disco
distributed computer systems

Technische Universität Kaiserslautern

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

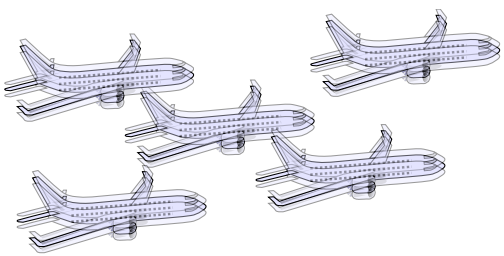
Matthias Schäfer, Vincent Lenders and Ivan Martinovic

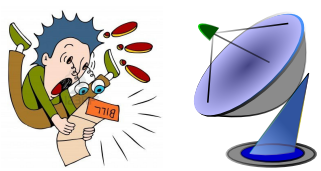
June 27th, 2013

Introduction

Current Air Traffic Surveillance

- ATM crucial for avoiding collisions
- Technologies used since World War II:
  - Primary Surveillance Radar
  - Secondary Surveillance Radar (Mode A/C/S)
- But there are some major problems:



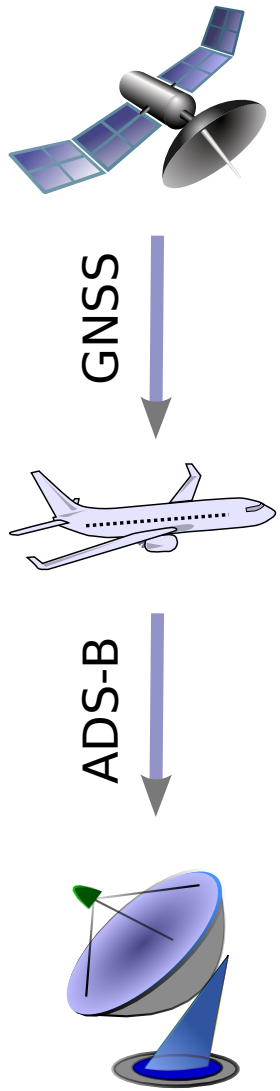


- Insufficient accuracy
- Expensive
- Expected doubling of traffic until 2025

- NextGen (US) and CASCADE (Europe)

2020: NextGen Air Traffic Surveillance

- Automatic: no explicit interrogation necessary
- Dependant: aircraft determines its precise location in space on-board
- Surveillance: precise and up-to-date position, velocity, identification, ...



Automatic Dependent Surveillance – Broadcast

- Aircraft continuously determine their position and velocity using GNSS
- Position, ID, velocity and status are broadcasted periodically

Security in ADS-B...

- ... does not exist!

ADS-B

- Designed for cost efficiency and accuracy
- Legacy compatibility for a smooth transition
- 20 years from development to final deployment
- worldwide coordination and deployment

Attacker

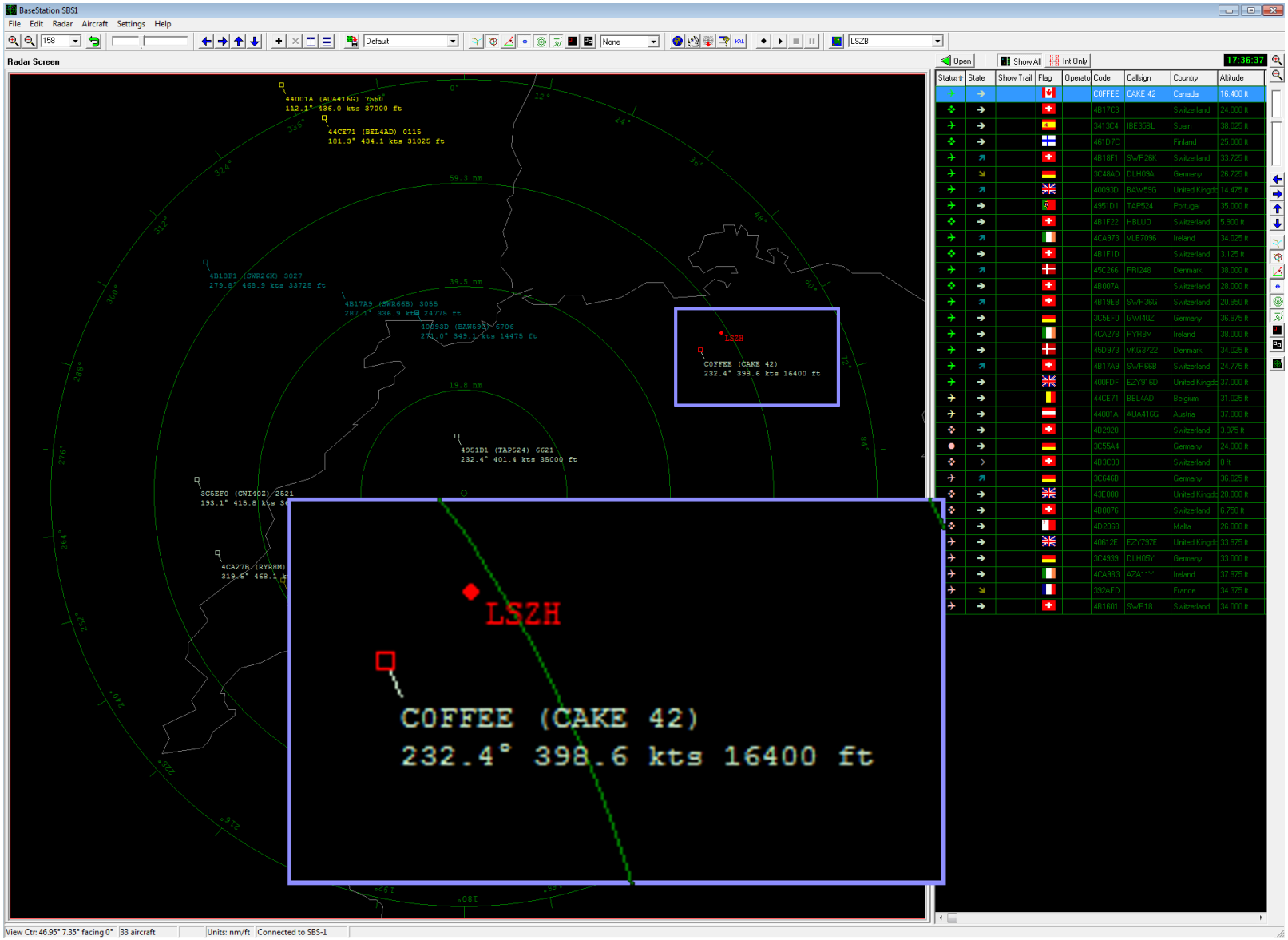
- Rapid technological progress
- Easily accessible knowledge
- Cheap equipment available off-the-shelf
- Attacks usually local, e.g. one ground station

Attacks

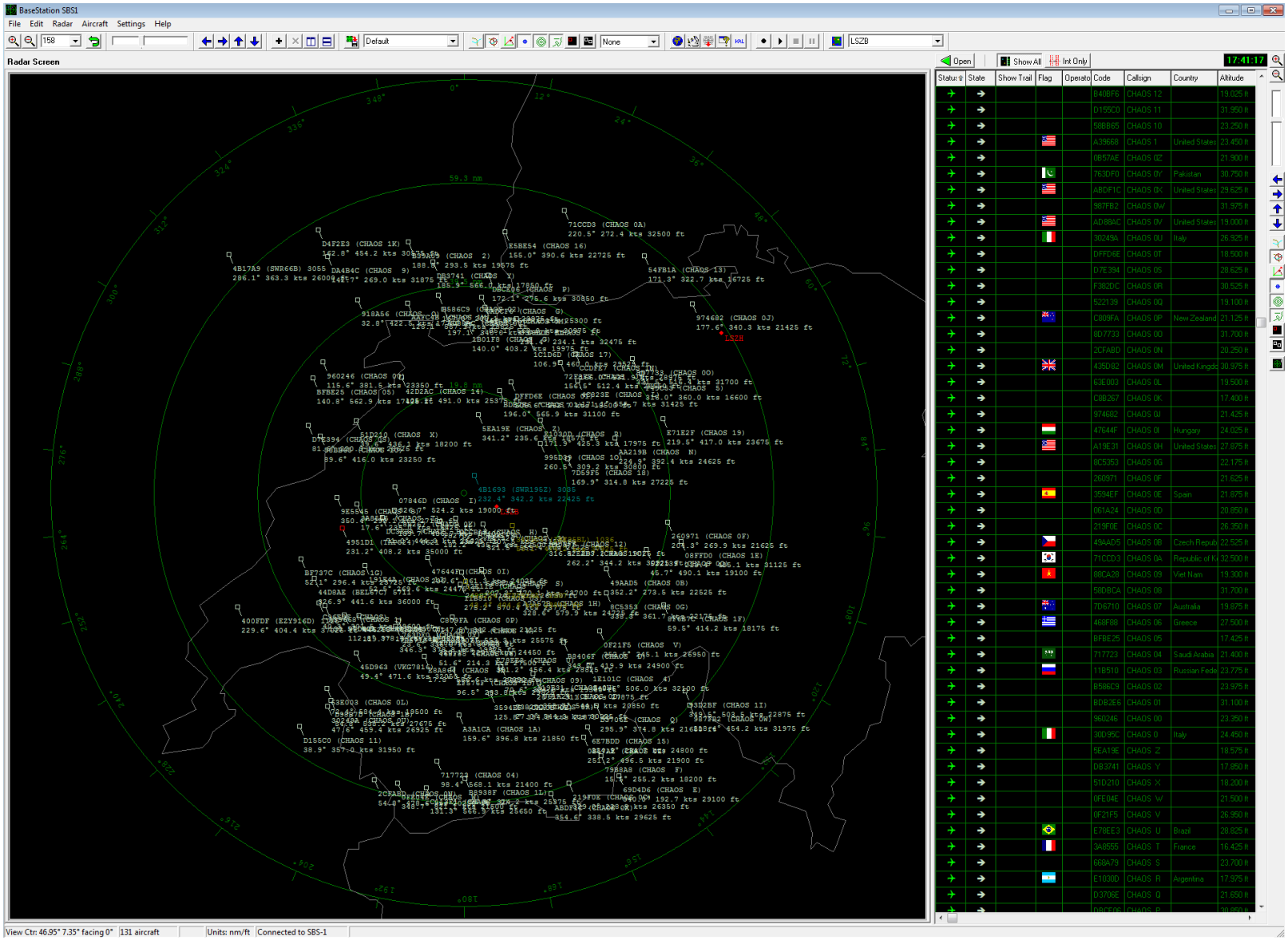
Attacks

- Passive attacks are trivial due to the lack of encryption
- But: passive attacks may support active attacks
- Active attacks:
  - Injection of ghost aircraft
  - Modification of the position of existing aircraft
  - Jamming attacks
  - Deletion of existing aircraft from the screen
  - ...

Example 1: Ghost aircraft injection



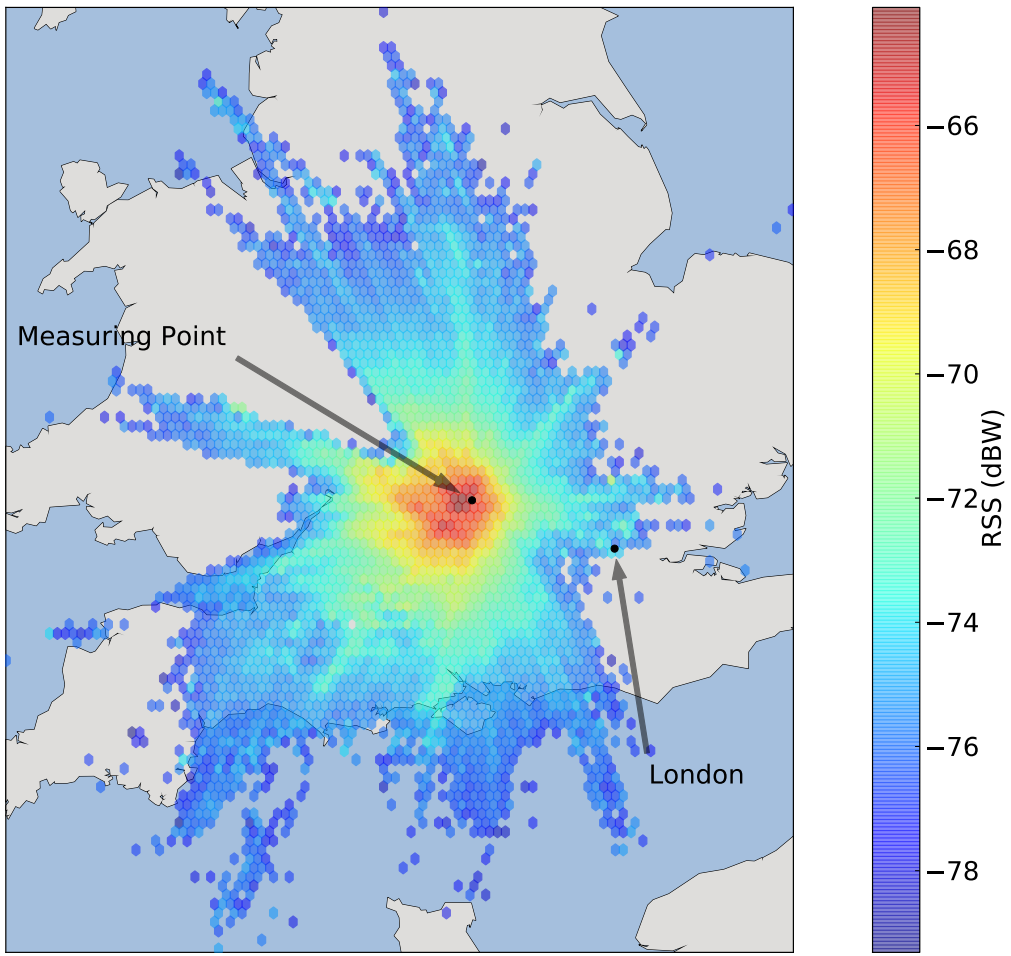
Example 2: Ghost aircraft flooding



Limitations

Passive Attacks

- Line-of-sight link



Active Attacks

- Message injection: $P/N > \delta$
- (Selective) Message deletion:
  - Timing: reacting time in the order of 100 μs
  - Position: distance to attacked ground station $\leq$ 10 km
- Message modification:
  - Timing: stricter than that of message deletion (few μs)
  - Synchronization with the signal with a precision $<$ 1 μs
  - But: deletion + injection = modification

Discussion

Lessons learned?

1. Technological progress must be considered when designing new critical systems (especially cyber-physical systems)
2. Patches to secure the existing system needed until appropriate security measures are integrated
3. Manufacturers and authorities in the aviation sector should provide more information about infrastructure to support research
4. ATC should not rely on ADS-B exclusively

The End

Thank you very much.