IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 7, 2021, accepted October 21, 2021, date of publication November 1, 2021, date of current version November 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3124510

A Key Agreement Scheme for IoD Deployment Civilian Drone

SAEED ULLAH JAN[1], IRSHAD AHMED ABBASI[2,3], AND FAHAD ALGARNI[2,3]

[1]Department of Computer Science and IT, University of Malakand, Chakdara 18800, Pakistan
[2]Department of Computer Science, Faculty of Science and Arts, University of Bisha, Belqarn, Sabt Al-Alaya 61985, Saudi Arabia
[3]Faculty of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia

Corresponding author: Irshad Ahmed Abbasi (aabasy@ub.edu.sa)

This work was supported by the University of Bisha, Saudi Arabia.

ABSTRACT Drones are of different shapes, sizes, characteristics, and configurations. It can be classified for the purpose of its deployment, either in the civilian or military domain. The earliest usage of drones was totally for military purposes, but manufacturers promptly tested it for civilian fields like border surveillance, disaster relief, pipeline inspection, and rescue. Drone manufacturing, equipment installation, power supply, multi-rotor system, and embedded sensors are not the pressing issues for researchers of drone technologies. What is required is to utilize a drone for a complex operation and ensure secured data broadcasting among drones with the ground control station via a self-organized, resourceless, and infrastructureless network (Flying Ad Hoc Networks (FANETs)). These operations are no less important in areas like an emergency, search and rescue operations, border surveillance, and physical phenomenon sensing for the end-user. However, it is not without some challenges for the researchers keeping in view the threats these operations are exposed to concerning security issues and challenges. To overcome these challenges, the researchers have to strive towards a secured drone operation by developing a robust and lightweight key agreement protocol for IoD deployment civilian drones. Consequently, the researchers in this study have attempted to design a key agreement scheme for the IoD deployment of civilian drones. The security of the proposed key agreement scheme has been verified by ProVerif2.02 and Real-Or-Random (ROR) model, while its performance scenario has been tackled by considering storage, computation, and communication overheads analysis. In comparing the proposed framework with prior protocols, it has been demonstrated that the scheme is quite efficient and may be recommended for operations in a given IoD environment.

INDEX TERMS UAV, latency, surveillance, cryptography, sensor, authentication, synergy.

I. INTRODUCTION

Internet-of-Drones (IoD) environment is operationalized for providing secure flying services to drones within the jurisdiction of the ground control station. It also monitors, supervises, manages, controls, and coordinates the overall drone activities for generic purposes. The rapid development of technology in the past decades has led to the successful adoption of IoD in the civilian domains. It is implemented for infrastructural inspection, searching rescue activities, smart city traffic monitoring, troops' movement, package delivery, cinematography, wild-life surveillance, and agricultural-land tracking [1].

The drone is remotely commanded by an operator from a powerful intelligence computer system. It can communicate with itself and with the GCS through wireless, infrastructureless, and self-organizing networks called FANETs, a sub-type of Mobile Ad Hoc Networks (MANET) but with limited transmission latency. However, the different applications/security protocols designed for MANET cannot be substituted for FANET. Usually, the drone has a set of micro-electromechanical systems, low-capacity batteries, airframes, microprocessors, and a limited capacity and volume of payload. Due to these meager capabilities, drone technology is not yet qualified for complex tactical tasks. Though, multi-drone systems that can operate across IoD using FANET allow drones and GCS to work collaboratively for completing such an arduous mission [2]. For further improvement in operations, synergy among all the participants is necessary. FANET, a self-organizing network, can cause networking problems in preventing a drone from effectively communicating with the ground control

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaolong Li.

station (GCS). Considering all the basic features of FANET, message authentication and identification authentication are challenging for researchers to efficiently provide path discovery, data transmission, and route maintenance services to all IoD participants [3]. Identification authentication can ensure cross-conversation among peers legitimately, while information authentication can be confirmed only by focusing on the design of a robust authentication scheme. However, this research is focused mainly on information authentication instead of identification authentication. The latter, i.e., identification authentication, falls outside the scope of this study.

A. MOTIVATION AND CONTRIBUTIONS

Different researchers have come up by designing different message authentication protocols is given in the second part of this research paper. However, some of these prior protocols have design issues, and others are either completed in three to four round trips or have the risk for different vulnerabilities. Due to modular exponentiation, these protocols have been observed for maximum communication and computation costs unable to resist privileged insider, impersonation, and GCS spoofing attacks, loss of anonymity and privacy, and do not preserve the balance of security with performance. Similarly, some inherent features of FANET like de-centralization, infrastructure-less, self-organizing, and clustering [4] cannot make it feasible for IoD deployment civilian drones. Therefore, in this paper, the researchers propose a simple cryptographic authentication scheme for FANET based on public key infrastructure (PKI). In PKI, there is no need to exchange keys privately as it is in conventional public-key cryptography but must be appropriately managed each time. During the whole process, the public-private key pair can be handled securely and efficiently [5]–[7]; firstly, the key pair is created and efficiently utilized, and secondly, the key pair is invalidated. The invalidation phase happens when the life cycle of the key pair becomes wind off or compromised. If the session of one key becomes expired and declared invalid, PKI can manage the null key. The key exchange is necessary because the public-private-key pair for encryption/decryption needs to be dynamically updated for the upcoming session, which is probably an appropriate choice. Because it allows IoD's participants to generate a mutually computed session key through a public network channel. Given the shortcomings of the available schemes, merits of PKI, and the need for a more efficient one motivated us to design a key agreement scheme for IoD deployment civilian drone.

B. SYSTEM ARCHITECTURE

The architecture presented in this research paper consists of Ground-Control-Station (GCS), Drone (D), and External User (U) or simply a user. Each participant first registers with GCS and then deploys for a practical task. Let suppose GCS is a fully trusted participant, while drone and user being considered partially trusted. The drone (D) is the key participant in the whole architecture. External users, when required, can access a designated drone from anywhere, like checking the infrastructure of a big city, traffic surveillance, sidewalk monitoring, etc. GCS can fully control the flying zone, drone legitimacy, and data access by an external user. Similarly, the GCS can also be responsible for "Who access whom," and the entry of illegitimate drone (D) or user (U) at any time is the sole responsibility of GCS along with trajectory, waypoint, and data communication-related phenomenon, as shown in Fig. 1.

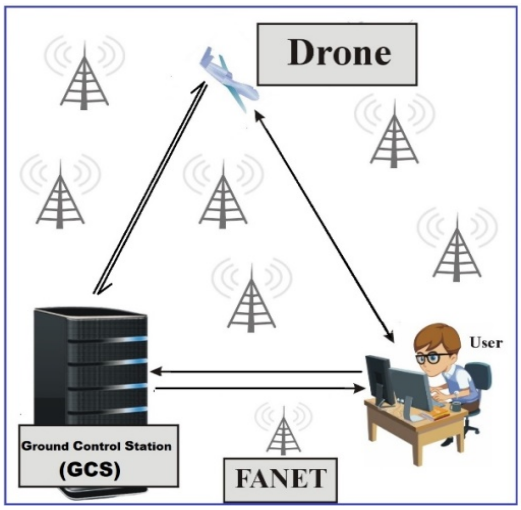

FIGURE 1. System architecture.

C. ADVERSARY AND THREAT MODELS

It is worth mentioning that modeling the role of attackers is an important topic in cyber defense since it helps to guarantee that security assessments are scientifically sound, especially for conceptual contributions that are difficult to test or where comprehensive testing is impossible. In a computer or networked system, an adversary model is a formalization of an attacker. Depending on how comprehensive this formalization is, the opponent might be an algorithm or a collection of assertions about skills and intentions. This umbrella encompasses a variety of techniques in many domains of computer security [8]. Therefore, keeping in view the adversary model, an adversary interacts with our IoD architecture by representing themselves as a malicious drone with GCS, D, or U, in the following manner.

i. An adversary may extract stored data from GCS's memory and use it to verify secret credentials.
ii. An adversary may alter, erase, upgrade, corrupt, or insert false information into a public network channel.
iii. Adversaries may replay, alter, or erase beneficial information exchanged between participants over a private channel.
iv. An adversary may acquire the internal sensitive credential from a stolen mobile device from a user (U) or shape the memory of a crashed/physically captured drone (D) using reverse engineering techniques or vital tags in offline mode, but not both simultaneously.

Similarly, threat modeling is another method for improving the security of an application, system, or business process by identifying objectives and vulnerabilities and design countermeasures to avoid or minimize the impacts of threats to the system. It also aids in identifying a system security requirement, i.e., anything that is mission-critical, sensitive, or made up of valuable data; identifying possible threats and vulnerabilities to decrease the risk to the system. It also assists system administrators in comprehending the effect of risks, quantifying their severity, and putting controls on time [9]. Therefore, keeping in view the threat model, all possible threats to our IoD architecture is given as under:

- Privacy and Signal Jamming Threat
- Collation and Flight Control Threats
- Forgery and Signal Spoofing Threats
- De-Authentication and Insider Threats
- De-Synchronization and Stolen-Verifier Threats
- Main-in-the-Middle and Drone Capture Threats

D. SECURITY REQUIREMENTS

Some security and functionalities are required for securing the IoD environment using the self-organizing and resourceless wireless network. These are as under:

1. Before accessing confidential information, all participants, including U, D, and GCS, should mutually authenticate each other.
2. IoD's participants (e.g., U, D, and GCS), after completing mutual authentication, create a session key between them to be used in subsequent communications. The session key cannot be obtained by anyone other than the participants in the session.
3. An adversary should be unaware of any connections among IoD's participants. The adversary should not follow the individuals' eavesdropped messages back to any participants.
4. U, D, and GCS should ensure that their identities are kept secret. In other words, only trusted parties are informed of the uniqueness of these.
5. Authorized organizations should be able to access network resources anytime they need them. The networks should avoid Denial-of-service (DoS) attacks.
6. The proposed scheme should be resistant to various known attacks, including drone capture, man-in-the-middle, stolen verifier, replay, user impersonation, server impersonation, privileged insider attacks, etc.
7. The authentication protocol should have provable protection in a statistical model (e.g., a real or random (RoR) model) that can be used to estimate the probability of an adversary breaching the protocol's security.
8. The proposed protocol's protection should be formally tested using formal verification methods like ProVerif2.02. ProVerif2.02, in particular, is a commonly used authentication method that can ensure the proposed scheme's private information is not exposed during execution.
9. The scheme should be effective in terms of low computation and communication costs.

II. RELATED WORKS

Sun *et al*. [10] demonstrated that a robust authentication mechanism is needed if unmanned aerial vehicles are operationalized in a cluster so that each UAV can send data securely to the cluster head. In this regard, they used a double watermarking authentication strategy. First, the cluster head authenticates the integrity of data received from other UAV and then aggregates it by applying the chaotic map method. However, the said technique is not adequate for such a low latency network like FANET and UAVN. Li *et al.* [11] stated that the UAV could be used for diverse purposes, but the wireless communication of information is unsafe; with limited hardware and short battery life, severe damage is expected to occur for performing a sensitive task. So, they proposed identity and ECC-based authentication protocol in which they claimed that their scheme guarantees for secure UAV mission. Unfortunately, stolen verifiers and insider threats still exist in their algorithms. Alladi *et al*. [12] developed a Physical Unclonable Function (PUF) based security mechanism for UAV deployment civilian domain using 5G network. Gope *et al.* [13] proposed an anonymous security mechanism for radio frequency identification (RFID)-enabled unmanned aerial vehicles. Instead of software, they used a circuit for authentication using the Physical Unclonable Function (PUF) concept. They claimed that PUF-enabled RFID equipment in the tag of UAV could execute the receiving signals effectively.

According to Chaudhry *et al.* [14], the IoD can acquire real-time data to interpret different participants, as many drones fly in various zones to carry out the assigned tasks. The data is accessed through an open network channel, and drones with limited battery power suffer from data broadcasting security. The security and privacy of drones are essential for mission-critical, safety-critical, or surveillance activities. Therefore, they produced a generic certificate-based access control method to allow inter-drone and drone to ground station access control/authentication (GCACS-IoD) mechanism. However, GCACS-IoD does not resist man-in-the-middle attack because some credentials are exchanged openly between the participants. The researchers in [15] have presented identity and ECC-based triple authentication scenarios consisting of initiation of certification, identity authentication, and consistent essential verification. Due to scalar multiplication and key escrow problem, the scheme is difficult to implement in the real-world environment. Also, the security features being utilized for IoT can be implemented in an IoD environment to confirm secure communication with each other and with the GSC. However, upon implementing the security framework of [15], the network topology is fused for drones in IoD due to its usage in entertainment, toys, agricultural-land monitoring, high-value industries, and wide applications in the defense field shooter products.

Seo *et al.* [16] focused on improving UAV's battery power, sensing systems, security, and other technologies. They

demonstrated their advantages when these things become incorporated into UAVs to achieve a top-rated product in the market for advancing various fields and activities. Upon enhancing UAVs, they can be deployed for enormous tasks like personal aerial photography, entertainment, commercial markets, disaster relief, animals and plants spraying, coasts, delivering transport goods, law enforcement tasks, and agricultural and industrial applications. These small UAVs in smart cities can also be utilized for a variety of purposes like traffic monitoring and management, merchandise distribution, health, and emergency services, and air taxi services can also increase the efficiency, effectiveness, timeliness, reliability, and performance of these services and may help reduce the cost of delivering these services. Tian *et al.* [17] also proposed a security framework for edge-assisted IoD using the securely computed authenticated key in online and offline mode for efficient open-access communication. Ever [18] demonstrated that the key features of drone-like mobility, energy consumption, reliability, and efficiency for an open network are fundamental because all the IoD participants are not designed with an integrated security phenomenon. Therefore, they proposed a security framework for IoD using Wireless Sensor Network (WSN). They used the elliptic curve discrete logarithmic function for secure computation of keys between the participants. However, it still suffered from a computation time complexity.

Abualigah *et al.* [19] delivered a detailed exploration of the literature regarding the Internet of Drones (IoD), including its applications, installations, and integration. They concentrated on two main areas: the practical implications of IoD, like for smart city surveillance, cloud fog, and mobile computing; and the integration of IoD, like privacy protection, authentication, security, neural networks, blockchain, and optimization-based methods. This is an interesting paper for the researchers who are looking to work in IoD. According to Meng *et al.* [20], the Internet of Vehicles (IoV) is defined as the use of the Internet of Things (IoT) in transportation where each car will function as a separate node with the capacity to collect data and transfer it to the network for onward submission to a base station. In this regard, a lightweight anonymous mutual authentication and key agreement scheme is required. So, they provided a blockchain-based method for obtaining the session key. To tackle the mutual authentication problem in an Autonomous Internet of Vehicles (AIoV) network, Adil *et al.* [21] proposed a three-byte-based Media Access Control (MAC) protocol. Interestingly, they claimed that their scenario is supervisor over the state of the art schemes in terms of detection rate, latency, throughput, and packet loss ratio. At the same time, Kumar *et al.* [22] worked on the security frameworks based on elliptic curve cryptography (ECC) for radio frequency identification (RFID) enabled IoD.

Moreover, the traditional communications networks may be fully or partially disrupted, IoT-based technologies and their use in post-disaster management is much needed in the era. By enabling IoT-based technology with limited mobile users' authentication rights, Al-Turjman *et al.* [23] developed a security mechanism based on bilinear pairing and elliptic-curve cryptosystems. Their scenario meets security requirements and shows resistance to node capture vulnerability. Chen *et al.* [24] came up with a new authentication mechanism. They concentrated on message authentication over identity due to the dire need of the era and for end-user security purposes. Because unmanned aerial vehicles (UAVs) are operated without humans, their security is interesting because it seems an accurate platform between authentication and anonymity. Their security approach was based on symmetric paring, which consisted of bunches of identities and made malicious module-altering attacks challenging for an adversary. Their CDHP and DLP-based scheme has achieved credential randomization, batch proof, cross-verification, and mutual authentication and is safe against offline identity guessing, location spoofing, and replay attacks. However, it is still suffered from stolen-verifier and privileged insider threats.

Cho *et al*. [26] devised the SENTINEL protocol to reduce the computation time complexity and traffic overheads associated with certificate exchanges and asymmetric cryptography calculations. Their scenario first creates a flight session key for a drone and a flight plan and then records it in a centralized database present in the ground station for future tactical tasks. When the drone is flying, the registered flight session key in the message authentication can authenticate the participant with the help of the ground station.

Therefore, keeping in view the literature study mentioned above, and the scenario presented by [27], it has been concluded that most authentication schemes have fixed random numbers that are the same for different message authentication phases (sessions) even if pseudo-identities become changed. These authentication schemes are not dynamic, same for other sessions; the previous message rebounded by drone to GCS in the upcoming new session. And if a drone goes out of the system or is taken down by an adversary, most schemes cannot broadcast, leaving information to GCS; resultantly, the cluster of drones cannot update its keys dynamically. Similarly, some inherent features of FANET like de-centralization, infrastructureless, self-organizing, and clustering cannot make it feasible for IoD deployment civilian drones.

III. PROPOSED SCHEME

This simple hash cryptographic function and PKI-based protocol is fast and secure because the powerful, intelligent computer system generates the key. The scheme consists of the setup/initialization phase, user's registration phase, drones registration phase, authentication& key-agreement phase, dynamic drone addition phase, and drone revocation phase. The different notations used are described in Table 1.

A. SETUP/INITIALIZATION PHASE

In the initialization phase, the GCS initiates the protocol, first generates a secret key S_{GCS}, and public private key pairs, s and l, and collision free one way has function $H:\{0, 1\}^* \rightarrow \{0, 1\}^l$.

TABLE 1. Summary of notations.

Notation	Description
U	User
D	drone
GCS	Ground-Control-Station
ID_U	User's Identity
S_{GCS}	GCS secret key
sk	User's secret key
ID_D	Drone's Identity
PID_D	Drone's pseudo-identity
R_U	User's random number
PID_U	User's pseudo-identity
H(.)	Hash-Function
s, *l*	Public-private key pair
PID_{GCS}	GCS's pseudo-identity
T_U, T_D, T_{GCS}	Time-stamp

B. USER'S (U) REGISTRATION PHASE

In this phase of the protocol, the Ground-Control-Station (GCS) selects the identity for the user (U), which is ID_U and secret key sk. The record of a user (ID_U, sk) is stored in the database of Ground-Control-Station (GCS) and also sends it to a user (U) through a secure channel, as shown in phase 1.

User (U)	Ground-Control-Station (GCS)
	Selects Identity ID_U
	Extract sk
	Store {ID_U, sk}
	{ID_U, sk} →
Stores {ID_U, sk} in user side	

Phase 1. User's registration phase.

C. DRONE'S (D) REGISTRATION PHASE

The Ground-Control-Station (GCS) defines another identity for Drone (D), which is ID_D and pseudo-identity PID_D, computes $Z_1 = H(S_{GCS}||PID_D)$, $Z_2 = H(ID_D||S_{GCS})$, injects ID_D in the database, and transmits $\{ID_D, Z_1, Z_2, PID_D\}$ to Drone through a secure channel as shown in phase 2.

Drone (D)	Ground-Control-Station (GCS)
	Selects Identity ID_D
	Selects Pseudo-Identity PID_D
	Computes: Z_1=$H(S_{GCS}||PID_D)$
	Z_2=$H(ID_D||S_{GCS})$
	{ID_D, PID_D, Z_1, Z_2} →
Stores (ID_D, PID_D, Z_1, Z_2)	

Phase 2. Drone registration phase.

D. KEY-AGREEMENT PHASE

This is a crucial and more technical phase of the scheme. This phase is completed in the following steps:

i. This is performed only when a user (U) is in the range of the Drone (D), the user (U) chooses a random number R_U and timestamp T_U, computes $S_1 = H(Z_1||T_U) \oplus ID_U)$, $S_2 = E_s(Z_2 \oplus R_U)$, $S_3 = H(PID_U||ID_U||T_U||R_U)$, and submits $\{S_1, S_2, S_3, T_U, PID_U\}$ message towards Drone (D) via a public network channel.

ii. Upon receiving the message form user (U), Drone (D) checks the validity T_S-$T_U \leq \Delta T$, decrypt S_2 to obtain Z_2 and R_U i.e. $D_l(S_2) = Z_2 \oplus R_U$, then Drone ($D$) choosesa nonce N_i and timestamp T_D, computes $Q_1 = H(sk||T_D) \oplus N_i$ and $Q_2 = E_s(H(S_1||S_2||N_i||ID_U||T_D||PID_D||T_U))$ and relays $\{S_1, S_2, S_3, T_D, PID_D, Q_1, Q_2, ID_U, T_U\}$ towards GCS over a public channel.

iii. Upon receiving $\{S_1, S_2, S_3, T_D, PID_D, Q_1, Q_2, ID_U\}$ message, the GCS decrypts Q_2 to obtain PID_D and ID_U, checks $T_D T_S$-$(T_D+T_U) \leq \Delta T$, Computes $I = S_1 \oplus H(sk||T_U)$ and confirms $S_2 = H(Q_1||Q_2||T_D||PID_D||I||ID_U||T_U)$. The GCS Computes $ID_D = S_2 \oplus H(H(S_{GCS}||PID_U||T_D)$ and $J = Q_2 \oplus H(ID_D||S_{GCS})$, confirms $S_3^{/} = H(PID_U||ID_U||T_U||R_U)$. The GCS selects another fresh pseudo-identity PID_{GCS} and time T_{GCS} and computes $K_{GCS} = H(ID_U||T_U||I||ID_D||N_i||T_D)$, $L_1 = H(N_i||sk||T_{GCS}) \oplus K_{GCS}$, $L_2 = H(I||K_{GCS}||T_{GCS}||ID_U)$, $L_3 = H(J||ID_D||T_{GCS})$, $L_4 = E_s(PID_{GCS} \oplus H(J||ID_D||T_{GCS}))$, $L_5 = H(S_{GCS}||PID_{GCS}) \oplus H(T_{GCS}||ID_D||J)$ and $L_6 = H(PID_D||ID_D||J||K_{GCS}||H(S_{GCS}||PID_{GCS})||T_{GCS})$; finally transmits $\{L_1, L_2, L_3, L_4, L_5, L_6, T_{GCS}\}$ message back towards Drone (D) over an open network channel.

iv. Upon receiving $\{L_1, L_2, L_3, L_4, L_5, L_6, T_{GCS}\}$ message by the Drone (D) it first decrypt $D_l(L_4) = PID_{GCS} \oplus H(J||ID_U||T_{GCS})$ to obtain PID_{GCS} and checks the time threshold T_S-$T_{GCS} \leq \Delta T$, if not found valid, the process terminates, else, computes $K_D = E_s(L_1 \oplus H(I||sk||T_{GCS}))$ and confirms $L_2^{/} = H(I||S_{GCS}||T_{GCS}||ID_U)$; if pass, the Drone ($D$) then transmits $\{L_3, L_4, L_5, L_6, T_{GCS}\}$ message toward user (U) over an open network channel.

v. User (U) first checks the timestamp T_S-$T_{GCS} \leq \Delta T$, decrypts $D_l(K_D) = L_1 \oplus H(I||sk||T_{GCS})$, computes $K_U = L_3 \oplus H(J||T_{GCS}||ID_D)$, $PID_{GCS} = L_4 \oplus H(J||ID_U||T_{GCS})$ and $Z_1^{new} = L_5 \oplus H(T_{GCS}||ID_U||J)$ and confirms $L_6 = H(PID_D||ID_D||J||K_{GCS}||Z_1^{new}||PID_{GCS}||T_{GCS})$, if founds valid, the U updates $\{Z_1, PID_D\}$ *with* $\{Z_1^{new}, PID_D^{/}\}$ as shown in phase 3.

E. DYNAMIC DRONE ADDITION PHASE

Suppose the GCS needs to dynamically add a newer drone for some other task or enhance existing drone capabilities (s). In that case, our protocol can provide the facility of adding a new drone to the system. Let suppose the newer drone is denoted by D^{new} and identity ID_D^{new}. The GCS extracts a unique identity ID_D^{new} and calculates

User (U)	Drone (D)	Ground-Control-Station (GCS)
Chooses a random number R_U		
Timestamp T_U		
Computes: $S_1=H(Z_1\|\|T_U)\oplus ID_U$		
$S_2=E_s(Z_2\oplus R_U)$		
$S_3=H(PID_U\|\|ID_U\|\|T_U\|\|R_U)$		
	$\{S_1, S_2, S_3, T_U, PID_U\}$ →	
	$T_S-T_U\leq\Delta T$	
	Decrypt $D_l(S_2)= Z_2\oplus R_U$	
	Choosesa nonce N_i *and time* T_D	
	Computes: $Q_1=H(sk\|\|T_D)\oplus N_i$	
	$Q_2=E_s(H(S_1\|\|S_2\|\|N_i\|\|ID_U\|\|T_D\|\|PID_D\|\|T_U))$	
		$\{S_1, S_2, S_3, T_D, PID_D, Q_1, Q_2, ID_U, T_U\}$ →
		$T_S-(T_D+T_U)\leq\Delta T$
		Decrypts Q_2 *to obtain* PID_D *and* ID_U, T_U
		$D_l(Q_2)=H(S_1\|\|S_2\|\|N_i\|\|ID_U\|\|T_D\|\|PID_D\|\|T_U)$
		Computes: $I=S_1\oplus H(sk\|\|T_U)$
		$S'_2=H(Q_1\|\|Q_2\|\|T_D\|\|PID_D\|\|I\|\|ID_U\|\|T_U)$
		Confirms: $S'_2?=S_2$
		Computes $ID_D=S_2\oplus H(H(S_{GCS}\|\|PID_U\|\|T_D)$
		$J=Q_2\oplus H(ID_D\|\|S_{GCS})$
		$S'_3= H(PID_U\|\|ID_U\|\|T_U\|\|R_U)$
		$S'_3?=S_3$
		Selects pseudo-identity PID_{GCS}
		Timestamp T_{GCS}
		Computes: $K_{GCS}=H(ID_U\|\|T_U\|\|I\|\|ID_D\|\|N_i\|\|T_D)$
		$L_1=H(N_i\|\|sk\|\|T_{GCS})\oplus S_{GCS}$
		$L_2=H(I\|\|K_{GCS}\|\|T_{GCS}\|\|ID_U)$
		$L_3=H(J\|\|ID_D\|\|T_{GCS})$
		$L_4=E_s(PID_{GCS}\oplus H(J\|\|ID_D\|\|T_{GCS}))$
		$L_5=H(S_{GCS}\|\|PID_{GCS})\oplus H(T_{GCS}\|\|ID_D\|\|J)$
		$L_6=H(PID_D\|\|ID_D\|\|J\|\|K_{GCS}\|\|H(S_{GCS}\|\|PID_{GCS})\|\|T_{GCS})$
		$\{L_1, L_2, L_3, L_4, L_5, L_6, T_{GCS}\}$ ←
	$T_S-T_{GCS}\leq\Delta T$	
	Decrypt $D_l(L_4)= (PID_{GCS}\oplus H(J\|\|ID_D\|\|T_{GCS}))$	
	Computes: $K_D= E_s(L_1\oplus H(I\|\|sk\|\|T_{GCS}))$	
	$L'_2= H(I\|\|K_{GCS}\|\|T_{GCS}\|\|ID_U)$	
	Confirm: $L'_2?=L_2$	
	$\{L_3, L_4, L_5, L_6, T_{GCS}\}$ ←	
$T_S-T_{GCS}\leq\Delta T$		
Decrypts $D_l(K_D)=L_1\oplus H(I\|\|sk\|\|T_{GCS})$		
$K_U= L_3\oplus H(J\|\|T_{GCS}\|\|ID_D)$		
$PID'_D=L_4\oplus H(J\|\|ID_U\|\|T_{GCS})$		
$Z_1^{new}=L_5\oplus H(T_{GCS}\|\|ID_U\|\|J)$		
$L'_6= H(PID_D\|\|ID_D\|\|J\|\|K_{GCS}\|\|H(S_{GCS}\|\|PID_{GCS})\|\|T_{GCS})$		
$L'_6?=L_6$		
$Z_1^{new}?=Z_1$		
Replace $\{Z_1, PID_D\}$ *with* $\{Z_1^{new}, PID'_D\}$ *and keep* K_{GCS}, K_D, K_U *as session shared key*		

Phase 3. **Key-agreement phase.**

$Z_1^{new} = H(S_{GCS}||PID_D^{new})$, $Z_2^{new} = H(ID_D^{new}||S_{GCS})$, stored ID_D^{new} in the memory of the newer drone and transmits $\{ID_D^{new}, Z_1^{new}, Z_2^{new}, PID_D^{new}\}$ towards the newer drone over a private channel. Finally, the newer drone stores $\{ID_D^{new}, Z_1^{new}, Z_2^{new}, PID_D^{new}\}$ and GCS keep their record also in their database for future correspondence.

F. DRONE REVOCATION PHASE

If the drone falls/fails, is caught by attackers, or is controlled by an undesirable entity while its data is present in the GCS,it poses a threat. The threat emanates its usage for nefarious purposes. Therefore, if its connection with the system is lost, the data needs to be secured by washing it out to keep the central system in order. The suggestions are made for the purpose as let a list reserved for saving the unique identity of takedown, captured, crashed, or compromised drone, add a private key sk to the list and then delete it from the record like $Z_1^{del} = h(ID^{del}||sk)$, $Z_2^{del} = h(ID_{del}||S_{GCS})$ and remove the tuple $\{Z_1^{del}, Z_2^{del}, ID^{del}, sk\}$. The GCS then matches Z_1^{del} with Z_1 and Z_2^{del} with Z_2, and if matched, it means the record of a compromised drone is still available in the system; otherwise, the deletion process has successfully been accomplished.

IV. SECURITY ANALYSIS

The key secrecy, reachability, authenticity, and confidentiality of the proposed protocol were verified by using a well-known programming toolkit, ProVerif2.02. Its code has been given in appendix – A of the paper. In contrast, the security of the PKI-based authentication protocol has also been conducted on a world-widely used method [27] called ROR (Real-Or-Random) model. Using RoR, our key-agreement scheme consists of two main entities, an adversary $\mathcal{A}$, and a responder $\mathcal{R}$. $\mathcal{A}$ established communication with GCS, let E_i denotes GCS, whereas i indicated the i^{th} occurrence of GCS; E_{DS} means adversary action to impersonate GCS or user/(Drone) by forging $\{ID_U, sk\}$. E_{SD} can also forge s or l, R_U, for impersonating any participant; E_{SC} is considered to be an action of the adversary for semantic security of the proposed mechanism, which is given as under:

i. ***Setup Query*** in which challenger C returns system parameters to $\mathcal{A}$.
ii. ***Hash Query*** in which C can store a list of parameters, apply one-way hash function hS_1, S_2, S_3) and h(L_1, L_2, L_3, L_4, L_5, L_6), and generates a random nonce NA of order prime and stored with any of the given hash messages and return it to $\mathcal{A}$.
iii. ***MAC*(Mi):** Next, C authenticates the message; if succeeded, return Mi to $\mathcal{A}$.
iv. ***Send*(*Ei*, Mi):** Now, C sends it towards GCS, acts as a legitimate user or drone, the response received also return to $\mathcal{A}$, but in our framework, we have added an extra steps $S_2^{/}? = S_2, S_3^{/}? = S_3$, during the computation of GCS. Before going to the next step, GCS must confirm $S_2^{/}? = S_2$ and $S_3^{/}? = S_3$, which in turn C cannot verify. Let suppose anything received by C can return to $\mathcal{A}$.
v. ***Execute*(Di$^{\infty}$, *GCS*)**: Upon sending, the proposed protocol returns l or s.
vi. ***Reveal(Ei)***: C given h(S_1, S_2, S_3) and h(L_1, L_2, L_3, L_4, L_5, L_6) to $\mathcal{A}$.
vii. ***Test(Ei)***: In this step, $\mathcal{A}$ can flip a coin if the output becomes 1, which means $\mathcal{A}$ won, 0 loss.

Similarly, the collision-free one-way hash function h is acceptable to U, D, GCS, and $\mathcal{A}$, and we modeled it as an oracle Oh. We will analyze the security of the h function used in the KAS-IoD in the following manner.

Let adversary $\mathcal{A}$ runs a polynomial times TM against the KAS-IoD using different parameters of an oracle O_h. Furthermore, let D is distributed dictionary of random numbers g. The probability with the adversary $\mathcal{A}$ to compromise our KAS-IoD is:

- $(Prob)_{\mathcal{A}}^{KAS-IoD} = (q_h^2/|h|)+(q_s/(2^{g-1}|D|))$
- $(Prob)_{\mathcal{A}}^{KAS-IoD} = |2Prob[Success_0]-1|$ is used by an adversary $\mathcal{A}$ for choosing an actual number to launch a fundamental attack on our KAS-IoD.
- An adversary uses $Prob[Success_1] = Prob[Success_0]$ for modeling whether the session key is real or random.
- $Prob[Success_1]$-$Prob[Sucess_2] \leq (q_h^2/2|h)$ equation is used by an adversary for fabricating any message of IoD's participants. Nevertheless, $\mathcal{A}$ cannot, as all the identities, random numbers, and other credentials are hidden in our KAS-IoD by hash function.

V. PERFORMANCE ANALYSIS

The performance can be evaluated by analyzing the computation, storage, and communication costs. Each is described as under:

A. COMPUTATION COST ANALYSIS

The computation cost based on the total computation cost of the proposed authentication scheme is 4.0198ms. The work done by [30] on Samsung Galaxy S5 of specification CPU 2.45Ghz Quad-Core, OS Android and 4GB RAM and Dell Personal Computer (PC) of specification Corei5, 4^{th} Generation 2.90Ghz, OS Microsoft Windows 8.1, 4GB RAM. Considering the PC as GCS and S5 as the D/Drone, the computation costs for different operations are described in Table 2. In the registration phase of the proposed authentication scheme, the total computation cost is $2t_h+0t_{\oplus}$. In the key agreement phase, D takes $6t_h+5t_{\oplus}$, DR $4t_h+5t_{\oplus}$, and GCS $14t_h+7t_{\oplus}$, so the total cost in the key-agreement phase equals $24t_h+17t_{\oplus}$. Now, hash-function takes 0.0552ms = cost $24 \times 0.0552 = 1.3248$ms, the computation cost for XOR is negligible equal to zero. And random numbers/Pseudo-Identity/Timestamp generation takes 0.539ms $= 5$ x $0.539 = 2.695$ms.

TABLE 2. Computation cost analysis.

Notation	Description	Execution Time in millisecond for different operations in Drone/D	Execution Time in milliseconds for various functions in GCS
T_h	Execution time for One-Way Hash-Function	0.056	0.007
T_{mul}	Modular multiplication	0.008	0.0001
T_{bp}	Execution time for Bilinear Mapping	32.713	5.427
T_{ext}	Execution time for exponentiation	2.249	0.001

B. STORAGE OVERHEADS ANALYSIS

As per experiment done by [30], ID_U, ID_D, pseudo-identity PID_D and PID_{GCS2} each one takes 64 bits space $= 5 \times 64 = 320$ bits occupy memory, k_j, S_{GCS} each one stored in 160 bits space $= 2 \times 160 = 320$ bits store in memory and T_D, T_U, T_{GCS} each takes 56 bits space $= 3 \times 56 = 168$ bits in memory space. Therefore, total storage overheads for the proposed authentication scheme are 808 bits memory space.

C. COMMUNICATION COST ANALYSIS

Here in this section, the space taken by each one message transmitted over public network channel. In this regard, Message $1 = \{S_1, S_2, S_3, T_D, PID_D\} = \{160 + 160 + 160 + 56 + 64\} = 600$ bits, Message $2 = \{S_1, S_2, S_3, T_U, PID_D, Q_1, Q_2, ID_U\} = \{160 + 160 + 160 + 56 + 64 + 160 + 160 + 64\} = 984$ bits, Message $3 = \{L_1, L_2, L_3, L_4, L_5, L_6, T_{GCS}\} = \{160 + 160 + 160 + 160 + 160 + 160 + 56\} = 1016$ bits, and Message $4 = \{L_3, L_4, L_5, L_6, T_{GCS}\} = \{160 + 160 + 160 + 160 + 56\} = 696$ bits. Therefore the total computation costs for the proposed authentication scheme are 3296 bits are transmitted over the line which is said to be the communication costs.

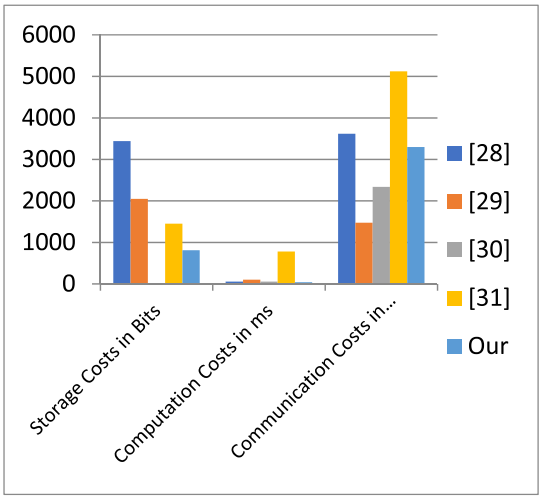

FIGURE 2. Comparison analysis.

TABLE 3. Comparison analysis.

Protocol / Attributes	[28]	[29]	[30]	[31]	Our
Storage Costs in Bits	3440	2048	XX	1448	808
Computation Costs in ms	53.734	100.00	54.292	779.00	40.198
Communication Costs in Bits	3616	1472	2336	5120	3296

D. COMPARISON ANALYSIS

By comparing the proposed protocol with Wu *et al.* [28], Zhang *et al.* [29], Nikooghadam *et al.* [30], and Teng *et al.* [31] in terms of storage overheads analysis, communication, and computation time complexity, it has been demonstrated that the proposed key agreement protocol for IoD deployment civilian drone is better as shown in Table 3.

The communication cost of the proposed scheme is slightly different from that of [29] and [30], but accurately satisfies the necessary needs of drones in IoD, but its computation cost and storage overheads are much better than that of other protocols; graphically, it can be represented as in Fig. 2.

VI. CONCLUSION

As seen in the literature, the operations of drones were not without attendant problems in an age that is dominated by technology, as seen in drones, AI, and robots, etc. however, these latest technologies are not without some loopholes. This study identified some loopholes causing security hazards to the researchers. As discussed, drone technology still suffers from security-related problems despite its efficacy and potential economic benefits. The IoD architecture is mainly experienced by security (e.g., confidentiality, integrity, access, authentication, authorization, and data breaches/dynamic session key updating flaw) and issues of data management (e.g., dynamisms, data segregation, backup, and virtualization). To countermeasure these, the researchers have designed a security protocol based on Public Key Infrastructure (PKI) in which public-private key pair is computed on ground control station (GCS) for a single session only and then going to null after completion of secure communication. The security analysis section has been solved using the ROR model. At the same time, the performance result shows that the proposed key-agreement scheme is robust, efficient, and ensures mutual authentication, forward secrecy, and cross-verification during data broadcasting.

APPENDIX A

For checking session key secrecy, confidentiality, and reachability, a software verification toolkit, ProVerif2.02, is used. The ProVerif2.02 simulation code for the proposed scheme is given as under:

```
(* ==========================*)
free Prch1: channel [private].
free Prch2: channel [private].
```

```
free Pubch1: channel.
free Pubch2: channel.
(* ============================*)
freeSgcs:bitstring [private].
freeKgcs:bitstring [private].
freeKd:bitstring [private].
freeKu:bitstring [private].
freesk:bitstring [private].
constIDu:bitstring [private].
constIDd:bitstring.
freeru:bitstring.
free l:bitstring.
free s:bitstring.
freetu:bitstring.
freetd:bitstring.
freetgcs:bitstring.
(* ============================*)
table d1(bitstring,bitstring).
table d2(bitstring,bitstring).
(* ============================*)
fun con(bitstring,bitstring):bitstring.
funxor(bitstring,bitstring):bitstring.
fun h(bitstring):bitstring.
(* ============================*)
equation forall m:bitstring,n:bitstring;xor(xor(m,n),n) = m.
(* ============================*)
eventUStart(bitstring).
eventUAuth(bitstring).
eventDStart(bitstring).
eventDAuth(bitstring).
eventGCSStart(bitstring).
eventGCSAuth(bitstring).
query attacker(SKgcs).
query attacker(SKd).
query attacker(SKu).
queryid:bitstring;inj-event(DAuth(id))==> inj-
event(DStart(id)).
queryid:bitstring;inj-event(UAuth(id))==> inj-
event(UStart(id)).
queryid:bitstring;inj-event(GCSAuth(id))==> inj-
event(GCSStart(id)).
(* ============================*)
let U = out(Prch1,(IDu));
in(Prch1,(S1:bitstring,S2:bitstring,
S3:bitstring,PIDu:bitstring, Tu:bitstring));
!
(
eventUStart(IDu);
newtu:bitstring;
newru:bitstring;
let S1 = xor(h(con(Z1,tu)),IDu)in
let S2 = xor(Z2,ru)in
let S3 = h(con(con(con(PIDu,IDu),tu),ru))in
let Message1 = (S1,S2,S3,tu,PIDu)in
out(Pubch1,Message1);
in(Pubch1,(L3u:bitstring,L4u:bitstring,L5U:bitstring,
L6U:bitstring,tgcs:bitstring));
let SKu = xor(L3u,h(con(con(ru,tgcs),IDu)))in
let PIDudash = xor(L4u,h(con(con(ru,IDu),tgcs)))in
let Z1new = xor(L5u,h(con(con(tgcs,IDu),ru)))in
if L6udash = h(con(con(con(con(con(PIDudash,IDu),ru),
SKu),Z1new),tgcs))then
let Z1 = Z1new in
letPIDu = PIDunew in
0
).
(* ============================*)
let D = out(Prch2,IDD);
in(Prch2,(sk:bitstring));
!
(
in(Pubch1,(L1D:bitstring,L2D:bitstring,L3D:bitstring,
tD:bitstring,PIDD:bitstring));
eventDStart(IDRj);
newNi:bitstring;
newtD:bitstring;
let Q1 = xor(h(con(Z2,Ni)),sk)in
let Q2 = h(con(con(con(con(con(con(S1D,S2D),
tD),PIDD),Ni),IDD),tD))in
let Message2 = (S1D,S2D,S3D,tD,PIDD,Q1,Q2,
IDD,tu)in
out(Pubch2,Message2);
in(Pubch2,(L1D:bitstring,L2D:bitstring,L3D:bitstring,
L4D:bitstring,L5D:bitstring,L6D:bitstring,tgcs:bitstring));
let SKd = xor(L1D,h(con(con(Ni,sk),tgcs)))in
if L2R = h(con(con(con(rgcs,SKd),tgcs),IDd))then
let Message3 = (L3D,L4D,L5D,D6R,tgcs)in
out(Pubch1,Message3);
0
).
(* ============================*)
let u = in(Prch1,(IDu:bitstring));
newPIDu:bitstring;
let Z1 = h(con(xu,PIDu))in
let Z2 = xor(h(con(IDu,xu)),PIDu)in
insert d2(IDu);
out(Prch1,(Z1,Z2,PIDu)).
(* ============================*)
let D = in(Prch2,IDd:bitstring);
newsk:bitstring;
insert d1(IDd,sk);
out(Prch2,(sk)).
(* ============================*)
letgcs = in(Pubch2,(S1gcs:bitstring,S2gcs:bitstring,
S3gcs:bitstring,
tgcsgcs:bitstring,PIDdgcs:bitstring,S1gcs:bitstring,
S2gcs:bitstring,IDugcs:bitstring,td:bitstring));
get d1( = IDd,sk)in
let J = xor(Q1gcs,h(con(sk,tgcsgcs)))in
if Q2gcs = h(con(con(con(con(con(con(S1gcs,
S2gcs),tdgcs),PIDdgcs),J), IDdgcs),tgcsgcs))then
eventDAuth(IDdgcs);
```

```
let IDdgcs = xor(S1gcs,h(con(h(con(Sgcs,PIDdgcs)),
tdgcs))) in get d2( = IDdgcs)in let rdTAgcs S3gcs = h
(con(con(con(PIDdgcs,IDdgcs),tdgcs),rdgcs))then
eventUAuth(IDdgcs);
newPIDdgcsdash:bitstring;
newtgcs:bitstring;
let SKgcs = h(con(con(con(con(con(IDdgcs,tdgcs),
rdgcs),IDugcs), Nigcs),J))in
let L1 = xor(h(con(con(Jgcs,sk),tgcs)),SKgcs) in
let L2 = h(con(con(con(J,SKgcs),tgcs),IDdgcs))in
let L3 = xor(h(con(con(rdgcs,tgcs),IDdgcs)),SKgcs)in
let L4 = xor(PIDdgcsdash,h(con(con(rdgcs,IDdgcs),
tgcs)))
in
let L5 = xor(h(con(Sgcs,PIDdgcsdash)),h(con(
con(tgcs,IDdgcs), rdgcs)))in
let L6 = h(con(con(con(con(con(PIDdgcsdash,
IDdgcs),rdgcs), SKgcs),h(con(Sgcs,PIDdgcsdash))),
tgcs))in
let Message3 = (L1,L2,L3,L4,L5,L6,tgcs)in
out(Pubch2,Message3).
(* ==========================*)
let GCS = U|D|gcs.
process ((!U)|(!D)|(!GCS))
```

ACKNOWLEDGMENT

The authors would like to express their sincere thanks to the University of Bisha, Bisha, Saudi Arabia, for the support provided during the research.

REFERENCES

[1] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of Drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[2] 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 Syst. J.*, 2021.

[3] S. U. Jan, F. Qayum, and H. U. Khan, "Design and analysis of lightweight authentication protocol for securing IoD," *IEEE Access*, vol. 9, pp. 69287–69306, 2021.

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

[5] J. R. Vacca, *Computer and Information Security Handbook*. Waltham, MA, USA: Newnes, 2012.

[6] R. L. Orsini, M. S. O'hare, and R. Davenport, "Systems and methods for managing cryptographic keys," U.S. Patent 8 135 134, Mar. 13, 2012.

[7] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, *Computer Security: Principles and Practice*. Upper Saddle River, NJ, USA: Pearson, 2012.

[8] P. Derbeko, S. Dolev, E. Gudes, and S. Sharma, "Security and privacy aspects in MapReduce on clouds: A survey," *Comput. Sci. Rev.*, vol. 20, pp. 1–28, May 2016.

[9] A. Almulhem, "Threat modeling of a multi-UAV system," *Transp. Res. A, Policy Pract.*, vol. 142, pp. 290–295, Dec. 2020.

[10] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, "A data authentication scheme for UAV ad hoc network communication," *J. Supercomput.*, vol. 76, pp. 4041–4056, Jun. 2020.

[11] Y. Li, X. Du, and S. Zhou, "A lightweight identity authentication scheme for UAV and road base stations," in *Proc. Int. Conf. Cyberspace Innov. Adv. Technol.*, New York, NY, USA, Dec. 2020, pp. 54–58.

[12] T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A novel authentication scheme for drone-assisted 5G networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2021, pp. 1–6.

[13] P. Gope, O. Millwood, and N. Saxena, "A provably secure authentication scheme for RFID-enabled UAV applications," *Comput. Commun.*, vol. 166, pp. 19–25, Jan. 2021.

[14] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria, "GCACS-IoD: A certificate based generic access control scheme for Internet of Drones," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107999.

[15] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[16] S.-H. Seo, J. Won, E. Bertino, Y. Kang, and D. Choi, "A security framework for a drone delivery service," in *Proc. 2nd Workshop Micro Aerial Vehicle Netw., Syst., Appl. Civilian Use*, Jun. 2016, pp. 29–34.

[17] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354.

[18] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, Apr. 2020.

[19] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of Internet of Drones (IoD): A review," *IEEE Sensors J.*, early access, Sep. 23, 2021, doi: 10.1109/JSEN.2021.3114266.

[20] X. Meng, J. Xu, W. Liang, Z. Xu, and K.-C. Li, "A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for Internet of Vehicles," *Comput. Electr. Eng.*, vol. 95, Oct. 2021, Art. no. 107431.

[21] M. Adil, J. Ali, M. Attique, M. M. Jadoon, S. Abbas, S. R. Alotaibi, V. G. Menon, and A. Farouk, "Three byte-based mutual authentication scheme for autonomous Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 29, 2021, doi: 10.1109/TITS.2021.3114507.

[22] S. Kumar, H. Banka, B. Kaushik, and S. Sharma, "A review and analysis of secure and lightweight ECC based RFID authentication protocol for Internet of Vehicles," *Trans. Emerg. Telecommun. Technol.*, p. e4354, Sep. 2021, doi: 10.1002/ett.4354.

[23] 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.

[24] 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 Commun.*, vol. 15, no. 5, pp. 61–76, May 2018.

[25] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of Vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[26] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.

[27] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.

[28] L. Wu, J. Wang, K.-K.-R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.

[29] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Oct. 2020.

[30] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.

[31] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards UAV networks," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 379–384.

SAEED ULLAH JAN received the Ph.D. degree in network security from the University of Malakand, in 2021. He is currently working as a Lecturer in computer science at the Higher Education, Achieves and Libraries Department, Government of Khyber Pakhtunkhwa, Pakistan. He is also working as a Coordinator for nine B.S. disciplines at the Government College Wari (Dir Upper)—a far-flung remote area of the province, where most of the youngsters have no access to Universities/Institutions for higher education. Furthermore, he has conducted research in many areas, including green computing, distributed computing, privacy-preserving parallel computation, and drone security and authentication. He has published over 15 research articles in prestigious conferences and journals and written an introductory book in computer science for beginners. The Government of Khyber Pakhtunkhwa awarded the Best Teacher Award for the year 2019–2020 out of 11000 college teachers in 309 public sector colleges in the province.

IRSHAD AHMED ABBASI received the Ph.D. degree in computer science from Universiti Malaysia Sarawak, Malaysia, and the M.S. degree in computer science from COMSATS University, Pakistan. He worked as a Senior Lecturer at King Khalid University, Saudi Arabia, from 2011 to 2015. He is currently working as an Assistant Professor with the Computer Science Department, University of Bisha, Saudi Arabia. He has over 12 years of research and teaching experience. He is the author of many articles published in top quality journals. His research interests include VANETs, MANETs, FANETs, mobile computing, the IoT, cloud computing, and drone security and authentication. He was declared as the Best Teacher at the Faculty of Science and Arts Belqarn, University of Bisha, in 2016. He has received multiple awards, scholarships, and research grants. He is serving as an editor. He is also acting as a reviewer for many well reputed peer-reviewed international journals and conferences.

FAHAD ALGARNI received the bachelor's degree (Hons.) from the Department of Computer Science, King Abdulaziz University, the M.I.T. degree in computer networks from La Trobe University, Melbourne, Australia, and the Ph.D. degree from the Clayton School of Information Technology, Monash University, Melbourne. He is currently the Dean of the College of Computing and Information Technology, University of Bisha, Saudi Arabia. His research interests include wireless sensor networks, cloud computing, systems' design and reliability, the IoT, and cyber security.