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

Project Proposal

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. Project Proposal 4

1.1. Introduction 4

1.2. Problem Domain 4

1.2.1. Threat Posed by Quantum Computers 4

1.2.2. Networking of Drones 4

1.3. Problem Definition 4

1.3.1. Problem Statement 5

1.4. Motivation 5

1.5. Existing Work 5

1.6. Research Gap 8

1.7. Contribution to The Body of Knowledge 8

1.7.1. Technical Contribution 8

1.7.2. Domain Contribution 8

1.8. Research Challenge 8

1.9. Research Questions 9

1.10. Research Aim 9

1.11. Research Objectives 10

1.12. Project Scope 12

1.12.1. In-Scope 12

1.12.2. Out-of-Scope 12

1.12.3. Prototype Diagram of the System 13

2. Methodology 14

2.1. Research Methodology 14

2.2. Development Methodology 14

2.3. Design Methodology 14

2.4. Evaluation Methodology 15

3. Project Management Methodology 16

3.1. Project Deliverables 16

3.2. Gantt Chart 17

3.3. Resource Requirements 17

3.3.1. Hardware Requirements 17

3.3.2. Software Requirements 18

3.3.3. Skills Requirements 18

3.4. Risk Management 19

References 20

List of Figures

Figure 1: Prototype diagram of the proposed system (Self-Composed). 13
Figure 2: Gantt chart. 17

List of Tables

Table 1: Comparison of existing communications protocols. 8
Table 2: Research objectives. 11
Table 3: Research methodology 14
Table 4: Project deliverables. 16
Table 5: Hardware requirements and justifications. 18
Table 6: Software requirements and justifications. 18
Table 7: Risks and mitigation strategies. 19

List of Abbreviations

Abbreviation	**Description**
AES-256-CBC	Advanced Encryption Standard using 256-bit blocks with the Cipher Block Chaining mode of encryption
CA	Certificate Authority
CI/ CD	Constant Integration/ Constant Deployment
CPU	Central Processing Unit
D2D	Drone to Drone
D2GCS	Drone to Ground Control Station
DOS	Denial Of Service
ECDH	Elliptic Curve Diffie Hellman
FANET	Flying Ad hoc Network
GCS	Ground Control Station
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMACSHA1	Hash-based Message Authentication using the SHA1 algorithm
IDE	Integrated Development Environment
IoD	Internet of Drones
KEM	Key Exchange Mechanism

MITM	Man In The Middle
NTRU-HRSS-KEM	Lattice based public key encryption algorithm used for key exchange
RAM	Random Access Memory
RLWE	Ring Learning With Errors
SHA1	Secure Hash Algorithm 1
SHA3	Secure Hash Algorithm 3
SSADM	Structured System Analysis and Design Method
SSD	Solid State Drive

1. Project Proposal

1.1. Introduction

This proposal aims to introduce the reader briefly to the problem of existing drone communication protocols. It also contains the threat produced by quantum computers and a survey of currently used and existing literature on secure communication protocols in this domain. The problems identified by the review are then used to justify why the proposed protocol is necessary for the future of secure drone communications.

1.2. Problem Domain

1.2.1. Threat Posed by Quantum Computers

Prime factorisation is used as the basis of many existing cryptographic algorithms such as the ECDH and RSA (Diffie, W., M. Hellman, 1976; Rivest, R. L., et al, 1978). Peter Shor, an American mathematician developed a new quantum algorithm called Shor's algorithm in 1994. Out of the three proposed algorithms, the factoring algorithm can factor an integer in polynomic time (Shor, 1994). Using this algorithm, an ideal quantum computer will be able to generate the integer factors used by the ECDH and RSA algorithms thus rendering these cryptographic algorithms vulnerable in the future.

1.2.2. Networking of Drones

With the advancements in drone technologies, future trends require drones to be interconnected to perform complex tasks. For example, for a search and rescue mission, multiple drones will scan a wide area and relay the necessary information back to a ground control station. Another application would be for emergency response. In the case of a natural disaster and where existing communications have failed, drones could be used to set up a temporary emergency communications system that people can use to communicate with others and with authorities. For these types of applications, drones require capabilities to securely communicate between themselves and with the ground control station.

For these purposes, a FANET is very suitable since it is easy to set up and has relatively low operational costs. It also works on a decentralized structure rendering it ideal for challenging scenarios (Asghar, et al., 2017).

1.3. Problem Definition

With the advancements of quantum computers in the modern era, these devices will arrive at a critical point where they can break these previously secure cryptographic algorithms. Since these algorithms are already used by a wide range of existing and newly emerging communications protocols, it renders all these systems vulnerable to different adversaries in the future.

Drones communicating in a FANET comes with its own set of challenges. Everything from routing packets to setting up trust within the network needs to be addressed and is actively being researched.

1.3.1. Problem Statement

Quantum computers pose an incredible threat to drone communications soon and implementing standardized quantum-secure protocols have not been done before on a FANET.

1.4. Motivation

Despite the large amount of research conducted on this topic, much of the research revolves around using these legacy cryptographic systems to secure communications mostly between drones without a way of networking them.

1.5. Existing Work

Most of the research on this topic has been conducted with the goal of authentication in mind, IoT applications, general assessments and reviews of existing protocols. A complete study of how to set up a secure communications protocol with all the main stages, authentication, secure encryption and routing in a FANET has not been done. The following is a list of research papers containing information about various independent aspects of secure communication protocols and their limitations and contributions.

Citation	**Brief**	**Limitations**	**Contributions**
Yang, Chun-Wei, and Chia-Wei Tsai, 2020	This paper proposes two advanced semi-quantum secure direct communications protocols.	It does not support existing hardware and requires Qubits to operate. It is very costly to emulate the algorithm using legacy computing hardware.	Improvement of previous research and address several security vulnerabilities. A secure direct communications protocol for quantum users.
Jan, Saeed Ullah, et al., 2021	This research proposes a hash-based lightweight authentication protocol for IoD applications.	This paper only describes the use of the HMACSHA1 algorithm for the authentication phase of the communications	A lightweight and secure authentication protocol to set up secure communications between two drones or between a drone

		protocol and is not a complete communications protocol that describes secure message encryption.	and a GCS based on HMACSHA1.
Li, Lin, et al., 2022	The authors propose a certificate signing based on an Elliptic Curve multiple authentication scheme.	The paper only describes an authentication mechanism for drones. The base algorithm, Elliptic Curve cryptography has been proven to be vulnerable against quantum computers in the future.	The authors propose a cluster-based system for drones to network and share information along with a mechanism to choose one drone as the key node. This key node is then used for mutual authentication. It is also proven to be efficient compared to other protocols.
Khan, Muhammad Asghar, et al., 2017	This paper contains a review of FANET configurations and discusses existing routing protocols that can be used by drones.	It does not discuss how to set up a secure communications channel.	Outlines the best FANET configuration and several routing protocols that can be used.
Kumar, Adarsh, et al., 2022	This paper proposes a lightweight, security-enabled, distributed, software-defined network for traffic monitoring applications for drones.	The proposed algorithm uses an elliptic curve cryptosystem for the session authentication that is proven to be vulnerable against quantum computers in the future.	This proposed solution contains a new method to securely exchange keys when setting up a secure communications channel. The paper uses a software-defined network as the networking solution used by the drones to communicate among themselves and with the GCS.
Autry, Christopher	This research paper proposes a decentralized	The proposed protocol is not used	This protocol uses the SHA3, AES-256-

Patrick, et al., 2022	secure quantum-resistant communications protocol that uses the NTRU-HRSS-KEM as the KEM.	and/ or demonstrated to be used in a FANET configuration.	CBC, NTRU-HRSS-KEM and HMAC algorithms to set up secure communications and to securely communicate information between drones and GCS.
Ko, Yongho, et al., 2021	This research proposes a secure communications protocol with two sub-protocols for D2D and D2GCS communications.	The proposed protocol uses ECDH as the KEM which is proven to be vulnerable against quantum computers in the future.	The authors propose a secure communications protocol with two sub-protocols that are to be used in D2D and D2GCS configurations. They describe 4 ways in which the protocol can be used in real-life situations.
Mishra, Dheerendra, et al., 2023	The authors propose a quantum-safe secure and authenticated communications protocol based on the RLWE problem on lattices.	The proposed protocol only contains the authentication phase of the communications stack and does not contain information about the network structure to be used and the full network stack.	The authors propose a custom encryption algorithm based on the RLWE problem on lattices for the key exchange phase. The paper also provides a security assessment and performance of the proposed protocol.
Lu, Shouqin, and Xiangxue Li., 2021	In this paper the authors design a lightweight quantum-resistant key agreement protocol for microgrids.	The proposed algorithm does not specify how to work on a FANET and is designed for IoT applications. Since the authors propose a new algorithm that is not standardized NIST or any other standards authority, adding hardware	The authors of this paper propose a custom quantum-resistant cryptographic algorithm for the authentication and key agreement phase based on the Learning Parity with Noise problem. The authors also contain information about the performance of

		support for this algorithm is limited.	this newly proposed algorithm.

Table 1: Comparison of existing communications protocols.

1.6. Research Gap

Existing research on secure communications protocol describes individual phases of the process. Most of the research papers and proposed protocols containing the full network stack lack quantum security. With this research, the identified research gap is a complete and comprehensive quantum-secure communication protocol including the whole network stack apart from the application and physical layers.

1.7. Contribution to The Body of Knowledge

Based on the identified research gap, the author wishes to contribute immensely to both the technical and research domain.

1.7.1. Technical Contribution

Secure communications between drones and GCS are one of the most important aspects of networked operations. Since quantum computers will be able to break the existing secure communications, target hardware such as drones will be susceptible to these types of attacks because of the lack of performance they offer for complex algorithms. To avoid this issue, the author proposes a secure communications protocol that encompasses a quantum-resistant cryptographic algorithm for the authentication and key agreement phase designed to run in a FANET.

1.7.2. Domain Contribution

This research will contribute to secure communications for IoD applications. Users will be able to use a framework to set up secure communications between drones and GCS. Practical applications of these types of communications range from search and rescue operations where multiple drones are used, to reconnaissance missions carried out by a military, or any type of communications where D2D or D2GCS communications, or both are required. With standardized quantum-resistant algorithms, developers will be able to add hardware support for these systems instead of using custom algorithms based on security reductions.

1.8. Research Challenge

Secure communications for drones are an active field of research because it’s an important piece of technology for a wide range of applications. From the preliminary research, there will be plenty of challenges to be addressed because most of the literature and existing implementations of secure communications either use legacy systems, use custom quantum-resistant algorithms for the KEM, or do not contain information on how to integrate the system with a FANET. The following list contains a list of challenges to be faced during the research process of this project.

- Researching and finding the best method of authentication with performance and configuration in mind.
- Finding the best method of securely exchanging the keys required for message encryption.
- Identifying the best mode of block encryption to use that provides the best of both worlds, performance vs. security.
- Designing and developing a framework that runs on multiple platforms, including embedded systems that developers can easily integrate and use.
- Optimizing the protocol to use less power and to do the computations in an efficient manner using available intrinsic and dedicated instructions (i.e.: AES instructions available in most hardware and platforms).

1.9. Research Questions

1. What is the newly standardized quantum-secure encryption algorithms and where do they fit in a communication protocol?
2. How can these algorithms run on limited hardware commonly used or can be used by drones?
3. How can these protocols work on a FANET?

1.10. Research Aim

This research aims to design and implement a framework that contains a secure communications protocol for IoD applications that uses the newly standardized post-quantum cryptographic algorithm to combat the threats posed by quantum computers in the future.

The protocol will contain an authentication and key exchange phase, along with a secure bulk encryption phase where two or more communicating parties can securely communicate (also known as the secure channel). It will also define the packet structure, how to identify drones and GCS uniquely and how to send data through them with a routing protocol.

This proposed protocol will be designed into a framework that can be used by multiple platforms where the users can integrate with their applications to communicate with the drones and GCS securely (D2D and D2GCS). The protocol and the design of the framework will be properly researched before development and will be available as free and open source for anyone to use and review. A test application with the framework will demonstrate how the protocol can be used in real-life applications.

1.11. Research Objectives

Research Objectives	**Description**	**Learning Outcome**
Problem identification	The objective of is to conduct a thorough investigation of the existing literature and protocols used in the industry and identify gaps that needs to be resolved. ● **RO1**: Research the secure communications of drones domain and identify the issues encountered. ● **RO2**: Research on how to overcome the issues identified by RO1. ● **RO3**: Research why the existing secure communication protocols do not address the above-identified problems. ● **RO4**: Research because the existing quantum-secure communications protocols use their own algorithm as opposed to using standardised algorithms.	LO1, LO2, LO4, LO6
Literature review	The objective is to carry out extensive research on available literature to achieve the required outcomes. ● **RO1**: Research and analyse the existing secure communications protocols for drones. ● **RO2**: Research on different cryptographic techniques used to secure communications against quantum computers. ● **RO3**: Research on the existing quantum-secure communications protocols. ● **RO4**: Research on existing quantum-secure communications protocols designed for drones. ● **RO5**: Research on how the existing communications protocols network with drones and how they validate certificates. ● **RO6**: Research on how the existing drone communications protocols work on different applications. ● **RO7**: Elaborate on how quantum computers pose a threat to secure drone communications and their impacts.	LO1, LO3, LO4, LO5, LO6
Research design	Research and design a framework to tackle the issues identified and which can be deployed in real-life applications. ● **RO1**: Choose a quantum-secure key exchange algorithm that can run on drones. ● **RO2**: Design the secure communications protocol which can run on target hardware with limited capabilities.	LO2, LO3, LO4, LO5

	● **RO3**: Design a system to validate certificates automatically and authenticate other drones in the network. ● **RO4**: Design a complete networking solution with all the components. ● **RO5**: Design a framework which can be used by desktop and embedded systems which implement the communications protocol. ● **RO6**: Design a desktop application to demonstrate how the protocol works. ● **RO7**: Design the embedded hardware to test the system.	
Implementation	Implement an efficient framework and test system to setup secure communications between drones and to test the system. ● **RO1**: Develop the authentication algorithm with quantum-secure encryption algorithms. ● **RO2**: Develop the message encryption algorithm with block encryption algorithms. ● **RO3**: Develop a routing protocol used for packet routing. ● **RO4**: Develop the whole networking stack by bringing all the other components together. ● **RO5**: Develop the desktop application for testing. ● **RO6**: Develop the embedded application for testing.	LO2, LO3, LO4, LO5, LO7
Testing and evaluation	The objective is to test and evaluate the proposed framework thoroughly. ● **RO1**: Test and evaluate the individual components of the framework (unit testing, integration testing). ● **RO2**: Benchmark, test and evaluate the framework on both desktop and target hardware. ● **RO3**: Produce a detailed evaluation and report for the academic and research community.	LO5, LO6, LO7
Publish findings	Publish the findings of this research and contribute to the body of knowledge. ● **RO1**: Validate the proposed solution to the identified research gap. ● **RO2**: Specify the limitations and other factors for future studies to address. ● **RO3**: Publish a well-structured document with the findings and contribute to the body of knowledge.	LO4, LO5, LO7, LO8

Table 2: Research objectives.

1.12. Project Scope

1.12.1. In-Scope

The following is the list of parts that this project will cover.

- A secure communications protocol that uses legacy and quantum-resistant cryptographic algorithms.
- A system to identify trustworthy drones and maintain a chain of trust.
- A library that can be used by drones and desktop machines to communicate with drones using the proposed protocol securely.
- A review of routing protocols that this protocol can use.
- Performance review of the proposed protocol in a few popular target hardware systems.

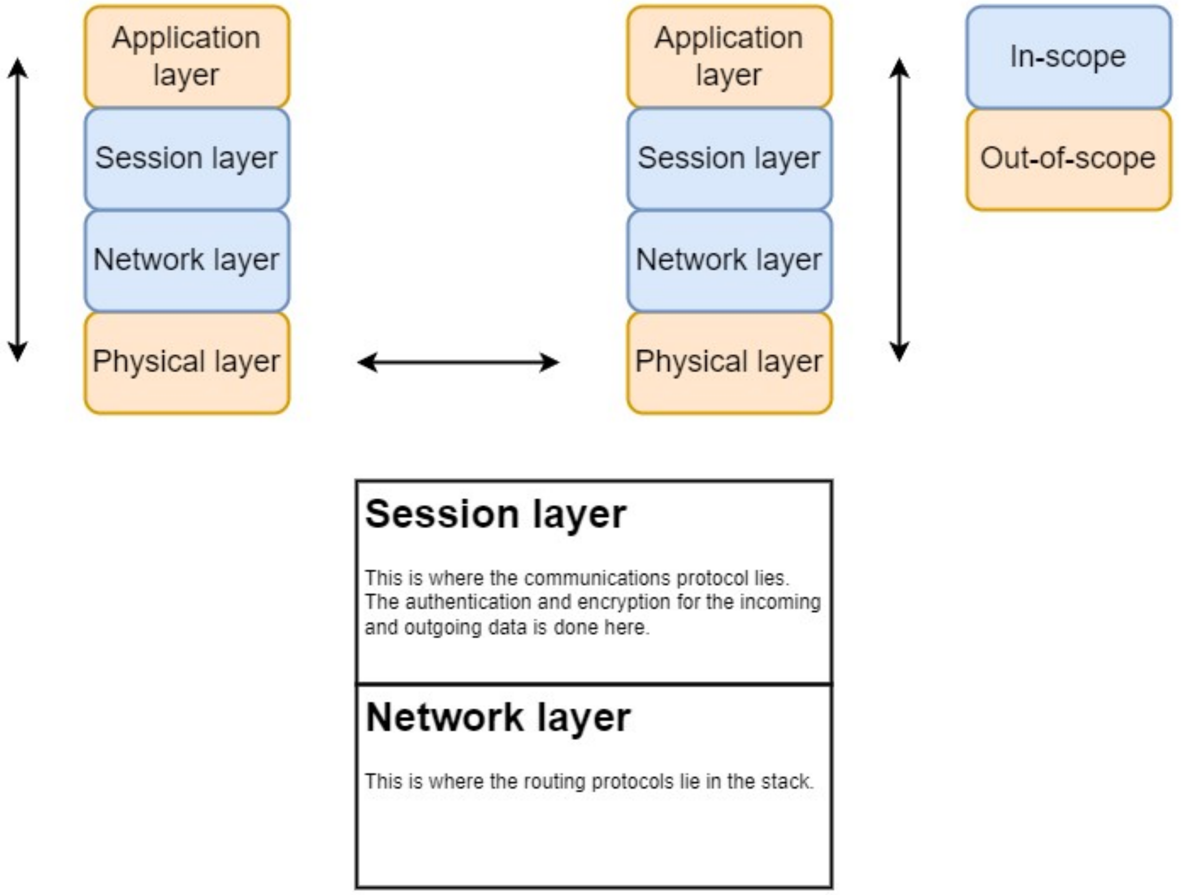
1.12.2. Out-of-Scope

The following is the list of items that this project will not cover.

- The proposed protocol can use physical communication algorithms and protocols.
- An application to communicate with drones with a GUI.
- A complete survey of hardware that could run the proposed protocol and data link that supports the system.
- Application layer protocols communicate with other components of the drone and GCS.

1.12.3. Prototype Diagram of the System

(Samaranayake, Draw.IO, 2023)



Session layer

This is where the communications protocol lies. The authentication and encryption for the incoming and outgoing data is done here.

Network layer

This is where the routing protocols lie in the stack.

Figure 1: Prototype diagram of the proposed system (Self-Composed).

2. Methodology

2.1. Research Methodology

The following table contains information about the various research methodologies that are needed for a successful research project.

Philosophy	This research will utilize **pragmatism** and **inductive reasoning** since it gives a broader perspective, specifically within the problem-solving aspects of the study.
Approach	**The Deductive** method of research is used in this study as the proposed solution contains components which are yet to be tested with modern hardware, or currently do not contain capabilities to be tested.
Strategy	**Experiments** and **research analysis** will be conducted for this project with existing literature.
Choice	**Quantitative** research is used in this project. This is because both performance metrics and security reductions of the encryption algorithms in terms of time taken to break the cypher are taken into consideration.
Time Horizon	Cross-sectional research is chosen as the time horizon since it does not require data to be gathered over a long period of time.

Table 3: Research methodology.

2.2. Development Methodology

Considering all the other options, the author has selected the prototype development methodology for this project. The reason for this decision is that the framework can be considered a critical piece of software in an application and requires good testing before being implemented and released. Once implemented, an agile development model will be used to add additional features and to fix any bugs and security issues with the framework.

2.3. Design Methodology

For this project, the author will be using the SSADM model for the design methodology. Using this method, the author can better plan how the system should behave and add optimizations to different aspects of the framework and for platforms with limited capabilities. It also enabled the author to have better control over the project management and provide secure and high-quality code.

2.4. Evaluation Methodology

The author identifies a couple of the most important points of measurement: security and performance on limited hardware. Because of this, a security analysis of the system is considered (both operational and cryptographic) as well as a performance on not only desktop usage of the framework but also on target hardware with limited computing power. In terms of cryptographic security analysis, the protocol will be evaluated to be safe against several attacks such as MITM attacks, DOS attacks, and CA compromises.

3. Project Management Methodology

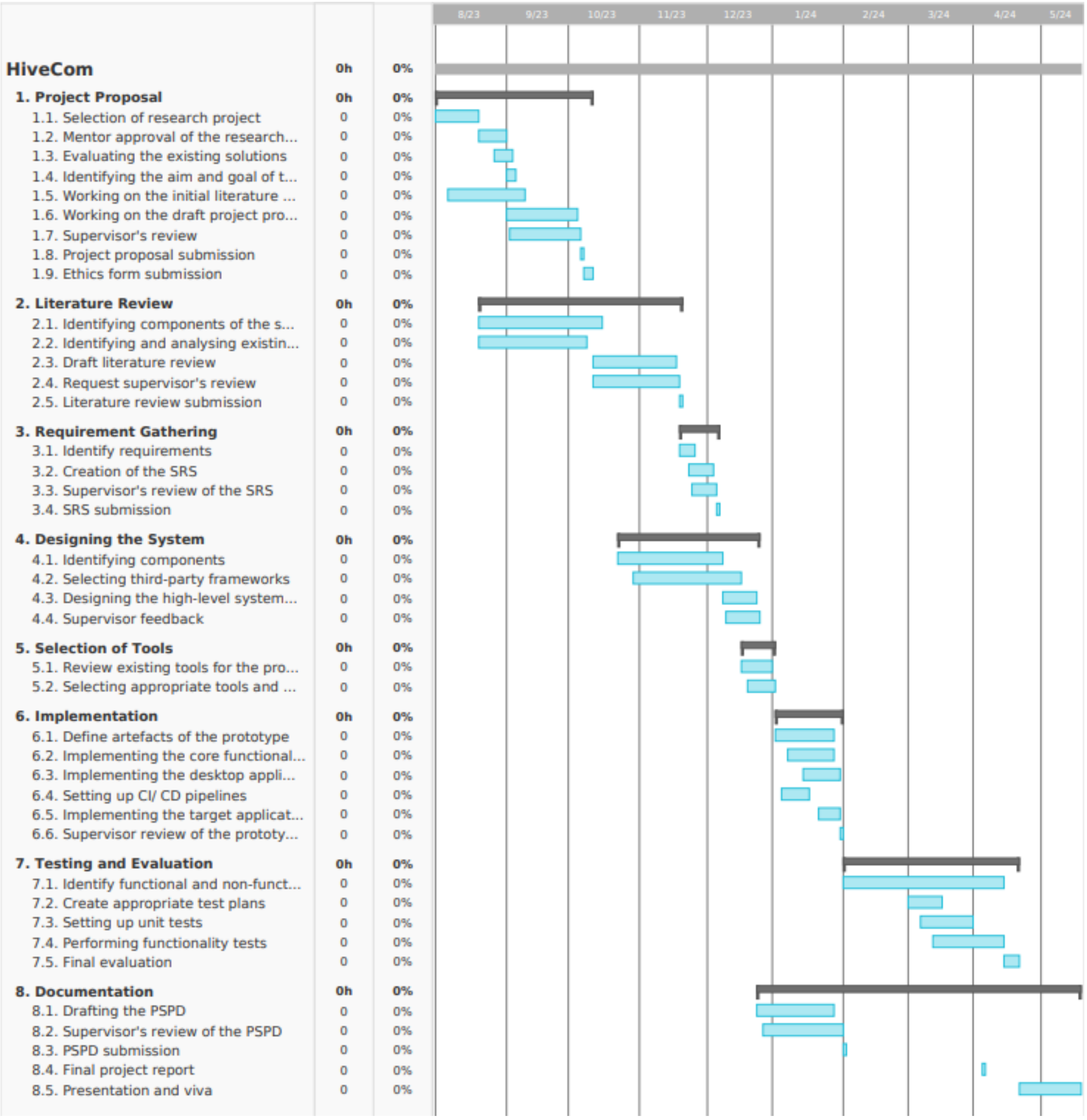
3.1. Project Deliverables

Project Deliverable	**Tentative Submission Date**
Project Proposal	5th October 2023
Review Paper	20th November 2023
Software Requirement Specification	6th December 2023
System Design Document	15th January 2024
Prototype	1st February 2024
Thesis	15th March 2024
Project Research Paper	4th April 2024

Table 4: Project deliverables.

3.2. Gantt Chart

(Samaranayake, Team Gantt, 2023)



HiveCom	0h	0%
1. Project Proposal	0h	0%
1.1. Selection of research project	0	0%
1.2. Mentor approval of the research...	0	0%
1.3. Evaluating the existing solutions	0	0%
1.4. Identifying the aim and goal of t...	0	0%
1.5. Working on the initial literature ...	0	0%
1.6. Working on the draft project pro...	0	0%
1.7. Supervisor's review	0	0%
1.8. Project proposal submission	0	0%
1.9. Ethics form submission	0	0%
2. Literature Review	0h	0%
2.1. Identifying components of the s...	0	0%
2.2. Identifying and analysing existin...	0	0%
2.3. Draft literature review	0	0%
2.4. Request supervisor's review	0	0%
2.5. Literature review submission	0	0%
3. Requirement Gathering	0h	0%
3.1. Identify requirements	0	0%
3.2. Creation of the SRS	0	0%
3.3. Supervisor's review of the SRS	0	0%
3.4. SRS submission	0	0%
4. Designing the System	0h	0%
4.1. Identifying components	0	0%
4.2. Selecting third-party frameworks	0	0%
4.3. Designing the high-level system...	0	0%
4.4. Supervisor feedback	0	0%
5. Selection of Tools	0h	0%
5.1. Review existing tools for the pro...	0	0%
5.2. Selecting appropriate tools and ...	0	0%
6. Implementation	0h	0%
6.1. Define artefacts of the prototype	0	0%
6.2. Implementing the core functional...	0	0%
6.3. Implementing the desktop appli...	0	0%
6.4. Setting up CI/ CD pipelines	0	0%
6.5. Implementing the target applicat...	0	0%
6.6. Supervisor review of the prototy...	0	0%
7. Testing and Evaluation	0h	0%
7.1. Identify functional and non-funct...	0	0%
7.2. Create appropriate test plans	0	0%
7.3. Setting up unit tests	0	0%
7.4. Performing functionality tests	0	0%
7.5. Final evaluation	0	0%
8. Documentation	0h	0%
8.1. Drafting the PSPD	0	0%
8.2. Supervisor's review of the PSPD	0	0%
8.3. PSPD submission	0	0%
8.4. Final project report	0	0%
8.5. Presentation and viva	0	0%

Figure 2: Gantt chart.

3.3. Resource Requirements

3.3.1. Hardware Requirements

Requirement	**Justification**
AMD Ryzen 5 3600 6-core processor or Apple M2 Pro processor	Required CPU specifications for cross-platform development of the framework.
16 - 32 GB RAM	Optimum RAM for the IDEs used to develop the framework.

10 GB or more HDD or SSD space	The space required by the repository to build the required testing binaries and libraries.
ESP32 development board	Target hardware to test and benchmark the framework in real-life scenarios.
NRF24L01+PA+LNA wireless transceiver	Test and benchmark secure wireless communications with the framework.

Table 5: Hardware requirements and justifications.

3.3.2. Software Requirements

Requirement	**Justification**
Operating system (Windows 11, MacOS, Linux, FreeRTOS)	The operating system is required for the development and testing of the framework. Since the framework is required to have cross-platform capabilities all the major operating systems are used to make sure the framework works on all these platforms. FreeRTOS is used by the ESP32 development board and is used to test and benchmark the framework in target platforms.
Visual Studio, Visual Studio Code, and XCode	Development IDEs are used to develop, test and build the framework.
Google Docs, Microsoft Word	For documenting and keeping reports of the framework.
GitHub	Version control system used by the framework.
Botan	C/ C++ cryptographic library that supports both legacy and post-quantum cryptographic algorithms such as Kyber.
Semantic Scholar	To find and keep track of all the research papers related to this project.
PlatformIO	Development platform to develop, test and deploy embedded applications.

Table 6: Software requirements and justifications.

3.3.3. Skills Requirements

- Knowledge of existing cryptographic algorithms and protocols used for network communications.
- Knowledge of authentication and KEM algorithms currently used.
- Knowledge and skills in cross-platform application and framework development.
- Knowledge of evaluating the developed framework in terms of both security and performance.

- Knowledge and skills in developing applications for target hardware for testing and evaluation.

3.4. Risk Management

The development of a framework, targeted to run on multiple platforms which also requires a great deal of performance comes with a set of risks that needs to be addressed. The table below presents the risks identified and mitigation strategies to overcome these.

Risks	**Severity**	**Frequency**	**Mitigation plan**
Target hardware does not have the required capabilities to run the proposed solution.	4	2	Optimize the solution with platform-specific instructions and opt to use better and more powerful hardware.
Inability to conduct proper benchmarking and testing on desktop and target hardware.	3	3	Set up and maintain a proper testing strategy and CI/ CD pipelines to test the individual components of the system. Set up and maintain a benchmarking strategy for each prototype.
Corruption of data and introduction of bugs to the framework.	2	4	Use a proper version control system such as GitHub, and to use CI/ CD pipelines to validate tests to ensure bugs are not introduced when developing the framework.
Cross-platform development and testing.	3	3	Have supported operating systems installed in the workstation and use CI/ CD pipelines to test and ensure the framework compiles and runs fine on different platforms.
Inability to submit the required documents and materials within the deadlines.	3	2	Organize and use reminders to prepare the necessary documents before the deadlines to ensure the required submissions are ready before the deadline date.

Table 7: Risks and mitigation strategies.

References

Diffie, H. (1976). *New Directions in Cryptography.* IEEE.

Rivest, S. A. (1978). *A method for obtaining digital signatures and public-key cryptosystems.* ACM.

Shor. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring.* IEEE.

Khan, M. A. (2017). *Flying Ad-Hoc Networks (FANETs): A Review of Communication Architectures, and Routing Protocols.* IEEE.

Yang, T. (2020). *Advanced Semi-Quantum Secure Direct Communication Protocol Based on Bell States against Flip Attack.*

Jan, Q. K. (2021). *Design and Analysis of Lightweight Authentication Protocol for Securing IoD.* IEEE.

Li, L. W. (2022). *CSECMAS: An Efficient and Secure Certificate Signing Based Elliptic Curve Multiple Authentication Scheme for Drone Communication Networks.* MDPI.

Kumar, Y. G. (2022). *A secure drone-to-drone communication and software defined drone network-enabled traffic monitoring system.* Elsevier B.V.

Autry, H. M. (2022). *Fully Decentralized Post-Quantum Resistant Authentication, Encryption Protocol with Full Data Interoperability Universally Deployable in Any Network Environment.* IEEE.

Ko, K. D. (2021). *Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone.* MDPI.

Singh, R. P. (2023). *Quantum-Safe Secure and Authorized Communication Protocol for Internet of Drones'.* IEEE.

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