SPAKE-DC: A Secure PUF Enabled Authenticated Key Exchange for 5G-Based Drone Communications

Azeem Irshad, Bander A. Alzahrani, Aiiad Albeshri, Khalid Alsubhi, Anand Nayyar, *Senior Member, IEEE*, and Shehzad Ashraf Chaudhry, *Member, IEEE*

***Abstract*—The tremendous growth in the realm of Internet of Things (IoT) has materialized the architecture of Internet of Drones (IoD). Being an extension of the IoT technology, the IoD may control and monitor the drones in a particular flight area. The emerging 5G mobile communication infrastructure can greatly help in transmitting the High-Definition (HD) data making the drones to communicate even faster. Nonetheless, these drones remain vulnerable to known security threats due to exchange of communication messages on public channel. In addition, the drones may also be exposed to physical capture and examination by the malicious adversaries. Thus, more concerted efforts are required to address the security challenges for drone communication in IoD-based ecosystem. We propose a novel PUF-based authentication protocol SPAKE-DC to protect not only the drone communication on public channel but also if the drone is physically intercepted with captured resources. The SPAKE-DC protocol supports anonymity, mutual authenticity, perfect forward secrecy, and is also immune from drone physical capture attack. The proposed scheme is duly evaluated and formally analyzed under Real-or-Random Oracle model. The performance results show that SPAKE-DC carry convincing findings in terms of security, computation and communication. Moreover, it supports 42% more number of security features as compared to previous techniques.**

***Index Terms*—Authentication, Internet of Things (IoT), Internet of Drones (IoD), 5G network.**

I. Introduction

THE IoT network is undeniably capable of meeting the needs of users by collecting real-time information from a particular network area having deployed sensors in the field. Due to the limited communication distance, the IoT nodes employ Bluetooth or WiFi-based data transmission modes [1]. Thus, the research academia came with many related research studies with respect to fourth generation (4G) mobile communication for supporting high data rates and even extending the communication range for remote users. Nonetheless, the speed of transmission of data is unsteady, slow and sparse coverage. As a result, a novel fifth generation (5G) mobile communication architecture was adopted to meet the high bandwidth needs of remote users [2], [3]. The adoption of 5G communication technology for IoT applications enhances the signal coverage, equipment access, as well as stability of the signal.

Lately, we can witness that due to the massive adoption of artificial intelligence and IoT-based technologies, the UAV networks are being adapted into IoT-led Internet of Drones (IoD) [4]. This gives rise to numerous openings for the highly sophisticated UAV applications. These drones could be monitored with a ground station controller. Moreover, these drones may include sensor, actuator, communicating module, recorder and receiver. The drones have been mostly inducted in military application, but it is now finding civil applications as well such as surveillance and monitoring, entertainment and aerial photography, disaster reporting, and inspection scenarios etc. The IoD bears the same communication technology as is adopted for IoT. The IoT-oriented drones bear limited communication range for restricted support of distance of Bluetooth and WiFi. Therefore, research academia came forward with a novel mode of communication that engages base stations for connecting and monitoring drones. Since the 4th generation technology might face resolution and positioning issues while capturing the scenarios, we can witness many security solutions for internet of drones with the combination of 5G technology. The 5G may support secure communication of high-definition data with less latency, and eventually less delay in the implementation of ground-based commands and instructions [5], [6], [7]. The architecture for IoD is depicted in Fig. 1. The architecture for internet of drones comprises user, drone, server and ground control station. The user acquires up-to-date real time information from drones inducted in any specific geographical domain. The drones are embedded with sensors and built-in cameras to monitor the physical environment and capture the targeted snaps. The users submit a request query to servers for obtaining the up-to-date status of drones in any area. Those servers locate the deployed drones in a particular domain and get authenticated with that

Manuscript received 12 January 2023; revised 1 June 2023 and 6 September 2023; accepted 10 November 2023. Date of publication 30 November 2023; date of current version 22 April 2024. The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under grant no. (RG-5-611-43). The review of this article was coordinated by Prof. Quan Yu. *(Corresponding authors: Anand Nayyar; Shehzad Ashraf Chaudhry).*

Azeem Irshad is with the Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan (e-mail: irshadazeem2@gmail.com).

Bander A. Alzahrani, Aiiad Albeshri, and Khalid Alsubhi are with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: baalzahrani@kau.edu.sa; aaalbeshri@kau.edu.sa; kalsubhi@kau.edu.sa).

Anand Nayyar is with the Graduate School, Faculty of Information Technology, Duy Tan University, Da Nang, Vietnam (e-mail: anandnayyar@duytan.edu.vn).

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, Istanbul , Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/TVT.2023.3333398

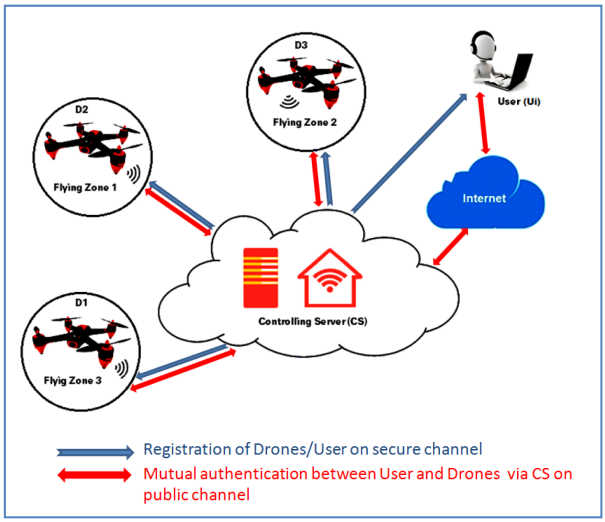


Fig. 1. System model.

drone to obtain the captured information. The information is then transmitted using 5G technology for meeting the needs of the user.

Nevertheless, the drones in an IoD setting may always be vulnerable to attacks including forgery, privacy and physical capture attacks due to communication on public channel and the induction of drones in hostile environment [8]. The communication data might be significantly critical for its confidentiality and importance. If it becomes available to attackers on public channel, it could be detrimental for the organization. In addition, the drones that are being flown in a particular field or area could also be accessed physically by malicious entities. In this way, the later may recover its data from its memory and manipulate for its mala fide intentions. These issues necessitate the design of secure and robust security protocols for ensuring protection communication. Since the drones carry limited computational and storage resources, these contributed protocols must be lightweight however with adequate security requirements. This study takes a thorough review of the current security protocols in IoT-based drones and then we propose an efficient and secure PUF-oriented protocol in the light of pointed drawbacks in state-of-the-art IoT-based authentication protocols. We used Physical Unclonable Function (PUF) circuit for securing the drone from physical capture attacks. The drones are open to physical attacks due to its nature of operations, and require an extra effort to protect its memory from physical capture threats. The drones need not store contents in its memory due to embedded PUF chip which is unique and unclonable for its manufacturing properties.

The objectives of the paper are as follows:

- To conduct the background study and enlighten Literature review by coming up with a resilient and efficient authenticated key agreement (AKA) scheme for power-deficient IoT-enabled drones.
- To propose a secure PUF-oriented AKA scheme, i.e., SPAKE-DC for establishing an agreed session key between user and drone which not only provides anonymity to the user but also warrants mutual authentication, perfect forward secrecy and immunity from drone physical capture attack.
- To test and validate the proposed scheme in terms of supported security features, computational and communicational costs.
- To evaluate the SPAKE-DC protocol under rigorous Real-or-Random (RoR) Oracle model, and depict in the respective sections of performance evaluation, formal and informal analysis that SPAKE-DC protocol supports enhanced security features as compared to other existing techniques [9], [18], [19], [20], [21], [22], [23], [24], [33].

A. Scheme Organization

The paper is organized as follows: Section II describes the related work. Section III illustrates the preliminary details including system model. The proposed authentication scheme is elaborated in section IV. Section V presents informal and formal security analysis. Section VI demonstrates the comparative analysis and performance of various schemes. Section VII concludes the paper.

II. Related Work

There are many studies focusing on the design of up-to-date authentication protocols for Internet of Things (IoT) intending to cure the most recent flaws in those protocols. In this regard, Turkanovic et al. [9] presented a lightweight authenticated key agreement (AKA) scheme for IoT system in 2014. Nonetheless, Farash et al. [10] indicated that the scheme [9] does not offer anonymity to the users as well as sensors, and is vulnerable to sensor-impersonation threat, stolen smart card threat and session key disclosure threat. In addition, Farash et al. presented an improved scheme for Turkanovic et al. and asserted that it is more security resilient than scheme [9]. Nonetheless, Amin et al. [11] presented a three factor AKA scheme that claims that the protocol is capable of achieving anonymous protection. Afterwards, we can witness few studies with the combination of 5G and IoT in the literature [12], [13], [14]. Lee et al. [12] in 2020 demonstrated a cross-layer authentication scheme designed for physical layer. Meanwhile, Jangirala et al. [13] put forward a blockchain-oriented authentication protocol. This scheme employs bit rotation operation and radio frequency identification (RFID) for implementing the security in IoT based system. Later, Ayub et al. [14] presented another AKA schemefor IoT environment based on elliptic curve encryption (ECC) operations. Lately, many authentication schemes for IoD environment can be witnessed [15], [16], [17], [18], [19], [20], [21], [22]. The IoD architecture enables the secure communication of users, control room and smart devices with drones. Most of the above frameworks enable the secure interaction between users and drones. However, there might be other applications that require protected communication between drones and other external smart gadgets in IoT-based ecosystem. In this regard, Bera et al. [15] proposed a blockchain-oriented controlling protocol employing ECC, hash and digital signature based crypto-primitives. Then Tian et al. [16] introduced a privacy preserving authentication scheme for

TABLE I
TABULAR DEPICTION OF STATE-OF-THE-ART LITERATURE

Scheme	*Features*	*Limitations*	*Year*
Turkanovic *et al*. [9]	(AKA) scheme for IoT system	The protocol lacks anonymity	2014
Amin *et al*. [11]	Anonymous three factor AKA scheme	Lacking mutual authentication	2016
Teng *et al*. [17]	ECC-based lightweight protocol	It sends costly messages through public key infrastructure (PKI)-based encryption.	2017
Wazid *et al*. [22]	An anonymous AKA scheme	No mutual authenticity and prone to forgery and insider threats	2018
Srinivas *et al*. [20]	An authentication scheme based on temporal credentials	Stolen verifiers threat, lacks mutual authenticity and anonymity	2019
Chen *et al*. [23]	anonymous authentication scheme for IoD environment	Replay and temporary information disclosure threats	2020
Zhang *et al*. [24]	a lightweight authentication protocol for drones	Traceable and prone to stolen smart card attack	2020
Hussain *et al*. [19]	a symmetric encryption key-based authentication protocol for drones inducted in smart cities	vulnerable for drone capture, forgery and privileged insider threats	2022
Pu *et al*. [37]	Bilinear Pairing and PUF Based Lightweight Authentication Protocol for IoD Environment	Costly bilinear pairing operations	2022

IoD environment based on modular multiplication and costly digital signatures. Furthermore, Teng et al. [17] designed another ECC-based lightweight protocol that sends costly messages through public key infrastructure (PKI)-based encryption. Ever et al. [18] demonstrated another AKA scheme to achieve authentication between drones and users, however it used costly bilinear pairing operations. In addition, the protocol [18] was vulnerable to drone capture threats and is neither anonymous nor untraceable for the user. Later, Hussain et al. [19] presented a symmetric encryption key-based authentication protocol for drones inducted in smart cities. However, it was found to be vulnerable for drone capture, forgery and privileged insider threats. Most of the above protocols are costly for computations and could be hard to implement in drone-orient low-end applications.

Thereafter, few research studies can also be seen employing lightweight crypto-primitives for AKA protocols in drone environment. In 2019, Srinivas et al. [20] presented an authentication scheme that was based on temporal credentials. Later, Ali et al. [21] pointed that [20] is vulnerable to few threats based on stolen verifiers, mutual authenticity and anonymity. Meanwhile, Wazid et al. [22] introduced an anonymous AKA scheme, however it does not provide mutual authenticity, and is also prone to forgery and insider threats. Chen et al. [23] designed an anonymous authentication scheme for IoD environment, however it was vulnerable to replay and temporary information disclosure threats. Later, Zhang et al. [24] presented a lightweight authentication protocol for drones, however the scheme is not untraceable, and is also prone to stolen smart card attack.

Recently, few latest schemes in IoD have been presented with the combination of 5G communication technology for improving the transmission bandwidth and security. Abdel-Malek et al. [25] introduced a two-factor 5G authentication scheme for drones. Abdel-Malek et al. [26] presented another signature-based 5G authentication protocol. Later, Alladi et al. [40] also demonstrated a PUF-based 5G protocol to ensure mutual authenticity among the user, drone and 5G oriented base stations. The summary of related work is depicted in Table I.

III. PRELIMINARIES

This section throws light on preliminaries including Physical Unclonable Function, system model and threat model as elaborated below:

A. Physical Unclonable Function

The Physical Unclonable Function (PUF), being a physical circuit, can map a bit-string pair termed as Challenge-Response Pair [30]. A PUF circuit takes a random number as input challenge and generates a unique outcome of an arbitrary bit string. In this protocol, the PUF circuit is used for generating a unique secret after inputting a random integer, without storing it in the drone's memory. In this manner, many security features including perfect forward secrecy may be duly ensured.

Some features of PUF are given below:

- It is quite intricate to clone or replicate an existing PUF circuit.
- The PUF being a physical micro structure is embedded in other device.
- The resultant outcome of the PUF is always unpredictable.
- The hardware security is enhanced with the exploitation of PUF-based inherent device variations.

B. RoR Model

The suggested model is evaluated under formal analysis based on Random or Real (RoR) model [3], [31] that studies the properties of semantic security, proofs and the extent to which the SPAKE-DC attains the required level of session key (SK) security. The SPAKE-DC comprises three participating entities including Ui, Dj and CS. In this model, we assume that $\prod_{U_i}^{a}$, $\prod_{D_j}^{b}$ and $\prod_{CS}^{c}$ characterize the a-th, b-th and c-th instance of Ui, Dj and CS respectively which may also be called as oracles. We also assume that the attacker bears the understated query-based competencies: $Q_R = \{\prod_{U_i}^{a}, \prod_{D_j}^{b}, \prod_{CS}^{c}\}$.

- *Execute*(Q_R): Using the Execute query, the attacker may eavesdrop the communicated messages among the entities Ui, Dj and CS on the public channel.
- *Send*(Q_R, M_{sg}): Using the Send query, the attacker may send as well receive the message M_{sg} to and from the entity Q_R.
- *Hash_*Q_R*(string):* This hash query may be performed by adversary that returns the corresponding hash value after receiving any random input string.
- *Reveal*(Q_R): Using the Reveal query, the adversary may get the private secrets including high entropy long term keys,

smart card credentials, and short term temporary random values.

Test(Q_R): After the execution of this query, the attacker may flip an unbiased coin C. In case, it gets C = 1, the attacker might recover the accurate session key. In case it gets C = 0, the attacker is returned a random string with an equivalent length of session key SK.

C. System Model

The generic system model comprises of a controlling server (CS), user (U_i) and drone (D_j) as shown in Fig. 1. As per the UAV-based network model, different drones D_j collect the sensed data in their specific zones of a target domain, and submits that data towards CS. There might be some external user who wants to access the data of drones deployed in various fields, it must connect with the controlling server. To access the data, a secure key agreement is needed between U_i and D_j while this key agreement takes place through CS. Thereafter, U_i and CS come into agreement with a mutual session key and initiate communication. The detail of entities is described as under:

User (U_i): The U_i registers with CS to receive secret credentials for possible secure communication with D_j.

Controlling server (CS): The controlling server serves as a trusted authority with adequate computing resources. Moreover, it mediates and enables the authentication process between U_i and D_j. During registration process, it furnishes the credentials to user U_i and drone D_j, using their respective identities.

Drone (D_j): The D_j collects the sensed data from a particular flying zone (FZ). It is also registered from CS for establishing a secure communication session with a particular U_i. After collection it submits the data to U_i for further calculations.

D. Threat Model

The threat model is referred to assume the capabilities of the adversary for initiating the attack on protocol. In our scheme, we used eCK-based threat model [27], [28] where the attacker $\mathcal{A}$ is supposed to be capable enough for controlling and monitoring the insecure communication channel. To be more precise, the attacker may eavesdrop on the communication over public channel among user, controlling server and drones. It may edit, delete, insert, replay and forge the exchanged messages among entities. It might even prevent the message being communicated on the communication channel in some way or other. The attacker, upon the application of power differential analysis [29], may read the transmitted data from physically stolen smart card as well as memory of physically detained drone. It might have the complete knowledge of the identities of legal entities, and could attempt to initiate other attacks on the basis of those identities. On the other hand, $\mathcal{A}$ could not recover the private key of any legitimate member. The symbols used in this scheme are given in Table II.

IV. Proposed Scheme

The proposed scheme comprises three main phases such as drone registration phase, user registration phase and mutual authentication phase. The proposed model contains three key entities that participate in the protocol to agree on a mutually agreed session key which lets the entities to securely communicate onwards. The detail of these sections is illustrated below.

TABLE II
Symbols with Definitions

Symbols	Definition
CS, U_i, D_j:	Controlling Server, i^{th} User, j^{th} drone
ID_u, ID_d:	Identities of U_i and D_j
K_p:	Master secret key of *CS*
k_u, k_d	Random integers for U_i and D_j (Registration)
PID_u:	Pseudo-identity of U_i
PUF_i:	Physical Cloneable Function for U_i
PWD_u/BIO_u	Password and Biometric identity of U_i
GEN()/REP():	Fuzzy Extractor Generation and Reproduction
n_1 , n_2, n_3	Random integers (short term secrets)
$\mathcal{A}$:	Malicious adversary
SK:	Session key between U_i and D_j
$\oplus$, $\|\|$, h(.)	XOR, Concatenation, One-way hash function

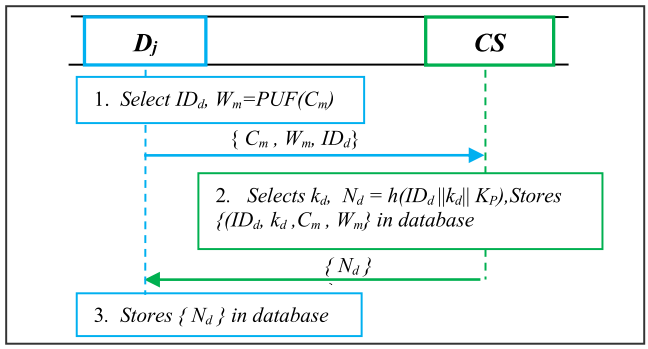


Fig. 2. Registration of Drone (D_j).

A. Drone Registration Phase

The drones D_j are registered with Controlling Server CS. The registration procedure is given below:

i) First the drone D_j selects its identity as ID_d and computes $W_m = PUF(C_m)$ using PUF circuit. Then it submits the message $\{C_m, W_m, ID_d\}$ to CS on secure channel.
ii) The CS selects k_d and computes $N_d = h(ID_d \| k_d \| K_p)$ and stores $\{(ID_d, k_d, C_m, W_m\}$ in database. Then it submits the message $\{N_d\}$ to D_j.
iii) The D_j stores N_d safely to finalize the registration as shown in Fig. 2.

B. User Registration Phase

The users U_i are registered with Controlling Server CS. The registration steps in this phase are mentioned below:

i) First the Ui selects its identity ID_u, password PWD_u, and imprints its biometric identity BIO_u. Next it selects a random integer q and computes $Gen(BIO_u) = (\delta_u, \eta_u)$. Then it sends the identity ID_u to *CS* on secure channel for further proceedings.
ii) The *CS* after receiving the message chooses k_u and PID_u. Then it computes $JID_u = h(ID_u \| k_u)$, $N_u = h(JID_u \| k_u \| K_p)$, $JID_u* = JID_u \oplus h(k_u \| K_p)$ and stores $\{PID_u, JID_u*,$

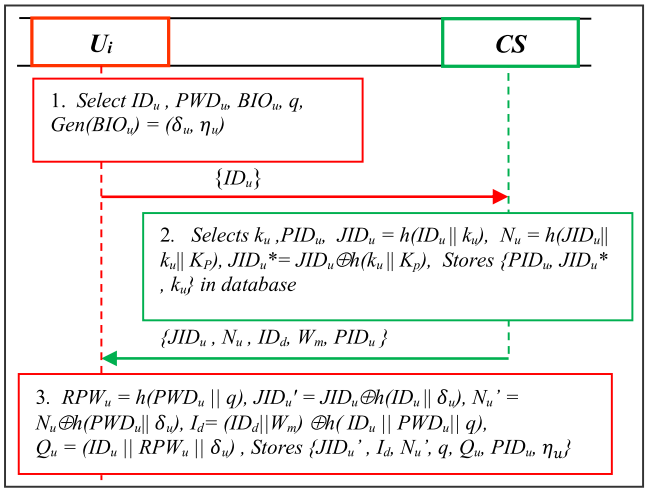


Fig. 3. Registration of User (Ui).

$k_u\}$ in its repository. Next it sends the message $\{JID_u, N_u, ID_d, W_m, PID_u\}$ to complete the registration procedures as shown in Fig. 3.

iii) Upon the receipt of message from CS, the Ui computes $RPW_u = h(PWD_u \| q)$, $JID_u' = JID_u \oplus h(ID_u \| \delta_u)$, $N_u' = N_u' \oplus h(PWD_u \| \delta_u)$, $I_d = (ID_d \| W_m) \oplus h(ID_u \| PWD_u \| q)$, $Q_u = (ID_u \| RPW_u \| \delta_u)$ and stores the parameters $\{JID_u', ID_d', N_u', q, Q_u, PID_u, \eta_u\}$ in its database.

C. Mutual Authentication Phase

In mutual authentication phase, the U_i and D_j develop an agreed session key *SK* with the help of CS. The steps can be pictorially seen in Fig. 2, and are also elaborated below:

i) First the U_i inserts its identity ID_u, password PWD_u, imprints biometric identity BIO_u and computes $\delta_u' = Rep(BIO_u, \eta_u)$, $RPW_u = (PWD_u \| q)$, $Q_u* = (ID_u \| RPW_u \| \delta_u)$. Then it checks the equality $Q_u' ? = Q_u$. It terminates the session if it does not hold true. Otherwise, further computes $JID_u = JID_u' \oplus (PWD_u \| \delta_u')$, $(ID_j \| W_m) = I_d \oplus (ID_u \| PWD_u \| q)$, $N_u = N_u' \oplus (PWD_u \| \delta_u')$. Next, it selects n_1, T_1 and PID_u^{New} and computes $Z_1 = h(JID_u \| T_1) \oplus n_1$, $Z_2 = ID_d \oplus h(N_u \| JID_u \| T_1)$, $Z_3 = h(n_1 \| JID_u \| N_u \| T_1) \oplus PID_u^{New}$, $R_1 = h(JID_u \| ID_d \| n_1 \| T_1)$. Finally it sends the message $M_1 = \{Z_1, Z_2, Z_3, R_1, PID_u, T_1\}$ towards *CS* on public channel for verification.

ii) After receiving the message, the CS verifies the timestamp $T_1 - Tc < \Delta T$. If it is not true, it aborts. Otherwise, it searches its database for the entry $\{JID_u*, k_d\}$ against PID_u, then it computes $JID_u = JID_u* \oplus h(k_u \| K_p)$, $n_1 = h(JID_u \| T_1) \oplus Z_1$, $ID_d = Z_2 \oplus h(N_u \| JID_u \| T_1)$, $R_1 = h(JID_u \| ID_d \| n_1 \| T_1)$, and checks $R_1' ? = R_1$. In case it is not true, it aborts. Otherwise, it selects n_2, T_2 and computes $PID_u^{New} = h(n_1 \| JID_u \| N_u \| T_1) \oplus Z_3$ and recovers C_m using ID_j. Then it computes $N_d = h(ID_d \| k_d \| K_p)$, $Z_4 = n_2 \oplus h(ID_d \| N_d)$, $Z_5 = h(N_d \| ID_d) \oplus PID_u^{New}$, $Z_6 = JID_u \oplus h(ID_d \| N_d \| T_2)$, $Z_7 = C_m \oplus h(N_d \| ID_d \| T_2)$, $R_2 = h(ID_d \| C_m \| N_d \| n_2 \| T_2)$ and sends the message $M_2 = \{Z_1, Z_4, Z_5, Z_6, Z_7, R_2, T_1, T_2\}$ to D_j for further verification.In addition it adds the pseudonym PID_u^{New} in its database and deletes the old pseudonym PID_{u-1} if it persists.

iii) Upon the receipt of message, the D_j checks the freshness of timestamp by $T_2 - Tc < \Delta T$. If it holds valid, it computes $JID_u = h(ID_d \| N_d \| T_2) \oplus Z_6$, $n_2 = h(ID_d \| N_d) \oplus Z_4$, $C_m = Z_7 \oplus h(N_j \| ID_j \| T_2)$, $R_2' = h(ID_d \| C_m \| N_d \| n_2 \| T_2)$ and verifies the equality for $R_2' ? = R_2$. If it is not valid, the D_j aborts. On the other hand, it computes $n_1 = h(JID_u \| T_1) \oplus Z_1$ and selects n_3 as well as T_3. Then it further computes $W_m' = PUF(C_m)$, $SK = h(JID_u \| W_m' \| ID_d \| n_1 \| n_2 \| n_3)$, $Z_8 = h(JID_u \| T_3) \oplus n_3$, $Z_9 = h(ID_d \| T_3) \oplus n_2$, $PID_u^{New} = h(N_d \| ID_d) \oplus Z_5$, $Z_{10} = h(JID_u \| ID_d \| T_3) \oplus PID_u^{New}$ and $R_3 = h(SK \| ID_d \| JID_u \| W_m' \| n_1 \| n_3)$. Next, it submits the message $M_3 = \{Z_8, Z_9, Z_{10}, R_3, T_3\}$ towards U_i as shown in Fig. 4.

iv) The U_i checks the freshness by verifying $T_3 - Tc < \Delta T$. If it is valid, it further computes $n_3 = h(JID_u \| T_3) \oplus Z_8$, $n_2 = h(ID_d \| T_3) \oplus Z_9$, $SK = h(JID_u \| W_m \| ID_d \| n_1 \| n_2 \| n_3)$, $R_3' = h(SK \| ID_d \| JID_u \| W_m \| n_1 \| n_3)$ and verifies the equality $R_3' ? = R_3$. If it is true, it computes $PID_u^{New} = h(JID_u \| ID_d \| T_3) \oplus Z_{10}$, adds PID_u^{New} in its database and finally deletes PID_{u-1}.

V. Security Analysis

This section describes informal and formal security analysis in the following sub-sections:

A. Informal Security Analysis

1) Mutual Authentication: The SPAKE-DC supports mutual authentication as both entities U_i and drone authenticate one another with the CS. First the U_i sends the message $M_1 = \{Z_1, Z_2, Z_3, R_1, PID_u, T_1\}$ to CS which authenticates the former on the basis of R_1. After checking the timestamp, the CS searches for $\{ID_d, JID_u*, k_d\}$ using the key PID_u. Then it computes JID_u, n_1, ID_d as well as $R_1 = h(JID_u \| ID_d \| n_1 \| T_1)$ which enables the verification for the authenticity of Ui. The CS knows that JID_u cannot be constructed by the adversary but only legal user U_i may develop this using its legal PW_u and BIO_u. The drone D_j authenticates the CS by verifying the equality $R_2' ? = R_2$. D_j knows the fact that N_d can only be constructed by a legitimate CS using $N_d = h(ID_d \| k_d \| K_p)$. Moreover, the timestamp used in the R_2 is fresh, duly authenticates the CS. Likewise, the Ui authenticates Dj on the basis of verification for $R_3' = h(SK \| ID_d \| JID_u \| W_m \| n_1 \| n_3)$. The U_i knows that the session key $SK = h(JID_u \| ID_d \| n_1 \| n_2 \| n_3)$ cannot be constructed by any other entity than D_j since only D_j bears the corresponding PUF that may only generate the legal W_m parameter that helps in the verification of R_3 parameter. Thus in this protocol, all participants authenticate one another on mutual basis, substantiating the feature of mutual authentication for the proposed scheme.

2) Anonymity and unlinkability: The proposed scheme warrants anonymity as well as unlinkability features. It does not send the user's identity on public channel in plaintext. For

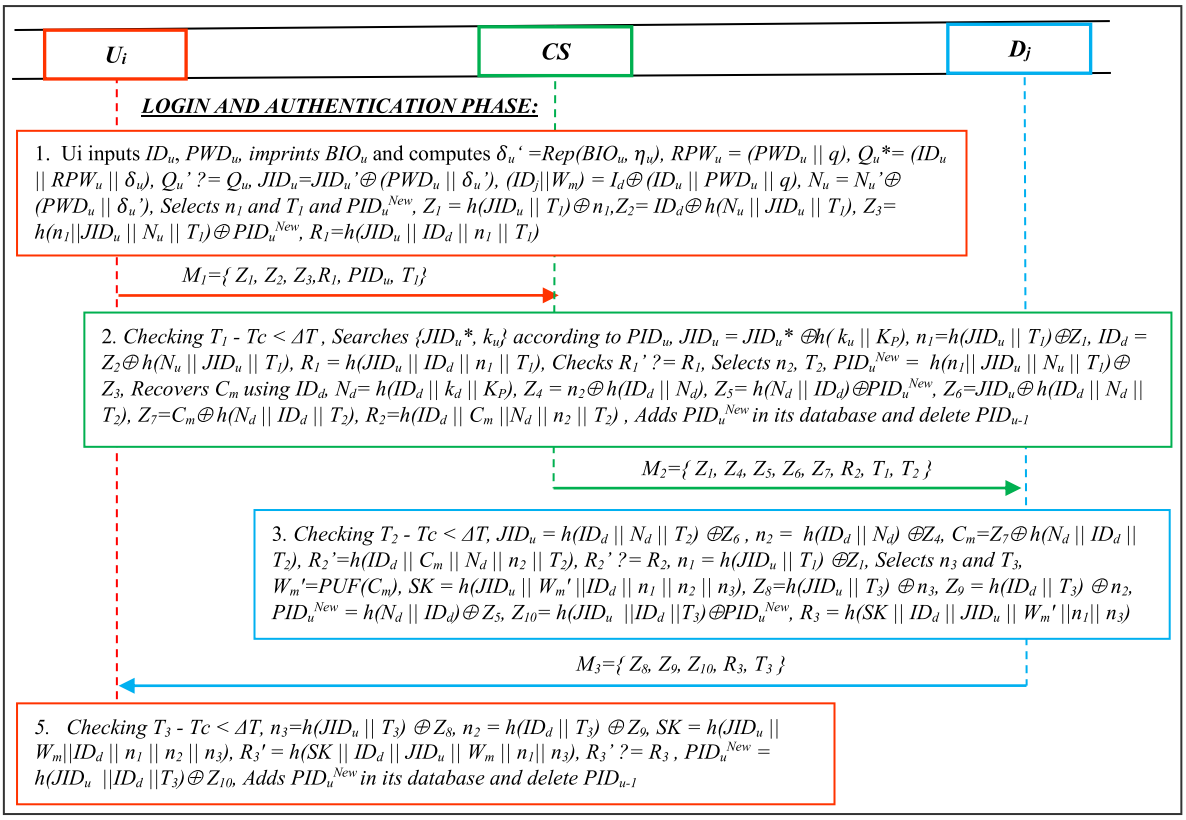


Fig. 4. Proposed scheme (SPAKE-DC).

this purpose, the SPAKE-DC submits its pseudo-identity PID_u for the purpose of synchronization between U_i and server CS. The PID_u is exposed in later session every time it is agreed between the entities. Upon the disclosure of PID_u, the attacker cannot recover the original identity of user ID_u. Moreover, an adversary cannot differentiate any two sessions of the same user on the basis of similarity of factors. No factor is repeatedly used among various sessions, that is, the factors are renewed in every session. Thus, we can safely conclude that the protocol ensures anonymity and unlinkability features for the user.

3) Replay attack: In case of replayed message M_1 by the adversary towards CS, the latter may thwart this attack primarily by checking the freshness of the timestamp T_1. In addition, it verifies the correctness of R_1 parameter. If it is replayed, the message M_1 may not pass either of the checks. This is because the adversary has no access to the legal identity ID_d, and other parameters such as JID_u and n_1. Similarly, if $\mathcal{A}$ attempts to replay the message M_2 towards D_j, the later may foil this attack after checking the freshness of timestamp and the validity of R_2 parameter. An adversary cannot construct a valid R_2 message with an updated timestamp. Similarly, after receiving the replayed M_3 message, the U_i may easily discard it if either the timestamp is not fresh or R_3 is found to be inconsistent. Thus the SPAKE-DC scheme can resist replay attack.

4) Impersonation attack: If $\mathcal{A}$ attempts to impersonate any of the legitimate entities such as U_i, CS or D_j, it will not be successful in launching this attack. This is because, if attacker tries to construct the message M_1, it will not be able to do so due to lack of legal JID_u and N_u parameters. Similarly, the attacker may not construct a valid M_2 message due to lack of K_p, k_d and ID_d parameters which are required to further generate N_d, Z_4, Z_5, Z_6 and Z_7 factors and constitute the M_2 message. Likewise, the valid construction of M_3 message requires N_d, ID_d and a particular PUF. If these parameters are not held by the participant, it cannot construct a legal message other than a fabricated message. Hence the SPAKE-DC is protected from impersonation attack.

5) Drone Physical capture attack: The proposed SPAKE-DC protocol is protected from physical drone capture attack. Since, even if an attacker is able to intercept the drone physically and access all of its contents and secrets in its memory, our scheme is immune to such type of attack. This is because; we employ a specific PUF chip during the registration of drone and user [35]. This chip bears a unique biometric signature and no other chip can serve the same purpose. The outcome of that chip is used in the construction of messages for submission to U_i. An adversary having all private and public secrets available on public channels would need this PUF chip to produce that particular factor to convince the user [36]. Hence the proposed SPAKE-DC protocol is immune to drone physical capture attack.

6) Session specific ephemeral secrets leakage attack: In our scheme, even if the attacker recovers the session specific temporary information such n_1, n_2 or n_3 from any of compromised participating entities such as U_i, CS or D_j, respectively, the attacker will not be able to compute the session key $SK = h(JID_u$

$||W_m||ID_d \ ||n_1 \ ||n_2 \ ||n_3)$ for lacking JID_u and ID_d. Thus the proposed scheme can withstand this attack.

7) Perfect forward secrecy: In case, the adversary is able to recover the private key secrets of either user or CS or drone, then the former cannot recover the current or previous session keys. In case of user, it must recover short term secrets along with the long term private secrets like password. However, it is a hard assumption for the adversary to compromise both kinds of secrets simultaneously. Similarly, if the long term secret of CS is compromised, the engagement of PUF chip for producing the integral factor used in the construction of session key makes it a hard for the adversary to guess the current or previous session keys. Likewise, if a drone is intercepted with compromised keys, yet the current or previous session keys are protected due to the PUF-based factor included in the session key. Therefore, our scheme abides by the perfect forward secrecy.

8) Denial-of-Service attack: An adversary may render the server unresponsive by depleting its resources through generating thousands of requests at a time. Alternatively, it could attempt to saturate the bandwidth of the channel by initiating Denial of Service (DoS) attack towards CS entity in SPAKE-DC. A misconfigured server may have to maintain the session variables of partially completed fake request-based sessions causing significant delays and poor quality of service (QoS). An adversary may attempt to exploit this limitation and affect the overall bandwidth of the system. However, in SPAKE-DC, the CS may thwart such attempts by authenticating the user requests using the equality verification of R_1' against R_1. The CS knows the fact that only a legal user can generate R_1 for having access to valid JID_u. If it holds, the CS warrants the genuineness of the user and dispels any chances of replay, DoS or man-in-the-middle threats. Thus, the SPAKE-DC is resistant of any kind of DoS or similar threat intended to encroach on the network bandwidth and useful resources of the controlling system.

B. Formal Security Analysis

In this section we employed RoR model to examine the security features of contributed scheme. This model was put forward by Canetti et al. [31], and Wu et al. [32] which suggested the mathematical formulations to study the security properties of protocols by gauging the probability measures for breaking SK using several rounds of game. The proof for SK-security for SPAKE-DC is provided in Theorem 1.

Theorem 1: It is assumed that the adversary $\mathcal{A}$ may apply the above mentioned queries in Real-or-Random (RoR) model. The probability for breaking the contributed protocol SPAKE-DC in polynomial amount of time is given as

$$Adv_{\mathcal{A}}^{SAKED}(t) \leq \frac{q_{s_n}}{2^{l-2}} + \frac{3q_{\mathrm{h_f}}^2}{2^{l-1}} + 2\max\left\{C'_n.q_{\mathrm{s_n}}^{s'}, \ \frac{q_{s_n}}{2^l}\right\} \quad (1)$$

where q_{sn} denotes the total number of queries that are executed; q_{hf} denotes the number of times the hash queries are executed; l characterize the length of the biological string while $\mathrm{C_n}'$ and s $'$ are the constants.

Proof: This proof comprises seven rounds of games, i.e., from $\mathrm{G_{R0}}$ to $\mathrm{G_{R6}}$. The $Sucs_{\mathcal{A}}^{G_{R0}}(\mathrm{t})$ depicts the probability that the adversary could win the game in $\mathrm{G_{R0}}$ to $\mathrm{G_{R6}}$ rounds.

$\boldsymbol{G_{R0}}$: This is the first game round, termed as $\mathrm{G_{R0}}$ which is deemed to be factual attack that does not initiate with query. It will be initiated with the flipping of coin C. Thus, the probability of successfully breaking the *SPAKE-DC* protocol can be calculated as:

$$Adv_{\mathcal{A}}^{SAKED}(t) = \left|2\Pr\left[Sucs_{\mathcal{A}}^{G_{R0}}\right] - 1\right| \quad (2)$$

$\boldsymbol{G_{R1}}$: This game is transformation of game G_{R0} with an added query of *Execute* ($\mathrm{Q_R}$) while the adversary eavesdrops the communication messages $\{\mathrm{M_1}$–$\mathrm{M_3}\}$ exchanged on public channel in G_{R1}. The adversary may not calculate the session key using test ($\mathrm{Q_R}$) query as it is ignorant of the values ID_d, n_1, n_2, n_3 and JID_u. Hence, the probability for $G_{R1}$is equal to G_{R0} for equal amount of advantage.

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R0}}\right] = \Pr\left[Sucs_{\mathcal{A}}^{G_{R1}}\right] \quad (3)$$

$\boldsymbol{G_{R2}}$: This game is further transformation of G_{R1} with an added Send (QR) query. Using Zipf's law [34], we get the following probability for G_{R2}, i.e.,

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R2}}(\mathrm{t})\right] - \Pr\left[Sucs_{\mathcal{A}}^{G_{R1}}(\mathrm{t})\right] | \leq \frac{q_{s_n}}{2^l} \quad (4)$$

$\boldsymbol{G_{R3}}$: This game is further transformation of $\boldsymbol{G_{R2}}$with an added Hash (Q_R) query. Referring to birthday paradox, we get the probability for $\boldsymbol{G_{R3}}$ as:

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R3}}(\mathrm{t})\right] - \Pr\left[Sucs_{\mathcal{A}}^{G_{R2}}(\mathrm{t})\right] | \leq \frac{q^2 h_f}{2^{l+1}} \quad (5)$$

$\boldsymbol{G_{R4}}$**:** This game uses the Real-or-Random (RoR) model for analyzing the two events to prove the protocol's security. First, it needs to recover the high entropy long term secret K_P for proving the feature of perfect forward secrecy, while the other one is to recover ephemeral random information regarding any participating entity for proving the fact that the scheme is immune to session specific ephemeral secrets disclosure threat.

1) *Perfect forward secrecy:* The adversary utilizes $\prod_{CS}^{w}$ for recovering the high entropy long term secret of CS as K_P, or using $\prod_{U_i}^{u}$ and $\prod_{D_j}^{v}$ for extracting the private secrets established in the registration procedure.
2) *Known session specific ephemeral secrets disclosure attack:* The adversary utilizes $\prod_{U_i}^{u}$, $\prod_{D_j}^{v}$ and $\prod_{CS}^{w}$ for getting the randomly defined numbers for three participating entities.

For the first event, even if the adversary recovers the long term secret K_P of CS, or other private secrets being shared among the participants, the parameters $\{n_1, n_2, n_3, JID_u, ID_d\}$ may not be recovered or calculated in polynomial time. Thus the adversary might not calculate the session key $SK = h(JID_u \ || \ ID_d \ || \ n_1 \ \| \ n_2 \ \| \ n_3)$. As far second event, if the attacker gets the random numbern_1, the other parameters $\{n_2, n_3, JID_u, ID_d\}$ remain confidential, hence the session key remains protected. Even if we assume that the attacker gets the parameters n_2 and

n_3, the session can neither be recovered. This is because,

$$\Pr\left|\left[Sucs_{\mathcal{A}}^{G_{R4}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R3}}(\mathrm{t})\right]\right|\leq\frac{q_{s_n}}{2^l}+\frac{q_{\mathrm{h_f}}^2}{2^{l+1}} \quad (6)$$

***G_{R5}*:** This game uses*Reveal* (Q_R) for querying the factors {*JID_u', ID_d', N_u', q, Q_u, PID_u, η_u*}, however despite this the SPAKE-DC protocol may defy the offline password guessing threat. The user is registered with CS with the help of password PWD_u and biometric identity BIO_u. If the adversary attempts to guess the $Q_u = (ID_u \,||\, RPW_u \,||\, \delta_u)$ it might not succeed since the identity ID_u and RPW_u are confidential parameters with adequate protection. The adversary chances to guess the l-bits for biological identity is given as $1/2^l$. On the other hand, in accordance with the Zipf's law [34], in case the equation $q_{sn} \leq 10^6$ holds, the chances of the adversary guessing the PWD_u remain higher than 0.5. Thus, we can show the probability for G_{R5} as:

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R5}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R4}}(\mathrm{t})\right]|\leq\max\left\{C_n'.\,q_{\mathrm{s_n}}^{s'},\frac{q_{s_n}}{2^l}\right\} \quad (7)$$

***G_{R6}*:** This game verifies the capability of the protocol to encounter forgery threats including impersonation attack. The adversary employs this query for guessing the parameters $h(JID_u \,||\, ID_d \,||\, n_1 || \, n_2 \,||\, n_3)$ to terminate the game, however its probability is:

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R6}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R5}}(\mathrm{t})\right]|\leq\frac{q_{\mathrm{h_f}}^2}{2^{l+1}} \quad (8)$$

For the above query, the winning probability of the adversary $\mathcal{A}$ is 0.5, i.e.,

$$\Pr\left[Sucs_{\mathcal{A}}^{G_{R6}}(\mathrm{t})\right]=1/2 \quad (9)$$

Thus using the above equations, we infer

$$\begin{aligned}
&1/2Adv_{\mathcal{A}}^{SAKED}(t)=|2Pr\left[Sucs_{\mathcal{A}}^{(G_R0)}\right]-1/2|\\
&\Pr\left[Sucs_{\mathcal{A}}^{G_{R0}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R6}}(\mathrm{t})\right]\\
&\Pr\left[Sucs_{\mathcal{A}}^{G_{R1}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R6}}(\mathrm{t})\right]\\
&\leq\sum_{k=0}^{5}\left|\Pr\left[Sucs_{\mathcal{A}}^{G_{R_{k+1}}}(\mathrm{t})\right]-\Pr\left[Sucs_{\mathcal{A}}^{G_{R_k}}(\mathrm{t})\right]\right|\\
&=\frac{q_{s_n}}{2^{l-1}}+3\frac{q_{\mathrm{h_f}}^2}{2^l}\max\left\{C_n'.q_{\mathrm{s_n}}^{s'},\frac{q_{s_n}}{2^l}\right\} \quad (10)
\end{aligned}$$

Hence, we get

$$Adv_{\mathcal{A}}^{SAKED}(t)\leq\frac{q_{s_n}}{2^{l-2}}+3\frac{q_{\mathrm{h_f}}^2}{2^{l-1}}+2\max\left\{C_n'.\,q_{\mathrm{s_n}}^{s'},\frac{q_{s_n}}{2^l}\right\} \quad (11)$$

VI. Performance Evaluation

The performance of several related studies in terms of computational and communicational cost is evaluated in this section against the proposed scheme. The computational cost comprises the cost of symmetric and asymmetric crypto-primitives or operations, while communication cost represent the bits needed by the parameters to traverse and reach the destination. We performed an experiment-based simulation to evaluate the execution timings of operations used in the protocol. We employed mobile phone (Lenovo Zuk Z1) for user comprising Quad-core 2.6 Ghz-Processor, 4 GB RAM with Android OS V5.1.3, and for server Ubuntu 18.4 LTS with CPU Intel core i5-10400 2.9 GHz and RAM 4 GB. Then we utilized PBC-0.5.14 cryptographic library to implement the protocol. For drone, we employed Raspberry PI setting as "Raspberry PI 4B (2019) model, 64b CPU architecture, 1.5 Ghz Quadcore processor, Ubuntu 20.4.2 LTS and 8G RAM". For each crypto-primitive we run the experiment 100 times, and take the measurements for maximum, minimum and average milliseconds. However, we computed the computational costs by using average case timing (*ms*) for user (mobile phone), server (desktop) and drone (Raspberry PI) as shown in Table III.

TABLE III
Experimental Cost of Crypto-Primitives (millisecs.)

Operations	U_i	*Server*	D_j
T_h	0.031	0.011	0.019
T_{SYM}	0.065	0.021	0.049
T_{PUF}	0.144	0.67	0.81
T_{EPM}	10.81	5.09	7.107
T_f	0.065	-	-
T_{BP}	26.52	13.73	20.63

TABLE IV
Computational Costs

	U_i	CS	D_j	Total cost (millisecs.)
[19]	T_f+ $15T_h$	$2T_{sym}$+ $9T_h$	$7T_h$	T_f+ $31T_h$+$2T_{sym}$≈$_{0.807}$
[18]	$2T_{bp}$+ $5T_h$	$2T_{bp}$+ $3T_h$	$4T_{sym}$+ $2T_{bp}$+ $9T_h$	$6T_{bp}$+ $8T_h$+$4T_{sym}$≈$_{122.31}$
[22]	T_f+ $16T_h$	$8T_h$	$7T_h$	T_f+ $31T_h$≈$_{0.785}$
[20]	T_f+ $14T_h$	$9T_h$	$9T_h$	T_f+ $32T_h$≈$_{0.772}$
[21]	$10T_h$ +$1T_f$	$7T_H$+$3T_{sym}$	$7T_h$	$1T_{fe}$ +$24T_h$ +$3T_{sym}$≈$_{0.619}$
[33]	T_f+ $12T_h$	$9T_h$	$8T_h$	T_f+ $29T_h$≈$_{0.691}$
[24]	-	$12T_H$+$3T_{sym}$	$6T_H$+$1T_{sym}$	$18T_h$+ $4T_{sym}$≈$_{0.358}$
[9]	$7T_h$	$5T_h$	$7T_H$	$19T_h$≈$_{0.427}$
[38]	$9T_h$	$7T_h$+$2T_{sym}$	$7T_H$	$23T_h$+$2T_{sym}$≈$_{0.531}$
Ours	T_f+ $15T_h$	$12T_h$	$4T_h$+$1T_{PUF}$	T_f+$31T_h$+$1T_{PUF}$≈$_{1.541}$

According to the above experiment, the observed timing of T_h, T_{sym}, T_f, T_{bp} and T_{PUF} crypto-primitives is given in Table III. The Table IV depicts the total cost of computations for [9], [18], [19], [20], [21], [22], [24], [33], [38] and the proposed scheme. Our scheme bears the total computational latency as 1.541ms, while other schemes [9], [18], [19], [20], [21], [22], [24], [33], [38] take 0.691 ms, 0.358 ms, 0.785 ms, 0.807 ms, 0.427 ms, 0.772 ms, 122.31 ms, 0.619 ms, 0.531 ms respectively. It is obvious that the schemes [9], [19], [20], [21], [22], [24], [33], [38] bear less computational cost as compared to proposed scheme.

It is evident that the proposed scheme addresses to all security issues exhibited in Table V. In Hussain et al. [19], the authors could not address the vulnerabilities related to impersonation attack, drone capture attack and privileged insider attack. In Ever [18], the scheme was prone to anonymity, capture and temporary information leakage attacks. The Wazid et al. [22] is susceptible to impersonation attack, temporary information attack, privileged insider attack, and also lacks anonymity and mutual authentication. The Srinivas et al. [20] is vulnerable to

TABLE V
SECURITY ATTRIBUTES AND COMPARISON

	[19]	[18]	[22]	[20]	[21]	[33]	[24]	[9]	[38]	Ours
SA1	✓	×	×	×	✓	×	✓	×	✓	✓
SA2	✓	✓	×	✓	✓	✓	✓	×	✓	✓
SA3	×	✓	×	×	✓	✓	✓	×	✓	✓
SA4	×	×	✓	×	×	×	✓	×	×	✓
SA5	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SA6	×	✓	×	✓	✓	✓	✓	✓	✓	✓
SA7	✓	×	×	×	✓	✓	✓	×	✓	✓
SA8	✓	-	-	-	×	✓	✓	×	✓	✓
SA9	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
SA10	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
SA11	✓	✓	✓	✓	✓	✓	✓	✓	×	✓

SA1: Anonymity and unlinkability, SA2: Mutual authentication, SA3: Defend forgery/impersonation threats, SA4: Defend drone capture threats, SA5: Defend Man-In-The-Middle threats, SA6: Defend privileged insider threats, SA7: Defend temporary information leakage threats, SA8: Sustains perfect forward & backward secrecy, SA9: Session key conformity, SA10: Defend replay attack, SA11: Resist dos attack, ✓: Security attribute supported, ×: Security attribute not supported.

TABLE VI
COMMUNICATIONAL OVERHEAD (BITS)

Schemes	[19]	[18]	[22]	[20]	[21]	[33]	[24]	[9]	[38]	Ours
Comm. cost	2061	5344	1696	1536	1696	2176	2688	2720	2304	2528

drone capture attack, temporary session key information attack, and impersonation attack. Moreover, it lacks anonymity. Ali et al. [21], Wu et al. [33] and Turkanovic et al. [9] suffer from drone capture threats. In addition, Wu et al. [33] does not support anonymity, and Turkanovic et al. [9] was vulnerable to impersonation attack.

To compute the communication cost, we assume that the communication cost of transmitting hash-based message is 160-bits, the cost of transmitting identity or pseudo-identity also takes 160-bits, the cost of submitting timestamp is 32-bits, and the cost of sending elliptic curve cryptographic operation takes 320 bits. The three messages such as $M_1 = \{Z_1, Z_2, Z_3, R_1, PID_u, T_1\}$, $M_2 = \{Z_1, Z_4, Z_5, Z_6, Z_7, R_2, T_1, T_2\}$ and $M_3 = \{Z_8, Z_9, Z_{10}, Z_{11}, R_3, T_3\}$ have been submitted by the Ui, CS and Dj entities, respectively. The communication cost of proposed scheme is calculated as 2688 bits. Likewise, the communication costs of Hussain et al. [19], Ever [18], Wazid et al. [22], Srinivas et al. [20], Ali et al. [21], Wu et al. [33], Zhang et al. [24], Turkanovic et al. [9], Akram et al. [38] and our scheme is computed as 2061 bits, 5344 bits, 1696 bits, 2176 bits, 2688 bits, 2720 bits, 2304 bits and 2528 bits, respectively as depicted in Table VI. It can be seen that the communication costs of [19], [22], [20], [21], [33] is less than the communication cost of proposed scheme. Although these costs are less than proposed scheme yet these are vulnerable to many threats. The communication cost for [18] and [24] is higher than our scheme. Fig. 5 represents the computational costs and the Supported Security Features (SSF) in pictorial form which exhibits that SPAKE-DC supports 42% more number of security features as compared to previous techniques. This percentage is computed by taking an average of supported security features as compared to proposed scheme, for all schemes individually. It can be witnessed in Fig. 6 part (a) and (b), that the curve for SPAKE-DC is lower than [18] which is bilinear pairing based scheme, however it is above than most

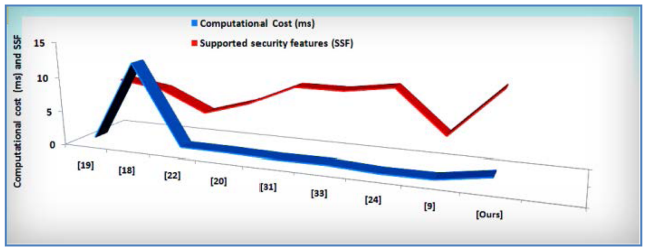
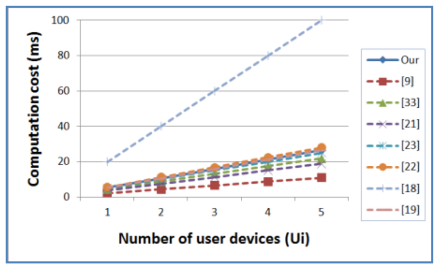
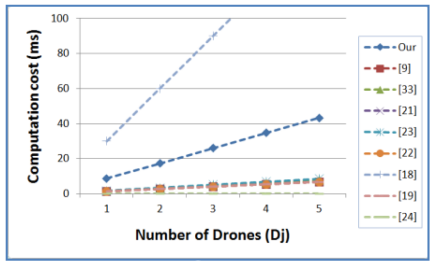


Fig. 5. Computational cost and Supported features.



(a)



(b)

Fig. 6. Computational cost comparison (a) mobile user (b) drones.

TABLE VII
SIMULATION CONTEXTUAL PARAMETERS

Parameters	*Description*
Platform	Ubuntu 18.4 LTS
Tool	NS-3
Area of Simulated Experiment	2600 × 2600 m^2
Number of D_j units	100
Number of CS units	1
Number of users	5
Mobility of U_i	5-10 meter per sec.
Mobility of D_j	20-30 meter per sec.
Routing protocol	AoDV
Packet size	512 byte
Simulation time	30 min
Traffic class	UDP
Wireless standard	IEEE 802.11

of symmetric-key based schemes [9], [19], [20], [21], [22], [23], [24], [33], and [38]. This is because that our scheme employs additional PUF that adds a little bit into the computational cost of SPAKE-DC though, it increases the security of drone from physical capture attacks as compared to other symmetric key-based schemes [38].

In addition, we performed a discrete-event based simulation for SPAKE-DC protocol in NS-3 tool [39]. The Table VII exhibits the parameters utilized in NS-3 based simulator. The simulation time is selected as 30 min. The D_j, CS and U_i represent *j*th drone, controlling server and *i*th user, respectively. We have taken a single CS unit for the simulation, while multiple

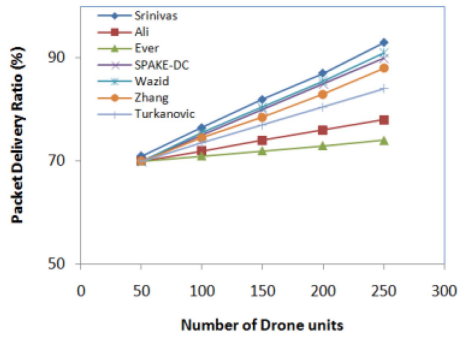


Fig. 7. Packet delivery ratio.

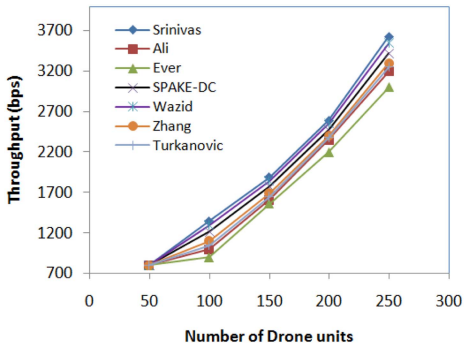


Fig. 8. Throughput.

instances of other units. The users Ui traverse with varying mobility, i.e., 5–10 mps. In this simulation, we considered Guass-Markov as the mobility model for the drones.

1) *Packet delivery ratio:* Packet delivery ratio (PDR) refers to the total number of delivered packets out of the broadcasted messages over the network. The Fig. 7 depicts the packet delivery ratio as per the simulation setting shown in Table VII. According to this, the SPAKE-DC bears more packet delivery rate, i.e., 75.2% with the increasing number of drone units in the system as compared to other UAV-based authentication schemes [9], [18], [21] and [24]. Although, the schemes [20] and [22] have a little bit higher PDR than SPAKE-DC, yet these schemes are prone to security threats as shown in Table V, which restrain their applicability. The basic metric for high performance of PDR is the least packet loss rate that enhances the PDR for the schemes including the proposed scheme.
2) *Throughput:* The throughput metric is referred to the total number of bits transmitted per unit time which can be computed as $(n_{pr} \times |Pkt_z|)/t_s$ wherein t_s depicts the aggregate time in seconds, Pkt_z the size of packet, and n_{pr} shows the aggregate number of received packets. It can be witnessed from Fig. 8 that SPAKE-DC bears more throughput in comparison with [9], [18], [21] and [24]. However, the schemes [20] and [22] carry a little bit more throughput than SPAKE-DC as per the simulation setting, however in security terms those schemes are susceptible to few security threats as shown in TABLE V, restraining the applicability of those schemes.

VII. Conclusion and Future Scope

This paper proposed a novel PUF-based lightweight authentication protocol SPAKE-DC for protecting the drone communication from physical capture attack in particular. For power-deficient IoT-enabled drones, the AKA technique supported by SPAKE-DC is not only efficient, but also secure. The proposed scheme sustains crucial security features such as anonymity, mutual authentication, and perfect forward secrecy in the face of encounter with malicious adversaries. The proposed scheme is formally analyzed using a rigorous Real-or-Random Oracle model. The performance findings and security comparison of functionalities exhibit compelling results in terms of computation, communication and security objectives making it well-suited for practical implications. In future we intend to explore and resolve the security issues for introducing 6G in IoD environment.

References

[1] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.
[2] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw*, vol. 32, pp. 17–31, 2015.
[3] T. Hewa, A. Braeken, M. Liyanage, and M. Ylianttila, "Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7174–7185, Oct. 2022, doi: 10.1109/TII.2022.3140792.
[4] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of Internet of Drones (IoD): A review," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25532–25546, Nov. 2021, doi: 10.1109/JSEN.2021.3114266.
[5] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A survey on IOT and 5G network," in *Proc. Int. Conf. Smart City Emerg. Technol.*, Mumbai, India, 2018, pp. 1–3.
[6] T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A novel authentication scheme for Drone-assisted 5G networks," in *Proc. IEEE INFOCOM-IEEE Conf. Comput. Commun. Workshops*, Vancouver, BC, Canada, 2021, pp. 1–6.
[7] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *J. Netw. Comput. Appl.*, vol. 131, pp. 66–74, 2019.
[8] C. Lin, D. He, N. Kumar, K. K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of Drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018, doi: 10.1109/MCOM.2017.1700390.
[9] M. Turkanovi´c, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, 2014.
[10] M. S. Farash, M. Turkanovi´c, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, 2016.
[11] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, 2016.
[12] Y. Lee, J. Yoon, J. Choi, and E. Hwang, "A novel cross-layer authentication protocol for the Internet of Things," *IEEE Access*, vol. 8, pp. 196135–196150, 2020, doi: 10.1109/ACCESS.2020.3033562.
[13] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 16, no. 11, pp. 7081–7093, Nov. 2020, doi: 10.1109/TII.2019.2942389.

[14] M. F. Ayub, K. Mahmood, S. Kumari, and A. K. Sangaiah, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," *Digit. Commun. Netw.*, vol. 7, pp. 235–244, 2021.
[15] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, 2020.
[16] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102354.
[17] L. Teng et al., "Lightweight security authentication mechanism towards UAV networks," in *Proc. Int. Conf. Netw. Netw. Appl.*, Daegu, Korea, 2019, pp. 379–384.
[18] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, 2020.
[19] S. Hussain, K. Mahmood, M. K. Khan, C. M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Comput. Standards Interfaces*, vol. 80, 2022, Art. no. 103566.
[20] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019, doi: 10.1109/TVT.2019.2911672.
[21] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020, doi: 10.1109/ACCESS.2020.2977817.
[22] 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, Apr. 2019, doi: 10.1109/JIOT.2018.2888821.
[23] C. L. Chen, Y. Y. Deng, W. Weng, C. H. Chen, Y. J. Chiu, and C. M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, 2020, Art. no. 62.
[24] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, 2020.
[25] M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, M. Cebe, and A. S. Ibrahim, "Enabling second factor authentication for drones in 5G using network slicing," in *Proc. IEEE Globecom Workshops*, Taipei, Taiwan, 2020, pp. 1–6.
[26] M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, and A. S. Ibrahim, "A proxy signature-based drone authentication in 5G D2D networks," in *Proc. IEEE 93rd Veh. Technol. Conf.*, Helsinki, Finland, 2021, pp. 1–7.
[27] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[28] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Comput. Secur.*, vol. 18, no. 8, pp. 727–733, Jan. 1999.
[29] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.*, Berlin, Germany, 1999, pp. 388–397.
[30] A. Mostafa, S. J. Lee, and Y. K. Peker, "Physical unclonable function and hashing are all you need to mutually authenticate IoT devices," *Sensors*, vol. 20, no. 16, 2020, Art. no. 4361.
[31] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *J. ACM*, vol. 51, pp. 557–594, 2004.
[32] T. Y. Wu, Y. Q. Lee, C. M. Chen, Y. Tian, and N. A. Al-Nabhan, "An enhanced pairing-based authentication scheme for smart grid communications," *J. Ambient Intell. Hum. Comput.*, to be published, doi: 10.1007/s12652-020-02740-2.
[33] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the security: An enhanced authentication protocol for drone communications over 5G networks," *Drones*, vol. 6, no. 1, 2021, Art. no. 10.
[34] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017, doi: 10.1109/TIFS.2017.2721359.
[35] B. Alzahrani, A. Barnawi, A. Irshad, A. Alhothali, R. Alotaibi, and M. Shafiq, "A secure key agreement scheme for unmanned aerial vehicles-based crowd monitoring system," *Comput., Mater. Continua*, vol. 70, no. 3, pp. 6141–6158, 2022.
[36] S. A. Chaudhry et al., "A physical capture resistant authentication scheme for the Internet of Drones," *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 62–67, Dec. 2021, doi: 10.1109/MCOMSTD.0001.2100006.
[37] C. Pu, A. Wall, and K. K. R. Choo, "Bilinear pairing and PUF based lightweight authentication protocol for IoD environment," in *Proc. IEEE 19th Int. Conf. Mobile Ad Hoc Smart Syst.*, 2022, pp. 115–121.
[38] M. W. Akram et al., "A secure and lightweight drones-access protocol for smart city surveillance," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 19634–19643, 2021.
[39] L. Tian, S. Deronne, S. Latré, and J. Famaey, "Implementation and validation of an IEEE 802.11ah module for NS-3," in *Proc. Workshop NS-3*, 2016, pp. 49–56.
[40] T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A novel authentication scheme for drone-assisted 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.