Lecture 14

Friday, 31 March 2023 08:46

e.g. satellites are also constrained, but in a different way

before: devices were constrained (e.g. energy/power)

here: deployment constraints

Low Earth Orbit: 320 – 1100 km altitude
90 minute orbital period

Medium Earth orbit: 8000 – 12000 km
2 – 24 hour orbital period

Geostationary orbit 36000 km
exactly 24 hour orbital period

Parameter	LEO	MEO	GEO
Number of Satellites per operator	40 +	10 to 15	3 to 4
Satellite Life	3 to 7 yrs	10 to 15 yrs	10 to 15 yrs
Space Segment Cost	High	Low	Medium
Terrestrial Gateway Cost	High	Medium	Low
Propagation Loss	Least	High	Highest

← purpose of GNSS systems

PNT:
- positioning
- navigating
- timing

space segment: MEO satellites

control segment: master control network, operators around world

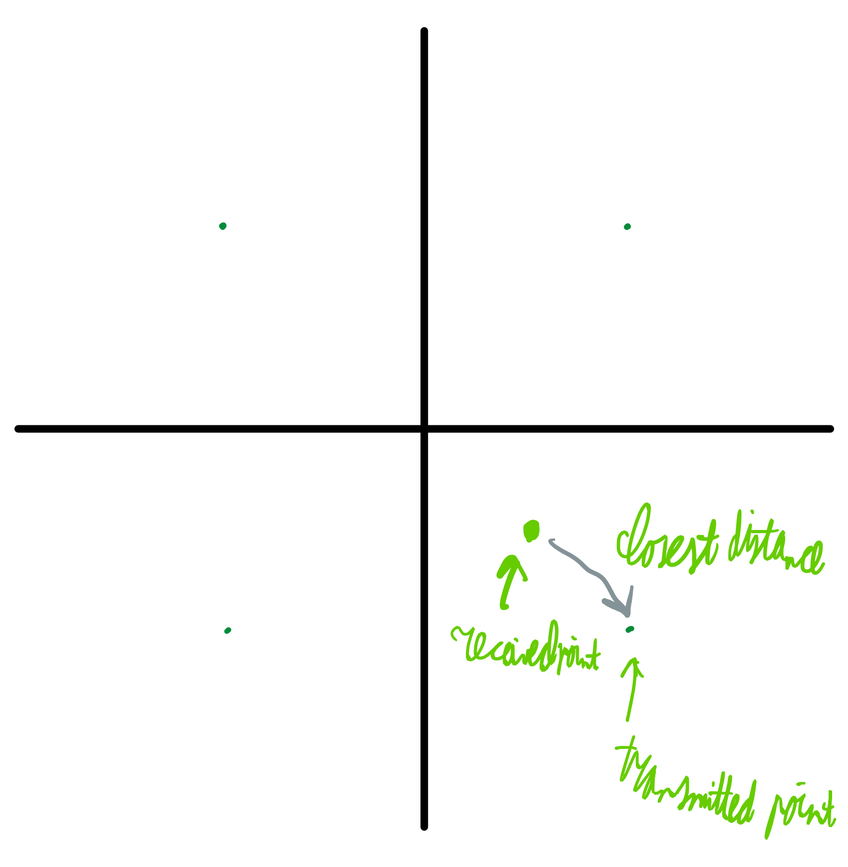
user segment: signal-receiving equipment, at least 4 satellites

intersection of 4 possible time ranges — many correction terms

3 m accuracy (x, y) for civil purposes, 5 m for altitude / z-coordinate

modulation used to provide robustness against noise

use closest symbol in plane (i.e. reconstruct based on minimum distance)



a satellite can be identified through a PRN sequence (PRN = pseudo-random noise)

GPS: 5 sub-frames transmitted in 30 seconds

1 sub-frame = 10 blocks = 300 bits, of which 240 bits data

24 × 8 bits data per 30 seconds

ephemeris = collection of GPS transmission time schedule for every transmission

very easy to transmit stronger signal than 'honest' signals → jamming / spoofing...
absence of security fields ↗

power ratio ≈ 1.1 = spoofed / authentic suffices to lift signal onto spoofed signal

meaconing: replay attack

security code estimation and replay (SCER): intelligent spoofing, to prevent sudden jumps in time/location

most GNSS modules do not report errors; they show the last location instead

spoofing is difficult to detect because of hardware compensating for low power of signals
which also removes signals that could be used to detect attacks

spoofing is difficult in practice

four categories of countermeasures

cryptographic techniques: military-grade, Spreading Code Encryption, periodic change of keys
NMA / NME: navigation message authentication / encryption — elliptic curve cryptography; periodically add signatures into GPS message

correlation with other sources:
- civilian + military signals are out of phase in spoofing
- accelerometer data should be consistent with change in location
- e.g. NTP, cellular networks
- adversary may also manipulate other sources...

signal-processing based systems: inconsistencies in physical layer data (waves)

satellites can be identified through PRN codes or Doppler shift
no modification at satellite needed, not perfectly accurate, requires hardware-control

Receiver Autonomous Integrity Monitoring (RAIM) → look for inconsistencies in GPS constellation
does not work against newer methods which spoof the entire constellation

Doppler shift is difficult to emulate for attacker, because it must change wavelengths for all emulated satellites
even more difficult with multiple different / unpredictable receivers

power-based metrics → high-power messages may not be trustworthy

multiple antennas: anomalies are more likely to be found when considering multiple synchronized viewpoints
angle of arrival of signal