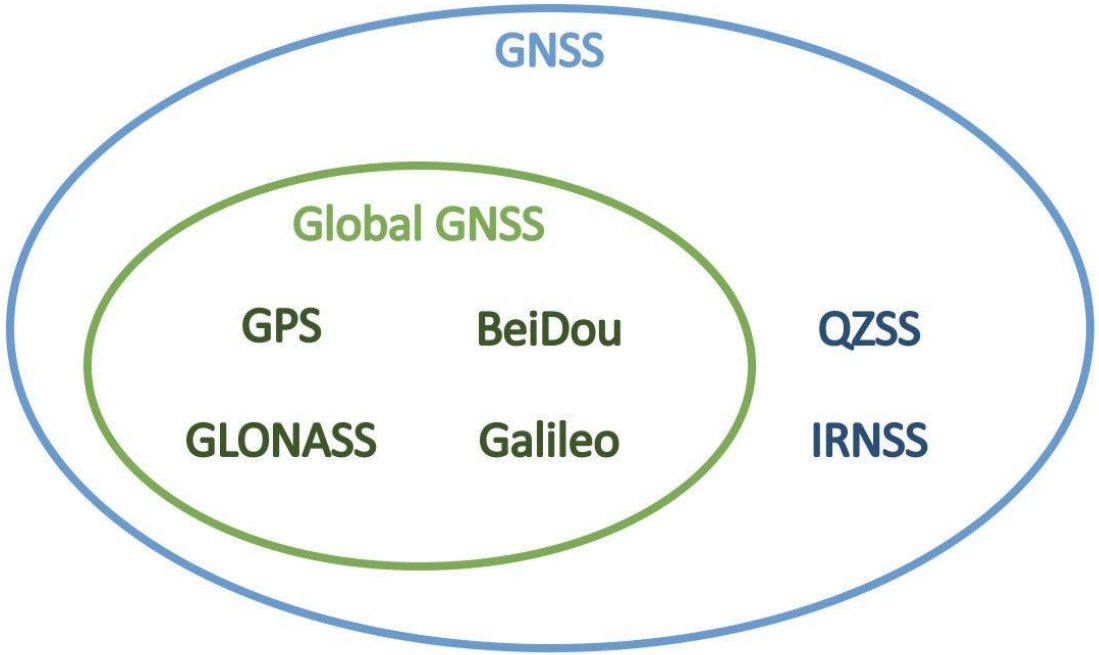
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

Can you trust your location and timing?

GNSS or GPS?

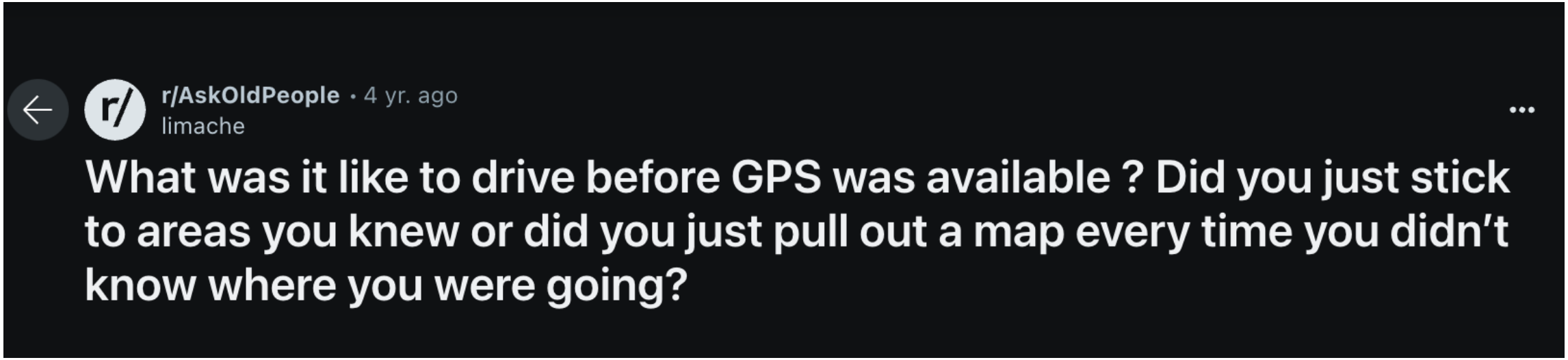
- Most people should be familiar with GPS, but many may not hear of GNSS often.
- GNSS stands for **Global Navigation Satellite System**, including all navigation systems which use satellites to provide autonomous geo-spatial positioning.



GPS

- GPS is the first GNSS launched in 1978 and developed by the U.S., and there are many satellite navigation systems out there established by other organizations.
- Originated during the Cold War to develop an all-weather, 24-hour, truly global navigation system to support the positioning requirements for the armed forces of the U.S. and its allies.
- The total investment by the U.S. military in the GPS system to date is well over $10 BILLION!

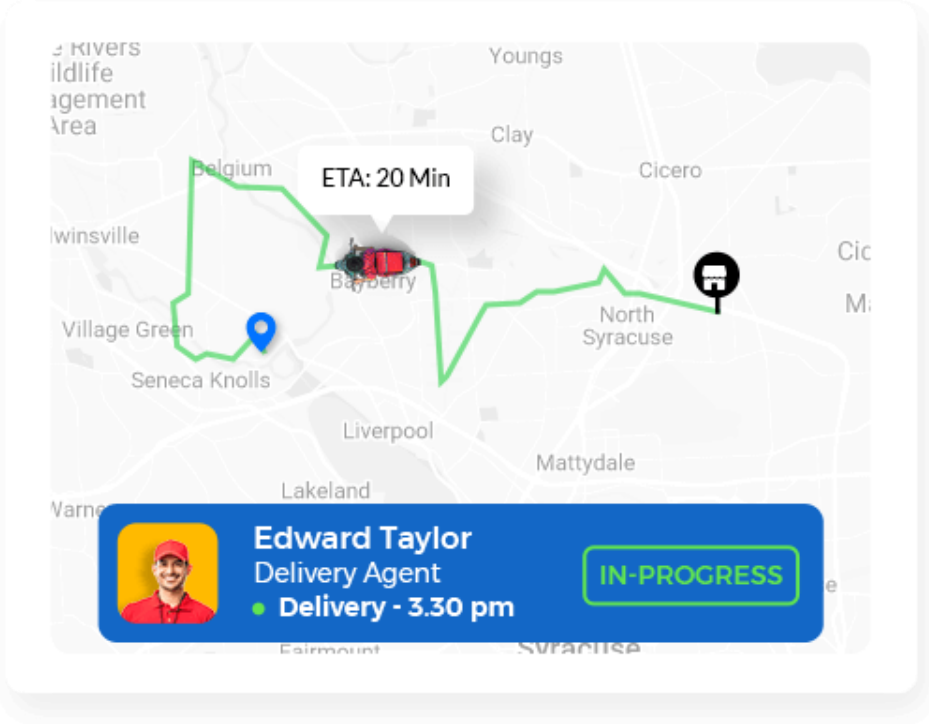
What was life before GPS?



Beyond Navigation and Mapping

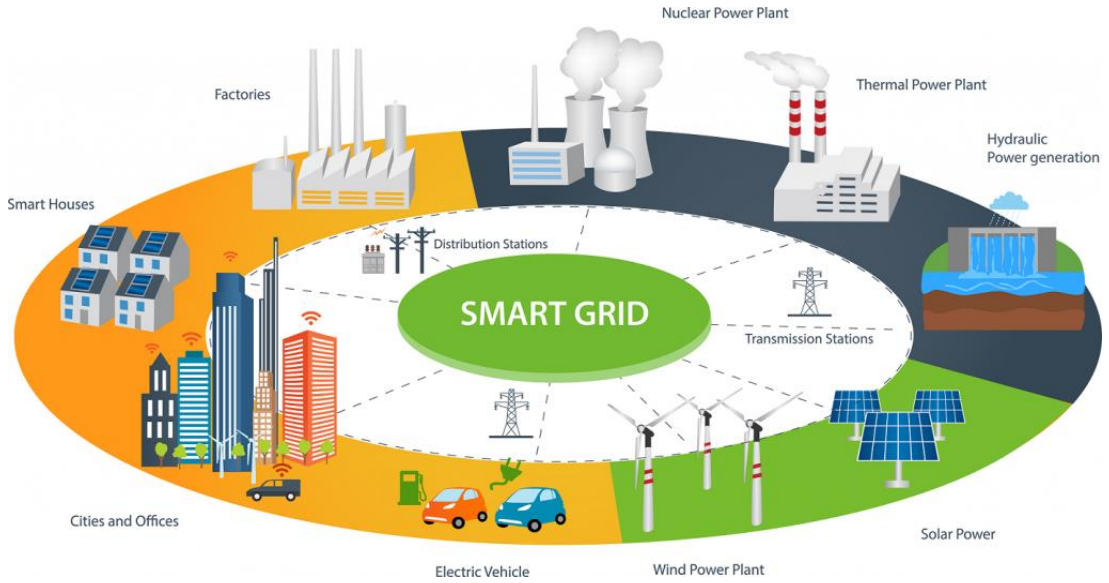
Many popular apps use GPS and location data to provide tailored services or improve user experience

- Fitness and Health Apps
- Food Delivery / E-commerce and Retail Apps
- Social Media/Networking Apps/ Dating
- Gaming Apps
- Weather Apps
- Safety and Security Apps

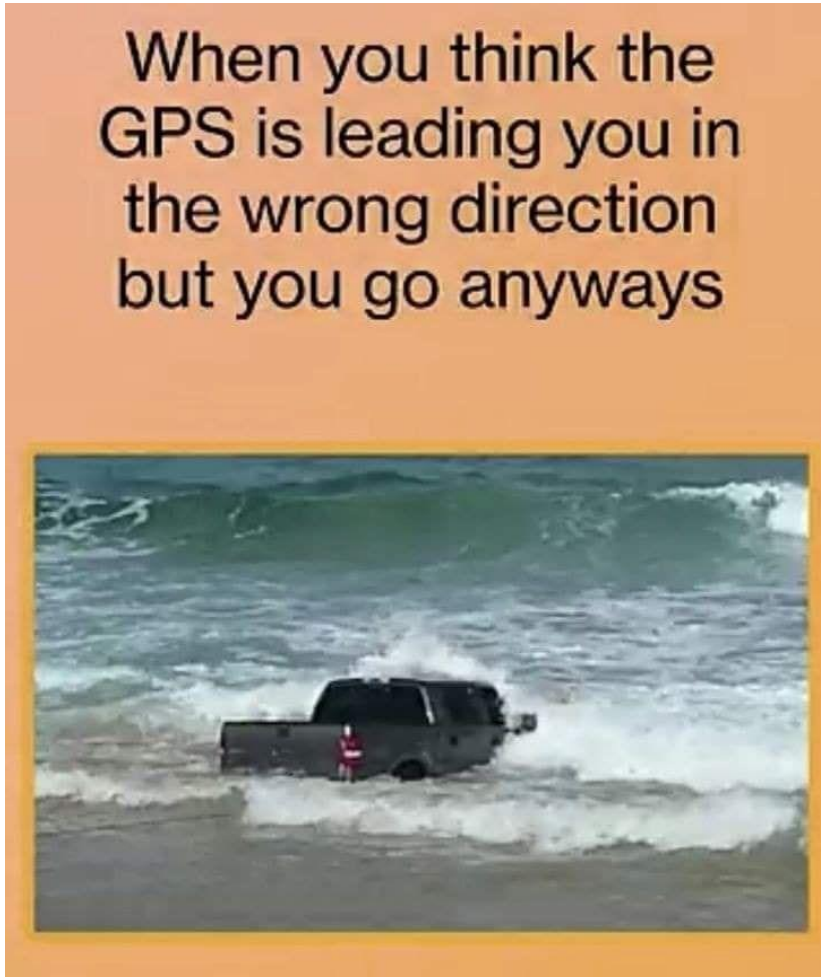


Position, Navigation and… TIMING!

- Telecommunications
- Power Grids
- Financial Services (Trading/Stock Market/Banking/ATM/)
- Broadcasting
- Emergency Services
- …



What if the GPS is wrong?



Misnavigation

2016 U.S.–Iran naval incident

3 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

On January 12, 2016, two United States Navy riverine command boats were seized by Iran's Islamic Revolutionary Guard Corps (IRGC) Navy after they entered Iranian territorial waters near Iran's Farsi Island in the Persian Gulf. Initially, the U.S. military claimed the sailors inadvertently entered Iranian waters owing to mechanical failure, but it was later reported that they entered Iranian waters because of navigational errors.[3]

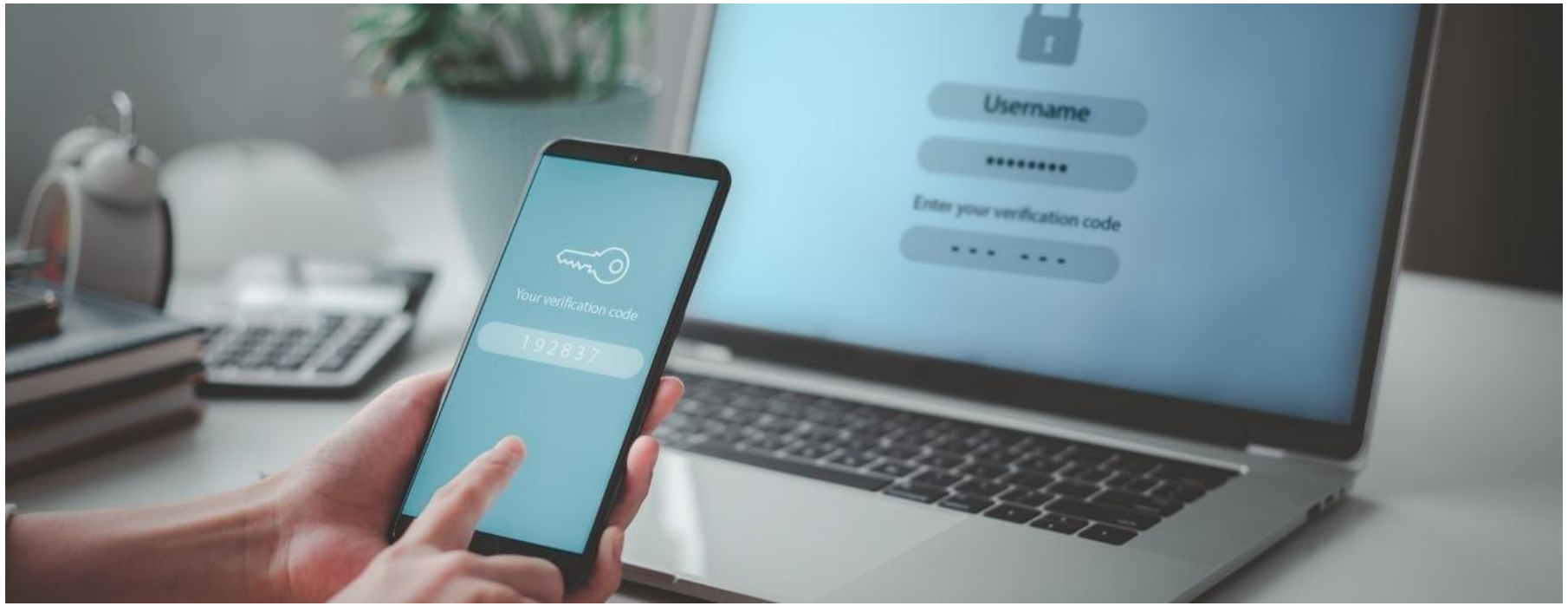
U.S. Secretary of State John Kerry called Iranian foreign minister Mohammad Javad Zarif within five minutes, the first of a series of phone calls between the two. The sailors had a brief verbal exchange with the Iranian military and were released, unharmed, 15 hours later.

The release was hailed by the Obama administration as an unintended benefit of the new diplomatic relationship. Iran released pictures of captured U.S. sailors. Some U.S. Republican 2016 presidential candidates such as Ted Cruz, Marco Rubio, and Donald Trump criticized the U.S. response to the detention, which they deemed too weak.[4]

2016 U.S.–Iran naval incident	
Date	12 January 2016, 5:10 p.m
Location	Persian Gulf 27°59′35″N 50°10′21″E
Result	Iranian victory sailors released after 15 hours
Belligerents	
United States	Iran
Commanders and leaders	
Cmdr. Eric Rasch (executive officer of CRS-3)	Cpt. Ahmad Dolabi
Units involved	
United States Navy • Fifth Fleet • Task Force 56 • CTG 56.7 • Coastal	IRGC Navy • 2nd Zone • 214th "Hazrat-e Amir" Special Force Flotilla[2]

Misnavigation or Spoofing?

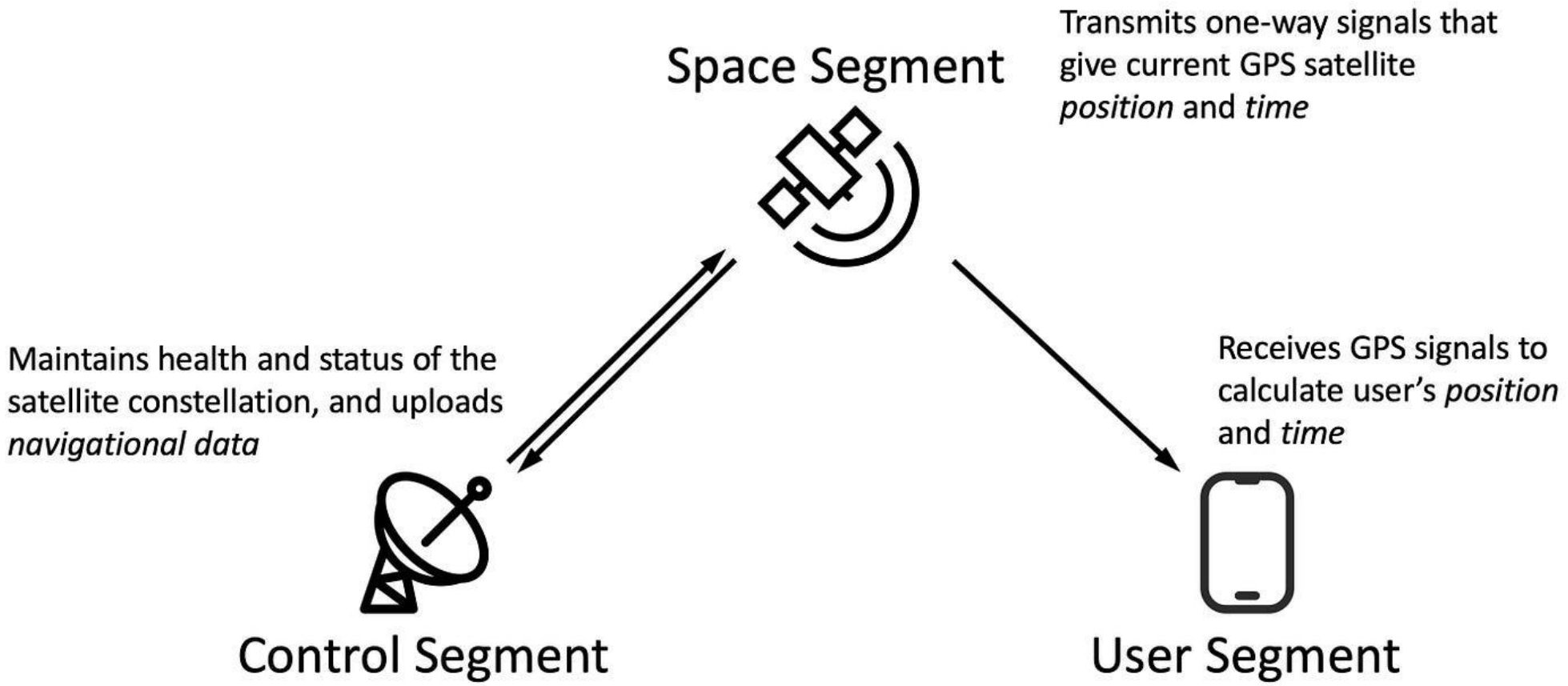
Not only military!



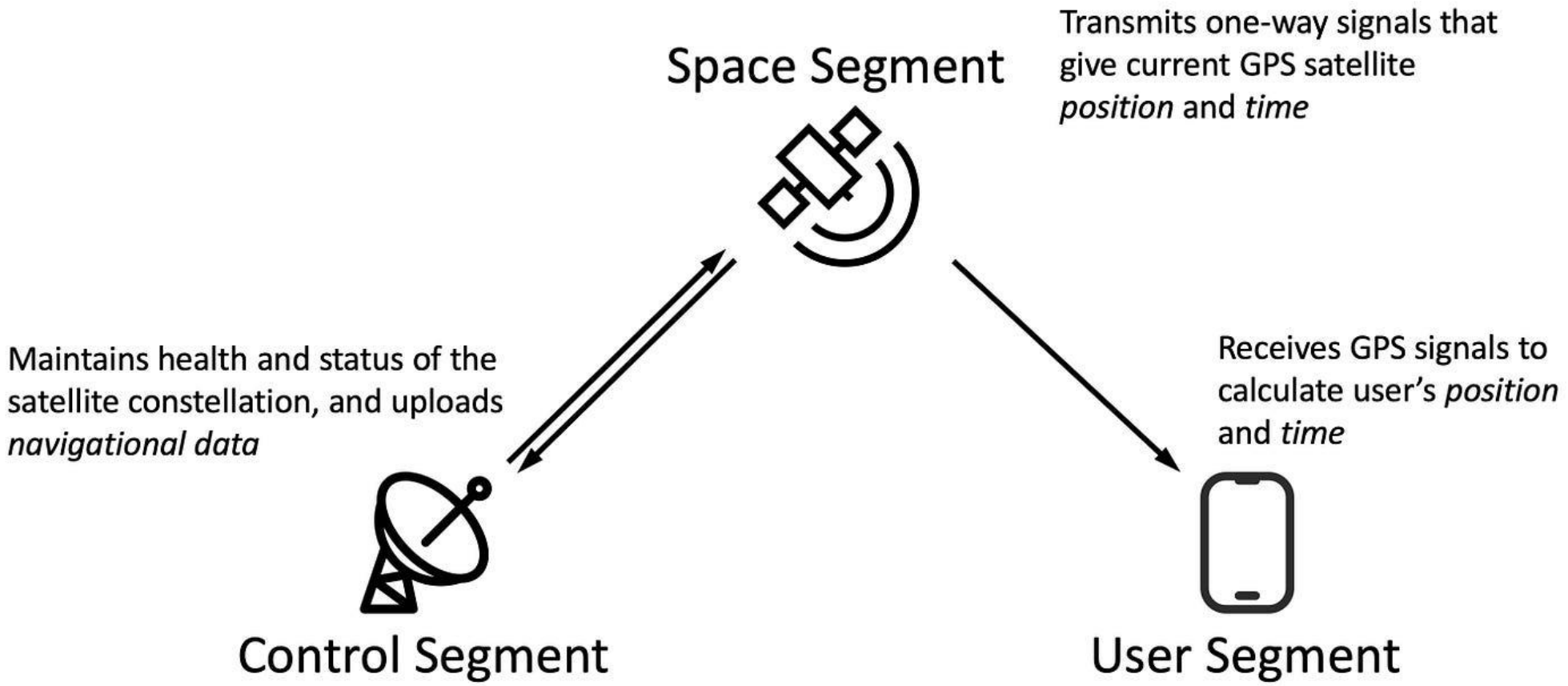
TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

What is GPS and how does it work?

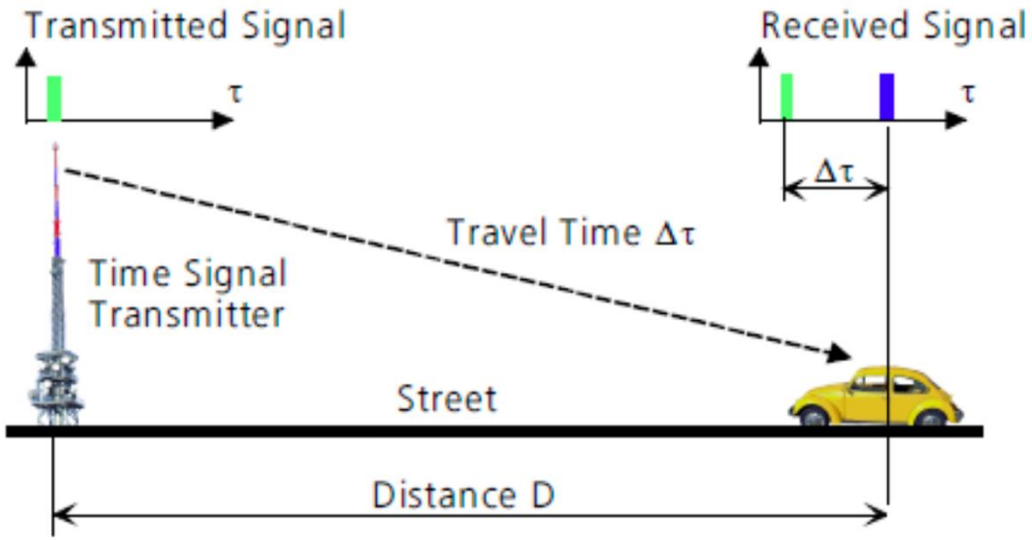
GPS components



GPS components



Ranging



Distance = Travel Time x Speed of radio wave

After signal decoding:

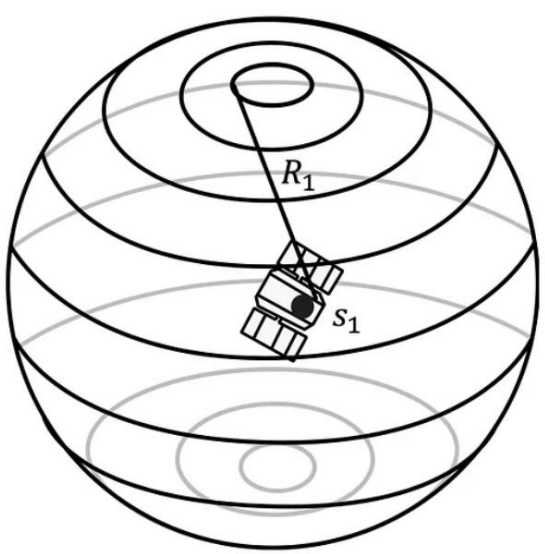
- The three-dimensional position of each satellite p^s
- Time t^s when GPS signal is transmitted

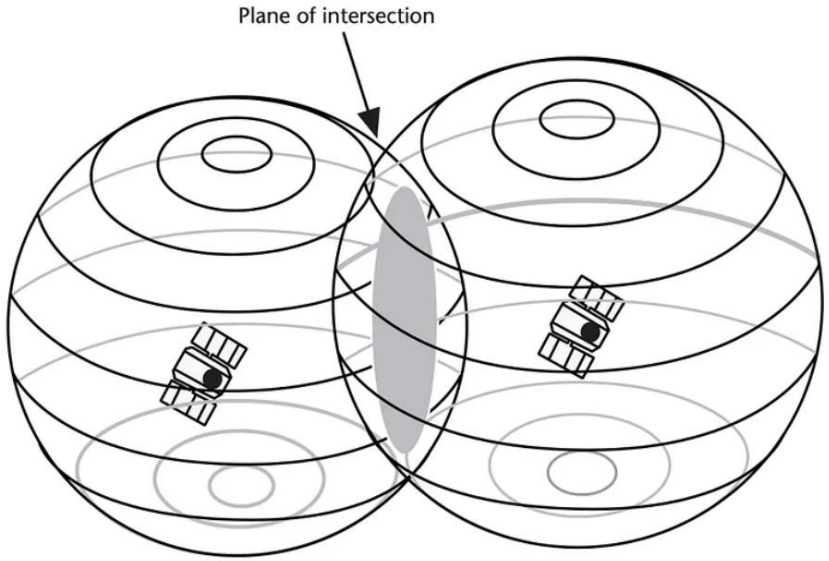
Satellites are way above the sky, thus when GPS signal is received, it would be delayed by some time Δt:

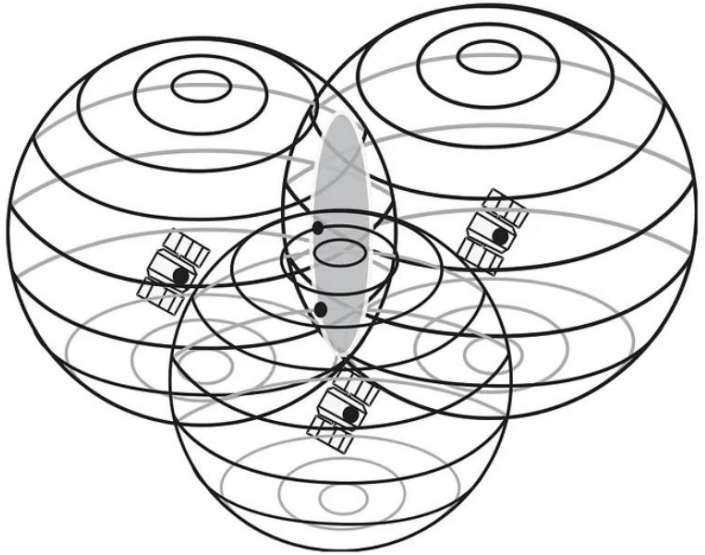
- Time t_r when GPS signal is received, which can be read from user clock
- Distance $R=c\Delta t=c(t_r-t^s)$, where c is the speed of light (GPS signal speed)

Trilateration

- $R_1=c(t_r-t^s_1)=\|p_r-s_1\|$
  $R_2=c(t_r-t^s_2)=\|p_r-s_2\|$
  $R_3=c(t_r-t^s_3)=\|p_r-s_3\|$

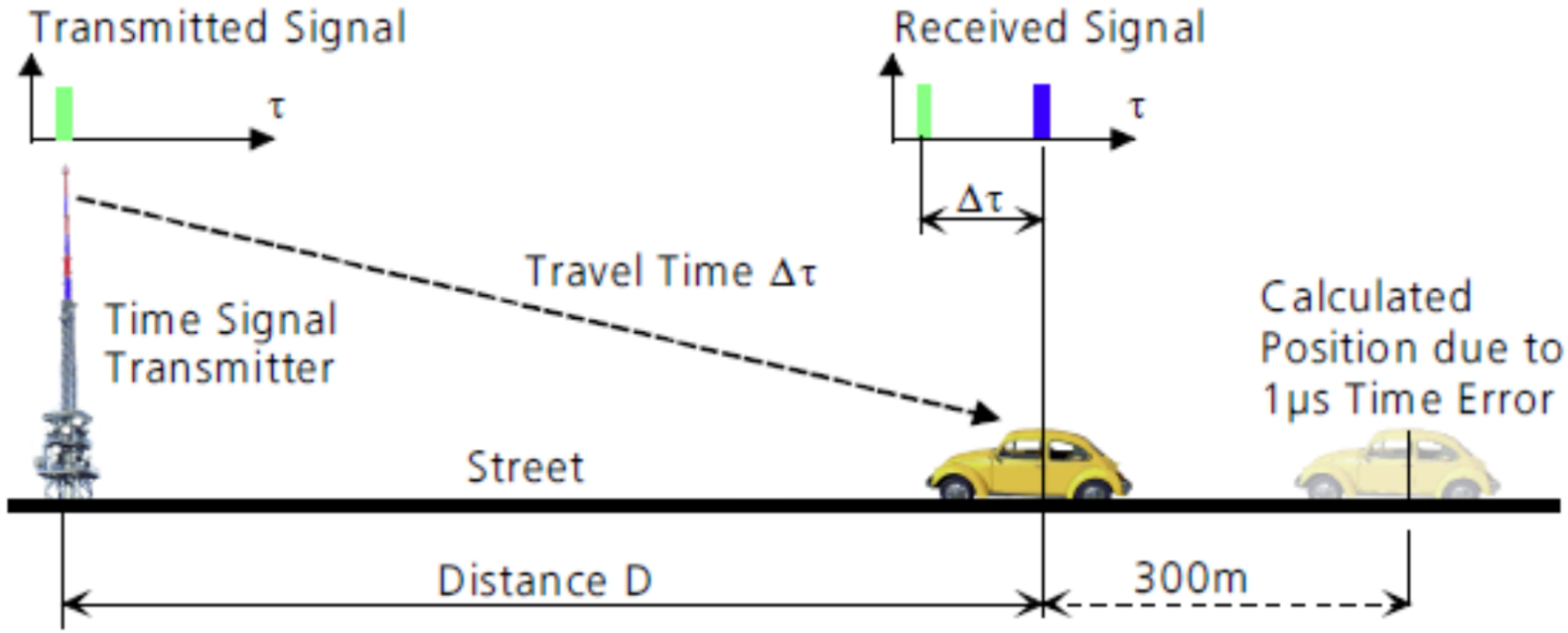






Clock offset

- However, user clock time may not be accurate enough.
- If the user clock is not accurate, let's say it has an offset of only 1 *μs* compared with true time, then an error of 300 *m* would be introduced when calculating the distance between user and satellite (suppose satellite time is accurate).



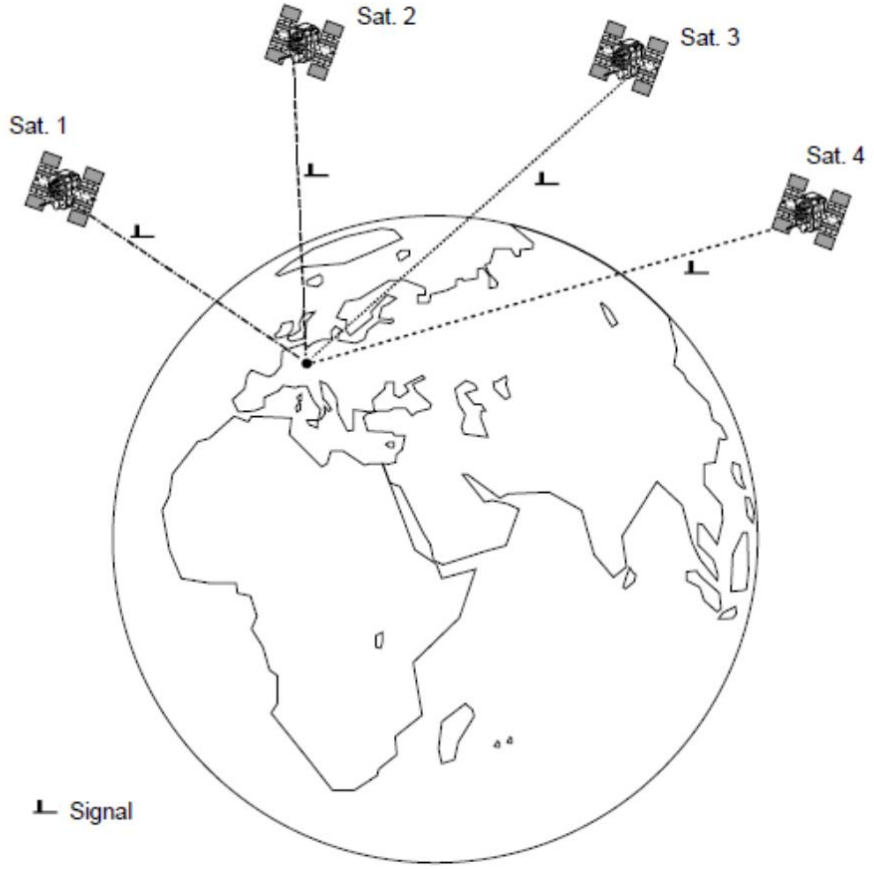
- Add one more variable, user clock offset *dt*, into user time and rewrite as $R=c(t_r+dt-t^s)=\|p_r-s\|$

- Since there are four unknowns instead of three, then why not add one more satellite?

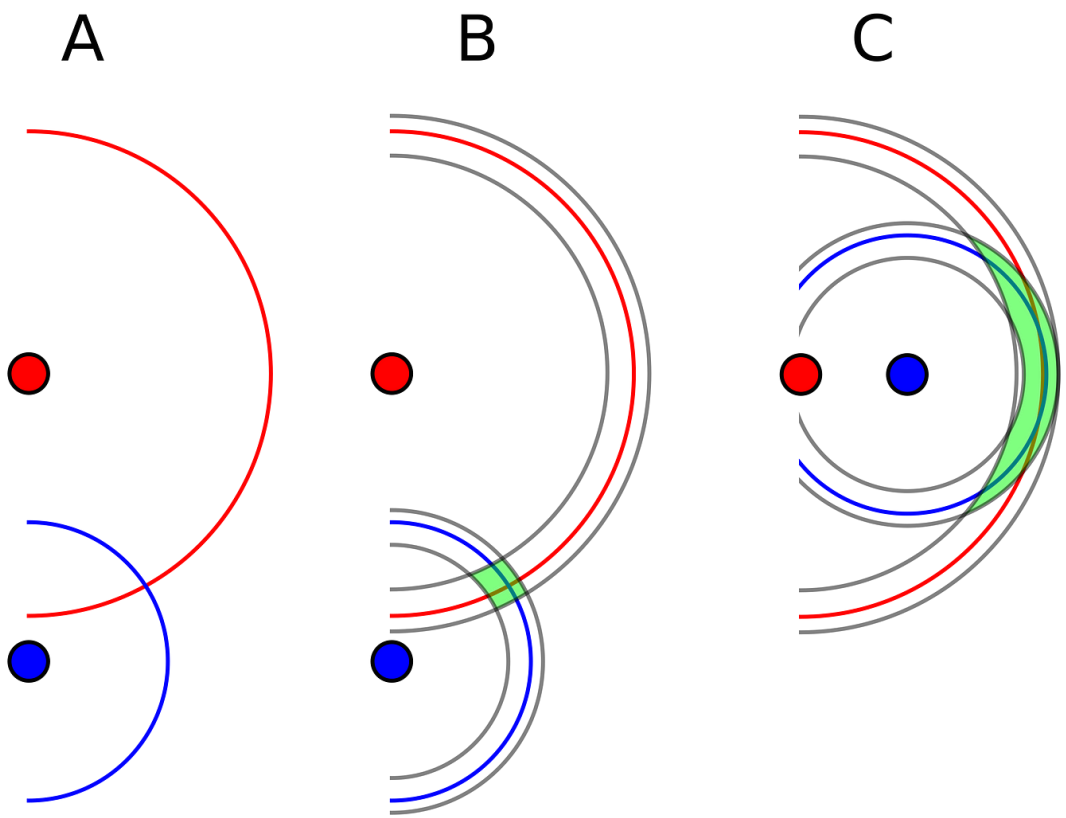
$$R_1=c(t_r+dt-t^s_1)=\|p_r-s_1\|$$
$$R_2=c(t_r+dt-t^s_2)=\|p_r-s_2\|$$
$$R_3=c(t_r+dt-t^s_3)=\|p_r-s_3\|$$
$$R_4=c(t_r+dt-t^s_4)=\|p_r-s_4\|$$

Problem Solved!

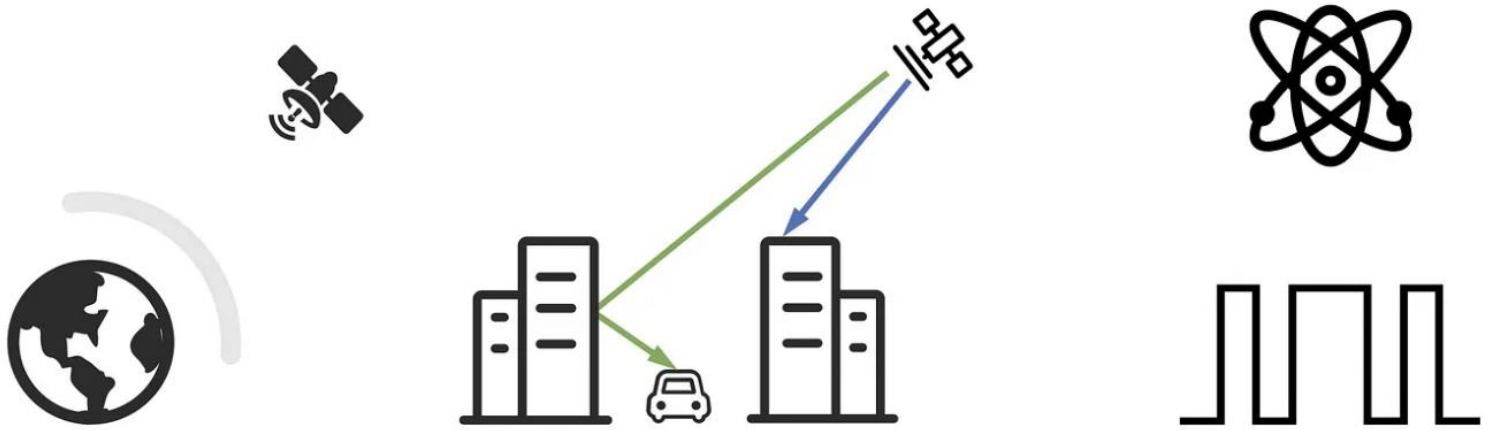
Constellation of satellite for their visibility



Diluition of precision



Unintentional sources of error

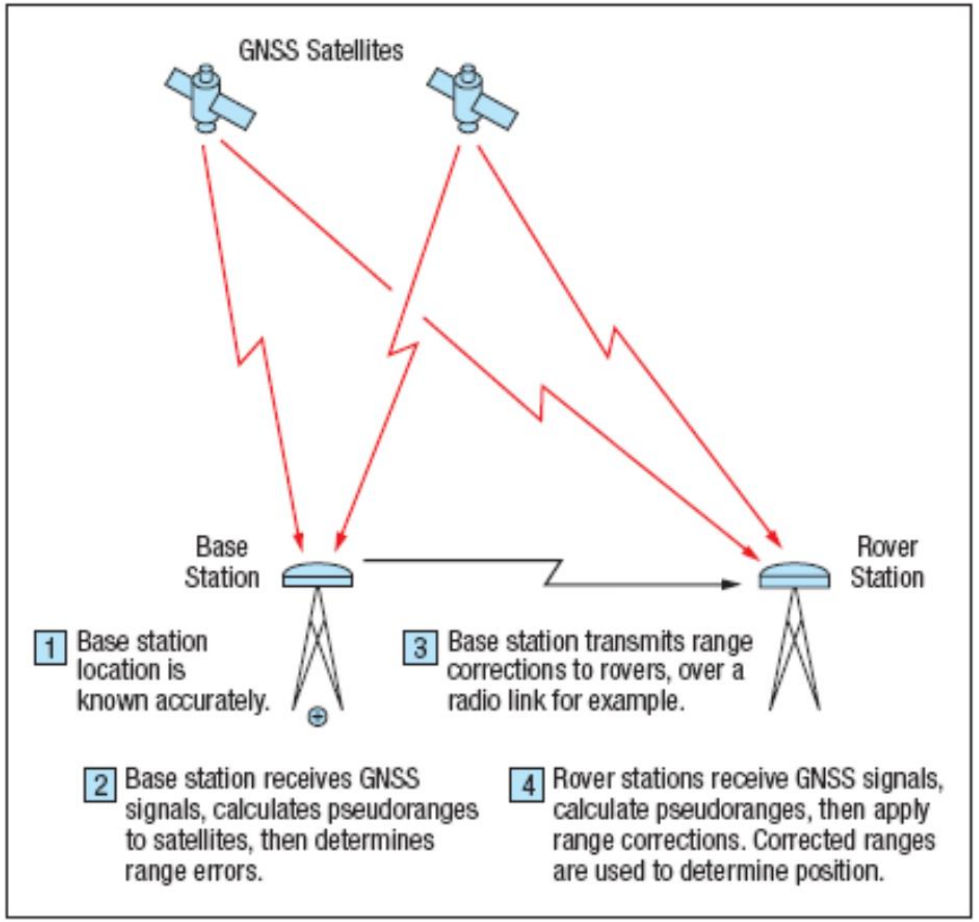


Atmospheric effects
Multipath effects
Satellite ephemeris and clock errors
Signal arrival time measurement

Selective Availability

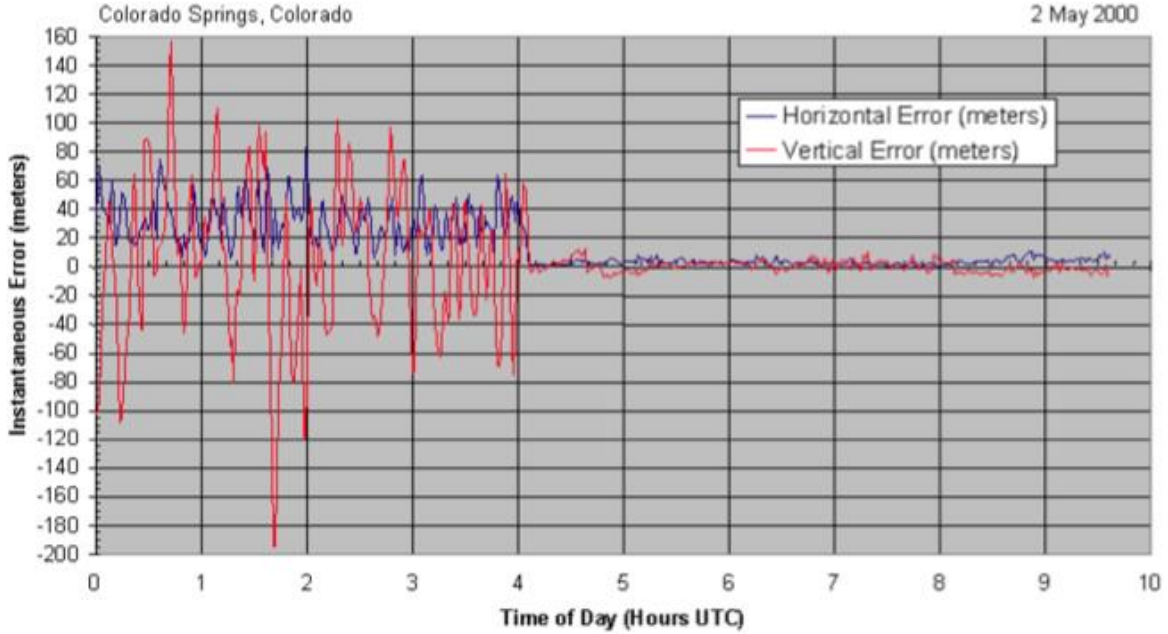
- Designed to have low accuracy of about 100 meters for civilian users, and high accuracy only for military uses.
- “Selective Availability”, or SA, was introduced to **deliberately degrade** the accuracy for non-military users.
- SA is outsmarted by outstanding scientists with the invention of Differential GPS (DGPS)

Differential GPS

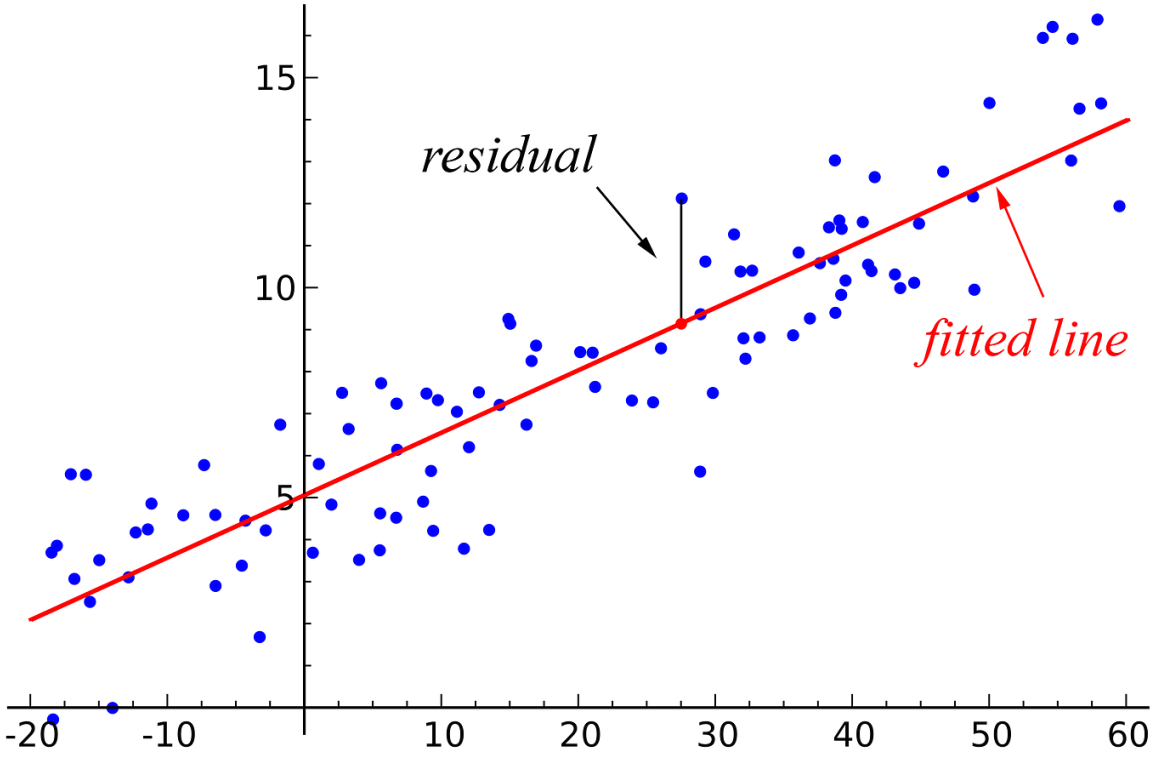


Selective Availability

- Designed to have low accuracy of about 100 meters for civilian users, and high accuracy only for military uses.
- “Selective Availability”, or SA, was introduced to **deliberately degrade** the accuracy for non-military users.
- SA is outsmarted by outstanding scientists with the invention of Differential GPS (DGPS)

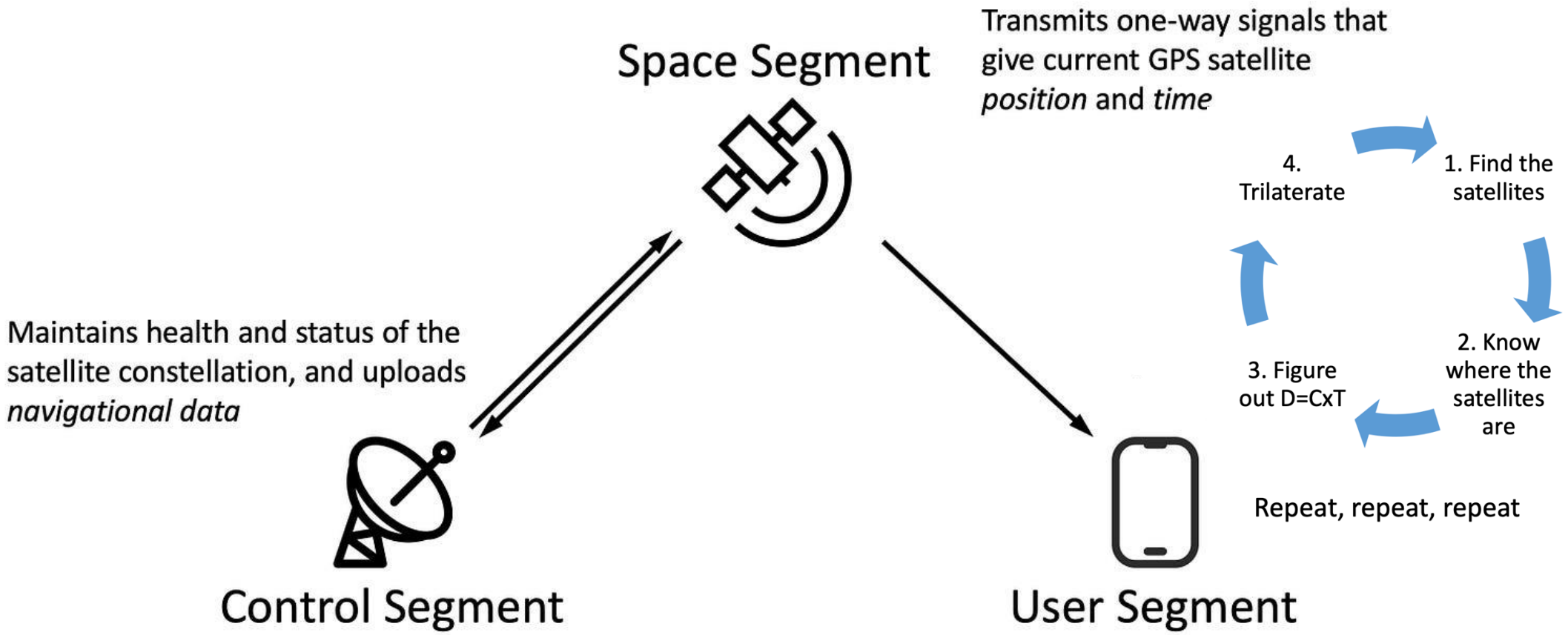


Uncertainty on the measured time

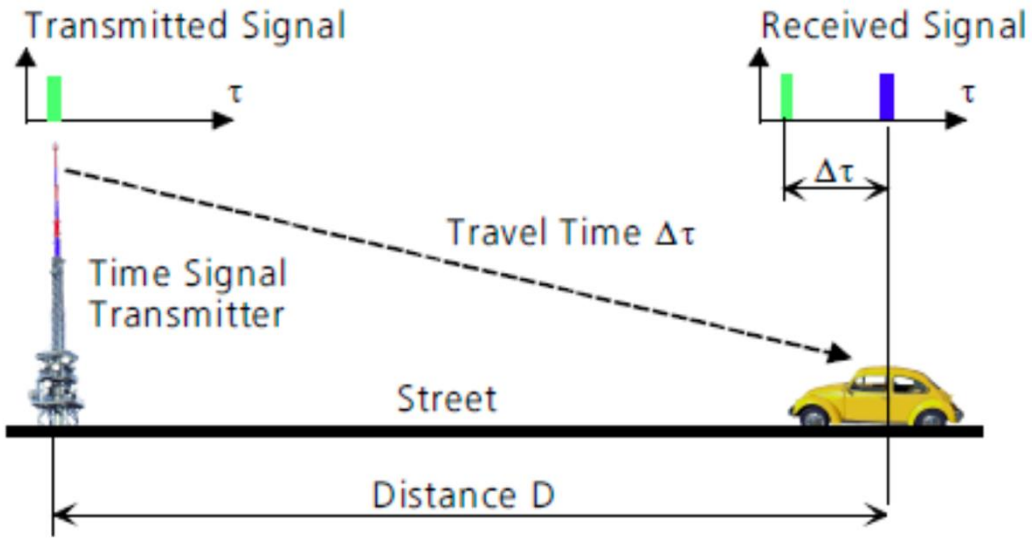


- So what if we have more satellites? Then
  $R_1=c(t_r+dt-t^s_1)=\|p_r-s_1\|$
  …
  $R_i=c(t_r+dt-t^s_i)=\|p_r-s_i\|$
  can be formulated as a non-linear least square problem and solved by the *Gauss-Newton* algorithm.
- RAIM techniques monitor the integrity of the GPS data by measuring the residuals

Let’s go a little bit down in the stack



Ranging

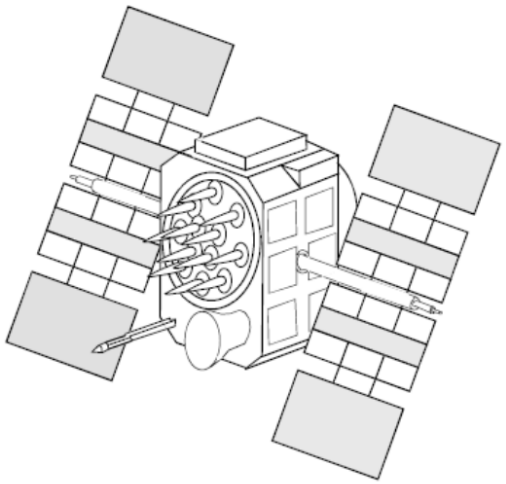


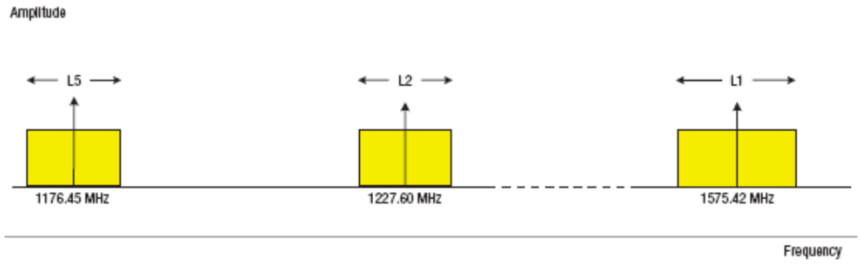
Distance = Travel Time x Speed of radio wave

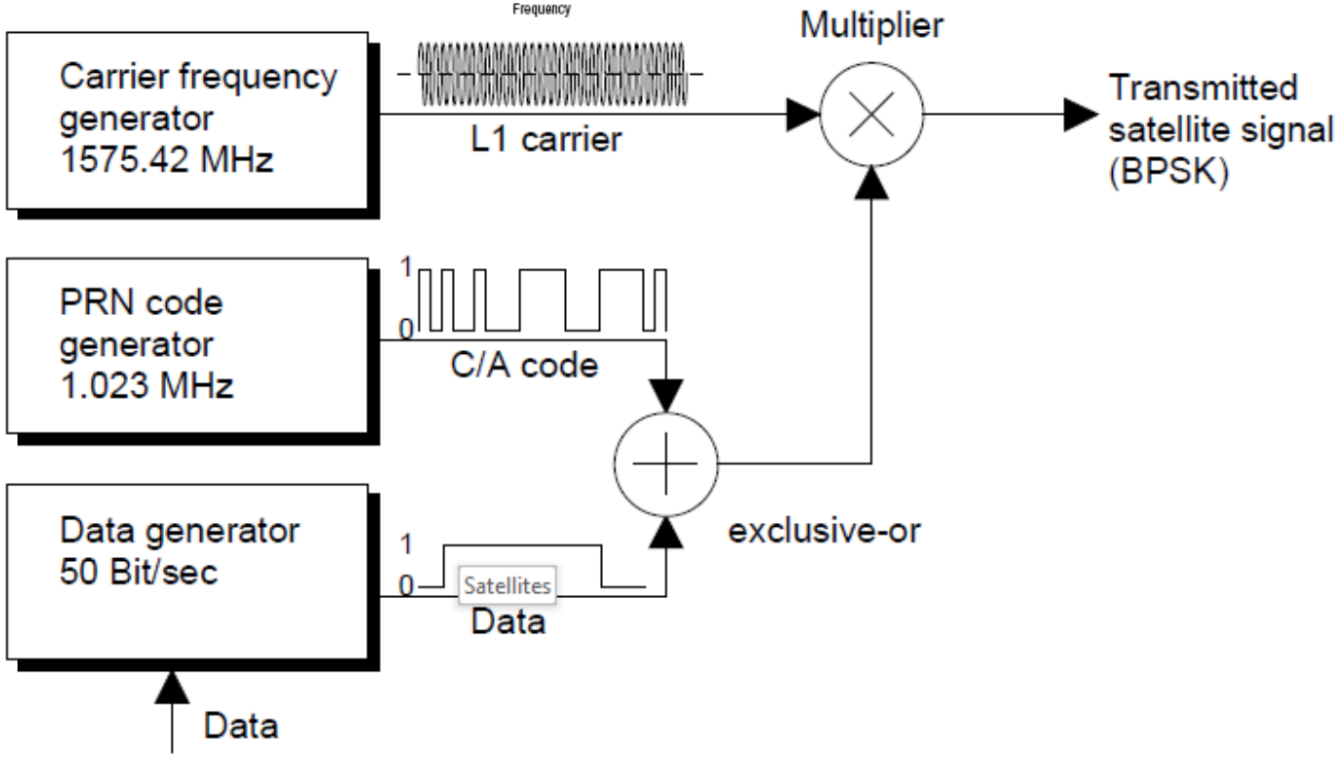
Which satellites do I select?

How do I measure the receiving time?

GPS signal structure and signal modelling

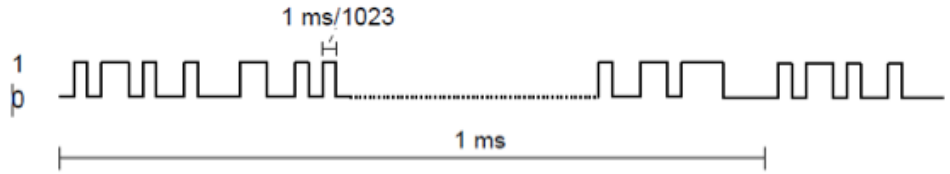






The pseudo-random noise (PRN) code

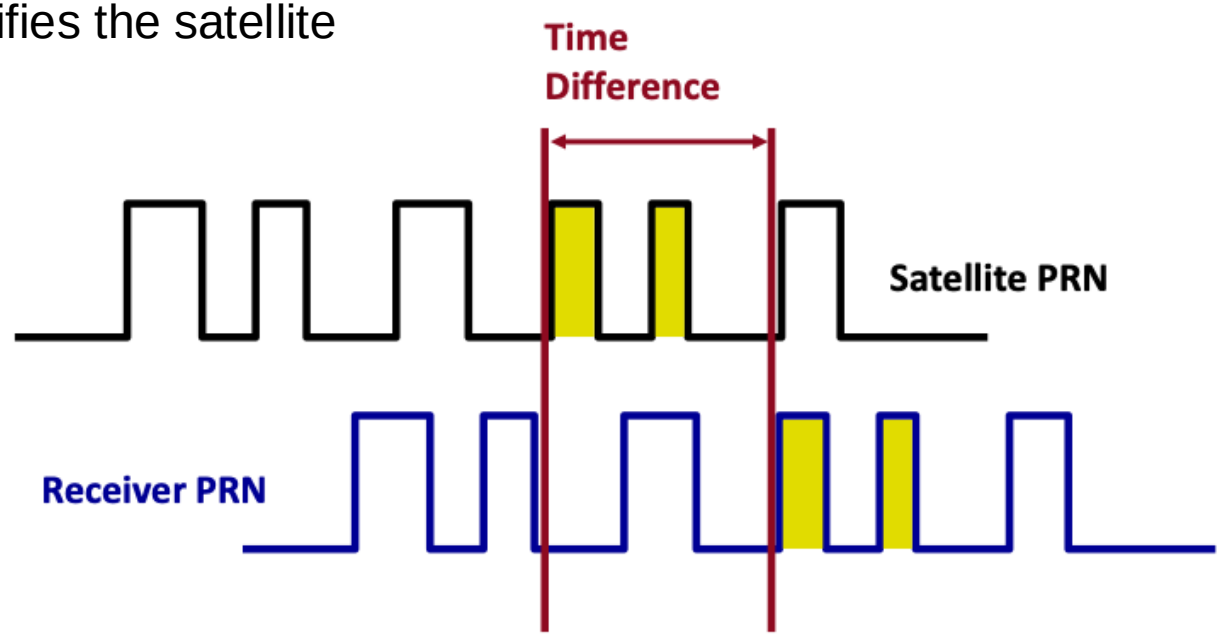
- Each GPS satellite transmits a unique signature assigned to it. This signature consists of a Pseudo Random Noise (PRN) Code of 1023 zeros and ones, broadcast with a duration of 1ms and continually repeated .
- PRC two purposes for the receiver
  1. Identification: the unique signature pattern identifies the satellite from which the signal originated
  2. Signal travel time measurement



PRN Code	Length (chips)	Period	Chip Frequency (MHz)
Coarse Acquisition (C/A) Code	1023	1 ms	1.023
Precise (P) Code	6.18×10^12	1 week	10.23

The pseudo-random noise (PRN) code

PRC two purposes for the receiver
1. Identification: the unique signature pattern identifies the satellite from which the signal originated
2. Signal travel time measurement



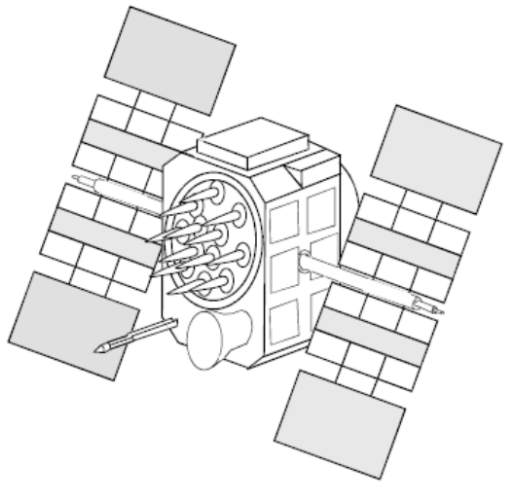
GPS receiver generates the same PRC as satellite, i.e. they start “counting” at the same time.
By determining how far off the satellite and receiver are in their counting, determines difference in time it took for signal to reach receiver.

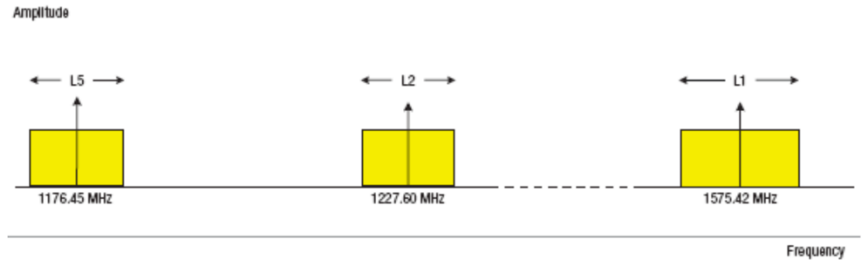
The navigation message

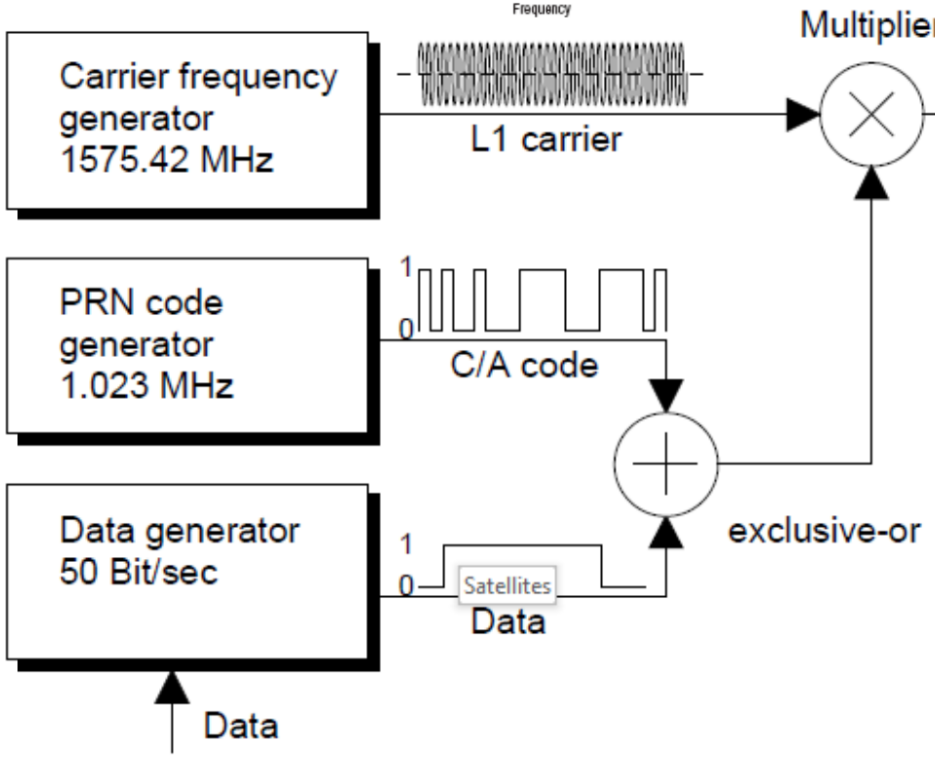
- The navigation message is the data modulated on carrier waves and PRN code.
- The minimum pulse of the data signal is referred to as a bit which is the smallest measurement of transmitted data.
- The navigation message is broadcasted by each satellite at 50 bits per second and provides essential information for positioning solutions.

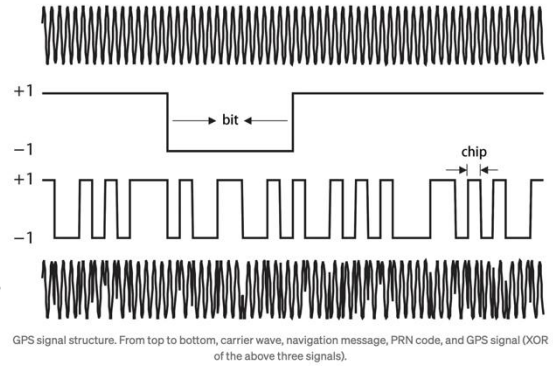
Navigation Data	Contents	Update Frequency
Satellite parameters	Contains signal transmission time, SV health status, etc.	Data will be updated per 2 hours
Ephemeris	Contains detailed orbital information for *each* satellite	Data will be updated per 2 hours
Almanac	Contains inaccurate position over time for *all* satellites	Data will be updated per week approximately

GPS signal structure and signal modelling









GPS signal structure. From top to bottom, carrier wave, navigation message, PRN code, and GPS signal (XOR of the above three signals).

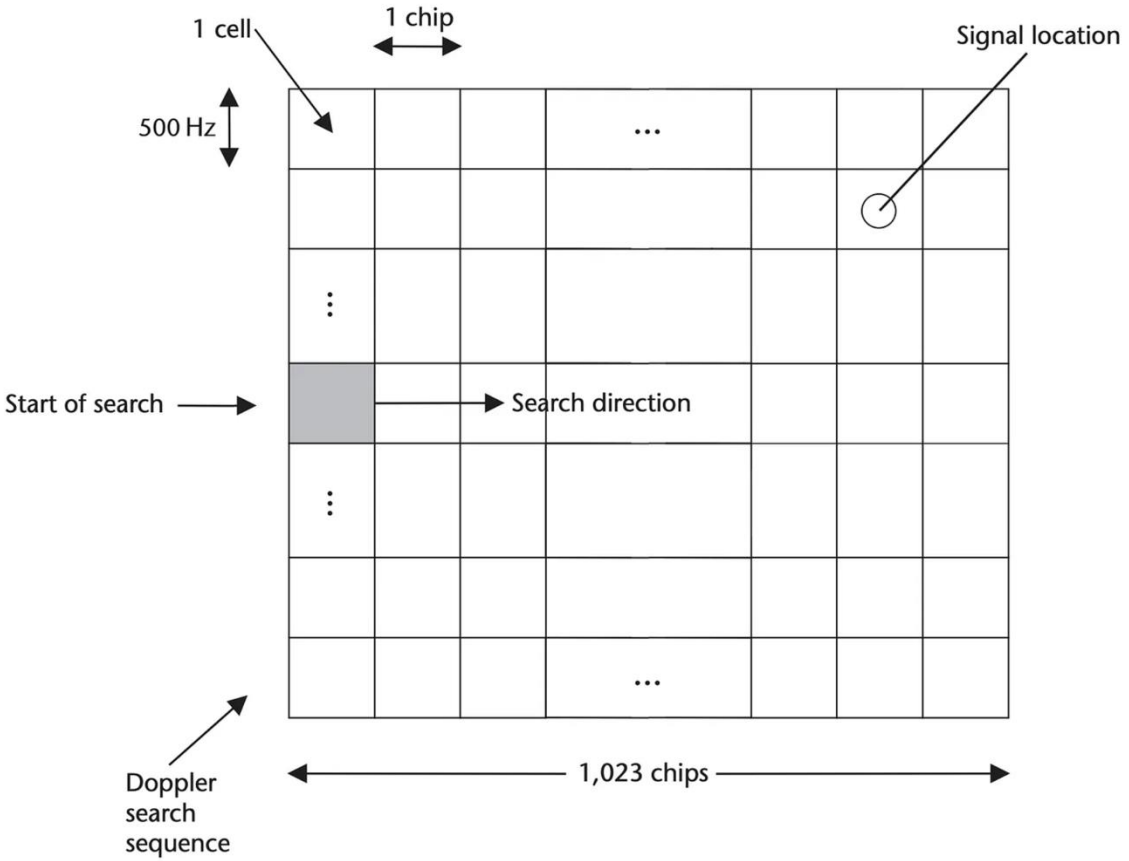
$$y(t) = \mathrm{Re}\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)] e^{j[\omega_c t - \phi_i(t)]}\right\}$$

Acquisition and Tracking

In order to have a correlation peak, receive and copied signals should have the same:

- Carrier wave frequency,
- Carrier wave phase,
- PRN code sequence, and
- PRN code phase.

Signal Acquisition



The total search space is 31 × 41 × 1023 for C/A signal acquisition.

For P code signal, it's even worse given that the P code phase dimension is 6.18×10^{12}!!

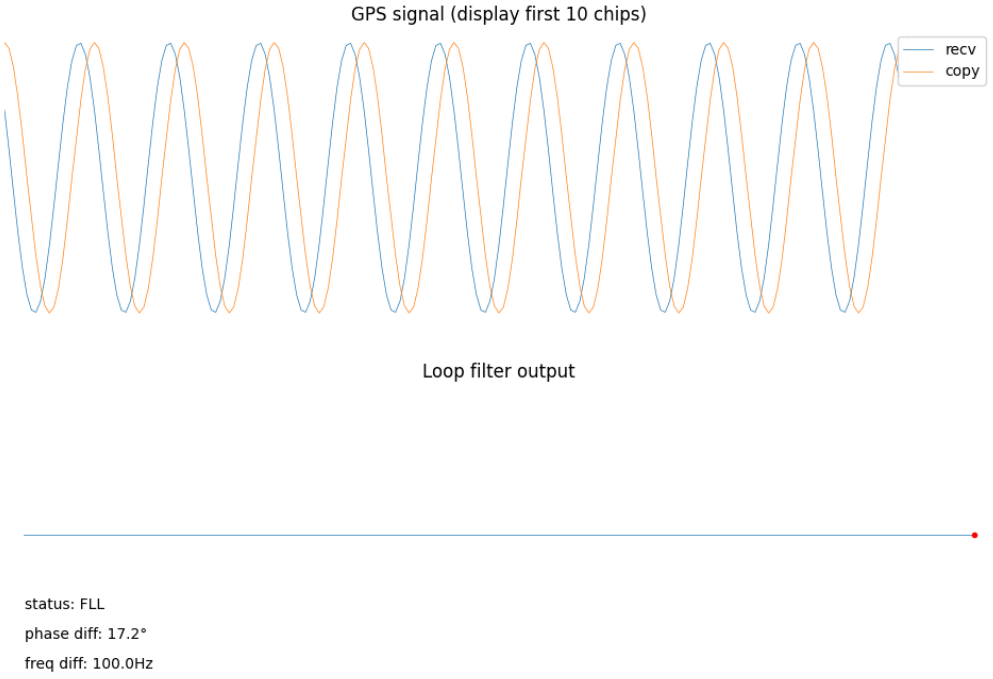
With almanac data including estimated satellite position, the user knows all visible satellites given the user's rough location, reducing one dimension for satellite search.

With ephemeris data, the user could estimate the Doppler shift and code phase in a narrower interval, greatly reducing the remaining 2D search space.

C/A code acquisition as pre-step for P code acquisition

Tracking

- FLL and PLL are used to track carrier wave frequency and phase respectively, thus the generator will generate a sine wave. For FLL, the discriminator will calculate the frequency difference to the received signal and user's copied signal. Similarly, PLL will discriminate phase difference of the two signals.



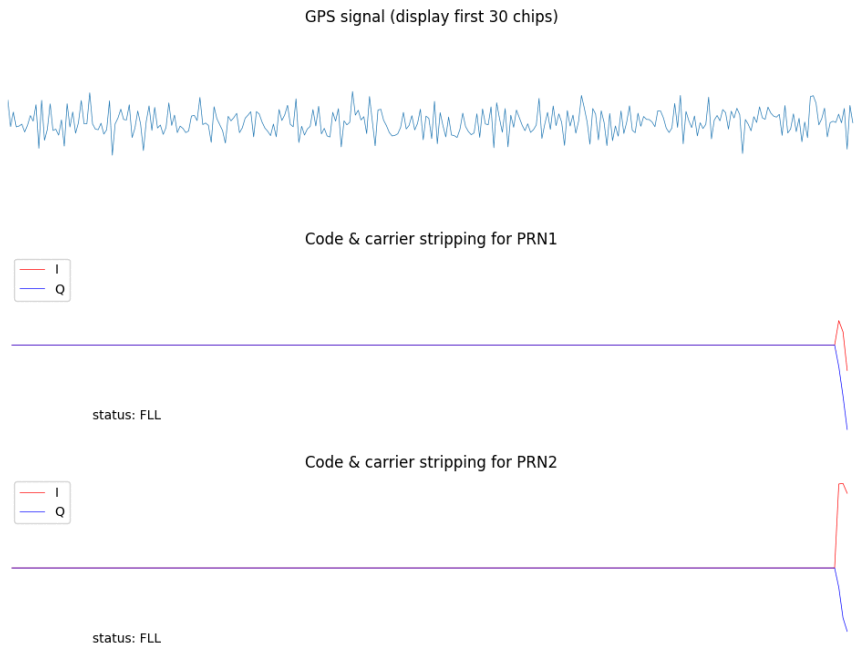
Tracking

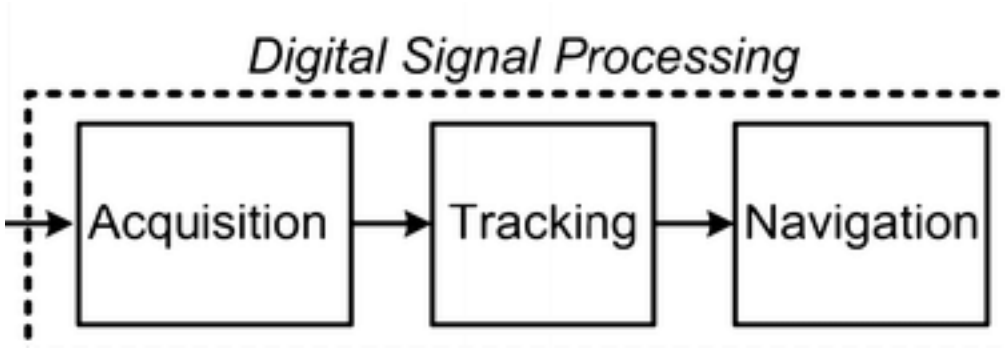
- FLL and PLL are used to track carrier wave frequency and phase respectively, thus the generator will generate a sine wave. For FLL, the discriminator will calculate the frequency difference to the received signal and user's copied signal. Similarly, PLL will discriminate phase difference of the two signals.

- DLL is used to track code phase of the PRN signal, so it generates a code signal and discriminates code phase difference. The purpose is to make sure the present signal locates at the peak of the correlation results when stabilized

Demodulation

- PLL and DLL make sure the copied signal has the maximum correlation with the received signal. Data demodulation is then indicated by correlation result. If the correlation is above 0, the data modulated on the signal is +1, otherwise it's -1.

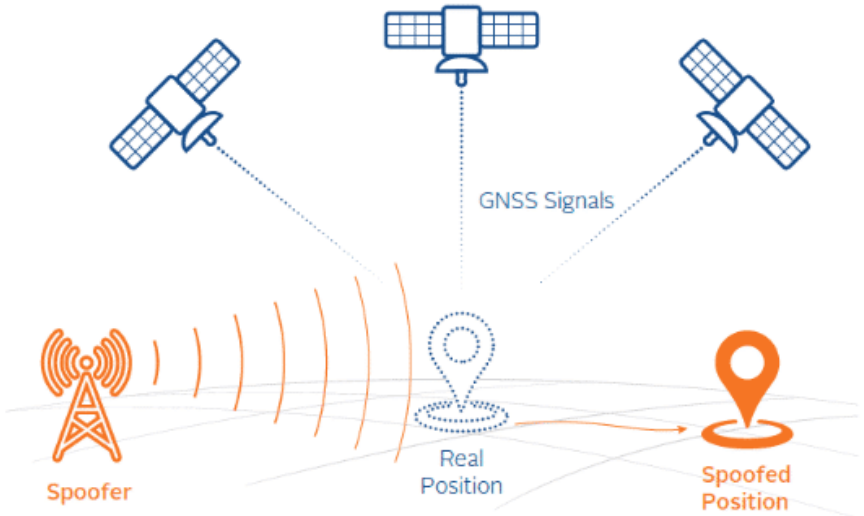


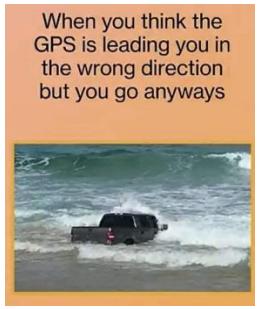


TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

How does a GPS spoofer works?

Scope of a GNSS spoofer

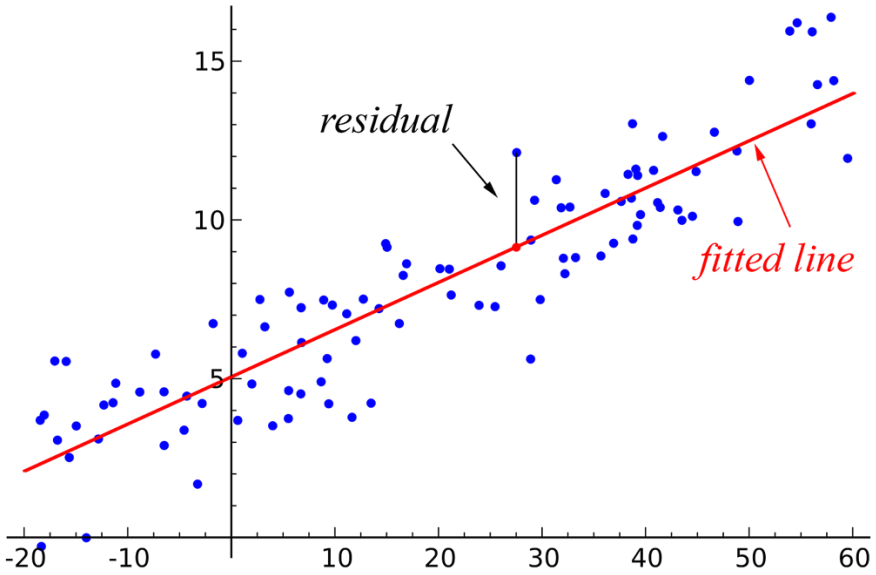




$R_1 = c(t_r + dt - t^s_1) = \|p_r - p^s_1\|$

...

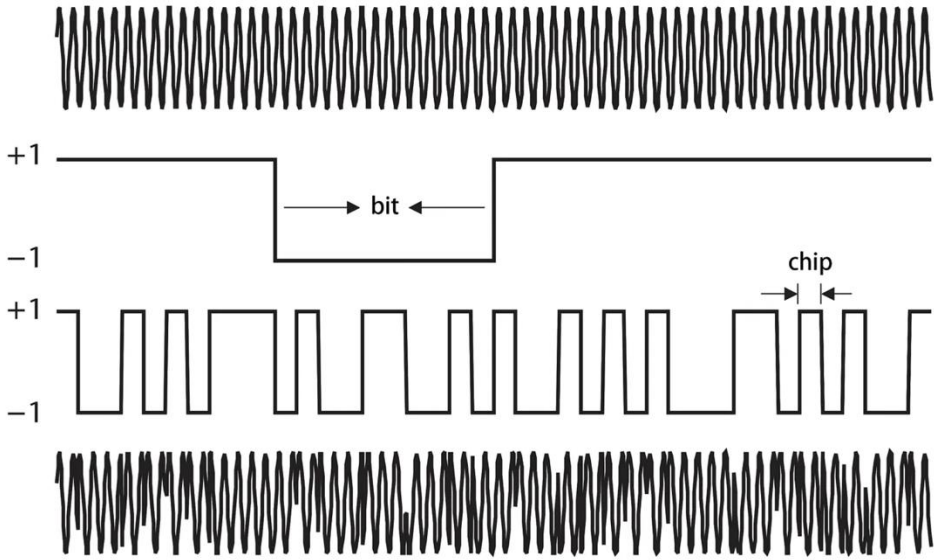
$R_i = c(t_r + dt - t^s_i) = \|p_r - p^s_i\|$



GPS spoofer signal structure

- Description of a GPS spoofer

$$y(t) = \mathrm{Re}\left\{\sum_{i=1}^{N} A_i D_i[t-\tau_i(t)] C_i[t-\tau_i(t)] e^{j[\omega_c t - \phi_i(t)]}\right\}$$



GPS signal structure. From top to bottom, carrier wave, navigation message, PRN code, and GPS signal (XOR of the above three signals).

$$y_s(t) = \mathrm{Re}\left\{\sum_{i=1}^{N_s} A_{si} \hat{D}_i[t-\tau_{si}(t)] C_i[t-\tau_{si}(t)] \times e^{j[\omega_c t - \phi_{si}(t)]}\right\}$$

$$y_{\mathrm{tot}}(t) = y(t) + y_s(t) + \nu(t)$$

A_{si}, $\tau_{si}(t)$, and $\phi_{si}(t)$

spoofed amplitudes, code phases, and carrier phases

Self-consistent spoofing

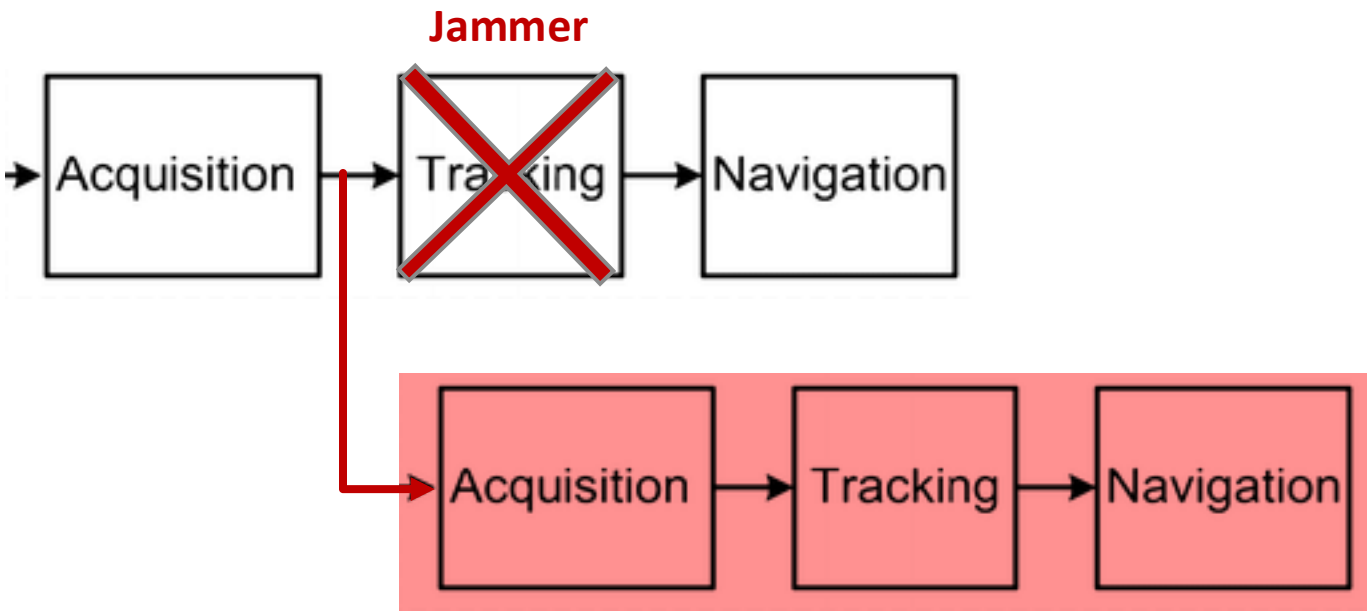
- Self-consistent spoofers design their attacks to defeat the legacy RAIM strategy that considers pseudorange residuals.
- They do this by synthesizing their false code phases $\tau_{s1}(t), \ldots, \tau_{sN_s}(t)$ in a way that induces a desired false position/timing fix at the victim
- The spoofed beat carrier phases are typically designed to vary consistently with the spoofed code phases so that

$$\dot{\omega_c}[\tau_{si}(t_b) - \tau_{si}(t_a)] = [\phi_{si}(t_b) - \phi_{si}(t_a)]$$

- How to lock into the false signal?

Jamming and Re-acquisition

- One is to start by jamming the victim in order to disrupt normal tracking and induce reacquisition.
- Spoofed signals are significantly stronger than the true signals, i.e., $A_{si} \gg A_i$



Capture the victim receiver tracking loops

- Transmit the false signals so that they are code-phase- and Doppler-matched to the true signals at the location of the victim antenna.
- The spoofed power starts low and increases until it suffices to capture the tracking loops. Finally, the spoofer drags off the code and carrier phases in a self-consistent way
- By avoiding the need for jamming and reacquisition, this latter method has a better potential to avoid detection

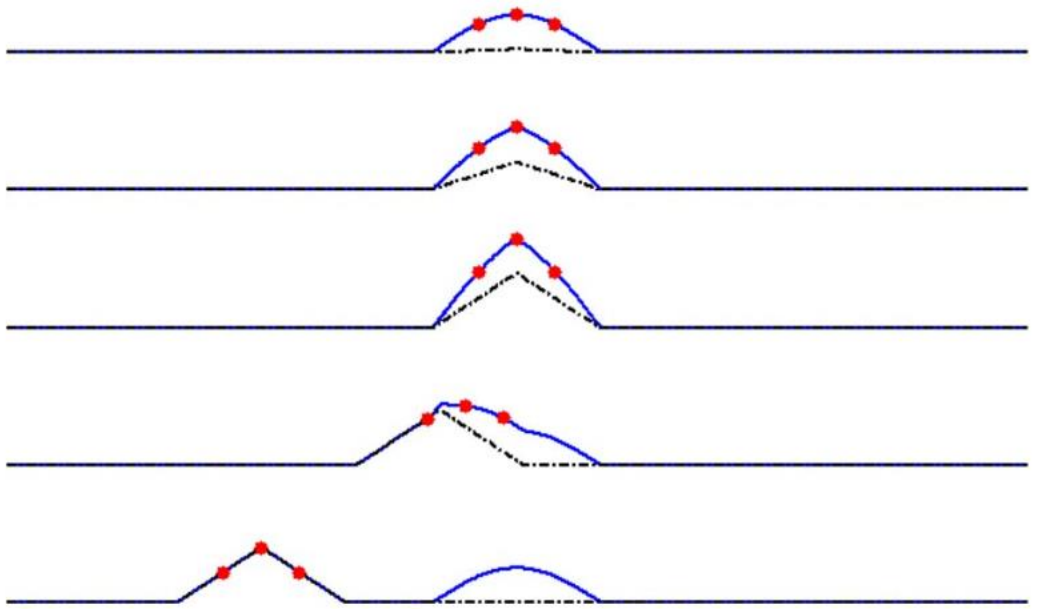


Fig. 1. ***Receiver/spoofer attack sequence viewed from a victim receiver channel. Spoofer: black dash-dotted curve; sum of spoofer and truth: blue solid curve; receiver tracking points: red dots.***

Capture the victim receiver tracking loops

- Transmit the false signals so that they are code-phase- and Doppler-matched to the true signals at the location of the victim antenna.

$$A_{si} \approx 0 \text{ and } \tau_{si}(t) \approx \tau_i(t)$$

$$\tau_{si}(t) = \tau_i(t) \qquad A_{si} > A_i$$

- Therefore, the spoofer must also be a receiver and know its geometric relationship to the victim in order to extrapolate from its received amplitude and code phase values to those of the victim.

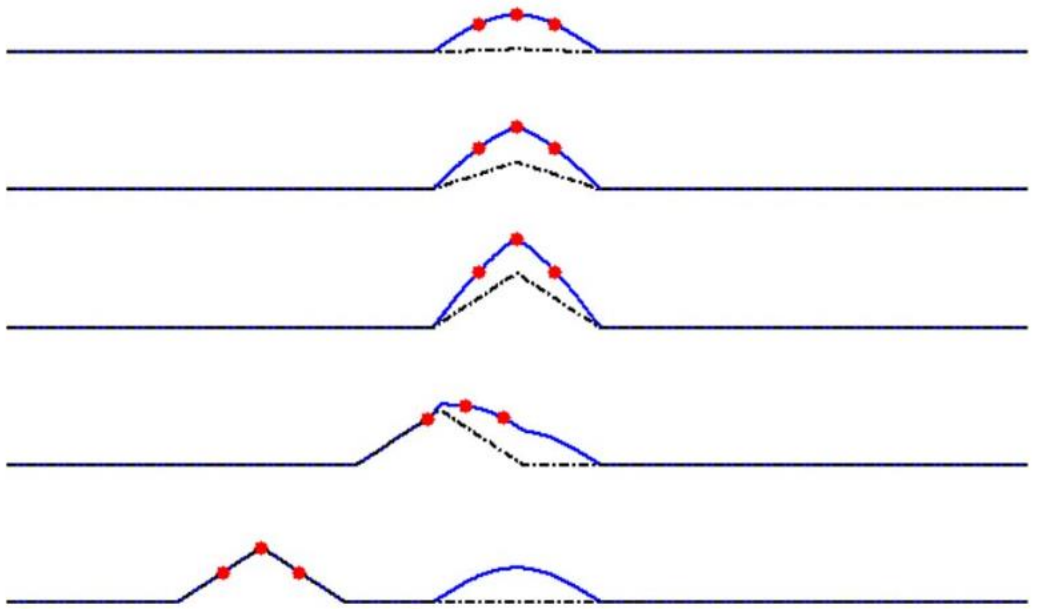


Fig. 1. ***Receiver/spoofer attack sequence viewed from a victim receiver channel. Spoofer: black dash-dotted curve; sum of spoofer and truth: blue solid curve; receiver tracking points: red dots.***

Challenges

- Recreate the transmitted spreading code C and the transmitted data bit stream D, which are easy to synthesize if they are perfectly predictable.
- If not predictable, the spoofer must synthesize approximate replicas of C and D “on the fly” based on noisy received versions of them.
- The U.S. GPS includes military signals that have encrypted spreading codes. A secure military receiver has the necessary key, but a spoofer presumably does not

Meaconing Attack

- Meaconing records the true GNSS signals and replays the signals through a transmitter with enough gain to overwhelm the true signal at the victim antenna. A meaconer has the potential to spoof any GNSS signal, even an encrypted military signal.

- The simplest meaconer/spoofer uses a single reception antenna.

- The victim receiver's false position fix will be that of the spoofer's reception antenna. Its false clock fix will deduce a false time that will be earlier than true time

$$\tau_{si}(t) > \tau_i(t)$$

- A meaconer has the potential to spoof any GNSS signal, even an encrypted military signal.

Meaconing Attack

- A more sophisticated meaconer might use multiple receiver antennas and phased-array signal processing.
- Individual record-and-replay channels could point increased gain at individual GNSS satellites and could implement independent delay variations.
- Such a system could independently steer the relative delays of its false transmissions to produce any conceivable false position fix.

$$\tau_{si}(t) > \tau_i(t)$$

- Constraint on the relationship between the spoofed clock fix and the spoofed position fix.

Security Code Estimation and Replay (SCER)

- The spoofer estimates D, the unpredictable bits, and it broadcasts them as soon as it has reliable estimates.
- Such a system allows the spoofer to use arbitrary relative delays between the different spoofed channels. Unlike the meaconer, it would not need to use a multielement receiver antenna with independently steerable gains in order to induce an arbitrary spoofed location.

Advanced forms of Spoofing

- **Nulling**: The spoofer transmits two signals for each spoofed signal. One is the spoofed version that acts in concert with all other spoofed signals in order to induce a false position/timing fix. The other is the negative of the true signal.
- **Multi-antenna spoofer**: An advanced spoofer acting against a multiantenna victim receiver might use multiple independent spoofer transmission antennas and match each one to a corresponding receiver antenna. The relative geometry of each spoofer/victim antenna pair would need to be known
- The requirement of physical reasonableness forces the spoofer to be patient.

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

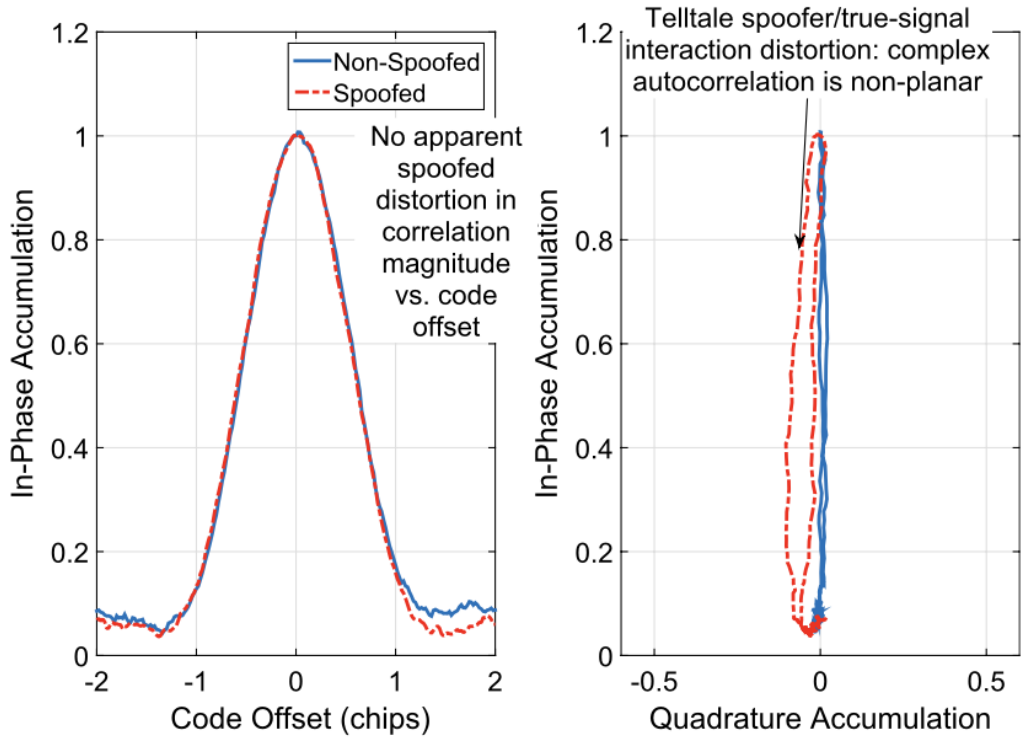
Defense against GPS spoofers

Spoofing detection

- One method is to look for differences between the spoofed signals and the true signals, differences that can be detected by the intended victim receiver. Despite the public definition of civilian GNSS signals, there are usually noticeable differences of spoofer signals unless the spoofer is sophisticated and expensive.
- The other method is to look for interaction between the true and spoofed signals. Interaction is unavoidable for the spoofer except in two situations. One is a nulling attack. The other situation is a vastly overpowered attack.
- An overpowered attack, however, has an obvious difference from the expected power levels of true signals. Thus, good detection strategies are typically multipronged, e.g., combining power monitoring with some form of interaction monitoring.

Spoofing detection

Another technique looks in detail at the complex correlation function from which a receiver synthesizes discriminators for its tracking loops. During the initial drag-off of a spoofing attack, misalignments between the true and spoofed code and carrier phases result in distorted autocorrelation functions.

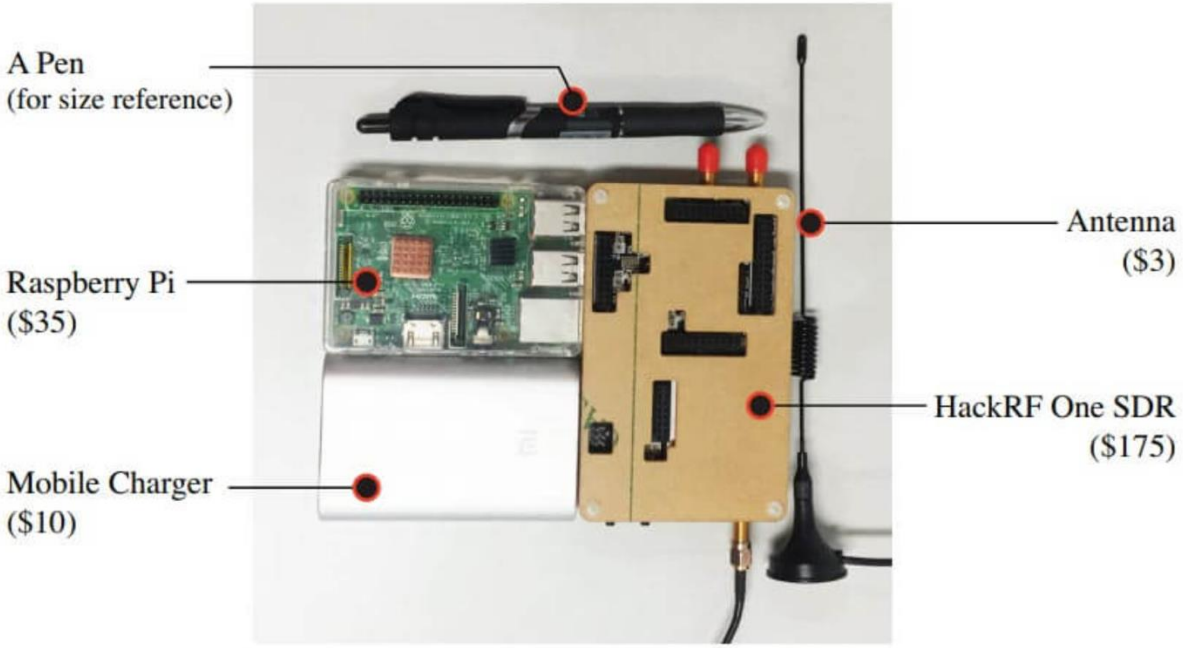


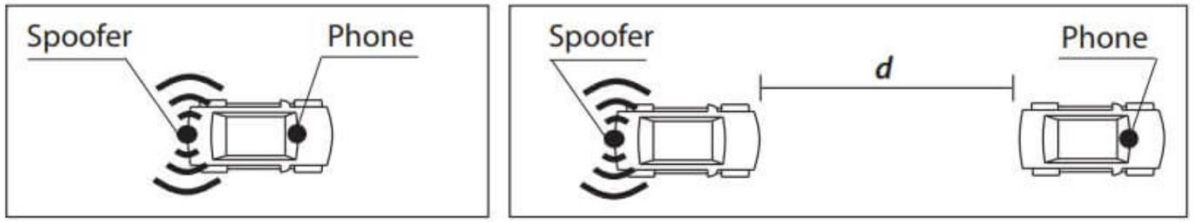
Other defense mechanisms

- Drift monitoring
- Encryption
- Signal-Geometry-Based Defenses

Todd Humphreys assembles a GPS spoofer at home in 2009

Today

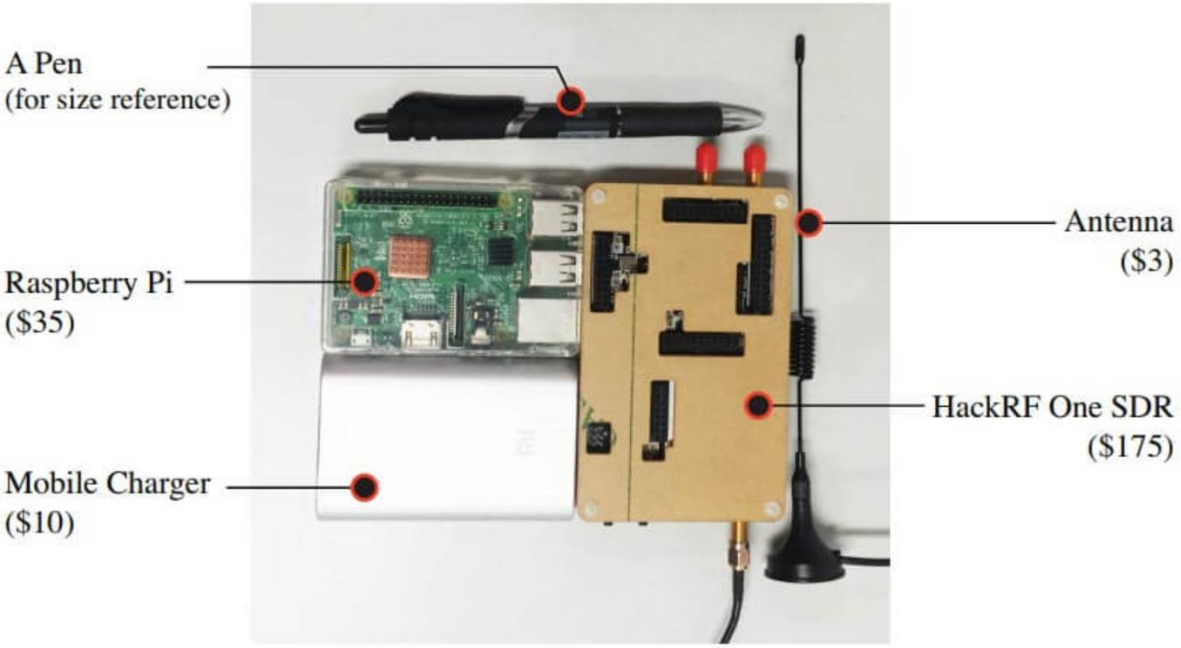


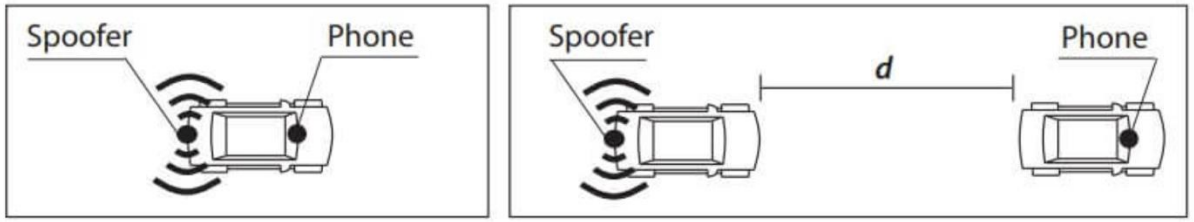


(a) Same-car Test (b) Two-car Test

Hardware and Method used to Spoof Car GPS Navigation.

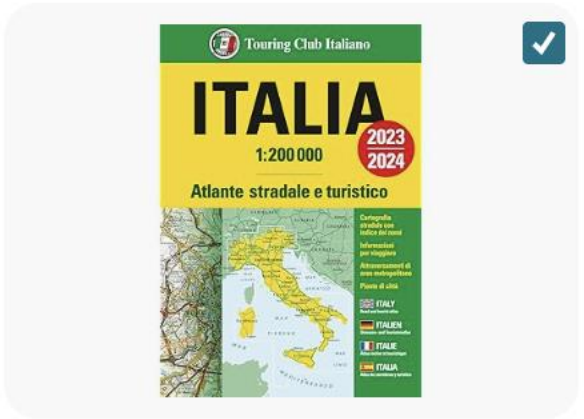
Today





(a) Same-car Test (b) Two-car Test

Hardware and Method used to Spoof Car GPS Navigation.



Questo articolo: Italia. Atlante stradale e turistico. 1:200.000. Ediz. multilingue

21,75 €

tony red

★★★★★ **Unico**

Recensito in Italia il 29 agosto 2024

Acquisto verificato

Ottimo! Questa è la terza edizione che acquisto, perché negli anni ovviamente gli atlanti invecchiano, ma è insostituibile soprattutto per capire dove stai andando

Utile | Segnala

Sources

- M. L. Psiaki, T. E. Humphreys and B. Stauffer, "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," in *IEEE Spectrum*, vol. 53, no. 8, pp. 26-53, August 2016
- M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258-1270, June 2016
- https://medium.com/@penrosewang/introduction-to-gnss-ii-gps-signal-processing-dd9eae0bdade

TOR VERGATA

UNIVERSITÀ DEGLI STUDI DI ROMA