Literature Review

Table Of Contents

[1. Chapter Overview 3](#_Toc150172647)

[2. Concept Graph 4](#_Toc150172648)

[3. Problem domain 5](#_Toc150172649)

[3.1. Drone Communications 5](#_Toc150172650)

[3.2. Quantum Computers 5](#_Toc150172651)

[3.3. Flying Ad Hoc Networks 5](#_Toc150172652)

[3.4. Proposed Architecture 5](#_Toc150172653)

[4. Existing work 6](#_Toc150172654)

[4.1. Authentication 6](#_Toc150172655)

[4.1.1. Certificate-based Authentication 6](#_Toc150172656)

[4.1.2. Certificate-less Authentication 6](#_Toc150172657)

[4.2. Key Exchange 6](#_Toc150172658)

[4.3. Block Encryption 6](#_Toc150172659)

[4.4. Benchmarking 7](#_Toc150172660)

[5. Technological Review 8](#_Toc150172661)

[6. Evaluation 9](#_Toc150172662)

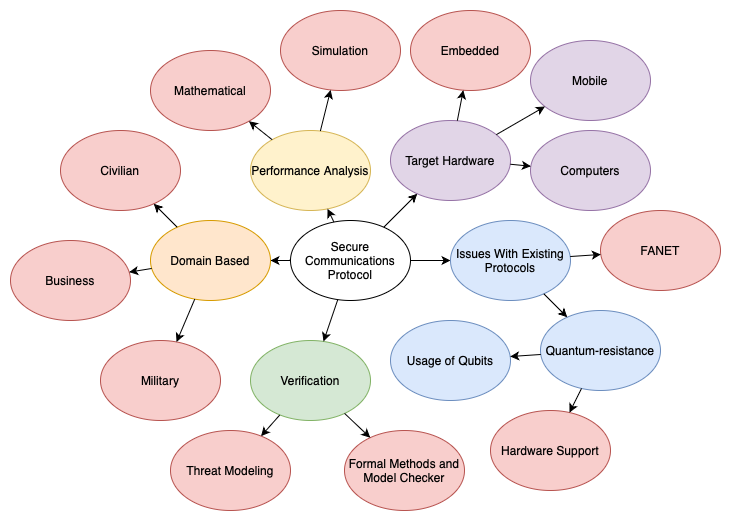
[7. Chapter Summary 10](#_Toc150172663)

[8. References 11](#_Toc150172664)

# 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.

# Concept Graph



*Figure n: Concept graph.*

# 

# Problem domain

## 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.

## 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.

## 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.

## Proposed Architecture

# Existing work

## 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.

### 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.

### 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.

## 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.

The most common approach to this problem is the use of public-key infrastructure.

## 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.

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 the Electronic Codebook mode (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 or Cipher Block Chaining. 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.

## Benchmarking

# 

# Technological Review

# 

# Evaluation

# 

# Chapter Summary

# References