Wireless Security

GNSS Security

Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland

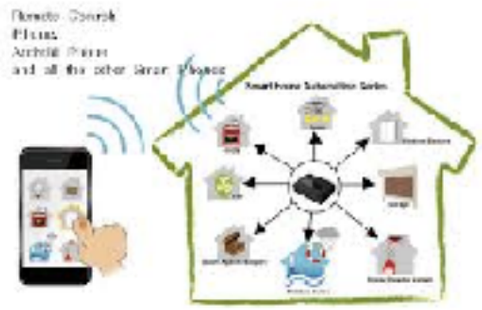
All photographs, imagery, media belong to their respective owners/creators.

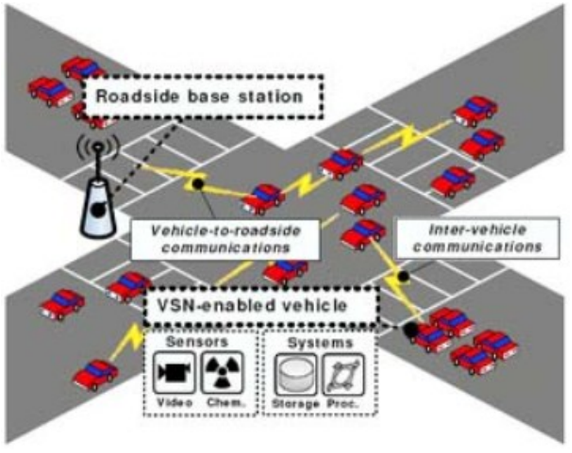
Recommended Readings

- GPS Compendium (from ublox) https://www.u-blox.com/sites/default/files/gps_compendiumgps-x-02007.pdf
- **On the requirements for successful GPS spoofing attacks.** *Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun*. (CCS'11)
- **SPREE: a spoofing resistant GPS receiver.** *Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun.* (MobiCom 2016)
- **GPS software attacks.** *Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley.* (CCS' 12)

...

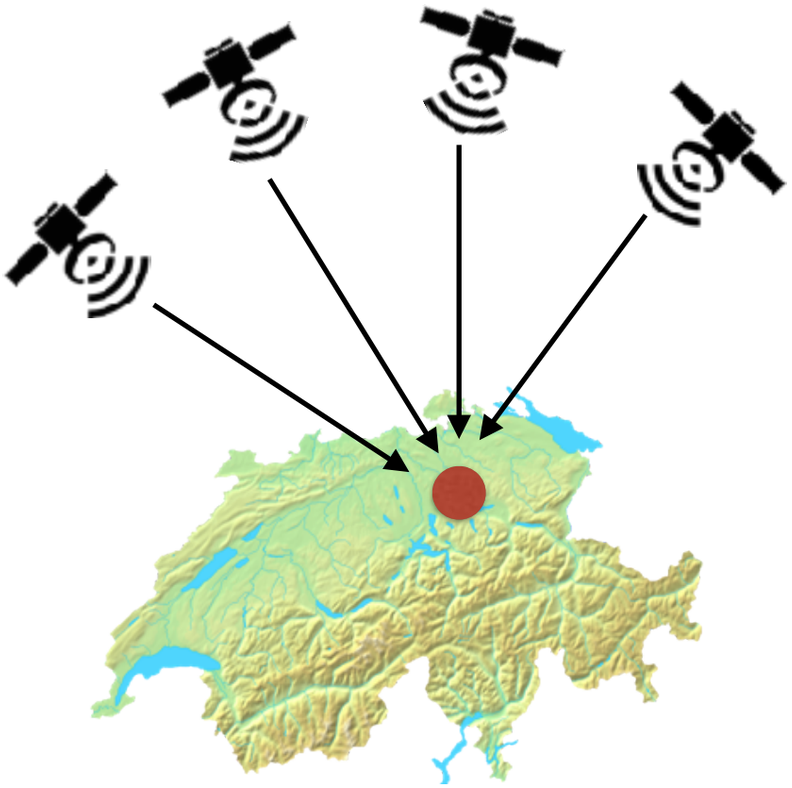
IoT, Smart Homes, Smart Healthcare, Smart Grids, Smartphones, Drones, Autonomous Cars, Vehicular Networks, Cyber-Physical Systems, …





Various Internet Sources.

GPS



- 24 satellites at ~ 20,200 Km above earth. Each satellite transmits navigation messages containing its location and precise time of transmission

- Unique pseudorandom codes are used

- GPS receiver measures each navigation message's arrival time and estimates its distance to the satellite.

- Receiver's position and time is calculated using trilateration

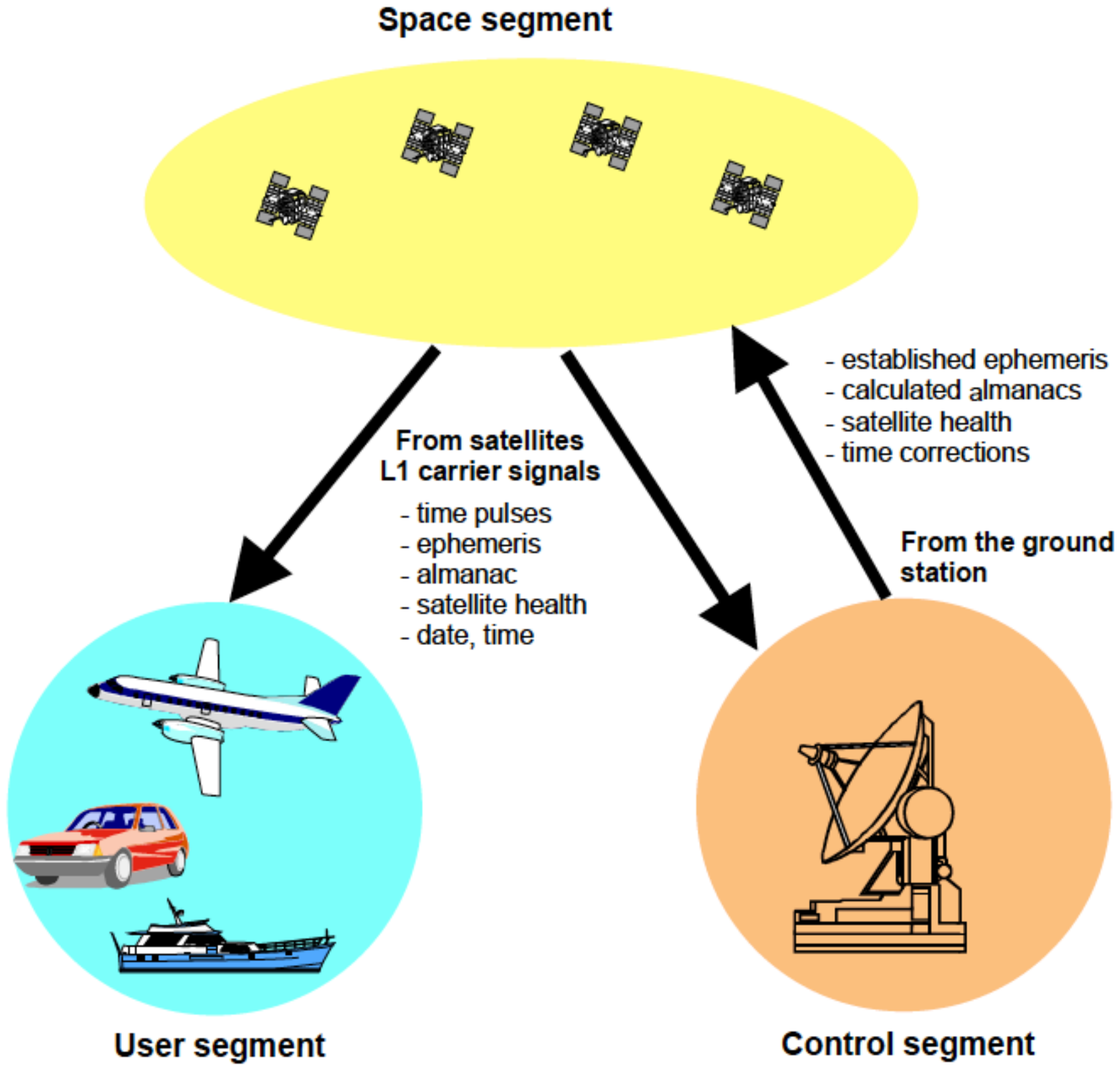


Figure 34: The three GPS segments

Satellite signals can be received anywhere within a satellite's effective range. Figure 36 shows the effective range (shaded area) of a satellite located directly above the equator/zero meridian intersection.

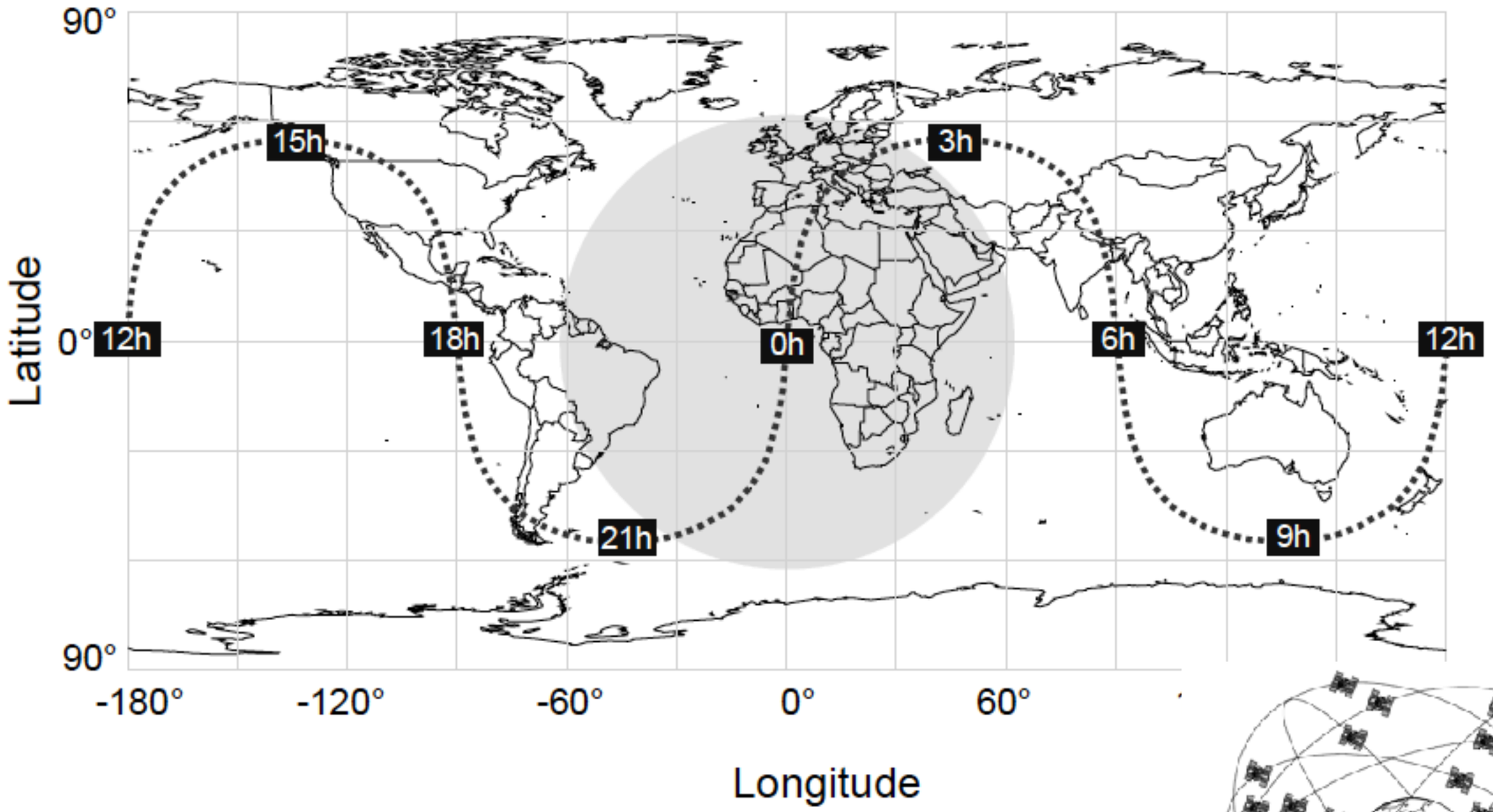


Figure 36: 24 hour tracking of a GPS satellite with its effective range

figure 35: GPS satellites orbit the Earth on 6 orbital planes

The distribution of the satellites at a specific time can be seen in Figure 37. It is due to this ingenious pattern of distribution and to the high orbital altitudes that communication with at least 4 satellites is ensured at all times anywhere in the world.

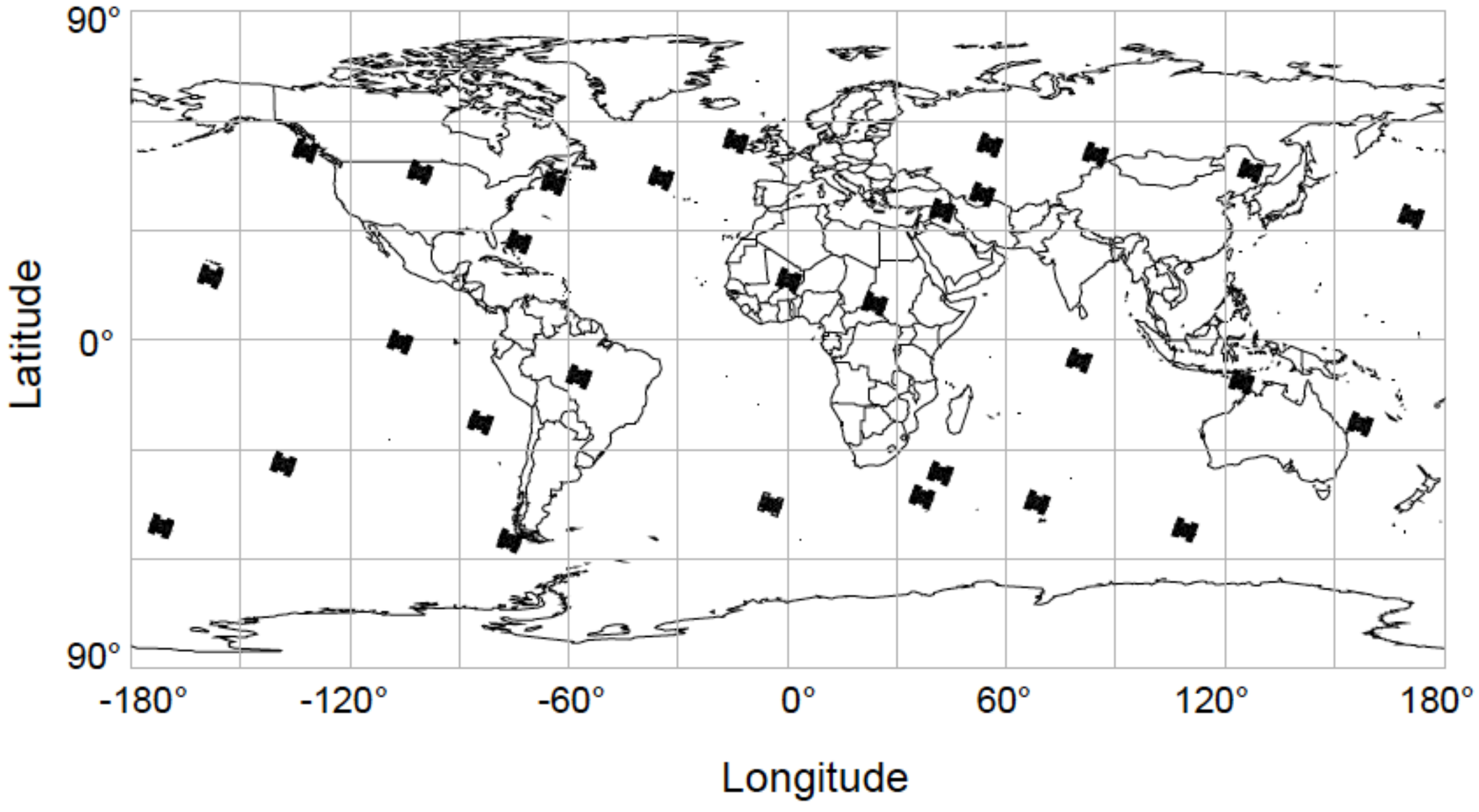
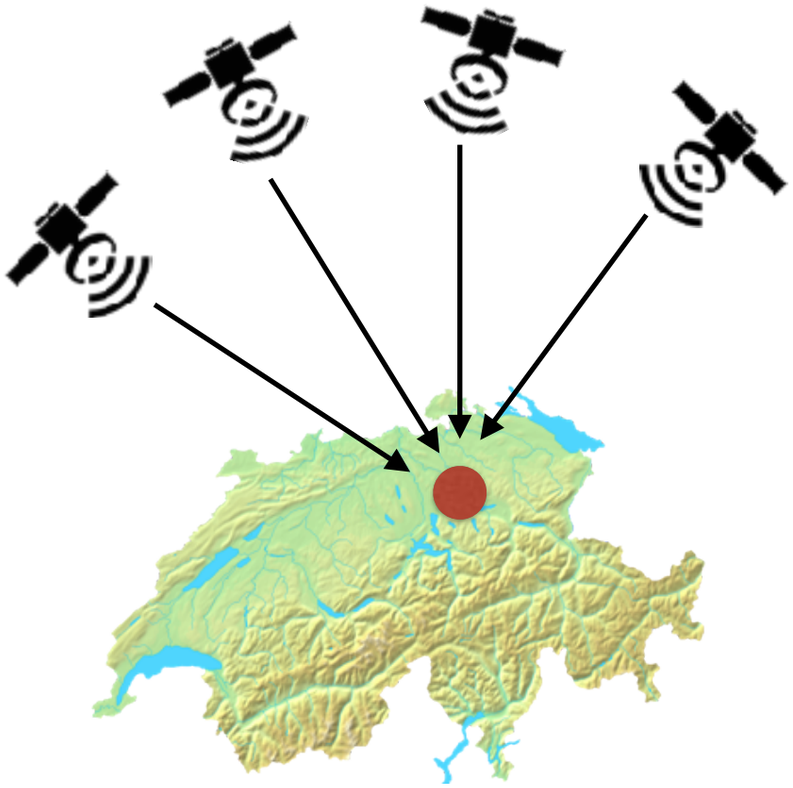
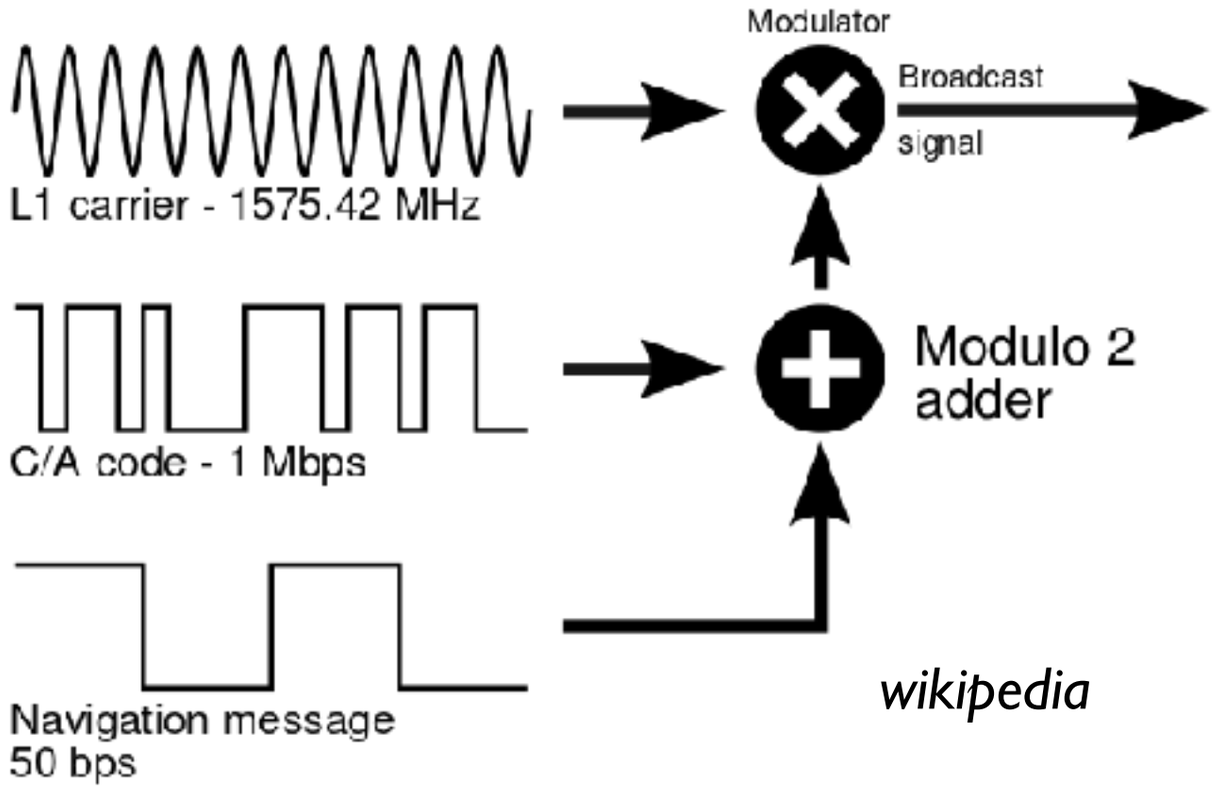


Figure 37: Position of the GPS satellites at 12:00 hrs UTC on 14th April 2001

Global Positioning System (GPS)



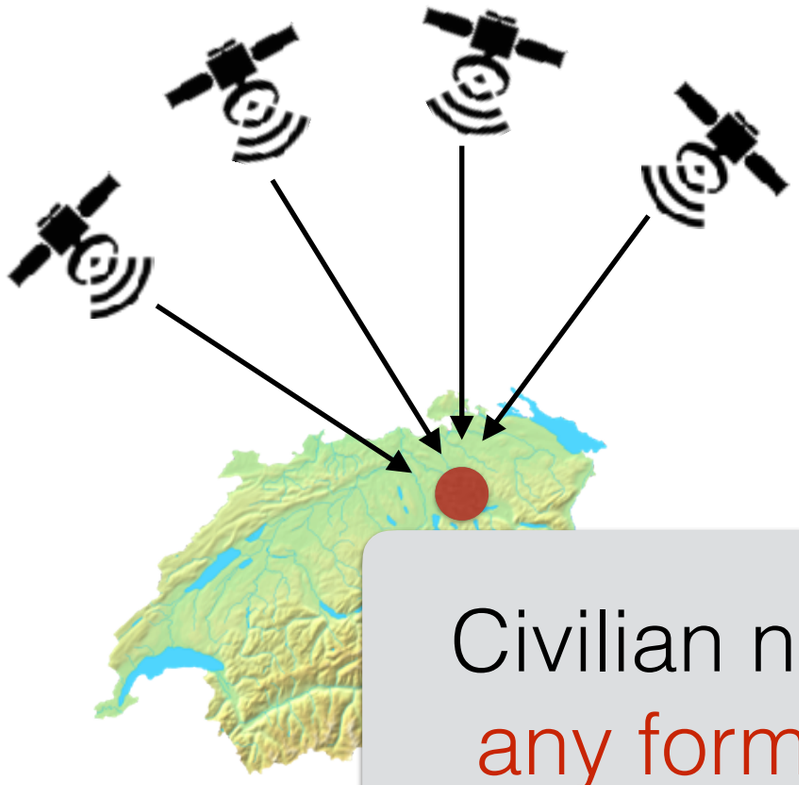


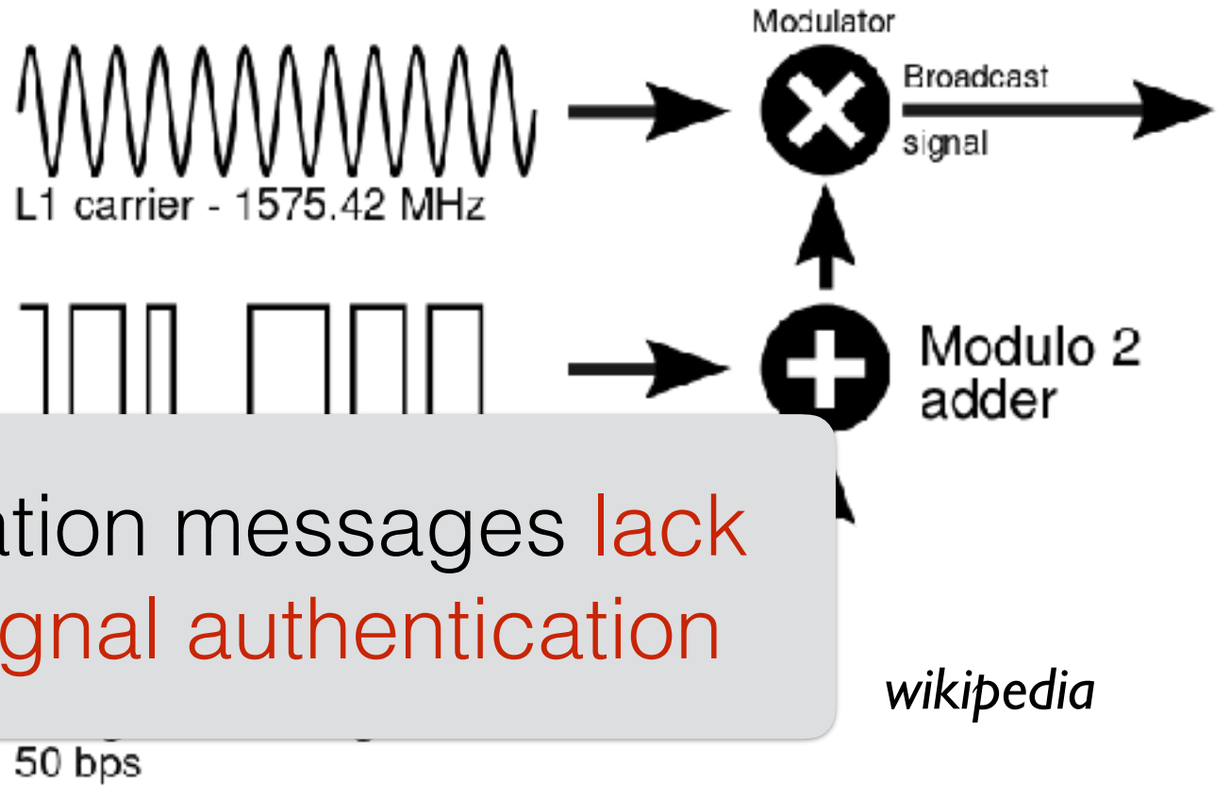
wikipedia

1575.42 MHz (L1);
1227.60 MHz (L2).

- **C/A** (Coarse Acquisition) codes: Gold Codes, 1023 chips, transmitted at 1.023 Mbits (i.e., repeats every 1ms), uses L1 only
- **P** (precision) codes: 6.1871×10^{12} chips long, transmitted at 10.23 Mbit/s, (i.e. repeats once a week), uses L1 and L2 only
- **Y** (P(Y)) code: encrypted P code (modulated with secret W code)
- new: L2C, L1C, …

Global Positioning System (GPS)





Civilian navigation messages lack any form of signal authentication

wikipedia

1575.42 MHz (L1);
1227.60 MHz (L2).

- **C/A** (Coarse Acquisition) codes: Gold Codes, 1023 chips, transmitted at 1.023 Mbits (i.e., repeats every 1ms), uses L1 only
- **P** (precision) codes: 6.1871×10^{12} chips long, transmitted at 10.23 Mbit/s, (i.e. repeats once a week), uses L1 and L2 only
- **Y** (P(Y)) code: encrypted P code (modulated with secret W code)
- new: L2C, L1C, …

GPS

The link budget analysis (Table 6) between a satellite and a user is suitable for establishing the required level of satellite transmission power. According to the specifications, the minimum amount of power received must not fall below –160dBW (-130dBm). In order to ensure this level is maintained, the satellite L1 carrier transmission power, modulated with the C/A code, must be 21.9W. Polarization mismatch and antenna reception gain are a function of receiver design. The sum of these two parameters may vary largely. Depending on the design values between +5 dB to -10dB are typical.

	Gain (+) /loss (-)	Absolute value
Power at the satellite transmitter		13.4dBW (43.4dBm=21.9W)
Satellite antenna gain (due to concentration of the signal at 14.3°)	+13.4dB	
Radiate power EIRP (Effective Integrated Radiate Power)		26.8dBW (56.8dBm)
Loss due to polarization mismatch	-3.4dB	
Signal attenuation in space	-184.4dB	
Signal attenuation in the atmosphere	-2.0dB	
Gain from the reception antenna	+3.0dB	
Power at receiver input		-160dBW (-130dBm=100.0*10^{-18}W)

Table 6: L1 carrier link budget analysis modulated with the C/A code

According to the specifications, the power of the received GPS signal in open sky is at least -160dBW (-130dBm). The maximum of the spectral power density of the received signal is given as -190dBm/Hz (Figure 39). The spectral power density of the thermal background noise is about –174dBm/Hz (at a temperature of 290K). Thus the maximum received signal power is approximately 16dB below the thermal background noise level.

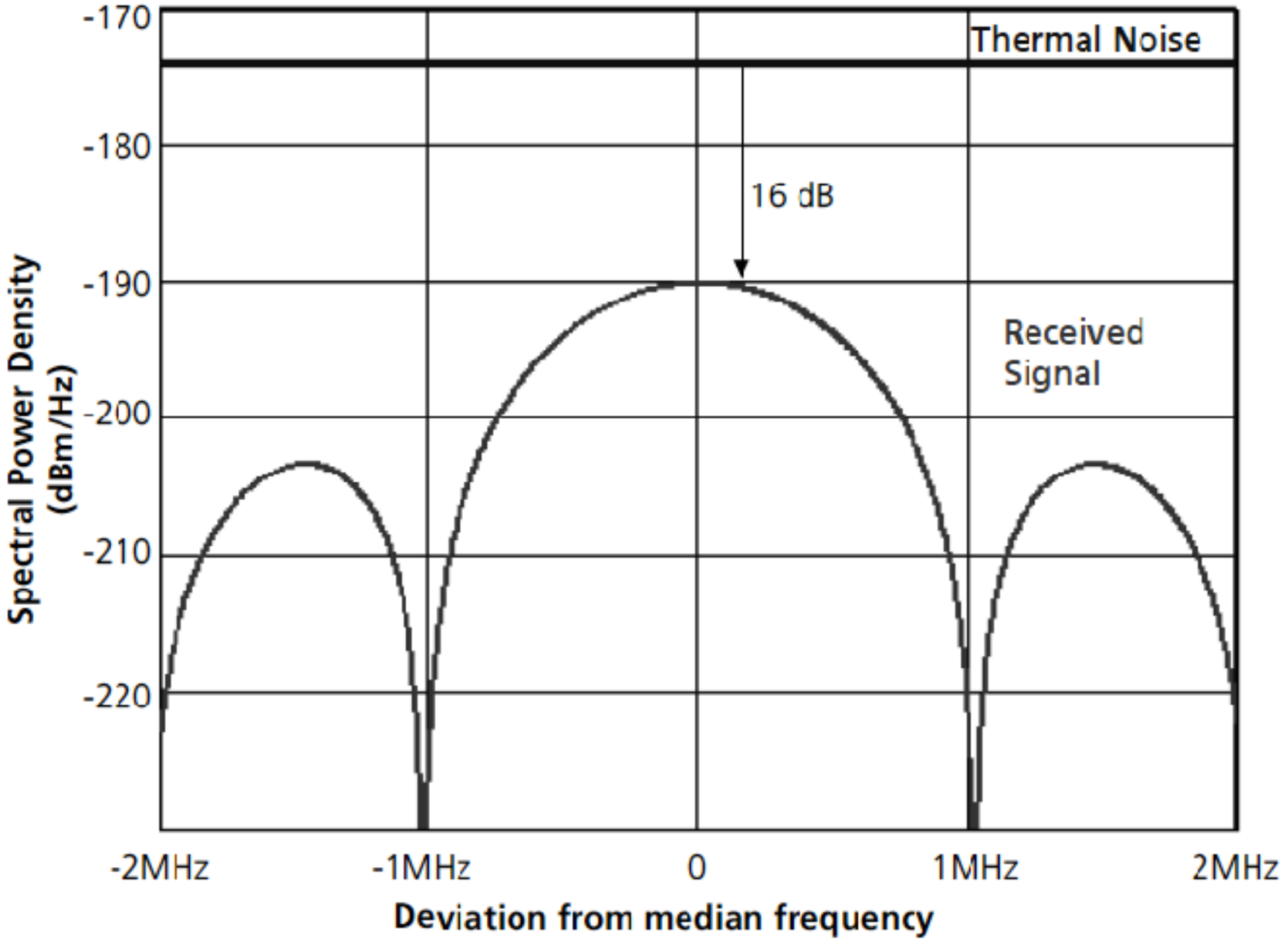


Figure 39: Spectral Power Density of received signal and thermal noise

4.3.2.3 Satellite signals

The following information (the navigation message) is transmitted by the satellite at a rate of 50 bits per second [15]:

- Satellite time and synchronization signals
- Precise orbital data (ephemeris)
- Time correction information to determine the exact satellite time
- Approximate orbital data for all satellites (almanac)
- Correction signals to calculate signal transit time
- Data on the ionosphere
- Information on the operating status (health) of the satellite

The time required to transmit all this information is 12.5 minutes. By using the navigation message, the receiver is able to determine the transmission time of each satellite signal and the exact position of the satellite at the time of transmission.

Each GPS satellite transmits a unique signature assigned to it. This signature consists of a Pseudo Random Noise (PRN) Code of 1023 zeros and ones, broadcast with a duration of 1ms and continually repeated (Figure 40).

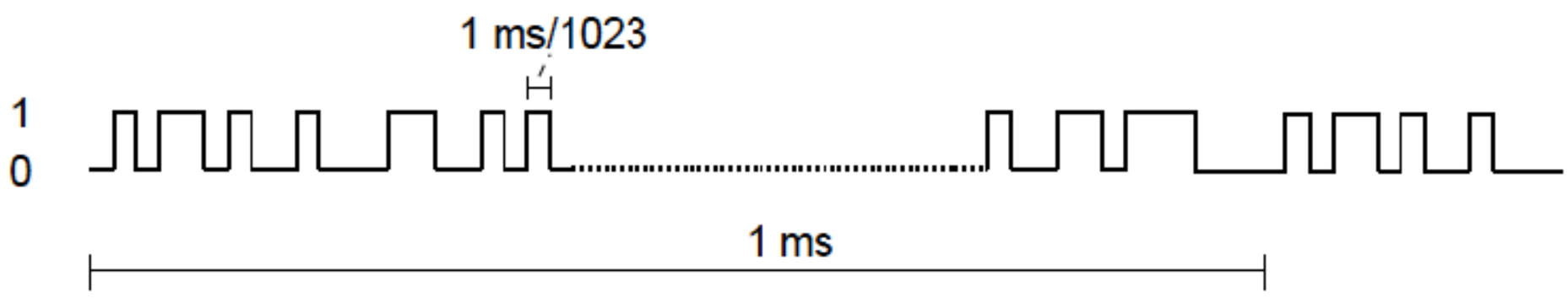


Figure 40: Pseudo Random Noise (PRN)

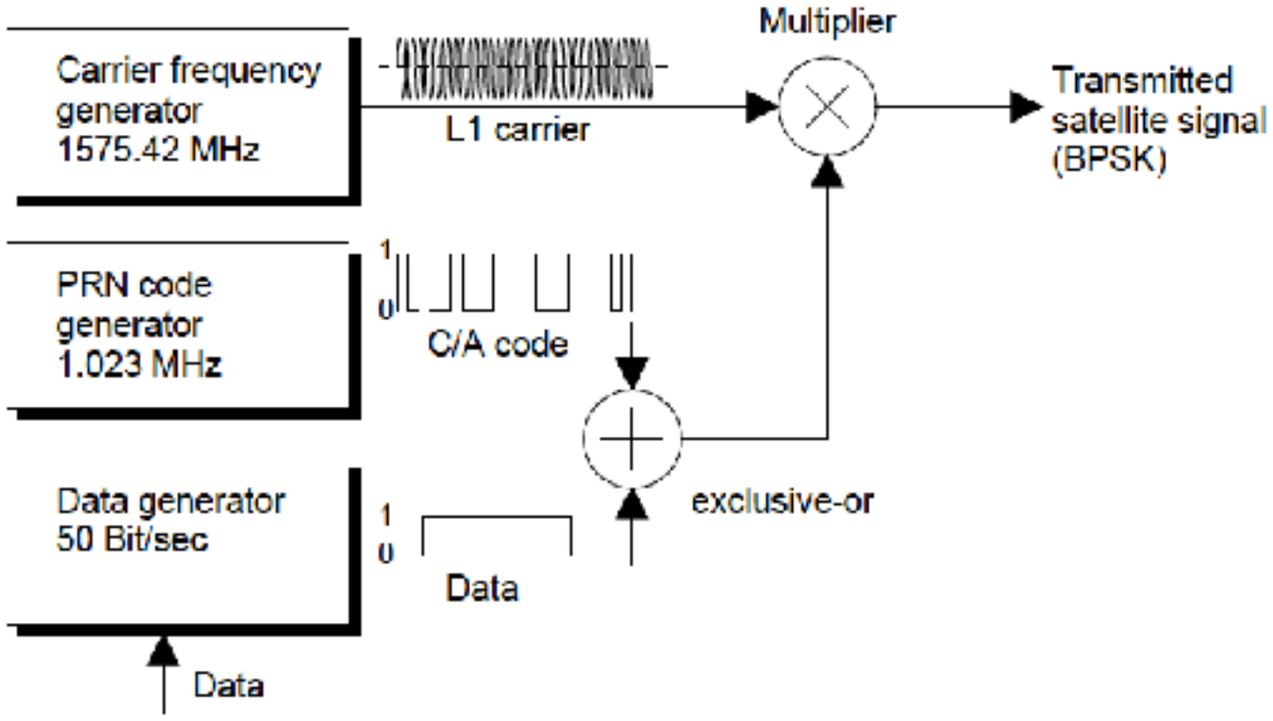


Figure 41: Simplified satellite block diagram

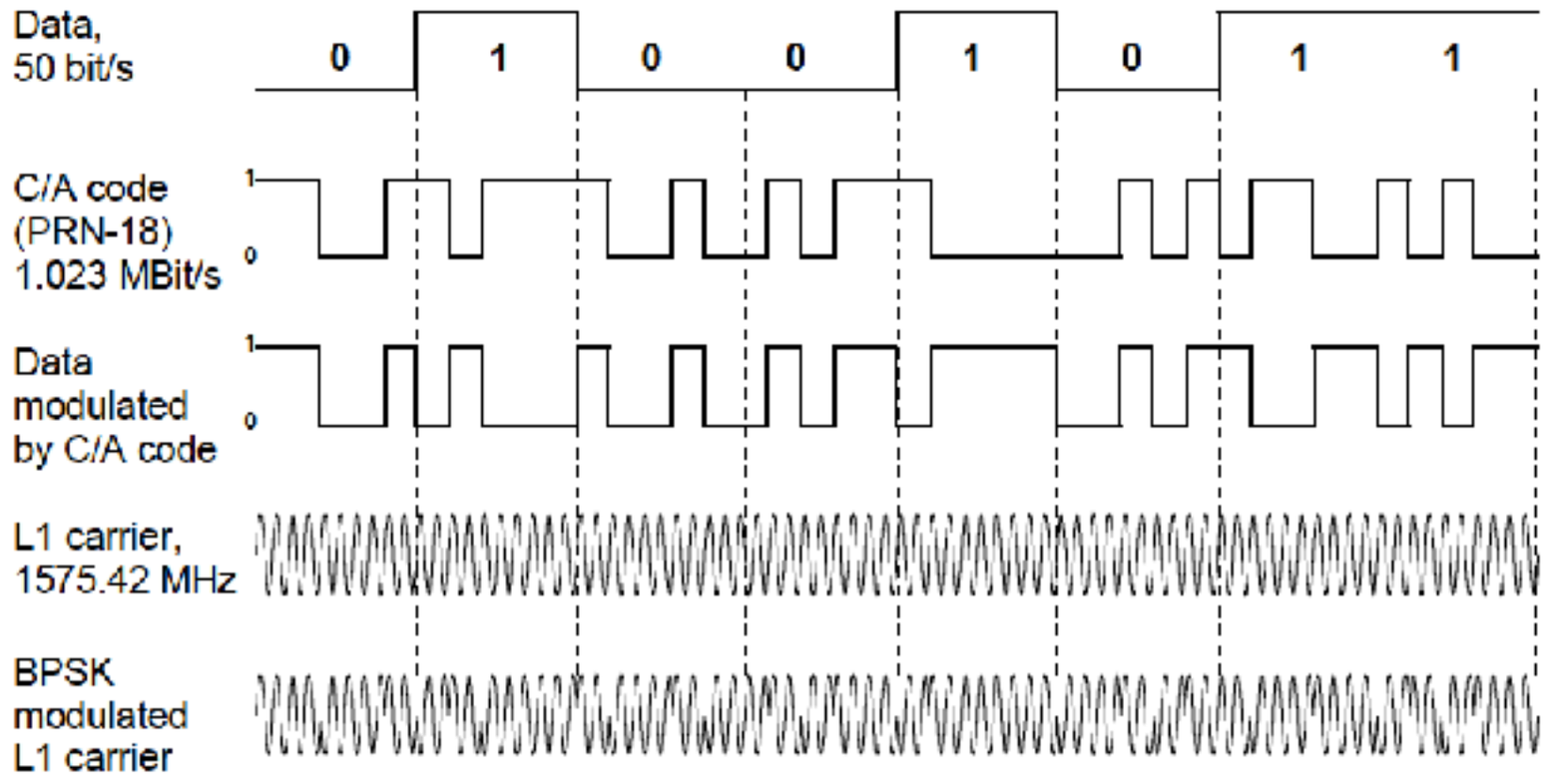


Figure 42: Data structure of a GPS signal

GPS

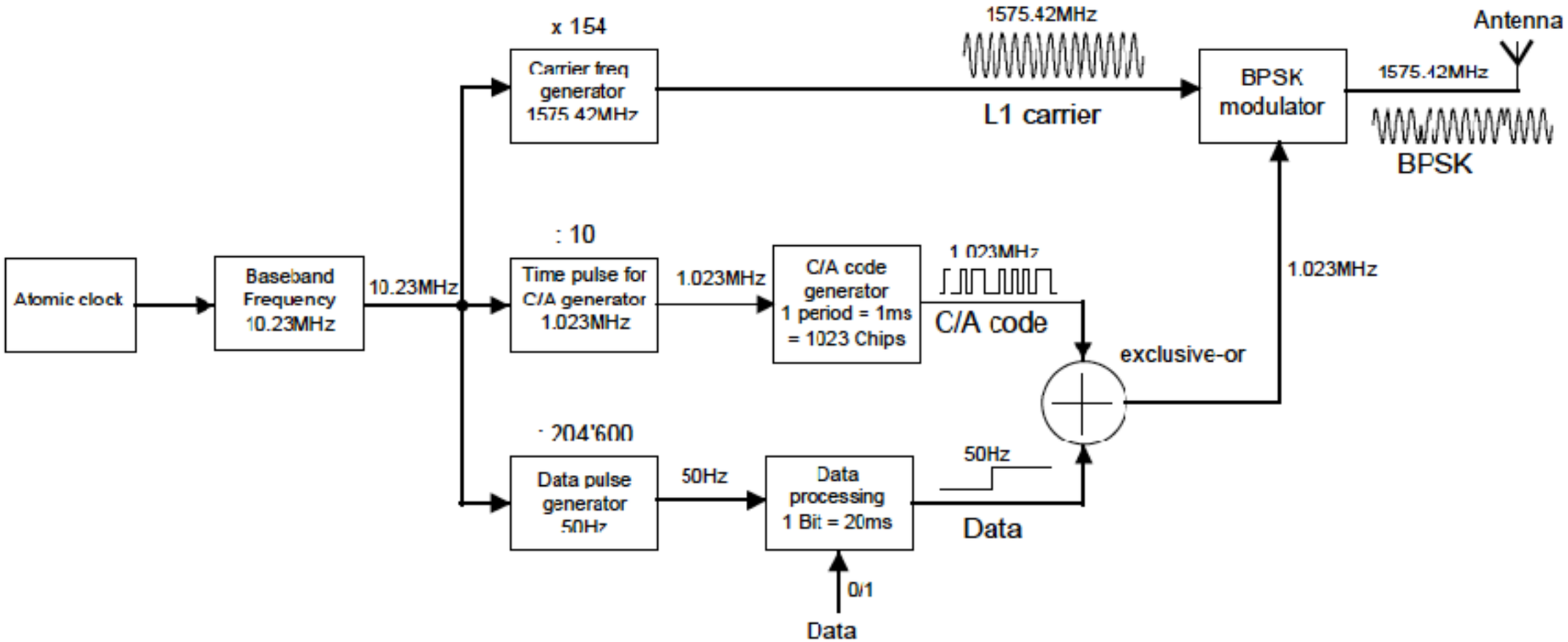


Figure 43: Detailed block diagram of a GPS satellite

GPS: Time of Arrival

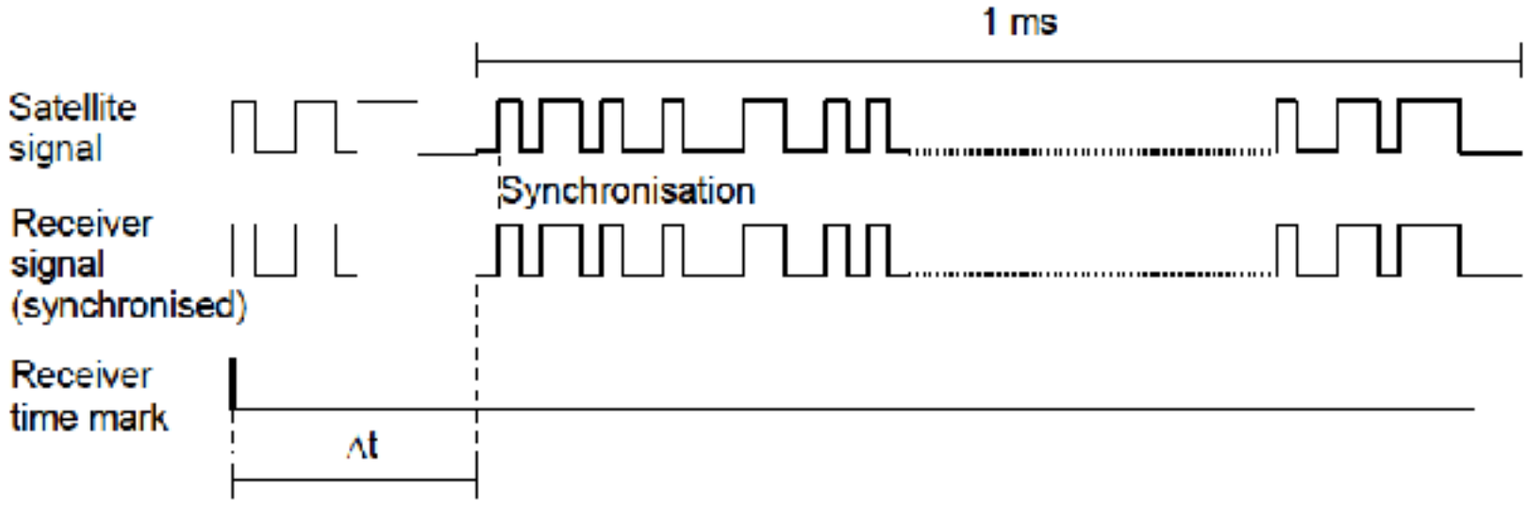


Figure 46: Measuring signal travel time

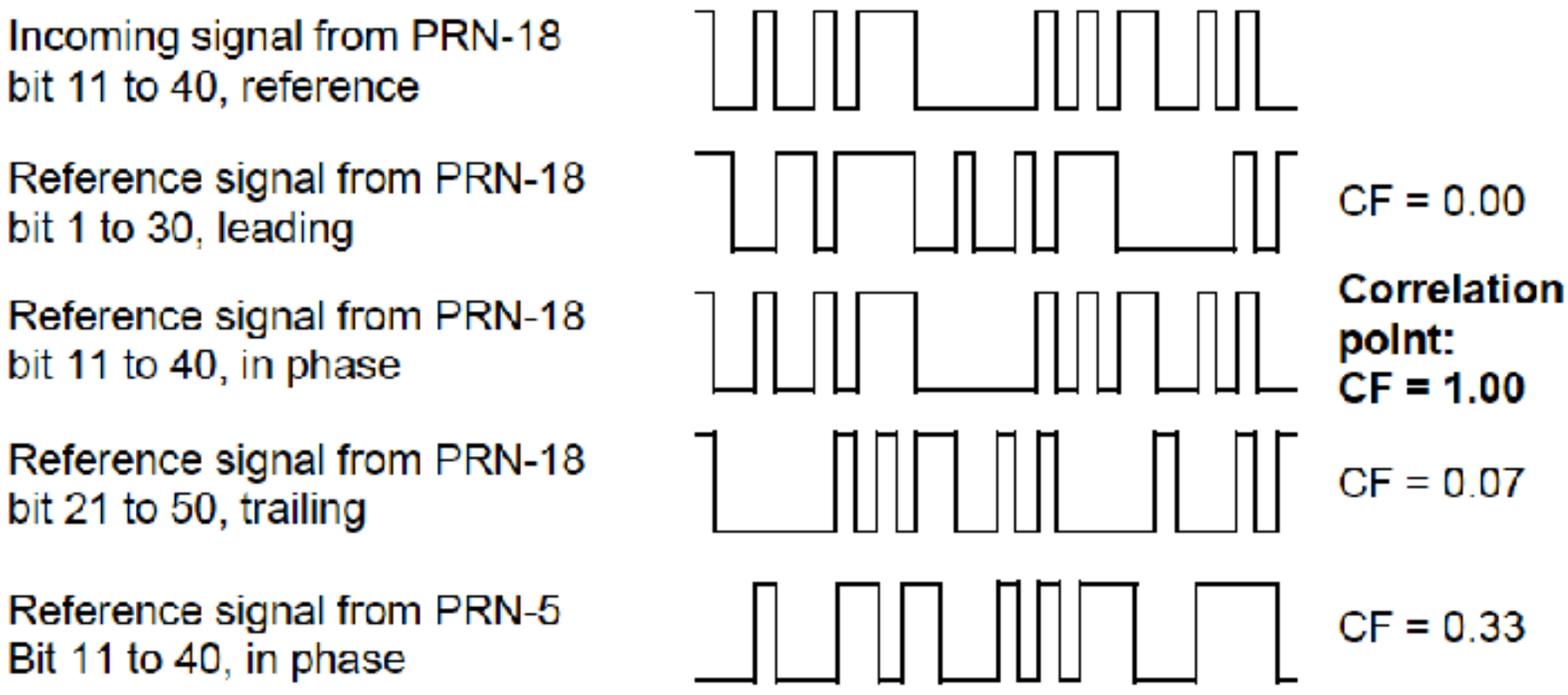
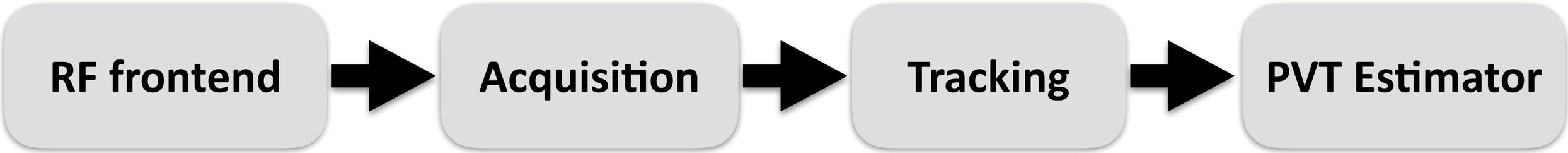
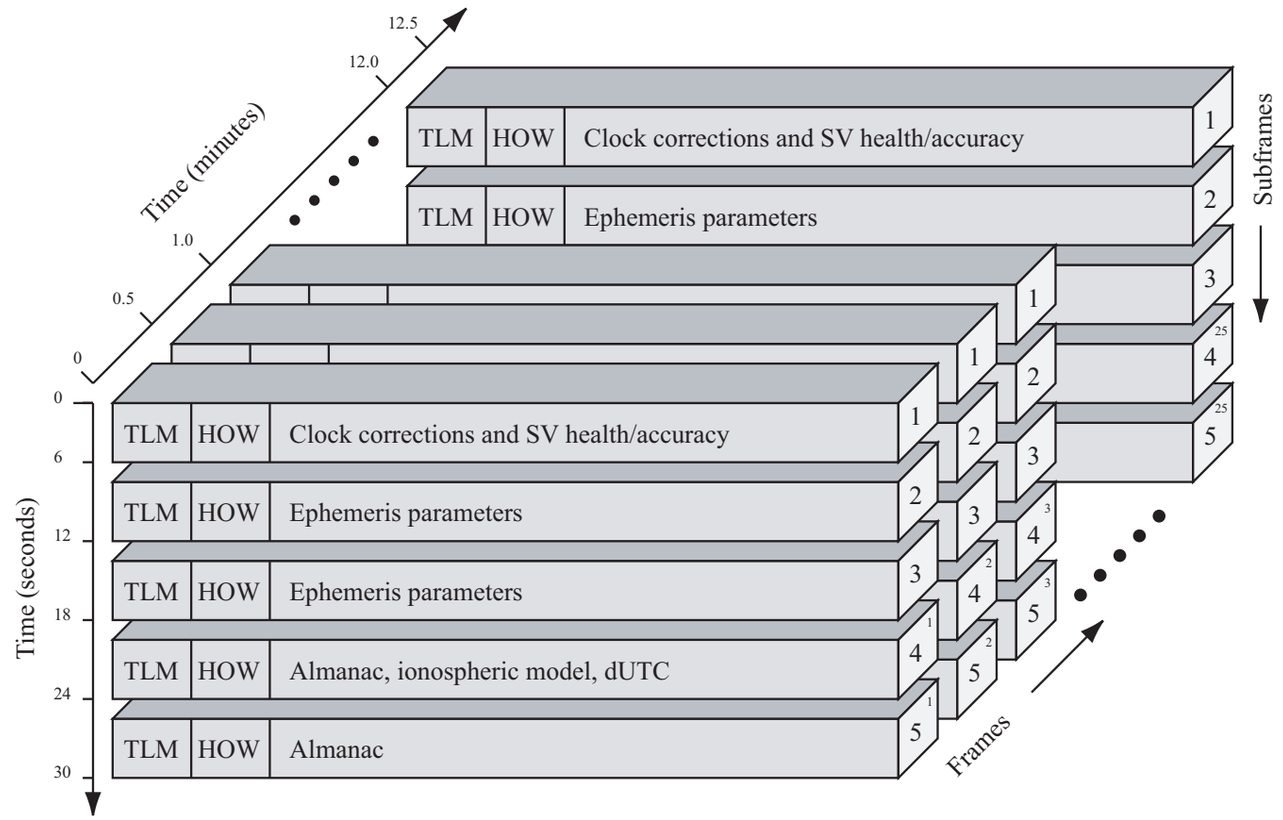


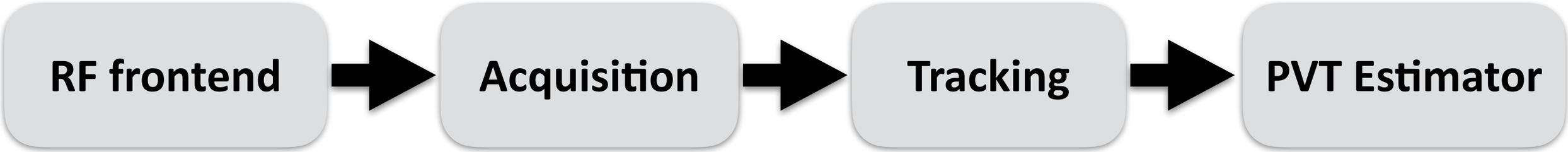
Figure 47: Demonstration of the correction process across 30 bits

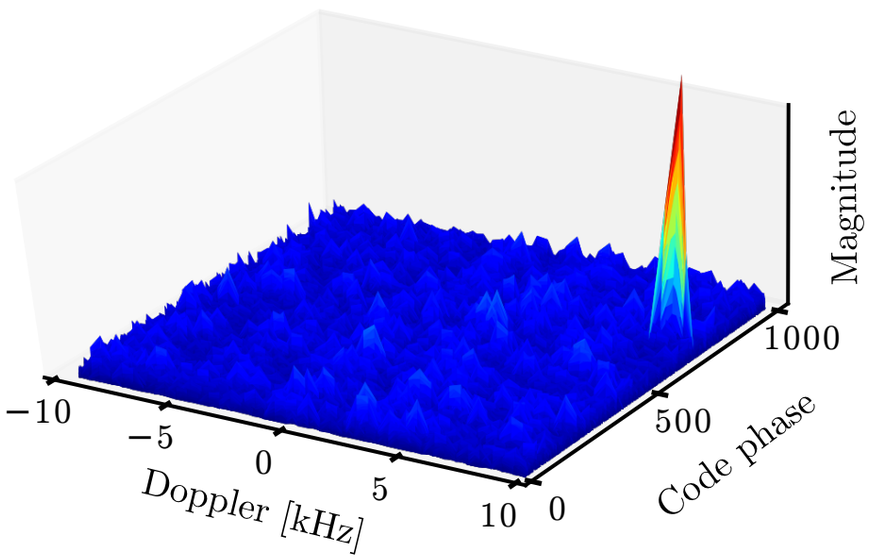
Typical GPS Receiver Architecture

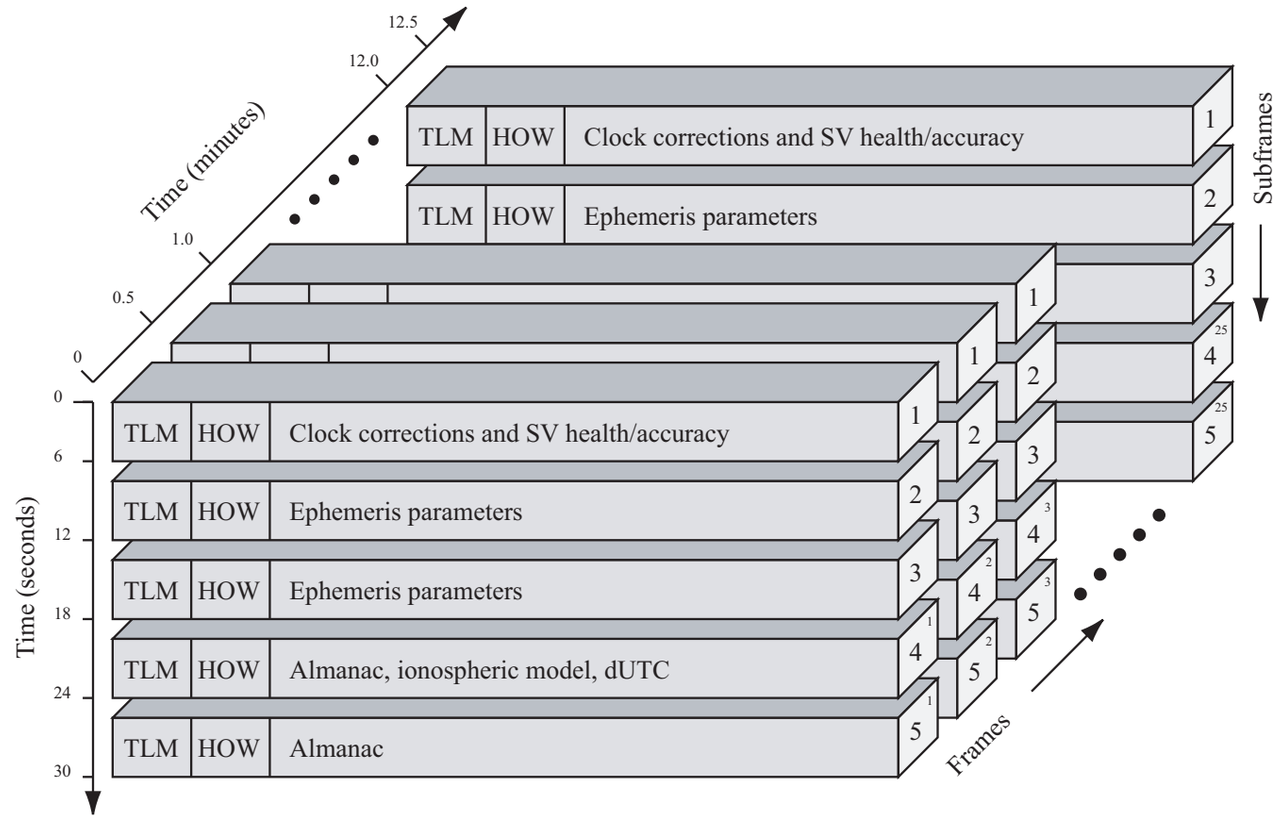




Typical GPS Receiver Architecture







GPS: Time of Arrival + Doppler

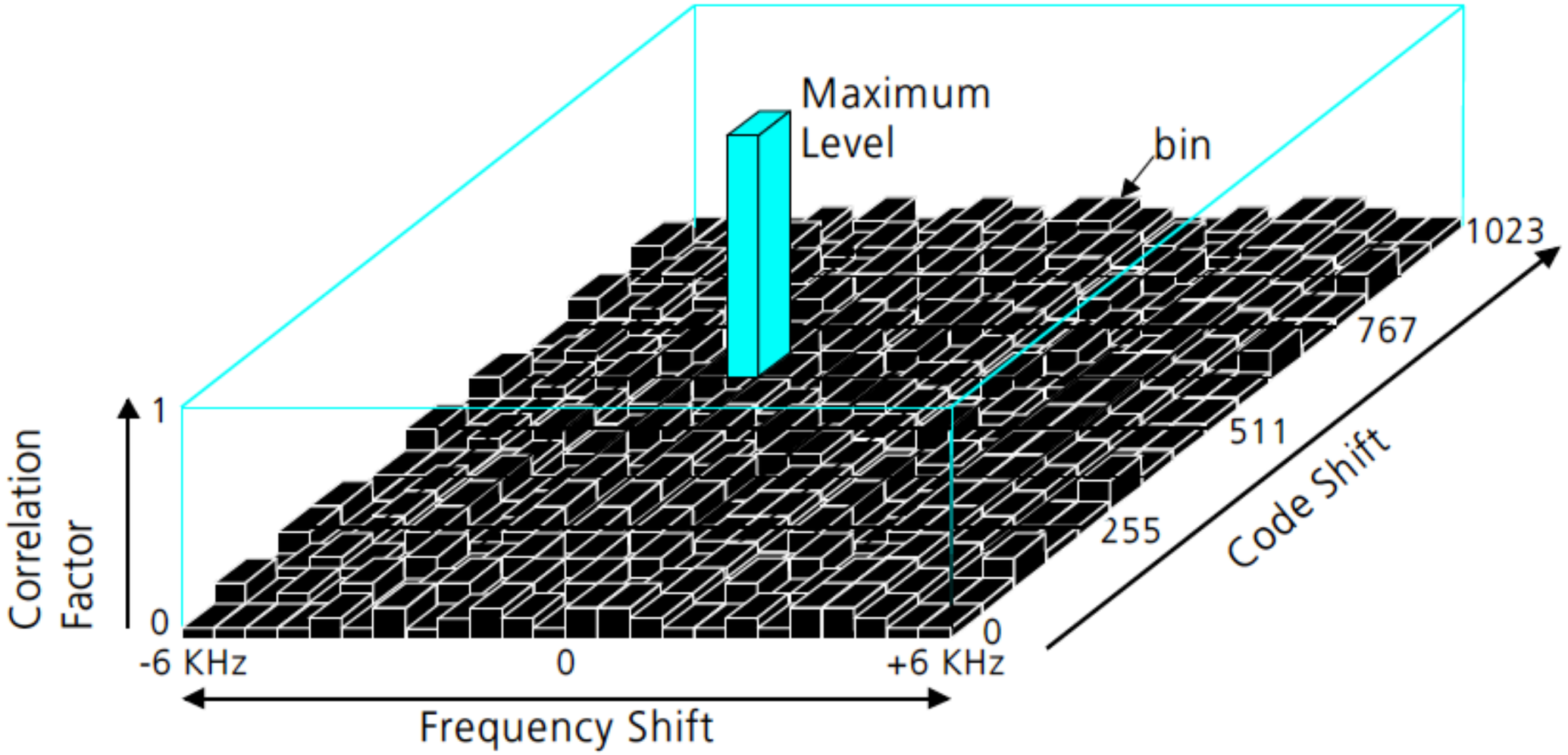


Figure 48: Search for the maximum correlation in the code and carrier frequency domains

GPS: “Digging the Signal out of the Noise”

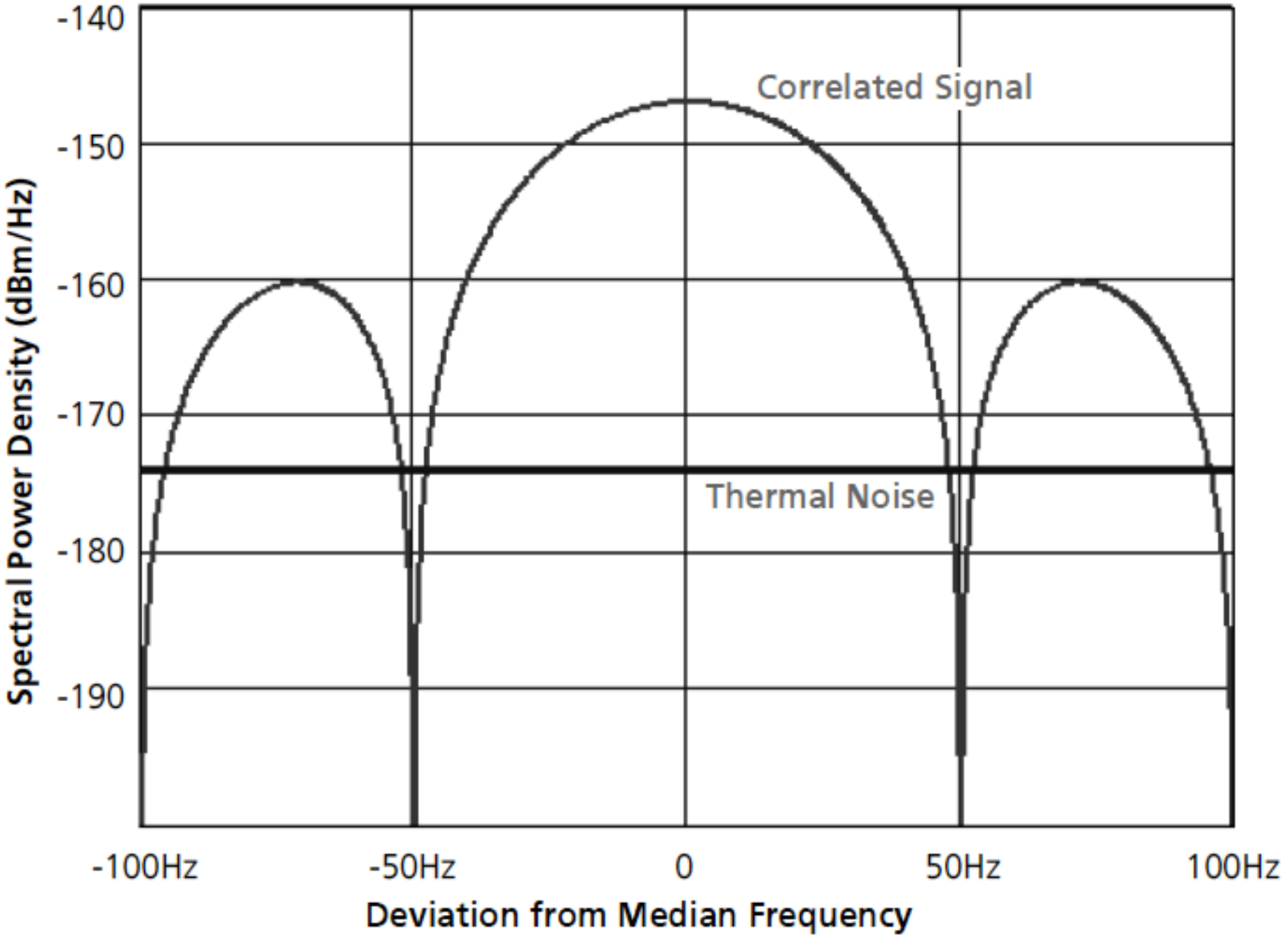
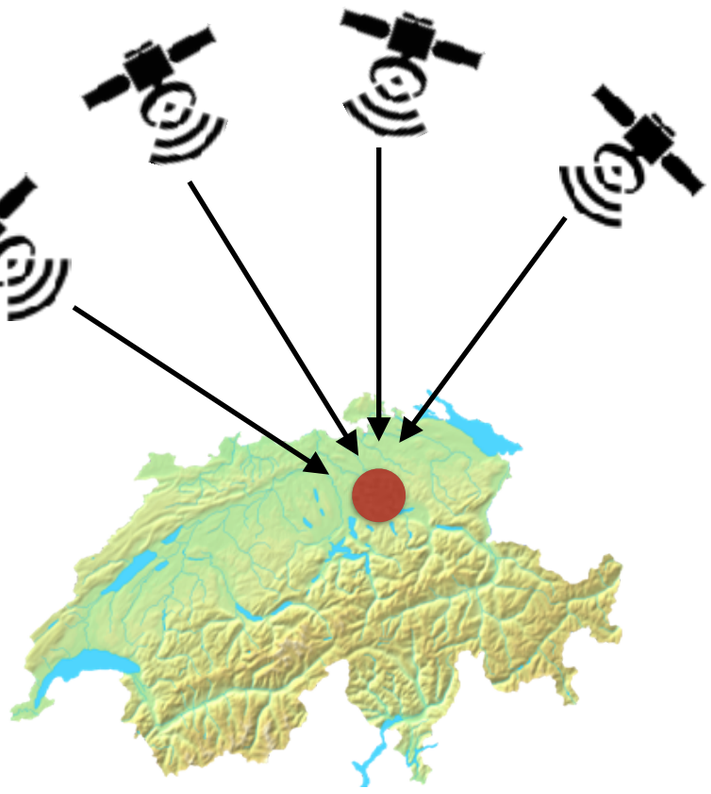
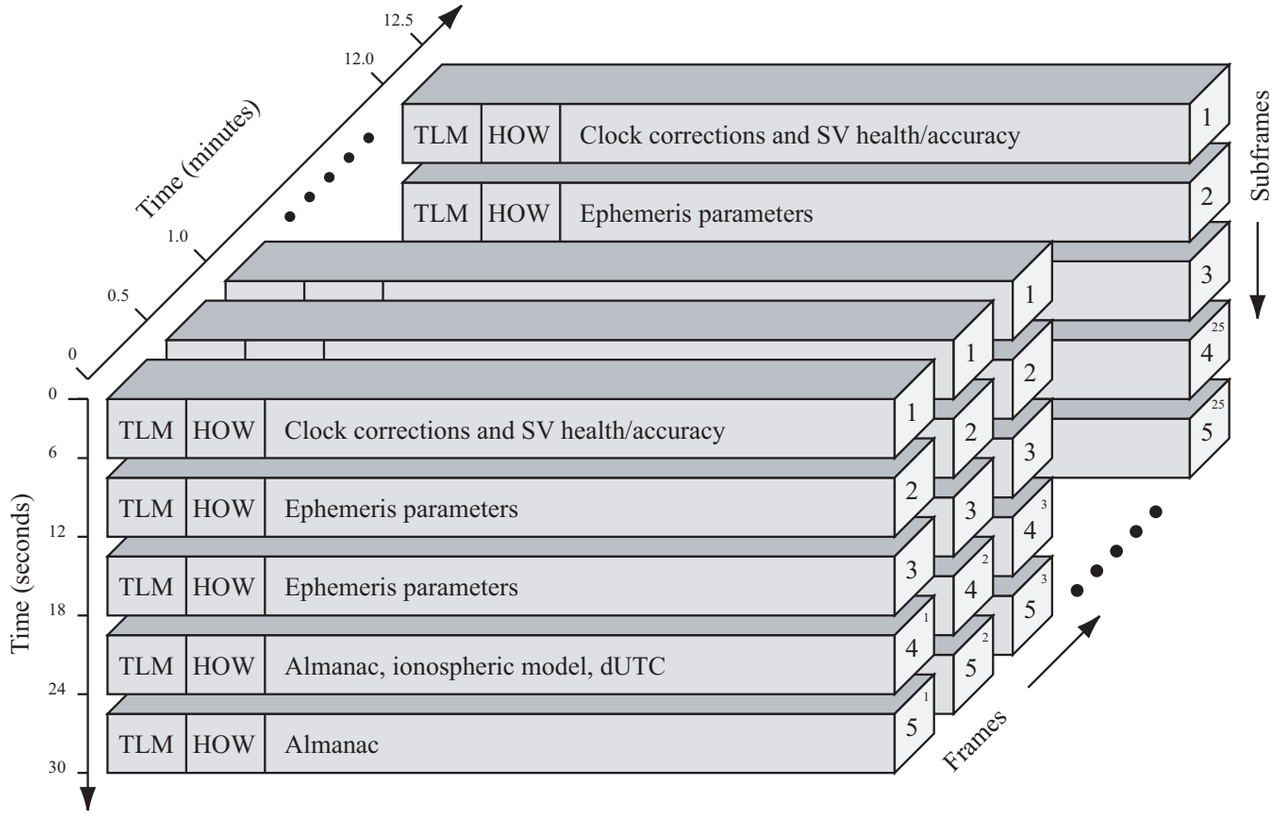


Figure 49: Spectral power density of the correlated signal and thermal signal noise

GPS messages





- Satellite clock
- Ephemeris (precise satellite orbit)
- Almanac component
(satellite network synopsis, error correction
e.g., ionospheric delay error)

http://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf

GPS messages

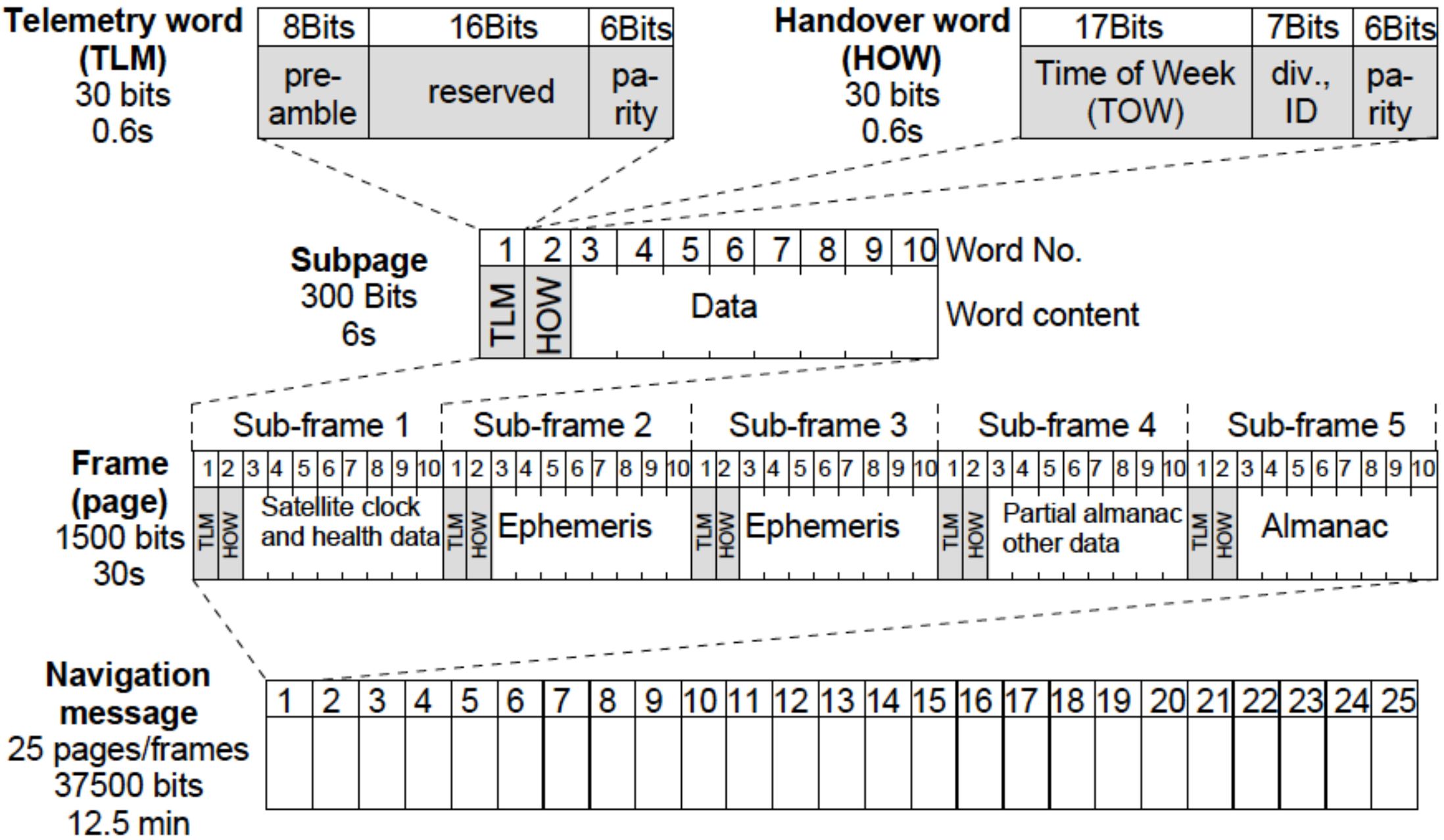


Figure 50: Structure of the entire navigation message

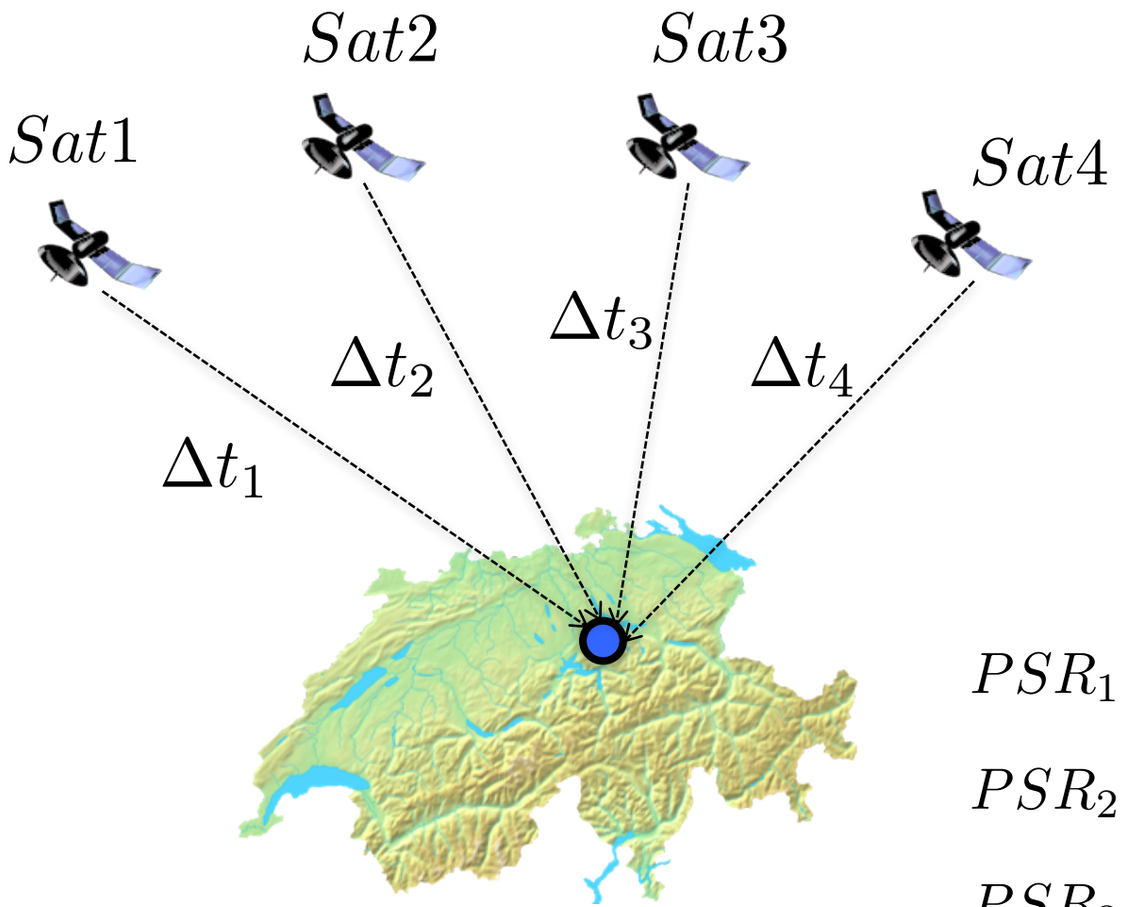
GPS messages

4.6.3 Information contained in the subframes

A frame is divided into five subframes, each subframe transmitting different information.

- Subframe 1 contains the time values of the transmitting satellite, including the parameters for correcting signal transit delay and onboard clock time, as well as information on satellite health and an estimate of the positional accuracy of the satellite. Subframe 1 also transmits the so-called 10-bit week number (a range of values from 0 to 1023 can be represented by 10 bits). GPS time began on Sunday, 6th January 1980 at 00:00:00 hours. Every 1024 weeks the week number restarts at 0. This event is called a "week rollover".
- Subframes 2 and 3 contain the ephemeris data of the transmitting satellite. This data provides extremely accurate information on the satellite's orbit.
- Subframe 4 contains the almanac data on satellite numbers 25 to 32 (N.B. each subframe can transmit data from one satellite only), the difference between GPS and UTC time (leap seconds or UTC offset) and information regarding any measurement errors caused by the ionosphere.
- Subframe 5 contains the almanac data on satellite numbers 1 to 24 (N.B. each subframe can transmit data from one satellite only). All 25 pages are transmitted together with information on the health of satellite numbers 1 to 24.

GPS: Estimating Position

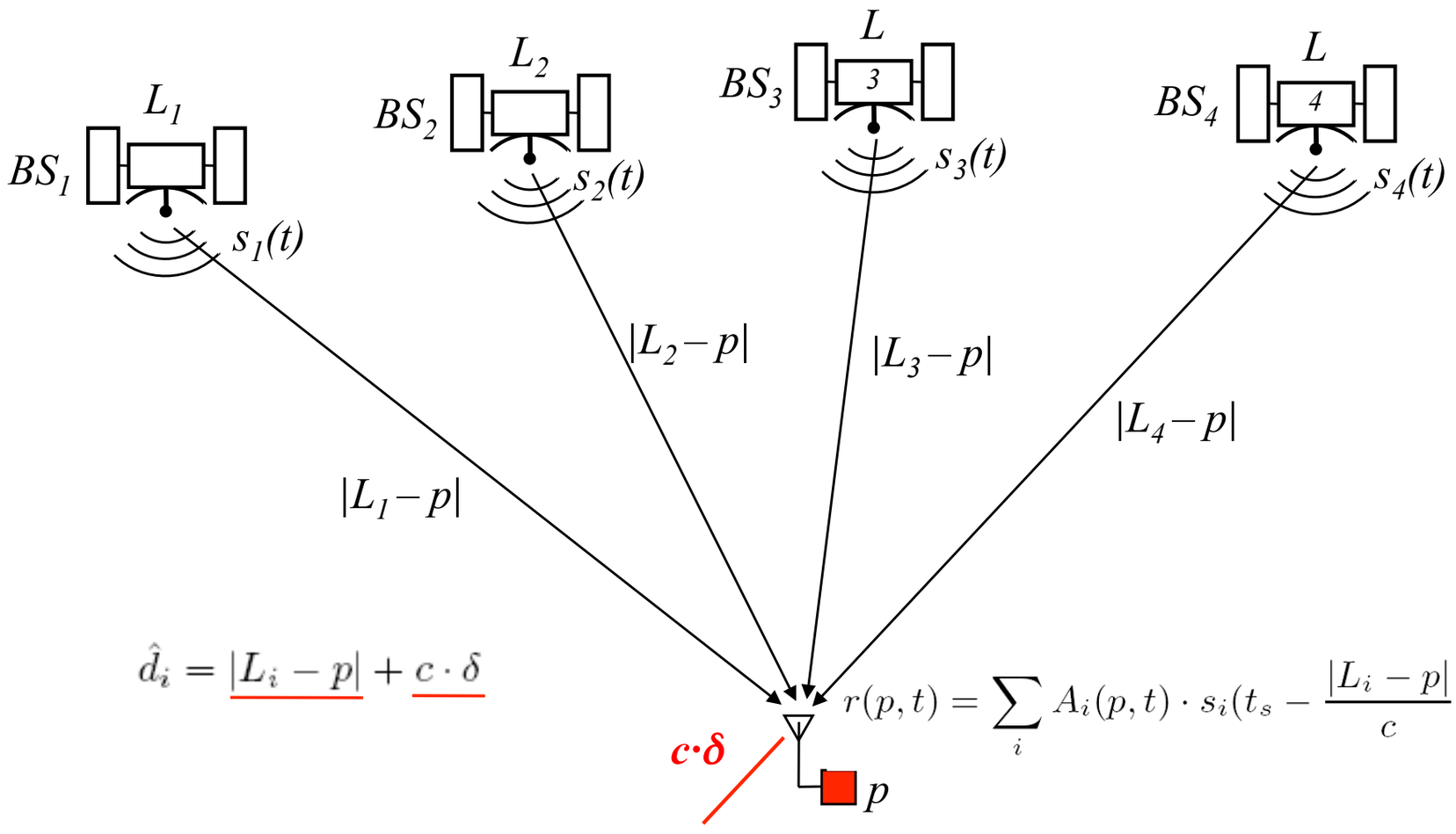


τ	Receiver clock error
$(x_{sati}, y_{sati}, z_{sati})$	Known satellite coordinates
(x, y, z)	User co-ordinates
Δt_i	Signal transit times

$$PSR_1 = \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y) + (z_{sat1} - z)^2} + c \cdot \tau$$
$$PSR_2 = \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y) + (z_{sat2} - z)^2} + c \cdot \tau$$
$$PSR_3 = \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y) + (z_{sat3} - z)^2} + c \cdot \tau$$
$$PSR_4 = \sqrt{(x_{sat4} - x)^2 + (y_{sat4} - y) + (z_{sat4} - z)^2} + c \cdot \tau$$

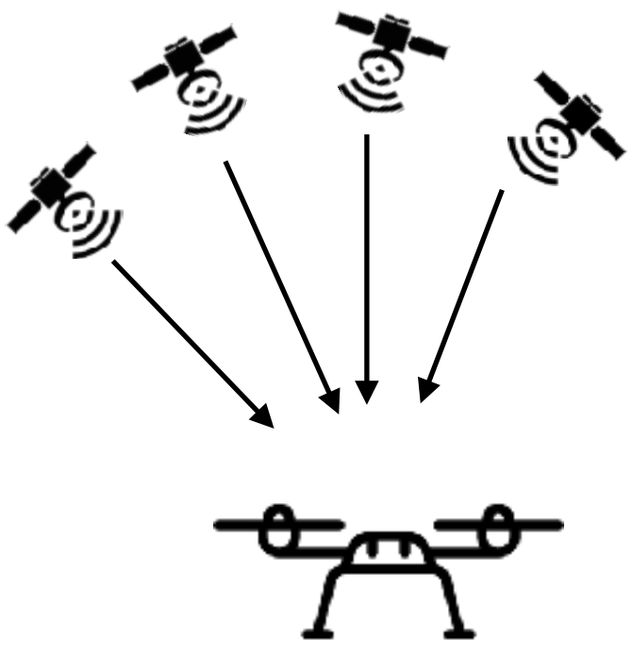
(x, y, z) is determined by solving the above equations using Taylor series linearization and simplification

GPS position calculation



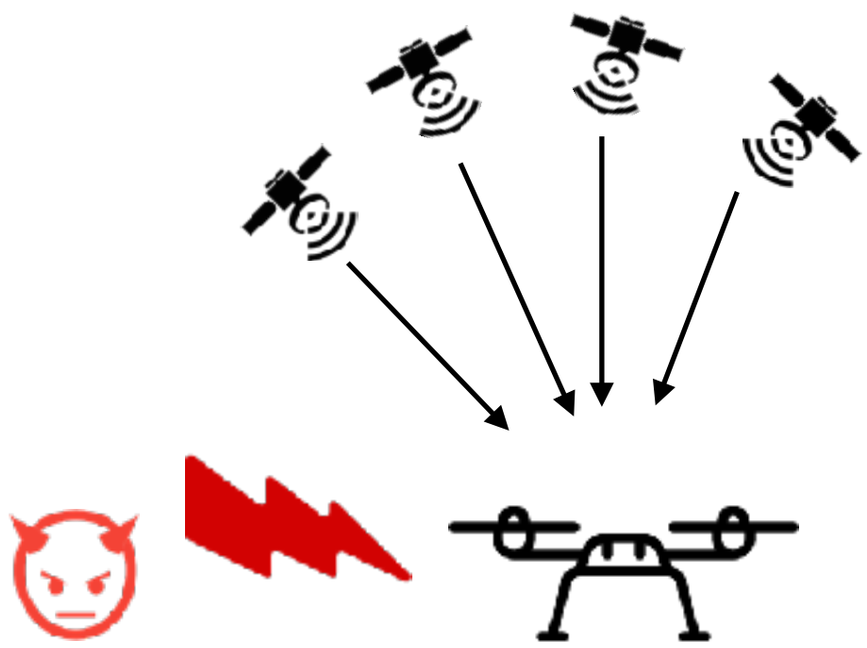
$$
\begin{aligned}
(t_r^1 - t_s) \cdot c &= |L_1 - p| + c \cdot \delta \\
(t_r^2 - t_s) \cdot c &= |L_2 - p| + c \cdot \delta \\
(t_r^3 - t_s) \cdot c &= |L_3 - p| + c \cdot \delta \\
(t_r^4 - t_s) \cdot c &= |L_4 - p| + c \cdot \delta
\end{aligned}
$$

GPS Signal Spoofing Attack



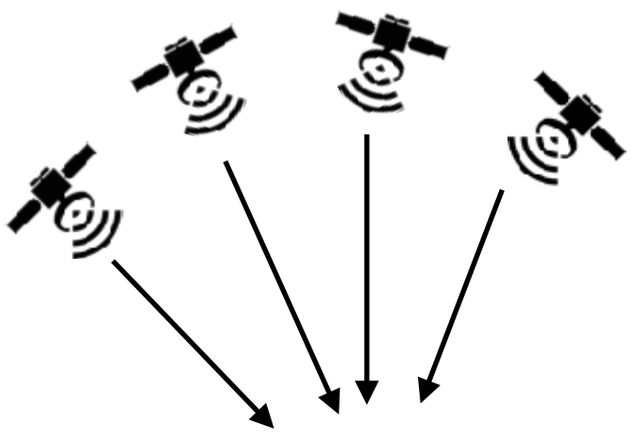
- Attacker transmits specially crafted signals identical to satellite signals but at higher power to overshadow legitimate satellite signals
    - either modify the navigation message contents or manipulate the time of arrival
- Receiver computes a false location based on the attacker's spoofing signals
- Increasing availability of commercial GPS signal generators and low-cost radio hardware.

GPS Signal Spoofing Attack



- Attacker transmits specially crafted signals identical to satellite signals but at higher power to overshadow legitimate satellite signals
    - either modify the navigation message contents or manipulate the time of arrival
- Receiver computes a false location based on the attacker's spoofing signals
- Increasing availability of commercial GPS signal generators and low-cost radio hardware.

GPS Signal Spoofing Attack

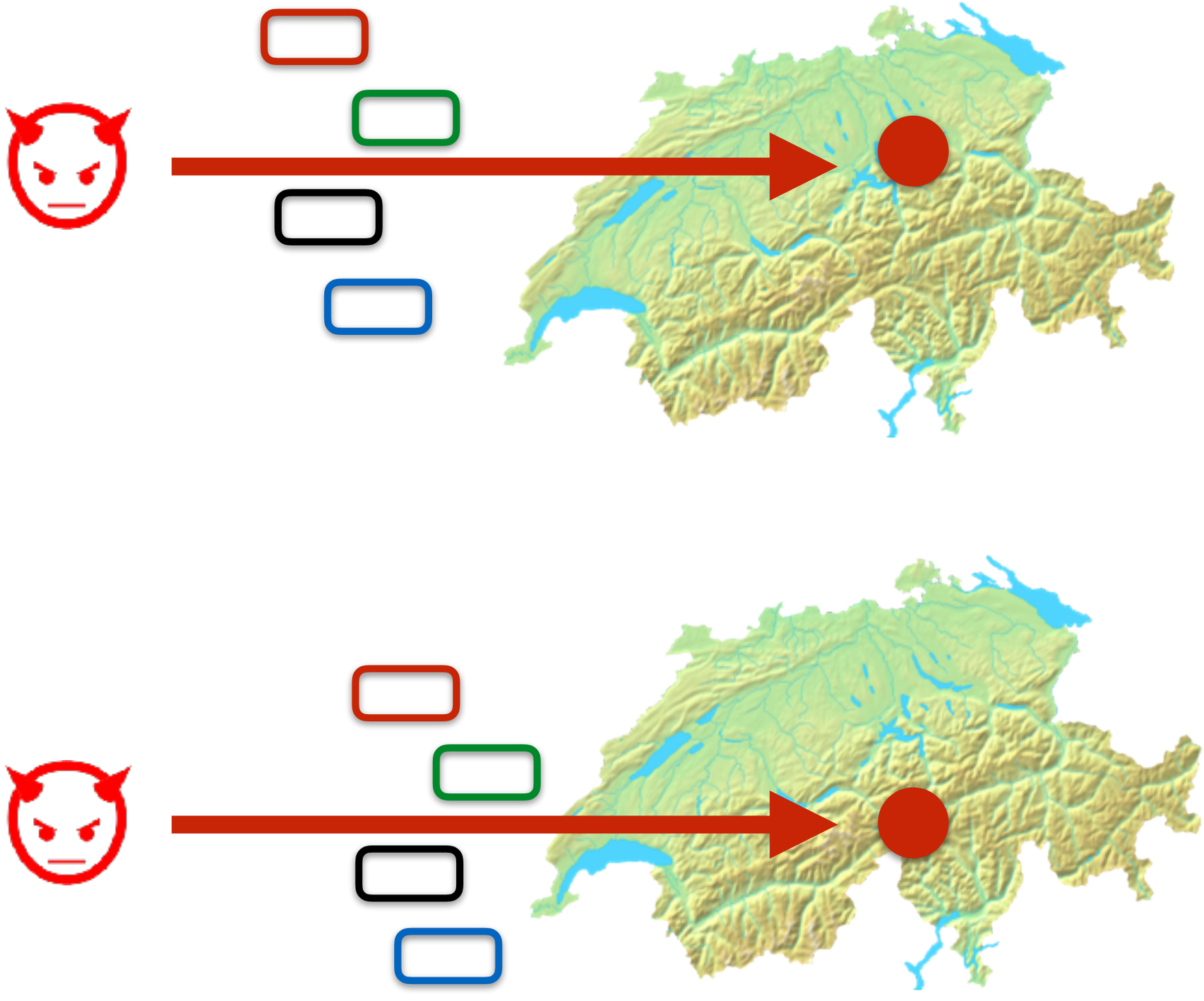


- Attacker transmits specially crafted signals identical to satellite signals but at higher power to overshadow legitimate satellite signals
  - either modify the navigation message contents or manipulate the time of arrival

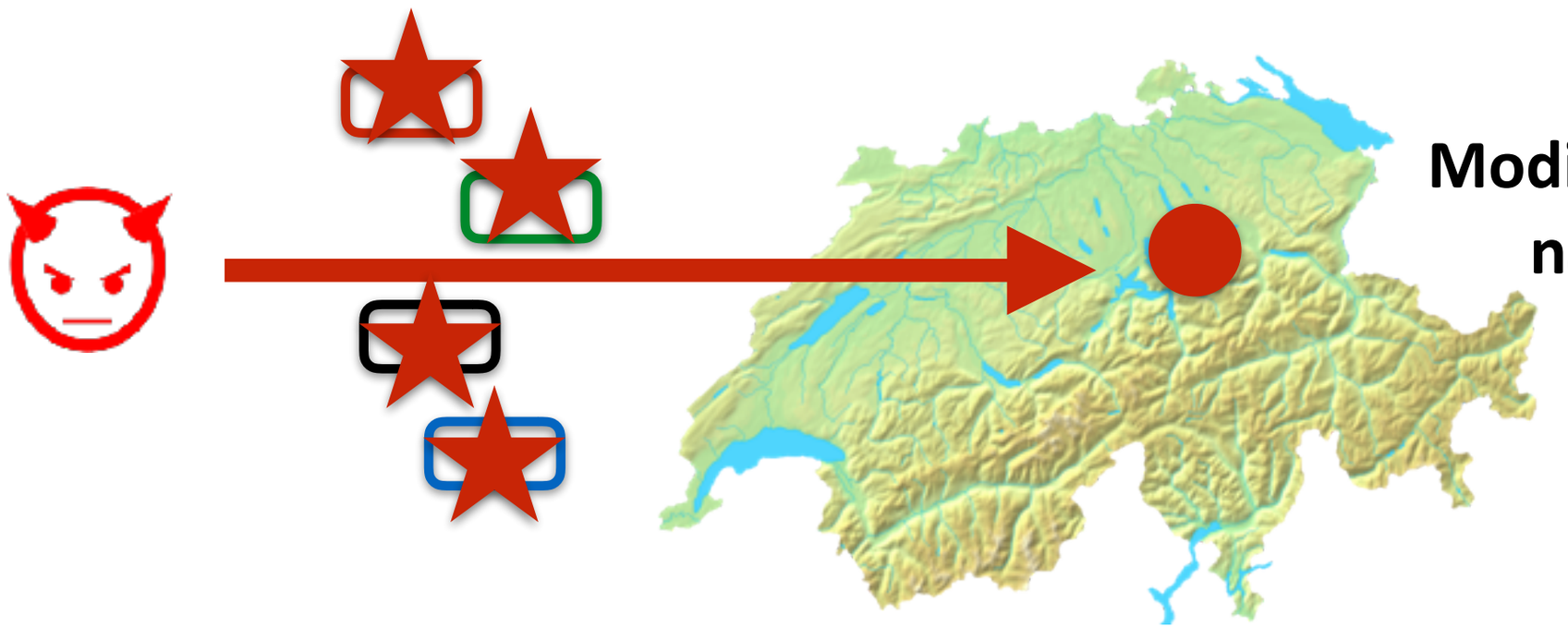
- Receiver computes a false location based on the attacker's spoofing signals

- Increasing availability of commercial GPS signal generators and low-cost radio hardware.

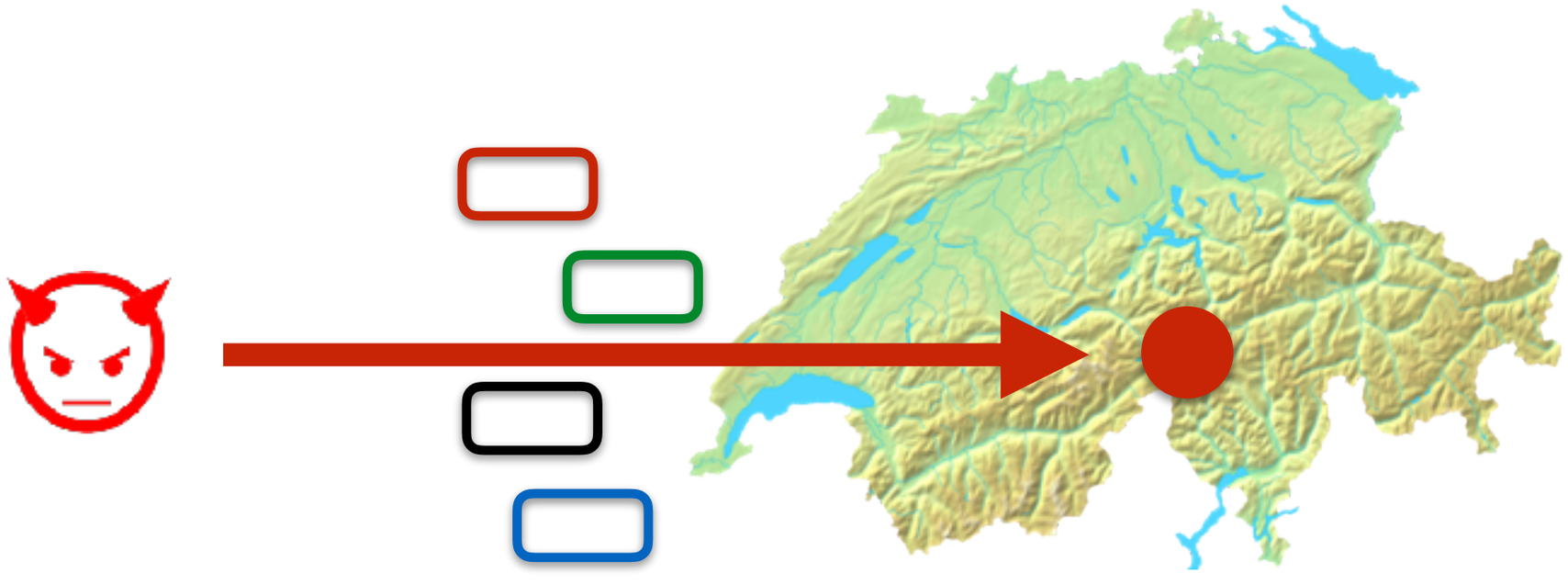
GPS spoofing attacks



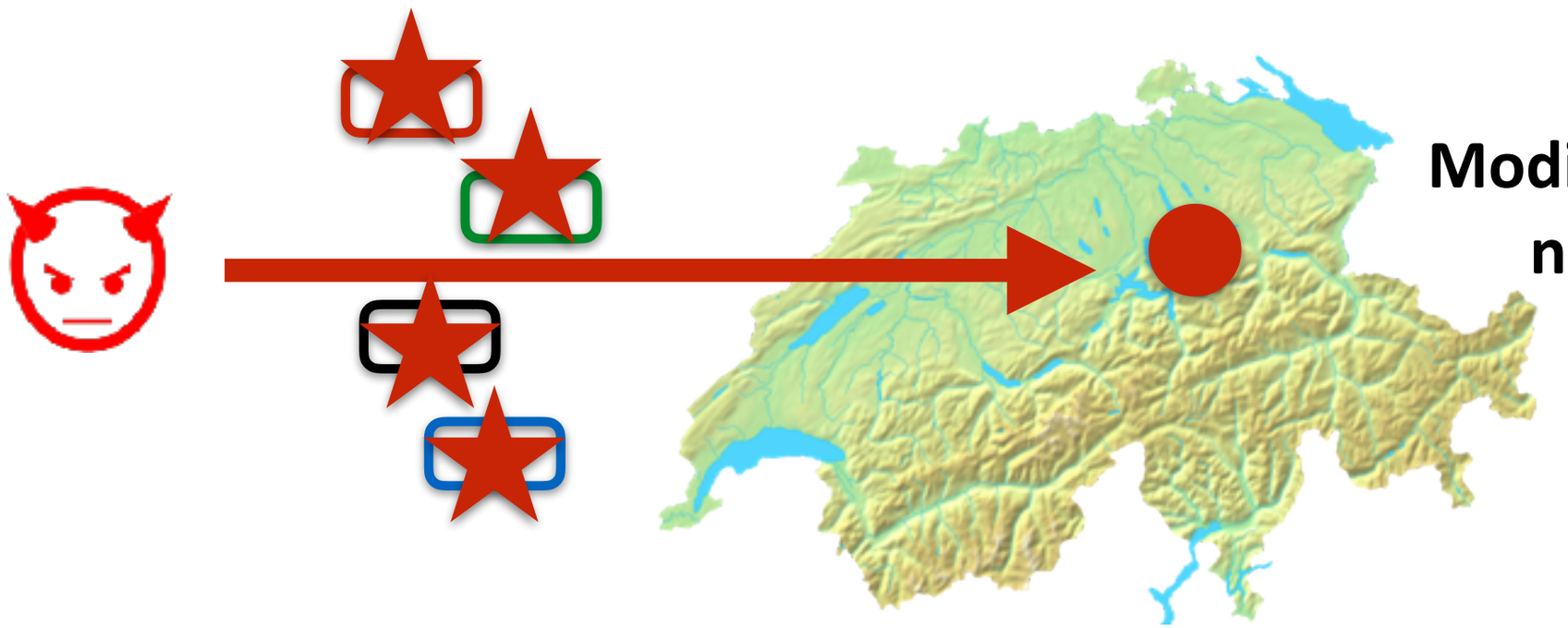
GPS spoofing attacks



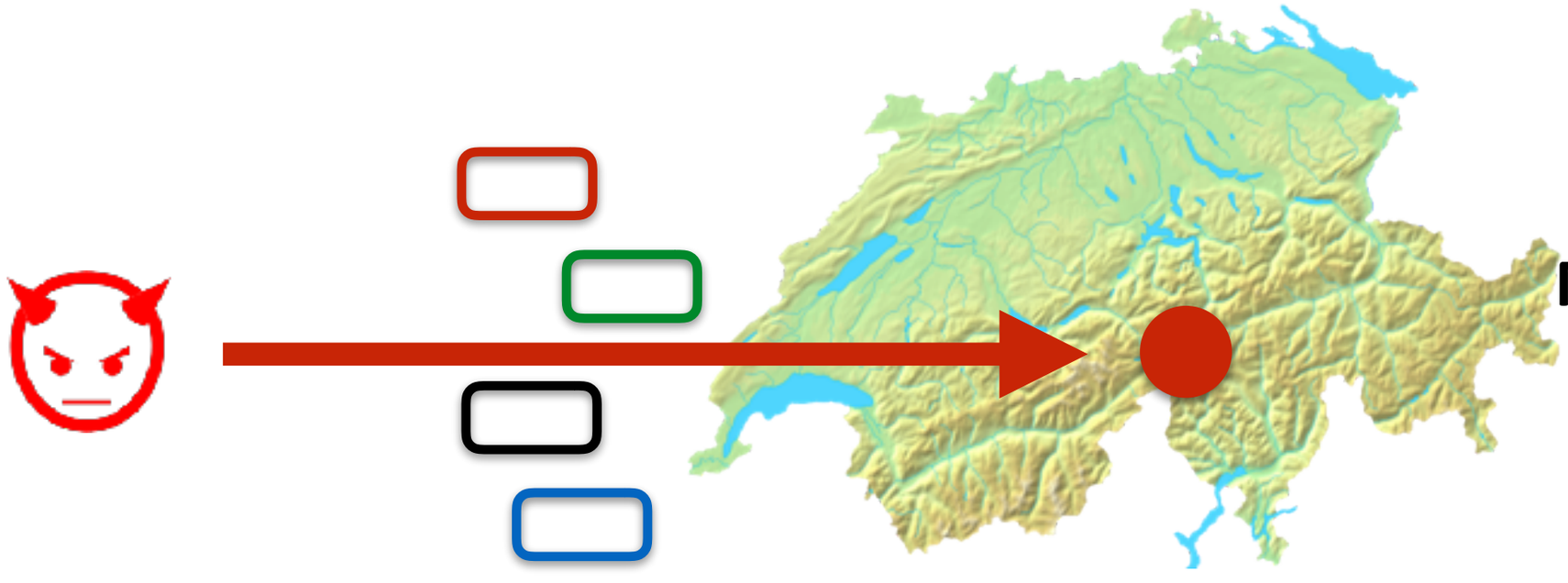
Modify the contents of the navigation message



GPS spoofing attacks

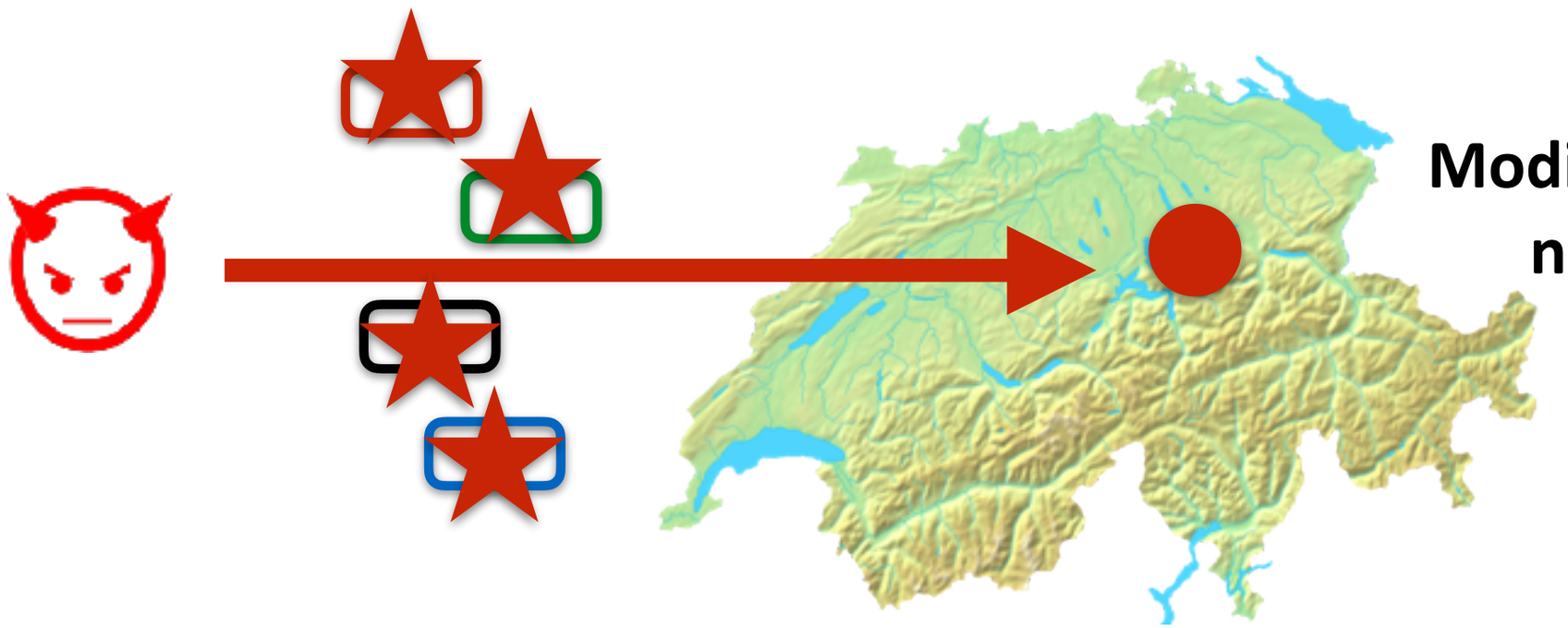


Modify the contents of the navigation message

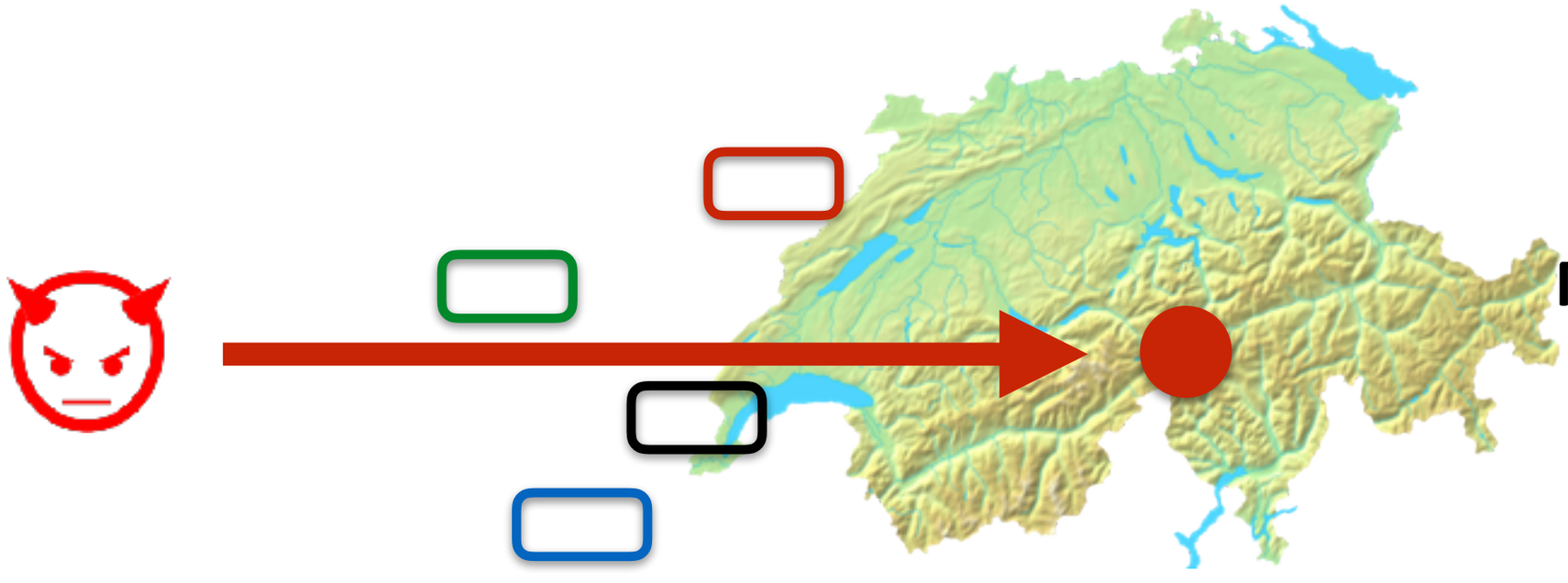


Modify the arrival time

GPS spoofing attacks

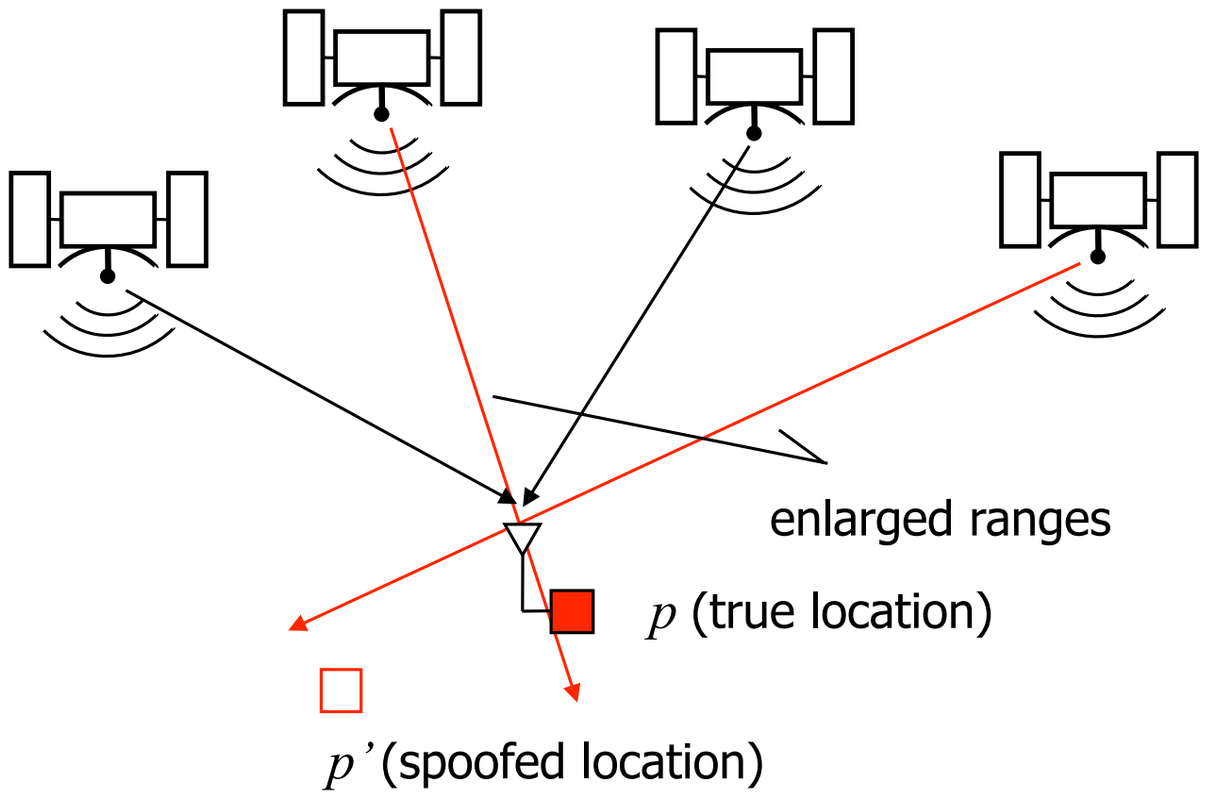


Modify the contents of the navigation message



Modify the arrival time

GPS spoofing



Attacker either modifies the navigation message contents or manipulates the time of arrival

Civilian GPS are not authenticated and can be generated OR delayed
Military GPS signals can only be delayed

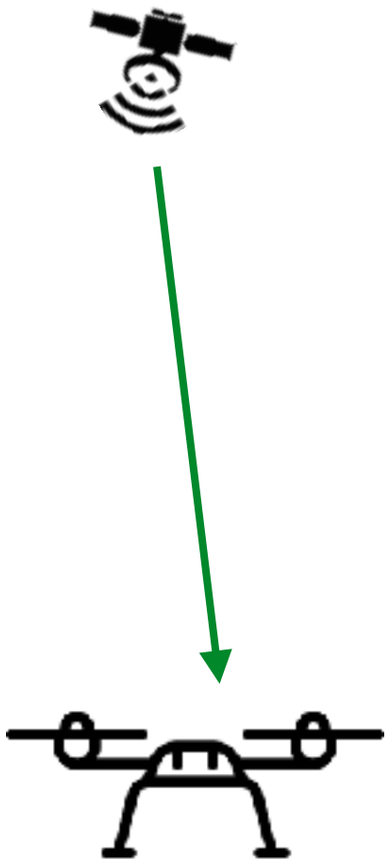
Detection and Mitigation of GPS Spoofing

- Infrastructure modifications (e.g., cryptographic)
- Receiver end modifications

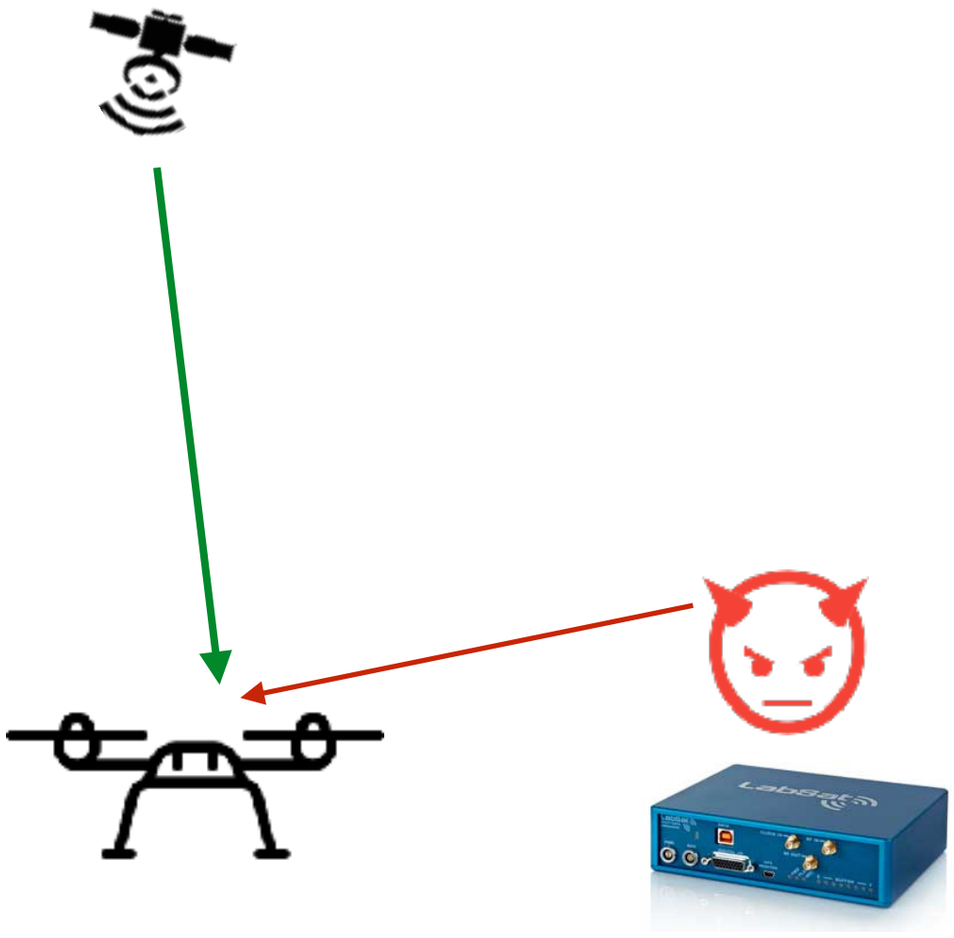
Countermeasures

- Adding cryptographic authentication to the navigation messages
- Non-Cryptographic countermeasures
    - Spatial characteristics of the received signal (e.g., direction of arrival, carrier phase measurements)
    - Other physical-layer characteristics of the received GPS signals (e.g., received signal strength, AGC)
    - Additional sensors or receivers to validate the estimated position, velocity and time.

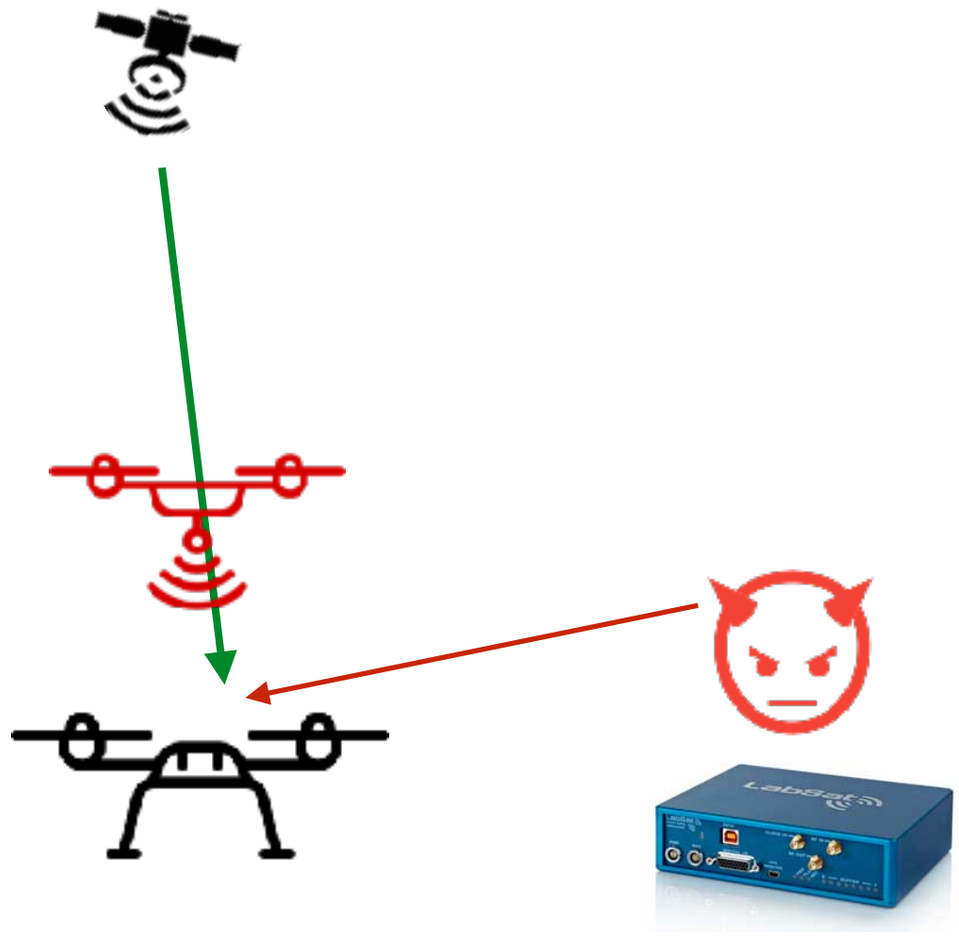
Angle of arrival



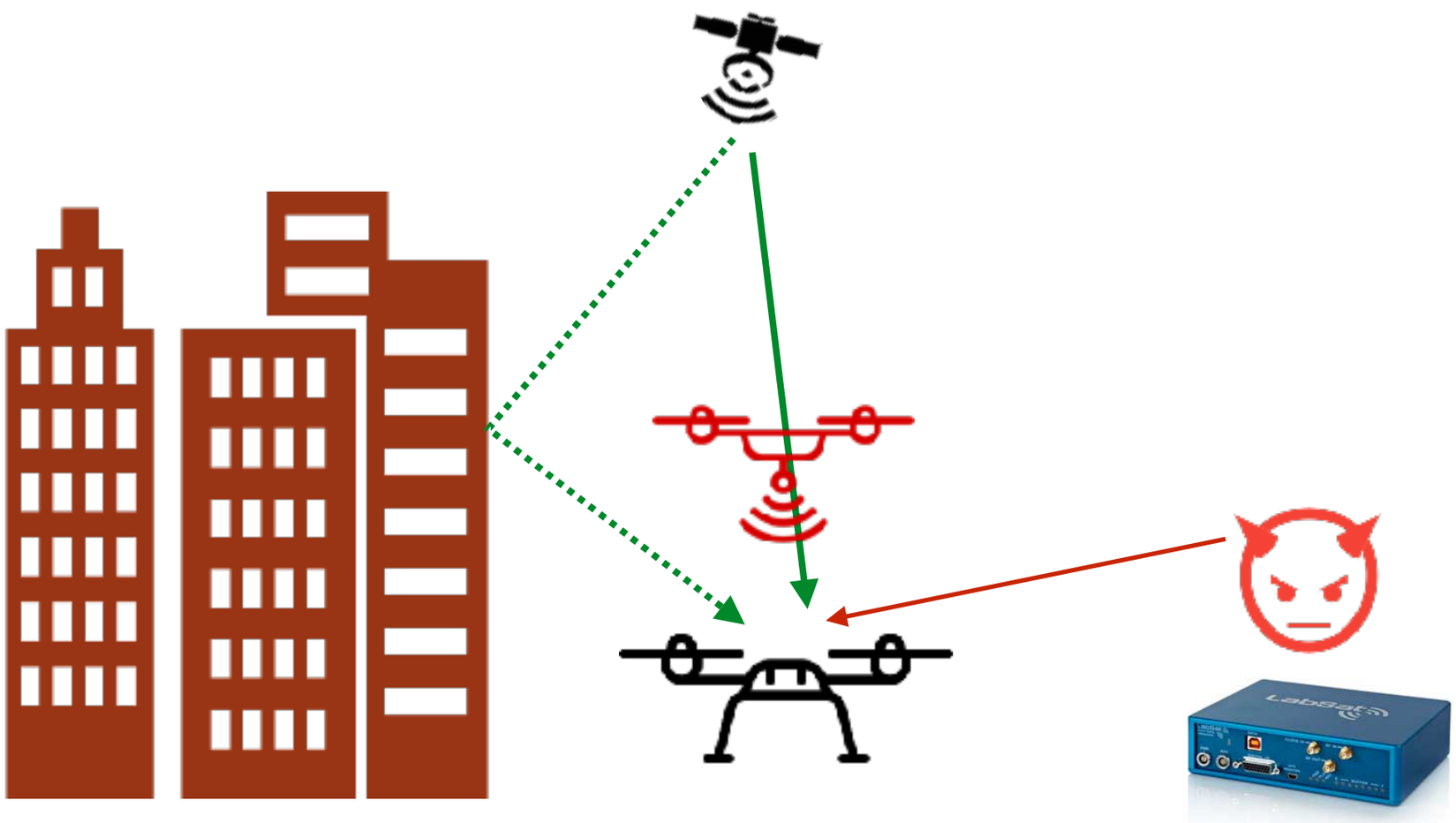
Angle of arrival



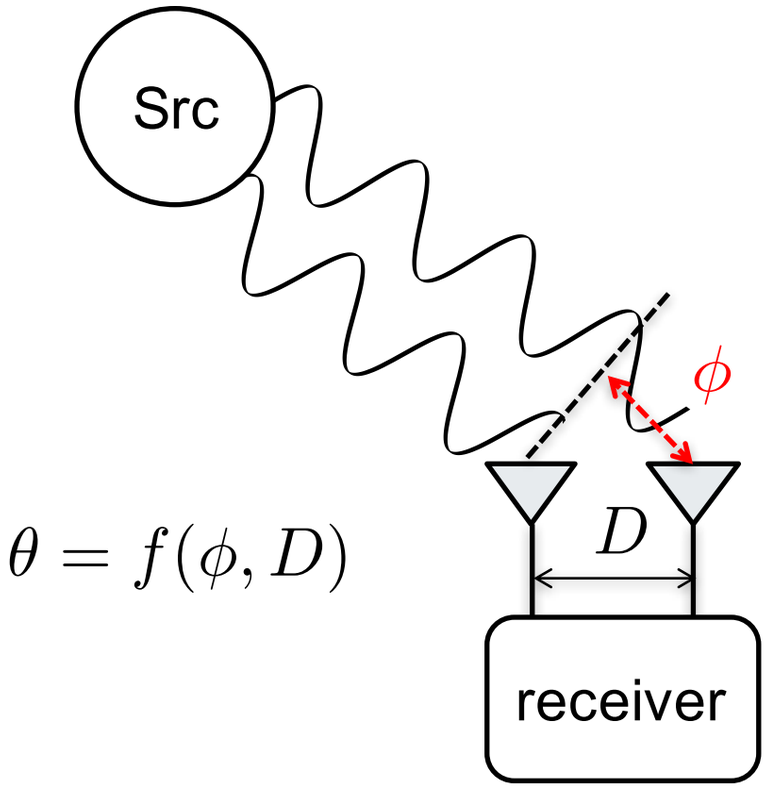
Angle of arrival



Angle of arrival

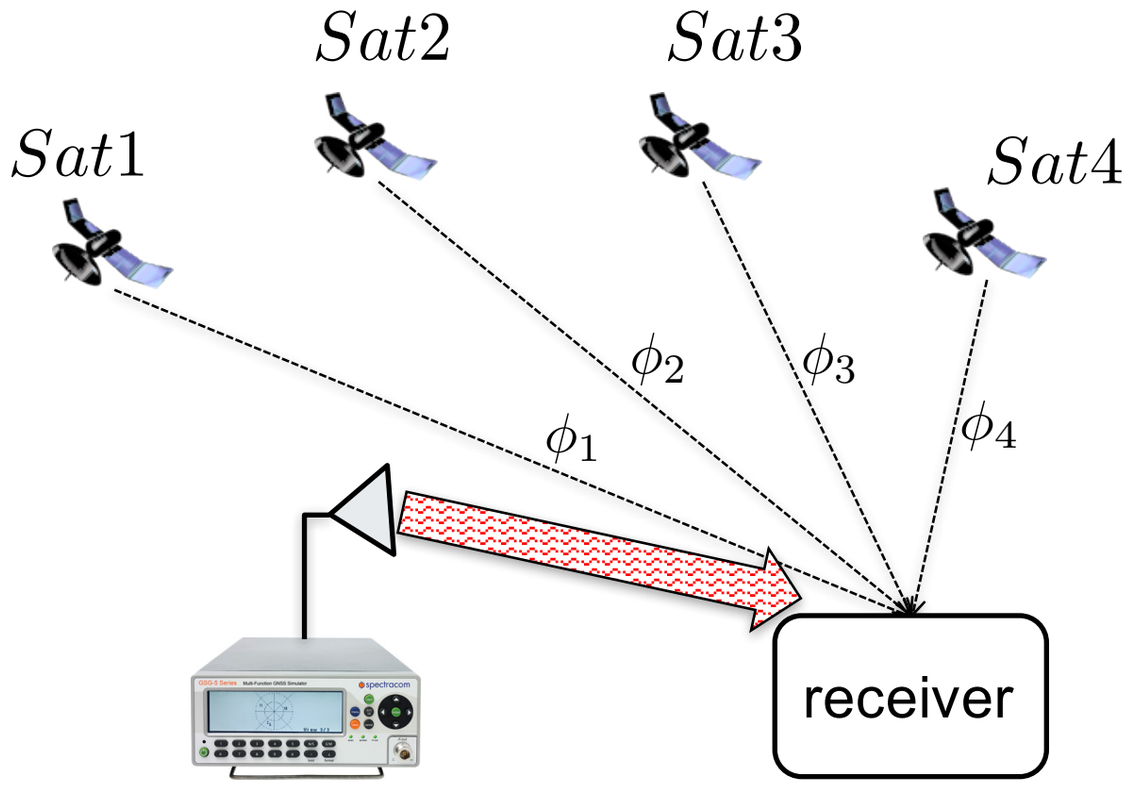


Angle of Arrival based Spoofing Detection



$\theta = f(\phi, D)$

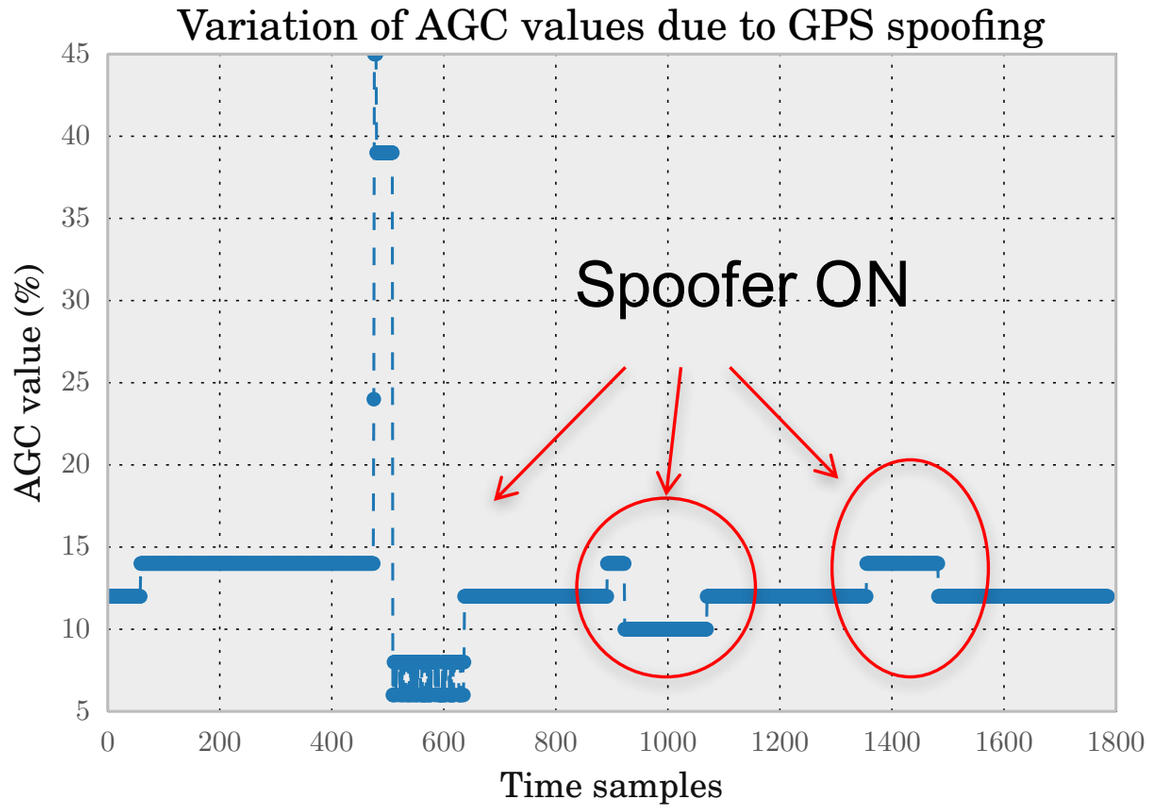
Angle of arrival is a function of the measured signal phase difference (Φ) at both the antennas and their separation D.



Spoofed scenario: $\phi_1 \sim \phi_2 \sim \phi_3 \sim \phi_4$

Phase measurement is computationally expensive and requires receiver hardware modifications.

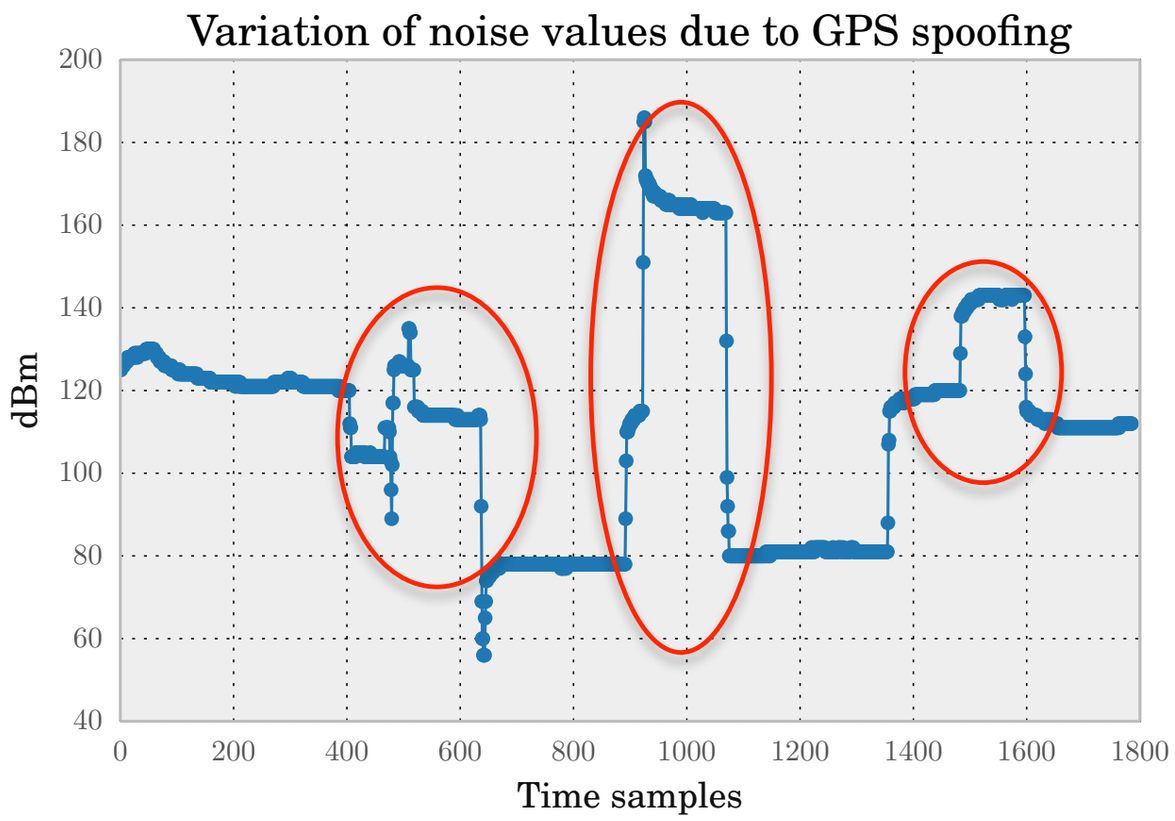
Monitoring Signal Characteristics

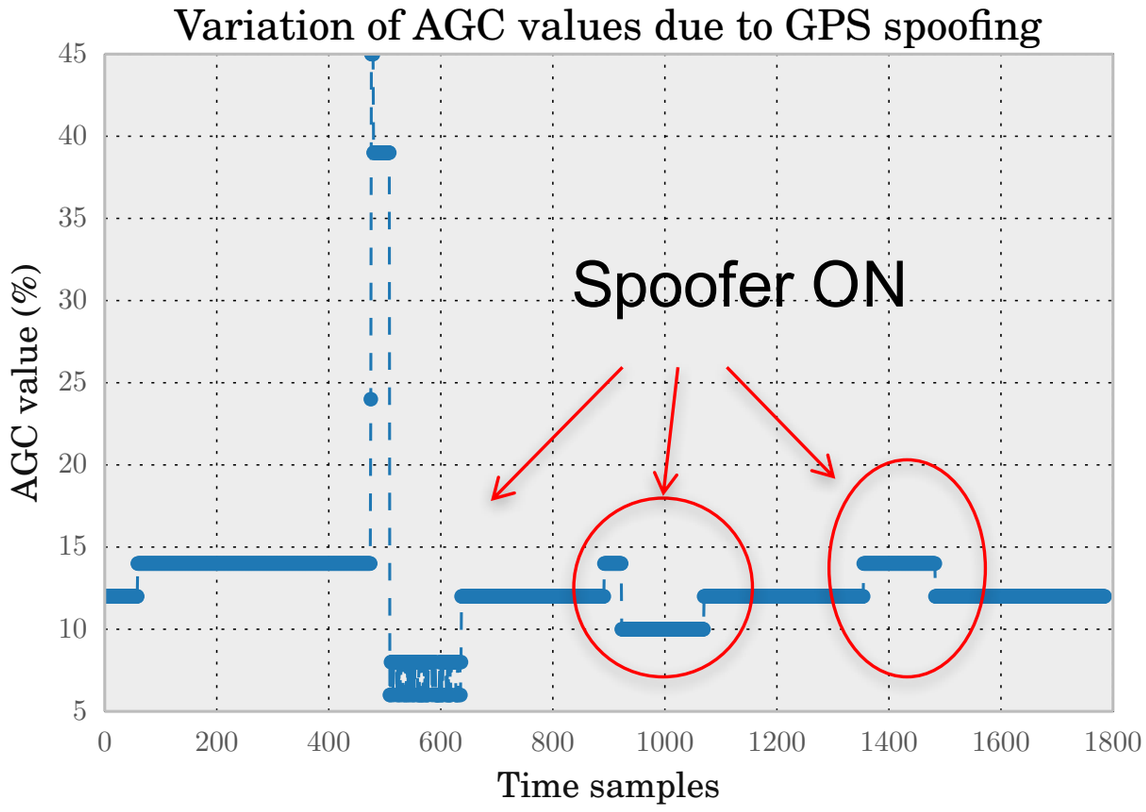


Monitoring Signal Characteristics

Spoofing Detection without changes to GPS

- Monitor AGC, Noise level, # of satellites
- Autocorrelation Peak Distortion
- Spatial Diversity (AoA, …)



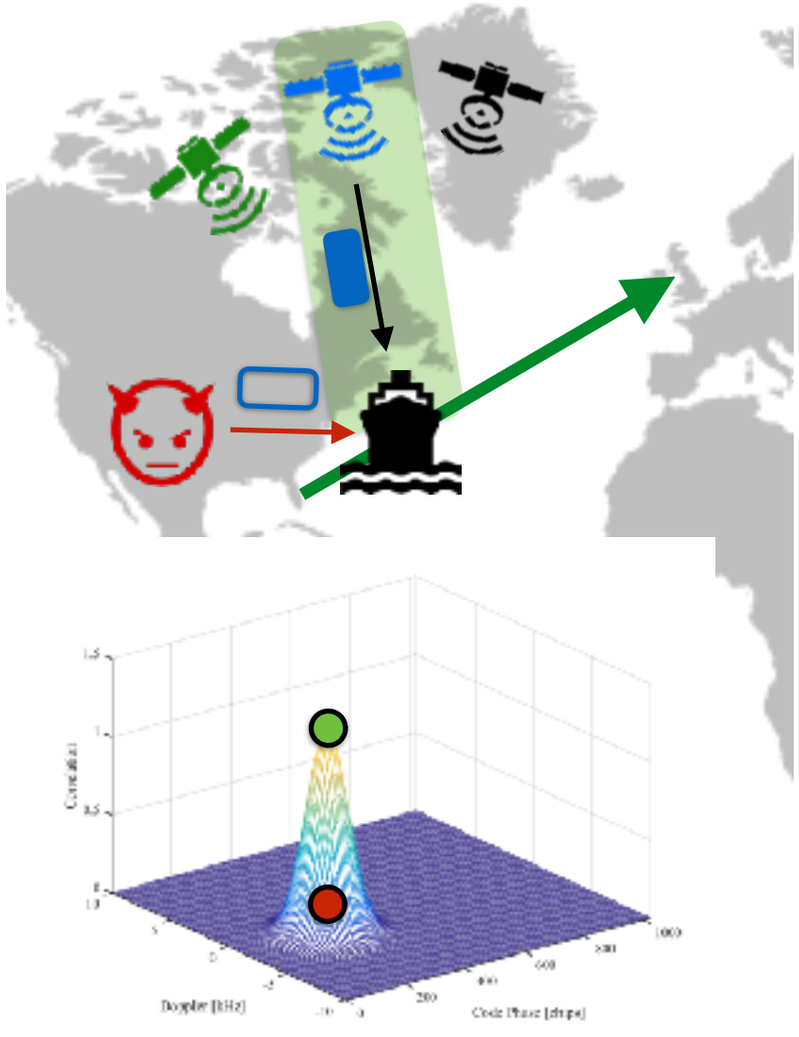


SPREE: Auxiliary Peak Tracking

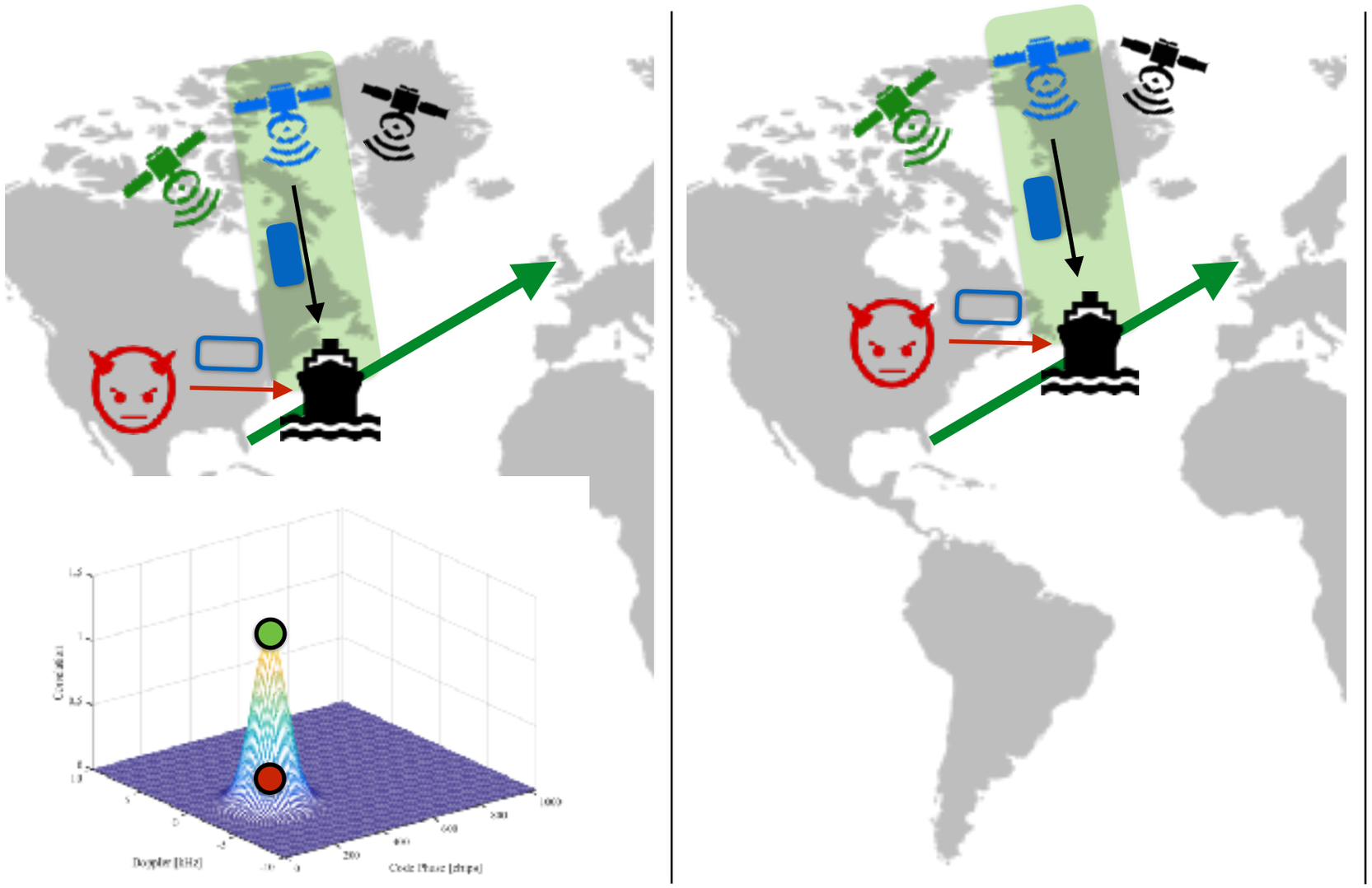
SPREE: Auxiliary Peak Tracking

SPREE: Auxiliary Peak Tracking

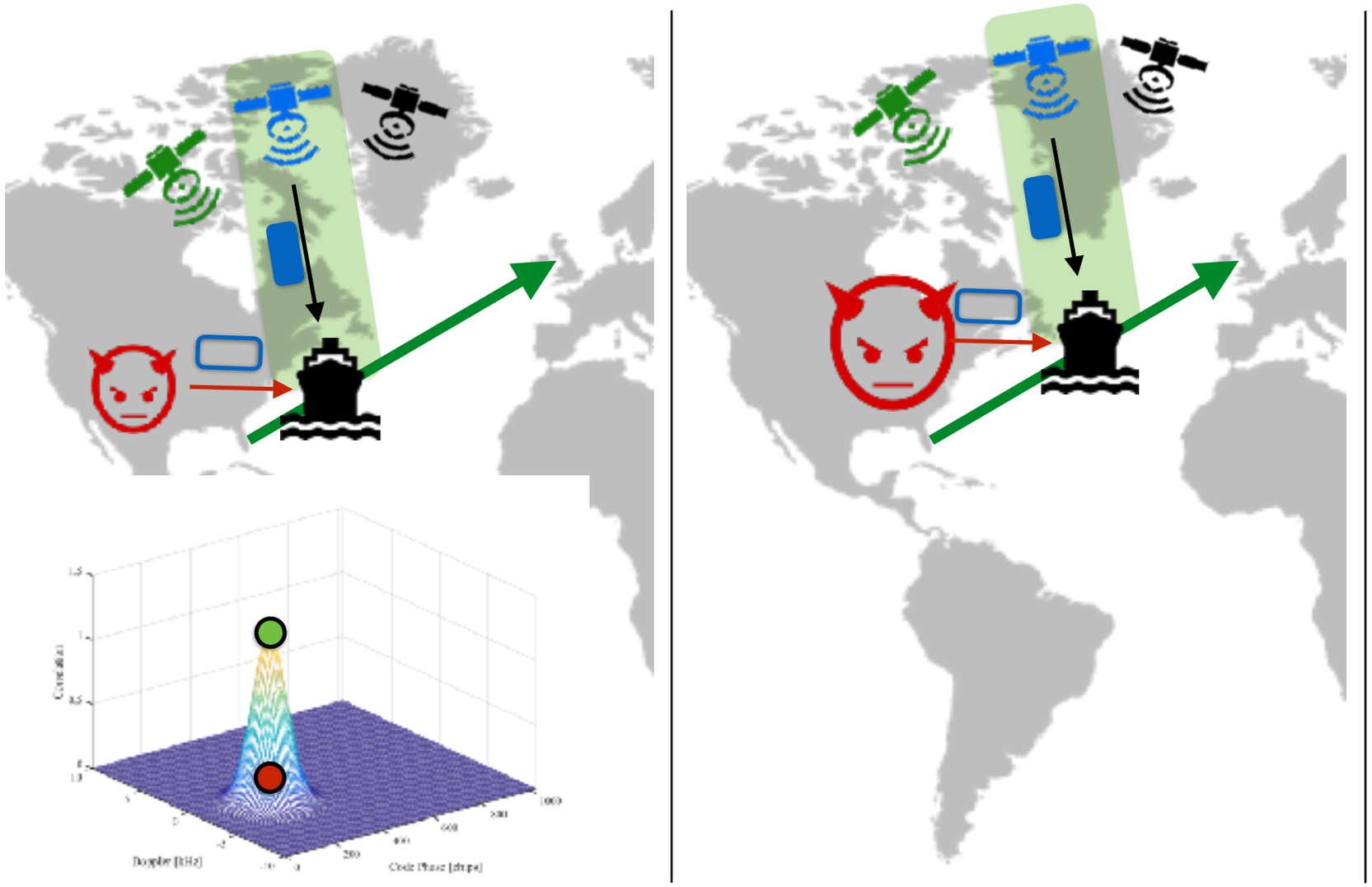
SPREE: Auxiliary Peak Tracking



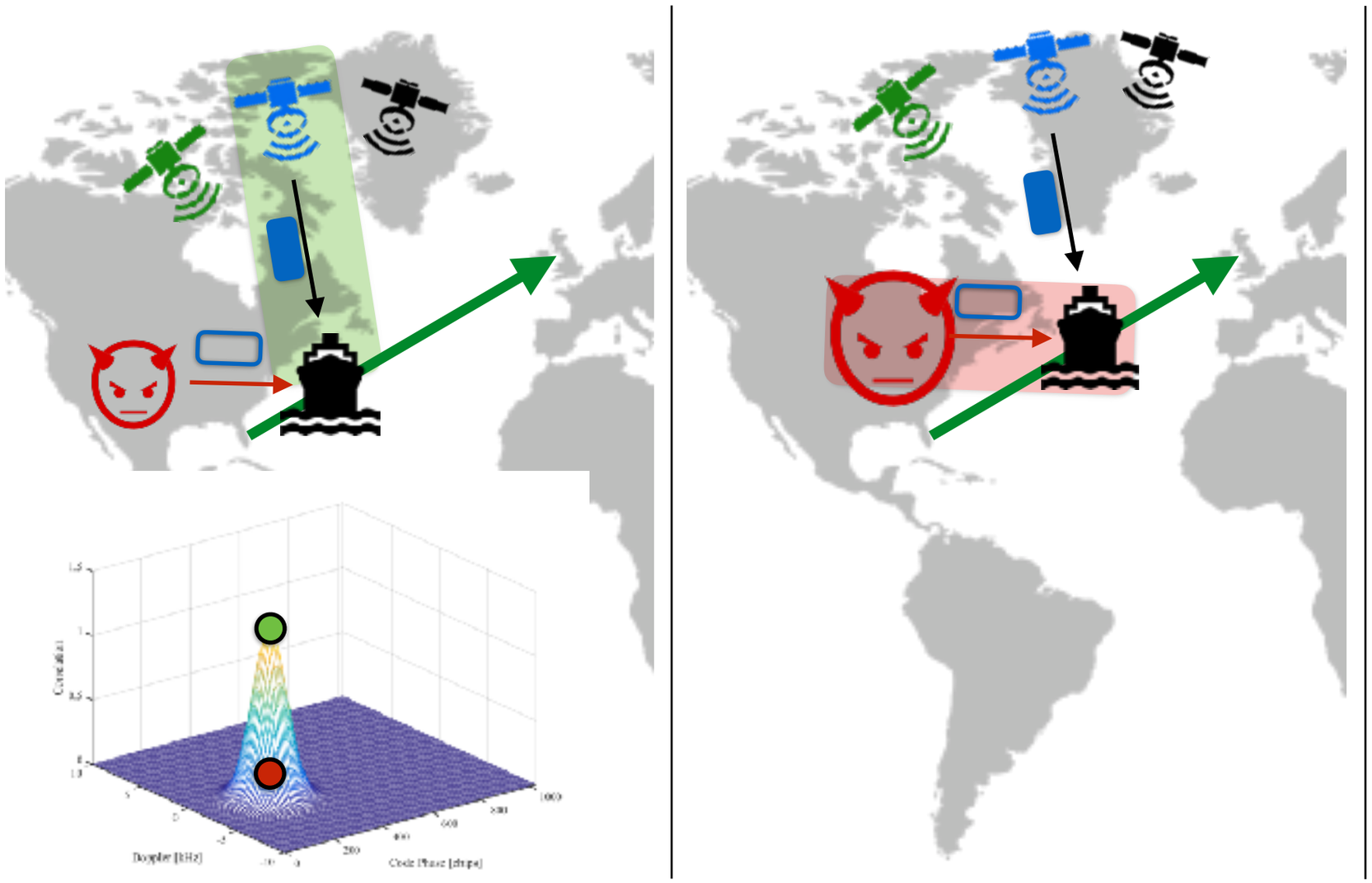
SPREE: Auxiliary Peak Tracking



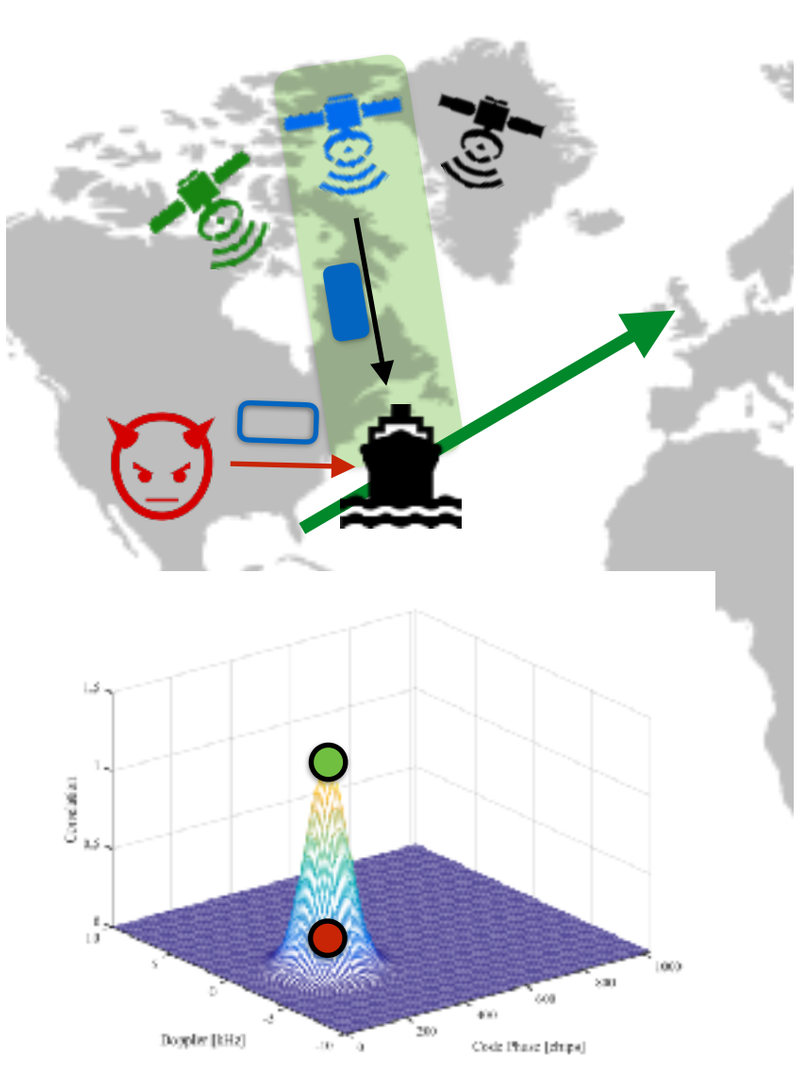
SPREE: Auxiliary Peak Tracking

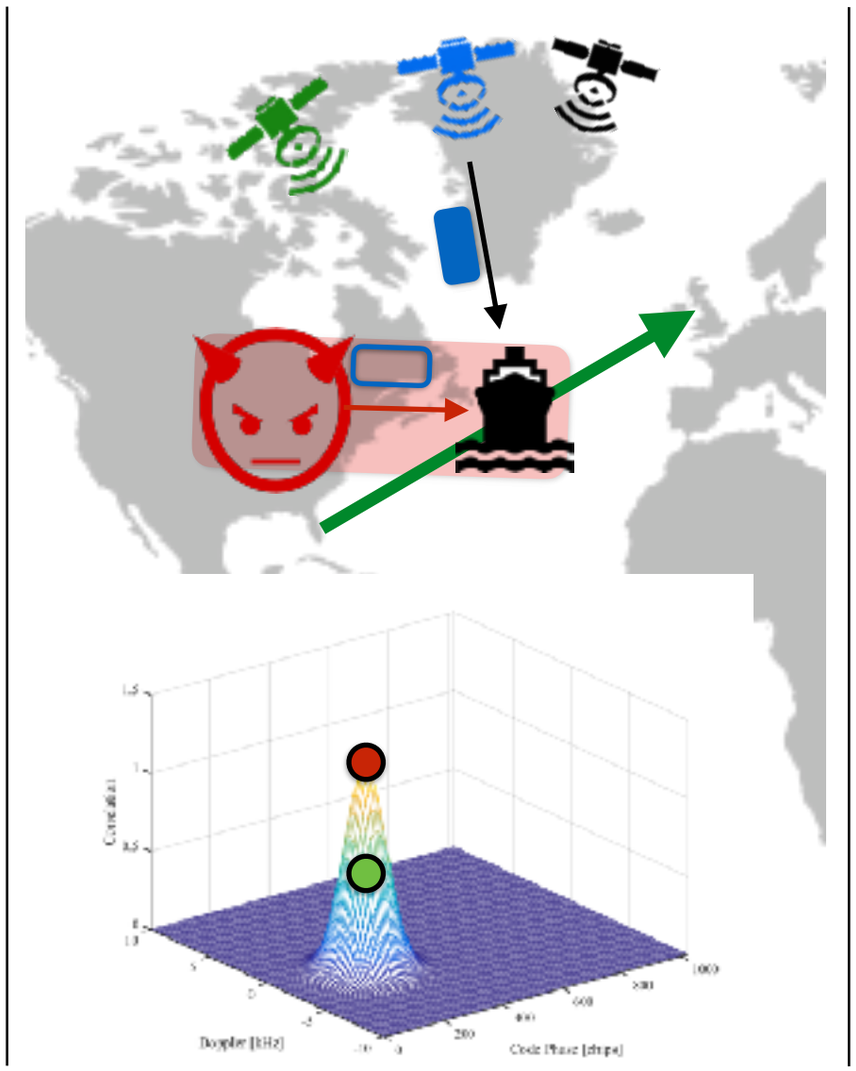


SPREE: Auxiliary Peak Tracking

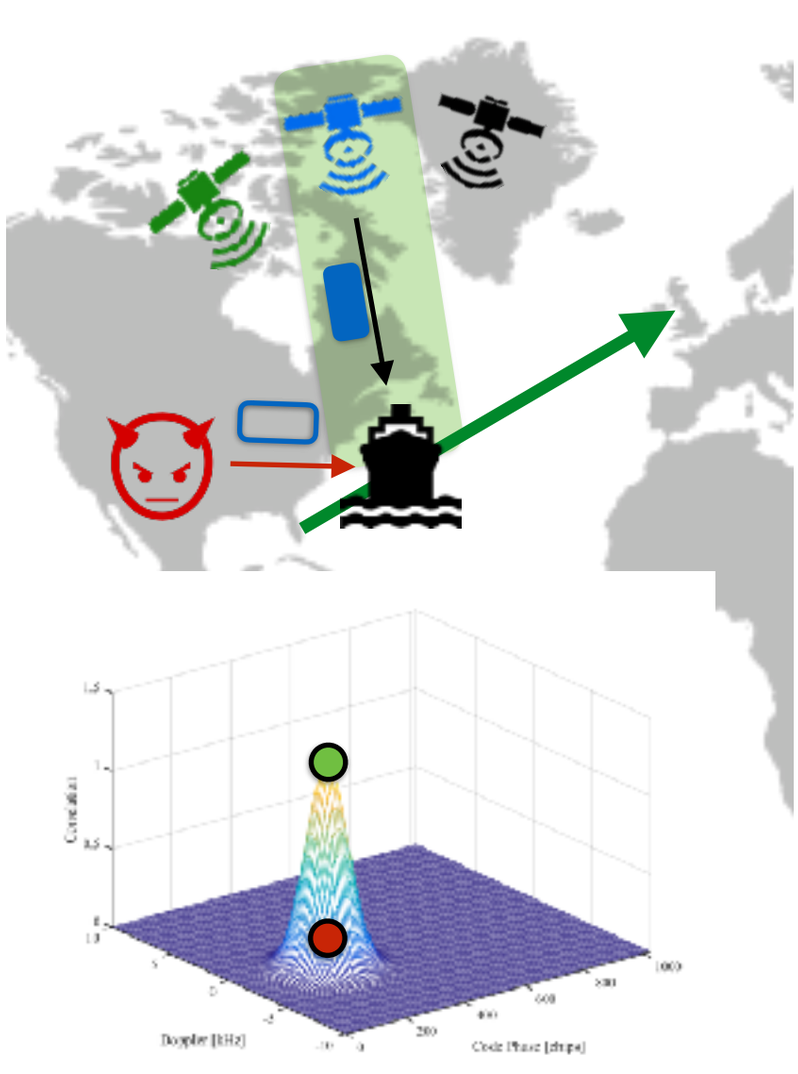


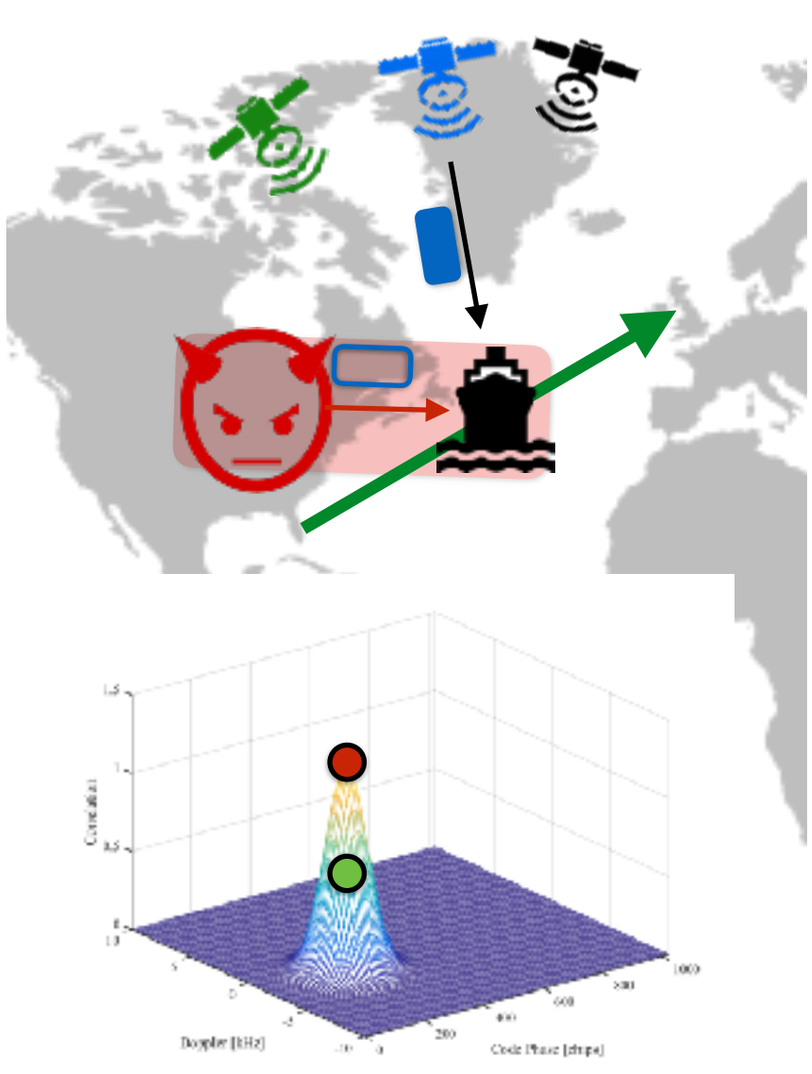
SPREE: Auxiliary Peak Tracking

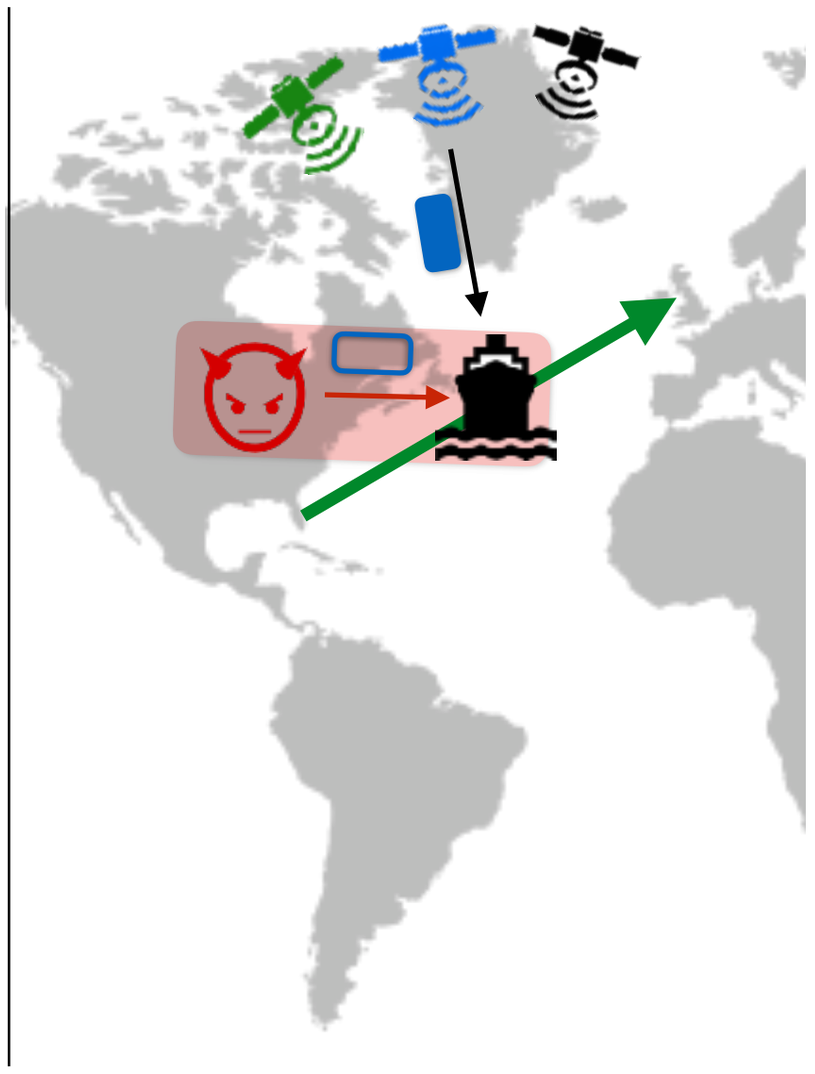




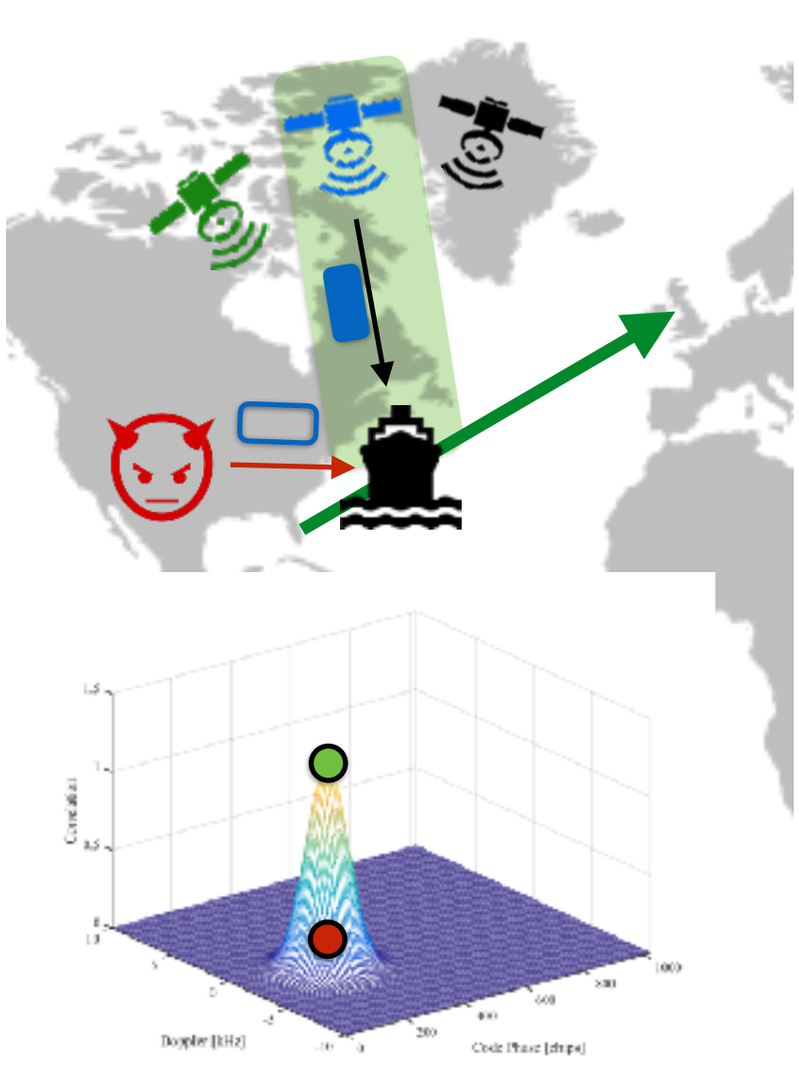
SPREE: Auxiliary Peak Tracking

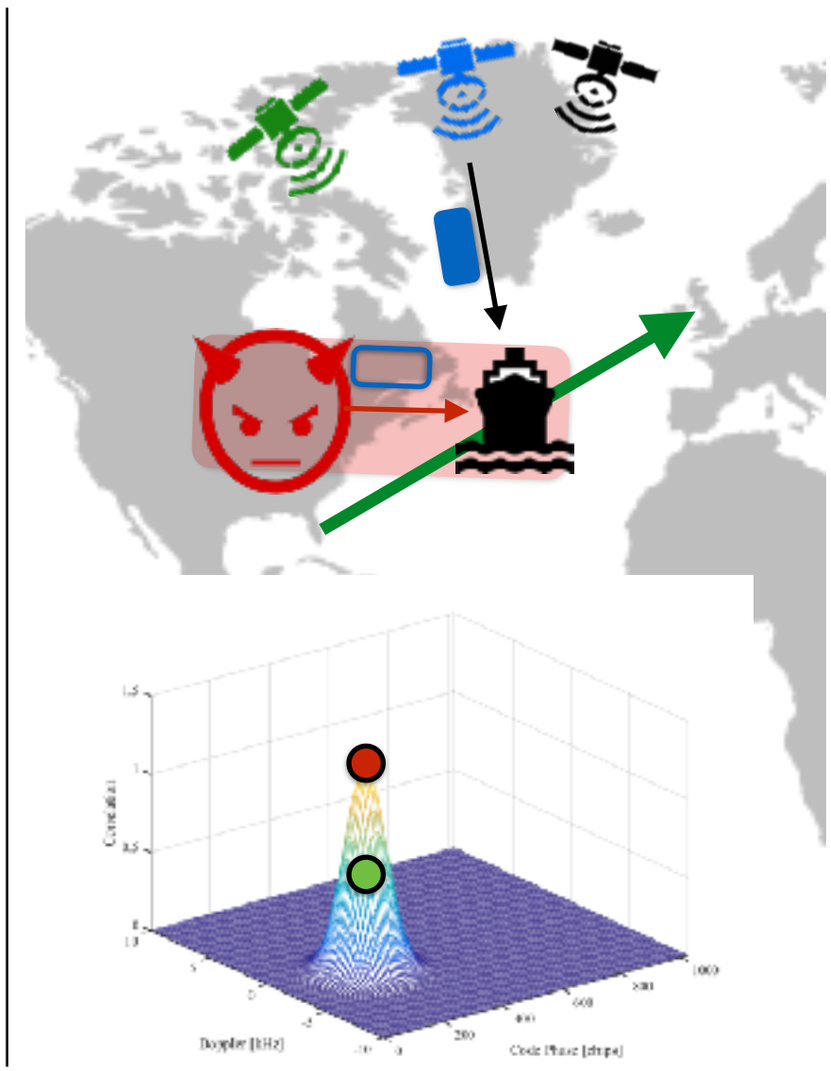


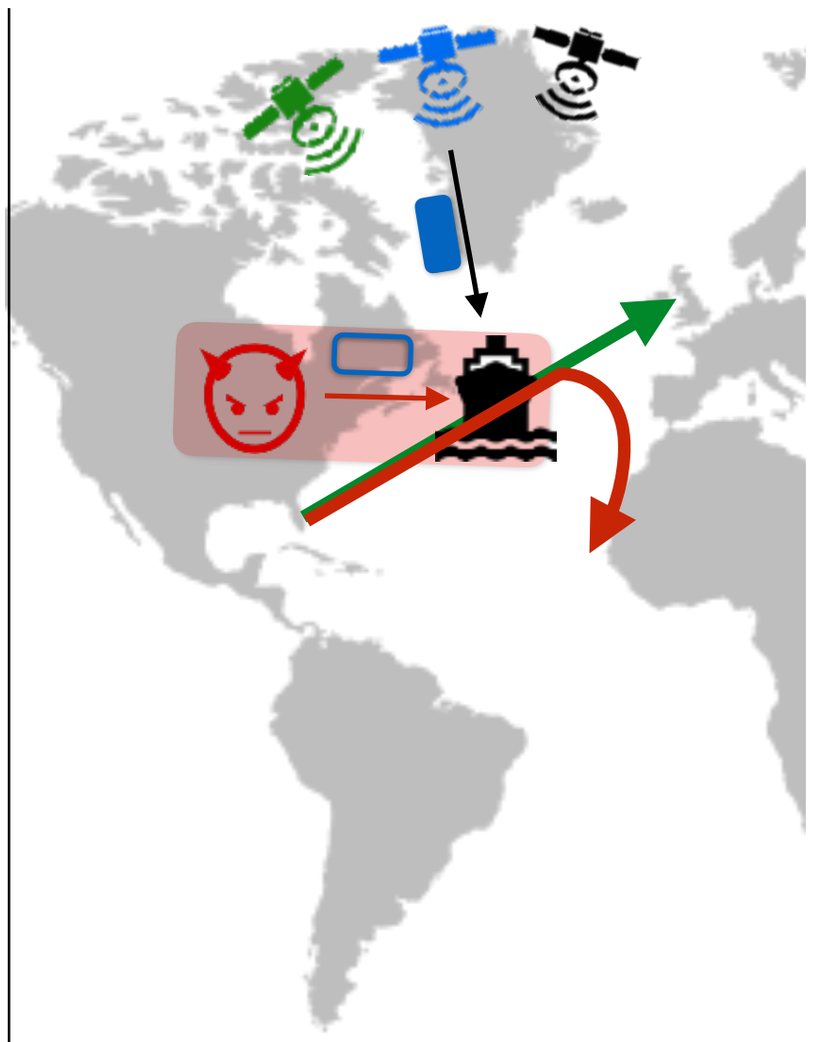




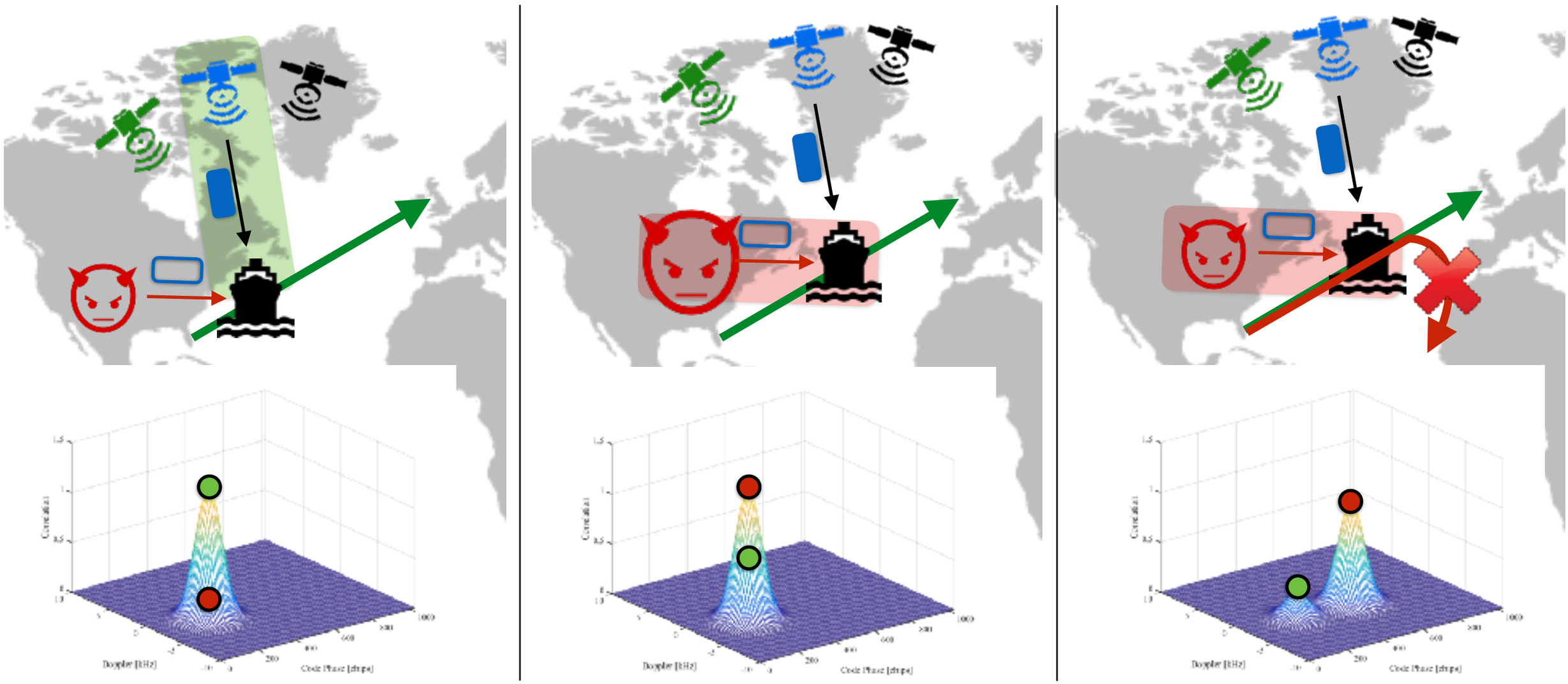
SPREE: Auxiliary Peak Tracking







SPREE: Auxiliary Peak Tracking



Detecting Spoofing With a Single Receiver?

- SPoofing REsistant GPS rEceiver (SPREE), the first GPS receiver capable of detecting *(up to an accuracy)* all known spoofing attacks.
- A novel auxiliary peak tracking technique enables detection of a seamless takeover attacks *(tracks all peaks …)*

Auxiliary Peak Tracking

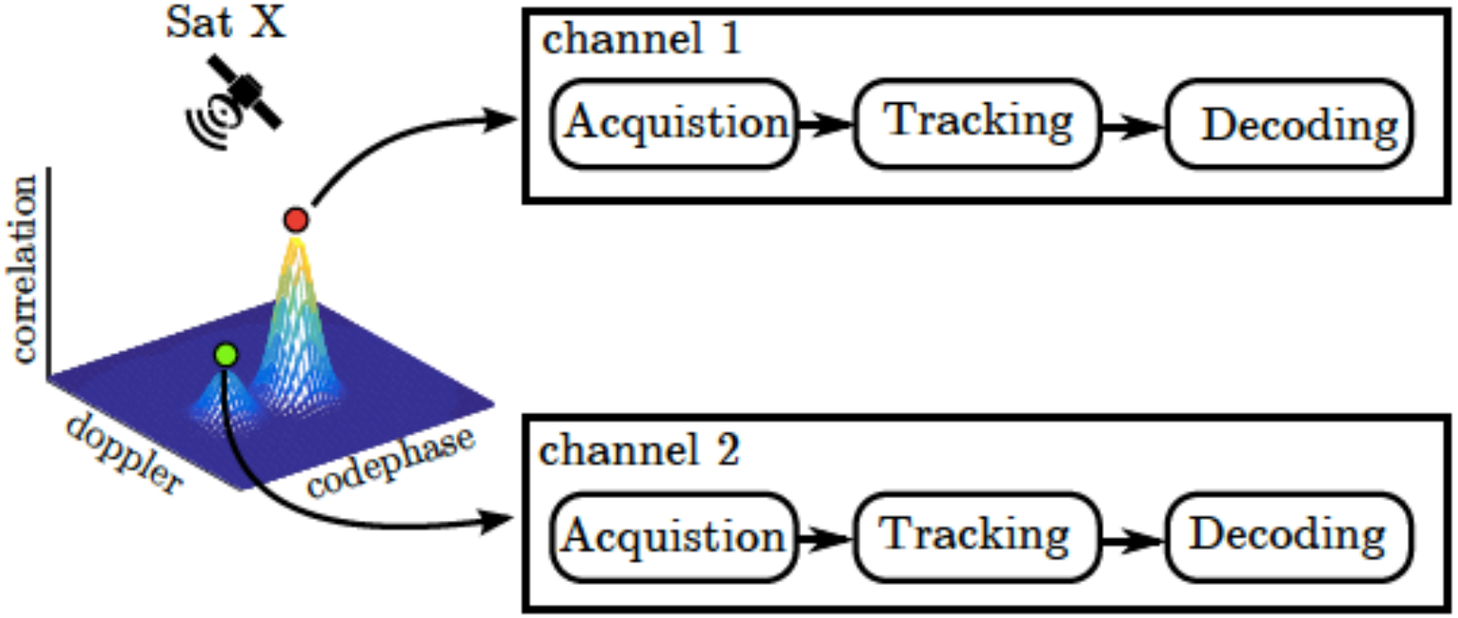
Acquires and tracks multiple acquisition peaks for the same satellite

Navigation Message Inspector

Checks consistency and sanity of decoded navigation message contents

Detecting Spoofing With a Single Receiver?

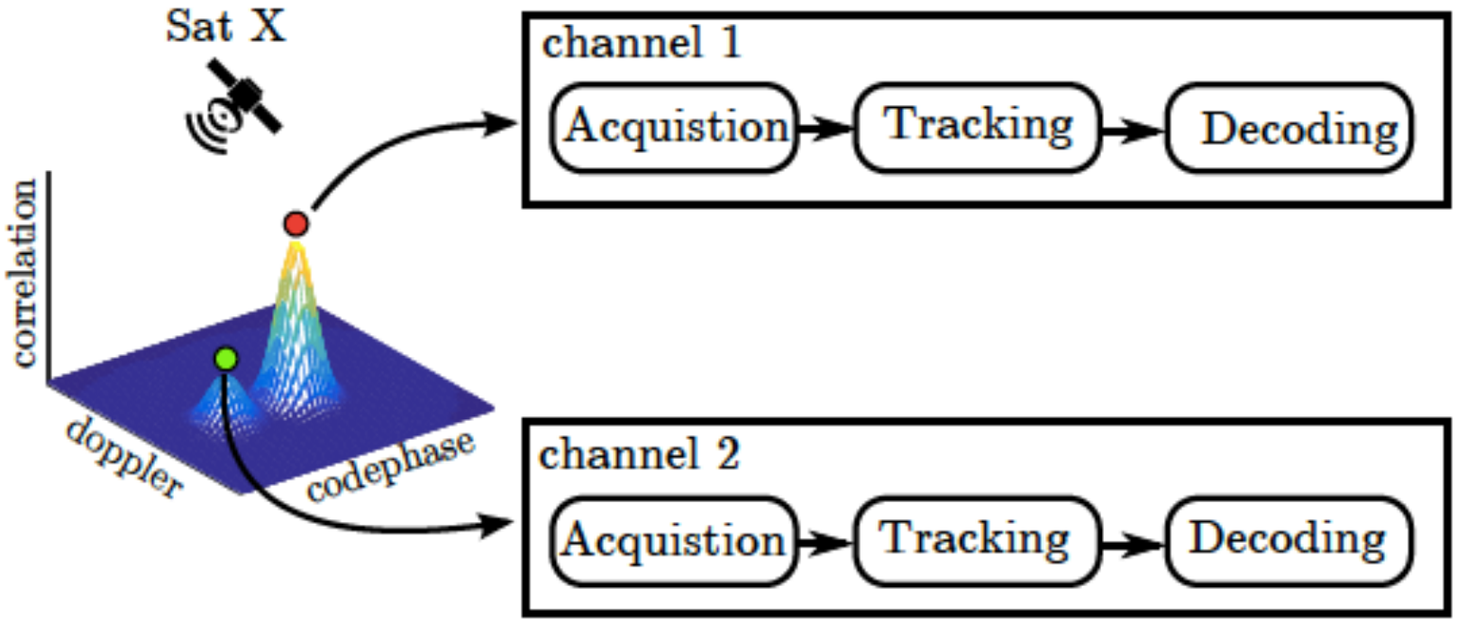
- SPoofing REsistant GPS rEceiver (SPREE), the first GPS receiver capable of detecting *(up to an accuracy)* all known spoofing attacks.
- A novel auxiliary peak tracking technique enables detection of a seamless takeover attacks *(tracks all peaks …)*



Detecting Spoofing With a Single Receiver?

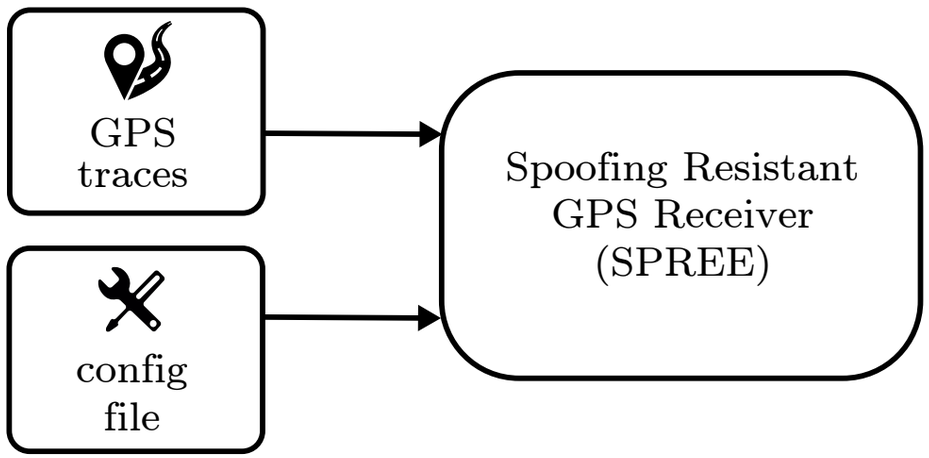
- SPoofing REsistant GPS rEceiver (SPREE), the first GPS receiver capable of detecting *(up to an accuracy)* all known spoofing attacks.

- A novel auxiliary peak tracking technique enables detection of a seamless takeover attacks *(tracks all peaks …)*



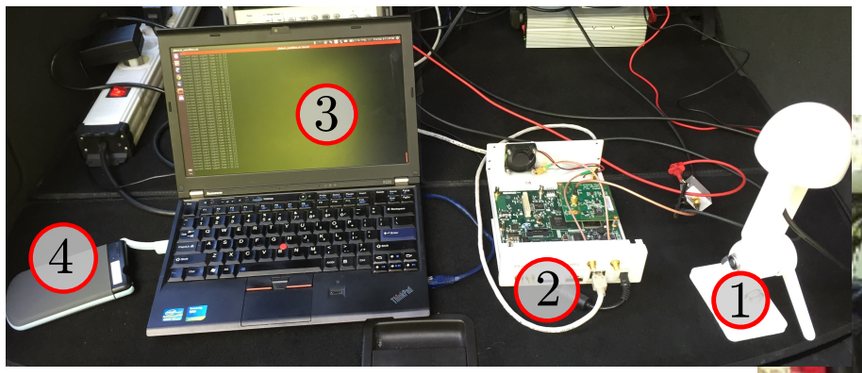
- SPREE is based on GNSS-SDR and open source [2016]: https://www.spree-gnss.ch/
  MobiCom 2016

Results So Far …

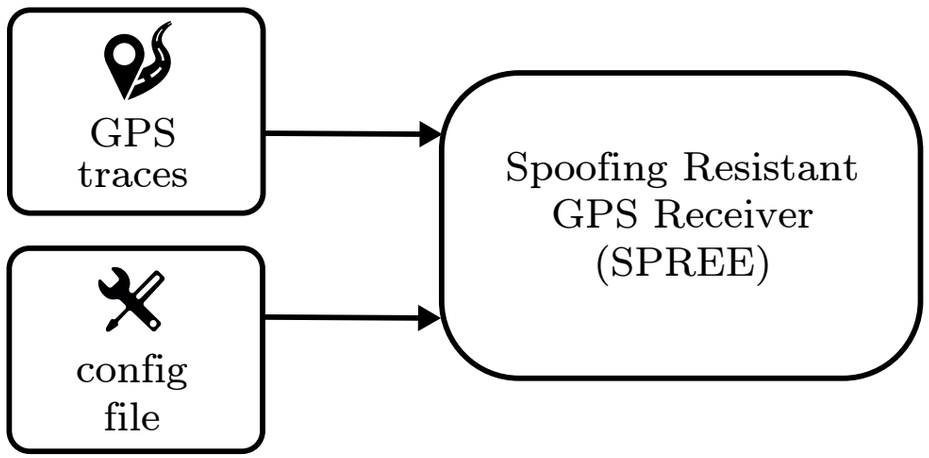


GPS Signal Traces

- Our own GPS simulators
- TEXAS Spoofing Battery (TEXBAT)
  - de-facto standard of publicly available spoofing traces (includes seamless takeover attack)
- Wardriving

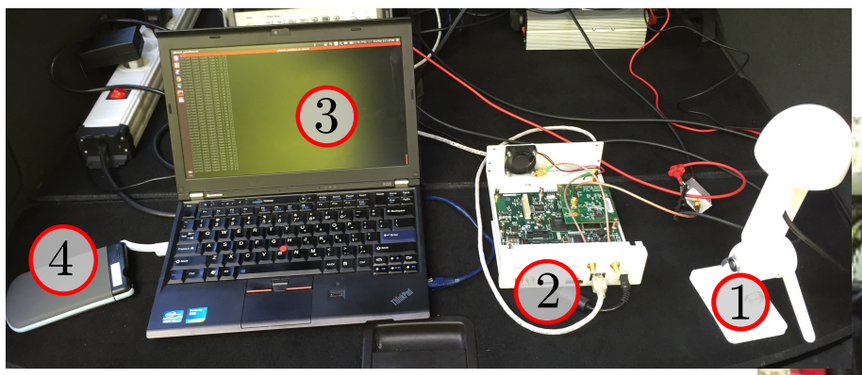


Results So Far …



GPS Signal Traces

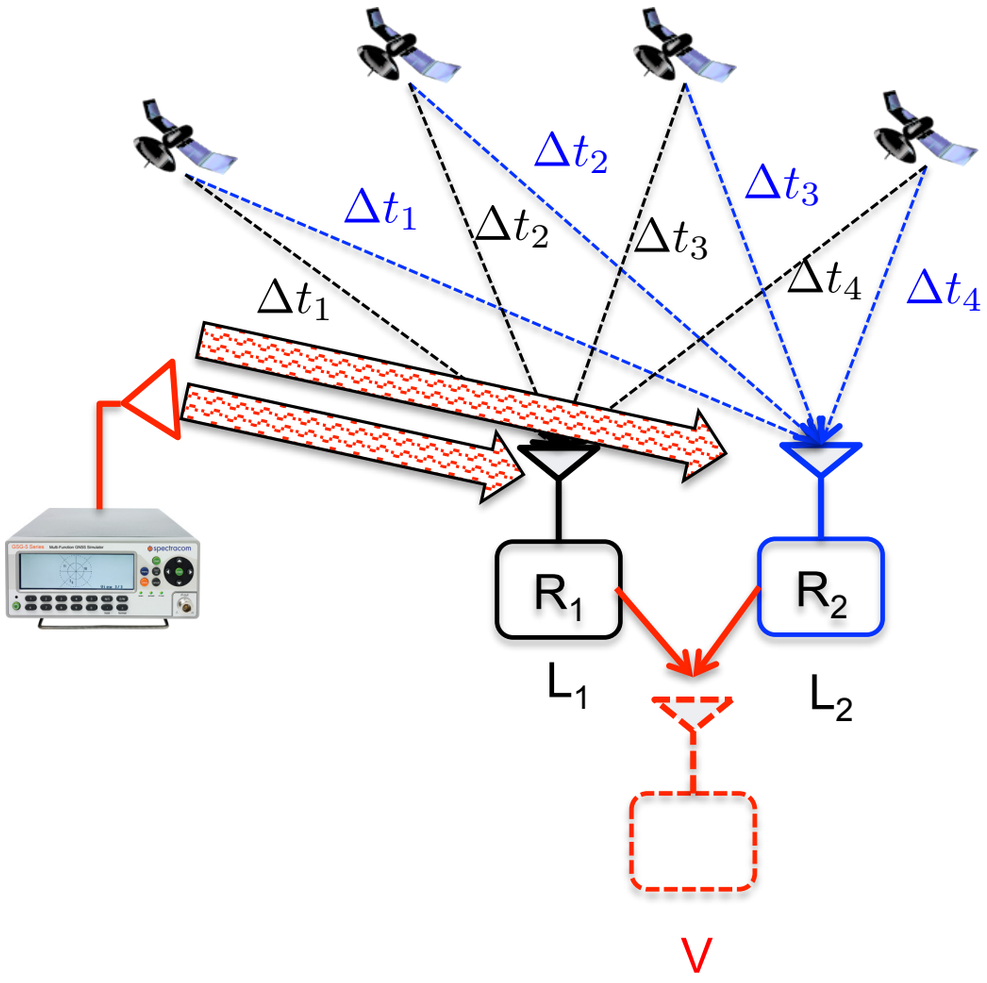
- Our own GPS simulators
- TEXAS Spoofing Battery (TEXBAT)
  - de-facto standard of publicly available spoofing traces (includes seamless takeover attack)
- Wardriving

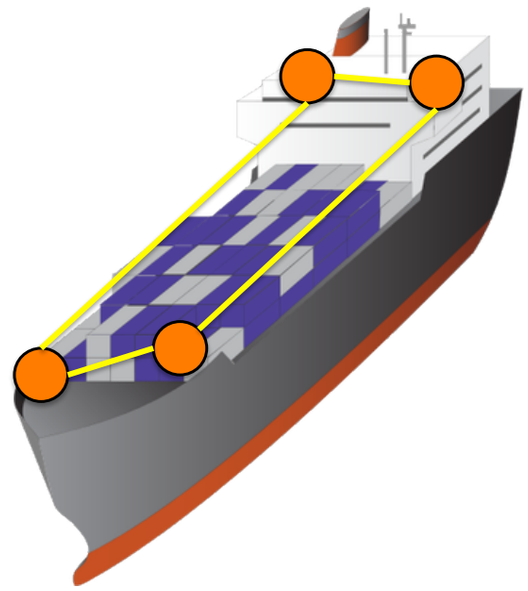


All spoofing attacks >1km detected! (DY adversary)
(peak separation clearly distinguishable from multi-path)

Detecting GPS Spoofing using Multiple Receivers

Leveraging Spatial Diversity





If d(R1,R2) is known

=> spoofing detection

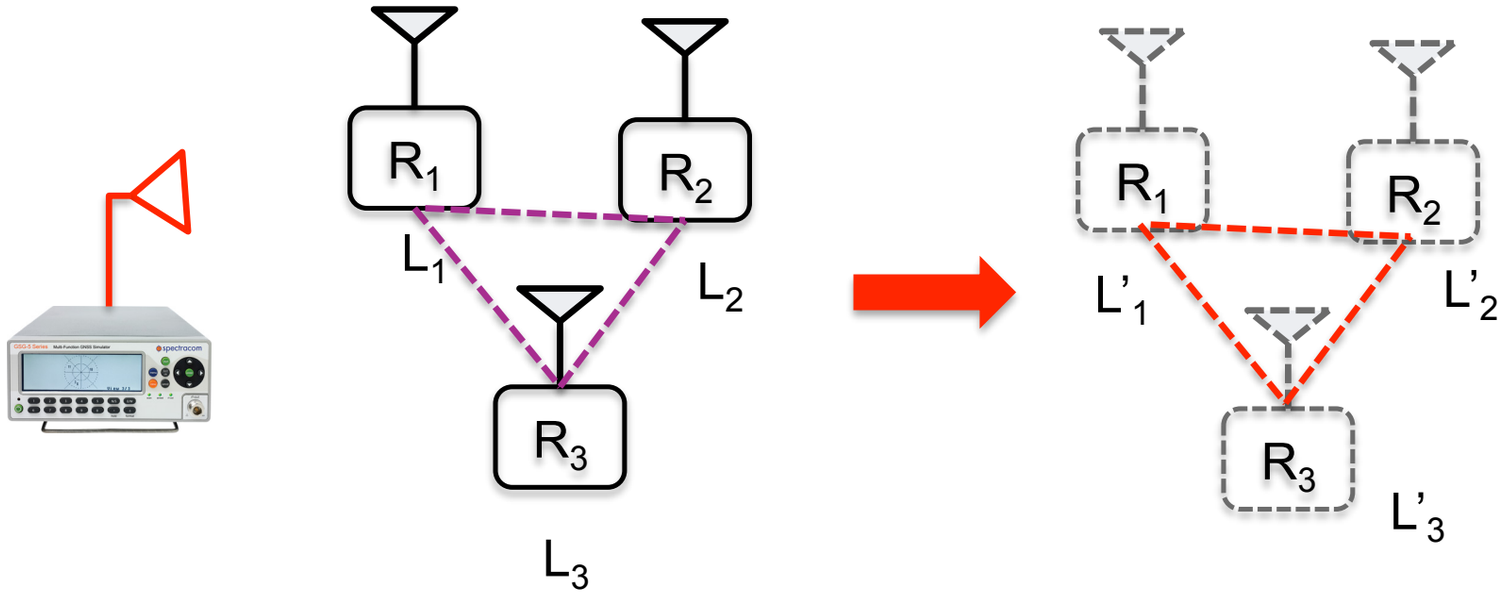
Attacker transmits omnidirectionally

=> Both R1 and R2 compute their positioning at V

- Tippenhauer, Popper, Rasmussen, Capkun, On the requirements for successful GPS spoofing attacks, ACM CCS 2011

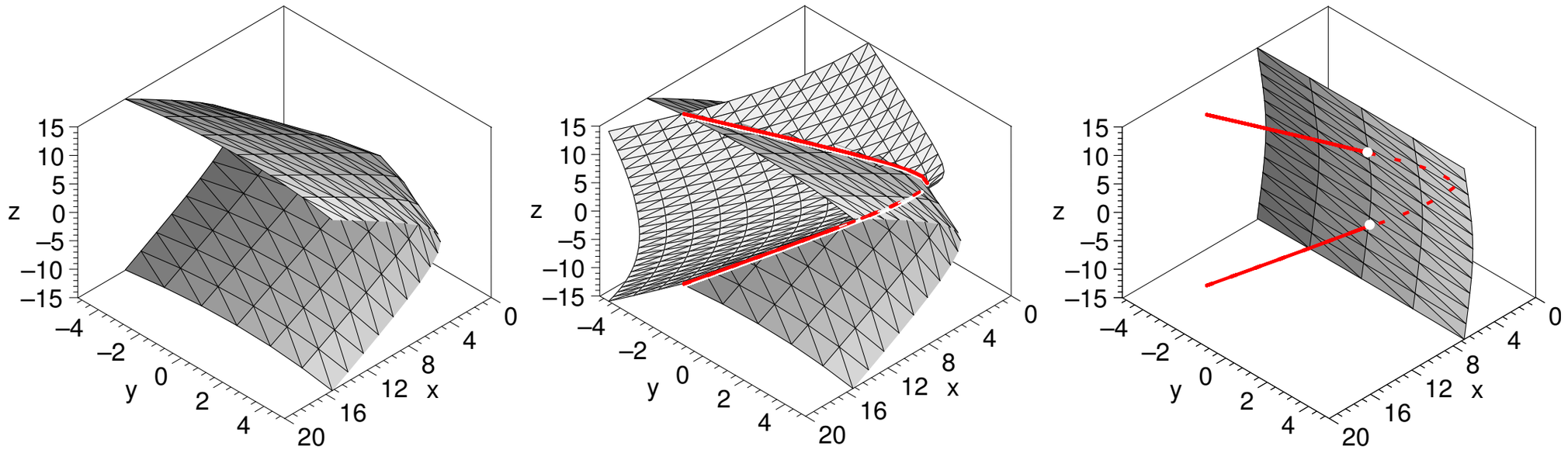
Leveraging Spatial Diversity

"***The GPS Group Spoofing Problem*** is the problem of finding combinations of ***GPS signals*** (sent by the attacker), ***transmission times*** (at which the spoofing signals are sent), and ***spoofer locations*** such that the location or time of each victim is spoofed to the desired location/time."



L'_i are spoofed locations

Spatial Diversity Constrains the Attacker



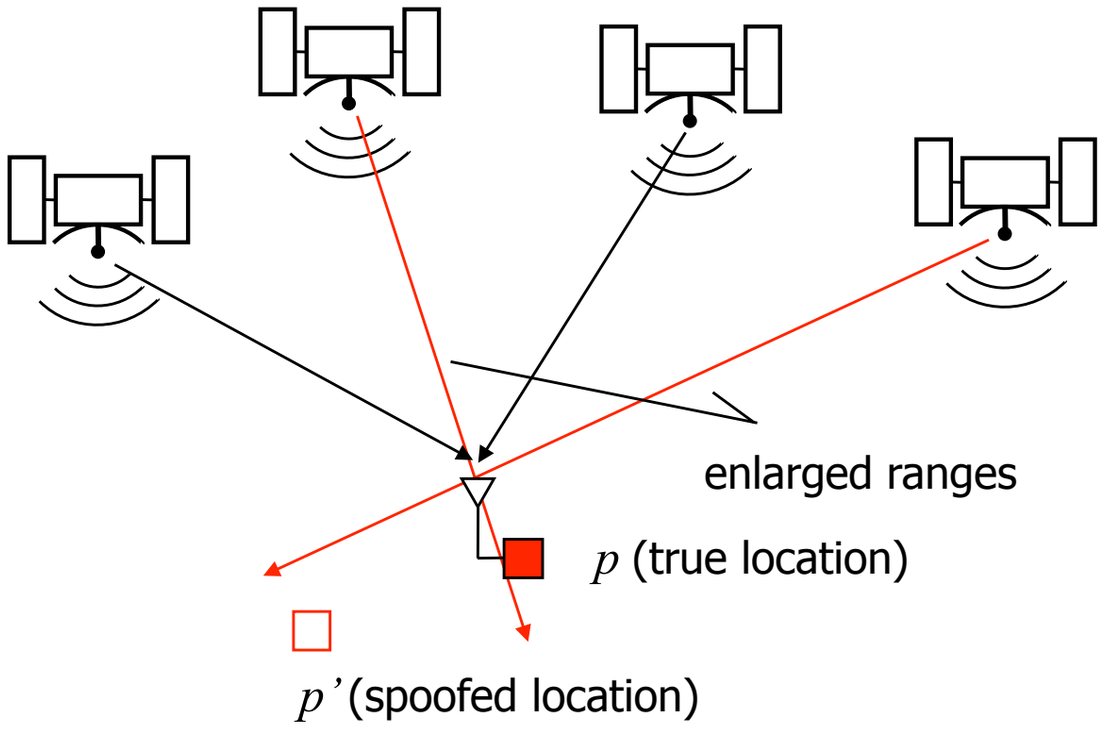
(a) 2 receivers (b) 3 receivers (c) 4 receivers

Shows the locations where the attacker can place spoofers to successfully spoof (assuming omnidirectional attacker).

	Spoofing to one location	Spoofing to multiple locations (preserved formation)	
n	Civ. & Mil. GPS	Civilian GPS	Military GPS
1	$P_i^A \in \mathbb{R}^3$	-	-
2	$P_i^A \in \mathbb{R}^3$	set of hyperboloids	one hyperboloid
3	$P_i^A \in \mathbb{R}^3$	set of intersections of two hyperboloids	intersection of two hyperboloids
4	$P_i^A \in \mathbb{R}^3$	set of 2 points	2 points
$\geq$5	$P_i^A \in \mathbb{R}^3$	set of points	1 point

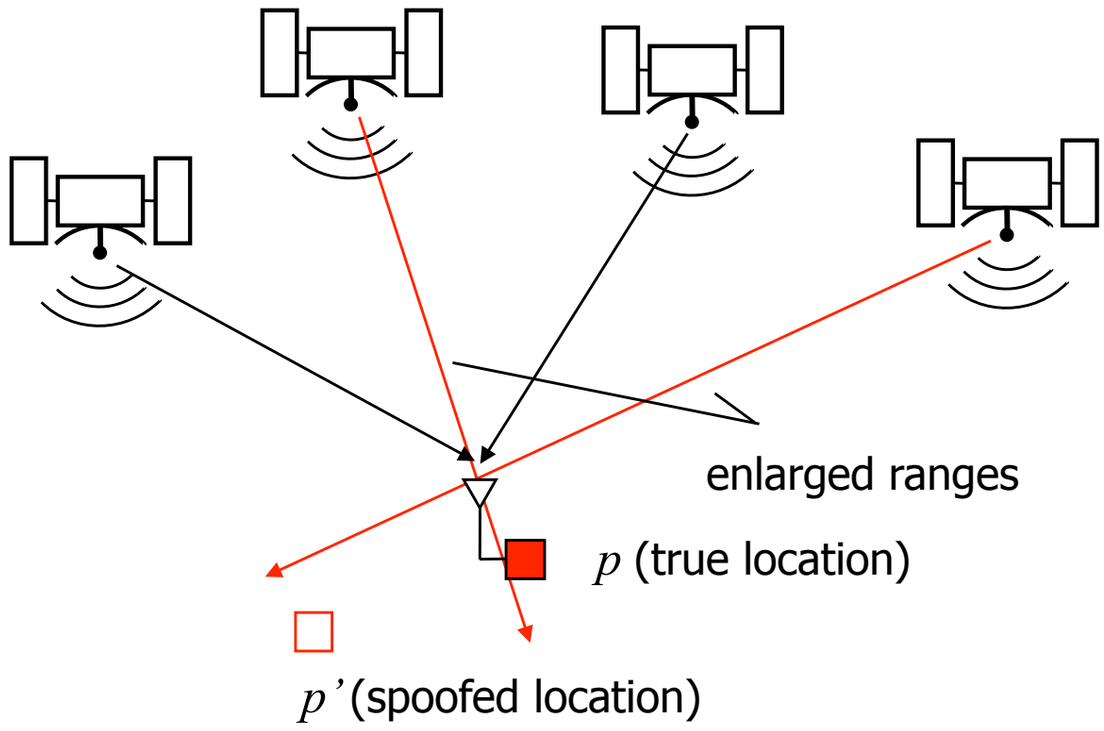
GPS Spoofing can be Prevented in a number of Scenarios but …

*Broadcast systems like GPS cannot be **fully** secured*
(ASSUMING DY ATTACKER) !!!



GPS Spoofing can be Prevented in a number of Scenarios but …

*Broadcast systems like GPS cannot be **fully** secured*
(ASSUMING DY ATTACKER) !!!



- Secure positioning requires either:
  - bidirectional communication ***or***
  - communication from the device to the infrastructure

Cryptographic Countermeasures

Proposal for a Secure GPS (Kuhn)

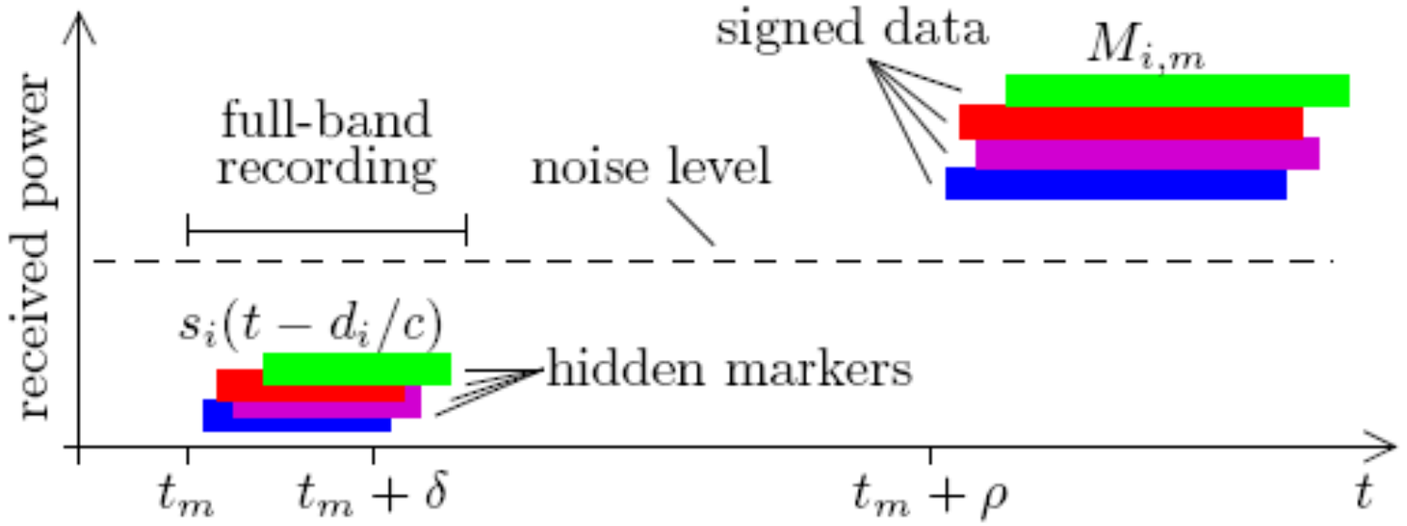
Devices hold satellite public keys

At time t, a satellite uses a secret code to spread the navigation signal

- The receiver uses a broadband receiver to receive the whole signal band (receiver does not know the despreading code yet)
- At time t+dt, the satellite discloses its secret code, signed with its private key
- The receiver gets the code, verifies the signatures and de-spreads the signals.

Prevents the generation of fake signals and their individual shifts.

Proposal for a Secure GPS (Kuhn)



$$\hat{d}_i = |L_i - p| + c \cdot \delta \qquad \Rightarrow \qquad \hat{d}_i = |L_i - p| - c \cdot \delta + c \cdot \Delta_i$$

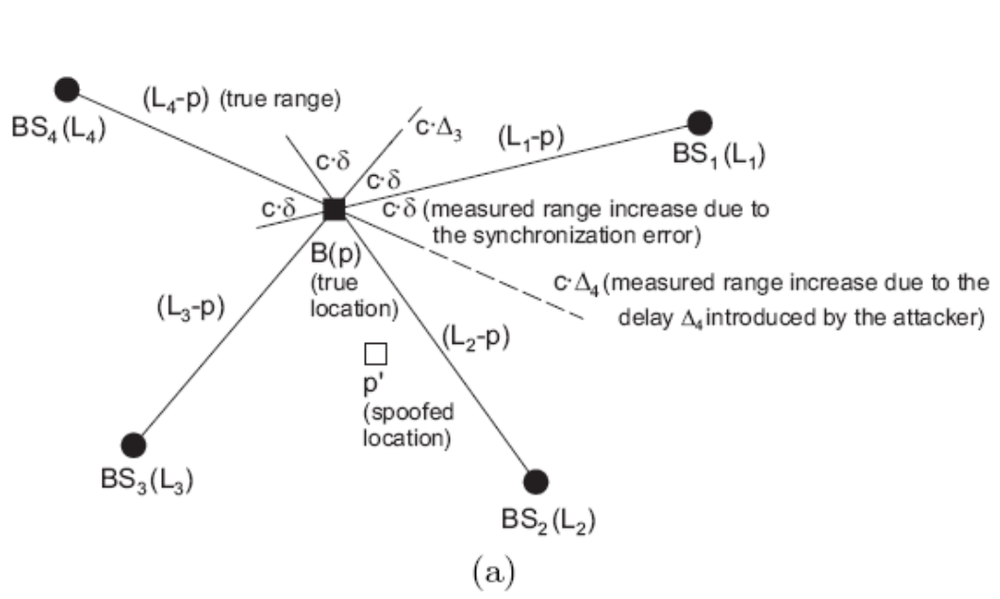
$$\begin{aligned}
(t_r^1 - t_s) \cdot c &= |L_1 - p| + c \cdot \delta + \Delta \\
(t_r^2 - t_s) \cdot c &= |L_2 - p| + c \cdot \delta + \Delta \\
(t_r^3 - t_s) \cdot c &= |L_3 - p| + c \cdot \delta + \Delta \\
(t_r^4 - t_s) \cdot c &= |L_4 - p| + c \cdot \delta + \Delta
\end{aligned}$$

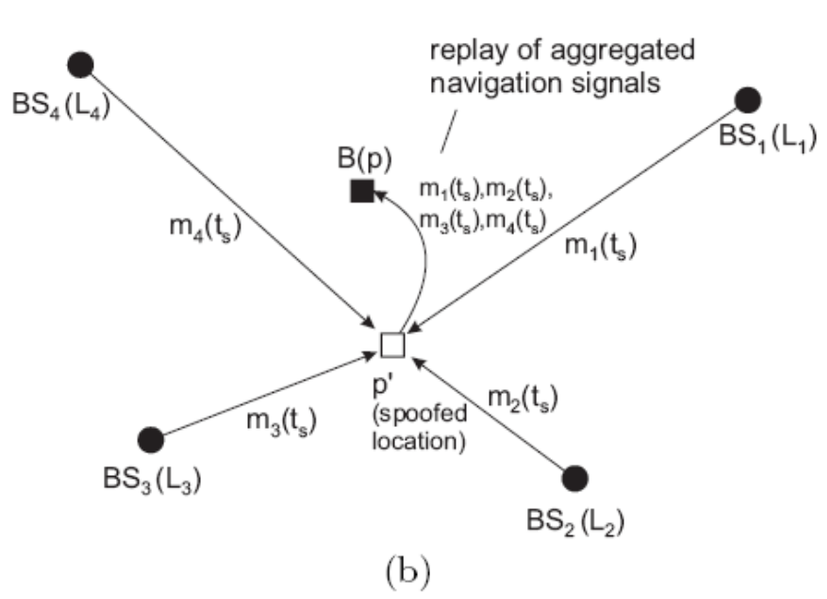
Proposal for a Secure GPS (Kuhn)

The scheme

- Prevents pulse-delay of individual signals (a)
- But not of aggregated signals (full band) (b)

There are issues with its efficiency (it might add additional seconds to the signal lock).





M. Kuhn, An Asymmetric Security Mechanism for Navigation Signals (2004 Information Hiding Workshop, Proceedings, Springer-Verlag, LNCS 3200)
www.cl.cam.ac.uk/~mgk25/ih2004-navsec.pdf