A physical capture resistant authentication scheme for Internet of Drones

Shehzad Ashraf Chaudhry, Jamel Nebhen, Azeem Irshad, Ali Kashif Bashir, Rupak Kharel, Keping Yu, Yousaf Bin Zikria

***Abstract*—The internet of drones (IoD) can encompass many essential services, including surveillance and emergencies/rescue operations. While IoD is getting popular and is witnessing a rapid usage increase, privacy and security are the main concerns of avoiding leakage of critical information and/or denial of services by a single drone or whole IoD network. In addition to traditional privacy cum security issues, the physical capturing of a single drone can severely impact the entire IoD network. This article provides an overview of the security challenges and requirements for IoD environments in addition to a discussion related to IoD communication/security standards. Moreover, this article proposes a novel scheme for securing IoD, specifically, from drone physical capturing and related attacks.**

***Index Terms*—Authentication, Drone capture attack, Smart City security , IoT security, Key-agreement, Internet of Drones.**

I. Introduction

THE Internet of Drones (IoD) is a novel paradigm in wireless networks that employs the Internet of Things (IoT)-based technology to accomplish its different critical ventures. The Unmanned Aerial Vehicles (UAVs) or drones acting as the flying IoT-based sensing objects have found their widespread application in diverse nature of domains due to their flexibility and economy [1]. UAVs' notable applications encompass disaster and rescue management, security surveillance systems, smart transport-based systems, package delivery and distribution, environment monitoring systems, aerial monitoring, medical emergency services, agriculture, real-time object recognition, and tracking, etc. The drones The IoD being the synthesis of IoT domain as well as smart drones technology, embodies a layered network control architecture that is specifically designed for controlling the airspace and establishing coordination among the drones. In general, drones can enhance convenience, network coverage, energy efficiencies, reliability, and real-time or liveness factor in various services. The drones can be controlled remotely either by a human or based on autonomous learning through the environment. In the past decade, the IoT-based technology has been nearly integrated into each conventional application with promising results [2]–[5]. Owing to IoT integration, the physical systems have been able to communicate with computer systems, and therefore could be managed reliably with less operational cost [6].

The Fig. 1 depicts a high-level pictorial representation of IoD architecture, which describes IoD as an interconnection of Ground Service Station (GSS) as well as smart drones deployed into the airspace of the system. According to the recent forecasts, on account of the increasing number of applications for commercial drones, there will be more than 100 billion USD market share for drones in the near future. A drone, being a crucial element of IoD, collects the data from any particular Fly Zone (FZ) and submits that data to GS. These drones are equipped with high-vision cameras, IoT sensors with limited memory, power, and less computational capabilities, GPS receivers for delivering diverse high altitude services, and a communication module to transmit the collected information towards respective GSS. The cost-efficient operational solutions, including UAVs control and monitoring, localization, trajectory setting, authenticated key agreement, security, and privacy, are the main requirements for successfully implementing IoD networks. Despite many advancements in UAVs communication systems, authentication, security, and privacy in IoD networks are still a significant problem [1], [7]. The drones may be physically compromised and examined by adversaries. The communication nature among the entities is wireless in nature, which exposes the drones to physical attacks leading to exposure of stored secrets in its memory. The IoD networks, being resource-constrained in memory, power, and computational capabilities, need to devise an efficient Authentication inevitably and Key Establishment (AKE) protocol [8]–[10] through employing low-cost cryptographic encryption/decryption techniques and making the IoD operationally viable.

Security Challenges and Requirements in IoD

The IoD environment is mostly exposed to similar kinds of security threats as posed to other networks, notably Wireless Sensor Networks (WSN), Internet of Vehicles (IoV), and other IoT-based networks. In general, the drones in IoD networks are resource-constrained in terms of storage, power, and computation. In contrast, the induction of resource-deficient UAVs in safety critical applications or rescue operations may seriously undermine the mission's objectives. This emphasizes the need

S.A. Chaudhry is with Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey e-mail: (ashraf.shehzad.ch@gmail.com).

J. Nebhen is with Prince Sattam bin Abdulaziz University, College of Computer Engineering and Sciences, P.O. Box 151 Alkharj 11942, Saudi Arabia., e-mail: (j.nebhen@psau.edu.sa).

A. Irshad is with Department of Computer Science, International Islamic University, Islamabad, Pakistan, e-mail: (irshadazeem2@gmail.com).

A.K. Bashir is with Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom, e-mail: (dr.alikashif.b@ieee.org).

R. Kharel is with Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom, e-mail: (r.kharel@mmu.ac.uk).

K. Yu is with Global Information and Telecommunication Institute, Waseda University, Shinjuku, Tokyo, 169-8050, Japan , e-mail: (keping.yu@aoni.waseda.jp).

Y.B.Zikria (corresponding author) is with Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea, e-mail: (yousafbinzikria@ynu.ac.kr).

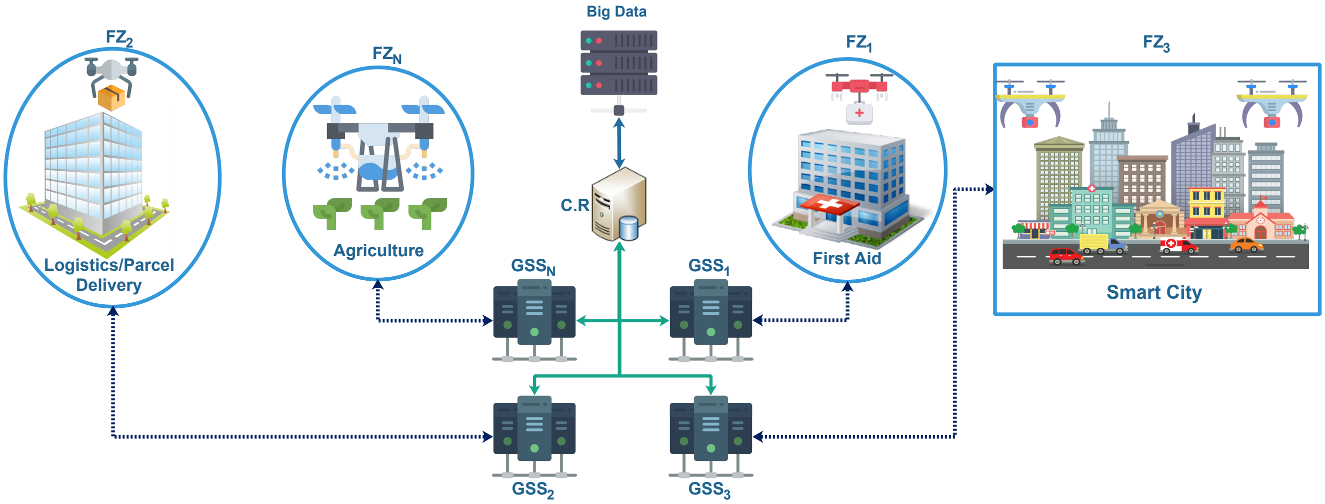

Figure 1: IoD Environment Monitoring System

for earnest efforts to devise more cost-effective authentication and key agreement solutions for the IoD ecosystem.

Challenges

Following are the main challenges in the IoD ecosystem includes:

- **Physical capture:** An adversary may access the infused secret information from the physical capturing of drones and smart device of user, and later attempt to corrupt other drones of the system or use the extracted information to deploy malicious drones in the system. Moreover, in the case of a stolen smart device of the user, the adversary can try to guess the password on an offline basis or attempt to impersonate the system's legal members.
- **Malicious interruption:** An adversary may attempt to impersonate the system's legal entities by altering the contents on real-time basis or injecting viruses into the system, which may lead to man-in-the-middle or denial of service threats.
- **Data Alteration:** An adversary may attempt to damage the rescue and critical operations' objectives by altering the communication on open public channels. The integrity of the communication messages is one of the major challenges to IoD networks.
- **Illegal Access:** Due to wireless communication, any unauthorized intruder may access the messages in the drone and user path. Then it could inject malicious codes to impersonate the legal entities of the system.

Requirements

To combat the security challenges, the Authentication and Key Agreement (AKA) in IoD networks must fulfill the following:

- **Mutual Authentication:** This ensures authorized access to the drone's services for the user. This feature bounds the entities to authenticate the other entities on both ends sharing the agreed session key. The ground station server (GSS), being resourceful in every manner, enables both participants as an intermediary to achieve this feature with the help of verification of participants with the employment of repository verifiers.
- **User Anonymity:** This feature is needed to protect the user's anonymity. The identity ID_i of the user must be embedded in such a way that it becomes unfeasible for the adversary to recover ID_i from the public messages. The exposure of identity may become an inconvenience for the user and lead to impersonation attacks and compromise untraceability objectives.
- **Untraceability Support:** If an IoD-based AKA scheme lacks untraceability feature, it might become uncomfortable for the user or damage the user's anonymity objective. Hence, the adversary must not be able to link different protocol sessions of the same user to assure untraceability.
- **Resistance against Physical Device Capture threat:** The drones cannot be monitored 24×7 in any flying zone, and there always remains a chance for drones to be captured physically by malicious attackers. Those attackers may recover the stored secret credentials from the drone's memory by exercising power analysis techniques. However, a sound AKA scheme in the IoD setting must warrant that if the adversary can compromise a drone, it should not compromise the security of non-compromised drones. Moreover, it must not be able to impersonate other drones after recovering the parameters of the compromised drone.
- **Resistance against Stolen Verifier's threat:** Suppose an adversary happens to steal the verifier secrets from the user's smart card. In that case, it must not be able to recover previously computed session keys between a user of the smart card device and the drone. The stolen verifiers may also lead to the user, GSS, and drone impersonation attack, which could be restrained already through protecting the verifiers.
- **Session key agreement:** For countering the forgery on

account of the adversary, the mutually agreed session key must be used to encrypt all communication messages following the authentication protocol.

- **Forward and Backward secrecy:** The underlying IoD AKA scheme must ensure to protect the forward as well as backward secrecy so that an adversary may not be able to access future and previous session keys in the IoD ecosystem, respectively.

Network Model

In IoD architecture, the Control Room (CR) serves as a trusted registration authority that registers all drones (DR_i) as well as Ground Station Servers (GSS) before deploying these entities into their assigned application domains. The GSS stores the received data safely. Besides, it also stores the key credentials related to the drone, flying zones, and users. In the IoD environment-based network model, the drone's airspace could be divided into several disjoint Fly Zones (FZs). In contrast, multiple drones may be deployed in any particular FZ for collecting real-time data and monitoring the airspace environment. The drone DR_i collects the real-time data or information from the deployed zone's surrounding environment and reports to their GSS.

Adversarial Model

This paper adopts the CK model, where the attacker $\mathcal{A}$ controls the wireless communication media and $\mathcal{A}$ is strong enough to listen, remove, alter and replay the messages exchanged among drones and between a drone and GSS. The $\mathcal{A}$ can expose the secret parameters stored in the memory of a captured drone. Under the standard CK model, the system identities are publicly announced. The drones' private keys and GSS cannot be revealed to any attacker, except for the captured drones.

IoD Standards for Security

When cooperate, the Unmanned Ariel vehicles (UAV)/drones form an adhoc communication infrastructure. The cooperating UAVs equipped with IoT-based sensing technology are the basis of the Internet of Drones (IoD). Ensuring communication security and safety are the main challenges for IoD. Among other security-related issues, the resistance to physical capturing of a drone has got much importance due to the network's dynamicity. Recently, some communication and security standards for UAVs are aroused. Here, we provide a brief discussion on the standards of UAVs.

IEEE P1920

The IEEE 1920.1 provides Ariel communication and networking standards for all categories of networks (Cellular, wireless, etc.). Moreover, IEEE 1920.1 can be applied over all types of air-crafts, including manned or drones, irrespective of network size and usage type (civilian, commercial, etc.). The V2V standard communication protocol is provided by IEEE 1920.2 stack. It extends inter-drone communication and is independent of line of sight and radio line of sight. The protocol IEEE 1920 also provides the security architecture for drones communications.

ISO 21384-3

Recently, in 2019, the ISO 21384-3 was announced to standardized the operational procedures of drones, also termed as Unmanned Aircraft Systems (UAS). The ISO 21384-3 provides the globally agreed standards for safe and secure commercial operations requirements.

3GPP Rel-17

The 3GPP provides a standard solution for Beyond the Line of Sight (BLoS) and Beyond Radio Line of Sight (BRLoS) communication for drones. The technical reports of 3GPP release 17 (3GPP Rel-17) provide the framework for inter-drone and drone to infrastructure communication through the inclusion of 3GPP, framed in the technical report TR 22.125. The Technical Report TR 22.829 provides standards for 5G inclusion in drone communication, while TR 23.755 provides application layer support. The 3GPP TR 23.754 was also released as part of 3GPP Rel-17 For inter-drone specification and drone to infrastructure communication and authorization and authentication.

ITU-T

The ITU-T Y.UAV.arch provides recommendations for drones and controllers architecture on IMT-2020 networks. It recommends the application, application support layers functionalities, and security capabilities, while ITU-T F.749.10 provides communication standards for civilian drones.

IoD:Authentication Schemes

This section focuses on the state-of-the-art authentication schemes for IoD networking. The solutions include both the symmetric key and public key infrastructure primitives and are briefly explained in the following subsections as well as depicted through Table I:

Srinivas et al.

The Srinivas et al. [11] suggested a three-factor authentication protocol "Temporal credential-based anonymous lightweight authentication scheme, called TCALAS" for IoD environment. The scheme comprises three participants, i.e., the trusted Ground Station Server (GSS), drone User (U_i), and Remote Drone (RD_j). The GSS enables establishing session key between U_i and RD_j on the public channel in a particular cluster. The drones are allocated to their respective flying zones called as clusters. A control room accompanies the GSS. U_i registers with GSS to access the services of RD_j. After the registration phase, the mutual authentication phase, password/biometric update phase, revocation and reissue phase, and dynamic remote drone addition phases are followed. After the successful login attempt using fuzzy extractor in the login and authentication phase, the U_i computes and forwards the message MSG_1 to GSS. The GSS checks the timestamp freshness and validates U_i. Then, U_i forwards the message MSG_2 to RD_j. Next, RD_j sends the message MSG3 to U_i directly using the public channel. If the U_i verifies the RD_j, it computes the session key SK, otherwise, it aborts the session. Although the Srinivas et al. was a lightweight authentication scheme, it could only be employed with drones assigned to a single cluster [13]. Those drones could never be deployed in more than one cluster since the authentication message MSG_1 in the suggested protocol does not bear any clue regarding the cluster identity. Hence, it does not support the GSS in any manner for identifying the user or the respective flying zone. Secondly, the Srinivas et al. scheme is prone to traceability attacks since the adversary may compute a user's computed factor HID_i for all sessions. Moreover, a privileged insider

Table I: Summary of Limitations/Drawbacks of Previous User Authentication Schemes in Internet of Drones Environment

Scheme	Year	Cryptographic Method used	Properties
Srinivas et al. [11]	2019	Symmetric key primitives	It is susceptible to impersonation attack based on stolen verifier, have traceability issue and scalability issue. Also, it lacks the feature of no clock synchronization.
Wazid et al. [12]	2019	Symmetric key primitives	It is susceptible to stolen-verifier, user and server impersonation attack, drone impersonation attack, Session key security leakage attack, server broadcasting, and traceability issues.
Ali et al. [13]	2020	Symmetric key primitives	It does not provide protection against node tampering attack and prone to cloning attack, lacks the feature of no clock synchronization.
Bera et al. [14]	2020	Elliptic curve cryptography	it lacks mutual authentication and traceability issues.
Zhang et al. [15]	2020	Symmetric key primitives	It lacks provision of perfect forward secrecy and susceptible to stolen-verifier and insider attacks. Session key agreement and mutual authentication are also missing.

$\mathcal{A}$ may approach the drone's verifier repository and initiate a GSS impersonation attack towards remote drone DR_i.

Wazid et al.

Wazid et al. [12] designed a novel lightweight remote user authentication and key agreement for the IoD environment. The Wazid et al. comprises four participating entities into the system, i.e., User (U_i), mobile device (MD_i), drone (DR_j), and server (S). The server acts as the trusted authority and registers all drones DR_j before deployment in the IoD environment. The server employs a symmetric bivariate polynomial over the Galois field to compute the pre-deployment factors. After pre-deployment and user registration phase, login and authentication phase, password and biometric updation phase, dynamic drone addition, and drone key management phase is followed. In the login and key agreement phase, the mobile device (MD_i) computes the message Msg1 after biometric verification using the fuzzy extractor function and sends it to the server. The server (S), after checking the timestamp, verifies the authenticity of MD_i. Then, it computes Msg2 and submits it to the DR_j using the public channel. The DR_j verifies the timestamp and validates the authenticity of both MD_i and server. Then, it computes the session key SK_{ij} as well as the message Msg3. The message Msg3 is forwarded to the mobile device MD_i for further verification. The user/MD_i checks the timestamp and computes the session key SK_{ij}. Then, it compares the computed messages against the received messages from the DR_j. Upon successful verification, it validates drone DR_j and finalizes the agreed session key SK_{ij}. However, there were two major drawbacks in the Wazid et al. scheme, i.e., In Wazid et al., any registered however unfair user may initiate a successful traceability attack against any legitimate user of the system. Moreover, it was vulnerable to stolen verifier attack in the hands of a privileged adversary who can initiate a successful user impersonation attack later on.

Ali et al.

Ali et al. [13] suggested a temporal credential-based anonymous lightweight authentication protocol for IoD after critically examining the Srinivas et al. scheme for the IoD environment. The scheme employed lightweight symmetric key crypto-primitives to present (iTCALAS) scheme. The system model includes three participating entities, i.e., mobile device user (MD_i), remote drones (RD_j), and ground station server (GSS). Ali et al.'s scheme comprise four phases: user registration phase, login, and authentication phase, user password and biometric modification phase, user revocation, re-registration phase, and dynamic drone addition phase. The MD_i submits the authentication request message MSG1 towards GSS in the login and authentication phase following the registration phase. Then, GSS after the verification of MD_i's authenticity computes and submits MSG2 towards RD_j. After checking the time stamp and verification of the MD_i and GSS, the latter calculates MSG3 and submits to MD_i. The MD_i, then verifies the authentication of both GSS and RD_j and constructs an agreed session key SK. Although the scheme of Ali et al. is a lightweight security solution, however, it is not protected against ephemeral secret leakage (ESL) attack.

Bera et al.

The Bera et al. [14] suggests a novel blockchain-based data delivery and collection (DDC) scheme for IoT-oriented 5G IoD environment. The scheme assumed well-synchronized clock timing across the system to help counter replay attacks. The system model for Bera et al. comprises five entities, namely Registration Authority (RA), Control Rooms (CRJ), Ground station servers (GSS_j), drones (DR_i), and blockchain center (BC). The RA, a trusted entity registers CRJ, and in return the CRJ registers GSS_j and DR_i entities. Then registered DR_i are assigned to their respective Flying Zones (FZj). The scheme includes the system initialization phase, registration phase, access control phase, secure DDC phase, block generation, verification, addition in BC phase, and dynamic addition of drones phase. The GSS_j collects data from DR_i and submits to GSS_j, which form the transaction blocks to add in its private BC center. After the registration process, the drones are allocated in their respective FZj. The mutual authentication procedure is followed to authenticate DR_i by the GSS_j . Mutual authentication utilizes elliptic curve cryptography (ECC) for signatures and verification of the certificate. Upon the successful execution procedure between DR_i and GSS_j , an agreed Session Key Verifier (SKV) is developed. However, one of the major drawbacks in Bera et al. is that in this scheme, the DR_i can never authenticate the GSS_j. This is because the former entity is unable to verify the signature as constructed by the GSS_j. The Bera et al. scheme is unable to impart anonymity to DR_i entity since the employed pseudo-identity remains the same in all initiated sessions and hence traceable by the adversary. Moreover, Bera et al. utilize the session nonces injudiciously since those nonces are serving no purpose in the protocol. The above limitations render the Bera et al. scheme inapplicable for practical implementation in the blockchain environment.

Zhang et al.

Zhang et al. [15] suggested an authentication protocol for IoD environment using lightweight symmetric key operations.

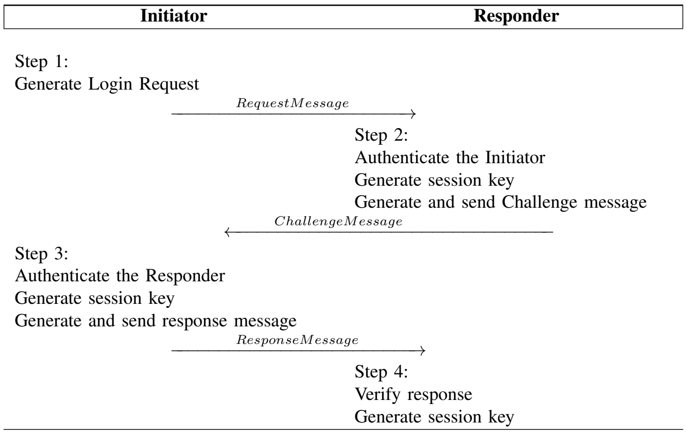

Figure 2: Proposed Framework

The network model comprises three participating entities, i.e., Control Server (CS), drones (V_j), and mobile Users (U_i). The CS acts as a trusted third party and registers all users as well as drones in the system by providing secret keys on the secure channel so that those entities get authenticated onwards during the mutual authentication phase to acquire the network services. Zhang et al. comprise three phases, i.e., setup phase, registration, and mutual authentication phase. The U_i computes the authentication request message in the mutual authentication phase after having input the user credentials and submits to CS. The CS, upon receiving the message, validates the timestamp and authenticity of U_i. Next, it computes another authentication message for drone V_j. The V_j authenticates both entities after comparing the computed parameters against the received message and submits the authentication response message towards U_i. The U_i, upon receiving the message from V_j verifies the computed factors against the received parameters. Upon a successful match, the session key SK_{ij} is finalized as a mutually agreed token between the participants and validates the drone for further proceedings. Otherwise, U_i simply terminates the session. One of the major drawbacks of the scheme of Zhang et al. is that it does not provide anonymity due to the usage of a generic parameter PID_s, which is hashed along with the current timestamp. The PID_s can be extracted from any stolen device or by a deceitful user, and the current timestamp can be taken from the request message. It can easily expose pseudo-identity PID_i of U_i, which remains the same for all sessions. Secondly, It requires a trusted intermediary to initialize and register the entities in the system. Moreover, the user is not verified correctly during the login phase, while the authentication request could be initiated towards CS even with the user's wrong password. Moreover, in the scheme of Zhang et al., the server stores verifier entry in its' database/table for each registered user, which can lead to the stolen verifier attack.

IoD Access control framework

The proposed IoD access control framework is built upon Elliptic Curve Cryptography (ECC) and symmetric hash functions. It works on the notion of public-private key pair of each entity and avoids bilinear pairings. It involves four types of entities: Certificate authority CA initializes the system and assigns public/private key pair to the rest of the entities, which includes Drone/s, user/s, and GSS/s. Initially, each participant (Drone/s, user, GSS) gets register with the CA and gets it public/private key of the form $Q_k = a_k P$, $s_k = h(ID_k, Q_k)s_{CA} + a_k$, where a_k is a randomly generated scalar. After getting the key pair, any two parties like user-GSS, user-drone, GSS-drone, and drone-drone can authenticate each other. This framework is generic, and any of the entities can be the initiator, and the entity on the other serves as a responder. Consisting of four-step, the initiator using its' private key and randomly generated number, computes and sends login requests. On receiving the request, the responding entity first verifies the timestamp freshness and authenticates the sender. Using its own private key, the responding entity computes and sends a challenge message to the initiator. On receiving the challenge message, the initiator first verifies the timestamp freshness and authenticates the responder. Upon successfully verifying both, the initiator computes the session key, generates, and sends the response message. The responder verifies the freshness of the message and the response message. On successful verification, it generates the session key. The process is depicted in Fig. 2. The device-specific public and private keys Q_k and s_k make it computationally infeasible for an attacker to extract the private key of the certificate authority and the random device-specific scalar a_k. Therefore, any drone's physical capturing may not expose any critical information that can be used to compromise any of the non-captured drones.

Table II: Functionality and Security features

	Srinivas et al. [11]	Wazid et al. [12]	Ali et al. [13]	Bera et al. [14]	Zhang et al. [15]	Our
F_1	✓	✓	✓	✓	✓	✓
F_2	×	×	✓	×	×	✓
F_3	✓	✓	✓	✓	✓	✓
F_4	×	×	✓	✓	×	✓
F_5	✓	✓	✓	×	✓	✓
F_6	✓	✓	✓	✓	✓	✓
F_7	✓	✓	✓	✓	✓	✓
F_8	✓	✓	✓	✓	✓	✓
F_9	✓	✓	×	✓	×	✓
F_{10}	×	✓	✓	✓	✓	✓
F_{11}	×	×	×	✓	×	✓

Note:Resistance Against (RA), F_1:RA Drone Physical Capture; F_2: Anonymity & Untraceability; F_3:RA Stolen Mobile/smart card; F_4:RA Stolen Verifier; F_5:RA GSS/User/Drone Impersonation; F_6:RA Replay; F_7:RA man in middle; F_8:Provides Mutual Authentication & Key agreement; F_9:Provides forward secrecy/resists ephemeral secret leakage; F_{10}: Correctness/Scalability issues; F_{11}: D2D direct access control.

Performance Comparisons

In this section, the security features, computation, and communication costs comparisons among the proposed framework and exiting schemes are performed.

The proposed framework accommodates all security features ($F_1 - F_9$); whereas, the schemes of Srinivas et al. [11], and Wazid et al. [12] do not provide user untraceability (F_2) and resistance against stolen verifier attack (F_4), in addition to the scalability/correctness issues persistent in Srinivas et al.'s scheme. Likewise, the scheme of Ali et al. [13] has no provision of forwarding secrecy (F_9) due to non-resistance

Table III: Experimental Running Time

↓Operation/ Device→	Mobile	GSS	Drone
T_e: ECC Point Multiplication	5.116	0.926	4.107
T_r: Random number Generation	2.011	0.118	1.185
T_s: Symmetric enc-decryption	0.019	0.007	0.014
T_a: ECC Point Addition	0.013	0.006	0.018
T_h: One-way Hash	0.009	0.004	0.006

against ephemeral secret leakage attack, the scheme of Bera et al. [14] does not provide user anonymity/untraceability (F_2) and cannot resist impersonation attack. The scheme of Zhang et al. [15] does not provide mutual authentication (F_8) among communicating entities, has no provision of forwarding secrecy (F_9), and lacks resistance against stolen verifier attack (F_4). The security feature comparisons are shown in Table II.

For computation cost analysis, a real-time testbed was formed using MIRACL Library. The experiment was conducted among three devices: ① Xiaomi Redmi Note 8, the smartphone with Octa-core Max 2.01GHz processor and 4 GB RAM over Andriod v.9 and MIUI 11.0.7 to represent the smart-mobile/user, ②. The HP Elite-Book 8460P with RAM size of 4 GB and Processor 2.7 GHz speed (Intel(R) Core(TM) i7-2620M) executed through Ubuntu 16.0 LTS operating system was used to represent the GSS, ③ whereas, to represent a drone, Pi3 B+ Cortex-A53(ARMv8) was used with 1GB LPDDR2 SDRAM RAM and 64-bit SoC @ 1.4GHz processor. The experimental results are shown in Table III, for fuzzy extractor the computation time t_f is approximated with t_e using the similar analogy presented in [12]. We fixed identities and timestamps at 160 and 32 bits for communication cost analysis, respectively. We employed $SHA-1$ with 160 bits hash digest, and the selection of 160 bit-length random numbers was performed. Moreover, in compliance with the NIST recommendations, ECC points' size is taken 320 bits of length.

Table IV depicts the computation and communication costs comparisons among the proposed and related schemes [11]–[15]. The proposed scheme performs better than the ECC-based scheme [14] of Bera et al. and is quite expensive than symmetric key-based schemes [11]–[13], [15]. The proposed scheme provides all security features ($F_1 - F_9$) and has the least communication cost than related schemes.

Conclusion

In this article, we reviewed some of the recently published IoD access control schemes. We then proposed a generic framework to cope with the security pitfalls of the existing schemes. Based on ECC-based public/private key pairs, the proposed framework facilitates direct secure communication among any two of the participating entities. A comparative study is also conducted to show the proposed and existing methods' security features and performance. While incurring extra computation, the proposed framework provides a direct device-to-device access control with the least communication cost and security against the known attacks.

Acknowledgements

Yousaf Bin Zikria is a corresponding author. Jamel Nebhen is supported by the Deanship of Scientific Research at Prince Sattam bin Abdulaziz University, Saudi Arabia.

References

[1] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[2] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent iov," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13784–13795, 2020.

[3] 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*, 2020.

[4] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework," *IEEE Transactions on Industry Applications*, 2020.

[5] R. Arul, G. Raja, A. K. Bashir, J. Chaudry, and A. Ali, "A console grid leveraged authentication and key agreement mechanism for lte/sae," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2677–2689, 2018.

[6] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for iot based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[7] Z. Uddin, M. Altaf, M. Bilal, L. Nkenyereye, and A. K. Bashir, "Amateur drones detection: A machine learning approach utilizing the acoustic signals in the presence of strong interference," *Computer Communications*, 2020.

[8] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," *IEEE transactions on instrumentation and measurement*, vol. 64, no. 8, pp. 2072–2085, 2015.

[9] 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*, pp. 1–11, 2020.

[10] R. Arul, G. Raja, A. O. Almagrabi, M. S. Alkatheiri, S. H. Chauhdary, and A. K. Bashir, "A quantum-safe key hierarchy and dynamic security association for lte/sae in 5g scenario," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 681–690, 2019.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, 2020.

Biographies

Shehzad Ashraf Chaudhry is working as an Associate Professor in Istanbul Gelisim University, Istanbul Turkey. With an H-index of 29 and an I-10 index 62 and over 120 publications on his credit, his work has been cited over 2500 times. He has published in Top venues and has won several national and international awards.

Table IV: Performance Comparisons

	CC-User	CC-GSS	CC-Drone	RT(ms)	BE
Srinivas et al. [11]	$14T_h + T_f + T_r$	$9T_h + T_r$	$7T_h + T_r$	8.634	1536
Wazid et al. [12]	$16T_h + T_f + T_r$	$8T_h + T_r$	$7T_h + T_r$	8.648	1696
Ali et al. [13]	$10T_h + T_f + T_r$	$7T_h + 3T_s + T_r$	$7T_h + T_r$	8.611	1696
Bera et al. [14]	$6T_h + 4T_e + T_a + T_r$	$-$	$6T_h + 6T_e + 2T_a + T_r$	48.441	2336
Zhang et al. [15]	$10T_h + T_r$	$7T_h$	$7T_h + T_r$	3.356	1472
Our	$4T_h + 4T_e + T_a + T_r$	$-$	$4T_h + 4T_e + T_a + T_r$	40.179	1376

CC: Computation Cost, RT(ms): Approximate Running time in milliseconds, BE: Bits Exchanged.

Jamel Nebhen received the Ph.D. degree from the Aix-Marseille University, France, in 2012. Since 2019, he joined the Prince Sattam bin Abdulaziz University in Alkharj, Saudi Arabia, as an Assistant Professor. His research interests are mainly in the design of analog and RF integrated circuits, IoT, biomedical circuit, and sensors instrumentation.

Azeem Irshad received his PhD from International Islamic University, Islamabad, Pakistan. With over 70 publication including 45 in SCI Journals and having 14 H-index, 20 i-10 Index, his research work has been cited over 850 times. His research interests include cryptographic protocols and their applications.

Ali is a Reader of Networks and Security and Program Leader of Cyber Forensics and Security at the Department of Computing and Mathematics, Manchester Metropolitan University, UK. He has obtained over 2 Million USD Industry and Government funding. He is an SMIEEE and serving EIC of IEEE Future Directions Newsletter.

Rupak is currently a Reader within the Department of Computing and Mathematics, Manchester Metropolitan University, UK; research interests include various use cases and the challenges of IoT and cyber physical systems including cyber security; Principal Investigator of multiple government and industry funded projects; Membership – SMIEE, MIET, FHEA-UK.

Keping Yu [S'11, M'17] received his Ph.D. degree from Waseda University, Japan, in 2016. He is currently a researcher at Waseda University. His research interests include smart grids, information-centric networking, the Internet of Things, artificial intelligence, blockchain, and information security.

Yousaf Bin Zikria (SM'17) works as an Assistant Professor in the Department of Information and Communication Engineering, Yeungnam University, South Korea. He authored more than 80 articles, conferences, book chapters, and patents. He published papers at the top venue, including IEEE Commun. Surv. Tutor, IEEE Wireless Commun and Network Magazine, etc.