Spoofing Aspects at Receiver Start-Up

Manuel Appel
German Aerospace Center (DLR)
Institute of Communications and Navigation
manuel.appel@dlr.de

Meeting #3
WGC – Resilience Subgroup
10.04.2018
Maspalomas, Gran Canaria
Simulations

Lab Setup

Common Constellation:

Log:
Position
Raw Observables
Simplistic Setup (unsynchronized)

Timing

Nominal On  Spoofer On  End of Test

Bunch of different runs:
- Different speed
- Different Power

Location

Nominal Location

Legend
- ≤ 10m
Simplistic Setup (unsynchronized) – with RFI
Depends on Receiver

Timing with “knock-out”

Legend

- Green: < 50m
- Red: ≥ 50m

No Pattern
Interference forces receiver into reacquisition.

Dependent on search strategy, either authentic or fake peak is found first and tracked.
Receiver Aspects – Startup, Acquisition

- Search strategy (in Acq. or Reacq.) in 2D-grid if serial search is implemented

- Search method (either serial or parallel FFT-based)

- Noise floor estimation at startup
Effect of loop parametation on spoofing sync (peaks overlap!)
Feasibility Issues (1)

- Since no synchronization is necessary, feasibility is given by using commercial hardware

- Either signal simulators or SDR Platforms will be enough (software on Github)

- Very unlikely that correlation functions overlap, i.e. only one peak per PRN will be tracked.

Feasibility Issues (2)

Issue: Power calibration of spoofer to match nominal power

Easier (for spoofer) if farther away!
Possible Occurrences

Every time the victim is “parked” and navigation is turned on or restarted

Examples:
- Airport
- Parked train, train passing tunnel
- Harbor

If mix is found/tracked: Allows for ARAIM based detection
Questions to the group

- How does this fit in the current threat model? (see threat_notes_v0.9)
- Are ARAIM methods (would be a link to the other subgroup) useful? Which ones?
- How to deal with receiver implementation aspects?
- Possible defend strategies?

Countermeasure proposals:

- Second peak constant search/acquisition
- Second peak tracking if overlapped
- Recommendation for loop implementation (Tobias Bamberg)