IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 July 2022, accepted 29 August 2022, date of publication 6 September 2022, date of current version 15 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3204793

RESEARCH ARTICLE

Authenticated Secure Quantum-Based Communication Scheme in Internet-of-Drones Deployment

HUSSEIN ABULKASIM[1,2], (Member, IEEE), BRIAN GONCALVES[1], ATEFEH MASHATAN[1], AND SHOHINI GHOSE[3,4]

[1]Cybersecurity Research Laboratory, Ted Rogers School of Information Technology Management, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada
[2]Faculty of Science, New Valley University, El-Kharga 71511, Egypt
[3]Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, ON N2L 3C5, Canada
[4]Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada

Corresponding author: Hussein Abulkasim (abulkasim@ryerson.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada and in part by NXM Labs Inc.

ABSTRACT The rapid advance of manufacturing Unmanned Aerial Vehicles (UAVs, aka drones) has led to a rise in the use of their civilian and commercial applications. The access of these drones to controlled airspace can be efficiently coordinated through particular layered network architecture, often referred to as the Internet-of-Drones (IoD). The nature of IoD, which is deployed in an open-access environment, brings significant safety and security concerns. Classical cryptosystems such as elliptic curve cryptography, Rivest-Shamir-Adleman, and Diffie-Hellman are essential building blocks to secure communication in the IoD. However, with the rapid development of quantum computing, it will be easy to break public-key cryptosystems using efficient quantum algorithms like Shor's algorithm. Thus, building quantum-safe solutions to enhance IoD security has become imperative. Fortunately, quantum technologies can provide unconditional security solutions to protect data and communications in the IoD environment. This paper proposes a quantum-based scheme to prevent unauthorized drones from accessing a specific flight zone and authenticates the identities and shared secret messages of involved entities. To do so, we used a quantum channel to encode the private information based on a pre-shared key and a random key generated in a session. The involved entities also perform mutual authentication and share a secret key. We also provide the security proofs and analysis of the proposed scheme that indicates its resistance to well-known attacks.

INDEX TERMS Authentication, internet-of-drones, quantum-based communication, quantum cryptography.

I. INTRODUCTION

Recently, the IoD has received a lot of attention from both research and industry thanks to the fact that the IoD can provide direct or indirect access to drones. In this scenario, the drones may only operate as mobile routers to forward information to distant nodes or be a part of the operations themselves, establishing autonomous swarms or mesh networks of drones for Unmanned Aerial System (UAS) applications. Ongoing developments in communication and wireless networked systems make drones attractive systems to be employed in a wide range of applications and services ranging from military to civilian applications. Also, rapid technological advancements in manufacturing high-quality and low-cost commercial drones have opened up a slew of new business opportunities for consumer services like rescue operations, goods delivery, aerial photography and videography, live streaming, firefighting, disaster relief, crop spraying, crop

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

monitoring, etc. By 2025, the potential economic impact of integrated UAS is expected to reach $82 billion and generate employment of up to 100,000 individuals, thanks to increased government initiatives to simplify the regulatory environment [43], [44]. Aerial technology can provide services at a lower cost and higher efficiency not easy to provide by traditional methods, making giants such as Amazon and Walmart praise it as the future of e-commerce. UAS involve critical strategic and financial information, making them vulnerable to attacks by unauthorized users that target communication, transmitted data, or even physical elements. Without robust security and privacy communication systems, drones can be used for illegal acts ranging from simple surveillance to serious crimes like terrorist attacks and targeted assassinations. In the beginning, researchers and engineers were focused on the development of drone architecture and their functional effectiveness without giving much attention to protecting the integrity or confidentiality of drones' communications and data. Therefore, several recent papers have been published to address the problems of security and privacy based on classical cryptography [1], [2], [3], [4], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38]. However, none of these recent papers considered the threat of quantum computing and only focused on the classical sense of security. In such works, public-key cryptosystems like elliptic curve cryptography, Rivest-Shamir-Adleman (RSA), and Diffie-Hellman are essential building blocks to secure communication. All these classical cryptosystems have one thing in common: they are all based on the difficulty of solving some complex mathematical problems. To assure the security of such cryptosystems, it must be shown that cracking them is as difficult as solving an intractable mathematical problem without possessing a secret piece of information. The security of such a cryptosystem is guaranteed by the hardness of adopted mathematical problems like the discrete logarithm problem and the integer factorization problem. If an advanced cryptanalysis algorithm defeats the hardness, such a cryptosystem is deemed compromised. In 1994, Shor developed a quantum cryptanalysis algorithm that could find discrete logarithms and factor integers exponentially faster than classical algorithms [39]. Shor's algorithm theoretically enables quantum computers to crack the majority of public-key cryptosystems currently in use. Quantum computers exist presently, but they need significant technical improvement to be widely utilized. It is believed that a quantum computer with around 20 million quantum bits (qubits) is required to break an RSA-2048 algorithm [40]. Once scaled, quantum computers will catastrophically break most of our commonly used standardized mechanisms for ensuring the integrity and confidentiality of the data [5], [6]. Fortunately, quantum cryptography is able to provide unconditional security for the stored and communicated data (i.e., a protocol remains secure even if an attacker has unlimited computing power or a powerful quantum computer) [41], [42]. Therefore, securing the communication of drones based on quantum cryptography could resist the potential threat of a powerful quantum computer and is significant for scenarios where the communicated data is of high value to the attackers.

In 2020, Liu *et al.* [7] experimentally developed an airborne mobile quantum communication network using a quantum-based drone. They used the quantum-based drones as nodes capable of generating and measuring quantum bits (qubits); hence the drones can build a secure quantum channel among communicators. Liu *et al.*'s mobile quantum network could be used for multiple functions: 1) to interconnect quantum satellites with quantum fiber ground networks; 2) to connect two quantum ground nodes or servers; 3) to connect quantum drones with other quantum ground nodes or users and so on. Their work opens the door for a new era of quantum-based drone development that could be used in real life. In this paper, we propose an authentication scheme based on quantum cryptography for authenticating the involved entities and securing the transmitted data in the IoD deployment. The network model of the proposed scheme contains various drones deployed in many zones that send their data to a ground station. We will prove the security of communication between entities against related common attacks such as impersonation attacks and man-in-the-middle attacks.

A. MOTIVATION

Previous works have indicated that there are many challenges threatening the expansion of the use of drones for civilian and military purposes [8]. Among these threats and challenges are the authentication of drones and the other involved entities, controlling and hacking of the drones, jamming of the broadcast communication, and others. Recently, several drone incidents have occurred due to a lack of drone authentication. For example, many heavy-traffic airports in different countries were closed and incurred huge financial losses due to unauthorized access from suspicious drones (a recent relevant survey on this topic can be found in [9]). Therefore, it is crucial to achieve authentication between ground stations and drones to check whether a drone is authorized to access a certain zone or not. Also, in some special cases, authentication is needed between a drone and another drone for sharing some information as well as authenticating the sensitive transmitted messages among participants. The importance of authentication and such incidents motivate the need to propose and design secure authentication schemes for drones. As a result, several schemes employed classical cryptosystems to ensure the security and privacy of communications in the IoD environment [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38]. However, Quantum computing can efficiently break those classical cryptosystems that rely on the complexity of these problems [39]. In 2016, NIST (National Institute of Standards and Technology) published a report on post-quantum cryptography, anticipating that a universal quantum computer capable of breaking 2000-bit RSA in a few hours will be available by 2030, making the existing public-key infrastructure (PKI) insecure [45]. Therefore, quantum-safe schemes based on quantum cryptography or post-quantum cryptography to secure the IoD is imperative.

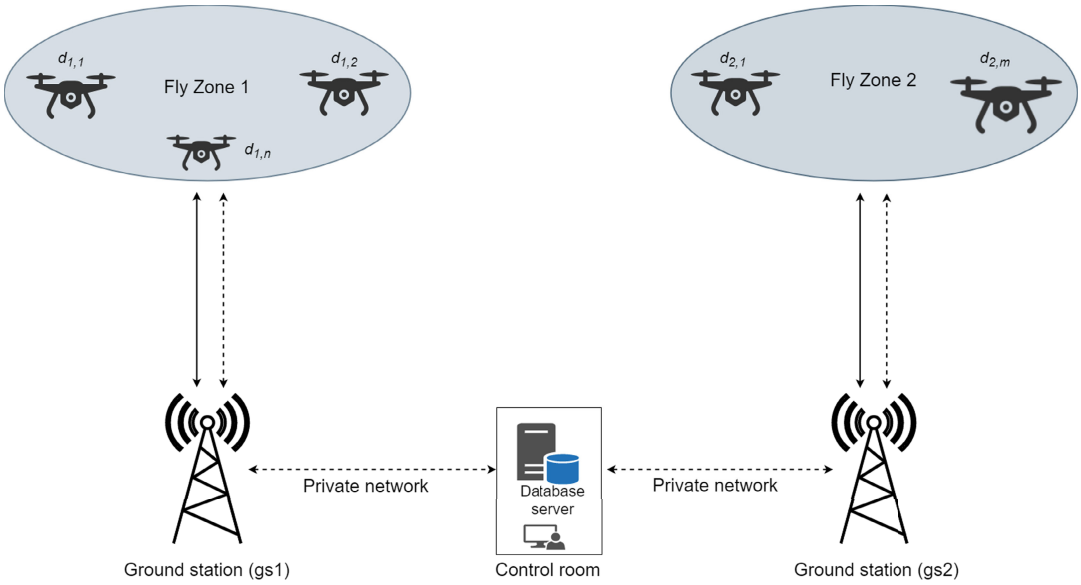

FIGURE 1. Proposed model.

B. RELATED WORK

In 2018, Wazid *et al.* [10] provided a comparative study on some previous authentication protocols for the IoD in terms of communication overheads and the features of functionality and security. They also introduced a generalized taxonomy of the authentication protocols in the IoD environment. Moreover, the authors provided a list of practical challenges for designing secure authenticated protocols in the IoD deployment. In 2019, Srinivas *et al.* [11] presented an authenticated lightweight method for users in the IoD environment with temporal credentials. The authors employed the techniques of hash function and fuzzy extractor. Also, they provided a comparative analysis of their proposed mechanisms with other existing schemes, demonstrated that their scheme is better in both security and functionality, and has lower computation and communication costs. In 2020, Alladi *et al.* [12] provided a lightweight authentication scheme to secure the communication between drones and their ground stations based on the technique of Physical Unclonable Function. Pu and Li [31] presented a lightweight authentication scheme to provide secure communications between ground stations and drones. The basic idea behind their scheme is that the ground station and drone employ the chaotic maps' seed value to randomly rearrange genuine messages according to the created chaotic sequence. Also, Pu *et al.* [22] proposed a lightweight mutual authentication and key agreement scheme with protecting privacy for the IoD. A chaotic system and physical unclonable function are used to provide mutual authentication and create a session key between IoD system communication parties. However, drones are vulnerable to device capturing and certain types of attacks because of remote environments and limited resources. This raises the possibility of attackers stealing drone data. In the same context, several authentication protocols have been presented [3], [4], [13], [14], [15]. However, securing communication channels in such schemes are based on classical cryptosystems, which are vulnerable to the massive power of a quantum computer or classical computing resources [5], [6]. As a response to those problems, quantum cryptography, as one of the most mature quantum computing applications, has been adopted to provide unconditionally secure solutions in various communication systems that seek optimal security of sensitive data and communication against attackers [16]. In 2019, Liu *et al.* demonstrated a drone-based mobile communication system for multi-node construction and real-time all-location coverage. The designed system has been proven robust against all-weather conditions and can be scaled to multi-node structures. In 2021, Yu *et al.* designed an airborne quantum key distribution model that connects terrestrial networks with satellite networks to establish a real-time on-demand quantum network. These works focused on the ability to build quantum communication through drones and its efficiency in the IoD deployment and did not consider significant security features such as authentication, key sharing, and key management. Inspired by Liu *et al.* [7] and other related works [17], [18], [19], this work introduces a robust and lightweight authentication scheme to secure the communication and data in the IoD deployment.

C. RESEARCH CONTRIBUTIONS

- We propose a mutual identity and message authentication scheme between the drones and the ground stations.
- A pre-shared secret key can be reused without information leaks.
- Sharing a secure random key among authenticated entities for securing transmitted data.
- The proposed model is secure against well-known attacks.

The remainder of the paper is organized as follows. In Section II, we introduce the model considered for the main result of this paper, provide a table of notation, then

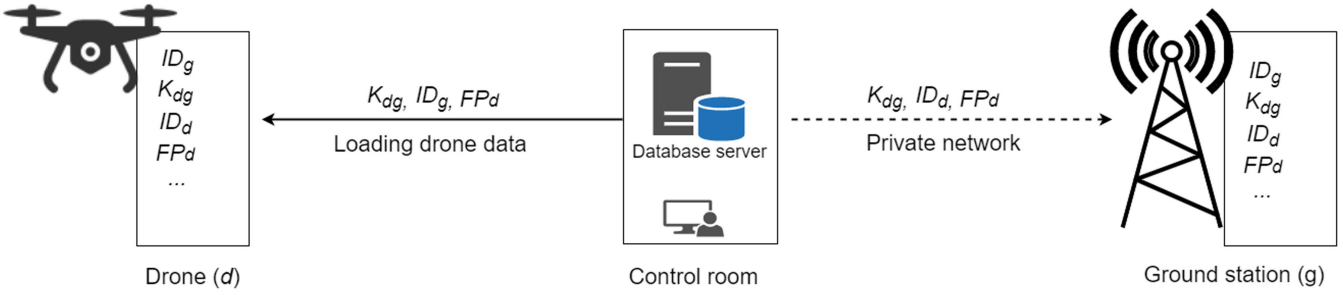

FIGURE 2. Database server pre-shares K_dg with both the drone and the ground station and preloads the drone data into the drone before taking off. The dashed line refers to a quantum channel.

describe our new protocol. Section III introduces system models. In Section IV, we prove the security of our protocol against an adversary attempting to become authenticated and access a secret session key. We then provide a description of other possible attacks that an adversary may attempt and argue security against such attacks.

II. SYSTEM MODELS

We consider two models in designing the proposed work as follows.

A. NETWORK MODEL AND ASSUMPTIONS

Fig. 1 depicts the network model for remote mutual authentication. The airspace includes multiple fly zones, and each fly zone may contain several drones in order to monitor a certain environment according to the network concept. A deployed drone in a certain fly zone collects targeted data from the surrounding environment and transmits it to a database server in a control room through a ground station. The database server stores sensitive information related to all involved entities and the airspace. It also stores the data collected by legitimate drones. An internal trusted user in the control room can access the control room's database server to monitor the IoD system. Quantum technologies are used to provide secure wired/wireless connectivity in the IoD environment. Private keys are pre-shared between the server and the involved entities (i.e., drones and ground station) through a secure private channel. Generally, a drone in a specific fly zone and a ground station must authenticate each other before establishing a secure session key to secure their future communications. This work assumes that the server, drones, and ground station are equipped with quantum capabilities to generate and measure quantum photons. We also assume that quantum channels are optimal, i.e., quantum channels are noiseless and lossless. Each drone has a GPS, inertial measurement units, and inertial navigation system to determine its present geographical location and mobility.

B. THREAT MODEL

Our threat model is based on the following principles:

- Drones are usually deployed in unattended or hostile environments. Thus, involved entities can use public channels and endpoint nodes are honest. An adversary has the ability to intercept the communication channels and can also forge or modify the exchanged message.
- It is possible that an adversary has unlimited computing power and can use it to apply powerful computational attacks. However, the server and ground stations are considered secure entities in this work. Thus, the adversary cannot extract useful information from the quantum channels that are information-theoretically-secure thanks to the principles of quantum physics.

III. THE PROPOSED WORK

In this paper, we consider the following model of drones, ground stations, and a central control room with a database server. The database server is able to communicate with each ground station and each pre-take off drone through secure private channels. Each ground station is also able to communicate with the drones within a known fly zone but cannot communicate with other ground stations. The drones are able to communicate with other drones within and beyond their current fly zone.

A. MUTUAL AUTHENTICATION BETWEEN THE DRONE AND GROUND STATIONS

Before a drone d takes off, the database server pre-shares a secret K_{dg} with both a drone (d) and a ground station (g) through a secure private channel (see also Fig. 2). Additionally, the database server preloads ID_g and FP_d into the d, and sends ID_d and FP_d to g through a secure private channel. Throughout this work, we assume that quantum channels are optimal, i.e., quantum channels are noiseless and lossless. Also, we assume that all involved entities agree on the four Bell states $\{|\phi_{00}\rangle, |\phi_{01}\rangle, |\phi_{10}\rangle, |\phi_{11}\rangle\}$, indicated in (1), and the four unitary operations $\{\sigma_{00}, \sigma_{01}, \sigma_{10}, \sigma_{11}\}$, indicated in (2), to represent the four two-bits classical information {00, 01, 10, 11}, respectively.

$$\begin{aligned}
|\phi_{00}\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} = (|{+}{+}\rangle + |{-}{-}\rangle)/\sqrt{2},\\
|\phi_{01}\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} = (|{+}{+}\rangle - |{-}{-}\rangle)/\sqrt{2},\\
|\phi_{10}\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} = (|{+}{-}\rangle + |{+}{-}\rangle)/\sqrt{2},\\
|\phi_{11}\rangle &= (|01\rangle - |10\rangle)/\sqrt{2} = (|{+}{-}\rangle - |{+}{-}\rangle)/\sqrt{2}. \quad (1)\\
\sigma_{00} &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},
\end{aligned}$$

TABLE 1. List of notifications.

Notations	Description
ID_d	The identity of a drone d, $ID_d \in \{0,1\}^{\frac{n}{2}}$, where n is even, and $n \geq 2$
ID_g	The identity of a ground station g, where $ID_g \in \{0,1\}^{\frac{n}{2}}$
FP_d	The flight plan of a drone d, where $FP_d \in \{0,1\}^{\frac{n}{2}}$
$\oplus$	The XOR operation
$\|\|$	The concatenation operation
$\{\sigma_{00}, \sigma_{01}, \sigma_{10}, \sigma_{11}\}$	The four unitary operations
$\{\|\phi_{00}\rangle, \|\phi_{01}\rangle, \|\phi_{01}\rangle, \|\phi_{11}\rangle\}$	The four Bell states
$h()$	One-way hash function
m	Number of registered drones
$K_{dg} = k_1 \| k_2$	A pre-shared key, where $k_1, k_2 \in \{0,1\}^{3n}$
r_d	A random key generated by d, where $r_d \in \{0,1\}^n$
K_g	A secret key generated by the ground station g, $K_g \in \{0,1\}^{\frac{n}{2}}$
$m_d = ID_d \| FP_d$	The secret message of a drone d, where $m_d \in \{0,1\}^n$
$m_g = ID_g \| K_g$	The secret message of a ground station g, where $m_g \in \{0,1\}^n$
$h(m_d)$	The hashing of m_d, where $h(m_d) \in \{0,1\}^n$
$h(m_g)$	The hashing of m_g, where $h(m_g) \in \{0,1\}^n$

$$\sigma_{01} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\sigma_{10} = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$
$$\sigma_{11} = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \quad (2)$$

The detailed steps of the proposed model are as follows:

Step 1: The drone d prepares the sequence $S_0 = h(ID_d \oplus ID_g)$, where ID_d and ID_g represent the destination identity of the drone d and the ground station g, respectively.

Step 2: The drone d randomly generates $3n$ Bell quantum states selected from the agreed four Bell states in (2). Then, d divides the $3n$ Bell states into four sequences: $S_1 = d_1, d_2, \ldots, d_n$, $S_2 = d_{n+1}, d_{n+2}, \ldots, d_{3n}$, $S_3 = g_1, g_2, \ldots, g_n$, and $S_4 = g_{n+1}, g_{n+2}, \ldots, g_{3n}$. Here, d_i and g_i $(i = 1, 2, \ldots, 3n)$ represent the first and the second photons of the *ith* Bell state, respectively.

Step 3: d creates an $n - bit$ random number (r_d) and gets $(r_d \oplus m_d) \| (h(r_d) \oplus h(m_d))$ by using the XOR operation and then the one-way hash function. Using the four unitary operations $\{\sigma_{00}, \sigma_{01}, \sigma_{10}, \sigma_{11}\}$, d encodes r_d and $(r_d \oplus m_d) \| (h(r_d) \oplus h(m_d))$ on S_3 and S_4, respectively, obtaining $S'_3 = e_r(S_3)$ and $S'_4 = e_{(r_d \oplus m_d) \| (h(r_d) \oplus h(m_d))} S_4$, where e represents the encoding process based on the four unitary operations. For example, when $n = 2$, if $r_d = 00$ d applies the unitary operation σ_{00} on S_3, and if $(r_d \oplus m_d) \| (h(r_d) \oplus h(m_d)) = 0111$, d applies the unitary operations σ_{01} and σ_{11} on S_4.

Step 4: d determines the initial basis for each qubit in the sequence $S'_3 \| S'_4$ based on the pre-shared key k_1 producing $S^{re}_{34} = b_{k1}(S'_3 \| S'_4)$ according to the following rule: if $k_{1,i} = 0$ the drone d selects the $Z - basis = \{|0\rangle, |1\rangle\}$ to transfer the corresponding qubit in the sequence $S'_3 \| S'_4$; otherwise, d selects the $X - basis = \{|+\rangle, |-\rangle\}$ to transfer the corresponding qubit in the sequence $S'_3 \| S'_4$, where b_{k1} represents the selected measurement bases based on k_1. Similarly, d determines the initial basis for each qubit in the sequence $S_1 \| S_2$ based on the pre-shared key k_2 producing $S_d = b_{k2}(S_1 \| S_2)$ according to the same rule, i.e., if $k_{2,i} = 0$ the drone d selects the $Z - basis$ to transfer the corresponding qubit in the sequence $S_1 \| S_2$; otherwise, the drone d selects the $X - basis$ to transfer the corresponding qubit in the sequence $S_1 \| S_2$, where b_{k2} represents the selected measurement bases based on k_2. Here, $k_1 = k_{1,1}, k_{1,2}, \ldots, k_{1,3n}$, $k_2 = k_{2,1}, k_{2,2}, \ldots, k_{2,3n}$ and $i = 1, 2, \ldots, 3n$.

Step 5: The drone d generates a sufficient number of decoy-qubits, where every decoy-qubit is randomly selected from the quantum states $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, or $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle\}$. Then, d randomly inserts these decoy-qubits into the sequences S_0, S^{re}_{34}, and S_d.

Step 6: Through a quantum channel, d sends the sequences S_0, S^{re}_{34} and S_d to the ground station g.

Step 7: Upon g receiving S_0, S^{re}_{34} and S_d, the drone d announces the positions of each decoy-qubits and its corresponding initial bases to g. Subsequently, based on the received information, g measures these decoy-qubits to compute the error value. If the error rate is lower than a preset value, d and g continue to the next process. Otherwise, they must terminate the protocol.

Step 8: Upon confirming that the quantum channel between d and g is secure, d sends the hashing value of the random key r_d, i.e., $h(r_d)$, to g through a quantum channel. d and g also employs the decoy-qubits technique used in *Step 5* and *Step 7* to ensure the security of transmitting $h(r_d)$.

Step 9: The ground station g checks whether $S_0 = h(ID_{dj} \oplus ID_g)$ is identical with its corresponding data (i.e., $S'_0 = h(ID_d \oplus ID_g)'$) or not. If $S_0 = S'_0$; g partially authenticates the identity of d and continues to the next step. Otherwise, g revokes d's request and ends the protocol.

Step 10: Upon confirming that S_0 is valid, g uses the pre-shared key (k_2) and the rules indicated in *Step 4* to measure $(S_1 \| S_2)$ getting $(S'_3 \| S'_4)$; note, if g has the identical pre-shared key (k_2), $(S'_1 \| S'_2)$ is identical to $(S_1 \| S_2)$. Also, g uses the pre-shared key k_1 and the rules indicated in Step 4 to measure $S^{re}_{34} = b_{k1}(S'_3 | S'_4)$ getting $(S''_3 \| S''_4)$; note, if g has the identical pre-shared key (k_1), $(S'_3 \| S'_4)$ is identical to $(S''_3 \| S''_4)$. Based on $(m_g \| h(m_g))$, g applies unitary operations selected from the set $\{\sigma_{00}, \sigma_{01}, \sigma_{10}, \sigma_{11}\}$ to S''_4 getting a new evolved sequence S'''_4.

Step 11: Using Bell measurement, g measures every corresponding pair (d_i and g_i) in $(S'_3 \| S'_4)$ and $(S''_3 \| S'''_4)$ getting the result $r'_d \| M$; note, r_d is identical to r'_d if the quantum channels are secure and g has the matching pre-shared key (K_{dg}). The ground station g then computes $(r'_d \| h(r'_d)) \oplus M \oplus (m_g \| h(m_g))$ getting a computation result representing $m'_d \| h(m_d)'$. After that, g performs two comparisons: 1) g computes $h(m'_d)$ and checks whether $h(m'_d)$ is identical to $h(m_d)'$or not; 2) g computes $h(r'_d)$ and checks whether $h(r'_d)$ is identical to $h(r_d)$ or not. If so, g knows with certainty that the message is genuine and fully authenticates the identity of d. Otherwise, g and d end the protocol and restart the protocol from the beginning.

Step 12: g sends M to d through a quantum channel and checks the security of transmission with d as in Steps 6 & 7.

Step 13: Upon confirming the secure transmission of M, g also sends $h(r_d \oplus K_g)$ to d through a quantum channel and checks the security of transmission with d as in Steps 6 & 7.

Step 14: d computes $(r_d \oplus h(r_d)) \oplus M \oplus (m_d \oplus h(m_d))$ getting the computation result $m'_g \| h(m_g)'$. Subsequently, d computes $h(m'_g)$ and checks whether $h(m'_g)$ is identical to $h(m_g)'$or not. If so, d deduces the shared secret key K'_g, where $m'_g = m_g = ID_g \| K'_g$. Finally, d checks whether $h(r_d \oplus K'_g)$ is identical to $h(r'_d \oplus K_g)$ or not. If so, d believes that K'_g is genuine and authenticates the identity of g. Otherwise, d and g end the protocol and restart the protocol from the beginning.

IV. SECURITY ANALYSIS AND PROOFS

In this section of the paper, we perform our security analysis of our proposed protocol beginning with its provable security against an adversary attempting to be authenticated and acquire the shared secret key. Following that, we provide heuristic arguments for security against additional quantum-based attacks.

A. THE PROVABLE SECURITY OF THE PROPOSED SCHEME

Definition 1: In [20], Wootters-Zurek introduced the *no-cloning theorem,* which proved that it is impossible to duplicate an unknown quantum state without knowing the polarization basis of that quantum state. Due to the no-cloning theorem, eavesdroppers cannot infer useful information from a quantum channel without being detected. Eavesdroppers must know all required information, e.g., the initial bases, to correctly measure the transmitted qubits from one legitimate user to another. Without knowing this information before transferring qubits, there is a high probability eavesdroppers will be caught when they try to intercept them.

Definition 2: Assume $MB \in \{Z - basis, X - basis\}$ is the qubit-creation algorithm [21]. An observer O has two polarization bases $Z - basis, X - basis$ and receives an arbitrary single qubit q. O can know q that was generated by the algorithm MB with probability ξ. Here, we can define the advantage $adv(O)$ of the observer O to predict the polarization bases as $adv(O) = \xi - (\frac{1}{2})$. So, we can say that the qubit-creation algorithm (MB) is secure against predicting the correct polarization basis when $adv(O)$ is close to Zero or negligible.

Theorem 1: Assume there is an eavesdropper E trying to authenticate himself and get the shared secret key (K_g) from g. The highest probability for the attacker (E) succeeding is equal to $\frac{1}{2^{2(7n+l)}}$, where l is the length of the decoy-photons and n is a security parameter.

Proof of Theorem 1: To prove *Theorem 1*, we first explain why other methods of attack for E cannot be successful; thus, the highest probability for E is to guess the information necessary to authenticate themselves and get the shared key. In the next session, we discuss various attacks in more detail. During communications between d and g, E is unable to obtain copies of the private messages sent between the two parties without a high probability of being detected. If E were to be detected, the two parties would restart the session with new random values to be generated. The only information E could obtain without the risk of being detected would be the announcement of the information of decoy photons, which does not cause leakage of any private information used to generate any of the messages in the protocol. Additionally, E is unable to intercept any messages sent between d and g without being detected with high probability. This prevents E from attempting to recover or inject information needed to be authenticated and/or get the shared key. Thus, E must attempt to guess the information necessary to be authenticated and get the shared key.

In *Step*1, d uses the XOR function to encrypt the ID_d and ID_g and uses a one-way hash function to produce S_0. Then, based on a randomly generated key r_d, the secret data $m_d = ID_d \| FP_d$, and the two shared sub-keys k_1 and k_2, d creates the sequences S^{re}_{34} and S_d and sends them to g in Step 6. To get K_g, E needs to 1) successfully guess the generated $3n$ Bell states; 2) get the transmitted sequences $\bar{S_0}$, $\bar{S^{re}_{34}}$, $\bar{S_d}$, and $h(\bar{r_d})$ that are sent by d correctly (i.e., S_0, S^{re}_{34}, S_d, and $h(r_d)$); 3) then successfully pass the eavesdropping check process in Steps 7 & 8. So, the probability (P) of getting K_g is as follows:

1) In *Step*1, d randomly generates $3n$ Bell states from the four states in (1). So, the probability ($P1$) of E correctly guessing the Bell states is as follows:

$$P1 = \frac{1}{4^{3n}} = \frac{1}{2^{6n}} \tag{3}$$

2) To successfully know S_0, S^{re}_{34}, S_d, and $h(r_d)$, E must correctly guess $\bar{r_d}$, $\bar{m_d}$, $\bar{k_1}$, and $\bar{k_2}$. So, the probability ($P2$) of guessing the correct sequences for E is as follows:

$$\begin{aligned} P2 &= Pr[r_d = \bar{r_d}]Pr[m_d = \bar{m_d}] \\ &\quad Pr[k_1 = \bar{k_1}]Pr[k_2 = \bar{k_2}] \\ &= \frac{1}{2^n} \times \frac{1}{2^n} \times \frac{1}{2^{3n}} \times \frac{1}{2^{3n}} \\ &= \frac{1}{2^{8n}}. \end{aligned} \tag{4}$$

3) In Steps 7 & 8, d and g employ l decoy photons to detect E. To successfully pass this check, E must correctly guess the measurement basis of the targeted photon and must also guess the initial basis to resend it to g. The probability of deciding the correct measurement basis (z-basis) is 50%, and the probability of deciding the initial basis is also 50%. Therefore, the probability ($P3$) of passing the eavesdropping check is as follows:

$$P3 = (\frac{1}{2} \times \frac{1}{2})^l = \frac{1}{2^{2l}} \tag{5}$$

Finally, the overall probability of getting K_g is as follows:

$$\begin{aligned} P &= P1 \times P2 \times P3 \\ &= \frac{1}{2^{6n}} \times \frac{1}{2^{8n}} \times \frac{1}{2^{2l}} \\ &= \frac{1}{2^{2(7n+l)}}. \end{aligned} \tag{6}$$

Drone (d)	Ground station (g)
Step 1: $S_0 = h(ID_d \oplus ID_g)$	
Step 2: $S_1 = \{d_1, d_2, \ldots, d_n\}$, $S_2 = \{d_{n+1}, d_{n+2}, \ldots, d_{3n}\}$, $S_3 = \{g_1, g_2, \ldots, g_n\}$, and $S_4 = \{g_{n+1}, g_{n+2}, \ldots, g_{3n}\}$.	
Step 3: Creates r_d; $(r_d \oplus m_d) \parallel (h(r_d) \oplus h(m_d))$, Compute $S_3' = e_r(S_3)$, $S_4' = e_{(r_d \oplus m_d) \parallel (h(r_d) \oplus h(m_d))} S_4$,	
Step 4: $S_{34}^{re} = b_{k1}(S_3' \parallel S_4')$, $S_d = b_{k2}(S_1 \parallel S_2)$.	
Step 5: Insert decoy-qubits into S_0, S_{34}^{re}, and S_d	
Step 6: $S_0, S_{34}^{re}, S_d.$ ⇢	
	Step 7: Detecting eavesdroppers
Step 8: $h(r_d)$ ⇢ & Detecting eavesdroppers	
	Step 9: Checks $h(ID_d \oplus ID_g) \equiv? h(ID_d \oplus ID_g)'$.
	Step 10: $(S_1' \parallel S_2') \leftarrow b_{k2}(S_d)$, $(S_3'' \parallel S_4'') \leftarrow b_{k1}(S_{34}^{re})$, $S_4''' \leftarrow e_{(m_g \parallel h(m_g))} S_4''$.
	Step 11: $r_d' \parallel M \leftarrow Bell\ measurement\ ((S_1' \parallel S_2'), (S_3'' \parallel S_4'''))$ Computes $m_d' \parallel h(m_d)' \leftarrow (r_d' \parallel h(r_d')) \oplus M \oplus \left(m_g \parallel h(m_g)\right)$. Checks $h(r_d) \equiv? h(r_d')$ & $h(m_d)' \equiv? h(m_d')$.
	Step 12: M ⇠ & Detecting eavesdroppers
	Step 13: $h(r_d' \oplus K_g)$ ⇠ & Detecting eavesdroppers
Step 14: Computes $m_g' \parallel h(m_g)' \leftarrow (r_d \oplus h(r_d)) \oplus M \oplus (m_d \oplus h(m_d))$, Checks $h(m_g)' \equiv? h(m_g')$, and gets m_g'. d deduces ID_g' & K_g' from m_g', where $m_g' = ID_g' \parallel K_g'$, If $ID_g \equiv ID_g'$; d authenticates the identity of g. Finally, d checks $h(r_d \oplus K_g') \equiv? h(r_d' \oplus K_g)$ to approve K_g.	

FIGURE 3. Steps of the proposed method. The dashed arrow represents a quantum channel.

B. FURTHER SECURITY DISCUSSIONS

We now discuss additional security notions that an adversary may try to exploit to gain information or access to private information.

1) INFORMATION LEAKAGE

Preventing information leakage is crucial for some quantum authentication protocols that enable attackers to deduce the secret message or extract useful information from the classical public channels. In this subsection, we show that the proposed protocol can prevent the information leakage issue. In the proposed protocol, the drone transfers S_0, S_{34}^{re}, and S_d to the ground station through a quantum channel. These sequences are encoded based on the $K_{dg} = k_1 \| k_2, m_d$, and r_d. As indicated in *Theorem 1*, any attackers who try to recover secret information will be caught with high probability. Moreover, the decoy-photon protocol [46] that is used for detecting eavesdroppers in *Step* 7 just uses the inserted decoy-photons to check the security of transmission and does not expose any other photons used for encoding secret data.

In addition, if legitimate users detect an intruder in any step through the protocol, they start the protocol from the beginning. d will select different random Bell states and generate a new r_d for encoding the secret information. Hence, the newly transmitted data will be completely different and will be carrying the same secret data as well as the pre-shared keys that can be reused safely. Thus, the proposed protocol is secure against information leakage.

2) INTERCEPT-AND-RESEND ATTACK

In Steps 6 & 8, before the drone d sends the quantum sequences (S_0, S_{34}^{re}, and S_d) to g, it must randomly insert decoy-qubits in the states $\{|0\rangle, |1\rangle, |+\rangle, \text{or } |-\rangle\}$ into the sequences S_0, S_{34}^{re} and S_d. d stores a recording of decoy-qubits positions and sends the quantum sequences to g and asks it to measure these qubits in the two bases $Z-basis, X-basis$ according to their initial bases. Then, d and g check the measurement results. Since E does not know the positions and the states of the decoy qubits, they will possibly measure them with incorrect bases. Therefore, E will be detected with probability $1-(\frac{3}{4})^l$, where l is the number of decoy-qubits. Hence, the probability is close to 1 when l is large enough (see also Fig. 4).

3) ENTANGLE-AND-MEASURE ATTACK

An attacker (E) may steal partial information about secret messages by using ancillary photons to entangle the qubits sent to the ground station and measuring the ancillary photons. E may use a unitary operation U_E to entangle a random qubit on the decoy-qubits and measure the random qubit in the $Z-basis$ or $X-basis$ to steal the secret. In the following, E performs a unitary operation U_E to entangle a qubit $|E\rangle$, on the decoy-qubits in the quantum states ($|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$).

$$\begin{aligned} U_E|0\rangle|E\rangle &= a_1|0\rangle|E_{00}\rangle + a_2|1\rangle|E_{01}\rangle, \\ U_E|1\rangle|E\rangle &= a_3|0\rangle|E_{10}\rangle + a_4|1\rangle|E_{11}\rangle, \end{aligned} \tag{7}$$

where $|a_1|^2 + |a_2|^2 = |a_3|^2 + |a_4|^2 = 1$. Since the decoy-qubits involved in the proposed protocol, the unitary operation U_E must meet the following conditions:

$$\begin{aligned} U_E|0\rangle|E\rangle &= a_1|0\rangle|E_{00}\rangle, \\ U_E|1\rangle|E\rangle &= a_4|1\rangle|E_{11}\rangle, \\ U_E|+\rangle|E\rangle &= \frac{1}{2}[|+\rangle(a_1|E_{00}\rangle + a_2|E_{01}\rangle \\ &\quad + a_3|E_{10}\rangle + a_4|E_{11}\rangle)], \\ U_E|-\rangle|E\rangle &= \frac{1}{2}[|-\rangle(a_1|E_{00}\rangle - a_2|E_{01}\rangle \\ &\quad - a_3|E_{10}\rangle + a_4|E_{11}\rangle)]. \end{aligned} \tag{8}$$

When the operation of E introduces no error, U_E must meet the following conditions:

$$\begin{aligned} a_1|E_{00}\rangle + a_2|E_{01}\rangle &= a_3|E_{10}\rangle + a_4|E_{11}\rangle, \\ a_1|E_{00}\rangle - a_2|E_{01}\rangle &= -a_3|E_{10}\rangle + a_4|E_{11}\rangle. \end{aligned} \tag{9}$$

We can easily obtain $a_1 + a_4 = 1$ and $a_2 + a_3 = 0$, and $|E_{00}\rangle = |E_{11}\rangle$. We have $U_E|0\rangle|E\rangle = a_1|0\rangle|E_{00}\rangle$, and $U_E|1\rangle|E\rangle = a_4|1\rangle|E_{11}\rangle$, which means that E introduces no errors only if $|E\rangle$ and the targeted states are product states. Therefore, E cannot perform the entangled-and-measure-attack without being caught.

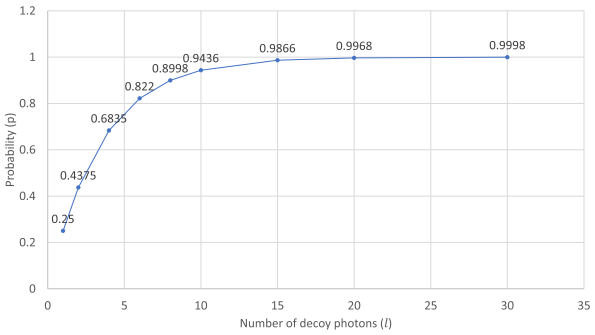

FIGURE 4. Probability of detecting intercept-and-resend attacks.

4) IMPERSONATION ATTACK

In the Case of Impersonating the Drone (d): If the attacker tries to impersonate the drone (d) by sending forged sequences S_{0a}, S_{34a}^{re} and S_{da} to the ground station, they will be detected in Step 9 because the attacker does not know ID_d and ID_d that are required to produce $h(ID_d \oplus ID_g)$.

In Case of Impersonating the Ground Station (g): If the attacker tries to impersonate g, they will send to d an invalid data (i.e., M in Step 12 and $h(r_d' \oplus k_g)$ in Step 13) because the attacker does not know the pre-shared key (K_{dg}) that was used to reorder the transmitted sequences. Hence, the attacker can be detected in Step 14 when d checks whether: 1) $h(m_g)'$ is identical to $h(m_g')$ or not; 2) $h(r_d \oplus K_g')$ is identical to $h(r_d' \oplus K_g)$ or not.

5) MODIFICATION ATTACK

In this attack, the attacker tries to modify the contents of the transmitted photons (in Step 2 or Step 6) to make the communicants obtain different secret messages without being caught. Then, in the first case, the attacker tries to modify S_0, S_{34}^{re} and S_d in Step 6 and send the modified quantum sequences, S_{0a}, S_{34a}^{re} and S_{da} to the ground station. But, the attacker may also modify the decoy-photons since they cannot distinguish between the decoy-photons and secret photons. Thus, the attacker could be detected in Steps 7 & 8 when d and g check the security of the quantum channel. Also, even if a single photon has been modified; the ground station will detect the modification when checking the hash values of $h(ID_{dj} \oplus ID_g)$ in Step 9. Also, the attacker may try to modify the sequences M transmitted in Step 9. However, both the drone and ground station perform a security check using the decoy-photon protocol as in Step 7. Thus, the attacker will be detected with high probability.

6) PERFECT FORWARD SECRECY

A proposed scheme supports perfect forward secrecy when an attacker cannot deduce the shared secret key using a compromised pre-shared secret key of any node. In this work, the final shared secret message/key of the session (K_g) is shared between d and g using a random number r_d, that is not

included in the pre-shared secret information K_{dg}, ID_g, ID_d and FP_d, or transmitted through the communication of the protocol. As such, the attacker cannot gain any information about r_d from the pre-shared secret information. Thus, the proposed scheme achieves the perfect forward secrecy.

V. CONCLUSION

In this work, we focused on the problem of authenticating the identity and the secret messages of the involved entities in the IoD environment. To address this problem, we proposed a quantum-based authenticated communication scheme for drones in Internet-of-Drones Deployment. A database server is used to pre-share private information with both the ground station and the legitimate drones through secure private channels. The drone uses its private information and a randomly generated key to encode some generated quantum states and then sends them through a quantum channel to the ground station. The randomly generated value by the drone is used to encode the transmitted secret which has not been transmitted through any of the communication channels, which guarantees the security of the secret messages. Both the drone and ground station check the security of the transmission based on the principles of quantum physics; they then authenticate their identity and the transmitted secret messages. The security proofs and analysis show that attackers can be detected with high probability. Through informal security discussions, the proposed protocol is shown to be secure against well-known attacks.

ACKNOWLEDGMENT

NXM's autonomous security technology enables devices, including connected vehicles, to communicate securely with each other and their surroundings without human intervention while leveraging data at the edge to provide business intelligence and insights. NXM ensures data privacy and integrity by using a novel blockchain-based architecture which enables rapid and regulatory-compliant data monetization. Toronto Metropolitan University is in the ''Dish With One Spoon Territory''. The Dish With One Spoon is a treaty between the Anishinaabe, Mississaugas, and Haudenosaunee that bound them to share the territory and protect the land. Subsequent Indigenous Nations and peoples, Europeans and all newcomers, have been invited into this treaty in the spirit of peace, friendship and respect. Wilfrid Laurier University is located on the traditional territory of the Neutral, Anishnawbe, and Haudenosaunee peoples. The authors thank them for allowing them to conduct research on their land.

REFERENCES

[1] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, ''Security and privacy for the Internet of Drones: Challenges and solutions,'' *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[2] P. Gope and B. Sikdar, ''An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones,'' *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020.

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

[4] 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.

[5] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, and J. Kelsey, ''Status report on the second round of the NIST post-quantum cryptography standardization process,'' U.S. Dept. Commerce, NIST, Gaithersburg, MD, USA, Tech. Rep. 8309, 2020.

[6] D. Bernstein and T. Lange, ''Post-quantum cryptography,'' *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[7] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, ''Drone-based entanglement distribution towards mobile quantum networks,'' *Nat. Sci. Rev.*, vol. 7, no. 5, pp. 921–928, May 2020.

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

[9] G. Lykou, D. Moustakas, and D. Gritzalis, ''Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies,'' *Sensors*, vol. 20, no. 12, p. 3537, Jun. 2020.

[10] M. Wazid, A. K. Das, and J.-H. Lee, ''Authentication protocols for the Internet of drones: Taxonomy, analysis and future directions,'' *J. Ambient Intell. Humanized Comput.*, pp. 1–10, Aug. 2018, doi: 10.1007/s12652-018-1006-x.

[11] J. Srinivas, A. K. Das, N. Kumar, and J. J. 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, Oct. 2019.

[12] T. Alladi, N. Naren, G. Bansal, V. Chamola, and M. Guizani, ''SecAuthUAV: A novel authentication scheme for UAV-base station scenario,'' *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15068–15077, Dec. 2020.

[13] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, ''Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles,'' *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

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

[15] T. Alladi, V. Chamola, and N. Kumar, ''PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks,'' *Comput. Commun.*, vol. 160, pp. 81–90, Jul. 2020.

[16] K. Shannon, E. Towe, and O. K. Tonguz, ''On the use of quantum entanglement in secure communications: A survey,'' 2020, *arXiv:2003.07907*.

[17] D. Zhu, X. Wang, and H. Zhu, ''Semi-quantum-honest key agreement scheme with three-particle entangled states in cross-realm setting,'' *Quantum Inf. Process.*, vol. 19, no. 10, pp. 1–18, Oct. 2020.

[18] H. Abulkasim, S. Hamad, K. El Bahnasy, and S. Z. Rida, ''Authenticated quantum secret sharing with quantum dialogue based on bell states,'' *Phys. Scripta*, vol. 91, no. 8, Aug. 2016, Art. no. 085101.

[19] H. Zhu, L. Wang, and Y. Zhang, ''An efficient quantum identity authentication key agreement protocol without entanglement,'' *Quantum Inf. Process.*, vol. 19, no. 10, pp. 1–14, Oct. 2020.

[20] W. K. Wootters and W. H. Zurek, ''A single quantum cannot be cloned,'' *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[21] T. Hwang, K. C. Lee, and C. M. Li, ''Provably secure three-party authenticated quantum key distribution protocols,'' *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 1, pp. 71–80, Jan. 2007.

[22] C. Pu, A. Wall, K.-K.-R. Choo, I. Ahmed, and S. Lim, ''A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment,'' *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9918–9933, Jun. 2022.

[23] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. Park, ''BlockCLAP: Blockchain-assisted certificateless key agreement protocol for Internet of vehicles in smart transportation,'' *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8092–8107, Aug. 2021.

[24] S. R. Chinthi-Reddy, S. Lim, G. S. Choi, J. Chae, and C. Pu, ''DarkSky: Privacy-preserving target tracking strategies using a flying drone,'' *Veh. Commun.*, vol. 35, Jun. 2022, Art. no. 100459.

[25] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, ''Amassing the security: An ECC-based authentication scheme for Internet of Drones,'' *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.

[26] S. Hussain, K. Mahmood, M. K. Khan, C.-M. Chen, B. A. Alzahrani, and S. A. Chaudhry, ''Designing secure and lightweight user access to drone for smart city surveillance,'' *Comput. Standards Interface*, vol. 80, Mar. 2022, Art. no. 103566.

[27] H. N. S. S. Jagarlapudi, S. Lim, J. Chae, G. S. Choi, and C. Pu, ''Drone helps privacy: Sky caching assisted k-anonymity in spatial querying,'' *IEEE Syst. J.*, early access, May 19, 2022, doi: 10.1109/JSYST.2022.3171211.

[28] S. U. Jan, I. A. Abbasi, and F. Algarni, "A key agreement scheme for IoD deployment civilian drone," *IEEE Access*, vol. 9, pp. 149311–149321, 2021.
[29] M. Masuduzzaman, A. Islam, K. Sadia, and S. Y. Shin, "UAV-based MEC-assisted automated traffic management scheme using blockchain," *Future Gener. Comput. Syst.*, vol. 134, pp. 256–270, Sep. 2022.
[30] C. Pu and L. Carpenter, "Psched: A priority-based service scheduling scheme for the Internet of Drones," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4230–4239, Sep. 2021.
[31] C. Pu and Y. Li, "Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN*, Jul. 2020, pp. 1–6.
[32] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1339–1353, Jan. 2022.
[33] C. Pu and P. Zhu, "Defending against flooding attacks in the Internet of Drones environment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.
[34] K. N. Qureshi, M. A. S. Sandila, I. T. Javed, T. Margaria, and L. Aslam, "Authentication scheme for unmanned aerial vehicles based Internet of vehicles networks," *Egyptian Informat. J.*, vol. 23, no. 1, pp. 83–93, Mar. 2022.
[35] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, "Anonymous mutual and batch authentication with location privacy of UAV in FANET," *Drones*, vol. 6, no. 1, p. 14, Jan. 2022.
[36] P. T. Selvi, T. S. Sri, M. N. Rao, B. S. S. V. R. Babu, K. V. Rao, and A. Srikanth, "Toward efficient security-based authentication for the Internet of Drones in defense wireless communication," *Soft Comput.*, vol. 26, no. 10, pp. 4905–4913, May 2022.
[37] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," *IEEE Internet Things J.*, early access, Jan. 12, 2022, doi: 10.1109/JIOT.2022.3142251.
[38] C. Pu, A. Wall, K.-K.-R. Choo, I. Ahmed, and S. Lim, "A lightweight and privacy-preserving mutual authentication and key agreement protocol for Internet of Drones environment," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9918–9933, Jun. 2022.
[39] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 94, pp. 124–134.
[40] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, and R. Barends, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.
[41] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 2020, *arXiv:2003.06557*.
[42] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, p. 441, Jul. 2000.
[43] (2020). *Commercial Unmanned Aerial Vehicle (UAV) Market Analysis*. [Online]. Available: https://www.businessinsider.com/commercial-uav-market-analysis
[44] (May 2022). *Federal Aviation Administration*. [Online]. Available: https://www.faa.gov/uas/
[45] L. Chen, "Report on post-quantum cryptography," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8105, 2016.
[46] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901.

HUSSEIN ABULKASIM (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science from South Valley University, in 2004, 2012, and 2016, respectively.

From 2006 to 2011, he was a Web Developer with the Center for Information and Communication Technology, South Valley University. From 2012 to 2014, he was with the College of Computer Sciences and Information Systems, Jazan University. From 2019 to 2021, he worked as a Postdoctoral Researcher with the Cybersecurity Research Laboratory, Toronto Metropolitan University. He is currently working as an Assistant Professor of computer science with the Department of Mathematics and Computer Science, New Valley University. His current research interests include quantum cryptography, cybersecurity, IoT security, and blockchain security.

BRIAN GONCALVES received the H.B.Sc. and M.Sc. degrees from McMaster University, Hamilton, ON, Canada, in 2016 and 2018, respectively. He is currently pursuing the Ph.D. degree with Toronto Metropolitan University, Toronto, ON. He is also a Research Assistant at the Cybersecurity Research Laboratory, Toronto Metropolitan University. His current research interests include agile cryptography for the IoT devices, provably secure quantum-resistant public key cryptography, and blockchain security.

ATEFEH MASHATAN received the B.Math. degree (Hons.) from Carleton University, in 2002, the M.Math. degree from the University of Waterloo, in 2003, and the Ph.D. degree in combinatorics and optimization from the University of Waterloo, in 2009. From 2009 to 2012, she was a Scientific Collaborator at the Security and Cryptography Laboratory, School of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL). From 2012 to 2016, she was a Senior Information Security Consultant in cryptography at the Canadian Imperial Bank of Commerce. Since 2016, she has held a faculty position at the Toronto Metropolitan University (formerly Ryerson University), where she is currently a Canada Research Chair and an Associate Professor at the Ted Rogers School of Information Technology Management. She is also the Founder and the Director of the Cybersecurity Research Laboratory. Her research interest includes development of novel cybersecurity designs based on emerging technologies. She investigates challenges and opportunities brought forward by these new technologies and how they change the threat landscape of cybersecurity.

Dr. Mashatan is a Certified Service Oriented Architect (SOA) with Hons. She holds a Certified Information Systems Security Professional (CISSP) Certification from the International Information Systems Security Certification Consortium (ISC2) and Enterprise Architecture.

SHOHINI GHOSE received the B.S. degree in physics and the B.A. degree in mathematics from Miami University, Oxford, OH, USA, in 1996, and the M.S. and Ph.D. degrees in physics from the University of New Mexico, in 1999 and 2003, respectively.

From 2003 to 2005, she was a Postdoctoral Research Fellow at the University of Calgary. Since 2005, she has held a faculty position at Wilfrid Laurier University, Waterloo, Canada. She is currently a Professor of physics and computer science, and the NSERC Chair for Women in Science and Engineering. She is also the Director of the Laurier Centre for Women in Science. She is the author of two books, and more than 60 articles, and has given over 200 invited talks about her work. Her research interest includes quantum information science. Her research team was the first to observe a connection between chaos theory and quantum entanglement.

Dr. Ghose is a TED Senior Fellow and a 2017 Inductee into the Royal Society of Canada's College of New Scholars, Artists and Scientists. She is a past President of the Canadian Association of Physicists and sits on the Scientific Advisory Board of the UNESCO International Basic Sciences Program. She is the first Canadian member of the Working Group on Women in Physics of the International Union of Pure and Applied Physics.