A Security Enhanced Chaotic-Map-Based Authentication Protocol for Internet of Drones

Khalid Mahmood, *Senior Member, IEEE*, Zahid Ghaffar, Muhammad Farooq, Khalid Yahya, Ashok Kumar Das, *Senior Member, IEEE*, and Shehzad Ashraf Chaudhry, *Member, IEEE*

***Abstract*—The Internet of Drones (IoD) extends the capabilities of unmanned aerial vehicles, enabling them to participate in a connected network. In IoD infrastructure, drones communicate not only among themselves but also with users and a control center. This interconnected communication framework holds promise for various applications, from collaborative decision-making to real-time data exchange. However, the expansion of communication in IoD also introduces new challenges, particularly in terms of security, privacy and authentication. Unfortunately, the current authentication protocols are inadequate in offering robust security features against various attacks in the IoD environment. To address these security issues and limitations, we proposed a secure protocol for the IoD environment using chaotic maps and hash functions. In addition, we also employed a physically unclonable function in the development of the proposed protocol. We assess the security of the protocol through both informal and formal security analysis. The formal security analysis is conducted through a widely used random or real (RoR) model. The informal analysis shows the rigorous security features against various attacks, such as masquerading, anonymity violation, and physical cloning attacks. Moreover, we compare the performance of the devised protocol with similar existing protocols across important performance parameters, such as communication overhead, computation overhead, and security features. The devised protocol provides a 67.86% and 17.80% reduction in computation and communication overheads, respectively, as compared to related protocols. The analysis demonstrates the proposed protocol's capacity to support secure communication in the IoD environment and satisfy desirable security attributes.**

Manuscript received 24 December 2023; revised 13 February 2024 and 10 March 2024; accepted 18 March 2024. Date of publication 20 March 2024; date of current version 7 June 2024. Shehzad Ashraf Chaudhry acknowledges financial support from Abu Dhabi University's Office of Research and Sponsored Programs Grant number: 19300810. *(Corresponding author: Shehzad Ashraf Chaudhry.)*

Khalid Mahmood is with the Graduate School of Intelligent Data Science, National Yunlin University of Science and Technology, Douliu 64002, Taiwan (e-mail: khalidm.research@gmail.com).

Zahid Ghaffar is with the Graduate School of Engineering Science and Technology, National Yunlin University of Science and Technology, Douliu 64002, Taiwan (e-mail: chzahid337@gmail.com).

Muhammad Farooq is with the Department of Mathematics and Statistics, College of Arts and Sciences, Abu Dhabi University, Abu Dhabi, UAE (e-mail: farooq-muhammad@hotmail.com).

Khalid Yahya is with the Department of Electrical and Electronics Engineering, Istanbul Gelisim University, 34310 Istanbul, Turkey, and also with the Department of Electrical Engineering, Faculty of Engineering, Sabratah University, Regdalen, Libya (e-mail: Khalid.omy@gmail.com).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology (Hyderabad), Hyderabad 500 032, India (e-mail: iitkgp.akdas@gmail.com).

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, UAE, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Digital Object Identifier 10.1109/JIOT.2024.3379930

***Index Terms*—Anonymity, authentication, impersonation attack, mutual authentication, security.**

I. Introduction

THE Internet of Drones (IoD) plays a pivotal role across diverse sectors, with applications ranging from military surveillance and logistical operations to agricultural monitoring. These drones, often equipped with advanced sensors, facilitate real-time data collection and remote operation, primarily through wireless technologies like Bluetooth and WiFi. While IoD offers substantial benefits, such as enhanced efficiency and data accuracy, challenges include security risks and potential privacy violations [1], [2], [3].

One of the main reasons IoD became popular is due to their portability [4], [5], [6]. Each drone's unique build is carefully tailored to perform a certain task. Drones used for aerial photography often feature high-resolution cameras and sensitive microphones, while those used for disaster assistance typically feature infrared detectors and cameras to navigate and analyze tough areas. Drones used for logistics and transportation must also have precise positioning systems to ensure timely deliveries. These specialized layouts highlight the adaptability and goal-oriented strategy that characterize IoD technology [7], [8], [9].

In today's quickly expanding technological era, the data generated by IoD systems is invaluable, especially in the domain of big data analytics. Individual behavior and social patterns can both be better understood and predicted with the use of this information [7], [10]. However, the IoD system has significant issues in the areas of access control, data delivery, and maintaining data confidentiality. The network is susceptible to a range of security threats, including impersonation, replay, hijacking, MITM attacks, and unauthorized access, to the control center (CC_s), and vulnerabilities arising from privileged insiders. The presence of these vulnerabilities presents significant threats to the integrity, confidentiality, authenticity, and overall data transmission in the IoD network [11], [12], [13]. Therefore, it is of utmost importance to acknowledge and tackle these challenges.

The implementation of user authentication and access control mechanisms is of utmost importance in order to ensure the protection of drone resources within the context of the IoD. Several authentication protocols have been designed in the literature. Tanveer et al. [14] presented an authentication protocol that is both secure and dependable. In previous

studies, researchers have introduced AES and hash-based authentication protocols as potential solutions for securing the IoT. These proposed protocols have been designed to mitigate various vulnerabilities effectively and have been evaluated using Scyther and random oracle model (ROM) as validation tools [15]. Guo et al. [16] presented the intelligent clustering routing algorithm (ICRA), which aims to improve the performance of underwater sensor networks. ICRA consists of three main modules that utilize reinforcement learning techniques to achieve adaptive performance enhancement. The IoD environment is secured via an authentication protocol based on signcryption, as described in [17]. The safety of the session key is checked using the ROM. Nevertheless, the hash function-based authentication protocol proposed in [18] is susceptible to attacks such as impersonation.

Hsu and Lin [19] suggested a password-based authentication protocol utilizing chaotic maps for secure communication and establishing shared secret session keys. He and Wang [20] developed an efficient three-factor authentication protocol in multiserver environments, integrating biometrics, passwords, and smart cards. Jiang et al. [21] proposed an authentication protocol using a chaotic map, noted for its proven security and enhanced performance. Roy et al. [22] presented a robust authentication protocol using three-factor with extended chaotic maps, incorporating user biometrics and ensuring anonymity in IoT settings. Additionally, Jie et al. [23] introduced a new authentication protocol employing the Cuckoo filter. A conditional privacy-preserving authentication protocol was designed by Jing et al. [24], based on the Chinese Remainder Theorem. It operates without the need for ideal hardware [25].

The bi-linear pairing-based protocol discussed in [26] is not capable of mitigating insider threats or preventing session key leaks, and it also requires significant computational resources. Furthermore, the study conducted by [27] demonstrates a deficiency in effectively addressing the issue of impersonation and fails to provide a mechanism for mutual authentication. In contrast, Pu et al. [28] devised a resource-efficient architecture for securing the IoD. For vehicle networks, Liu et al. [29] offered a privacy-protecting trust management protocol that balances trust and privacy with low-communication costs. Finally, Qiu and Ma [30] presented an authentication protocol that utilizes symmetric encryption and hash functions, highlighting the ongoing advancements in IoD security. Therefore, we proposed a secure and efficient authentication protocol for the IoD infrastructure to address all of these security issues and limitations. The proposed protocol works efficiently against security attacks so that drones can work effectively in surveillance.

A. Motivation and Contributions

Recent advancements in IoD applications have significantly enriched smart cities, providing an array of benefits and essential services. Despite these advantages, existing authentication protocols in this domain often encounter challenges related to information security. Vulnerabilities to various online threats, including insider, MITM, and impersonation attacks, are prominent issues. In response to these security concerns, this study introduces an innovative authentication method employing chaotic maps. This method is both efficient and secure in terms of resource utilization. The proposed protocol effectively mitigates cybersecurity risks and ensures critical security aspects, facilitating the seamless operation of environments that rely on the IoD. This article delineates the following primary contributions.

1) We introduce a chaotic-map-based lightweight authentication protocol to facilitate secure and authenticated communication among users, control center, and drones situated in geographical areas in the IoD framework.
2) In the devised protocol, we incorporate the physically unclonable function (PUF). This protocol enhances resistance to physical cloning attacks on drones, thereby ensuring that our protocol demonstrates robust and efficient performance against such threats.
3) The informal analysis confirms that the designed protocol upholds strong security features, effectively countering various security attacks. Furthermore, to substantiate the protocol's security, formal security validation and analysis are carried out utilizing the widely recognized ROM.
4) The outcomes of the evaluation and performance analysis reveal that the proposed protocol surpasses several competing protocols, achieving notable resource efficiencies in both computation and communication overhead. Specifically, the protocol demonstrates resource-efficient results, evidenced by an average reduction of approximately 63.13% and 18.51% in computation and overheads, respectively.

B. Paper Organization

This article layout is as follows: Section II provides an overview of the system model and first ideas, while Section III presents a comprehensive analysis of the developed protocol. Section IV explores the security analysis of our suggested protocol. The protocol's performance analysis is examined in Section V. Ultimately, the conclusion is stated in Section VI.

II. System Model and Preliminaries

In this section, we have explained the system model employed in the creation of the proposed protocol and the fundamental concepts crucial for understanding its operational complexities.

A. System Model

The authentication model illustrated in Fig. 1 defines the framework of IoD. It involves users ($\mathcal{USR}_i | i = 1, 2.3 \cdots N_{\text{USR}}$), Control Center $\mathcal{CC}_s$, and drones ($\mathcal{DRN}_j | j = 1, 2.3 \cdots N_{\text{DRN}}$) Here, N_{USR} and N_{DRN} signify the count of users and drones deployed.

Drone ($\mathcal{DRN}_j$): In the IoD environment, drones play a central role by gathering crucial data from the surroundings and relaying it to the control center $\mathcal{CC}_s$. For example, these

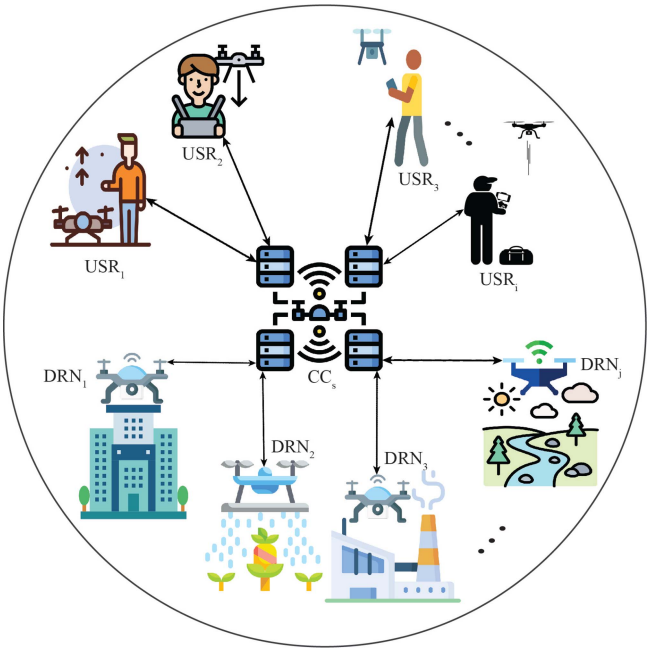

Fig. 1. Schematic illustration of the IoD infrastructure.

drones are utilized in smart cities to monitor traffic. They collect essential data on traffic congestion across various routes and transmit this information to the $\mathcal{CC}_s$.

Control Center ($\mathcal{CC}_s$): $\mathcal{CC}_s$ serves as the backbone of the IoD environment, ensuring its seamless operation. It's tasked with gathering sensitive data of drones and keeping information linked to users securely. Moreover, it manages communication among drones and users within the system.

User ($\mathcal{USR}_i$): The user avoids utilizing stored data at the control center and prefers real-time information directly gathered by drones to ensure immediate decisions. In a smart city context, such as ensuring timely hospital arrivals for ambulances, access to up-to-date traffic details is vital. Securely identifying users becomes imperative to grant authorized access solely to drone resources. Strengthening security design significantly minimizes the risk of unauthorized entry into crucial elements of the smart city infrastructure.

B. Adversarial Model

We consider Dolev-Yao (DY) [31] adversarial capabilities to model potential attacks on our protocol. Such capabilities enable an adversary $\mathcal{E}_{\text{adv}}$ to eavesdrop on any message exchanged between two entities through a public channel. It also allows an $\mathcal{E}_{\text{adv}}$ to manipulate the eavesdropped message, delete certain information, or inject any false information into the eavesdropped message. In contrast, Canetti and Krawczyk's (CK) [32] model empowers an $\mathcal{E}_{\text{adv}}$ to compromise the forward secrecy of the designed protocol if he has successfully stolen ephemeral information of any particular session. Moreover, the $\mathcal{E}_{\text{adv}}$ can obtain cryptographic keys and related information from the memory of drones through power analysis methods.

TABLE I
COMMON USED NOTATIONS

Common Notations	Elucidation
$\mathcal{USR}_i$	ith User
id_i, pid_i	$\mathcal{USR}_i$'s Unique Identity and Pseudonym
pw_i, bio_i	$\mathcal{USR}_i$'s Password and Bio
$\mathcal{DRN}_j$	ith Drone
id_i	Identity of $\mathcal{DRN}_i$
pid_i	Pseudo Identity of $\mathcal{DRN}_i$
CRP_i	Challenge-Response Pair of $\mathcal{DRN}_i$
$\mathcal{CC}_s$	Control Center
pid_s	Pseudonym of $\mathcal{CC}_s$
$\mathcal{E}_{adv}$	The Adversary
$T_s(x)$	Chebyshev Chaotic Map Operation

C. Chebyshev Polynomial (Chaotic Map)

Definition 1: Let I be an integer, y belong to the interval $[-1, 1]$, and a $I-order$ Chebyshev polynomial mapping $T_I(y) : [-1, 1] \rightarrow [-1, 1]$ can be represented as

$$T_I(y) = \cos\Big(I\cos^1(y)\Big). \tag{1}$$

The Chebyshev polynomial map can be shown recursively as follows:

$$T_I(y) = 2yT_{I-1}(y) - T_{I-1}(y) \tag{2}$$

where $T_0(y) = 1, T_1(y) = y, I \geq 2$.

Definition 2: The semi-group property of Chebyshev polynomials can be defined as

$$T_m(T_n(y)) = T_{mn}(y) = T_m(T_n(y)) \tag{3}$$

where m and n are two integers, and y belongs to the interval $[-1, 1]$.

Definition 3: The chaotic map Diffie-Hellman problem (CMDHP) is characterized by three parameters: $y, T_m(y)\ mod\ Q$, and $T_n(y)\ mod\ Q$. It poses a challenge to determine $T_{mn}(y)\ mod\ Q$. $\mathcal{E}_{\text{adv}}$'s advantage in solving CMDHP within polynomial time (p_{tm}) is represented by $Adt^{CMDHP}_{\mathcal{E}_{\text{adv}}}(p_{tm})$ and defined as $Adt^{CMDHP}_{\mathcal{E}_{\text{adv}}}(p_{tm}) = Pr[A(y, T_m(y)\ mod\ Q, T_n(y)\ mod\ Q) = T_{op}(y)\ mod\ Q : m, n \in Z^{*n}]$, where Q is a large prime number.

D. Fuzzy Extractor

The Fuzzy Extractor (F_E) consists of two key functions: 1) $F_E.Gen(.)$ for generating and 2) $F_E.Rep(.)$ for reproducing. Specifically, $F_E.Gen(.)$ produces a secret biometric key bio_i within the range $[0, 1]^{l_n bio_i}$, with $l_n bio_i$ representing the key's length derived from biometric data bio_i. The generation function is defined mathematically as $(bio_i, hd) = F_E.Gen(Bio_i)$, where hd stands for the helper data.

III. PROPOSED PROTOCOL

This section introduces the proposed protocol explicitly designed for performing secure mutual authentication among the entities of the IoD and establishing common session keys for secure communication. In the design of the proposed protocol, we employed the Chebyshev Chaotic Map and PUF functions to keep our protocol resource-friendly. Our protocol

$\mathcal{USR}_i$	$\mathcal{CC}_s$
Chooses: id_i, pw_i	
Imprints bio_i	$Ver(A_i, id_i \Vert Rev_i \Vert \eta_2) \stackrel{?}{=} 1$
Computes: $(\eta_1, \eta_2) = Gen(bio_i)$	Generates: n_2
Computes: $A_i = sig(id_i \Vert Rev_i \Vert \eta_1 \Vert \eta_2)$	Computes:
$\xrightarrow{\{id_i, A_i, \eta_2\}}$	$\chi = h(sr \Vert pid_s), T_\chi(x)$
	$X_i = h(id_i \Vert \chi)$
$Y_i^* = Y_i \oplus id_i$	$Y_i = X_i \oplus A_i \oplus id_i$
$Y_i^* = X_i \oplus A_i$	$PID_i = E_{T_\chi}(id_i \Vert n_2 \Vert \chi)$
$Z_i = h(id_i \Vert Y_i^* \oplus A_i \Vert \eta_1 \Vert \eta_2)$	$\xleftarrow{\{PID_i, Y_i\}}$
Stores $\{PID_i, Y_i^*, \eta_i, Z_i, Resv_i\}$	

Fig. 2. Registration phase of proposed protocol.

can efficiently complete the authentication cycle while ensuring resistance against potential threats. Moreover, the proposed protocol is not a system. It functions within the seven-layer stack architecture of network systems, specifically focusing on the data link and transport layer. At the data link layer, the main focus is often on securing communication between entities on the same network (like between a drone and its control center). This might involve ensuring that the devices exchanging information are authenticated to communicate with each other. Authentication ensures secure sessions or connections between devices or networks at the transport layer. This could be important for establishing secure communication channels over which drones transmit data to a controller or server. Before moving to subsections below for the explanation of the phases of the proposed scheme, please refer to Table I for the notation guide.

A. User Registration

$\mathcal{CC}_s$ enrolls every third-party user $\mathcal{USR}_i$ into its system so that he can seamlessly and securely access desired information. To this end, $\mathcal{CC}_s$ performs the trailing steps as illustrated in Fig. 2.

1) At first, $\mathcal{USR}_i$ chooses id_i, pw_i and imprints bio_i. Afterward, $\mathcal{USR}_i$ computes: $(\eta_1, \eta_2) = Gen(bio_i)$ and $A_i = sig(id_i \Vert Rev_i \Vert \eta_1 \Vert \eta_2)$. $\mathcal{USR}_i$ then sends $\{id_i, A_i, \eta_2\}$ toward $\mathcal{CC}_s$.
2) On receiving $\{id_i, A_i, \eta_2\}$ from a new $\mathcal{USR}_i$, $\mathcal{CC}_s$ checks whether $Ver(A_i, id_i \Vert Rev_i \Vert \eta_2) \stackrel{?}{=} 1$. If it returns true, $\mathcal{CC}_s$ generates n_2 and computes $\chi = h(sr \Vert pid_s)$, $T_\chi(x)$, $X_i = h(id_i \Vert \chi)$, $Y_i = X_i \oplus A_i \oplus id_i$ and $PID_i = E_{T_\chi}(id_i \Vert n_2 \Vert \chi)$. Finally, $\mathcal{CC}_s$ sends registration parameters $\{PID_i, Y_i\}$ to requested $\mathcal{USR}_i$.
3) To securely keep the received registration parameters $\{PID_i, Y_i\}$, $\mathcal{USR}_i$ computes: $Y_i^* = Y_i \oplus id_i$, $Y_i^* = X_i \oplus A_i$, and $Z_i = h(id_i \Vert Y_i^* \oplus A_i \Vert \eta_1 \Vert \eta_2)$. At the end, $\mathcal{USR}_i$ keeps $\{PID_i, Y_i^*, \eta_i, Z_i, Resv_i\}$ in its memory.

B. Drone Enrollment Phase

Likewise to $\mathcal{USR}_i$, $\mathcal{CC}_s$ enrolls every $\mathcal{DRN}_j$ into the target IoD system. For this purpose, $\mathcal{CC}_s$ randomly picks id_j and pid_j. Thereafter, $\mathcal{CC}_s$ selects a random pair of CRP_i. Finally, it stores all this information in the memory of the drone. At the same time, $\mathcal{CC}_s$ also records this information in its repository.

C. Authentication Phase

This phase allows $\mathcal{USR}_i$ to get access to real-time surveillance of potential drones flying over the desired area. The details of this phase are given as follows and also demonstrated in Fig. 3.

1) $\mathcal{USR}_i$ first inputs id_i, pw_i into its PDA and imprints his bio_i. $\mathcal{USR}_i$ then computes: $(\eta_1, \eta_2) = Rep(bio_i)$ and $A_i = sig(id_i \Vert Rev_i \Vert \eta_1 \Vert \eta_2)$. $\mathcal{USR}_i$ checks whether $Z_i \stackrel{?}{=} h(id_i \Vert Y_i^* \oplus A_i \Vert \eta_1 \Vert \eta_2)$ returns true or not. If it holds true, $\mathcal{USR}_i$ generates n_3 and furnishes LI_i, and computes: $M_1 = T_{n_3}(x) \mod P$, $M_2 = (n_3 \Vert pid_j \Vert LI_i) \oplus id_i$ and $M_3 = h(id_i \Vert M_1 \Vert Y_i^* \oplus A_i \Vert LI_i)$. Finally, it requests $\mathcal{CC}_s$ with the login message $\{id_i, A_i, \eta_2\}$.
2) $\mathcal{CC}_s$ receives $\{id_i, A_i, \eta_2\}$ and computes: $(id_i \Vert n_2 \Vert \chi) = D_{T_{\chi(x)}}(PID_i)$, $X_i = h(id_i \Vert \chi)$ and $(n_3 \Vert pid_j \Vert LI_i) = M_2 \oplus id_i$. Afterward, $\mathcal{CC}_s$ checks $M_3 \stackrel{?}{=} h(id_i \Vert M_1 \Vert X_i \Vert LI_i)$. If it returns true, $\mathcal{CC}_s$ reads $< CRP_i, id_j >$ against pid_j and generates n_4. $\mathcal{CC}_s$ then computes: $PID_i^{new} = E_{T_\chi}(id_i \Vert n_4 \Vert \chi)$, $M_4 = Res_j \oplus (PID_i^{new} \Vert n_4 \Vert M_1)$, $M_5 = h(id_j \Vert pid_j \Vert Res_j \Vert n_4)$, and sends challenge message $\{M_4, M_5, Cha_j\}$ to $\mathcal{DRN}_j$.
3) $\mathcal{DRN}_j$ receives $\{M_4, M_5, Cha_j\}$ from $\mathcal{CC}_s$ and computes $Res_j = PUF_j(Cha_j)$, and $(PID_i^{new} \Vert n_4 \Vert M_1) = Res_j \oplus M_4$. After that, $\mathcal{DRN}_j$ validates $M_5 \stackrel{?}{=} h(id_j \Vert pid_j \Vert Res_j \Vert n_4$. If it holds, $\mathcal{DRN}_j$ generates: n_5 and computes: $SK = T_{n_5}(M_1)$, $M_6 = T_{n_5}(x) \mod p$, $M_7 = pid_i^{new} \oplus pid_j$, and $M_8 = h(pid_j \Vert M_1 \Vert M_7 \Vert SK)$.

To demonstrate the essential steps and prototype of our presented solution, we have presented the flow diagram in Fig. 4. From Fig. 4, it is clear that each participant (i.e., $\mathcal{USR}_i$, $\mathcal{CC}_s$, and $\mathcal{DRN}_j$) first authenticates the sending party to ensure the legitimacy of the exchanged message and participant. Once the authentication process is successful, all entities agree on a symmetric key. Hence, our protocol achieves secure authentication and key agreement among participants.

IV. Security Analysis

This section provides a thorough evaluation of the devised protocol's resilience within the Internet of Drones (IoD) context. It includes both informal and formal analyses aimed at assessing the protocol's robustness and its ability to withstand a variety of attacks under different scenarios.

A. Informal Security Analysis

The informal security analysis presented in this section rigorously examines the protocol's defense mechanisms against potential security vulnerabilities. By dissecting its key security features and underlying design principles, we gain a comprehensive insight into how the protocol withstands not only common threats but also counters advanced cyber-attacks effectively.

1) Offers Anonymity: In the suggested protocol, $\mathcal{USR}_i$ does not disclose its Id_i on a public channel. In addition, the public message $\{PID_i, M_1, M_2, M_3\}$ transmitted by $\mathcal{USR}_i$ does not contain any information about id_i. In addition, it is important to note that every session is allocated a distinct

$\mathcal{USR}_i$	$\mathcal{CC}_s$	$\mathcal{DRN}_j$
Inputs id_i, pw_i		
Imprints bio_i		
Compute:		
$(\eta_1, \eta_2) = Rep(bio_i)$	$(id_i \| n_2 \| \chi) = D_{T_{\chi(x)}}(PID_i)$	
$A_i = sig(id_i \| Rev_i \| \eta_1 \| \eta_2)$	$X_i = h(id_i \| \chi)$	
$Z_i \stackrel{?}{=} h(id_i \| Y_i^* \oplus A_i \| \eta_1 \| \eta_2)$	$(n_3 \| pid_j \| LI_i) = M_2 \oplus id_i$	
Generates: n_3	Verifies $M_3 \stackrel{?}{=} h(id_i \| M_1 \| X_i \| LI_i)$	
Furnishes: LI_i	Reads $< CRP_i, id_j >$ against pid_j	Computes: $Res_j = PUF_j(Cha_j)$
Computes: $M_1 = T_{n_3}(x) \mod P$	Generates random numbers n_4	$(PID_i^{new} \| n_4 \| M_1) = Res_j \oplus M_4$
$M_2 = (n_3 \| pid_j \| LI_i) \oplus id_i$	Computes:	$M_5 \stackrel{?}{=} h(id_j \| pid_j \| Res_j \| n_4$
$M_3 = h(id_i \| M_1 \| Y_i^* \oplus A_i \| LI_i)$	$PID_i^{new} = E_{T_\chi}(id_i \| n_4 \| \chi)$	Generates: n_5
$\xrightarrow{\{PID_i, M_1, M_2, M_3\}}$	$M_4 = Res_j \oplus (PID_i^{new} \| n_4 \| M_1)$	Computes: $SK = T_{n_5}(M_1)$
	$M_5 = h(id_j \| pid_j \| Res_j \| n_4)$	$M_6 = T_{n_5}(x) \mod p$
	$\xrightarrow{\{M_4, M_5, Cha_j\}}$	$M_7 = pid_i^{new} \oplus pid_j$
		$M_8 = h(pid_j \| M_1 \| M_7 \| SK)$
		$\xleftarrow{\{M_6, M_7, M_8\}}$
$SK = T_{n_3}(M_6)$		
$pid_i^{new} = pid_j \oplus M_7$		
$M_8 \stackrel{?}{=} h(pid_j \| M_1 \| M_7 \| SK)$		

Fig. 3. Proposed authentication phase for IoD environment.

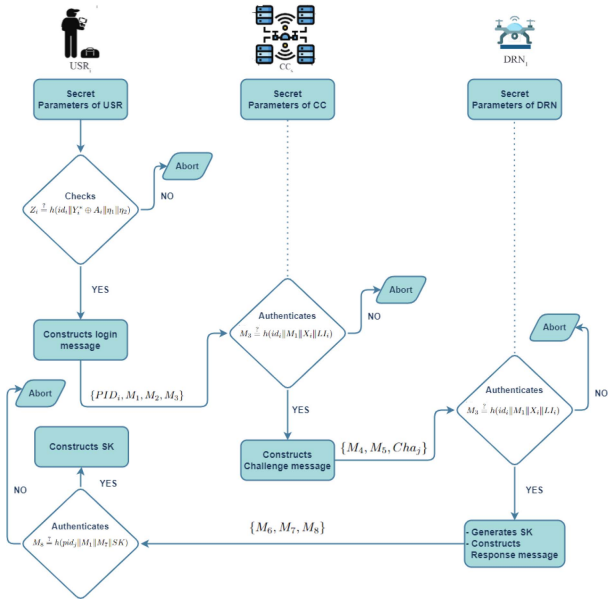

Fig. 4. Flow diagram of proposed protocol.

pseudo identity PID_i. This ensures that $\mathcal{E}_{\text{adv}}$ is unable to trace $\mathcal{USR}_i$ by observing two distinct messages associated with the same $\mathcal{USR}_i$. As a consequence of the inability of $\mathcal{E}_{\text{adv}}$ to track his activities through public channel messages, as well as his inability to determine the true id_i of $\mathcal{V}_i$. Hence, the justification for offering anonymity and untraceability in the proposed protocol is evident.

2) Resists $\mathcal{USR}_i$ Impersonation Attack (SF_1): The adversary ($\mathcal{E}_{\text{adv}}$), may try to create a legitimate login message $\{PID_i, M_1, M_2, M_3\}$ with the intention of impersonating $\mathcal{USR}_i$. Nevertheless, in order to effectively create the original message, $\mathcal{E}_{\text{adv}}$ must ascertain the values of id_i, A_i, and LI_i. As, id_i, A_i, and LI_i are neither saved nor publicly transmitted, it is infeasible for $\mathcal{E}_{\text{adv}}$ to ascertain these values. As a result, $\mathcal{E}_{\text{adv}}$ is unable to accurately determine the true values of $\{PID_i, M_1, M_2, M_3\}$. Consequently, the proposed protocol effectively mitigates $\mathcal{USR}_i$ impersonation attacks.

3) Resists $\mathcal{CC}_s$ Impersonation Attack (SF_2): In the devised protocol, $\mathcal{E}_{\text{adv}}$ must create valid messages $\{M_4, M_5, Cha_j\}$ to proceed $\mathcal{CC}_s$ impersonation attack. Notably, $\mathcal{E}_{\text{adv}}$ must first develop id_i, χ and id_j which are required for the calculation of $\{M_4, M_5, Cha_j\}$. However, χ and id_j are only known to $\mathcal{CC}_s$ and id_i cannot expose to $\mathcal{E}_{\text{adv}}$ as discussed in Section IV-A1. Therefore, $\mathcal{E}_{\text{adv}}$ is unable to determine $\{M_4, M_5, Cha_j\}$. So, the proposed protocol efficiently resists $\mathcal{CC}_s$ impersonation attack.

4) Resists $\mathcal{DRN}_j$ Impersonation Attack (SF_3): In the suggested protocol, if $\mathcal{E}_{\text{adv}}$ attempts to relay challenge message $\{M_6, M_7, M_8\}$ on behalf of a legitimate $\mathcal{DRN}_j$, it is required that $\mathcal{E}_{\text{adv}}$ accurately compute the values of M_6 and M_7. To compute M_7, it is necessary for $\mathcal{E}_{\text{adv}}$ to possess valid values of pid_i^{new} and pid_j. The computation of pid_i^{new} necessitates id_i of $\mathcal{USR}_i$, and the calculation of pid_j requires the availability of id_j. However, $\mathcal{E}_{\text{adv}}$ does not possess access to these identifiers. Hence, the proposed protocol offers a robust defense mechanism against drone impersonation assaults.

5) Resists Physical Attack (SF_4): $\mathcal{E}_{\text{adv}}$ can try to compromise the $\mathcal{DRN}_j$ physically. In the devised protocol, we employed the PUF function to each $\mathcal{DRN}_j$. The independent, safe, and different characteristics of the PUF prevent $\mathcal{E}_{\text{adv}}$ from accurately predicting or replicating the true response message Res_j. If $\mathcal{E}_{\text{adv}}$ tries to capture any $\mathcal{DRN}_j$ with the intention of physically corrupting the PUF, it will cause fluctuations in the PUF's intrinsic desired output. As a result, it is not possible for $\mathcal{E}_{\text{adv}}$ to accurately replicate the actual Res_j values using the corrupted $\mathcal{DRN}_j$. Consequently, the devised protocol confirms security measures against both physical and cloning threats.

6) Provides Forward Secrecy (SF_5): The session key is derived as $SK = T_{n_3}(M_6)$. In the devised protocol, n_3 updates uniquely at each session's end. Therefore, revealing the current session key $SK = T_{n_3}(M_6)$ doesn't compromise

the previous ones, as recalculating them using the current n_3 is infeasible. This mechanism ensures that an adversary $\mathcal{E}_{\text{adv}}$ cannot backtrack to earlier session keys, thereby achieving perfect forward secrecy.

7) Resists Ephemeral Secret Leakage Attack (SF_6): Under the assumptions detailed in Section II-B, $\mathcal{E}_{\text{adv}}$ could reconstruct the session key *SK* by uncovering the ephemeral secrets of a given session. Our protocol generates *SK* using nonpublic ephemeral secrets n_3, n_4, and n_5. Even in the extreme case where $\mathcal{E}_{\text{adv}}$ deciphers *SK* for a specific session, previous session keys remain unaffected. Thereby, the proposed protocol preserves ephemeral secret leakage attacks.

B. ROM-Based Formal Security Analysis

The security of the session key (*SK*) generated during the authentication phase of the proposed protocol undergoes formal analysis utilizing the ROM. The constituents of the ROM are illustrated as follows.

Participants: In the proposed protocol, three fundamental parties or participants, namely, $\mathcal{USR}_i$, $\mathcal{CC}_s$, and $\mathcal{DRN}_j$, are involved. We represent the instances $C1$, $C2$, and $C3$ of $\mathcal{USR}_i$, $\mathcal{CC}_s$, and $\mathcal{DRN}_j$ as $\Theta^{C1}_{\mathcal{USR}_i}$, $\Theta^{C2}_{\mathcal{CC}_s}$, and $\Theta^{C3}_{\mathcal{DRN}_j}$ serving the role of oracles.

Partnership: The instances $\Theta^{C1}_{\mathcal{USR}_i}$ and $\Theta^{C3}_{\mathcal{DRN}_j}$ become partners in the acceptance state if they share a common *SK*.

Freshness: $\mathcal{E}_{\text{adv}}$ is restricted from disclosing the *SK* established during the authentication phase between $\Theta^{C1}_{\mathcal{USR}_i}$ and $\Theta^{C2}_{\mathcal{CC}_s}$. Furthermore, $\mathcal{E}_{\text{adv}}$ influences various queries in subsequent stages to mount different attacks on the proposed authentication protocol.

CorruptSDE(Θ^{C1})*:* $\mathcal{E}_{\text{adv}}$ will execute this query to retrieve the long-term secret and sensitive credentials stored in SDEi's memory.

Test(Θ^{C1})*:* $\mathcal{E}_{\text{adv}}$ will conduct this query to determine if the speculative *SK* constitutes a legitimate session key or just a random result.

Reveal(Θ^{C1})*:* This query allows $\mathcal{E}_{\text{adv}}$ to acquire the *SK* generated during the authentication phase, maintained by Oracle Θ^{C1}.

Send(Θ^{C1},*MSG):* $\mathcal{E}_{\text{adv}}$ executes a real attack using this query. Following the attack model, Θ^{C1} has the capability to send *MSG* to Θ^{C1} and receive a response accordingly.

Execute($\Theta^{C1}_{\mathcal{USR}_i}$, $\Theta^{C2}_{\mathcal{CC}_s}$, $\Theta^{C3}_{\mathcal{DRN}_j}$)*:* By executing this query, $\mathcal{E}_{\text{adv}}$ is empowered to retrieve or intercept all messages exchanged during the authentication phase, constituting a passive assault.

Definition 4: In the ROM, a probabilistic polynomial-time (p_{tm}) adversary $\mathcal{E}_{\text{adv}}$ is present with the objective of distinguishing the *SK* from an arbitrarily engendered nonce of the same size. $\mathcal{E}_{\text{adv}}$ is endowed with the capability to execute queries, including *Execute*, *Send*, and *CorruptSDE*, at any given time. However, $\mathcal{E}_{\text{adv}}$ is constrained to performing a single Test operation on a specific instance. Subsequently, $\mathcal{E}_{\text{adv}}$ proposes its hypothesis, evaluating if the *Test* query's result matches the accurate session key. $\mathcal{E}_{\text{adv}}$ achieves success in the game when the value b'_t, obtained from the Test query, matches the initially speculated value b_t. The probability of $\mathcal{E}_{\text{adv}}$ winning the game is expressed as $Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = |2.Adt^{G_n} - 1|$. The IoD protocol is deemed secure within the ROM if the value of $Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm})$ is negligibly small.

Theorem 1: There is speculation about the advantage gained when a polynomial-time adversary $\mathcal{E}_{\text{adv}}$ attempts to compromise the security of the *SK* during the authentication phase in IoD

$$Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) \leq \frac{H_p^2}{|HO|} + \frac{Sn_p}{2^{l_n bio_i - 1}.PW_d} + 2.\text{Adv}^{\text{CMDHP}}_{\mathcal{E}_{\text{adv}}}(p_{tm}) \tag{4}$$

where $l_n bio_i$ represents the bit length of the biometric key, $|HO|$ denotes the size of the password dictionary, PW_d refers to the hash output, H_p^2 indicates the hash function, and Sn_p signifies the number of send queries. Additionally, $Adt^{CMDHP}_{\mathcal{E}_{\text{adv}}}(P_{tm})$ show $\mathcal{E}_{\text{adv}}$'s advantage in compromising CMDHP's security inp_{tm}, respectively.

Proof: We illustrate the proof of Theorem 1 using the following five games. ($G_n|n = 0, 1, 2, 3, 4$). $Adt^{CMDHP}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = |2.Pr[Sucss] - 1|$ denotes $\mathcal{E}_{\text{adv}}$'s advantage in compromising the security of the compromised *SK* during the authentication phase. Moreover, the term $Pr[Sucss]$ indicates the probability of $\mathcal{E}_{\text{adv}}$ achieving success by accurately predicting the bit b_t in each G_n.

G_0: In G_0, $\mathcal{E}_{\text{adv}}$ executes a real attack against the proposed protocol. Based on the implication of success, we arrive at the following:

$$Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = \left|2.Adt^{G_0} - 1\right|. \tag{5}$$

G_1: This game allows $\mathcal{E}_{\text{adv}}$ to capture all the transmitted messages $\{PID_i, M_1, M_2, M_3\}$, $\{M_4, M_5, Cha_j\}$,$\{M_6, M_7, M_8\}$ through the eavesdropping attack initiated using the *Execute*($\Theta^{C1}_{\mathcal{USR}_i}$ query. After intercepting all transmitted messages, A endeavors to produce a correct $SK = T_{n_5}(M_1)$, which includes an arbitrary number n_5, n_4 and long-term secret credentials pid_i of $\mathcal{DRN}_j$. Moreover, $\mathcal{E}_{\text{adv}}$ executes Reveal(Θ^{C1}) to unveil the guessed *SK* and subsequently employs the Test(Θ^{C1}) query to evaluate the difference between the actual *SK* and a randomly generated result bit. $\mathcal{E}_{\text{adv}}$ cannot reconstruct the actual *SK* unless both the ephemeral and long parameters are retained. Consequently, the probability of $\mathcal{E}_{\text{adv}}$ winning is very low. As a result, G_0 and G_1 are interchangeable. Thus, at this point, we have

$$Adt^{G_0} = Adt^{G_0}. \tag{6}$$

G_2: In this game, $\mathcal{E}_{\text{adv}}$ initiates a real attack by executing *HO* queries. The hash function produces *SK* on $\mathcal{USR}_i$ and $\mathcal{DRN}_j$, similar to our IoD protocol. $\mathcal{E}_{\text{adv}}$ aims to breach the *SK* security by attempting to uncover collisions through *HO* queries. However, the hash function employed in constructing the devised protocol is secure, and the likelihood of collisions in the hash function's result is minimal. Consequently, the birthday paradox will come into play

$$Adt^{G_2} - Adt^{G_1} \leq \frac{H_p^2}{2|HO|}. \tag{7}$$

G_3: In this particular game, $\mathcal{E}_{\text{adv}}$ initiates an active attack by utilizing the CorruptOBU($\Theta^{C1}_{\mathcal{USR}_i}$) query. After capturing the OBU, $\mathcal{E}_{\text{adv}}$ can obtain $\{PID_i, Y_i^*, \eta_i, Z_i, Resv_i\}$ stored in the memory of OBU. $\mathcal{E}_{\text{adv}}$ will acquire the login information for $\mathcal{USR}_i$. The probability of guessing the biometric key is $[1/(2^{l_n bio_i})]$, which is highly unlikely. Furthermore, $\mathcal{USR}_i$ is constrained by a limited number of failed password attempts, making it feasible to exploit vulnerabilities in such situations

$$Adt^{G_3} - Adt^{G_2} \leq \frac{Sn_p}{2^{l_n bio_i}.PW_d}. \tag{8}$$

G_4: In this particular game, $\mathcal{E}_{\text{adv}}$, by executing the Execute query Execute($\Theta^{C1}_{\mathcal{USR}_i}$, $\Theta^{C2}_{\mathcal{CC}_s}$, $\Theta^{C3}_{\mathcal{DRN}_j}$) and get $\{PID_i, M_1, M_2, M_3\}$, $M_4, M_5, Cha_j\}$,$\{M_6, M_7, M_8\}$. The primary objective of $\mathcal{E}_{\text{adv}}$, after intercepting the messages, is to obtain the secret parameters shared among $\mathcal{USR}_i$, $\mathcal{CC}_s$, and $\mathcal{DRN}_j$ during the authentication phase and construct SK. To achieve this goal, $\mathcal{E}_{\text{adv}}$ needs to compromise the security of the *CMDHP* within polynomial time (p_{tm}). In accordance with Definition 3, we obtain the following:

$$Adt^{G_4} - Adt^{G_3} \leq Adt^{CMDHP}_{\mathcal{E}_{\text{adv}}}(P_{tm}). \tag{9}$$

$\mathcal{E}_{\text{adv}}$ upon completing all $(G_n | n = 0, 1, 2, 3, 4)$ games, gains no significant advantage in determining the valid bit b_T Consequently, we conclude that

$$Adt^{G_4} = \frac{1}{2}. \tag{10}$$

From (5) and (6), we obtain

$$Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = \left| 2.Adt^{G_0} - \frac{1}{2} \right|. \tag{11}$$

From (11) we obtain

$$\frac{1}{2}.Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = \left| Adt^{G_0} - Adt^{G_4} \right|. \tag{12}$$

By using (10) and (12), we obtain

$$\frac{1}{2}.Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) = \left| Adt^{G_1} - Adt^{G_4} \right|. \tag{13}$$

Upon considering the triangular inequality, we get

$$\begin{aligned} \left| Adt^{G_1} - Adt^{G_4} \right| &\leq \left| Adt^{G_1} - Adt^{G_2} \right| \\ &\quad + \left| Adt^{G_2} - Adt^{G_4} \right| \\ &\leq \left| Adt^{G_1} - Adt^{G_2} \right| + \left| Adt^{G_2} - Adt^{G_3} \right| \\ &\quad + \left| Adt^{G_3} - Adt^{G_4} \right|. \end{aligned} \tag{14}$$

Equation (14) is expressing that the overall advantage of an adversary in the first game compared to the fourth game can be broken down into the sum of three steps: the advantage in the first game compared to the second game, then the advantage in the second game compared to the third game, and finally, the advantage in the third game compared to the fourth game.

By using (7), (8), and (14), we get

$$Adt^{IoD}_{\mathcal{E}_{\text{adv}}}(P_{tm}) \leq \frac{H_p^2}{|HO|} + \frac{Sn_p}{2^{l_n bio_i - 1}.PW_d} + 2.\text{Adv}^{\text{CMDHP}}_{\mathcal{E}_{\text{adv}}}(p_{tm}). \tag{15}$$

TABLE II
EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

Operation(s)	Description(s)	Machine-1	Machine-2
T_{hs}	Hash function	0.55 ms	1.25 ms
T_{mu}	Point multiplication	0.98 ms	1.81 ms
T_{pa}	Point addition	0.11 ms	0.30 ms
T_{cmap}	Chaotic map	0.66 ms	0.92 ms
T_{bp}	Bi-linear pairing	2.31 ms	2.99 ms
$T_{se/sd}$	Encryption/decryption	0.71 ms	1.39 ms
T_p	Physical unclonable function	0.22 ms	0.91 ms

Equation (15) is expressing the adversary's advantage in terms of the security parameter, lengths of various parameters, such as hash output, bio-metric key, and password dictionary, as well as the adversary's interaction with specific oracles, i.e., CMDHP in polynomial time under oracle model. It's a way to quantify the security of a protocol or system under the assumptions and conditions specified in the ROM. ■

V. PERFORMANCE EVALUATION

This section offers an analysis of our protocol's performance and conducts a comparison with the related work of Tanveer et al. [1], Ever [26], Irshad et al. [33], and Chaudhary et al. [34]. The comparison focuses on computational and communication overheads, as well as the security features provided by each protocol. We consider two machines to implement the cryptographic operations for computation overhead to get the experimental results.

To execute the operations of $\mathcal{CC}_s$, we consider Machine-1 with Intel Core I7, @ 5.10-GHz CPU, 16-GB RAM, and OS Windows. Furthermore, to execute the operations of $\mathcal{USR}_i$ and $\mathcal{DRN}_j$, we consider Machine-2 with Core-2 duo CPU, 2-GB RAM, and OS Windows. We utilize the PyCharm library to implement cryptographic operations on the machines mentioned above. Table II shows the cryptographic notations, description, and running time on respective machines.

A. Computation Cost Analysis

The proposed and related protocols use various cryptographic operations, including hash function, point multiplication, point addition, chaotic map, bi-linear pairing, symmetric encryption/decryption, PUF, etc. The notations for all these operations are listed in Table II. In the proposed protocol, $\mathcal{CC}_s$ uses the hash function three times and chaotic map two times, which costs $(2 \times 0.66) + (4 \times 1.85) \approx 2.97$ ms. Similarly, $\mathcal{USR}_i$ and $\mathcal{DRN}_j$ collectively use one-time chaotic map, five times hash function, and one-time PUF, which costs $(1 \times 0.92) + (5 \times 1.98) + (1 \times 1.37) \approx 8.08$ ms. Thus, the total computation cost of our protocol is $(2.97 + 8.08) \approx 11.05$ ms. The computation cost of other competing protocols of [1], [26], [33], and [34] is calculated using a similar way. Table III and Fig. 5 shows the in-depth comparison of proposed and relevant protocols regarding computation cost. It is evident from the given comparison that our protocol offers 56.62%, 80.58%, 59.96%, and 74.28% reductions in computation cost in comparison to the protocols of [1], [26], [33], and [34], respectively.

TABLE III
COMMUNICATION AND COMPUTATION COSTS COMPARISON

Protocol	Communication Cost (bits)	Computation Cost (ms)		
	Total Cost	$\mathcal{CC}_s$	$\mathcal{USR}_i$ and $\mathcal{DRN}_j$	Total Cost
Proposed	1888	$2T_{cmap} + 3T_{hs} \approx 2.97$	$1T_{cmap} + 5T_{hs} + 1T_p \approx 8.08$	11.05
Tanveer et al. [1]	1952	$1T_{cmap} + 3T_{hs} + 2T_{se/sd} \approx 3.73$	$4T_{cmap} + 10T_{hs} + 4T_{se/sd} \approx 21.74$	25.47
Ever et al. [26]	1984	$2T_{bp} + 3T_{hs} \approx 6.27$	$4T_{mu} + 14T_{hs} + 4T_{bp} \approx 36.70$	42.97
Irshad et al. [33]	3296	$2T_{mu} + 9T_{hs} + 2T_{se/sd} + 1T_{pa} \approx 8.44$	$9T_{mu} + 25T_{hs} + 3T_{pa} \approx 48.44$	56.88
Chaudhary et al. [34]	2464	$7T_{hs} \approx 3.85$	$19T_{hs} \approx 23.75$	27.60

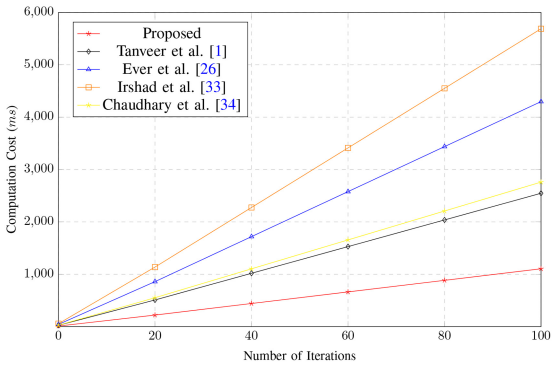

Fig. 5. Computation cost comparison.

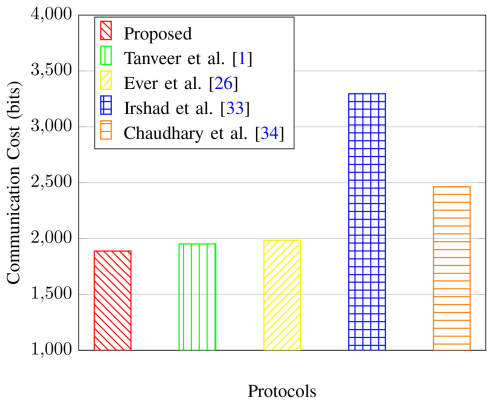

Fig. 6. Communication cost comparison.

B. Communication Cost Analysis

To determine the communication cost of our and analogous relevant protocols, we consider the length of symmetric encryption/decryption, identity, pseudo-identity, time stamp, concatenation, XOR, hash function, and chaotic map 128, 160, 160, 160, 160, 160, 256, and 320 bits, respectively. In our protocol, the authentication phase is accomplished through the exchange of three messages. First, $\mathcal{USR}_i$ transmits a message $\{PID_i, M_1, M_2, M_3\}$ toward $\mathcal{CC}_s$, which costs (160+160+160+256)=736 bits. Second, $\mathcal{CC}_s$ sends a message $\{M_4, M_5, Cha_j\}$ to $\mathcal{DRN}_j$, which costs (160+256+160)=576 bits. At last, $\mathcal{DRN}_j$ relays a message $\{M_6, M_7, M_8\}$ toward $\mathcal{USR}_i$ and it costs (160+160+256)=576 bits. Hence, the total communication cost of our protocol amounts to (736+576+576)= 1888 bits. The communication cost of other competing protocols of [1], [26], [33], and [34] is determined in the same way. Table III and Fig. 6 show the detailed communication cost comparison among our devised and related protocols. It is evident from the given comparison that our protocol offers 3.28%, 42.72%, 23.38%, and 4.84% reductions in communication cost as compared to the protocols of [1], [26], [33], and [34], respectively.

C. Security Features Comparison

We compare the devised protocol with the protocol of Tanveer et al. [1], Ever et al. [26], Irshad et al. [33], and Chaudhary et al. [34] to determine their security functionality and features. The protocol [26] fails to ensure user anonymity, forward secrecy, and resist physical attack. Similarly, the protocols of [1], [33], and [34] neither offer perfect forward secrecy nor resist physical attack. The detailed security features comparison is shown in Table IV, which indicates that our protocol offers some extra security features in comparison to related protocols [1], [26], [33], [34]. Therefore, it is claimed that the devised protocol provides better security than related protocols.

TABLE IV
SECURITY FEATURES COMPARISON

Security Features→ Protocols ↓	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6
Proposed	✓	✓	✓	✓	✓	✓
Tanveer et al. [1]	✓	✓	✓	✓	✗	✗
Ever et al. [26]	✗	✓	✓	✓	✗	✗
Irshad et al. [33]	✓	✓	✓	✓	✗	✗
Chaudhary et al. [34]	✓	✓	✓	✓	✗	✗

✓Provides; ✗Doesn't Provide

Through rigorous comparison and analysis, it has proved that our protocol surpasses the related protocols regarding communication overhead, computation overhead, and security features. This remarkable performance underscores the significance of our protocol and its potential to advance in the IoD domain.

VI. CONCLUSION

In this article, we address the critical security needs of the IoD by introducing a lightweight authentication protocol. Utilizing chaotic maps, hash functions, and a PUF, the proposed protocol demonstrates robust defense against known IoD security threats like impersonation, replay, and physical cloning attacks. Our extensive security evaluations, encompassing informal and formal analysis with the ROM, affirm the protocol's effectiveness in reinforcing IoD communication privacy and security. Furthermore, the performance assessment reveals that the devised protocol not only ensures the provision of added security features but it also provides 67.86% and 17.80% reduction in computation and communication overheads, respectively, compared to related protocols. The devised protocol offers a practical solution to

IoD security challenges and sets a foundation for advancements in secure drone communication networks. In the future, we will focus on scaling the IoD authentication protocol in larger networks, integrating with AI and blockchain, ensuring quantum-resistant security, and exploring user authentication. Furthermore, we will investigate energy-efficient drone implementations, address evolving threat landscapes, and pursue standardization and interoperability efforts.

REFERENCES

[1] M. Tanveer, H. Alasmary, N. Kumar, and A. Nayak, "SAAF-IoD: Secure and anonymous authentication framework for the Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 232–244, Jan. 2024.

[2] A. Irshad, B. A. Alzahrani, A. Albeshri, K. Alsubhi, A. Nayyar, and S. A. Chaudhry, "SPAKE-DC: A secure PUF enabled authenticated key exchange for 5G-based drone communications," *IEEE Trans. Veh. Technol.*, early access, Nov. 30, 2023, doi: 10.1109/TVT.2023.3333398.

[3] S. A. Chaudhry, K. Yahya, S. Garg, G. Kaddoum, M. M. Hassan, and Y. B. Zikria, "LAS-SG: An elliptic curve-based lightweight authentication scheme for smart grid environments," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1504–1511, Feb. 2023.

[4] R. Valentino, W.-S. Jung, and Y.-B. Ko, "A design and simulation of the opportunistic computation offloading with learning-based prediction for unmanned aerial vehicle (UAV) clustering networks," *Sensors*, vol. 18, no. 11, p. 3751, 2018.

[5] N. Khan, J. Zhang, G. A. Mallah, and S. A. Chaudhry, "A secure and efficient information authentication scheme for e-healthcare system," *Comput., Mater. Continua*, vol. 76, no. 3, 2023, pp. 3878–3896.

[6] S. A. Chaudhry et al., "An anonymous device to device access control based on secure certificate for Internet of Medical Things systems," *Sustain. Cities Soc.*, vol. 75, Dec. 2021, Art. no. 103322.

[7] 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. Stand. Interfaces*, vol. 80, Mar. 2022, Art. no. 103566.

[8] S. A. Chaudhry et al., "A lightweight authentication scheme for 6G-IoT enabled maritime transport system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2401–2410, Feb. 2023.

[9] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "BSDCE-IoV: Blockchain-based secure data collection and exchange scheme for IoV in 5G environment," *IEEE Access*, vol. 11, pp. 36158–36175, 2023.

[10] S. Hussain, M. Farooq, B. A. Alzahrani, A. Albeshri, K. Alsubhi, and S. A. Chaudhry, "An efficient and reliable user access protocol for Internet of Drones," *IEEE Access*, vol. 11, pp. 59688–59700, 2023.

[11] S. Samanth, K. V. Prema, and M. Balachandra, "Security in Internet of Drones: A comprehensive review," *Cogent Eng.*, vol. 9, no. 1, 2022, Art. no. 2029080.

[12] C.-M. Chen, Z. Chen, A. K. Das, and S. A. Chaudhry, "A security-enhanced and ultralightweight communication protocol for Internet of Medical Things," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10168–10182, Mar. 2024.

[13] K. Mahmood, T. Tariq, A. K. Sangaiah, Z. Ghaffar, M. A. Saleem, and S. Shamshad, "A neural computing-based access control protocol for AI-driven intelligent flying vehicles in industry 5.0-assisted consumer electronics," *IEEE Trans. Consum. Electron.*, early access, May 19, 2023, doi: 10.1109/TCE.2023.3276066.

[14] M. Tanveer, A. Badshah, H. Alasmary, A. U. Khan, and S. A. Chaudhry, "CMAF-IIoT: Chaotic map-based authentication framework for Industrial Internet of Things," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100902.

[15] M. Tanveer, G. Abbas, Z. H. Abbas, M. Bilal, A. Mukherjee, and K. S. Kwak, "LAKE-6SH: Lightweight user authenticated key exchange for 6LoWPAN-based smart homes," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2578–2591, Feb. 2022.

[16] J. Guo et al., "ICRA: An intelligent clustering routing approach for UAV Ad Hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2447–2460, Feb. 2023.

[17] M. A. Khan et al., "Securing Internet of Drones with identity-based proxy signcryption," *IEEE Access*, vol. 9, pp. 89133–89142, 2021.

[18] 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.

[19] C.-L. Hsu and T.-W. Lin, "Password authenticated key exchange protocol for multi-server mobile networks based on Chebyshev chaotic map," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, 2013, pp. 90–95.

[20] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Sep. 2015.

[21] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li, and A. Alelaiwi, "Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy," *Nonlin. Dyn.*, vol. 83, pp. 2085–2101, Mar. 2016.

[22] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2884–2895, Aug. 2018.

[23] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.

[24] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular Ad-Hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021.

[25] J. Cui, J. Yu, H. Zhong, L. Wei, and L. Liu, "Chaotic map-based authentication scheme using physical unclonable function for Internet of Autonomous Vehicle," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3167–3181, Mar. 2023.

[26] 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, Apr. 2020.

[27] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.

[28] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones Environment," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9918–9933, Jun. 2022.

[29] Z. Liu et al., "PPTM: A privacy-preserving trust management scheme for emergency message dissemination in space–air–ground-integrated vehicular networks," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5943–5956, Apr. 2022.

[30] Y. Qiu and M. Ma, "A mutual authentication and key establishment scheme for M2M communication in 6LoWPAN networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2074–2085, Dec. 2016.

[31] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn.*, 2002, pp. 337–351.

[32] 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.

[33] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber–physical systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, Sep. 2023.

[34] D. Chaudhary, T. Soni, K. L. Vasudev, and K. Saleem, "A modified lightweight authenticated key agreement protocol for Internet of Drones," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100669.