IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 February 2024, accepted 10 April 2024, date of publication 15 April 2024, date of current version 29 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3388500

RESEARCH ARTICLE

VSKAP-IoD: A Verifiably Secure Key Agreement Protocol for Securing IoD Environment

ABDULRAHMAN AHMED ALZAHRANI
Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
e-mail: aasalzahrani1@uj.edu.sa

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-23-DR-102), therefore, the author thanks the University of Jeddah for its technical and financial support.

ABSTRACT The Internet of Drones (IoD) presents a crucial framework for managing drones in a decentralized manner, facilitating control, navigation, and access through the Internet. Given its importance in future generations, ensuring secure communication within this infrastructure is paramount. While existing authentication schemes have been proposed, they often suffer from design flaws or performance limitations, necessitating the development of more robust solutions. In response to these challenges, this article introduces a novel authentication scheme based on asymmetric cryptography tailored for the IoD environment. The scheme aims to address vulnerabilities in communication channels by providing strong authentication and cross-verification mechanisms. Formal scrutiny through GNY logic and ProVerif and informal validation through proposition demonstrate the security of the proposed scheme. Moreover, the scheme's performance is rigorously analyzed regarding computation, communication, and storage overheads. The comparative analysis highlights the scheme's ability to balance security and performance, positioning it as a viable solution for real-world implementation in IoD environments. Overall, this proposed authentication scheme represents a significant advancement in securing communication within the Internet of Drones, offering robust security and efficient performance for future applications.

INDEX TERMS Cryptography, GNY logic, authentication, secrecy, reachability, confidentiality, vulnerability.

I. INTRODUCTION

The Internet of Drones (IoD) concept is fascinating and holds significant potential across various sectors. Integrating drones into existing networks opens up many opportunities for enhancing efficiency and productivity in numerous fields, as you mentioned [1]. In infrastructure surveillance, drones can be deployed to monitor critical infrastructure such as bridges, pipelines, and power lines, allowing for early detection of issues and proactive maintenance [2]. In healthcare systems, drones can deliver medical supplies to remote or inaccessible areas and provide timely assistance during emergencies or natural disasters [3]. Agriculture benefits greatly from IoD technology, with drones employed for crop monitoring, precision agriculture, and crop spraying. The ability to gather real-time data on soil conditions, crop health, and weather patterns can significantly optimize farming practices and improve yields [4]. Search-and-rescue operations also see a substantial boost from IoD, as drones equipped with cameras, thermal sensors, and other technologies can cover large areas quickly, locating missing persons or assessing disaster-stricken regions [5]. As with any emerging technology, ensuring proper regulation, privacy protection, and ethical considerations are crucial to harnessing the full potential of IoD while mitigating potential risks and challenges. Nonetheless, the prospects offered by the Internet of Drones are undeniably exciting and have the potential to revolutionize various aspects of our lives [6].

Indeed, the widespread use of remotely controlled technology, often drones, has transformed various sectors, including military operations, traffic monitoring, wildlife conservation, cinematography, and surveillance [7]. However, along with these benefits come significant security challenges. As mentioned, information communication is crucial in

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

IoD environments, and ensuring the security of this communication is essential. The increasing sophistication of adversaries means that the IoD environment must be vigilant in addressing security threats to prevent unauthorized access, data breaches, and other cyber-attacks [8]. Some of the security threats faced in IoD environments include: (i) Hackers or malicious actors may attempt to gain unauthorized access to sensitive information or control systems remotely, (ii) Breaches of confidentiality and integrity can occur if data transmitted within IoD networks are intercepted or manipulated, (iii) Attackers may attempt to disrupt IoD operations by overwhelming networks or systems with excessive traffic, rendering them unavailable to legitimate users, (iv) IoD networks are vulnerable to malware infections, which can compromise the security of data and systems and (v) insider attack, where attackers encrypt data and demand control drone from their device, are also a significant concern.

If all participating entities are securely authenticated in the IoD environment, it will ensure the confidentiality of exchanged information. It means authentication protocols play a vital role in verifying the authenticity of all IoD participants as a secret key is exchanged among them, which they then utilize for the upcoming exchange of secret values [9]. On the other hand, a drone has limited computing and storage resources, so the protocols must be lightweight. Various lightweight protocols have recently been proposed for use in UAVs for communications or Unmanned Aerial Vehicular Networks (UAVNs). All these protocols try to provide security features such as authentication, confidentiality, and user privacy [10]. They resist important and well-known attacks such as key disclosure, forgery, man-in-the-middle (MITM), and denial-of-service (DoS) attacks [11].

Overall, robust authentcaition can address the security challenges inherent in IoD environments and UAV networks and offers robust protection against known threats while minimizing communication/computation overhead and ensuring efficient operation on resource-constrained devices like drones [12]. The main benefits of a flawless/robust/lightweight authentication protocol include (i) addresses the unique requirements and constraints of the IoD environment, as well as the limited resources of drones, (ii) showing a solid resistance to various security threats commonly encountered in communication systems, including key disclosure, forgery, man-in-the-middle (MITM) attacks, and denial-of-service (DoS) attacks, (iii) ensuring the integrity, confidentiality, and availability of exchanged information, (iv) advances security features such as authentication, confidentiality, and user privacy. These features are essential for protecting sensitive information exchanged within the IoD environment and ensuring that only authorized entities can access it, and (v) enhancing the overall security posture of IoD systems and supporting their effective operation in diverse applications and scenarios. Therefore, this research presents a flawless/robust/lightweight authentication protocol for the IoD environment that can resist all known threats to the system. The main contributions of the study are as follows:

- To design a protocol for securing communication among all participants in an IoD environment.
- To present a protocol based on asymmetric cryptography in which the adversary cannot find the internal secret in the ground control station (GCS).
- To analyze the protocol for security formally using GNY logic and ProVerif simulation and informally using widely used global techniques of pragmatic illustration.
- To analyze the protocol for performance using the communication and computation costs.
- To comparatively analyze the scheme for performance metrics with state-of-the-art work to balance security with performance often missing in prior works.

The remainder of the paper is organized as section II, which introduces the key concepts and background information relevant to the research. It provides readers with the foundation to understand the rest of the paper. It will briefly explain any essential terms, theories, or methodologies used later in this research article. Section III presents a review of existing literature and research that can summarize previous studies, methods, and findings and critically evaluate their strengths, weaknesses, and contributions to the said field. We will also demonstrate the current state of knowledge and identify gaps that your research aims to address. Section IV will present the details of our proposed protocol that can efficiently manage the identified gaps in the literature. Section V involves evaluating the security aspects of the proposed protocol, assessing its robustness against various types of attacks, potential vulnerabilities, and compliance with security requirements that can validate the effectiveness and reliability of the protocol. Section VI conducts the performance evaluation of the proposed protocol in terms of speed, scalability, resource utilization, and overhead. We also will compare our protocol with existing solutions to demonstrate its superiority in improvement. Section VII ties everything together and gives the reader a clear understanding of the paper's outcomes.

II. PRELIMINARIES

This section of the article defines the basic concept of this research, such as which threat model was adopted, what asymmetric cryptography is, what the system model is, which bitwise XOR operation was used, etc.

A. THREAT MODEL

This research adopted the threat model from [6] and [7] in which the adversary can launch passive, active, or both attacks. The adversary eavesdrops or monitors the open network channel in the first one. At the same time, in the later one, they can copy, delete, alter, or update the transmitted message between legal peers on the open channel. These attacks are summarized as follows:

1. **Passive Attack:** In a passive attack, the adversary eavesdrops or monitors the communication channel without altering the transmitted data. The goal is typically to

intercept sensitive information such as passwords, personal data, or confidential business information. Passive attacks are often harder to detect because they leave no visible trace and do not disrupt the communication flow.

2. **Active Attack:** In contrast, a vigorous attack involves the adversary actively manipulating the data transmitted between legitimate network parties. This can include copying, deleting, altering, or injecting false data into the communication stream. The goal of an active attack may be to disrupt communication, steal information, or impersonate legitimate users.
3. **Combined Attacks:** An adversary may also deploy passive and active attack techniques to achieve their objectives. For example, they may passively eavesdrop on communication to gather information about potential vulnerabilities or weaknesses in the system and then launch active attacks to exploit those weaknesses for their benefit.

B. ASYMMETRIC KEY CRYPTOGRAPHY

A type of cryptography in which the sender/receiver uses different keys; for example, if peer A uses key K for encryption and PK for decryption, then peer B uses key SK for decryption and PK for encryption [8]. The asymmetric method is explained as (i) Public Key (PK) is widely distributed and known to everyone. It's used for encryption if someone wants to send a secure message to the public key's owner, and (ii) the Private Key (SK) is kept secret and known only to the owner. It's used to decrypt messages that have been encrypted using the corresponding public key. When Peer A wants to send a secure message to Peer B, Peer A encrypts the message using Peer B's public key (PK), and Peer B decrypts the message using A's private key (SK). Conversely, if Peer B wants to send a secure message to Peer A, like when Peer B encrypts the message using Peer A's public key (PK) and Peer A decrypts the message using their private key (SK). This, in turn, can secure the communication without requiring both parties to share a secret key beforehand.

C. BITWISE XOR OPERATIONS

A technique in which parity bits are generated for checking fault and comparing two input bits and one output bit. If the bits are the same, the result is 0; otherwise, the result is 1. With a single key and a message of the same size, this bitwise operation encodes and decodes the plaintext. The key is secret and produced at random each time, which is termed a "***One Time Pad***" and makes it impossible for an adversary to break the cypher [9]. Bitwise XOR operation "One Time Pas" is performed in the following manner:

- Each plaintext bit is combined with a corresponding key bit using an XOR (exclusive OR) operation.
- If the plaintext and key bit are the same, the result is 0; otherwise, the result is 1.
- This process generates the ciphertext for each bit in the plaintext
- The same key is used in an XOR operation with each bit of the ciphertext to decrypt the ciphertext.
- Since XOR is its inverse (XORing the same value twice cancels out), performing the XOR operation with the key effectively reverses the encoding process, yielding the original plaintext.
- The key used for encryption and decryption is as long as the plaintext and is generated randomly.
- Each key should be used only once and discarded, hence the name "One Time Pad."
- The key must be kept entirely secret and shared securely between the sender and the receiver.
- The One Time Pad's security relies on the key's randomness and secrecy.
- If implemented correctly with a truly random key that is at least as long as the plaintext, the One Time Pad is theoretically unbreakable.
- This is because each ciphertext can correspond to any possible plaintext of the same length, making cryptanalysis impossible.

D. SYSTEM MODEL

The system or network model presented in this article consisted of three participants: the GSC, drone (D), and mobile operator (M), as shown in Figure 1. The GSC is considered to be trusted, whereas drones play a vital role, and the M is an external user that may or may not be trusted. These participating entities are defined as follows:

i. **Drone (D):** The drone is the fundamental entity in the network model, which can be deployed for tactical tasks. The drone can first be registered with the GCS and then be deployed in an IoD environment for numerous tasks.
ii. **Mobile Device (M):** An operator uses a mobile device to receive IoD services. The user (MO) operates the mobile device to communicate with the D and GCS to avail services safely in the IoD environment. This entity, first registered with the GCS, stores identities, passwords, and other sensitive information for mutual authentication and legitimate services.
iii. **Ground Control Station (GCS):** The GCS is a reliable third party with sufficient processing and storage power. In IoD environments, the GCS serves as the system manager. Additionally, the GCS facilitates M's access to D by authenticating with both M and D data. For M and D, the GCS generates secret keys against their identities.

III. LITERATURE REVIEW AND PROBLEM DEFINITION

Over the past ten years, researchers have encountered difficulties with secure transmission in the Internet of Drones (IoD) environment. To ensure that no one can steal the private information shared between the user and drone, numerous steps have been taken to make it prone-free. An ECC-based lightweight authentication protocol for drone deployment in smart city surveillance was proposed by Nikooghadam et al. [10]. To create secure keys, they employed an elliptic curve discrete logarithmic function. They then used the Scyther toolkit to simulate the security

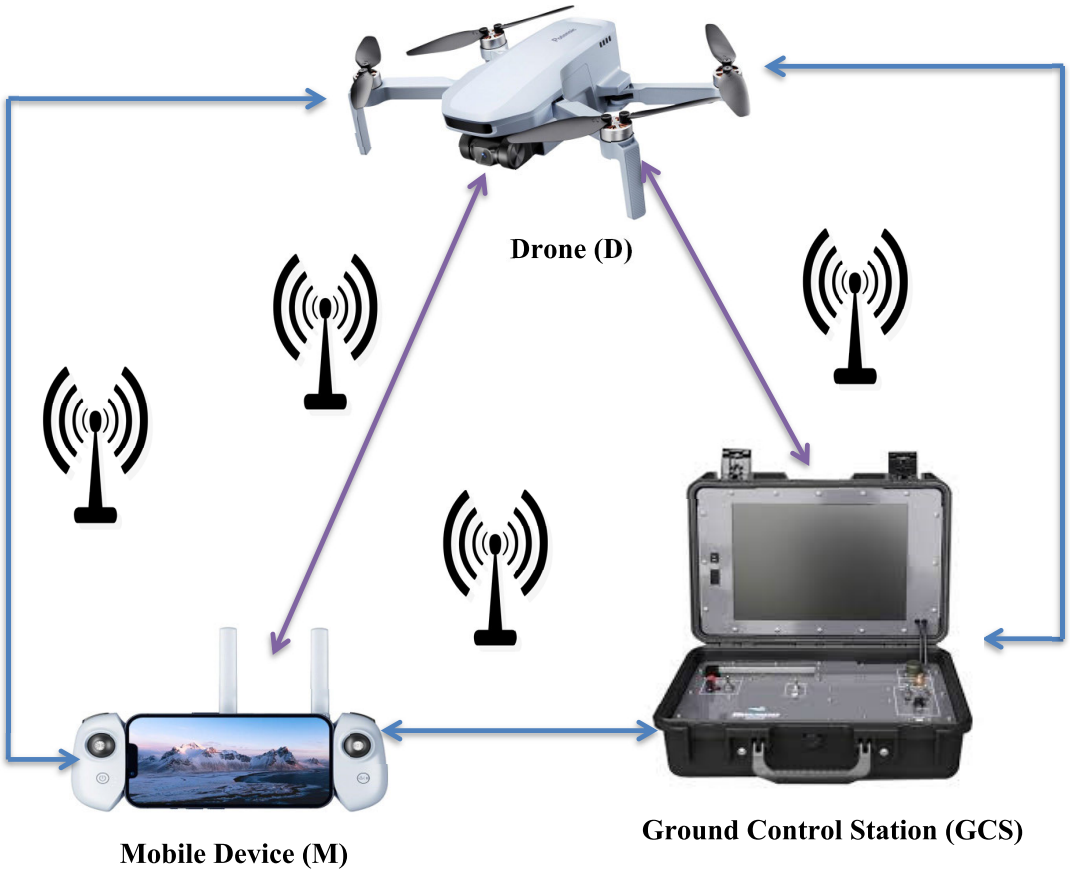


FIGURE 1. System model.

and the Random Oracle Model (ROM) to examine it. They've made a great effort to protect information exchange in the Internet of Drones (IoD) environment. Additionally, an ECC-based authentication system for flying ad hoc networks was developed by Guo et al. [11]. They stated that their protocol provides effective services between satellite and ground stations and can be proven secure. They used the AVISPA toolkit to simulate their protocol and used the ROM to analyze the security of their protocol.

A physical unclonable function (PUF) based key agreement mechanism for a smart grid was proposed by Tahavori and Moazam [12]. They discussed attacks using informal security analysis and utilized the Scyther tools to simulate them. They did not, however, examine the security using a global approach such as BAN, ROM, ROR, and GNY proofs. As a result, their plan cannot be implemented practically for the smart grid. Zhang et al. [13] suggested a straightforward, lightweight, and reliable authentication technique (AKA) based on hash cryptography for the IoD environment. Their system model employed drones, control servers, and an external user. They examined the Turing Machine, lemmas, theorems, their scheme's security, and informal discussions. They did not, however, assist users in resetting their passwords, and there was no step for drone revocation, re-registration, or re-issuance.

A service and temporal credentials-based protocol for IoD deployment drones operating in clusters was proposed by El-Zawawy et al. [14]. They asserted that their plan is the first protocol to offer the gathered data and is impervious to vulnerabilities that could allow information to leak. They employed the ROR model for security analysis and simulation; they used the AVISPA program. They quantified the efficiency of their devised protocol and stated that it requires 20% less computing than their rivals. With their Boyko-Peinado-Venkatesan-based three-factor key agreement procedure, Zhang et al. [15] asserted that the FourQ curve outperforms the traditional ECC by a factor of five. In addition, FourQ has more security and is lighter than other cryptographic primitives.

According to Nyangaresi and Petrovic [16], side-channel, replay, MITM, replay, and desynchronization attacks are common in Internet of Drones (IoD) environments, and the traditional cryptographic algorithms that have been published in the literature have not been able to prevent these vulnerabilities. Thus, they suggested a PUF-based authentication system to address the abovementioned shortcomings. They asserted that the simulation finding is more substantial than previous studies and that their security analysis is proven. Their suggested tactics combine hybrid techniques based on cryptography; nonetheless, their scenario is challenging to

apply in practice. They then proposed an ECC-based method and a PKI. In their proposal, Irshad et al. [17] claimed that their blockchain-based protocol will enable safe data transmission in an Internet of Things system enabled by 5G. All IoD participants were authenticated by their blockchain-oriented DDC (Data-Delivery Collection) security, which also withstood multiple dangers emphasized in the literature. Tian et al. [18] presented a buffer pseudonym-based PKI-based authentication technique for an edge-assisted IoD system.

Chen et al. [19] proposed an ECC-based authentication and key agreement scheme for the IoT environment. They also used a secure hash algorithm and exclusive operations for the design of their protocol. However, their scheme doesn't resist DoS or replay attacks, and the anonymity issue has also been noticed. Banerjee et al. [20] used advanced encryption standards, a secure hash algorithm and exclusive operations for the design of their lightweight session key exchange protocol. Nevertheless, their scheme has a design flaw as well as doesn't resist server secret dictionary attack. Srinivas et al. [21] also proposed an ECC, SAH-1 and XOR-based scheme and named it TCALAS (Temporal credential-based anonymous lightweight authentication scheme). But their scheme is suffering from impersonation, password guessing and privileged insider attacks.

Wazid et al. [22] proposed an ultra-lightweight authentication scheme for securing the IoD environment that is vulnerable to identity guessing and impersonation attacks. Ali et al. [23] identified flaws in TCALAS [21] and proposed an improved scheme based on advanced encryption standards, secure hash algorithms and xor operations. After analysis, their scheme is vulnerable to forgery and DoS attacks and cannot offer perfect forward secrecy. Ever [24] presented an ECC-based authentication framework for IoD applications. They also used a secure hash algorithm and xor operations to design their protocol. However, their scheme doesn't offer perfect forward secrecy, and the stored credentials are not updated dynamically.

Alladi et al. [25] proposed a scheme based on PUF (Physically Unclonable Function) hash message authentication code (HMAC) and XOR operations and named it PARTH (PUF-based Authentication for Remote Hovering Devices). The cryptanalysis result demonstrated that their scheme has key freshness and forward secrecy issues and cannot resist stolen-verifier and DoS attacks. Sadhukhan et al. [26] proposed a scheme for IoT based on ECC and XOR operations. However, it is vulnerable to man-in-the-middle (MITM) and DoS attacks. The summary of the literature review is shown in Table 1.

A. REVIEW ANALYSIS OF BASELINE SCHEME

Recently, Jan et al. [5] proposed a scheme based on HMAC and PBKDF in which a trusted third party can register the GCS and drone and then deploy it for practical tasks. The scheme they have presented is shown in explained as under:

1) GCS Registration Phase:GCS takes the following steps while registering with the certificate authority.

GCS selects cer_{gcs}, secret key sk_{gcs} and nonce n_{gcs}, compute pms= $sk_{gcs}||pk_{gcs}$ build a message $\{cer_{gcs}, n_{gcs}, pms\}$ and send towards CA where it keeps $\{cer_{gcs}, n_{gcs}, pms\}$ parameters in the memory and computes $A_{gcs} = h(\{cer_{gcs})$and transmit back towards gcs.

2) Drone Registration: The drone selects identity id_d, $cert_d$, and n_d computes $A_d = (n_d \oplus id_d)$and $PBKDF= h(cert_d||A_d)||n_d$ and sends $\{A_d, PBKDF\}$ to CA. the CA computes $B = h(A_d||PBKDF)$, $C = h(A_d||sk_{gcs})\oplus PBKDF$ and $\{B, C, h(\cdot)\}$and send $D=\{B, C, pk_d, h(\cdot)\}$message to drone for storing it.

3) Key Agreement Phase: The drone chooses $cert_d$,id_d, n_d and calculates $A_d^* = (n_d \oplus id_d)$, confirms $A_d^*?=A_d$, if validated, $PBKDF^* = h(cert_d||A_d)||n_d$ confirms $PBKDF^*?=PBKDF$ if confirmed, calculates $E_1 = id_d \oplus h(T_1||id_d||n_d)$, $E_2 = A_d^* \oplus h(id_d||T_1||cert_d)$ and sends $= \{E_1, E_2, cert_d, fp_d\}$ message to gcs. On receiving $= \{E_1, E_2, cert_d, fp_d\}$ message the gcs chooses sk_{gcs}, n_{gcs}, computes $F_1 = E_1 \oplus h(T_1||id_d||n_d)$, $F_2 = h(cert_d||A_d)||n_{gcs}$, $F_3 = Enc_{skgcs}((n_d \oplus n_{gcs})||T_2)$, and sends $\{F_3, cert_{gcs}, T_3\}$ message back to drone. The drone when receiving $\{F_3, cert_{gcs}, T_3\}$ message, chooses $cert_{gcs}$, pk_{gcs}, decrypts $(n_d \oplus n_{gcs})||T_2 = Dec_{pkgcs}(F_3)$, confirm $Cert_d$ by extracting all public parameters, calculates $G_1 = id_d \oplus h(n_{gcs}||pk_d)$, $G_2 = h(C \oplus cer_d)||cert_d||pk_{gcs}$, $G_3 = h(id_d||pk_{gcs}||G_2||T_5)$ and sends $\{G_1, G_2, G_3, cert_d, T_5\}$ message towards gcs. The GCS, when receiving $\{G_1, G_2, G_3, cert_d, T_5\}$ message, first confirm $Cert_d$, extract pk_d from it, calculates $I_1 = id_d \oplus h(pk_d||T_5)$, $I_2 = h(h(id_d||pk_d)||cert_d||pk_{gcs})$, $I_3 = h(id_d||pk_{gcs}||G_2||T_5)$, confirm $I_3?=G_3$, if validated, gcs further computes $J_1 = (n_{gcs} \oplus n_d)||T_7$, $J_2 = h(pms||cert_d||T_7)$, $J_3 = Enc_{pkd}((pms)||sk_{gcs})$, $pms=(sk_d \oplus pk_d) \oplus cert_{gcs}$ and sends $\{J_1, J_2, J_3, T_7\}$ message back to drone. The drone when getting $\{J_1, J_2, J_3, T_7\}$ message decrypts $pms||sk_{gcs} = Dec_{skgcs}(J_3)$, calculates $pms^* = (sk_d \oplus pk_d)||pms)$, $L_1 = h(id_d||cert_d||T_7)$, confirm $L_1?=J_2$, if validated, calculates $k_d = PBKDF(pms \oplus (n_d||n_{gcs}) \oplus iter)$ and keep it shared session key.

B. CRYPTANALYSIS OF BASELINE SCHEME

The following issues were noted in the scheme [5].

i. **Heavyweight:** The scheme presented in [5] consisted of the Enc(.)/Dec(.) function, PBKDF, HMAC, Certificate, random nonce, and one hash function that make the communication and computation costs heavyweight.
ii. **Susceptible to Brut Fore Attack:** PBKDF is a function that can take five inputs, i.e., PBKDF(Password, Sequence of Bits, Pseudo-Random Function, iterations, derived key), and generate a secret key from it. This key is susceptible to brute force attack. Therefore, the key in [5] $k_d = PBKDF(pms \oplus (n_d||n_{gcs}) \oplus iter)$ doesn't resist brute force attack.

TABLE 1. Critical literature review.

Ref	Year	Methodology used	Limitations
[19]	2018	ECC, SHA1 and XOR	The anonymity issue doesn't resist DoS and Reply attacks
[20]	2019	AES, XOR Operation, SHA1	The protocol has a design flaw and cannot resist a Server Secret Dictionary (SSD) attack.
[21]	2019	ECC, XOR operation and SHA1	Suffering from user impersonation, password guessing and privileged insider attacks
[22]	2019	SHA and XOR operations	Vulnerable to user impersonation, identity guessing and device impersonation attacks
[23]	2020	AES, SHA1, and XOR Operations	Forgery and DoS attacks and doesn't provide perfect forward secrecy.
[24]	2020	ECC, SHA and XOR Operations	The key secrecy is suffering from dynamic key updates and needs to provide perfect forward secrecy.
[25]	2020	Hash Message Authentication Code (HMAC) and XOR Operations	Key freshness issue, perfect forward secrecy issue, and doesn't resist stolen-verifier and DoS attacks
[26]	2021	ECC, SHA1, XOR operations	Posed to man-in-the-middle and DoS attacks.

iii. **DoS Attack**: The scheme presented in [5] consisted of five round-trips, which make the protocol vulnerable to DoS attacks. Attackers actively monitor the open channel and cause the services denied for legitimate drones.

iv. **Replay Attack**: In [5], if an attacker gets the message $\{E_1, E_2, cert_d, fp_d\}$ from the open network channel, $E_1 = id_d \oplus h(T_1||id_d||n_d)$ has drone identity Id_d in raw format, attacker can easily extract it from $\{E_1, E_2, cert_d, fp_d\}$ message and replay some other time on the system.

Keeping in view, the vulnerabilities highlighted above in different schemes [19], [20], [21], [22], [23], [24], [25] and the cryptanalysis of the scheme [5] demonstrate that authentication is crucial to ensure that sensitive information is only shared among trusted parties, preventing privacy breaches and maintaining trust in the system. However, implementing security measures in such an environment is complex due to challenges like key secrecy breaches, computational overhead, communication costs, and design issues. Therefore, this article will present a security scheme that offers provable security, takes less round-trip during key computation, and efficiently delivers services to the system by mitigating all the addressed challenges.

IV. PROPOSED SOLUTION

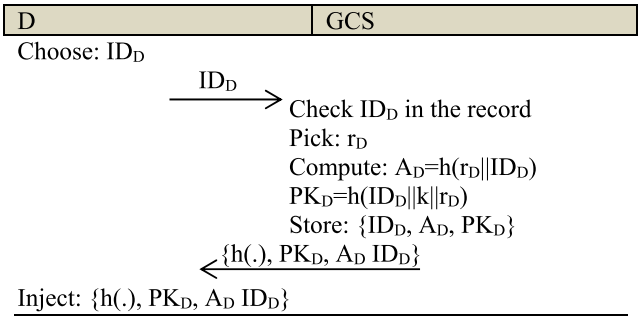
The proposed protocol consists of six phases: the drone registration phase, the user device registration phase, the authentication phase, the password change phase, drone addition, and the revocation/re-issue phases. The different notations used are shown in Table 2, and the phases are briefly described as follows.

A. DRONE (D) REGISTRATION

The D first chooses an ID_D and sends it to the GCS over a private channel. The GCS checks ID_D in its record; if found, it sends a message back to the operator to select another one; otherwise, it picks a random number r_D, computes $A_D = h(r_D||ID_D)$ and $PK_D = h(ID_D||k||r_D)$, stores $\{ID_D, A_D, PK_D\}$ in its record, and sends $\{h(.), PK_D, A_D\ ID_D\}$ back towards the drone over a reliable channel. The D injects $\{h(.), PK_D, A_D\ ID_D\}$ parameters in its record for future usage.

TABLE 2. Notations used in the proposed scheme.

Notation	Description
ID_D	Drone Identity
r_D	Drone Random number
k	Secret values
PK_D	Drone Public Key
h(.)	Hash Function
$\|\|$	Concatenation Function
ID_M	User Identity
PW_M	User Password
r_M	User Random number
r_1, r_2, r_3, r_4, r_5	Random nonce
T_1, T_2, T_3, T_4, T_5	Timestamp
$\oplus$	XOR Operations

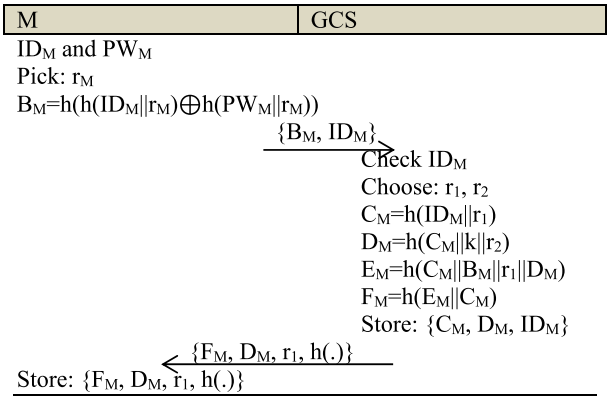


PHASE 1. Drone registration phase.

B. MOBILE (M) REGISTRATION

The hand-held M selects identity ID_M, password PW_M, picks a random number r_M, computes $B_M = h(h(ID_M||r_M) \oplus h(PW_M||r_M))$, and transmits $\{B_M, ID_M\}$ towards the GCS

over a secure channel. The GCS checks the ID_M in its record; if found, it sends a message back to the operator to select a unique identity for their Mobile device; otherwise, it chooses two numbers, r_1 and r_2; computes $C_M = h(ID_M||r_1)$, $D_M = h(C_M||k||r_2)$, $E_M = h(C_M||B_M||r_1||D_M)$, and $F_M = h(E_M||C_M)$; and keeps $\{C_M, D_M, ID_M\}$ in memory and $\{F_M, D_M, r_1, h(.)\}$ towards the M for keeping it in the record of Mobile device.



PHASE 2. Mobile device registration phase.

C. KEY AGREEMENT

This phase can take the following steps:

- The M provides ID_M; password PW_M; computes $B_M^* = h(h(ID_M||r_M)\oplus h(PW_M||r_M))$, $C_M^* = h(ID_M||r_1)$, $E_M^* = h(C_M||B_M^*||r_1||D_M)$, and $F_M^* = h(E_M^*||C_M^*)$; and confirms $F_M? = F_M^*$. If it does not match, the process is rejected; otherwise, it picks a random number r_3, records time T_1, computes $PK_M = r_3.P$ and $G_M = h(C_M||D_M||T_1)$, and transmits $\{A_D, C_M, G_M, PK_M, T_1\}$ towards the GCS over a public channel.
- First, it checks the freshness of the message T_2-$T_1 \leq \Delta T$; repossesses ID_M, C_M, and D_M from the stored record; computes $G_M^* = h(C_M||D_M||T_1)$; confirms $G_M?=G_M^*$. If it does not match, the process is rejected; otherwise, it computes $H_{DM} = D_M\oplus PK_D$ and $I_M = h(A_D||PK_D||ID_D||D_M)$ and transmits $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$ towards the D over an open channel.
- Then, it checks the timestamp, T_3-$T_2 \leq \Delta T$, computes $D_M = H_{DM}\oplus PK_D$ and $I_M^* = h(A_D||PK_D||ID_D||D_M)$, and confirms $I_M^*? = I_M$. If it does not match, the process is rejected; otherwise, it picks a random number, r4, records timestamp T_5, and computes $PK_D^* = r_4.PK_M$, $SK_D = h(ID_D||D_M||C_M)$, and $Auth_D = h(SK_D||C_M||D_M||T_5)$; and transmits $\{Auth_D, PK_D^*, T_5\}$ back towards the GCS over an open channel.
- Next, it checks the time stamp, T_6-$T_5 \leq \Delta T$, computes $SK_{GCS} = h(ID_D||D_M||C_M)$ and $Auth_{GCS} = h(SK_D||C_M||D_M||T_7)$, confirms $Auth_{GCS}?=Auth_M$, and transmits $\{Auth_{GCS}, PK_D^*, T_7\}$ back towards the M over a public network channel.
- The M first checks the timestamp T_8-$T_7 \leq \Delta T$, computes $SK_M = h(ID_D||D_M||C_M)$ and $Auth_M = h(SK_D||C_M||D_M||T_7)$, and confirms $Auth_D?=Auth_M$. The process is rejected if it does not match; otherwise, it keeps $SK_D = SK_{GCS} = SK_M$ as the shared secret session key as shown in phase 3.

D. PASSWORD CHANGE FACILITY

The M provides ID_M and password PW_M; the device computes $B_M^* = h(h(ID_M||r_M)\oplus h(PW_M||r_M))$, $C_M^* = h(ID_M||r_1)$, $E_M^* = h(C_M||B_M^*||r_1||D_M)$, and $F_M^* = h(E_M^*||C_M^*)$; and verifies $F_M? = F_M^*$. The operator will be asked to provide a newer password PW_M^{new}; compute $B_M^{new} = h(h(ID_M||r_M)\oplus h(PW_M||r_M))$, $C_M^{new} = h(ID_M||r_1)$, $E_M^{new} = h(C_M||B_M^{new}||r_1||D_M)$, and $F_M^{new} = h(E_M^{new}||C_M^{new})$; and replace B_M, C_M, E_M, and F_M with B_M^{new}, C_M^{new}, E_M^{new}, and F_M^{new}.

E. DRONE ADDITION FACILITY

If a legitimate system operator desires to deploy a drone into the system dynamically, the GCS will provide an ID_D^{new} identity and send it to the GCS. The GCS checks it in the database and, if found, sends a message back to the operator for selecting a unique identity; if not found, GCS chooses a large random number r_D^{new}, computes $A_D^{new} = h(r_D^{new}||ID_D^{new})$, $PK_D^{new} = h(ID_D^{new}||k^{new}||r_D^{new})$, stores $\{ID_D^{new}, A_D^{new}, PK_D^{new}\}$ in memory and send $\{ID_D^{new}, A_D^{new}, PK_D^{new}\}$ message back towards the newly added drone for injecting in its record to operate in the IoD environment securely.

F. DRONE REVOCATION FACILITY

The departed/revoked drone's record is necessary to be removed from the system; in this record, the IoD owner must create a list DL and add a secret key k_1 to the list for the revoked drone, the GCS computes $W_D = h(ID_D||k||r_D)$, $A_D = h(r_D||ID_D)$ and $PK_D^* = h(ID_D|| = k_1||r_D)$, confirms $PK_D^*?=PK_D$, if matched, the system will delete the record from memory, and cancel its future authorization in the system.

V. SECURITY ANALYSIS

This article section can be accomplished via GNY logic [27]. This is the modified version of BAN logic [28] and was first introduced by Gang-Needham-Yahalom in 1990.

A. GNY ANALYSIS

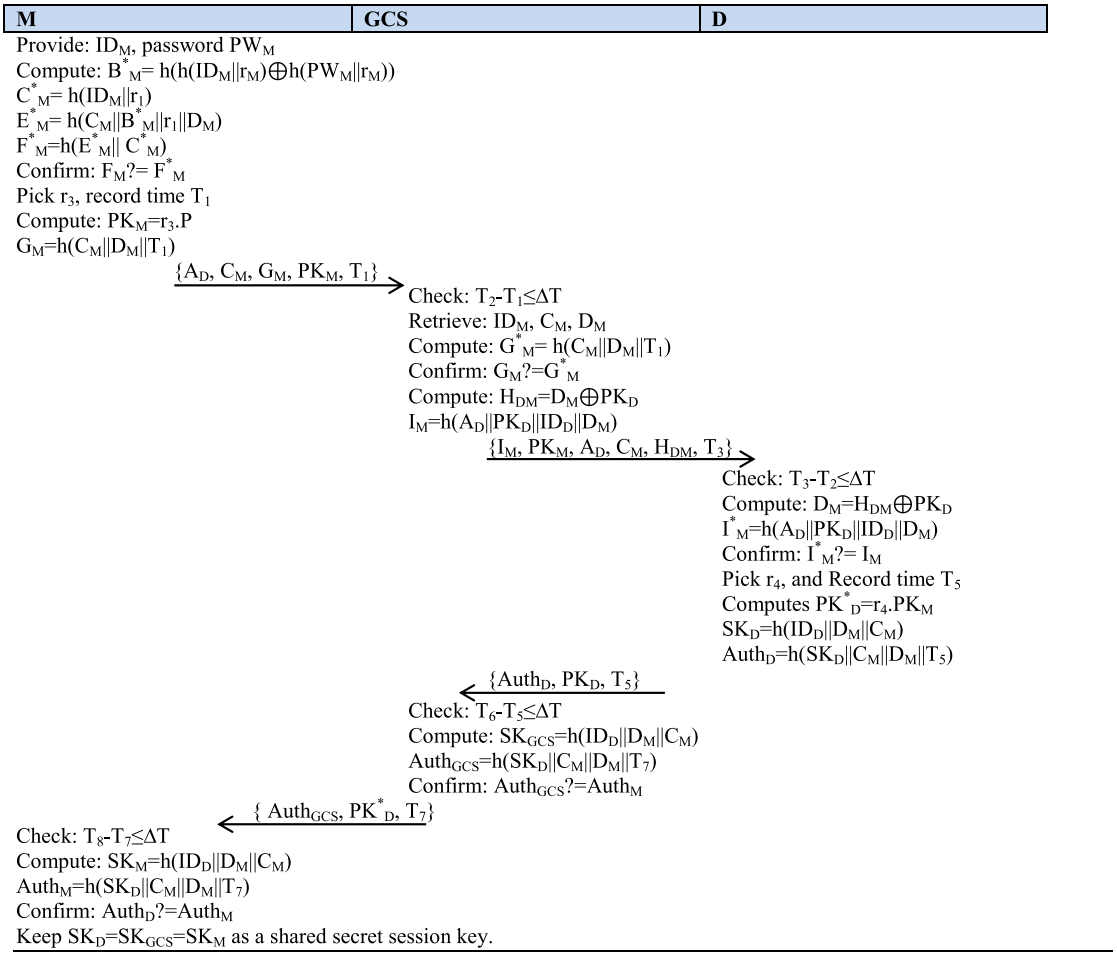
The different formulas and statements used are shown in Table 3, and the analysis follows.

1) GNY POSTULATES

There are five types of postulates in GNY logic. These are described as follows:

a: TOLD RULES

If one peer is told another message, which is encrypted with public key K, then the same peer also knows the description



PHASE 3. **Key agreement phase.**

TABLE 3. **Formulas and statements.**

Notations/ Formulas/ Statements/	Meanings/ Descriptions
{X, Y}	The conjunction of two formulas
$\{X\}_K$	Encryption over key K
$\{X\}_K^{-1}$	Decryption over key K
$\{X\}_K$	Public Key Encryption
$\{X\}_{-K}$	Public key Decryption
H(X)	One-way hashing of X
$F(X_1, X_2, \ldots\ldots, X_n)$	Computationally feasible function (many-to-one)
$P \lhd X$	P told X
$P \ni X$	P possesses X
$P \mid\sim X$	P conveyed X
$P \mid\equiv X$	P believes X
$P \mid\equiv \#(X)$	P believes the freshness of X
$P \mid\equiv \phi(X)$	P believes the recognition of X
$P \mid\equiv P \overset{S}{\leftrightarrow} Q$	P believes that the exchange of secrete between P and Q is suitable
$P \mid\equiv P \overset{K}{\leftrightarrow} Q$	P believes that the public key K is suitable among P and Q
$P \lhd {}^*X$	P told X that is not conveyed in any round-trip previously
$P \mid\Rightarrow X$	P jurisdiction over X

of the same message in the other peer, as given as follows:

$$\frac{P \lhd (X, Y)}{P \lhd X} \quad \text{A1}$$

$$\frac{P \lhd \{X, Y\}_K, P \ni K}{P \lhd X} \quad \text{A2}$$

b: POSSESSION RULES

If a peer possesses two messages, X and Y, it also possesses its combination, including concatenation or XOR, hash function or all.

$$\frac{P \lhd X}{P \ni X} \quad \text{B1}$$

$$\frac{P \ni X, P \ni Y}{P \ni (X, Y), P \ni f(X, Y)} \quad \text{B2}$$

c: FRESHNESS RULES

If a peer believes a message in a protocol is fresh, then the peer also considers that all its components are new and believes in the Enc(.)/Dec(.) process via public/private (PK/SK) keys.

$$\frac{P| \equiv \#(X)}{P| \equiv \#(X, Y), P| \equiv \#(f(x))} \quad \text{C1}$$

$$\frac{P| \equiv \#(X), P \ni X}{P| \equiv \#(\{X_K\}), P| \equiv \#(\{X_{K^{-1}}\})} \quad \text{C2}$$

d: RECOGNIZABLE RULES

If a peer believes in recognizing a message, then it also believes in identifying all its components, combinations, and

computability over different functions.

$$\frac{\mathrm{P}| \equiv \Phi(\mathrm{X})}{\mathrm{P}| \equiv \Phi\,(\mathrm{X},\,\mathrm{Y})\,,\,\mathrm{P}| \equiv \Phi\,(\mathrm{f}\,(\mathrm{X}))} \quad \text{D1}$$

$$\frac{\mathrm{P}| \equiv \Phi\,(\mathrm{X})\,,\,P \ni X}{\mathrm{P}| \equiv \Phi(X_K\}),\,P| \equiv \#\left(\left\{X_{K^{-1}}\right\}\right)} \quad \text{D2}$$

e: INTERPRETATION RULES

If a peer believes a message encryption over key K, possesses key K, believes the shared secrets among both peers, feels its freshness and is recognizable, then the same peer or other participating peer can also believe it is once conveyed and possesses key K.

$$\frac{\mathrm{P} \lhd * \{X\}_K\,,\,\mathrm{P} \ni \mathrm{X},\,\mathrm{P}| \equiv \mathrm{P} \overset{K}{\longleftrightarrow} \mathrm{Q},\,\mathrm{P}| \equiv \Phi\,(\mathrm{X})\,,\,\mathrm{P}| \equiv \#(\mathrm{X},\,\mathrm{K})}{\mathrm{P}| \equiv \mathrm{Q}| \sim \mathrm{X},\,\mathrm{P}| \equiv \mathrm{Q}| \sim \{X\}_K\,,\,P| \equiv Q \ni K} \quad \text{E1}$$

$$\frac{\mathrm{P}| \equiv \mathrm{Q}| \sim \mathrm{X},\,\mathrm{P}| \equiv \#(\mathrm{X})}{\mathrm{P}| \equiv Q \ni X} \quad \text{E2}$$

f: RATIONALITY RULES

If peer one is entitled to possess a message, the second peer can also have its concatenation, encryption/decryption, xor, and hash functions.

$$\frac{P| \equiv Q \ni X, P| \equiv Q \ni Y}{P| \equiv Q \ni f(X, Y)} \quad \text{F1}$$

$$\frac{Q| \equiv \mathrm{P} \ni X, Q| \equiv \mathrm{P} \ni Y}{Q| \equiv \mathrm{P} \ni f(X, Y)} \quad \text{F2}$$

Proof of the Proposed Protocol: Using GNY logic, we transform several symbols into the symbols used in the protocol as follows:

1): M→GCS: $\{\mathrm{A_D},\ \mathrm{C_M},\ \mathrm{G_M},\ \mathrm{PK_M},\ \mathrm{T_1}\}$: $\{\mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{h(C_M||D_M||T_1)}\}_{\mathrm{PKM}}$

2): GCS→D: $\{\mathrm{I_M},\ \mathrm{PK_M},\ \mathrm{A_D},\ \mathrm{C_M},\ \mathrm{H_{DM}},\ \mathrm{T_3}\}$: $\{\mathrm{h(A_D||PK_D||ID_D||D_M)},\ \mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{D_M \oplus PK_D},\ \mathrm{T_3}\}_{\mathrm{PKM}}$

3): D→GCS: $\{\mathrm{Auth_D},\ \mathrm{PK_D},\ \mathrm{T_5}\}$: $\{\mathrm{h(SK_D||C_M||D_M||T_5)}\}_{\mathrm{PKD}}$

4): GCS→M: $\{\mathrm{Auth_{GCS}},\ \mathrm{PK_D},\ \mathrm{T_7}\}$: $\{\mathrm{h(SK_D||C_M||D_M||T_7)}\}_{\mathrm{PKD}}$

1) *Message Content*

The M believes the message transmitted initially towards the GCS is recognizable.

$$\mathrm{M}| \equiv \Phi(\{\mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{h(C_M||D_M||T_1)}\}_{\mathrm{PKM}}) \quad \text{Goal1}$$

The GCS believes the message received from the M in the first round trip is recognizable

$$\mathrm{GCS}| \equiv \Phi(\{\mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{h(C_M||D_M||T_1)}\}_{\mathrm{PKM}}) \quad \text{Goal2}$$

Both the M and GCS believe the message transmitted/received is recognizable

$$\mathrm{M}| \equiv \mathrm{GCS}| \equiv \Phi(\{\mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{h(C_M||D_M||T_1)}\}_{\mathrm{PKM}}) \quad \text{Goal3}$$

The GCS believes the message transmitted towards the D in the second round trip is recognizable

$$\mathrm{GCS}| \equiv \Phi(\{\mathrm{h(A_D||PK_D||ID_D||D_M)},\ \mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{D_M \oplus PK_D},\ \mathrm{T_3}\}_{\mathrm{PKM}}) \quad \text{Goal4}$$

The D believes the message arriving from the GCS is recognizable

$$\mathrm{D}| \equiv \Phi(\{\mathrm{h(A_D||PK_D||ID_D||D_M)},\ \mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{D_M \oplus PK_D},\ \mathrm{T_3}\}_{\mathrm{PKM}}) \quad \text{Goal5}$$

Both the GCS and D believe the message transmitted/received is recognizable

$$\mathrm{GCS}| \equiv \mathrm{D}| \equiv \Phi(\{\mathrm{h(A_D||PK_D||ID_D||D_M)},\ \mathrm{h(r_D||ID_D)},\ \mathrm{h(ID_M||r_1)},\ \mathrm{D_M \oplus PK_D},\ \mathrm{T_3}\}_{\mathrm{PKM}}) \quad \text{Goal6}$$

The D believes the message transmitted towards the GCS is recognizable

$$\mathrm{D}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_5)}\}_{\mathrm{PKD}}) \quad \text{Goal7}$$

The GCS believes the message arriving from the D is recognizable

$$\mathrm{GCS}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_5)}\}_{\mathrm{PKD}}) \quad \text{Goal8}$$

Both the D and GCS believe the message transmitted/received is recognizable.

$$\mathrm{D}| \equiv \mathrm{GCS}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_5)}\}_{\mathrm{PKD}}) \quad \text{Goal9}$$

The GCS believes the message transmitted toward the M is recognizable

$$\mathrm{GCS}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_7)}\}_{\mathrm{PKD}}) \quad \text{Goal10}$$

The M believes the message arriving from the GCS is recognizable

$$\mathrm{M}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_7)}\}_{\mathrm{PKD}}) \quad \text{Goal11}$$

Both the GCS and M believe the message transmitted/received is recognizable.

$$\mathrm{GCS}| \equiv \mathrm{M}| \equiv \Phi(\{\mathrm{h(SK_D||C_M||D_M||T_7)}\}_{\mathrm{PKD}}) \quad \text{Goal12}$$

2. Message Origin The M believes the message is conveyed towards the GCS (1^{st} run)

$$\mathrm{M}| \equiv \mathrm{GCS}| \sim (\mathrm{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)_{PKM}}) \quad (1)$$

The GCS believes the message is conveyed towards the M (2^{nd} run)

$$\mathrm{GCS}| \equiv \mathrm{M}| \sim (\mathrm{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)_{PKM}}) \quad (2)$$

The GCS believes the message is conveyed towards the D (3^{rd} run)

$$\mathrm{GCS}| \equiv \mathrm{D}| \sim (\{\mathrm{h(A_D||PK_D||ID_D||D_M)||h(r_D||ID_D)}\ ||(\mathrm{h(ID_M||r_1)||D_M)} \oplus \mathrm{PK_D)||T_3}\}_{\mathrm{PKM}} \quad (3)$$

The D believes the message is conveyed towards the GCS (4^{th}run)

$$\begin{aligned} \mathrm{D}| \equiv \mathrm{GCS}|\sim(\{\mathrm{h}(\mathrm{A_D}||\mathrm{PK_D}||\mathrm{ID_D}||\mathrm{D_M})||\mathrm{h}(\mathrm{r_D}||\mathrm{ID_D}) \\ ||(\mathrm{h}(\mathrm{ID_M}||\mathrm{r_1})||\mathrm{D_M})\oplus\mathrm{PK_D})||\mathrm{T_3}\}_{\mathrm{PKM}} \end{aligned} \tag{4}$$

The GCS believes the message is conveyed towards the M (5^{th}run)

$$\mathrm{GCS}|\equiv\mathrm{M}|\sim(\mathrm{h}(\mathrm{SK_D}||\mathrm{C_M}||\mathrm{D_M}||\mathrm{T_5})_{\mathrm{PKD}} \tag{5}$$

The M believes the message is conveyed towards the GCS (5^{th}run)

$$\mathrm{M}|\equiv\mathrm{GCS}|\sim(\mathrm{h}(\mathrm{SK_D}||\mathrm{C_M}||\mathrm{D_M}||\mathrm{T_5})_{\mathrm{PKD}} \tag{6}$$

1) *Session Key Establishment Credentials*

The random numbers r_1 and r_3 are exchanged among the M and GCS in which the M and GCS both believe the shared secret numbers between the M and GCS and vice versa.

$$\mathrm{M}| \equiv \mathrm{GCS}|\equiv \mathrm{M} \xleftarrow{r_1 \oplus r_3} \mathrm{GCS} \tag{7}$$

$$\mathrm{GCS}| \equiv \mathrm{M}|\equiv \mathrm{GCS} \xleftarrow{r_1 \oplus r_3} \mathrm{M} \tag{8}$$

The random numbers r_2 and r_4 are exchanged among the GCS and D in which the GCS and D both believe they share secret r_2 and r_4 numbers between the GCS and M and vice versa.

$$\mathrm{GCS}| \equiv \mathrm{D}|\equiv\mathrm{GCS} \xleftarrow{r_2 \oplus r_4} \mathrm{D} \tag{9}$$

$$\mathrm{D}| \equiv \mathrm{GCS}|\equiv\mathrm{D} \xleftarrow{r_2 \oplus r_4} \mathrm{GCS} \tag{10}$$

1) *Assumptions*

The GCS generates k, r_{UA}, r_1, and r_2 because the GCS possesses and believes its freshness.

$$\mathrm{A1}: \text{ The GCS generates secret values k, } \mathrm{r_D},\ \mathrm{r_1},\ \mathrm{r_2} \tag{11}$$

$$\mathrm{A2}: \mathrm{GCS}\ni\mathrm{k},\ \mathrm{GCS}\ni\mathrm{r_D},\ \mathrm{GCS}\ni\mathrm{r_1},\ \mathrm{GCS}\ni\mathrm{r_2} \tag{12}$$

$$\mathrm{A3}: \mathrm{GCS}|\equiv\#(\mathrm{k}),\ \mathrm{GCS}|\equiv\#(\mathrm{r_D}),\ \mathrm{GCS}|\equiv\#(\mathrm{r_1}),\ \mathrm{GCS}|\equiv\#(\mathrm{r_2}) \tag{13}$$

The M generates k, r_M, and r_3 because the M possesses and believes its freshness.

$$\mathrm{A4}: \text{ The M generates } \mathrm{r_M},\text{ and } \mathrm{r_3} \tag{14}$$

$$\mathrm{A5}: \mathrm{M}\ni\mathrm{r_M},\ \mathrm{M}\ni\mathrm{r_3} \tag{15}$$

$$\mathrm{A6}: \mathrm{M}|\equiv\#(\mathrm{r_M}),\ \mathrm{M}|\equiv\#(\mathrm{r_3}) \tag{16}$$

The D generates r_4 because the D possesses and believes its freshness.

$$\mathrm{A7}: \text{ The D generates } \mathrm{r_4} \tag{17}$$

$$\mathrm{A8}: \mathrm{D}\ni\mathrm{r_4} \tag{18}$$

$$\mathrm{A9}: \mathrm{D}|\equiv\#(\mathrm{r_4}) \tag{19}$$

$$\mathrm{M}|\equiv\mathrm{GCS} \xleftarrow{k} \mathrm{M} \tag{20}$$

$$\mathrm{M}|\equiv\mathrm{GCS}|\Rightarrow\mathrm{M} \xleftarrow{r_1 \oplus r_3} \mathrm{GCS} \tag{21}$$

$$\mathrm{GCS}|\equiv\mathrm{M}|\Rightarrow\mathrm{GCS} \xleftarrow{r_1 \oplus r_3} \mathrm{M} \tag{22}$$

$$\mathrm{GCS}|\equiv\mathrm{D}|\Rightarrow\mathrm{GCS} \xleftarrow{r_2 \oplus r_4} \mathrm{D} \tag{23}$$

$$\mathrm{D}|\equiv\mathrm{GCS}|\Rightarrow\mathrm{D} \xleftarrow{r_2 \oplus r_4} \mathrm{GCS} \tag{24}$$

Now, the GNY logic is implemented to analyse the proposed protocol. We get this by taking A1 and A2 and applying to Goal1 for GCS A1, as shown at the bottom of page 8.

According to Eq: (7), (11) and E1, E2, we get

$$\frac{GCS \ni \{ID\}_{PK_{MO}}, GCS \ni r_1 \oplus r_3}{GCS \ni ID_{UAV}, GCS \ni r_2 \oplus r_4} \tag{26}$$

Eq: (5), (7), E2 and possesses rule, we get

$$\frac{GCS\ni \mathrm{h}(\mathrm{ID_{MO}}||\mathrm{r_1}),\ GCS\ni k}{GCS\ni \mathrm{h}(\mathrm{ID_{MO}}||\mathrm{r_1}),\ GCS\ni \mathrm{h}(\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_1})_{PK_{MO}}} \tag{27}$$

Eq: (2), A1, A2, Goal2 and told rules, we get (28), as shown at the bottom of the next page, E1, E2, Eq: (8) and possesses rule, we get

$$\frac{UAV \ni \{ID\}_{PK_{MO}}, UAV \ni r_2 \oplus r_4}{UAV \ni ID_{UAV}, UAV \ni r_1 \oplus r_3} \tag{29}$$

E2, Eq: (5) it possesses rule, we get

$$\frac{UAV\ni \mathrm{h}(\mathrm{ID_{MO}}||\mathrm{r_1}),\ UAV\ni T_3}{UAV\ni \mathrm{h}(\mathrm{ID_{MO}}||\mathrm{r_1}),\ UAV\ni \mathrm{h}(\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_1})_{PK_{MO}}} \tag{30}$$

A1, A2, Goal3, and told rules, we get

$$\frac{GCS\lhd\{\mathrm{h}(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_5})\}_{PK_{UAV}},\ GCS \lhd \mathrm{SK_{UAV}}}{GCS\ni\{\mathrm{h}(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_5})\}_{PK_{UAV}},\ GCS\ni T_5} \tag{31}$$

Eq: (9), E1, E2, and possesses rule, we get

$$\frac{GCS \ni \{SK\}_{UAV} GCS \ni r_1 \oplus r_3}{GCS \ni ID_{UAV}, GCS \ni r_2 \oplus r_4} \tag{32}$$

Eq: (6), E2, and possesses rule, we get

$$\frac{GCS\ni\{\mathrm{h}(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_5})\}_{PK_{UAV}},\ GCS\ni T_5}{GCS\ni\{\mathrm{h}(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_5})\}_{PK_{UAV}},\ GCS\ni ID_{UAV}} \tag{33}$$

Eq: (33) for the M becomes

$$\frac{MO\ni\mathrm{h}\{(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{\mathrm{PK_{UAV}}},\ MO\ni T_7}{MO\ni\mathrm{h}\{(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{\mathrm{PK_{UAV}}},\ MO\ni\mathrm{SK_{UAV}}} \tag{34}$$

Eq: (10), E1, E2, possesses rule, we get

$$\frac{MO \ni \{PK\}_{UAV}, MO \ni r_1 \oplus r_3}{MO \ni ID_{UAV}, MO \ni r_2 \oplus r_4} \tag{35}$$

B1, B2, Eq: (6) and told rules, we get (36), as shown at the bottom of the next page M, GCS, and told rules, we get

$$\frac{MO \lhd \{h\,(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{PK_{UAV}}}{GCS\ni\{h\,(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{PK_{UAV}}} \tag{37}$$

Taking Message (3) and (4), in interpretation rule is (38), as shown at the bottom of the next page.

The interpretation rule for the GCS, D, and secret keys, we get

$$\frac{GCS \lhd \{\mathrm{h}\,(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{PK_{UAV}} GCS\ni\mathrm{SK_{UAV}}}{UAV\ni\{\mathrm{h}\,(\mathrm{SK_{UAV}}||\mathrm{C_{MO}}||\mathrm{D_{MO}}||\mathrm{T_7})\}_{PK_{UAV}} UAV \lhd \mathrm{SK_{UAV}}} \tag{39}$$

The interpretation rule for the different messages among the M, GCS, and D, we get (40)–(51), as shown at the bottom of the page.

The recognizable rules for the different messages exchanged aMng M, GCS, and D, we get (52), as shown at the bottom of the next page.

$$\frac{\{GCS \lhd h(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ GCS \lhd \mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1),\ GCS \lhd \mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}}{\{GCS \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ GCS \ni \mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1),\ GCS \ni \mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}} \tag{25}$$

$$\frac{\{UAV \lhd \mathrm{h}(\mathrm{A}_{UAV}||\mathrm{PK}_{UAV}||\mathrm{ID}_{UAV}||\mathrm{D}_{MO})\}_{PK_{MO}},\ UAV \lhd ID_{MO}}{UAV \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ \mathrm{D} \ni \mathrm{h}(\mathrm{ID}_{\mathrm{MO}}||\mathrm{r}_1),\ \mathrm{D} \ni \{\mathrm{D}_{MO} \oplus \mathrm{PK}_{UAV}\}_{PK_{MO}}} \tag{28}$$

$$\frac{GCS \lhd \{\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}}{MO \ni \{\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}} \tag{36}$$

$$\frac{UAV \lhd \{h(\mathrm{A}_{UAV}||\mathrm{PK}_{UAV}||\mathrm{ID}_{UAV}||\mathrm{D}_{MO})||\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{D}_{MO}) \oplus \mathrm{PK}_{UAV}||\mathrm{T}_3\}_{PK_{UAV}}}{GCS \ni \{h(\mathrm{A}_{UAV}||\mathrm{PK}_{UAV}||\mathrm{ID}_{UAV}||\mathrm{D}_{MO})||\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{D}_{MO}) \oplus \mathrm{PK}_{UAV}||\mathrm{T}_3\}_{PK_{UAV}}} \tag{38}$$

$$\frac{GCS \xleftarrow{r_1 \oplus r_3} MO}{\{GCS \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ GCS \ni \mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1),\ GCS \ni \mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}} \tag{40}$$

$$\frac{MO \xleftarrow{r_1 \oplus r_3} GCS}{\{MO \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ MO \ni \mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1),\ MO \ni \mathrm{h}(\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_1)\}_{PK_{MO}}} \tag{41}$$

$$\frac{GCS \xleftarrow{r_2 \oplus r_4} UAV}{GCS \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ \mathrm{GCS} \ni \mathrm{h}(\mathrm{ID}_{\mathrm{MO}}||\mathrm{r}_1),\ \mathrm{GCS} \ni \{\mathrm{D}_{MO} \oplus \mathrm{PK}_{UAV}\}_{PK_{MO}}} \tag{42}$$

$$\frac{UAV \xleftarrow{r_2 \oplus r_4} GCS}{UAV \ni \mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV}),\ \mathrm{D} \ni \mathrm{h}(\mathrm{ID}_{\mathrm{MO}}||\mathrm{r}_1),\ \mathrm{D} \ni \{\mathrm{D}_{MO} \oplus \mathrm{PK}_{UAV}\}_{PK_{MO}}} \tag{43}$$

$$\frac{MO \xleftarrow{r_1 \oplus r_3} GCS}{MO \ni \mathrm{h}\{(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_7)\}_{\mathrm{PK}_{UAV}},\ MO \ni \mathrm{SK}_{UAV}} \tag{44}$$

$$\frac{GCS \xleftarrow{r_1 \oplus r_3} MO}{GCS \ni \mathrm{h}\{(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_7)\}_{\mathrm{PK}_{UAV}},\ GCS \ni \mathrm{PK}_{UAV}} \tag{45}$$

$$\frac{GCS \xleftarrow{r_2 \oplus r_4} UAV}{GCS \ni \{\mathrm{h}(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_5)\}_{PK_{UAV}},\ GCS \ni T_5} \tag{46}$$

$$\frac{UAV \xleftarrow{r_2 \oplus r_4} GCS}{UAV \ni \{\mathrm{h}(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_5)\}_{PK_{UAV}},\ UAV \ni T_5} \tag{47}$$

$$\frac{GCS \xleftarrow{r_1 \oplus r_3} MO}{GCS \ni \mathrm{h}\{(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_7)\}_{\mathrm{PK}_{UAV}},\ GCS \ni ID_{UAV}} \tag{48}$$

$$\frac{GCS \xleftarrow{r_1 \oplus r_3} MO}{MO \ni \mathrm{h}\{(\mathrm{SK}_{UAV}||\mathrm{C}_{MO}||\mathrm{D}_{MO}||\mathrm{T}_7)\}_{\mathrm{PK}_{UAV}},\ MO \ni ID_{UAV}} \tag{49}$$

$$\frac{GCS \xleftarrow{r_2 \oplus r_4} UAV}{GCS \ni \{h(\mathrm{A}_{UAV}||\mathrm{PK}_{UAV}||\mathrm{ID}_{UAV}||\mathrm{D}_{MO})||\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{D}_{MO}) \oplus \mathrm{PK}_{UAV}||\mathrm{T}_3\}_{PK_{UAV}}} \tag{50}$$

$$\frac{UAV \xleftarrow{r_2 \oplus r_4} GCS}{UAV \ni \{h(\mathrm{A}_{UAV}||\mathrm{PK}_{UAV}||\mathrm{ID}_{UAV}||\mathrm{D}_{MO})||\mathrm{h}(\mathrm{r}_{UAV}||\mathrm{ID}_{UAV})||\mathrm{h}(\mathrm{ID}_{MO}||\mathrm{r}_1)||\mathrm{D}_{MO}) \oplus \mathrm{PK}_{UAV}||\mathrm{T}_3\}_{PK_{UAV}}} \tag{51}$$

Recognition of r_3, we get (53), as shown at the bottom of the next page.

Recognition of secret values k (54), shown at the bottom of the next page.

Recognition of random nonce r_D (55), shown at the bottom of the next page.

Recognition of random nonce r_1 (56), shown at the bottom of the next page.

Recognition of random nonce r_2 (57), shown at the bottom of the next page.

Keeping in view the analysis given above, C1, C2, if the GCS believes that $\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM}$ is recognizable Eq: (25), and the GCS possesses the key Eq: (31), then the GCS is entitled in believing the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (57), the GCS recognizes the message $\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM}$. From this, we have achieved Goal1.

Recognition of random nonce r_4 (58), shown at the bottom of the next page.

Recognition of random nonce r_3

$$\frac{MO|\equiv\Phi\,(r_3)}{MO\ni\{h\,(SK_{UAV}\,||C_{MO}||\,D_{MO}|\,|T_5)\}_{PK_{UAV}},\ MO\ni T_5} \tag{59}$$

Recognition of random nonce r_D

$$\frac{GCS|\equiv\Phi\,(r_{UAV})}{GCS\ni\{h\,(SK_{UAV}\,||C_{MO}||\,D_{MO}|\,|T_5)\}_{PK_{UAV}},\ GCS\ni T_5} \tag{60}$$

Keeping in view the analysis given above, E1, E2, if the GCS believes the M, that $\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM}$ is recognizable Eq: (36), and the GCS possesses the M and the key in Eq: (36), then the GCS is entitled in believing the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (60), both the GCS and M recognize the message $\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM}$. From this, we have achieved Goal6(b).

Recognition of random nonce r_4

$$\frac{UAV|\equiv\Phi\,(r_4)}{UAV\ni\{h\,(SK_{UAV}\,||C_{MO}||\,D_{MO}|\,|T_5)\}_{PK_{UAV}},\ UAV\ni T_5} \tag{61}$$

Keeping in view the analysis given above, D1 if the D believes that $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$ is recognizable Eq: (38)-(39), and the D recognizes the key in Eq: (38), then the D is entitled in believing the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (61), the D recognizes the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$. From this, we have achieved Goal7.

Recognition of random nonce r_2

$$\frac{GCS|\equiv\Phi\,(r_2)}{GCS\ni\{h\,(SK_{UAV}\,||C_{MO}||\,D_{MO}|\,|T_5)\}_{PK_{UAV}},\ GCS\ni T_5} \tag{62}$$

Keeping in view the analysis given above, D1 if the GCS believes that $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$ is recognizable Eq: (38)-(39), and the GCS recognizes the key in Eq: (38), then the GCS is entitled in believing the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (62), the GCS recognizes the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$. From this, we have achieved Goal8.

Recognition of random nonce r_{1s}

$$\frac{GCS\,|\equiv D|\equiv\Phi\,(r_1),\ \ (r_{UAV})}{GCS\,|\equiv D|\equiv\{h\,(SK_{UAV}\,||C_{MO}||\,D_{MO}|\,|T_5)\}_{PK_{UAV}},\ GCS\ni T_5} \tag{63}$$

Keeping in view the analysis given above, D1, D2 if the D and GCS believe that $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$ is recognizable via Eq: (38)-(39), and both the D and GCS recognize the key in Eq: (39), then both the D and GCS are entitled in believing the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (63), both the D and GCS recognize the message $\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$. From this, we have achieved Goal9.

Recognition of random nonce r_M and r_3 (64), as shown at the bottom of the next page.

Keeping in view the analysis given above, D1, D2, if the M believes that $|\sim(\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM})$ is recognizable Eq: (34), and the M possesses the key Eq: (35), then the M is entitled in believing the message $(\{h(SK_D||C_M||D_M||T_5)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (64), the M recognizes the message $\{h(r_D||ID_D)||h(ID_M||r_1)||h(C_M||D_M||T_1)\}_{PKM}$. From this, we have achieved Goal2.

Recognition of random nonce r_1, r_D, r_2 and k (65), as shown at the bottom of the next page.

Keeping in view the analysis given above, D1, D2, if the GCS believes that $\{h(A_D||PK_D||ID_D||D_M)$, $h(r_D||ID_D)$, $h(ID_M||r_1)$, $D_M\oplus PK_D$, $T_3\}_{PKM}$ is recognizable Eq: (38), and the GCS possesses the key in Eq: (38), then the GCS is entitled in believing the message $\{h(A_D||PK_D||ID_D||D_M)$, $h(r_D||ID_D)$, $h(ID_M||r_1)$, $D_M\oplus PK_D$, $T_3\}_{PKM}$, which is recognized by PK_D, and D_M; therefore, Eq: (65), the GCS recognizes the message $\{h(A_D||PK_D||ID_D||D_M)$, $h(r_D||ID_D)$, $h(ID_M||r_1)$, $D_M\oplus PK_D$, $T_3\}_{PKM}$. From this, we have achieved Goal3.

Recognition of random nonce r_4 (66), as shown at the bottom of the next page.

Keeping in view the analysis given above, D1, D2, if the D believes that $\{h(A_D||PK_D||ID_D||D_M)$, $h(r_D||ID_D)$, $h(ID_M||r_1)$, $D_M\oplus PK_D$, $T_3\}_{PKM}$ is recognizable Eq: (28), and the D possesses the key in Eq: (29), then the D is entitled in believing the message $\{h(A_D||PK_D||ID_D||D_M)$, $h(r_D||ID_D)$, $h(ID_M||r_1)$, $D_M\oplus PK_D$, $T_3\}_{PKM}$, which is

$$\frac{MO|\equiv\Phi\,(r_{MO})}{\{MO\ni h(r_{UAV}|\,|ID_{UAV})\,,\ MO\ni h\,(ID_{MO}|\,|r_1)\,,\ MO\ni h\,(C_{MO}\,||D_{MO}||\,T_1)\}_{PK_{MO}}} \tag{52}$$

recognized by PK_M, and D_M; therefore, Eq: (66), the D recognizes the message $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$. From this, we have achieved Goal4.

Recognition of random nonce key PK_M, we get (67), as shown at the bottom of the page.

Keeping in view the analysis given above, D1, D2, if the D believes that $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$ is recognizable Eq: (28), and the D possesses the key in Eq: (29), then the D is entitled in believing the message $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$, which is recognized by PK_M, and D_M; therefore, Eq: (67), the D recognizes the message $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$. From this, we have achieved Goal5.

According to D2, Eq: (65) and (67) can be written as (68), as shown at the bottom of the page.

$$\frac{MO|\equiv \Phi\ (r_3)}{\{MO \ni h(r_{UAV}||ID_{UAV}),\ MO \ni h\ (ID_{MO}||r_1),\ MO \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{53}$$

$$\frac{GCS|\equiv \Phi\ (k)}{\{GCS \ni h(r_{UAV}||ID_{UAV}),\ GCS \ni h\ (ID_{MO}||r_1),\ GCS \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{54}$$

$$\frac{GCS|\equiv \Phi\ (r_{UAV})}{\{GCS \ni h(r_{UAV}||ID_{UAV}),\ GCS \ni h\ (ID_{MO}||r_1),\ GCS \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{55}$$

$$\frac{GCS|\equiv \Phi\ (r_1)}{\{GCS \ni h(r_{UAV}||ID_{UAV}),\ GCS \ni h\ (ID_{MO}||r_1),\ GCS \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{56}$$

$$\frac{GCS|\equiv \Phi\ (r_2)}{\{GCS \ni h(r_{UAV}||ID_{UAV}),\ GCS \ni h\ (ID_{MO}||r_1),\ GCS \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{57}$$

$$\frac{UAV|\equiv \Phi\ (r_4)}{\{UAV \ni h(r_{UAV}||ID_{UAV}),\ UAV \ni h\ (ID_{MO}||r_1),\ UAV \ni h\ (C_{MO}||D_{MO}||T_1)\}_{PK_{MO}}} \tag{58}$$

$$\frac{MO\ |\equiv \Phi\ (r_{MO}),\ MO|\equiv \Phi\ (r_3)}{MO \ni \{h(A_{UAV}||PK_{UAV}||ID_{UAV}||D_{MO})||h\ (r_{UAV}\ ||ID_{UAV})|\ |h\ (ID_{MO}\ ||r_1)|\ |D_{MO}) \oplus PK_{UAV}|\ |T_5\}_{PK_{UAV}}} \tag{64}$$

$$\frac{GCS\ |\equiv \Phi\ (k),\ GCS|\equiv \Phi\ (r_{UAV}),GCS|\equiv \Phi\ (r_1),\ GCS|\equiv \Phi\ (r_2)}{GCS \ni \{h(A_{UAV}||PK_{UAV}||ID_{UAV}||D_{MO})||h\ (r_{UAV}\ ||ID_{UAV})|\ |h\ (ID_{MO}\ ||r_1)|\ |D_{MO}) \oplus PK_{UAV}|\ |T_3\}_{PK_{UAV}}} \tag{65}$$

$$\frac{UAV|\equiv \Phi\ (r_4)}{UAV \ni \{h(A_{UAV}||PK_{UAV}||ID_{UAV}||D_{MO})||h\ (r_{UAV}\ ||ID_{UAV})|\ |h\ (ID_{MO}\ ||r_1)|\ |D_{MO}) \oplus PK_{UAV}|\ |T_3\}_{PK_{UAV}}} \tag{66}$$

$$\frac{UAV|\equiv \Phi\ (PK_{MO})}{UAV \ni \{h(A_{UAV}||PK_{UAV}||ID_{UAV}||D_{MO})||h\ (r_{UAV}\ ||ID_{UAV})|\ |h\ (ID_{MO}\ ||r_1)|\ |D_{MO}) \oplus PK_{UAV}|\ |T_3\}_{PK_{MO}}} \tag{67}$$

$$\frac{GCS\ |\equiv\ UAV|\equiv \Phi\ (PK_{MO}),\ k,\ r_1,\ r_2}{GCS|\equiv UAV \ni \{h(A_{UAV}||PK_{UAV}||ID_{UAV}||D_{MO})||h\ (r_{UAV}\ ||ID_{UAV})|\ |h\ (ID_{MO}\ ||r_1)|\ |D_{MO}) \oplus PK_{UAV}|\ |T_3\}_{PK_{MO}}} \tag{68}$$

Keeping in view the analysis given above, D2, if both the GCS and D believe that $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$ is recognizable Eq: (39), and both the GCS and D possess the key in Eq: (40), then both the GCS and D are entitled in believing the message $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$, which is recognized by PK_M, and D_M; therefore, Eq: (68), the GCS and D recognize the message $\{h(A_D||PK_D||ID_D||D_M), h(r_D||ID_D), h(ID_M||r_1), D_M \oplus PK_D, T_3\}_{PKM}$ and from this analysis we have achieved Goal6 (a).

$$\frac{MO|\equiv \Phi\,(\mathrm{PK}_{UAV})}{MO \ni \{h\,(\mathrm{SK}_{UAV}\,||\mathrm{C}_{MO}||\,\mathrm{D}_{MO}|\,|\mathrm{T}_5)\}_{PK_{UAV}},\ MO \ni T_7} \quad (69)$$

Keeping in view the analysis given above, D1, if the GCS believes that $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ is recognizable Eq: (36)-(37), and the GCS possesses the key in Eq: (45), then the GCS is entitled in believing the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (69), the GCS recognizes the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ and from this analysis we have achieved Goal10.

$$\frac{GCS|\equiv \Phi\,(\mathrm{PK}_{UAV})}{GCS \ni \{h\,(\mathrm{SK}_{UAV}\,||\mathrm{C}_{MO}||\,\mathrm{D}_{MO}|\,|\mathrm{T}_5)\}_{PK_{UAV}},\ GCS \ni T_7} \quad (70)$$

Keeping in view the analysis given above, D1, if the M believes that $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ is recognizable Eq: (34), and the M possesses the key in Eq: (35), then the M is entitled to believe the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (70), the M recognizes the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ and from this analysis we have achieved Goal11. (71), as shown at the bottom of the next page.

Keeping in view the analysis given above, D1, D2, if both the GCS and M believe that $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ is recognizable Eq: (36)-(37), and both the GCS and M possess the key in Eq: (35), then both the GCS and M are entitled in believing the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$, which is recognized by PK_D, C_M, and D_M; therefore, Eq: (71), the GCS and M recognize the message $\{h(SK_D||C_M||D_M||T_7)\}_{PKD}$ and from this analysis we have achieved Goal12.

B. PROVERIF SIMULATION

To test the secrecy, confidentiality, authorization, and reachability of the secret session key, a well-known toolkit called ProVerif [29] is used. The summary of the results demonstrated that the attacker couldn't crack the SK and identity at any stage of the protocol.

```
Verification summary:
Query inj-event(endM(IDM)) ==> inj-event(startM(IDM)) is true.
Query inj-event(endD(IDD)) ==> inj-event(startD(IDD)) is true.
Query inj-event(endGCS(IDGCS)) ==> inj-event(startGCS(IDGCS))
is true.

Query not attacker(SK[]) is true.
```

C. INFORMAL SECURITY ANALYSIS

In this subsection of the article, we present a discussion of attacks on the proposed protocol by considering [6] and [7]. These attack discussions are as follows:

1. *Replay Attack:* In the authentication phase of the protocol, an attacker tries to send $\{A_D, C_M, G_M, PK_M, T_1\}$, $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$, $\{Auth_D, PK_D^*, T_5\}$, and $\{Auth_{GCS}, PK_D^*, T_7\}$ packets. Due to the random nonce r_1, r_2, r_3, and r_4 in each round trip of the protocol and different checks like $F_M ?= F_M^*$, $G_M ?= G_M^*$, and $I_M ?= I_M^*$, such an attempt is not possible. So, the proposed protocol is safe against replay attacks.
2. *Impersonation Attack:* To impersonate the system using $\{A_D, C_M, G_M, PK_M, T_1\}$, the attacker must know ID_M and PW_M; they can't identify any of the above secrets. Similarly, while using $\{I_M, PK_M, A_D\}$ and $\{C_M, H_{DM}, T_3\}$, they have the knowledge of D_M and G_M^*, which is also impossible. The same is true for $Auth_D, PK_D^*, T_5\}$ and $\{Auth_{GCS}, PK_D^*, T_7\}$. Therefore, the proposed protocol is safe against impersonation attacks.
3. *Privacy Protection:* The different credentials stored are dynamically changed for the upcoming session key computation; if, for example, the attacker computes or reaches the previous session key, they cannot launch any attack due to not finding useful parameters. Similarly, the messages communicated over a public network channel are without any identity or plaintext; if an attacker copies it and tries to figure out something useful, they can't due to the 160-bit ECC key and SHA-1 algorithm. Therefore, in the proposed protocol, the privacy of a drone is preserved.
4. *Privileged Insider Attack:* If a privileged user desires to enter the GCS and impersonate a D or Mobile user (M), as we have calculated the identity by concatenating a random nonce for extracting $A_D = h(r_D||ID_D)$, $PK_D = h(ID_D||k||r_D)$ credentials, and again attaching $C_M = h(ID_M|r_1)$, $D_M = h(C_M|k|r_2)$, $E_M = h(C_M|B_M|r_1|D_M)$, and $F_M = h(E_M|C_M)$ along with timestamp, so the attacker could not at any stage launch a privileged insider attack.
5. *Anonymity:* In the authentication phase of the protocol, the identity is very protected because it is concatenated with nonce, public key, and many other credentials. Similarly, we have used a time threshold for each round trip; if someone desires to identify a legitimate user, they cannot because of complex calculations and different checks. So, the privacy of a legal user is preserved in our scheme.
6. *Forward Secrecy:* The proposed protocol has a user password change phase, in which a legal user can easily, securely, and efficiently update their password without interacting with the GSS, which means the proposed secure framework offers high scalability and offloads the GSS.
7. *Stolen Verifier Attack:* The GCS stores $ID_D, A_D, PK_D, C_M, D_M$, and ID_M, whereas the Mobile device stores F_M, D_M, and r_1, h where $A_D = h(r_D||ID_D)$, $C_M = h(ID_M|r_1)$, and

TABLE 4. Comparative analysis (performance metrics).

Schemes	Communication Costs (Bits)	Computation Costs (Milliseconds)
Amin et al. [3]	4320	14.08
Jan et al. [5]	3720	17.793
Nikooghadam et al. [10]	432	54.242
Tian et al. [18]	5856	136.2
Chen et al. [19]	3168	29.418
Banerjee et al. [20]	2560	159.58
Srinivas et al. [21]	1536	26.7
Wazid et al. [22]	1696	27.02
Ali et al. [23]	1696	27.02
Proposed	3232	12.447

$D_M = h(C_M||k||r_2)$. If someone steals the Mobile device and tries to verify identity, key, nonce, password, etc., they must know the GCS secret key k, which is impossible from any stored values.

8. *MITM Attack:* In the authentication phase of the proposed protocol, if an adversary A desires to capture a message, update, delete, insert false information, eavesdrop, or alter the flow of messages, they cannot, as the attacker must pass many steps. Each message has a timestamp, and each round trip has checks; the adversary must pass them before identifying something valuable in the message. To do so, they need help finding the 160-bit long key, secret values of the server, and other credentials. Therefore, MITM is not possible in our scheme.
9. *DoS Attack:* Suppose an adversary copies a message from the public network channel and struggles for a DoS attack. In that case, the attacker must pass many checks like $F_M?=F_M^*$, $G_M?=G_M^*$, and $I_M?=I_M^*$ present in the round trips of the protocol. Similarly, an adversary can validate the timestamp precisely as required; such attempts are impossible. So, the proposed protocol is safe against DoS attacks.
10. *Clock Synchronization Issue:* The clock synchronization issue can be addressed by configuring each participant to the global clock to establish the start and finish time slot and correct the offset and drift rate of the participants' clock with rest to global time.

D. PROTOCOL ADAPTABILITY

In the continuously evolving IoD application environment, there must be certain adaptability and flexibility to accommodate the proposed protocol for future technological transformations. One must keep the following things in mind when designing a secure framework for such an exhaustive environment:

- The security framework should be designed in a manner that doesn't compromise the functionalities of the drone.
- Secure session key computation can be minimized so the battery can survive longer.
- Focus should be given to the design of accelerometers, LiDAR (Light Detection and Ranging), and GPS so that drones can precisely navigate and control.
- The security features and performance metrics should be balanced with each other; if one is enhanced, the other will degrade and vice versa, so these contradicting features must be carefully tackled.
- Synergy among all the drone equipment and entities of IoD is crucial; anyone who designs a drone must take into consideration that they are perfectly accomplishing tactical tasks collaboratively.
- Besides these, regulatory, limited flight, collision avoidance and accountability can also be mitigated.

VI. PERFORMANCE ANALYSIS

The feature of the protocol can be measured by considering storage, communication, and computation costs. It is worth mentioning that owing to special features, implementing authentication protocols presents a number of difficulties, including scalability, dynamic networking topology, operationalizing drones in different contexts, and creating a unified, standardized protocol. Similarly, the biggest barriers to implementing a security standard in IoD are Low latency and bandwidth-limited networking, ECC Key and device life cycle management, growing adversary power for attacks, interoperability and regulatory concerns. These things create hurdles to implementing the proposed protocol in an actual IoD environment. However, standard values of [30] and [31] will be used for measuring the performance metrics of the proposed protocol, which are described one by one as follows:

A. COMMUNICATION OVERHEADS

The communication cost/overhead of a protocol is the total number of messages exchanged, typically expressed in bits or bytes. Standard values [30] and [31] are used to calculate the length of various parameters in bits. The hash code is 256 bits long, the public key is 160, and the time stamp is 32, according to [30] and [31]. To calculate the protocol's overall communication cost, all participants, messages exchanged, values and costs and finally the total costs are $M \rightarrow GCS$, $\{A_D, C_M, G_M, PK_M, T_1\}$, $256+256+256+160+32 \approx 960$ bits; $GCS \rightarrow D$, $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$, $256+256+256+160+416+32 \approx 1376$ bits; $D \rightarrow GCS$, $\{Auth_D, PK_D^*, T_5\}$, $256+160+32 \approx 448$ bits; $GCS \rightarrow M$, $\{Auth_{GCS}, PK_D^*, T_7\}$, $256+160+32 \approx 448$ bits. Therefore, the communication cost of the proposed scheme is 3232 bits.

$$\frac{GCS|\equiv MO|\equiv \Phi\,(\mathrm{PK}_{UAV})}{GCS|\equiv MO \ni \{h\,(\mathrm{SK}_{UAV}\,||\mathrm{C}_{MO}||\,\mathrm{D}_{MO}|\,|\mathrm{T}_5)\}_{PK_{UAV}},\ GCS|\equiv MO \ni T_7} \tag{71}$$

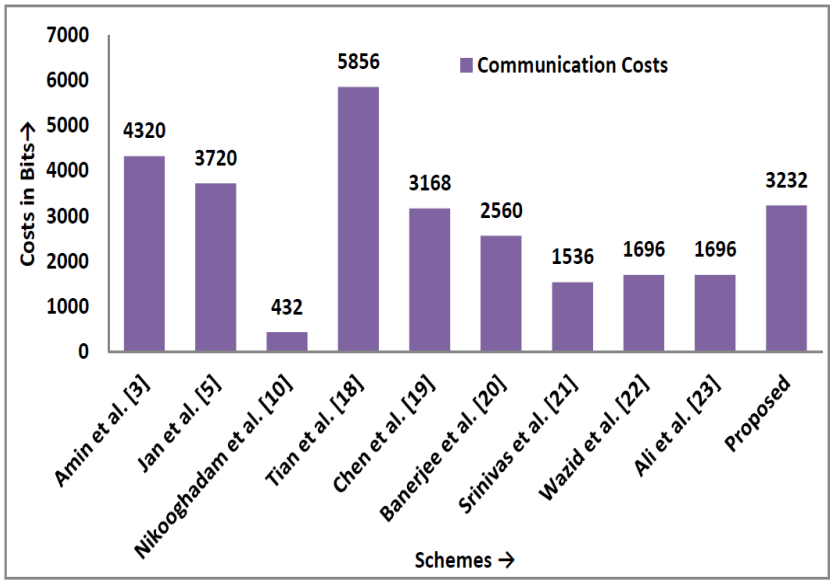


FIGURE 2. Communication costs comparison.

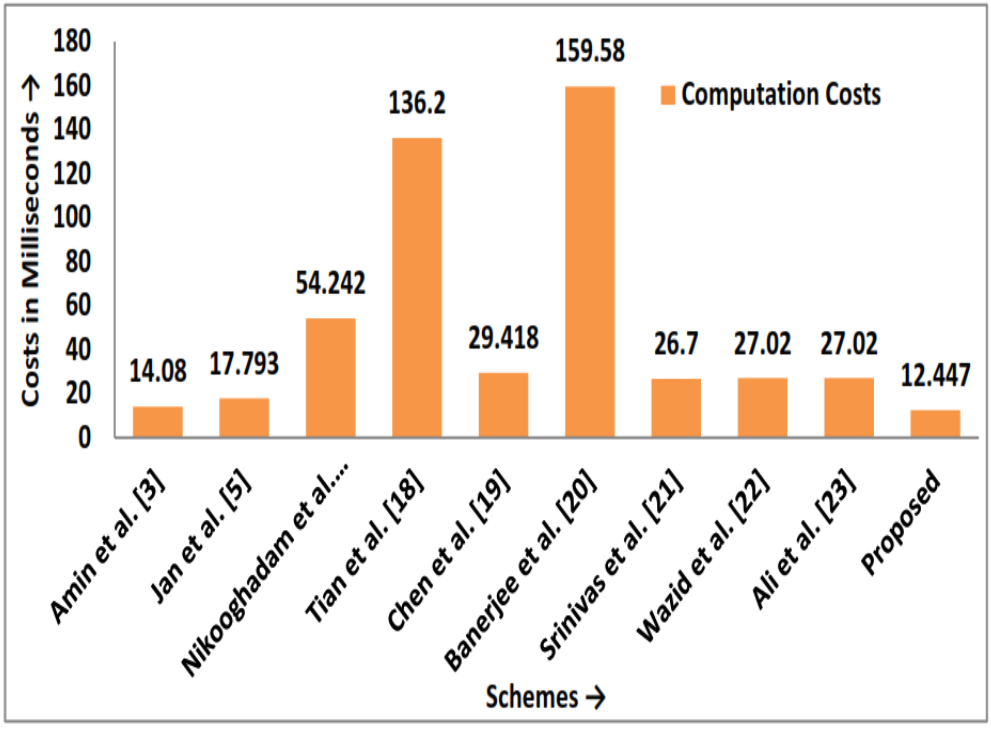


FIGURE 3. Computation costs comparison.

B. COMPUTATION OVERHEADS

Computation time, overhead, and cost are defined as the time required for a protocol to compute various operations at which they are executed on multiple entities in authentication protocols. Standard time values from [30] and [31] are used in the proposed protocol for the many operations that it involves. Some of the values are listed below:

- T_H means computation time for one-way hash function = 0.046ms
- T_E means computation time for extracting nonce/ random number = 2.011ms
- T_{xor} is the computation time for xor operation = 0 ms

Now, the computation costs of the proposed protocol are at GCS side $4T_H+ 1T_E+ 1T_{xor}$, 1.84+2.011≈3.851 ms; at drone side $3T_H+2T_E+1T_{xor}$, 0.138+4.022≈4.16 ms and at mobile-device peer it is $9T_H+2T_E+1T_{xor}$, 0.414+ 4.022≈4.436. The overall computation cost of the proposed protocol is 12.447 ms

TABLE 5. Comparative analysis (security features).

Security Functionalities	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[Our]
A-DoS Attack	Y	N	N	N	Y	N	Y	Y	N
B-Replay Attack	Y	N	N	N	N	N	N	N	N
C-Server Secret Directory Attack	N	Y	N	N	N	Y	N	N	N
D-Impersonation Attack	N	N	Y	Y	N	N	N	N	N
E-Password Guessing Attack	N	N	Y	N	N	N	N	N	N
F-Privileged Insider Attack	N	N	N	N	N	N	N	N	N
G-Forgery Attack	N	Y	N	N	Y	N	N	N	N
H-Insider Attack	N	N	N	Y	N	N	N	N	N
I-Stolen-Verifier Attack	N	Y	Y	N	N	Y	Y	N	N
J-Man-in-the-middle Attack	Y	N	N	Y	N	N	N	Y	N

C. COMPARATIVE ANALYSIS

Table 4 demonstrates the comparative analysis of the proposed protocol with exisiting works. This analysis has been made in terms of communication and computation overheads with existing schemes, including [3], [5], [10], [18], [19], [20], [21], [22], and [23]. The results are shown in Figures 2 and 3, where it is clear that the proposed protocol outperformed most of its competitor schemes. The proposed protocol achieved a minimum of 13.11% and a maximum of 44.80% communication efficiency compared to its counterparts. However, the schemes presented in [10], [20], [21], [22] and [23] perform better regarding communication cost; however, their security could be more robust than the proposed protocol.

Similarly, in terms of computation overhead, as shown in Figure 3, the proposed protocol again outperformed all of its competitors by obtaining the lowest computation time of 12.447ms, achieving a minimum of 11.59% and a maximum of 90.86 % computation efficiency compared to its counterparts. Mean the communication costs of [10], [20], [21], [22], and [23] are better than the proposed scheme. However, its computation costs are higher than our scheme. Similarly, the security of this scheme is also weaker than our scheme shown in Table 5. So, our scheme shows a delicate balance of security with performance, which is often missing in this scheme.

VII. CONCLUSION

A secure authentication protocol for the Internet of Drones (IoD) environment is presented in this article. Asymmetric key cryptography, a collision-free one-way hash function, and xor operations were used to design the proposed protocol. The storage, communication, and computing costs analysis was used to examine the performance of the proposed protocol; the GNY model and ProVerif were used to investigate its security. It is advised that the proposed protocol be implemented in an actual IoD setting because the findings demonstrate that its security is robust against known attacks and performance is lightweight. Blockchain technology may be used to redesign the proposed protocol, and AVISPA may be used to simulate it.

ACKNOWLEDGMENT

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-23-DR-102), therefore, the author thanks the University of Jeddah for its technical and financial support.

REFERENCES

[1] Z. Zhang, C. Hsu, M. H. Au, L. Harn, J. Cui, Z. Xia, and Z. Zhao, "PRLAP-IoD: A PUF-based robust and lightweight authentication protocol for Internet of Drones," *Comput. Netw.*, vol. 238, Jan. 2024, Art. no. 110118.

[2] M. Alkanhal, A. Alali, and M. Younis, "A distributed lightweight PUF-based mutual authentication protocol for IoV," *IoT*, vol. 5, no. 1, pp. 1–19, Dec. 2023.

[3] R. Amin, S. Jayaswal, V. Sureshkumar, B. Rathore, A. Jha, and M. Abdussami, "IoDseC++: Authenticated key exchange protocol for cloud-enabled Internet of Drone communication," *J. Ambient Intell. Humanized Comput.*, vol. 7, pp. 9529–9542, May 2023.

[4] U. C. Cabuk, G. Dalkilic, and O. Dagdeviren, "CoMAD: Context-aware mutual authentication protocol for drone networks," *IEEE Access*, vol. 9, pp. 78400–78414, 2021.

[5] 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.

[6] D. Bolignano, "An approach to the formal verification of cryptographic protocols," in *Proc. 3rd ACM Conf. Comput. Commun. Secur. (CCS)*, 1996, pp. 106–118.

[7] P. Modesti and R. Garcia, "Formal modeling and security analysis of security protocols," in *Handbook of Formal Analysis and Verification in Cryptography*. Boca Raton, FL, USA: CRC Press, 2023, pp. 213–274.

[8] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. India: Pearson Education, 2006.

[9] K. N. Kumar, G. R. Kumar, G. V. Kumar, and P. C. Sekhar, "Bitwise operations based encryption and decryption," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 1, pp. 46–50, 2011.

[10] 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.

[11] J. Guo, Y. Du, Y. Zhang, and M. Li, "A provably secure ECC-based access and handover authentication protocol for space information networks," *J. Netw. Comput. Appl.*, vol. 193, Nov. 2021, Art. no. 103183.

[12] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 5, pp. 1616–1628, Sep. 2020.

[13] 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, Mar. 2020.

[14] M. A. El-Zawawy, A. Brighente, and M. Conti, "SETCAP: Service-based energy-efficient temporal credential authentication protocol for Internet of Drones," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108804.

[15] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for Internet of Drones," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 3319–3332, Sep. 2021.

[16] V. O. Nyangaresi and N. Petrovic, "Efficient PUF based authentication protocol for Internet of Drones," in *Proc. Int. Telecommun. Conf. (ITC-Egypt)*, Jul. 2021, pp. 1–4.
[17] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment," *Comput. Netw.*, vol. 195, Aug. 2021, Art. no. 108219.
[18] 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.
[19] Y. Chen, L. López, J.-F. Martínez, and P. Castillejo, "A lightweight privacy protection user authentication and key agreement scheme tailored for the Internet of Things environment: LightPriAuth," *J. Sensors*, vol. 2018, pp. 1–16, Sep. 2018.
[20] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8739–8752, Oct. 2019.
[21] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.
[22] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[23] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.
[24] Y. Kirsal 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.
[25] T. Alladi, V. Chamola, Naren, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, Jul. 2020.
[26] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, vol. 77, no. 2, pp. 1114–1151, Feb. 2021.
[27] L. Gong, R. Needham, and R. Yahalom, "Reasoning about belief in cryptographic protocols," in *Proc. IEEE Symp. Res. Secur. Privacy*, May 1990, p. 234.
[28] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[29] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial," *Version*, pp. 5–16, May 2018.
[30] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014.
[31] A. F. Baig, K. M. U. Hassan, A. Ghani, S. A. Chaudhry, I. Khan, and M. U. Ashraf, "A lightweight and secure two factor anonymous authentication protocol for global mobility networks," *PLoS ONE*, vol. 13, no. 4, Apr. 2018, Art. no. e0196061.

ABDULRAHMAN AHMED ALZAHRANI received the bachelor's degree in computer science, the master's degree in computer science, engineering management, information systems and technology, and business administration, and the Ph.D. degree in information systems and technology.

He teaches several courses to bachelor's and master's students. He is currently the Head of the Computer Engineering and Network Department. He is an Assistant Professor with the Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. His research interests include information security and innovations in data science, machine learning, health informatics, the Internet of Things (IoT), and the Internet of Drones (IoD).