On the Implications of Spoofing and Jamming Aviation Datalink Applications

Harshad Sathaye, Guevara Noubir, Aanjhan Ranganathan

Northeastern University, Boston, USA

Northeastern University

15000 flights!!

https://www.flightradar24.com/15.79,73.1/2

Aviation Datalink (ACARS)

- A digital text-based link between air traffic controllers (ATC) and pilots
  - CPDLC – Controller-Pilot Data Link Communication (ATC instructions)
  - ADS-C – Automatic Dependent Surveillance Contract (Position, maneuver reports)
- Alternative to voice communications –
  - To date applications have saved 2.28 million minutes of radio time
- Used in strategic command and control message exchanges

Contributions

- Systematically analyze security guarantees of aviation datalink applications and present a spoof-and-jam attack strategy to stealthily inject malicious messages
- Present single aircraft and coordinated multi-aircraft attacks that exploit specific message exchanges
- Implement and evaluate an aircraft communications, addressing, and reporting system (ACARS) message spoofer and a first reactive jammer with 1.48 ms reaction time and 98.85% jamming success
- Geo-spatial analysis of historic air-traffic data and identify 48 regions with 90% chance of encountering favorable conditions for multi-aircraft attacks
- Propose potential countermeasures for preventing and detecting reactive jammers

Attacker goals and assumptions

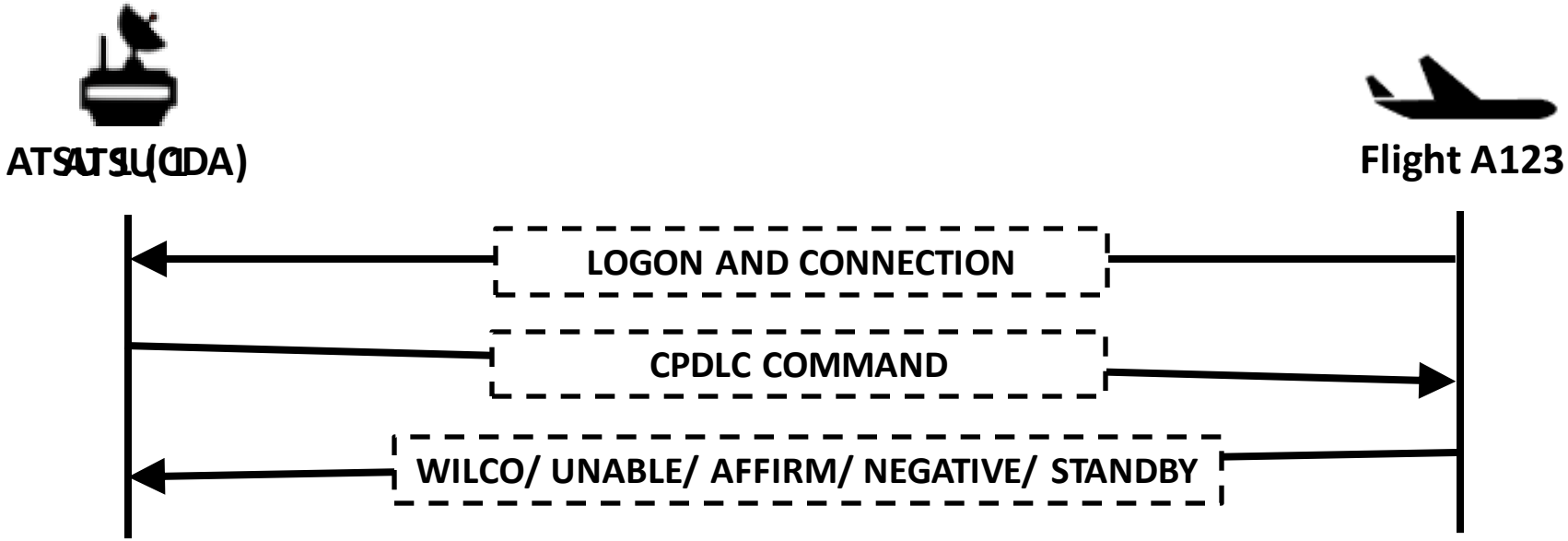
Primary Objective :

Inject malicious messages to influence flight crew's decision making

Assumptions :

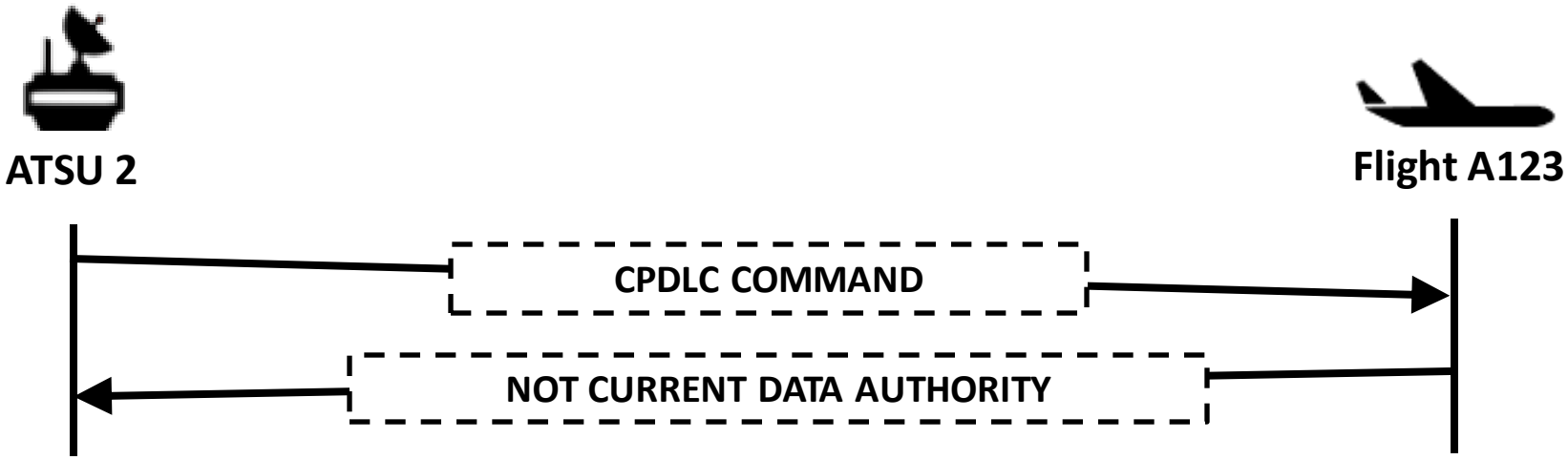
- Attacker is equipped with SDRs capable of RX/TX in VHF band
- Attacker has access to historic air-traffic data for attack planning
- Attacker can track aircraft through ADS-B messages

CPDLC Command Exchange



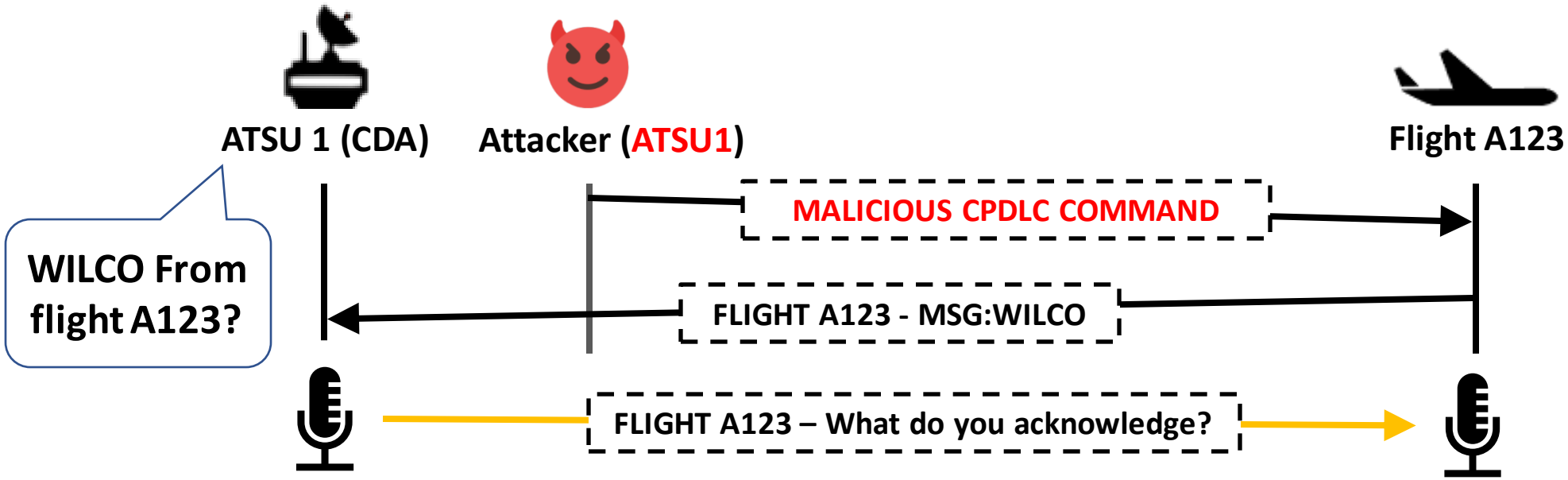
- All messages require flight crew acknowledgement

CPDLC Command Exchange



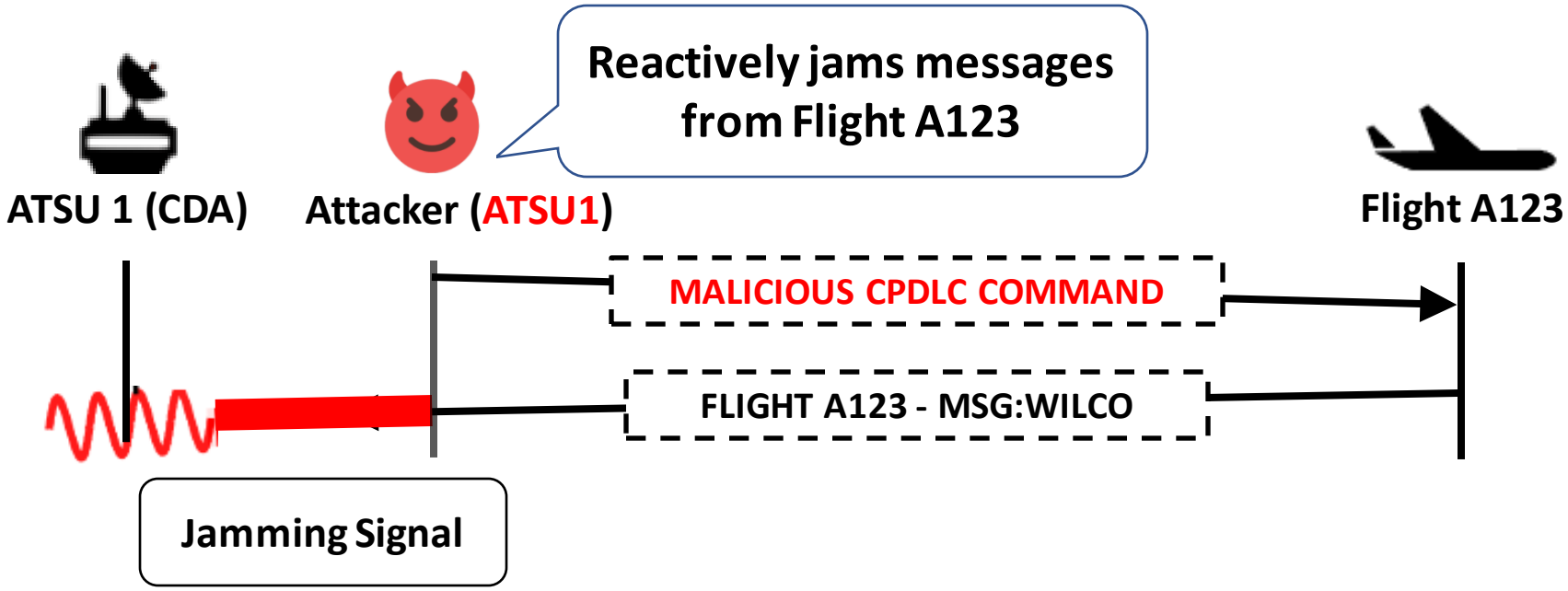
- Messages from a non-CDA addresses will be dropped

Naïve CPDLC Command Injection



- Suspicious, unexpected, and invalid messages will prompt verification over voice channels

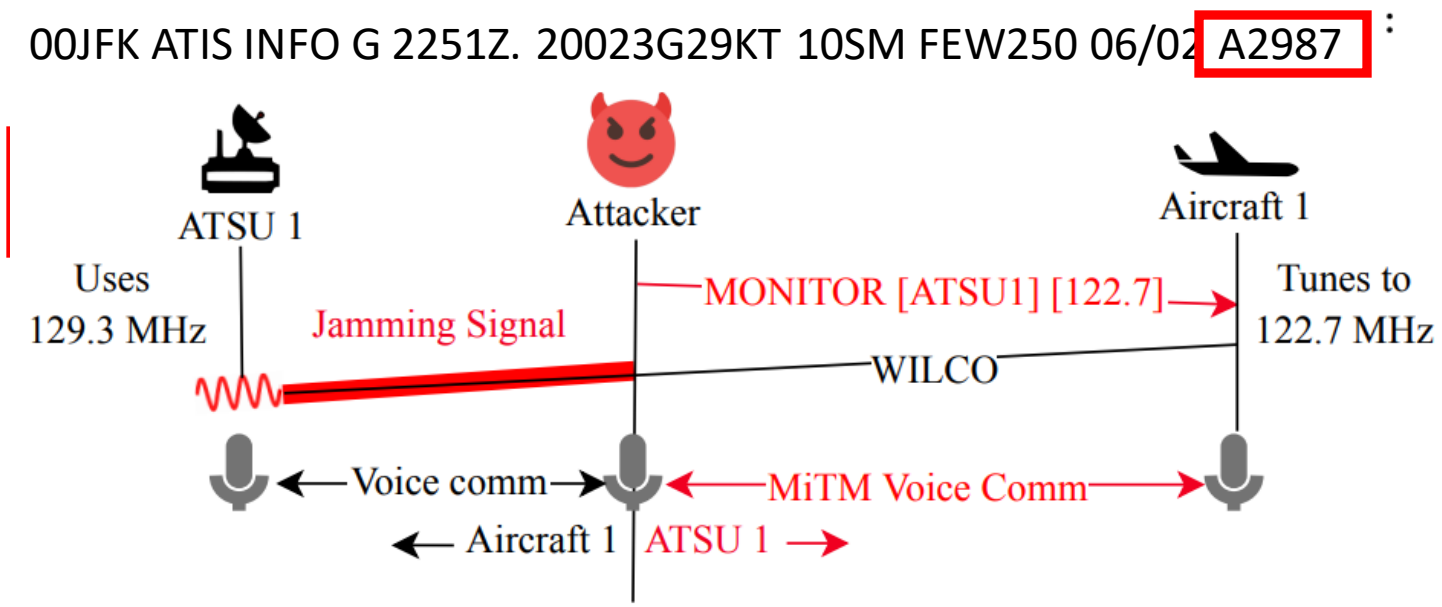
Spoof and Jam Strategy



- Response jamming
- ADS-C report jamming

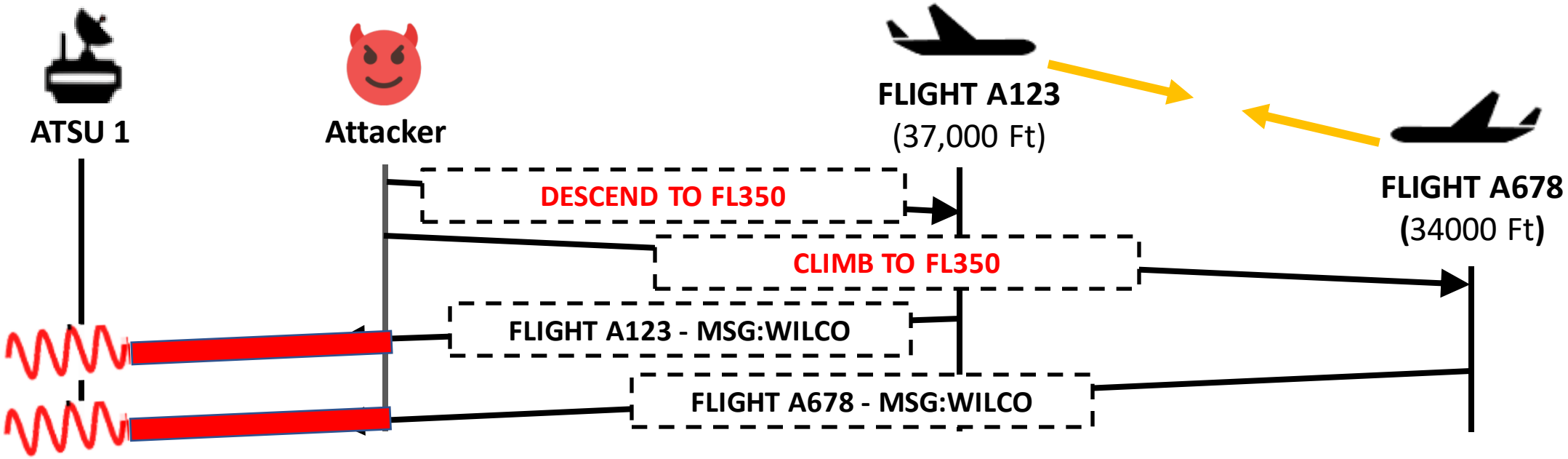
Examples of Single Aircraft Attacks

- Clearance manipulation
  - Squawk code
  - Flight plan
  - Post takeoff instructions
- Altimeter calibration
- VHF Voice MiTM



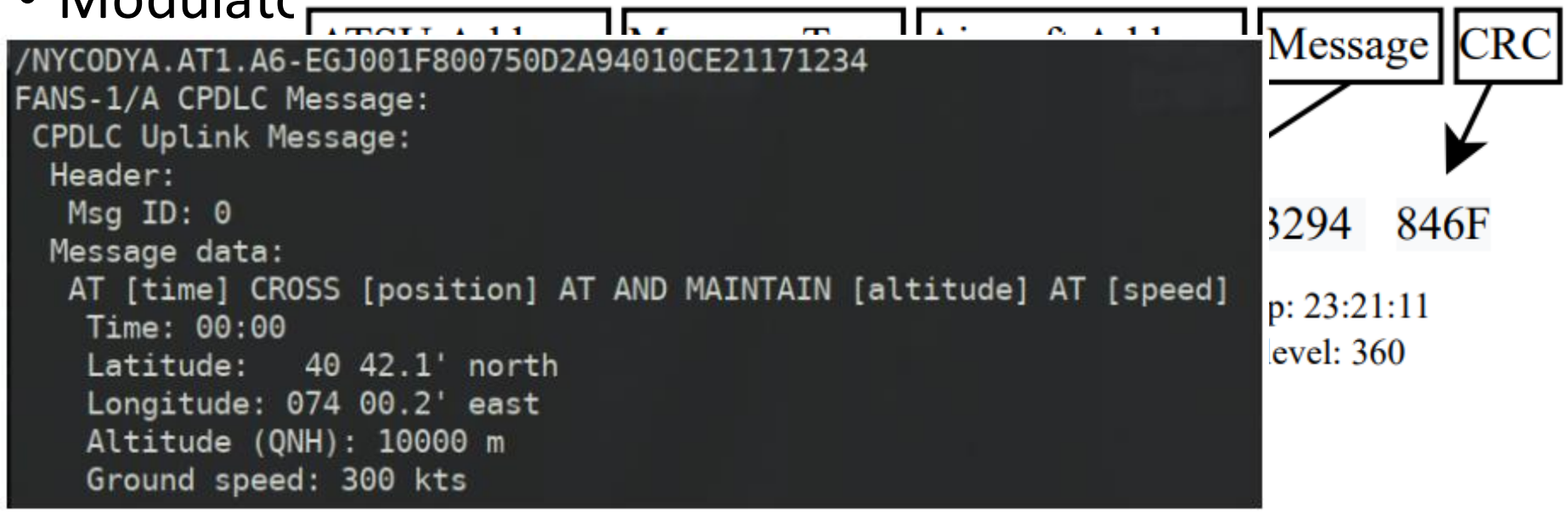
Co-ordinated Multi-Aircraft Attacks

- Targets trajectory altering messages e.g., ALTITUDE, WAYPOINT etc..
- Flights with intersecting routes are favorable for multi-aircraft attacks



Attacker Components

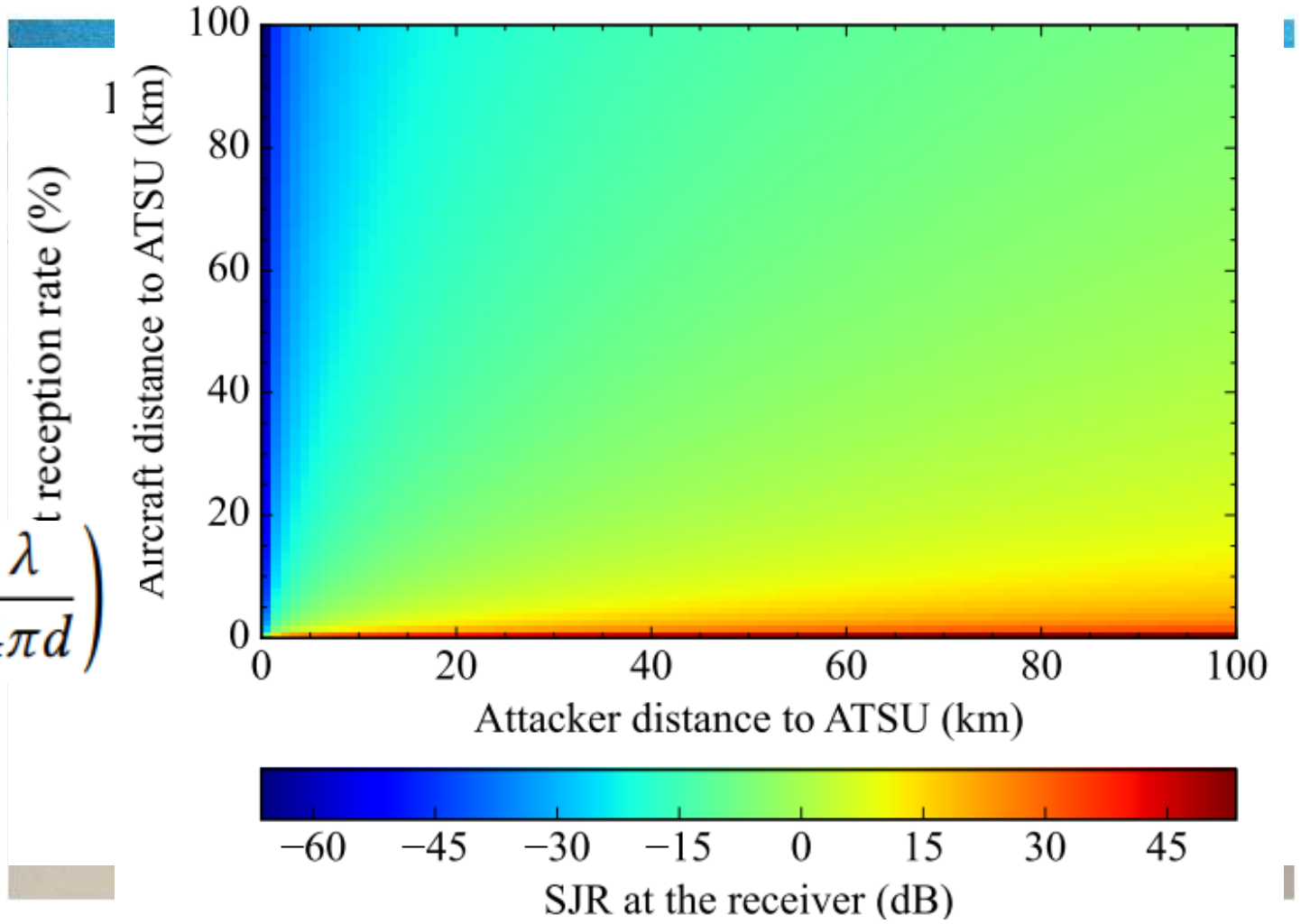
- ACARS receiver (opensource software – *acarsdec, libacars)*
- ACARS message generator [5, 23]
- FANS 1/A - CPDLC application message generator [18]
- Modulator and transmitter



Experimental Evaluation

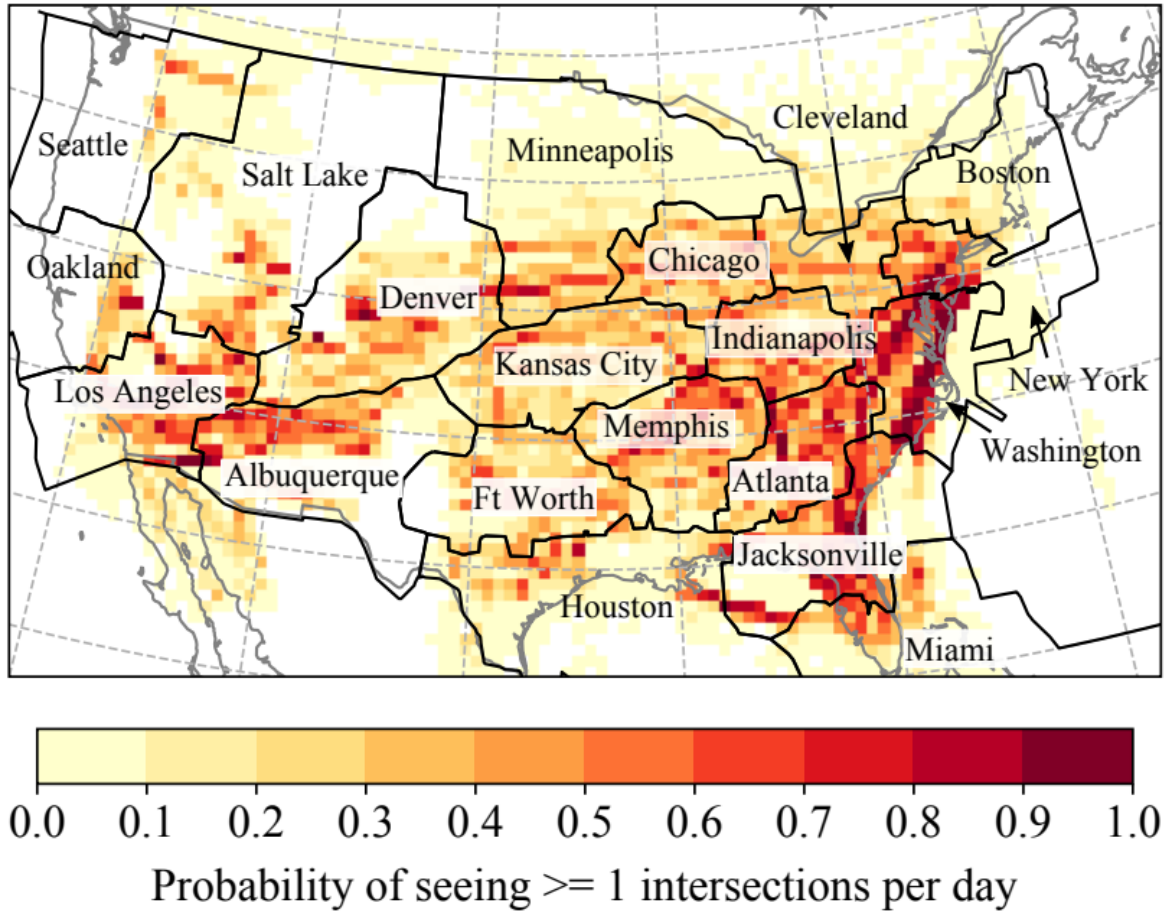
- Jammer Evaluation Setup
- Signal to Jammer ratio (noise source)
- Jammer Placement

$$P_r = P_t + G_t + G_r + 20log_{10}\left(\frac{\lambda}{4\pi d}\right)$$



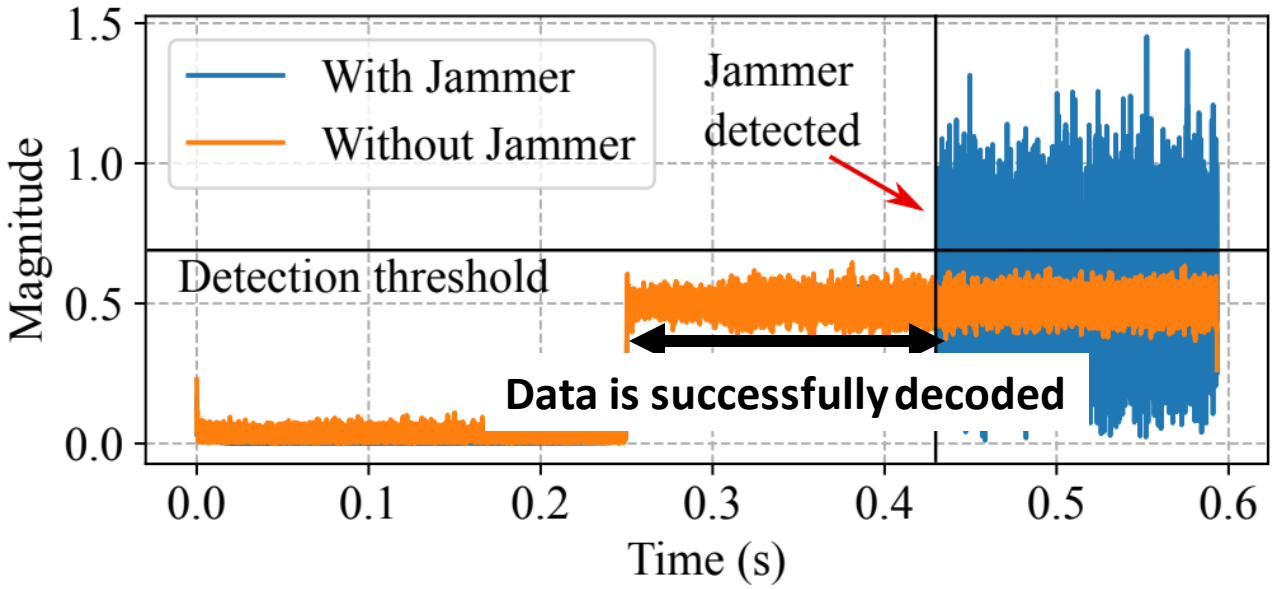
Probability of Intersecting Routes

- Airspace is divided in 2500 km cells
- Flight constraints
  1. Horizontal separation < 100 m
  2. Altitude > 5000 m
- 592,224 total intersections
- 6.44% in top 10 cells
- Most intersections between 1200 - 2200 Hrs UTC



Countermeasures

- Public Key Infrastructure
- Reactive jammer detection
- Detect and revert to voice/satcom
- Operational Redundancies



Takeaways

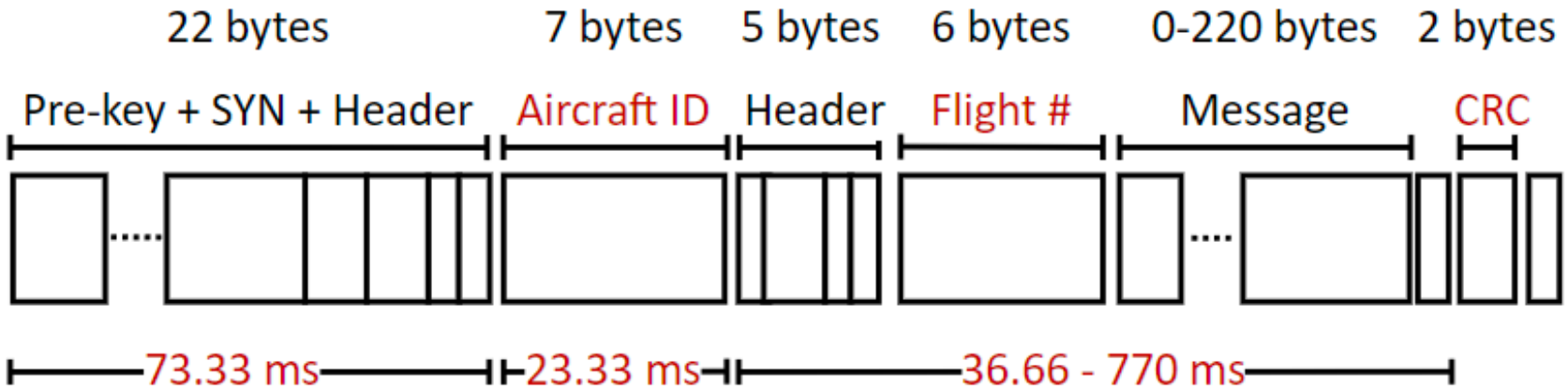
- Aviation datalink provides an attack vector to directly influence flight crew's decision making
- Designed and evaluated reactive jammer can ensure stealthy injection of CPDLC commands
- Standalone attack have lower probability of causing harm
- Threat is magnified when combined with attacks on other avionics
- Redundancies, planes are **NOT** going to fall out of sky!
- Essential to secure individual systems as well as collective security of entire ecosystem

Thank you!

Harshad Sathaye
sathaye.h@northeastern.edu

ACARS Signal in space configuration

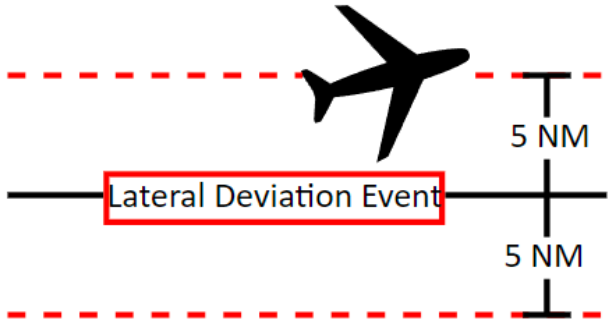
Data rate	2400 bits/s
Baseband modulation	Minimum Shift Keying (MSK) (1200 Hz, 2400 Hz)
Sampling rate	48000 samples/s
Symbol duration	416.67$\mu secs$
Message length	<= 220 ASCII characters
Carrier frequency	131 – 137 MHz

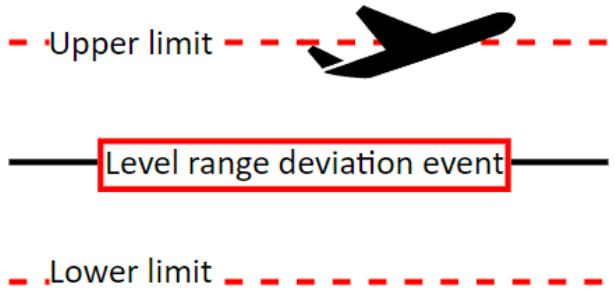


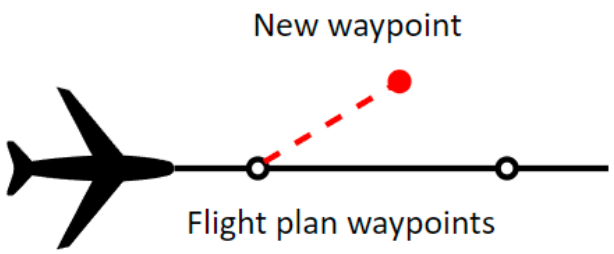
Automatic Dependent Surveillance – Contract (ADS-C)

- ATSU establishes contracts with the aircraft
- Aircraft automatically transmits ADS-C messages as per contract
- Types of contract:

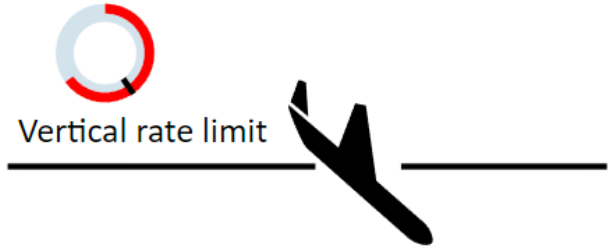
1. Position report
2. Event report
3. Flight plan predictions







Waypoint change event



Vertical rate chane event

Spoof and Jam Strategy