac}_{sk}(\cdot)$ and $\mathsf{Vrfy}(\cdot,\cdot)$. $\mathcal{F}$ randomly selects $k^* \leftarrow [1, q_s]$. In the k^*-th session $\mathcal{F}$ uses the oracles instead of MAC key $mk_{i,j}$.
2) If a forged MAC appears with respect to the target instance, $\mathcal{F}$ outputs the forged MAC and message pair and then quits. Otherwise, $\mathcal{F}$ stops when $\mathcal{A}$ stops.

If $\mathcal{F}$ correctly selects k^*, $\mathcal{F}$ does not fail. So the following inequality holds:

$$\mathsf{Adv}^{\mathrm{SUF}}_{\mathcal{F}} \geq \frac{1}{q_s}\Pr[\exists \text{ a forged MAC in } \mathsf{game}_{q_s}]$$
$$\geq \frac{1}{q_s}\mathsf{Adv}^{FS,Case\ 1}_{\mathcal{A},\mathsf{game}_{q_s}}.$$

So Lemma 2 follows.

Proof of Lemma 3: Lemma 3 is obvious from the fact that $\mathcal{A}$ cannot get any information about W used to make a session key $sk_{i,j}$ for the Test session, since W is randomly selected not calculated with $PID_i = g^{r_i}$ and $PID_j = g^{r_j}$. Therefore, $\mathsf{Adv}^{FS,Case\ 2}_{\mathcal{A},\mathsf{game}_{q_s}} = \frac{1}{2}$. □

B. ANONYMITY AND FORWARD UNLINKABILITY

Theorem 2. Our key exchange protocol provides forward unlinkability in the random oracle model if a symmetric encryption scheme SE is RoR-secure.

Proof: Let $\mathcal{A}$ be a polynomial-time adversary against the forward unlinkability of the key exchange protocol. Then, we show that $\mathcal{A}$'s the advantage is bounded as follows:

$$\mathsf{Adv}^{FU}_{\mathsf{KE},\mathcal{A}}(\theta, q_s) \leq \frac{1}{2} + 2\mathsf{Adv}^{DDH} + 2\mathsf{Adv}^{RoR},$$

where θ is a security parameter.

We first define the following games:

- game_0: game_0 is the original game defined in the experiment for the key exchange protocol.
- game_1: game_1 is the same as game_0 except that in the transcript t_0, $g^{r_i r_j}$ in $ek_{i,j}$ and $mk_{i,j}$ is replaced by random g^{w_1}.
- game_2: game_2 is the same as game_1 except that in the transcript t_1, $g^{r_i r_j}$ in $ek_{i,j}$ and $mk_{i,j}$ is replaced by random g^{w_2}.
- game_3: game_3 is the same as game_2 except that in the transcript t_0, plaintexts $ID_i||r_{ID_i}||y_i$ of c_i and $ID_j||r_{ID_j}||y_j$ of c_j are replaced by random $W_{3,i}$ and $W_{3,j}$, respectively.
- game_4: game_4 is the same as game_3 except that in the transcript t_1, plaintexts $ID_i||r_{ID_i}||y_i$ of c_i and $ID_j||r_{ID_j}||y_j$ of c_j are replaced by random $W_{4,i}$ and $W_{4,j}$, respectively.

Lemma 4. The advantage difference between game_{k-1} and game_k, for $1 \leq k \leq 2$, is bounded as $\mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_{k-1}} - \mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_k} \leq \mathsf{Adv}^{DDH}$.

Lemma 5. The advantage difference between game_{k-1} and game_k, for $3 \leq k \leq 4$, is bounded as $\mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_{k-1}} - \mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_k} \leq \mathsf{Adv}^{RoR}$.

Lemma 6. The advantage in game_4 is bounded as $\mathsf{Adv}^{FS}_{\mathcal{A},\mathsf{game}_4} \leq \frac{1}{2}$.

Therefore, by the hybrid argument the advantage of $\mathcal{A}$ is bounded as follows:

$$\mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_0} = 2\mathsf{Adv}^{DDH} + 2\mathsf{Adv}^{RoR} + \mathsf{Adv}_{\mathcal{A}}, \mathsf{game}^{FU}_4$$
$$= 2\mathsf{Adv}^{DDH} + 2\mathsf{Adv}^{RoR} + \frac{1}{2}.$$

Next, we prove the above three lemmas.

Proof of Lemma 4: We omit the proof of this lemma, since the proof of Lemma 4 is the same as that of Lemma 1.

Proof of Lemma 5: We can construct distinguisher $\mathcal{D}$ which breaks the RoR security of the underlying encryption scheme SE with the advantage difference of $\mathcal{A}$ between game_2 and game_3.

$\mathcal{D}$ is given an encryption oracle $\mathsf{E}_{sk}(RR(\cdot, b))$ in the experiment of the RoR experiment, and uses it to make the ciphertexts c_i and c_j of the transcripts t_0 in simulating the key exchange protocol to $\mathcal{A}$. The more concrete description of $\mathcal{D}$ is as follows:

1) $\mathcal{D}$ is given an encryption oracle $\mathsf{E}_{sk}(RR(\cdot, b))$.
2) $\mathcal{D}$ makes $c_i = \mathsf{E}_{sk}(RR(ID_i||r_{ID_i}||y_i), b)$ and $c_j = \mathsf{E}_{sk}(RR(ID_j||r_{ID_j}||y_j), b)$ using the encryption oracle.
3) When $\mathcal{A}$ stops outputting σ, $\mathcal{D}$ stops outputting σ.

$\mathcal{D}$ simulates game_2 or game_3 depending on whether $b = 0$ or $b = 1$. So the following inequality holds:

$$\mathsf{Adv}^{RoR}_{\mathcal{D}} \geq \Pr[\mathcal{D}^{\mathsf{E}_{sk}(RR(\cdot,0))}() = 1] - \Pr[\mathcal{D}^{\mathsf{E}_{sk}(RR(\cdot,1))}() = 1]$$
$$\geq \Pr[\mathcal{A}() = 1 \text{ in } \mathsf{game}_2] - \Pr[\mathcal{A}() = 1 \text{ in } \mathsf{game}_3]$$
$$\geq \mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_2} - \mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_3}.$$

Similarly, we can construct distinguisher $\mathcal{D}'$ which breaks the RoR security of the underlying encryption scheme SE with the advantage difference of $\mathcal{A}$ between game_3 and game_4 by making the ciphertexts c_i and c_j of the transcripts t_1.

Proof of Lemma 6: In game_6 $\mathcal{A}$ cannot get any information about the identity information of the communicating parties, since all the identity information of the communicating parties is replaced by random strings. Therefore, $\mathsf{Adv}^{FU}_{\mathcal{A},\mathsf{game}_4} = \frac{1}{2}$. □

C. EFFICIENCY

In Table 2, we analyzed the number of rounds, the total size of messages, and the total computations with respect to a user and a drone among the related key exchange protocols.

TABLE 2. Efficiency comparison among relevant protocols.

Schemes	Num. of rounds	Total size of transmitted messages			Total computations		
		User	Drone	Server	User	Drone	Server
WDKVR [4]	3	$4\ell_h + \ell_m$	$3\ell_h + \ell_m$	$3\ell_h + \ell_m$	$16t_h + t_b$	$7t_h$	$8t_h$
SDKR [5]	3	$4\ell_h + \ell_m$	$2\ell_h + \ell_m$	$3\ell_h + \ell_m$	$14t_h + t_b$	$7t_h$	$9t_h$
ZHLC [6]	3	$4\ell_h + \ell_m$	$2\ell_h$	$3\ell_h$	$10t_h$	$7t_h$	$7t_h$
JBJ [11]	6	$2\ell_h + \ell_e + 4\ell_m$	$\ell_h + \ell_e + 3\ell_m$	$2\ell_h + 2\ell_e + 4\ell_m$	$8t_h + 4t_e$	$7t_h + 2t_e$	$8t_h + 4t_e$
Our schemes	3	$\ell_h + \ell_e + 3\ell_m$	$\ell_h + \ell_e + 3\ell_m$	–	$6t_h + 2t_e + t_m + 4t_{ex}$	$6t_h + 2t_e + t_m + 4t_{ex}$	–

ℓ_h (length of a hash value), ℓ_m (length of a message (e.g. ID, timestamp, etc.)), ℓ_e (length of a ciphertext), t_h (time for a hash function), t_s (time for modular squaring), t_b (time for a biometric fuzzy extractor or BioHashing), t_m (time for ECC multiplication), t_e (time for symmetric encryption/decryption), t_{ex} (time for exponentiation)

VI. CONCLUSION

In this paper, we proposed an authenticated key exchange protocol between drones and users in the IoD environment. Our key exchange protocol can be initiated by either a user or a drone and establishes a session key between the user and the drone without involvement of the server.

Our key exchange protocol provides both forward secrecy and forward unlinkability for users and drones in the formal security model. Moreover, in our protocol a party can run several sessions concurrently.

The security of our key exchange protocol is based on the decisional Diffie-Hellman assumption. As a future work, it would be interesting to make a key exchange protocol providing forward secrecy and forward unlinkability based on the weaker assumptions.

REFERENCES

[1] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.
[2] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, T. R. Gadekallu, and G. Srivastava, "SP2F: A secured privacy-preserving framework for smart agricultural unmanned aerial vehicles," *Comput. Netw.*, vol. 187, Mar. 2021, Art. no. 107819.
[3] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 218–223, Aug. 2017.
[4] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[5] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[6] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.
[7] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021.
[8] B. Sharma, G. Srivastava, and J. C.-W. Lin, "A bidirectional congestion control transport protocol for the Internet of Drones," *Comput. Commun.*, vol. 153, pp. 102–116, Mar. 2020.
[9] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020.
[10] S. U. Jan, I. A. Abbasi, and F. Algarni, "A key agreement scheme for IoD deployment civilian drone," *IEEE Access*, vol. 9, pp. 149311–149321, 2021.
[11] J. Y. Jeong, J. W. Byun, and I. R. Jeong, "Key agreement between user and drone with forward unlinkability in Internet of Drones," *IEEE Access*, vol. 10, pp. 17134–17144, 2022.
[12] M. Wazid, A. K. Das, and J.-H. Lee, "Authentication protocols for the Internet of Drones: Taxonomy, analysis and future directions," *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Aug. 2018.
[13] D. Fiore and R. Gennaro, "Identity-based key exchange protocols without pairings," in *Transactions on Computational Science X*, 2010, pp. 42–77.
[14] I. R. Jeong, J. O. Kwon, and D. H. Lee, "A Diffie–Hellman key exchange protocol without random oracles," in *Proc. CANS*, Dec. 2006, pp. 37–54.
[15] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proc. 38th Annu. Symp. Found. Comput. Sci.*, 1997, pp. 394–403.
[16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*, 2nd ed. 2007.
[17] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

JAE YEOL JEONG received the B.S. degree in mathematics and the M.S. and Ph.D. degrees in information security from Korea University, South Korea, in 2010, 2013, and 2022, respectively. From March 2022 to February 2024, he was a Research Professor with the BK21 Four R and E Center for Cybersecurity, Korea University. Currently, he is a member of the Faculty of the Department of Information Security, Soonchunhyang University, Chungcheongnam, South Korea. His current research interests include biometric security and authenticated key exchange.

HYUNG WOO KANG received the B.S. and M.S. degrees in computer science and the Ph.D. degree in information security from Korea University, South Korea, in 1997, 1999, and 2006, respectively. From January 2000 to September 2006, he was a Senior Engineer with the National Security Research Institute (NSRI), South Korea. From September 2006 to February 2021, he was the Head of the Information Security Team, Financial Supervisory Service (FSS), South Korea. Currently, he is an Advisor of Kim and Chang, Seoul, South Korea. His current research interests include authentication protocol, blockchain, financial security, and personal information protection.

IK RAE JEONG received the B.S. and M.S. degrees in computer science and the Ph.D. degree in information security from Korea University, Seoul, South Korea, in 1998, 2000, and 2004, respectively. From June 2006 to February 2008, he was a Senior Engineer with the Electronics and Telecommunications Research Institute (ETRI), South Korea. Currently, he is a member of the Faculty in the School of Cybersecurity, Korea University. His current research interests include cryptography, theoretical computer science, blockchain, and biometrics.