International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2390634

# Applications, Restrictions, and Evaluation of Quantum Cryptography for Secure Unmanned Aerial Vehicle Communication

**Tejas Saraf*[1], Darshan Deshmukh[2], Chaitrali Kadam[3]**

*[1]Department of Information Technology, Savitribai Phule Pune University, Pune, Maharashtra, India

[2,3]Department of Computer Science, Savitribai Phule Pune University, Pune, Maharashtra, India

ARTICLEINFO

**Article History:**

Accepted: 01 Dec 2023

Published: 16 Dec 2023

**Publication Issue**

Volume 9, Issue 6

November-December-2023

**Page Number**

232-246

ABSTRACT

Because of the abrupt increase in demand for security, researchers have developed immediate safety solutions that outperform state-of-the-art solutions. Data security was first sought for during the Spartan period. These days, efforts are being made to broaden this area of study by challenging the status quo and creating novel algorithms that outperform their weaker predecessors. Unmanned aerial vehicles, or UAVs, are widely used in a variety of industries, including agriculture, the military, healthcare, monitoring and surveillance, and many more, because of their svelte designs and adaptable mobility. In this post, we go over the significance of drone technology as well as its growth and demand. The study also discusses the current state of security concerns in real-time settings and how quantum cryptography outperforms conventional methods in protecting data. This inspires us to offer an overview of quantum cryptography's significance, function, and advantages in protecting UAV communications that go beyond 5G networks. Additionally, a unique layered architectural approach based on quantum cryptography is suggested to ensure excellent data security and effective transmission. A case study on the Internet of Military Things' implementation in the battlefield is also included in this presentation. The latency, security, and dependability of the suggested case study system are taken into account while assessing its performance.

Keywords : Unmanned Aerial Vehicle, Quantum Computing, Quantum Cryptography, Military, Blockchain, Security.

## INTRODUCTION

Drones, sometimes referred to as unmanned aerial vehicles (UAVs), were initially created for military use. UAVs were upgraded in the early 1900s during World War I. UAVs have a restricted operational range and are more like remote pilot control. Later on, the defense industry took notice of this attribute [1]. Subsequently, this technology was used in a wide range of real-time applications, including package delivery,

transportation, healthcare, and agriculture. In [2], the authors talked about the value of UAVs in the agriculture industry for a few particular uses, such sky-farming, precision farming, and irrigation system monitoring. UAV technology is viewed as a potential asset that might help in various sectors because to its wider application breadth.

Pathak et al. [3] emphasized the usage of UAVs in the gas and oil sectors, where they are used for long-distance

airborne site supervision and leak detection. UAVs are also used for work status monitoring and inspection at civil construction sites.Drones are utilized in the mining industry for 3D mine mapping and aerial photography. Drones are useful in this pandemic-affected environment for contactless healthcare delivery and safety [4].

UAVs can be utilized for specimen transport and lab monitoring in medical lab services. These days, UAVs are utilized across the supply chain for intelligent deliveries in logistics that are quick, efficient, and economical. The previously listed uses of UAVs have automated these industries' workflows in a way that saves money and time. UAVs are becoming more and more common and have left their imprint on the international scene. The current global market size evolution for UAVs is depicted in FIGURE 1.

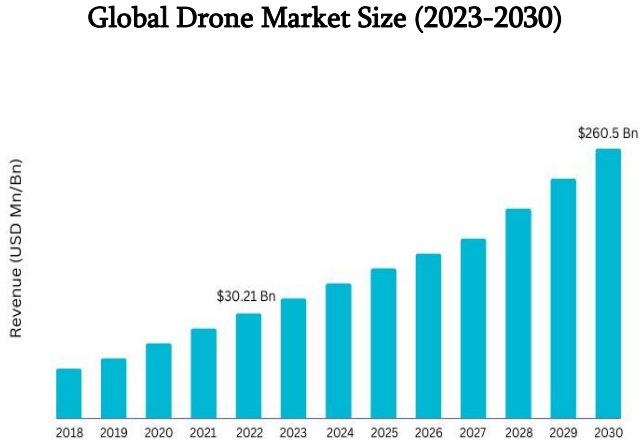


Figure 1: Market Size of drones across the globe.

There are $43.35 billion drones on the market worldwide as of 2023. The graph's upward-pointing bars indicate the level of demand for UAVs. In India, drones are creating a billion-dollar business. The data that UAVs carry forms the foundation of cyberattacks as their usage rises [5]. UAVs are therefore extremely vulnerable to hostile activity. It is imperative that this serious issue be resolved so that people can continue to enjoy this privilege.

The authors of [7] spoke about how attackers may easily capture unmanned aerial vehicles (UAVs) by interfering with the UAVs' communication hub and remote communication channels. A UAV using a wireless communication channel to communicate with other UAVs is very vulnerable to several types of security attacks, including man-in-the-middle, ADS-B, data alteration, denial of service, spying, and dispatch system assaults.

The communication and cryptography protocols that drone system architectures employ are the source of the previously described assaults against UAVs. Unmanned Aerial Vehicles (UAVs) employ many communication methods to achieve successful drone flight. UAVs have utilized a variety of worldwide wireless communication technologies, including 3G, 4G, 5G, and 6G. The 3G era began in early 2000, with communication delay ranging from 100 to 500 ms. With a latency of less than 10 ms, 4G, the 3G network's successor, became widely used in 2009. Then, in 2020, 5G networks with latency of less than 5 ms were introduced. These standards' progression shows a diminishing order of dependability.The network's latency, or round-trip time, is a crucial component of any UAV communication. A low latency network is necessary for many sensitive applications, including the military, intelligent transportation systems, and healthcare. Such applications are very appropriate for the 5G and 6G networks. A tiny bit of latency is acceptable in several other applications, such aerial photography, farming, site inspection, etc.

To protect UAV communication, a variety of cryptographic techniques have been employed. The methods for establishing a successful UAV communication with cryptography have been covered in the publications [8], [9]. The several methods used to provide safe communication between UAVs are displayed in FIGURE 2. For the purpose of securing UAV communication, symmetric and asymmetric key exchange techniques are mentioned. While just one key is needed for safe data sharing in symmetric key cryptography, two keys are utilized in asymmetric key cryptography to encrypt the information sent. It is also possible to achieve security in the communication layer by protecting the UAV's physical layer.

Many strategies have been put out to stop assaults on any specific communication channel. One use of machine learning techniques is the detection of malicious and invasive network activities. Machine learning techniques are used in learning-based intrusion detection systems. K-means clustering and SVM are two examples of algorithms that identify a pattern in the network to identify an intrusion.

The system's pre-defined rules are used in rule-based intrusion detection. These guidelines are encoded on the UAV's chip, and each one has a precise cut-off level that must be adhered to. These antiquated cryptography methods rely on laborious mathematical calculations. Because of this, these algorithms' complexity is exponential. As a result, encryption and decryption take longer.

The blockchain ecosystem is another example of a communication security idea. Security issues in the dissemination of vital information may be resolved by using a blockchain-based system in UAV communication. Blockchain fosters a decentralized atmosphere that promotes trust, transparency, and data security [9]. It maintains several copies of the same data on every network node, and data integrity is guaranteed by its consensus procedures. It stops bad things from happening in the communication environment. Even with the previously mentioned advantages, the blockchain has drawbacks of its own. In a blockchain system, mining a block takes time and requires a lot of energy and resources.The current approaches to protecting UAV communication are not suitable for some delicate uses of UAVs where time is constantly of the essence, including military operations when UAVs must make snap choices. Therefore, we require an improved method to enable UAV communication that is both quick and safe.

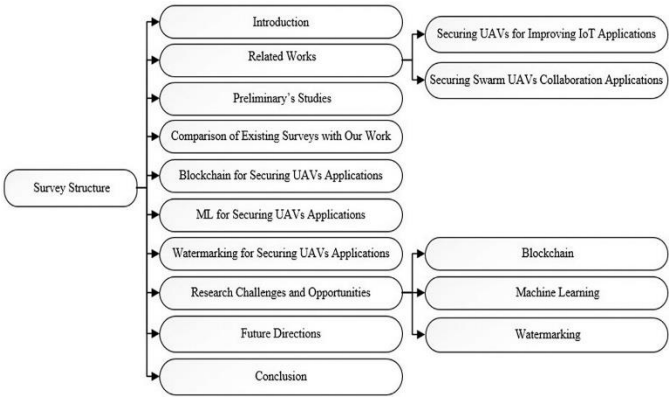


Figure 2 : Various Techniques to Secure UAV communications

When we wish to use UAV technology in sensitive sectors, the previously suggested solutions to the UAV security and networking problems are impractical. In order to address these problems, we provide in this work a revolutionary architecture built on quantum cryptography, which is far more dependable, safe, quick, and trustworthy than traditional encryption.

### 1.1. Scope of research

A blockchain-based architecture called BHEALTH has been developed by the authors in [10] as a way to secure UAV-based healthcare systems. Next, a blockchain-based Healthcare 4.0 architecture with UAV path planning was described by Aggarwal et al. [11]. The suggested architecture protects sensitive medical data from cyberattacks and enables secure data exchange. Next, a new cybersecurity paradigm for UAVs that would enable safe and secure data transport was proposed by Haque et al. [12]. a system that

guarantees the security and privacy of data. Using techniques from Steganography, the data was encrypted. Zhu et al. [13] provided an examination of the use of blockchain technology in the military. Next, in order to achieve high security and trust, Alladi et al. [14] conducted a detailed investigation on the usage of blockchain in UAV communication and submitted a review paper. Then, in order to defend against cyberattacks, Kumari et al. [15] presented a secure UAV architecture based on SDN and blockchain. The goal of the planned effort was to grow and protect the UAV network. Neji et al. [16] presented the results of a quantitative evaluation of crops conducted with unmanned aerial vehicles. Algorithms like secure hash algorithm (SHA), Rivest-Shamir-Adleman (RSA), and others are used for communication security. The comparison study of the current state-of-the-art methods for safe UAV communications is displayed in Table 1.

### 1.2. Motivation

Scholars and scientists now have a multitude of study options to devote their attention to as a result of the unexpected boom in the drone industry. Since the application areas for drone deployment have been determined, the popularity of these tiny IoT devices with low power consumption is growing over time. With their distinct qualities, potential drones can aid in automating and regulating the sector. The main ideas that drove this research project's continued development of a proof of concept are as follows:

- Drones are adaptable enough to gather vital information in remote areas, including monitoring chemical pipelines and comprehending volcanic eruptions. Up till now, UAV operability and safe communication have been the main concerns.
- Things might become worse in mission-critical applications like the military, healthcare, and intelligent transportation, where using drones to collect vital data is essential.
- Significant advancements and research in the field of power-constrained Internet of Things (IoT) devices expose them to security and privacy risks.
- It is imperative that communication be protected as much as possible right now.
- This study's attempt to find the optimum technology for UAV data transfer led them to create a revolutionary architecture that enables UAV data transmission to be more safeguarded.

### 1.3. Research Contribution

The paper's principal research contributions are as follows:

- To carefully examine the security flaws and weaknesses in the blockchain- and cryptography-based UAV communication technologies now in use.
- To address security concerns with the conventional UAV communication system, we suggest a quantum cryptography-based UAV communication system.
- To validate the proposed technology, we give a case study on its implementation in the battlefield. Furthermore, the case study's suggested application's performance is assessed by taking latency and throughput characteristics into account.

### 1.4. Organization

The remainder of the paper is set up as follows. The background information on UAVs and quantum cryptography is included in Section 2. The comprehensive explanation of the UAV and quantum cryptography integration is provided in Section 3. The suggested quantum cryptography-based UAV communication system is presented in Section 4. The case study of the suggested system in the context of a military application is covered in Section 5. The problems and unresolved concerns are covered in Section 6. The paper is finally concluded in Section 7.

| Author | Year | Objective | Blockchain? | Security Algorithm? | Application | Results | Pros | Cons |
|---|---|---|---|---|---|---|---|---|
| [17] | 2018 | secure and operate a network of semi-autonomous Unmanned Aerial Vehicles | yes | UAVNet cyber-security threats | semi-autonomous UAVs | PoG consensus algorithm uses partitioning of UAV groups | Every UAV networks capable for read transaction and autonomous information exchange | autonomous information exchange circuits - dynamic partitioning is required. |
| [12] | 2018 | Presented a cyber-security framework for securing UAV data communication | No | Steganography | UAVs | Ensures data security and confidentiality by tailoring traditional security solutions | Offers network security and flexibility | Too old technique used to achieve security |
| [18] | 2019 | Blockchain Technology for Networked Swarms of UAVs | yes | immutable ledger technology | Networked Swarms of UAVs | Developers will be able to design trustworthy UAV systems | Hyper-ledger widens the swarm UAV environment. | construct reliable UAV systems |
| [16] | 2019 | Communication technology for Unmanned Aerial Vehicles | no | RSA, AES, etc. | Agriculture | Zigbee is no longer the ideal contender for the BVLOS situation because of limited range. | The best technology that carries the communication between UAV and GCS. | The reconfigurable UAV can upgrade its communication technology in nominal and degraded settings. |
| [10] | 2020 | To secure UAV-based healthcare system using blockchain called BHEALTH | Yes | Classic algorithm | Healthcare | | Threat analysis and protection against threats | No motivation to reward and improve validator performance. |
| [13] | 2020 | Presented the role of blockchain technology in military application prospects | Yes | Blockchain | Military | It is a survey of the benefits of blockchain in military applications | Focused towards the military applications and security | High cost and processing required |
| [15] | 2020 | Presented a blockchain-based decentralized and secure architecture to mitigate cyber-attacks | Yes | Blockchain | UAV communication | SDN-based secure UAV network management | Considered network management along with security | No implementation |
| [19] | 2020 | Blockchain and UAV-assisted secure communication for military applications | yes | Blockchain | Military | Preventing cyber-attacks in internet of military things network | Offers security to the military network | Only focused on devices in proximity |
| [11] | 2021 | UAV Path Planning for Healthcare 4.0 | yes | blockchain-based | Healthcare | Architecture offers data transfer method and protecting sensitive healthcare information | The architecture provides a distributed platform for UAVs ensures security. | Storage capacity issue because of the large amount of real-time data in Gigabytes. |

Table 1: Analysis of various existing state-of-the-art techniques for secure UAV communications

## 2. BACKGROUND CONCEPTS

This section provides a quick overview of the essential principles related to blockchain technology, quantum cryptography, and UAVs and their applications.

### 2.1 Unmanned Aerial Vehical : Application and Security Prespective.

Unmanned aerial vehicles, or drones, have proliferated in the last several years. They are widely used for both

military and non-military purposes. The military UAV market is anticipated to grow to 26.11 billion USD by 2028 [20]. According to a number of studies, the usage of UAVs for non-military purposes may soon outpace that of UAVs for military purposes, hence removing the need for further wars. A UAV is a self-contained, remote-controlled vehicle.

One of two methods can be used to operate a UAV: (i) self-control or (ii) ground control channel (GCS). Recent years have seen a rise in research and development, which has enhanced the utilization of UAVs. Hackers and attackers may find UAVs to be an enticing target because they are common and safe targets. As technology advances, there are a few security solutions for communication between UAVs. Most of these concepts are still in the ideation phase or are only suggestions.

### A. Application scenarios of UAV's

This section identifies a number of unique situations in which UAVs can produce valuable data, and the same data can be utilized for further in-depth analysis and astute real-time decision-making. A overview of several real-time UAV application scenarios, including agricultural, healthcare, and volcano monitoring, is provided in Table 3.

### B. Security issues in UAV's

Typically, communication protocols like MAVLink, UranusLink, and UAVCAN are used to facilitate communication between UAVs and GCS [31]. Messages are sent using these protocols while a GCS is

communicating. It's possible that the majority of security procedures in place weren't meant for situations like this.

They either don't use resources efficiently or don't provide safety precautions while using these communication platforms. The most popular and commonly used method of this kind of communication between GCS and UAVs is MAVLink. But there isn't a secret method for protecting lightweight protocols. Security is a major concern while using any digital technology. Security is much more of a concern because of the unmanned nature of the UAV and distant wireless connection. The worried UAVs are more likely to lose their communication routes if attackers take over the flying cell base stations. Moreover, they could encounter serious interference issues while utilizing line-of-sight (LOS) connectivity [32].

Thus, when there is an open wireless communication channel, the security of UAV communication is crucial. UAVs are extremely susceptible to several types of cyberattacks, the goal of which is to jeopardize the data and infrastructure integrity and privacy. Attacks using keylogging and eavesdropping might jeopardize the privacy of data transmitted between UAVs and GCS. Unauthorized access to private information is thus caused by a lack of efficient communication and encryption standards.

Keyloggers are computer programs that capture data typed into a keyboard. They were first created to keep an eye on kids' activities, track sensitive information employees input, and find criminals [33]. Keyloggers are being used more and more to steal data. Either in UAVs, where the privacy of data sent between many UAVs is compromised, or in ATMs, where keyboard sniffers can recover pins. Keyloggers are invisible to antivirus software and can access your data remotely via the Internet. The process of listening to signals without authorization is known as eavesdropping, and it may be used to manage communications between many UAVs.

There is also a chance that deauthentication, GPS spoofing [34], and message injection attacks would alter data that is transferred and attempt to take over the UAV and its communication system, which might lead to causalities. Based on satellites, the GPS navigation system gives users information about the location and arrangement of traffic. In GPS spoofing, high-power devices send fake GPS signals, which cause nodes to accept the false signals in place of the real ones. It can result in UAV nodes being seized, crashing, or colliding with one another, which makes it risky. Pseudo-legitimate messages injected with a genuine message's structure are known as message injections. These signals deceive the aircraft or the computer at the ground station into believing it to be an actual plane.

## 2.2 Quantum Cryptography

The goal of quantum cryptography is to enable communication between two users via more secure channels than those provided by conventional cryptography. Cryptographic security was traditionally based on mathematics and considered the limitations of our current computing capacity. It was believed that breaking a cryptographic code would require factoring extraordinarily large numbers into two primes, usually longer than 100 digits. This task was thought to be unachievable in a reasonable amount of time (less than a million years), even if all of the computers in use today focused only on one such problem. Nonetheless, this does not exclude the future discovery of an algorithm that is sufficiently efficient to do factoring rapidly.

Rather than dispensing with conventional cryptography, quantum cryptography facilitates a more secure key exchange for encoding and decoding. Although quantum cryptography cannot transport

very big or quick amounts of data, it can transfer incredibly safe amounts of data. The secret key is sent using quantum coding to maximize speed, size, and security of the transfer; the data is encoded and sent using conventional techniques and algorithms. By ensuring that their key is as safe as current technology allows it to be, users may increase their level of anonymity while still exchanging data as fast as feasible.

| Applications | Objective | Roles of UAV technology |
|---|---|---|
| Smart healthcare [21] | Generate, monitor, and analysis patient's health data using smart wearable devices to understand their physiological conditions remotely | UAVs can be used to deliver medicines to critical patients and take immediate real-time actions in case of medical emergencies (in situations like pandemics) |
| Volcano monitoring [22] | The change in the Volcanic erupting areas needs real-time images and environmental data for preventive measures | UAVs are helpful in gathering real-time data of the nearby volcanic disasters for immediate decisions |
| Smart agriculture [2] | Surveillance of crops in the form of images or video feeds | UAVs can be used to strengthen smart agriculture and precision irrigation. It analyzes the real-time conditions of agricultural land and is also helpful in watering crops |
| Traffic monitoring [23] | Real-time traffic data monitoring and to analyze on a timely basis | UAVs can be used to control traffic and monitor those who disobey traffic rules |
| Social Distancing [24] | The distancing data between people across the desired region or place while monitoring | UAVs can be used to monitor the social distancing during the pandemic situations (COVID-19 let's say) |
| Forest inspection [25] | Real-time detection and monitoring of wildlife activities | UAVs can be used to monitor animals on the verge of extinction. Real-time notifications can be generated in case of urgency |
| Coastal engineering [26] | To acquire landscape data for monitoring the coastal shore activities | UAVs can be used herein to surveil the water behavior in coastal areas to assess the storm situations |
| Construction projects [27] | To monitor the work progress at high floored buildings | To capture the work done on daily basis for tracking progress by civil engineer can be done using UAVs, it can be deployed anywhere in the construction site especially in the risk prone high under construction buildings |
| Archaeology [28] | To survey the archaeological sites for historical insights | The mobility of drones allow them to travel anywhere for remote monitoring. This trait can be used for drone archaeology survey |
| Disaster management [29] | The pre and post disaster activities can be identified and communicated via drones | In an area hit by either an accident or natural calamity, people can be saved and found (in case of lost). The rapid damage assessment can also be performed using drones |
| Smart parking [30] | To study the parking lots using UAVs | The proper studying of huge parking lots without putting more cost into human labour, UAVs can be installed in the required parking area for better and fast parking facilities |

Table 2. Summary of selected real-time UAV application scenarios

### A) Quantum Key Distribution (QKD)

Through the use of quantum communication, this sophisticated quantum cryptography system creates a public key between two parties without disclosing the secret to a third party. If an outsider or listener tries to find out The quantum states being broadcast over a channel may be disturbed, revealing more about the key that Alice and Bob see being put up. The two parties in communication will be able to detect the intervention. They are commonly used to secure the connection in the conventional manner after they have already been created. One-time pads and other suitable cryptography can be utilized with the sent key, for instance [39].

It is feasible to conceptually illustrate the security of quantum key deployment by tracing the actions of eavesdroppers along the process, something that is not achievable with standard key distribution. Although certain basic presumptions are necessary, like the

validity of quantum physics and Alice and Bob's ability to trust one another, Eve shouldn't be allowed to pose as either Alice or Bob since it may lead to a man-in-the-middle assault.

### B) Mistrustful Quantum Cryptography

People that use distrusting cryptography don't trust each other very much. When Alice and Bob, the participants, provide their own private feedback while working to finish a survey, for instance. Conversely, Alice doesn't think highly of Bob, and Bob Has little trust in Alice. Therefore, when the calculation is completed, Alice must certify that Bob did not cheat, and Bob must confirm that Alice did not cheat in order to secure cryptographic work. Cryptographic techniques that are deemed untrustworthy encompass secure accounting and commitment systems, as well as money transfers and irreversible transactions.

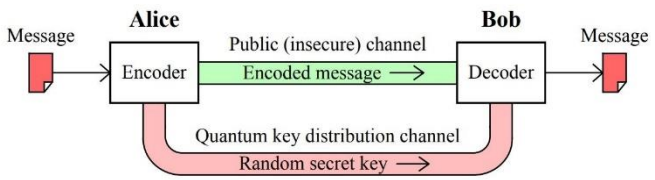


Figure 3: Quantum Cryptography

## 3. INTEGRATION OF UAV'S AND QUANTUM CRYPTOGRAPHY

UAVs are susceptible to a wide range of cyberattacks. such as open Wi-Fi, GPS jamming, spoofing, password theft, man-in-the-middle attacks, and denial of service (DoS) attacks. A strike against A drone might be possible in a number of ways. Brute-force attacks, password theft, and mathematical attacks are a few examples. By managing the communication between the two parties, MITM has access to confidential data without the user's awareness or consent. When a drone is GPS spoofing, its attacker transmits misleading signals regarding its flying route. The de-authentication program will impose a speed limit on the data transport. In light of this, quantum cryptography offers a unique defense against UAV cyberattacks methodology. To protect UAV communication, it makes use of features of quantum physics. The superposition and entanglement features of quantum computers allow them to perform transactions much faster than conventional computers while consuming a lot less energy.

### A) Quantum Entanglement

When actions are taken on one particle, they affect the other regardless of their distance from one another due to a property known as quantum entanglement, which is seen at the subatomic level. Entanglement in quantum mechanics is a characteristic of quantum mechanics. It is the basis for the interaction gap between quantum and conventional mechanics techniques. Physical properties that can be fully integrated in some circumstances include location, pressure, spin, and segmentation as determined by imprisoned particles.When one particle rotates clockwise along the first axis and zero spins generate reduced particles, the second particle's rotation measured along the same axis opposes the motion of the clock.

In the case of entangled particles, a measurement might have system-wide effects.
Nonetheless, research has shown that the polarization or spins of entangled particles at various places statistically violate Bell's inequalities, supporting the theory of quantum mechanics.
forecasts that seem contradictory. Results for one event that was clearly diverted to the area could not be ruled out, and for the second part of the term in earlier testing, the results are in. The distances between the components allowed for the creation of a link with the speed of light, although in one case, the distance may have been 10,000 times greater than the time between measurements. It has been demonstrated that electrons,

photons, neutrinos, buckyball molecules, and even small diamonds may all exhibit quantum entanglement. a topic that is now being researched and innovatively used in relationship, computer, and quantum radar applications.

### B) Quantum Superposition

The argument posits that legitimate quantum states can be joined (or "superposed") to create a new one appropriate quantum state. Each quantum state may be represented as the sum of two or more distinct unique states, which is similar to how waves work in conventional physics. The basic locations of quantum computing, 0 and 1, are superposed to form a quantum conceptual qubit state. In Dirac notation, which has been enhanced in classical logic by measurement, the quantum state is always 0. There is always truth to the first condition. A qubit, in contrast to traditional bits, may exist in two states simultaneously and can only exist in one of them: 0 or 1. Consequently, it is seldom 0.0-1.0 to determine if a qubit is 0 or 1. The same qubits are not always measured with the same outcome. Therefore, these two characteristics of quantum computing are superior to those of traditional cryptography. We are utilizing these qualities for that reason.

## 4. THE PROPOSED QUANTUM CRYPTOGRAPHY BASED SOLUTION

The suggested architecture for secure UAV communications is described in this section and is based on quantum cryptography. Based on quantum cryptography, we provide a unique layered architecture that renders UAV communication unbreakable.

The control layer, Internet layer, quantum security layer, physical/UAV layer, and monitoring layer make up the tiered suggested architecture seen in Figure 4. The next subsections include a thorough explanation of each layer.

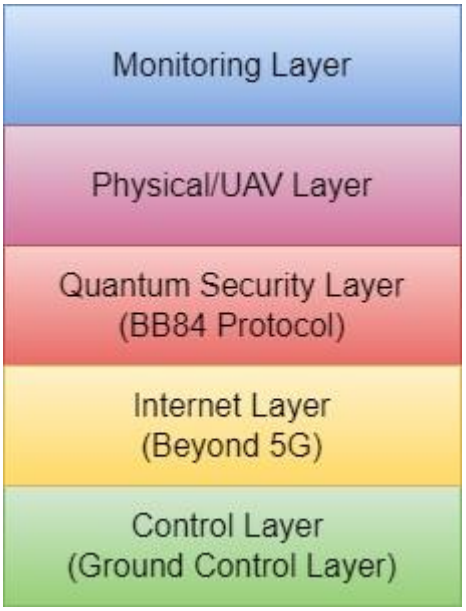


Figure 4: The proposed Layered Architecture

### A) Monitoring Layer

This layer's only goal is to collect data from all of the desired places. Locations such as L1 (city), L2 (water body), and L3 (forest region) are regarded as entities in this case L4 (the boundary between two regions) and several more locations such that {L1, L2, L3,..., LX } ∈ Lall. A vast quantity of data with a range of attributes, including variety, volume, and velocity, may be produced by any La ∈ Lall, where "a" is any arbitrary whole number. Here, data can be produced as an image or as a stream of pictures, or videos. The location-specific factors determine how frequently data is generated in every given La ∈ Lall. For instance, data unique to borders (L4) might produce data on events occurring over the border, but data generated by L3 can correspond to disasters occurring within the densely forested area that need surveillance.Thus, in accordance with the needs of the application, this layer is primarily in charge of creating

data from any given environment. All of the ground work, which would be extremely challenging for people to execute manually, is completed by the monitoring layer. To gather all the necessary data for additional analysis, the monitoring layer uses UAV cameras. The monitoring layer employs the below formulas for operation.

$$a, X > 0, a < X \quad (1)$$

$$Lall\ 6\ != NULL, LX \in Lall \quad (2)$$

Equation (1) places restrictions on the location entity. It turns any random location set Lall into a finite set. Conversely, Equation (2) ensures that there is at least one Lall place where monitoring has to be done. The monitoring layer cannot function in real time without these two equations. Next, the data produced by any Lx is sent to the topmost tier of the architectural stack.

B) Physical / UAV Layer

This layer contains the real UAVs that are physically stationed at any specific La lla Lall site in order to generate data. The lightweight hardware of UAVs makes them portable, affordable, and simple to operate. Because of this, it is a highly attractive option for on-site deployment for any type of location-based survey or information generation work. The UAVs on the surveillance area fly in three dimensions above the ground. This layer has the ability to create a chain of drones that communicate with one another. We also call this UAV swarming. When many drones coordinate with one another to complete a certain task, this is known as UAV swarming. We can use UAV layering to provide long-distance communication as each deployed UAV has a limited range. This allows us to teleport information to a remote area.

UAV swarm technology therefore enters the picture. By employing UAVs to relay communications, it is possible to conserve UAVs that are using limited energy and send messages over a longer distance than what is predetermined for UAVs. The group of UAVs stationed on the ground, designated as {U1, U2, U3...., Un }, create the transmission chain where necessary attention is needed in this particular situation. In this layer, the several potential cyberattacks covered in Section 2 seem important. For mission-specific applications, where data integrity and confidentiality are critical outcomes and UAVs are utilized, a cyberattack might result in significant losses. For these reasons, we utilize the quantum layer, which is the next layer in the architectural stack that is suggested. A system can attain a higher architectural security than classical security, which is vulnerable to cyber-invasions, by utilizing a variety of quantum mechanics features.

C) Quantum Layer

Secure data transfer takes place in this layer, producing data from the layers above. Here, we employ quantum cryptography as a benefit to shield Lall's sensitive data from the oversight layer. In order to enable secure communication, quantum cryptography makes use of physics principles. Using currently available QKD protocols, we safely exchange the private key in this case by utilizing a quantum key distribution paradigm. A protocol like that is the BB84 protocol, which is explained.

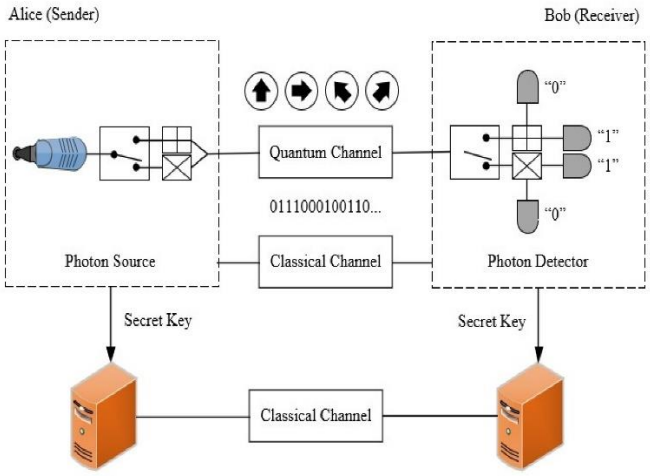


Figure 5: BB84 Protocol Structure

### 1) BB84 Protocol

The polarization of a single photon state is used in this protocol, known as BB84, to explain data transfer. The BB84 protocol flow is depicted in FIGURE 6. However, the two pairs of neighboring states that are useful for the protocol and the contrast-to-coded states seen in many fiber-based implementations are specified as BB84. An exchange of quantum states is possible through a quantum communication channel that links the transmitter (U1) and receiver (U2) of the two parties (two UAVs, the UAV, and the ground control station). In terms of photons, this usually refers to an open-plan setting or a fiber-optic link.

Conventional media, such as radio and the internet, can also be used for public communication. Assuming that an adversary can obstruct the quantum channel in any manner, the protocol is based on the assumption that the classical channel has to be confirmed. Protocol security is guaranteed by the use of encryption for data in non-orthogonal states. This inability to measure these states without destroying the original state is known as quantum uncertainty. The two states of the BB84 are at opposite angles to one another, and every pair is linked to another pair. It is used to describe two orthogonal states as the "basis."

Quantum transmission is the first step of BB84. The sender generates a random bit, either 0 or 1, and then chooses between the two bases—rectilinear or diagonal, as given by Eq. (3).

$$\text{Basis} = \{R, D\} \quad (3)$$

$$R = \{0, 90\} \quad (4)$$

$$D = \{45, 135\} \quad (5)$$

As seen in the following FIGURE 6, the value of the bits and the base controls the polarization of both photons.One is recorded as in the diagonal basis (x) of the 135 state, while zero is encoded as in the polarization of the drive's vertical position in a rectilinear basis (+). Eqs. (4) and (5) help you visualize this.

| Transmitting station bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| Transmitting station basis | + | + | X | + | X | X | X | + |
| Polarization | ↑ | → | ↖ | ↑ | ↖ | ↗ | ↗ | → |
| Receiving station basis | + | X | X | X | + | X | + | + |
| Receiving measurement | ↑ | ↗ | ↖ | ↗ | → | ↗ | → | → |
| Open channel discussion | | | | | | | | |
| Shared key | 0 | | 1 | | | 0 | | 1 |

Figure 6: BB84 protocol working with shared key.

U2 is unsure of the optimal basis for photon storage. He is thus limited to choosing an arbitrary foundation, such as measuring in diagonal or rectilinear space. The measurement result for every photon is obtained, together with a record of the measurement time. The center of the system's activity is U2, who is speaking to U1 on the public classical channel. The foundation for sending the bits is then made public by the sender.The accuracy of the basis used to measure the qubit states is then confirmed by the U2. In this way, the shared random key is produced between two parties when the wrong measurements are subsequently discarded by both sides. Now, a predefined subset of the bit strings that remain for the sender and recipient are compared. The receiver's observations will be biased if there is information available to a third party regarding the photons' polarization. Errors may also arise from other factors, such as environmental influences. Because the security of the key cannot be guaranteed, they reject the key and restart, maybe with a different quantum channel, when more than p bits disagree.

### D) Internet Layer

The data path between two areas is made via the internet layer. High speed (Sx = up to 2 GBits/s [50]) may be achieved with 5G, one of the newest mobile communication technologies. Here, the internet layer utilizes technologies beyond 5G networks. The

rationale behind utilizing beyond 5G is its capacity to offer scalability, huge spectrum (better than previous generations), low latency (≤ 1 millisecond), and pervasive connection. In keeping with virtualization, all of these characteristics facilitate rapid data flow in UAV swarming networks. Information transmission delays are intolerable for many sensitive applications, including those in the medical field, emergency management, military, etc.

### E) Control Layer

In the architectural stack, it is the last layer. It is made up of a centralized data and control center for unmanned aerial vehicles (UAVs) that stores and retrieves real-time data produced by the layers above.This layer includes a suitable cloud-based architecture, all storage facilities, and quantum computing equipment. On the servers, the Lall data will be kept. Real quantum computers at the control station can be used to execute the QKD between any arbitrarily chosen Ua and Ub where a,b ∈ Uall. Additionally, this layer is in charge of managing the ground-based UAV activities.

## 5. Conclusion

Since drone usage is becoming more and more commonplace worldwide, this study is primarily focused on enhancing the security of UAV communication. Because of its widespread use across many industries, data created and delivered by UAVs is valued highly. In the realm of cryptography today, the actual difficulties in managing data security and transport need to be solved. This research examined the several facets of ensuring secure UAV communication in mission-specific applications. Here, we take advantage of quantum cryptography's properties as well as those of networks that go beyond 5G to increase drone communication's ability to secure data transport and data itself. Specifically, we have incorporated BB84, a quantum cryptography method that is exceedingly secure and distinct from the current standard cryptography techniques.

The work that has been suggested above is especially useful in situations where there is a need for specialized infrastructure or when there is a need to complete a task quickly.. Future directions for this research will focus on implementing tamper-proof communication between the drones and resolving any potential obstacles.

In the area of drone communication, we want to create a simulated or actual layered architecture and then implement it using real quantum hardware (by quantum infrastructure providers as IBM qiskit, AWS-Braket, etc.). Quantum technology, which will surpass conventional methods of data security, is what cryptography has to look forward to.

## REFERENCES

[1]. Peter W. Shor. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society Press, 124–134. DOI: http://dx.doi.org/10.1109/SFCS.1994.365700

[2]. Frank Arute, et al 2019. Quantum supremacy using a programmable superconducting processor. Nature 574, 7779 (Oct. 2019), 505–510. DOI: http://dx.doi.org/10.1038/s41586-019-1666-5

[3]. Charles H. Bennett, Gilles Brassard et al. 1984. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175. 8. Retrieved from http://www.cs.ucsb.edu/chong/.

[4]. Masahide Sasaki. 2011. Tokyo QKD network and the evolution to secure photonic network. In Proceedings of the Conference on Laser Applications to Photonic Applications (CLEO'11), Vol. 1. OSA, Washington, D.C.,

JTuC1. DOI: http://dx.doi.org/10.1364/CLEOAT.2011.JTuC1

[5]. Park, Man-Kyu, et al. "A Study of Future Internet Testbed Construction using NetFGA/OpenFlow Switch on KOREN/KREONET." Journal of the Institute of Electronics Engineers of Korea TC 47.7 (2010): 109–117.

[6]. Ma, Xiongfeng, et al. "Quantum random number generation." npj Quantum Information 2.1 (2016): 1–9.

[7]. Krawczyk, Hugo, and Pasi Eronen. "Hmac-based extract-and- expand key derivation function (hkdf)." RFC 5869, May, 2010.

[8]. Chip Elliott, David Pearson, and Gregory Troxel. 2003. "Quantum cryptography in practice", In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03). 227. DOI: http://dx.doi.org/10.1145/863981.863982

[9]. Chip Elliott and H. Yeh. 2007. "DARPA Quantum Network Testbed. Technical Report", BBN Technologies Cambridge, New York, New York. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord.

[10]. Alexander Sergienko. 2005. "Quantum Communications and Cryptography." Vol. 2005. CRC Press. Retrieved from http://books.google.com /books?hl=en

[11]. Thomas Langer. 2013. "The Practical Application of Quantum Key Distribution". Ph.D. Thesis. University of Lausanne.

[12]. M. Peev, C. Pacher, R. Alleaume, et al. 2009. "The SECOQC quantum ´ key distribution network in Vienna", New J. Phys. 11, 7 (July 2009), 75001. DOI: http://dx.doi.org/10.1088/1367-2630/11/7/075001

[13]. A. R. Hall and C. J. Coyne, "The political economy of drones," Defence Peace Econ., vol. 25, no. 5, pp. 445–460, Sep. 2014.

[14]. P. K. R. Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T. R. Gadekallu, W. Z. Khan, and Q.-V. Pham, "Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges," IEEE Sensors J., vol. 21, no. 16, pp. 17608–17619, Aug. 2021.

[15]. N. Pathak, A. Mukherjee, and S. Misra, "AerialBlocks: Blockchainenabled UAV virtualization for industrial IoT," IEEE Internet Things Mag., vol. 4, no. 1, pp. 72–77, Mar. 2021.

[16]. A. E. Oigbochie, E. B. Odigie, and B. I. G. Adejumo, "Importance of drones in healthcare delivery amid a pandemic: Current and generation next application," Open J. Med. Res., vol. 2, no. 1, pp. 1–13, Apr. 2021.

[17]. S. Dahiya and M. Garg, "Unmanned aerial vehicles: Vulnerability to cyber attacks," in Proc. Int. Conf. Unmanned Aerial Syst. Geomatics. Springer, 2019, pp. 201–211.

[18]. Markets and Markets. (2021). Drone Services Market by Type (Platform Service, MRO, and Training & Simulation), Application, Industry, Solution (End-to-End, Point), and Region (North America, Europe, Asia Pacific, Middle East, and Row)-Global Forecast to 2026. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/drone-servicesmarket-80726041.html

[19]. E. Shaikh, N. Mohammad, and S. Muhammad, "Model checking based unmanned aerial vehicle (UAV) security analysis," in Proc. Int. Conf. Commun., Signal Process., Appl. (ICCSPA), Mar. 2021, pp. 1–6.

[20]. A. Shafique, A. Mehmood, and M. Elhadef, "Survey of security protocols and vulnerabilities in unmanned aerial vehicles," IEEE Access, vol. 9, pp. 46927–46948, 2021.

[21]. R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges,"

IET Commun., vol. 15, no. 10, pp. 1352–1367, 2021.

[22]. A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," Comput. Electr. Eng., vol. 84, Jun. 2020, Art. no. 106627.

[23]. S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchainbased UAV path planning for healthcare 4.0: Current challenges and the way ahead," IEEE Netw., vol. 35, no. 1, pp. 20–29, Jan. 2021.

[24]. M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," in Proc. Int. Conf. Secur. Privacy Commun. Syst. in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 239, 2018, pp. 113–122.

[25]. Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A study of blockchain technology development and military application prospects," J. Phys., Conf. Ser., vol. 1507, no. 5, Apr. 2020, Art. no. 052018.

[26]. T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Veh. Commun., vol. 23, Jun. 2020, Art. no. 100249.

[27]. A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," Comput. Commun., vol. 161, pp. 304–323, Aug. 2020.

[28]. N. Neji and T. Mostfa, "Communication technology for unmanned aerial vehicles: A qualitative assessment and application to precision agriculture," in Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS), Jun. 2019, pp. 848–855.

[29]. A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in Proc. IEEE Int. Conf. Service Oper. Logistics, Inform. (SOLI), Jul. 2018, pp. 32–37.

[30]. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM), Jun. 2019, pp. 1–7.

[31]. M. Golam, J.-M. Lee, and D.-S. Kim, "A UAV-assisted blockchain based secure device-to-device communication in Internet of Military Things," in Proc. Int. Conf. Inf. Commun. Technol. Converg., Oct. 2020, pp. 1896–1898.

[32]. Fortune Buiness Insights. (2021). The Global Military Drone Market. [Online]. Available: https://www.fortunebusinessinsights.com/militarydrone-market-102181

[33]. R. Gupta, A. Shukla, P. Mehta, P. Bhattacharya, S. Tanwar, S. Tyagi, and N. Kumar, "VAHAK: A blockchain-based outdoor delivery scheme using UAV for healthcare 4.0 services," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020, pp. 255–260.

[34]. T. Nakano, I. Kamiya, M. Tobita, J. Iwahashi, and H. Nakajima, "Landform monitoring in active volcano by UAV and SFM-MVS technique," Int. Arch. Photogramm., Remote Sens. Spatial Inf. Sci., vol. 40, no. 8, p. 71, 2014.

[35]. K. Kanistras, G. Martins, M. J. Rutherford, and K. P. Valavanis, "A survey of unmanned aerial vehicles (UAVs) for traffic monitoring," in Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS), May 2013, pp. 221–234.

[36]. Z. Shao, G. Cheng, J. Ma, Z. Wang, J. Wang, and D. Li, "Real-time and accurate UAV pedestrian detection for social distancing monitoring in COVID-19 pandemic," IEEE Trans. Multimedia, early access, Apr. 28, 2021, doi: 10.1109/TMM.2021.3075566.

[37]. M. Drauschke, J. Bartelsen, and P. Reidelstuerz, "Towards UAV-based forest monitoring," in

Proc. Workshop UAV-Based Remote Sens. Methods Monitor. Vegetation, Cologne, Germany, 2014, pp. 21–32.

[38]. C. D. Drummond, M. D. Harley, I. L. Turner, A. N. A. Matheen, and W. C. Glamore, "UAV applications to coastal engineering," in Proc. Australas. Coasts Ports Conf., 22nd Australas. Coastal Ocean Eng. Conf., 15th Australas. Port Harbour Conf., 2015, p. 267.

[39]. J. G. Martinez, M. Gheisari, and L. F. Alarcón, "UAV integration in current construction safety planning and monitoring processes: Case study of a high-rise building construction project in Chile," J. Manage. Eng., vol. 36, no. 3, May 2020, Art. no. 05020005.

[40]. N. G. Smith, L. Passone, S. Al-Said, M. Al-Farhan, and T. E. Levy, "Drones in archaeology: Integrated data capture, processing, and dissemination in the Al-Ula Valley, Saudi Arabia," Near Eastern Archaeol., vol. 77, no. 3, pp. 176–181, Sep. 2014.

[41]. M. Erdelj and E. Natalizio, "UAV-assisted disaster management: Applications and open issues," in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2016, pp. 1–5.

[42]. M. D'Aloia, M. Rizzi, R. Russo, M. Notarnicola, and L. Pellicani, "A marker-based image processing method for detecting available parking slots from UAVs," in Proc. Int. Conf. Image Anal. Process. Cham, Switzerland: Springer, 2015, pp. 275–281.

[43]. N. A. Khan, N. Z. Jhanjhi, S. N. Brohi, and A. Nayyar, "Emerging use of UAV's: Secure communication protocol issues and challenges," in Drones Smart-Cities. Amsterdam, The Netherlands: Elsevier, 2020, pp. 37–55.

[44]. G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescapè, "A SVM-based detection approach for GPS spoofing attacks to UAV," in Proc. 23rd Int. Conf. Autom. Comput. (ICAC), Sep. 2017, pp. 1–11.

[45]. K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks— An approach to the risk assessment," in Proc. 5th Int. Conf. Cyber Conflict (CYCON), Jun. 2013, pp. 1–23.

**Cite this article as :**

Tejas Saraf, Darshan Deshmukh, Chaitrali Kadam, "Applications, Restrictions, and Evaluation of Quantum Cryptography for Secure Unmanned Aerial Vehicle Communication", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.232-246, November-December-2023. Available at doi : https://doi.org/10.32628/CSEIT2390634
Journal URL : https://ijsrcseit.com/CSEIT2390634