T-SAR (2019-2022)

AI-Powered Testing of False Data Injection Attacks Against Transport Infrastructures

Improving the resilience of control systems against false data injection attacks

Dusica Marijan (Principal Investigator), Pierre Bernabé, Arnaud Gotlieb, Helge Spieker

Partners: Simula Research Lab. (No, Coordinator), UBFC (Fr), TUG (Au), StatSat As (No)

Motivations and Partners

- **Public and private software-based infrastructures** such as Control Systems, SCADA, Intelligent Transport Systems are threatened by more and more **complex cyberattacks**

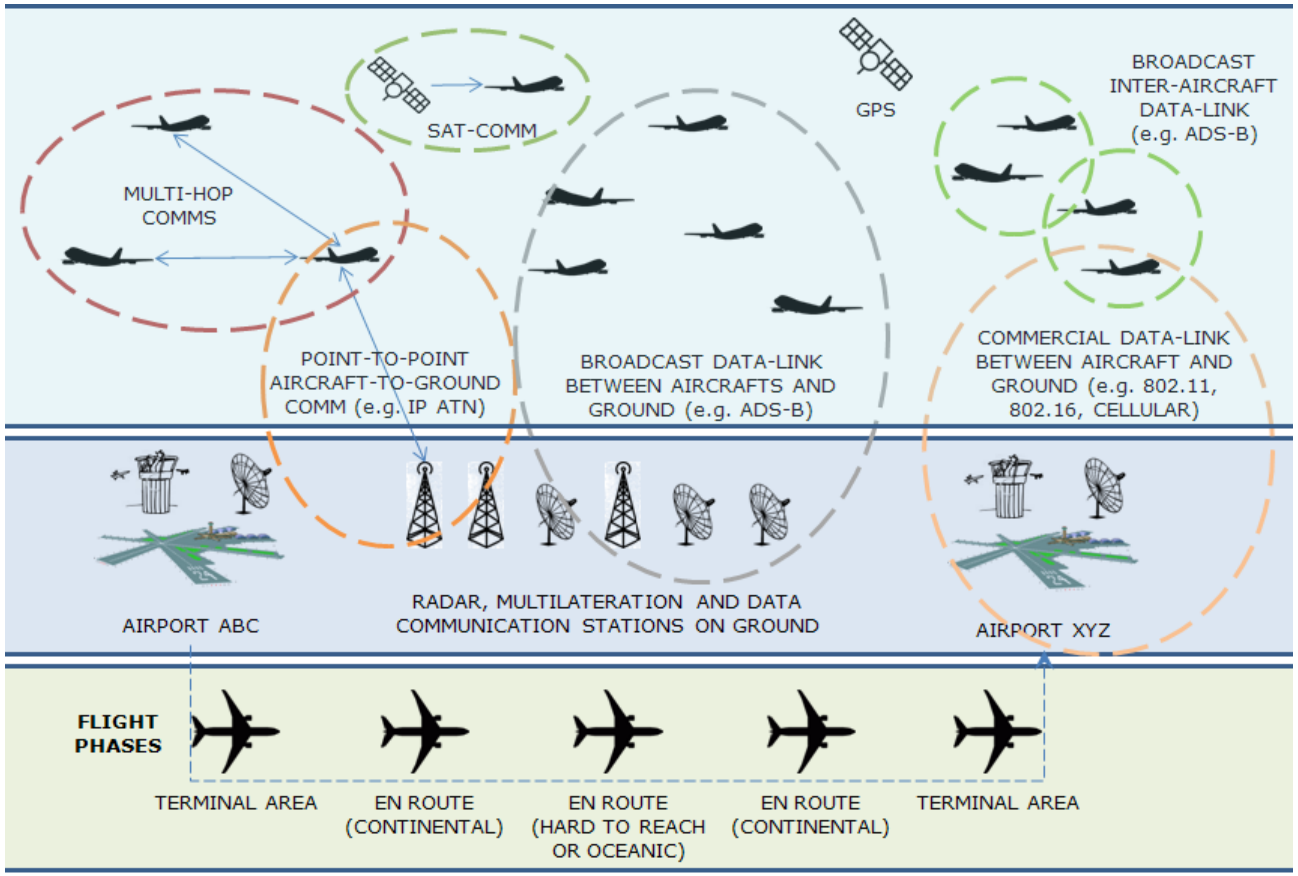
- **False Data Injection Attacks** are an emerging and important class of attacks based on altering the business data : an attacker wishes to destabilize the system by compromising a subset of sensors and sending corrupted messages/data

- **FDIA** are difficult to detect as they alter data semantics while preserving syntactical correctness (e.g., by adding/removing/multiplying elements on a real-time control board).
  → few available real-world examples

- Artificial Intelligence techniques (Constraint Optimization, Natural Language Processing, Machine Learning, Computer Vision, …) can leverage their generation and detection using **Intelligent Testing Methods**

- Partners: Simula Research Lab., StatSat AS (Space Norway), CNRS-Femto Institute, TU Wiena (Statsat operates two satellites for the Norwegian Costal Administration, AISSat-1 and -2)

Example 1 – ADS-B protocol for Air Traffic Control



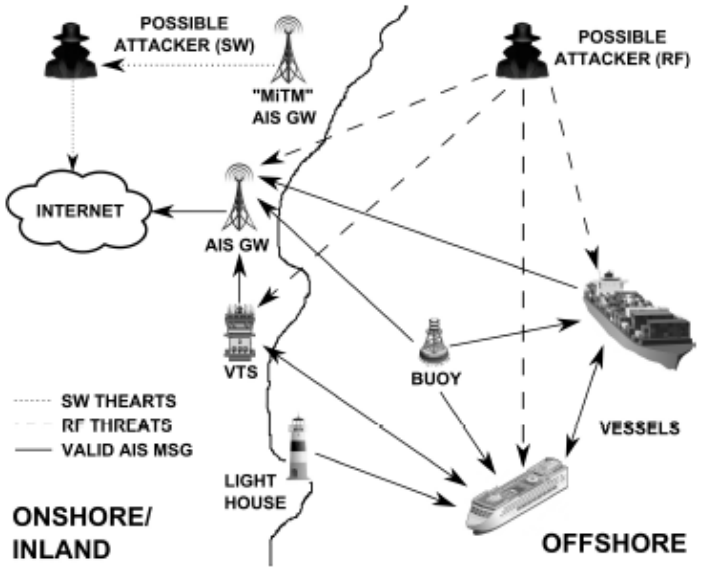
ADS-B Traces are:
- Publically available using cheap devices
- Non-encrypted
- Based on radio waves

Ghost Aircraft Injection. The goal is to create a nonexisting aircraft by broadcasting fake ADS-B messages on the communication channel.
Ghost Aircraft Flooding. This attack is similar to the first one but consists of injecting multiple aircraft simultaneously with the goal of saturating the RAP and thus a denial of service of the controller's surveillance system.
Virtual Trajectory Modification. Using either message modification or a combination of message injection & deletion, the goal of this attack is to modify the trajectory of an aircraft.
False Alarm Attack. Based on the same techniques as the previous attack, the goal is to modify the messages of an aircraft in order to indicate a fake alarm. A typical example would be modifying the squawk code to 7500, indicating the aircraft has been hijacked.
Aircraft Disappearance. Deleting all messages emitted by an aircraft can lead to the failure of collision avoidance systems and ground sensors confusion. It could also force the aircraft under attack to land for safety check.
Aircraft Spoofing. This scenario consists of spoofing the ICAO of an aircraft through message deletion and injection. This could allow an enemy aircraft to pass for a friendly one and reduce causes for alarm when picked up by PSR.

Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices,
A. Costin, A. Francillon, Black Hat USA, 1-12- 2012

Example 2 – Maritime Domain – AIS Data (Automatic Identification System)

An AIS-equipped system on board a ship presents the bearing and distance of nearby vessels in a radar-like display format.

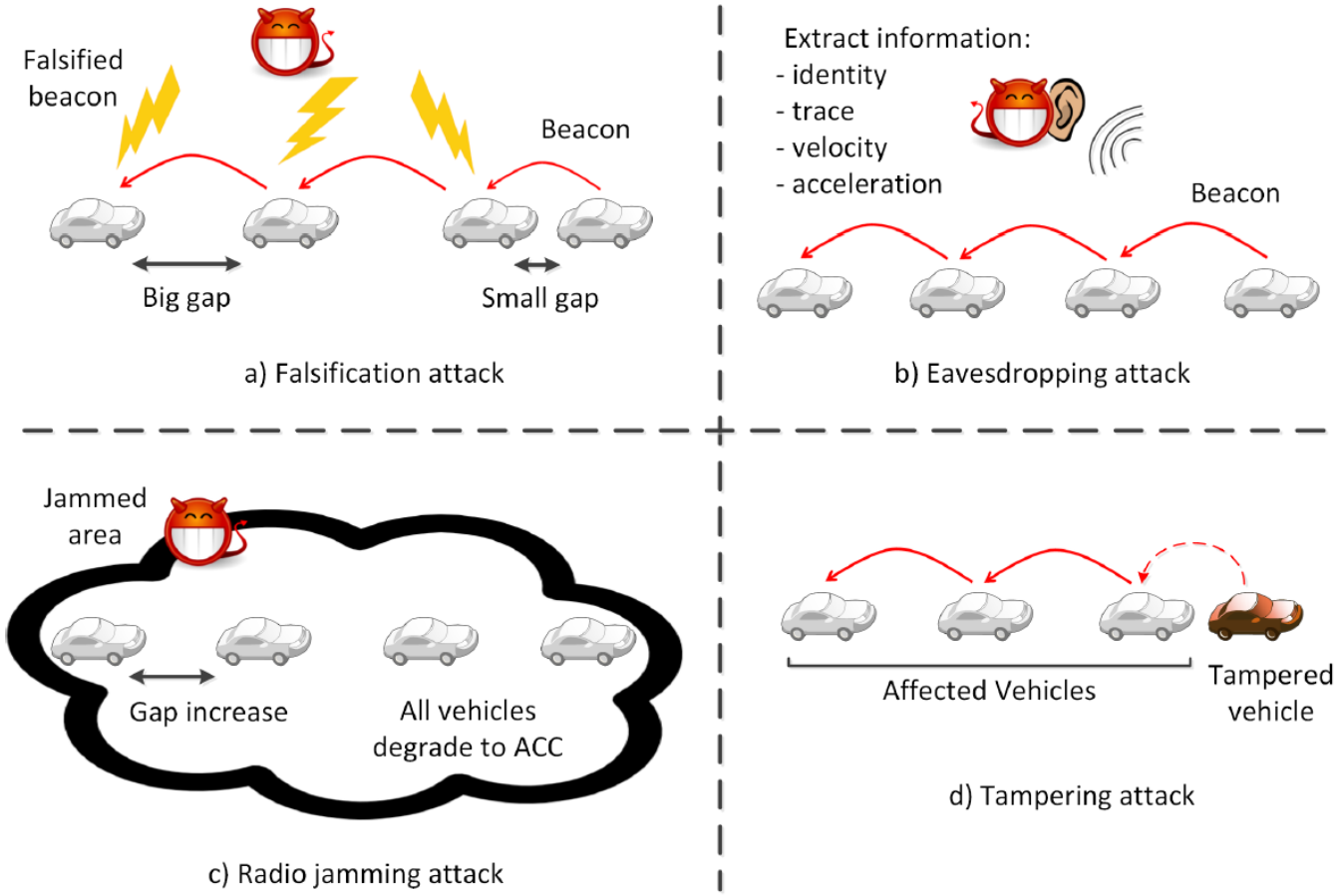


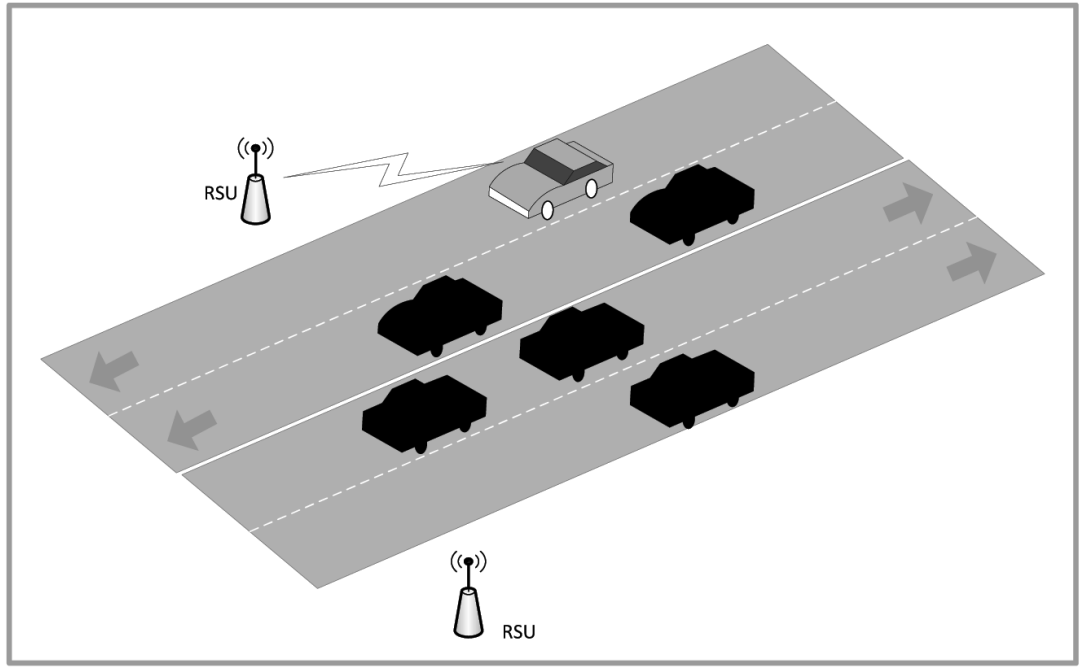
Procedure:
Tampering with existing AIS data by spoofing, hijacking and availability disruption

Effects :
1. Triggering fake Search And Rescue alerts (SAR)
2. Luring a victim ship into navigating to a hostile sea space
3. Spoofing a collision
4. Bringing a ship off course

A Security Evaluation of AIS Automated Identification System. Balduzzi M., Pasta A., Wilhoit K. International Secure Systems Lab. Jan. 2015

Example 3 – Connected Vehicles





M. Amoozadeh et al., *"Security vulnerabilities of connected vehicle streams and their impact on cooperative driving", IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126-132, Jun. 2015.

Cognitive Vehicular Networks, Anna Maria Vegni, Dharma P. Agrawal. February 17, 2016 by CRC Press

AI-driven FDIA Detection

Cybersecurity Expert

Domain Specific Language

Defining FDIA patterns

```
1  create plane from 20 seconds until 320 seconds
2  with_values ICAO = "39AC47"
3  and GROUNDSPEED = 102.2 assert "GS too low"
4  and CALLSIGN = "SAMU25"
5  global assert "Fake aircraft detected"
```

Fig. 2: Example of a Ghost Aircraft Injection

Artificial Intelligence Expert

ML Models

Traffic Controller

Training with True and Falsified Scenarios

1. FDIA Generation using constraint-based testing

2. FDIA Detection using deep reinforcement learning

3. Analysis and Recommend.

Real Traffic Scenarios

Testing with Falsified Scenarios

FDIA Comparaison and Classification

Traffic Controller

Operational Traffic Management Systems

Air, Maritime, Connected Vehicles

FDIA Alerts

T-SAR

AI-Powered Testing of False Data Injection Attacks Against Transport Infrastructures