Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir

Presentation by Colton Asnes

Table of Contents

Background

How ILS systems work

Attacks

Attack vulnerabilities; Experiment set up and results

Review

Acceptance/Rejection of paper; Discussion

Background

Everyday approximately 5,000 flights are in the air at any given time

- Atlanta's Airport handles around 2500 takeoffs and landings each day

Air traffic controllers rely on wireless technologies

- Communication with pilots via VHF
- Automatic Dependent Surveillance Broadcast (ADS-B)
- Traffic Alert and Collision Avoidance System (TCAS)
- Aircraft Communications Addressing and Reporting System (ACARS)
- Navigation aids such as GPS, Non-directional radio beacons (NDB), Distance Measuring Equipment (DME), and Instrument Landing System (ILS)

Current Documented Vulnerabilities

01

ADS-B Spoofing

Injecting non-existing aircraft into the sky

02

ADS-B Jamming

Can modify the route of victim aircrafts

03

Unsecure ACARS

Leaked personal passenger info, including medical/financial

04

TCAS Spoof

False resolution advisories that force the pilot to conduct avoidance maneuvers

Goal of the paper

To investigate the vulnerability of aircraft instrument landing systems (ILS) to wireless attacks

Instrument Landing System (ILS)

59% of fatal accidents in flight occur during descent, approach and landing (Boeing)

- First deployed in 1932 in Berlin
- ILS provides horizontal and vertical guidance
- FAA typically does not allow landing using visual estimates

Nearly 95% of landings at Boston Logan - essential to evaluate its vulnerability to cyber-physical attacks

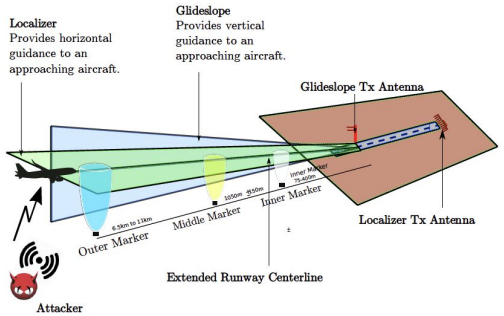


Figure 1: Overview of ILS sub-systems. The ILS consists of three subsystems: i) Localizer, ii) glideslope, and (iii) marker beacons.

Instrument Landing System (ILS) continued

Three independent subsystems:

1. Localizer
2. Glideslope
3. Marker beacons

In total, provides aircraft with horizontal and vertical guidance to indicate the distance to the desired point of landing

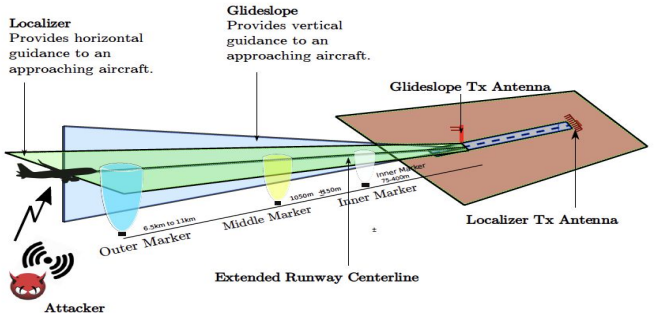
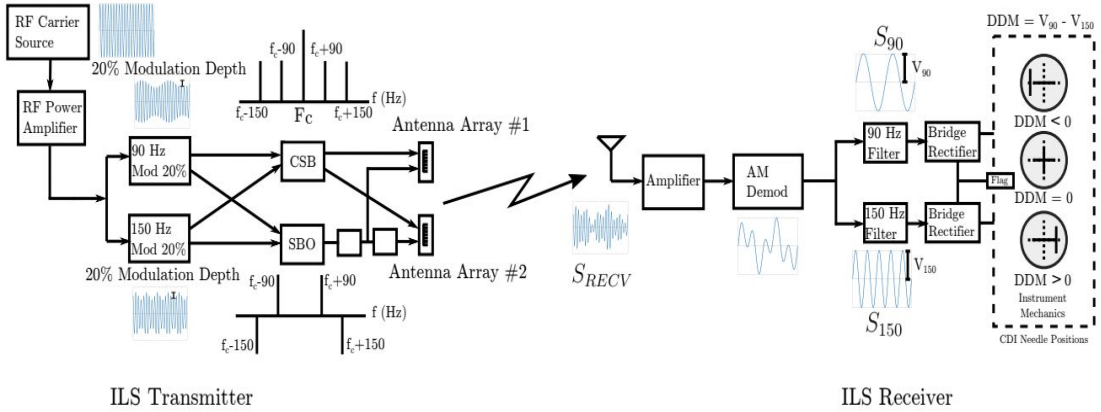
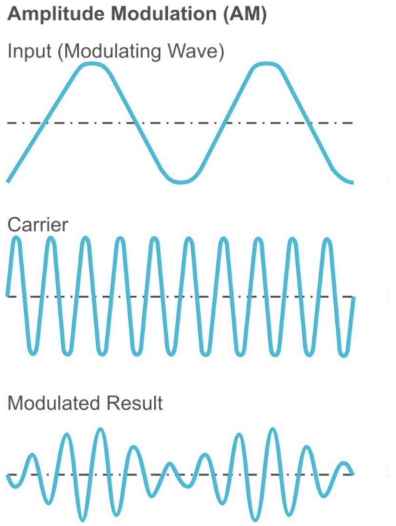


Figure 1: Overview of ILS sub-systems. The ILS consists of three subsystems: i) Localizer, ii) glideslope, and (iii) marker beacons.

ILS Transmitter and Receiver





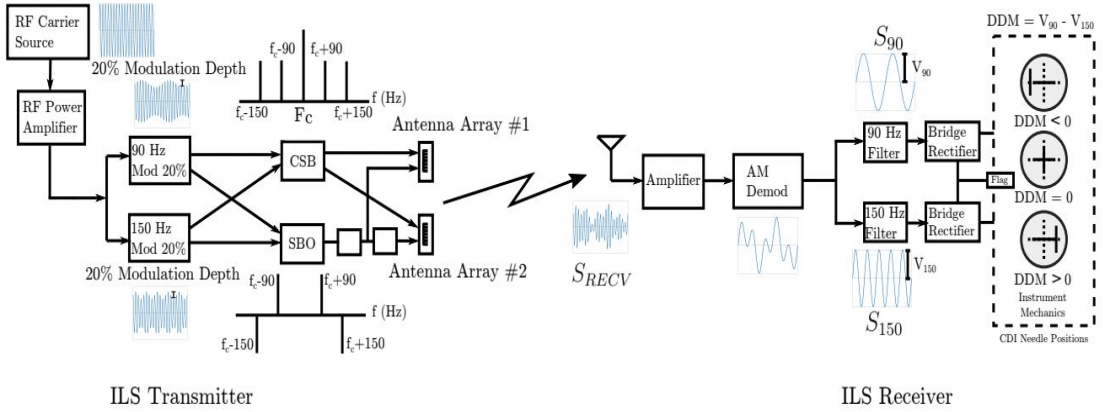
Instrument Landing System (ILS) continued

ILS Receiver:

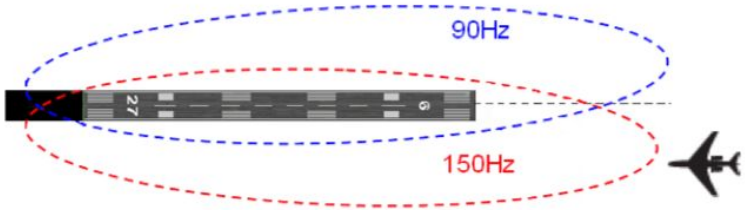
Amplified, demodulated, converted to recover DC voltage levels

Directly proportional to depth of modulation

Full scale deflection: DDM > 0.155 or DDM < −0.155 for localizer and if DDM > 0.175 or DDM < −0.175 for glideslope

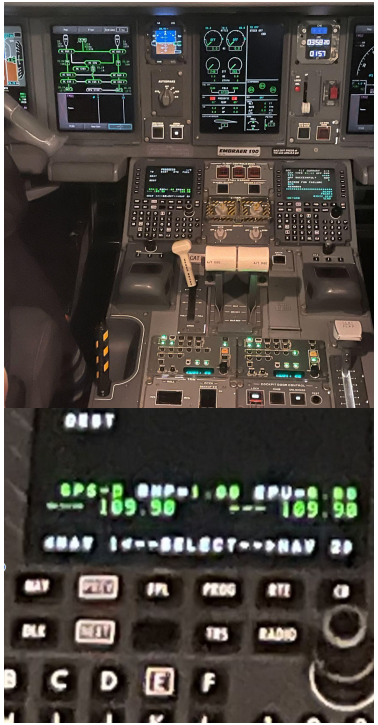


Approach scenario



Pilot enters localizer frequency into autopilot.

ILS receiver intercepts localizer



Pilots make adjustments

Wireless Attacks on ILS

Overshadow Attack

Specially crafted ILS signals

Single-Tone Attack

Transmission of one sideband tone

Overshadow Attack

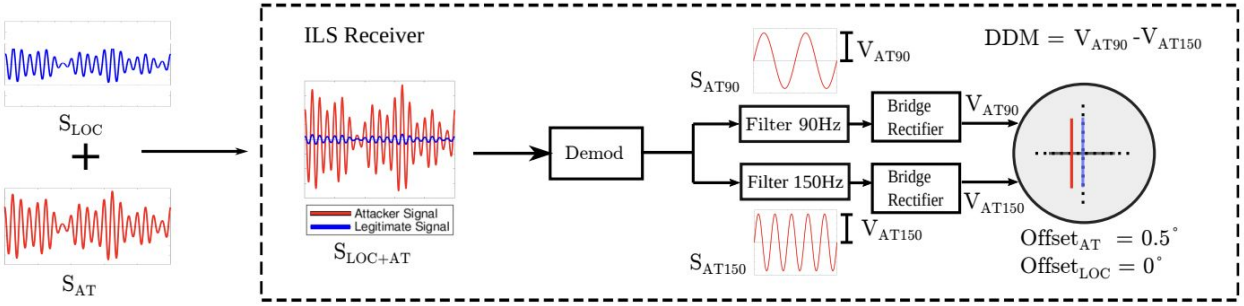


Figure 3: Schematic of the overshadow attack. The attacker's signal has a preset DDM corresponding to 0.5° to the right of the runway. Attacker's signal overshadows the legitimate signal. The blue line represents the needle position without attack.

Overshadow Attack continued

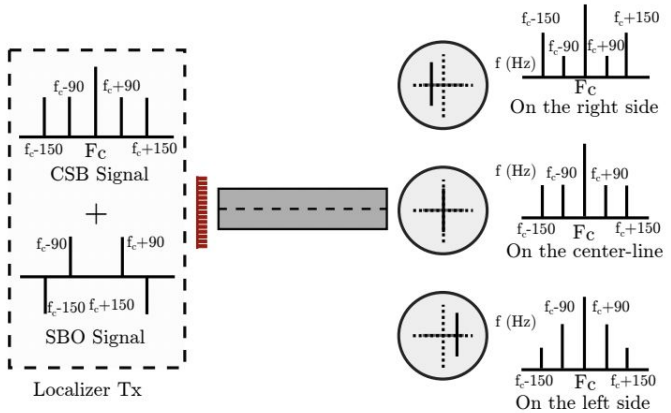
Amplitude is dependent on the position of the aircraft relative to the runway and its approach path angle

DDM = VLOC90 – VLOC150.

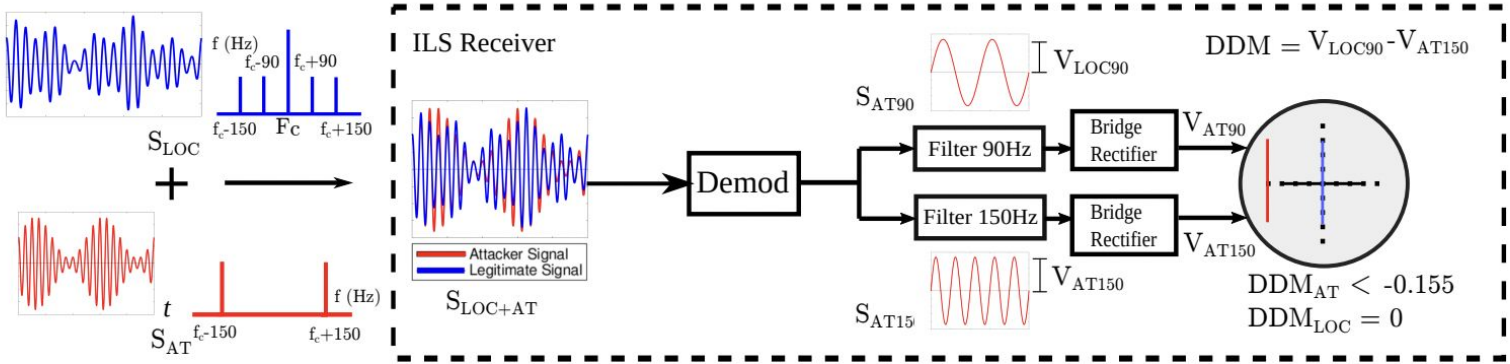
With the attacker spoof, the new depth is: [VLOC90 +VAT90]–[VLOC150 +VAT150].

Since VAT90 >>VLOC90 and VAT150 >>VLOC150

the resulting DDM = VAT90 –VAT150



Single-Tone Attack



Experimental Setup

X-Plane 11 flight simulator

Attacker control unit

USRP B210s

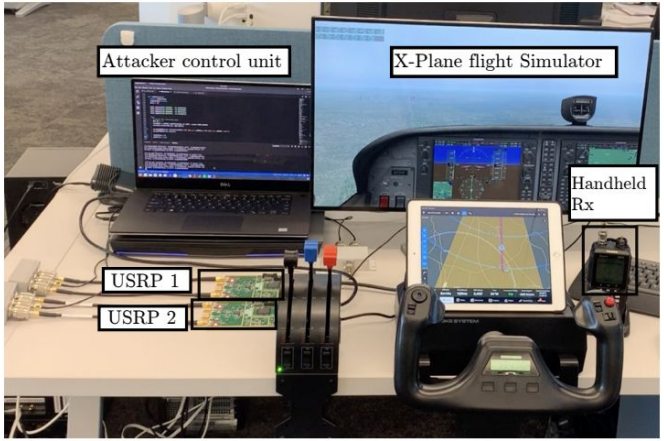
Commercial aviation grade handheld navigation receivers: Yaesu FTA-750L and Sporty's SP-400 Handheld NAV/COM Aviation

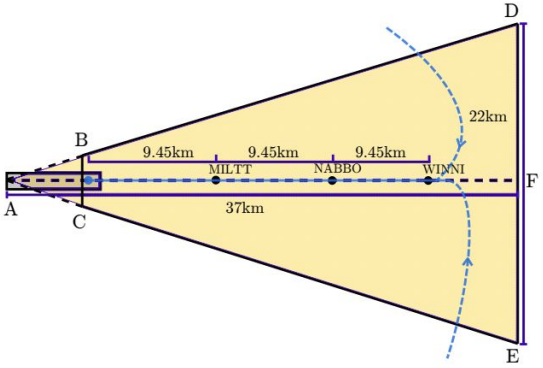
Attacker control unit

Spoofing Zone Detection

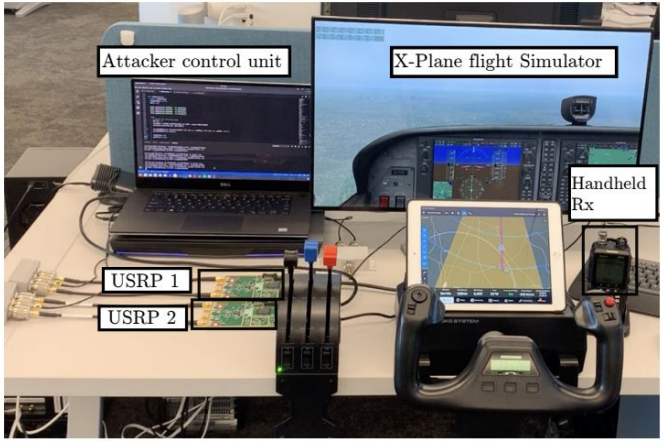
Automated and timely triggering of the spoofing signal

Even-Odd algorithm in scalable vector graphics (SVG)





Attacker control unit



Offset Correction Algorithm

Current offset = θ = tan−1[(mCA−mBA)/(1+mBA ∗mCA)], where m is the slope

DDM = (DDMfullscale ∗Δ)/2.5 (2.5 = angle for full-scale deviation)

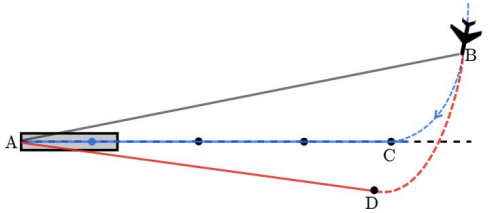
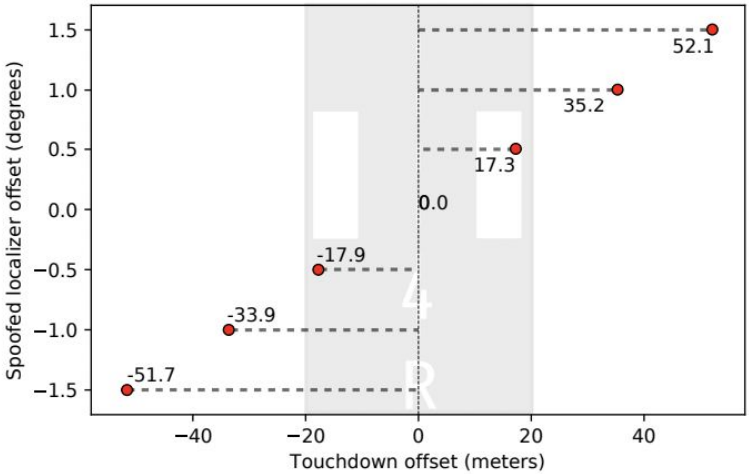


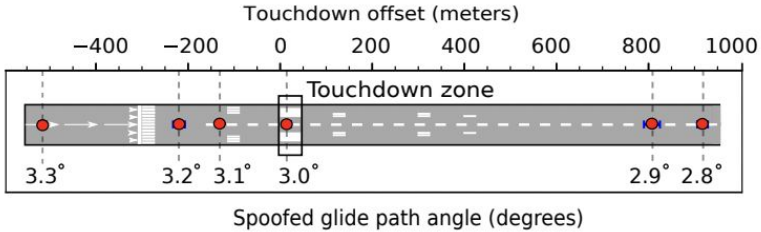
Figure 11: Offset correction algorithm takes into account aircraft's current position to calculate the difference in the spoofed offset and the current offset.

Algorithm 1 Offset correction algorithm.

procedure GETANGLEDIFFERENCE
  $\angle DAC \leftarrow TargetedLocalizerOffset$
  $\angle BAC \leftarrow GetAngle(location)$
  $difference \leftarrow \angle DAC - \angle BAC$
  return $difference$
procedure CALCULATEDDM
  $difference \leftarrow GetAngleDifference$
  $ddm \leftarrow (0.155 * difference)/2.5$
  $AT90 \leftarrow 0.2 + (ddm)/2$
  $AT150 \leftarrow 0.2 - (ddm)/2$
  $ChangeAmplitude(AT90, AT150)$

Evaluation of Overshadow Attacks





Evaluation of Single-Tone Attacks

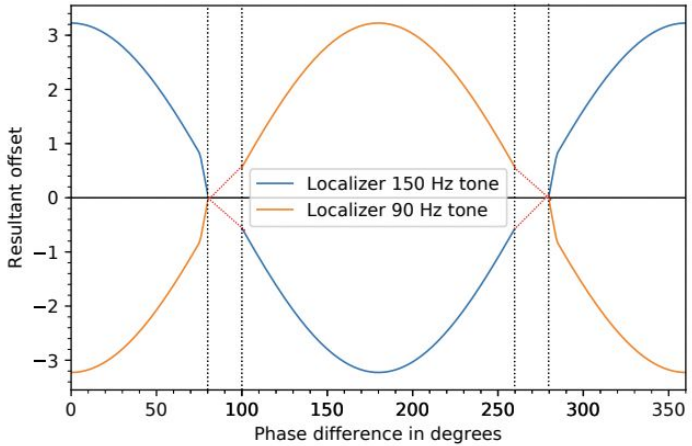


Figure 14: Comparison of calculated offset and the phase difference for localizer

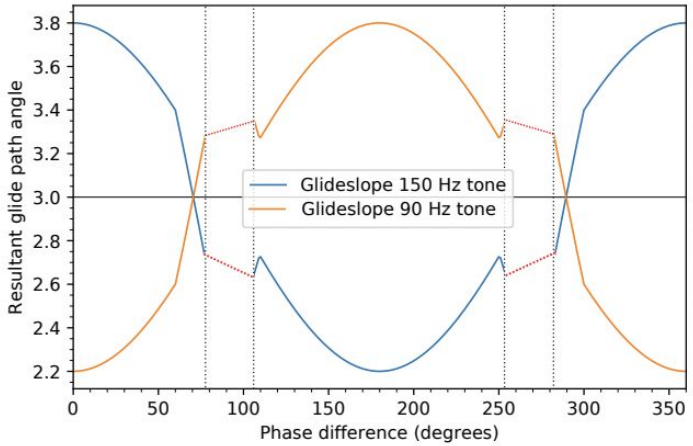


Figure 15: Comparison of calculated offset and the phase difference for glideslope

Results of Real-Time Amplitude Scaling

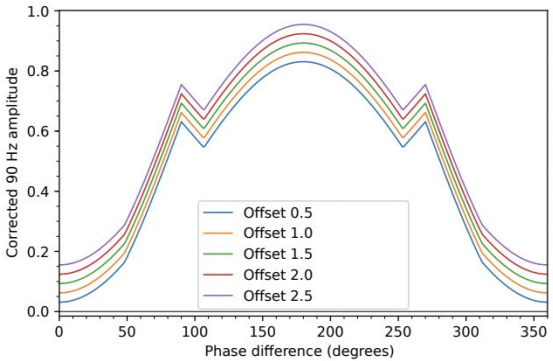


Figure 16: Amplitude scaling algorithm evaluation localizer. Amplitude required to compensate for the effect of phase

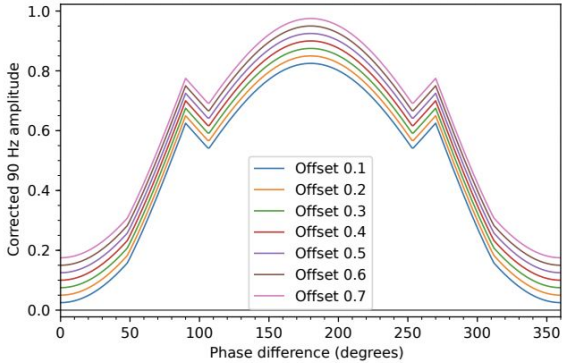


Figure 17: Amplitude scaling algorithm evaluation glideslope. Amplitude required to compensate for the effect of phase

Power Requirements

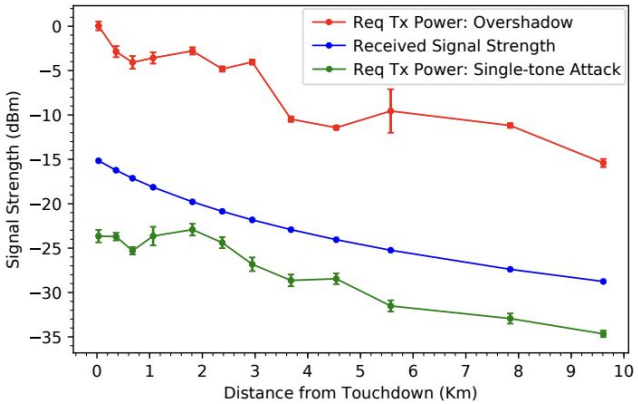


Figure 18: Comparison of required received signal strength for attack methodologies for the localizer

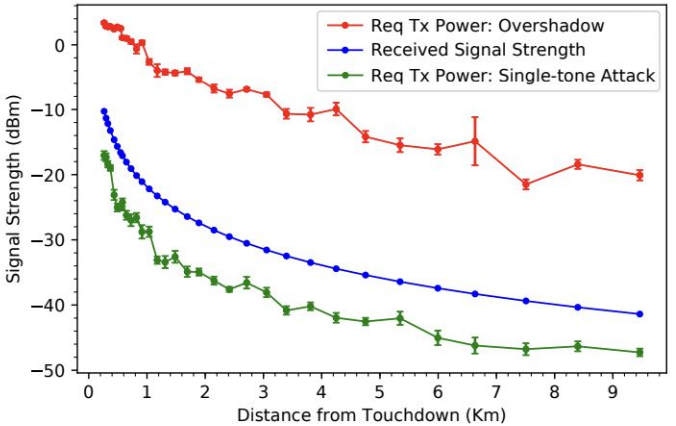


Figure 19: Comparison of required received signal strength for attack methodologies for glideslope

Acception/Rejection

Accept with limitations

Questions

Discussion

Autonomous Commercial Flights

Autonomous systems are already evident in commercial flights with landing and cruise control systems. Would you feel comfortable taking a flight without pilots in the cockpit, or should there always be human intervention as a failsafe?

ILS

How can ILS be secured or improved? It is demonstrated that the FAA prefers pilots to use instrument based landing rather than visual.


slidesgo