WIRELESS ATTACKS ON AIRCRAFTS

Mohan Prabhu Selvaraj, MS-IoT, INSA

Presentation Agenda

1. Introduction
2. Signal Spoofing Attacks
3. Attacks Evaluation & Results
4. Conclusion

■ Author's Agenda

The authors wrote that "resilience of the aircraft landing systems to adversarial wireless attacks have not yet been studied in the open literature, despite their criticality and the increasing availability of low-cost software-defined radio (SDR) platforms."

So, the authors did— ***explore and show the vulnerability of aircraft instrument landing systems to wireless attacks.***

■ Key Technologies

ILS, Localizer, Glideslope, GPS, SDR, ILS spoofing, Overshadow attack, Single-tone attack, Air traffic controller

INTRODUCTION

Research Problems

ILS Subsystems, Signal generation

Landing course correction

Aircraft Wireless technologies

- ADS-B, TCAS, ACARS, GPS, ILS
  - *Localization, collision avoidance, addressing & reporting, Landing guidance*
- 59% of fatal accidents during landing (**Boeing**)

Research Problem

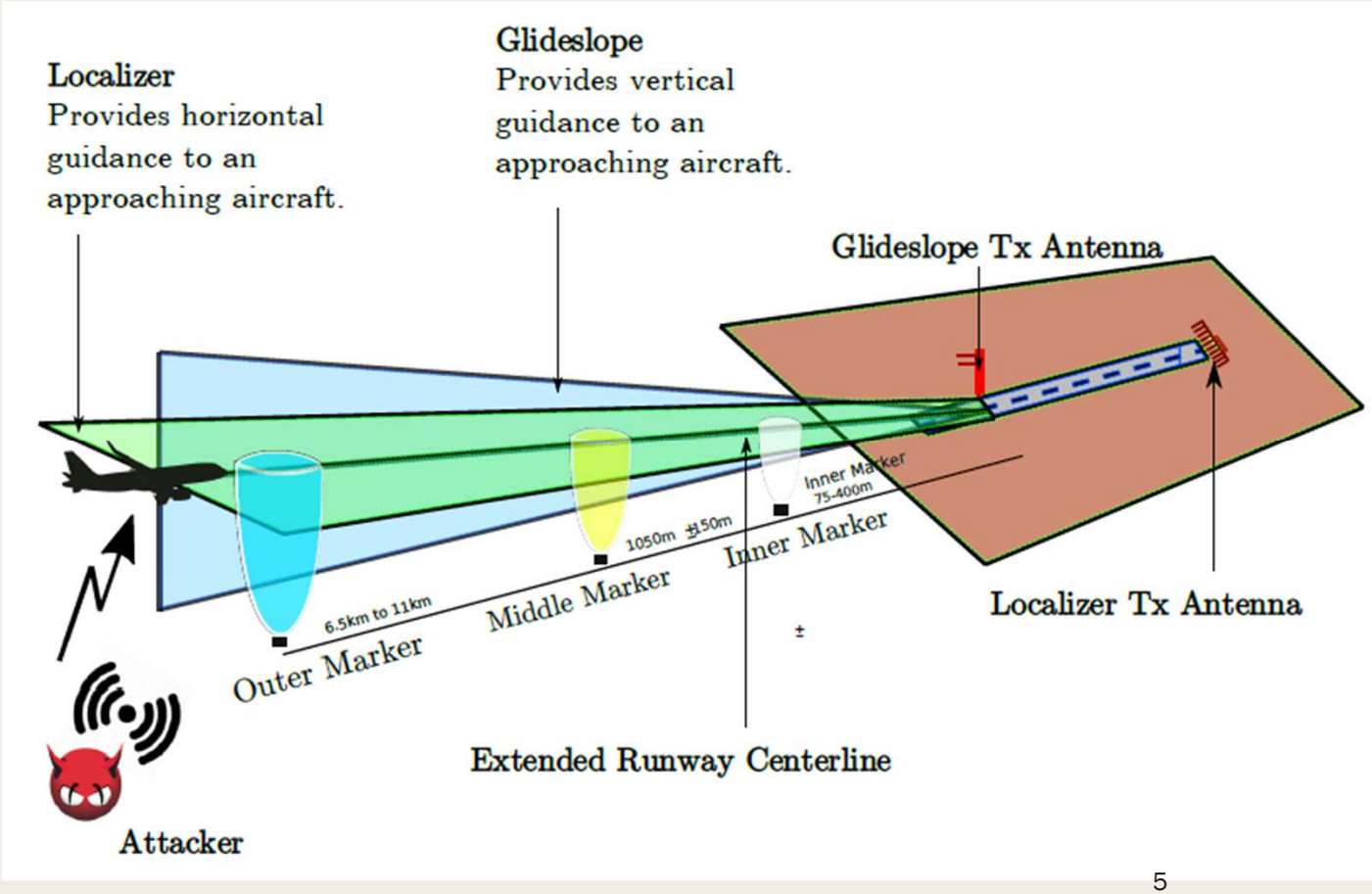
- How vulnerable are the landing technologies (ILS systems) to the wireless attacks?
- How feasible is to spoof the ILS radio signals using the SDR?
- How the potential attacks can be demonstrated and how they can be evaluated?

ILS Sub-systems

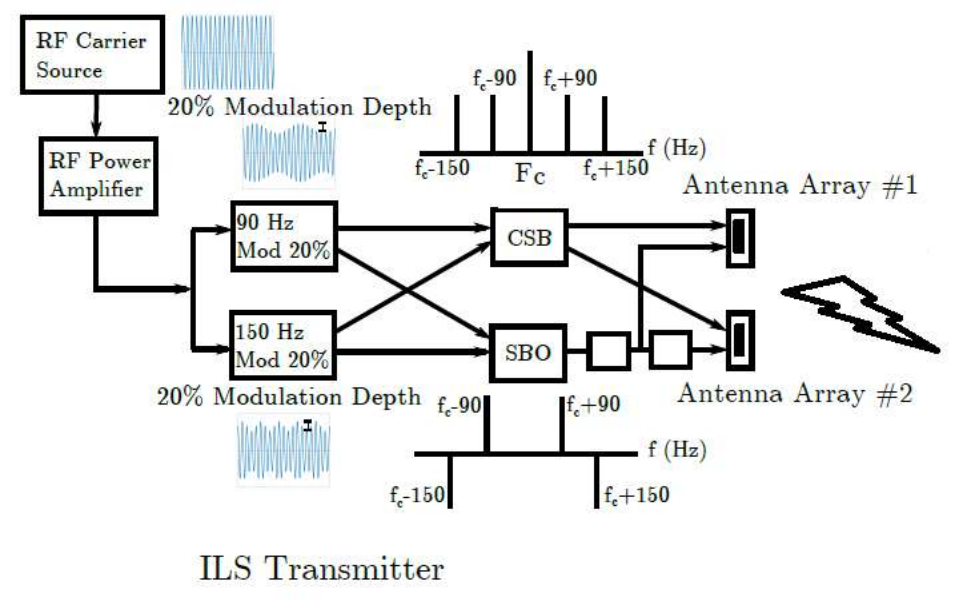
- Real-time guidance
- Localizer - Vertical
- Glideslope - Horizontal
- Beacons

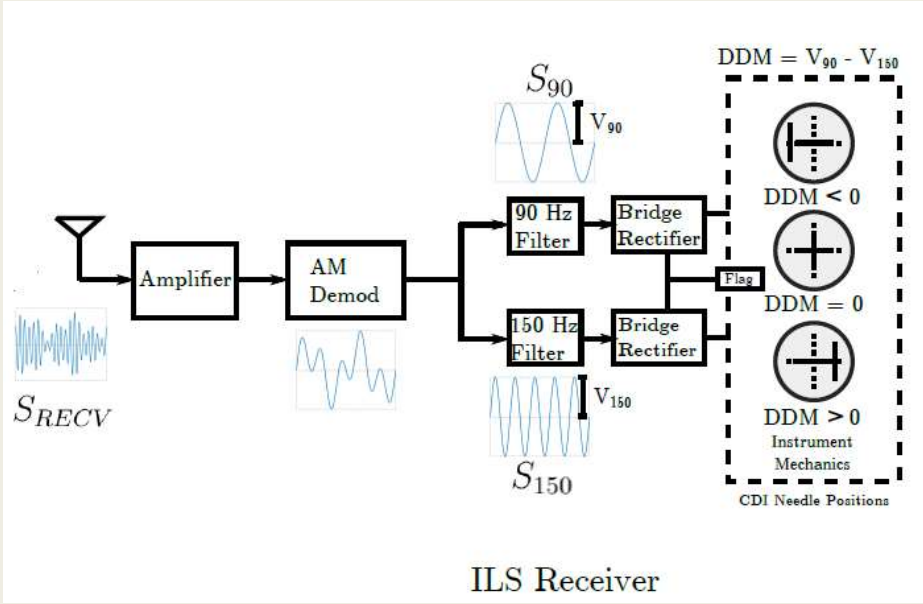
- No encryption or auth
- 300 ILS related accidents

- 600$ SDR attack method



ILS Signal Generation





- 5 MESSAGES: Center, Left, Right, Above, Below
- 150 Hz and 90 Hz signals
- Amplitude Modulation of 150 Hz & 90 Hz
- Generating the DDM

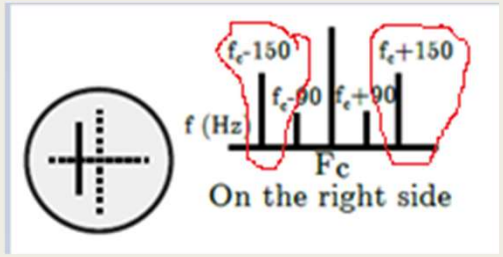
- DDM – Difference in Depth of Modulation
- Scenario's:
  - ***DDM = 0,*** *Flight is on Runway (Center)*
  - ***DDM < 0,*** *Flight is on RIGHT of center (OR) above the glide path*
  - ***DDM > 0,*** *Flight is on LEFT of center (OR) below the glide path*

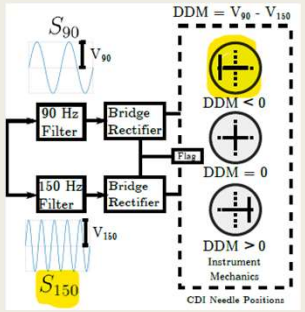
How ILS guides course correction

- **Flight is on RIGHT of Runway**

  150 Hz signal is made dominant;

  it indicates the pilot to steer left

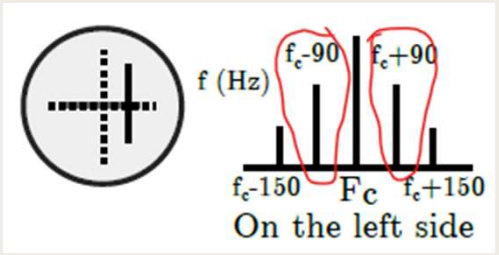


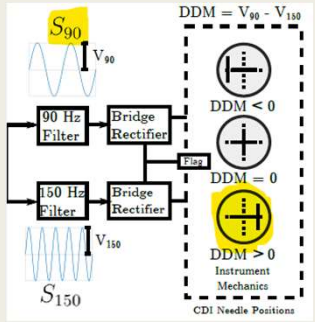


- **Flight is on LEFT of Runway**

  90 Hz signal is made dominant;

  it indicates the pilot to steer right.





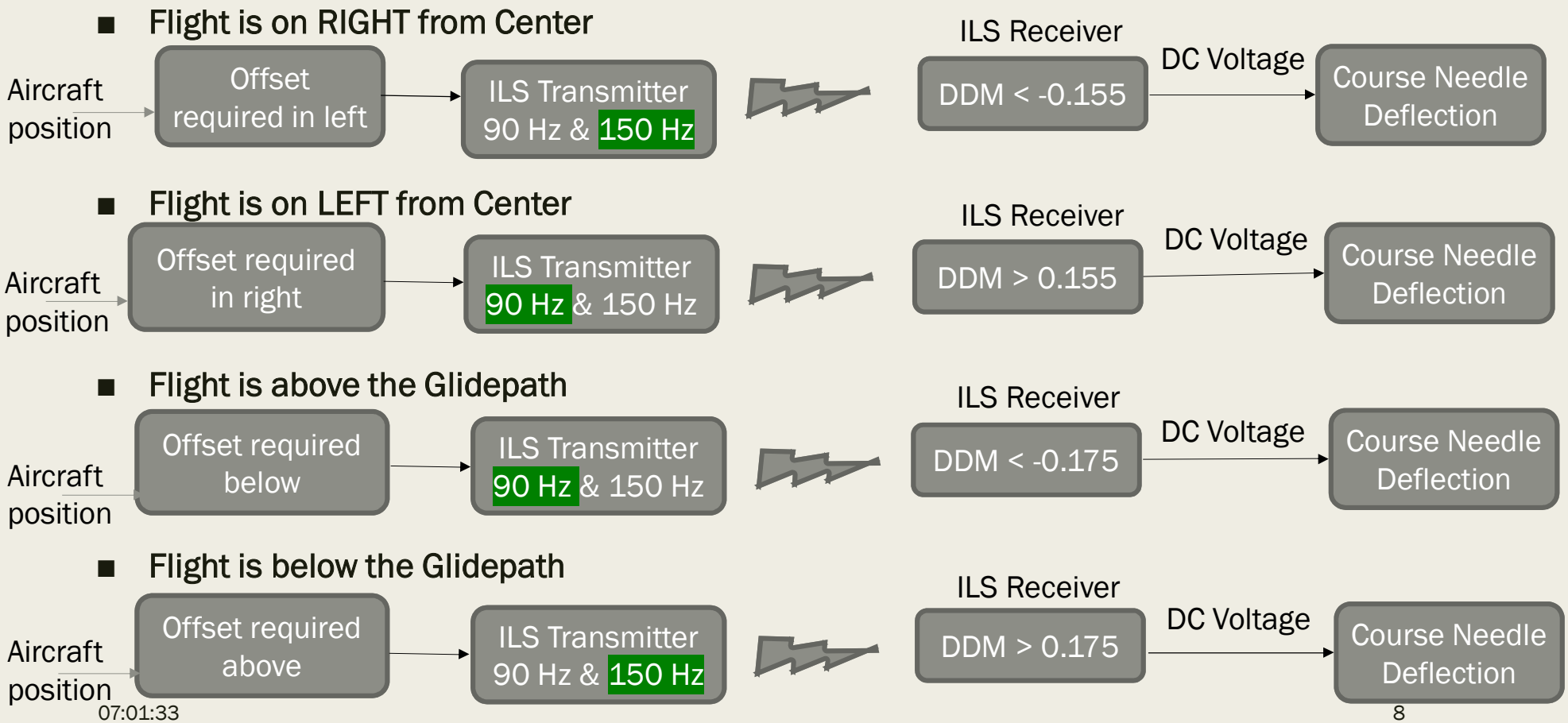
- **Flight is above the Glidepath**

  90 Hz signal is made dominant; it indicates the pilot to steer below.

- **Flight is below the Glidepath**

  150 Hz signal is made dominant; it indicates the pilot to steer above.

How course correction maneuvers work



SIGNAL SPOOFING ATTACKS

Attack Situation

Overshadow attack

Single-tone attack

Attack Situation

Aircraft in landing phase

- Pilot receives the landing clearance
- Pilot tunes to localizer/Glideslope freq
- Pilot verifies the runway identifier
- Chooses manual or auto-land feature

Attacker waiting to launch attack

- Assumptions on attacker
  - *Expert in ILS signalling*
  - *Expert in using SDR*
  - *Location: Onboard or on ground*

How Overshadow attack works

- Overshadow the legitimate ILS signal by overpowering the ILS Tx signal.
- How does the attacker thinks?

Where to misguide the Aircraft?
- Right or left of the runway?
- Above or below the glidepath?

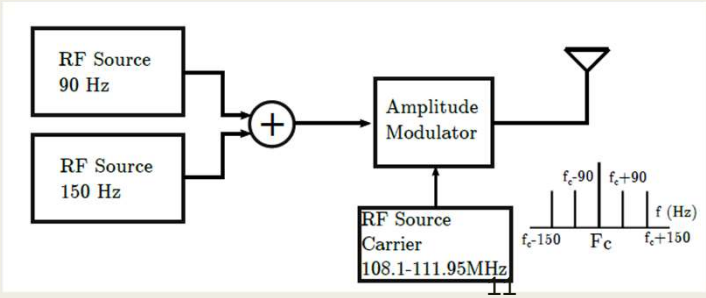
What is the desired offset?
- How much right or left?
- How much below or above?

What should be the DDM value?
- DDM < -0.155
- DDM > 0.155
- DDM < -0.175
- DDM > 0.175

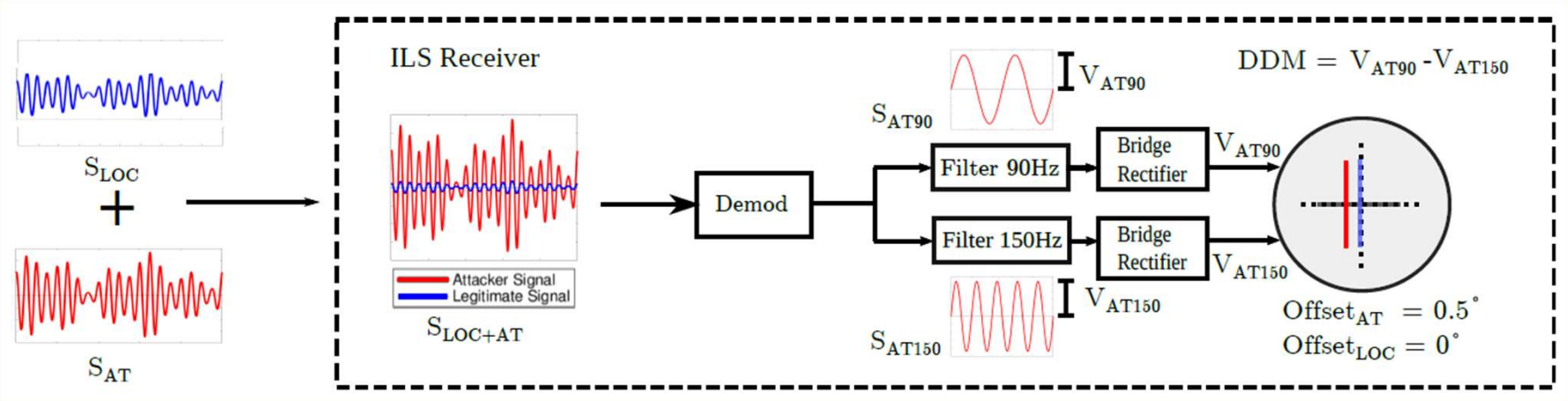
How much amplitude modulation?
- **Localizer**: Dominant - 90 hz or 150 hz?
- **Glideslope:** Dominant – 90 hz or 150 hz?

- Overshadow successful?
- CDI needle deflection as desired?

Overshadow Signal Generator



Misguiding to Steer left

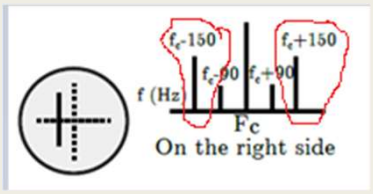


- Overshadow ‘Precrafted’ signal is sent as -> “Flight is on RIGHT from Center”

The attacker makes Offset = 0.5 ° and 150 Hz signal as dominant; it indicates the pilot to steer left.

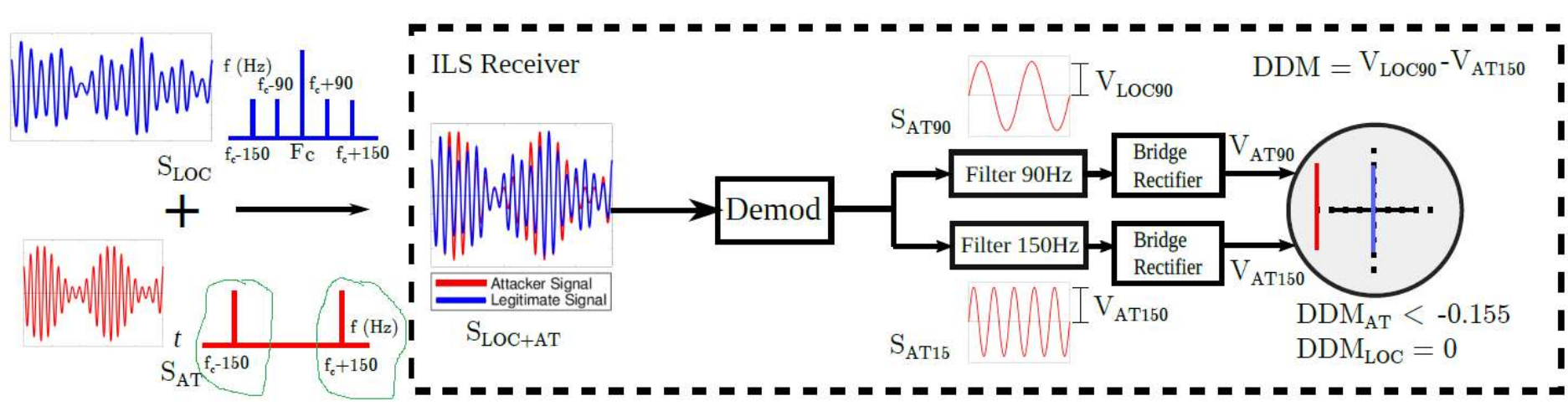
Offset = 0.5 ° to steer left → DDM < -0.155 → ILS Transmitter 90 Hz & 150 Hz

ILS Receiver



DC Voltage → Course Needle Deflection

How Single-tone attack is different?



- **Single-tone 'Precrafted' signal is sent as -> "Flight is on RIGHT of Runway"**

  The attacker makes transmits ONLY the dominant 150 Hz signal;

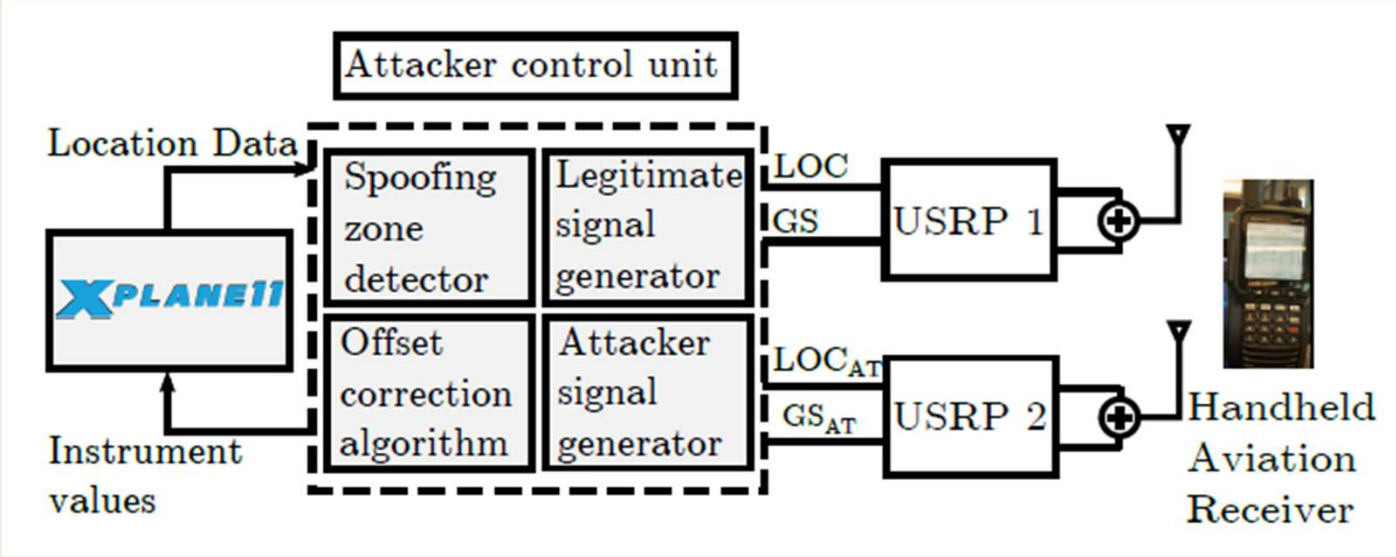
  It indicates the pilot to steer left.

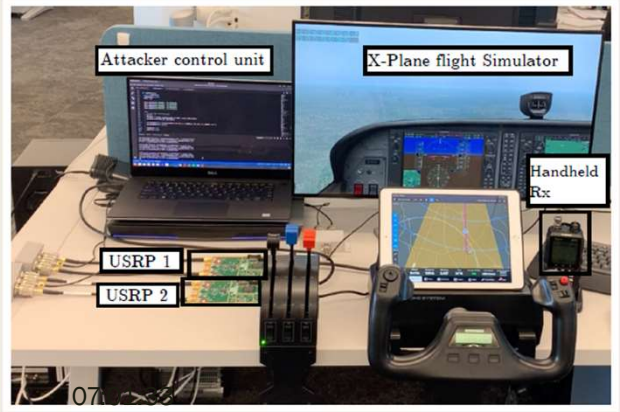
ATTACKS EVALUATION & RESULTS

Experiment Setup

Results

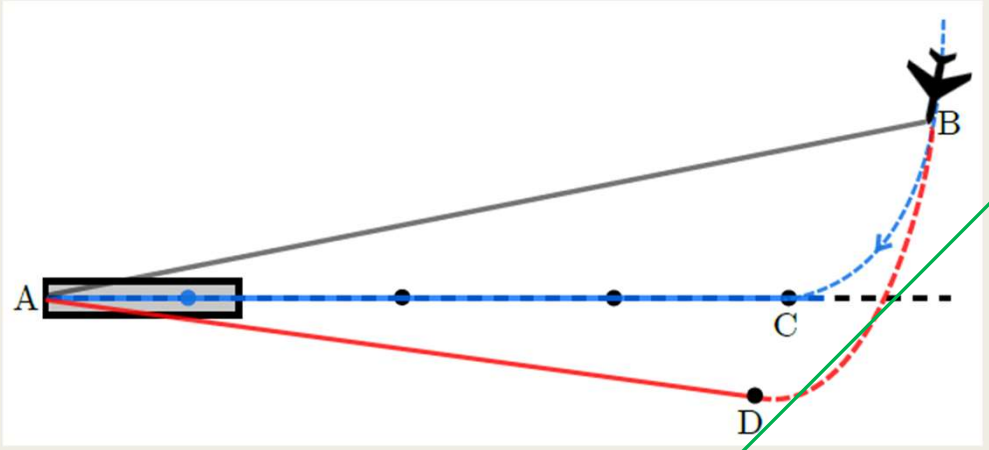
Attack Experiment Setup





- Spoofing zone detection
  - *Final approach patterns, even-odd algorithm*
- Offset correction Algorithm
  - *Aircraft location data (from ADS-B), real-time offsets*

Attack Signal Generation



Algorithm 1 Offset correction algorithm.

```
1: procedure GETANGLEDIFFERENCE
2:     ∠DAC ← TargetedLocalizerOffset
3:     ∠BAC ← GetAngle(location)
4:     difference ← ∠DAC − ∠BAC
5:     return difference
6: procedure CALCULATEDDM
7:     difference ← GetAngleDifference
8:     ddm ← (0.155 ∗ difference)/2.5
9:     AT90 ← 0.2 + (ddm)/2
10:    AT150 ← 0.2 − (ddm)/2
11:    ChangeAmplitude(AT90, AT150)
```

- Right or left of the runway? -> **LEFT**

Where to misguide the Aircraft?

What is the desired offset?

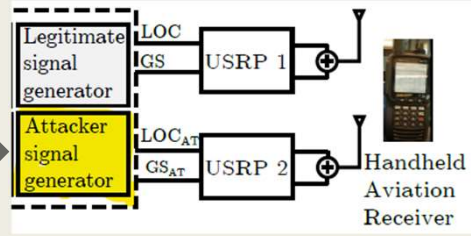
- **How much** left?

- What is the DDM?

What should be the DDM value?

How much amplitude modulation?

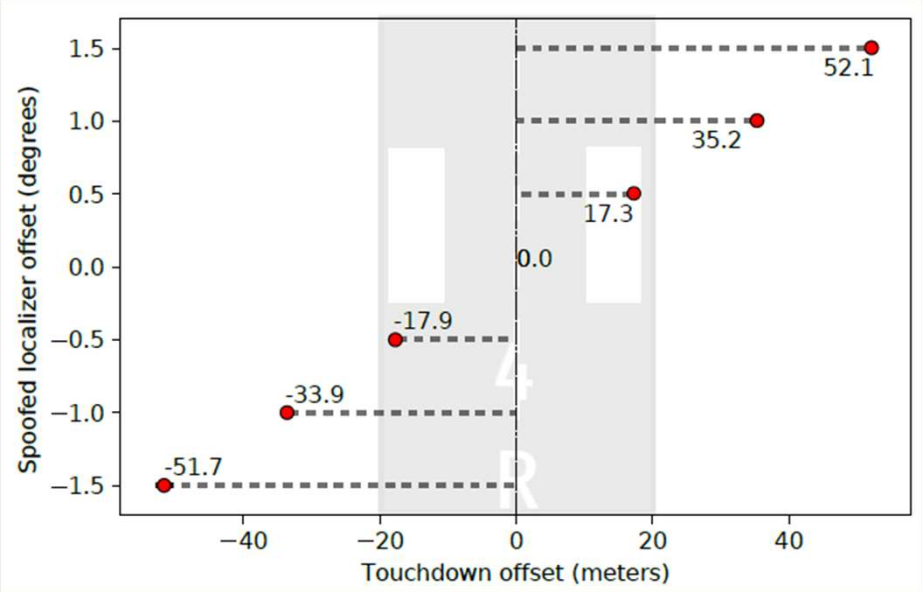
- **Localizer:** How much Dominant 150 hz?



Evaluation Results

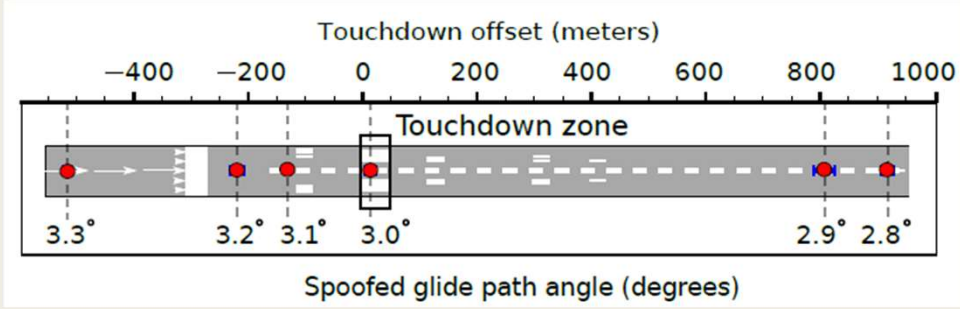
Horizontal Spoofing

- Localizer Offsets



Vertical Spoofing

- Glideslope Offsets



- Horizontal Spoofing (Localizer) Offsets
  - *-0.5, -1.0, -1.5 (LEFT)*
  - *0.5, 1.0, 1.5 (RIGHT)*
- Vertical Spoofing (Glideslope) Offsets
  - *2.8° to 3.3°*

CONCLUSION

Security solutions

Further research

CONCLUSION

- ILS is vulnerable; GPS failsafe solutions do fail.
- ADS-B and other supporting technologies are also vulnerable
- Cryptographic solutions are not sufficient to prevent the localization attacks
- Widespread availability of powerful & low cost SDR platforms has increased the threats

FURTHER RESEARCH

- Wide-area secure localization system & secure proximity verification techniques
- GPS spoofing mitigation solutions & new systems for ‘receiver’ end
- GNSS based security
  - Septentrio AIM+ *(Advanced Interference Mitigation)*
  - *Commercial Authentication Service (CAS)*
  - *Chimera authentication system*

THANK YOU