

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, Guevara Noubir
Northeastern University, Boston MA



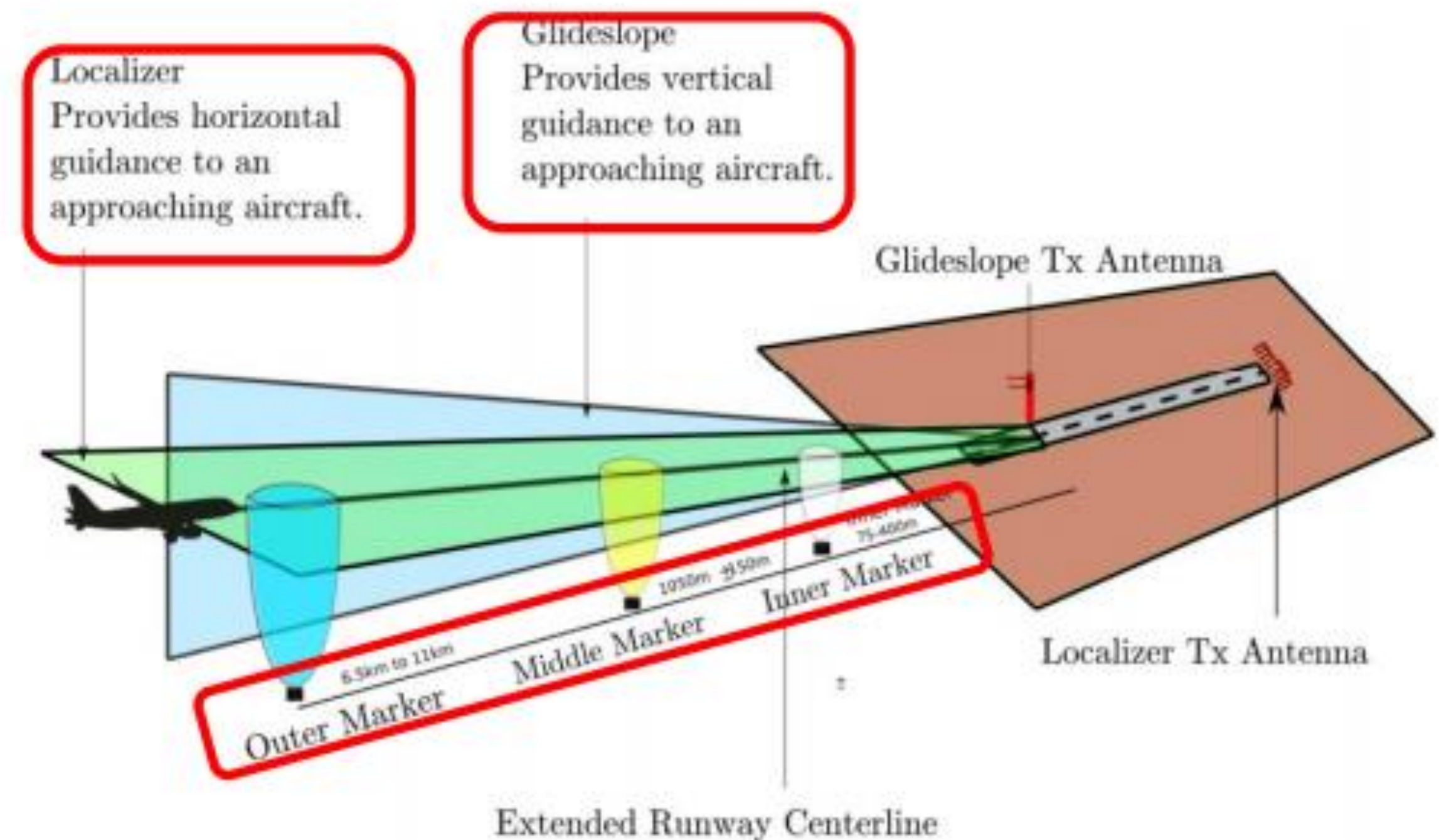
15000 flights!!



<https://www.flightradar24.com/1.27,51.96/3>

Aircraft Instrument Landing System (ILS)

- Final approach or landing phase is one of the **most critical** phases
- According to Boeing **59%** of the fatal accidents occur during the final approach phase
- ILS provides **precise lateral** and **vertical** guidance even in extreme weather conditions using wireless radio signals



Incident: Singapore B773 at Munich on Nov 3rd 2011, runway excursion

By Simon Hradecky, created Monday, Dec 17th 2018 16:15Z, last updated Monday, Dec 17th 2018 16:15Z

On Dec 17th 2018



**Turkish Airlines – Boeing B737-800
(TC-JGE) flight TK1951**

False Localizer Signal

A business jet was in clouds when the pilots initiated a steep descent, following a spurious navigation signal high terrain.

by Mark Lacagnina | October 6, 2010

The flight crew initiated an emergency return to an Irish airport after the Gulfstream IV-SP's windshield cracked during takeoff in instrument meteorological conditions. The aircraft was outside the localizer coverage area when the crew armed the autopilot approach mode. As a result, the autopilot captured a false localizer signal. The crew then deviated from the instructions they had received from air traffic control (ATC) and initiated a rapid descent while

Russian Tu-22M3 crash: Expert says instrument landing system to blame 'hard' landing

Jan 27, 2019 | Aviation News



Spectre of false glideslope emerges in Bishkek 747 crash

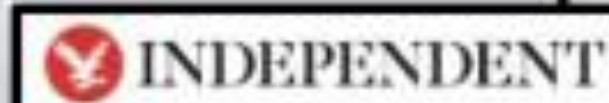
09 FEBRUARY, 2017 | SOURCE: FLIGHT DASHBOARD | BY: DAVID KAMINSKI-MORROW | LONDON

Preliminary information about the Boeing 747-400F crash at Bishkek appears to indicate that the aircraft encountered a false glideslope before initiating its fatal descent, and that the crew attempted a go-around.

Avionics
ATM Modernization, Commercial, Military

Securing ACARS: Data Link in the Post-9/11 Environment

By Charlotte Adams | June 1, 2006
Send Feedback



Security of ADS-B: State of the Art and Beyond

Martin Strohmeier*, Vincent Lenders+, Ivan Martinovic*
*University of Oxford, United Kingdom
+armasuisse, Switzerland

ENABLING NEXT-GENERATION AIRBORNE COMMUNICATIONS

Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B

Martin Strohmeier, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic

RESEARCHER SHOWS HOW TO HACK (AND CRASH) A PASSENGER AIRCRAFT WITH AN ANDROID PHONE...

Personalized - Security Research Team - April 2013

Hugo Teso

The Register
Biting the hand that feeds IT

Security

Texas students hijack superyacht with GPS-spoofing luggage

Don't panic, yet

By Iain Thomson in San Francisco 29 Jul 2013 at 18:04

58 SHARE

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department
EURECOM

Sophia-Antipolis, France
a.costin@eurecom.fr, aurelien.francillon@eurecom.fr

AINonline

ADS-B Is Insecure and Easily Spoofed, Say Hackers

by Matt Thurber - September 3, 2012, 12:45 AM

A \$225 GPS spoofer can send sat-nav-guided vehicles into oncoming traffic *

* Some restrictions apply.

DAN GODDIN - 7/18/2018, 7:30 AM

ADS-B Security Risk Remains Unresolved for US Military

By Woodrow Bellamy III | October 4, 2018
Send Feedback | @WBellamyIIIAC

ADS-B, DoD, FAA, security

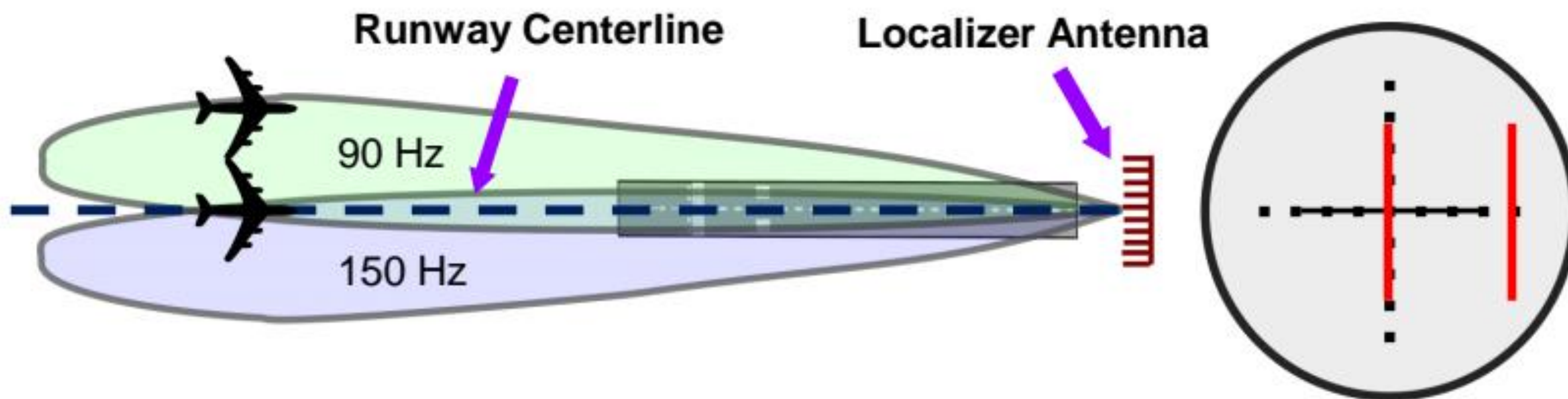


Our contributions

- Demonstrate two types of attacks: 1) **Overshadow** and 2) **Single-tone attack** for taking over ILS
- Develop a **closed loop tightly controlled** ILS spoofer that in real-time adjusts the spoofing signals as a function of aircraft's current location
- Demonstrate the attacks on a **flight simulator software** which satisfies **FAA certification** requirements (X-Plane)
- Systematically evaluate the performance of the attack using **X-Plane's AI based autoland feature** resulting in touchdown offsets of **18 meters** to over **50 meters**

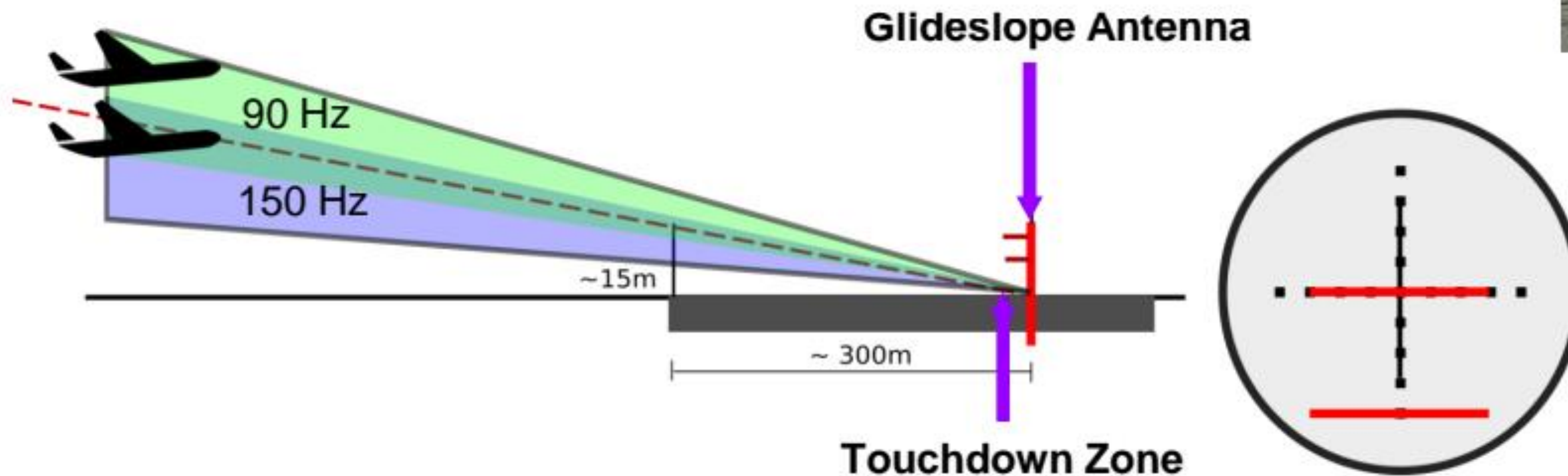
Localizer

- Enables the receiver to calculate its **location** with respect to the **runway centerline**
- The instrument guides the pilot to properly align itself
- Antenna array installed at the **end of the runway** transmits a **25W signal**
- Transmission pattern creates a lobe on each side of the runway centerline:

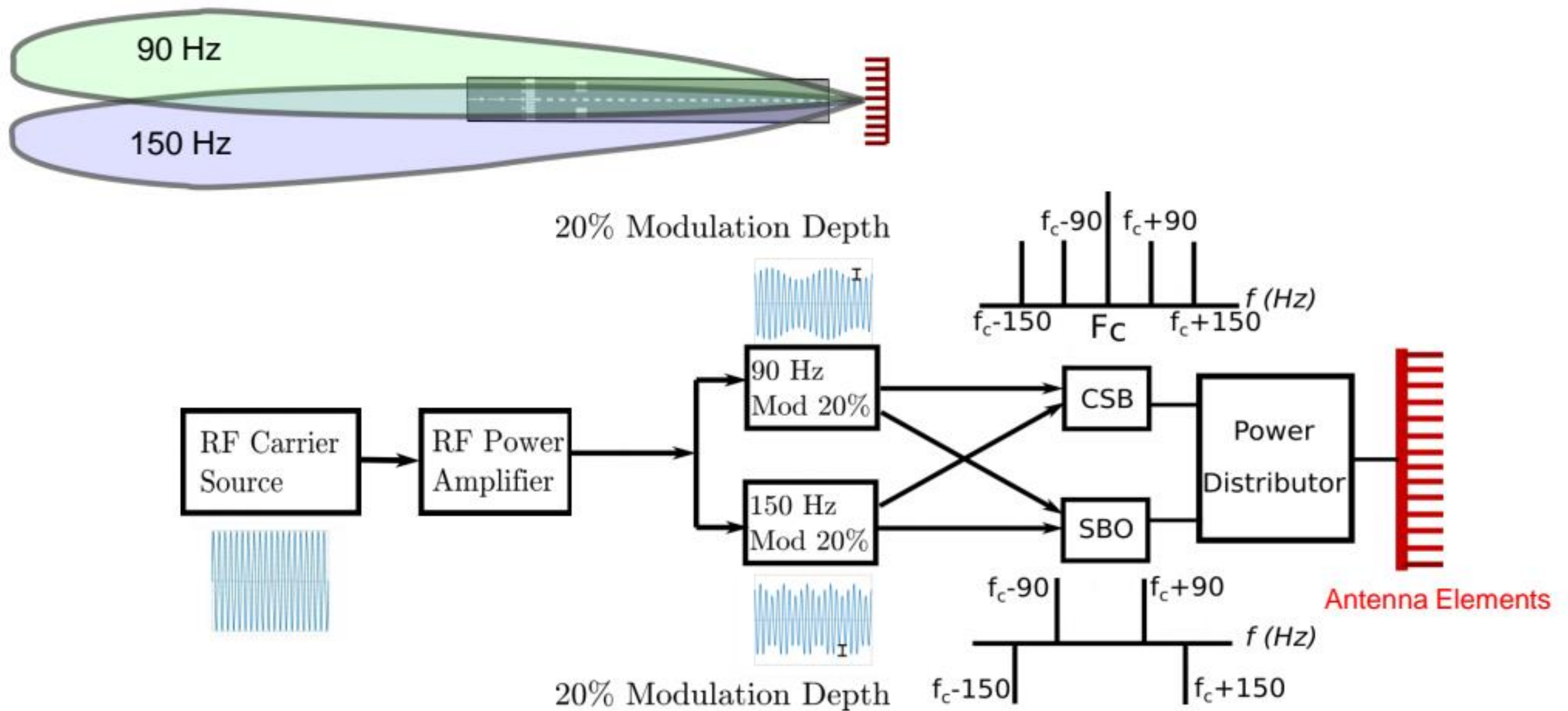


Glideslope

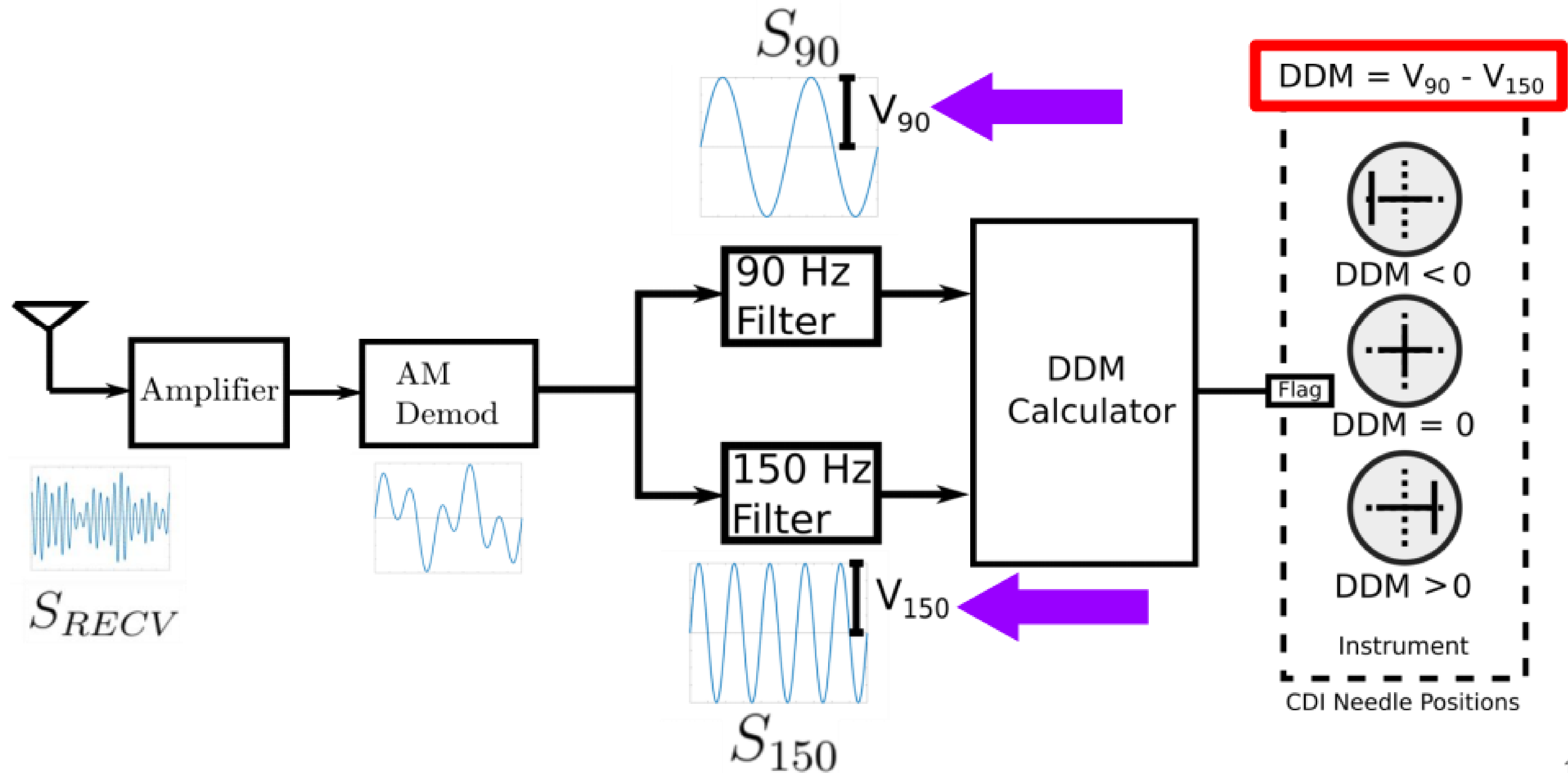
- Enables the receiver to calculate its location with respect to the **glidepath**
- The instrument guides the pilot to set a perfect glidepath angle
- Antenna installed near the **touchdown zone** transmits an **8W signal**
- Transmission pattern creates a lobe on each side of the glidepath



ILS Transmitter



ILS Receiver



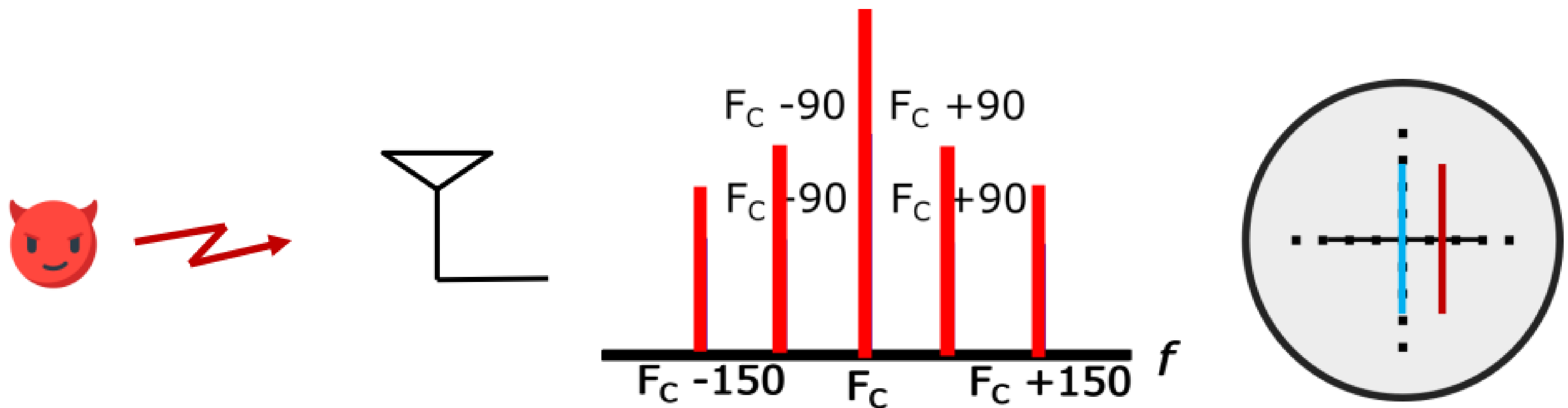
Wireless Attacks

- Needle deflection depends only on the **power of the received 90 Hz and 150 Hz tones!**
- **Objective of the attacker:**
 - Manipulate DDM calculation
 - Force the aircraft to **overshoot the runway** or **completely miss the approach**
- We discuss two attacks:
 - Overshadow attack
 - Single-tone attack

With minor changes, the attacks work for both the localizer and the glideslope

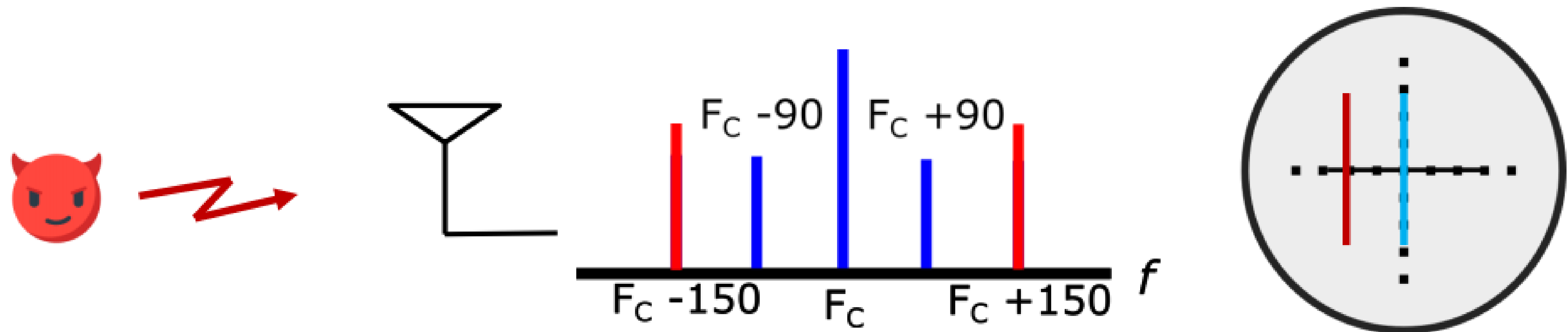
Wireless Attacks: Overshadow Attack

- Attacker transmits a **high power pre-crafted** ILS signals
- A typical wireless receiver always **locks on to the stronger signal**
- It is sufficient to generate and transmit **signals similar to the received legit ILS signal**



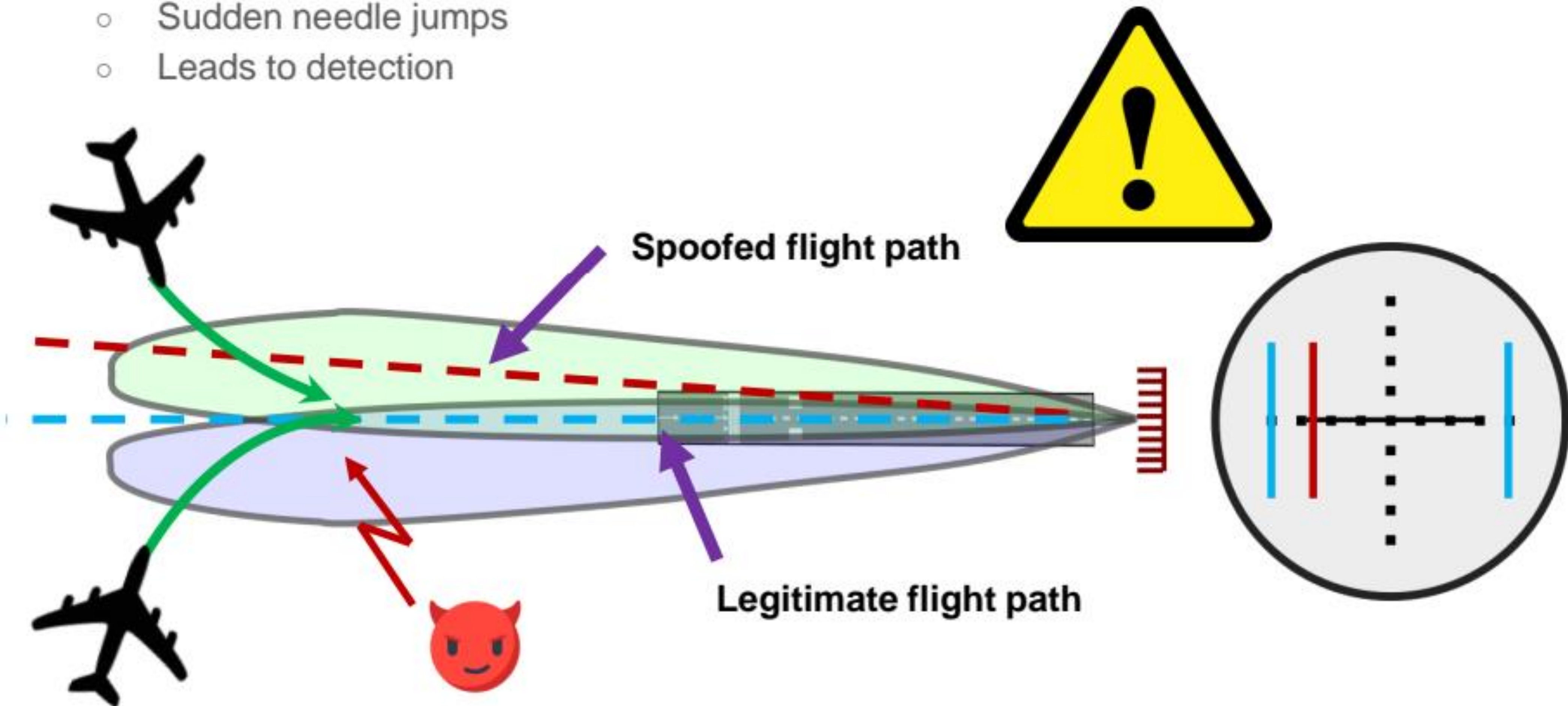
Wireless Attacks: Single-tone Attack

- Attacker **transmits** only **one of the two tones** that make up the ILS signal
- Transmitted tone interferes with the existing tones to cause needle deflection
- The attacker signal is similar to a **double sideband suppressed carrier** signal which is known to be **spectrally efficient** than a regular AM signal



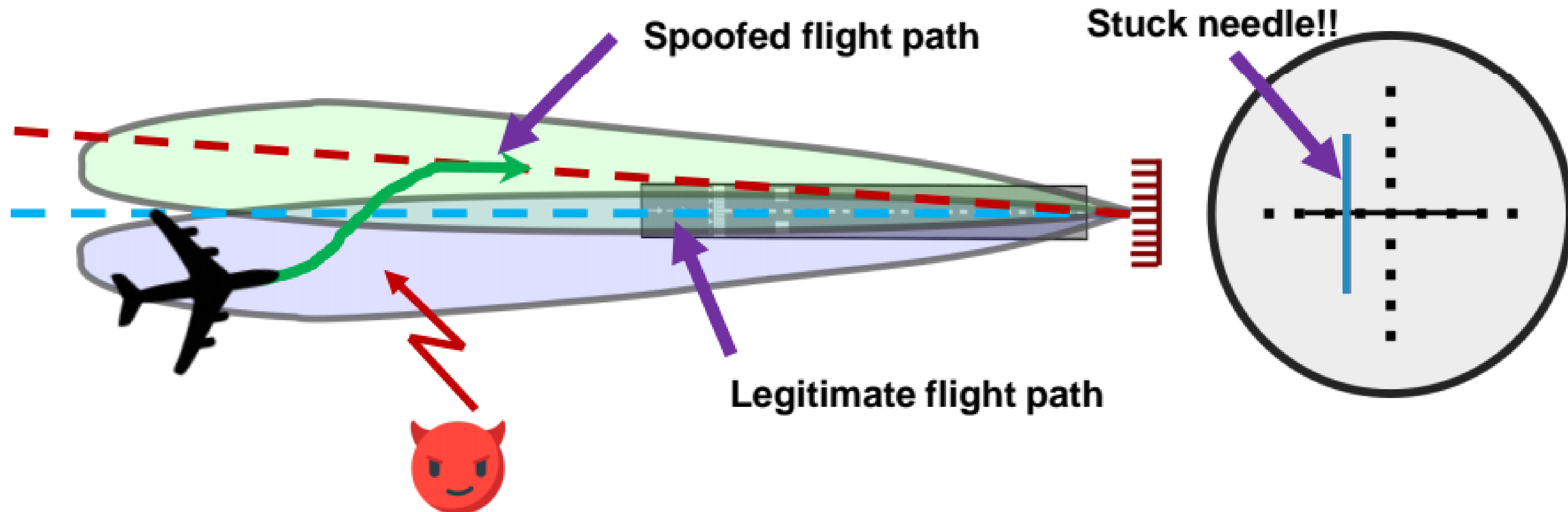
Attacker Challenges

- **Aircraft can intercept the localizer from multiple directions**
 - Sudden needle jumps
 - Leads to detection



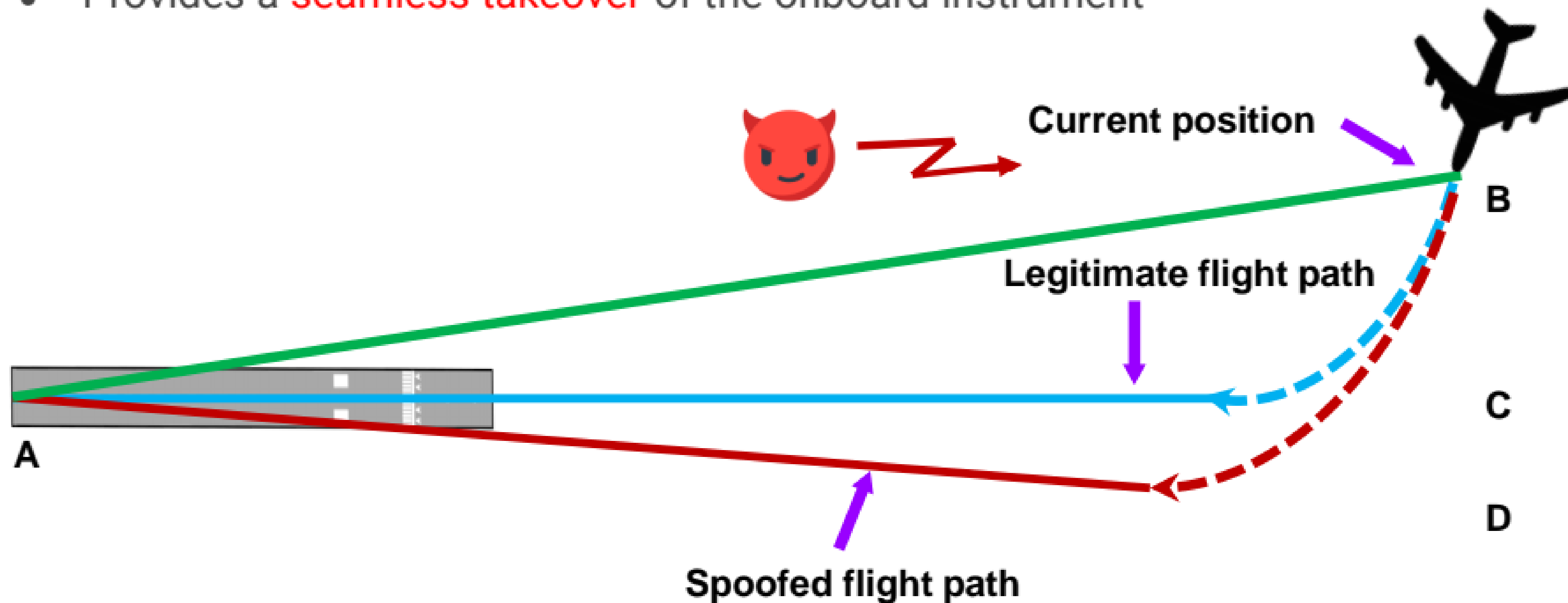
Attacker Challenges

- **Naïve overshadow attack results in fixed unreactive offset**
 - Easy detection
 - Attack never succeeds



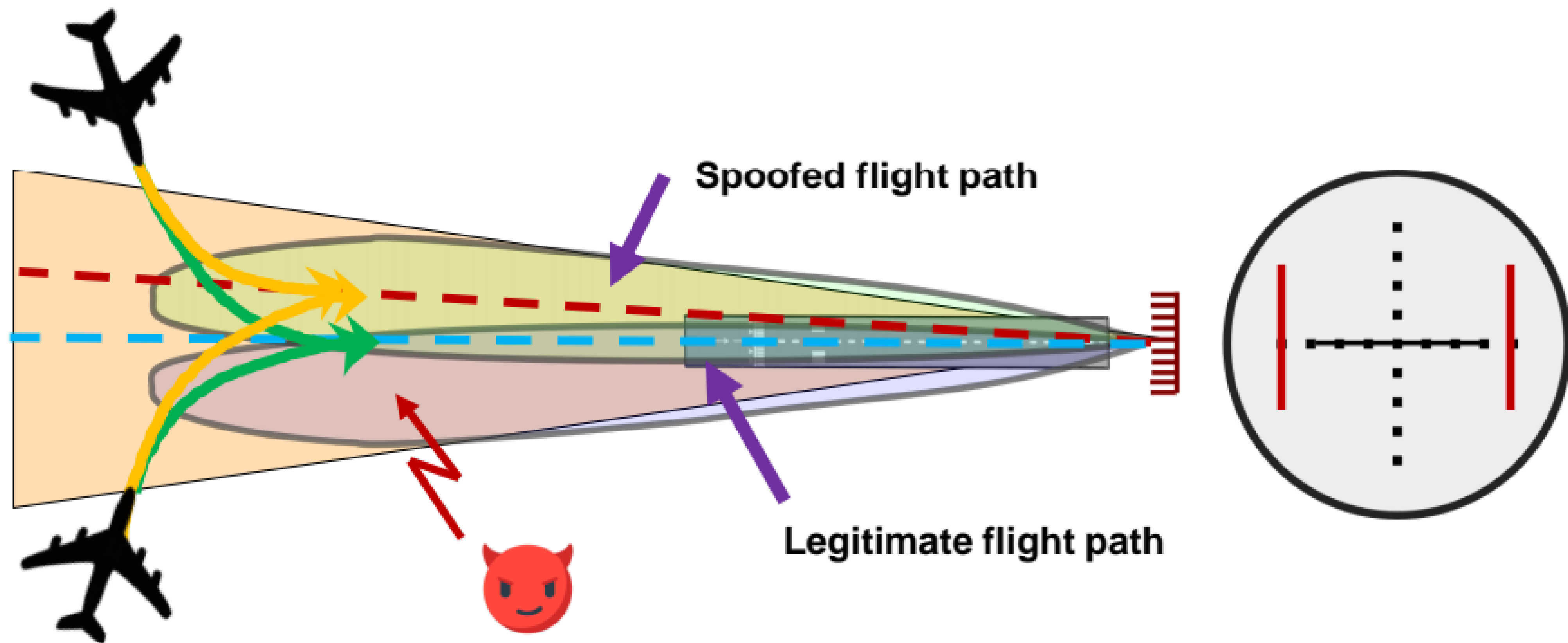
Offset Correction Algorithm

- **Real time** offset calculation and signal generation
- Adjusts attacker's signal as a **function of aircraft's GPS location**
- Provides a **seamless takeover** of the onboard instrument

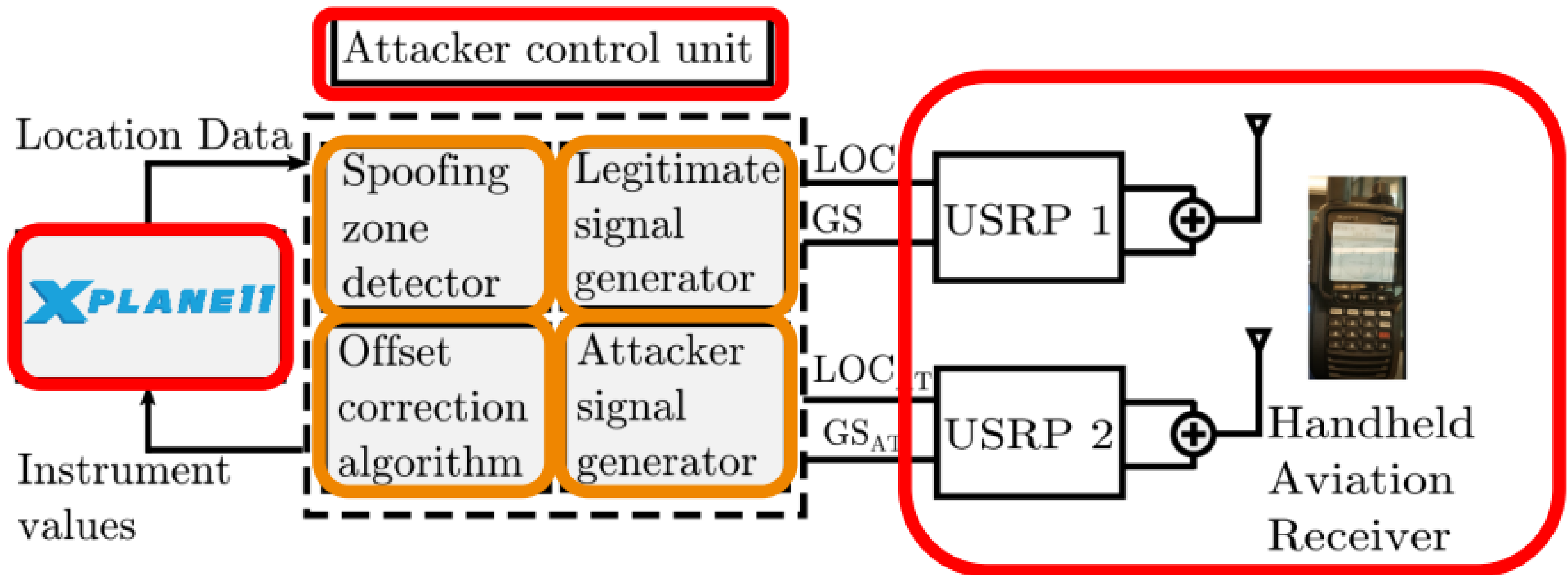


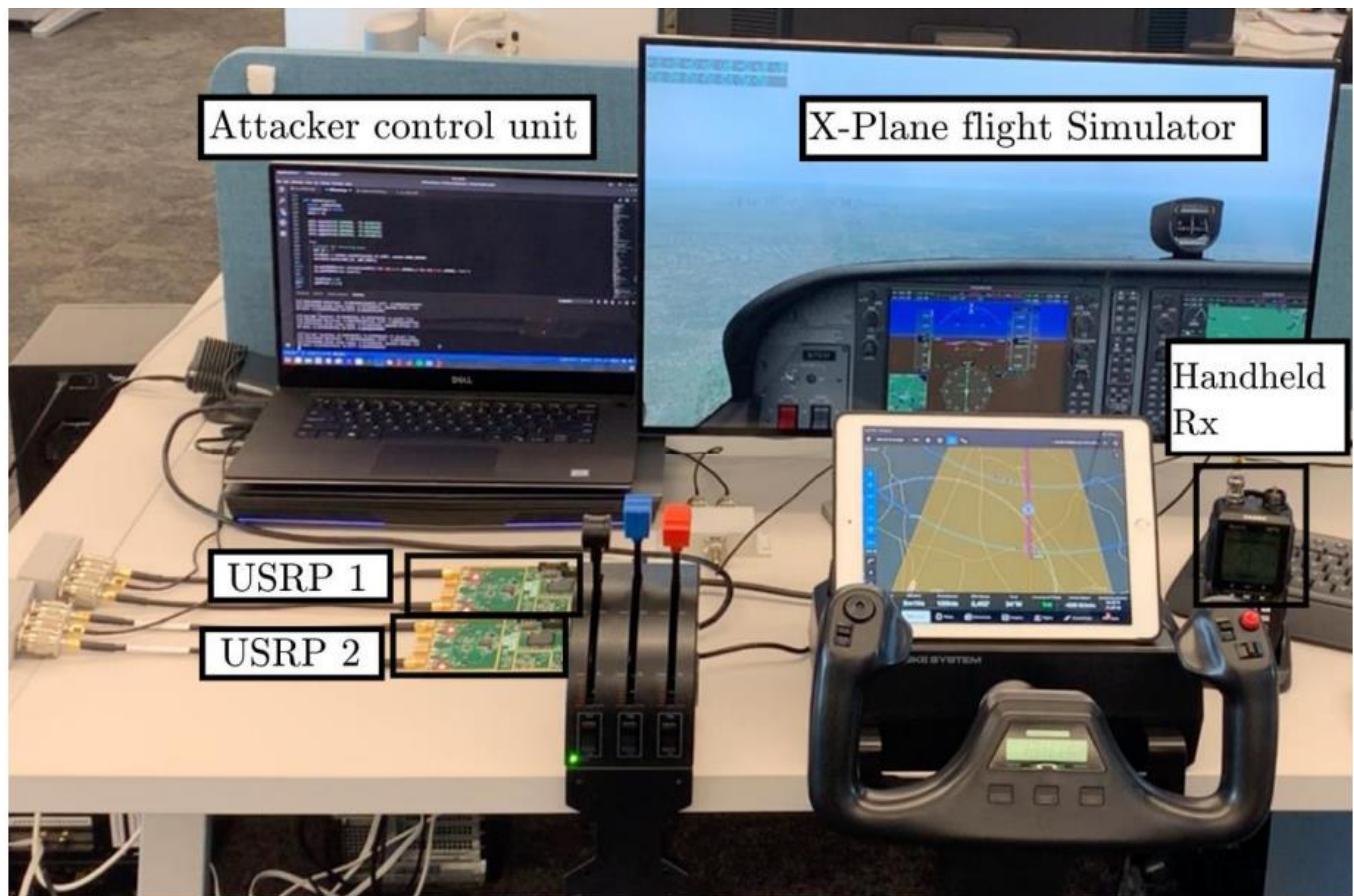
Spoofing Zone Detector

- Enables **timely** and **automated triggering** of the attack
- Detects if the target aircraft has entered the **area of final approach**
- Avoid sudden needle jumps



Experimental Setup

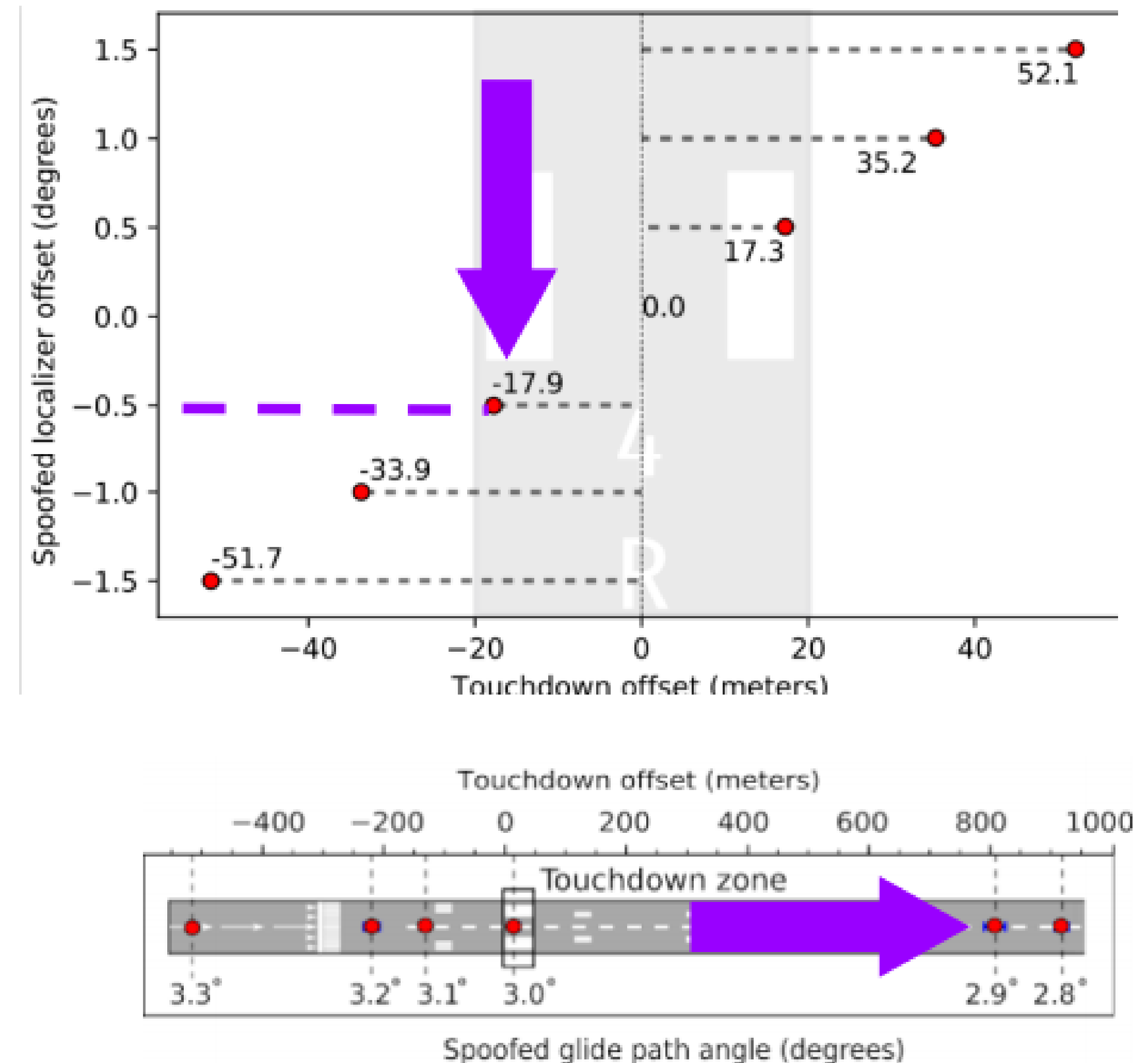




Demo

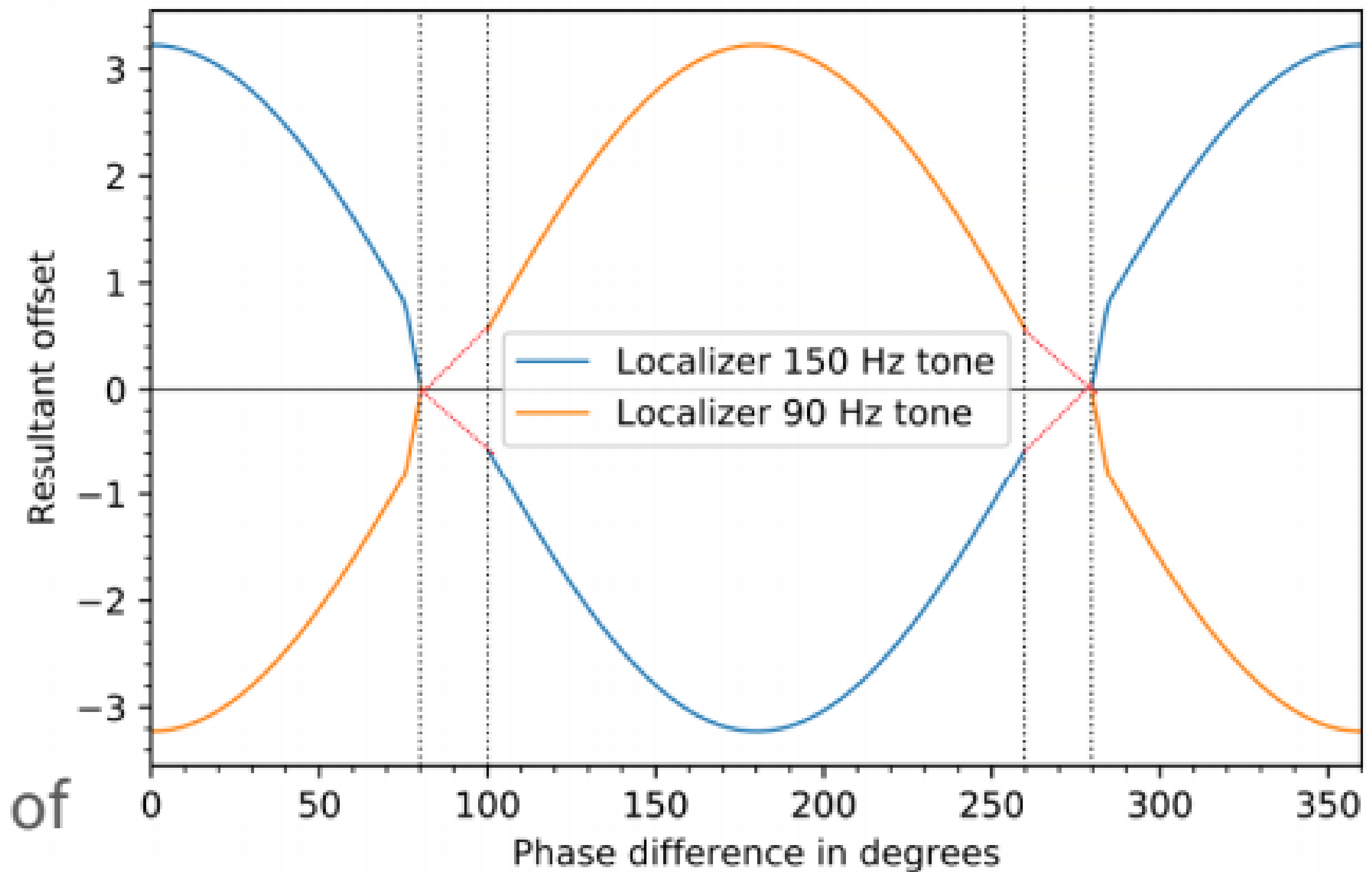
Evaluation of Overshadow Attack

- **5 test flights** with AI based automated landing were flown for **each spoofed offset**
- Even minute offsets have significant effects
- **A certified pilot** was called in to test the setup and **fly the approach** with and without spoofing

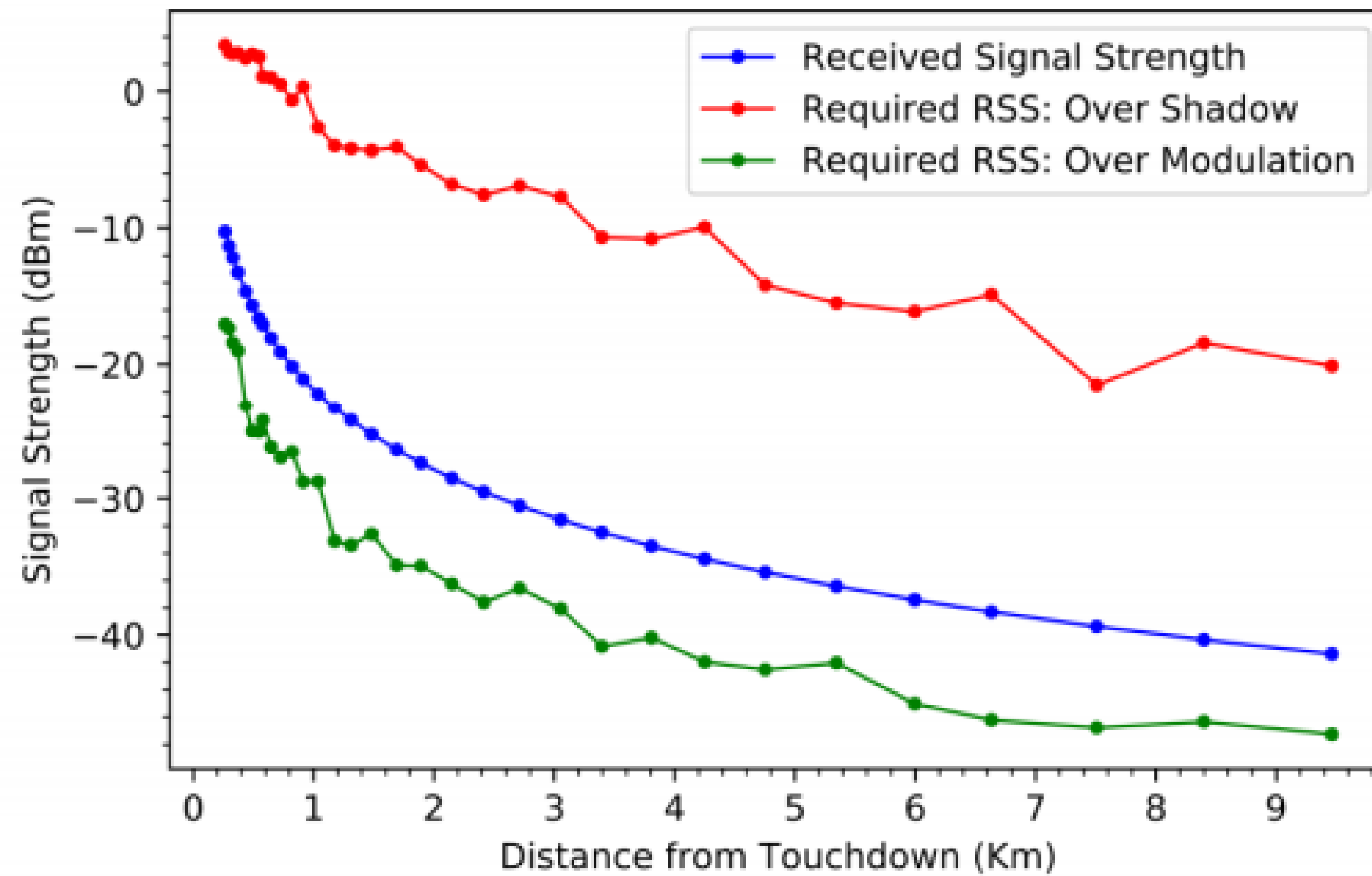


Evaluation of Single-tone Attack

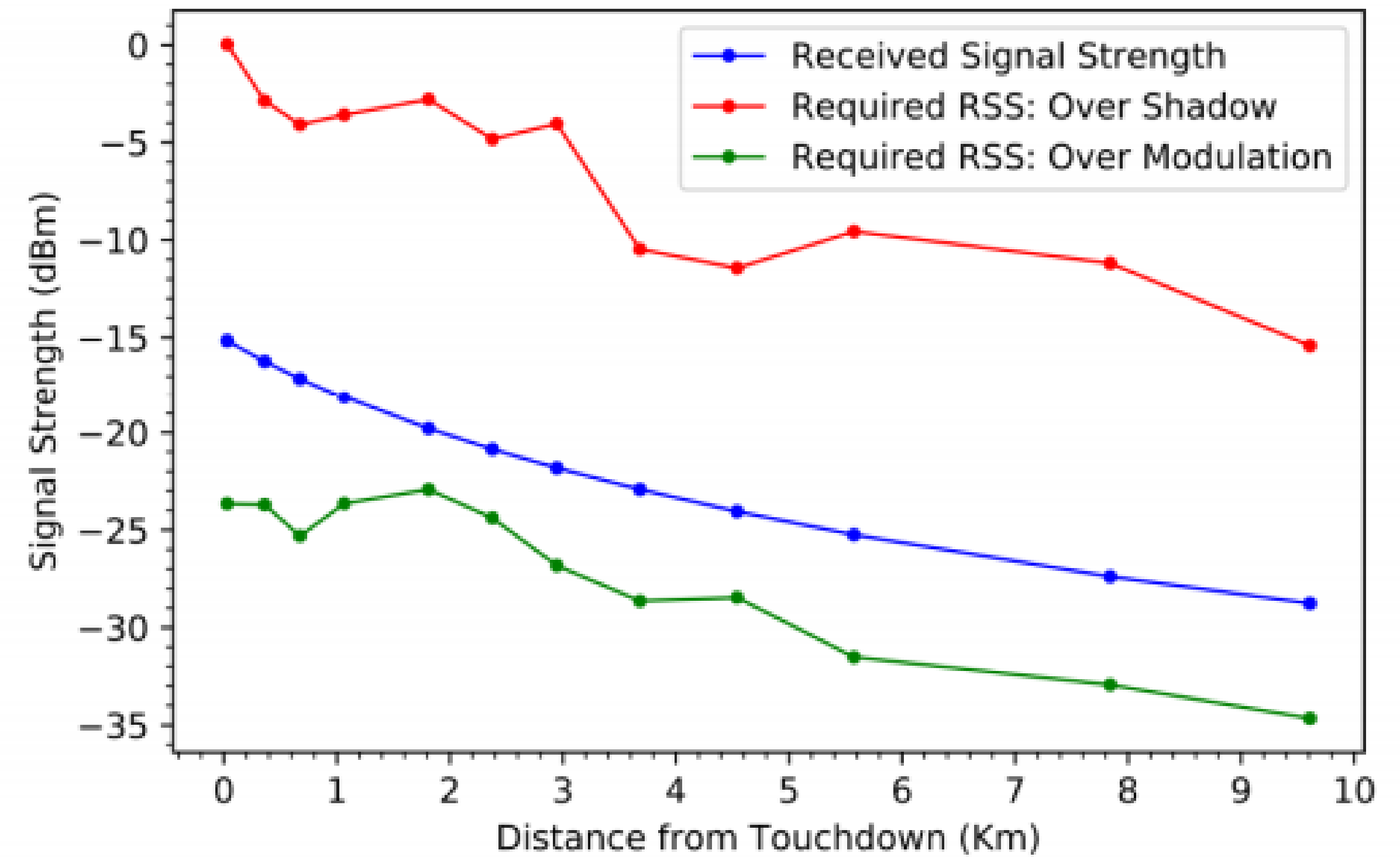
- Single-tone attack is susceptible to phase changes
- Effect was **less severe** on the handheld receiver:
It depends on:
 - **Speed of the approaching aircraft**
 - **Refresh rate of the instrument**
- Amplitude scaling for countering the effect of phase
- Unpredictable needle deflections can be used as a low power last minute DoS attack



Comparison of Power Requirements



Localizer



Glideslope

Summary

- ILS is vulnerable to spoofing attack
- The attacks were **successfully demonstrated** on **flight simulator software** which satisfies **FAA certification** requirements
- Pure analog nature makes it fundamentally challenging to secure these critical navigation systems
- Pilots have multiple other systems which they can rely on for recovery if the attack is detected in time

Thank you!

sathaye.h@husky.neu.edu
harshadsathaye.com

Conclusion and Discussion

- What do these attacks target in the autonomous system pipeline?
- Do you think that the authors' assumptions about:
 - The knowledge of the aircraft location is valid/strong? (Offset Correction Algorithm)
 - The knowledge of the runway Fc for both attacks
- Securing against ILS attacks:
 - Sensor Fusion
 - Sensor Design/Wireless Signal Modifications