A
SEMINAR REPORT
ON

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

In partial fulfillment of requirements for the degree

Third Year Computer Engineering

By

Kasturi Mahesh Shirole
Exam Seat No. :
Roll No. : 53

Under the guidance of

Mrs. V.S.Nikam

DEPARTMENT OF COMPUTER ENGINEERING

University Of Pune

Gokhale Education Society's

R. H. Sapat College of Engineering, Management Studies and Research,

Nashik - 422 005, (M.S.), INDIA

[2023 – 2024]

Gokhale Education Society's

R. H. Sapat College of Engineering,
Management Studies and Research,
Nashik - 422 005, (M.S.), INDIA

CERTIFICATE

This is to certify that the seminar report entitled **"Quantum Cryptography as a Service for Secure UAV Communication: Applications and Challenges"** is being submitted herewith by "Kasturi Mahesh Shirole-A-53" has successfully completed her seminar work in partial fulfillment of requirements for the degree of Third Year Computer Engineering of Savitribai Phule Pune University.

Date:

Place: Nashik

Mrs. V.S.Nikam
Seminar Guide

Dr. D. V. Patil
Head of the Department

Savitribai Phule Pune University
Gokhale Education Society's
R. H. Sapat College of Engineering, Management Studies and Research,
Nashik - 422 005, (M.S.), INDIA

Seminar Approval Sheet

This Seminar entitled

"*Quantum Cryptography as a Service for Secure UAV Communication: Applications and Challenges*" prepared and submitted by *Samradni Vishwanath Salunke* has been approved and accepted in partialfulfillment of the requirements for the degree Third Year Computer Engineering.

Mrs. V.S.Nikam
Seminar Guide

Ms. R. D. Narwade
Seminar Coordinator

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to everyone for providing their invaluable guidance, comments and suggestion throughout the course of seminar project. I would specially thank Mrs.V.S.Nikam for timely checking my progress constantly motivating me to work harder.
In this report, I hope to highlight the enormous opportunities presented by technology for making everyone aware of Quantum Cryptography and it's role in UAV Communications.
These few details lead me to realize that like all human endeavors this project is not perfect and may contain errors and shortcomings. Thus I remain open to all criticisms and suggestions which could present me with new sources of inspiration as I develop my ability to research and learn.

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 achievehigh 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.

CONTENTS

List of Figures

CHAPTER 1

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.

1.1 Necessity

Drones are making billion dollars market in India. As increasing UAV consumption, the data it carries becomesthe nucleus for cyberattacks . 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. Different global wireless communication standards have been used for UAVs viz 3G, 4G, 5G, and 6G. The 5G and 6G networks are very much suitable for such applications. Various cryptography protocols have been used to secure UAV communication. It mentions symmetric and asymmetric key exchange protocols to secure UAV communication. Blockchain-based system in UAV communication can potentially be used to address security concerns in the distribution of critical information. 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. 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.

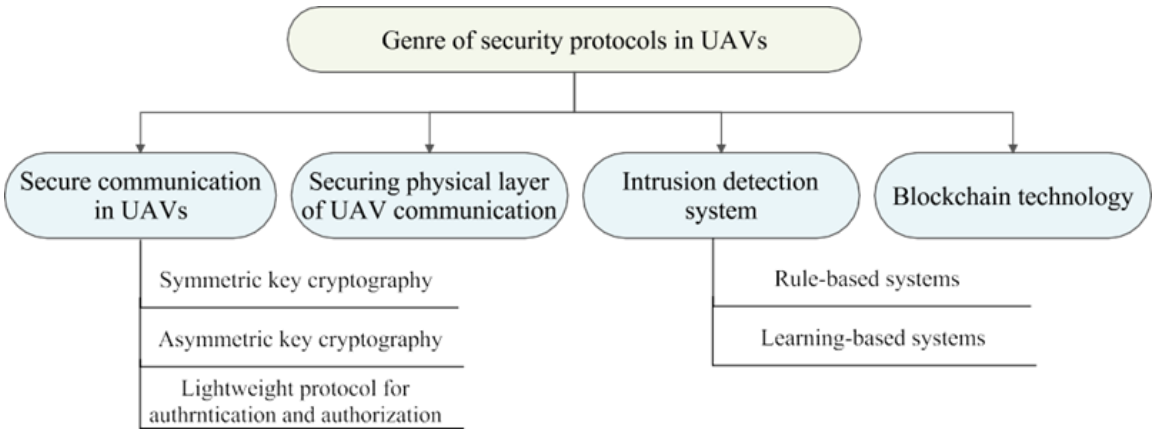

Fig 1.1 Various techniques to secure UAV communication

1.2 Objectives

- To propose a novel architecture based on quantum cryptography.
- To improve security in UAV Communications.
- To build a faster, secure, trusted, and reliable crptographic technique than classical cryptography.

1.3 Features

- Utilizes Quantum Mechanical Phenomena: Employs principles from quantum mechanics to secure cryptographic operations.
- Quantum Key Distribution (QKD): Addresses the problem of securely exchanging cryptographic keys.
- Data Non-Copyability: Quantum states cannot be copied due to the no-cloning theorem.
- Vulnerability to Reading Attempts: Attempts to read the data can alter the quantum states, providing a means to detect eavesdropping.
- Impossibility of Copying Quantum State Labels: Quantum cryptography offers a level of security that is not possible to achieve using traditional communication methods alone.
- Expanding the Boundaries of Cryptographic Tasks: Quantum cryptography enables cryptographic tasks that were once deemed impossible or highly challenging using classical communication methods.

1.4 Applications:

- Quantum Cryptography in UAV Communication: Rising drone usage necessitates secure communication between drones and ground stations.
- Quantum Cryptography in Cloud Computing: Addresses concerns about data transit security and storage on shared servers.
- Quantum Cryptography in Voting Security: Ensured protection against hacking and unintentional data manipulation.
- Quantum Cryptography in Future E-commerce: Enables secure agreement between customers and sellers through quantum-encoded messages.
- Quantum Cryptography in Smart Card: Utilizes mechanical physics principles for encryption, diverging from complex mathematical approaches.
- Applicable in telecommunications, banking, financial transactions, wireless Internet, electronic voting, vehicle access, and government/defense scenarios.

CHAPTER 2

LITERATURE SURVEY

2.1 Paper Surveys

1. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR), Oct. 2017, pp. 194–199.:-

Gilles Brassard and Steven Wiesner 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.

2. IEEE Netw., vol. 35, no. 1, pp. 20–29, Jan. 2021:-

S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad 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.

3. Proc. Int. Conf. Secur. Privacy Commun. Syst. in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 239, 2018, pp. 113–122.:-

M. S. Haque and M. U. Chowdhury, ‘‘A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV),’’ suggested a new cyber- security 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 Steganogra- phy methods.

4. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, ‘‘Experimental quantum cryptography,’’ J. Cryptol., vol. 5, no. 1, pp. 3–28, Jan. 1992.:-

. Bennett and Brassard created the BB84 [36], a soon dynamic communication device in 1984 based on their earlier work..

5. A. K. Ekert, ‘‘Quantum cryptography based on Bell’s theorem,’’ Phys. Rev. Lett., vol. 67, no. 6, p. 661, 1991.:-

In a 1991 work by Arthur Eckert [37], 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.

CHAPTER 3

SYSTEM ANALYSIS

3.1 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.

3.2 Security Issues in UAVs

UAVs and GCS generally communicate through communication protocols, such as MAVLink, UranusLink, UAVCAN. These protocols are used to transfer messages during communication from GCS. Most of the existing security protocols may not be intended for such an environment. . 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 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.

3.3 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.

The study of executing security tasks using concepts of quantum-mechanics is known as cryptography. Quantum cryptography 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.

3.4 The Proposed Quantum Cryptography based solution

This section describes the proposed quantum cryptographybased architecture to secure UAV communications. We propose a novel layered architecture that makes the UAV communication indestructible based on quantum. the layered proposed architecture comprises of control layer, Internet layer, quantum security layer, physical/UAV layer, and monitoring layer.

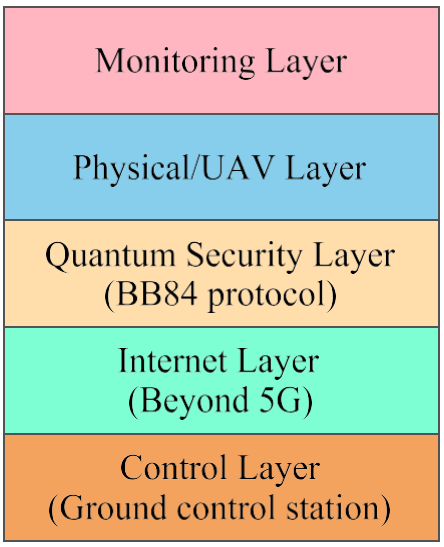

Fig. 3.1. The Proposed Layered Architecture

Monitoring Layer:

1. Focuses on capturing data from various designated locations (entities) such as cities, water bodies, forest areas, etc.
2. Each location entity can generate a substantial volume of data with diverse properties like variety, volume, and velocity.
3. Data can be in the form of images or streams (videos) and is generated at frequencies specific to each location's requirements.
4. The layer employs UAV cameras for data capture, eliminating the need for manual intervention.

UAV Layer:

1. Houses the actual UAVs physically deployed at specific locations for data generation.
2. UAVs operate in 3D space above the ground, and they can form chains or swarms for synchronized tasks.
3. UAV swarm technology enables multiple drones to work together efficiently on a specific task.

Quantum Layer:

1. Quantum cryptography leverages the principles of physics to ensure secure transmission of sensitive information from the monitoring layer.
2. Utilizes a quantum key distribution paradigm for secure key exchange, employing existing QKD protocols like the BB84 protocol.

3.5 BB84 Protocol:

1. BB84 protocol involves the transmission of data using the polarization of a single photon state.
2. It defines two pairs of nearby states for the protocol and the contrast-coded states used in fiber-based implementations.
3. A quantum communication channel connects the sender (U1) and receiver (U2), allowing the exchange of quantum states.
4. The protocol assumes that an adversary may interfere with the quantum channel, emphasizing the need to verify the classical channel.
5. Encryption of data in non-orthogonal states ensures protocol security, leveraging quantum uncertainty.
6. The polarization of photons is determined by random bit selection and basis choice (rectilinear or diagonal).

Working of BB84 Algorithm:

1. The sender (U1) produces a random bit (0 or 1) and selects a basis (rectilinear or diagonal) to encode the photon's polarization.
2. U1 sends the single photon through a quantum channel to the receiver (U2), repeating the process for each photon.
3. Quantum physics allows discrimination between non-orthogonal polarization states, enabling measurements in an orthonormal basis.
4. U2 measures each photon's polarization, recording the basis and time of measurement.
5. U1 publicly broadcasts the basis used for encoding the bits, allowing U2 to verify the correctness of his measurements.
6. Both parties discard incorrectly measured photons, generating a shared random key between them.
7. A subset of the remaining bit strings is compared to ensure the key's security, rejecting it if a third party may have learned anything about the photons' polarization.

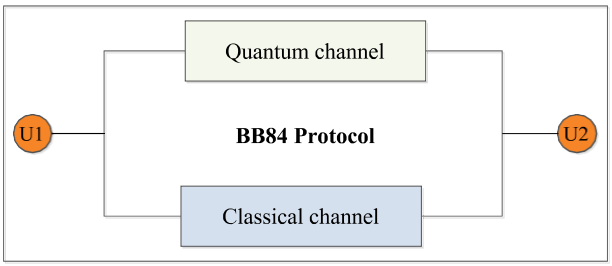

Fig 3.5: BB84 protocol structure.

CHAPTER 4

DISCUSSIONS

4.1 Open Issues and Challenges

1. DATA HANDLING
   Massive volume of data generated by UAV sensors requires efficient handling and processing.
   Beyond 5G communication network's high data transmission rates and bandwidth pose a challenge in simultaneous data management.

2. ENERGY MANAGEMENT:
   UAVs and beyond 5G infrastructure demand significant computing power, which strains the UAVs' limited battery life.
   Managing data in a decentralized manner can alleviate computation requirements and preserve energy.

3. PHYSICAL ATTACKS ON UAVs
   UAVs are vulnerable to physical attacks such as hijacking and tampering, particularly in mission-sensitive domains like the military.

4. BB84 VULNERABILITY ON MITM ATTACKS
   BB84, a quantum key distribution protocol, is susceptible to Man-in-the-Middle attacks due to its use of classical channels for authentication.

5. PNS ATTACK DURING KEY EXCHANGE
   Photon Number Splitting (PNS) attacks exploit the presence of multiple photons, potentially compromising key exchange security.

6. QUANTUM STATES DISINTEGRATION UPON MEASUREMENT:
   Quantum states collapse into classical bits upon measurement, requiring the restart of qubit transmission in case of intrusion.

7. QUANTUM CHANNEL BREAKDOWN
   The quantum channel, though secure, is susceptible to interception and disruption by third parties, hindering quantum communication.

8. COST EFFICIENCY
   Quantum facilities require specialized storage conditions, potentially leading to high costs for end users.
   Cloud-based quantum services may be expensive if utilized extensively.

9. CENTRAL NODE FAILURE
   Centralized systems reliant on a central node for key exchange face potential failure risks, especially in mission-critical applications.
   Decentralization and advancements in quantum technology may mitigate this dependency.

These challenges highlight the need for ongoing research and innovation in quantum cryptography to address security, efficiency, and scalability concerns in various real-world application.

CHAPTER 5

CONCLUSION

5.1 Future Scope

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.

5.2 Conclusion

This study highlights the pressing need for heightened security in UAV communication, given the widespread global use of drones and the immense value of their generated data. Focusing on mission-specific applications, it identifies the challenges in securing data transfer in today's cryptographic landscape.The integration of quantum cryptography and beyond 5G networks emerges as a promising strategy to bolster drone communication and protect data. The adoption of the BB84 quantum cryptographic algorithm signifies a significant departure from traditional cryptographic methods, ensuring a superior level of security. The proposed innovative architecture aims to enhance UAV-to-UAV and UAV-to-GCS communication, particularly advantageous for time-sensitive tasks and highly sensitive data.

REFERENCES

[1] A. R. Hall and C. J. Coyne, ‘‘The political economy of drones,’’ Defence Peace Econ., vol. 25, no. 5, pp. 445–460, Sep. 2014.
[2] S. P. Priyadharshini and J. Kalaivani, ‘‘A study on quantum cryptography,’’ Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 3185–3191, 2018.
[3] R. Renner, ‘‘Security of quantum key distribution,’’ Int. J. Quantum Inf. vol. 6, no. 1, pp. 1– 127, Feb. 2008.
[4] D. Mayers, ‘‘Unconditionally secure quantum bit commitment is impossible,’’ Phys. Rev. Lett., vol. 78, no. 17, p. 3414, 1997.
[5] R. Aggarwal, H. Sharma, and D. Gupta, ‘‘Analysis of various attacks over BB84 quantum key distribution protocol,’’ Int. J. Comput. Appl., vol. 20, no. 8, pp. 28–31, Apr. 2011.
[6] D. Mayers and A. Yao, ‘‘Quantum cryptography with imperfect apparatus,’’ in Proc. 39th Annu. Symp. Found. Comput. Sci., 1998, pp. 503–509.
[7] C. H. Bennett and G. Brassard, ‘‘Quantum cryptography: Public key distribution and coin tossing,’’ 2020, arXiv:2003.06557.
[8] J. Huang, Y. Wang, H. Wang, Z. Li, and J. Huang, ‘‘Man-in-the-middle attack on BB84 protocol and its defence,’’ in Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol., Aug. 2009, pp. 438–439.
[9] R. Aggarwal, H. Sharma, and D. Gupta, ‘‘Analysis of various attacks over BB84 quantum key distribution protocol,’’ Int. J. Comput. Appl., vol. 20, no. 8, pp. 28–31, Apr. 2011.
[10] D. Mayers and A. Yao, ‘‘Quantum cryptography with imperfect apparatus,’’ in Proc. 39th Annu. Symp. Found. Comput. Sci., 1998, pp. 503–509.
[11] A. Goyal, S. Aggarwal, and A. Jain, ‘‘Quantum cryptography & its comparison with classical cryptography: A review paper,’’ in Proc. 5th IEEE Int. Conf. Adv. Comput. Commun. Technol., 2011, pp. 428–432.
[12] C. H. Bennett and G. Brassard, ‘‘Quantum cryptography: Public key distribution and coin tossing,’’ 2020, arXiv:2003.06557.
[13] 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 Netw., vol. 35, no. 1, pp. 20–29, Jan. 2021.
[14] M. S. Haque and M. U. Chowdhury, ‘‘A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV),’’ in Proc. Int. Conf. Secur. Privacy Commun. Syst. in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunica- tions Engineering, vol. 239, 2018, pp. 113–122.
[15] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, ‘‘A study of blockchain technology development and military application prospects,’’ J. Phys., Conf. Ser., vol. 1507, no. 5, Apr. 2020, Art. no. 052018.
[16] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, ‘‘Applications of blockchain in unmanned aerial vehicles: A review,’’ Veh. Commun., vol. 23, Jun. 2020, Art. no. 100249.
[17] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, ‘‘A taxonomy of blockchain-enabled softwarization for secure UAV network,’’ Comput. Commun., vol. 161, pp. 304–323, Aug. 2020.
[18] N. Neji and T. Mostfa, ‘‘Communication technology for unmanned aerial vehicles: A qualitative assessment and application to precision agricul- ture,’’ in Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS), Jun. 2019, pp. 848–855.
[19] A. Kuzmin and E. Znak, ‘‘Blockchain-base structures for a secure and oper- ate network of semi-autonomous unmanned aerial vehicles,’’ in Proc. IEEE Int. Conf. Service Oper. Logistics, Inform. (SOLI), Jul. 2018, pp. 32–37.
[20] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, ‘‘Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs),’’ in Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM), Jun. 2019, pp. 1–7.