Savitribai Phule Pune University
Gokhale Education Society's

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

DEPARTMENT OF COMPUTER ENGINEERING
Third Year Computer Engineering
Year 2023– 2024

Roll No: 53

Name of Student: Kasturi Mahesh Shirole

Mobile No.:(+91) 7841011771

official-Mail ID: kasturishirole808@gmail.com

Seminar Title : Quantum Cryptography as a Service for Secure UAV communication: Application , Challenges and Case Study.

Seminar Guide : Mrs. V.S.Nikam

Area of the Seminar: Cryptography

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.

Keywords : Unmanned aerial vehicle, quantum computing, quantum cryptography, military, blockchain.

Introduction

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 . Later, this technology found its place in many real-time applications such as agriculture, healthcare, transportation, package delivery, and many more. 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 . As a result, UAVs are very much assailable towards malicious activities. 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.

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.

Architecture

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

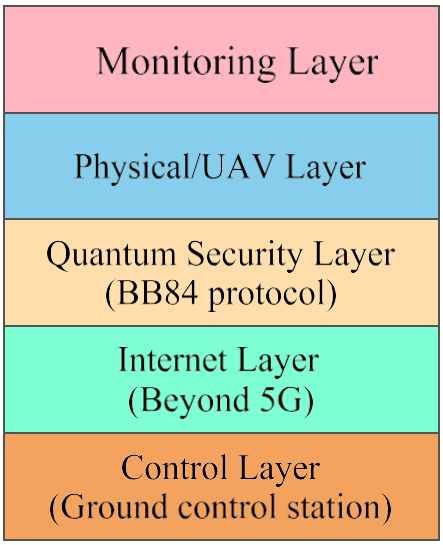

FIGURE 1. The proposed layered architecture.

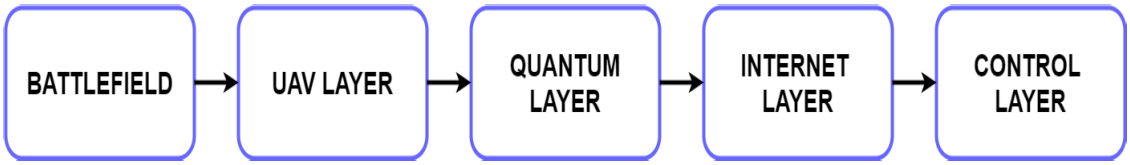

FIGURE 2. Battlefield application architecture.

Method

• BB84 is a key exchange protocol which can generates a random shared private key between two parties (let's say two UAVs U1 and U2).

• BB84 protocol make use of classical communication channel for the authentication of U1 and U2.

• BB84 is a measure and prepare algorithm. In which we measure the state of the quantum bit (qubit) to get information present in it.

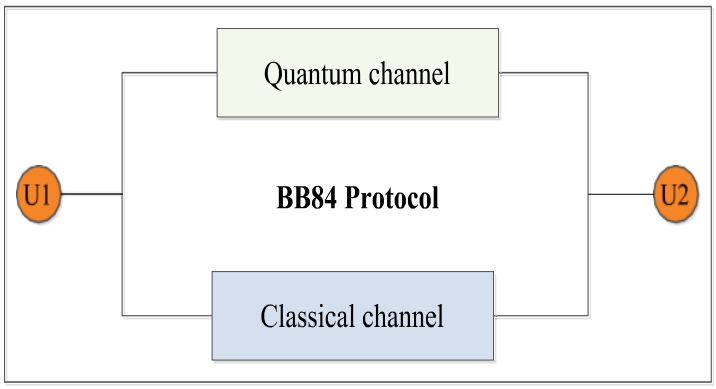

FIGURE 3. BB84 protocol structure.

Working

Alice's random bit	0	1	1	0	0	1	1	0
Alice's basis	+	+	x	+	x	+	x	+
Alice's photon polarization	↑	→	↘	↘	↗	→	↘	→
Bob's basis (Random)	+	+	+	x	x	+	+	x
Bob's photon polarization	↑	↘	↘	↑	↗	↘	↘	↑

(+) : Rectilinear basis (0^0, 90^0)

(x) : Diagonal basis (45^0, 135^0) **Shared key: 0101**

FIGURE 4. BB84 protocol Working with shared key 0101.

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] P. K. R. Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T. R. Gadekallu, W. Z. Khan, and Q.-V. Pham, ‘‘Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges,’’ IEEE Sensors J., vol. 21, no. 16, pp. 17608–17619, Aug. 2021.

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

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

[5] S. P. Priyadharshini and J. Kalaivani, ‘‘A study on quantum cryptography,’’ Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 3185–3191, 2018.

[6] R. Renner, ‘‘Security of quantum key distribution,’’ Int. J. Quantum Inf. vol. 6, no. 1, pp. 1–127, Feb. 2008.

[7] D. Mayers, ‘‘Unconditionally secure quantum bit commitment is impossible,’’ Phys. Rev. Lett., vol. 78, no. 17, p. 3414, 1997.