






# Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones

Sajid Hussain , Shehzad Ashraf Chaudhry , Osama Ahmad Alomari, Mohammed H. Alsharif ,  
Muhammad Khurram Khan , *Senior Member, IEEE*, and Neeraj Kumar , *Senior Member, IEEE*

**Abstract**—The continuous innovation and progression in hardware, software and communication technologies helped the expansion and accelerated growth in Internet of Things based drone networks (IoD), for the devices, applications and people to communicate and share data. IoD can enhance comfort in many applications including, daily life, commercial, and military/rescue operations in smart cities. However, this growth in infrastructure smartness is also subject to new security threats and the countermeasures require new customized solutions for IoD. Many schemes to secure IoD environments are proposed recently; however, some of those were proved as insecure and some degrades the efficiency. In this article, using elliptic curve cryptography, we proposed a new authentication scheme to secure the communication between a user and a drone flying in some specific flying zone. The security of the proposed scheme is solicited using formal Random oracle method along with a brief discussion on security aspects provided by proposed scheme. Finally, the comparisons with some related and latest schemes is illustrated.

**Index Terms**—Authentication, drone capture attack, Internet of Drones (IoD), Internet of Things (IoT) security, key-agreement, provable security, smart city security, three-factor authentication.

## I. INTRODUCTION

THE development and innovation in information and telecommunication, hardware, and software have played a vital role in the expansion of the Internet of Things (IoT) with

Manuscript received April 6, 2020; revised June 23, 2020, September 11, 2020, September 18, 2020, and December 20, 2020; accepted January 27, 2021. Date of publication March 1, 2021; date of current version August 26, 2021. This work was supported by Researchers Supporting Project under Grant RSP-2020/12, King Saud University, Riyadh, Saudi Arabia. (*Corresponding author: Neeraj Kumar.*)

Sajid Hussain is with the Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000, Pakistan (e-mail: sajid.mscs840@iiu.edu.pk).

Shehzad Ashraf Chaudhry and Osama Ahmad Alomari are with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul 34310, Turkey (e-mail: ashraf.shehzad.ch@gmail.com; oalomari@gelisim.edu.tr).

Mohammed H. Alsharif is with the Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, Seoul 05006, South Korea (e-mail: malsharif@sejong.ac.kr).

Muhammad Khurram Khan is with the Center of Excellence in Information Assurance, College of Computer and Information Sciences, King Saud University, Riyadh 11653, Saudi Arabia (e-mail: mkhurram@ksu.edu.sa).

Neeraj Kumar is with the Department of CSED, Thapar Institute of Engineering and Technology, Punjab 147004, India, with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India, with the Department of Computer Science and Information Engineering, Asia University, Taichung City 41354, Taiwan, and also with the King Abdul Aziz University, Jeddah 21589, Saudi Arabia (e-mail: neeraj.kumar@thapar.edu).

Digital Object Identifier 10.1109/JSYST.2021.3057047

the number of connected devices growing by the day [1]–[3]. The exceptional unprecedented propagation of the IoT devices, such as smartphones, medical sensors, fitness trackers, and smart security system, has empowered people to share information [4]–[7] endlessly. Now, the city users can be benefited by endless connectivity extended by the proposed generation of networks including 6G/IoT. The explosion of devices and smartness of infrastructure along with population increase may effect the daily life of the citizens, especially in large cities. In aid to traditional ways of surveillance, the Drones with surveillance capabilities can enhance the quality of life and can be very helpful in reducing crime rate. Moreover, such drones can be deployed in inaccessible places or places with hard access like: fire sites, mountain peaks, etc.

A drone is an unpowered aircraft or spacecraft, also known as an “unmanned aerial vehicle,” or UAV. Internet of drones (IoD) is an extension of IoT, where things are specified by drones and that, also, in 3-D environments, the rest of the IoD domain properties are the same as of IoT. IoT are static, while drones can move dynamically toward the IoT devices and gather information, initiate a real-time connection, process the data, and send information through the group of nodes. A drone has more computation processing power as compared to IoT, which has less power. Some security risks exist, such as spoofing/sniffing, key logging, information gathering, and signal jamming and many more attacks, which equally influence in case of an IoD or IoT. IoD is envisioned to become an indispensable milestone in the development of drones [8]. In the IoD access control, data, confidentiality and data sharing are challenges that IoD face. IoD is potentially prone to attacks, such as impersonation, drone capture, man-in-the-middle, replay, insider attacks, and broadcasting issues. Drones can be captured/stolen physically, and the secret data in the memory of the drone can be exposed. Resilience against physical capture is very important for smooth functioning of an IoD network. Security threats and vulnerabilities can result to an attack on confidentiality, integrity, authenticity, and availability of IoD. Collection of data of different regions, securely and efficiently sharing this collected data that only authorized entities have access to the data, remains an ongoing challenge. Gharibi *et al.* [9] described IoD as a “layered network control architecture” which supports drones for coordination. In the IoD environment, many drones consolidate and create a network while transmitting and receiving data from each other. The drones gather environment-related information including the surveillance, and the data are further

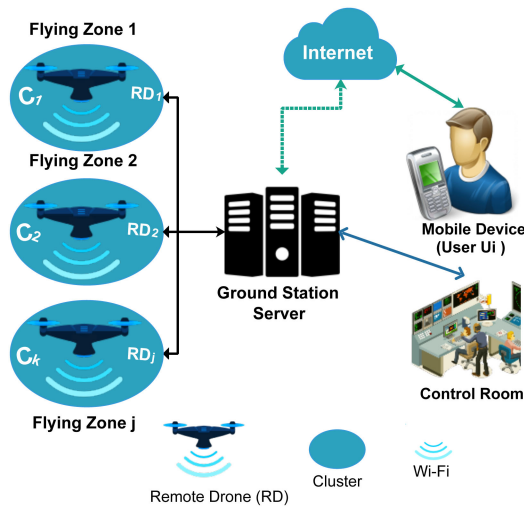


Fig. 1. IoT environment monitoring system.

transmitted to users through ground station/server. The real-time drone data are very useful for environment relating monitoring. Drone tracking can also be used for wicked intentions too. A deceitful attacker (insider or otherwise) with malevolent intentions can trace the location-related whereabouts of the drones with to disrupt consequential services, escaping from surveillance and apprehending drones themselves. As shown in Fig. 1, the legal user can access the remote drone through the internet. A number of methods to access the smart devices in the IoT environment are proposed in the recent past and most of these recent schemes are based on three factors (smart card, password, biometric) [10]–[13] due to their enhanced security. Recently, Turkanović *et al.* [14] proposed a lightweight key-agreement scheme to remote user to securely share a session key with a sensor node and to provide mutual authentication between user, sensor node, and the gateway node. However, Banerjee *et al.* [15] proved that scheme proposed in [14] is prone to sensor node capture attack, denial-of-services (DoS) attack, insecure login phase and related attacks. Banerjee *et al.* then proposed an enhanced scheme to overcome these flaws. Farash *et al.* [16] also proved that the scheme of Turkanović *et al.* has weaknesses against some cryptographic attacks. Farash *et al.* then proposed an improved scheme to secure 3 party setting usable in wireless sensor networks. In 2017, Challa *et al.* [17] also proposed a signature based authentication scheme for three party settings in IoT environments. In 2018, Challa *et al.* [18] yet proposed another scheme to secure three party settings in cloud based IoT environments. However, Chaudhry *et al.* [19] argued the correctness and in-applicability of their both schemes [17], [18] in real-world scenarios. Another scheme to protect industrial IoT in three party settings was proposed by Das *et al.* [20] in 2018. However, in their comment, Hussain and Chaudhry [21] stated some crucial weaknesses in the scheme of Das *et al.* Won *et al.* [22] proposed schemes to secure drones in one to one, one to many and many to one settings using certificate-less cryptography. Another scheme using only symmetric cryptography was proposed by Srinivas *et al.* [23], due to usage

of verifier in the scheme [23] and using generic parameters for pseudonymity of the user, their scheme lacks anonymity and susceptible to stolen verifier attack [24]. In 2019, Wazid *et al.* [25] proposed a new mechanism for securing IoD communication and claimed that their protocol is secure and withstands the known attacks. However, similar to Srinivas *et al.*'s scheme, Wazid *et al.*'s scheme lacks anonymity and susceptible to stolen verifier attack. At last, in Table I, a summary of the schemes and their properties including limitations/drawbacks of previous user authentication schemes related to the IoD environment is presented.

### A. Motivations and Contributions

The secure and uninterrupted user access to specified drones can realize a large number of applications from commercial to government and military purposes. Deployment of drones for such applications is otherwise considered as risky due to sensitive nature of applications and inherited insecurities of the public channel including: real-time data modification, clogging, replay, jamming, etc. Although, in recent past some security schemes were proposed for IoD; however, many such schemes were proved insecure or inapplicable, as shown in Table I, the insecurities of exiting works are already explored in literature. Therefore, an authentication scheme, which can ensure security as well as privacy is the need of time. The contributions of this article are as follows.

- 1) Using ECC and symmetric key primitives, we proposed an authentication scheme to secure user-drone communication. The scheme based on password, biometrics, and mobile device is designed.
- 2) The security of the proposed scheme is analyzed formally using random oracle model (ROM) supplemented by a brief discussion on security features.
- 3) As per the analysis, proposed scheme can resist the known attacks and provides a very good tradeoff between security and efficiency.

### B. Outline

Rest of the article is organized as follows. The notation guide is given in Table II. The system model is briefly explained in Section I-C. The attack model is given in Section I-D; the proposed scheme is solicited in Section II; while formal and informal security analysis of our proposal is discussed in Section III. Communication and computation costs based comparative analysis is performed in Section IV. Finally, Section V concludes this article.

### C. System Model

The system model is shown in Fig. 1, which involves four types of entities including 1-drones deployed in some target flying zones. A cluster of drones are deployed in some specified flying zone, here, we consider the Garibi *et al.*'s [9] proposed system model. The drones and users first get register with the server, which is an entity inside the control room and is responsible for the registration. The drones are deployed in different zones to

TABLE I  
SUMMARY OF LIMITATIONS/DRAWBACKS OF PREVIOUS USER AUTHENTICATION SCHEMES IN IOD ENVIRONMENT

Scheme	Year	Properties/Weaknesses
Turkanovic et al. [14]	2014	It is susceptible to sensing device impersonation attack, user impersonation attack, stolen smart card attack, off-line password guessing attack, privileged insider attack and formal security analysis is missing.
Farash et al. [16]	2016	It is susceptible to leakage of the secret key of the gateway, user impersonation attack, stolen smart card attack, offline password guessing attack, new smart-card issue, does not provide user anonymity and formal security analysis is missing.
Jiang et al. [12]	2016	It is susceptible to denial-of-service attack. Also, computation cost is very high and formal security analysis is missing.
Challa et al. [17]	2017	Computation cost is very high and formal security analysis is not provided.
Srinivas et al. [23]	2019	It is susceptible to impersonation attack based on stolen verifier, have traceability issue and scalability issue
Wazid et al. [25]	2019	It is susceptible to stolen-verifier attack, user and server impersonation attack, drone impersonation attack, session key leakage attack, server broadcasting and traceability issues.
Bera et al. [26]	2020	It is susceptible to user anonymity attack and computation is high.
Ever [27]	2020	Formal security analysis is missing and computation cost is very high.
Ali et al. [28]	2020	It is susceptible to masquerades, man-in-the-middle and session key exposure attacks.
Proposed Scheme		It provides protection against various known attacks, formal security analysis is provided and computation cost is very low.

TABLE II  
NOTATION GUIDE

Symbols	Representations
$\mathcal{U}_i, \mathcal{DR}_j$	User, Drone
$\mathcal{S}$	Ground Station Server
$k, P_{pub} = kP$	Private and public key of the GSS
$E_p(\alpha, \beta), P$	Elliptic curve and a point on $E_p(\alpha, \beta)$
$N_i^x, N_j^y$	$x$ and $y$ coordinates of $N_i \in E_p(\alpha, \beta)$
$ID_i, RID_i$	real and alias identity of $\mathcal{U}_i$
$ID_j, RID_{DRj}$	real and alias identity of $\mathcal{DR}_j$
$PID_i, PID_{DRj}$	Dynamic identities of $\mathcal{U}_i$ and $\mathcal{DR}_j$
$\ , H(\cdot)$	Concatenation and Hash functions

monitor/sense the field and send sensed data to the server. A registered user can also ask data from the drones sensing in a specific flying zone. Like, the rescuers may want to acquire areal data of a disaster site, the law enforcers may require surveillance information of a specific flying zone and the ambulance driver/traveler may require the data of the traffic congestion in a specific zone, etc., he connects to a drone deployed in a specific area via GSS. The GSS acts as an intermediary agent for the sharing of session keys among the user and the drones. Before sharing a session key both entities (user and drone) authenticate each other.

#### D. Adversarial Model

We have adopted the common attack model [29]–[32], with a strong adversary  $\mathcal{A}$  as mentioned in the eCK adversary model [33], which has the following capabilities.

- 1)  $\mathcal{A}$  controls the public communication link and is considered to be adept enough to interrupt, replay, alter, eliminate, or send a new fake/forged message.
- 2)  $\mathcal{A}$  can expose the engraved information using power analysis or leaked data from a mobile device/smart card [29], [32].
- 3)  $\mathcal{A}$  may be a distrustful user or an outsider.
- 4) The identities of system entities are publicly available.
- 5) Under the eCK model,  $\mathcal{A}$  can try to launch key compromise attack.

- 6) The private key of the GSS/server is assumed to be secure and no attacker is considered as powerful enough to know the GSS/server’s private key.

## II. PROPOSED SCHEME

This section presents our Elliptic curve cryptography (ECC) based scheme, designed mainly to provide a secure user access to the drone on a public channel. The phases of the proposed scheme are explained in following subsections.

### A. Setup Phase

For setting up the system, the GSS ( $\mathcal{S}$ ) selects  $E_p(\alpha, \beta)$  (elliptic curve) over finite field  $\mathcal{Z}_p^*$ , and a base point  $P$  over  $E_p(\alpha, \beta)$ , where  $n = \infty$ .  $\mathcal{S}$  then picks  $k$  (secret master key) along with a one-way hash  $h(\cdot)$  and computes  $P_{pub} = k.P$  as public key of itself.  $\mathcal{S}$  further selects probabilistic generation function  $\text{Gen}(\cdot)$ , which takes users  $\text{BIO}_i$  as input, and returns biometric key  $\sigma_i \in \{0, 1\}^l$  of length  $l$  and a public parameter  $\tau_i$ , another function  $\text{Rep}(\cdot)$  is also selected by  $\mathcal{S}$ , which takes  $\tau_i$  as an input and provides hamming distance  $d(\sigma'_i, \text{BIO}_i) \leq t$ , where  $t$  is number of tolerated errors.  $\text{Rep}(\cdot)$  function outputs the original biometric key  $\sigma_i = \text{Rep}(\text{BIO}'_i, \tau_i)$ . Finally,  $\{E_p(\alpha, \beta), P, h(\cdot), P_{pub}, \text{Gen}(\cdot), \text{Rep}(\cdot), t\}$  are announced publicly and  $k$  is kept secret by the  $\mathcal{S}$ .

### B. Predeployment Phase

In this phase,  $\mathcal{S}$  registers all the drones in offline mode before deployment in the IoD field. For predeployment purposes,  $\mathcal{S}$  picks a unique identity  $\text{ID}_{DRj} : \{j = 1, 2, \dots, n\}$  for each drone and computes corresponding pseudoidentity for drone as  $\text{RID}_{DRj} = h(\text{ID}_{DRj} || k)$ . Finally,  $\mathcal{S}$  stores  $\{\text{ID}_{DRj}, \text{RID}_{DRj}\}$  in the memory of drone and deploys every registered drone in the field and stores the parameters  $\{\text{ID}_{DRj}\}$  in its own database.

### C. User Registration Phase

This phase is invoked by  $U_i$  (an unregistered user), to get registered with  $\mathcal{S}$  for gaining postregistration real-time surveillance information from desired drone  $\mathcal{DR}_j$  in the IoD



User ( $\mathcal{U}_i$ )	GSS( $\mathcal{S}$ )	Drone ( $\mathcal{DR}_j$ )
Enter $ID_i$ , $PWD'_i$ and $BIO'_i$ $\sigma_i = \text{Rep}(BIO'_i, \tau_i)$ $A_i \stackrel{?}{=} h(ID_i    PWD'_i    \sigma'_i)$ Choose $r_1, r_2 \in \mathcal{Z}_p^*$ Compute $M_i = r_1 \cdot P$ , $N_i = r_1 \cdot P_{pub} = (N_i^x, N_i^y)$ , $R_i = R'_i \oplus h(PWD_i    \sigma_i)$ $RID_i = RID'_i \oplus h(ID_i    \sigma_i)$ , $G = h(R_i    T_u)$ $E_i = G \oplus N_i^x$ , $r'_2 = r_2 \oplus N_i^x$ $RID'_i = RID_i \oplus N_i^x$ , $ID'_{DR_j} = ID_{DR_j} \oplus N_i^y$ $M_{sg1} = \{E_i, RID'_i, ID'_{DR_j}, r'_2, M_i, T_u\}$ (1) $\xrightarrow{\text{(via open channel)}}$	Check if $ T_u - T_c  < \Delta T$ Compute $N_s = M_i \cdot k = (N_s^x, N_s^y)$ $G = E_i \oplus N_s^x$ , $r_2 = r'_2 \oplus N_s^x$ $ID_{DR_j} = ID'_{DR_j} \oplus N_s^y$ $RID_i = RID'_i \oplus N_s^x$ $G \stackrel{?}{=} h(h(RID_i    k)    T_u)$ Generate $T_s$ , Check $ID_{DR_j}$ Compute $RID_{DR_j} = h(ID_{DR_j}    k)$ $V = h(RID_i    r_2    ID_{DR_j}    T_s)$ $V' = RID_{DR_j} \oplus V$ , $W = h(RID_{DR_j}    V    T_s)$ $W' = RID_{DR_j} \oplus W$ , $PID_i = h(N_s    RID_i)$ $PID_{DR_j} = h(RID_{DR_j}    T_s    ID_{DR_j})$ $M_{sg2} = \{PID_i, PID_{DR_j}, V', W', T_s\}$ (2) $\xrightarrow{\text{(via open channel)}}$	Check if $ T_s - T_c  < \Delta T?$ $PID_{DR_j} \stackrel{?}{=} h(RID_{DR_j}    T_s    ID_{DR_j})$ $V = V' \oplus RID_{DR_j}$ $h(RID_{DR_j}    V    T_s) \stackrel{?}{=} W' \oplus RID_{DR_j}$ Generate $T_{DR}$ $SK_{DR_j} = h(V    ID_{DR_j}    h(RID_{DR_j}    V    T_s)    T_{DR})$ $Y = h(RID_{DR_j}    V    T_s) \oplus V$ $Z = h(SK_{DR_j}    ID_{DR_j}    T_{DR})$ $M_{sg3} = \{PID_i, Y, Z, T_s, T_{DR}\}$ (3) $\xleftarrow{\text{(via open channel)}}$
Check if $ T_{DR} - T_c  < \Delta T?$ $PID_i \stackrel{?}{=} h(N_i    RID_i)$ Compute $L = h(RID_i    r_2    ID_{DR_j}    T_u)$ $h(RID_{DR_j}    V    T_s) = L \oplus Y$ $SK_{U_i} = h(L    ID_{DR_j}    h(RID_{DR_j}    V    T_s)    T_{DR})$ $Z \stackrel{?}{=} h(SK_{U_i}    ID_{DR_j}    T_{DR})$		

Fig. 2. Proposed login/authentication phase.

environment. For registration,  $\mathcal{U}_i$  selects  $ID_i$ , generates  $r_0$  randomly, computes pseudoidentity  $RID_i = h(ID_i || r_0)$  for  $\mathcal{U}_i$ , and sends  $RID_i$  to  $\mathcal{S}$  through private/secure channel. After receiving the message, GSS  $\mathcal{S}$  computes  $R_i = h(RID_i || k)$  and sends the reply containing  $R_i$  to  $\mathcal{U}_i$  through secure channel. After receiving the registration reply from GSS,  $\mathcal{U}_i$  chooses  $PWD_i$  and inputs his  $BIO_i$  into mobile device  $MD_i$  which compute  $\text{Gen}(BIO_i) = (\sigma_i, \tau_i)$ ,  $A_i = h(ID_i || PWD_i || \sigma_i)$ ,  $R'_i = R_i \oplus h(PWD_i || \sigma_i)$ ,  $RID'_i = RID_i \oplus h(ID_i || \sigma_i)$ . In the final step,  $\mathcal{U}_i$  saves  $\{A_i, R'_i, \tau_i, \text{Gen}(\cdot), \text{Rep}(\cdot), h(\cdot)\}$  into  $MD_i$  memory.

#### D. Login and Authentication

A registered user  $\mathcal{U}_i$  invokes this procedure to get authenticated and share a secret/shared key with a deployed drone  $\mathcal{DR}_j$  through  $\mathcal{S}$ , when he wants to acquire real-time surveillance data or otherwise. For successful accomplishment of this phase, the steps as illustrated in Fig. 2 and explained below are executed between  $\mathcal{U}_i$ ,  $\mathcal{S}$ , and  $\mathcal{DR}_j$ .

PL 1:  $\mathcal{U}_i$  enters  $ID_i$ ,  $PWD'_i$  and  $BIO'_i$  into mobile device and computes  $\sigma_i = \text{Rep}(BIO'_i, \tau_i)$ ,  $A'_i = h(ID_i || PWD'_i || \sigma'_i)$ , checks  $A_i \stackrel{?}{=} A'_i$  and upon success, chooses random numbers  $r_1, r_2 \in \mathcal{Z}_p^*$ .  $\mathcal{U}_i$  further computes  $M_i = r_1 \cdot P$  and  $N_i = r_1 \cdot P_{pub} = (N_i^x, N_i^y)$ . Then,  $\mathcal{U}_i$  computes  $R_i = R'_i \oplus h(PWD_i || \sigma_i)$ ,  $RID_i = RID'_i \oplus h(ID_i || \sigma_i)$ ,  $G = h(R_i || T_u)$ ,  $E_i = G \oplus N_i^x$ ,  $r'_2 = r_2 \oplus N_i^x$ ,  $RID'_i = RID_i \oplus N_i^x$  and  $ID'_{DR_j} = ID_{DR_j} \oplus N_i^y$ .  $\mathcal{U}_i$  now sends login request message  $M_{sg1} = \{E_i, RID'_i, ID'_{DR_j}, r'_2, M_i, T_u\}$  to GSS through public channel.

PL 2: On receiving,  $\mathcal{S}$  verifies the time freshness  $|T_u - T_c| < \Delta T$ , on success,  $\mathcal{A}$  computes  $N_s = M_i \cdot k = (N_s^x, N_s^y)$ ,  $G = E_i \oplus N_s^x$ ,  $r_2 = r'_2 \oplus N_s^x$ ,  $ID_{DR_j} = ID'_{DR_j} \oplus N_i^y$ ,  $RID_i = RID'_i \oplus N_s^x$  and verifies  $G \stackrel{?}{=} h(h(RID_i || k) || T_u)$ , on success user is considered as authenticated else session is aborted immediately.  $\mathcal{S}$  picks  $T_s$  and verifies that  $ID_{DR_j}$  exist in the GSS database and on existence of  $ID_{DR_j}$ , the  $\mathcal{S}$  computes  $RID_{DR_j} = h(ID_{DR_j} || k)$ ,  $V = h(RID_i || r_2 || ID_{DR_j} || T_u)$ ,  $V' = RID_{DR_j} \oplus V$ ,  $W = h(RID_{DR_j} || V || T_s)$ ,  $W' = RID_{DR_j} \oplus W$ ,  $PID_i = h(N_s || RID_i)$ ,  $PID_{DR_j} = h(RID_{DR_j} || T_s || ID_{DR_j})$ .  $\mathcal{S}$  sends  $M_{sg2} = \{PID_i, PID_{DR_j}, W, V', T_s\}$  to Drone  $\mathcal{DR}_j$  through open channel.

PL 3:  $\mathcal{DR}_j$  on reception, first checks time-freshness  $(|T_2 - T_2^*| \leq \Delta T)$  and on success,  $\mathcal{DR}_j$  checks if  $PID_{DR_j} \stackrel{?}{=} h(RID_{DR_j} || T_s || ID_{DR_j})$ , and on success computes  $V = RID_{DR_j} \oplus V'$ .  $\mathcal{DR}_j$  further checks if  $W' \oplus RID_{DR_j} \stackrel{?}{=} h(RID_{DR_j} || V || T_s)$ , on success picks  $T_{DR}$  and computes session key  $SK_{DR_j} = h(V || ID_{DR_j} || h(RID_{DR_j} || V || T_s) || T_{DR})$ ,  $Y = V \oplus h(RID_{DR_j} || V || T_s)$ ,  $Z = h(SK_{DR_j} || ID_{DR_j} || T_{DR})$  and sends  $M_{sg3} = \{PID_i, Y, Z, T_s, T_{DR}\}$  to  $\mathcal{U}_i$  directly.

PL 4:  $\mathcal{U}_i$  after receiving the authentication reply, first checks time-freshness  $|T_{DR} - T_c| < \Delta T?$ , upon success checks  $PID_i \stackrel{?}{=} h(N_i || RID_i)$ ; and on success,  $\mathcal{U}_i$  computes  $L = h(RID_i || r_2 || ID_{DR_j} || T_u)$ ,  $h(RID_{DR_j} || V || T_s) = L \oplus Y$ ,  $SK_{U_i} = h(L || ID_{DR_j} ||$

$h(\text{RID}_{DR_j}||V||T_s)||T_{DR})$  and finally check  $Z \stackrel{?}{=} h(\text{SK}_{U_i}||\text{ID}_{DR_j}||T_{DR})$  if so then User  $\mathcal{U}_i$  and Drone  $DR_j$  saves the session key  $\text{SK}_{U_i} = \text{SK}_{DR_j}$  for future secure communication.

### E. Biometric and Password Update Phase

This phase executes without intervention of GSS and the user can change his password and biometrics locally on his mobile device  $\text{MD}_i$ . For execution of this step,  $\mathcal{U}_i$  enters  $\text{ID}_i$ ,  $\text{PWD}_i^{\text{old}}$  and  $\text{BIO}_i^{\text{old}}$ . Mobile device  $\text{MD}_i$  computes  $\sigma_i^{\text{old}} = \text{Rep}(\text{BIO}_i^{\text{old}}||\tau_i^{\text{old}})$  and checks whether  $A_i^{\text{old}} \stackrel{?}{=} h(\text{ID}_i||\text{PWD}_i^{\text{old}}||\sigma_i^{\text{old}})$ . On success,  $\text{MD}_i$  prompts to enter new biometric  $\text{BIO}_i^{\text{new}}$  and password  $\text{PWD}_i^{\text{new}}$ .  $\mathcal{U}_i$  enters new credentials  $\text{PWD}_i^{\text{new}}$  and  $\text{BIO}_i^{\text{new}}$ ,  $\text{MD}_i$  computes  $\text{Gen}(\text{BIO}_i^{\text{new}}) = (\sigma_i^{\text{new}}, \tau_i^{\text{new}})$ ,  $A_i^{\text{new}} = h(\text{ID}_i||\text{PWD}_i^{\text{new}}||\sigma_i^{\text{new}})$  and  $R_i^{\text{new}} = R_i^{\text{old}} \oplus h(\text{PWD}_i^{\text{old}}||\sigma_i^{\text{old}}) \oplus h(\text{PWD}_i^{\text{new}}||\sigma_i^{\text{new}})$ . Mobile device finally replaces  $\{A_i^{\text{old}}, R_i^{\text{old}}, \tau_i^{\text{old}}\}$  with  $\{A_i^{\text{new}}, R_i^{\text{new}}, \tau_i^{\text{new}}\}$  in its memory.

### F. Drone Addition Phase

Adding drone dynamically in an existing network is very similar to drone predeployment phase, where  $\mathcal{S}$  picks a unique identity  $\text{ID}_{DR_j}^{\text{new}}$  for the new drone.  $\mathcal{S}$  computes corresponding pseudoidentity  $\text{RID}_{DR_j}^{\text{new}} = h(\text{ID}_{DR_j}^{\text{new}}||k)$ , where  $k$  is the secret key of GSS.  $\mathcal{S}$  stores  $\{\text{ID}_{DR_j}^{\text{new}}, \text{RID}_{DR_j}^{\text{new}}\}$  in the memory of drone and deploys it in the field,  $\mathcal{S}$  then stores  $\{\text{ID}_{DR_j}^{\text{new}}\}$  in its own database.

## III. SECURITY ANALYSIS

The formal provable security analysis is solicited here. For the purpose of security analysis, we consider the widely accepted adversarial model briefed in Section I-D. Following sections provide evidences of the robustness of the proposed scheme, while combating several attacks.

### A. Security Model

In this article, we followed the security model utilized in [34] and [35] to prove the robustness of proposed scheme new authentication and key agreement scheme (NAKAS) formally under RoM model [36]. Under the ROM model, an adversary  $\mathcal{A}$  connects with  $E^t$ , the  $t$ th instance of an executing entities (e.g., in NAKAS it can be a legitimate user  $\mathcal{U}_i$ , the GSS or a drone  $DR_j$ ). The attacker  $\mathcal{A}$  can send various queries and the challenger  $\mathcal{C}$  responds accordingly, as mentioned in Table III.

The  $\mathcal{A}$  can guess the value of flipped coin  $c'$  during query Test.  $\mathcal{A}$  breaks the security of NAKAS scheme  $\pi$ , if  $c' = c$ . Now, let the event  $E_{ac}$  is the event about correct guessing of coin  $c$ . The advantage of  $\mathcal{A}$  can be denoted as  $\text{Adv}_{\text{NAKAS}}^{\text{AKA}}(\mathcal{A}) = |2\text{Pr}[E_{ac}] - 1|$ . Following are some definitions.

**Definition 1:** ( $\text{AKA}_{D_j}^{U_i}$  - Secure): The proposed NAKAS protocol  $\pi$  is  $\text{AKA}_{D_j}^{U_i}$  - Secure if  $\text{Adv}_{\text{NAKAS}}^{\text{AKA}}(\mathcal{A})$  is negligible.

The proposed NAKAS protocol provides mutual authentication (MA-Secure) between a user and drone through mediation

TABLE III  
QUERIES AND THEIR ANSWERS

<i>Sys</i> - Setup: On execution of this query, $\mathcal{C}$ returns system parameters to $\mathcal{A}$
<i>h</i> ( $m_x$ ): On execution of this query, $\mathcal{C}$ selects random $r_x \in \mathbb{Z}_p^*$ , add $\{m_x, r_x\}$ in $L_h$ list and reply $r_x$ to $\mathcal{A}$ .
<i>Send</i> ( $E^t, msg$ ): Through this query, $\mathcal{A}$ dispatches $msg$ and $\mathcal{C}$ replies as per the specification of the proposed NAKAS protocol.
<i>CorruptU</i> : On execution of this query with $\text{ID}_i$ , $\mathcal{C}$ replies with $U_i$ 's private key to $\mathcal{A}$ .
<i>CorruptD</i> : On execution of this query with $\text{ID}_{DR_j}$ , $\mathcal{C}$ replies with $DR_j$ 's private parameter $\text{RID}_{DR_j}$ to $\mathcal{A}$ .
<i>Reveal</i> ( $E^t$ ): Execution of this query allows to reveal current session key $SK$ between $E^t$ and $\mathcal{A}$ .
<i>Test</i> ( $E^t$ ): $\mathcal{U}_A$ requests $E_i$ for the key $SK$ and $E_i$ replies probabilistically an outcome of a flipped unbiased coin $c$

of GSS provided if  $\mathcal{A}$  cannot generate any of the: ① legitimate request message  $M_{sg1}$  by user, ② mediated message  $M_{sg2}$  by GSS, and ③ response message  $M_{sg3}$  by drone. Let  $E_{US}$ ,  $E_{SD}$ , and  $E_{DU}$  represent events that  $\mathcal{A}$  can generate message ①, ②, and ③, respectively.  $\mathcal{A}$ 's advantage to break MA of NAKAS can be defined as  $\text{Adv}_{\text{NAKAS}}^{\text{MA}}(\mathcal{A}) = \text{Pr}[E_{US}] + \text{Pr}[E_{SD}] + \text{Pr}[E_{DU}]$ .

**Definition 2:** ( $\text{MA}_{D_j}^{U_i}$  - Secure): The proposed NAKAS protocol  $\pi$  is  $\text{MA}_{D_j}^{U_i}$  - Secure if  $\text{Adv}_{\text{NAKAS}}^{\text{MA}}(\mathcal{A})$  is negligible.

### B. Provable Security

This section proves the security of proposed NAKAS protocol under the security model described in above-mentioned section.

**Theorem 1:** The proposed NAKAS protocol achieves mutual authentication.

**Proof:** The attacker  $\mathcal{A}$  can consider to run the query  $\text{Send}(U_i, M_{sg1})$  and if the challenger  $\mathcal{C}$  gets verify  $G \stackrel{?}{=} h(h(\text{RID}_i||k)||T_u)$ , then  $M_{sg1}$  is legitimate, where  $M_{sg1} = \langle E_i, \text{RID}'_i, \text{ID}'_{DR_j}, r'_2, M_i, T_u \rangle$ .  $\mathcal{C}$  using private key  $k$  can verify validity and freshness of  $M_{sg1}$ .  $\mathcal{C}$  can acquire a record from the maintained list  $L_h$  with the probability  $1/q_h$ . So,  $\mathcal{A}$  can forge  $M_{sg1}$  and the probability of this event is  $\text{Pr}[E_{US}] = 1/q_h$ . Likewise, The attacker  $\mathcal{A}$  can consider to run the query  $\text{Send}(S, M_{sg2})$  and if the challenger  $\mathcal{C}$  gets verify ①  $\text{PID}_{DR_j} \stackrel{?}{=} h(\text{RID}_{DR_j}||T_s||\text{ID}_{DR_j})$ , ②  $h(\text{RID}_{DR_j}||V||T_s) \stackrel{?}{=} W' \oplus \text{RID}_{DR_j}$ , and ③  $\text{PID}_i \stackrel{?}{=} h(N_i||\text{RID}_i)$ , then  $M_{sg2}$  is legitimate, where  $M_{sg2} = \langle \text{PID}_i, \text{PID}_{DR_j}, V', W', T_s \rangle$ .  $\mathcal{C}$  can acquire a record from the maintained list  $L_h$  with the probability  $1/q_h$ . If two legal messages  $\langle \text{PID}_i, \text{PID}_{DR_j}, V', W', T_s \rangle$  and  $\langle \overline{\text{PID}}_i, \text{PID}_{DR_j}, V', W', T_s \rangle$  are generated then  $\mathcal{C}$  can compute  $(r_1 - \overline{r_1}) \cdot P_{\text{pub}}$ . Therefore, the probability of this event is  $\text{Pr}[E_{SD}] = 1/p \cdot q_h^2$ . So,  $\mathcal{A}$  can forge  $M_{sg2}$  and the probability is  $1/p \cdot q_h^2$ . As last resort,  $\mathcal{A}$  can consider to run the query  $\text{Send}(D, M_{sg3})$  and if the challenger  $\mathcal{C}$  gets verify ①  $\text{PID}_i \stackrel{?}{=} h(N_i||\text{RID}_i)$ , and ②  $Z \stackrel{?}{=} h(\text{SK}_{U_i}||\text{ID}_{DR_j}||T_{DR})$ , then  $M_{sg3}$  is legitimate, where  $M_{sg3} = \langle \text{PID}_i, Y, Z, T_s, T_{DR} \rangle$ . If two legal messages  $\langle \text{PID}_i, Y, Z, T_s, T_{DR} \rangle$  and  $\langle \overline{\text{PID}}_i, Y, \overline{Z}, T_s, T_{DR} \rangle$  are generated then  $\mathcal{C}$  can compute  $(r_1 - \overline{r_1}) \cdot P_{\text{pub}}$  with probability  $1/p$ ; moreover  $\mathcal{C}$  can acquire a record from the maintained list  $L_h$  with the probability  $1/q_h$ . Therefore, the probability of this

event is  $Pr[E_{DU}] = 1/q_h$ . So,  $\mathcal{A}$  can forge  $M_{sg3}$  and the probability is  $1/p.q_h$ . Therefore, we can deduce that  $\text{Adv}_{\text{NAKAS}}^{\text{AKA}}(\mathcal{A})$  is negligible.

*Theorem 2:* The proposed NAKAS protocol is semantically secure if DLP over ECC is hard.

*Proof:* On querying Test,  $\mathcal{C}$  can get non-negligible advantage  $\epsilon$  to get the right session key (sk), this event is denoted by  $E_{\text{sk}}$ . The probability for  $\mathcal{A}$  to guess  $c$  in Test session is  $\geq 1/2$ , so it leads to  $Pr[E_{\text{sk}} \geq \epsilon/2]$ . Now, let  $E_{\text{Test}}^U$  and  $E_{\text{Test}}^{Dr}$  represent the events that  $U_i$  and  $DR_j$  are queried through Test. We have the following:

$$\begin{aligned} \epsilon/2 &\leq Pr[E_{\text{sk}}] \\ &= Pr[E_{\text{sk}} \wedge E_{\text{Test}}^U] + Pr[E_{\text{sk}} \wedge E_{\text{Test}}^D \wedge E_{US}] + \\ &Pr[E_{\text{sk}} \wedge E_{\text{Test}}^D \wedge \neg E_{US}] \\ &Pr[E_{\text{sk}} \wedge E_{\text{Test}}^U] + Pr[E_{\text{sk}} \wedge E_{\text{Test}}^D \wedge \neg E_{US}] \leq \\ &\epsilon/2 - Pr[E_{US}]. \end{aligned} \quad (1)$$

Since  $Pr[E_{\text{Test}}^D \wedge \neg E_{US}] = E_{\text{Test}}^U$ , therefore

$$Pr[\text{sk} = h(L||\text{ID}_{DR_j}||h(\text{RID}_{DR_j}||V||T_s)||T_{DR})] \geq \epsilon/4 - Pr[E_{US}]/2. \quad (3)$$

1) *User Impersonation Attack:* Let  $\mathcal{A}$  tries to impersonate as  $U_i$  toward  $\mathcal{S}$ .  $\mathcal{A}$  has to generate a valid request message  $M_{sg1}^A = \{E_i^A, \text{RID}_i^A, \text{ID} * r_{DR_j}^A, r_2^A, M_i^A, T_u^A\}$  on behalf of  $U_i$ .  $\mathcal{A}$  needs to compute all mentioned parameters in  $M_{sg1}^A$ .  $\mathcal{A}$  can generate its own timestamp  $T_u^A$ , selects its own random number  $r_1^A$  and computes  $M_i^A = r_1^A.P$ ,  $N_i^A = r_1^A.P_{\text{pub}}$ . However, as per Theorem 1, without having the secret parameters  $\{R_i, \text{ID}_i, \text{PWD}_i, r_1, r_2, \sigma_i\}$ ,  $\mathcal{A}$  cannot successfully construct the login message  $M_{sg1}$ , which can pass  $G \stackrel{?}{=} h(h(\text{RID}_i||k)||T_u)$  from the challenger with non-negligible advantage. So, as a result  $\mathcal{U}_A$  cannot impersonate as a legal user  $U_i$ .

2) *GSS Impersonation Attack:*  $\mathcal{A}$  may try to impersonate as a GSS  $\mathcal{S}$  toward the drone  $DR_j$ . To do this  $\mathcal{A}$  constructs a message  $M_{sg2}^A = \{\text{PID}_i^A, \text{PID}_{DR_j}^A, V^A, W^A, T_s^A\}$  by generating its own current timestamp  $T_s^A$ . However, as per theorem 1,  $\mathcal{A}$  cannot successfully construct the login message  $M_{sg2}$  which can pass ①  $\text{PID}_{DR_j} \stackrel{?}{=} h(\text{RID}_{DR_j}||T_s||\text{ID}_{DR_j})$ , ②  $h(\text{RID}_{DR_j}||V||T_s) \stackrel{?}{=} W' \oplus \text{RID}_{DR_j}$ , and ③  $\text{PID}_i \stackrel{?}{=} h(N_i||\text{RID}_i)$  tests from the challenger  $\mathcal{C}$ , with non-negligible advantage. Therefore,  $\mathcal{A}$  cannot impersonate as a GSS.

3) *Drone Impersonation Attack:*  $\mathcal{A}$  may try to impersonate as  $DR_j$  and tries to constructs a message  $M_{sg3}^A = \{\text{PID}_i^A, Y^A, Z^A, T_{DR}^A, T_s^A\}$  by generating its own current timestamp  $T_{DR}^A$  and sending this message to  $U_i$ .  $\mathcal{A}$  has to construct  $M_{sg3}$ , which can pass ①  $\text{PID}_i \stackrel{?}{=} h(N_i||\text{RID}_i)$ , and ②  $Z \stackrel{?}{=} h(\text{SK}_{U_i}||\text{ID}_{DR_j}||T_{DR})$  tests from  $\mathcal{C}$ . However, as per Theorem 1,  $\mathcal{A}$  cannot pass ① and ② from  $\mathcal{C}$  with non-negligible advantage. Therefore,  $\mathcal{A}$  cannot impersonate as a remote drone toward  $U_i$ .

4) *Anonymity and Untraceability:*  $\mathcal{A}$  cannot trace the user, because for each session new random numbers and current

timestamps are generated, which leads to distinct messages  $M_{sg1}, M_{sg2}, M_{sg3}$  for each session. Moreover, the pseudo or real identities of user and drone are never shared openly. And pseudorandom-identities are used by both user and drone ( $\text{PID}_i, \text{PID}_j$ ) to communicate with each other and are discarded after each session. So the scheme provides both the anonymity and untraceability properties.

5) *DoS Attack:* In the proposed scheme user is logged-in locally by checking the condition  $A_i = A'_i$  (step Plog 1 in Section II-D) or  $A_i^{\text{old}} \stackrel{?}{=} A_i$  (in Section II-E) in the updation of user credentials including: password and biometrics. The login request of  $U_i$  is sent  $\mathcal{S}$  only after successful verification, additionally both the biometric and password update completes in offline manner. As per Theorems 1–3, no adversary can generate any of the  $M_{sg1}, M_{sg2}$ , and  $M_{sg3}$  with non-negligible advantage. Hence, the proposed scheme protects from DoS attack.

6) *Offline Password Guessing Attack:* Let  $U_i$  be a registered user of the system and his smart device was stolen by a deceitful insider or outsider  $\mathcal{U}_A$ . The adversary  $\mathcal{U}_A$  can extract the sensitive information  $\{A_i, R'_i, \text{RID}'_i, \tau_i, \text{Gen}(\cdot), \text{Rep}(\cdot), h(\cdot), t\}$  out of the mobile device through power analysis [32]. However,  $\mathcal{U}_A$  cannot drive the secret credentials  $A_i = h(\text{ID}_i||\text{PWD}_i||\sigma_i)$  due to the biometric key. Furthermore, due to hash function's one-way property  $\mathcal{U}_A$  cannot extract password and identity simultaneously.

7) *Password Change Attack:* An attacker  $\mathcal{U}_A$  using the stolen mobile device may try to change password of the original user  $U_i$  and for this  $\mathcal{U}_A$  can extract the sensitive information  $\{A_i, R'_i, \tau_i, \text{Gen}(\cdot), \text{Rep}(\cdot), h(\cdot), t\}$  from the mobile-device through power analysis [32]. However,  $\mathcal{U}_A$  cannot change the password because  $U_i$  needs to authenticate himself from the mobile device, and for that  $\mathcal{U}_A$  requires  $\text{ID}_i, \text{PWD}_i$ , and  $\text{BIO}_i$  of user  $U_i$ . Therefore, without the knowledge of valid credentials  $\mathcal{U}_A$  cannot authenticate him/her self. Hence, the proposed scheme is secure against password change attack.

8) *Stolen Mobile Device Attack:* As described in Section III-B6 that if  $\mathcal{U}_A$  steals the mobile device, yet he cannot extract any sensitive information. Hence, the proposed scheme is secure against stolen mobile device attack.

#### IV. SECURITY AND PERFORMANCE ANALYSIS

In this section, we perform the security and performance comparisons of the proposed and related schemes [14], [17], [23], [25]–[27].

##### A. Security Requirements

Table IV provides an overview of the security features inherent in the proposed scheme and related schemes presented in [14], [17], [23], and [25]–[27]. Referring Table IV, all related compared schemes [14], [17], [23], [25]–[27] are prone to various attacks like the scheme proposed by Turkanović *et al.* [14] and Wazid *et al.*'s [25] are prone to privileged-insider attack, Challa *et al.*'s [17] scheme lacks key-management phase and Srinivas *et al.*'s [23] scheme is prone to user impersonation attack, the scheme of Bera *et al.* [26] does not provide anonymity



TABLE IV  
COMPARISON OF FUNCTIONALITY FEATURES

↓Features	[14]	[17]	[23]	[25]	[26]	[27]	Our
$SReq_1$	✓	✓	×	✓	×	✓	✓
$SReq_2$	×	✓	✓	×	✓	✓	✓
$SReq_3$	×	✓	✓	✓	✓	✓	✓
$SReq_4$	×	✓	✓	✓	✓	✓	✓
$SReq_5$	✓	✓	✓	×	✓	✓	✓
$SReq_6$	×	✓	✓	×	✓	✓	✓
$SReq_7$	✓	✓	✓	✓	✓	✓	✓
$SReq_8$	✓	✓	✓	✓	✓	✓	✓
$SReq_9$	✓	✓	✓	×	✓	✓	✓
$SReq_{10}$	✓	✓	✓	×	✓	✓	✓
$SReq_{11}$	×	✓	×	×	✓	✓	✓
$SReq_{12}$	✓	✓	✓	✓	✓	✓	✓
$SReq_{13}$	✓	✓	✓	✓	—	—	✓
$SReq_{14}$	×	✓	✓	✓	✓	✓	✓
$SReq_{15}$	×	✓	✓	✓	—	—	✓
$SReq_{16}$	×	×	✓	✓	✓	✓	✓
$SReq_{17}$	×	✓	✓	✓	✓	×	✓
$SReq_{18}$	✓	×	✓	×	✓	✓	✓
$SReq_{19}$	✓	✓	×	×	✓	✓	✓

Note:  $SReq_1$ : User anonymity;  $SReq_2$ : Privileged-insider attack;  $SReq_3$ : Password guessing attack;  $SReq_4$ : Stolen mobile device or smart card attack;  $SReq_5$ : Denial of service attack;  $SReq_6$ : User Impersonation attack;  $SReq_7$ : Replay attack;  $SReq_8$ : Man-in-the-middle attack;  $SReq_9$ : Mutual authentication;  $SReq_{10}$ : Session key agreement;  $SReq_{11}$ : Untraceability;  $SReq_{12}$ : Drone capture attack;  $SReq_{13}$ : Password update phase;  $SReq_{14}$ : Drone/sensing device capture attack;  $SReq_{15}$ : Biometric update phase;  $SReq_{16}$ : Key management phase;  $SReq_{17}$ : Formal security verification;  $SReq_{18}$ : GSS impersonation attack;  $SReq_{19}$ : Session key Security. ✓: Security feature Provision, ×: Nonprovision of security feature, —: N/A.

TABLE V  
COMMUNICATION COST ANALYSIS

Exchange ↓	[14]	[17]	[23]	[25]	[26]	[27]	Our
Bits	2720	2528	1536	1696	1696	1920	2208
Messages	4	3	3	3	3	6	3

due to transmission of same certificate in each authentication message and the scheme of Ever [27] is proposed without any formal security validation; whereas, the scheme of Wazid *et al.* [25] is vulnerable to traceability as well as stolen verifier based impersonation attacks. Moreover, in Wazid *et al.*'s scheme, the broadcasting of messages by GSS to drones may create battery drain issues in drones. A list of complete security requirements are listed in Table IV against schemes, which are already developed [14], [17], [23], [25]–[27].

### B. Communication Cost Analysis

The comparison of the proposed and schemes proposed in [14], [17], [23], and [25]–[26] with respect to the bits exchanged is solicited in Table V. For comparison purposes and to keep simplicity, user identities are considered as 128 b, identity of each drone is considered as 16 b, the random numbers and timestamps are taken as 128 and 32 bits long, the employed hash  $SHA - 1$  is having 160 b digest; whereas, the size of ECC point is fixed at 320 b to keep comparable security level with RSA 1024 b. The communication cost of the proposed scheme is slightly higher than the schemes of Srinivas *et al.*, Wazid *et al.*, Bera *et al.*, and Ever *et al.*; whereas, the proposed scheme has less communication overhead as compared with the schemes of

TABLE VI  
EXPERIMENTAL RESULTS

↓Operation/ Device→	Mobile	GSS	Drone
$T_b$ : Bilinear-Pairing	17.36	4.038	12.52
$T_e$ : ECC Point Multiplication	5.116	0.926	4.107
$T_a$ : ECC Point Addition	0.013	0,006	0.018
$T_h$ : One way Hash	0.009	0.004	0.006
$T_r$ : Random number Generation	2.011	0.118	1.185

TABLE VII  
COMPARISON OF COMPUTATION COSTS

	User	GSS	Drone	RT(ms)
[14]	$7T_h + T_r$	$5T_h + T_r$	$7T_h$	2.254
[17]	$5T_h + T_f + 5T_e + T_r$	$4T_h + 5T_e + T_r$	$3T_h + 4T_e + T_r$	55.147
[23]	$14T_h + T_f + T_r$	$9T_h + T_r$	$7T_h + T_r$	8.634
[25]	$16T_h + T_f + T_r$	$8T_h + T_r$	$7T_h + T_r$	8.648
[26]	$4T_e + 2T_a + 4T_h + T_r$	—	$4T_e + 2T_a + 4T_h + T_r$	40.21
[27]	$2T_b + 5T_h + T_r$	$2T_b + 3T_h$	$2T_b + 9T_h + T_e$	86.386
Our	$2T_e + 8T_h + T_f + 2T_r$	$T_e + 7T_h$	$6T_h$	20.432

RT(ms): Approximate Running time in milliseconds.

challa *et al.* and Turkanović *et al.* However, the proposed scheme is more secure than the all rest of the schemes as proved earlier.

### C. Computation Cost Analysis

This section briefs the comparative computation cost analysis of our scheme and related schemes [14], [17], [23], [25]–[27]. For measuring the computation time and cost, we set up a real-time environment, where we conduct an experiment using MIRACL Library, over Smartphone: Xiaomi Redmi Note 8, with 4 GB RAM and Octa-core Max 2.01 GHz processor, the underlying android version is 9 and MIUI version is 11.0.7, the smartphone represents a user/mobile device. For GSS, we used HP EliteBook 8460P with Intel Core i7-2620 M 2.7 GHz Processor and 4 GB RAM over Ubuntu 16.0 LTS operating system. Likewise, we used Pi3 B+ with Cortex-A53(ARMv8) 64-bit SoC @ 1.4 GHz processor, 1 GB LPDDR2 SDRAM RAM to replicate a drone. The simulation results on each device are given in Table VI; moreover, using the analogy of [25], we consider  $T_f \approx T_e$ , where  $T_f$  is the running time of executing a fuzzy extractor. The running time of the proposed and related schemes [14], [17], [23], [25]–[27] are illustrated in Table VII. The proposed scheme completes one cycle of authentication with cost  $3T_e + 21T_h + 2T_r + 1T_f$  and in approximately 20.432 ms. The proposed scheme achieves much better performance as compared with the schemes of Challa *et al.*[17], Bera *et al.*[26], and Ever [27], whereas it incurs more computation cost when compared with other related schemes [14], [23], [25] but the proposed scheme is more secure than the rest of the schemes.

## V. CONCLUSION

Drones are having large application area, and can be deployed even on remote sites with difficult or no human access. However,

due to underlying public insecure channel drones are subject to various insecurities including the modification, replay, and impersonation attacks along with privacy concerns. To realize the advantages, securing the drone environment is of vital importance. In recent past, several methods were proposed; however, many such methods were proved either insecure or inapplicable in drone environments. In this article, we proposed an ECC and symmetric key primitives based authentication method to secure communication between drone and user using three-factor including user's mobile device, password, and biometrics. We proved the security of the proposed scheme formally through ROM as well as informally. The comparative analysis depicts that the proposed scheme performs better in security and has a better tradeoff between security and efficiency for the drones. Hence, the proposed scheme is best suitable for gaining surveillance or otherwise data securely through drones network in smart cities.

## REFERENCES

- [1] J. Dizdarevic, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Comput. Surv.*, vol. 51, no. 6, 2019, Art. no. 116.
- [2] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating systems for low-end devices in the Internet of things: A survey," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 720–734, Oct. 2016.
- [3] Y. Xu, V. Mahendran, W. Guo, and S. Radhakrishnan, "Fairness in fog networks: Achieving fair throughput performance in MQTT-based iots," in *Proc. 14th IEEE Annu. Consumer Commun. Netw. Conf.*, 2017, pp. 191–196.
- [4] A. I. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A surv. on enabling technologies, protocols, and applications," *IEEE Commun. Surv. Tut.*, vol. 17, no. 4, pp. 2347–2376, Oct.–Dec. 2015.
- [5] C. Perera, A. B. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 1, pp. 414–454, Jan.–Mar. 2014.
- [6] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, 2019.
- [7] 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.
- [8] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of Drones (IoD): Threats, vulnerability, and security perspectives," 2018, *arXiv:1808.00203*.
- [9] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.
- [10] C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 933–945, Dec. 2009.
- [11] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.
- [12] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, 2016.
- [13] D. Kumar, H. K. Singh, and C. Ahlawat, "A secure three-factor authentication scheme for wireless sensor networks using ECC," *J. Discrete Math. Sci. Cryptography*, vol. 23, no. 4, pp. 879–900, 2019.
- [14] M. Turkanović, 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.
- [15] S. Banerjee, C. Chunka, S. Sen, and R. S. Goswami, "An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards," *Wireless Pers. Commun.*, vol. 107, no. 1, pp. 243–270, 2019.
- [16] M. S. Farash, M. Turkanović, 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.
- [17] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.
- [18] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, 2020.
- [19] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 53, pp. 527–537, 2020.
- [20] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based Industrial Internet of things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec 2018.
- [21] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, Dec. 2019.
- [22] J. Won, S. Seo, and E. Bertino, "Certificateless cryptographic protocols for efficient drone-based smart city applications," *IEEE Access*, vol. 5, pp. 3721–3749, 2017.
- [23] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
- [24] 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.
- [25] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
- [26] 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.
- [27] Y. Kirsal Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, 2020.
- [28] Z. Ali *et al.*, "Itssaka-ms: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments," *IEEE Access*, vol. 8, pp. 107993–108003, 2020.
- [29] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Oct. 1983.
- [30] S. A. Chaudhry, "Correcting talk: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Elect. Power Energy Syst.*, vol. 125, 2021, Art. no. 106529.
- [31] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.
- [32] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
- [33] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proc. Int. Conf. Provable Secur.*, 2007, pp. 1–16.
- [34] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.
- [35] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, 2019.
- [36] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptography*, 2005, pp. 65–84.