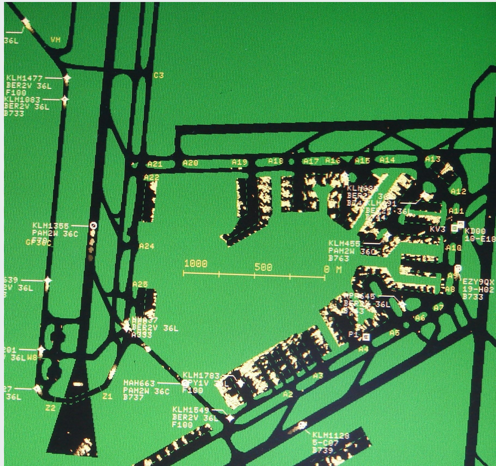
Automatic Dependent Surveillance-Broadcast (ADS-B)

Tim de Boer (tim.deboer@os3.nl)



Source: https://nl.wikipedia.org/wiki/Radar, Mark Brouwer

Background

- First radar in used during WWII - Primary Surveillance Radar (PSR)
- First transponders in the 70's - Secondary Surveillance Radar (SSR)
    - 1030 MHz interrogation, 1090 MHz reply, pulse position modulation (PPM)
    - 4 digit "squawk" code, assigned by the ATC (Mode A)
    - added the pressure altitude (Mode C)
    - selective mode (Mode S)
        - 24 bit uniquely assigned address by ICAO
        - more relevant data available; position, speed, course
- Automatic Dependent Surveillance-Broadcast (ADS-B)
    - to improve air safety
    - periodically transmitted

Research question(s)

How can malicious broadcasts of the ADS-B be detected to protect Air Traffic Control (ATC) from Denial-of-Service (DoS) and disinformation attacks?

Sub-questions:

- What types of attacks are possible in terms of DoS and disinformation?
- In what way can historical or predictive modelling be used for the purpose of filtering disinformation signals?
- How can detection and filtering algorithms aid in signal integrity and authenticity validation?
- What kind of advantages can signal fingerprinting offer for the detection of malicious broadcasts?

Related work

Costin et al. investigated the (in)security aspects of the ADS-B protocol and demonstrated that attacks are both easy and feasible for a moderately sophisticated attacker.

Xuhang Ying et al. created a ADS-B message classifier based on a Deep Neural Network (DNN), to enhance detection of unauthorised broadcasts by using raw in-phase and quadrature components (IQ)-samples.

Wei-Jun Pan et al. looked closer into an enhancement of ADS-B and proposed signing the ADS-B messages with a public key certificate (X.509) to prevent replay attacks and verification of the authenticity of the message.

How does ADS-B work? - Transponder Format

- Preamble for synchronisation
- Downlink Format
  - Normal Mode -S Squitter uses Downlink Format 11 (DF11)
  - Extended Squitter uses DF17, with a extra 56-bit data block
- Capability
- 24 bit uniquely assigned address by ICAO
- Extra 56 bit field
- Cyclic Redundancy Check (CRC) to detect transmission errors

8 μs	112 μs				
	5 bits	3 bits	24 bits	56 bits	24 bits
Preamble	**Downlink Format**	**Capability**	**Aircraft Address**	**ADS-B Data**	**Parity Check**

How does ADS-B work? - Data Format

General format

5 bits	51 bits
Type Code	**Type specific format**

5 bits	3 bits	48 bits
Type Code (1-4)	**Aircraft Type**	**Callsign (8 chars)**

5 bits	3 bits		22 bits	11 bits		8 bits
Type Code (9-18)	**Sub Type**		**Horizontal Velocity**	**Vertical Velocity**		**Difference Baro Altitude**

Type Code	Content
1 - 4	Aircraft identification
5 - 8	Surface position
9 - 18	Airborne position (w/ Baro Altitude)
19	Airborne velocities
20 - 22	Airborne position (w/ GNSS Height)
23 - 27	Reserved
28	Aircraft status
29	Target state and status information
31	Aircraft operation status

Types of attack

- Disinformation
  - Replaying earlier recorded messages
  - Generating fake messages
  - Filtering messages
  - Altering messages
- Denial-of-Service (DoS)
  - Jamming RF-signal (white/pink noise)
  - Pollute bandwidth with disinformal messages

Lab environment

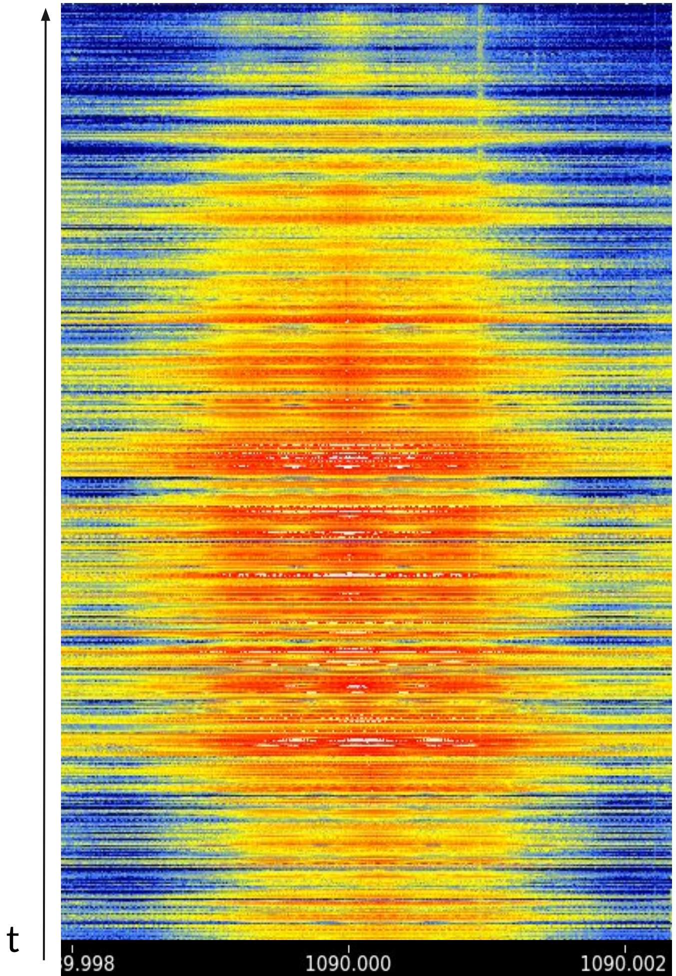
- Ettus Research USRP2
    - Ettus Research WBX daughterboard
    - NooElec 1090MHz ADS-B Antenna
- Generic computer
    - Kali Linux 2020.1a
    - GNU Radio Companion (version 3.8.1.0)
    - Gqrx (version 2.12.1-1)
    - dump1090-fa (version 3.7.0)

Signal quality

- Signal strength decreases with distance
- Free Space Path Loss formula:

$$FSPL = \left(\frac{4\pi d}{\lambda}\right)^2$$

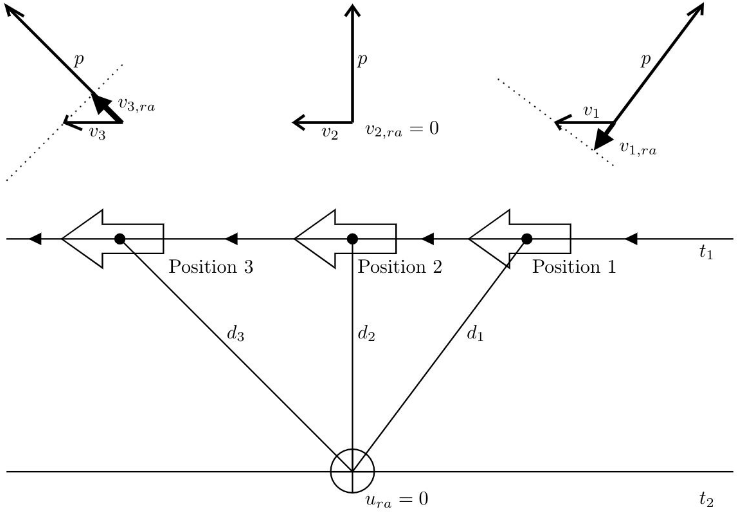
- Verify the transmitter is moving

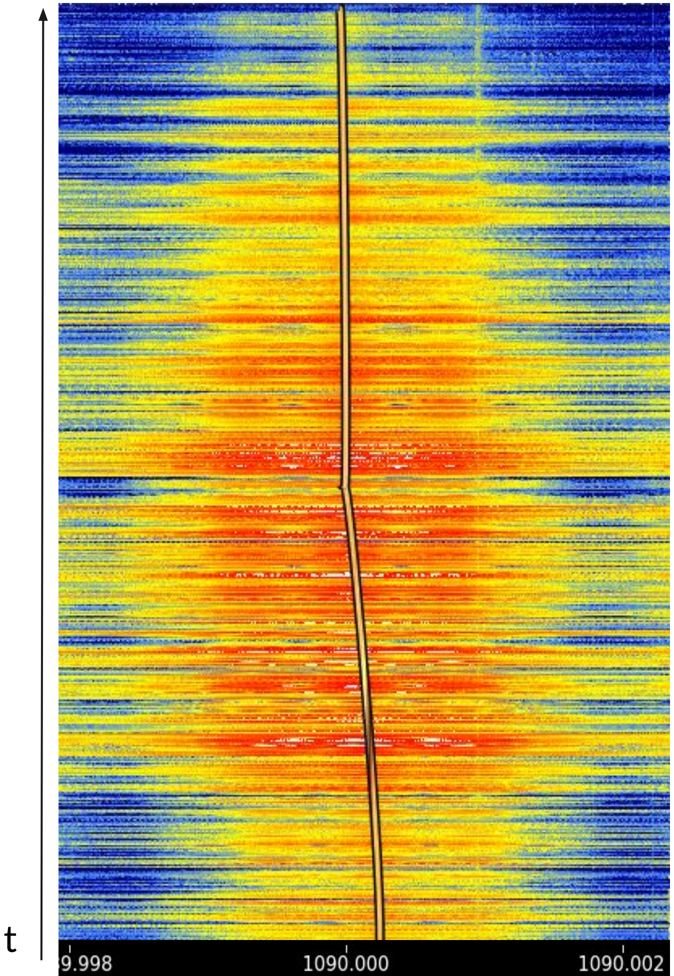


Doppler shift

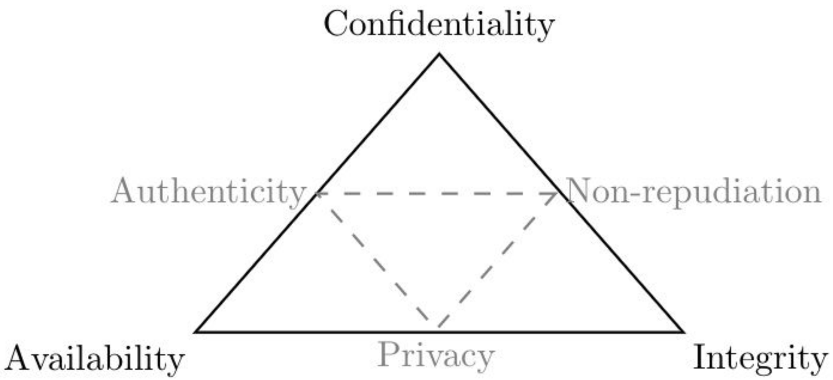
- Observed frequency changes with velocity
- Doppler shift formula:
  - 125m/s = 455 Hz shift

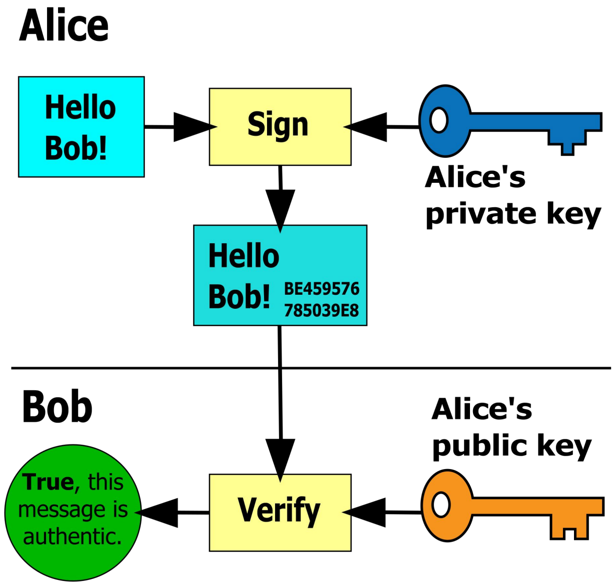
$$f_r = \left(\frac{c + \cancel{u_{ra}}^{0}}{c + v_{ra}} \right) f_a$$





Security enhancement

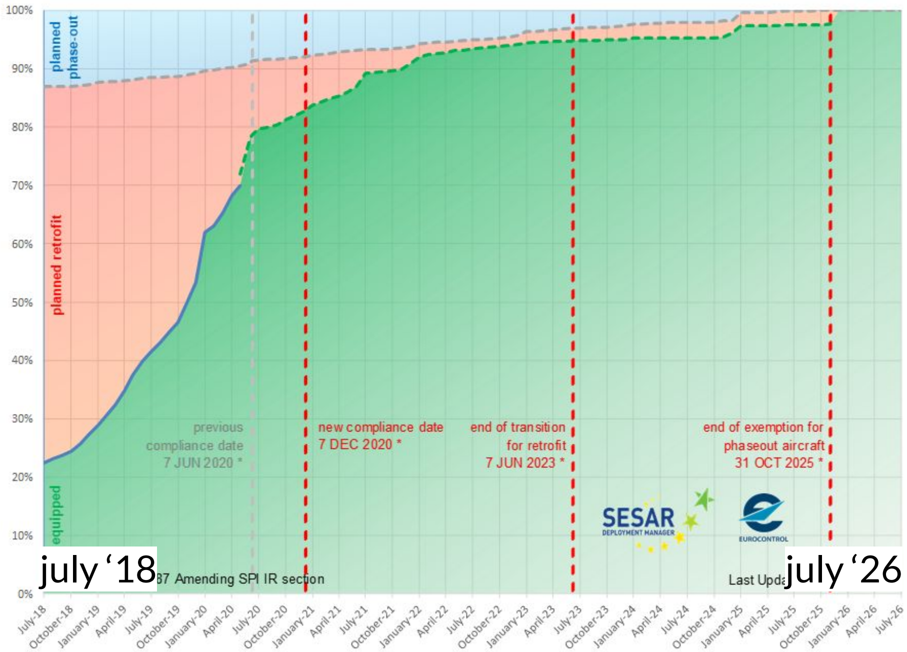




Source: https://en.wikipedia.org/wiki/Digital_signature, FlippyFlink

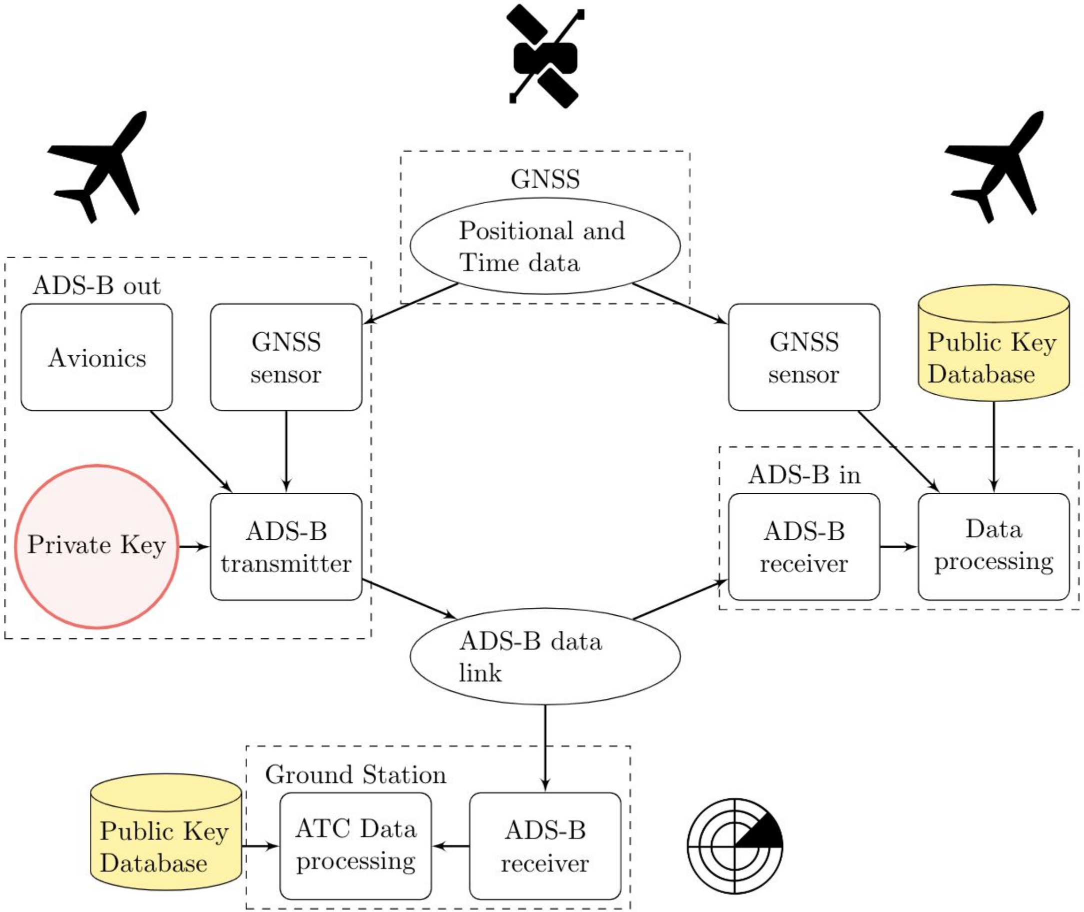
Security enhancement

- Current message format is small
- Implementation of new standards takes decades in the aerospace industry
- ADS-B equipment expects 120µs
- Add GPS timestamp against replay attacks
    - Week number rollover



Source: https://ads-b-europe.eu/, SESAR

8 µs	112 µs					189 µs		
	5 bits	3 bits	24 bits	56 bits	24 bits	10 bits	19 bits	160 bits
Preamble	**Downlink Format**	**Capa bility**	**Aircraft Address**	**ADS-B Data**	**Parity Check**	**GPS Week Number**	**GPS Time of Week**	**Signature Data**


GNSS
Positional and Time data
ADS-B out
Avionics
GNSS sensor
Private Key
ADS-B transmitter
GNSS sensor
Public Key Database
ADS-B in
ADS-B receiver
Data processing
ADS-B data link
Public Key Database
Ground Station
ATC Data processing
ADS-B receiver

Conclusion

How can malicious broadcasts of the ADS-B be detected to protect Air Traffic Control (ATC) from Denial-of-Service (DoS) and disinformation attacks?

- Analyse RF-signal parameters
  - signal quality
  - doppler shift
- Sign the ADS-B messages

Discussion

- High quality receiving equipment is required
  - Clock drift in transmitter, receiver or both
- Signed ADS-B messages require longer transmission time
  - potential problems with busy airspaces
  - less frequent signing messages
  - different frequency or modulation

Future research

- What other signing methods are available?
- Are other security properties also feasible to further improve the protocol? (encryption)
- What security attacks are available for Aircraft-to-Aircraft communication? (collision avoidance)

Questions?