Cyber-Security of GPS

Peter Volgyesi

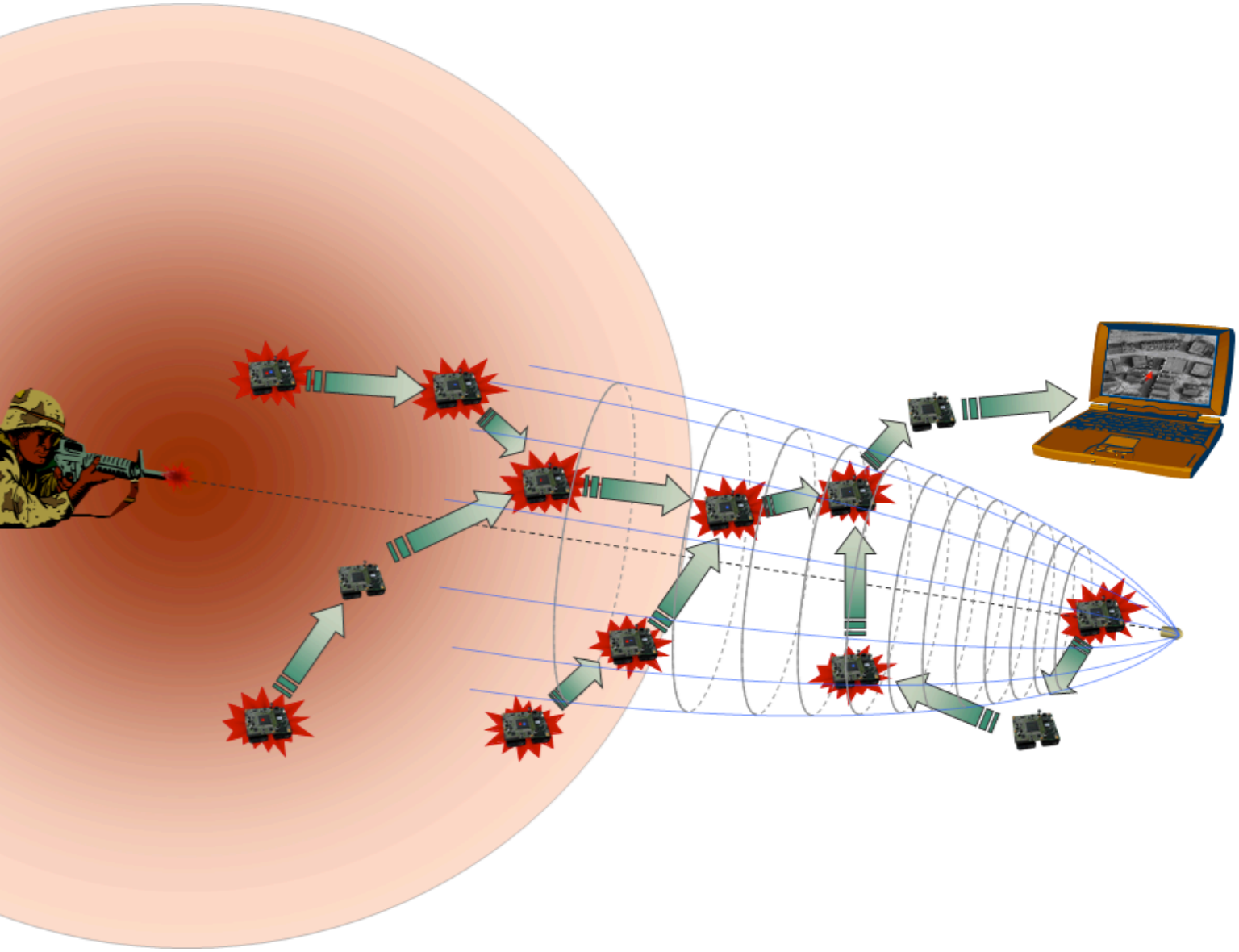
How GPS Works

… at all

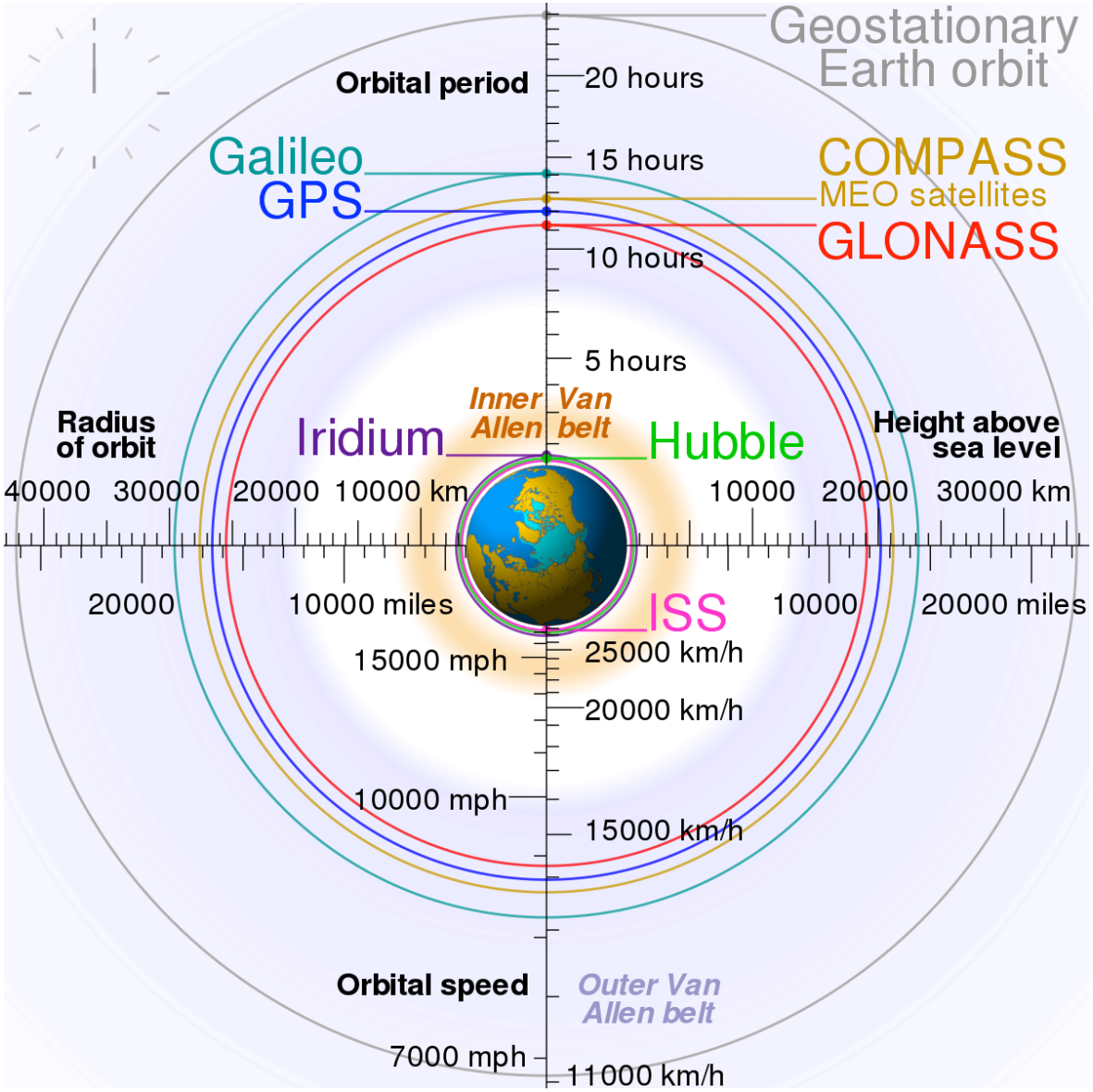
Time - distance measurement w/ speed of light
Power and noise - 25 W from 20,000km
Shared frequency - 32 operational satellites
Doppler effect - 5-10 kHz, changing even for stationary receivers

History

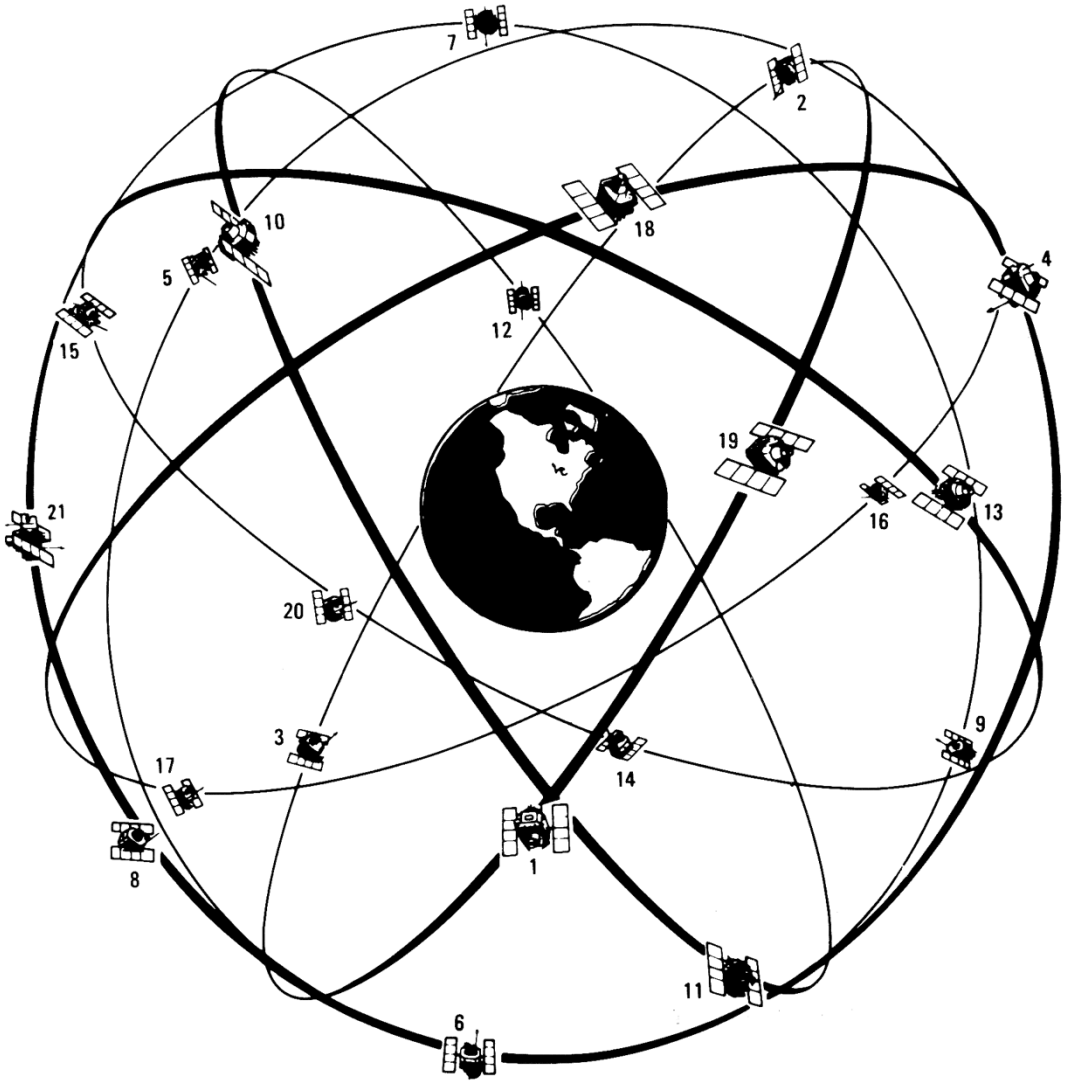
- 1957: **Sputnik**
  - *locate the satellite using known ground receiver positions*
- Military need: nuclear submarines (**SLBM**) - Polaris
- 1960: **TRANSIT** - Doppler-shift curve fitting
  - LEO orbits
  - fewer satellites (one required, only for a fix)
  - One fix / hour
- 1964: **Timation** - time of flight
  - atomic clocks
- 1978: first GPS satellites launched
  - 1995: fully operational



Motivation - shooter localization

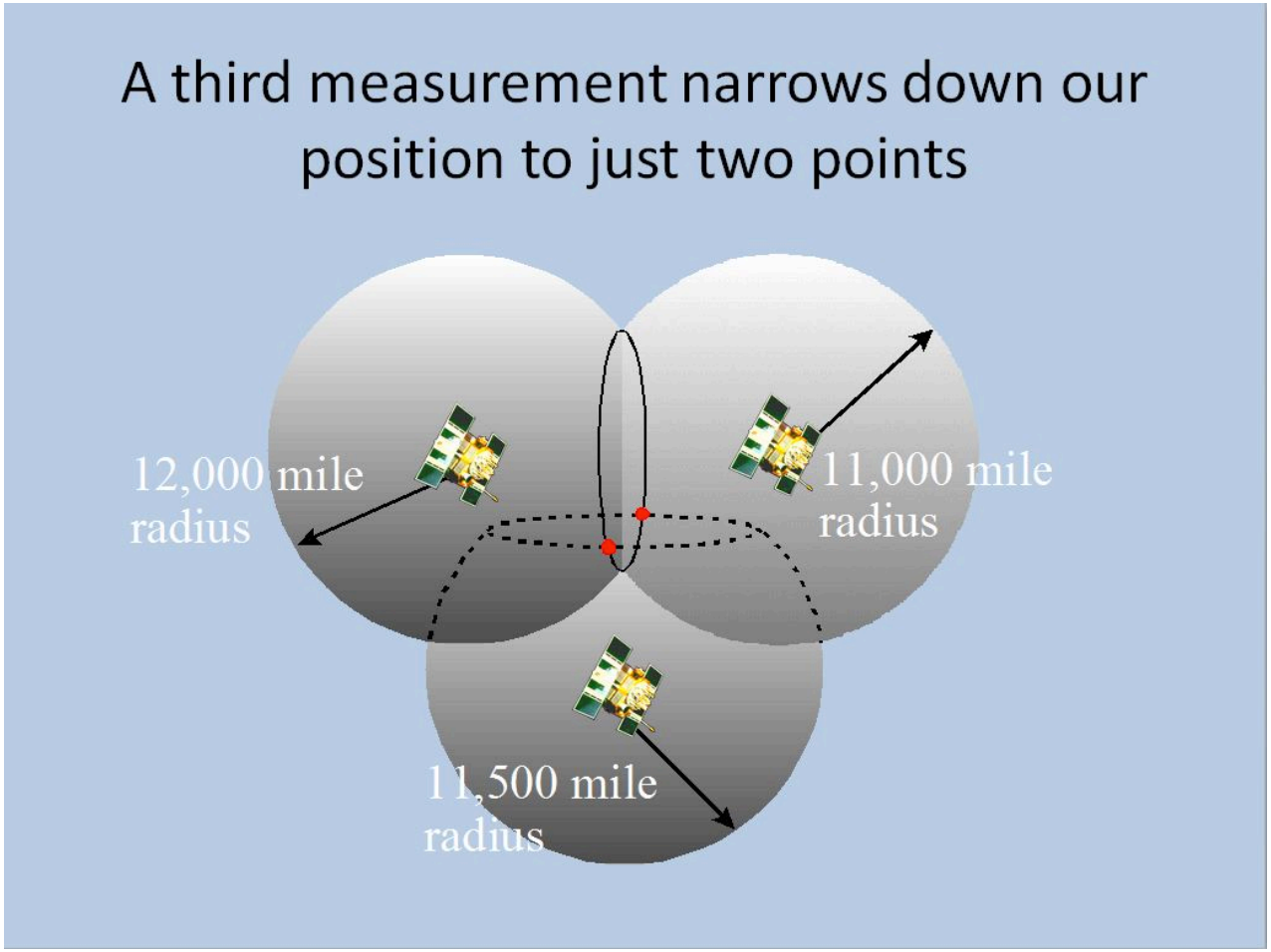


Earth orbits



- 32 satellites
- 6 orbital planes
- MEO: 20,000 km (12,500 mi)
- Lifetime: ~ 10 years
- Atomic clocks
- Ground stations (MCS in Colorado)
- *Music box*: time and trajectory information

Basics



Errors, more satellites, previous results:

Do not solve, but optimize...

$$(x_1 - \mathbf{x})^2 + (y_1 - \mathbf{y})^2 + (z_1 - \mathbf{z})^2 = d_1^2$$
$$(x_2 - \mathbf{x})^2 + (y_2 - \mathbf{y})^2 + (z_2 - \mathbf{z})^2 = d_2^2$$
$$(x_3 - \mathbf{x})^2 + (y_3 - \mathbf{y})^2 + (z_3 - \mathbf{z})^2 = d_3^2$$

Trilateration - wish it were so easy...

Receiver time synchronization

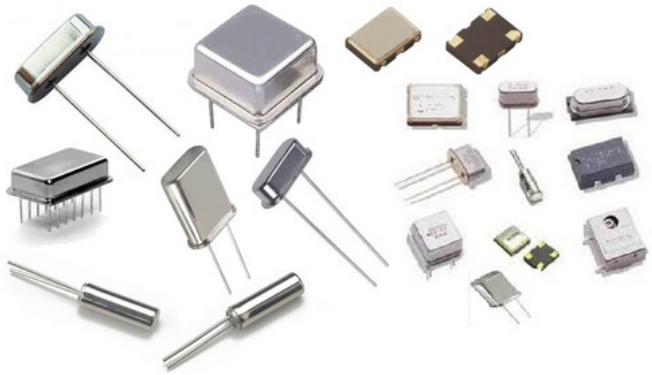
Range measurements (d_i) @ speed of light

300,000,000 meters / second

1 meter ~ 3 nanoseconds

Bad news:

- Crystal oscillators: 50ppm
  - 50 us within a second (**15km**)
  - 1-2 minutes within a month
- Atomic clocks
  - Expensive
  - Big
  - Cannot buy them on Amazon.com



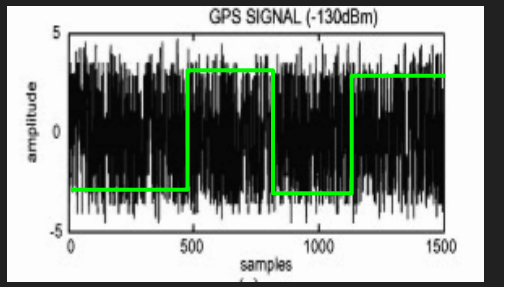
Receiver time synchronization

- Solution: accept and embrace the problem
- Use the receiver clock - as bad it is - for ranging:

PSEUDORANGE

- Additional unknown**: receiver time (error)**
  - One more (4) minimum measurements / eqs
  - *Difference in time of arrival* (DToA)
- **All ranging (d_i) should happen at the same time**

Weak Signal

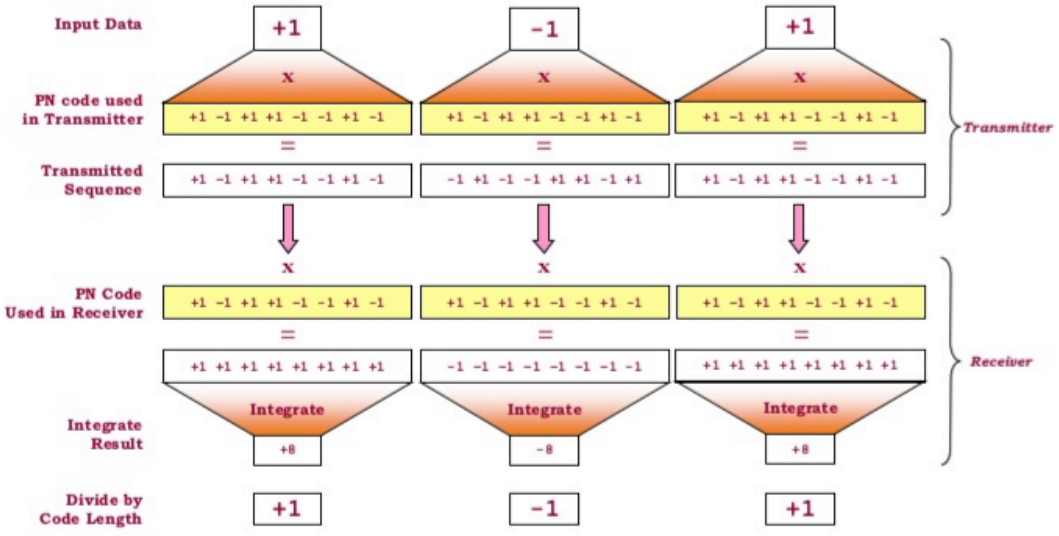


- Transmit power (solar panels): **25.6W**
- 13 dBi Antenna gain: **500W** (57dBm)
- Free space loss (20,000km): 182dB
- At the receiver: ~ **10^{-16} W** (130 dBm)
- Thermal noise floor (bandwidth, temp): ~ **10^{-14} W** (110dBm)
- **SNR: -20dB (1:100 power)**!

$$C = B \log_2 \left(1 + \frac{S}{N}\right)$$

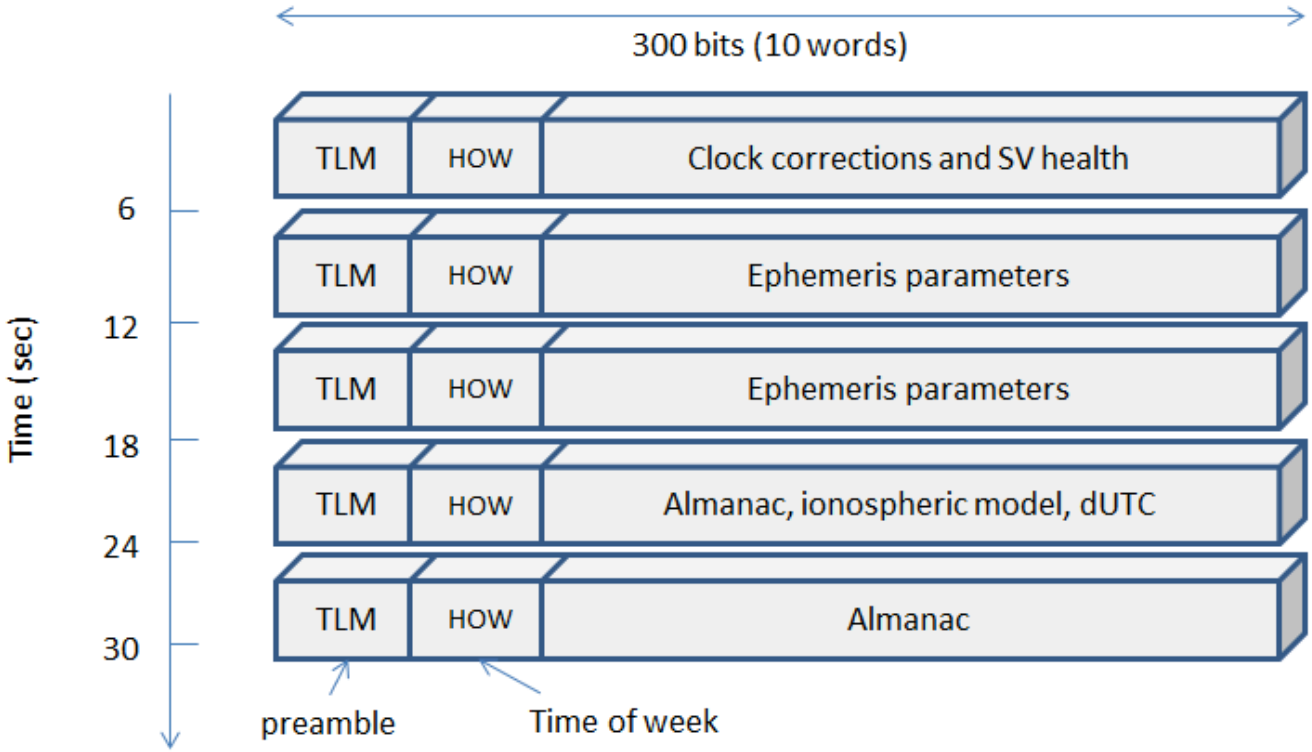
Spectrum spreading

- Redundancy - ***speak slowly*** **+** ***correlation***
- Pseudorandom sequences: **Gold code**

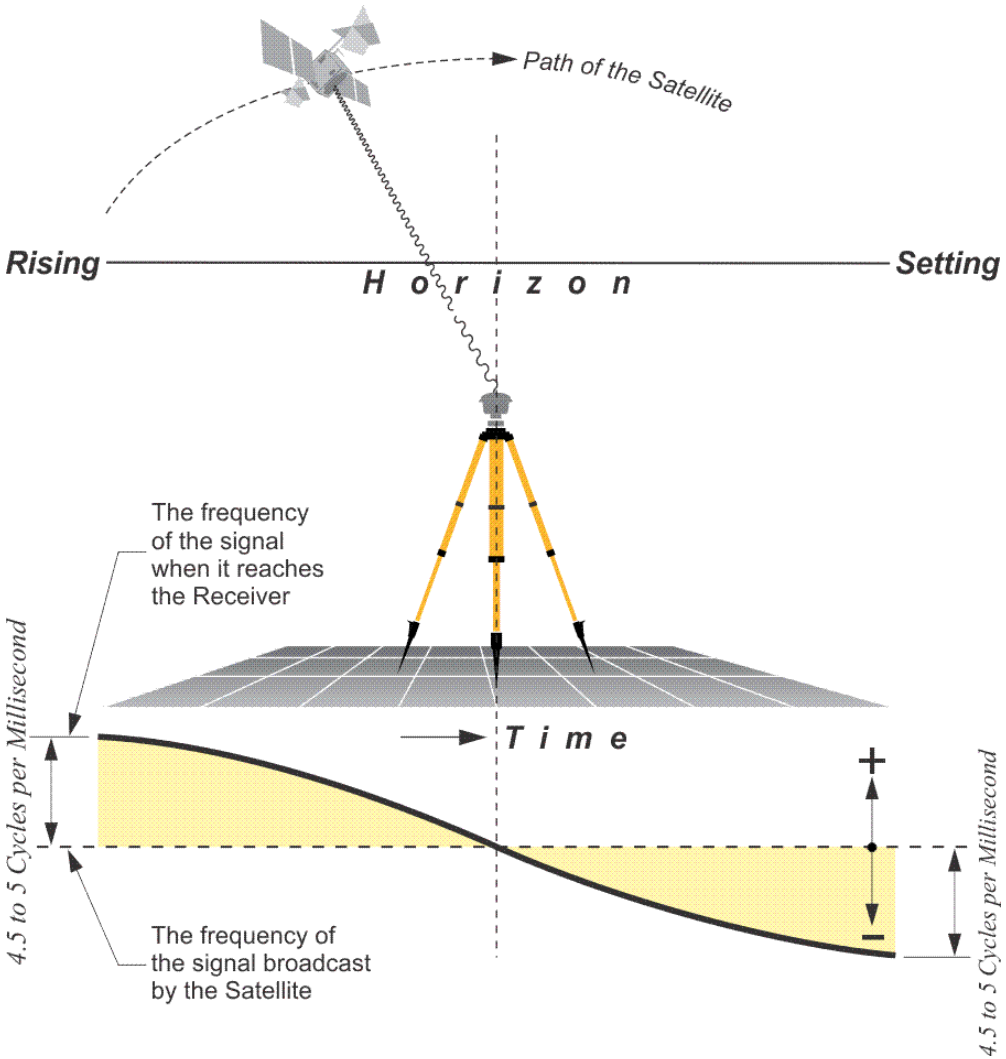


- **Weak-signal** + **multiple** GPS satellites

Data Packets



Source: Jie Liu: GPS Fundamentals

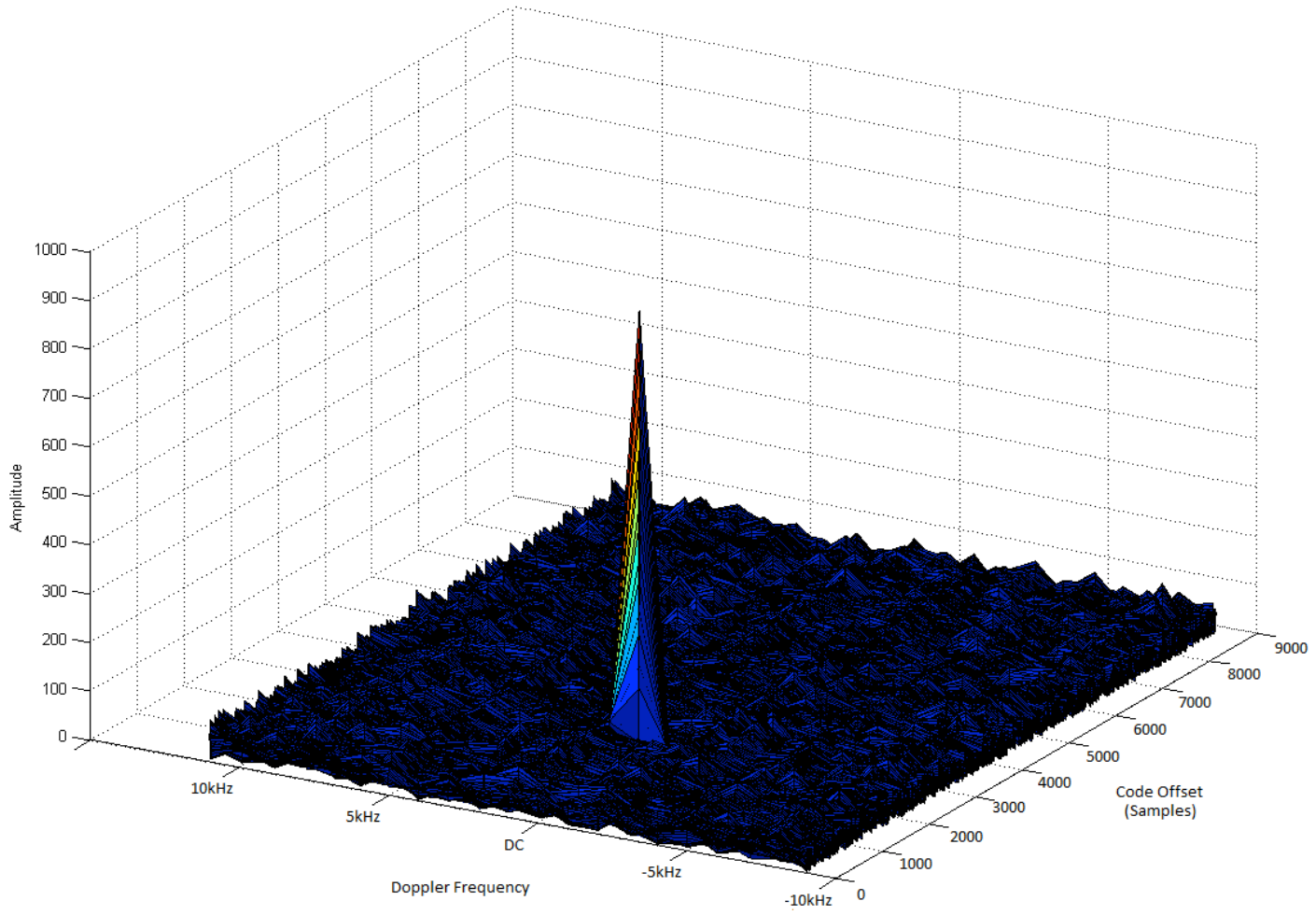


+/- 5kHz (stationary)

Receiver needs to find and track:

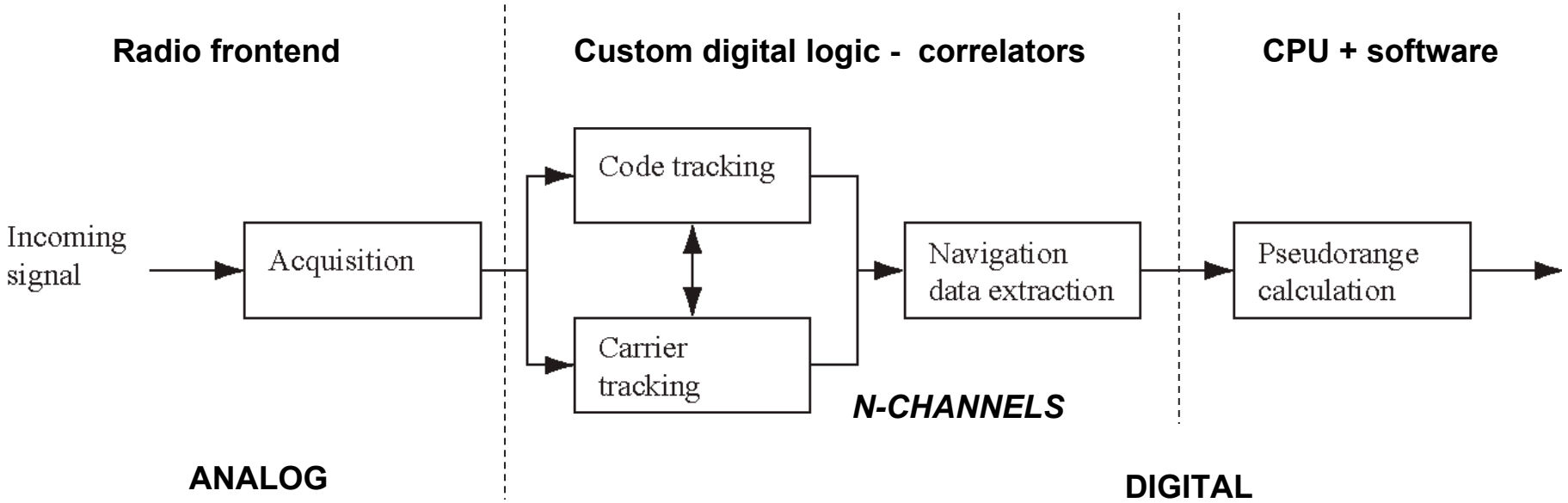
delay and frequency

Doppler Shift



Correlation - time and frequency shift

Inside the GPS Receiver



ANALOG

DIGITAL

Vulnerabilities - Jamming

- Easy and cheap
  - Random powerful transmission
- **Dangerous**
  - **Examples - critical infrastruct**
- **Illegal**
  - **Easy to detect and localize**
  - **Federal crime**
- Defense options
  - Directional antennae
  - Sophisticated RF frontends

Vulnerabilities - Spoofing

- Not that easy
  - should override existing satellite signals (**all of them**)
  - needs consistent signal streams (**at receiver**)
  - might require multiple frequencies
- Simpler options
  - Replay attack
  - SBAS / augmentation attack
- **Dangerous and Illegal**
- Defense
  - Additional location sources (WiFi, Cellular)