electronics

MDPI

Article

A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles

Vincent Omollo Nyangaresi [1], Hend Muslim Jasim [2], Keyan Abdul-Aziz Mutlaq [3], Zaid Ameen Abduljabbar [2,4,5,*], Junchao Ma [6,*], Iman Qays Abduljaleel [7] and Dhafer G. Honi [2]

[1] Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya
[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[3] IT and Communication Center, University of Basrah, Basrah 61004, Iraq
[4] Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
[5] Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China
[6] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
[7] Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
* Correspondence: zaid.ameen@uobasrah.edu.iq (Z.A.A.); majunchao@sztu.edu.cn (J.M.)

Abstract: Unmanned aerial vehicles have found applications in fields such as environmental monitoring and the military. Although the collected data in some of these application domains are sensitive, public channels are deployed during the communication process. Therefore, many protocols have been presented to preserve the confidentiality and integrity of the exchanged messages. However, numerous security and performance challenges have been noted in the majority of these protocols. In this paper, an elliptic curve cryptography (ECC) and symmetric key-based protocol is presented. The choice of ECC was informed by its relatively shorter key sizes compared to other asymmetric encryption algorithms such as the Rivest–Shamir–Adleman (RSA) algorithm. Security analysis showed that this protocol provides mutual authentication, session key agreement, untraceability, anonymity, forward key secrecy, backward key secrecy, and biometric privacy. In addition, it is robust against smart card loss, password guessing, known secret session temporary information (KSSTI), privileged insider, side-channeling, impersonation, denial-of-service (DoS), and man-in-the-middle (MitM) attacks. The comparative performance evaluation showed that it has relatively low computation, storage, and communication complexities.

Keywords: UAV; authentication; security; privacy; attacks

check for updates

Citation: Nyangaresi, V.O.; Jasim, H.M.; Mutlaq, K.A.-A.; Abduljabbar, Z.A.; Ma, J.; Abduljaleel, I.Q.; Honi, D.G. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. *Electronics* **2023**, *12*, 3688. https://doi.org/10.3390/electronics12173688

Academic Editor: Dimitra I. Kaklamani

Received: 4 July 2023
Revised: 1 August 2023
Accepted: 25 August 2023
Published: 31 August 2023

1. Introduction

Unmanned aerial vehicles (UAVs), popularly known as drones, are smart machines with Internet of Things (IoT) connections that fly over certain regions to provide numerous real-time services [1]. For instance, they have been extensively deployed in areas such as intelligent transportation systems (ITSs), the detection and collection of environmental data, emergency rescue, autonomous driving, the creation of high-definition maps in real-time, and military applications [2,3]. In UAV-enabled ITSs, car sharing, real-time map creation, and autonomous driving can be facilitated [4]. In the military, surveillance, reconnaissance, intelligence collection, ground strikes, and fire guidance are enabled. As explained in [5,6], UAVs can also be applied in civil aviation, industrial setups, and areas that are dangerous or difficult for humans to reach, such as during earthquake searches and gas leak detection. In some cases, these drones can serve as relay nodes in mobile and wireless sensor network (WSN) communications. The authors of [7] pointed out that UAVs can be considered as extensions of Internet of Vehicle (IoV) communication that can offer aerial interfaces for vehicles. All these applications stem from the various salient UAV features, such as low cost and flexible operation [8].

In some of the above UAV application domains, sensitive data are collected and exchanged with cellular networks as well as other ubiquitous devices [9]. Unfortunately, message exchange across UAV networks is accomplished over public channels [10–12]. This renders these networks susceptible to attacks such as impersonation, session key disclosure, message replays, man-in-the-middle (MitM) attacks, tracking, and eavesdropping [4,13–17]. The deployment of drones in dangerous, remote, and unmonitored regions exposes them to physical capture attacks [3,18]. Upon capture attacks, the security parameters stored in the UAV memory can be retrieved, and hence confidential information can be leaked. This leads to privacy and security violations [19]. It is also possible for these data to be compromised and the drone to be deployed as a weapon by the attacker [20]. In addition, message replays can cause inaccurate information to be transmitted to UAVs, which can cause their collision. Moreover, data breaches and theft are on the rise in UAV and Internet of Drones (IoD) networks [21]. Most of the UAV-assisted IoV protocols depend on local edge infrastructure and are unable to independently execute secure data transmissions [22–25]. Therefore, strong data encryption and mutual authentication should be implemented. However, UAVs are resource-limited in terms of energy, storage, communication, and computing capabilities [9]. As such, they are not able to the handle extensive cryptographic operations required in most of conventional encryption schemes [3].

1.1. Problem Statement and Motivation

UAVs have been deployed in highly sensitive domains such as military surveillance. As such, strong security protection should be accorded to the exchanged messages. Therefore, numerous cryptographic key encryption schemes have been deployed for confidentiality preservation in UAVs. However, the conventional key distribution techniques used in these schemes present some difficulties in dynamic environments where UAVs randomly join and leave the network [26]. Worse still, many UAVs do not have inbuilt authentication mechanisms [27]. There is therefore a need for innovative approaches to securing the UAV communication environment. This may include access control, key management, intrusion detection, user authentication, intrusion prevention, and location and identity privacy [28].

1.2. Contributions

The main contributions of this paper include the following:

- An authentication protocol that leverages symmetric key and elliptic curve cryptography was developed to protect UAV message exchanges.
- A masking technique was deployed to preserve both operator biometric privacy and anonymity.
- Extensive security analysis was carried out to show that our protocol upholds mutual authentication, session key agreement, untraceability, anonymity, forward key secrecy, backward key secrecy, and biometric privacy. In addition, this protocol was demonstrated to be resilient against smart card loss, password guessing, KSSTI, privileged insider, side-channeling, impersonation, DoS, and MitM attacks.
- A performance evaluation was executed to show that the proposed protocol attained a 87.5% improvement in privacy and security provision at relatively low computation, storage, and communication complexities.

The rest of this paper is structured as follows: Section 2 discusses the related work, while Section 3 presents the proposed protocol. Section 4 details the security evaluation of our protocol. This is followed by the performance evaluation in Section 5. Finally, Section 6 concludes the paper and presents future research directions.

2. Related Work

UAV security and privacy has attracted a lot of attention from industry and academia, and hence many schemes have been developed in the recent past. For instance, blockchain-based authentication schemes were presented in [4,29], while a blockchain-based risk management system for drones was introduced in [30]. However, the deployment of blockchain technology incurs high storage, communication, and computation overheads during consensus building [31]. To address this challenge, lightweight authentication schemes were introduced in [3,32–35]. However, the protocol in [33] failed to offer session key agreement and was not robust against de-synchronization attacks. Although the Physically Unclonable Functions (PUFs) used in [3,32] prevent physical capture attacks, PUFs have stability issues [36], while the scheme in [34] was susceptible to drone capture attack [9]. The protocol in [35] was vulnerable to side-channel attacks, which could be employed to retrieve the credentials stored in memory [9]. This problem could be alleviated by the elliptic curve cryptography (ECC) and symmetric key-based protocol developed in [37]. However, this approach incurred high communication and processing overheads [9].

To enhance privacy, authentication schemes were introduced in [38–41]. Unfortunately, the authentication of all drones was centralized in [38], which could present a single point of failure. The scheme in [39] was vulnerable to privileged insider attacks, while the protocol in [40] had high computation costs. Similarly, the certificate-based technique in [41] lacked mutual authentication, and hence the integrity of the communication process was not upheld [42]. Based on symmetric key functions, an authentication scheme was introduced in [43]. However, the usage of the management server's static identity during authentication implied that anonymity was not preserved. In addition, the deployed timestamps were publicly shared, and this could lead to de-synchronization attacks. Although the ECC and blockchain-based protocol in [44] could solve this challenge, the blockchain technology and multiplication operations utilized here resulted in extensive computation costs [45]. Similarly, the robust authentication scheme presented in [46] had high computation costs associated with ECC multiplication operations. In addition, this protocol failed to preserve reliability and anonymity [9].

To provide authentication between UAVs and the vehicles in a UAV-enabled ITS environment, an ECC-based protocol was developed in [47]. Similarly, an ECC-based scheme was introduced in [48]. However, the deployed public key cryptosystem in [47] resulted in high computation overheads [49]. In addition, this scheme failed to authenticate the drone to the roadside unit (RSU). The protocol developed in [48] did not solve privacy leakages [9]. The scheme in [50] was lightweight and could address the performance challenges in [47]. Similarly, the protocol in [51] was anonymous and hence could solve the privacy leak issues in [48]. However, the technique in [50] was not scalable, could only be used within one flying zone, and could not preserve untraceability [3]. In addition, it was susceptible to stolen verifier attacks, which could further facilitate user or drone spoofing [9]. The protocol developed in [52] could potentially solve this problem. However, this scheme did not support re-authentication and was vulnerable to node capture and tampering attacks. In addition, it incurred heavy computation costs [9]. Similarly, the protocol presented in [53] had high computation costs owing to its extensive ECC multiplication operations.

To offer dynamic membership authentication, a trusted authority (TA)-based protocol was introduced in [54]. However, the usage of public-key cryptosystem during mutual authentications resulted in high computation overheads [55]. Similarly, the protocol presented in [56] incurred huge communication and computation costs. In addition, it could not provide traceability or confidentiality and was vulnerable to ephemeral secret leakage attacks [29]. The quadratic residue-based technique presented in [57] could address this issue, although it failed to provide session key agreement and resilience against privileged insider attacks.

It is evident that most of the current techniques for UAVs still have some performance, security, and privacy issues that need to be solved. In addition, the majority of the current techniques deal with user and UAV authentication, ignoring the security issues in mobile sink nodes [58]. The proposed scheme is shown to address some of these security and privacy issues at relatively low complexities.

3. The Proposed Protocol

The network model in our protocol includes a registration authority (RA), UAVs, and their operators, as shown in Figure 1. During the registration process, secure communication channels are deployed. However, public wireless channels are utilized during the subsequent authentication, key agreement, and data exchanges.

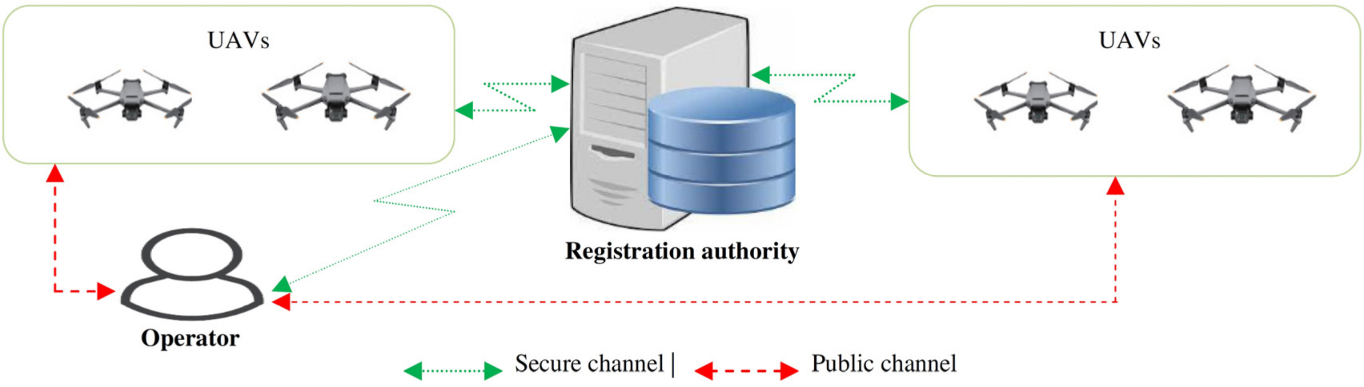


Figure 1. Network model.

In terms of execution phases, the proposed protocol consists of five major phases. These include system initialization, registration, mutual authentication, the session parameter update phase, and the revocation phase. Table 1 presents the symbols used throughout this paper.

Table 1. Symbols.

Symbol	Description
E_X (Z)	Cipher text of message Z with key X
$SS_{K_{RA}}$	Session key shared between RA and operator
C_{AG}	Cyclic additive group of the order *r*
$\mathbb{P}$	The generator of C_{AG}
SK_{RA}	RA secret key
PK_{RA}	RA private key
PUK_{RA}	RA public key
h(.)	Hashing operation
ID_{RA}	RA unique identity
ID_{UAV}	UAV identity
$SS_{K_{UAV}}$	Session key shared between RA and the UAV
R_i	Random numbers
ID_{OP}	UAV operator unique identity
PID_{OP}	UAV operator pseudonym
ID_{SC}	Smart card unique serial number
$SS_{K_{OP}}$	Session key shared between the operator and the UAV
PW_{OP}	UAV operator password
β	Operator biometrics
β_K	Biometrics key

Table 1. *Cont.*

Symbol	Description
V_F	Fuzzy verifier
| |	Concatenation operation
$\oplus$	XOR operation

3.1. System Initialization Phase

During this phase, the registration authority generates and distributes the security tokens that are deployed in the later stages, including mutual authentication and key agreement. This process is depicted in Figure 2 below.

Step 1: To commence this process, the RA generates its unique identity ID_{RA}; channel parameter C_P; and cyclic additive group C_{AG}, whose order is r. This is followed by the selection of SK_{RA} as the secret key, h(.) as the one-way hashing function, $\mathbb{P}$ as the generator of C_{AG}, and PK_{RA} as the private key.
Step 2: Next, the RA computes $PUK_{RA} = \mathbb{P}.PK_{RA}$, followed by the publication of parameter $\{\mathbb{P}, PK_{RA}, h(.)\}$. Here, $\mathbb{P}$, SK_{RA}, $PK_{RA} \subseteq Z_r^*$, h: $[0, 1]^* \rightarrow [0, 1]^n$; C_P is an integer gauging the fuzzy verifier's robustness against online guessing attacks; and n is h(.)'s output length.

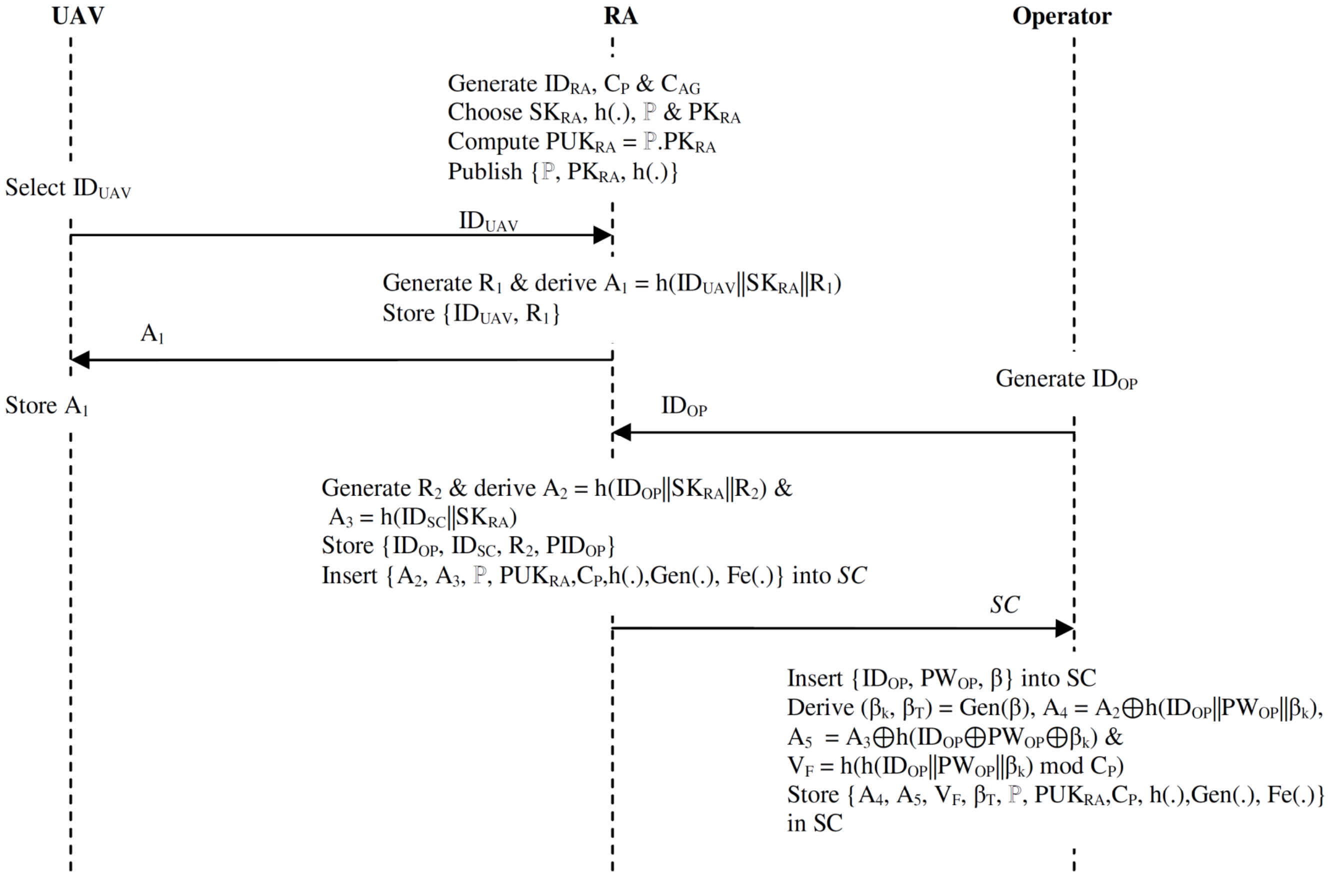

UAV
RA
Operator
Generate ID_{RA}, C_P & C_{AG}
Choose SK_{RA}, h(.), $\mathbb{P}$ & PK_{RA}
Compute $PUK_{RA} = \mathbb{P}.PK_{RA}$
Publish $\{\mathbb{P}, PK_{RA}, h(.)\}$
Select ID_{UAV}
ID_{UAV}
Generate R_1 & derive $A_1 = h(ID_{UAV}||SK_{RA}||R_1)$
Store $\{ID_{UAV}, R_1\}$
A_1
Store A_1
Generate ID_{OP}
ID_{OP}
Generate R_2 & derive $A_2 = h(ID_{OP}||SK_{RA}||R_2)$ &
$A_3 = h(ID_{SC}||SK_{RA})$
Store $\{ID_{OP}, ID_{SC}, R_2, PID_{OP}\}$
Insert $\{A_2, A_3, \mathbb{P}, PUK_{RA}, C_P, h(.), Gen(.), Fe(.)\}$ into *SC*
SC
Insert $\{ID_{OP}, PW_{OP}, \beta\}$ into SC
Derive $(\beta_k, \beta_T) = Gen(\beta)$, $A_4 = A_2 \oplus h(ID_{OP}||PW_{OP}||\beta_k)$,
$A_5 = A_3 \oplus h(ID_{OP} \oplus PW_{OP} \oplus \beta_k)$ &
$V_F = h(h(ID_{OP}||PW_{OP}||\beta_k) \bmod C_P)$
Store $\{A_4, A_5, V_F, \beta_T, \mathbb{P}, PUK_{RA}, C_P, h(.), Gen(.), Fe(.)\}$
in SC

Figure 2. System initialization and registration phases.

3.2. Registration Phase

Before the UAVs and operators can start the communication process, they have to be registered at the RA. In this phase, the registration authority generates and forwards a secret key for each UAV. On the other hand, the RA stores the operator secret keys in the smart card (SC) before issuing this card to the UAV operator.

Step 1: During UAV registration, the UAV chooses its identity ID_{UAV}, which is then sent to the RA through certain secure channels, as shown in Figure 2.
Step 2: Upon receiving identity ID_{UAV}, the RA generates random number R_1, which it utilizes to derive $A_1 = h(ID_{UAV} || SK_{RA} || R_1)$. It then stores parameter set $\{ID_{UAV}, R_1\}$ in its database. Finally, it securely transmits $\{A_1\}$ to the UAV, which in turn stores it securely in its memory.
Step 3: During UAV operator registration, each operator generates a unique identity ID_{OP} and sends it to the RA through certain secure channels.
Step 4: On receiving ID_{OP} from the operator, the RA generates random number R_2 before deriving $A_2 = h(ID_{OP} || SK_{RA} || R_2)$ and $A_3 = h(ID_{SC} || SK_{RA})$. Next, it stores parameter set $\{ID_{OP}, ID_{SC}, R_2, PID_{OP}\}$ in its database. Finally, the RA inserts parameters $\{A_2, A_3, \mathbb{P}, PUK_{RA}, C_P$, h(.),Gen(.), Fe(.)} into the smart card before securely delivering this card to the operator.
Step 5: Upon receiving the smart card, the operator inputs parameter set $\{ID_{OP}, PW_{OP}, \beta\}$ to the smart card reader, at which point the biometric key and template algorithms are invoked, deriving $(\beta_k, \beta_T) = Gen(\beta)$, $A_4 = A_2 \oplus h(ID_{OP} || PW_{OP} || \beta_k)$, $A_5 = A_3 \oplus h(ID_{OP} \oplus PW_{OP} \oplus \beta_k)$ and fuzzy verifier $V_F = h(h(ID_{OP} || PW_{OP} || \beta_k) \bmod C_P)$. Lastly, the user stores $\{A_4, A_5, V_F, \beta_T, \mathbb{P}, PUK_{RA}, C_P$, h(.),Gen(.), Fe(.)} in the smart card.

3.3. Mutual Authentication and Key Negotiation Phase

During this phase, the operator identity is validated so as to establish several secure channels between the RA, UAV, and operator. This is a seven-step process, as described below and depicted in Figure 3.

Step 1: To access the UAV network, the operator inserts the smart card into the reader, at which point the security parameters $\{ID_{OP}^*, PW_{OP}^*, \beta^*\}$ are input. Thereafter, the SC derives $\beta_k^* = Gen\ (\beta_T, \beta^*)$, $V_F^* = h(h(ID_{OP}^* || PW_{OP}^* || \beta_k^*) \bmod C_P)$. It then checks if $V_F^* \overset{?}{=} V_F$ such that the session is terminated when these two values are not equivalent. Otherwise, it computes parameters $A_2 = A_2 \oplus h(ID_{OP}^* || PW_{OP}^* || \beta_k^*)$ and $A_3 = A_5 \oplus h(ID_{OP}^* \oplus PW_{OP}^* \oplus \beta_k^*)$.
Step 2: Next, it generates random number $R_3 \subseteq Z_r^*$ and secret key S_{K_1} before computing security parameters $B_1 = (R_3.\mathbb{P})$, $B_2 = h(B_1 || ID_{OP} || ID_{RA})$, $B_3 = (A_2\mathbb{P} + B_1B_2)$, $B_4 = E_{PUK_{RA}}(A_2 + R_3B_2)$, $B_5 = h(ID_{OP} || A_2 || A_3 || S_{K_1})$, $C_1 = h(B_4 || B_3 || ID_{RA})$, and $C_2 = E_{C_1}(ID_{OP} || B_1 || B_5 || ID_{UAV})$. Finally, the operator composes message $M_1 = \{B_3, C_2, S_{K_1}\}$, which it transmits to the RA over public channels.
Step 3: Upon receiving message M_1 from the operator, the RA derives $B_4 = PK_{RA}B_3$ and $C_1 = h(B_4 || B_3 || ID_{RA})$. It then deploys the just computed C_1 to decipher C_2 and obtain parameter set $\{ID_{OP}, B_1, B_5$, and $ID_{UAV}\}$. Next, it retrieves the ID_{SC} and R_2 corresponding to the obtained ID_{OP}. Thereafter, it derives $A_2 = h(ID_{OP} || SK_{RA} || R_2)$, $A_3 = h(ID_{SC} || SK_{RA})$, $B_2 = h(B_1 || ID_{OP} || ID_{RA})$, $B_5^* = h(ID_{OP} || A_2 || A_3 || S_{K_1})$, and $B_3^* = (A_2.\mathbb{P} + B_1.B_2)$. It then checks if $B_5^* \overset{?}{=} B_5$ and $B_3^* \overset{?}{=} B_3$ such that it rejects the authentication request and terminates the session. Otherwise, it accepts the operator as a legitimate entity.
Step 4: The RA generates random number $R_4 \subseteq Z_r^*$ and secret key S_{K_2}, followed by the computation of security parameters $C_3 = (R_4.\mathbb{P})$ and $C_4 = (R_4.B_1)$ and session key $SS_{K_{RA}} = h(ID_{OP} || ID_{RA} || B_1 || C_3 || C_1 || A_2 || C_4)$, which its shares with the operator. Next, the RA retrieves the R_1 corresponding to this particular ID_{UAV} followed by the derivation of secret tokens $A_1 = h(ID_{UAV} || SK_{RA} || R_1)$ and $C_5 = h(ID_{OP} || ID_{UAV} || ID_{RA} || C_4 || S_{K_2})$. Next, the RA computes $D_1 = E_{A_1}(ID_{OP} || ID_{UAV} || ID_{RA} || C_5 || S_{K_1} || S_{K_2})$ and $D_2 = h(ID_{OP} || ID_{UAV} || ID_{RA} || C_5 || S_{K_1} || S_{K_2} || A_1)$. Finally, it constructs message $M_2 = \{D_1, D_2\}$, which is then sent to the UAV over insecure channels.
Step 5: After receiving message M_2 from the RA, the UAV decrypts security parameter D_1 using its secret key A_1. This is followed by the derivation of parameters $D_2^* = h(ID_{OP} || ID_{UAV} || ID_{RA} || C_5 || S_{K_1} || S_{K_2} || A_1)$. It then checks if $D_2^* \overset{?}{=} D_2$ such that the session is terminated when these two values are dissimilar. Otherwise, the UAV generates random number $R_5 \subseteq Z_r^*$ before computing session key $SS_{K_{UAV}} = h(ID_{UAV} || ID_{RA} || S_{K_2} || R_5 |$

$|A_1$), which it shares with the RA. Next, it derives session key $SS_{K_{OP}}$ = h ($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||R_5$), which it shares with the operator. This is followed by the derivation of D_3 = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_2}||R_5||A_1$) before constructing message M_3 = {R_5, D_3}, which is transmitted over to the RA.

Step 6: Upon receiving message M_3, the RA derives D_3* = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_2}||R_5||A_1$), which it deploys to validate the UAV's identity. As such, it checks if $D_3^* \overset{?}{=} D_3$ such that the session is terminated if the two parameters are not identical. Otherwise, it computes $SS_{K_{UAV}}$ = h($ID_{UAV}||ID_{RA}||S_{K_2}||R_5||A_1$), which is shared with the UAV. This is followed by the derivation of security parameter D_4 = h($ID_{OP}||ID_{RA}||C_3||C_1||A_2||C_4||S_{K_1}||S_{K_2}||R_5$), which is utilized to validate its own identity on the UAV operator side. Finally, it constructs message M_4 = {C_3, D_4, S_{K_2}, R_5}, which it transmits over to the operator.

Step 7: After receiving message M_4 from the RA, the operator computes C_4 = ($R_3.C_3$), D_4* = h($ID_{OP}||ID_{RA}||C_3||C_1||A_2||C_4||S_{K_1}||S_{K_2}||R_5$) to validate the RA's legitimacy. As such, it checks if $D_4^* \overset{?}{=} D_4$ and terminates the session when these two values are dissimilar. Otherwise, it derives security parameter C_5 = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_4||S_{K_2}$); session key $SS_{K_{RA}}$ = h($ID_{OP}||ID_{RA}||B_1||C_3||C_1||A_2||C_4$), which it shares with the RA; and session key $SS_{K_{OP}}$ = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||R_5$).

3.4. Parameter Update Phase

The proposed protocol offers some mechanisms through which the UAV operator may update the deployed biometrics and password. This is crucial, especially if these security parameters are compromised by an adversary. This is a three-step process, as discussed below.

Step 1: The operator inserts the smart card into the card reader and inputs security parameters {ID_{OP}*, PW_{OP}*, β*}. Afterwards, the SC computes β_k* = Fe(β_T, β*), V_F* = h(h(ID_{OP}*$||PW_{OP}$*$||\beta_k$*) mod C_P). Next, it checks whether $V_F^* \overset{?}{=} V_F$ such that the session is terminated if the two values do not match. Otherwise, it derives A_2* = $A_2 \oplus$h(ID_{OP}*$||PW_{OP}$*$||\beta_k$*) and A_3* = $A_5\oplus$h(ID_{OP}*$\oplus PW_{OP}$*$\oplus\beta_k$*).

Step 2: The operator generates a new password PW_{OP}^{New} and inputs new biometrics β^{New}. Upon receiving updated parameters PW_{OP}^{New} and β^{New}, the smart card computes (β_k^{New}, β_T^{New}) = Gen(β^{New}), A_4^{New} = $A_2\oplus$h(ID_{OP}*$||PW_{OP}^{New}||\beta_k^{New}$), A_5^{New} = $A_3\oplus$h(ID_{OP}*$\oplus PW_{OP}^{New}\oplus\beta_k^{New}$), and V_F^{New} = h(h($ID_{OP*}||PW_{OP}^{New}||\beta_k^{New}$) mod C_P).

Step 3: The smart card substitutes security parameters {A_4, A_5, V_F, β_T} with their updated equivalents {A_4^{New}, A_5^{New}, V_F^{New}, β_T^{New}}.

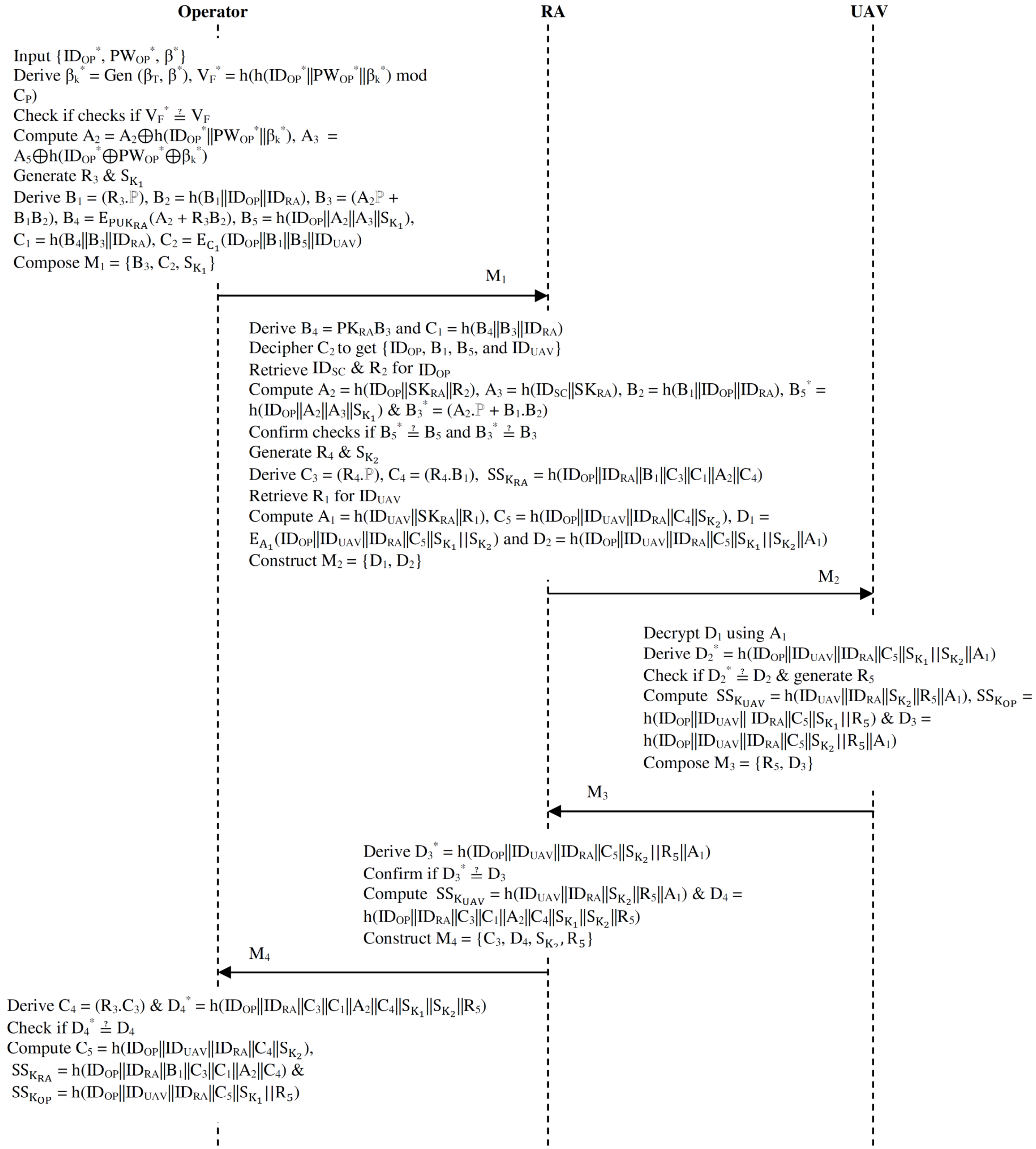
3.5. Smart Card Revocation Phase

This phase is invoked whenever the UAV operator loses the smart card or the security tokens stored in it are compromised in any way.

Step 1: The UAV operator generates new identity ID_{OP}** and pseudonym PID_{OP}**, which are then sent to the RA over secure channels.

Step 2: Upon receiving these operator credentials, the RA validates their authenticity such that the revocation request is rejected if they are invalid. Otherwise, the RA generates random number R_2^{New} and derives parameters A_2 = h(ID_{OP}**$||SK_{RA}||R_2^{New}$) and A_3 = h($ID_{SC}^{New}||SK_{RA}$). Next, the RA substitutes previous security parameter set {ID_{OP}, ID_{SC}, R_2, PID_{OP}} with updated parameter set {ID_{OP}**, ID_{SC}^{New}, R_2^{New}, PID_{OP}**}.

Step 3: After the parameter updates in step 2 above, the operator executes the rest of the registration steps as detailed in the registration phase above.



Input $\{ID_{OP}^{*}, PW_{OP}^{*}, \beta^{*}\}$
Derive $\beta_k^{*} = Gen(\beta_T, \beta^{*})$, $V_F^{*} = h(h(ID_{OP}^{*} \| PW_{OP}^{*} \| \beta_k^{*})\ mod\ C_P)$
Check if checks if $V_F^{*} \overset{?}{=} V_F$
Compute $A_2 = A_2 \oplus h(ID_{OP}^{*} \| PW_{OP}^{*} \| \beta_k^{*})$, $A_3 = A_5 \oplus h(ID_{OP}^{*} \oplus PW_{OP}^{*} \oplus \beta_k^{*})$
Generate R_3 & S_{K_1}
Derive $B_1 = (R_3.\mathbb{P})$, $B_2 = h(B_1 \| ID_{OP} \| ID_{RA})$, $B_3 = (A_2\mathbb{P} + B_1B_2)$, $B_4 = E_{PUK_{RA}}(A_2 + R_3B_2)$, $B_5 = h(ID_{OP} \| A_2 \| A_3 \| S_{K_1})$, $C_1 = h(B_4 \| B_3 \| ID_{RA})$, $C_2 = E_{C_1}(ID_{OP} \| B_1 \| B_5 \| ID_{UAV})$
Compose $M_1 = \{B_3, C_2, S_{K_1}\}$

Derive $B_4 = PK_{RA}B_3$ and $C_1 = h(B_4 \| B_3 \| ID_{RA})$
Decipher C_2 to get $\{ID_{OP}, B_1, B_5$, and $ID_{UAV}\}$
Retrieve ID_{SC} & R_2 for ID_{OP}
Compute $A_2 = h(ID_{OP} \| SK_{RA} \| R_2)$, $A_3 = h(ID_{SC} \| SK_{RA})$, $B_2 = h(B_1 \| ID_{OP} \| ID_{RA})$, $B_5^{*} = h(ID_{OP} \| A_2 \| A_3 \| S_{K_1})$ & $B_3^{*} = (A_2.\mathbb{P} + B_1.B_2)$
Confirm checks if $B_5^{*} \overset{?}{=} B_5$ and $B_3^{*} \overset{?}{=} B_3$
Generate R_4 & S_{K_2}
Derive $C_3 = (R_4.\mathbb{P})$, $C_4 = (R_4.B_1)$, $SS_{K_{RA}} = h(ID_{OP} \| ID_{RA} \| B_1 \| C_3 \| C_1 \| A_2 \| C_4)$
Retrieve R_1 for ID_{UAV}
Compute $A_1 = h(ID_{UAV} \| SK_{RA} \| R_1)$, $C_5 = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_4 \| S_{K_2})$, $D_1 = E_{A_1}(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_1} \| S_{K_2})$ and $D_2 = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_1} \| S_{K_2} \| A_1)$
Construct $M_2 = \{D_1, D_2\}$

Decrypt D_1 using A_1
Derive $D_2^{*} = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_1} \| S_{K_2} \| A_1)$
Check if $D_2^{*} \overset{?}{=} D_2$ & generate R_5
Compute $SS_{K_{UAV}} = h(ID_{UAV} \| ID_{RA} \| S_{K_2} \| R_5 \| A_1)$, $SS_{K_{OP}} = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_1} \| R_5)$ & $D_3 = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_2} \| R_5 \| A_1)$
Compose $M_3 = \{R_5, D_3\}$

Derive $D_3^{*} = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_2} \| R_5 \| A_1)$
Confirm if $D_3^{*} \overset{?}{=} D_3$
Compute $SS_{K_{UAV}} = h(ID_{UAV} \| ID_{RA} \| S_{K_2} \| R_5 \| A_1)$ & $D_4 = h(ID_{OP} \| ID_{RA} \| C_3 \| C_1 \| A_2 \| C_4 \| S_{K_1} \| S_{K_2} \| R_5)$
Construct $M_4 = \{C_3, D_4, S_{K_2}, R_5\}$

Derive $C_4 = (R_3.C_3)$ & $D_4^{*} = h(ID_{OP} \| ID_{RA} \| C_3 \| C_1 \| A_2 \| C_4 \| S_{K_1} \| S_{K_2} \| R_5)$
Check if $D_4^{*} \overset{?}{=} D_4$
Compute $C_5 = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_4 \| S_{K_2})$, $SS_{K_{RA}} = h(ID_{OP} \| ID_{RA} \| B_1 \| C_3 \| C_1 \| A_2 \| C_4)$ & $SS_{K_{OP}} = h(ID_{OP} \| ID_{UAV} \| ID_{RA} \| C_5 \| S_{K_1} \| R_5)$

Figure 3. Authentication and key negogiation phase.

4. Security Evaluation

In this section, a number of theorems are formulated and proved to demonstrate the resilience of the proposed protocol against attacks. A similar approach is followed to illustrate the many salient privacy and security features provided by our scheme.

Theorem 1. *The proposed protocol is robust against smart card loss and side-channeling attacks.*

Proof. Suppose that an adversary wants to mount offline password guessing attacks against the proposed protocol. To achieve this, the security parameters {A_4, A_5, V_F, $\mathbb{P}$, PUK_{RA}, C_P, h(.),Gen(.), Fe(.)} stored in the smart card are extracted. Here, (β_k, β_T) = Gen(β) and $V_F = h(h(ID_{OP}||PW_{OP}||\beta_k) \bmod C_P)$. As such, even if an adversary manages to compromise the smart card and operator biometrics, the operator identity ID_{OP}* and password PW_{OP}* still need to be correctly guessed. Obtaining these security parameters from the fuzzy verifier is difficult due to the one-way hashing operation. Consequently, any bogus identity $ID_{OP}{}^{bogus}$ and password $PW_{OP}{}^{bogus}$ will be detected when the operator checks if $V_F{}^* \overset{?}{=} V_F$, where $V_F{}^* = h(h(ID_{OP}{}^{bogus}||PW_{OP}{}^{bogus}||\beta_k{}^*) \bmod C_P)$. Suppose now that an attacker has captured message M_1 = {B_3, C_2, S_{K_1}} sent from the operator towards the RA. Here, $A_4 = A_2 \oplus h(ID_{OP}||PW_{OP}||\beta_k)$, $A_5 = A_3 \oplus h(ID_{OP} \oplus PW_{OP} \oplus \beta_k)$, $B_3 = (A_2.\mathbb{P} + B_1.B_2)$, and $C_2 = E_{C_1}(ID_{OP}||B_1||B_5||ID_{UAV})$. Using parameters A_4 and A_5 extracted from the smart card, the attacker derives $A_2{}^* = A_4 \oplus h(ID_{OP}{}^*||PW_{OP}{}^*||\beta_k{}^*)$, $A_3{}^* = A_5 \oplus h(ID_{OP}{}^* \oplus PW_{OP}{}^* \oplus \beta_k{}^*)$, and $B_5{}^* = h(ID_{OP}{}^*||A_2{}^*||A_3{}^*||S_{K_1})$. However, based on the elliptic curve computational Diffie–Hellman (ECCDH) difficulty, the attacker is unable to compute $B_5 = h(ID_{OP}||A_2||A_3||S_{K_1})$ from $C_2 = E_{C_1}(ID_{OP}||B_1||B_5||ID_{UAV})$. As such, the adversary is unable to derive B_5, which is required to effectively authenticate ID_{OP}* and PW_{OP}*. □

Theorem 2. *Strong mutual authentication is executed in the proposed scheme.*

Proof. To authenticate the operator, the RA verifies whether $B_5{}^* \overset{?}{=} B_5$ and $B_3{}^* \overset{?}{=} B_3$, where $B_5 = h(ID_{OP}||A_2||A_3||S_{K_1})$ and $B_3 = (A_2.\mathbb{P} + B_1.B_2)$. As such, an entity masquerading as the operator must derive a valid B_3 and B_5. However, an adversary is unable to derive these parameters without the operator identity ID_{OP}, password PW_{OP}, or parameters A_4 and A_5 stored in the smart card. On the other hand, the UAV authenticates the RA through the verification of whether $D_2{}^* \overset{?}{=} D_2$, where $D_2 = h(ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||S_{K_2}||A_1)$. Since security parameter $A_1 = h(ID_{UAV}||SK_{RA}||R_1)$ is only known to the UAV and RA, an attacker is unable to obtain authentication. Similarly, the RA authenticates the UAV by verifying whether $D_3{}^* \overset{?}{=} D_3$, where $D_3 = h(ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_2}||R_5||A_1)$, while the operator authenticates the RA by checking if $D_4 = h(ID_{OP}||ID_{RA}||C_3||C_1||A_2||C_4||S_{K_1}||S_{K_2}||R_5)$. The derivation of a valid D_4 requires secrets SK_{RA} and A_2, among others. Similarly, secrets PK_{RA} and SK_{RA}, which are only known to the RA and the operator, are also required. □

Theorem 3. *The proposed protocol offers UAV operator untraceability.*

Proof. Suppose that an adversary is interested in tracking a particular UAV operator. To achieve this, authentication messages exchanged in the channels must be intercepted. Thereafter, an attempt is made to associate the various communication sessions with the operator. During the authentication phase, messages M_1 = {B_3, C_2, S_{K_1}} and M_4 = {C_3, D_4,S_{K_2}, R_5} both relate to the UAV operator. Here, $B_3 = (A_2.\mathbb{P} + B_1.B_2)$, $B_1 = (R_3.\mathbb{P})$, $C_2 = E_{C_1}(ID_{OP}||B_1||B_5||ID_{UAV})$, $C_3 = (R_4.\mathbb{P})$, and $D_4 = h(ID_{OP}||ID_{RA}||C_3||C_1||A_2||C_4||S_{K_1}||S_{K_2}||R_5)$. Evidently, random numbers R_3, R_4, and R_5 imply that these messages are stochastic and hence session-specific. As such, it is infeasible to associate any two or more sessions with a particular operator. □

Theorem 4. *Online password guessing attacks are curbed in the proposed protocol.*

Proof. During the login phase, the UAV operator inputs password PW_{OP}*, identity ID_{OP}*, and biometrics β*. Afterwards, the fuzzy verifier is derived as $V_F{}^* = h(h(ID_{OP}{}^*||PW_{OP}{}^*||\beta_k{}^*) \bmod C_P)$. The computed verifier is then validated against the fuzzy verifier $V_F = h(h(ID_{OP}||PW_{OP}||\beta_k) \bmod C_P)$ stored in the smart card. As such, any adversarial password guesses are easily detected, and the session is immediately terminated. □

Theorem 5. *The proposed protocol facilitates the negotiation of session keys.*

Proof. During the authentication process, the operator and RA establish a session key $SS_{K_{RA}}$ = h($ID_{OP}||ID_{RA}||B_1||C_3||C_1||A_2||C_4$). Evidently, the derivation of this session key requires secrets C_1, C_4, and A_2, which are only known to the UAV operator and the RA. On the other hand, the session key $SS_{K_{OP}}$ = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||R_5$) is negotiated between the operator and the UAV. The derivation of this session key requires secret C_5, which is only known to the operator and the UAV. Similarly, session key $SS_{K_{UAV}}$ = h($ID_{UAV}||ID_{RA}||S_{K_2}||R_5||A_1$) is established between the UAV and the RA using secret A_1, which is only known to the UAV and the RA. □

Theorem 6. *UAV operator anonymity is upheld in the proposed protocol.*

Proof. Suppose that an attacker is interested in deciphering the operator identity ID_{OP}. To attain this goal, all the messages exchanged between the operator and other entities are captured. For instance, in message M_1 = {B_3, C_2, S_{K_1}}, operator identity is masked and enciphered in C_2 = E_{C_1}($ID_{OP}||B_1||B_5||ID_{UAV}$). As such, to obtain this identity ID_{OP}, an adversary must access secret key C_1 = h($B_4||B_3||ID_{RA}$) to decrypt C_2. Another technique is to deploy the RA's private key PK_{RA} to derive B_4 = $PK_{RA}B_3$. However, this is infeasible, since this private key is only known to the RA. Similarly, for the attacker to obtain identity ID_{OP}, secret values R_3 and A_2 must be obtained so as to derive B_4 = $E_{PUK_{RA}}$(A_2 + R_3B_2). However, this presents a difficult ECCDH problem. In addition, security parameter A_2 is masked with password PW_{OP} and biometrics β in the smart card and hence is difficult to obtain. □

Theorem 7. *The proposed protocol offers easy recovery from smart card loss.*

Proof. Suppose that the UAV operator's smart card is stolen or lost, along with the credentials stored in it. However, the RA stores security parameters {ID_{OP}, ID_{SC}, R_2, PID_{OP}} in its database. As such, the operator only needs to invoke the smart card revocation phase of this protocol, at which point the value of ID_{SC} is updated without changing identity $ID_{OP.}$ □

Theorem 8. *The security of the negotiated session key is upheld in this protocol.*

Proof. During the generation of the session key $SS_{K_{RA}}$ = h($ID_{OP}||ID_{RA}||B_1||C_3||C_1||A_2||C_4$) that is shared between the operator and the RA, session-specific parameters B_1 = ($R_3.\mathbb{P}$) and C_3 = ($R_4.\mathbb{P}$) are deployed. This is because these parameters are stochastically selected for each authentication session. As such, even if the session key is compromised by an adversary, secret values C_1 and A2 cannot be obtained due to the irreversibility of the one-way hashing operation. Consequently, an attacker is unable to derive the session key for the subsequent communication process. Similarly, an adversary is unable to derive C_5 in $SS_{K_{OP}}$ = h($ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||R_5$), and hence this session key also remains secure in other sessions even if the current key is under attack. □

Theorem 9. *UAV operator biometric privacy is preserved and impersonation prevented.*

Proof. Once the operator imprints the biometric data β, the processing is carried out locally on the operator side such that the RA cannot access any information related to β. In addition, before storage in the smart card, a biometric encryption algorithm is executed to convert it into hash values as (β_k, β_T) = Gen(β), A_4 = $A_2 \oplus$h($ID_{OP}||PW_{OP}||\beta_k$), A_5 = $A_3 \oplus$h($ID_{OP} \oplus PW_{OP} \oplus \beta_k$), and fuzzy verifier V_F = h(h($ID_{OP}||PW_{OP}||\beta_k$) mod C_P). As such, the operator biometrics appear as A_4, A_5, V_F, and β_T in the smart card. Consequently, even if the current biometric information in the smart card is leaked, an attacker is unable to derive β from the leaked information. Consequently, operator impersonation using β is thwarted. □

Theorem 10. *Privileged insider attack is prevented.*

Proof. This attack normally happens when certain entities take advantage of their higher security clearance levels and attempt to compromise the communication process. During these compromises, security parameters such as unique identities and passwords may be recovered and misused. To curb this attack, the operator only transmits identity to the registration authority (RA) during the UAV operator registration phase. As such, the registration authority is never allowed to access any information that may facilitate the recovery of the operator password. □

Theorem 11. *The proposed protocol achieves forward key secrecy.*

Proof. At any authentication and communication phase, the UAV operator maintains three long-term secret tokens, A_4, PW_{OP}, and β, where $A_4 = A_2 \oplus h(ID_{OP}||PW_{OP}||\beta_k)$. On the other hand, the registration authority (RA) maintains two long-term secret tokens, PK_{RA} and SK_{RA}. In addition, for the generation of the shared session keys $SS_{K_{RA}} = h(ID_{OP}||ID_{RA}||B_1||C_3||C_1||A_2||C_4)$, $SS_{K_{UAV}} = h(ID_{UAV}||ID_{RA}||S_{K_2}||R_5||A_1)$, and $SS_{K_{OP}} = h(ID_{OP}||ID_{UAV}||\ ID_{RA}||C_5||S_{K_1}||R_5)$, random parameters R_3, R_4, and R_5 have to be dynamically generated. Here, it is infeasible to compute $C_4 = (R_4.B_1)$ with $B_1 = (R_3.\mathbb{P})$ due to the difficulty of solving the ECCDH problem. Consequently, the exposure of these long-term secrets cannot compromise the security of the negotiated session keys. □

Theorem 12. *Denial-of-service attacks are thwarted.*

Proof. In the proposed protocol, the registration authority (RA) does not need to maintain a verifier table that will be searched for verification tokens during the authentication process. On the other hand, the RA only stores parameter set $\{ID_{OP}, ID_{SC}, R_2, PID_{OP}\}$ in its database. Since none of these parameters are derived from the UAV operator passwords, there is no need for an exhaustive search for verification tokens in tables. Schemes using verifier tables are vulnerable to denial-of-service attacks when this table is compromised. □

Theorem 13. *Ephemeral leakage and MitM attacks are prevented.*

Proof. The assumption made in this attack is that intermediary security parameter $R_3 \subseteq Z_r^*$ has been captured by an adversary. As such, the attacker may attempt to derive session key $SS_{K_{RA}} = h(ID_{OP}||ID_{RA}||B_1||C_3||C_1||A_2||C_4)$. However, the crucial parameter required for the derivation of this session key is $C_1 = h(B_4||B_3||ID_{RA})$, in which $B_4 = E_{PUK_{RA}}(A_2 + R_3.B_2)$. Evidently, an attacker cannot compute B_4 without security parameter A_2, which is stored in the smart card and encapsulated in password PW_{OP} and UAV operator biometrics β. □

5. Performance Evaluation

Many authentication protocols have utilized various complexities to appraise their performance. The most common complexities include computation, communication, and storage. As such, this section presents the derivation as well as the comparative evaluation of the proposed protocol using these complexities. In addition, the supported security features and attack resilience are deployed towards the end of this section to appraise the proposed protocol.

5.1. Computation Complexity

During the mutual authentication and key negotiation phase, various cryptographic operations are executed at the RA, smart card reader, and UAV. Specifically, 10 elliptic curve multiplications, 2 elliptic curve additions, 4 symmetric encryptions/decryptions, and 25 one-way hashing operations are executed. Taking the duration of a single elliptic curve multiplication, elliptic curve addition, symmetric encryption/decryption, and one-way hashing operation as T_{EM}, T_{EA}, T_{SED}, and T_H, respectively, the total computation complexity of the proposed protocol is $25T_H$ + $10T_{EM}$, $2T_{EA}$ + $4T_S$. Table 2 presents the implementation environment for the proposed protocol.

Table 2. Implementation environment.

Feature	Description
Processor	Intel (R) core (TM) i5-4210U CPU
RAM	4 GB
Clock speed	2.4 GHz
Operating system	Ubuntu 22.04.2 LTS
Programming language	Python
Cryptographic library	PyCrypto
Symmetric encryption and decryption algorithm	Advanced Encryption Standard (AES)
Asymmetric encryption and decryption algorithm	Rivest–Shamir–Adleman (RSA)

Using the parameters in Table 2, above, the duration of each cryptographic operation is presented in Table 3 below.

Table 3. Duration of cryptographic operations.

Cryptographic Operation	Time (ms)
One-way hashing (T_H)	0.043
Modular squaring (T_{MS})	1.865
Square-root modular P (T_{SQ})	3.354
Symmetric encryption/decryption (T_S)	0.485
Asymmetric encryption/decryption (T_A)	8.736
Chebyshev polynomial computing (T_{CP})	5.284
Bilinear pairing operation (T_{BP})	12.263
Exponential operation (T_E)	8.561
Map-to-point hash function operation (T_{MH})	6.782
Montgomery operation (T_M)	0.285
Hashed message authentication code (T_{HM})	0.193
Elliptic curve multiplication (T_{EM})	1.029
Elliptic curve addition (T_{EA})	0.016

Based on the cryptographic durations in Table 3 above, the computation complexities for the proposed protocol as well as other related schemes were derived, as shown in Table 4 below. The selection of the schemes in [33,39,51,57] was informed by the fact that these schemes deploy similar symmetric and asymmetric cryptographic operations. As such, it was feasible to carry out some comparative evaluations with the proposed protocol.

Table 4. Computation complexity comparisons.

Scheme	Operations	Time (ms)
Yang et al. [33]	$12T_{\mathrm{H}} + 4T_{\mathrm{M}} + 2T_{\mathrm{SQ}} + 4T_{\mathrm{S}} + 10T_{\mathrm{HM}}$	12.234
Tan [39]	$18T_{\mathrm{H}} + T_{\mathrm{MS}} + T_{\mathrm{SQ}} + 2T_{\mathrm{CP}} + T_{\mathrm{S}}$	17.046
Shao et al. [51]	$13T_{\mathrm{BP}} + 17T_{\mathrm{E}} + 2T_{\mathrm{MH}} + 3T_{\mathrm{A}}$	344.728
Zhou et al. [57]	$13T_{\mathrm{H}} + 6T_{\mathrm{MS}} + 8T_{\mathrm{SQ}}$	38.581
Proposed	$25T_{\mathrm{H}} + 10T_{\mathrm{EM}} + 2T_{\mathrm{EA}} + 4T_{\mathrm{S}}$	13.625

As shown in Table 4, the computation complexity of the proposed protocol was 13.625 ms. On the other hand, the schemes in [33,39,51,57] had computation complexities of 38.581 ms, 17.046 ms, 344.728 ms, and 12.234 ms, respectively. It is evident from Figure 4 that the protocol developed in [51] incurred the highest computation complexities.

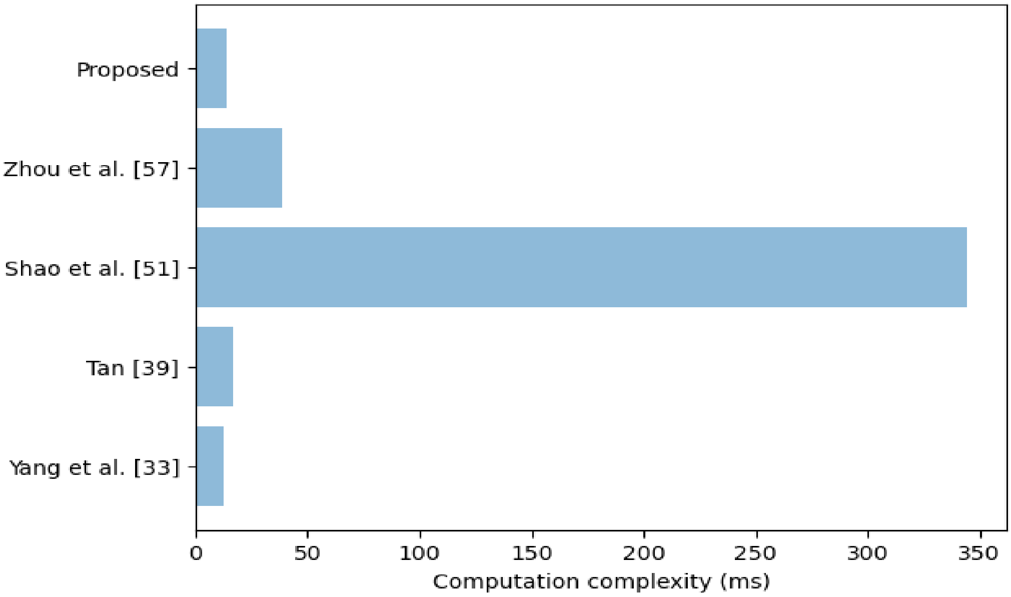


Figure 4. Computation complexity comparisons.

This was followed by the protocols in [39,57], the proposed protocol, and the scheme in [33], respectively. The extensive computation complexities in [51] were attributed to the many bilinear pairing operations that had to be executed. Although the protocol in [33] yielded the lowest computation complexities, it failed to offer session key agreement and was susceptible to privileged insider, KSSTI, MitM, and packet replay attacks.

5.2. Communication Complexity

In the process of carrying out mutual authentication and key negotiation, four messages are exchanged in the proposed protocol. These messages include $M_1 = \{B_3, C_2, S_{K_1}\}$, $M_2 = \{D_1, D_2\}$, $M_3 = \{R_5, D_3\}$ and $M_4 = \{C_3, D_4, S_{K_2}, R_5\}$. Here, $B_3 = (A_2\mathbb{P} + B_1B_2)$, $C_2 = E_{C_1}$ $(ID_{OP}||B_1||B_5||ID_{UAV})$, $D_1 = E_{A_1}$ $(ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||S_{K_2})$, $D_2 = h(ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_1}||S_{K_2}||A_1)$, $D_3 = h(ID_{OP}||ID_{UAV}||ID_{RA}||C_5||S_{K_2}||R_5||A_1)$, $C_3 = (R_4.\mathbb{P})$, and $D_4 = h(ID_{OP}||ID_{RA}||C_3||C_1||A_2||C_4||S_{K_1}||S_{K_2}||R_5)$. Using the values in [18,59], Table 5 presents the sizes of the various cryptographic outputs.

Based on the cryptographic output sizes in Table 5 above, the derivation of the communication complexity of the proposed protocol is illustrated in Table 6 below.

Table 5. Cryptographic output sizes.

Cryptographic Operation	Size (bits)
Random nonce	128
Hash output	160
Identity	32
Elliptic curve point	320
Modular exponentiation	1024
Timestamp	32
Symmetric encryption/decryption	128

Table 6. Communication complexity derivation.

Message	Size (bits)
$M_1 = \{B_3, C_2, S_{K_1}\}$ $B_3 = 320, C_2 = S_{K_1} = 128$	576
$M_2 = \{D_1, D_2\}$ $D_1 = 128, D_2 = 160$	288
$M_3 = \{R_5, D_3\}$ $R_5 = 128, D_3 = 160$	288
$M_4 = \{C_3, D_4, S_{K_2}, R_5\}$ $C_3 = 320, D_4 = 160, S_{K_2} = R_5 = 128$	736
Total	1888

As shown in Table 6 above, the total communication complexity was 1888 bits. Table 7 below offers a comparative evaluation of the obtained communication complexity with those of other related protocols.

Table 7. Communication complexity comparisons.

Scheme	No. of Exchanged Messages	Size (bits)
Yang et al. [33]	2	1120
Tan [39]	3	2294
Shao et al. [51]	2	3648
Zhou et al. [57]	5	4128
Proposed	4	1888

As shown in Table 7, the schemes in [33,39,51,57] incurred communication complexities of 4128 bits, 2294 bits, 3648 bits, and 1120 bits, respectively. It is evident from Figure 5 that the protocol in [57] incurred the highest communication complexities and required the highest number of message exchanges. This was followed by the protocol in [51], even with its two message exchanges.

The protocol in [39] had the third highest communication complexity even though it required only three message exchanges. Although the scheme in [33] had the lowest communication complexity, it could not provide session key agreement. In addition, it was prone to attacks such as privileged insider, KSSTI, MitM, and packet replays. Figure 6 shows the comparative evaluation based on the number of message exchanges.

As shown in Figure 6, the protocol in [57] required five messages to be exchanged during the authentication and key negotiation phase. This was followed by the proposed protocol, with four message exchanges. On the other hand, the scheme in [39] required three message to be exchanged, while the protocols in [33,51] needed only two messages to be exchanged. This low number of message exchanges was attributed to the lack of mutual authentication in [51] and the lack of session key agreement in [33].

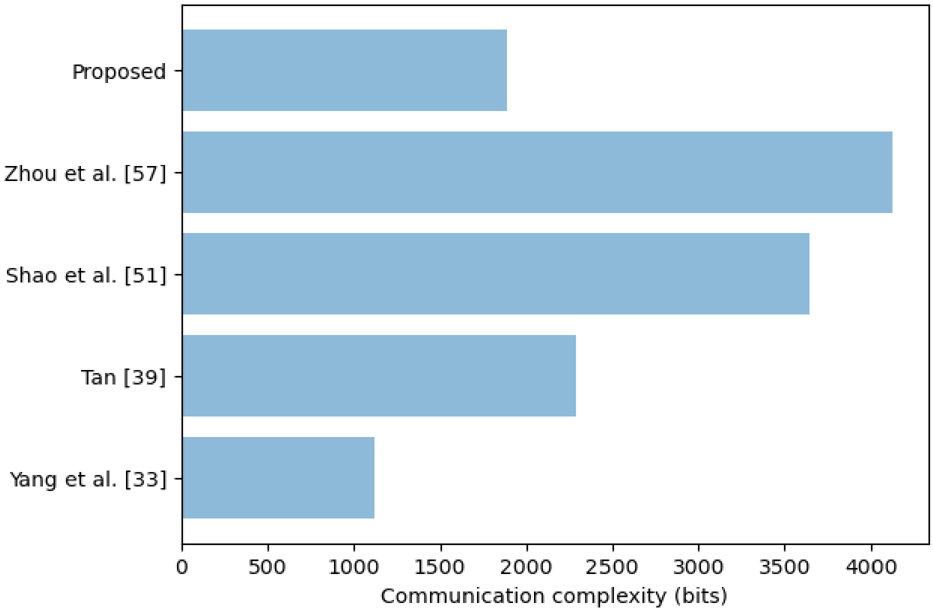


Figure 5. Communication complexity comparisons.

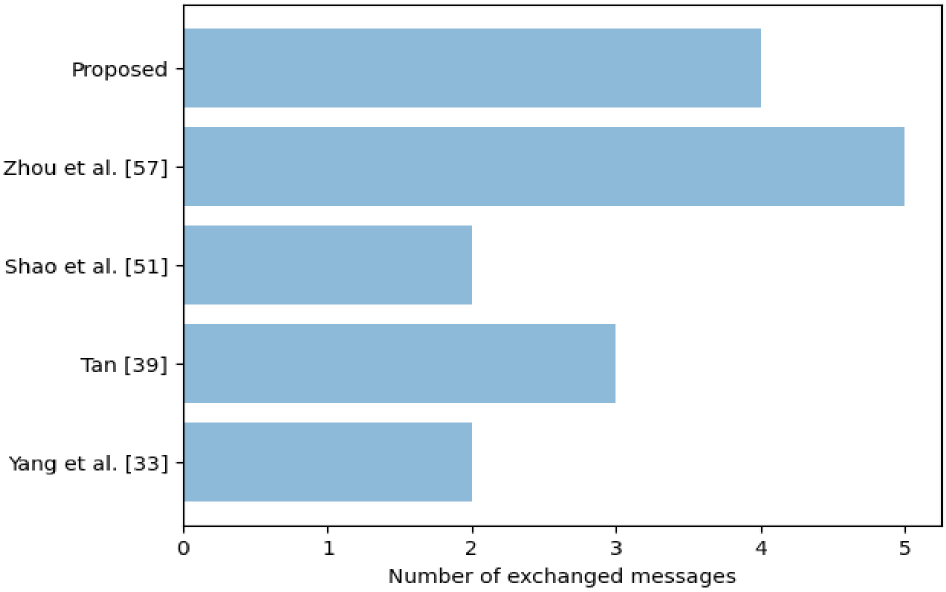


Figure 6. Message volume comparisons.

5.3. Storage Complexity

In our scheme, the RA stores parameter set {ID_{UAV}, R_1, ID_{OP}, ID_{SC}, R_2, PID_{OP}} in its database during the registration phase. On the other hand, the UAV stores parameter A_1 in its memory, while the smart card stores {A_2, A_3, $\mathbb{P}$, PUK_{RA}, C_P, h(.), Gen(.), Fe(.), ID_{OP}, PW_{OP}, β, A_4, A_5, V_F, β_T} during the registration phase. Here, A_1 = $h(ID_{UAV}||SK_{RA}||R_1)$, $A_2 = h(ID_{OP}||SK_{RA}||R_2)$, $A_3 = h(ID_{SC}||SK_{RA})$, $PUK_{RA} = \mathbb{P}.PK_{RA}$, $A_4 = A_2 \oplus h(ID_{OP}||PW_{OP}||\beta_k)$, $A_5 = A_3 \oplus h(ID_{OP} \oplus PW_{OP} \oplus \beta_k)$, and $V_F = h(h(ID_{OP}||PW_{OP}||\beta_k) \bmod C_P)$. Using the values in [14,35], $ID_{UAV} = ID_{OP} = ID_{SC} = PID_{OP} = PW_{OP} = \beta = \beta_T = C_P$ = Gen(.) = Fe(.) = 32 bits, $R_1 = R_2$ = 128 bits, $A_1 = A_2 = A_3 = A_4 = A_5$ = h(.) = V_F =160 bits, and $\mathbb{P} = PUK_{RA}$ = 320 bits. As such, the storage complexities at the RA, UAV, and smart card are 384 bits, 160 bits, and 1824 bits, respectively. Therefore, the total storage complexity in our protocol is 2368 bits. Table 8 presents a comparative evaluation of the obtained storage complexity in relation to those of other protocols.

Table 8. Storage complexity comparison.

Scheme	Size (bits)
Yang et al. [33]	2608
Tan [39]	1920
Shao et al. [51]	2080
Zhou et al. [57]	2496
Proposed	2368

As shown in Table 8, the storage complexities of the schemes in [33,39,51,57] were 2496 bits, 1920 bits, 2080 bits, and 2608 bits, respectively. It is evident from Figure 7 that the protocol in [57] incurred the highest storage complexity. This was followed by the protocol in [33], the proposed scheme, and the protocols in [39,51], in that order.

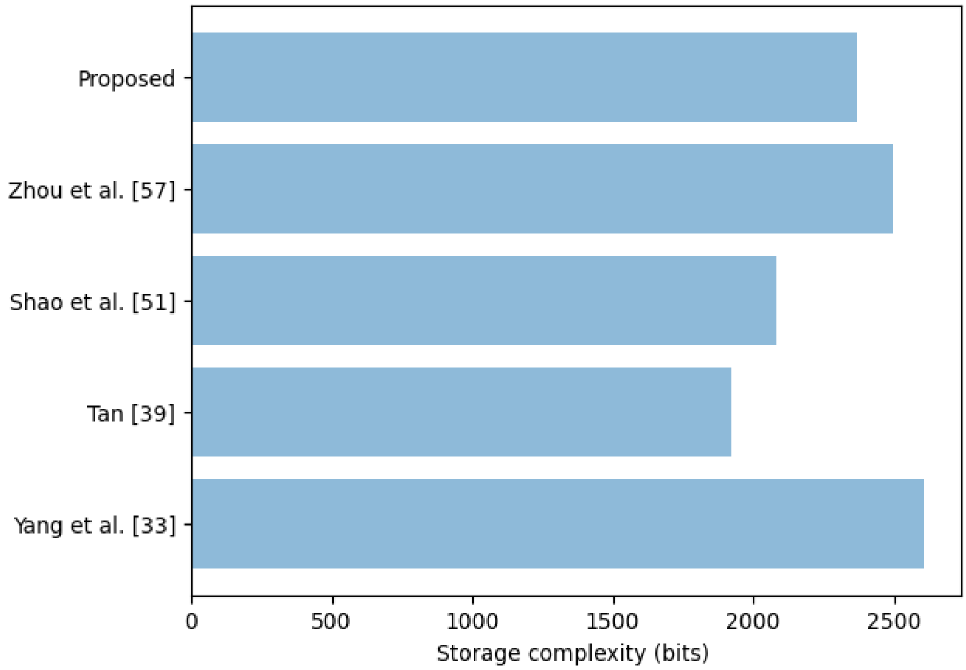


Figure 7. Storage complexity comparison.

Although the protocol in [39] incurred the least storage complexities, it was vulnerable to privileged insider, impersonation, and KSSTI attacks. Similarly, the scheme in [51] incurred relatively low storage complexities but was not robust against side-channeling, impersonation, and privileged insider attacks. In addition, it failed to provide mutual authentication and unlinkability.

5.4. Supported Security Features

In this sub-section, the security features supported by our protocol as well as the resilience it provides are compared to those of other related schemes. Table 9 shows the results of this comparative evaluation.

Table 9. Security feature comparison.

	[57]	[39]	[51]	[33]	**Proposed**
Security features					
Mutual authentication	√	√	×	√	√
Session key agreement	-	√	√	×	√
Untraceability	-	√	-	√	√
Anonymity	√	√	√	√	√
Forward key secrecy	√	√	√	√	√
Backward key secrecy	√	√	√	√	√
Biometric privacy	-	-	-	-	√
Attack Resilience					
Smart card loss	√	-	-	-	√
Password guessing	-	√	-	-	√
Privileged insider	×	×	×	×	√
KSSTI	×	×		×	√
Side-channeling	-	-	×	-	√
Impersonation	√	×	×	√	√
Denial of service	-	-	-	√	√
MitM	×	√	×	×	√

Key √: supported; ×: not supported; **-**: not considered.

As shown in Table 9, the schemes in [33,39,51,57] supported six, eight, four, and seven security and privacy features, respectively. On the other hand, the proposed protocol supported all 15 features. As such, using the eight supported features in [39] as a basis, the proposed protocol yielded a 87.5% improvement in privacy and security provision. Although our scheme incurred slightly higher computation, communication, and storage complexities, it was the most robust against attacks and supported the highest number of salient security features.

It was shown that the proposed protocol executed 10 elliptic curve multiplications, which led to slightly high computation complexities. Similarly, the 2368 bits storage requirements and four messages exchanged during the authentication and key agreement phase were slightly higher compared to the other related schemes. However, these high complexities led to the strong security of the proposed protocol, as shown in Table 9 above. Overall, the proposed protocol offers good trade-offs between security and performance.

6. Conclusions

Unmanned aerial vehicles exhibit characteristics such as low cost and flexible operations. This has made them popular for deployment in a myriad of application domains, such as intelligent transportation systems, the detection and collection of environmental data, emergency rescue, autonomous driving, and the creation of high-definition maps in real time as well as in military applications. Clearly, large amounts of sensitive data are collected and exchanged among several ubiquitous devices to realize these services. Unfortunately, message exchanges are accomplished over public channels. This exposes exchanged data to attacks such as impersonation, session key disclosure, message replay, MitM, tracking, and eavesdropping attacks. Although many protocols have been put forward to secure the UAV communication process, a number of them still suffer from security vulnerabilities or exhibit high complexities. The developed scheme was shown to offer features such as untraceability, anonymity, key secrecy, and biometric privacy. In addition, it was demonstrated to withstand numerous attacks, such as password guessing, KSSTI, and privileged insider attacks. The comparative performance evaluation carried out showed that the scheme has relatively lower computation, storage, and communication complexities.

Author Contributions: Conceptualization, K.A.-A.M.; Methodology, V.O.N. and Z.A.A.; Software, V.O.N. and Z.A.A.; Validation, H.M.J.; Investigation, V.O.N. and I.Q.A.; Resources, K.A.-A.M. and I.Q.A.; Data curation, H.M.J. and D.G.H.; Writing—original draft, Z.A.A.; Writing—review & editing, J.M., I.Q.A. and D.G.H.; Visualization, I.Q.A. and D.G.H.; Supervision, J.M.; Project administration, Z.A.A. and J.M.; Funding acquisition, Z.A.A. and J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Natural Science Foundation of Top Talent of SZTU (grant No. 20211061010016).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Syed, F.; Gupta, S.K.; Hamood Alsamhi, S.; Rashid, M.; Liu, X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4133. [CrossRef]
2. Boccadoro, P.; Striccoli, D.; Grieco, L.A. An extensive survey on the Internet of Drones. *Ad Hoc Netw.* **2021**, *122*, 102600. [CrossRef]
3. Zhang, L.; Xu, J.; Obaidat, M.S.; Li, X.; Vijayakumar, P. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. *IET Commun.* **2022**, *16*, 1142–1159. [CrossRef]
4. Son, S.; Kwon, D.; Lee, S.; Jeon, Y.; Das, A.K.; Park, Y. Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems using Blockchain and PUF. *IEEE Access* **2023**, *11*, 60240–60253. [CrossRef]
5. Xu, X.; Zhao, J.; Li, Y.; Gao, H.; Wang, X. BANet: A balanced atrous net improved from SSD for autonomous driving in smart transportation. *IEEE Sens. J.* **2020**, *21*, 25018–25026. [CrossRef]
6. Li, X.; Tan, J.; Liu, A.; Vijayakumar, P.; Kumar, N.; Alazab, M. A novel UAV-enabled data collection scheme for intelligent transportation system through UAV speed control. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 2100–2110. [CrossRef]
7. Khan, M.A.; Ullah, I.; Nisar, S.; Noor, F.; Qureshi, I.M.; Khanzada, F.U.; Amin, N.U. An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network. *IEEE Access* **2020**, *8*, 36807–36828. [CrossRef]
8. Calafate, C.T.; Tropea, M. Unmanned Aerial Vehicles—Platforms, Applications, Security and Services. *Electronics* **2020**, *9*, 975. [CrossRef]
9. Nyangaresi, V.O.; Ibrahim, A.; Abduljabbar, Z.A.; Hussain, M.A.; Al Sibahee, M.A.; Hussien, Z.A.; Ghrabat, M.J.J. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021; pp. 1–6.
10. Al Sibahee, M.A.; Nyangaresi, V.O.; Ma, J.; Abduljabbar, Z.A. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In *International Conference on Internet of Things as a Service*; Springer International Publishing: Cham, Switzerland, 2022; pp. 3–18.
11. Nyangaresi, V.O.; Abduljabbar, Z.A.; Al Sibahee, M.A.; Abduljaleel, I.Q.; Abood, E.W. Towards Security and Privacy Preservation in 5G Networks. In Proceedings of the 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, 23 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
12. Nyangaresi, V.O.; Khalefa, M.S.; Abduljabbar, Z.A.; Al Sibahee, M.A. Low Bandwidth and Side-Channeling Resilient Algorithm for Pervasive Computing Systems. In Proceedings of the International Conference on Communication and Computational Technologies; Kumar, S., Hiranwal, S., Purohit, S.D., Prasad, M., Eds.; Algorithms for Intelligent Systems. Springer Nature Singapore: Singapore, 2023; pp. 193–208, ISBN 978-981-19395-0-1.
13. Ryu, J.; Oh, J.; Kwon, D.; Son, S.; Lee, J.; Park, Y.; Park, Y. Secure ECC-based three-factor mutual authentication protocol for telecare medical information system. *IEEE Access* **2022**, *10*, 11511–11526. [CrossRef]
14. Wazid, M.; Das, A.K.; Choo, K.K.R.; Park, Y. SCS-WoT: Secure communication scheme for web of things deployment. *IEEE Internet Things J.* **2021**, *9*, 10411–10423. [CrossRef]
15. Cho, Y.; Oh, J.; Kwon, D.; Son, S.; Yu, S.; Park, Y.; Park, Y. A secure three-factor authentication protocol for e-governance system based on multiserver environments. *IEEE Access* **2022**, *10*, 74351–74365. [CrossRef]
16. Al Sibahee, M.A.; Lu, S.; Abduljabbar, Z.A.; Liu, X.; Abdalla, H.B.; Hussain, M.A.; Hussien, Z.A.; Jassim Ghrabat, M.J. Lightweight Secure Message Delivery for E2E S2S Communication in the IoT-Cloud System. *IEEE Access* **2020**, *8*, 218331–218347. [CrossRef]
17. Nyangaresi, V.O.; Abduljabbar, Z.A.; Abduljabbar, Z.A. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In Proceedings of the 2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC), Tunis, Tunisia, 20 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 188–193.
18. Wazid, M.; Das, A.K.; Lee, J.H. Authentication protocols for the internet of drones: Taxonomy, analysis and future directions. *J. Ambient Intell. Humaniz. Comput.* **2018**, 1–10. [CrossRef]

19. Ilgi, G.S.; Ever, Y.K. Critical analysis of security and privacy challenges for the Internet of drones: A survey. In *Drones in Smart-Cities*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 207–214.
20. Abualigah, L.; Diabat, A.; Sumari, P.; Gandomi, A.H. Applications, deployments, and integration of internet of drones (iod): A review. *IEEE Sens. J.* **2021**, *21*, 25532–25546. [CrossRef]
21. Yahuza, M.; Idris, M.Y.I.; Ahmedy, I.B.; Wahab, A.W.A.; Nandy, T.; Noor, N.M.; Bala, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **2021**, *9*, 57243–57270. [CrossRef]
22. Tan, H.; Zheng, W.; Vijayakumar, P. Secure and Efficient Authenticated Key Management Scheme for UAV-Assisted Infrastructure-Less IoVs. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 6389–6400. [CrossRef]
23. Liu, R.; Liu, A.; Qu, Z.; Xiong, N.N. An UAV-enabled intelligent connected transportation system with 6G Communications for internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2045–2059. [CrossRef]
24. Bai, L.; Liu, J.; Wang, J.; Han, R.; Choi, J. Data aggregation in UAV-aided random access for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 5755–5764. [CrossRef]
25. Wang, W.; Han, Z.; Alazab, M.; Gadekallu, T.R.; Zhou, X.; Su, C. Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps. *IEEE Trans. Ind. Appl.* **2022**, *58*, 5616–5623. [CrossRef]
26. Aydin, Y.; Kurt, G.K.; Ozdemir, E.; Yanikomeroglu, H. Authentication and handover challenges and methods for drone swarms. *IEEE J. Radio Freq. Identif.* **2022**, *6*, 220–228. [CrossRef]
27. Jan, S.U.; Abbasi, I.A.; Algarni, F. A key agreement scheme for IoD deployment civilian drone. *IEEE Access* **2021**, *9*, 149311–149321. [CrossRef]
28. Gao, H.; Liu, C.; Li, Y.; Yang, X. V2VR: Reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3533–3546. [CrossRef]
29. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A.K. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1346–1358. [CrossRef]
30. Muram, F.U.; Javed, M.A. Drone-based risk management of autonomous systems using contracts and blockchain. In Proceedings of the 2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, HI, USA, 9–12 March 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 679–688.
31. Nyangaresi, V.O. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. *Ad Hoc Netw.* **2023**, *142*, 103117. [CrossRef]
32. Alladi, T.; Bansal, G.; Chamola, V.; Guizani, M. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15068–15077. [CrossRef]
33. Yang, X.; Yi, X.; Khalil, I.; Zeng, Y.; Huang, X.; Nepal, S.; Cui, H. A lightweight authentication scheme for vehicular ad hoc networks based on MSR. *Veh. Commun.* **2019**, *15*, 16–27. [CrossRef]
34. Jan, S.U.; Qayum, F.; Khan, H.U. Design and analysis of lightweight authentication protocol for securing IoD. *IEEE Access* **2021**, *9*, 69287–69306. [CrossRef]
35. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J. 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]
36. Nyangaresi, V.O.; Petrovic, N. Efficient PUF based authentication protocol for internet of drones. In Proceedings of the 2021 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 13 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–4.
37. Alzahrani, B.A.; Barnawi, A.; Chaudhry, S.A. A resource-friendly authentication protocol for UAV-based massive crowd management systems. *Secur. Commun. Netw.* **2021**, *2021*, 3437373. [CrossRef]
38. Gope, P.; Sikdar, B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. *IEEE Trans. Veh. Technol.* **2020**, *69*, 13621–13630. [CrossRef]
39. Tan, Z. Privacy-preserving two-factor key agreement protocol based on chebyshev polynomials. *Secur. Commun. Netw.* **2021**, *2021*, 6697898. [CrossRef]
40. Khan, M.A.; Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Shah, J.A.; Uddin, M.I.; Algarni, F. A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems. *IEEE Trans. Ind. Inform.* **2021**, *18*, 3416–3425. [CrossRef]
41. 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]
42. Khalid, H.; Hashim, S.J.; Ahamed, S.M.S.; Hashim, F.; Chaudhary, M.A. Secure Real-Time Data Access Using Two-Factor Authentication Scheme for the Internet of Drones. In Proceedings of the 2021 IEEE 19th Student Conference on Research and Development (SCOReD), Kota Kinabalu, Malaysia, 23–25 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 168–173.
43. Tanveer, M.; Zahid, A.H.; Ahmad, M.; Baz, A.; Alhakami, H. LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of Drone environment. *IEEE Access* **2020**, *8*, 155645–155659. [CrossRef]
44. Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Lorenz, P.; Alazab, M. Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9097–9111. [CrossRef]
45. Nyangaresi, V.O. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *J. Syst. Archit.* **2022**, *133*, 102763. [CrossRef]
46. Nikooghadam, M.; Amintoosi, H.; Islam, S.H.; Moghadam, M.F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *J. Syst. Archit.* **2021**, *115*, 101955. [CrossRef]

47. Zhang, J.; Cui, J.; Zhong, H.; Bolodurina, I.; Liu, L. Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks. *IEEE Trans. Netw. Sci. Eng.* **2020**, *8*, 2982–2994. [CrossRef]
48. Tanveer, M.; Kumar, N.; Hassan, M.M. RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones. *IEEE Internet Things J.* **2021**, *9*, 1339–1353. [CrossRef]
49. Abduljabbar, Z.A.; Omollo Nyangaresi, V.; Al Sibahee, M.A.; Jassim Ghrabat, M.J.; Ma, J.; Qays Abduljaleel, I.; Aldarwish, A.J. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 55. [CrossRef]
50. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6903–6916. [CrossRef]
51. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [CrossRef]
52. Semal, B.; Markantonakis, K.; Akram, R.N. A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. In Proceedings of the 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC), London, UK, 23–27 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
53. El-Zawawy, M.A.; Brighente, A.; Conti, M. Authenticating Drone-Assisted Internet of Vehicles Using Elliptic Curve Cryptography and Blockchain. *IEEE Trans. Netw. Serv. Manag.* **2022**, *20*, 1775–1789. [CrossRef]
54. Cheng, Y.; Xu, S.; Zang, M.; Kong, W. LPPA: A lightweight privacy-preserving authentication scheme for the internet of drones. In Proceedings of the 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 13–16 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 656–661.
55. Hussien, Z.A.; Abdulmalik, H.A.; Hussain, M.A.; Nyangaresi, V.O.; Ma, J.; Abduljabbar, Z.A.; Abduljaleel, I.Q. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. *Appl. Sci.* **2023**, *13*, 691. [CrossRef]
56. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **2020**, *155*, 143–149. [CrossRef]
57. Zhou, Z.; Wang, P.; Li, Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 3603–3615. [CrossRef]
58. Gao, H.; Huang, W.; Yang, X. Applying Probabilistic Model Checking to Path Planning in an Intelligent Transportation System Using Mobility Trajectories and Their Statistical Data. *Intell. Autom. Soft Comput.* **2019**, *25*, 547–559. [CrossRef]
59. Jiang, Q.; Zeadally, S.; Ma, J.; He, D. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access* **2017**, *5*, 3376–3392. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.