A Key Agreement Scheme for IoD Deployment
Civilian Drone

Saeed Ullah Jan¹, Irshad Ahmed Abbasi², and Fahad Algarni²
¹Department of Computer Science & IT, University of Malakand, Chakdara, 18800, Pakistan
²Faculty of Science & Arts, Department of Computer Science, University of Bisha, Belqarn, Subt Al-Alaya, 61985, Saudi Arabia
Corresponding author: Irshad Ahmad Abbasi (e-mail:irshad_upesh@yahoo.com).

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 relief, and security. Drone’s 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 (FANET)). These operations are no less important in areas like 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 designers have to strive towards a secured drone operation by developing a robust and lightweight key agreement protocol for IoD deployment civilian drone. Consequently, the researchers in this study have attempted to design a verifiably secure and lightweight authentication scheme for IoD deployment civilian drones. The proposed security protocol 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 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 later, 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 verifiably secure, lightweight, and robust authentication 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. 2.

![Figure 1: System Architecture](image)

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
- Collision 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, and each UAV sends data security to the cluster head. In this regard, they used a double watermarking authentication strategy. The cluster head, first authenticates the integrity of data received from other UAVs and then aggregates it by applying the chaotic map method. However, the said technique is not operational 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 the sensitive task. So, they proposed an 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 Uncloneable 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 concept of physical Uncloneable function (PUF), in which they claimed that PUF-enabled RFID equipment in the tag of UAV could execute the receiving signals in a fast and secure manner. According to Chaudhry et al. [14], the IoD can apply to acquired real-time data for interpretation by different participants, as many drones flying in various zones to carry out the assigned tasks; in this regard, the IoD can be beneficial to gather real-time data for interpretation by users. The data is accessed through an open network channel and less battery-powered of drones; as a result, the security and privacy of drones are essential for mission-critical, safety-critical, or surveillance activities. Therefore, they created a generic certificate-based access control method to allow inter-drone and drone to ground station access control/authentication (GCACS-IoD) framework to address the above-mentioned tactical task. However, anyone can quickly launch a man-in-the-middle attack because the nonce exchange is performed open via a public network channel, in [14] constructed identity and ECC-based triple authentication scenario consisting of initiation of certification, identity authentication, and consistent
essential verification. Nevertheless, the scheme is difficult to implement in the real-world environment due to scalar multiplication and key escrow problem. Also, the security features being utilized for the Internet of Things (IoT) can be implemented in an IoD environment to communicate securely with each other and with the GSC. But network topology development is incorporated for drones in IoD because it is used for consumer conveniences like entertainment, toys, agricultural-land monitoring, high-value industries, and wide applications in the defense field shooter product [15].

Seo et al. [16] said that if someone can improve UAV’s battery power, sensing systems, security, and other technologies and incorporating them into it, it will be considered a top-rated product in the market for advancing various fields and activities. In such cases, very small UAVs can be utilized for enormous tasks and significant application versatility, like personal aerial photography, entertainment, commercial markets, etc. It can also be used in a range of surveillance activities, such as disaster relief, in diverse environments involving animals and plants, coasts and borders, transport goods, military and police enforcement tasks, and agricultural and industrial applications. The smart city features like traffic monitoring and management, merchandise distribution, health and emergency services, and air taxi services can 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 WSN. They used the elliptic curve discrete logarithmic function for secure computing keys between the participants. However, it still suffered from a key-escrow problem.

Abualigah et al. [19] provided a thorough investigation 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 and fog frameworks, WSN, mobile computing, and business paradigms; and IoD integration, which includes privacy protection, security authentication, neural networks, blockchain, and optimization-based methods. This is an interesting paper for the researchers who are looking for research in IoD. Internet of Vehicles (IoV) is defined as the use of the Internet of Things (IoT) in transportation, according to Meng et al. [20]. On the Internet of Vehicles, each car will function as a separate node with the capacity to gather data and transfer it to the network. A lightweight anonymous mutual authentication and key agreement scheme are required for this purpose. As a result, 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 state of the art 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).

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. However, because enabling IoD-based technologies have limited authentication rights for mobile users, Al-Tarjman et al. [23] developed a security mechanism based on bilinear pairing and elliptic-curve cryptosystems. Their system meets security requirements and is resistant to node capture attempts. Chen et al. [24] came up with a new authentication mechanism. They chose message authentication over identity instead of the user. Because unmanned aerial vehicles (UAVs) are operated without humans, their method was appealing because it seemed an accurate platform between authentication and anonymity. Their security approach was based on symmetric pairing, which consisted of bunches of identities and made malicious module-altering attacks challenging for an adversary. The scheme has achieved credential randomization, batch proof, cross-verification, and mutual authentication. Chen et al. [25] found flaws in previous protocols, including an offline identity guessing attack, location spoofing attack, replay attack, and longer to authenticate. They proposed an improved mechanism based on the Computational Diffie-Hellman Problem (CDHP) and discrete logarithms Problem (DLP).

Cho et al. [26] devised the SENTINEL protocol to reduce the computational and traffic overheads associated with certificate exchanges and asymmetric cryptography calculations, standard in previous authentication methods. Their scenario first creates a flight session key for a drone, flight plan, records the flight session key, and the drone’s flight plan in a centralized database that ground stations may access. While the drone is flying, the registered flight session key is the message authentication code to authenticate the drone by the ground station.

Therefore, keeping in view the literature study mentioned above, it has been concluded that 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 cannot make it feasible for IoD deployment civilian drones.

III. PROPOSED SCHEME
This simple hash cryptographic function and PKI-based protocol are lightweight and robust 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 I.

### Table I
**SUMMARY OF NOTATIONS**

| Notation | Description |
|----------|-------------|
| U        | User        |
| D        | Drone       |
| GCS      | Ground-Control-Station |
| ID_U     | User’s Identity |
| X_{GCS}  | GCS secret key |
| k_U      | User’s secret key |
| PID_D    | Drone’s Identity |
| PID_U    | User’s pseudo-identity |
| R_D      | User’s random number |
| s, t     | Public-private key pair |
| L, D, T_{GCS} | Time-stamp |

#### A. SETUP/INITIALIZATION PHASE
The Ground-Control-Station (GCS) first generates a secret key $X_{GCS}$ and collision-free one-way hash function $H(\cdot):\{0, 1\}^* \rightarrow \{0, 1\}^l$.

#### 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 $k_U$. The record of a user ($ID_U$, $k_U$) is stored in the database of Ground-Control-Station (GCS) and also sends it to a user (U) through a secure channel.

**User (U) → Ground-Control-Station (GCS)**

- Selects Identity $ID_U$
- Extracts $k_U$.
- Stores $\{ID_U, k_U\}$ 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 $PID_D$. It computes $Z_D = H(X_{GCS}||PID_D)$, injects $ID_D$ in the database, and transmits $\{ID_D, Z_D, Z_{ID}\}$ to Drone through a secure channel.

### Drone (D) → Ground-Control-Station (GCS)

- Selects Identity $ID_D$
- Selects Pseudo-Identity $PID_D$
- Computes: $Z_D = H(X_{GCS}||PID_D)$
- $Z_{ID} = H(ID_D||X_{GCS})$
- Stores $\{ID_D, PID_D, Z_D, Z_{ID}\}$

**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 $S_1 = H(Z_D||T_U||ID_U)$, and submits $\{S_1, S_2, S_3, T_U, PID_U\}$ message towards Drone (D) through a secure channel.

ii. Upon receiving the message form user (U), Drone (D) decrypts $S_2$ to obtain $Z_D$ and $R_U$. It then chooses another nonce $N$ and timestamp $T_D$, computes $Q_1 = H(k_U||T_D||R_U)$, and sends $\{Q_1, S_3, T_D, PID_D, Q_2, ID_U, T_U\}$ message 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 $T_D$, checks $T_D - T_U < \Delta T$, selects another fresh pseudo-identity $PID_GCS$ and time $T_{GCS}$, and computes $K_{GCS} = H(ID_D||T_{GCS}||ID_U||N||T_D)$, $L_1 = H(N)||k_U||T_{GCS}||T_D\rangle\oplus K_{GCS}$, $L_2 = H(L_1||ID_D||T_{GCS}||ID_U)$, $L_3 = H(X_{GCS}||PID_D||T_{GCS}||ID_D)$, and $L_4 = H(PID_D||ID_D||T_{GCS}||ID_U)$.

iv. The GCS computes $L_5 = H(ID_D||T_{GCS}||ID_U)$, then forwards $\{L_1, L_2, L_3, L_4, L_5, T_{GCS}\}$ message back towards Drone (D) over an open network channel.

v. Upon receiving $\{L_1, L_2, L_3, L_4, L_5, T_{GCS}\}$ message by the Drone (D) it first decrypts $D_1 = PID_D||H(L_1||ID_D||T_{GCS})$ to obtain PID_GCS and checks the time threshold $T_D - T_{GCS} \leq \Delta T$, if not found valid, the process terminates, else, computes $K_D = H(L_1||ID_D||T_{GCS})$, forwards $L_6 = H(L_1||ID_D||T_{GCS})$, and submits $\{L_6, L_7, L_8, L_9, T_{GCS}\}$ message toward user (U) over an open network channel.

vi. User (U) first checks the timestamp $T_D - T_{GCS} \leq \Delta T$, decrypts $D_1 = PID_GCS||H(L_1||ID_D||T_{GCS})$, computes $K_U = H(L_1||ID_D||T_{GCS})$.
| User (U) | Drone (D) | Ground-Control-Station (GCS) |
|----------|-----------|-------------------------------|
| Chooses a random number $R_U$ | Timestamp $T_U$ | Computes: $S_1 = H(Z_1 || T_U) \oplus ID_U$ |
| | | $S_2 = E_K(Z_2 \oplus R_U)$ |
| | | $S_3 = H(PID_U || ID_U || T_U || R_U)$ |
| $[S_1, S_2, S_3, T_U, PID_U]$ | $T_{S-T_U} \leq \Delta T$ | Decrypt $D_3(S_2) = Z_2 \oplus R_U$ |
| | | Chooses a nonce $N_i$ and time $T_D$ |
| | | Computes: $Q_1 = H(k_i || T_D) \oplus N_i$ |
| | | $Q_2 = E_K(S_1 || S_2 || N_i || ID_U || T_D || PID_U || T_U)$ |
| | $[S_1, S_2, S_3, T_D, PID_U, Q_1, Q_2, ID_U, T_U]$ | $T_{S-T_D+T_U} \leq \Delta T$ | Decrypts $Q_2$ to obtain $PID_D$ and $ID_U$, $T_U$ |
| | | $D_2(Q_2) = H(S_1 || S_2 || N_i || ID_U || T_D || PID_U || T_U)$ |
| | | Computes: $I = S_1 \oplus H(k_i || T_D)$ |
| | | $S_2 = H(Q_2 || Q_1 || T_D || PID_U || I || ID_U || T_U)$ |
| | | Confirms: $S_2' = S_2$ |
| | | Computes $ID_D = S_2 \oplus H(H(X_{GCS}) || PID_U || T_D)$ |
| | | $J = Q_2 \oplus H(ID_U || X_{GCS})$ |
| | | $S_3' = H(ID_U || T_D || R_U)$ |
| | | $S_3' = S_3$ |
| | | Selects pseudo-identity $PID_{GCS}$ |
| | | Timestamp $T_{GCS}$ |
| | | Computes: $K_{GCS} = H(ID_U || T_D || I || ID_U || N_i || T_D)$ |
| | | $L_1 = H(N_i || k_i || T_{GCS} \oplus K_{GCS})$ |
| | | $L_2 = H(I || K_{GCS} || T_{GCS} || ID_U)$ |
| | | $L_3 = H(I || ID_U || T_{GCS})$ |
| | | $L_4 = E_K((PID_{GCS} \oplus H(J || ID_U || T_{GCS}))$ |
| | | $L_5 = H(X_{GCS}) || PID_{GCS} \oplus H(T_{GCS} || ID_U || J)$ |
| | | $L_6 = H(PID_{GCS} || ID_U || J || K_{GCS} || H(X_{GCS}) || PID_{GCS} || T_{GCS})$ |
| | $[L_1, L_2, L_3, L_4, L_5, L_6, T_{GCS}]$ | $T_{S-T_{GCS}} \leq \Delta T$ |
| | | Decrypts $D_3(K_D) = L_1 \oplus H(I || k_i || T_{GCS})$ |
| | | Computes: $K_D = E_K(L_1 \oplus H(I || k_i || T_{GCS}))$ |
| | | $L_2' = H(I || K_{GCS} || T_{GCS} || ID_U)$ |
| | | Confirms: $L_2' = L_2$ |
| | $[L_2, L_4, L_5, L_6, T_{GCS}]$ | $T_{S-T_{GCS}} \leq \Delta T$ |
| | | Decrypts $D_3(K_D) = L_1 \oplus H(I || k_i || T_{GCS})$ |
| | | Computes: $K_D = E_K(L_1 \oplus H(I || k_i || T_{GCS}))$ |
| | | $PID_D = L_4 \oplus H(I || ID_U || T_{GCS})$ |
| | | $Z_{i^{new}} = L_5 \oplus H(T_{GCS} || ID_U || J)$ |
| | | $L_6' = H(PID_D || ID_U || J || K_{GCS} || H(X_{GCS}) || PID_{GCS} || T_{GCS})$ |
| | | $L_6' = L_6$ |
| | | $Z_{i^{new}} = Z_i$ |
| | | Replace $\{Z_i, PID_D\}$ with $\{Z_{i^{new}}, PID_D\}$ and keep $K_{GCS}, K_D, K_U$ as session shared key |

**Phase 3: Login & Authentication Phase**
and $Z_{i}\text{new} = L_{i}\mathcal{E}H(T_{GCS})||ID_{i}||J$ and confirms $L_{i}=H(PID_{D}||ID_{D}||I||K_{GCS}||Z_{i}\text{new}||PID_{D}||T_{GCS})$, if founds valid, the $U$ updates $[Z_{i}, PID_{D}]$ with $[Z_{i}\text{new}, PID_{D}]$. Finally $K_{GCS}$, $K_{D}$ and $K_{U}$ are the session shared keys for Ground-Control-Station (GCS), user ($U$) and Drone ($D$) respectively. All participants share key $K_{GCS,D,U}$ for secure communication with each other.

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 $D_{\text{new}}$ and identity $ID_{D_{\text{new}}}$. The GCS extracts a unique identity $ID_{D_{\text{new}}}^{\text{new}}$ and calculates $Z_{1}\text{new} = H(X_{GCS}||PID_{D_{\text{new}}})$, $Z_{2}\text{new} = H(ID_{D_{\text{new}}}||X_{GCS})$, stored $ID_{D_{\text{new}}}^{\text{new}}$ in the memory of the newer drone and transmits $\{ID_{D_{\text{new}}}^{\text{new}}, Z_{1}\text{new}, Z_{2}\text{new}, PID_{D_{\text{new}}}^{\text{new}}\}$ towards the newer drone over a private channel. Finally, the newer drone stores $\{ID_{D_{\text{new}}}^{\text{new}}, Z_{1}\text{new}, Z_{2}\text{new}, PID_{D_{\text{new}}}^{\text{new}}\}$ 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 $Z_{i}\text{del} = h(ID_{D_{i}}||sk)$, $Z_{2}\text{del} = h(ID_{D_{i}}||X_{GCS})$ and remove the tuple $\{Z_{1}\text{del}, Z_{2}\text{del}, ID_{D_{i}}\}$, $sk$). The GCS then matches $Z_{1}\text{del}$ with $Z_{1}$ and $Z_{2}\text{del}$ 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.

VI. SECURITY ANALYSIS

The key secrecy, reachability, authenticity, and confidentiality were verified by simulating the proposed protocol 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 been conducted on worldwide used method [27] called ROR (Real-Or-Random) model. Using ROR, our authentication protocol consists of two main entities, an adversary $\mathcal{A}$, and a responder $\mathcal{R}_{i}$. $\mathcal{A}$ established communication with GCS, let $E_{i}$ denotes GCS, whereas $i$ indicated the $i^{th}$ occurrence of GCS; $E_{S}$ means adversary action to impersonate GCS or user/(Drone) by forging $\{ID_{U}, k_{j}\}$, $E_{S}$ can also forge $s$ or $l$, $R_{j}$, 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 $h(S_{1}, S_{2}, S_{3})$ and $h(L_{1}, L_{2}, L_{3}, L_{4}, L_{5}, L_{6})$, and generates a random nonce $N_{A}$ of order prime and stored with any of the given hash messages and return it to $\mathcal{A}$.

iii. MAC($M_{i}$): Next, $C$ authenticates the message; if succeeded, return $M_{i}$ to $\mathcal{A}$.

iv. Send($E$, $M_{i}$): 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 $S_{i}' = S_{2}$, $S_{i}' = S_{3}$ during the computation of GCS. Before going to the next step, GCS must confirm $S_{i}' = S_{2}$ and $S_{i}' = S_{3}$ which in turn $C$ cannot verify. Let suppose anything received by $C$ can return to $\mathcal{A}$.

v. Execute($D_{\infty}$, GCS): Upon sending, the proposed protocol returns $l$ or $s$.

vi. Reveal($E$): 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($E$): 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:

- $(\text{Prob})^{KAS-IoD}(q_{A}^{h(.)}) = q_{A}^{h(.)}||h(.))||h(q_{A}^{h(.)}||D||)$
- $(\text{Prob})^{KAS-IoD}[\text{Prob}][\text{Success}]_{1} = 0$ is used by an adversary $\mathcal{A}$ for choosing an actual number to launch a fundamental attack on our KAS-IoD.
- An adversary uses $\text{Prob}||\text{Success}_{1} = \text{Prob}||\text{Success}_{0}$ for modeling whether the session key is real or random.
- $\text{Prob}[\text{Success}_{1}] = \text{Prob}[\text{Success}_{2}] = q_{A}^{h(.)}||D||$ is 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, 4th 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 II. In the registration phase of the proposed authentication scheme, the total computation cost is $2t_D+4t_G$. In the key agreement phase, D takes $6t_d+5t_G$, DR $4t_d+5t_G$, and GCS $14t_D+7t_G$, so the total cost in the key-agreement phase equals $24t_d+17t_G$. Now, hash-function takes 0.0552ms = cost $24x0.0552 = 1.3248$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 II  
**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                                                   |
| $T_{pp}$ | Execution time for Modular Multiplication                                    | 32.713                                                           | 5.427                                                    |
| $T_{ex}$ | Execution time for exponentiation                                           | 2.249                                                            | 0.001                                                    |

**B. STORAGE OVERHEADS ANALYSIS**

As per experiment done by [30], $ID_D$, $ID_D$, pseudo-identity $PID_D$ and $PID_{GCS}$ each one takes 64 bits space = $5 x 64 = 320$ bits occupy memory, $k_p$, $X_{GCS}$ each one stored in 160 bits space = $2 x 160 = 320$ bits store in memory and $T_D$, $T_U$, $T_{GCS}$ each takes 56 bits space = $3 x 56 = 168$ 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 = \{$S_p$, $S_d$, $T_D$, $PID_D$\} = \{160 + 160 + 160 + 56 + 64\} = 600 bits, Message 2 = \{ $S_p$, $S_d$, $T_U$, $PID_D$, $Q_I$, $Q_S$, $ID_U$\} = \{160 + 160 + 56 + 64 + 160 + 160 + 56 + 64\} = 984 bits, Message 3 = \{ $L_I$, $L_D$, $L_S$, $L_A$, $L_Q$, $L_G$, $T_{GCS}$\} = \{160 + 160 + 160 + 160 + 160 + 160 + 56\} = 1016 bits, and Message 4 = \{ $L_S$, $L_D$, $L_S$, $T_{GCS}$\} = \{160 + 160 + 160 + 160 + 56\} = 696 bits. Therefore the total communication costs for the proposed authentication scheme are 3296 bits are transmitted over the line which is said to be the communication costs.

**D. COMPARISON ANALYSIS**

By comparing the proposed protocol with Wu et al. [28], Zhang et al. [29], Nikooghadam et al. [30], and Li 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 III.

### TABLE III  
**COMPARISON ANALYSIS**

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

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.

**Figure 2:** Comparison Analysis

**IV. 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) 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 lightweight, secure, and ensures mutual
authentication and cross-verification during data broadcasting.

**APPENDIX – A**

Simulation code for the proposed protocol is given as under:

```plaintext
(*===============================*)
free Prch1: channel [private].
free Prch2: channel [private].
free Pubch1: channel.
free Pubch2: channel.
(*===============================*)
free Xgcs: bitstring [private].
free Kgcs: bitstring [private].
free Kd: bitstring [private].
free Ku: bitstring [private].
free ki: bitstring [private].
const IDu: bitstring [private].
const IDd: bitstring [private].
free ru: bitstring.
free l: bitstring.
free s: bitstring.
free tu: bitstring.
free td: bitstring.
(*===============================*)
table d1(bitstring,bitstring).
table d2(bitstring,bitstring).
(*===============================*)
fun con(bitstring,bitstring):bitstring.
fun xor(bitstring,bitstring):bitstring.
fun h(bitstring):bitstring.
(*===============================*)
equation forall m:bitstring,n:bitstring;xor(xor(m,n),n)=m.
(*===============================*)

let U=
out(Prch1,(IDu));
in(Prch1,(S1:bitstring,S2:bitstring,S3:bitstring,PIDu:bitstring, Tu:bitstring));
!
(event UStart(IDu);
new tu:bitstring;
new ru: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
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
if L2R=h(con(con(con(rgcs,SKd),tgcs),IDd))then
let Message3=(L3D,L4D,L5D,L6D,tgcs)in
out(Pubch1,Message3);
0).
(*===============================*)

let D=
out(Prch2,IDD);
in(Prch2,(ki:bitstring));
!
let d1=(IDd,ki)in
if Q2gcs=h(con(con(con(con(con(S1gcs,S2gcs),tdgcs),PIDdgcs),J),IDdgcs),tdgcs))then
let Message2=(S1gcs,S2gcs,S3gcs,tdgcs,PIDdgcs,SKgcs)in
out(Pubch2,Message2);
in(Pubch2,(L1D:bitstring,L2D:bitstring,L3D:bitstring,
L4D:bitstring,L5D:bitstring,tgcs:bitstring));
let SKd=xor(L1D,h(con(con(Ni,ki),tgcs)))in
if L2R=h(con(con(con(rgcs,SKd),tgcs),IDd))then
let Message3=(L3D,L4D,L5D,L6D,tgcs)in
out(Pubch1,Message3);
0).
(*===============================*)

let u=
in(Prch1,(IDu:bitstring));
new PIDu:bitstring;
let Z1=h(con(xu,PIDu))in
let Z2=xor(h(con(IDu,xu)),PIDu)in
insert d2=(PIDu);
out(Prch1,(Z1,Z2,PIDu)).
(*===============================*)

let gcs=
in(Pubch2,(S1gcs:bitstring,S2gcs:bitstring,S3gcs:bitstring,
J=xor(Q1gcs,h(con(ki,tgcsgcs)))in
if Q2gcs=h(con(con(con(con(con(S1gcs,S2gcs),tdgcs),PIDdgcs),J),IDdgcs),tgcs))then
event DAuth(IDdgcs);
let IDdgcs=xor(S1gcs,h(con(con(xgcs,PIDdgcs),tgcs)))in
let Message2=(S1gcs,S2gcs,S3gcs,tgcs,SKgcs)in
out(Pubch1,Message2);
in(Pubch1,(L1u:bitstring,L2u:bitstring,L3u:bitstring,
L4u:bitstring,tgcs:bitstring));
let SKu=xor(L3u,h(con(con(ru,tgcs),IDu)))in
```

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/
REFERENCES

[1] M. Yahuza et al., “Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges,” in 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,” in IEEE Systems Journal, pp. 1-8, 2021.

[3] S. U. Jam Jan, F. Qayum and H. U. Khan. “Design and Analysis of Lightweight Authentication Protocol for Securing IoD,” in IEEE Access, vol. 9, pp. 69287-69306, 2021.

[4] M. Gujarib, R. Bautaba and S. L. Waslander, “Internet of Drones,” in IEEE Access, vol. 4, pp. 1148-1162, 2016.

[5] Vacca, and R. John, “Computer and information security handbook.” Newnes, 2012.

[6] M. Orsini, L. Rick, S. Mark, O’hare, and R. Davenport, “Systems and methods for managing cryptographic keys,” U.S. Patent 8,135,134, issued March 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 Education, 2012.

[8] P. Derbeko, S. Dolev, E. Gudes, and S. Sharma, “Security and privacy aspects in MapReduce on clouds: A survey,” Computer science review, vol. 20, pp.1-28, 2016.

[9] A. Almulhem., “Threat modeling of a multi-UAV system,” Transportation Research Part A: Policy and Practice, vol. 142, pp.290-295, 2020.

[10] J. Sun, W. Wang, L. Kou, et al., “A data authentication scheme for UAV ad hoc network communication,” J Supercomput, vol. 76, pp. 4041–4056, 2020.

[11] Y. Li, X. Du, and S. Zhou, ”A lightweight identity authentication scheme for UAV and road base stations,” In Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies (CIAT 2020), ACM, New York, USA, 2020, pp. 54–58.

[12] T. Alladi, V. Venkatesh, V. Chamoila and N. Chaturvedi, “Drone-MAP: A Novel Authentication Scheme for Drone-Assisted 5G Networks,” IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1-6.

[13] P. Gope, O. Millwood, and N. Saxena, “A provably secure authentication scheme for RFID-enabled UAV applications,” Computer Communications, vol. 166, pp. 19-25, 2021.

[14] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zekria, “GCACS-IoD: A certificate-based generic access control scheme for Internet of drones,” Computer Networks, vol. 191, p.107999, 2021.

[15] S. Challa et al., “Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,” in 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 Proceedings of the 2Nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, 2016, pp. 29-34.

[17] Y. Tian, J. Yuan, and H. Song, “Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones,” Journal of Information Security and Applications, vol. 48, p.102354, 2019.

[18] Y. K. Ever, “A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications,” Computer Communications, vol. 155, pp. 143-149, 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 Journal, 2021.

[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,” Computers & Electrical Engineering, vol. 95, 2021.

[21] M. Adil et al., “Three Byte-Based Mutual Authentication Scheme for Autonomous Internet of Vehicles,” IEEE Transactions on Intelligent Transportation Systems, 2021.

[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,” Transactions on Emerging Telecommunications Technologies, p.e4354, 2021.

[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 Communications, vol. 15, no. 5, pp. 61-76, 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,” Applied Sciences, vol. 10, no. 9, p.3149, 2020.

[27] R. Canetti, A. Jain and A. Scafuro, “Practical UC security with a global random oracle,” In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pp. 597-608, 2014.

[28] L. Wu, J. Wang, K. K. R. Choo, and D. He, “Secure key agreement and key protection for mobile Drone user authentication,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 319–330, 2018.

[29] Zhang, Yunru, D. He, L. Li, and B. Chen, “A lightweight authentication and key agreement scheme for internet of drones,” Computer Communications, vol. 154, pp. 455-464, 2020.

[30] M. Nikooghadam, H. Amintosni, S. K. H. Islam, and M. F. Moghaddam, “A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance,” Journal of Systems Architecture, p.101955, 2020.

[31] L. Teng, M. Jianfeng, F. Pengbin, M. Yse, M. Xindi, Z. Jiawei, C. Gao, and L. Di, “Lightweight security authentication mechanism towards uav networks,” In 2019 International Conference on Networking and Network Applications (NaNA), IEEE, 2019, pp. 379–384.