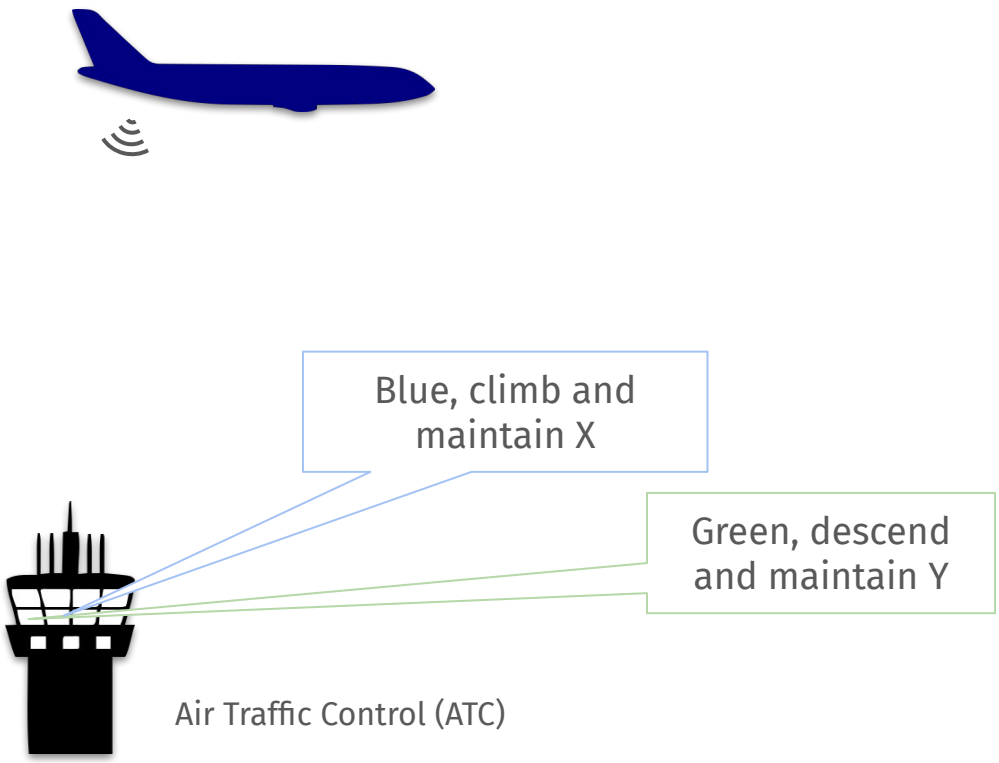
Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS)

Giacomo Longo, Giacomo Ratto, Alessio Merlo, and Enrico Russo
NDSS 2026
{giacomo.longo,giacomo.ratto,alessio.merlo}@unicasd.it, enrico.russo@unige.it

UniGe | DIBRIS

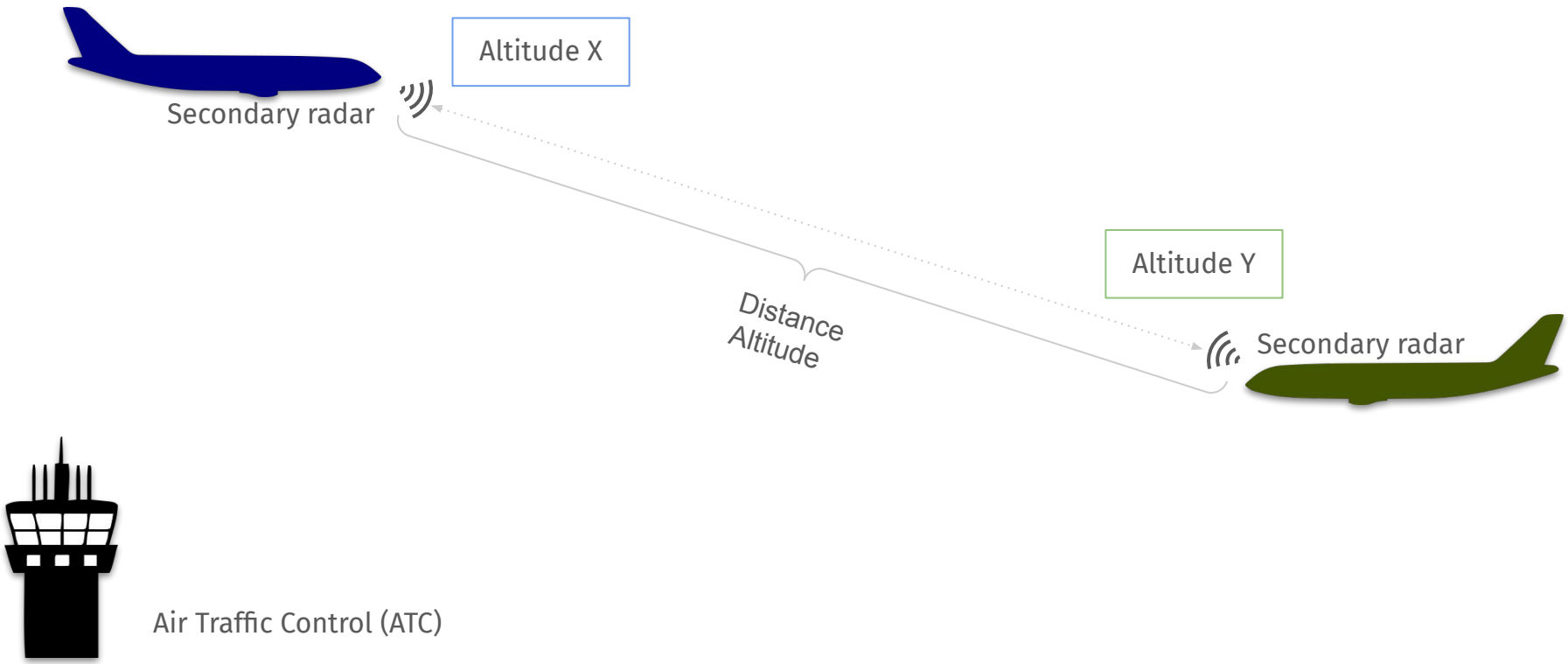
Artifact Evaluated
NDSS
Available
Functional
Reproduced

First defence against mid air collisions: Air Traffic Control

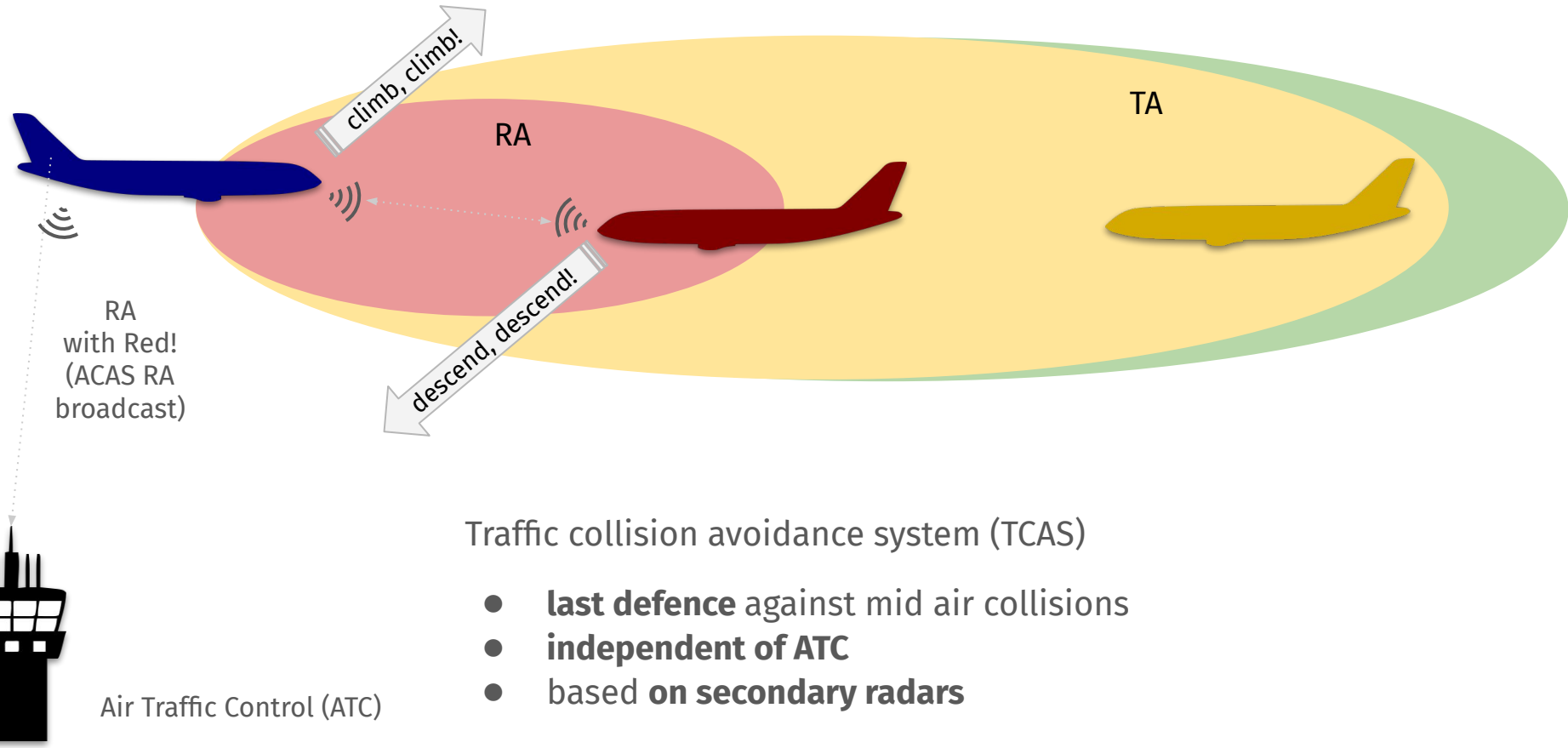


G. Longo, G. Ratto, A. Merlo, E. Russo. 2026. *Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS).* Network and Distributed System Security (NDSS) Symposium

Second defence: Secondary Radar and TCAS



Second defence: Secondary Radar and TCAS



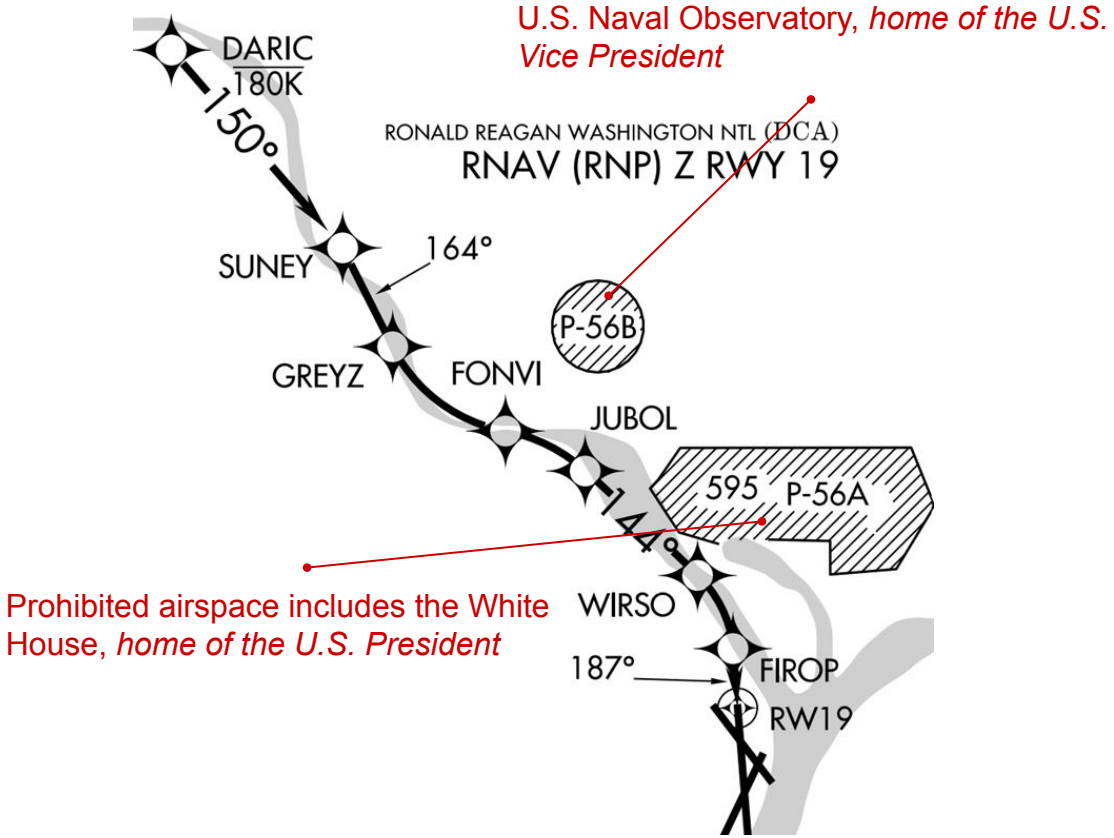
Traffic collision avoidance system (TCAS)

- **last defence** against mid air collisions
- **independent of ATC**
- based **on secondary radars**

1st March 2025 - Washington DCA

Several TCAS TA and RA alerts occurred between 11:10 and 14:10 UTC along the approach path to the runway of Washington National Airport (DCA)

- There has been no official explanation from the US Federal Aviation Administration (FAA)
- Two US representatives have attributed the interference to Secret Service counter-drone (C-UAS) systems*



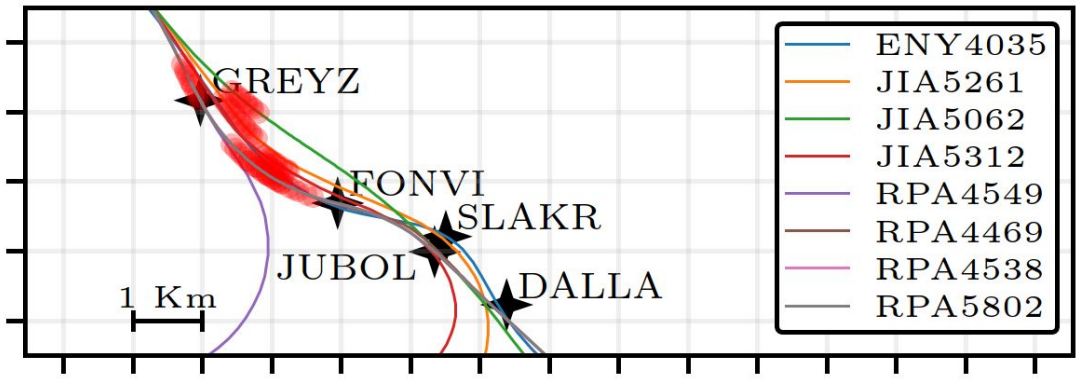
*Rick Larsen and Bennie G. Thompson, members of the US Congress (Ranking Members of the Transportation and Homeland Security Committees) - letter to the US Congress dated April 14, 2025

Analysis from open sources

Position reports, RA reports, radio communications

- 10 aircraft involved (8 with RA) and 3 go-arounds
- approximately 5 km visibility
- single intruder at a fixed altitude of approximately 700 m
- not detected by ATC and visually unnoticed by pilots*

- intruder was transmitting using an old technology (Mode C): altitude only, no position
- RA reports (Mode C only) include information about the intruder:
  - distance: on average approximately 400 m
  - direction: between 315 degrees and 345 degrees (around 11 o'clock position)

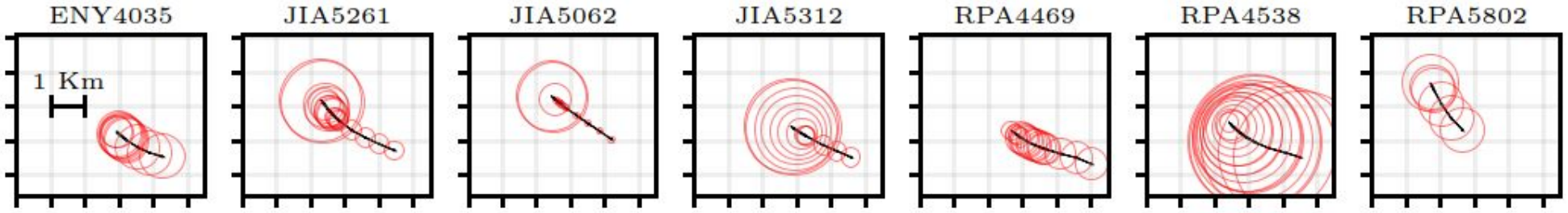


*https://www.youtube.com/watch?v=pOXV3AjESVU

Analytical deduction

The geometric analysis of the distances shows that the intruder is moving together with the victim aircraft.

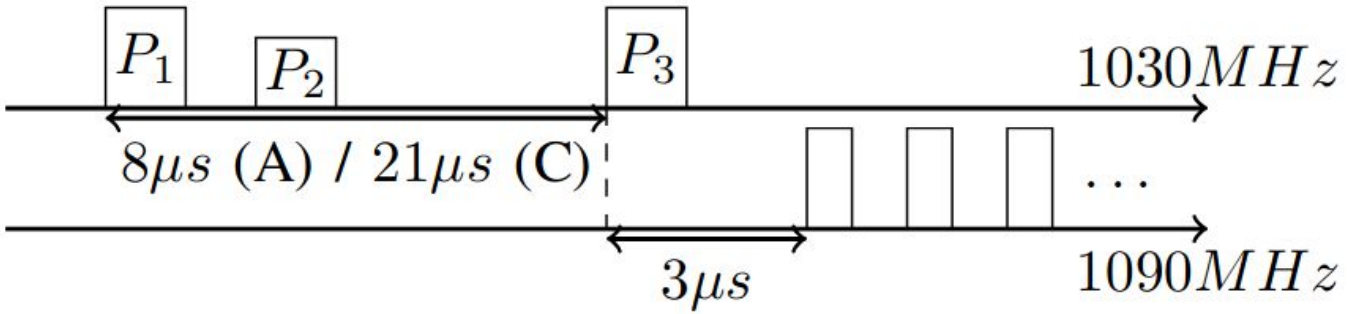
- object in flight: impossible not to see or detect an object with such behavior
- ground transmitter: more plausible hypothesis, but
  - is it possible to inject false aircraft contacts using Mode C?
  - is the Washington incident compatible with a fixed ground transmitter?



Artifact Evaluated
NDSS
Available
Functional
Reproduced

TCAS and Mode C

- TCAS relies on the Mode S protocol
- However, TCAS is backward compatible with Mode C
- Mode C estimates distance by measuring response delay assuming a processing time of **just 3 microseconds**



Attacking the final defence against mid-air collisions (TCAS)

- Previous work* focused on attacking Mode S
- We present a novel attack on TCAS using **Mode C to inject non-existing aircraft**
- Attackers can **spoof their distance** from the victim aircraft

* G. Longo, M. Strohmeier, E. Russo, A. Merlo, V. Lenders. 2024.
On a Collision Course: Unveiling Wireless Attacks to the Aircraft Traffic Collision Avoidance System (TCAS).
In Proceeding of the 33rd Usenix Security Symposium (USENIX 2024)

Injecting non-existing aircraft: triggering RA

Mode C is not authenticated.
Attack technique consists in answering interrogations from the victim:

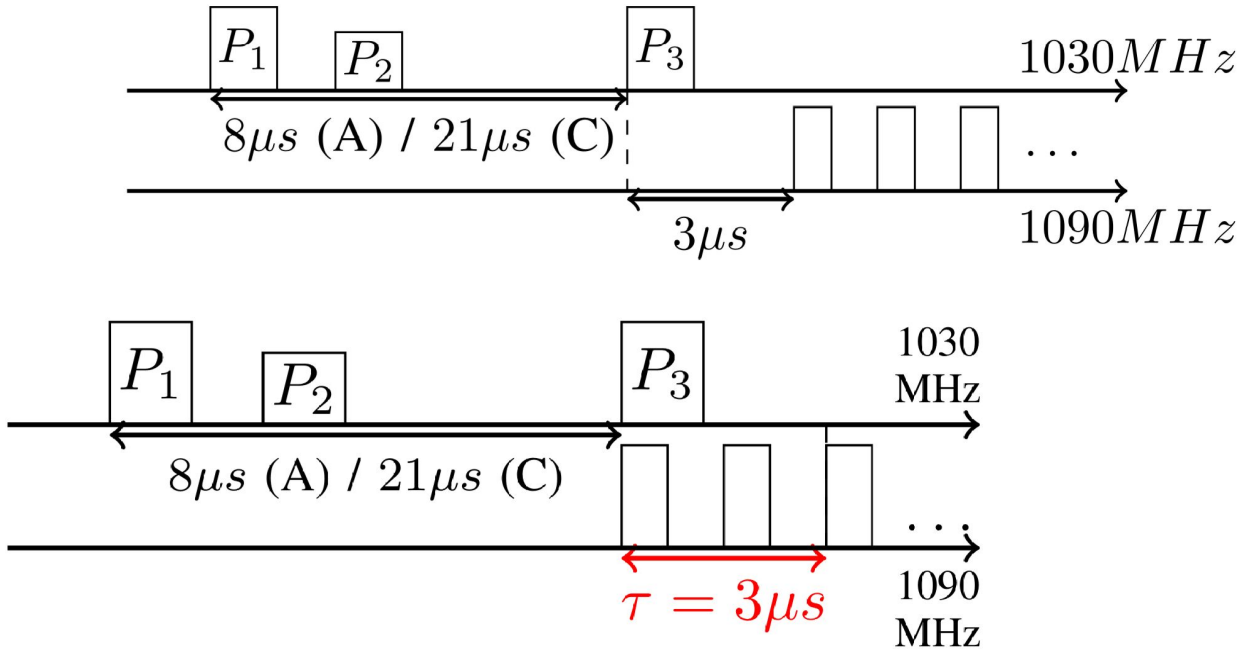
- with altitude equals to the victim
- with distance as low as possible (ideally zero)

Spoofing the distance requires **answering in advance**.

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Injecting non-existing aircraft: spoofing the distance

To make an attacker appear closer w.r.t. its location it can **answer in advance**

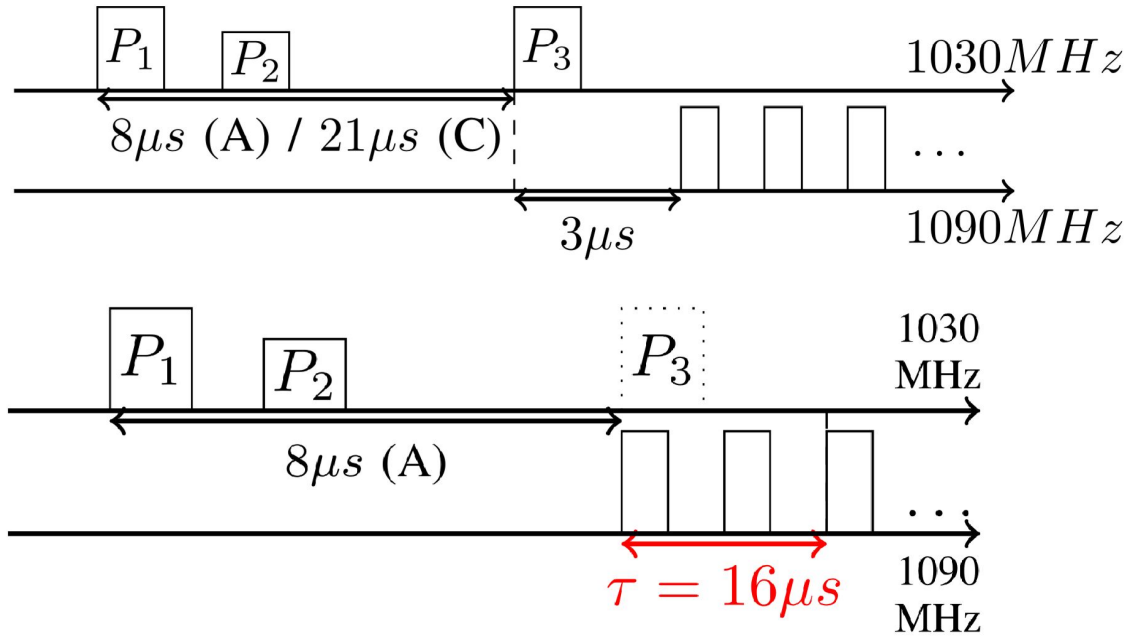


1st technique, preemptive reply, ~800m

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Injecting non-existing aircraft: spoofing the distance

To make an attacker appear closer w.r.t. its location it can **answer in advance**

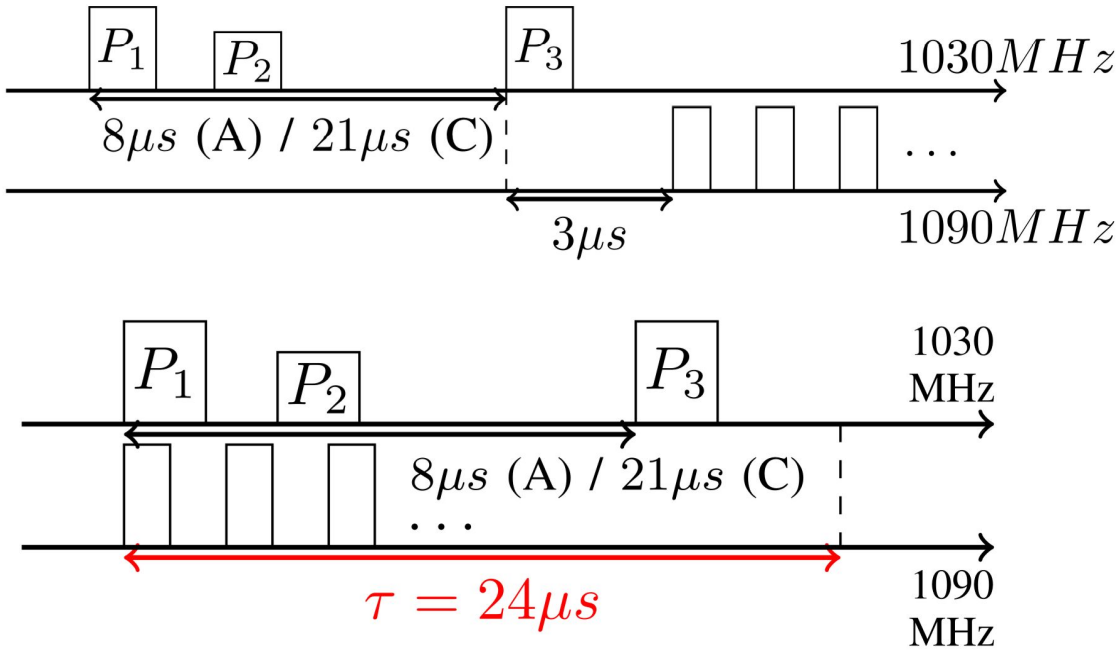


2nd technique, mode discrimination, ~2400m

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Injecting non-existing aircraft: spoofing the distance

To make an attacker appear closer w.r.t. its location it can **answer in advance**



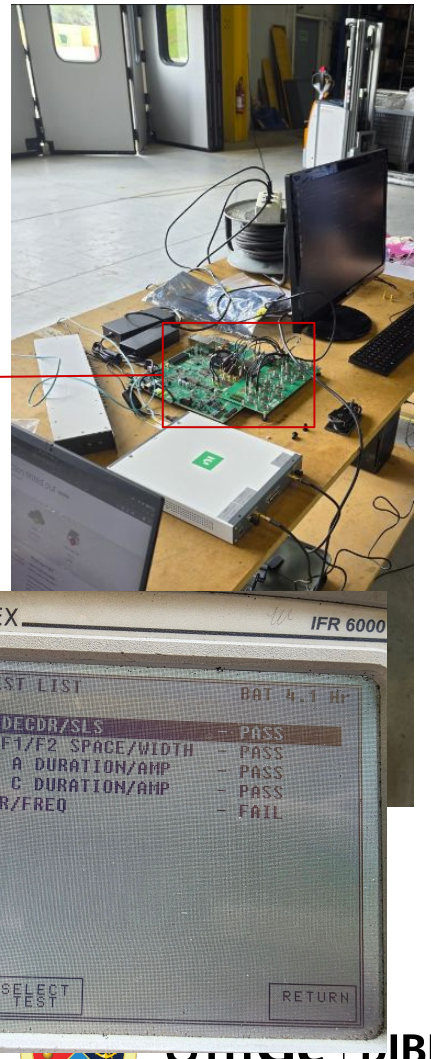
3rd technique, preemptive reply, ~3500m, creates artifacts

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Attack implementation against Mode C

Appear at zero distance by anticipating the reply to an interrogation

- fixed reference delay: about 3 microseconds
- implementation on RFSoC (FPGA plus RF front end plus ARM/Linux CPU)
- maximum spoofed distance of about 2 km
- certified operation using the Aeroflex IFR6000* avionics test set



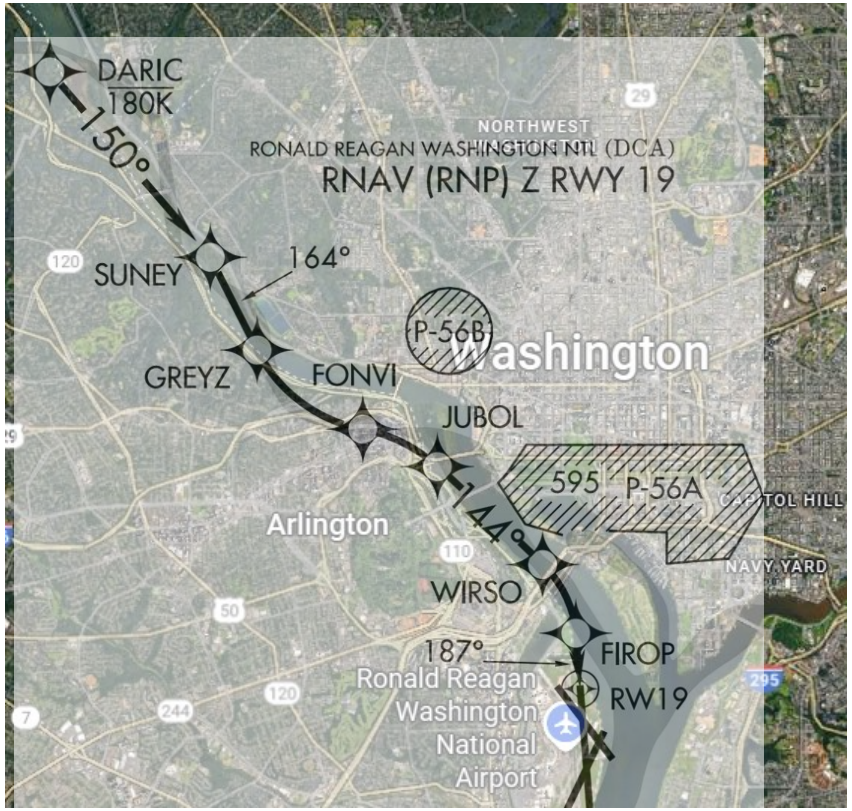
*with the technical support of Baykar Piaggio Aerospace

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Detection of a Fixed Transmitter

System based on Sequential Monte Carlo to estimate the position of a fixed transmitter

- find the position that makes the recorded observations most likely
- tests on synthetic data*:
  - if the transmitter is mobile, the result becomes diffuse ("does not converge")
  - correctly identified the fixed source in 95 percent of the cases, with an error of about 855 m
  - average execution time of about 8 s

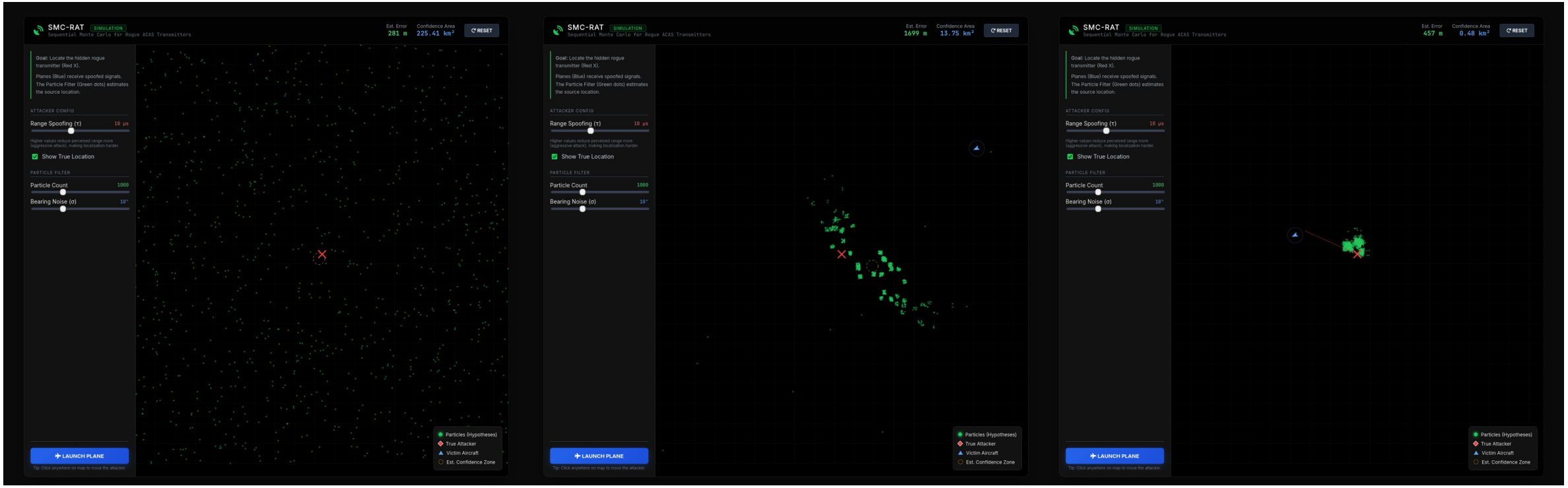


*300.000 independent trials on scenarios comparable to DCA or more complex

G. Longo, G. Ratto, A. Merlo, E. Russo. 2026. *Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS).* Network and Distributed System Security (NDSS) Symposium

Artifact Evaluated
NDSS
Available
Functional
Reproduced

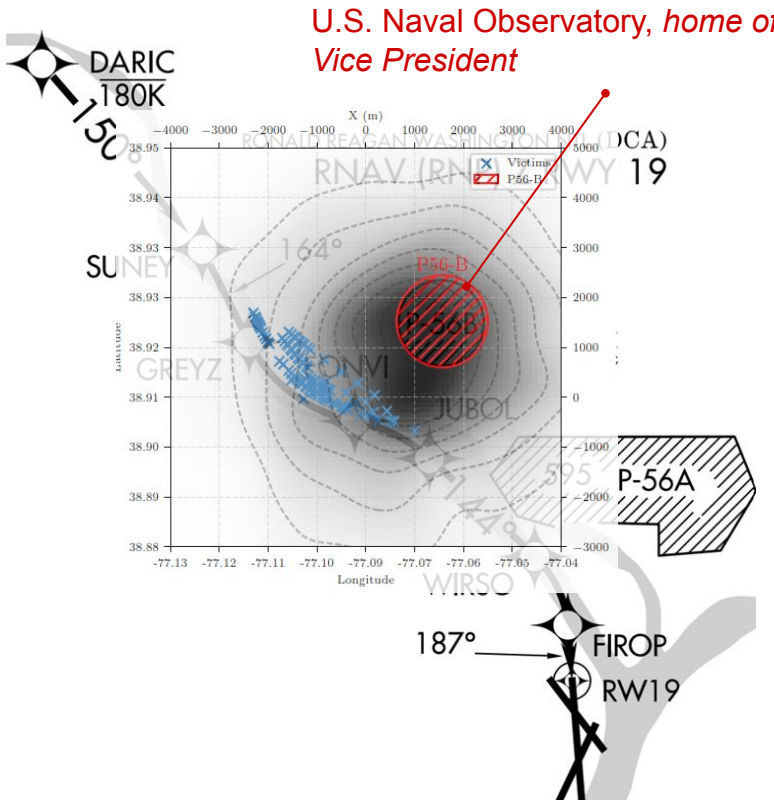
Detection of a Fixed Transmitter: Simulation



Detection of the Transmitter: DCA

Stable distribution consistent with
a **fixed ground source**

- Source estimated at about 890 m from the center of P-56B
- Ninety four percent probability that the transmitter lies within the restricted area
- In forty minutes, after two encounters, the system would have narrowed the source location to about four square kilometers



G. Longo, G. Ratto, A. Merlo, E. Russo. 2026. *Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS).* Network and Distributed System Security (NDSS) Symposium

Artifact Evaluated
NDSS
Available
Functional
Reproduced

Q&A

Scan for full paper, artifacts and demo

{giacomo.longo,giacomo.ratto,alessio.merlo}@unicasd.it, enrico.russo@unige.it

G. Longo, G. Ratto, A. Merlo, E. Russo. 2026. *Unknown Target: Uncovering and Detecting Novel In-Flight Attacks to Collision Avoidance (TCAS).* Network and Distributed System Security (NDSS) Symposium