CERIAS
The Center for Education and Research in Information Assurance and Security

Securing Aviation Communications: A Network-Based Approach

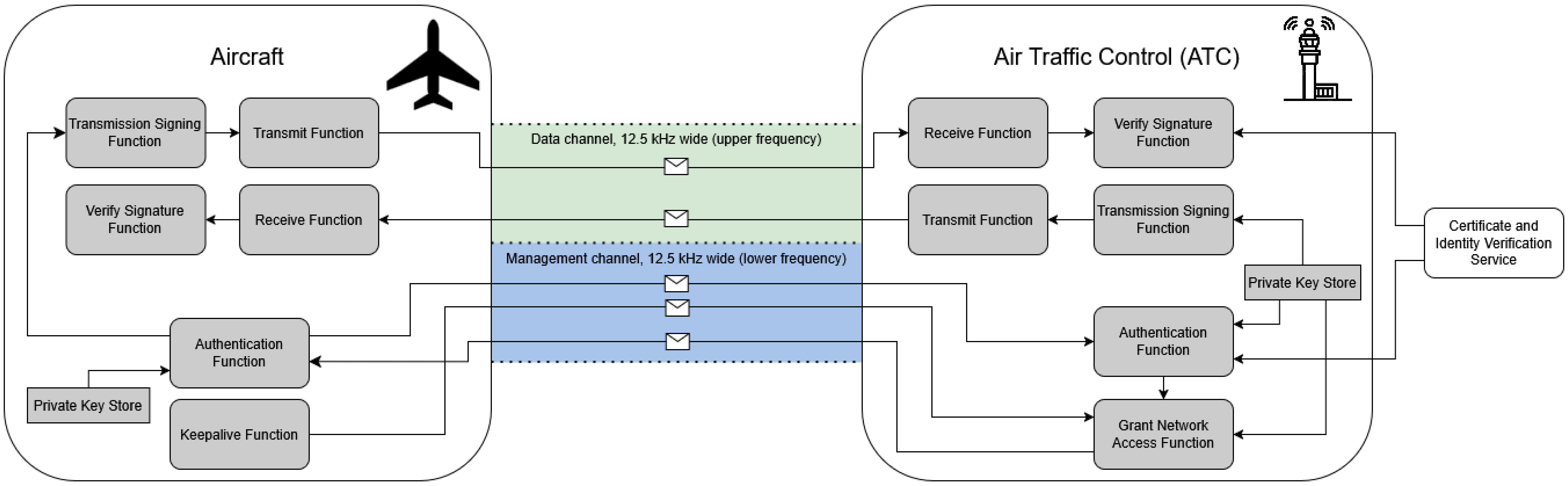
Andrew Markel
markela@purdue.edu

Overview

Insecure aircraft communications pose a significant threat to aviation security due to the risk of spoofing and interception. This research introduces a secure authentication and integrity verification framework for Air Traffic Control (ATC) communications. Using Public Key Infrastructure (PKI), this solution ensures that only authenticated pilots and ATC stations participate in critical voice communications.

Solution

Pilots and ATC stations need a way to verify the integrity of all transmissions broadcast over an aviation frequency. Additionally, ATC stations need a way to authenticate aircraft attempting to communicate on a frequency. Using digital radio technologies, aircraft authenticate to ATC networks using a challenge-response protocol. Once authenticated, all transmissions are signed with a digital certificate that can be verified by all other stations.


Aircraft
Transmission Signing Function
Transmit Function
Verify Signature Function
Receive Function
Authentication Function
Private Key Store
Keepalive Function
Data channel, 12.5 kHz wide (upper frequency)
Management channel, 12.5 kHz wide (lower frequency)
Air Traffic Control (ATC)
Receive Function
Verify Signature Function
Transmit Function
Transmission Signing Function
Private Key Store
Authentication Function
Grant Network Access Function
Certificate and Identity Verification Service

Key Elements

Integrity Verification

Integrity between aircraft and ATC verified using digital certificates to sign each transmission

Authentication

Authentication is done using an encrypted management channel to exchange certificates and identify information.

No Encryption

All communications occur over a plaintext channel, preventing the significant computing overhead necessary for encryption

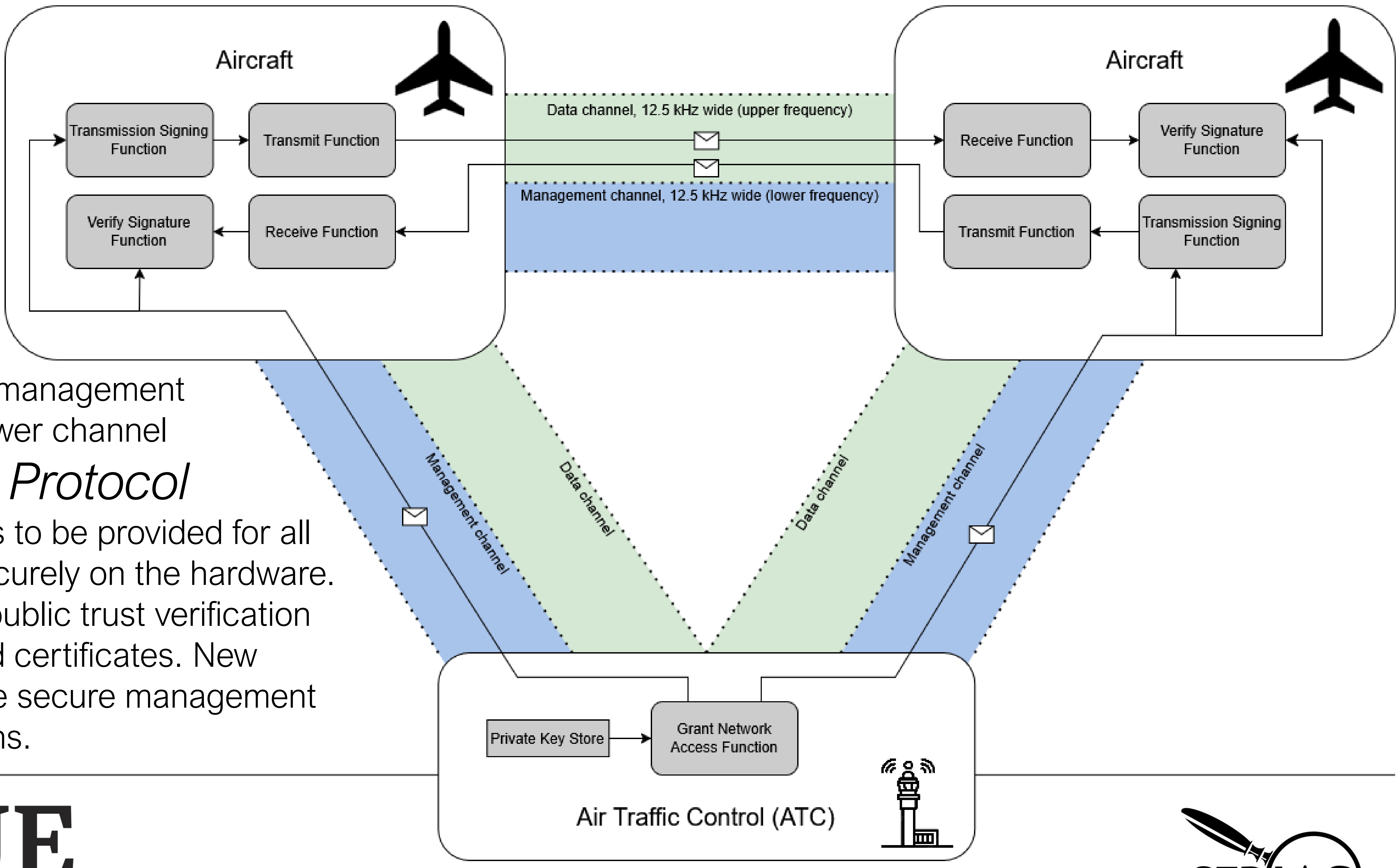
Technologies

Frequency Division

The current 25 kHz bands used for analog aviation communications are split into two separate bands of 12.5 kHz separation for digital transmissions. Audio data is transmitted on the upper channel, and management communication is transmitted on the lower channel

Trust and Secure Network Protocol

This protocol requires digital certificates to be provided for all aircraft and ATC stations and stored securely on the hardware. Certificates can be revoked through a public trust verification service, and the FAA may revoke invalid certificates. New certificates can be provided through the secure management channel when connected to ATC stations.


Aircraft
Transmission Signing Function
Transmit Function
Verify Signature Function
Receive Function
Data channel, 12.5 kHz wide (upper frequency)
Management channel, 12.5 kHz wide (lower frequency)
Aircraft
Receive Function
Verify Signature Function
Transmit Function
Transmission Signing Function
Management channel
Data channel
Data channel
Management channel
Private Key Store
Grant Network Access Function
Air Traffic Control (ATC)

PURDUE UNIVERSITY
CERIAS