GNSS Timing – Threats and Countermeasures

November 4, 2021

Samuli Pietila
Philipp Richter
Zdenek Chaloupka

Outline

GNSS as a part of critical infrastructure

- Several critical infrastructure sectors rely on accurate time/synchronization
  - Wireless communications
  - Power distribution
  - Data centers
  - Financial sector

Threat types and impacts

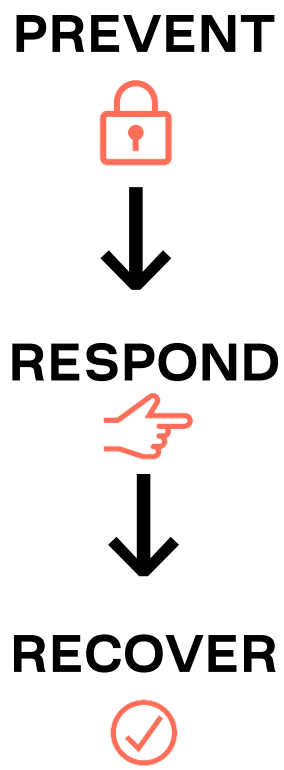
Threat type	Impact
Jamming • Unintentional interference • Intentional jamming	• CW jamming – ghost satellites, denial of service • Wideband jamming – reduced SNR, reduced accuracy, loss of service
Spoofing • Meaconing (rebroadcasting) • Broadcasting fake signals	• Aim to make receiver provide false PVT • Impact can vary from nothing to false PVT to no PVT
GNSS system issues • Dec 2020: Galileo ground system atomic clock failure • Jan 2016: GPS UTC parameter error	• Large PVT errors • Service unavailability

Threat actors

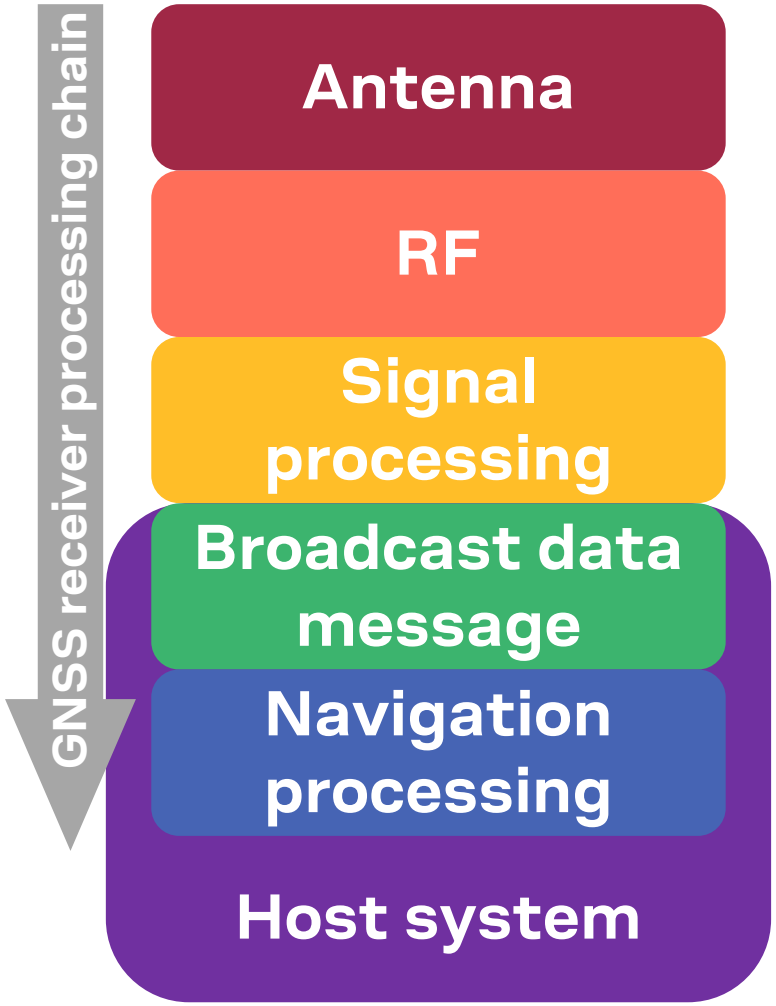
Type	Motivation	Capability
Privacy Seekers **Script Kiddies**	• Privacy • Boredom	• Low
Hacktivists	• Political	• Medium
Researchers	• Improve security • Self-marketing	• High
Cybercriminals	• Financial	• High
Foreign state	• Damage foreign systems	• Advanced

Jamming countermeasures

- Adaptive antenna systems, null steering antennas
- Out-of-band interference: Antenna and RF front-end filtering
- In-band jamming:
  - In-band jamming cannot be removed with fixed SAW filters without effecting also the GNSS signal → therefore more sophisticated methods must be used
  - In-band notch filter banks
    - Static/slow varying CW and narrowband jammers
    - Adaptive notch filters against fast chirp jammers
  - Signal blanking, effective against duty-cycled jammers
  - Multi-band receiver may switch to un-jammed band
- Monitor AGC, power levels, signal spectrum
- Recover after attack



Spoofing countermeasures



- Antenna arrays for angle-of-arrival detection
- Power level and spectrum checks
  - Changes over time, between GNSS and frequency bands
- Signal quality and consistency monitoring
  - Between GNSS systems and frequency bands
- Navigation data validity checks (eg DHS whitelist)
- Navigation data authentication (Galileo OS-NMA)
- Consistency of PVT solution
  - vs known boundaries and motion, vs clock characteristics
- Consistency vs other time sources
  - Atomic clock, network time
  - Other receivers using different GNSS system, frequency band, time base, antenna location

➢ **Redundancy at all levels**

Conclusion

- GNSS is an excellent source of time and synchronization, well worth protecting
  - Affordability – free service, easy installation
  - Accuracy – ”atomic clock”-level without atomic clocks
  - Availability – global coverage
- Effective countermeasures cover all stages from antenna to application
- Redundancy is key – multi-GNSS, multi-band
- Threats exist, but also countermeasures evolve

It is an arms race – We’ll keep on fighting!

Thank you
for your attention