IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study

VISHAKHA K RALEGANKAR[1], JAGRUTI BAGUL[1], BHAUMIKKUMAR THAKKAR[1], RAJESH GUPTA[1], (STUDENT MEMBER, IEEE), SUDEEP TANWAR[1], (SENIOR MEMBER, IEEE), GULSHAN SHARMA[2], I. E. DAVIDSON[2], (SENIOR MEMBER, IEEE),

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India (e-mails: 20mced18@nirmauni.ac.in, 20mcec02@nirmauni.ac.in, 20mcec17@nirmauni.ac.in, 18ftvphde31@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)
[2]2Department of Electrical Power Engineering, Durban University of Technology, Steve Biko Campus, Durban 4001, South Africa (e-mail: (gulshanS1@dut.ac.za, innocentD@dut.ac.za)

Corresponding author: Gulashan Sharma (e-mail: gulshanS1@dut.ac.za) and Sudeep Tanwar (e-mail: sudeep.tanwar@nirmauni.ac.in).

ABSTRACT The sudden demand rises in security made researchers come up with solutions that provide instantaneous safety better than the state of the art solutions. The quest for securing data began in the Spartan era. People are now looking to expand this field of research by attacking the existing paradigms and inventing new algorithms that prove to be better than their vulnerable counterparts. Unmanned aerial vehicles (UAVs) are very much prevailing due to their sleek design and flexible mobility in many sectors such as agriculture, army, healthcare, monitoring and surveillance, and many more. We discuss the growth and demand of drone technology along with its importance in this article. The paper also throws some light on the ongoing security issues in real-time scenarios and the role of quantum cryptography in securing the information over the traditional solutions. Motivated by this, we present a survey on quantum cryptography's importance, role, and benefits in securing UAV communications underlying beyond 5G networks. A novel quantum cryptography-based layered architectural solution is also proposed to achieve high data security and efficient transmission. This paper also present a case study on the battlefield application on the Internet of military things. The performance of the proposed case study system is evaluated by considering the latency, security, and reliability.

INDEX TERMS Unmanned aerial vehicle, quantum computing, quantum cryptography, military, blockchain.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs), popularly known as drones, were first developed for military use. During World War I in the early 1900s, UAVs were modernized. UAVs are more akin to remote pilot control, with a limited range of operation. This trait drew the attention of the military industry in later days [1]. Later, this technology found its place in many real-time applications such as agriculture, healthcare, transportation, package delivery, and many more. The authors in [2] discussed the importance of UAVs in the agricultural domain under some specific tasks such as precision farming, monitoring irrigation systems, and surveilling land from the sky (i.e., sky-farming). Due to its broader application in-scope, UAV technology is seen as a potential asset that could contribute in to many domains. Pathak *et al.* [3] highlighted the role of UAVs in the industries like gas and oil make use of UAVs for leakage detection and long-distance aerial supervision of the sites. UAVs also play a role in civil construction sites for work status monitoring and inspection. In mining, drones are used for aerial photography and 3D mine mapping. In this pandemic world, drones are beneficial in healthcare delivery (which is contactless) and ensure the safety [4]. UAVs can also be used in medical labs services for specimen delivery and lab monitoring. Even in the supply chain, UAVs are used these days for intelligent deliveries in logistics for fast, timely, and cost-effective deliveries. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

aforementioned applications of UAVs have automated the workflow of these industries in a cost-effective and time-saving fashion. UAVs are gaining a lot of popularity and has made their mark in the global market.

FIGURE 1 shows the current progression in the market size of UAVs across the world. The current market(2021) of drones across the world is 13.9 billion. The upward direction of the bars in the graph reveals the demand for UAVs. Drones are making billion dollars market in India. As increasing UAV consumption, the data it carries becomes the nucleus for cyberattacks [5]. As a result, UAVs are very much assailable towards malicious activities. This is a severe problem that needs to be addressed so that mankind can cherish this luxury.

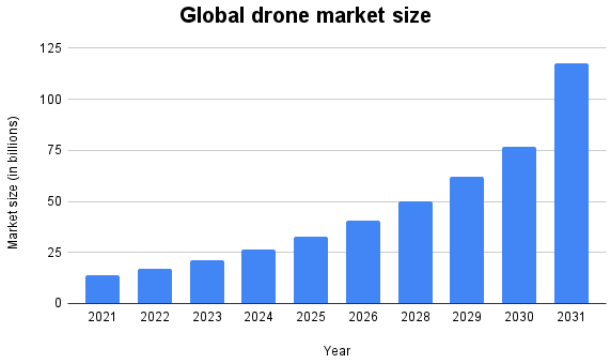

FIGURE 1: Market size of drones across the world [6]

Authors in [7] discussed how attackers find UAVs easy prey to catch by tampering their communication with the distant UAVs along with its communication center. A UAV communicating with other UAVs over a wireless communication channel is highly susceptible to various security attacks such as data modification, denial of service, snooping, dispatch system, ADS-B, man-in-the-middle, and WiFi attacks.

The aforementioned attacks on UAVs come from the type of communication and cryptographic protocols a drone system architecture uses. UAVs uses various communication protocols to accomplish the triumphant flight of a drone. Different global wireless communication standards have been used for UAVs viz 3G, 4G, 5G, and 6G. Early 2000 was the 3G era, whose communication latency was 100-500ms. The successor of 3G network is 4G, which gained its popularity in 2009 with a latency of less than 10ms. Then, 5G networks came in 2020 whose latency is less than 5ms. The reliability of these standards is in the decreasing order of their evolution. The important aspect of any UAV communication lies in the latency of the network, which is a round-trip time. Many sensitive applications such as military, intelligent transportation systems, and healthcare require a low latency network. The 5G and 6G networks are very much suitable for such applications. The are some other applications where a slight delay is acceptable in applications such as aerial photography, agriculture, site inspection etc.

Various cryptography protocols have been used to secure

Abbreviations	Explanation
UAV	Unnamed aerial vehicle
5G	Fifth-generation
GCS	Ground control channel
LOS	Line-of-sight
GPS	Global positioning system
QKD	Quantum key distribution
BQSM	Bounded and noisy-quantum-storage model
DES	Data encryption standard
RSA	Rivest–Shamir–Adleman
AES	Advanced encryption standard
ECC	Elliptic curve cryptography
SHA	Secure hash algorithm
AI	Artificial intelligence
ML	Machine learning
QSDC	Quantum secure direct communication
MITM	Man in the middle
DoS	Denial of service
SDN	Software-defined networking
PoG	Proof of game
BVLOS	Beyond visual line of sight
UCAV	Unmanned combat aerial vehicle
ATGM	Anti-tank guided missile
US	United state
IoMT	Internet of military things
RTTs	Round-trip times
PNS	Photon number splitting

TABLE 1: List of abbreviations.

UAV communication. The articles [8], [9] have discussed the cryptography techniques used to establish a successful UAV communication. FIGURE 2 shows various techniques that ensure secure communication between UAVs. It mentions symmetric and asymmetric key exchange protocols to secure UAV communication. In asymmetric key cryptography, two keys are used to encrypt the information passed, whereas, in symmetric key cryptography, only one key is used for secure data exchange. Security in the communication layer can also be accomplished by securing the physical layer of the UAV.

In order to prevent the attacks on any particular communication channel, various methods have been proposed. Machine learning algorithms, for example, can be used to detect harmful and intrusive network activity. Learning-based intrusion detection makes use of machine learning algorithms. These algorithms detect the intrusion by recognizing a pattern in the network, such as K-means clustering and SVM. Rule-based intrusion detection involves the rules which are pre-defined by the system. These rules are coded in the chip of the UAV and a cut-off threshold for each rule has to be followed strictly. These traditional cryptographic techniques are based on tiring mathematical computations. Hence, the complexity of these algorithms is exponential. The time taken for encryption and decryption thus increases.

Another such concept of securing the communication is the blockchain environment. Blockchain-based system in UAV communication can potentially be used to address security concerns in the distribution of critical information. Blockchain creates a decentralised environment that encour-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

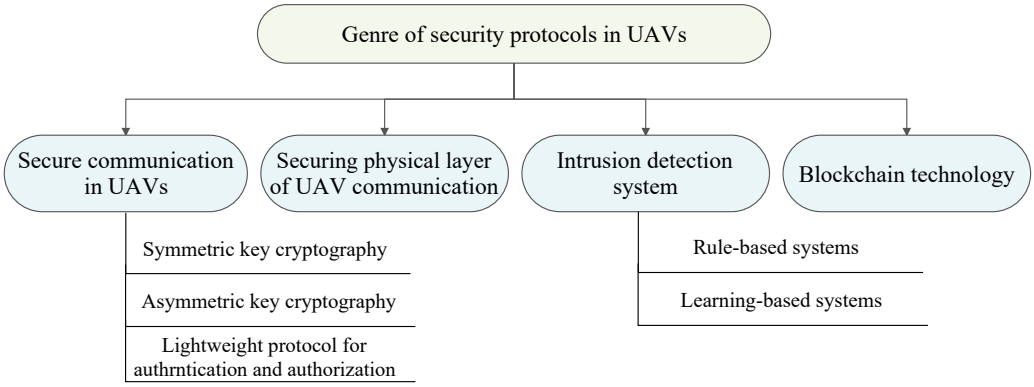

FIGURE 2: Various techniques to secure UAV communication [9] [8]

ages data security, transparency, and trust [9]. It keeps various copies of the same data on each node present in the network and its consensus protocols ensure data integrity. It prevents malicious activities from taking place in the communication environment. Despite the aforementioned benefits, the blockchain has its own lacunae. The time to mine a block in the blockchain environment is costly in terms of resource and energy consumption. These existing paradigms on securing UAV communication are not congenial to some of the fragile applications of UAV in which there is always curtailment of time, such as military operations where UAVs have to take immediate decisions. Thus we need a better solution to make UAV communication fast and secure at the same time.

The aforementioned solutions to solve the UAV security and networking are not feasible when we want to manoeuvre the UAV technology in sensitive domains. To solve these issues, in this study, we propose a novel architecture based on quantum cryptography, which is much faster, secure, trusted, and reliable than classical cryptography.

A. SCOPE OF THE SURVEY

Authors of [10] have proposed the BHEALTH, a blockchain-based architecture to secure UAV-based healthcare systems. Then, Aggarwal *et al.* [11] presented a blockchain-based Healthcare 4.0 architecture with UAV Path Planning. The proposed architecture provides a secure data transmission and safeguarding sensitive healthcare data from cyber-attacks. Then, Haque *et al.* [12] suggested a new cybersecurity paradigm for UAVs that would allow for safe and secure data transfer. A system that ensures data security and confidentiality. The data was encrypted using Steganography methods. Zhu *et al.* [13] presented the analysis of the implementation of blockchain in military domain. Then, Alladi *et al.* [14] presented a review article by thoroughly investigating the use of blockchain in UAV communication to achieve high security and trust. Then, kumari *et al.* [15] proposed a blockchain and SDN-based secure UAV architecture to combat cyber-attacks. The proposed work was designed to secure and scale the UAV network. The findings of a quantitative assessment of crops using UAVs were given by Neji *et al.* [16]. For communication security, algorithms such as Rivest–Shamir–Adleman (RSA), secure hash algorithm (SHA), and others are utilized. Table 2 shows the comparative analysis of various existing state-of-the-art techniques for secure UAV communications.

B. MOTIVATION

The sudden surge in the drone market has given birth to various research opportunities in which academicians and scientists can invest their time. The application areas where the drones can be deployed has been identified and hence these small power-constraint IoT devices are becoming popular with time. Potential drones can help automate and regulate the industry with their unique features. Following are the key points that motivated this research work to develop a proof of concept further:

- Drones are flexible enough to capture essential data at extreme locations, such as understanding volcano eruptions, surveillance of the chemical pipeline.
- The safe communication and operability of UAVs have been a primary concern till now.
- The scenario can go worst in the case of mission-critical applications such as military, healthcare and intelligent transportation where drones are deployed and data captures by them is of utmost importance.
- Major development and research in the domain of power-constraint IoT devices expose them to security and privacy issues.
- The need of the hour is to protect the communication in the best possible way.

The quest to use the best technology for UAVs data transfer made this study develop a novel architecture that can allow the UAV information transmission to be more safeguarded.

C. RESEARCH CONTRIBUTIONS

Following are the major research contributions of the paper:

- To scrutinize various security issues and vulnerabilities

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 2: Comparative analysis of various existing state-of-the-art techniques for secure UAV communications.

in the existing cryptographic and blockchain-based solutions for UAV communications.

- We propose a quantum cryptography-based UAV communication system to overcome security issues in the traditional UAV communication system.
- We present a case study on battlefield application to validate the proposed system. Also, the performance of the proposed application in the case study is evaluated by considering latency and throughput parameters.

D. ORGANIZATION

Rest of the paper is organized as follows. Section 2 discusses the background concepts of UAVs and quantum cryptography. Section 3 presents the detailed description on the integration of UAVs and quantum cryptography. Section 4 present the proposed quantum cryptography-based solution for UAV communication. Section 5 discusses the case study of the proposed system in the battlefield application. Section 6 discusses the open issues and challenges. Finally, Section 7 concludes the paper. Table 1 depicts the abbreviations and its explanation used in the paper.

II. BACKGROUND CONCEPTS

In this section, we briefly discuss various fundamental concepts of UAVs and its applications, quantum cryptography, and blockchain technology.

A. UNMANNED AERIAL VEHICLE: APPLICATION AND SECURITY PERSPECTIVE

UAVs also called drones, have grown significantly in recent years. They are widely used in various military and civilian applications. The UAV military market is expected to hit 26.11 billion USD by 2028 [20]. Numerous studies have revealed that shortly the consumption of UAVs for public purposes can be more than military purposes, ultimately overcoming the need for war in the future. A UAV is a self-contained or remote-controlled vehicle. Two different methods can control a UAV: (i) self-control or (ii) ground control channel (GCS). In recent years, the increase in research and development in UAVs has improved its usage functionalities. The widespread use and safety of UAVs have made them possible an attractive target for hackers and attackers. As the technology progresses, there exists a few security solutions for UAV communication. Most of these solutions are just suggestions or at the beginning of their development process.

1) Application Scenarios of UAVs

This section discovers various distinct scenarios where UAVs can be used to generate useful data and the same data can be used for further meaningful analysis and smart real-time decision-making process. Table 3 describes the summary of various real-time UAV application scenarios, such as healthcare, volcano monitoring, agriculture, etc.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

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 [23]	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 [24]	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 [25]	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 [26]	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 [27]	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 [28]	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 [29]	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 [30]	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 [31]	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 3: Summary of selected real-time UAV application scenarios.

2) Security Issues in UAVs

UAVs and GCS generally communicate through communication protocols, such as MAVLink, UranusLink, UAVCAN [32]. These protocols are used to transfer messages during communication from ground control stations (GCS). Most of the existing security protocols may not be intended for such an environment. Either they do not make good use of resources, or use these communication systems do not offer safety measures. Among these processes, MAVLink is a common and the most widely used for communication between GCS and UAVs. However, there is no hidden way to secure lightweight protocols. While working with any digital system, security is a significant issue. Because of the unmanned nature of the UAV and remote wireless communication, security is even more of a worry. If attackers acquire control of the flying cellular base stations, the concerned UAVs are more likely to lose their communication paths. They may also experience significant interference concerns while using line-of-sight (LOS) links [33].

So, the security of UAV communication is of prime concern in the presence of the open wireless communication channel. UAVs are highly vulnerable to various cyber-attacks, with the attacker's aim to compromise the integrity and privacy of the UAV infrastructure as well as data. Eavesdropping and keylogging attacks pose a hazard to data in communication between UAV and GCS, threatening the

information's privacy. Thus, the lack of effective communication and encryption standards, resulting in unauthorized access to private information. Keyloggers are the software that record information entered into a keyboard and was initially designed to monitor children's activities, track sensitive data entered by employees, and track criminals [34]. Keyloggers are increasingly being utilized to steal data. Either in ATMs, where keyboard sniffers can recover pins or in UAVs, where the privacy of information transferred between numerous UAVs is compromised. Antivirus software cannot identify keyloggers, and they can access your data remotely over the Internet. Eavesdropping, as the word means, is the act of listening to transmissions without permission and can be used to control communications between numerous UAVs.

Deauthentication, GPS spoofing [35], and message injection attacks also pose a risk of modifying exchanged data and trying to take control of the UAV and its communication mechanism, resulting in causalities. The GPS navigation system, based on satellites, provides users with information about traffic positioning and location. False GPS signals are sent by high-power devices in GPS spoofing, resulting in nodes accepting false GPS signals instead of authentic signals. It's dangerous because it can cause UAV nodes to be captured, crash, or collide with one another. Message injections are the injection of pseudo-legitimate messages with a structure similar to that of a legitimate message. These messages trick the aircraft or the ground station machine into thinking it is a real plane. Message deletion and modification can also be used to make fake messages appear to be authentic. Management packets are needed to authenticate UAV and GCS and create a communication link between them. These packets are modified by sending de-authentication frames to both, effectively disconnecting their communication and allowing the attacker to take control of either UAV or GCS.

B. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a technique of cryptographic operations that makes use of the quantum mechanical phenomenon. Quantum key distribution was a perfect quantum cryptography system that solved the exchange key problem with safe data. It is not allowed to copy data contained in quantum mode, for example. Quantum states can be altered if the entered data is attempted to read because of the function's reduced quality. This may be used to identify audio declines in quantum key distribution.

Gilles Brassard and Steven Wiesner [36] have worked on the creation of the quantum key distributions. Wiesner invented the theory of quantum conjugate coding, you Pareira College, Columbia University, New York, in the 1970s. The Society for developing the theory, i.e., IEEE rejected their extensive study on conjugate coding, but it was published in SIGACT Journal in 1983. Bennett and Brassard created the BB84 [37], a soon dynamic communication device in 1984 based on their earlier work. In a 1991 work by Arthur Eckert [38], for a more extensive description of quantum cryptography, David Deutsch's strategy to produce a safe key distribution combining quantum mechanics, non-locality, and Bell inequalities is based on the confusion, ships for free in the darkness.

The study of executing security tasks using concepts of quantum-mechanics is known as cryptography. Quantum cryptography [36], which uses quantum key distribution, is the most widely used because it gives an information-theoretically safe solution to the underlying exchange difficulties. Copying the label information of a quantum state, for example, is challenging. Quantum cryptography also offers the advantage of allowing you to do cryptographic tasks that are either stated or considered to be impossible to complete using merely regular communication. We discuss various quantum cryptographic concepts in this subsection structurally presented in FIGURE 3.

1) Quantum key distribution (QKD)

It is an advanced quantum cryptography scheme that establishes a public key between two parties by utilizing a quantum communication without a third party learning anything about the key. If the third party or eavesdropper attempts to learn more about the key that Alice and Bob observe being put up, the quantum states getting transmitted over a channel might be disrupted and the two parties communicating will be able to detect the intervention. After the keys were already established, they can frequently be used to secure the connection traditionally. For example, the transmitted key can be used for compatible cryptography (e.g. one-time pad) [40].

The security of quantum key deployment may be demonstrated conceptually with eavesdropper activities getting traced on the way, which is not possible with the traditional key distribution. While some fundamental assumptions are required, such as that quantum physics is valid and that Alice and Bob may trust one another, Eve should not be able to impersonate Alice or Bob since a man-in-the-middle attack is possible.

2) Mistrustful quantum cryptography

Participants of mistrustful cryptography have little trust in one another. When both participants, i.e., Alice and Bob, offer private inputs, for example, work to complete a survey. Alice, on either hand, has little faith in Bob, and Bob has little faith in Alice. As a result, securing cryptographic work necessitates Alice's confirmation that Bob did not cheat after the computation was performed, as well as Bob's confirmation that Alice did not cheat. Mistrustful cryptographic processes include commitment systems and secure accounting, including money procedures and unforgettable transfers.

- *Quantum coin flipping*: The process of quantum money laundering involves two persons who do not trust each other. The quantum channel was used to communicate and information was transmitted via quantum transmission. When compared to regular communication techniques, quantum communications have been proved to have significant security benefits [37]. In certain cases, a coin flip protocol looks like this:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

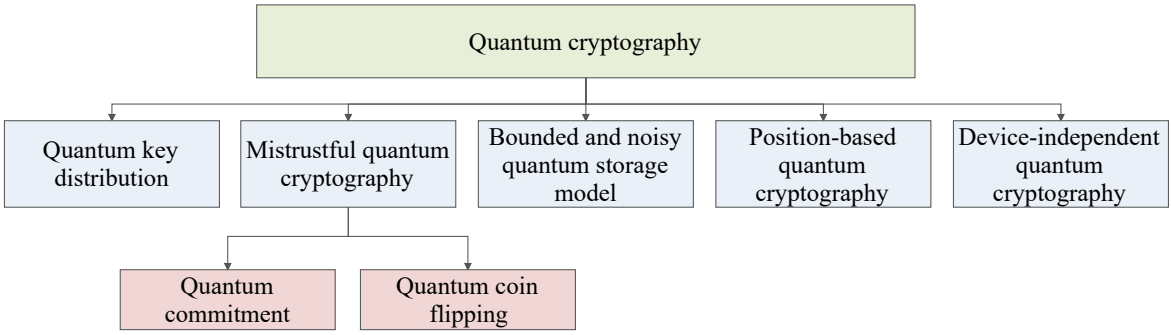

FIGURE 3: Diverse concepts of quantum cryptography [39].

1) Alice selects a base-like diagonal and creates a string of photons on that basis to deliver to Bob.
2) Bob picks a rectangular or diagonal base to evaluate each photon at random, noting the base he used for the recorded value.
3) Bob makes a public guess about the foundation on which Alice sent her qubits.
4) Alice reveals her choice of basis and sends Bob her original string.
5) Bob validates Alice's string by comparing it to his table.

- *Quantum commitment*: It is a paradigm where a user agrees on a value with the facility to reveal it later. These schemes were invented to make sure that the committed statement or values do not mutate over time viz a party committing on a value shall not change it one committed. Commitment mechanisms are frequently included in cryptographic agreements. Mayers has demonstrated that quantum commitment is impossible (without conditions) [41]. An unlimited computer attacker can defeat any quantum commitment scheme. On the other side, Kilian has demonstrated that anonymous transmission may be utilized to create practically any distributed computer that is safe and the findings of Crepeau and Kilian do not imply that the commitment and quantum channels can be used to produce a secure calculation of multiple groups [42].

3) Position-based quantum cryptography

Position-based quantum cryptography aims to focus entirely on the player's location for verification. Among opposing enemies, position verification using traditional protocols is impossible. In 2010, the concept of exploiting quantum effects in spatial validation was first published in the research literature. It is claimed that quantum processes can be unconditionally validated locally due to the combination of force and time. It has links to a Quantum Teleportation Protocol that is based on ports [39].

4) Device-independent quantum cryptography:

Device-independent quantum cryptography is necessary to assess the situations in which the devices are faulty or hostile while evaluating the security of such an agreement. Mayers and Yao proposed that quantum protocols be created by hiring quantum "self-testing" devices. Given the fact that the Bell test devices are "very noisy," some difficulties have been found to allow the device to be insecure and identity [43].

5) Bounded- and noisy-quantum-storage model (BQSM)

BQSM will be used to build commitment and unforgettable transfer procedures. The logical assumption is that the enemy's quantum memory is finite. In the final sound idea, the opponent can make use of quantum storage devices with issues of any size. In this sense, trusted groups should also utilize a lot of RAM. As a result, these techniques are insufficient until it comes to overcoming true memory obstacles. In the old situation, the same result may be reached by restricting the quantity of old (non-value) data that the opponent can maintain [39].

Based on the above discussed quantum cryptography facts and procedures, below mentioned are its potential benefits:

- It revolutionizes secure communication by relying on basic physical principles rather than mathematical methods or current computer technology to provide security.
- It's completely impenetrable.
- It's quite easy to use.
- It requires fewer resources to keep it running.
- In QKD, it is used to detect eavesdropping. This is useful because it means that data contained in the quantum state could be copied. If someone tries to decode such encoded data, the quantum state will change.
- Such cryptographic systems are always improving in terms of performance. As a result, it has been quickly adopted for encrypting the government's and companies' most valuable secrets.

C. ORIGIN AND TIMELINE OF CRYPTOGRAPHY

FIGURE 4 shows the timeline of cryptography techniques from spartan scytale to quantum. Cryptography was born

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

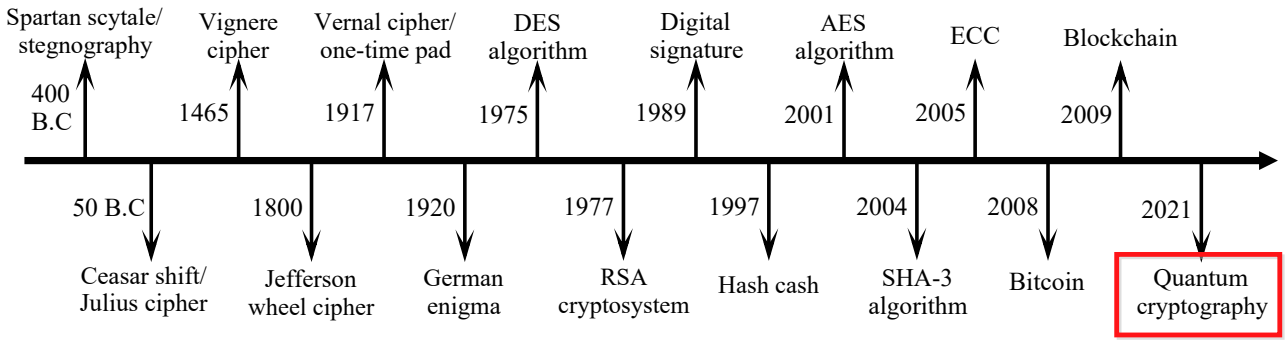

FIGURE 4: Timeline of quantum cryptography.

around 400 BC, and from then, it descended and evolved by making itself stronger following the human need for secure communications. The timeline started from steganography, whose major ambition was to mask the "message" into something that is not visible to the beholder. With the desire to procure higher security, the concept of ciphers came into the picture where the target message to be sent is encoded and then decoded at the other end (the receiver). The distinct ciphers were invented over a long time until the first generation of computers arrived. The involvement of computers induced a new branch of computer science known as cybersecurity. Various algorithms were proposed to secure the data that were implemented on the computers. These algorithms exploited the concepts of mathematics and provided a wide range of protection against the various types of interference in the field of communication. The early algorithms such as DES and AES were proved to be tamper-proof and they are still used in various applications where encryption is required. The realm of encryption was preceded by blockchain technology, where data security and trust became the significant pillars of its foundation. As per the timeline, the technology to execute message encipher has been improved and advanced by many researchers.

The progression of the computer hardware always lead to the improvisation of reliable and safe algorithms which can be implemented on them. One such advancement has left behind the traditional cryptography and blockchain technology. The development of quantum computers has opened opportunities for the researchers to make use of quantum physics rather than plain mathematics to accomplish the protect the data in case of sensitive application. The possible attacks on both traditional and blockchain based cryptography makes it ill-protected in the real world. Hence quantum cryptography comes into the scene which is way more secure than all the approaches proposed so far. The exploitation of the quantum properties such as entanglement and superpositon makes it a perfect candidate for the security purposes. The latest works in the field of quantum cryptography are still in its growing stage and can be seen as the future of the cryptography.

D. EDGE OVER TRADITIONAL CRYPTOGRAPHY

This section describes benefits of quantum cryptography over the traditional cryptography schemes.

1) Fundamental aspects

According to the rules, any traditional private channel can be seen anonymously without the sender or recipient knowing of such hearing. Traditional physics is the study of macroscopic associations and objects, such as radio transmissions. It allows the measurement of a single physical attribute of an item without impacting other qualities. The embedded physical symbols of an item or signal contain data entered as a cryptographic key. As a result, using traditional cryptography, passive monitoring is a serious possibility. All things are supposed to be directed by quantum theory, which is the foundation of quantum cryptography; however, its effects are usually negative. Single atoms or subatomic particles, such as small systems, can be seen. Traditional cryptography needs the usage of longer keys frequently. Power consumption doubles every 18 months, as does the cost of computing. Moore's law asserts that computing speed decreases with time [44].

2) Commercial aspects

In Commercial aspects, the organizations have sensitive data that they want to protect in the long run and that are attractive targets for hackers they use symmetric algorithms with long key lengths like AES and DES as possible and use perfect forward secrecy techniques to minimize the amount of data protected under each key when Diffie-Hellman is used to negotiate symmetric keys. For this reason, they should also consider making the switch to quantum-resistant algorithms as soon as possible because such algorithms are still in their infancy, it is best to start with hybrid algorithms.

There are commercial quantum computing solutions available. However, they are only suitable for point-to-point connections. On the other hand, older cryptography may be employed in software for a cheaper cost to clients. In addition, a cryptographic system based on classical cryptography can be applied to a small hardware object such as a smart card.

In contrast, the quantum cryptography that descends to that level requires much more research [44].

3) Application aspects

The digital signatures verify the digital data's authenticity and certify that a known sender has transmitted a message and is too without modification. Key generation, signing, and key verification are the three significant algorithms used by many applications, which are notoriously difficult to implement in quality control. As a result, quantum cryptography lacks numerous key capabilities, such as digital signatures and verified email [44].

4) Technological aspects

In the area of quantum communication (teleportation), or "fast transmission technology," Chinese scientists have accomplished the farthest distance. In partnership with China University of Technology and Tsinghua University, the Hefei National Laboratory conducted free space communication tests that successfully raised the communication distance to 9 miles [44]. Traditional cryptography, on the other hand, may be used to communicate over millions of kilometres. According to recent research, Toshiba has achieved a new recording rate for quantum key distribution, namely 1 Mbit / s on average [44]. On the other hand, traditional encryption is constrained by the amount of energy it consumes.

5) Other aspects

The communication channel is not compatible with traditional online writing because security is defined only by computer complexity. As a result, a secure connection is not required. Quantum cryptography connections, on the other hand, necessitate quantum routes such as fiber or air (wireless), and there is always the possibility of photon polarisation conversion owing to the Birefringence effect or negative consequences, such as changes in refractive index caused by damage [44]. Additionally, an old n-bit register can only hold one n-bit thread at a time. The quantum n-qbit register can maintain at any time the height of all 2pow(n) n-bit cables.

E. EDGE OVER BLOCKCHAIN TECHNOLOGY

Technology nowadays is based on other technologies. For example, the critical application in IoT like healthcare, transportation system, and surveillance is dependent on analysis results of Artificial Intelligence / Machine Learning (AI/ML) algorithms. Blockchain offers the participating members security and trust, but it still uses traditional cryptographic schemes such as digital signatures and Secure Hash Algorithm (SHA) 256 algorithms. This encourages almost all organizations to deploy it. According to Deloitte, more than 84% of businesses believe blockchain will provide superior security than traditional IT systems [45]. Due to conventional cryptographic algorithms, the data within the blockchain is still breachable and vulnerable to security attacks.

1) Blockchain security weakness:

Blockchain is based on the concept of interconnected nodes that can collaborate to make crucial decisions. It uses Secure Hash Algorithm (SHA)-256 and digital signature algorithms. These paradigms make use of one-way mathematical functions, which are difficult to trace back (or decrypt). These algorithms are inherently traditional and are vulnerable to various attacks. Blockchain proposes an architecture where immutability and multiple data copies are available. It allows the data to remain at its place for eternity. This makes the data availability 100% and hence more prone to attackers. Therefore, the blockchain-based protection to data over sensitive channels is therefore doubtful and this issue can be addressed by quantum cryptography.

With the use of Shor's algorithm, it is possible to break the public key cryptography. Quantum cryptography does not make use of traditional mathematical one-way functions for security purposes, but rather it is based on the concepts of quantum physics. The prepare and measure-based quantum encryption can be used to prevent and detect the intrusion of the attacker. The quantum states are responsible for storing the sensitive information, which when can be extracted right after the measurement of that particular quantum state and the state is destroyed upon measurement [21]. This ensures the integrity of the information and serves better than the blockchain ideology.

F. QUANTUM CRYPTOGRAPHY APPLICATIONS

This section briefly elucidates the applications in real world where quantum cryptography can be applied and utilized. Following is a list of few such applications:

1) *Quantum cryptography in UAV communication*: The sudden rise in drone usage due to its mobility benefit has opened a research area where drone to drone and drone to ground station communication has to be secured using cryptography. Traditional cryptography has its own limitations where they fail to secure communication. Quantum cryptography herein can deliver better. To cater the applications where data capture by a drone is an utmost important resource, quantum cryptography must be enforced.
2) *Quantum Cryptography in Cloud Computing*: As many users are using cloud platforms for data storage and processing for deploying large-scale applications. The purpose of new security for the cloud which uses the benefits of current protocols like Kerberos and the security advantages of Quantum Cryptography. Since everyday hackers are trying to hack powerful security like Apple and Dropbox for data transit in some of the applications occurs via a traditional network, storage on the same server for several users and malicious programmers have made a breakthrough, So cloud security has become a major concern [46].
3) *Quantum Cryptography in Voting Security*: Quantum cryptography was used to secure the Swiss Election

from hackers and unintentional data modification. The Federal Election in the State of Geneva takes place in October 2007, with communication from every data entry center—here, the paper votes are keyed into the computer. The data was protected by connecting to the state government's central data repository in Geneva through a quantum link. The fundamental goal, according to Geneva state chancellor Robert Hensler, is to make sure that the data is not compromised between entry and storage [47].

4) *Quantum cryptography in future E-commerce*: In future E-commerce, suppose the seller and customer and have finalized a deal over shopping mall under some constraints and sending messages to each other using quantum key distribution (QKD) and quantum secure direct communication (QSDC) theories in E-commerce applications. Using quantum cryptography protocol ignores the test qubits for simplification, but some testing methods are similar to BB84. Customers and sellers encode the messages by quantum techniques and send the encoded qubit to Online shopping malls. Then online shopping mall measures the entangled qubit pair and publishes the measurement outcomes. So, now a customer and seller have completed their agreement [48].
5) *Quantum cryptography in encrypted video call*: Wired published a blog post in January 2018 on a symposium hosted by Chinese and Australian researchers on quantum encrypted video-call. For the first time, the researchers are confident in their ability to conduct a teleconference. They tested quantum communications between satellites and ground stations for months before the teleconference. They launched a conference call, and it was determined that two people could talk for 75 minutes through a quantum link that is secure enough to interact [49].
6) *Quantum cryptography in smart card*: The most excellent approach to secure transactions and electronic communication is through overly complicated mathematics. Los Alamos National Laboratory created the QKarD and patented in 2010-11. This is groundbreaking technology. Instead of complex mathematical problems, the QKarD implements mechanical physics principles to encrypt the message/information. The applications of QKarD are telecommunications, banking, and financial transactions, wireless Internet, electronic voting facility, and vehicle access and information exchange for government/ defense. The benefits are Compact, Wireless, Portable, Low-cost development, Doesn't require dedicated fiber optics, and is invulnerable to both conventional and quantum computer attacks [50].

III. INTEGRATION OF UAVS AND QUANTUM CRYPTOGRAPHY

There are many cyber attacks possible in UAVs. i.e password theft, man in the middle (MITM), denial of service (DoS), GPS Jamming, Spoofing, open Wi-Fi, etc. An attack on the drone can be possible in diverse ways. A few instances are password theft, brute-force assaults, and mathematical attacks. MITM obtains access to sensitive information without the user's knowledge or agreement by controlling the communication between the two parties. In GPS spoofing, an attacker sends false messages about the drone's flight path. The data transfer at a high rate of speed will be limited by the de-authentication software. So, the novel solution for UAV cyber attacks can be achieved by the quantum cryptography technique. It uses quantum physics properties to secure UAV communication. Quantum computers are based on superposition and entanglement properties to process transactions at a higher speed than traditional computers and also use significantly less power.

A. QUANTUM ENTANGLEMENT

Quantum entanglement is a feature observed at the subatomic level in which entangled particles remain connected (in certain way) so that actions performed on one particle impact the other, regardless of their distance. Quantum entanglement is a property of quantum physics. It is the foundation of the interaction gap that exists from traditional and quantum mechanics methods. In some situations, physical characteristics like location, pressure, spin, and segmentation measured by trapped particles may be proven to be fully integrated. When zero spins produce reduced particles and one rotates clockwise in the first axis, the rotation of the second particle measured along the same axis opposes the clock's motion. When we're talking about entangled particles, a measurement might affect the entire system.

However, studies have discovered that the polarization or spins of entangled particles at different locations statistically violating Bell's inequalities, confirming quantum mechanics paradoxical predictions. It was impossible to exclude the findings in one episode that were transparently redirected to the region, and the results are in for the second portion of the term in previous tests. The pieces were far enough apart to draw a link with the speed of light, but there's a lot additionally one example, it might be worth 10,000 times longer than the interval between the measurements. Quantum entanglement was shown using photons, neutrinos, electrons, buckyball molecules, and even tiny diamonds. A current subject in research and innovation in applications to participate in a relationship, computing, and quantum radar.

B. QUANTUM SUPERPOSITION

The fundamental concept of quantum theory is Quantum Superposition. It argues that any two (or more) valid quantum states may be combined ("superposed") to generate another valid quantum state. It is similar to how waves function in conventional physics and that each quantum state may

be represented as the sum of two or more distinct unique states. It is a quantum conceptual qubit state corresponding to a superposition of 0 and 1, the fundamental positions in quantum computation. The quantum state is always 0 in Dirac notation, which has been improved in classical logic by measurement. The first condition is true all of the time. Unlike conventional bits, a qubit may be in both modes simultaneously and can only be in one of the states: 0 or 1. As a result, detecting whether a qubit is 0 or 1 is rarely 0.0-1.0, and measurements on the identical qubits do not always provide the same result. Hence, these two properties or features of Quantum Computing are better than classical cryptography. That's why we are using these properties.

IV. THE PROPOSED QUANTUM CRYPTOGRAPHY-BASED SOLUTION

This section describes the proposed quantum cryptography-based architecture to secure UAV communications. We propose a novel structured layer architecture that makes the UAV communication indestructible based on quantum cryptography. In FIGURE 5, we present all the layers presented in our architecture.

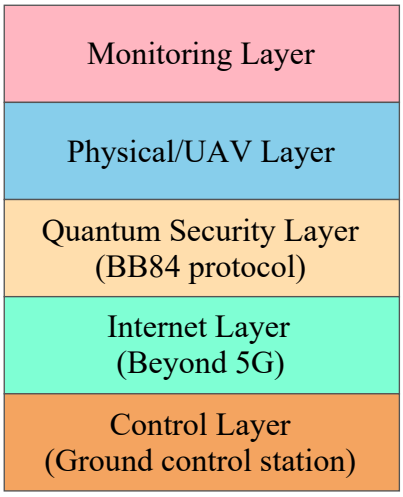

FIGURE 5: The proposed layered architecture

A. MONITORING LAYER

This layer solely focus on capturing the data from various desired locations. Here the locations are considered as entities for example L_1 (City), L_2 (Water body), L_3 (Forest area), L_4 (border between two areas) and many more s.t. $\{L_1,L_2,L_3,...,L_X\} \in L_{all}$. Any $L_a \in L_{all}$, where 'a' is any arbitrary whole number is capable of producing a huge amount of data which can possess various properties such as variety, volume, and velocity. The data generated here can be image or stream of images (i.e., videos). The frequency with which the data is generated in any location $L_a \in L_{all}$ totally depends on the specific location. For example, a data which is borderline specific (L_4) can generate the data containing the happenings across the borderline, L_3 can generate data in line with the occurrences of any disaster happening across the dense forest area in which the monitoring is required .Hence, this layer is responsible mainly for data generation from any given environment, as per the application requirement. The monitoring layer performs all the ground work which is very much difficult if performed manually by humans. Monitoring layer make use of a UAV cameras to capture all the relevant data for further analysis. The monitoring layer works with the following equations.

$$a, X > 0, a < X \tag{1}$$

$$L_{all} \neq NULL, L_X \in L_{all} \tag{2}$$

Equation (1) puts a constraint on the location entity. It makes any arbitrary location set L_{all} a finite set. Whereas eq(2) makes sure that there exist at least one location from L_{all} on which monitoring must be performed. These two equations are necessary for the working of monitoring layer in real time. The data generated from any L_x is then passed on to the upper layer of the architecture stack.

B. UAV LAYER:

This layer has the actual UAVs which are physically deployed on any particular location $L_a \in L_{all}$ for data generation. UAV has a light weight hardware which makes it mobile and a low cost device easy to use. This makes it location friendly and a very much desirable candidate for deploying it on ground level for any kind of location based survey or information generating tasks. The UAVs fly in the 3D space above the ground on the monitoring area. This layer is capable of producing a chain of UAVs interacting with each other. This is also known as UAV swarming. The swarming of UAVs is a process of multiple drones working in sync with each other to accomplish a particular piece of work. Since every UAV deployed is range specific therefore in order to teleport the information at the distant location we can make UAV layer to make a long distance communication.

Hence UAV swarm technology comes into the picture, The relaying of messages using UAVs can be performed in order to save UAVs running on limited energy and transmit message in a range greater than the pre-defined UAV range. $\{U_1,U_2,U_3....,U_n\}$ are the set of UAVs deployed in on ground which forms the chain of transmission alongside where needs to be taken care in this case. The various possible cyber-attacks discussed in section 2 appear significant in this layer. This is an open issue which needs to be addressed. The cyber-attack would cost a plenty of loss for mission specific since the data integrity and confidentiality are the important outlooks. which make use of UAVs. For these reasons, we make use of the next layer proposed in the architecture stack, i.e., quantum layer. Various properties of quantum mechanics can be exploited so that a system can achieve a better architectural security than the classical security which is prone to cyber-invasions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

C. QUANTUM LAYER

In this layer, the data produced by the above layers is transferred securely. Here, we make use of quantum cryptography as an amenity to protect the sensitive information present in L_{all} from the monitoring layer. The quantum cryptography exploits the concepts of physics in order to provide secure transmission. We make use of a quantum key distribution paradigm here to exchange the private key securely using existing QKD protocols. One such protocol is described here (i.e, BB84 protocol).

1) Background Concepts for BB84

- BB84 is a key exchange protocol which can generates a random shared private key between two parties (let's say two UAVs D_1 and D_2).
- BB84 protocol make use of classical communication channel for the authentication of D_1 and D_2.
- BB84 is a measure and prepare algorithm. In which we measure the state of the quantum bit (qubit) to get information present in it.
- BB84 make use of two different channels (quantum and classical), both channels can be implemented using the free space wireless communication.

2) BB84 Protocol

This protocol is termed BB84 which explains the transmission of data using the polarization of a single photon state. FIGURE 6 shows the flow of BB84 protocol. However, BB84 is defined as the two pairs of nearby states that can be utilized for the protocol and the contrast-to-coded states that are utilized in many fiber-based implementations. A quantum communication channel that connects the two parties (two UAVs, UAV and the ground control station) sender (D_1) to the receiver (D_2), allowing quantum states to be exchanged. When it comes to photons, this generally involves a fiber-optic connection or an open-plan environment. They can also communicate with the general public through traditional media like radio or the Internet. The protocol is built on the idea that an adversary can interfere with the quantum channel in any way, but the classical channel must be verified. Encryption of data in non-orthogonal states is used to ensure protocol security. Quantum uncertainty denotes the difficulty to measure these states without destroying the initial state. Each pair in the BB84 is connected to a different pair, and the two states are at various angles with one another. The term "basis" refers to a pair of orthogonal states.

In BB84, the initial phase of quantum transmission. The sender produces a random bit, either 0 or 1, and then selects one of two basis in this case: rectilinear, or diagonal can be defined in Eq. (3).

$$Basis = \{R, D\} \tag{3}$$

$$R = \{0, 90\} \tag{4}$$

$$D = \{45, 135\} \tag{5}$$

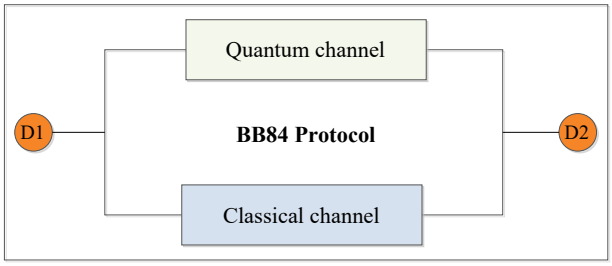

FIGURE 6: BB84 protocol structure.

The value of the bits and the base determines the polarization of both the photons, as indicated in the FIGURE 7 below.'0' is encoded as in polarization of the vertical position of the drive in a rectilinear basis (+), 1 is encoded as in diagonal basis (x) of 135 state. This can be visualized by Eqs. (4) and (5). Alice uses a quantum channel to send a single photon in the state specified to Receiver. The procedure is repeated from the random bit stage, with Sender storing the state, basis, and time of each photon delivered. Quantum physics (especially quantum indeterminacy) can discriminate between the four distinct polarization states since they are not all orthogonal. The only measurement that may be made is between any two orthogonal states (an orthonormal basis). Measuring on a rectilinear basis, for example, gives a horizontal or vertical result. This measures the proper state if the photon was generated as horizontal or vertical (rectilinear eigenstates). Still, if it was generated as 45° or 135° (diagonal eigenstates), the rectilinear measurement gives horizontally or vertically at randomness. Moreover, the photon is polarised in the state where it was measured (horizontal or vertical) after this measurement, and all information about its initial polarization is lost. Figure 7 shows the detailed working of BB84 algorithm.

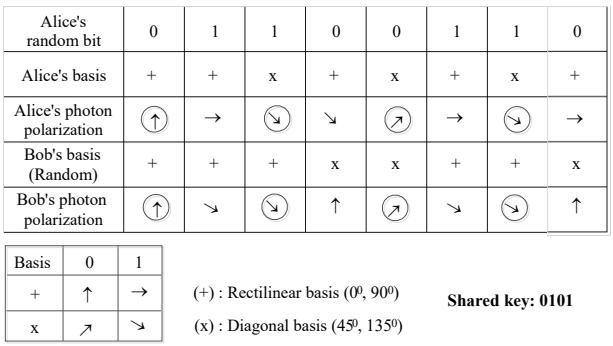

FIGURE 7: BB84 protocol Working with shared key 0101.

U_2 does not know which basis for photon storage is best. Therefore the only option he has is to select an arbitrary basis, such as to measure in either rectilinear or diagonal. The time taken to measure it is recorded, and the measurement result for each photon is received. U_2 is on the public classical

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

channel talking to the U_1, and he is the focus of the system's activities. The sender then broadcasts the basis using which it sends the bits publicly. The U_2 then verifies the correctness of the basis with which it measured the states of the qubits. The incorrectly measured are then discarded by both parties and this is how the shared random key is generated between two parties. A predetermined subset of sender and receiver's remaining bit strings is now compared. If a third party has learned anything about the polarisation of the photons, the receiver's observations will be skewed. Other conditions, such as the environment, might create mistakes in the same way. They reject the key and start again, potentially with another quantum channel, when more than p bits differ because the key's security cannot be guaranteed.

D. INTERNET LAYER

Internet layer makes the data route from one region to other regions. 5G is one of the latest mobile communication technology that can yield high speed (S_x = up to 2 GBits/s [51]). The internet layer here makes use beyond 5G network technology. The reason behind using beyond 5G is that it can provide ubiquitous connectivity, low latency ($\leq$ 1 millisecond), large spectrum (better than the previous generations), and scalability. All these properties support quick data transfer in line with virtualisation as well as in UAV swarming networks. Many sensitive applications (such as healthcare, disaster management, military, etc.) are intolerant of delays in information transmission. Therefore, beyond 5G networks are well-suited for such applications. The internet layer in this architecture is eligible for catering to the two communication channels (i.e., quantum and classical) mentioned in the quantum layer. The 5G wireless network is capable of carrying photons as well as classical bits. The real implementation of these channels makes use of the internet layer (which is the wireless communication layer). The low latency of the internet layer will make the communication faster and the quantum layer will make the communication very much secure.

E. CONTROL LAYER

It is the last layer in the architecture stack. It consists of a centralized data and control centre for UAVs for storing and fetching the real-time data generated by the above layers. This layer will consist of all the storage facilities, quantum computing equipment and a proper cloud-based infrastructure. The L_{all} data will be stored on the servers. The QKD between any arbitrary U_a and U_b where a,b $\in U_{all}$ will be performed using actual quantum computers present at the control station. This layer will also take care of controlling the UAV operations deployed on the ground.

V. BATTLEFIELD APPLICATION IN INTERNET OF MILITARY THINGS: A CASE STUDY

An unmanned combat aerial vehicle (UCAV), also termed as a combat drone that can be used for reconnaissance, surveillance, target detection, and the recognition of military weapons such as missiles, ATGMs, and/or bombs in regions where drone assaults are difficult to reach [52]. These drones are generally trailed in real-time and have varying levels of control. In contrast to unmanned aerial vehicles, surveillance, and reconnaissance, drone assault and combat intelligence are used. This type of drone doesn't need to be a pilot, as it runs without a pilot. The drones are small in size, low in weight and can be remote controlled via GCS.

Lee De Forest, U. A Sanabria, and the founder of radio devices brought the concept of combat drones. In 1940, there was an article published by them in Popular Mechanics. John Stuart Foster Jr., a nuclear scientist and former head of the Lawrence Livermore National Laboratory, invented the advanced military drone. Foster was a model airplane hobbyist in 1971 when he got the notion to use his pastime to manufacture weapons and drew out blueprints. The defence advanced research projects agency produced two prototypes, dubbed "Prairie" and "Calera," by 1973. They were launched into the air by a modified lawnmower motor and could stay in the air for two hours while carrying a 28-pound burden [53].

During the Yom Kippur War in 1973, Israel used unarmed US Ryan Firebee targeted drones to push Egypt to burn its entire anti-aircraft weapons [54]. This mission was accomplished with no damages to Israeli pilots, who instantly took advantage of Egypt's weakened defenses. During the Iran–Iraq War in the early '90s, Iran used a drone containing six RPG-7 rounds [55]. In January 2014, 2,400 individuals were reported to have perished as a consequence of US drone attacks. In June 2015, the death count from US drone attacks had risen to 6,000 in only five years. The Internet of military things (IoMT) for the battlefield application may be using traditional security techniques or cryptography methods to improve secure data communication, which is referred in Section 2.3 origin and timeline of cryptography. In traditionally the drone of battlefields application, they may be starts by the 1G to 5G communication concerning their latency that is 1G latency is $<$ 1000 ms, 2G latency is $<$ 600 to 750 ms, 3G latency is $<$ 100 ms, 4G latency is $<$ 10ms, 5G latency is $\sim$ 5ms. In battlefield application, we cannot even a bear delay of $1ms$. So, we need an ultra-low latency network that is beyond the 5G network which gives < 1 ms latency. The proposed system can be used for Battlefield application in the IoMT environment. There are some issues in battlefield applications with the traditional communication networks discussed in the next subsection.

A. ISSUES IN BATTLEFIELD APPLICATIONS

This subsection throws light briefly on the issues that have been identified in the traditional battlefield communication set-up. These issues are the very basis of this research article. We develop a full-fledged solution to address all the following issues by exploiting the quantum cryptography and latest generation of networks (beyond 5G). The flow of communication using the above proposed novel framework in battle field applications can be seen in FIGURE 8.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

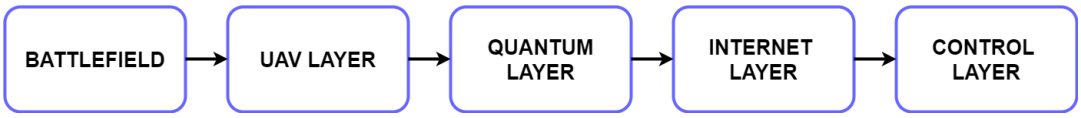

FIGURE 8: Battlefield application architecture.

1) Latency and Reliability

Communication latency and reliability in traditional network is not suitable for UAVs used in battlefield application. In such applications, the system cannot even bear a delay of $1ms$ and also can not afford system unavailability, which causes serious disaster to the people as well as the property. The proposed system uses beyond 5G networks that offers $< 1ms$ round-trip latency and 99.99999% reliability, which is quite suitable for military applications.

2) Security and Privacy

In battlefield application, the signal interception, deciphering, and reconnaissance in UAV communication may cause the breach of the nation's sensitive information. So, security and privacy of data is a major concern in UAV communication. To secure UAV communication from cyber criminals, various security algorithms (digital signatures, RSA, SHA256, and many more) and machine learning techniques (decision tree, ensemble learning, artificial neural networks, reinforcement learning, and many more) can be utilized. However still, the data can be changed, which might result in incorrect outcomes. To handle this, the proposed system uses quantum cryptography along with BB84 protocol to secure sensitive military information from cyber-attacks.

3) Throughput

Throughput means how much the data has been processed per unit time. The throughput of traditional 1G, 2G, 3G, 4G, and 5g are networks are estimated as 9.6 kbps, 2Mbps, 100 to 300 Mbps, up to 3 Gbps, and 1 Tbps respectively. So, such throughput are not highly preferable for battlefield application, where we need much higher throughput to process more tasks at single instance of time for better and efficient decision making. To achieve this, the proposed system's beyond 5G network is perfectly suitable.

4) Integrity

In battlefield application, the combat drone's integrity can be compromised if data sent across the channel is changed. The data or information sent between the combat drones and the GCS is incorrect, and the attacker can use it to manage these battlefields for his own purpose. Integrity vulnerabilities are may be responsible for different types of attacks like the man in the middle, hijacking, replay, and GPS spoofing attacks. The integrity of UAV-assisted battlefield applications can be ensured using quantum cryptography.

The utilization of drones in battlefield application make use of quantum cryptography to exchange the sensitive data over the wireless channel, such as beyond 5G networks. The communication can either be drone to drone or drone to ground station. The two party communication in here is very secure and fast. Hence it is exactly full-filing the requirement of mission-critical applications. The implementation of the proposed methodology performance is analyzed in the next subsection.

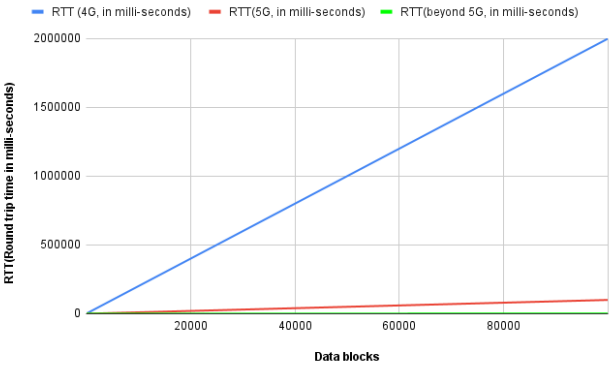

FIGURE 9: Comparison of round-trip time taken by 4G, 5G, and beyond 5G networks

B. CASE STUDY ANALYSIS (PERFORMANCE ANALYSIS)

This section covers the performance analysis of the proposed quantum cryptography-based system. We have performed a detailed theoretical analysis of the components of our novel architecture. The analysis involves the latency and throughput of the underlying network, which is to be used in the implementation and the quantum supremacy to achieve security above the existing classical security paradigms. Below is the detailed analysis for the same.

1) Latency Analysis

FIGURE 9 shows the comparative analysis of round-trip times (RTTs) of various communication protocols such as 4G, 5G, and beyond 5G. As observed from the graph, the time taken by beyond 5G networks is way less than that of 4G and 5G networks. This provides an edge to the beyond 5G networks over the others. Fast communication assists the mission sensitive tasks and hence it is very much required.

2) Quantum Cryptography

One of the major components of the above-proposed architecture is quantum technology. The properties of quantum physics introduced into the field of cryptography enhances the security aspect. Quantum cryptography is a budding area

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3138753, IEEE Access

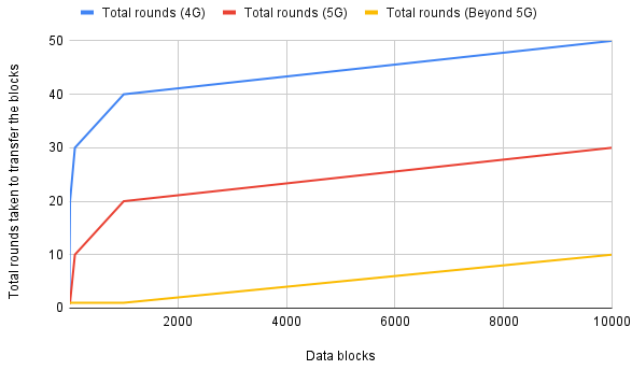

FIGURE 10: Comparison of throughput performance of 4G, 5G, and beyond 5G

of research in which cryptography can be seen in terms of physics and not rely on mathematical functions (as in traditional cryptography). The superposition and quantum state measurement allow the sender and receiver to trace the third party attacks.

3) Throughput Analysis

Throughput is described as the amount of time taken by the data to be processed by the network. The detailed analysis is presented in the graph below. FIGURE 10 shows the throughput comparison of 4G, 5G, and beyond 5G networks with respect to different data block sizes. From FIGURE 10, we can observe that the time taken by the packets to process the data blocks is the least in case of beyond 5G networks. Therefore, it is we choose to implement using the best available network that is beyond 5G.

VI. OPEN ISSUES AND CHALLENGES

A. DATA HANDLING

The data generated from UAV sensors is massive in volume due to the constant data sensing process. The beyond 5G communication network operates at a high frequency of 95 GHz to 3 THz, with data transmission rates of up to 1 Tb/s, and a bandwidth of 1 THz, which is faster than existing communication technologies. It also has a latency of less than $< 1ms$. Hence, handling and processing the data simultaneously will be an issue if we don't have enough resources to manage the data. The data has a "volume" feature, which generates with velocity 'v' and latency 'l'. The total data generation time(t) will be $t = l + v$. The big data handling will further require proper data analysis for the same. Thus, this is an open research area in which the data management is highly prioritized.

B. ENERGY MANAGEMENT

UAVs are lightweight and battery-operated flying devices with a limited flying time. UAVs and beyond 5G infrastructure generate huge amounts of some scenario-based applications of UAV data at specific intervals. As a result, handling such a huge quantity of data in a UAV scenario requires a lot of computing power, which will result in draining the short-lived batteries in the UAVs. To solve these issues, we can try to manage all the data separately in a decentralised manner. The ready-made data, when fed to the UAV, will result in less computation and processing. The energy vs computation trade-off will always affect the UAV's physical output performing capabilities when deployed in any workspace.

C. PHYSICAL ATTACKS ON UAVS

Although UAVs in real-time can generate and process a massive amount of data and transmit it to other UAVs and GCS. The security of UAV will always remain on high priority to safeguard it against physical attacks such as hijacking, physical tampering of UAV components, etc. A lightweight and power-constraint UAVs cannot protect themselves from the external factors disturbing them in the open airspace. UAVs can be hijacked despite their performance potential. UAVs deployed on the ground are highly prone to physical attacks, especially when deployed in the mission sensitive domains (such as the military), which can tamper with the hardware component of UAVs and make them non-functional. The physical intrusion of the UAV can affect its ongoing task performance in real-time.

D. BB84 IS PRONE TO MAN-IN-THE-MIDDLE ATTACK

BB84 is a quantum key distribution protocol that uses both quantum and classical communication channels for the key exchange process. The authentication of two parties (Alice and Bob) usually takes place using the classical channel, which exposes this protocol to intruders. When Alice and Bob try to exchange photons, there is a possibility that an intruder, Eve, can come and intervene in the transmission by mimicking itself as a sender (i.e., Alice in this case) since the authentication channel used here is very much prone to attacks. To which the possible solution is to integrate the distributed authentication process [56].

E. PNS ATTACK DURING KEY EXCHANGE

PNS stands for photon number splitting. This attack majorly focuses on the photons that are produced, not ideally single. The photon generator might not always have a single photon but multiple photons in one go. These multiple-photons are then become useful to the intruders. The intruder Eve will try to measure the tiny portion of the photon coming from Alice and then send the remaining photon to Bob. Measuring the tiny portions might help the intruder guess the key that is being exchanged by measuring the small number of photons on the correct basis publicly broadcasted by Alice later. The PNS attack is quite difficult to implement since the probability of multi-photon generation from the pulse emitter is 50% [57]. Even for measuring the portion of multi-photons, Eve would require proper hardware and algorithms. The implementation of this type of attack is hence a difficult operation. This attack is quite powerful if executed in real-time and hence not suitable for mission-specific applications.

F. QUANTUM STATES ARE DESTROYED ONCE MEASURED

The quantum states initially are in superposition when not measured. Upon measurement, the quantum state is disintegrated and becomes a classical bit whose value is either '0' or '1'. This property of qubits allows them to secure the system. The sender and receiver will know about the intrusion and will restart the qubits' transmission from the beginning. This process would be an overhead; the attacks are happening now and then on the system. The system will end up restarting the qubit streaming only.

G. QUANTUM CHANNEL BREAK DOWN

The quantum channel is a medium through which we can communicate quantum information (mostly qubits in this case). It is fairly a secure channel, also known as a trace-preserving channel. The quantum channel can be implemented using optical fibre or free airspace (wireless) in real-time. This channel is hence vulnerable to intruders. If not able to intercept and read the data, the third party is very much capable of demolishing the channel, which will refute the quantum services. The sender and receiver will not be able to connect and transmit using quantum technology.

H. COST EFFICIENCY

The quantum facility is difficult to store at room temperature since it requires everlasting cold storage. This whole quantum apparatus to be stored and managed properly require expertise. To solve this issue, we can use the virtualization of the quantum services through cloud infrastructure. Again, the cloud facilities will cost the end user more if the quantum facilities are utilized too much (as per the requirement of the application). The affordability of these services rendered by the cloud service providers that follow "pay-as-you-go" business model is still a question. We might be able to solve this issue by using mobile-edge computing.

I. CENTRAL NODE FAILURE

The solution to the previous issue was to use a hassle-free cloud amenity which is very prominent these days. Here, the cloud is considered the central entity for all the secure key exchange happening across the sender and the receiver. The central node completely runs the system. This node's availability and reliability is important here since the mission sensitive jobs cannot bear the central node failure. The dependency of the system in the central node can fail the whole system. This issue can be addressed using the concept of decentralization, where data is readily available as well as secure. Recently an Australian company named "Quantum brilliance" has successfully made a quantum computer that is adequately operable at room temperature. That quantum computer consists of only five qubits as of now. In future, if the quantum facility becomes temperature friendly, we can get rid of central dependency.

VII. CONCLUSION

This study is majorly focused on making UAV communication more secure as the usage of drones is getting popular across the globe. The data generated and transferred using UAVs is considered valuable due to its massive application in numerous domains. In today's cryptographic world, the real challenges towards handling data security and transfer must be addressed. This study analysed the various aspects of making the UAV communication safe and sound when the application is mission-specific. Herein we exploit the attributes of quantum cryptography and beyond 5G networks to make the drone communication more to shield the data transfer and the data itself. We specifically included one of the quantum cryptographic algorithms BB84, which is very safe and different from the existing traditional cryptographic algorithms. The heart of this research is the novel architecture in which we are proposing to improvise the UAV to UAV and UAV to GCS communication. The above-proposed work is majorly helpful for applications where the task is time-sensitive or the data is highly confidential, requiring special infrastructure. The proposed architecture is prone to various challenges discussed in section 7. The future directions of this study aim to resolve all the possible challenges and implement tamper-proof communication between the drones.

As a part of future work of this study, we aim to develop a simulated or real layered architecture and then implement it using real quantum hardware (by quantum infrastructure providers such as IBM qiskit, AWS- Braket, etc.) in the field of drone communication. The future of cryptography holds quantum technology which puts behind the traditional means of securing the data.

REFERENCES

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

[2] 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 Journal, pp. 1–1, 2021.

[3] N. Pathak, A. Mukherjee, and S. Misra, "Aerialblocks: Blockchain-enabled uav virtualization for industrial iot," IEEE Internet of Things Magazine, vol. 4, no. 1, pp. 72–77, 2021.

[4] A. Oigbochie, E. Odigie, and B. Adejumo, "Importance of drones in healthcare delivery amid a pandemic: Current and generation next application," Open Journal of Medical Research (ISSN: 2734-2093), vol. 2, no. 1, pp. 01–13, 2021.

[5] S. Dahiya and M. Garg, "Unmanned aerial vehicles: Vulnerability to cyber attacks," in International Conference on Unmanned Aerial System in Geomatics, pp. 201–211, Springer, 2019.

[6] Markets and markets, "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." https://www.marketsandmarkets.com/Market-Reports/drone-services-market-80726041.html. Accessed: 2021.

[7] E. Shaikh, N. Mohammad, and S. Muhammad, "Model checking based unmanned aerial vehicle (uav) security analysis," in 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pp. 1–6, 2021.

[8] 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.

[9] R. Gupta, A. Nair, S. Tanwar, and N. Kumar, "Blockchain-assisted secure

uav communication in 6g environment: Architecture, opportunities, and challenges," IET Communications, 2021.

[10] A. Islam and S. Young Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," Computers and Electrical Engineering, vol. 84, p. 106627, 2020.

[11] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-Based UAV Path Planning for Healthcare 4.0: Current Challenges and the Way Ahead," IEEE Network, vol. 35, no. 1, pp. 20–29, 2021.

[12] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, vol. 239, no. December, pp. 113–122, 2018.

[13] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A study of blockchain technology development and military application prospects," Journal of Physics: Conference Series, vol. 1507, no. 5, 2020.

[14] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Vehicular Communications, vol. 23, no. February, pp. 0–28, 2020.

[15] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "A taxonomy of blockchain-enabled softwarization for secure UAV network," Computer Communications, vol. 161, no. August, pp. 304–323, 2020.

[16] N. Neji and T. Mostfa, "Communication technology for unmanned aerial vehicles: A qualitative assessment and application to Precision Agriculture," 2019 International Conference on Unmanned Aircraft Systems, ICUAS 2019, pp. 848–855, 2019.

[17] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles," Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2018, pp. 32–37, 2018.

[18] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," 20th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2019, no. C, 2019.

[19] M. Golam, J. M. Lee, and D. S. Kim, "A UAV-assisted Blockchain Based Secure Device-to-Device Communication in Internet of Military Things," International Conference on ICT Convergence, vol. 2020-October, pp. 1896–1898, 2020.

[20] F. buiness insights, "The global military drone market." https://www.fortunebusinessinsights.com/military-drone-market-102181. Accessed: 2021.

[21] 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 IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 255–260, IEEE, 2020.

[22] T. Nakano, I. Kamiya, M. Tobita, J. Iwahashi, and H. Nakajima, "Landform monitoring in active volcano by uav and sfm-mvs technique," The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 40, no. 8, p. 71, 2014.

[23] 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 Journal, 2021.

[24] K. Kanistras, G. Martins, M. J. Rutherford, and K. P. Valavanis, "A survey of unmanned aerial vehicles (uavs) for traffic monitoring," in 2013 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 221–234, IEEE, 2013.

[25] 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 Transactions on Multimedia, 2021.

[26] M. Drauschke, J. Bartelsen, and P. Reidelstuerz, "Towards uav-based forest monitoring," in Proceedings of the Workshop on UAV-based Remote Sensing Methods for Monitoring Vegetation. Cologne, Germany: Geographisches Institut der Universität zu Köln—Kölner Geographische Arbeiten, pp. 21–32, 2014.

[27] C. D. Drummond, M. D. Harley, I. L. Turner, A. N. A Matheen, W. C. Glamore, et al., "Uav applications to coastal engineering," in Australasian Coasts & Ports Conference 2015: 22nd Australasian Coastal and Ocean Engineering Conference and the 15th Australasian Port and Harbour Conference, p. 267, Engineers Australia and IPENZ, 2015.

[28] 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," Journal of Management in Engineering, vol. 36, no. 3, p. 05020005, 2020.

[29] 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 Archaeology, vol. 77, no. 3, pp. 176–181, 2014.

[30] M. Erdelj and E. Natalizio, "Uav-assisted disaster management: Applications and open issues," in 2016 international conference on computing, networking and communications (ICNC), pp. 1–5, IEEE, 2016.

[31] 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 International Conference on Image Analysis and Processing, pp. 275–281, Springer, 2015.

[32] 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 in Smart-Cities, pp. 37–55, Elsevier, 2020.

[33] 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 2017 23rd International Conference on Automation and Computing (ICAC), pp. 1–11, IEEE, 2017.

[34] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks-an approach to the risk assessment," in 2013 5th international conference on cyber conflict (CYCON 2013), pp. 1–23, IEEE, 2013.

[35] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), pp. 194–199, IEEE, 2017.

[36] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," Journal of cryptology, vol. 5, no. 1, pp. 3–28, 1992.

[37] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," arXiv preprint arXiv:2003.06557, 2020.

[38] A. K. Ekert, "Quantum cryptography based on bell's theorem," Physical review letters, vol. 67, no. 6, p. 661, 1991.

[39] P. SP and J. Kalaivani, "A study on quantum cryptography," International Journal of Pure and Applied Mathematics, vol. 119, no. 15, pp. 3185–3191, 2018.

[40] R. Renner, "Security of quantum key distribution," International Journal of Quantum Information, vol. 6, no. 01, pp. 1–127, 2008.

[41] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," Physical review letters, vol. 78, no. 17, p. 3414, 1997.

[42] C. Cr and J. Kilian, "Achieving oblivious transfer using weakened security assumptions."

[43] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), pp. 503–509, IEEE, 1998.

[44] A. Goyal, S. Aggarwal, and A. Jain, "Quantum cryptography & its comparison with classical cryptography: A review paper."

[45] Deloitte, "Breaking blockchain open deloitte's 2018 global blockchain survey."

[46] M. Pandya, "Securing clouds-the quantum way,"

[47] "Quantum cryptography to protect swiss election." https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/. Accessed: 2007.

[48] C.-Y. Chen, G.-J. Zeng, F.-j. Lin, Y.-H. Chou, and H.-C. Chao, "Quantum cryptography and its applications over the internet," IEEE Network, vol. 29, no. 5, pp. 64–69, 2015.

[49] "Why this intercontinental quantum-encrypted video hangout is a big deal." https://www.wired.com/story/why-this-intercontinental-quantum-encrypted-video-hangout-is-a-big-deal/. Accessed: 2018.

[50] "Quantum crptography in smart card." https://www.lanl.gov/projects/feynman-center/_assets/pdf/qkard.pdf. Accessed: 2010.

[51] C. R. Murthy and R. Sundaresan, "5g and beyond," 2020.

[52] "Unmanned combat aerial vehicle." https://en.wikipedia.org/wiki/Unmanned_combat_aerial_vehicle. Accessed: 2021.

[53] "Drone." https://en.wikipedia.org/wiki/MIT_Technology_Review. Accessed: 2021.

[54] "Yom kipur war." https://en.wikipedia.org/wiki/Yom_Kippur_War. Accessed: 2021.

[55] "Us and israel drones." https://web.archive.org/web/20131212120127/http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus87.pdf. Accessed: 2021.

[56] Y. Wang, H. Wang, Z. Li, and J. Huang, "Man-in-the-middle attack on bb84 protocol and its defence," in 2009 2nd IEEE International Conference on Computer Science and Information Technology, pp. 438–439, IEEE, 2009.

[57] R. Aggarwal, H. Sharma, and D. Gupta, "Analysis of various attacks over bb84 quantum key distribution protocol," International Journal of Computer Applications, vol. 20, no. 8, pp. 28–31, 2011.