MANIPAL UNIVERSITY
JAIPUR

DEPARTMENT OF COMPUTER APPLICATIONS

Major Project

Project - Synopsis

MCA - IV Sem

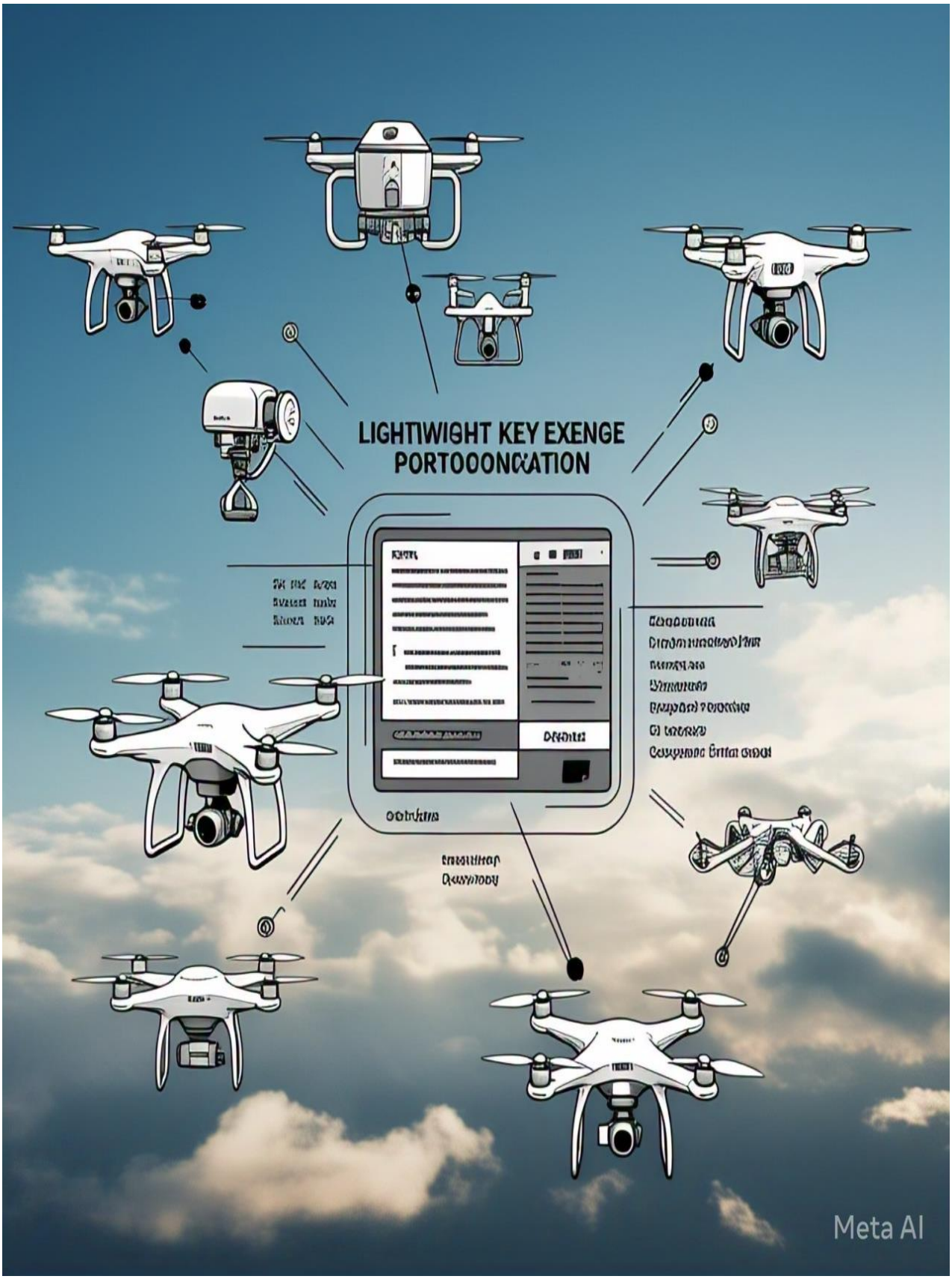
Subject Code: CA7270

Submitted By

Hrisikesh Roy

Faculty Coordinator

Dr. Pragya Vaishnav


LIGHTIWIGHT KEY EXENGE
PORTOOONCATION
Meta AI

Project Title:

Lightweight Key Exchange Protocol for Secure Drone Communication

Team Details

- **Name:** Hrisikesh Roy
- **Registration No.:** 23FS20MCA00049
- **Course:** MCA
- **Semester:** IV
- **Section** A

Project Guide

Guide:Dr. Dr. Pragya Vaishnav(internal)

Dr .Ummer Iqbal Khan (Scientist-D)(External)

INDEX

Sl no	Chapter Title	Page no
1	Abstract	5
2	Introduction	6
3	Technology Used	7
4	Problem Statement	8
5	Objectives	9
6	Proposed Methodology	10
7	Diagram	11
8	Table: Common security Attack in drone communication	12
9	Conclusion	13

Abstract

The rapid growth in the use of unmanned aerial vehicles (UAVs), commonly known as drones, in both civilian and military domains has underscored the critical need for secure, efficient communication protocols. Traditional cryptographic methods often impose significant computational overhead and energy consumption, making them less suitable for resource-constrained drone environments. This project aims to design, develop, and evaluate a lightweight key exchange protocol that maintains robust security while minimizing computational and energy burdens. By leveraging efficient cryptographic primitives and optimizing protocol design, the proposed solution seeks to provide secure authentication and confidentiality in drone communication, ensuring real-time responsiveness and enhanced operational reliability.

1. Introduction

Unmanned aerial vehicles (UAVs) are widely used in various applications, including military operations and commercial use cases such as package delivery and agricultural monitoring. The application of UAVs in critical systems necessitates robust security measures to prevent unauthorized access, data breaches, and malicious attacks. Drone communication typically relies on wireless media to transmit real-time sensor data and commands, making it vulnerable to various security risks. For instance:

- **Eavesdropping:** An attacker may intercept unencrypted communications between the UAV and the Ground Control Station (GCS) .
- **Spoofing:** An attacker can impersonate network nodes to disrupt communication.
- **Man-in-the-Middle Attacks:** Interception and modification of data can occur without the knowledge of either party.
- **Denial-of-Service (DoS) Attacks:** The communication channel can be overwhelmed with unsolicited messages.

These vulnerabilities necessitate the incorporation of strong security primitives in UAV communication systems. Key measures include ensuring confidentiality through encryption, mutual authentication to prevent impersonation, data integrity to protect against tampering, and non-repudiation for accountability

. Currently, many existing protocols, such as MAVLink (a commonly used protocol), do not inherently provide robust security features.

2. Technology Used

- MAVLink Protocol and Crystals-Kyber
- AES(symmetric Encryption)
- Elliptical Curve Cryptography (ECC)
- Avispa & Crystals- Delithum
- Scythe
- Flight Controller
- Network Sniffer
- Elliptic Curve Diffie-Hellman (ECDH)

3. Problem Statement

While robust key exchange mechanisms exist, many are either too resource-intensive or not optimized for the specific challenges of drone communication networks. The primary problem addressed by this project is:

How can we design and implement a lightweight key exchange protocol that provides strong security guarantees and is well-suited to the constrained computational and energy environments of modern drones?

Key challenges include:

- Balancing security and efficiency.
- Minimizing latency during key establishment.
- Ensuring scalability and adaptability to changing network topologies.

Diagram :

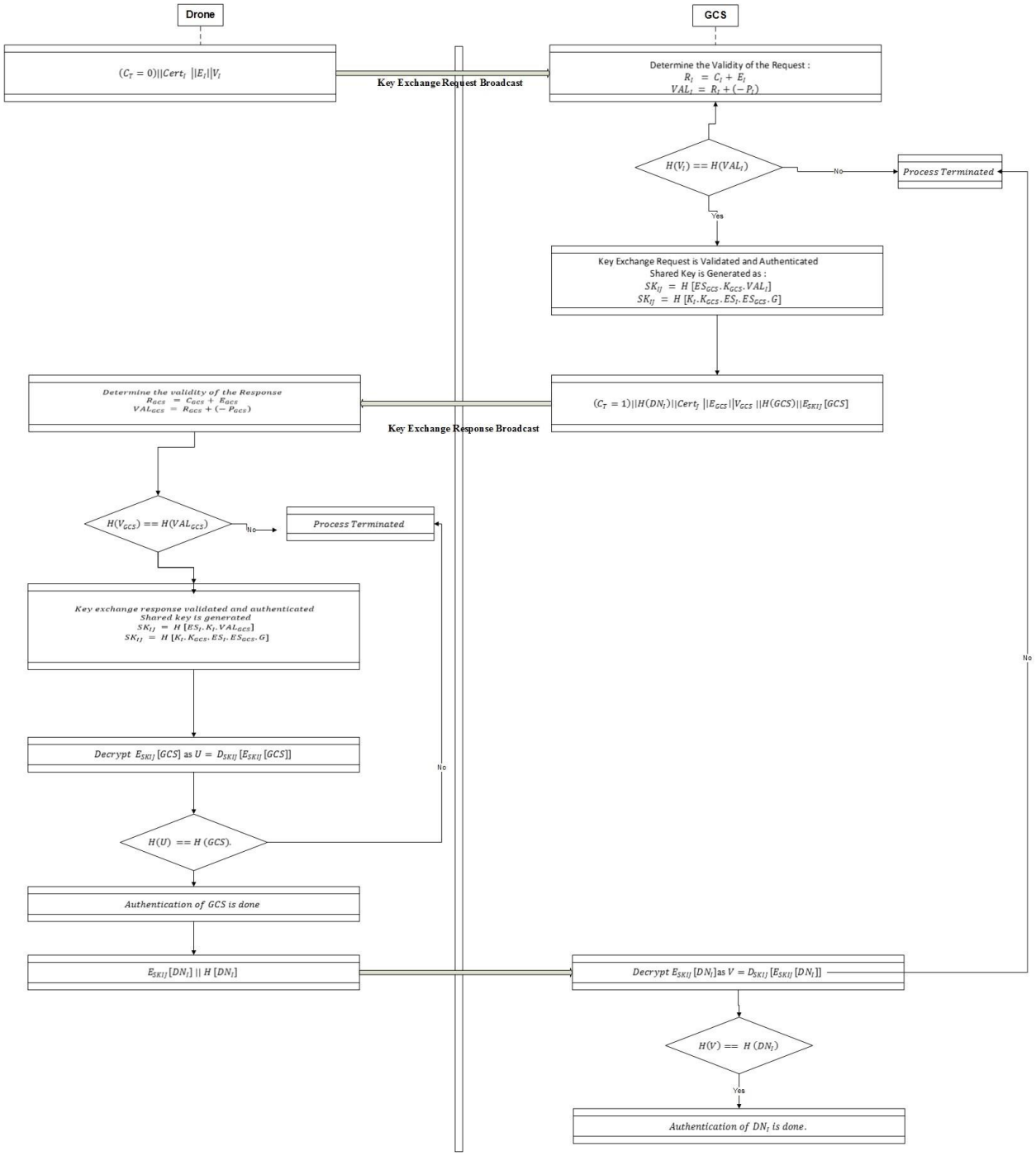


Figure 1

4. Objectives

1. **Design and Develop:**
   Create a key exchange protocol that is lightweight yet secure, optimized for the constraints of drone communication systems.
2. **Analyze Security:**
   Evaluate the protocol against common attacks (e.g., man-in-the-middle, replay attacks) and ensure compliance with security best practices.
3. **Performance Evaluation:**
   Benchmark the protocol's performance in terms of computational load, energy consumption, and latency using simulation and/or real-world drone testbeds.
4. **Integration:**
   Demonstrate how the protocol can be integrated into existing drone communication architectures.
5. **Documentation:**
   Provide comprehensive documentation and guidelines for implementation in real-world scenarios.

5. Proposed Methodology

5.1 Protocol Design

- **Cryptographic Foundations:**
  Evaluate and select lightweight cryptographic primitives (e.g., using optimized ECC parameters) to balance security and efficiency.
- **Protocol Structure:**
  Develop a protocol flow that minimizes handshake rounds and computational overhead. The design should incorporate:
  - Mutual authentication.
  - Session key derivation.
  - Forward secrecy.

5.2 Security Analysis

- **Threat Modeling:**
  Identify potential attack vectors (e.g., man-in-the-middle, replay attacks) and design countermeasures.
- **Formal Verification:**
  Use formal methods and simulation tools to verify the protocol's security properties.
- **Comparative Analysis:**
  Benchmark against standard protocols to highlight improvements in efficiency and energy consumption.

5.3 Simulation and Testing

- **Simulation Environment:**
  Utilize network simulation tools (e.g., NS-3, OMNeT++) to model drone communication scenarios under varying conditions.
- **Prototype Development:**
  Implement the protocol on a representative drone platform or embedded system (e.g., Raspberry Pi, Arduino) to assess real-world performance.
- **Performance Metrics:**
  Measure latency, throughput, energy consumption, and resilience to attacks.

5.4 Integration and Validation

- **System Integration:**
  Ensure the protocol can be seamlessly integrated with existing drone communication frameworks.
- **Field Testing:**
  Conduct controlled field tests to validate protocol performance in real operational environments.

6. Table: Common Security Attacks in Drone Communication

S.No	Attack	Description
1	**Man-in-the-Middle Attack**	An adversary intercepts drone communication and may manipulate, spoof, or alter the messages, posing a significant threat to UAV operations.
2	**Denial of Service Attack**	The communication nodes are overwhelmed with unsolicited messages, rendering the network inoperative or causing significant delays.
3	**Packet Injection Attack**	Malicious data packets are injected into the communication stream, potentially altering commands or data and compromising the mission objectives.
4	**Replay Attacks**	Valid data or control signals are captured and replayed, allowing unauthorized commands to be executed or outdated information to be processed.

7. Conclusion

This project aims to bridge the gap between security and efficiency in drone communication by developing a lightweight key exchange protocol tailored for constrained environments. By focusing on optimized cryptographic techniques and rigorous performance evaluation, the project is poised to contribute significantly to the field of UAV security. The anticipated outcomes include enhanced protection against prevalent cyber-attacks, improved energy efficiency, and minimized latency, ultimately offering a robust solution for secure drone operations in critical sectors.