Automatic Dependent Surveillance- Broadcast (ADS-B)

Cryptography Securing Next Generation Air Traffic Surveillance

Kevin Joseph
4th year CSE, Karunya Institute of Technology & Science

Abstract

The proposed next-generation air traffic control system depends crucially on a surveillance technology called ADS-B.

•*Real-time ADS-B is now the preferred method of surveillance for air traffic control in the NAS*

•*General aviation is safer with ADS-B traffic, weather, and flight-information services*

•*Safety and efficiency improve with advanced ADS-B applications*

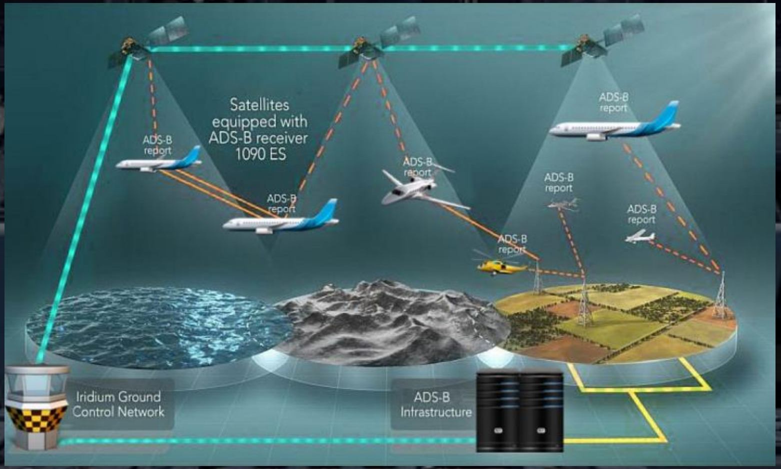
Introduction

ADS-B shifts the burden of surveillance from antiquated ground-based radar to modern satellite-navigation based aircraft transponders. Benefits of ADS-B include increased situational awareness, extended surveillance coverage, enhanced conflict detection, reduced operational costs, and improved routing efficiency,

Unfortunately, ADS-B as currently designed is riddled with security vulnerabilities. ADS-B messages are broadcast in-the-clear according to an open protocol without cryptographic security mechanisms such as encryption or digital signatures that could protect and authenticate them.

Methodology

ADS-B Out works by broadcasting information about an aircraft's GPS location, altitude, ground speed and other data to ground stations and other aircraft, once per second. Air traffic controllers and aircraft equipped with ADS-B In can immediately receive this information.



ADS-B In provides operators of properly equipped aircraft with weather and traffic position information delivered directly to the cockpit. ADS-B In-equipped aircraft have access to the graphical weather displays in the cockpit as well as text-based advisories, including Notices to Airmen and significant weather activity.

Cryptography for ADS-B

Asymmetric-Key Encryption: In an asymmetric-key encryption paradigm, users would encrypt the ADS-B message with the intended recipient's public key according to a specific public-key encryption technique (e.g., elliptic curve cryptography [ECC]). The recipient could then decrypt the message with his or her own private key. Confidentiality is also a byproduct of asymmetric-key encryption because only the sender's intended recipient can decrypt the transmission.

Digital Signatures: Digital signatures are similar to MACs in the sense that they are appended to the original inthe-clear ADS-B message. Digital signature algorithms take a message and a user's private key as input and return a digital signature unique to the input.

Conclusion

The burden of public-key management and the reduction in operational capacity over the 1090 MHz Mode-S ES channel would likely prove unacceptable to regulatory agencies, commercial airline companies, and general aviation enthusiasts. To avoid these difficulties, a possible alternative would be to broadcast signed ADS-B messages over a side channel such as the aviation-protected L-band at 960–1215 MHz. Meanwhile, ADS-B will continue to rely on radar for authentication— ironically, the very technology it was designed to replace.