Hindawi
Security and Communication Networks
Volume 2021, Article ID 3437373, 12 pages
https://doi.org/10.1155/2021/3437373

Research Article

A Resource-Friendly Authentication Protocol for UAV-Based Massive Crowd Management Systems

Bander A. Alzahrani,[1] **Ahmed Barnawi**,[1] **and Shehzad Ashraf Chaudhry**[2]

[1]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[2]*Department of Computer Engineering Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

Correspondence should be addressed to Shehzad Ashraf Chaudhry; sashraf@gelisim.edu.tr

Received 21 July 2021; Revised 18 September 2021; Accepted 25 September 2021; Published 5 November 2021

Academic Editor: Helena Rifà-Pous

As a part of the smart city revolution, crowd management is an emerging trend and it can enhance the quality of life. Unmanned ariel vehicles (UAVs) can help in making the crowd management process more efficient and more accurate. UAVs can monitor and collect environmental-related surveillance data and share real-time information with each other and with the decision makers. However, the battery-operated UAVs communicate over the open public channel making the privacy and security of the UAVs a crucial element in mission-critical applications. The weaknesses of the existing scheme pave the way to design a new lightweight authentication scheme for UAV environments. In this article, we present a symmetric key primitive-based scheme and provide authentication among a user and a UAV through an intermediate control center. Due to usage of symmetric key and elliptic curve cryptography, the proposed scheme fulfils the performance requirements of the UAVs. The security of the proposed scheme is substantiated through BAN logic, along with a discussion on security features extended by the proposed scheme. The performance and security comparisons show that the proposed scheme provides adequate security and efficiency and can be practically deployed in real UAV environments.

1. Introduction

With the advancements in software and hardware infrastructure for information and communication technologies, the UAV communication has become a reality, which is making daily life more easy and automated. The UAVs, also called drones, can be deployed in a variety of applications including smart cargo and surveillance. The UAVs can enhance quality of life and can be deployed at remote and inaccessible locations like depths and mountain peaks. In contrast to traditional roadways, the UAV/drone can reach inaccessible locations in a very speedy manner [1–3]. Moreover, in many emergency-like situations, the traditional transportation and surveillance could not respond in a rapid way and the slow response can cause irreparable losses like lives. Initially, developed for military operations, the UAVs can be very beneficial in many applications including smart agriculture, surveillance, goods delivery operations, and so on [4]. UAVs have many properties similar to IoT devices and have sensors, transmitters, and receivers for communication with the other entities including humans [5]. The UAVs collect specific environment data for initiating the decision-making process [6]. Reddy et al. [4] provided a good survey of the usage of UAVs in agriculture and related fields for interested readers. Among many other applications, UAVs can be adopted for crowdsourcing systems [7]. However, very similar to generic IoT devices, the UAVs are battery powered and can be used by dishonest attackers for deceitful intentions, and such unintended usage can be harmful for decision making. The attacker can trace user locations and can effect the quality of services as well as forge the collected data and deviate the UAVs from their designated task [8]. Therefore, the communication among several UAVs and users need to be secured from unintended receivers. The following subsections briefly explain the adopted system architecture and adversarial model for the UAV-based crowdsourcing systems.

1.1. System Architecture. A typical UAV-based crowd monitoring system is shown in Figure 1. The UAVs are deployed at several geographical monitoring locations, where each geographical location can be monitored by one or more UAVs which are connected to a ground station (GS). All GSs are linked with the UAV (trusted) control center (TC). The proposed architecture also contains the cloud edge and a monitoring system to facilitate monitoring-based decision making through human interaction. The UAVs monitor the crowd and send the sensed information to the respective GS. The GS sends these data to the control center and finally this information is sent to the crowd monitoring system. The GS acts as an intermediate entity that accumulates and sends the UAV sensed data, whereas UAV, TC, and the user at monitoring system are responsible for the confidentiality of the sensed data during transmission and authenticity of the communicating entities, i.e., user, TC, and UAV.

1.2. Adversarial Model. The communication among UAVs and other devices including user and TC is carried out on the insecure public channel. Therefore, UAV communication has an attractive infrastructure for the attackers for initiation of forgery. As per the widely accepted adversarial model, DY model (Dolev–Yao model) [9], the attacker can listen, modify, replay, and stop a message exchanged among two entities of a UAV network [10–14]. The attacker can try to forge any message sent from any of the entities including user, TC, and UAV. In addition to the DY model, the strong de facto CK adversarial model [15] has got more attention from the researchers. In this paper, we consider the CK model with an adversary having all capabilities of the adversary considered in DY model; in addition, the adversary can compromise any one of the long-term secrets, ephemeral secrets, and session keys. Therefore, in the CK model, the session keys should be formed using long and short-term keys. Moreover, the session keys should be statistically independent of each other, and the compromise of a session key may not affect any other. Moreover, as per [16, 17], if an attacker captures a drone or user mobile device, they can extract parameters stored in the captured/stolen device. In this paper, we consider an extended CK (eCK) adversarial model [18], where an attacker can also launch a key compromise impersonation (KCI) attack.

2. Related Work

To secure communication among the users and UAVs/relevant devices, some access control/authentication protocols are proposed. For securing user-UAV communication, a temporal credential-based framework is proposed using symmetric primitives [19]. The scheme of Srinivas et al. [19] lacks resistance to impersonation based on stolen verifier; also, their scheme lacks anonymity as proved in [20]. The scheme proposed by Ali et al. could not resist ephemeral secret leakage attacks. The scheme proposed by Zhou et al. [21] in a distributed IoT environment using pairing was proved as insecure to IoT device forgery attacks [22]. In 2019, Wazid et al. [23] also proposed a new protocol for securing user-UAV communication through symmetric key primitives. As debated by Hussain et al. [3], Wazid et al.'s scheme is weak against stolen verifier-based forgery of users, UAVs, and trusted control centers. The scheme of Wazid et al. also lacks untraceability. Another scheme was proposed by Zhang et al. in 2020 by using symmetric primitives [24], which also lacks forward secrecy and is weak against insiders and stolen verifier attacks. Zhang et al. managed anonymity using a parameter PID_s, which is generic for all users and any dishonest user can break the anonymity and untraceability of the user requesting for login. Moreover, in Zhang et al.'s scheme, the user credentials are not verified appropriately. Therefore, the login request can be sent to the TC even when wrong credentials are entered. In 2020, Bera et al. proposed a scheme for UAV network using blockchains and certificates constructed upon elliptic curve-based cryptography (ECC) [25]. However, their scheme was debated for having critical weaknesses against man-in-the-middle, replay, and impersonation attacks and lack of anonymity by Chaudhry et al. [2]. In the same year, i.e., 2020, Bera et al. proposed another scheme [26] using blockchains and certificates using ECC. Unfortunately, Bera et al.'s scheme does not extend anonymity owing to the use of static identity RID_{DR_j} of the UAV/user. Likewise, as proved by Irshad et al. [27], there is no verification of the signatures generated by the ground station from the UAV in Bera et al.'s second scheme [26]. It was also debated in [27] that owing to the similar identity RID_{DNi} for all sessions, the scheme of Bera et al. [26] does not extend UAV anonymity. Another scheme using symmetric key and elliptic curve cryptography was proposed recently by Nikooghadam et al. [28]. The related works are summarized in Table 1, which gives the properties of existing methods along with their weaknesses and cryptographic method used.

2.1. Motivation and Contributions. In the recent past, many authentication schemes were designed for securing the communication among UAV, user, and TC. However, some of these schemes do not offer performance efficiency and some other schemes suffer from one or many insecurities. In this connection, very recently in 2021, Nikooghadam et al. proposed a symmetric key-based lightweight authentication scheme to secure the communication among users, UAV, and TC [28]. However, it is proved in the coming sections/subsections of this paper that Nikooghadam et al.'s scheme has many insecurities and cannot be deployed in real-world scenarios. The multi-fold contributions of this study include the following:

(i) Initially, we highlight the importance of secure communication among entities of UAV environments.

(ii) We revisited the authentication scheme proposed by Nikooghadam et al. and proved that Nikooghadam et al.'s scheme has vulnerabilities against stolen verifier attacks and lacks user anonymity and untraceability. It is also proved that Nikooghadam

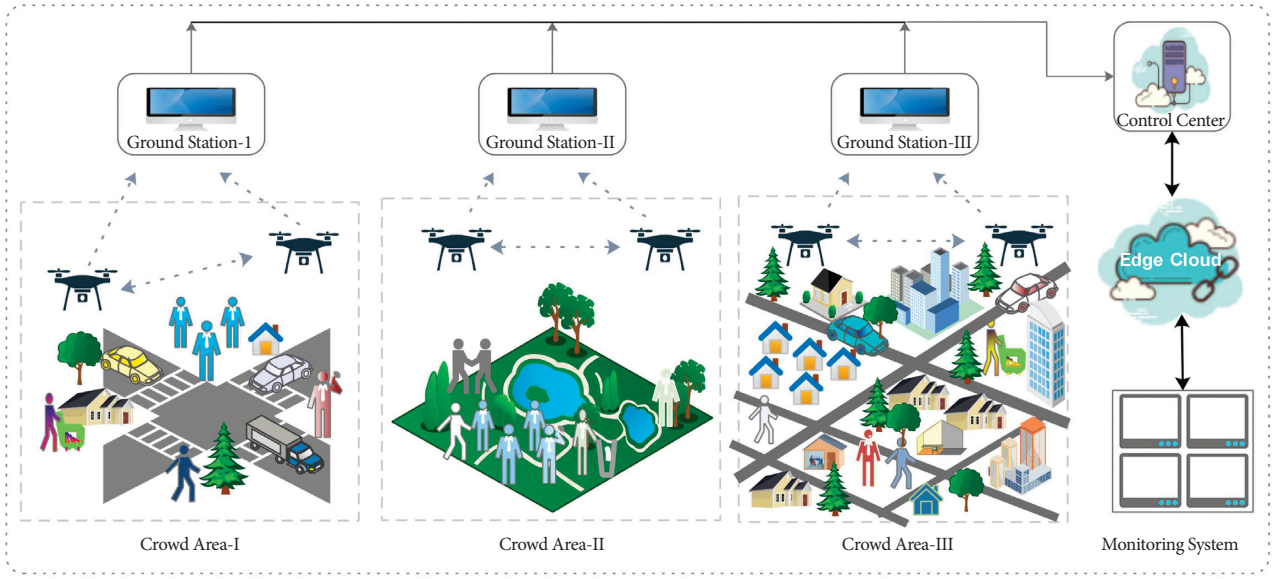

Figure 1: UAV-based crowd management system.

Table 1: Summary of related methods.

Protocol	Year	CMA	Properties/limitations
Turjman et al. [29]	2017	ECC and PR	Lacks resistance against replay attack.
Srinivas et al. [19]	2019	SKP	Lacks anonymity and resistance to impersonation based on stolen verifier.
Zhou et al. [21]	2019	ECC and PR	Insecure against IoT device forgery attack.
Wazid et al. [23]	2019	SKP	Weak against stolen verifier-based forgery of users, UAVs, and trusted control centers and lacks untraceability.
Zhang et al. [24]	2020	SKP	Lacks forward secrecy and is weak against insiders and stolen verifier attacks.
Bera et al.-I [25]	2020	ECC and BC	Weak against man-in-the-middle, replay, and impersonation attacks and lacks anonymity.
Bera et al.-II [26]	2020	ECC and BC	Lacks anonymity and the UAV does not verify signature authenticity of the ground station.
Kirsal [30]	2020	ECC and PR	Lacks perfect forward secrecy and is weak against known session key and insider attack.
Nikooghadam et al. [28]	2021	ECC	Lacks anonymity and is weak against stolen verifier attack and secret parameter exposure.
Proposed	—	ECC	Provides resistance to known attacks with comparable computation and communication costs.

Note. CMA: cryptographic method adopted; ECC: elliptic curve cryptography; PR: bilinear pairing; SKP: symmetric key primitives; BC: blockchain.

et al.'s scheme is not practical due to the exposure of secret parameters of the UAVs and the users.

(iii) A security-enhanced authentication scheme is proposed in this paper using only the lightweight symmetric key elliptic curve-based cryptography.

(iv) We used BAN logic and informal discussion on security properties for proving the security of the proposed scheme.

(v) By using MIRACL library, we set up a real-time environment, where we used a smartphone Xiaomi-Redmi Note-8 for replicating the user mobile device, Raspberry Pi3B + Cortex (A53-ARMv8) to replicate a UAV, and HP-EliteBook 8460-P to serve as the control center TC. We implemented the proposed scheme's primitives on these three devices for computation of the execution time of an authentication round.

(vi) Finally, a comparative study among proposed and related schemes based on performance and security features is conducted.

3. Revisiting the Scheme of Nikooghadam et al

The following subsections provide details on different phases of Nikooghadam et al.'s scheme for extending the authentication and session key among a user and a UAV through the control center. The notations used for the technical details of this paper are defined as per Table 2.

3.1. Initialization. The initialization is performed by the control center (TC) by selecting an elliptic curve E_p: $y^2 = x^3 + \alpha x + \beta \bmod p \in F_p$, where $p \geq |160|$bits, $\alpha, \beta \in F_p$, and $4\alpha^3 + 25\beta^2 \bmod p \neq 0$. Now, TC selects a base point $P \in E_p$ and a private key Pr_{tc}. TC also selects a hash function $H(\cdot)$: $\{0,1\}^* \longrightarrow \{0,1\}^l$, where $l \geq 160$ bits. Finally, TC secretly stores Pr_{tc} and publishes $E_p, G, P, H(\cdot)$.

3.2. User Registration. For completion of the registration, U_i selects an identity and passwords $\{\mathrm{ID}_i, \mathrm{PW}_i\}$ and a random number $d_i \in Z_p$. U_i now computes $\mathrm{PDW}_i = H(H(\mathrm{ID}_i \| d_i)$

Table 2: Notations.

Symbols	Explanations
TC	Trusted control center
U_i, Dr_j	User, UAV
$\mathrm{ID}_i, \mathrm{DID}_i$	Real and pseudo-identities of user
$\mathrm{Pr}_{tc}, \mathrm{Pub}_{tc}$	Public private key pair of TC
$\mathrm{Pr}_i, \mathrm{Pr}_j$	Secret keys of Vh_i and Dr_j
PID_j	Pseudo-identity of Dr_j
$\|, \oplus H(\cdot)$	Concatenation, XOR, hash
$E_s(\cdot), D_s(\cdot)$	Enc-decryption using s as key

$\oplus H(\mathrm{PW}_i \| d_i))$ and sends $\{\mathrm{ID}_i, \mathrm{PDW}_i\}$ to TC. On reception of $\{\mathrm{ID}_i, \mathrm{PDW}_i\}$, the TC checks the availability of ID_i and availability of ID_i, and the TC randomly selects f_i, q_i and computes $\mathrm{DID}_i = H(\mathrm{ID}_i \| f_i)$, $K_i = H(\mathrm{DID}_i \| \mathrm{Pr}_{tc} \| q_i)$, $A_i = H(\mathrm{DID}_i \| \mathrm{PDW}_i \| f_i \| K_i)$, and $B_i = H(A_i \| \mathrm{DID}_i)$ and transmits $\{f_i, K_i, B_i, H(\cdot)\}$ to U_i securely, in addition to storing the tuple $\{\mathrm{ID}_i, \mathrm{DID}_i, K_i\}$ in its verifier table. On receiving $\{f_i, K_i, B_i, H(\cdot)\}$, U_i stores these parameters in the memory of mobile device.

3.3. UAV Registration. For completion of the registration, Dr_j selects and transmits an identity ID_j to TC. On reception of $\{\mathrm{ID}_j\}$, the TC checks the availability of ID_j. On availability of ID_i, the TC randomly selects a_j and computes $\mathrm{PID}_j = H(a_j \| \mathrm{ID}_j)$ and $\mathrm{Key}_j = H(\mathrm{ID}_j \| \mathrm{Pr}_{tc} \| a_j)$ and transmits $\{\mathrm{ID}_j, \mathrm{PID}_j, \mathrm{Key}_j, H(\cdot)\}$ to U_i securely, in addition to storing the pair $\{\mathrm{ID}_j, \mathrm{PID}_j, \mathrm{Key}_j\}$ in its verifier table. On receiving $\{\mathrm{ID}_j, \mathrm{PID}_j, \mathrm{Key}_j, H(.)\}$, Dr_j stores the pair in its memory.

3.4. Login and Authentication. For login and authentication, the user U_i inputs the tuple $\{\mathrm{ID}_i, \mathrm{PW}_i\}$, and the mobile device computes $\mathrm{PDW}_i^* = H(H(\mathrm{ID}_i \| d_i) \oplus H(\mathrm{PW}_i \| d_i))$, $\mathrm{DID}_i^* = H(\mathrm{ID}_i \| f_i)$, and $A_i^* = H(\mathrm{DID}_i \| \mathrm{PDW}_i \| f_i \| K_i)$ and checks $B_i \stackrel{?}{=} H(A_i^* \| \mathrm{DID}_i)$. On success, the following steps as depicted in Figure 2 are performed between U_i, TC, and Dr_j.

ZDA 1: $U_i \longrightarrow$ TC: $M_1 = \{\mathrm{DID}_i, A_{1i}, Z_i, \mathrm{PID}_j, T_i\}$.

U_i generates $\{T_i, z_i\}$ and computes $A_{1i} = H(T_i \| \mathrm{DID}_i \| K_i)$, $Z_i = z_i P$, and sends $M_1 = \{\mathrm{DID}_i, A_{1i}, Z_i, \mathrm{PID}_j, T_i\}$ to TC.

ZDA 2: TC $\longrightarrow \mathrm{Dr}_j$: $M_2 = \{\mathrm{DID}_i, \mathrm{PID}_j, K_{ij}, Z_i, A_{3i}, T_{tc}\}$.

TC on receiving $M_1 = \{C_i, R_i, \rho_i, T_i\}$ checks the freshness of M_1 by checking $|T_c - T_i| \leq \Delta T$. On proven freshness, the TC extracts the related tuple $\{\mathrm{ID}_i, \mathrm{DID}_i, K_i\}$ and checks $A_{1i} \stackrel{?}{=} H(T_i \| \mathrm{DID}_i \| K_i)$. On success, TC generates T_{tc} and computes $K_{ij} = K_i \oplus \mathrm{Key}_j$ and $A_{3i} = H(\mathrm{PID}_j \| \mathrm{Key}_j \| \mathrm{ID}_j \| K_i)$. The TC transmits $M_2 = \{\mathrm{DID}_i, \mathrm{PID}_j, K_{ij}, Z_i, A_{3i}, T_{tc}\}$ to Dr_j.

ZDA 3: $\mathrm{Dr}_j \longrightarrow U_i$: $M_3 = \{Z_j, \mathrm{Aut}_j, T_j\}$.

Dr_j on receiving $M_2 = \{\mathrm{DID}_i, \mathrm{PID}_j, K_{ij}, Z_i, A_{3i}, T_{tc}\}$ checks the freshness of M_3 by checking $|T_c - T_{tc}| \leq \Delta T$. On proven freshness, Dr_j computes $K_i = K_{ij} \oplus \mathrm{Key}_j$ and checks $A_{3i} \stackrel{?}{=} H(\mathrm{PID}_j \| \mathrm{Key}_j \| \mathrm{ID}_j \| K_i)$. On proven validity, TC generates $\{g_j, T_j\}$ and computes $Z_{ij} = g_j Z_i = g_j z_i P$, $\mathrm{SK}_{ij} = H(\mathrm{ID}_j \| Z_{ij} \| K_i \| \mathrm{DID}_i)$, $Z_j = g_j P$, and $\mathrm{Aut}_j = H(\mathrm{SK}_{ij} \| \mathrm{DID}_i \| T_j \| K_i)$. Lastly, TC sends $M_3 = \{Z_j, \mathrm{Aut}_j, T_j\}$ to U_i.

ZDA 4: U_i on receiving $M_3 = \{Z_j, \mathrm{Aut}_j, T_j\}$ checks the freshness of M_3 by checking $|T_c - T_j| \leq \Delta T$. On proven freshness, U_i computes $Z_{ij} = z_i Z_j = z_i g_j P$ and the sess ion key $\mathrm{SK}_{ij} = H(\mathrm{ID}_j \| Z_{ij} \| K_i \| \mathrm{DID}_i)$ and checks the validity of session key by verifying $\mathrm{Aut}_j \stackrel{?}{=} H(\mathrm{SK}_{ij} \| \mathrm{DID}_i \| T_j \| K_i)$. On success, U_i keeps the SK_{ij} as session key authenticated with Dr_j.

4. Weaknesses of Nikooghadam et al.'s Scheme

This section explains the weaknesses of the scheme of Nikooghadam et al. [28] against secret key exposure and stolen verifier attack. Both of these attacks are very critical and common and render the scheme of Nikooghadam et al. inapplicable and impractical.

4.1. Stolen Verifier Attack. In the scheme of Nikooghadam et al., the trusted control center TC stores two separate verifier tables consisting of tuple $\{\mathrm{ID}_i, \mathrm{DID}_i, K_i\}$, where $i = 1, 2 \ldots n$ and $\{\mathrm{ID}_j, \mathrm{PID}_j, \mathrm{Key}_j, H(\cdot)\}$, where $j = 1, 2 \ldots m$ each for users (n numbers of users) and UAVs (m number of UAVs), respectively. As per the adopted CK adversarial model, the tables stored in the memory of TC can be exposed to the attacker. The whole authentication process can be compromised if these verifier tables are exposed to an attacker. An attacker with a verifier relating to users can impersonate on behalf of all users and an attacker with a verifier relating to the UAVs can impersonate on behalf of all UAVs. Therefore, the scheme of Nikooghadam et al. is not practical and is subject to stolen verifier attacks.

4.2. Lack of Anonymity and Untraceability. In the scheme of Nikooghadam et al.'s scheme, the user sends a pseudo-identity DID_i, which remains the same for all sessions. Therefore, Nikooghadam et al.'s scheme lacks anonymity and untraceability.

4.3. Secret Parameter Exposure. In the scheme of Nikooghadam et al., let user U_i be a dishonest user. U_i can initiate the login/authentication request, and for this, U_i transmits $M_1 = \{\mathrm{DID}_i, A_{1i}, Z_i, \mathrm{PID}_j, T_i\}$ to TC and TC transmits $M_2 = \{\mathrm{DID}_i, \mathrm{PID}_j, K_{ij}, Z_i, A_{3i}, T_{tc}\}$ to Dr_j. The dishonest user U_i while listening to the channel can receive $M_2 = \{\mathrm{DID}_i, \mathrm{PID}_j, K_{ij}, Z_i, A_{3i}, T_{tc}\}$. U_i can compute the secret parameter of Dr_j as follows:

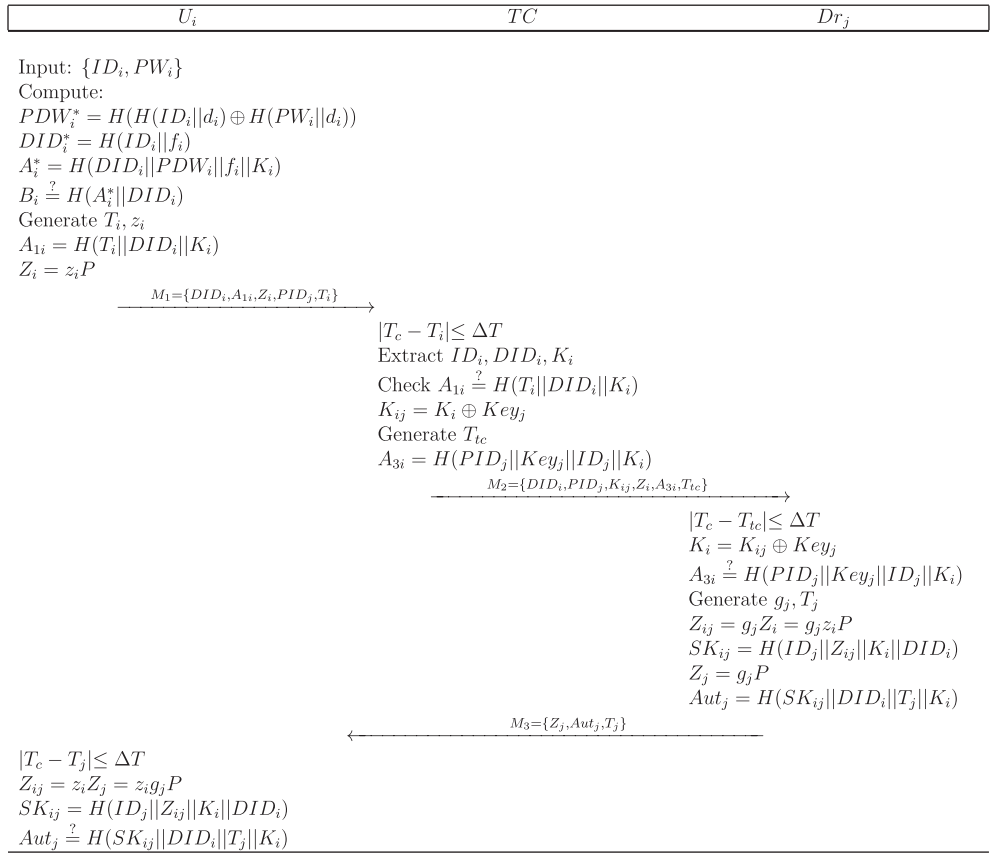

Figure 2: Nikooghadam et al.'s scheme.

$$\text{Key}_j = K_{ij} \oplus \text{Key}_i. \quad (1)$$

It is very clear that through equation (1), the dishonest user has computed the secret parameter Key_j of the UAV Dr_j.

4.3.1. Related Attacks Based on Secret Parameter Exposure. Once the secret parameter (Key_j) of a UAV (Dr_j) is revealed to a dishonest user say U_i, the U_i now using Key_j can impersonate not only on behalf of Dr_j but U_i can also use Key_j to extract the secret parameter K_i of any user requesting a session with Dr_j. Therefore, based on the secret parameter exposure attack, the malicious user can impersonate on behalf of any user requesting login with the Dr_j. Similarly, the malicious user can extract secret parameters of several or even all of the UAVs' Dr_j: $\{j = 1, 2 \ldots m\}$, and this can also lead to exposure of the secret parameters K_i: $\{i = 1, 2 \ldots n\}$ of all the registered users and the malicious user can impersonate on behalf of all the UAVs as well as all the users. Therefore, the scheme of Nikooghadam et al. cannot be practically deployed in any environment due to its weaknesses against the secret parameter exposure.

5. Proposed Scheme

In this section, we propose our improved scheme.

5.1. Initialization. The initialization is performed by the control center (TC) by selecting an elliptic curve E_p: $y^2 = x^3 + \alpha x + \beta \bmod p \in F_p$, where $p \geq |160|$bits, $\alpha, \beta \in F_p$, and $4\alpha^3 + 25\beta^2 \bmod p \neq 0$. Now, TC selects a base point $P \in E_p$, a private key Pr_{tc}, and a public key $\text{Pub}_{tc} = \text{Pr}_{tc}P$. TC also selects hash functions $H(.)$: $\{0,1\}^* \longrightarrow \{0,1\}^l$, where $l \geq 160$ bits, and a block cipher encryption/decryption algorithm $E_k/D_k(\cdot)$. Finally, TC secretly stores Pr_{tc} and publishes $\{E_p, \text{Pub}_{tc}, P, H(.), E_k/D_k(.)\}$.

5.2. User Registration. For crowd monitoring, a user has to register with the system. After registration, a user at monitoring system can authenticate a UAV through TC and can receive and interpret the crowd management-related data. For completion of the registration, U_i selects an identity and passwords $\{\text{ID}_i, \text{PW}_i\}$ and computes $\text{PDW}_i = H(H(\text{ID}_i \| \text{PW}_i)$. Now, U_i sends $\{\text{ID}_i, \text{PDW}_i\}$ to TC. On reception of $\{\text{ID}_i, \text{PDW}_i\}$, TC checks the availability of ID_i and availability of ID_i, and TC randomly selects k_i and computes $\text{Pr}_i = H(\text{ID}_i \| \text{Pr}_{tc} \| k_i)$, $A_i = \text{Pr}_i \oplus \text{PDW}_i$, and $B_i = H(A_i \| \text{Pr}_i \| \text{PDW}_i \| \text{ID}_i)$ and transmits $\{A_i, B_i, H(.)\}$ to U_i securely, in addition to storing the tuple $\{\text{ID}_i, \text{Pr}_i\}$ in its verifier table. On receiving $\{A_i, B_i, H(\cdot)\}$, U_i stores these parameters in the memory of mobile device. The registration process of the user is furnished through secure/private channel.

5.3. UAV Registration. For completion of the registration, Dr_j (the UAV) selects identity (DID_j) and sends it to TC. On reception of $\{DID_j\}$, TC checks the availability of DID_j. On availability of DID_j, TC randomly selects k_j and computes $Pr_j = H(DID_j \| Pr_{tc} \| k_j)$ and transmits $\{Pr_j\}$ to Dr_j securely, in addition to storing the pair $\{DID_j, k_j\}$ in its verifier table. On receiving $\{Pr_j\}$, Dr_j stores Pr_j in its memory and publishes $\{DID_j\}$. Like user registration, the registration process of the UAV is furnished through secure/private channel.

5.4. Authentication. For login, the user U_i inputs the tuple $\{ID_i, PW_i\}$, and the reader computes $PDW_i = H(ID_i \| PW_i)$ and $Pr_i = A_i \oplus PDW_i$ and checks $B_i \stackrel{?}{=} H(A_i \| Pr_i \| PDW_i \| ID_i)$. On success, U_i continues for authentication phase as depicted in Figure 3 detailed as follows:

IDA 1: $U_i \longrightarrow$ TC: $M_1 = \{C_i, R_i, \rho_i, T_i\}$.

Initially, U_i generates α_i, T_i and computes $r_i = H(\alpha_i \| Pr_i \| T_i)$, $R_i = r_i P$, $S_i = r_i Pub_{tc}$ and using $S_{i[x]}$ (x-coordinates of S_i) encrypts (ID_i, DID_j, T_i), i.e., $C_i = E_{S_{i[x]}}(ID_i, DID_j, T_i)$. Now, U_i computes $\rho_i = H(DID_j \| ID_i \| R_i \| S_i \| Pr_i \| T_i)$ and sends $M_1 = \{C_i, R_i, \rho_i, T_i\}$ to the trusted center TC.

IDA 2: TC $\longrightarrow$ Dr_j: $M_2 = \{C_{tc}, R_i, \delta_{tc}, T_{tc}\}$.

TC on receiving $M_1 = \{C_i, R_i, \rho_i, T_i\}$ checks the freshness of M_1 by checking $|T_c - T_i| \le \Delta T$. On proven freshness, TC computes $S_i = Pr_{tc} R_i = r_i Pub_{tc}$ and decrypts C_i and gets $[ID_i, DID_j, T_i] = D_{S_{i[x]}}(C_i)$. TC now verifies the validity of T_i, ID_i, DID_j, and on proven validity, TC computes $Pr_i = H(ID_i \| Pr_{tc} \| k_i)$ and verifies the validity of $\rho_i \stackrel{?}{=} H(DID_j \| ID_i \| R_i \| S_i \| Pr_i \| T_i)$. On success, TC computes $Pr_j = H(DID_j \| Pr_{tc} \| k_j)$ and generates T_{tc}. The TC now computes $\beta_{ij} = H(Pr_i \| S_i \| T_i)$, $C_{tc} = E_{H(Pr_j \| DID_j \| T_{tc})}(ID_i, DID_j, \beta_{ij}, T_{tc})$, and $\delta_{tc} = H(C_{tc} \| ID_i \| DID_j \| R_i \| Pr_j \| \beta_{ij} \| T_{tc})$ and transmits $M_2 = \{C_{tc}, R_i, \delta_{tc}, T_{tc}\}$ to Dr_j.

IDA 3: $Dr_j \longrightarrow$ TC: $M_3 = \{R_j, \Psi_j, \omega_j, T_j\}$.

TC on receiving $M_2 = \{C_i, R_i, \rho_i, C_j.\delta_j, T_j\}$ checks the freshness of M_3 by checking $|T_c - T_{tc}| \le \Delta T$. On proven freshness, Dr_j decrypts C_{tc} and gets $[ID_i, DID_j, \beta_{ij}, T_{tc}] = D_{H(Pr_j \| DID_j \| T_{tc})}(C_{tc})$. Now, Dr_j verifies the validity of $\delta_j \stackrel{?}{=} H(C_{tc} \| ID_i \| DID_j \| R_i \| Pr_j \| \beta_{ij} \| T_{tc})$. On proven validity of δ_j, Dr_j generates $\{r_j, T_j\}$ and computes $R_j = r_j P$, $\Psi_j = H(Pr_j \| \delta_j \| \beta_{ij} \| DID_j \| R_j \| T_j)$, $\gamma_{ij} = H(Pr_j \| \beta i j \| T_j)$ and session key $SK_{ij} = H(r_j R_i \| R_i \| R_j \| \beta_{ij} \| \gamma_{ij})$. Dr_j further computes $\omega_j = H(SK_{ij} \| DID_j \| ID_i \| \gamma_{ij})$ and transmits $M_3 = \{R_j, \Psi_j, \omega_j, T_j\}$ to the TC.

IDA 4: TC $\longrightarrow$ U_i: $M_4 = \{R_j, \omega_{tc}, \gamma_{tc}, T^2_{tc}\}$.

TC on receiving $M_3 = \{R_j, \Psi_j, \omega_j, T_j\}$ checks the freshness of M_3 by checking $|T_c - T_j| \le \Delta T$. On proven freshness, U_i checks $\Psi_j = H(Pr_j \| \delta_j \| \beta_{ij} \| DID_j \| R_j \| T_j)$, and on proven validity, TC computes $\gamma_{ij} = H(Pr_j \| \beta i j \| T_j)$. Now, TC generates T^2_{tc} and computes $\gamma_{tc} = \gamma_{ij} \oplus S_{i[y]}$, $\omega_{tc} = H(DID_j \| ID_i \| R_i \| R_j \| S_i \| T^2_{tc} \| \omega_j)$. TC finally sends $M_4 = \{R_j, \omega_{tc}, \gamma_{tc}, T^2_{tc}\}$ to U_i.

IDA 5: U_i on receiving $M_4 = \{R_j, \omega_{tc}, \gamma_{tc}, T^2_{tc}\}$ checks the freshness of M_4 by checking $|T_c - T^2_{tc}| \le \Delta T$. On proven freshness, U_i computes $\gamma_{ij} = \gamma_{tc} \oplus S_{i[y]}$, $\beta_{ij} = H(Pr_i \| S_i \| T_i)$ and the session key $SK_{ij} = H(r_j R_i \| R_i \| R_j \| \beta_{ij} \| \gamma_{ij})$. Finally, U_i computes $\omega_j = H(SK_{ij} \| DID_j \| ID_i \| \gamma_{ij})$ and checks the validity of session key by verifying $\omega_{tc} \stackrel{?}{=} H(DID_j \| ID_i \| R_i \| R_j \| S_i \| T^2_{tc} \| \omega_j)$. U_i keeps the SK_{ij} as session key authenticated with Dr_j.

6. Security Analysis and Discussion

In the following subsections, we prove the security of the proposed scheme formally as well as provide discussion on the attack resilience of the proposed scheme.

6.1. Formal Security Analysis through BAN. We demonstrate the formal security analysis of the contributed work using Burrows–Abadi–Needham logic (BAN) logic [31]. In this model, we conduct the security analysis with the consideration of session key protection and distribution along with mutual authenticity between the legal participants. Some related notations in this analysis are explained below:

(i) $S| \equiv : Z$ The principal S believes Z.

(ii) $S \triangleleft Z$: S sees Z.

(iii) $S| \sim Z$: S once said Z, and S believes it to be true.

(iv) $S| \Rightarrow Z$: S has jurisdiction over Z.

(v) $(\#(Z))$: Z is not replayed and is fresh.

(vi) (Z, Z'): Z or Z' are parts of a message.

(vii) $\{Z, Z'\}_k$: using K, Z or Z' are encrypted through symmetric encryption.

(viii) $S \longleftrightarrow^K S'$: the communication among S and S' is secured using K as the key.

Some related rules employed in this analysis are given as follows:

Rule 1: message meaning rule:

$$\frac{S| \equiv S \xrightarrow{K} S', S \triangleleft \langle Z \rangle_{Z'}}{S| \equiv S'| \sim Z}. \quad (2)$$

Figure 3: Proposed scheme.

Rule 2: nonce verification rule:

$$\frac{S| \equiv \#(Z), S| \equiv S'| \sim Z}{S| \equiv S'| \equiv Z}. \tag{3}$$

Rule 3: jurisdiction rule:

$$\frac{S| \equiv S' \Rightarrow Z, S| \equiv S'| \equiv Z}{S| \equiv Z}. \tag{4}$$

Rule 4: freshness conjunction rule:

$$\frac{S| \equiv \#(Z)}{S| \equiv \#(Z, Z')}. \tag{5}$$

Rule 5: belief rule:

$$\frac{S| \equiv (Z), S| \equiv (Z')}{S| \equiv (Z, Z')}. \tag{6}$$

Rule 6: session key rule:

$$\frac{S| \equiv \#(Z, S| \equiv S' \equiv Z}{S| \equiv S \longleftrightarrow KS'}. \tag{7}$$

(i) G-1: $\mathrm{TC}| \equiv (\mathrm{TC} \overset{S_i}{\longleftrightarrow} U_i)$.
(ii) G-2: $\mathrm{TC}| \equiv U_i| \equiv (\mathrm{TC} \overset{S_i}{\longleftrightarrow} U_i)$.
(iii) G-3: $U_i|| \equiv (\mathrm{TC} \overset{S_i}{\longleftrightarrow} U_i)$.
(iv) G-4: $U_i| \equiv \mathrm{TC}| \equiv (\mathrm{TC} \overset{S_i}{\longleftrightarrow} U_i)$.
(v) G-5: $\mathrm{Dr}_j| \equiv (\mathrm{Dr}_j \overset{Sk_{ij}}{\longleftrightarrow} U_i)$.
(vi) G-6: $U_i|| \equiv (\mathrm{Dr}_j \overset{Sk_{ij}}{\longleftrightarrow} U_i)$.

The idealized form of exchanged messages is given as follows:

(i) M_1: $U_i \longrightarrow \text{TC}$: C_i, R_i, ρ_i, T_i: $\{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

(ii) M_2: $\text{TC} \longrightarrow \text{Dr}_j$: $C_{tc}, R_i, \delta_{tc}, T_{tc}$: $\{(\text{DID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, r_iP, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}\rangle_{\text{Pr}_j}, \beta_{ij}, T_{tc}\}$

(iii) M_3: $\text{Dr}_j \longrightarrow \text{TC}$: $R_j, \Psi_j, \omega_j, T_j$: $\{r_jP, \langle \delta_j, \text{DID}_j, R_j, T_j\rangle_{\text{Pr}_j,\beta_{ij}}, \langle \text{DID}_j, \text{ID}_i, \langle T_j\rangle_{\text{Pr}_j,\beta_{ij}}\rangle_{SK_{ij}}, T_j\}$

(iv) M_4: $\text{TC} \longrightarrow U_i$: $R_j, \omega_{tc}, \gamma_{tc}, T_{tc}^2$: $\{R_j, \langle \text{DID}_j, \text{ID}_i, R_i, R_j\rangle_{S_i}, \langle \gamma_{ij}\rangle_{S_i[y]}, T_{tc}^2\}$

Next, the following premises have been constructed to prove the model.

(1) W_1: $U_i| \equiv \#(T_i)$

(2) W_2: $\text{TC}| \equiv \#T_{tc}$

(3) W_3: $\text{Dr}_j| \equiv \#T_j$

(4) W_4: $U_i| \equiv (U_i \longleftrightarrow \text{Pr}_i\ \text{TC})$

(5) W_5: $U_i| \equiv (U_i \longleftrightarrow SK_{ij}\ \text{Dr}_j)$

(6) W_6: $\text{TC}| \equiv (\text{TC} \longleftrightarrow \text{Pr}_iU_i)$

(7) W_7: $\text{TC}| \equiv \text{TC} \longleftrightarrow \text{Pr}_j\text{Dr}_j$

(8) W_8: $\text{Dr}_j| \equiv (\text{Dr}_j \longleftrightarrow SK_{ij}U_i)$

(9) W_9: $\text{Dr}_j| \equiv \text{Dr}_j \longleftrightarrow \text{Pr}_j\text{TC}$

(10) W_{10}: $U_i| \equiv \text{TC}| \Rightarrow (U_i \longleftrightarrow S_i\text{TC})$

(11) W_{11}: $\text{TC}| \equiv U_i| \Rightarrow (U_i \longleftrightarrow S_i\text{TC})$

(12) W_{12}: $\text{Dr}_j|| \equiv U_i| \Rightarrow (U_i \longleftrightarrow R_i\text{Dr}_j)$

(13) W_{13}: $\text{TC}| \equiv \text{Dr}_j| \Rightarrow (\text{Dr}_j \longleftrightarrow \beta_{ij}\text{TC}$

(14) W_{14}: $\text{Dr}_j| \equiv \text{TC}| \Rightarrow (U_i \longleftrightarrow R_i\text{TC}$

(15) W_{15}: $U_i| \equiv \text{Dr}_j| \Rightarrow (U_i \longleftrightarrow \gamma_{ij}\ \text{TC}$

Now we utilize the above idealizations in the following formulations considering M_1 and M_2 of the idealized formalization:

(i) M_1: $U_i \longrightarrow \text{TC}$: C_i, R_i, ρ_i, T_i: $\{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

(ii) M_2: $\text{TC} \longrightarrow \text{Dr}_j$: $C_{tc}, R_i, \delta_{tc}, T_{tc}$: $\{(\text{DID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, r_iP, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}\rangle_{\text{Pr}_j,\beta_{ij}}, T_{tc}\}$

Using seeing rule for M_1 and M_2, we get

(1) D_1: $\text{TC} \triangleleft C_i, R_i, \rho_i, T_i$: $\{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

(2) D_2: $\text{Dr}_j \triangleleft C_{tc}, R_i, \delta_{tc}, T_{tc}$: $\{(\text{ID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, r_iP, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}, \rangle_{\text{Pr}_j,\beta_{ij}}, T_{tc}\}$

According to D_1, D_2, W_8, W_9 and message meaning rule, we get

(3) D_3: $\text{TC}| \equiv U_i \sim \{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

(4) D_4: $\text{Dr}_j| \equiv \text{TC} \sim \{T_{tc}, (\text{ID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, r_iP, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}\rangle_{\text{Pr}_j,\beta_{ij}}\}$

Using D_3, W_1, freshness conjunction, and nonce verification rules, we get

(5) D_5: $\text{TC}| \equiv U_i \equiv \{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

Using D_4, W_2, freshness conjucatenation, and nonce verification rules, we get

(6) D_6: $\text{Dr}_j| \equiv \text{TC} \equiv \{T_{tc}, r_iP, (\text{ID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}\rangle_{\text{Pr}_j,\beta_{ij}}\}$

Using D_5, W_{12} and jurisdiction rule, we get

(7) D_7: $\text{TC}| \equiv \{(\text{ID}_i, \text{DID}_j, T_i)_{S_i}, r_iP, \langle \text{DID}_j, \text{ID}_i, R_i, T_i\rangle_{S_i,\text{Pr}_i}\}$

Using D_6, W_{14} and jurisdiction rule, we get

(8) D_8: $\text{Dr}_j| \equiv \{(\text{ID}_i, \text{DID}_j, \beta_{ij}, T_{tc})_{H(\text{Pr}_j,\text{DID}_j,T_{tc})}, r_iP, \langle C_{tc}, \text{ID}_i, \text{DID}_j, R_i, T_{tc}\rangle_{\text{Pr}_j,\beta_{ij}}, T_{tc}\}$

Using D_5, D_7 and session key rule, we get

(9) D_9: $\text{TC}| \equiv \text{TC} \longleftrightarrow S_iU_i$ (G-1)

Using D_5, D_7, W_6, W_8 and nonce verification rule, we get

(10) D_{10}: $\text{Dr}_j| \equiv \text{Dr}_j \longleftrightarrow \text{SK}_{ij}U_i$ (G-5)

Consider M_3 of the idealized form:

(11) M_3: $\text{Dr}_j \longrightarrow \text{TC}$: $R_j, \Psi_j, \omega_j, T_j$: $\{r_jP, \langle \delta_j, \text{DID}_j, R_j, T_j\rangle_{\text{Pr}_j,\beta_{ij}}, \langle \text{DID}_j, \text{ID}_i, \langle T_j\rangle_{\text{Pr}_j,\beta_{ij}}\rangle_{SK_{ij}}, T_j\}$

By applying seeing rule for M_3, we get

(12) D_{11}: $\text{TC} \triangleleft R_j, \Psi_j, \omega_j, T_j$: $\{r_jP, \langle \delta_j, \text{DID}_j, R_j, T_j\rangle_{\text{Pr}_j,\beta_{ij}}, \langle \text{DID}_j, \text{ID}_i, \langle T_j\rangle_{\text{Pr}_j,\beta_{ij}}\rangle_{SK_{ij}}, T_j\}$

Using D_{11}, W_7 and message meaning rule, we get

(13) D_{12}: $\text{TC}| \equiv \text{Dr}_j \sim \{r_jP, \langle \delta_j, \text{DID}_j, R_j, T_j\rangle_{\text{Pr}_j,\beta_{ij}}, \langle \text{DID}_j, \text{ID}_i, \langle T_j\rangle_{\text{Pr}_j,\beta_{ij}}\rangle_{SK_{ij}}, T_j\}$

Using D_{12}, W_3, W_{13}, freshness conjucatenation, and nonce verification rules, we get

(14) D_{13}: $\text{TC}| \equiv \text{Dr}_j| \equiv \{r_jP, \langle \delta_j, \text{DID}_j, R_j, T_j\rangle_{\text{Pr}_j,\beta_{ij}}, \langle \text{DID}_j, \text{ID}_i, \langle T_j\rangle_{\text{Pr}_j,\beta_{ij}}\rangle_{SK_{ij}}, T_j\}$

(15) $U_i| \equiv (\text{TC}^{S_i} \longleftrightarrow U_i)$ (G-3)

(16) $U_i| \equiv \text{TC}| \equiv (\text{TC}^{S_i} \longleftrightarrow U_i)$ (G-4)

Next, considering M_4 idealized form, we get

(17) M_4: $\text{TC} \longrightarrow U_i$: $R_j, \omega_{tc}, \gamma_{tc}, T_{tc}^2$: $\{R_j, \langle \text{DID}_j, \text{ID}_i, R_i, R_j\rangle_{S_i}, \langle \gamma_{ij}\rangle_{S_i[y]}, T_{tc}^2\}$

By applying seeing rule for M_4, we get

(18) D_{14}: $U_i \triangleleft R_j, \omega_{tc}, \gamma_{tc}, T_{tc}^2$: $\{R_j, \langle \text{DID}_j, \text{ID}_i, R_i, R_j\rangle_{S_i}, \langle \gamma_{ij}\rangle_{S_i[y]}, T_{tc}^2\}$

Using D_{14}, W_4, W_5, W_{11} and message meaning rule, we get

(19) D_{15}: $U_i| \equiv \text{TC} \sim R_j, \langle \text{DID}_j, \text{ID}_i, R_i, R_j\rangle_{S_i}, \langle\langle \gamma_{ij}\rangle\rangle_{S_i[y]}, T_{tc}^2$

By using D_{15}, W_2, W_3, freshness conjucatenation, and nonce verification rules, we get

(20) D_{16}: $U_i| \equiv \text{TC}| \equiv \{R_j, \langle \text{DID}_j, \text{ID}_i, R_i, R_j\rangle_{S_i}, \langle \gamma_{ij}\rangle_{S_i[y]}, T_{tc}^2\}$

Using D_{16}, W_4, W_{10}, W_{15} and jurisdiction rule, we get

(21) $D_{17}: U_i| \equiv \left\{R_j, \langle \mathrm{DID}_j, \mathrm{ID}_i, R_i, R_j\rangle_{S_i}, \langle \gamma_{ij}\rangle_{S_i[y]}, T_{tc}^2\right\}$

According to D_{17}, we apply the session key rule as

(22) $D_{18}: \mathrm{TC}| \equiv U_i| \equiv \mathrm{TC} \longleftrightarrow S_i U_i$ (G-2)

Using D_{18}, W_2, W_{14}, we apply the session key rule as

(23) $D_{19}: U_i| \equiv \mathrm{Dr}_j \longleftrightarrow \mathrm{SK}_{ij} U_i$ (G-6)

This analysis sufficiently proves that the proposed model achieves the specified goals by attaining mutual authenticity among the involved participants.

6.2. Informal Security Analysis. An informal security discussion on the security features of the proposed scheme is provided in the following subsection.

6.2.1. Mutual Authentication. In the proposed model, U_i and Dr_j entities mutually authenticate one another. This is because when U_i submits the authentication request message $M_1 = \{C_i, R_i, \rho_i, T_i\}$ towards TC, the latter verifies the freshness of timestamp T_i, and on successful verification, it computes S_i and Pr_i to further calculate $H(\mathrm{DID}_j \| \mathrm{ID}_i \| R_i \| S_i \| \mathrm{Pr}_i \| T_i)$ and match against ρ_i. If the equation holds valid, TC confirms the authenticity for U_i. Similarly, Dr_j after receiving the message checks the freshness of T_{tc} timestamp. Next, it computes $H(C_{tc} \| \mathrm{ID}_i \| \mathrm{DID}_j \| R_i \| \mathrm{Pr}_j \| \beta_{ij} \| T_{tc})$ using shared secret Pr_j and compares it against δ_j to completely verify TC. Likewise, Dr_j communicates the parameter γ_{ij} to U_i through TC. Then, U_i verifies the authenticity of Dr_j by computing $\beta_{ij} = H(\mathrm{Pr}_i \| S_i \| T_i)$, $SK_{ij} = H(r_j R_i \| R_i \| R_j \| \beta_{ij} \| \gamma_{ij})$, and $\omega_j = H(SK_{ij} \| \mathrm{DID}_j \| \mathrm{ID}_i \| \gamma_{ij})$. Then, it further computes $H(\mathrm{DID}_j \| \mathrm{ID}_i \| R_i \| R_j \| S_i \| T_{tc}^2 \| \omega_j)$ and verifies the equality check against ω_{tc}. If this holds true, U_i validates the authenticity for Dr_j. Hence, in the proposed scheme, both entities U_i and Dr_j mutually authenticate each other with the help of a trusted intermediary, i.e., TC.

6.2.2. User Anonymity. In the proposed scheme, U_i remains anonymous while submitting the authentication request to TC. U_i submits the message $M_1 = \{C_i, R_i, \rho_i, T_i\}$ to TC without disclosing the identity as plaintext. Since U_i encrypts its identity ID_i as $C_i = E_{S_{i[x]}}(\mathrm{ID}_i; \mathrm{DID}_j, T_i)$ using $S_{i[x]}$, C_i can only be decrypted by a legitimate TC. Moreover, the scheme supports untraceability since the authentication messages in our scheme do not bear any message parameter that remains constant among various sessions that could help the adversary in identifying the location of the user. Hence, our scheme ensures anonymity as well as untraceability for the user.

6.2.3. U_i Impersonation. The proposed scheme is immune to U_i impersonation attack. In case an adversary attempts to construct a fake authentication request message $M_1 = \{C_i, R_i, \rho_i, T_i\}$ with a fresh timestamp T_i, it would not be able to do this until it has access to secret key Pr_i which can only be computed by valid TC and can never be guessed or accessed by the adversary under ordinary circumstances. Hence, our scheme can resist U_i impersonation attack.

6.2.4. Man-in-the-Middle Attack. In the proposed scheme, no malicious entity can engage in the ongoing communication session of the legal participants. This is because of the fact that both participants such as U_i and Dr_j are deployed with secret keys, i.e., Pr_i, Pr_j, respectively, during the initialization phase by the trusted TC. Thus, all participants having possession to those secrets may engage in mutual authentication process and construct the mutually agreed session key $SK_{ij} = H(r_i R_j \| R_i \| R_j \| \beta_{ij} \| \gamma_{ij})$ on legal basis. Hence, the proposed scheme is very much immune to man-in-the-middle attack.

6.2.5. Session Key Security. The contributed protocol supports session key security because it supports mutual authentication and can resist man-in-the-middle as well as impersonation attacks, and the resistance against man-in-the-middle and impersonation attacks provide sufficient grounds to maintain this fact that our scheme ensures session key security in the face of crafty and malicious adversaries.

6.2.6. Denial of Service Attack. In DoS attack, an adversary may exploit vulnerability in the scheme if it is designed in such a way that the adversary may fabricate multiple authentication requests, while the server gets engaged to entertain each fake request and maintains that session for an indefinite time. In this manner, the attacker could initiate multiple fake requests towards the server and affect its capacity to serve the legal authentication request, which undermines its serving capacity. In our scheme, TC aborts the session immediately if either the timestamp T_i is not found to be fresh or the equality $\rho_i ? = H(\mathrm{DID}_j \| \mathrm{ID}_i \| R_i \| S_i \| \mathrm{Pr}_i \| T_i)$ does not hold true. In both cases, TC drops the session immediately which helps the protocol to avoid denial of service attack on the TC's end.

6.2.7. Replay Attack. Our scheme employs the feature of timestamp that allows the protocol participants to verify the freshness of the received message. To construct the authentication request $M_1 = \{C_i, R_i, \rho_i, T_i\}$, the U_i engenders the latest timestamp T_i and embeds the same in the parameter $\rho_i = H(\mathrm{DID}_j \| ID_i \| R_i \| S_i \| \mathrm{Pr}_i \| T_i)$ for submission to TC. TC verifies the freshness of timestamp T_i and verifies the calculated $H(\mathrm{DID}_j \| \mathrm{ID}_i \| R_i \| S_i \| \mathrm{Pr}_i \| T_i)$ against ρ_i. If true, it confirms the validity of U_i. Likewise, Dr_j after receiving the message confirms the freshness of T_{tc} timestamp and proceeds further to compute the response message. Upon successful verification, Dr_j submits the parameter γ_{ij} towards U_i via TC. Then, U_i verifies the authenticity of Dr_j by computing β_{ij} and verifying the corresponding timestamp

T_{tc}^2. In this manner, the replay attack can be successfully thwarted for the proposed scheme.

6.2.8. Physical Capturing Attack. In our scheme, the control center TC stores $\{\mathrm{DID}_j, \mathrm{Pr}_j\}$ in the memory of a UAV (say Dr_j), where $\mathrm{Pr}_j = H(\mathrm{DID}_j \| Pr_{tc} \| k_j)$. In addition, the TC stores $\{\mathrm{DID}_j, k_j\}$ in its verifier memory. DID_j is a randomly selected identity of the Dr_j, and it is different for each of the drone. Likewise, k_j is also uniquely selected for each of the drones. Henceforth, $\{\mathrm{DID}_j, \mathrm{Pr}_j\}$ are computed uniquely for each of the UAV. In case a UAV Dr_j is physically captured by a malicious entity, it cannot extend any advantage to the malicious entity to successfully forge any response message $M_{\bar{3}} = \{R_{\bar{j}}, \Psi_{\bar{j}}, \omega_{\bar{j}}, T_{\bar{j}}\}$ on behalf of another UAV say $\mathrm{Dr}_{\bar{j}}$, due to the uniqueness of parameters stored in each of Dr_j and $\mathrm{Dr}_{\bar{j}}$. In this manner, physical capturing is thwarted for the proposed scheme.

6.2.9. Perfect Forward Secrecy. In our scheme, the computation of the session key $SK_{ij} = H(r_j R_i \| R_i \| R_j \| \beta_{ij} \| \gamma_{ij})$ requires both session specific secrets (r_i, r_j) as well as long-term secrets of both the entities $(\beta_{ij}, \gamma_{ij})$, where $\beta_{ij} = H(\mathrm{Pr}_i \| S_i \| T_i)$ and $\gamma_{ij} = H(\mathrm{Pr}_j \| \beta ij \| T_j)$. It is clear that β_{ij} requires private key Pr_i of the user and γ_{ij} requires private key Pr_j of the UAV. Every session consists of unique short-term $\{r_i, r_j\}$ and long-term $\{\beta_{ij}, \gamma_{ij}\}$ parameters. The leakage of any of the session key or any of the long/short-term parameters may not extend any advantage to the attacker to gain abilities for compromising any future session.

7. Security and Performance Comparisons

In this section, the comparisons of the proposed scheme and related schemes presented in [19, 23, 24, 28–30] are conducted.

7.1. Security Features. Security feature comparisons of the proposed and relevant schemes proposed in [19, 23, 24, 28–30] are depicted in Table 3. All the relevant and compared schemes [19, 23, 24, 28–30] lack one or more security features: as proved in Section 4, the scheme of Nikooghadam et al. [28] has weaknesses against several attacks including stolen verifier, lack of untraceability, user and UAV impersonation based on secret parameter exposure of the UAVs, privileged insider and related attacks. The scheme of Wazid et al. has weaknesses against anonymity and untraceability, privileged insider and stolen verifier attacks, the scheme of Ever [30] lacks forward secrecy and prone to known session key and is privileged insider attacks. Similarly, the scheme of Zhang et al. [24] lacks mutual authentication, anonymity and untraceability, and forward secrecy, and the scheme of Turjman et al. [29] is also insecure against stolen verifier attack. The scheme of Srinivas et al. [19] lacks anonymity and untraceability and is also vulnerable to stolen verifier attacks. Only the proposed scheme provides all security features and resists known attacks.

Table 3: Security features.

Schemes	Ours	[28]	[23]	[30]	[24]	[29]	[19]
PMA	✓	✓	✓	✓	×	✓	✓
PAU	✓	×	×	✓	×	✓	×
RSV	✓	×	×	✓	✓	×	×
RUI	✓	✓	✓	✓	✓	✓	✓
RRA	✓	✓	✓	✓	✓	✓	✓
RPC	✓	✓	✓	✓	✓	✓	✓
PSK	✓	✓	✓	✓	✓	✓	✓
PFS	✓	✓	✓	×	×	✓	✓
RKS	✓	✓	✓	×	✓	✓	✓
RIA	✓	×	×	×	✓	✓	✓
RMM	✓	×	✓	✓	✓	✓	✓

Note. PMA: provides mutual authentication; PAU: provides anonymity and untraceability; RSV: resists stolen verifier; RUI: resists impersonation of the user, TC, and UAV; RRA: resists replay attack; RPC: resists physical capture; PSK: provides session key; PFS: provides forward secrecy; RKS: known session key attack; RIA: resists insider attack; RMM: resists man-in-the-middle attack; ✓: provision of the security feature; ×: non-provision of the security feature.

7.2. Computation Cost. This subsection provides the comparison of the proposed scheme with related schemes [19, 23, 24, 28–30] as per real-time experiment conducted over MIRACL library, where we used Xiaomi-Redmi Note-8 smart phone with RAM size of 4 GB and 2.01 GHz Octa core Max processor. The underlying operating system in smart phone is Android V-9 and MIUI V-11.0.7. For replicating the trusted control center TC in the experiment, HP-EliteBook 8460-P with 2.7 GHz Intel® Core-TM and 4 GB RAM along with Ubuntu LTS 16 OS was used. Likewise, to replicate a UAV, Pi3B + Cortex (A53-ARMv8) with 64 bit-SoC, 1.4 GHz processor, and 1 GB LPDDR2-SDRAM was used in the experiment. The running times and notations used for each cryptographic operation for each of the user/mobile, TC, and UAV are depicted in Table 4.

The authentication process in the proposed scheme is furnished between U_i, TC, and Dr_j, where, U_i executes $6T_{hs} + 6T_{e\,d} + 3T_{me}$ operations. The TC executes $9T_{hs} + 7T_{e\,d} + 1T_{me}$ operations; in addition, Dr_j executes $5T_{hs} + 3T_{e\,d} + 2T_{me}$ operations. Therefore, in proposed scheme, the running time to complete authentication among U_i, TC, and Dr_j is ≈25.877 ms. The running time to complete authentication in Nikooghadam et al.'s scheme [28] is ≈18.544 ms. As per the experimental results given in Table 5, the running times of the schemes presented in [19, 23, 24, 29, 30] are ≈5.334 ms, ≈84.366 ms, ≈0.16 ms, ≈49.392 ms, and ≈49.392 ms, respectively.

7.3. Communication Cost. The communication cost comparison of the proposed and related schemes [19, 23, 24, 28–30] is shown in this subsection. In proposed scheme, we utilized SHA − 1 with 160 bit size. We used AES as the symmetric cryptographic algorithm with 128 bit cipher size

Table 4: Operation running time.

Operations	Notations	User/mobile	UAV	Server
Pairing-bilinear	T_{pb}	17.36	12.52	4.038
Point multiplication over ECC	T_{me}	5.116	4.107	0.926
Point addition over ECC	T_{ae}	0.013	0.018	0.006
Secure hash	T_{hs}	0.009	0.006	0.004
Symmetric operations	$T_{e\,d}$	0.017	0.013	0.008

Table 5: Comparison of computation and communication costs.

Protocol	U_i	TC	Dr_j	RT	BE
Srinivas et al. [19]	$14T_{hs} + 1T_f$	$9T_{hs}$	$30T_{hs} + 1T_f$	≈10.574 ms	192
Turjman et al. [29]	$10T_{hs} + 1T_{pb}$	$14T_{hs} + 1T_{pb} + 3T_{me}$	$5T_{hs} + 2T_{pb}$	≈49.392 ms	300
Zhang et al. [24]	$10T_{hs}$	$7T_{hs}$	$7T_{hs}$	≈0.16 ms	184
Kirsal [30]	$5T_{hs} + 2T_{pb}$	$3T_{hs} + 2T_{pb}$	$9T_{hs} + 2T_{pb} + 4T_{me}$	≈84.366 ms	240
Wazid et al. [23]	$16T_{hs} + 1T_f$	$8T_{hs}$	$7T_{hs}$	≈5.334 ms	212
Nikooghadam et al. [28]	$8T_{hs} + 2T_{me}$	$2T_{hs}$	$3T_{hs} + 2T_{me}$	≈18.544 ms	356
Proposed	$6T_{hs} + 3T_{e\,d} + 3T_{me}$	$9T_{hs} + 7T_{e\,d} + 1T_{me}$	$5T_{hs} + 3T_{e\,d} + 2T_{me}$	≈25.877 ms	408

Note. RT: running time in milliseconds; BE: bytes exchange.

and 192 bit key. The output sizes of asymmetric cryptographic techniques are taken as per NIST recommended sizes which are 1024 bits and 320 bits each for RSA and ECC. The size of random numbers are also taken as 160 for simplicity and the size of a timestamp is fixed at 32 bits. Moreover, all the identities are taken as 128 bits long. U_i sends $M_1 = \{C_i, R_i, \rho_i, T_i\}$ to TC, where, $C_i = E_{S_{i[x]}}(\text{ID}_i, \text{DID}_j, T_i)$, the size of each of the identity is 128 bits, and size of $T_i = 32$ bits, so total size of $C_i = \{128 + 128 + 32 = 288\}$, which requires three symmetric encryption operation each of size 128 bits. Therefore, to encrypt C_i, we require 48 bytes. The total size of M_1 is $\{384 + 320 + 160 + 32\} = 896$ bits. Similarly, $M_2 = \{C_{tc}, R_i, \delta_{tc}, T_{tc}\}$ requires to send $\{512 + 320 + 160 + 32\} = 1024$-bits from TC to Dr_j. Dr_j sends $M_3 = \{R_j, \Psi_j, \omega_j, T_j\}$, which requires transmission of $\{320 + 160 + 160 + 32\} = 672$-bits. Finally, TC sends $M_4 = \{R_j, \omega_{tc}, \gamma_{tc}, T_{tc}^2\}$ to U_i, which also requires transmission of $\{320 + 160 + 160 + 32\} = 672$ bits. Therefore, total communication cost of the proposed scheme is $\{896 + 1024 + 672 + 672\} = 3264$ bits, which is 408 bytes. The communication cost of the Nikooghadam et al.'s scheme [28] is 356 bytes. The communication cost of the schemes presented in [19, 23, 24, 29, 30] is 212, 240, 184, 300, and 192 bytes, respectively.

8. Conclusion

We initiated this article by highlighting the importance of secure communication among entities of a UAV network for crowd management. We revisited and proved that Nikooghadam et al.'s scheme has vulnerabilities against stolen verifier attacks and lacks user anonymity and untraceability. It is also proved that Nikooghadam et al.'s scheme is not practical due to the exposure of secret parameters of the UAVs and the users, which can ultimately lead to the total failure scenario. Therefore, a security-enhanced authentication scheme is proposed in this article using only the lightweight symmetric key primitives and ECC. We implemented the proposed scheme in a real-time environment to extract the running time of each of the entities involved in the authentication process. The BAN logic-based security analysis and a discussion on the security features affirm that the proposed scheme can resist known attacks while raising some computation. In future, we intend to implement the proposed protocol in real world for securing crowdsourcing systems.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors express their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (227).

References

[1] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[2] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria, "Gcacs-iod: a certificate based generic access control scheme for internet of drones," *Computer Networks*, vol. 191, Article ID 107999, 2021.

[3] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: an ECC-based authentication scheme for internet of drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, 2021.

[4] P. K. R. Maddikunta, S. Hakak, M. Alazab et al., "Unmanned aerial vehicles in smart agriculture: applications,

requirements, and challenges," *IEEE Sensors Journal*, vol. 21, no. 16, Article ID 17608, 2021.

[5] B. Li, Z. Fei, and Y. Zhang, "UAV communications for 5g and beyond: recent advances and future trends," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2241–2263, 2018.

[6] Y. Wu, H.-N. Dai, H. Wang, and K. K. R. Choo, "Blockchain-based privacy preservation for 5G-enabled drone communications," *IEEE Network*, vol. 35, no. 1, pp. 50–56, 2021.

[7] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities," *Computer Standards and Interfaces*, vol. 76, Article ID 103517, 2021.

[8] B. D. Deebak and F. A. Turjman, "A smart lightweight privacy preservation scheme for iot-based UAV communication systems," *Computer Communications*, vol. 162, pp. 102–117, 2020.

[9] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[10] A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 12, pp. 5529–5552, 2016.

[11] C. Peng, M. Luo, L. Li, K.-K. R. Choo, and D. He, "Efficient certificateless online/offline signature scheme for wireless body area networks," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14287–14298, 2021.

[12] S. A. Chaudhry, "Correcting "PALK: password-based anonymous lightweight key agreement framework for smart grid"," *International Journal of Electrical Power and Energy Systems*, vol. 125, Article ID 106529, 2021.

[13] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.

[14] X. Li, J. Tan, A. Liu, P. Vijayakumar, N. Kumar, and M. Alazab, "A novel UAV-enabled data collection scheme for intelligent transportation system through UAV speed control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2100–2110, 2021.

[15] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," *Lecture Notes in Computer Science*, Springer, in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 453–474, May 2001.

[16] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[17] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the Annual International Cryptology conference*, pp. 388–397, Santa Barbara, CA, USA, August 1999.

[18] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of the International Conference on Provable Security*, pp. 1–16, Wollongong, NSW, Australia, November 2007.

[19] 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 Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[20] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. A. Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, Article ID 43711, 2020.

[21] Y. Zhou, T. Liu, F. Tang, and M. Tinashe, "An unlinkable authentication scheme for distributed iot application," *IEEE Access*, vol. 7, Article ID 14757, 2019.

[22] S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: a pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," *IEEE Systems Journal*, pp. 1–8, 2020.

[23] 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 of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

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

[25] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in iot-enabled internet of drones deployment," *Computer Communications*, vol. 153, pp. 229–249, 2020.

[26] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.

[27] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5g-enabled iod environment," *Computer Networks*, vol. 195, Article ID 108219, 2021.

[28] 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," *Journal of Systems Architecture*, vol. 115, Article ID 101955, 2021.

[29] F. A. Turjman, Y. K. Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless key agreement framework for mobile-sink in iot based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, Article ID 24617, 2017.

[30] Y. E. Kirsal, "A secure authentication scheme framework for mobile-sinks used in the internet of drones applications," *Computer Communications*, vol. 155, pp. 143–149, 2020.

[31] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.