UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

Secure Communications Protocol For Drones Based On A Flying Ad Hoc Network

Literature Review

R. Wishal Dhiraj Samaranayake
20200903/ w1838836

Supervised by
Mr Geethapriya Liyanage

Key Words - Secure communications protocol, drone technology, quantum-resistant cryptography, flying ad hoc networks

Table of Contents

1. Chapter Overview 3
2. Concept Graph 4
3. Problem domain 5
3.1. Drone Communications 5
3.2. Quantum Computers 5
3.3. Flying Ad Hoc Networks 5
3.4. Proposed Architecture 5
4. Existing work 6
4.1. Authentication 6
4.1.1. Certificate-based Authentication 6
4.1.2. Certificate-less Authentication 6
4.2. Key Exchange 6
4.3. Block Encryption 7
4.4. Networks 7
4.5. Benchmarking 8
5. Technological Review 9
5.1. Post-Quantum Algorithms 9
5.2. Authentication 9
5.3. Key-Exchange 9
5.4. Block Encryption 9
5.5. Network 9
6. Evaluation 10
7. Chapter Summary 11
8. References 12

List of Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
D2D	Drone-to-drone
D2GCS	Drone-to-ground control station
DES	Data Encryption Standard
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
FANET	Flying Ad Hoc Network
LNP	Learning Parity with Noise
LWE	Learning With Errors
MAVLink	Micro Air Vehicle Link

NIST	National Institute of Standards and Technology
RF	Radio Frequency
UAV	Unmanned Arial Vehicle
Wi-Fi	Wireless Fidelity

1. Chapter Overview

This document introduces the reader to the existing research and technologies around secure drone communications and their contributions and limitations. These identified areas are then used to justify the need for the proposed protocol.

2. Concept Graph

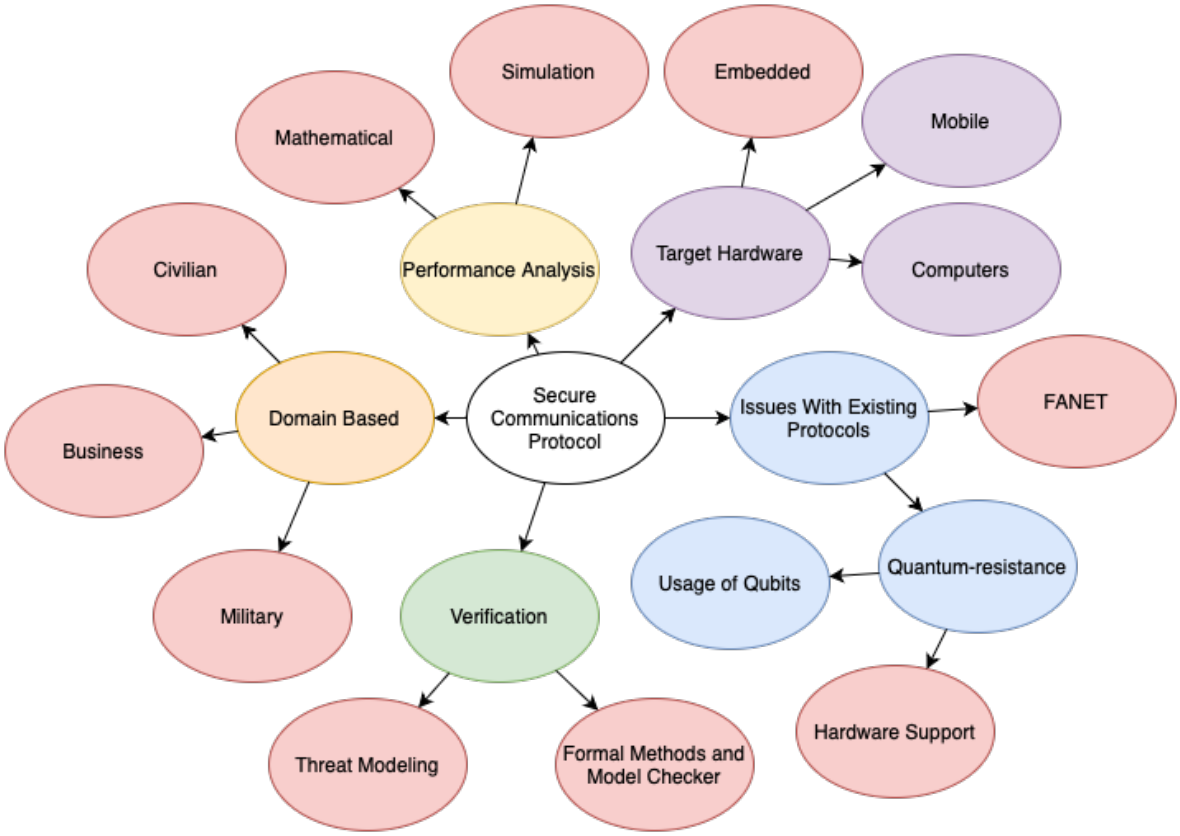

Figure n: Concept graph.

3. Problem domain

3.1. Drone Communications

Drones are an ever-evolving technology which sees new advancements and uses cases in each passing year. With the rapid development, the need for secure communications systems also increases.

Drones by their very nature can be used in various applications, including civilian, business and military applications. These separate sectors can be used for different use cases such as surveillance, search and rescue operations, terrain mapping, and use cases that involve sensitive data collection.

With the advancement of new technologies, one of the most rapidly growing areas is drone swarm communications and coordination for coordinated efforts. These types of applications require drones to communicate within themselves and with ground control stations. These types of communications are susceptible to attacks by different groups, primarily because of the limited power and performance budgets of these devices.

3.2. Quantum Computers

Unlike regular computers which use bits (binary digits), use qubits (quantum bits). Because of the quantum-uncertainty principle, each qubit can hold up to two bits worth of data. This enabled quantum computers to compute vast amounts of calculations which would take an incredible amount of time for traditional computers.

American mathematician Peter Shor introduced a new quantum algorithm known as Shor's algorithm to find the prime factors of an integer (Shor, 1994). Using this algorithm, quantum computers can calculate prime factors of integers far quicker than traditional computers. This poses an incredible threat to existing communications since public-key cryptographic algorithms heavily rely on the problem of integer factorization as their primary security reduction.

3.3. Flying Ad Hoc Networks

Ad hoc networks are a type of wireless network that works using decentralized nodes communicating with each other. Here, each node takes part in communication and routing and does not require pre-existing infrastructure.

Flying ad hoc networks use UAVs as communication data links. These types of networks give much more mobility to the network and can be used in critical situations such as natural disasters to set up a quick network which can be used by civilians and authorities to respond quickly.

3.4. Proposed Architecture

4. Existing work

4.1. Authentication

Authentication is the process of validating if the connecting party is trustable. There are multiple ways of authentication, including password-based, multi-factor, certificate-based, biometric, and token-based. However, the most common authentication method for digital communications is certificate-based authentication.

4.1.1. Certificate-based Authentication

Certificate based authentication is the process of authenticating a communicating party using a certificate which contains information that can be used to check if the communication party can be trusted. This information is based on a chain-like structure. The certificates are signed by a higher party which are also signed by a higher party. The final or root-node is called the Certificate Authority that has a self-signed certificate. Depending on whether this certificate authority is trusted will be the baseline in authenticating a communicating party.

4.1.2. Certificate-less Authentication

Certificate-less authentication is based on authenticating a communicating party without the need of public key infrastructures or digital certificates.

A quantum-resistant authentication protocol for fog-based microgrids was proposed by Shouqin Li and Xiangxue Li in 2021. The protocol uses a custom algorithm based on the Learning Parity with Noise (LNP) problem (Shouquin Li, 2021). The LNP problem is proven to be secure against quantum computers in the future.

Even though this algorithm is secure against quantum computers, it is difficult to keep track of drones and to properly make sure that they are kept secure and updated. When using a certificate-based system, the certificates need to be renewed before the certificate is expired. This means the drones can be registered and monitored by a central point which gives the trusted party more control over who can be trusted and who cannot. Another problem is that these custom protocols take a longer time or might never get hardware support because of custom implementations. This means the algorithms might not get performance improvements which can be gained from using standardized algorithms like Kyber.

4.2. Key Exchange

Key exchange is the process of sharing a cryptographic key between two communicating parties to encrypt and decrypt all the messages sent through the communication medium. The goal of key-exchange algorithms is to share information among two or more parties in a way which doesn't allow others to copy the original key that is being exchanged.

There are several key exchange algorithms used by drones and other communications systems to securely exchange encryption keys. Diffie Hellman, ECDH, and RSA are some of the most widely used key exchange algorithms.

Diffie Hellman is one of the first public-key key exchange algorithms. This algorithm is still widely used in conjunction with other algorithms such as Elliptic Curve cryptography and RSA (ECDHRSA) (Whitfield Diffie, 1976).

Elliptic Curve Diffie Hellman or ECDH for short, is a variant of Diffie Hellman which uses the Elliptic Curve cryptography. ECC is based on the security reduction of algebraic elliptic curve shape over finite fields. Its keys are smaller than other key-exchange algorithms that are being used. ECDH is another widely used algorithm for key exchange and often with RSA to enhance its security. But unfortunately, this algorithm is also considered to be vulnerable against quantum-computers.

The RSA algorithm is the most popular and widely used public-key encryption algorithm used by a wide range of communications and authentication algorithms. The name comes from the surnames of the three creators of the algorithm, Ron Rivest, Adi Shamir, and Leonard Adleman. The algorithm was proposed in 1977 and it is based on prime factorization to securely generate the private and public keys used by the protocol (R.L. Rivest, 1977). Even though it is still widely used by different communications protocols, it is proven to be vulnerable against quantum computers in the future.

4.3. Block Encryption

Block encryption is a classical type of encryption where the algorithm converts a block of incoming data into cyphertext using a single key. This key is used for both encryption and decryption. There are a wide range of block encryptions to choose from, but the most used algorithms are DES and AES.

The DES algorithm is based on the Feistel function, but it is now considered to be vulnerable against brute force attacks and is no longer advised to be used (W. Diffie, 1975).

AES-256 is the standard symmetric key encryption used for both communications and secure storage. It also has a wide range of hardware support and is also proven to be secure against quantum computers.

The AES algorithm comes with a few different block cipher modes which further improve the security. These modes are used when encrypting multiple blocks of information. The most primitive and fastest mode is ECB. Here each block is individually encrypted and is left as it is. Even though it's fast, the algorithm lacks diffusion and thus certain patterns can be discerned from the final ciphertext making it a weak cipher mode.

Another popular block cipher mode is CBC. In this mode, the cypher text output of the previous block is fed into the inputs of the next block to diffuse the incoming data.

4.4. Networks

Networks are interconnected nodes or entities that participate in communication of information. And there are different types of nodes, types, topologies, protocols and communicating devices. Drones can use a wide range of communications protocols and mediums for D2D and D2GCS communications. The most used types are Wi-Fi, Bluetooth, RF, 4G LTE/ 5G, and protocols such as MAVLink.

Most of the communications protocols use the typical TCP/ IP stack (i.e., Wi-Fi, 4G LTE/ 5G). One reason for this is the use of devices such as Raspberry Pi and ESP32 that contain networking capabilities using Wi-Fi or contains the necessary processing capabilities to communicate using these technologies. They are also widely used standards on the internet thus making them a good option for drone communications.

Technologies like Bluetooth and MAVLink use a different communicating system compared to the TCP/ IP stack-based communications. Here, they are a lot lower level and direct compared to the other approaches.

The proposed system does not depend on the individual communications hardware. But it works on top of this and allows developers and hardware vendors to have as much freedom as possible when building communications hardware which use the protocol.

Another type of networking is ad hoc networks. Here all communicating parties participating in routing data packets to the destination. Compared to typical networking devices (end points, routers, switches, hubs, servers), these are easy to set up since once two or more devices are connected to the network, sending data packets between the source and destination can be done using the connected nodes or entities. FANETs are based on the same philosophy but instead of static communicating entities, the nodes are drones or UAVs (Muhammad Asghar Khan, 2017).

4.5. Benchmarking

5. Technological Review

5.1. Post-Quantum Algorithms

As mentioned in the previous sections, existing key exchange algorithms based on integer factorization is vulnerable against quantum computers in the future. To address this threat, NIST held a six-year competition to find the next generation quantum-secure cryptographic algorithms that can tackle this situation. In mid 2022, four algorithms were selected and announced as quantum secure. These algorithms are CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+.

5.2. Authentication

CRYSTALS-Dilithium is recommended by NIST because of its high efficiency compared to Falcon and SPHINCS+. This algorithm is based on the Fiat-Shamir with Aborts security reduction for its security against quantum computers. The authors of this algorithm recommend using it with another pre-quantum algorithm for better security and to use the Dilithium3 parameters for more than 128 bits worth of security against classical and quantum attacks.

Falcon is another algorithm selected by NIST to be quantum secure. NIST recommends using Dilithium along with Falcon to reduce the signature sizes for required applications. This algorithm also uses a lattice-based security reduction to be secure against attacks from quantum computers.

SPHINCS+ algorithm is noted to be a lot slower than the other algorithms and generates signatures bigger than the other two. It is recommended to be used as a backup algorithm for maximum security. The algorithm is based on a stateless hash-based scheme which is secure against quantum computers. Another reason for this algorithm to be used as a backup is because it uses a different math problem compared to the other two algorithms (which are lattice-based).

5.3. Key-Exchange

CRYSTALS-Kyber algorithm is based on the LWE problem. The LWE based encryption algorithms are proven to be secure against quantum computers (Regev, 2005). Kyber is proven to be faster to compute than other widely used quantum-secure algorithms such as NTRU-HRSS (Viet Ba Dang, 2023). Kyber also have a comparatively smaller key size compared to other algorithms. The developers of Kyber recommend using Kyber-768 which conservatively has 128 bits worth of security against all known classical and quantum attacks. They also recommend using classical algorithms such as ECDH along with Kyber for better performance and security.

5.4. Block Encryption

5.5. Network

6. Evaluation

7. Chapter Summary

8. References

Shor, P. W. (1994). *Algorithms for quantum computation: Discrete logarithms and factoring.* IEEE.

Shouquin Li, X. L. (2021). *Quantum-Resistant Lightweight Authentication and Key Agreement Protocol for Fog-Based Microgrids.* IEEE.

Muhammad Asghar Khan, A. S. (2017). *Flying Ad-Hoc Networks (FANETs): A Review of Communication Architectures, and Routing protocols.* IEEE.

Viet Ba Dang, K. M. (2023). *High-Speed Hardware Architectures and FPGA Benchmarking of CRYSTALS-Kyber, NTRU, and Saber.* IEEE.

Regev, O. (2005). *On lattices, learning with errors, random linear codes, and cryptography.* Symposium on the Theory of Computing.

W. Diffie, M. H. (1975). *Exhaustive Cryptanalysis of the NBS Data Encryption Standard.* COMPUTER.

Whitfield Diffie, M. E. (1976). *New Directions in Cryptography.* IEEE.

R.L. Rivest, A. S. (1977). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* ACM.