Article:
Gope, P. and Sikdar, B. (2020) An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones. IEEE Transactions on Vehicular Technology. ISSN 0018-9545

https://doi.org/10.1109/tvt.2020.3018778

An Efficient Privacy-Preserving Authenticated Key Agreement Scheme for Edge-Assisted Internet of Drones

Prosanta Gope, *Member, IEEE* and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—There has been a a significant increase in the popularity of using Unmanned Aerial Vehicles (UAVs), popularly known as drones, in several applications. In many application scenarios, UAVs are deployed in missions where sensitive data is collected, such as monitoring critical infrastructure, industrial facilities, crops, and public safety. Due to the sensitive and/or safety critical nature of the data collected in these applications, it is imperative to consider the security and privacy aspects of the UAVs used in these scenarios. In this article, we propose an efficient privacy aware authenticated key agreement scheme for edge-assisted UAVs (Internet of Drones). Unlike the existing security solutions for UAVs, the proposed scheme does not need to store any secret keys in the devices but still can provide the desired security features. To the best of our knowledge, this is the first work where physical security of the UAV has been taken into account. The proposed system allows third-party communication and mobile edge computing service providers to authenticate the UAVs without any loss of provacy and outperforms existing methods in terms of computational complexity.**

***Index Terms*—Internet of Drones, Mutual Authentication, Double PUF, Computational Efficiency, Unmanned Aerial Vehicles.**

I. Introduction

With the recent development in aviation technologies, unmanned aerial vehicles (UAVs), popularly known as drones, have gained significant attention in both academia and industry. Nowadays, drones are being used for various applications that include military, public safety and first responses, surveillance and monitoring of industrial, agricultural and infrastructural facilities, telecommunications, and delivery of medical supplies, among others [1-4]. According to [5], there will be 2.7 million small-scale UAVs by 2020 and they will be used to launch a wide-range of services. UAVs typically occupy the low altitude airspace and this airspace is expected to get increasingly densely occupied. Therefore, connecting UAVs through the Internet of Connected Drones (IoD) can ensure significant benefits in traffic management and also in the quality of service for the UAVs. With such an IoD, UAVs will be able to make accurate and efficient flying strategies by exchanging traffic and airspace information between each others via the IoD.

Despite its numerous benefits, security and privacy are still major concerns in IoD environments. In many UAV applications, the UAV communication may contain sensitive information such as location, flying patterns, etc. Since IoD uses the public and open-access communication networks that can be exposed to potential adversaries, security issues such as authentication, privacy, and secure data outsourcing are some of the main concerns in IoD environments. While there have been some recent efforts at addressing these security issues, much of the work is still at a preliminary stage and aimed at providing high-level overviews without detailed construction of protocols [6-11].

Two of the major security concerns with IoD communications are authentication and privacy. The use of drones for sensitive applications makes them attractive targets for adversaries. In addition to the data that is collected by the drones, the identity of the drones and their geographical location (i.e., flight path) may also be targeted by the adversaries to gain confidential information related to use of drones and the facilities that they are monitoring. Further, in many applications, drones may have to interact with third-party services such as telecommunication service providers and mobile edge computing (MEC) services to offload and process their data in real-time [21-22] . Usually, MEC can provide cloud computing capabilities and IT service environment at the edge of the network, within the Radio Access Network (RAN) and in close proximity to mobile subscribers. Compared with cloud computing, MEC significantly reduces the network latency to its mobile subscribers, which hence ensures highly efficient network operation and service delivery, and offer an improved user experience. Thus, all parties involved in the communication to and from the drones have to be authenticated, and in the presence of third party MEC and communication service providers, drones should be protected against attacks on their privacy that can leak sensitive information about them. This paper addresses this problem and proposes a privacy-preserving authentication and key agreement mechanism for use with drones that use third party communication and MEC services.

In order to design an effective authentication framework for IoD with privacy protection, the following challenges need to be overcome simultaneously. First, given the fact that communication in IoD may contain time-sensitive, safety critical traffic information, the real-time authentication mechanism designed for IoD should be as efficient as possible. Also, since small-scale UAVs are usually resource constrained in terms of computation and energy, the design of authentication should only involve lightweight operations. Second, the

P. Gope is associated with the University of Sheffield, United Kingdom. (E-mail: p.gope@sheffield.ac.uk/p.gope@ieee.org)

B. Sikdar is associated with the National University of Singapore, Singapore. (E-mail: bsikdar@nus.edu.sg)

Corresponding author: Dr. Prosanta Gope

proposed framework needs to prevent malicious adversaries from learning the true identity of any valid UAV. However, when traffic accidents or certain misbehavior occur, it should be possible, if necessary, to conditionally reveal the identity of an UAV to legal authorities. Thus, we refer to such a privacy protection as conditional privacy as introduced in [16].

In this paper, we propose an efficient privacy-preserving authentication scheme for IoD-based UAV environments. Although several authentication schemes for drones have been proposed in literature, these schemes require the devices (such as UAVs) to store the security credentials (such as secret key), which could be exposed through various attacks (e.g., if the drone is physically captured by the adversary or through intelligent side channel attacks). This paper seeks to address this key security issue in IoD environments. One of the notable properties of the proposed scheme is that it does not require an UAV to store any secret key but it can still ensure higher level security. Towards this end, the proposed mechanism utilizes the concept of Physically Unclonable Functions (PUFs) to facilitate high levels of security while simultaneously minimizing the computational resource requirement in each device. To the best of our knowledge, this is the first paper which has considered physical security of the UAVs.

The key contributions of the paper are as follows:

- A *new prototype model* for edge-assisted Internet of Drones, which allows an UAV to collect information from the ground-level and constantly send updates to the control center with the help of a MEC or communication service operated by a third-party company, where service rate and effectiveness of a service provider may vary based on the location and other factors.
- A *novel double-PUF-based* privacy-preserving authenticated key agreement protocol that may be used by the third-party service provider to verify the legitimacy of an UAV (without compromising its privacy), before receiving services to the UAV.
- A comparative study of the proposed scheme with respect to a closely related recently proposed authentication scheme for IoD. Our results demonstrate that the proposed scheme is secure and computationally more *efficient* as compared to the existing schemes.

The remainder of this paper has been organized as follows. Section II presents an overview of related work, and the system and adversary models are presented in Section III. The proposed scheme is presented in Section IV. Security analysis of the proposed scheme is presented in Section V. A discussion on the performance of the proposed scheme is presented in Section VI. Finally, conclusions are drawn in Section VII. The symbols and cryptographic functions of the proposed scheme are defined in Table I.

Table I
SYMBOLS AND CRYPTOGRAPHIC FUNCTION

Symbol	Definition
ID_u	Identity of the MU
PID_u^i	i-th Pseudo identity of UAV
CRP(C, R)	Challenge-Response pair
SK	Session Key
$P_u(\cdot)$	Physically uncloneable function
$h(\cdot)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|$	Concatenation operation

II. RELATED WORK

Issues related to security and privacy in IoD environments have received increasing attention in recent years. High-level overviews of security and privacy issues in IoD have been identified and presented in [6-11], and [15]. However, the majority of the work in this area focuses on the general security issues, without providing any concrete security solutions for IoD environments. For instance, in [7], the authors have mainly tried to show how to efficiently and effectively organize IoD. On the other hand, in [8], the authors have pointed out some security issues such as authentication, privacy leakage, secure data outsourcing, in IoD. However, no detailed construction of protocols or solutions are proposed to address these issues. While [9] suggested several potential solutions for enhancing the security of IoD, these are high-level ideas. For example, the authors highlight the need for mutual authentication for secure communication without providing any protocol level description.

There have been some recent works on developing authentication mechanisms for IoD environments. In [15], the authors proposed a privacy preserving authentication framework for IoD by using a certificate-based digital signature scheme. However, the proposed solution does not provide security against location threats as well as security against any physical attacks. In [16], Zhang et al. proposed a lightweight authentication scheme for IoD. However, after a detailed investigation, we found that the proposed authentication protocol is insecure against forgery attacks, where an attacker can intercept the first message communicated between user U_i and the control server (CS). The attacker can then change the timestamp ST_1, but the CS cannot identify that. Besides, in the protocol proposed [16], the drone needs to store certain security credentials for participating in the authentication protocol. Thus, if an attacker succeeds to physically capture the drone, then he/she can access the device's memory or subject it to side-channel attacks to get the stored credentials. Consequently, the attacker can compromise the drone (i.e., change the settings) but neither the CS nor U_i will be able to identify that. The protocol proposed in [17] is also vulnerable to similar security threats and issues. In addition, since the schemes proposed in [15-17] are based on the use of timestamps, they also suffer from the global-time-synchronization problem. Apart from [15-17], recently a few more interesting IoD-based authentication schemes [18-20] have been proposed in the literature. Unfortunately, similar to [15-17], the protocols presented in [18-20] also suffer from the same issue, i.e., those resulting from the physical security of the UAVs.

III. System and Adversary Model

A. System Model

Figure 1 shows the system model considered in this paper, in which we consider three major participants: a set of UAVs, a set of communication infrastructure or mobile edge computing operators [12], and a UAV service provider (USP) or the organization that owns the UAVs. Note that the communication/MEC operators are companies that are different from the USP and specialize in providing connectivity, real-time analytics, and data processing support to the UAVs. For simplicity, we refer to these third-party communication service providers as well as mobile edge computing service providers as "MEC operators". There are two major entities in an USP: control and monitoring center (CMC), and cloud data center (CDC). All UAVs are equipped with two PUFs [13] and also integrated with other services such as global positioning system (GPS), wireless communication interface, etc.

In order to embark on a mission and be operational, each UAV first needs to register with the USP. Similarly, each MEC operator is required to register with the USP as well and they communicate with the USP via a secure channel. Each UAV is required to send its field data to the USP via a MEC operator. The MEC operators have enough computational capability to support both the UAV and the USP to establish a session key for facilitating secure communication. Since the operational region of the UAVs may span large geographical areas, the area over which a MEC operator provides its service is divided into several smaller regions. Also, it is possible that a single MEC operator does not provide coverage over all regions of interest for a USP. Thus, a USP may rely on more than one MEC operator for its operation. Also, in places with more than one MEC operator, the service rate and effectiveness of each MEC operator may vary based on the location and other factors. For instance, the service rate provided by the MEC operator in region Y (RegY in Fig. 1) could be higher than that in region X (RegX in Fig. 1). Thus, the UAVs should be capable of authenticating with multiple MEC operators without any compromise in their privacy.

B. Adversary Model

In our system model, the UAVs mainly use public network based communication. Consequently, there is a possibility of various attacks by a wide range of adversaries. In this paper, we consider the following security and privacy threats:

- **Authentication Threat:** Before obtaining any field data of a particular region from a UAV and establishing a secure session key, the USP needs to authenticate the UAV. In this context, the MEC operators help them in exchanging their messages. However, in our threat model we consider the MEC operator as a semi-honest adversary, who may try to modify the messages exchanged between the participants (UAV and USP). Besides, since the authentication process will also be carried out through an insecure public channel, any external adversary can modify the messages received/sent by the UAV.
- **Privacy Threat:** The identity of the UAV should be known only to the USP. Thus, the real identity of the UAV should be kept hidden from the MEC operator. Here, the threat considered is that the MEC operator may try to trace the flight-path of the UAV as it moves from one region to another. In addition, any outside adversary (eavesdropper) also should not be able to identify the UAV and trace the UAV's trajectory.
- **Location Threat:** Based on the system model presented earlier (with different service quality in different regions), a dishonest MEC operator may also falsify its signal to a UAV, in order to charge higher prices for its service. Therefore, the USP also needs to validate the location information of the UAVs using their location area identifier (LAI).
- **Session-key Security Threat:** After a successful authentication, an UAV and the USP need to establish a secure session key that will be used for secure communication between the USP and the UAV. The protocol for setting up the key should also support the property of backward secrecy for the session key (i.e., if the session key gets leaked for a given session, the session keys of the previous sessions should not get compromised).
- **Physical Security Threat:** Since UAVs are often used for military, surveillance, and monitoring purposes, there is a possibly that an attacker may attempt to physically capture a UAV. Additionally, it is also possible that an UAV involved in an accident is found and taken over by the adversary. Physical access to the UAV may allow the adversary to subject it to a range of attacks to gain access to the stored data in the UAV. In addition, the adversary may also get access to security credentials stored in the UAV's memory and then use it disclose any encrypted data or authenticate with the USP.

IV. Proposed Double-PUF-based Authenticated Key Agreement Scheme

This section presents the proposed authentication and key establishment protocol. Before describing the protocol, we first provide a brief introduction to PUFs that form one of its key components.

A PUF is a one-way function that is embedded into the hardware components of a physical circuit [13]. The output of a PUF is dependent on the small inherent random variations in the dimensions and composition of hardware components introduced by the chip manufacturing process. When queried with a challenge x, a PUF produces a response $y \Leftarrow \mathrm{PUF}(x)$ that depends on x and the internal physical (sub-)microscopic structure of the device. Due to variations in environmental and operational factors such as the ambient temperature and terminal voltages, the PUF output may vary slightly when queried with the same challenge multiple times. However, fuzzy extractors can be used to eliminate these variations (noise) and convert them into deterministic functions [23-25]. A PUF can be used as a tool for hardware authentication and generating secure keys, among others. Robustness against physical and invasive attacks, and the ability to retain keys without actually storing them, makes PUFs ideal candidates for IoT security. A PUF can be of several types, e.g., delay-based PUFs which leverage the variation among circuit delays,

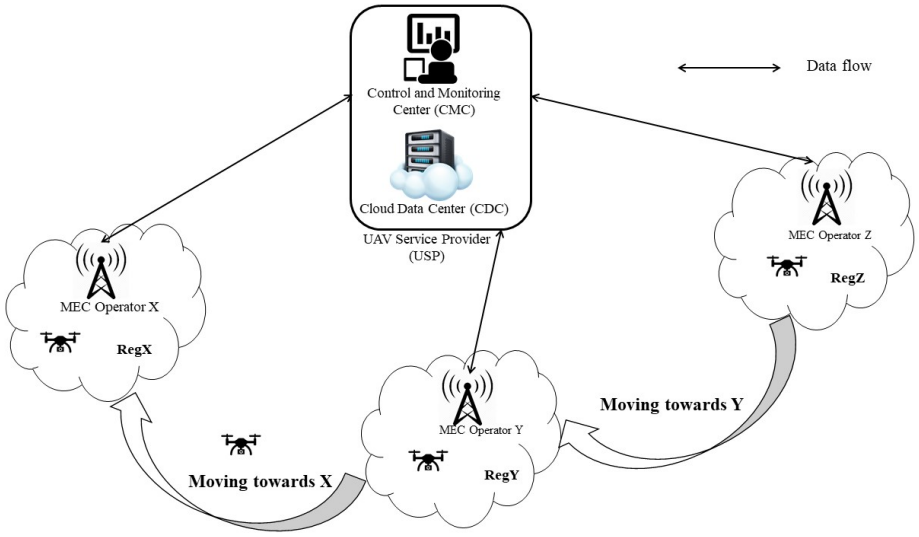

Figure 1. System model for the proposed scheme.

and memory based PUFs which exploit the random process variations in the memory cells.

There are two phases in the proposed scheme: the registration phase and the authentication phase. In the registration phase, each UAV needs to request the USP for registration. After a UAV successfully registers itself with the USP, it is provided with a set of secret credentials. These secret credentials are used by the USP to authenticate the UAV during subsequent authentication attempts (e.g., when the UAV needs to authenticate itself before sending data to the USP). If the authentication is successful, then the UAV will be able to securely transfer the field information to the USP via a third-party MEC service provider.

A. Assumptions

- Each UAV is embedded with two PUFs. The first one is directly embedded in the memory of the UAV, where recorded field information is stored. The second one is embedded with the main control circuit of the UAV.
- An adversary is not able to tamper with UAV's PUFs. Moreover, any such attempt will make the PUFs useless [13] and the USP will be detect that through the execution of our proposed authentication scheme.
- The PUFs used in the proposed scheme are in ideal-state. Thus, there is no issue of noise in the response from a PUF.

B. Registration Phase

For the one-time, initial registration process of the proposed scheme, the UAV and USP need to execute the following steps:

1) **Step R1:** The UAV sends its identity ID_u to the USP for service registration through a secure channel.
2) **Step R2:** The USP generates a challenge C_i for use in the i-th round of authentication (i.e., the i-th execution of the authentication phase) and sends it to the UAV. The USP also generates a set of challenges $C_{syn} = \{c_1, \cdots, c_n\}$ and sends them to the UAV. This set of challenges is used for addressing desynchronization or denial-of-service (DoS) attacks.
3) **Step R3:** The UAV uses its two PUFs (P_u^x, P_u^y) and extracts the PUF outputs $R_i^x = P_u^x(C_i)$, $R_i^y = P_u^y(C_i)$ and $R_{syn}^x = P_u^x(C_{syn})$, $R_{syn}^y = P_u^y(C_{syn})$ and subsequently sends $\{(R_i^x, R_i^y), (R_{syn}^x, R_{syn}^y)\}$ to the USP through the secure channel.
4) **Step R4:** Next, the USP generates a unique pseudo identity PID_u^i and a set of fake identities $\text{FID} = \{\text{fid}_1, \cdots, \text{fid}_n\}$ and sends them to the UAV. Finally, the USP needs to store $\{(PID_u^i, \text{FID}), ID_u, (C_i, R_i^x, R_i^y), (C_{syn}, R_{syn}^x, R_{syn}^y)\}$ for each UAV. On the other hand, the UAV needs to store only $\{(PID_u^i, \text{FID})\}$.

Note that the requirement for a secure channel for the UAVs is only for the initial registration phase and this is not required for the subsequent authentication phases.

C. Authentication Phase

Consider an UAV that has been assigned to collect field information from a particular region. In each region, a MEC operator selected by the USP helps the UAV in transferring/receiving packets. In this phase of the proposed scheme, both the UAV and USP authenticate each other and establish a session key for secure communication. In this regard, the MEC operator helps them in exchanging the communication messages. The detailed description of the phase is as follows:

1) **Step AU1:** The UAV initiates the authentication process with a "*Hello*" message to the MEC operator. Upon receiving the "*Hello*" message from the UAV, the MEC operator responds with an acknowledgment (Ack) and its identity ID_{MEC}.
2) **Step AU2:** Next, the UAV generates a random number N_u and then submits its current pseudo identity PID_u^i, N_u, and the identity of the MEC operator ID_{MEC} to the USP via the MEC operator.

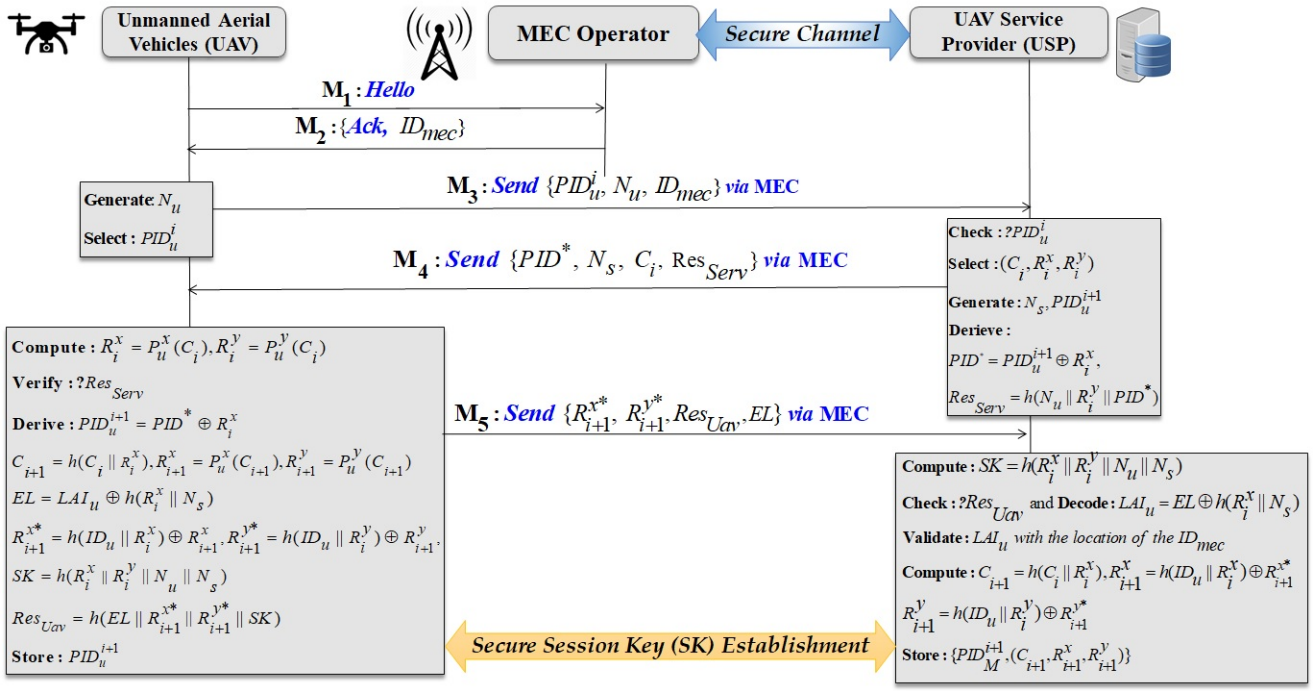

Figure 2. Proposed double-PUF-based privacy preserving authenticated key agreement scheme.

3) **Step AU3:** Upon receiving the authentication request, the USP first locates the pseudo identity PID_u^i in its records and subsequently selects the *challenge-response triplet*, (C_i, R_i^x, R_i^y), from its database. Next, the USP generates a nonce N_s, a unique pseudo identity for the (i+1)-th round PID_u^{i+1}, and subsequently, calculates $PID^* = PID_u^{i+1} \oplus R_i^x$ and $Res_{Serv} = h(R_i^y||PID^*||N_u)$. Hereafter, the USP composes a response message $\mathrm{M}_4 : \{PID^*, N_s, C_i, Res_{Serv}\}$ and sends M_4 to the UAV via the MEC operator.
4) **Step AU4:** After receiving $\{PID^*, N_s, C_i, Res_{Serv}\}$, the UAV first extracts the PUF outputs $R_i^x = P_u^x(C_i)$ and $R_i^y = P_u^y(C_i)$ and then computes and verifies the hash-response Res_{Serv}. If the verification is unsuccessful, the UAV aborts the execution of the protocol. Otherwise, the UAV derives $PID_u^{i+1} = PID^* \oplus R_i^x$, $C_{i+1} = h(C_i||R_i^x)$, $R_{i+1}^x = P_u^x(C_{i+1})$, $R_{i+1}^y = P_u^y(C_{i+1})$, $EL = LAI_u \oplus h(R_i^x||N_s)$, $R_{i+1}^{x*} = h(ID_u||R_i^x) \oplus R_{i+1}^x$, $R_{i+1}^{y*} = h(ID_u||R_i^y) \oplus R_{i+1}^y$, $SK = h(N_u||R_i^x||R_i^y||N_s)$ and $Res_{Uav} = h(EL||R_{i+1}^{x*}||R_{i+1}^{y*}||SK)$. The UAV then composes a message $\mathrm{M}_5 : \{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{Uav}, EL\}$ and sends M_5 to the USP via the MEC operator.
5) **Step AU5:** Upon receiving the response message M_5, the USP first computes $SK = h(N_u||R_i^x||R_i^y||N_s)$ and then checks the response parameter Res_{Uav}. If the verification is successful, then the USP decodes $LAI_u = EL \oplus h(R_i^x||N_s)$ and validates LAI_u with the location of the MEC operator ID_{MEC}. After successful validation, the USP computes $C_{i+1} = h(C_i||R_i^x)$, $R_{i+1}^x = h(ID_u||R_i^x) \oplus R_{i+1}^{x*}$, and $R_{i+1}^y = h(ID_u||R_i^y) \oplus R_{i+1}^{y*}$. Finally, the USP replaces $\{PID_u^i, (C_i, R_i^x, R_i^y)\}$ with $\{PID_u^{i+1}, (C_{i+1}, R_{i+1}^x, R_{i+1}^y)\}$.

Note that for addressing DoS or synchronization attacks, the proposed scheme utilizes the concept of synchronous challenge-response triplets $(C_{syn}, R_{syn}^x, R_{syn}^y)$ and the set of fake identities $\mathrm{FID} = \{\mathrm{fid}_1, \cdots, \mathrm{fid}_n\}$. Consider the cases where the USP cannot identify the pseudo identity PID_u^i of the UAV or where the UAV fails to receive any response message with the parameters $\{PID^*, N_s, C_i, Res_{Serv}\}$. In these cases, the UAV needs to choose an unused fake identity fid_j from the set of fake identities, i.e., FID, and the USP needs to select one of the unused synchronous challenge-response triplets $(c_x, r_{syn}^x, r_{syn}^y) \in (C_{syn}, R_{syn}^x, R_{syn}^y)$. Once both the UAV and the USP mutually authenticate each other by using the fake identity fid_j and unused synchronous challenge-response triplet $(c_x, r_{syn}^x, r_{syn}^y)$, the USP will delete $(c_x, r_{syn}^x, r_{syn}^y)$ from its database and both the UAV and the USP delete the fake identity fid_j from their memory. Details of the authentication phase are shown in Figure 2.

V. Security Analysis of the Proposed Scheme

In this section, we formally analyze the semantic security of the proposed protocol using the real-or-random (RoR) model [14]. The RoR security is commonly used to measure the indistinguishability of session keys. Here, we first demonstrate that the proposed scheme can accomplish mutual authentication along with the session key security. Then, we provide the informal security analysis of the proposed protocol.

A. Formal Security Analysis Using RoR Model

According to the RoR model, an attacker $\mathcal{A}$ interacts with the t-th participant instance Π^t. Following the proposed

scheme, we define the UAV's and the USP's instances by U and S, receptively. The RoR model uses Execute, Send, Reveal, CorruptDevice, and Test queries to simulate an attack scenario (as shown in Table II). In our proof, we use a collision resistant one-way hash function $h(\cdot)$ (a pseudo-random function), and a secure ideal PUF function P as random oracles.

B. Assumptions

The security proof makes the following assumptions:
(i) *Uncloneability assumption:* We can define a PUF as *PUF:* $\{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, where for a given input of length l_1 the PUF outputs an arbitary string of length l_2. We can determine the security of this function with the help of the following *challenge-response game*, which consists of two phases:

Phase1: For a given challenge C_i, an adversary $\mathcal{A}$ obtains the PUF response/output R_i.

Challenge: Next, $\mathcal{A}$ selects another arbitary challenge C_y that has not been queried before.

Phase 2: $\mathcal{A}$ is allowed to query the PUF for any challenge other than C_y.

Response: Finally, $\mathcal{A}$ outputs its guess for $R_y^{'}$ for the PUF's response R_y to C_y (i.e., $R_y = PUF(C_y)$).

We say $\mathcal{A}$ wins the game if $R_y^{'} = R_y$. Therefore, we can say $Adv_{\mathcal{A}}^{puf}(l_2) = \Pr\left[R_y = R_y^{'}\right]$.
(ii)*Pseudo random function assumption:* A pseudo random function PRF:$\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^{k'}$ which takes a secret security parameter $K \epsilon \{0,1\}^k$ and a message $\mathcal{M} \epsilon \{0,1\}^*$ as input and provides an arbitrary string PRF(K, $\mathcal{M}$) which is indistinguishable from random string. Now, assuming that *h* be a polynomial-time computable pseudorandom function. For distinguishing *h*, a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ may request polynomial bounded queries with its selected inputs and obtain the outputs computed by *h* for training. After the training phase, $\mathcal{A}$ is given a function, which is either *h* or a truly random function. We say that *h* is a pseudo-random function, if it is indistinguishable from a truly random function under $\mathcal{A}$. Namely, $\mathcal{A}$ is given either *h* or a truly random function according to a random bit {0, 1} and it has only the probability $\frac{1}{2} + \varepsilon$, to distinguish *h.*

Theorem 1: Let $\mathcal{A}$ be a polynomial time adversary running in time t against the protocol $\mathcal{P}$. Then, the advantage of $\mathcal{A}$ in breaking the semantic security of the proposed authenticated key-establishment (AKE) scheme can be represented as follows:

$$Adv_{\mathcal{A}}^{AKE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_P^2}{|PUF|} + \frac{2q_{send}}{|D|}$$

where q_h, q_P, and q_{send} denote the number of hash, PUF, and Send queries, respectively. Also, $|Hash|$, $|PUF|$, and $|D|$ denote the length of the hash output, length of the PUF-based output strings, and the length of the output of an algorithm that resolves a particular problem by running $\mathcal{A}$ on a simulation protocol, respectively.

Proof. Consider a sequence of games denoted by $\mathcal{G}_i$, where $i = 0, 1, \cdots, 4$. Let $Succ_{\mathcal{A}}^{\mathcal{G}_i}$ denote the event that $\mathcal{A}$ correctly guesses the random bit c in game $\mathcal{G}_i$. The advantage of the adversary to win the game can then be represented as $Adv_{\mathcal{A},\mathcal{G}_i}^{AKE} = \Pr\left[Succ_{\mathcal{A}}^{\mathcal{G}_i}\right]$. The proof, following the model in [14], consists of a sequence of games, starting with the real attack (executed in $\mathcal{G}_0$) against the proposed AKE scheme and ending the game in which the adversary's advantage is 0, and for which we can bound the difference in the adversary's advantage between any two consecutive games. For each game $\mathcal{G}_i$, we define an event $Adv_{\mathcal{A},\mathcal{G}_i}^{AKE}$ corresponding to the case in which the adversary correctly guesses the hidden bit c involved in the *Test* queries.

Game $\mathcal{G}_0$: It is simulated as an actual attack by $\mathcal{A}$ against the proposed solution in the RoR model. Since the bit c was chosen randomly at the start of $\mathcal{G}_0$, it is clear that

$$Adv_{\mathcal{A}}^{AKE} = \left|2Adv_{\mathcal{A},\mathcal{G}_0}^{AKE} - 1\right|. \tag{1}$$

Game $\mathcal{G}_1$: This game is modeled as an eavesdropping attack in which the adversary $\mathcal{A}$ intercepts the transmitted messages (such as $\mathrm{M}_3 : \{PID_u^i, N_u, ID_{mec}\}$, $\mathrm{M}_4 : \{PID*, N_s, Res_{Serv}\}$, and $\mathrm{M}_5 : \{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{Uav}\}$) during the authentication phase. Under this game, $\mathcal{A}$ invokes the *Execute* query. After that, $\mathcal{A}$ makes the *Reveal* and *Test* queries to verify whether it is the real session key SK or a random number derived between the UAV and the USP. In the proposed AKE scheme, SK is computed as $SK = h(R_i^x||R_i^y||N_u||N_s)$. Thus, $\mathcal{A}$ needs to know the secret PUF responses (R_i^x, R_i^y) to compute the session key SK correctly. Eavesdropped messages do not help to increase the adversary's winning probability for the game $\mathcal{G}_1$. Therefore, $\mathcal{G}_1$ and $\mathcal{G}_0$ are indistinguishable, and we can write

$$Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} = Adv_{\mathcal{A},\mathcal{G}_0}^{AKE}. \tag{2}$$

Game $\mathcal{G}_2$: This game simulates an active attack by hash queries. Now, $\mathcal{A}$ needs to find a message digest collision in order to deceive a participant and this may be done by using multiple hash queries. However, it should be noted that all the imperative transmitted messages such as $\mathrm{M}_4 : \{PID*, N_s, Res_{Serv}\}$ and $\mathrm{M}_5 : \{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{Uav}\}$ are protected by using the secret PUF responses (R_i^x, R_i^y). Hence, the games $\mathcal{G}_2$ and $\mathcal{G}_1$ are indistinguishable. Here, it is assumed that the collision probability of the hash function is negligible when $\mathcal{A}$ sends several $Send(\mathcal{P}^t, Msg)$ queries. Thus, from the birthday paradox of the hash function, we can write the following:

$$\left|Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_2}^{AKE}\right| \leq \frac{q_h^2}{2|Hash|}. \tag{3}$$

Game $\mathcal{G}_3$: The difference between G_2 and G_3 is that simulations of the *Send* and PUF queries are included in G_3. In the proposed scheme, we assume that the PUFs used in the UAVs are secure as defined in Section V-B. Therefore, as in G_2, we also have:

$$\left|Adv_{\mathcal{A},\mathcal{G}_2}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_3}^{AKE}\right| \leq \frac{q_p^2}{2|PUF|}. \tag{4}$$

Game G_4: In this game, the simulation *CorruptDevice is* included. In this context, the adversary can obtain the

Table II
QUERIES AND DESCRIPTIONS

Query	Purpose
Execute $(\prod_U^{t_1}, \prod_S^{t_2})$	It is modeled as an eavesdropping attack where $\mathcal{A}$ can intercept the messages communicated between U and S.
Send $(\prod^t, \mathcal{M})$	It is modeled as an active attack where $\mathcal{A}$ can send message $\mathcal{M}$ to $\prod^t$, and then receive response from $\prod^t$.
Reveal $(\prod^t)$	$\mathcal{A}$ obtains the session key SK established between $\prod^t$ and its partner using this query.
CorruptDevice $(\prod^t)$	It is an active attack where $\mathcal{A}$ can obtain all the sensitive information.
Test $(\prod^t)$	$\mathcal{A}$ requests $\prod^t$ for session key SK and receives a probabilistic output based on an unbiased coin or hidden bit c: (i) if SK is fresh and $c=1$, $\prod^t$ returns SK, (ii) if SK is fresh and $c=0$, $\prod^t$ delivers a random number, and (iii) otherwise $\prod^t$ delivers null ($\perp$).

information $\{PID_u^i, \text{FID}\}$, stored in the UAV U_i. In the proposed scheme, an UAV is not requires to store any secret information (such as keys) in its memory. Hence, $\mathcal{A}$ cannot obtain any secret information using *CorruptDevice*. Therefore, $\mathcal{A}$ cannot gain any additional advantages by simulating this game. Now, an algorithm D can be constructed after solving *CorruptDevice* by running $\mathcal{A}$ on simulation of the protocol. Accordingly, $\mathcal{G}_3$ and $\mathcal{G}_4$ are indistinguishable. Therefore, we can write the following:

$$\left| Adv_{\mathcal{A},\mathcal{G}_3}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_4}^{AKE} \right| \leq \frac{q_{send}}{|D|}. \tag{5}$$

After all the games are executed, $\mathcal{A}$ tries to guess c to win the game using the *Test* query. Therefore,

$$Adv_{\mathcal{A},\mathcal{G}_4}^{AKE} = \frac{1}{2}. \tag{6}$$

Combining (1), (2), and (5), we have

$$\begin{aligned} \frac{1}{2}Adv_{\mathcal{A}}^{AKE} &= \left| Adv_{\mathcal{A},\mathcal{G}_0}^{AKE} - \frac{1}{2} \right| \\ &= \left| Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} - \frac{1}{2} \right| \\ &= \left| Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_3}^{AKE} \right|. \end{aligned}$$

Using the triangular inequality with (4), (5), and (6), we have the following:

$$\begin{aligned} \frac{1}{2}Adv_{\mathcal{A}}^{AKE} &= \left| Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_3}^{AKE} \right| \\ &\leq \left| Adv_{\mathcal{A},\mathcal{G}_1}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_2}^{AKE} \right| + \left| Adv_{\mathcal{A},\mathcal{G}_2}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_3}^{AKE} \right| \\ &\quad + \left| Adv_{\mathcal{A},\mathcal{G}_3}^{AKE} - Adv_{\mathcal{A},\mathcal{G}_4}^{AKE} \right| \\ &\leq \frac{q_h^2}{2|Hash|} + \frac{q_P^2}{2|PUF|} + \frac{q_{send}}{|D|}. \end{aligned} \tag{7}$$

Finally, by multiplying both sides of (7) by 2, we get:

$$Adv_{\mathcal{A}}^{AKE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_P^2}{|PUF|} + \frac{2q_{send}}{|D|}.$$

■

C. Informal Security Analysis

In this subsection, we present a discussion on the robustness of the proposed protocol against different attacks. The detailed description of the informal security analysis is given below.

1) Mutual Authentication: In our proposed protocol, both the UAV and the service provider (USP) can authenticate each other. The USP authenticates the UAV by checking the parameter Res_{Uav}, which must be equal to $h(EL||R_{i+1}^{x*}||R_{i+1}^{y*}||SK)$, where $SK = h(N_u||R_i^x||R_i^y||N_s)$. Now, if an adversary $\mathcal{A}$ wants to impersonate as an UAV, then he/she needs to know the secret PUF responses, i.e., R_i^x and R_i^y, which are unavailable to him/her. On the other hand, the UAV authenticates the USP by evaluating the parameter Res_{Serv}, which must be the same as $h(R_i^y||PID^*||N_u)$. Now, if the adversary $\mathcal{A}$ wants to impersonate as a USP, then he/she needs to know the secret PUF response R_i^y, which is unavailable to him/her. As a result, the proposed scheme ensures mutual authentication and achieves security against impersonation attacks.

2) Resistance Against Tracking and Eavesdropping Attacks: An authentication protocol is said to be vulnerable against tracking and eavesdropping attacks if an adversary $\mathcal{A}$ can easily listen to the communication messages over a public channel and can retrieve any useful information from them. In the proposed protocol, each message is refreshed after every session which makes the adversary unable to extract any kind of useful information. For instance, in the proposed scheme, none of the parameters are allowed to be sent twice. Therefore, our designed protocol can withstand tracking and eavesdropping attacks.

3) Anonymity of UAVs: In the proposed scheme, the MEC is a third-party communication/computing service provider. When the MEC operator receives $\mathrm{M}_4 : \{PID^*, N_s, C_i, Res_{Serv}\}$ and $\mathrm{M}_5 : \{R_{i+1}^{x*}, R_{i+1}^{y*}, Res_{Uav}, EL\}$ from the USP and the UAV, respectively, then it may try to establish the identity of the UAV. However, each parameter in M_4 and M_5 is allowed to be sent only once. Hence, the MEC operator cannot identify the UAV. It should be noted that in the proposed scheme, for any two consecutive sessions i and i+1, $PID_u^i \neq PID_u^{i+1}$. Thus, it is difficult for an adversary to identify a particular UAV and this forms the basis for the proposed protocol's robustness against attacks on UAV anonymity.

4) Security Against Physical Attacks: In many application scenarios for UAVs, the drones collect important and sensitive information from the deployed environment and sends this

Table III
SECURITY FEATURE'S COMPARISON OF PROPOSED SCHEME WITH RESPECT TO TIAN ET AL.'S SCHEME[15]

Security Features	Tian et al. [15]	Zhang et al. [16]	Srinivas et al. [17]	Proposed Scheme
Mutual Authentication	Yes	No	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes
Security Against Forgery Attacks	Yes	Yes	Yes	Yes
Location Threat	No	No	No	Yes
Req. of Clock Synchronization	Yes	Yes	Yes	No
Physical Security of the UAV	No	No	No	Yes

Table IV
PERFORMANCE COMPARISON BASED ON COMPUTATION, COMMUNICATION, AND STORAGE COST

Cost	Tian et al. [15]	Proposed Scheme
Computation Cost at UAV	$E_{t_m} + E_{t_a} + E_{t_h} \simeq 33.77$ ms	$2E_{t_p} + 6E_{t_h} \simeq 4.76$ ms
Computation Cost at USP	$E_{t_{se}} + E_{t_m} + 2E_{t_h} \simeq 17.96$ ms	$7E_{t_h} \simeq 0.20$ ms
Communication Cost	916 bytes	224 bytes
Storage Cost at the UAV	296 bytes	96 bytes

information to the control center. To ensure privacy of the data, some applications may require the drone to encrypt the data by using a secret key (stored in drone's memory). However, a drone may experience a range of natural or adversarial conditions which can compromise it physical security. For example, an UAV may be involved in an accident or component failure which leads to a crash and the drone may eventually be found by the adversary. Similarly, an adversary may shoot down the UAV and physically capture it. An adversary can then obtain the secret key from the memory of the drone, and thus gain access to the encrypted data stored in the UAV. In the proposed scheme, an UAV does not store any secret keys in its memory. Therefore, even if an adversary physically captures the drone, he/she cannot get any secrets from the UAV's memory. Besides, if the adversary attempts to do any physical tampering on the drone's hardware, then the behavior of the PUFs will be changed and they will not generate the intended response. Therefore, the USP will be able to reject authentication attempts by UAVs with tampered hardware and the proposed protocol can ensure security against physical attacks on UAVs. In addition, since PUFs also provide the properly of uncloneability, the adversary cannot create a copy of the PUFs attached with the UAV.

5) Security Against Location Threats: In real-time applications with UAVs, an absence of the ability to track the location of the UAVs may allow an attacker to send incorrect location information regarding the UAVs to the USP by using spoofed/false signals. As described in our system model, a MEC operator may do the same in order get more service charge from the USP. However, in our proposed scheme, the USP can identify the UAV's exact location by using the parameter LAI_u. In order to obtain this parameter, the USP needs to use the PUF response R_i^x and the random number N_s, i.e., $LAI_u = EL \oplus h(R_i^x||N_s)$ and after decoding LAI_u from EL, the USP checks this LAI_u with the location of the MEC operator ID_{MEC}. In this way, the USP can keep track of the current location of the UAV and address any disputes with the MEC operator regarding the UAV's location.

6) No Requirement of Clock Synchronization: In general, to protect against replay attacks, most of the existing protocols in the literature use the concept of timestamps. In this approach, it is important for the participants of the protocol to synchronize their clocks. However, there is no need for clock synchronization in the proposed protocol. This is because in every session, specific random numbers are being used instead of timestamps.

VI. PERFORMANCE EVALUATION

In this section, we first compare the performance of the proposed scheme with that of three recently proposed IoD-based authentication schemes ([15], [16], and [17]) from the perspective of various security features. Subsequently, to ensure a fair comparison, we compare the proposed protocol with the scheme presented in [15] in terms of the execution time, computation overhead, and communication overhead. The protocol from [15] is chosen for this comparison because it uses the same underlying MEC-based environment as the proposed protocol. In contrast, [16] and [17] are primarily two-party-based authentication schemes.

A. Security Functionality

Table III shows the security capabilities of the proposed protocol as compared to the protocols presented in [15], [16], and [17]. As discussed in Section II, the protocol presented in [16] is vulnerable to forgery attacks, and hence it cannot ensure mutual authentication. In general, to keep the latency low and ensure seamless services, the MEC operator supports the UAVs by using computational infrastructure positioned close to the wireless infrastructure. However, in the protocol presented in [15], if a MEC node sends false signals (e.g., in terms of its location) to an UAV, there is no way to detect that. In contrast, the proposed protocol can easily detect such attempts by using the parameter LAI_u. Next, in the protocols proposed

in [15], [16], and [17], the UAV needs to store all the secret information (e.g., keys) in its memory. Thus, if an adversary obtains physical access to the drone, it can obtain the secret key from the memory of the UAV or change the settings of the UAV. Then, if the adversary uses this compromised UAV to send false information or manipulated information to the USP, the USP will not be able detect such attacks. Therefore, the protocols presented in [15], [16], and [17], cannot ensure security against physical attacks. Finally, unlike [15], [16], and [17], the proposed scheme does not use any timestamps to ensure security against replay attacks.

B. Computation Cost

We compare the computation cost by evaluating the overall execution time (in milliseconds) required by the cryptographic operations performed in Tian et al.'s protocol [15] and in the proposed scheme (since both of these schemes are based on MEC-enabled scenarios). The basic cryptographic operations used for computing the execution time are hash operation, simultaneous exponentiation operation, modular multiplication, modular addition, and PUF operation, and the expected time to execute them are denoted by E_{t_h}, $E_{t_{se}}$, E_{t_m}, E_{t_a}, and E_{t_p}, respectively. All the cryptographic operations (corresponding to E_{t_h}, E_{t_m}, $E_{t_{se}}$, E_{t_a}, and E_{t_p}) used on the UAV side are implemented on a ATMel ATMega2560 machine with a MSP430 micro-controller , while the operations used at server side (USP) are implemented on a desktop computer with Intel Core i7 processor with 16 GB RAM. For evaluating the execution time of these crypto-operations, we utilized the Java Cryptography Extension (JCE) library. We consider SHA-256 for hash operation, and for PUF operation, we consider a 128-bit arbiter PUF circuit. The PUF operation is conducted on the ATMel ATMega2560 machine. The values of E_{t_h}, E_{t_m}, $E_{t_{se}}$, and E_{t_a} at the USP are 0.029 ms, 13.7 ms, 4.26 ms, and 2.68 ms, respectively. Similarly, the values of E_{t_h}, E_{t_m}, $E_{t_{se}}$, E_{t_a}, and E_{t_p} at the UAV are 0.37 ms, 27.84 ms, 8.26 ms, 5.93 ms, and 1.27 ms, respectively. Based on these values, the time taken to execute the proposed protocol's operations at the UAV is $2E_{t_p} + 6E_{t_h} = 4.76$ ms, which is significantly lower than that required by Tian et al.'s scheme (33.77 ms). The detailed analysis of the computation time is given in Table 4. From Table 4 we can see that our entire authentication process takes 4.96 ms of computation time. In comparison, the entire authentication process in [15] takes 51.73 ms of computation time. Figure 3 shows that the performance of the proposed scheme in terms of computational overhead is significantly lower than that of Tian et al.'s scheme [15].

C. Other Costs

We now compare the communication and storage cost of the proposed protocols with that of Tian et al.'s scheme [15]. The communication cost of Tian et al.'s scheme is 916 bytes, whereas the communication cost of the proposed scheme is 224 bytes, which is significantly lower. In terms of storage cost, in Tian et al.'s scheme, an UAV needs to store 296 bytes of secret information. In comparison, in the proposed scheme an UAV needs to store $\{(PID_u^i, \text{FID})\}$ that requires $128+n\times$ 128 bits, where the maximum value of n is chosen to be 5. In that case, the storage cost of the proposed scheme at an UAV is only 96 bytes, which is significantly lower than than of [15]. Thus, we can conclude that the proposed protocol is efficient in term of storage and communication costs while providing reliable security features.

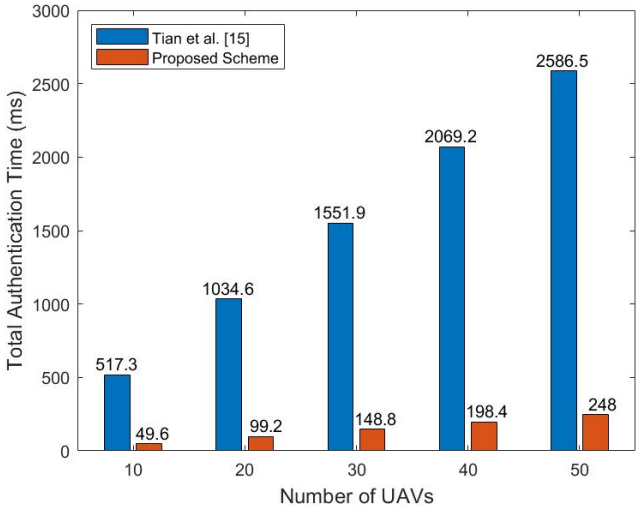

Figure 3. Authentication time as a function of the number of UAVs.

ACKNOWLEDGEMENTS

This research is supported by the National Research Foundation, Singapore under its Strategic Capability Research Centres Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

VII. CONCLUSION

Small-scale unmanned aerial vehicles have attracted increasing attention from both industry and academia due to their capability to assist a wide spectrum of applications, ranging from package delivery to surveillance. Similar to vehicular ad hoc networks (VANETs), edge assisted UAVs is a promising approach to provide connectivity, enhance flying safety, and ensure service quality of UAVs. However, connecting UAVs through third-party edge devices also brings security and privacy risks due to the open-access communication environment. In this paper, we proposed an efficient authenticated key agreement scheme for edge-assisted UAV environments. The proposed protocol utilizes computationally inexpensive cryptographic functions such as PUFs and hash operations. We have critically verified and evaluated the proposed protocol with the help of formal and informal security analysis in order to show its adequacy, security, and robustness. The informal security analysis shows that the proposed protocol has the ability to resist major security attacks. Moreover, we compared our protocol with a recently proposed protocol in terms of their performance and overhead. The performance analysis shows that our protocol is secure, efficient and agile as compared to the related protocol.

REFERENCES

[1] T. Tomic, K. Schmid, P. Lutz, A. Domel, M. Kassecker, E. Mair, I. L. Grixa, F. Ruess, M. Suppa, D. Burschka, Toward a fully autonomous uav: Research platform for indoor and outdoor urban search and rescue, IEEE Robotics Automation Magazine 19 (3) (2012) 46–56.

[2] L. Merino, F. Caballero, J. R. Mart´ ınez-de Dios, I. Maza, A. Ollero, An unmanned aircraft system for automatic forest fire monitoring and measurement, Journal of Intelligent & Robotic Systems 65 (1) (2012) 533– 548.

[3] M. Bhaskaranand, J. D. Gibson, Low-complexity video encoding for uav reconnaissance and surveillance, in: 2011 - MILCOM 2011 Military Communications Conference, 2011, pp. 1633–1638.

[4] I. Sa, S. Hrabar, P. Corke, Outdoor Flight Testing of a Pole Inspection UAV Incorporating High-speed Vision, Springer International Publishing, Cham, 2015, pp. 107–121.

[5] Federal Aviation Administration, FAA Aerospace Forecast, 2016-2036, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf.

[6] Amazon.com, Inc., Amazon Prime Air, https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011.

[7] A. Koubaa, B. Qureshi, M. F. Sriti, Y. Javed, E. Tovar, A ˆ service-oriented cloud-based management system for the internet-ofdrones, in: 2017 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC), 2017, pp. 329–335. doi:10.1109/ICARSC.2017.7964096.

[8] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in uav communication networks, IEEE Communications Surveys Tutorials 18 (2) (2016) 1123–1152.

[9] C. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel, X. Huang, Security and privacy for the internet of drones: Challenges and solutions, IEEE Communications Magazine 56 (1) (2018) 64–69. doi:10.1109/MCOM.2017.1700390.

[10] X. Lin, X. Sun, P. H. Ho, X. Shen, Gsis: A secure and privacy-preserving protocol for vehicular communications, *IEEE Transactions on Vehicular Technology*, Vol. 56 (6) (2007) 3442–3456.

[11] R. Lu, X. Lin, H. Zhu, P. H. Ho, X. Shen, Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications, in: INFOCOM 2008. *The 27th Conference on Computer Communications*. IEEE, 2008.

[12] L. Yang, H. Zhang, M. Li, J. Guo, H. Ji, Mobile edge computing empowered energy efficient task offloading in 5g, *IEEE Transactions on Vehicular Technology*, PP (99) (2018) 1–1.

[13] G. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in: Design Automation Conference, DAC '07, 44th ACM/IEEE, 2007, pp. 9–14.

[14] M. Abdalla et al., "Password-based authenticated key exchange in the three-party setting, " Proc. Public key Cryptogr., pp. 65-84, 2005.

[15] Y. Tian, J. Yuan and H. Song, "Efficient privacy-preserving authentication framework for e dge-assisted Internet of Drones, " *Journal of Information Security and Applications* 48 (2019) 102354 .

[16] Y Zhang, D He, L Li, B Chen, A lightweight authentication and key agreement scheme for internet of drones, *Computer Communications*, 154 (2020) 455–464.

[17] J. Srinivas, A. Das, N. Kumar, and J. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Transactions on Vehicular Technology*., vol. 68, no. 7, pp. 6903-6916, Jul. 2019.

[18] G Cho, J Cho, S Hyun, H Kim, "SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles, " *Applied Sciences*, 2020.

[19] L Teng, M Jianfeng, F Pengbin, M Yue, " Lightweight Security Authentication Mechanism Towards UAV Networks " *International Conference on Networking and Network Applications (NaNA)*, 2019.

[20] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. 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, 2019.

[21] L. Yang, H. Zhang, M. Li, J. Guo, H. Ji, " Mobile edge computing empowered energy efficient task offloading in 5g, " *IEEE Transactions on Vehicular Technology*, PP (99) , 2018.

[22] P. Gope et al., "Anonymous communications for secure device-to-device-aided fog computing: architecture, challenges, and solutions," *IEEE Consumer Electronics Magazine*, Vol. 8(3), pp. 10 - 16, 2019.

[23] J. Delvaux, D. Gu, I. Verbauwhede, M. Hiller, and M-D Yu, "Efficient Fuzzy Extraction of PUF-Induced Secrets: Theory and Applications," *In: Cryptographic Hardware and Embedded Systems (CHES).* LNCS vol. 8913 pp. 412-430, Springer (2016).

[24] P. Gope, "PMAKE: Privacy-Aware Multi-Factor Authenticated Key Establishment Scheme for Advance Metering Infrastructure in Smart Grid," *Computer Communications*, Volume 152, pp. 338-344 (2020).

[25] A. Van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A. Sadeghi, I. Verbauwhede, C. Wachsmann, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," *In: Keromytis, A.D. (ed.) FC 2012.* LNCS, vol. 7397, pp. 374-389. Springer, Heidelberg

Prosanta Gope (M'18) is currently working as an Assistant Professor (Lecturer) in the Department of Computer Science (Cyber Security) at the University of Sheffield, UK. Dr. Gope served as a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). Primarily driven by tackling challenging real-world security problems, he has expertise in lightweight anonymous authentication, authenticated encryption, access control, security of mobile communications, healthcare, Internet of Things, Cloud, RFIDs, WSNs, SmartGrid and hardware security of the IoT devices. He has authored more than 75 peer-reviewed articles in several reputable international journals and conferences and has four filed patents. He received the *Distinguished Ph.D. Scholar* Award 2014 by National Cheng Kung University (Taiwan). Several of his papers have been published in high impact journals such as IEEE TIFS, IEEE TDSC, IEEE TIE, IEEE TII, IEEE TSG, IEEE JBHI, IEEE TVT, etc. Dr. Gope has served as TPC member in several international conferences such as IEEE GLOBECOM, ARES, etc. He currently serves as an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE SYSTEMS JOURNAL, IEEE SENSORS JOURNAL, the *Security and Communication Networks*, and the *Mobile Information Systems Journal*.

Biplab Sikdar (S'98-M'02-SM'09) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include computer networks, and security for IoT and cyber physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing.