Hindawi
Security and Communication Networks
Volume 2023, Article ID 9864893, 1 page
https://doi.org/10.1155/2023/9864893

Retraction

Retracted: TC-PSLAP: Temporal Credential-Based Provably Secure and Lightweight Authentication Protocol for IoT-Enabled Drone Environments

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Z. Ali, B. A. Alzahrani, A. Barnawi, A. Al-Barakati, P. Vijayakumar, and S. A. Chaudhry, "TC-PSLAP: Temporal Credential-Based Provably Secure and Lightweight Authentication Protocol for IoT-Enabled Drone Environments," *Security and Communication Networks*, vol. 2021, Article ID 9919460, 10 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 9919460, 10 pages
https://doi.org/10.1155/2021/9919460

Research Article

TC-PSLAP: Temporal Credential-Based Provably Secure and Lightweight Authentication Protocol for IoT-Enabled Drone Environments

Zeeshan Ali,[1] **Bander A. Alzahrani**,[2] **Ahmed Barnawi**,[2] **Abdullah Al-Barakati**,[2] **Pandi Vijayakumar**,[3] **and Shehzad Ashraf Chaudhry**[4]

[1]*Department of Computer Science & Software Engineering, International Islamic University, Islamabad, Pakistan*
[2]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[3]*Department of Computer Science and Engineering, University College of Engineering, Tindivanam, India*
[4]*Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey*

Correspondence should be addressed to Pandi Vijayakumar; vijibond2000@gmail.com

Received 13 October 2021; Revised 15 November 2021; Accepted 20 November 2021; Published 18 December 2021

Academic Editor: Muhammad Arif

In smart cities, common infrastructures are merged and integrated with various components of information communication and technology (ICT) to be coordinated and controlled. Drones (unmanned aerial vehicles) are amongst those components, and when coordinated with each other and with the environment, the drones form an Internet of Drones (IoD). The IoD provides real-time data to the users in smart cities by utilizing traditional cellular networks. However, the delicate data gathered by drones are subject to many security threats and give rise to numerous privacy and security issues. A robust and secure authentication scheme is required to allow drones and users to authenticate and establish a session key. In this article, we proposed a provably secure symmetric-key and temporal credential-based lightweight authentication protocol (TC-PSLAP) to secure the drone communication. We prove that the proposed scheme is provably secure formally through the automated verification tool AVISPA and Burrows–Abadi–Needham logic (BAN logic). Informal security analysis is also performed to depict that the proposed TC-PSLAP can resist known attacks.

1. Introduction

Over time, more of the rural population is moving to urban areas. Hence, it is right to say that urbanization is the future, and 66% of the society will move to urban areas by 2050 [1]. So, with the rise of the urban population, it becomes crucial to building smart cities by employing information and communication technologies (ICT) [2, 3]. These services incorporate smart home, smart meter, smart grid, edge computing, Internet of Things (IoT), and smartphone which enable the individuals to log in into applications and transmit and receive data [4].

In making cities smarter, drone technology has undoubtedly played a significant role. It is challenging to envision a smart city without incorporating drone services [5]. Drones (also known as unmanned aerial vehicles (UAVs)) are employed in diverse areas ranging from transportation, safety and security, agriculture, environmental protection, disaster mitigation, and surveillance and in a variety of areas as illustrated in Figure 1. A typical drone consists of a battery, sensors, actuators, recorder, computing, and communication module [6]. The typical architecture of a drone is depicted in Figure 2.

Drones are adequately smart, can communicate with one other, and can also make judgments without human involvement [7]. When several drones work together, intercommunicate, accumulate data, and reside in a designated flying zone, then this is referred to as an Internet of Drones

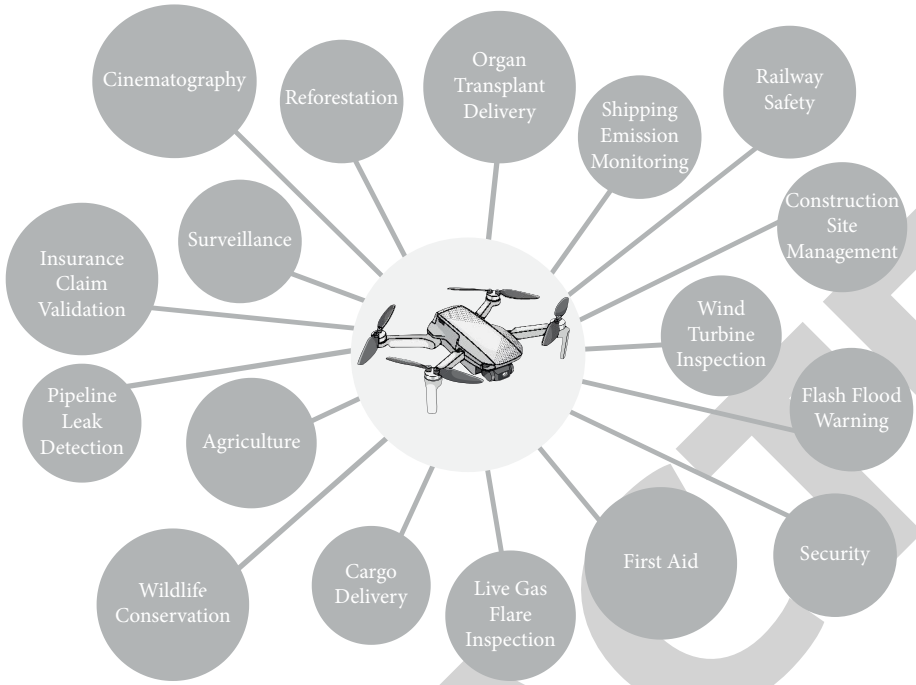

Figure 1: Uses of drones.

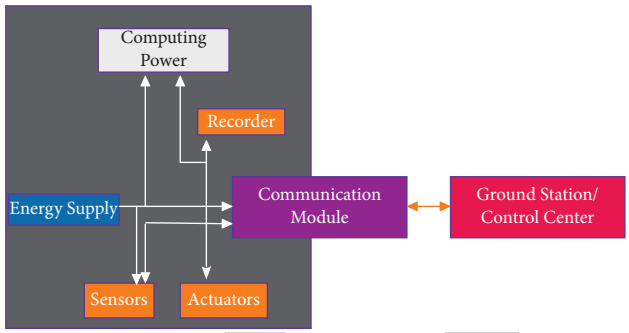

Figure 2: Typical architecture of the drone (adopted from [6]).

(IoD) [8]. Data gathered by the drones are then transmitted to a remote server/ground station/base station where they are further analyzed [9].

These drones gather sensitive data from their environment and transmit them to the base station over the insecure wireless channel. So, an attacker can capture and modify the unfeigned environment-related data. Moreover, an attacker can access these drones and can use them for their wicked purposes such as the illegal surveillance of an individual [10, 11]. Consequently, IoD needs a security mechanism to evade proscribed access and to render availability in addition to confidentiality and data integrity.

In the recent past, many researchers have presented authentication and key agreement (AKA) schemes and surveys related to drones' security, privacy, and limitations. As drones rely on the insecure wireless channel to communicate, they are susceptible to many security threats [12–14]. Yaacoub et al. [7] recently presented a detailed survey related to drones, in which they have discussed various aspects associated with UAVs in detail. They have discussed regulations, architecture, communication types, UAV types, crash, collision, and obstacle-collision methods. They have also discussed use domains, various security, privacy, and safety concerns, and existing threats and vulnerabilities related to drones along with suggestions and recommendations to enhance drone security.

Alsamhi et al. [5] presented the survey in which they discussed how the collaboration between smart drones and IoT increases the smartness of the smart city. Zhang et al. [15] introduced a lightweight AKA scheme for the IoD. The scheme of Zhang et al. exploits the resource-friendly bitwise exclusive OR (XOR) and noninvertible hash functions (Hash) to provide a lightweight and efficient authentication process. Zhang et al. also stated that the scheme can withstand various known attacks. Kirsal Ever [16] proposed an AKA framework for mobile sinks in the IoD applications. Deebak and Al-Turjman [17] proposed a lightweight scheme for IoT-based drones to provide privacy preservation and to support mutual authentication. Their scheme is based on XOR, Hash, and hash-based message authentication (HMAC). Chen et al. [18] proposed an authentication scheme for UAVs with direct anonymous attestation with low computation cost to enhance performance.

Srinivas et al. [19] introduced an anonymous lightweight authentication scheme for the IoD based on the temporary credentials. In their scheme, the user and drone need to be registered with the ground station server (GSS) first to access the remote drone. They stated that their scheme can withstand known attacks such as offline password guessing attack, user, GSS, remote drone impersonation attack, and reply attack and renders user anonymity and untraceability.

However, Ali et al. [6] proved that [19] is not secure and is prone to traceability attack and impersonation attack based on the stolen verifier attack and does not scale well. To

overcome these issues, they introduced an improved scheme. They also stated that their scheme is secure and can withstand stolen mobile devices, impersonation, reply, man-in-the-middle, remote drone impersonation attack, and various other known attacks.

Nikooghadam et al. [20] also proposed a lightweight authentication scheme for the IoD for smart city surveillance. Their scheme is based on elliptic curve cryptography (ECC), one-way hash function, and bitwise (XOR). Their scheme consists of three entities, namely, user, drone, and control server. They stated that their scheme is safe and can withstand various attacks. However, their scheme suffers from user impersonation, control server impersonation, drone impersonation based on the stolen verifier attack, privileged insider attack, and leakage of secret parameters, does not render user anonymity, and lacks untraceability.

1.1. Paper Organization. The rest of the paper is arranged as follows: the notations used in the manuscript are provided in Table 1. The adversarial model adopted in this paper is outlined in Section 1.2. Our protocol is outlined in Section 2, and its security analysis is performed in Section 3. The comparative analysis is performed in Section 4. The paper is finally concluded in Section 5.

1.2. Threat Model. The common CK adversarial model [21, 22] is adopted in this article, where the adversary $\mathscr{A}$ has the following competencies:

(1) Communication over the public/open channel is under the full control of $\mathscr{A}$

(2) $\mathscr{A}$ can forge a message and can also delay, restrain, retransmit, and alter the former message

(3) By employing the power analysis, $\mathscr{A}$ can extract the information from the smart card/mobile device/drone

(4) An outsider or insider/privileged user can compromise the privacy and security of the system

(5) An insider says $U_{\mathscr{A}}$ can endanger/access the verifier information put in the database controlled by CS [23]

(6) Servers' private key cannot be compromised

2. Proposed TC-PSLAP

In this section, an enhanced scheme is introduced. The proposed TC-PSLAP comprises mainly four processes, namely, (i) initialization process, (ii) registration process, (iii) login and authentication process, and (iv) password update process. The proposed scheme as depicted in Figure 3 is described in the subsequent sections.

2.1. TC-PSLAP: Initialization Process. In this process, the control server (CS) picks a private master key $\text{MSK} \in \mathscr{Z}_p$ and a one-way hash function $H(.)$ and makes the parameters $\{H(.)\}$ public, while {MSK} is kept private.

2.2. TC-PSLAP: Registration Process. This phase describes the procedure of registering a user and a drone with the system.

2.2.1. TC-PSLAP: User Registration Process. To access the system and to utilize its resources, user U_k first needs to register with the CS over the private channel. Subsequent are the steps performed by U_k to register with the CS:

URG 1: user (U_k) picks an identity PID_k, a password PWD_k, and an arbitrary number $R_{\text{and}_1} \in \mathscr{Z}_p^*$ and transmits PID_k over the secure channel to the control server (CS).

URG 2: CS receives the registration request from U_k, picks an arbitrary number $R_{\text{and}_2} \in \mathscr{Z}_p^*$ and a temporary identity $\text{TID}_k \in \mathscr{Z}_p^*$, and transmits the message containing $\{X_k, A_k, \text{TID}_k\}$ to U_k over the secure channel where $A_k = H(\text{PID}_k \| \text{MSK} \| R_{\text{and}_2})$ and $X_k = E_{H(\text{MSK})}[\text{PID}_k, R_{\text{and}_2}]$. CS also stores the parameter TID_k into the database.

URG 3: upon receiving the response from CS, U_k computes $V_k = H(\text{PWD}_k \| R_{\text{and}_1})$, $\text{AUTH}_k = H(\text{PID}_k \| \text{PWD}_k \| R_{\text{and}_1})$, $X_k^+ = X_k \oplus V_k$, $A_k^+ = A_k \oplus V_k$, $\text{TID}_k^+ = \text{TID}_k \oplus V_k$, $R_{\text{and}_1}^+ = R_{\text{and}_1} \oplus H(\text{PID}_k \| \text{PWD}_k)$.

URG 4: finally, U_k saves the parameters $\{\text{AUTH}_k, X_k^+, A_k^+, \text{TID}_k^+, R_{\text{and}_1}^+\}$ into the mobile device (MD_k).

2.2.2. TC-PSLAP: Drone Registration Process. Following are the steps performed to register the drone with the system in an offline mode:

DRG 1: a remote drone (DR_l) picks an identity ID_{DR_l} and transmits it to the CS over the secure channel.

DRG 2: upon receiving the registration request from DR_l, CS picks an arbitrary number $R_{\text{and}_3} \in \mathscr{Z}_p^*$ and pseudo-identity $\text{TID}_l \in \mathscr{Z}_p^*$. Next, CS computes $X_l = H(\text{ID}_{\text{DR}_l} \| R_{\text{and}_3} \| \text{TID}_l)$, $\text{KEY}_{\text{cs},l} = H(H(\text{MSK}) \| X_l)$ and transmits the message containing $\{\text{TID}_l, \text{KEY}_{\text{cs},l}\}$ to DR_l via the secure channel. CS also stores the parameters $\{\text{TID}_l, X_l\}$ in the database.

DRG 3: DR_l also stores the parameters $\{\text{ID}_{\text{DR}_l}, \text{TID}_l, \| \text{KEY}_{\text{cs},l}\}$ into the memory securely.

2.3. TC-PSLAP: Login and Authentication Process. After successful registration, U_k and DR_l can establish a session key to communicate securely with the help of CS. Subsequent steps as depicted in Figure 4 are performed by U_k, CS, and DR_l to establish a session key:

LAU 1: U_k provides his/her identity PID_k^+ and password PWD_k^+, and MD_k computes $I_k = H(\text{PID}_k^+ \| \text{PWD}_k^+)$ and $R_{\text{and}_1} = R_{\text{and}_1}^+ \oplus I_k$. If the condition $\text{AUTH}_k \stackrel{?}{=} H(\text{PID}_k^+ \| \text{PWD}_k^+ \| R_{\text{and}_1})$ is true, then the process continues; else, it terminates.

Table 1: Notations' guide.

Symbols	Representations
$U_k, \text{PID}_k, \text{PWD}_k$	k^{th} user, its personal identity, password
BIO_k	k^{th} users' personal biometric
MD_k	k^{th} users' mobile device
CS, MSK	Control server and its private master key
$\text{DR}_l, \text{ID}_{\text{DR}_l}$	l^{th} drone and its identity
$\text{sk}_{lk} (= \text{sk}_{kl})$	Shared session key between U_k and DR_l
P	ECC base point $E_p(a, b)$
R_{and_m}	m^{th} random number of 160 bits
T_{cs}, T_k, T_l	Current timestamps of CS, U_k, and DR_l
δT, TC	Maximum allowable transmission delay and present time
$i \stackrel{?}{=} j$	Checks if i is equal to j
$H(.)$	Cryptographic one-way hash function
$\oplus, \|$	Bitwise XOR and concatenation operators
$\mathcal{A}, U_{\mathcal{A}}$	An adversary and privileged insider

LAU 2: upon successful verification, MD_k picks a present timestamp T_k and an arbitrary number R_{and_4} and computes $A_k = A_k^+ \oplus I_k, V_k' = H(\text{PWD}_k \| R_{\text{and}_1}), J_k = H(A_k \| T_k)$, $X_k = X_k^+ \oplus V_k', \text{TID}_k = \text{TID}_k^+ \oplus V_k'$, $Z_k = H(A_k \| \text{TID}_k \| R_{\text{and}_4} \| T_k)$, $\text{TID}_l^+ = \text{TID}_l \oplus J_k$, and $R_{\text{and}_4}^+ = R_{\text{and}_4} \oplus J_k$. Finally, MD_k transmits the message containing $\text{MSG}_1 = \langle X_k, Z_k, R_{\text{and}_4}^+, \text{TID}_k, \text{TID}_l^+, T_k \rangle$ to CS via the insecure channel.

LAU 3: upon receiving MSG_1 from U_k, CS first checks the freshness of the message by examining the condition $|\text{TC} - T_k \le \delta T|$ and checks whether TID_k exists in the database or not. If both conditions are true, CS computes $[\text{PID}_k, R_{\text{and}_2}] = D_{H(\text{MSK})}[X_k]$, $A_k' = H(\text{PID}_k \| \text{MSK} \| R_{\text{and}_2})$, $J_k' = H(A_k' \| T_k)$, and $R_{\text{and}_4} = R_{\text{and}_4}^+ \oplus J_k'$ and checks the condition $Z_k \stackrel{?}{=} H(A_k' \| \text{TID}_k \| R_{\text{and}_4} \| T_k)$. If false, the process exits; else, the next step is executed.

LAU 4: CS picks $R_{\text{new}}, R_{\text{and}_5}, \text{TID}_k^{\text{new}}$, further computes $\text{TID}_l = \text{TID}_l^+ \oplus J_k', \text{KEY}_{\text{cs},l}^+ = H(H(\text{MSK}) \| X_l)$, $W_{\text{cs}} = H(R_{\text{and}_4} \| \text{PID}_k \| H(\text{TID}_k \| \text{TID}_k^{\text{new}}) \| A_k)$, $Z_{\text{cs}} = H(\text{KEY}_{\text{cs},l}^+ \| R_{\text{and}_5} \| T_{\text{cs}})$, $\text{TID}_k^+ = \text{TID}_k^{\text{new}} \oplus J_k', W_{\text{cs}}^+ = W_{\text{cs}} \oplus \text{KEY}_{\text{cs},l}^+$, $R_{\text{and}_5}^+ = R_{\text{and}_5} \oplus \text{KEY}_{\text{cs},l}^+, \overline{A_k} = H(\text{PID}_k \| \text{MSK} \| R_{\text{new}}) \oplus J_k'$, and $\overline{X_k} = E_{H(\text{MSK})}[\text{PID}_k, \overline{A_k}, R_{\text{new}}] \oplus J_k'$, and replaces TID_k with $\text{TID}_k^{\text{new}}$. CS finally transmits the message containing $\text{MSG}_2 = \langle W_{\text{cs}}^+, \overline{A_k}, \overline{X_k}, Z_{\text{cs}}, R_{\text{and}_5}^+, \text{TID}_k^+, \text{TID}_l, T_{\text{cs}} \rangle$ to DR_l via the insecure channel.

LAU 5: upon receiving MSG_2 from CS, DR_l first checks the freshness of the message by examining the condition $|\text{TC} - T_{\text{cs}} \le \delta T|$ and checks whether TID_l received is the same as saved in DR_l's memory. If both conditions are true, DR_l computes $R_{\text{and}_5} = R_{\text{and}_5}^+ \oplus \text{KEY}_{\text{cs},l}$ and checks the condition $Z_{\text{cs}} \stackrel{?}{=} H(\text{KEY}_{\text{cs},l} \| R_{\text{and}_5} \| T_{\text{cs}})$.

LAU 6: if true, SR_l selects the present timestamp T_l and R_{and_6} and further computes $W_{\text{cs}} = W_{\text{cs}}^+ \oplus \text{KEY}_{\text{cs},l}, R_{\text{and}_6}^+ = R_{\text{and}_6} \oplus W_{\text{cs}}, \text{SK}_{lk} = H(R_{\text{and}_6} \| W_{\text{cs}})$, and $\text{Auth}_l = H(\text{SK}_{lk} \| \text{TID}_l \| T_l)$. DR_l finally transmits the message containing $\text{MSG}_3 = \langle \overline{A_k}, \overline{X_k}, R_{\text{and}_6}^+, \text{Auth}_l, \text{TID}_k^+, T_l \rangle$ to U_k via the insecure channel.

LAU 7: upon receiving MSG_3 from DR_l, MD_k first checks the freshness of the message by examining the condition $|\text{TC} - T_l \le \delta T|$. If true, MD_k computes $\text{TID}_k^{\text{new}} = \text{TID}_k^+ \oplus J_k, W_{\text{cs}}' = H(R_{\text{and}_4} \| \text{PID}_k \| H(\text{TID}_k \| \text{TID}_k^{\text{new}}) \| A_k)$, and $R_{\text{and}_6} = R_{\text{and}_6}^+ \oplus W_{\text{cs}}', \text{SK}_{kl} = H(R_{\text{and}_6} \| W_{\text{cs}}')$ and examines the condition $\text{Auth}_l \stackrel{?}{=} H(\text{SK}_{kl} \| \text{TID}_l \| T_l)$. If true, $\text{SK}_{kl} (= \text{SK}_{lk})$ is used as a session key to secure the communication and the next step is executed; else, the process terminates.

LAU 8: finally, MD_k replaces the parameters $\text{TID}_k^+, A_k^+, X_k^+$ with $\text{TID}_K'^{\text{new}}, A_K^{\text{new}}, X_K^{\text{new}}$, where $\text{TID}'_K{}^{\text{new}} = \text{TID}_k^{\text{new}} \oplus V_k', A_k^{\text{new}} = \overline{A_k} \oplus J_k \oplus V_k'$, and $X_k^{\text{new}} = \overline{X_k} \oplus J_k \oplus V_k'$.

2.4. TC-PSLAP: Password Update Process. If a user wants to update his/her password, he/she can do this without the involvement of the control server by adopting the subsequent procedure:

(1) First, the user needs to get verified by adopting the procedure as described in Section 2.3

(2) After successful verification, U_k will be prompted to provide a new password $\text{PWD}_k^{\text{new}}$

(3) Next, MD_k will compute $V_k^{\text{new}} = H(\text{PWD}_k^{\text{old}} \| R_{\text{and}_1})$, $\text{AUTH}_k^{\text{new}} = H(\text{PID}_k \| \text{PWD}_k^{\text{new}} \| R_{\text{and}_1})$, $X_k^{\text{new}} = X_k^+ \oplus V_k$, $A_k^+ = A_k \oplus V_k$, $\text{ID}_k^+ = \text{TID}_k \oplus V_k$, and $R_{\text{and}_1}^+ = R_{\text{and}_1} \oplus H(\text{PID}_k \| \text{PWD}_k)$

3. Security Analysis: TC-PSLAP

In this section, automated formal security analysis and informal security analysis of the introduced scheme have been presented.

3.1. Informal Analysis. The subsequent sections explore and explain that our TC-PSLAP scheme provides robustness for the known vulnerabilities.

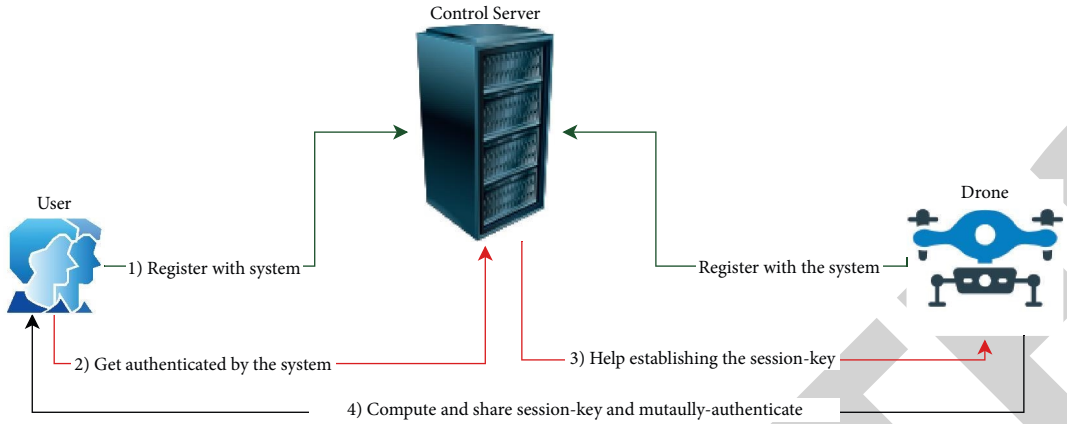

Figure 3: Working of the proposed TC-PSLAP architecture.

3.1.1. Mutual Authentication. In the proposed TC-PSLAP, all of the entities involved in the communication authenticate one another before proceeding with the process. CS receives MSG_1 from U_i and authenticates it by examining $Z_k \stackrel{?}{=} H(A_k' \| \text{TID}_k \| R_{\text{and}_4} \| T_k)$. DR_l also verifies the authenticity of CS by examining the condition $Z_{\text{cs}} \stackrel{?}{=} H(\text{KEY}_{\text{cs},l} \| R_{\text{and}_5} \| T_{\text{cs}})$. Upon receiving the message from DR_l, U_k also authenticates the drone by examining the condition $\text{AUTH}_l \stackrel{?}{=} H(\text{SK}_{kl} \| \text{TID}_l \| T_l)$. Hence, the scheme successfully achieves the mutual authentication.

3.1.2. Anonymity and Traceability. To render anonymity, the identities of the entities involved in the communication are not shared over the public channel. All of the identities are concealed and temporal, and pseudo-identities are used to communicate. So, the scheme provides pseudo-anonymity. Also, the presence of timestamps $\{T_k, T_{\text{cs}}, T_l\}$ and arbitrary numbers $\{R_{\text{and}_4}, R_{\text{and}_5}, R_{\text{and}_6}\}$ in messages $\{\text{MSG}_1, \text{MSG}_2, \text{MSG}_3\}$ makes the scheme untraceable as these parameters are updated in each session. Hence, the proposed scheme renders anonymity and traceability.

3.1.3. Perfect Forward Secrecy. In the proposed TC-PSLAP, both long- and short-term secrets are incorporated to yield the perfect forward secrecy. Suppose an adversary $\mathcal{A}$ had the knowledge of short-term secrets $\{R_{\text{and}_4}, R_{\text{and}_5}, R_{\text{and}_6}, \text{TID}_k\}$, but he/she also requires long-term secrets $\{\text{PID}_k, A_k\}$ in order to compute the session key. Therefore, the TC-PSLAP supports perfect forward secrecy.

3.1.4. Stolen Verifier Attack. In the TC-PSLAP, the parameters $\{\text{TID}_k\}$ and $\{\text{TID}_l, X_l\}$ are stored in the database of the CS. Now, if a privileged insider has access to these parameters, he/she cannot employ these parameters in any way to compromise the security of the system. TID_k changes after each session, TID_l is not employed to compute anything, and X_l is also a hash digest. Therefore, the TC-PSLAP can successfully defend against stolen verifier attacks.

3.1.5. Stolen Mobile Device and Drone Attack. Assume that a legal user U_k has lost his/her mobile device or it is stolen by the adversary. Now, through power analysis, $\mathcal{A}$ can extract the parameters $\{\text{AUTH}_k, X_k^+, A_k^+, \text{TID}_k^+, R_{\text{and}_1}^+\}$ from MD_k. None of these parameters reveal any information about the user or the system. Also, all of these parameters are encrypted with the help of XOR. Now, $\mathcal{A}$ can also extract the parameters stored in the drone which are $\{\text{ID}_{\text{DR}_l}, \text{TID}_l, \text{KEY}_{\text{cs},l}\}$. None of these parameters can be used to compute the session key as this also requires short-term and other long-term secrets. Therefore, it can withstand the stolen mobile device and drone attack.

3.1.6. Reply Attack. In the TC-PSLAP, timestamp is employed to prevent $\mathcal{A}$ from launching the reply attack. In the messages $\{\text{MSG}_1, \text{MSG}_2, \text{MSG}_3\}$, timestamp is sent openly and is also hashed with other parameters. Now, if $\mathcal{A}$ replaces the old timestamp in any of these messages and retransmits the messages, still he/she would not be able to successfully get authenticated due to the usage of a timestamp in other parameters. Hence, the scheme is secure against reply attacks.

3.1.7. Known Session Key Attack. In the TC-PSLAP, the session key is computed by employing the parameters $\{R_{\text{and}_4}, R_{\text{and}_6}, \text{PID}_k, A_k\}$. Now, if $\mathcal{A}$ has the information of an old session key, he/she cannot obtain any other session-specific key as the parameters employed in producing the session key are novel in each session. So, the TC-PSLAP can bear the known session key attack.

3.1.8. User Impersonation Attack. $\mathcal{A}$ may try to impersonate as a legal user U_k. To impersonate as U_k, $\mathcal{A}$ needs A_k, which is $A_k = H(\text{PID}_k \| \text{MSK} \| R_{\text{and}_2})$. Now, A_k is also session-specific and is updated after each session. And MSK is the private master key of CS, which is inaccessible to $\mathcal{A}$. Hence, it is not feasible for $\mathcal{A}$ to impersonate as a legal user U_k.

3.1.9. Drone Impersonation Attack. U_k authenticates DR_l by examining the condition $\text{AUTH}_l = H(\text{SK}_{lk} \| \text{TID}_l \| T_l)$. Now, to impersonate as DR_l, $\mathcal{A}$ requires the knowledge of

Figure 4: TC-PSLAP: login and authentication process.

$\{R_{\text{and}_6}, W_{\text{cs}}\}$, where W_{cs} contains A_k which further contains the private master key of CS and is not accessible by $\mathscr{A}$. Hence, the scheme can withstand the drone impersonation attack.

3.2. Formal Security Proof Using the BAN Logic. In this section, the TC-PSLAP is tested for robustness under the formal BAN logic.

3.2.1. Postulates. Table 2 shows the postulates and corresponding purposes. In addition, Table 3 shows notations used in the BAN logic and corresponding descriptions.

3.2.2. Establishing the Security Goal. Following are the security goals for the TC-PSLAP under the BAN logic: G_1: $U_k \mid \equiv \text{DR}_l \mid \equiv U_k \overset{\text{SK}}{\longleftrightarrow} \text{DR}_l$.

3.2.3. Messages' Generic Form. Following is the generalized form of the TC-PSLAP:

MSG_0: $U_i \rightarrow \text{CS}$: $(X_k^+ \oplus V_k', H(A_k \| \text{TID}_k \| R_{\text{and}_4} \| T_k), R_{\text{and}_4} \oplus J_k, \text{TID}_k, \text{TID}_l \oplus J_k, T_k)$, MSG_1: $\text{CS} \rightarrow \text{DR}_l$: $(W_{\text{cs}} \oplus \text{KEY}_{\text{CS},l}, H(\text{PID}_k \| \text{MSK} \| R_{\text{new}}) \oplus J_k', E_{H_{\text{key}}}[\text{PID}_k, \overline{A_k}, R_{\text{new}}] \oplus J_k', H(\text{KEY}_{\text{cs},l}^+ \| R_{\text{and}_5} \| T_{\text{cs}}), R_{\text{and}_5} \oplus \text{KEY}_{\text{CS},l}^+, \text{TID}_k^{\text{new}} \oplus J_k', \text{TID}_l, T_{\text{cs}})$, MSG_2: $\text{DR}_l \rightarrow U_k$: $(H(\text{PID}_k \| \text{MSK} \| R_{\text{new}}) \oplus J_k', E_{H_{\text{key}}}[\text{PID}_k, \overline{A_k}, R_{\text{new}}] \oplus J_k', R_{\text{and}_6} \oplus W_{\text{cs}}, H(\text{SK}_{lk} \| \text{TID}_l \| T_l), \text{TID}_k \oplus J_k', T_l)$.

3.2.4. Messages' Idealized Form. The idealized form of messages in our TC-PSLAP is given in the following.

MSG_0: $U_k \rightarrow \text{CS}$: $(\langle X_k \rangle_{V_k'}, \langle \text{CS} \overset{A_k}{\leftrightarrow} U_k, \text{CS} \overset{\text{TID}_k}{\leftrightarrow} U_k, T_k \rangle_{R_{\text{and}_4}}, \langle R_{\text{and}_4} \rangle_{\text{CS} \overset{J_k}{\leftrightarrow} U_k}, \langle \text{CS} \overset{\text{TID}_l}{\leftrightarrow} \text{DR}_l \rangle_{\text{CS} \overset{U_k}{\leftrightarrow} U_k}, \text{CS} \overset{\text{TID}_k}{\leftrightarrow} U_k, T_k)$ MSG_1: $\text{CS} \rightarrow \text{DR}_l$: $(\langle W_{\text{cs}} \rangle_{\text{CS} \overset{\text{Key}_{\text{cs},l}}{\leftrightarrow} \text{DR}_l}, \langle \text{CS} \overset{\text{PID}_k}{\leftrightarrow} U_k, \text{MSK}, R_{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\leftrightarrow} U_k}, \langle \{\text{CS} \overset{\text{PID}_k}{\leftrightarrow} U_k, \overline{A_k}, R_{\text{new}}\}_{\text{key}} \rangle_{J_k'}, \langle \text{KEY}_{\text{cs},l}^+, T_{\text{cs}} \rangle_{R_{\text{and}_5}}, \langle \text{KEY}_{\text{cs},l}^+ \rangle_{R_{\text{and}_5}}, \langle \text{TID}_k^{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\leftrightarrow} U_k}, \text{CS} \overset{\text{TID}_l}{\leftrightarrow} \text{DR}_l, T_{\text{cs}})$ MSG_2: $\text{DR}_l \rightarrow U_k$: $(\langle \text{CS} \overset{\text{PID}_k}{\leftrightarrow} U_k, \text{MSK}, R_{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\leftrightarrow} U_k}, \{\text{CS} \overset{\text{PID}_k}{\leftrightarrow} U_k, \overline{A_k}, R_{\text{new}}\}_{\text{key}} \rangle_{\text{CS} \overset{J_k'}{\leftrightarrow} U_k}, \langle W_{\text{cs}} \rangle_{R_{\text{and}_6}}, \langle \text{SK}_{lu}, U_k \overset{\text{TID}_l}{\leftrightarrow} \text{DR}_l, T_l \rangle, \langle \text{TID}_k^{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\leftrightarrow} U_k}, T_l)$.

3.2.5. Assumptions.

$$
\begin{aligned}
A_1&: \text{CS}| \equiv \#\left(R_{\text{and}_4}, T_k\right),\\
A_2U_k&| \equiv \#\left(R_{\text{new}}, R_{\text{and}_5}, T_l\right),\\
A_3&: \text{DR}_l| \equiv \#\left(R_{\text{and}_6}, T_{\text{cs}}\right),\\
A_4&: U_k| \equiv \text{DR}_l| \Rightarrow \text{DR}_l| \sim X,\\
A_5&: U_k| \equiv \text{DR}_l| \Rightarrow \left(U_k \overset{\text{SK}_{lu}}{\longleftrightarrow} \text{DR}_l\right),\\
A_6&: \text{DR}_l| \equiv \text{CS}| \Rightarrow \text{CS}| \sim X,\\
A_7&: U_k| \equiv \left(U_k \overset{\text{TID}_l}{\longleftrightarrow} \text{DR}_l\right),\\
A_8&: \text{CS}| \equiv \left(\text{CS} \overset{\text{TID}_l}{\longleftrightarrow} \text{DR}_l\right),\\
A_9&: U_k| \equiv \text{CS}| \equiv \left(U_k \overset{J_k}{\longleftrightarrow} \text{CS}\right),\\
A_10&: U_k| \equiv \text{CS}| \equiv \left(U_k \overset{A_k}{\longleftrightarrow} \text{CS}\right),\\
A_{11}&: U_k| \equiv \left(U_k \overset{\text{PID}_k}{\longleftrightarrow} \text{CS}\right),\\
A_{12}&: \text{DR}_l| \equiv \left(\text{CS} \overset{\text{TID}_l}{\longleftrightarrow} \text{DR}_l\right).
\end{aligned}
\tag{1}
$$

The mutual authentication between U_k and DR_l is proved using the following steps:

S_1: from MSG_2, we get $U_k \triangleleft \langle \text{CS} \overset{\text{PID}_k}{\longleftrightarrow} U_k, \text{MSK}, R_{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\longleftrightarrow} U_k}$, $\{\text{CS} \overset{\text{PID}_k}{\longleftrightarrow} U_k, \overline{A_k}, R_{\text{new}}\}_{\text{key}} \rangle_{\text{CS} \overset{J_k'}{\longleftrightarrow} U_k}$, $\langle W_{\text{cs}} \rangle_{R_{\text{and}_6}}$, $\langle \text{SK}_{lu}, U_k \overset{\text{TID}_l}{\longleftrightarrow} \text{DR}_l, T_l \rangle$, $\langle \text{TID}_k^{\text{new}} \rangle_{\text{CS} \overset{J_k'}{\longleftrightarrow} U_k}, T_l$ S_2: based on S_1, assumptions A_1, A_2, A_3, and message-meaning rule, we get $U_k \triangleleft \langle \text{MSK}, R_{\text{new}} \rangle, \{\overline{A_k}, R_{\text{new}}\}_{\text{key}}, \langle W_{\text{cs}} \rangle$

Table 2: BAN logic: postulates.

Rule	Description
$A\mid \equiv A\overset{K}{\longleftrightarrow}B, A\triangleleft\langle X\rangle_K/A\mid \equiv Y\mid \sim K$	Message-meaning rule
$A\mid \equiv \#\{X\}, A\mid \equiv B\mid \sim X/A\mid \equiv B\mid \equiv X$	Nonce verification rule
$A\mid \equiv B, A\mid \equiv C/A\mid \equiv (B,C)$	Acceptance conjunction
$A\mid \equiv B\mid \equiv (X,Y)/A\mid \equiv B\mid \equiv X$	Belief rule
$A\mid \equiv \#X/A\mid \equiv \#(X,Y)$	Fresh conjuncatenation rule
$A\mid \equiv B\mid \equiv X, A\mid \equiv B\mid \Rightarrow X/A\mid \equiv X$	Jurisdiction rule
$A\mid \equiv \#\{X\}, A\mid \equiv B\mid \equiv X/A\mid \equiv A\overset{K}{\longleftrightarrow}B$	Session key

Table 3: BAN logic: notations.

Notation	Explanation
$A\mid \overset{\equiv}{K} B$	A believes statement B
$A\overset{K}{\longleftrightarrow}Y$	Share a key K between A and Y
$\#B$	B is fresh
$A\triangleleft B$	A sees B
$A\mid \sim B$	A said B
$(B,C)_K$	B,C are hashed by key K
$\{B\}_K$	B is hashed with key K
$\langle B\rangle_K$	B is encrypted with key K

$_{R_{\text{and}_6}}, \langle \text{SK}_{lu}, T_l\rangle$, $\langle \text{TID}_k^{\text{new}}\rangle, T_l\, S_3$: based on S_2 and the message belief rule, we get $U_k\mid \equiv U_k\triangleleft \langle \text{MSK}, R_{\text{new}}\rangle, \{\overline{A_k}, R_{\text{new}}\}, \langle W_{\text{cs}}\rangle_{R_{\text{and}_6}}, \langle \text{SK}_{lu}, T_l\rangle$, $\langle \text{TID}_k^{\text{new}}\rangle$, $T_l\, S_4$: based on S_3, nonce verification, and freshness rule, we get $U_k\mid \equiv \text{DR}_l\mid \equiv \langle \text{MSK}, R_{\text{new}}\rangle, \{\overline{A_k}, R_{\text{new}}\}$, $\langle W_{\text{cs}}\rangle_{R_{\text{and}_6}}$, $\langle \text{SK}_{lu}\rangle, \langle \text{TID}_k^{\text{new}}\rangle\, S_5$: based on S_4, assumption A_4, and jurisdiction rule, we get $U_k\mid \equiv \langle \text{MSK}, R_{\text{new}}\rangle, \{\overline{A_k}, R_{\text{new}}\}$, $\langle W_{\text{cs}}\rangle_{R_{\text{and}_6}}, \langle \text{SK}_{lu}\rangle, \langle \text{TID}_k^{\text{new}}\rangle\, S_6$: based on S_4, S_5, assumption A_4, A_5, A_9, and belief rule, we get $U_k\mid \equiv \text{DR}_l\mid \equiv U_k\overset{\text{SK}_{lu}}{\longleftrightarrow}\text{DR}_l$

4. The Comparisons

This section explains the comparisons of the introduced TC-PSLAP with existing protocols introduced in [15, 16, 20, 24].

4.1. Functionality Comparison. Functionality comparison amongst introduced and related protocols is depicted in Table 4. It is evident from Table 4 that the introduced protocol renders superior security in contrast to [20] and also renders more enhanced security features as contrasted to other related protocols. √ tells if a particular feature exists or protocol can resist an attack, × tells if a protocol lacks a particular feature or cannot resist an attack, whereas – means that a particular feature/security requirement is not applicable.

4.2. Computation Analysis. For comparing computation costs of different protocols, the results, as computed in [26], are adopted. The notations pertaining to several cryptographic operations and their running times are briefed in Table 5.

As depicted in Table 6 and Figure 5, the computation cost of the introduced TC-PSLAP is less than all the competing schemes [15, 16, 20, 24], and it completes the authentication process in approximately 0.149 ms, whereas the scheme of Zhang et al. [15] completes the same in approximately 0.160 ms. The schemes of Kirsal Ever [16], Nikooghadam et al.

Table 4: Comparison of functionality features.

Requirements	[15]	[16]	[20]	[25]	[24]	Ours
Perfect forward secrecy	×	×	√	√	√	√
Anonymity	√	√	√	×	×	√
Stolen verifier attack	×	√	×	√	√	√
Replay attack	√	√	×	√	–	√
User impersonation attack	√	√	×	×	√	√
Drone impersonation attack	√	√	×	×	×	√
Man-in-the-middle attack	√	√	×	×	√	√
Insider attack	×	×	×	×	√	√
Session key agreement	×	√	√	√	√	√
Formal verification	√	√	√	×	√	√
Mutual authentication	×	√	×	×	√	√
Control server impersonation attack	√	√	×	√	√	√
Stolen mobile device/smart card attack	×	√	×	–	√	√
Untraceability	√	√	×	–	√	√
Drone/device capture attack	√	√	√	√	√	√
DoS attack	√	√	×	√	√	√
Forgery attack	√	√	×	√	√	√
Secret leakage	√	√	×	×	√	√

Table 5: Experimental computation results.

↓ Entity/operation ⟶	T_h	T_{ecm}	T_{eca}	T_{sed}	T_{bp}
User	0.009	5.116	0.013	0.017	17.36
Drone	0.006	4.107	0.018	0.013	12.52
Control station	0.004	0.926	0.006	0.008	4.038

Time is computed in milliseconds; TTC: time to compute; T_h: TTC hash operation; T_{ecm}: TTC point multiplication on ECC; T_{eca}: TTC point addition on ECC; T_{sed}: TTC block cipher operation; T_{bp}: TTC pairing operation; $T_{\text{fe}} \approx T_{\text{ecm}}$: TTC fuzzy extractor.

Table 6: Performance comparison.

Protocol	User	CS	Drone	RT	C_1	C_2
Zhang et al. [15]	$10T_h$	$7T_h$	$7T_h$	0.160	3	1472
Kirsal Ever [16]	$5T_h + 2T_{bp}$	$9T_h + 2T_{bp} + 4T_{ecm}$	$3T_h + 2T_{bp}$	71.639	3	1952
Nikooghadam et al. [20]	$9T_h + 2T_{ecm}$	$2T_h + 1T_{ecm}$	$3T_h + 2T_{ecm}$	19.479	3	2336
Malani et al. [24]	$8T_h + 7T_{ecm} + 3T_{eca}$	–	$8T_h + 7T_{ecm} + 3T_{eca}$	64.774	2	2783
Ours	$9T_h$	$10T_h + 2T_{sed}$	$3T_h$	0.149	3	2783

RT: running time in ms; C_1: number of exchange messages; C_2: bits exchanged.

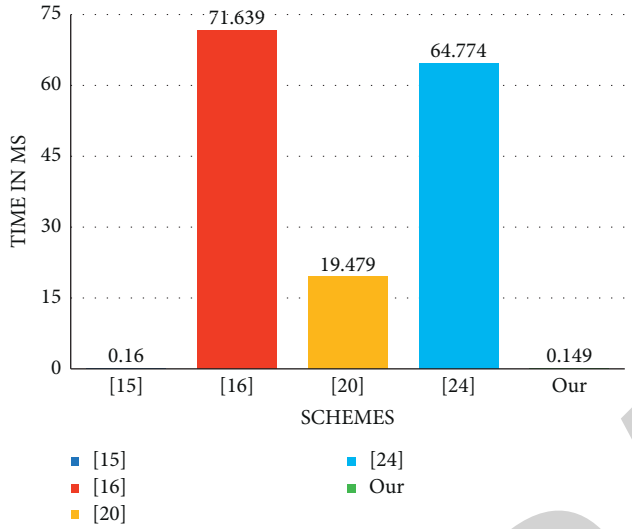

Figure 5: Computation cost comparison.

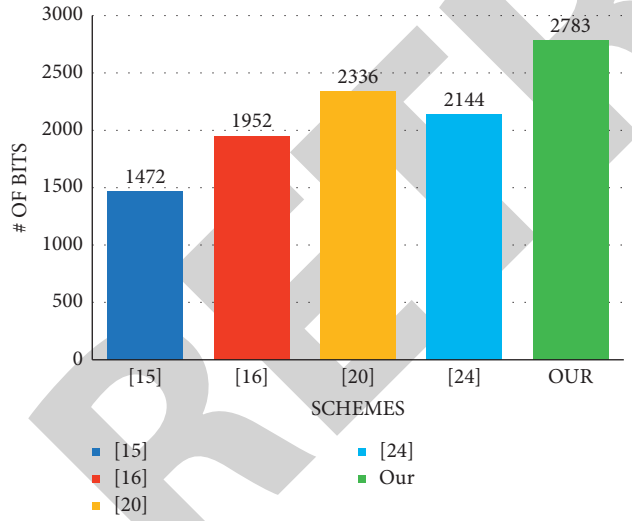

Figure 6: Communication cost comparison.

[20], and Malani et al. [24] complete the same in 0.160, 19.479, and 64.774 ms, respectively. Hence, our introduced protocol is more lightweight and provides better security as compared to the rest of the protocols, as shown in Table 4.

4.3. Communication Analysis. The communication expense estimate is represented in Table 6. For comparison, identities are considered as 160 bits of length, the size of a timestamp is taken as 32 bits, a hash output of SHA-1 is 160 bits, the size of a random number is assumed 160 bits long, and the block size of symmetric enc/decryption is 128 bits, respectively. The communication cost of various protocols is also shown in Figure 6. The introduced TC-PSLAP exchanges 2783 bits for the completion of the login and authentication phase. Table 6 and Figure 6 explain that the communication cost of the introduced TC-PSLAP is a bit higher than that of the compared protocols [15, 16, 20, 24], but the introduced TC-PSLAP offers better security than remaining protocols.

5. Conclusion

The IoT-enabled drones can be utilized efficiently for surveillance and related tasks in urban areas. However, the privacy and security issues related to drone operations are expanding as their adaption surges. In this article, we initiated a lightweight authentication protocol TC-PSLAP for secure drone communication. The introduced TC-PSLAP, while preserving the lightweight property of symmetric cryptography, defies the related known attacks, which is confirmed through security analysis and comparisons of the security and performance of our TC-PSLAP with related schemes.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This project was funded by the Deanship of Scientific and Research (DSR) at King Abdulaziz University, Jeddah under grant no. RG-3-611-41. The authors, therefore, acknowledge with thanks DSR for the technical and financial support.

References

[1] C. P. Szabo, "Urbanization and mental health," *Current Opinion in Psychiatry*, vol. 31, no. 3, pp. 256-257, 2018.

[2] R. Rani, V. Kashyap, and M. Khurana, "Role of IoT-cloud ecosystem in smart cities : review and challenges," *Materials Today: Proceedings*, 2020.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[4] M. Nikooghadam, H. Amintoosi, and S. Kumari, "A provably secure ECC-based roaming authentication scheme for global mobility networks," *Journal of Information Security and Applications*, vol. 54, Article ID 102588, 2020.

[5] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and internet of things for improving smartness of smart cities," *IEEE Access*, vol. 7, Article ID 128125, 2019.

[6] 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.

[7] J.-P. Yaacoub, N. Hassan, O. Salman, and C. Ali, "Security analysis of drones systems: attacks, limitations, and recommendations," *Internet of Things*, vol. 11, Article ID 100218, 2020.

[8] Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in UAV-aided 5g and beyond communications: a survey," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 3, pp. 872–891, 2020.

[9] F. Al-Turjman, M. Abujubbeh, A. Malekloo, and L. Mostarda, "UAVs assessment in software-defined IoT networks: an overview," *Computer Communications*, vol. 150, pp. 519–536, 2020.

[10] F. Mohammed, I. Ahmed, N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "UAVs for smart cities: opportunities and challenges," in *Proceedings of the 2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, Orlando, FL, USA, May 2014.

[11] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*, pp. 3–32, Springer Netherlands, New York USA, 2012.

[12] F. Al-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, pp. 24617–24631, 2017.

[13] Y. Kirsal Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 456–467, 2019.

[14] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. K. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *Journal of Information Security and Applications*, vol. 52, Article ID 102502, 2020.

[15] 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.

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

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

[18] L. Chen, S. Qian, M. Lim, and S. Wang, "An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems," *China Communications*, vol. 15, no. 5, pp. 61–76, 2018.

[19] J. Srinivas, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and 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] M. Nikooghadam, S. K. Haleh Amintoosi, 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.

[21] C. Ran and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proceedings of the International conference on the theory and applications of cryptographic techniques*, pp. 453–474, Springer, Innsbruck, Austria, May 2001.

[22] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.

[23] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, W. Xiao, M. Chen, and A. Al-Barakati, "ILAS-IoT: an improved and lightweight authentication scheme for IoT deployment," *Journal of Ambient Intelligence and Humanized Computing*, 2020.

[24] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9762–9773, 2019.

[25] J. Singh, A. Gimekar, and S. Venkatesan, "An efficient lightweight authentication scheme for human-centered industrial internet of things," *International Journal of Communication Systems*, p. e4189, 2019.

[26] 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.