A Physical Capture Resistant Authentication Scheme for the Internet of Drones

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

Abstract

The internet of Drones (IoD) can encompass many essential services, including surveillance and emergency/rescue operations. While IoD is becomin popular and experiencing a rapid usage increase, privacy and security are the main concerns to avoid leakage of critical information and/or denial of services by a single drone or a whole IoD network. In addition to traditional privacy cum security issues, the physical capture 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 physical drone capturing and related attacks.

Introduction

The Internet of Drones (IoD) is a novel paradigm in wireless networks that employs Internet of Things (IoT)-based technology to accomplish its different critical ventures. Unmanned aerial vehicles (UAVs), or drones, acting as flying IoT-based sensing objects have found widespread application in diverse 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, tracking, and more. The IoD, being the synthesis of the IoT domain as well as smart drone 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 efficiency, 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, IoT-based technology has been nearly integrated into each conventional application with promising results [2–5]. Due to IoT integration, physical systems have been able to communicate with computer systems, and therefore can be managed reliably with lower operational cost [6].

Figure 1 depicts a high-level representation of IoD architecture that describes IoD as an interconnection of a ground service station (GSS) as well as smart drones deployed in the airspace of the system. According to recent forecasts, because of the increasing number of applications for commercial drones, there will be more than US$100 billion market share for drones in the near future. A drone, as a crucial element of IoD, collects the data from any particular fly zone (FZ) and submits that data to the GSS. These drones are equipped with high-vision cameras, IoT sensors with limited memory and power, and less computational capabilities, GPS receivers for delivering diverse high-altitude services, and a communication module to transmit the collected information toward respective GSSs. Cost-efficient operational solutions, including UAV 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]. Drones may be physically compromised and examined by adversaries. The communication among the entities is wireless in nature, which exposes the drones to physical attacks leading to exposure of stored secrets in their memory. IoD networks, being resource-constrained in memory, power, and computational capabilities, need to devise an efficient authentication and key establishment (AKE) protocol [8–10] through employing low-cost cryptographic encryption/decryption techniques and making 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), the 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 for earnest efforts to devise more cost-effective authentication and key agreement solutions for the IoD ecosystem.

Shehzad Ashraf Chaudhry is with Istanbul Gelisim University, Turkey; Jamel Nebhen is with Prince Sattam bin Abdulaziz University, Saudi Arabia; Azeem Irshad is with International Islamic University, Pakistan; Ali Kashif Bashir is with Manchester Metropolitan University, United Kingdom; Rupak Kharel is with theUniversity of Central Lancashire, United Kingdom; Keping Yu is with Waseda University, Japan; Yousaf Bin Zikria is with Yeungnam University, South Korea.

Digital Object Identifier:
10.1109/MCOMSTD.0001.2100006

2471-2825/21/$25.00 © 2021 IEEE

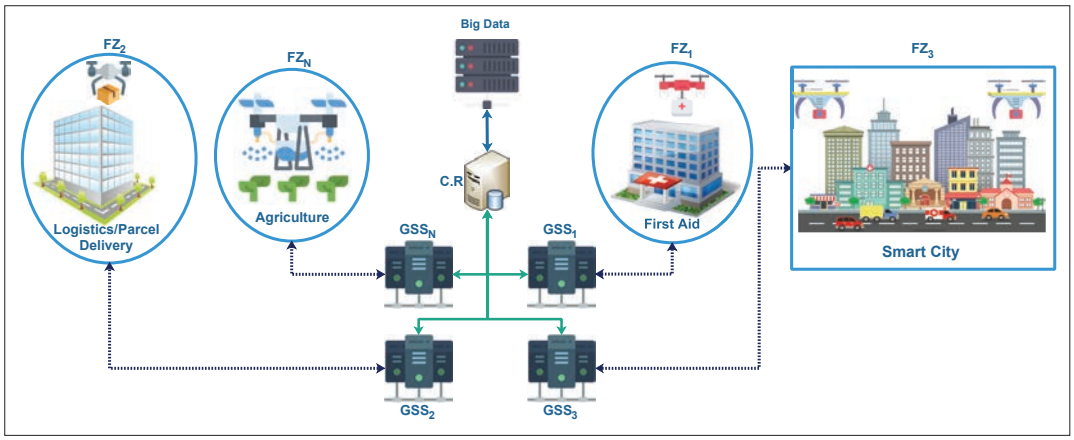

FIGURE 1. IoD environment monitoring system.

CHALLENGES

The main challenges in the IoD ecosystem include:

- **Physical capture:** An adversary may access infused secret information through the physical capture of drones and smart devices of users, and later attempt to corrupt other drones in the system or use the extracted information to deploy malicious drones in the system. Moreover, in the case of a stolen smart device of a user, the adversary can try to guess the password on an offline basis or attempt to impersonate the system's legitimate members.
- **Malicious interruption:** An adversary may attempt to impersonate the system's legitimate entities by altering the contents in real time 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 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 for IoD networks.
- **Illegal Access:** Due to wireless communication, any unauthorized intruder may access messages in the drone and user path. Then it could inject malicious codes to impersonate the legitimate 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 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 infeasible for an adversary to recover ID_i from public messages. The exposure of identity may become an inconvenience for the user and lead to impersonation attacks, compromising untraceability objectives.
- **Untraceability Support:** If an IoD-based AKA scheme lacks untraceability, it might become uncomfortable for the user or damage the user's anonymity objective. Hence, an adversary must not be able to link different protocol sessions of the same user to ensure untraceability.
- **Resistance against Physical Device Capture Threat:** 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 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:** To countere forgery on the part 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 protection of the forward as well as backward secrecy so that an adversary cannot 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 *GSS*s before deploying these entities into their assigned application domains. The *GSS* stores the received data safely. Furthermore, it also stores the key credentials related to the drone, flying zones, and users. In the IoD environment net-

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.

Scheme	Year	Cryptographic method used	Properties
Srinivas *et al.* [11]	2019	Symmetric key primitives	It is susceptible to impersonation attack based on stolen verifier, and has traceability and scalability issues. 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 is prone to cloning attack, and lacks the feature of no clock synchronization.
Bera *et al.* [14]	2020	Elliptic curve cryptography	It lacks mutual authentication and traceability.
Zhang *et al.* [15]	2020	Symmetric key primitives	It lacks provision of perfect forward secrecy and is susceptible to stolen-verifier and insider attacks. Session key agreement and mutual authentication are also missing.

Table 1. Summary of limitations/drawbacks of previous user authentication schemes in the Internet of Drones environment.

work model, the drone's airspace could be divided into several disjoint 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 article 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 a GSS. $\mathcal{A}$ 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 GSSs cannot be revealed to any attacker, except those of captured drones.

IoD Standards for Security

When cooperating, drones form an ad hoc communication infrastructure. The cooperating UAVs equipped with IoT-based sensing technology are the basis of IoD. Ensuring communication security and safety are the main challenges for IoD. Among other security-related issues, resistance to physical capture of a drone has gained importance due to the network's dynamicity. Recently, some communication and security standards for UAVs have arisen. Here, we provide a brief discussion on the standards of UAVs.

IEEE P1920

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 aircraft, including manned or unmanned, irrespective of network size and usage type (civilian, commercial, etc.). The vehicle-to-vehicle (V2V) standard communication protocol is provided by the IEEE 1920.2 stack. It extends inter-drone communication and is independent of line of sight and radio line of sight. The IEEE 1920 protocol also provides the security architecture for drones' communications.

ISO 21384-3

In 2019, International Standards Organization (ISO) 21384-3 was announced to standardize the operational procedures of drones, also called unmanned aircraft systems (UAS). ISO 21384-3 provides the globally agreed standards for safe and secure commercial operations requirements.

3GPP Rel-17

The 3rd Generation Partnership Project (3GPP) provides a standard solution for beyond line of sight (BLoS) and beyond radio line of sight (BRLoS) communication for drones. The technical reports of 3GPP Release 17 (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. Technical report TR 22.829 provides standards for 5G inclusion in drone communication, while TR 23.755 provides layer support. 3GPP TR 23.754 was also released as part of Rel-17 for inter-drone specification and drone-to-infrastructure communication, authorization, and authentication.

ITU-T

International Telecommunication Union — Telecommunication Standardization Sector (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 1.

Srinivas *et al.*

Srinivas *et al.* [11] suggested a three-factor authentication protocol, the temporal credential-based anonymous lightweight authentication scheme (TCALAS) for the IoD environment. The scheme comprises three : the trusted GSS, drone user (U_i), and remote drone (RD_j). The GSS enables establishing a session key between U_i and RD_j on the public channel in a particular cluster. The drones are allocated to their respective FZs called clusters. A control room accompanies the *GSS*. U_i registers with the 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 a successful login attempt using a fuzzy extractor in the login and authentication phase, U_i computes and forwards message MSG_1 to the GSS. The GSS checks the timestamp freshness and val-

idates U_i. Then U_i forwards MSG_2 to RD_j. Next, RD_j sends MSG_3 to U_i directly using the public channel. If U_i verifies RD_j, it computes the session key (SK); otherwise, it aborts the session. Although 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 FZ. Second, 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 $\mathcal{A}$ may approach the drone's verifier repository and initiate a GSS impersonation attack toward 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. Wazid *et al.* comprises four participating entities in the system: User (U_i), mobile device (MD_i), drone (DR_j), and server. 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 the pre-deployment and user registration, the login and authentication phase, password and biometric updation phase, dynamic drone addition, and drone key management phase are followed. In the login and key agreement phase, the mobile device (MD_i) computes message Msg1 after biometric verification using the fuzzy extractor function and sends it to the server. The server, after checking the timestamp, verifies the authenticity of MD_i. Then it computes Msg2 and submits it to DR_j using the public channel. DR_j verifies the timestamp and validates the authenticity of both MD_i and the server. Then it computes session key SK_{ij} as well as Msg3. Msg3 is forwarded to MD_i for further verification. The user/MD_i checks the timestamp and computes SK_{ij}. Then it compares the computed messages against the received messages from DR_j. Upon successful verification, it validates DR_j and finalizes the agreed session key SK_{ij}. However, there were two major drawbacks in the Wazid *et al.* scheme: In Wazid *et al.*, any registered user, however unfair, 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.*

Bera *et al.* [14] suggested a novel blockchain-based data delivery and collection (DDC) scheme for the 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 a registration authority (RA), control rooms (CR_J), GSSs (GSS_j), drones (DR_i), and a blockchain center (BC). The RA, a trusted entity, registers CR_J, and in return CR_J registers GSS_j and DR_i. Then registered DR_is are assigned to their respective FZs (FZ_j). 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. GSS_j collects data from DR_i which submits it to GSS_j, and forms the transaction blocks to add in its private BC center. After the registration process, the drones are allocated in their respective FZ_j. The mutual authentication procedure is followed to authenticate DR_i by GSS_j. Mutual authentication utilizes elliptic curve cryptography (ECC) for signatures and verification of the certificate. Upon a 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, DR_i can never authenticate GSS_j. This is because the former entity is unable to verify the signature as constructed by GSS_j. The Bera *et al.* scheme is unable to impart anonymity to DR_i since the employed pseudo-identity remains the same in all initiated sessions and hence is traceable by the adversary. Moreover, Bera *et al.* utilize session nonces injudiciously since those nonces serve 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 the IoD environment using lightweight symmetric key operations. The network model comprises three participating entities: 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 onward during the mutual authentication phase to acquire network services. Zhang *et al.* describe three phases: the setup, registration, and mutual authentication phases. U_i computes the authentication request message in the mutual authentication phase after having input the user credentials and submits it to the CS. The CS, upon receiving the

Bera *et al.* [14] suggested a novel blockchain-based data delivery and collection (DDC) scheme for the IoT-oriented 5G IoD environment. The scheme assumed well-synchronized clock timing across the system to help counter replay attacks.

The proposed IoD access control framework is built on ECC and symmetric hash functions. It works on the notion of a public-private key pair of each entity and avoids bilinear pairings.

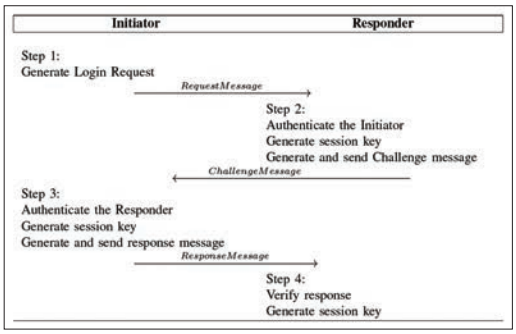

FIGURE 2. Proposed framework.

	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}	×	×	×	✓	×	✓

TABLE 2. Functionality and security features.

message, validates the timestamp and authenticity of U_i. Next, it computes another authentication message for drone V_j. V_j authenticates both entities after comparing the computed parameters against the received message and submits the authentication response message toward U_i. U_i, upon receiving the message from V_j, verifies the computed factors against the received parameters. Upon a successful match, 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 this scheme is that it does not provide anonymity due to the use of a generic parameter PID_s, which is hashed along with the current timestamp. 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. Second, 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 toward the CS even with the wrong user password. Moreover, in the scheme of Zhang *et al.*, the server stores a 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 on ECC and symmetric hash functions. It works on the notion of a 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, user, GSS) registers with the CA and gets its public/private key in the form $Q_k = a_kP$, $s_k = h(ID_k, Q_k)s_{CA} + a_k$, 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 steps, the initiator, using its private key and randomly generated number, computes and sends login requests. On receiving a 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, and generates and sends the response message. The responder verifies the freshness of the message and the response message. Upon 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 capture may not expose any critical information that can be used to compromise any of the non-captured drones.

Performance Comparisons

In this section, the security features, computation, and communication costs comparisons among the proposed framework and existing 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 against ephemeral secret leakage attack, and 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 2.

For computation cost analysis, a real-time testbed was formed using the MIRACL Library. The experiment was conducted among three devices: ① Xiaomi Redmi Note 8, a smartphone with an Octa-core Max 2.01 GHz 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 4 GB RAM and a processor with 2.7 GHz speed (Intel® Core™ i7-2620M) executed through the Ubuntu 16.0 LTS operating system was used to represent the GSS, ③ to represent a drone, Pi3 B+ Cortex-A53(ARMv8) was used with 1 GB LPDDR2 SDRAM RAM and a 64-bit SoC @ 1.4 GHz processor. The experimental results are shown in Table 3: for the fuzzy extractor the computation time t_f is approximated with t_e using the similar analogy pre-

sented 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 4 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 more expensive than symmetric key-based schemes [11–13, 15]. The proposed scheme provides all security features (F_1 – F_9) and has lower communication cost than related schemes.

Conclusion

In this article, we review some of the recently published IoD access control schemes. We then propose 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 direct device-to-device access control with the lowest communication cost and good security against known attacks.

Acknowledgment

Yousaf Bin Zikria is the corresponding author.

References

[1] C. Lin *et al.*, "Security and Privacy for the Internet of Drones: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, Jan. 2018, pp. 64–69.
[2] C. Feng *et al.*, "Attribute-Based Encryption with Parallel Outsourced Decryption for Edge Intelligent IOV," *IEEE Trans. Vehic. Tech.*, vol. 69, no. 11, 2020, pp. 13,784–95.
[3] S. A. Chaudhry *et al.*, "PFLUA-DIOT: A Pairing Free Lightweight and Unlinkable User Access Control Scheme for Distributed Iot Environments," *IEEE Systems J.*, 2020.
[4] A. Irshad *et al.*, "A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet Based Vehicle-to-Grid Technology Framework," *IEEE Trans. Industry Applications*, 2020.
[5] R. Arul *et al.*, "A Console Grid Leveraged Authentication and Key Agreement Mechanism for LTE/SAE," *IEEE Trans. Industrial Informatics*, vol. 14, no. 6, 2018, pp. 2677–89.
[6] S. A. Chaudhry *et al.*, "A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems," *IEEE Access*, vol. 8, 2020, pp. 139,244–54.
[7] Z. Uddin *et al.*, "Amateur Drones Detection: A Machine Learning Approach Utilizing the Acoustic Signals in the Presence of Strong Interference," *Computer Commun.*, 2020.
[8] K. Yu *et al.*, "A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," *IEEE Trans. Instrumentation and Measurement*, vol. 64, no. 8, 2015, pp. 2072–85.
[9] X. Li *et al.*, "A Novel UAV-Enabled Data Collection Scheme for Intelligent Transportation System Through UAV Speed Control," *IEEE Trans. Intelligent Transportation Systems*, 2020, pp. 1–11.
[10] R. Arul *et al.*, "A Quantum-Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario," *IEEE Trans. Industrial Informatics*, vol. 16, no. 1, 2019, pp. 681–90.
[11] J. Srinivas *et al.*, "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," *IEEE Trans. Vehic. Tech.*, vol. 68, no. 7, 2019, pp. 6903–16.
[12] M. Wazid *et al.*, "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment," *IEEE IoT J.*, vol. 6, no. 2, 2019, pp. 3572–84.
[13] Z. Ali *et al.*, "Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles," *IEEE Access*, vol. 8, 2020, pp. 43,711–24.
[14] B. Bera *et al.*, "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," *IEEE Trans. Vehic. Tech.*, vol. 69, no. 8, 2020, pp. 9097–9111.
[15] Y. Zhang *et al.*, "A Lightweight Authentication and Key Agreement Scheme for Internet of Drones," *Computer Commun.*, 2020.

↓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

Table 3. Experimental running time.

	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.

Table 4. Performance comparisons.

Biographies

Shehzad Ashraf Chaudhry (ashraf.shehzad.ch@gmail.com) is an associate professor at Istanbul Gelisim University, Turkey. With an H-index of 33 and an I-10 index 67, and over 140 publications on his credit, his work has been cited over 3000 times. He has published in top venues, and has won several national and international awards.

Jamel Nebhen (j.nebhen@psau.edu.sa) received his Ph.D. degree from the Aix-Marseille University, France, in 2012. In 2019, he joined Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia, as an assistant professor. His research interests are mainly in the design of analog and RF integrated circuits, IoT, biomedical circuits, and sensor instrumentation.

Azeem Irshad (irshadazeem2@gmail.com) received his Ph.D. from International Islamic University, Islamabad, Pakistan. With over 70 publication including 45 in SCI journals, and having 14 H-index and 20 i-10 Index, his research work has been cited over 850 times. His research interests include cryptographic protocols and their applications.

Ali Kashif Bashir [SM'16] (dr.alikashif.b@ieee.org) is a reader of networks and security and program leader of Cyber Forensics and Security in the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He has obtained over US$3 million in industry and government funding. He is the Editor-in-Chief of *IEEE Future Directions Newsletter*.

Rupak Kharel [SM'18] (rkharel1@uclan.ac.uk) is currently a professor at the University of Central Lancashire. His research interests include various use cases and the challenges of IoT and cyber-physical systems including cyber security. He is Principal Investigator of multiple government and industry funded projects. He is a member of IET and a Fellow of HEA-UK..

Keping Yu [S'11, M'17] (keping.yu@aoni.waseda.jp) 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] (yousafbinzikria@ynu.ac.kr) is an assistant professor in the Department of Information and Communication Engineering, Yeungnam University, South Korea. He has authored more than 100 journal articles, conference papers, book chapters, and patents. He has published papers in top venues, including *IEEE Communications Surveys & Tutorials*, *IEEE Wireless Communications*, and *IEEE Network*, among others.