Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

PKI-Enabled Authentication and Encryption for Enhanced Drone Communication

Mr. Pavan Jadhav, Mr. Shrikrishna S Chippalkatti, Dr. Mohammed Misbahuddin, and Dr. S D Sudarsan
Centre for Development of Advanced Computing (C-DAC),
Bengaluru, Karnataka- 560100, India

C-DAC

https://pkiindia.in

Social Media /pkiindia

IEEE BANGALORE SECTION

Overview

- Drones' widespread use highlights the need for secure communication.
- Communication channels are vulnerable to eavesdropping and tampering.
- PKI integration offers robust authentication and encryption for drones.
- Strong encryption ensures data integrity and confidentiality in drone networks.
- Lightweight cryptographic solutions are crucial for resource-constrained drones.

Introduction

Context

- Drones are widely used in fields like military, agriculture, and delivery etc.
- Growing drone usage demands secure communication with ground stations
- Ensuring communication security prevents data breaches and unauthorized access.

Problem Statement

- Open wireless channels pose significant security risks for drones
- Unsecured paths enable unauthorized access and data interception
- Vulnerabilities can compromise mission integrity and sensitive data

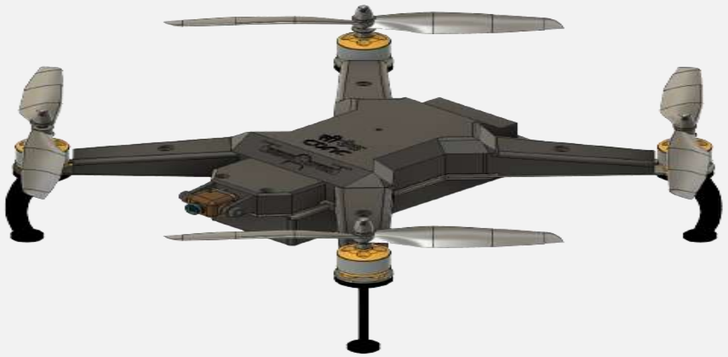
Objective

- PKI Integration: Integrate PKI into drone systems
- Secure Channels: Use PKI for secure communication
- Address Issues: Solve authentication and encryption problems with PKI

Comparative Analysis of Existing Security Primitives

Feature	Existing Security Primitives	Proposed Security Primitives with PKI Ecosystem
Authentication Method	Basic authentication or pre-shared keys	Public Key Infrastructure with ECC-based certificates
Encryption Technique	Symmetric encryption (e.g., AES)	Asymmetric encryption
Security Level	Moderate, vulnerable to key compromise	High, robust against key compromise due to ECC security
Key Management	Manual key distribution	Automated through PKI, with secure key generation and distribution
Communication Latency	Lower, due to simpler encryption	Slightly higher, due to complex ECC operations
Scalability	Limited, with manual key updates required	Highly scalable, automated key management in PKI
Resistance to Attacks	Susceptible to replay and man-in-the-middle attacks	Strong resistance to attacks, especially against replay and MITM
Certificate Revocation	Not applicable, no certificate usage	Supported through PKI, allowing for real-time certificate revocation
Operational Complexity	Simpler, fewer cryptographic operations	More complex, involves certificate management and ECC computations
Regulatory Compliance	Basic, may not meet stringent security standards	Compliant with modern security standards and regulations
Future-Proofing	Limited, may require upgrades for evolving threats	High, ECC and PKI provide long-term security with adaptability

Methodology



INDUSCOPTER

PKI Framework

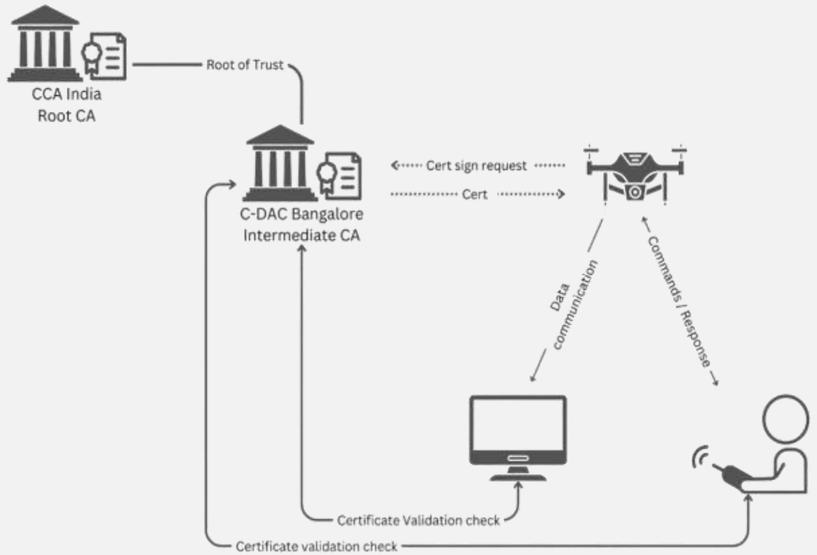
- Trusted CA: Use a Certificate Authority (CA) to issue digital certificates.
- Public Keys: Certificates contain public keys for authentication.
- Secure Channels: Enable secure communication between drones and ground stations.
- Hierarchical Structure: Employ a hierarchical PKI for secure and reliable authentication.
- Scalable Security: Ensure scalability in the authentication system for various deployment sizes.

Methodology

Encryption Techniques

- ECC Selection: Use Elliptic Curve Cryptography (ECC) for efficient encryption on resource-constrained drones.
- Lightweight Ciphers: Explore lightweight block ciphers like PRESENT and SIMON for optimized encryption.
- Resource Efficiency: Choose ECC for its low computational requirements.
- Data Protection: Protect data over insecure communication channels with optimized encryption methods.

Methodology



Implementation

- Microcontroller: Implement PKI using STM32 Based microcontroller
- Cryptographic Accelerator: Utilize dedicated cryptographic hardware for efficient algorithms
- Secure Communication: Ensure secure data transmission with the drone's communication system
- Integration: Seamlessly integrate PKI with existing drone communication systems for robust security

Challenges and Considerations in Implementing Drone PKI

- Implementing PKI for drone communication presents several challenges and considerations, including the need for robust security infrastructure, efficient key management, and compliance with regulatory requirements.
  - Scalability
  - Interoperability
  - Cost and Complexity
  - Performance

Conclusion and Future Outlook

- The integration of PKI with drone fleet management systems, along with the development of industry standards and regulatory compliance, will play a key role in shaping the future of secure drone communication.
- We are currently working on the project and plan to add cost and power considerations as a part project.

THANK YOU