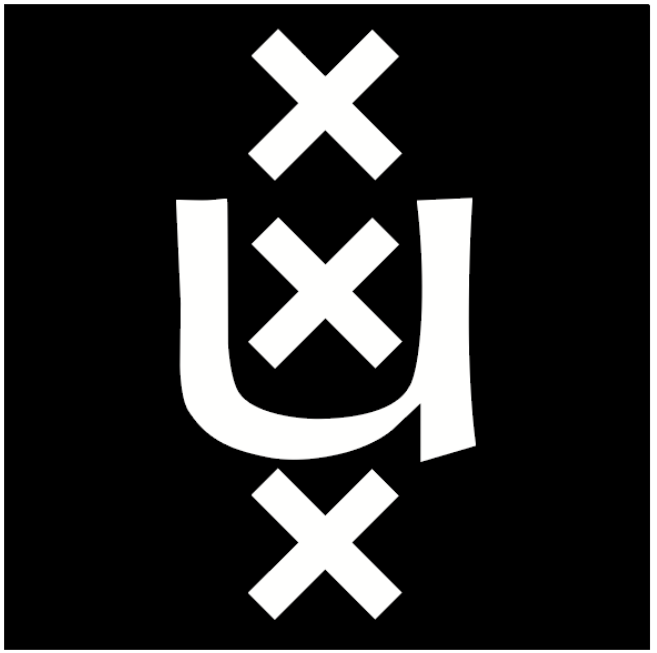
Research Project I

PROTECTING AGAINST RELAY ATTACKS FORGING INCREASED DISTANCE REPORTS

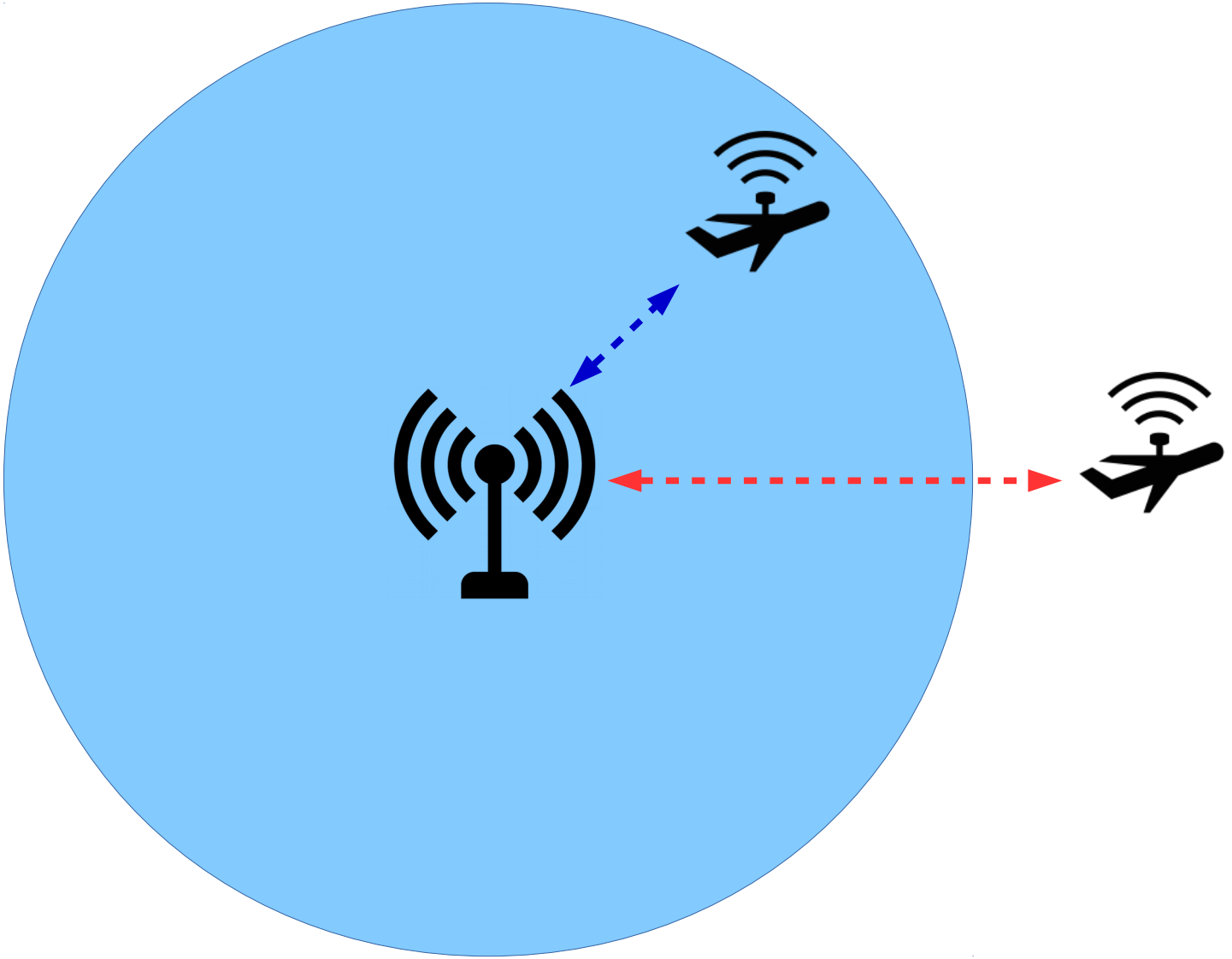


Xavier Torrent Gorjón

Summary

- Distance-bounding protocols
- Why other systems can't be used?
- Feasibility of the attack: study cases
  - Autonomous Cars
  - Drone MANETs
- Preventing increased distance reports
  - Behavior verification
  - Multiple distance-bounding signals
  - Distributed knowledge
- Conclusions

Distance-bounding protocols



Distance-bounding protocols

- With the current implementations, closer distances cannot be faked.
  - Proof through physical limitations: cannot go faster than speed of light.
- However, there are no systems to prevent increased distance reports.
  - Physical limitations cannot be used.
  - These attacks may have no use for Access Control Systems, but could be dangerous on other contexts.

Why other systems can't be used?

- It could be argued that distance-bounding protocols were not made for this purpose.
- However, other location systems present difficulties as well.

Why other systems can't be used?

- GPS location
- Radar detection
- Inertial Navigation System

Why other systems can't be used?

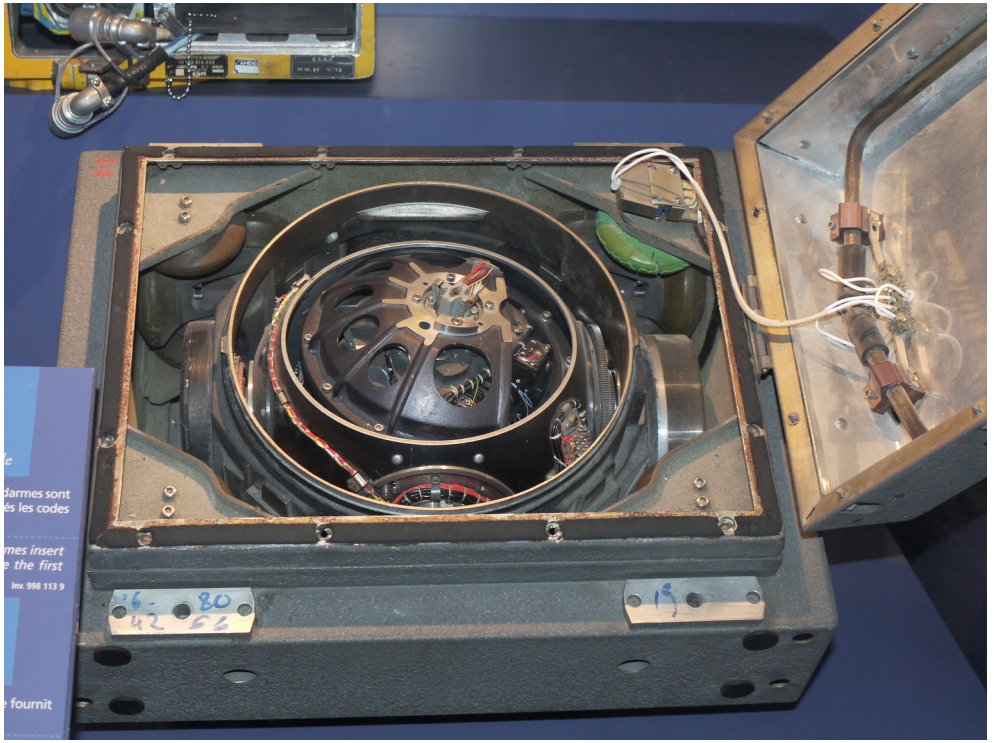
- GPS location
  - Can be disrupted
  - Sometimes not reliable even in non-dangerous environments (underground, inside buildings...)

Why other systems can't be used?

- Radar detection
  - Systems could attempt to physically detect attackers
  - Problem: stealth technology surpasses anti-stealth technology in the current state of the art

Why other systems can't be used?

- Inertial navigation system
  - Fits perfectly our purpose, but it cannot be reliably used as a stand-alone positioning system due its accuracy. This may change in the future.



Feasibility of the attack: study cases

- Autonomous Cars

Feasibility of the attack: study cases

- Drone MANETs

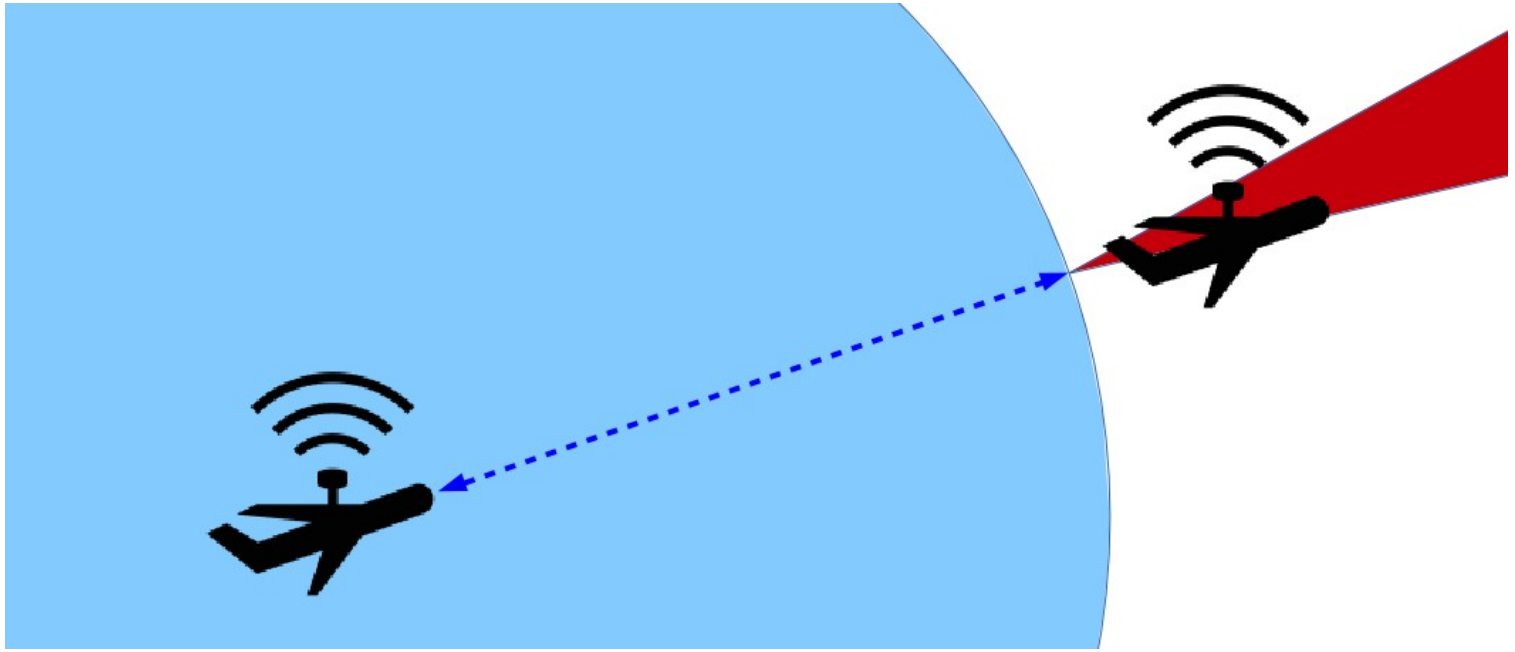
Image source: www.usatoday.com

Preventing increased distance reports

- Behavior verification
  - Similar idea to Intruder Detection System on networking environments.
  - Attempt to detect sudden changes in the received data, such as signal strength or large changes on the reported locations.

Preventing increased distance reports

- Multiple distance-bounding signals
  - Original distance-bounding only attempts to check if a reporter is inside or outside a certain range.
  - Use multiple distance-bounding signals to obtain approximate location, not only distance.



Preventing increased distance reports

- Distributed knowledge
  - Instead of relying only on its own measurement, a node could also ask for the measurements of other nodes.
  - It would be extremely difficult for an attacker to fake multiple different distances at the same time.

Conclusions

- Most of the systems discussed are not employed nowadays but they are a latent problem.
- Lower-distance bound cannot rely on physical limitations for its security: difficult to achieve perfect security.
- Proposed solutions -specially a combination of them- offer a reasonable decrease in the vulnerability of these systems.

Questions?

Final notes

- All images used come from wikipedia or are personal work, unless stated otherwise. All of them are licensed under CC or GNU licenses that allow to use them freely.