Lecture 15

Wednesday, 5 April 2023 13:29

GNSS and ADS-B both have constraints in the network which **affect** the security features which can be deployed

legacy technologies:
- primary surveillance radar (PSR)
- secondary surveillance radar (SSR)

radar signals broadcast from radar station reflected by aircraft

does not work well with high aircraft density

accuracy of 1–2 nmi ≈ 1.85–3.7 km

high cost

ADS-B : automatic dependent surveillance – broadcast

designed in 1992, made mandatory in 2020

use GPS to determine location, then **broadcast** this in a message → ADS-B out
+ timestamp, velocity

ADS-B in : receive information from other aircraft
maybe mandatory from 2025?

ES1090 used in most countries
as UAT is often occupied by other services
frequency

ADS-B ES1090 message size: 112 bits
of which
56 bits of data = 7 bytes, i.e. much lower than in IEEE802.15.4, which makes security even more difficult to implement

anyone can listen in, since there is no security
passive eavesdropping

selective jamming → aircraft disappearance

threats
- make aircraft appear in vicinity of another aircraft
- aircraft may appear all around a ground station
- make aircraft appear in no-fly zones

ADS-B is insecure because:
- it was developed in 1990 → security was 'not a thing'
- with a focus on performance

signing is difficult, because missing even one of the messages over which the signature is made makes it impossible to verify the signature

cost of securing ADS-B lies in long discussions before implementation

safety is more important than security
- safety ↓ risks people
- security ↓ risks systems

authentication + integrity could be important, but confidentiality is not

reliability of message delivery is low and even lower for receiving multiple consecutive messages in a row

security solutions

PKI

retroactive key publication

physical layer schemes

secure location verification

Sign with ECDSA with airplane key
- needs key management
- signature may still be for too large
- message fragmentation required, high overhead + bandwidth use

TESLA protocol → use hash of master key, preimage is next key
- disclose key after interval
- use symmetric key to 'sign' digest message (uses HMAC)

μTESLA: optimized for constrained environments

security depends on time synchronization

use hard-to-replicate imperfections e.g. in hardware/software, channel fingerprinting (did signals come from air or ground?) → easy to implement (+), changes in channel (-), requires bidirectional communication (-)
- ↳ hardware-based device fingerprinting → downside: authentication becomes probabilistic

alternative: uncoordinated frequency hopping → way more robust against eavesdropping + jamming, but leads to packet loss

double check authenticity of location claims from multiple vantage points
- susceptible to existence of multiple paths (e.g. due to signals bouncing around buildings)
- altitude is difficult to estimate, since all receivers are at approximately the same altitude

distance bounding

data fusion
- ↳ traffic modelling