https://unsplash.com/photos/cQWXGcHwVrg

3 – Global Navigation Satellite Systems (GNSS) Security

What is GNSS?

A long-stating problem

https://unsplash.com/photos/emH2e5SBifE (cut and annotated)

Problem

Estimating your position on the Earth

You need some reference

- Position of Sun, stars at night, etc.
- Time here (check the Sun) vs. time at departure (check your clock)
- Etc.

Keeping time is yet another non-trivial problem

Fascinating History, The Longitude Act

Clock that changed the world (H4, 1759)

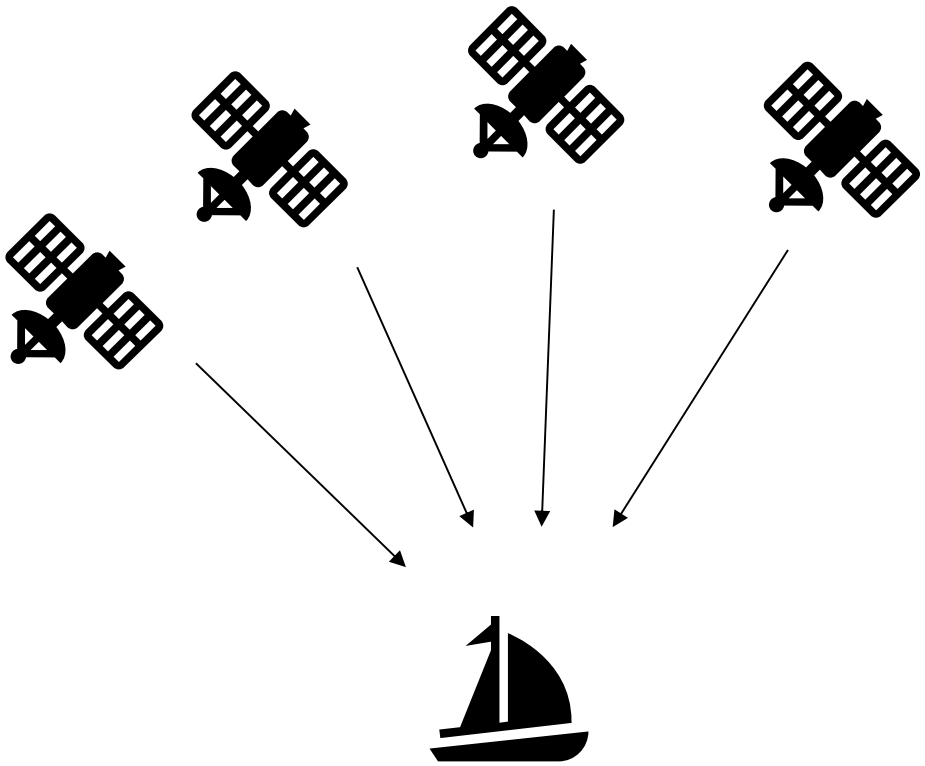
Problem

- Keep time of departure point at Sea
- So that you can estimate your Longitude

The Longitude Act

- 1714, UK Parliament establishes a prize
- 1765, John Harrison wins

GNSS, a modern solution for position & time



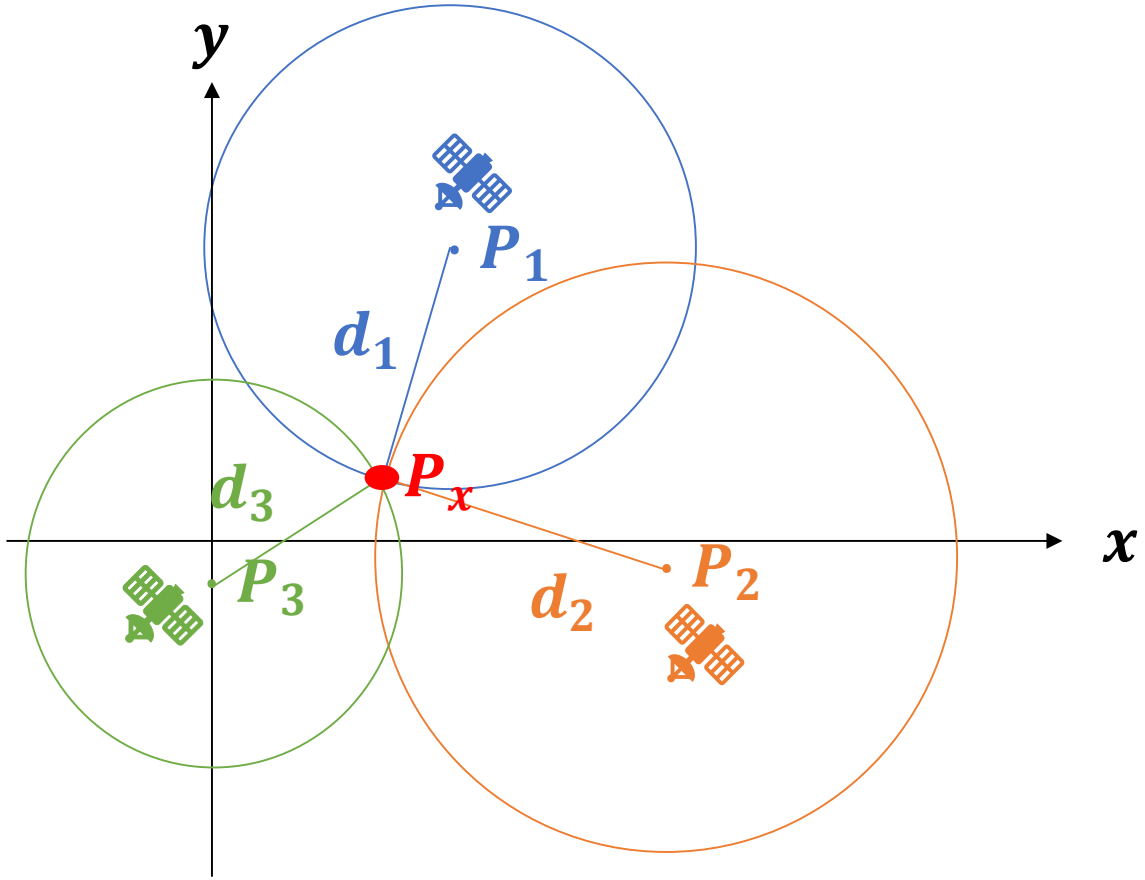
The principle

- Artificial constellation of satellites as reference
- Trilateration to find the position of the receiver

Many implementations

- GPS
- Galileo
- Glonass
- Beidou
- …

Trilateration, the intuition



Trilateration

- In 2D, if you know your distance from 3 points you can uniquely identify your position at the intersection of 3 circles
- Can be easily extended to the 3D case with spheres instead of circles

In practice, using time-of-flight

- t_s
- $S_i = (x_i, y_i, z_i)$

Known orbits
Atomic clocks
Correction from ground station

- $d_i = |S_i^{\text{satellite}} - X^{\text{receiver}}|$
- $d_i = c\Delta t^i$

Time of flight estimate
Unknown clock error
(Cheap inaccurate clock)

- $t_r^i = t_s + \Delta t^i + \delta t$
- $X = (x, y, z)$

Unknown position

In practice, using time-of-flight

- t_s
- $S_i = (x_i, y_i, z_i)$

- $d_i = |S_i - X|$
- $d_i = c\Delta t^i$

- $t_r^i = t_s + \Delta t^i + \delta t$
- $X = (x, y, z)$

"Pseudo-range"

$$\rho_i = \left(t_r^i - t_s\right)c$$

$$= \left(\left(t_s + \Delta t^i + \delta t\right) - t_s\right)c$$

$$= c\Delta t^i + c\delta t$$

$$= |S_i - X| + c\delta t$$

In practice, using time-of-flight

- t_s
- $S_i = (x_i, y_i, z_i)$

- $d_i = |S_i - X|$
- $d_i = c\Delta t^i$

- $t_r^i = t_s + \Delta t^i + \delta t$
- $X = (x, y, z)$

$$
\begin{cases}
(t_r^1 - t_s)c = |S_1 - X| + c\delta t \\
(t_r^2 - t_s)c = |S_2 - X| + c\delta t \\
(t_r^3 - t_s)c = |S_3 - X| + c\delta t \\
(t_r^4 - t_s)c = |S_4 - X| + c\delta t
\end{cases}
$$

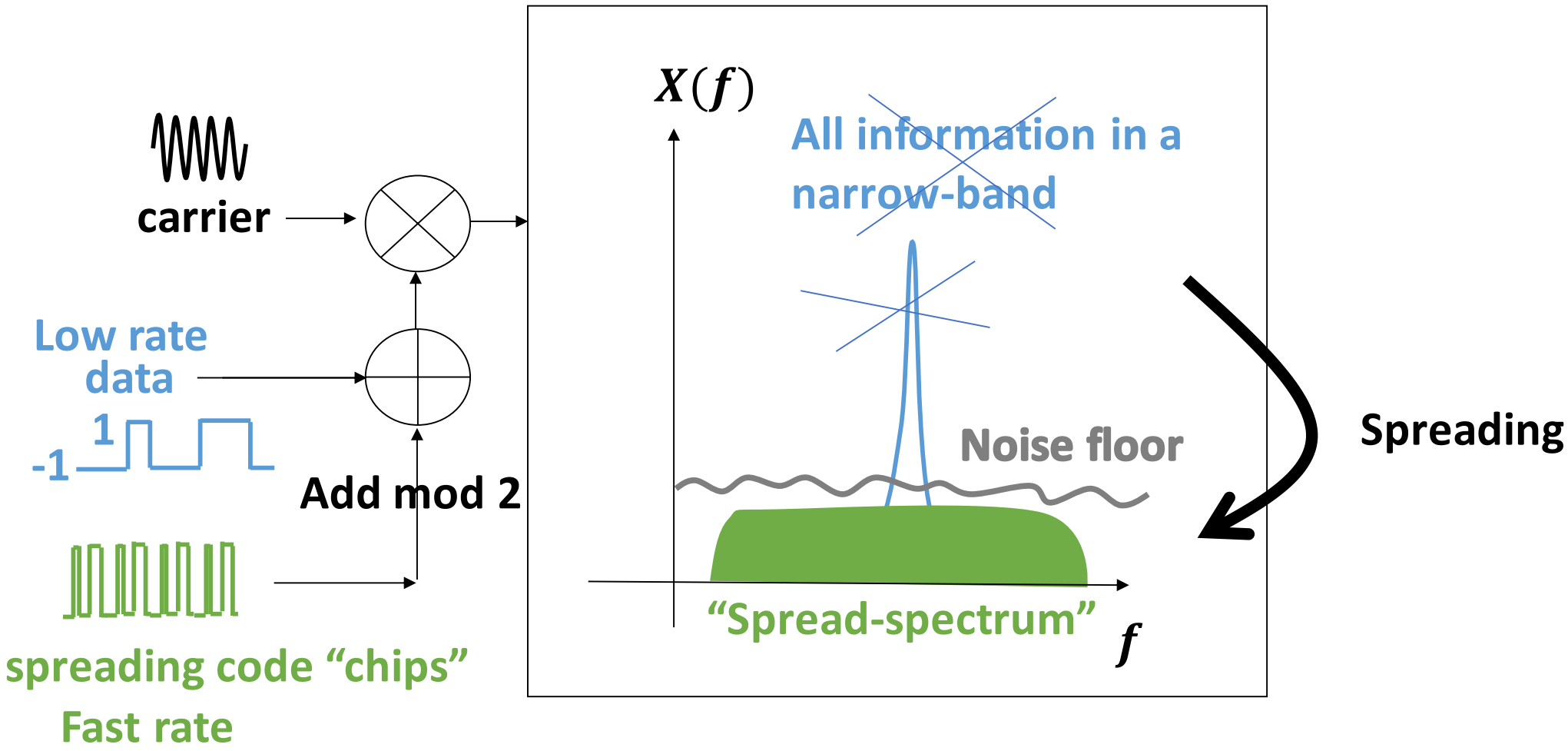
System of equations

- 4 unknowns $((x, y, z), \delta t)$
- At least 4 equations for solution
- Approximate numerical solution using Taylor series
- Estimate both position & time!
- Position Velocity Time (PVT)

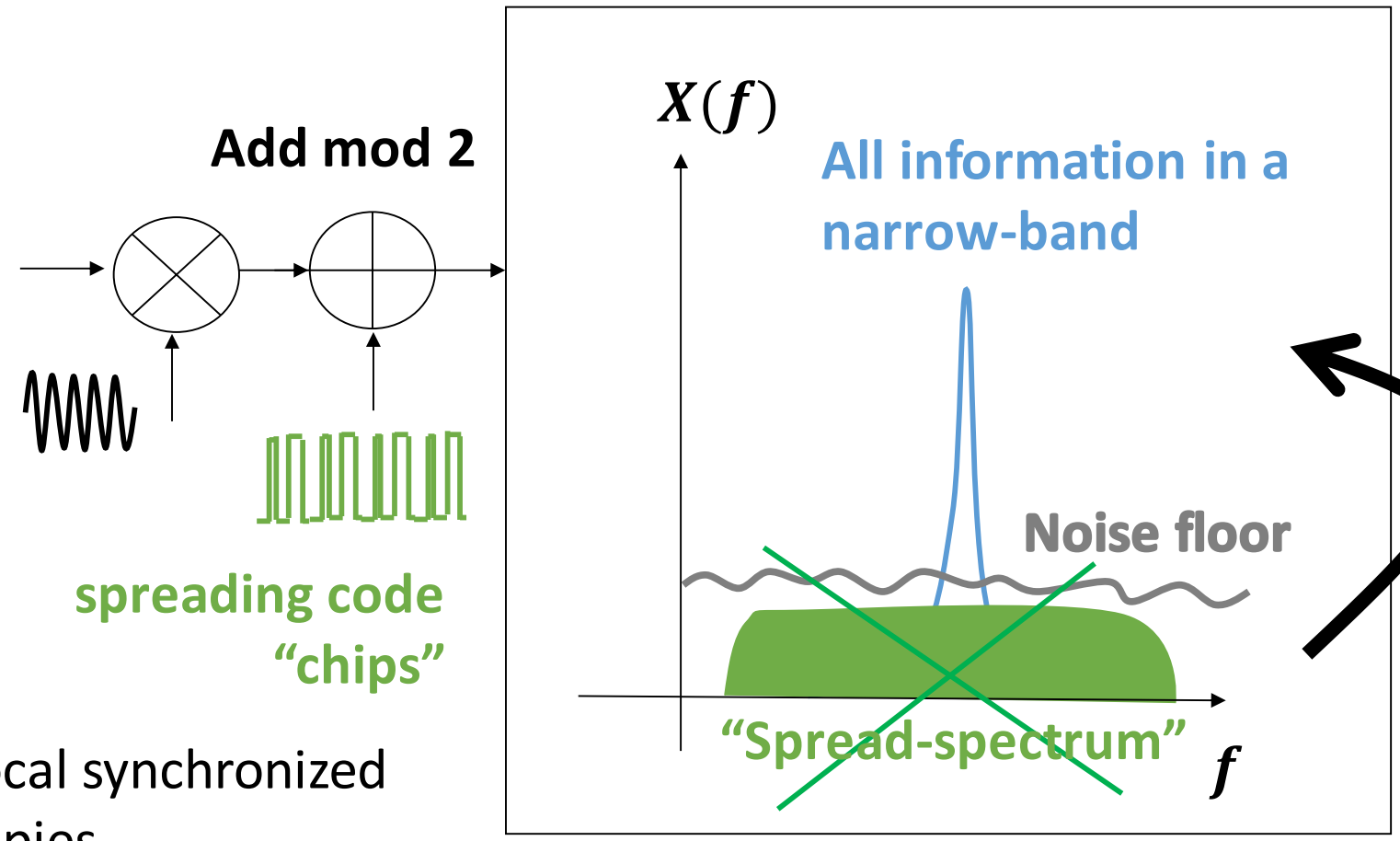
How is it implemented with radio signals?

DSSS Recap (TX)

For GNSS the data bits are navigation data with information about the satellite



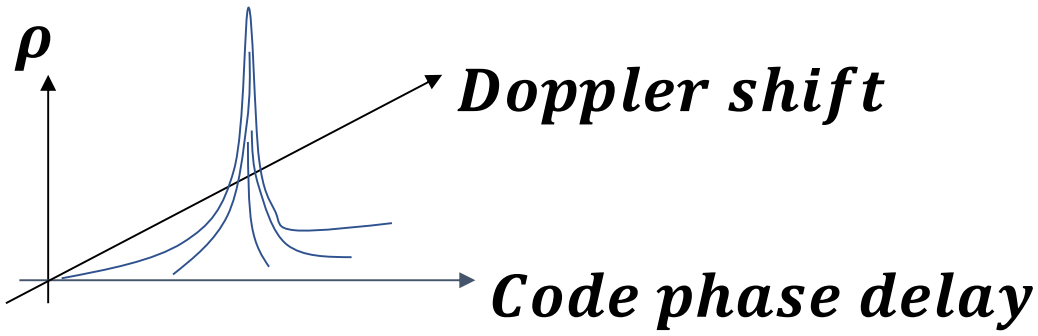
DSSS Recap (RX)



Processing gain:
chip rate / symbol rate

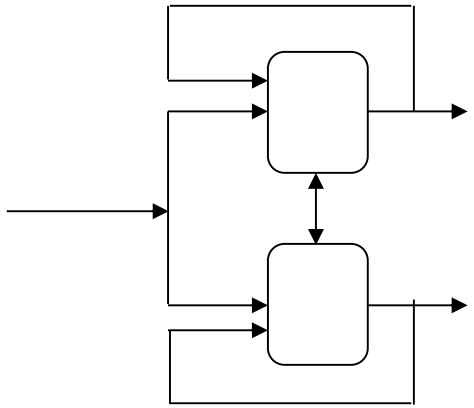
De-spreading
"Digging the signal out of noise"

DSSS Recap (Acquisition and Tracking)



Use cross-correlation!

- Compare local copy of the spreading code for each possible frequency shift and time delay
- Find the peak
- Bonus: you known **when** the signal arrived compared to your local time reference



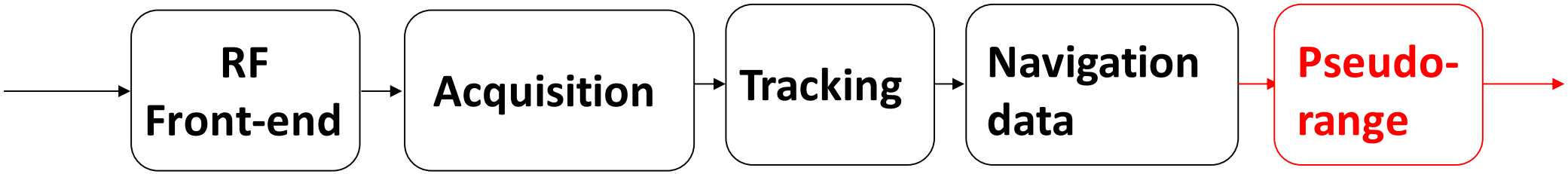
Local carrier

Local spreading code

Use control loops!

- Use a feedback loop to keep tracking shifts in time and frequency
- Bonus: use the local copy to de-spread and **get the navigation data bits**

Putting all together: the receiver



One channel for each satellite

Find the pseudo-range later used to compute the PVT solution

Types of start at the receiver

The intuition
The more the receiver knows the faster it can lock on the satellites in view and get a new position

Faster

Cold start
Start from scratch

Warm start
Remember last calculated position, almanac, UTC time

Hot start
Remember last calculated position, almanac, UTC time
Remember last satellites in view

+ Assisted GPS (A-GPS)
Get help from the cellular network

- Download data (e.g., ephemeris)
- Estimate of position (e.g., triangulation from cell towers)

References

Ublox GPS compendium. https://www.u-blox.com/sites/default/files/gps_compendiumgps-x-02007.pdf

Kai Borre et al., A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach (Springer Science & Business Media, 2007). https://www.ocf.berkeley.edu/~marsy/resources/gnss/A%20Software-Defined%20GPS%20and%20Galileo%20Receiver.pdf

Gnss-Sdr, n.d., https://gnss-sdr.org/.

osqzss, Gps-Sdr-Sim, 2015, https://github.com/osqzss/gps-sdr-sim.

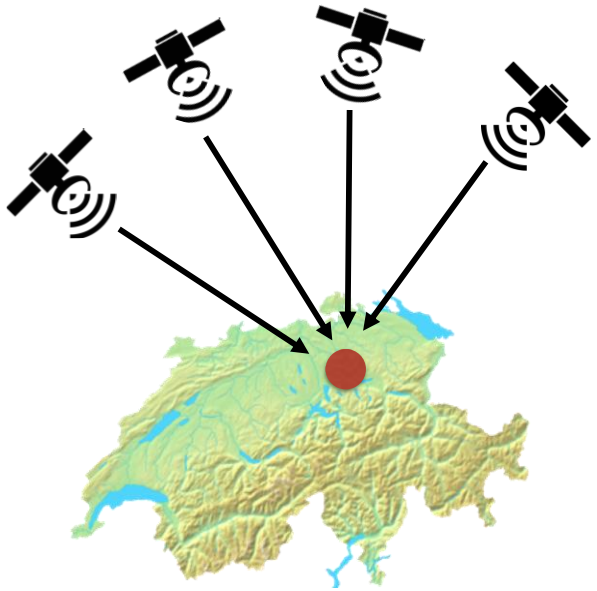
Free books recommended for in-depth understanding

Open-source code for RX and TX to put in practice (no need for hardware you can simulate)

Refer to the official specifications for details, for example for Galileo: https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf

More about GPS

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

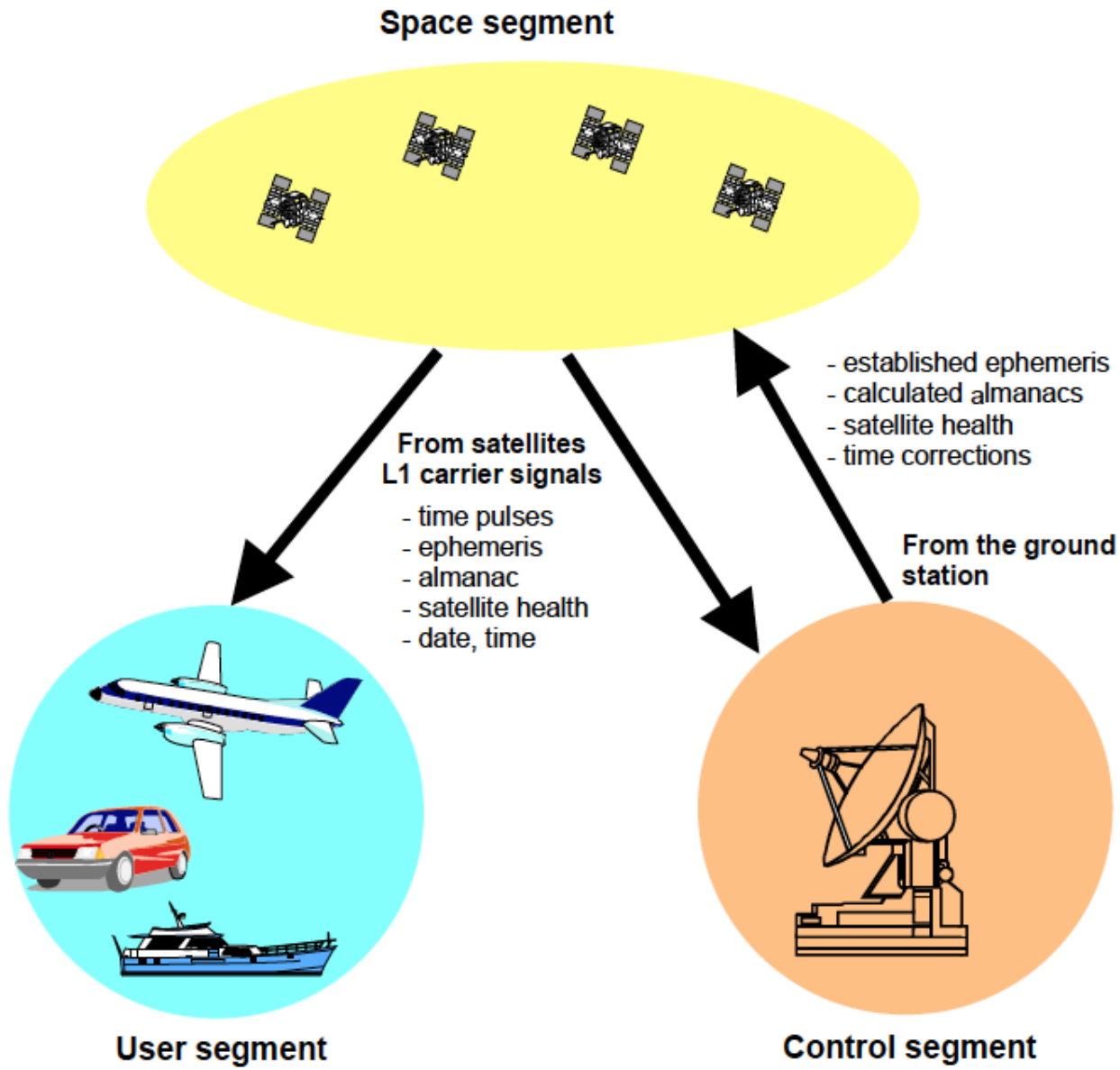
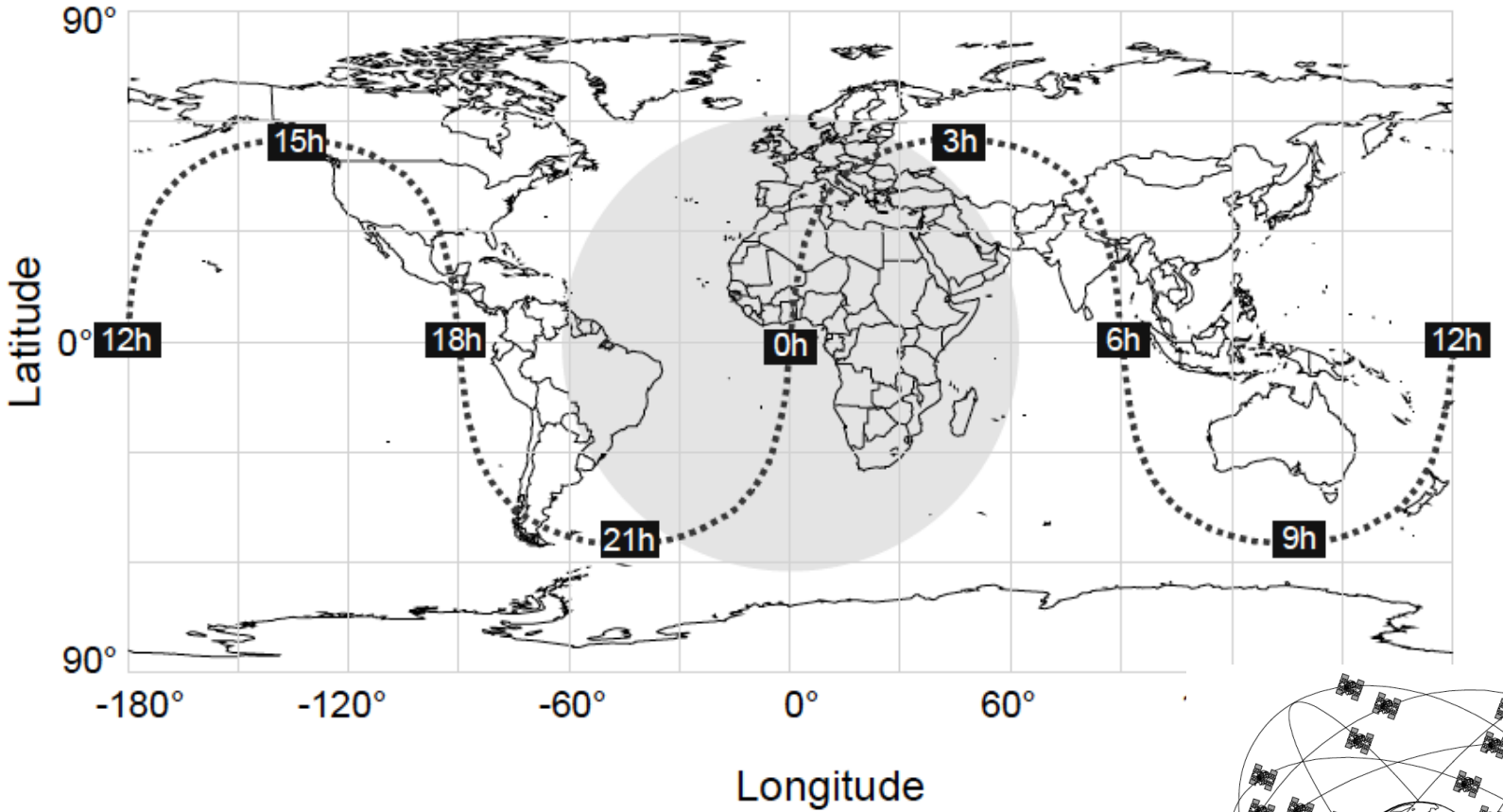
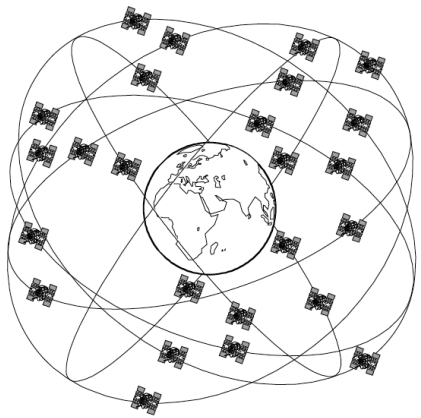


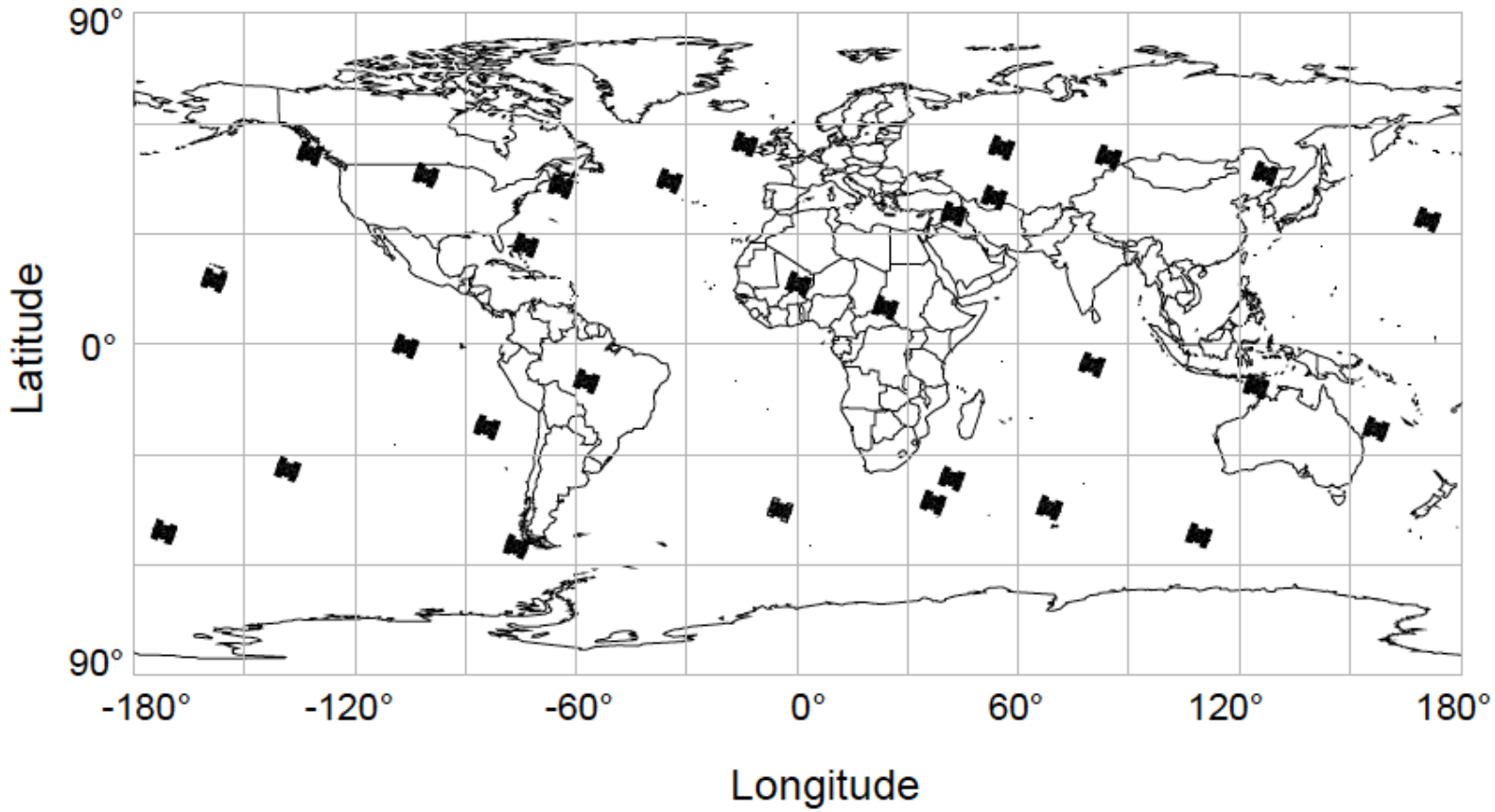
Figure 34: The three GPS segments

GPS

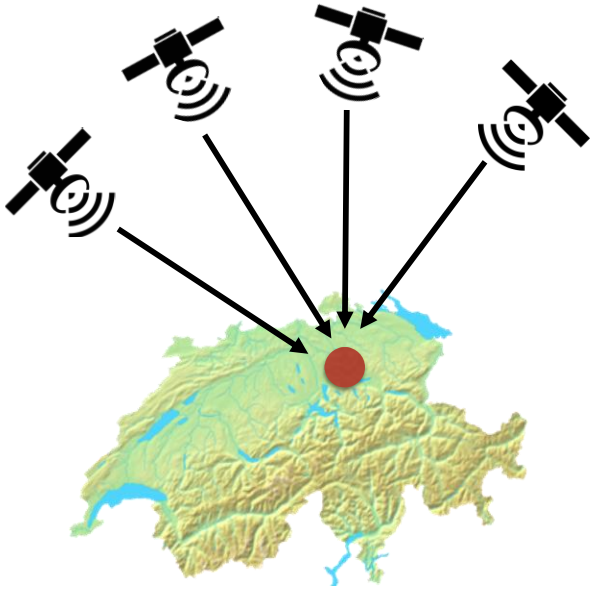

90°
0°
90°
Latitude
-180°
-120°
-60°
0°
60°
Longitude
15h
12h
18h
21h
0h
3h
6h
9h
12h

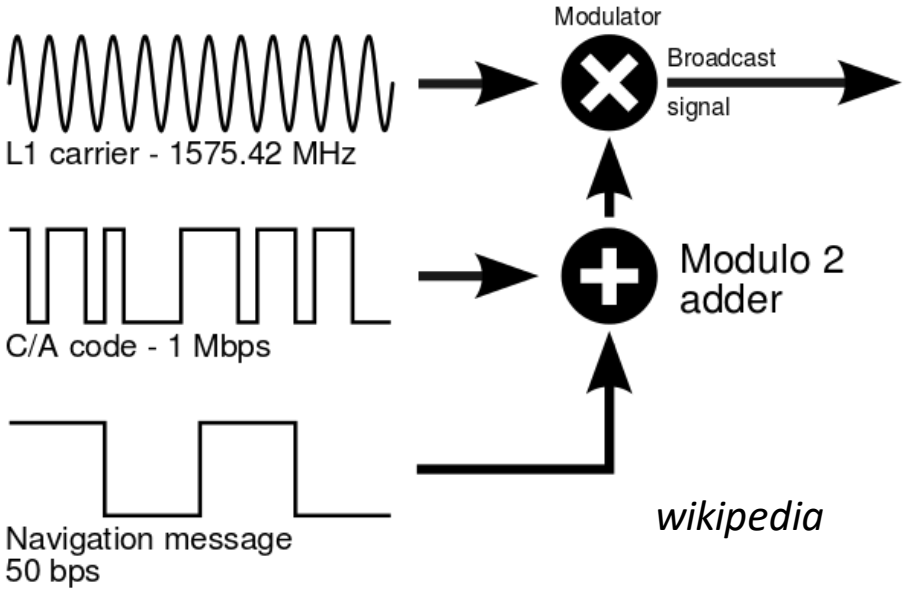


GPS



Global Positioning System (GPS)





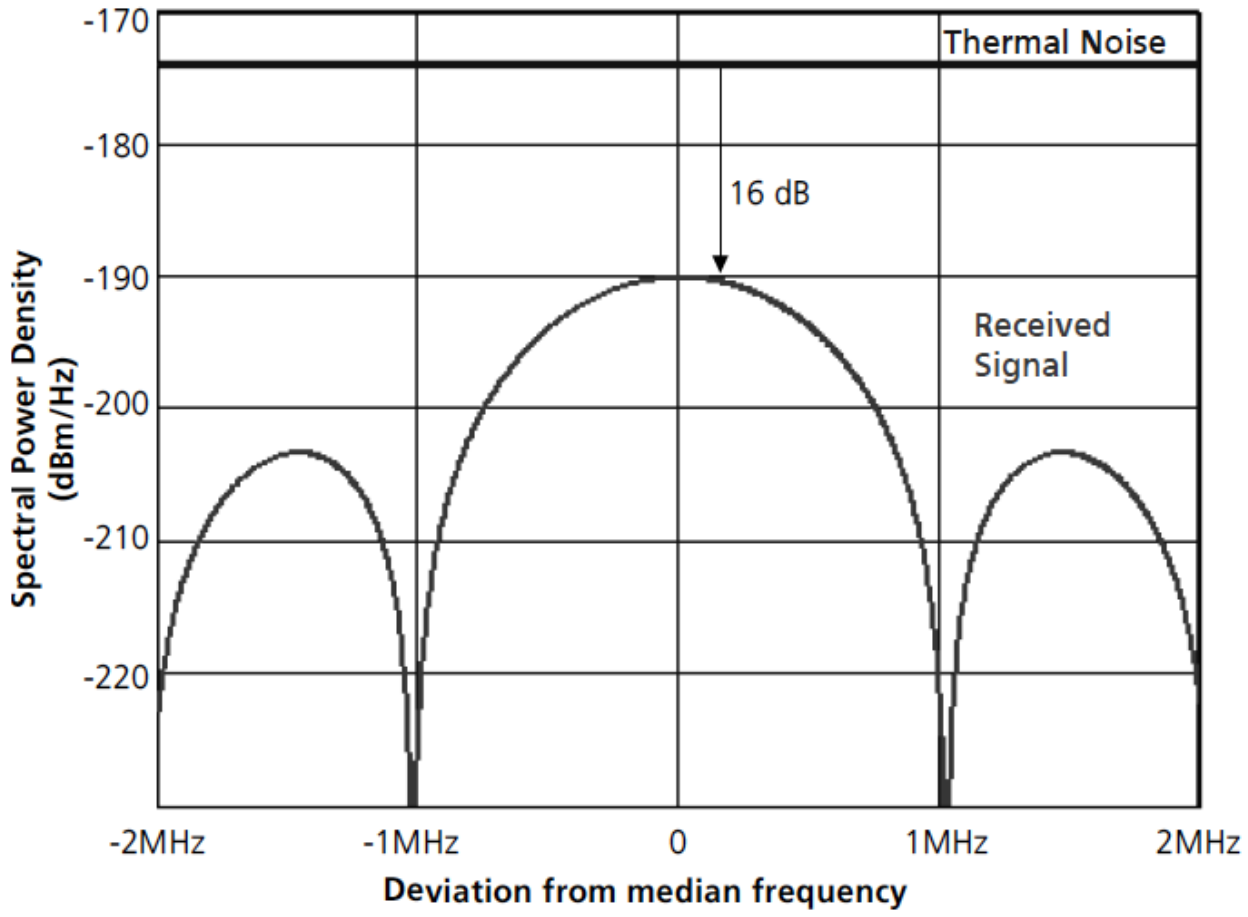
1575.42 MHz (L1);
1227.60 MHz (L2).

- **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

	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)

GPS


-170
-180
-190
-200
-210
-220
Thermal Noise
16 dB
Received
Signal
Spectral Power Density
(dBm/Hz)
-2MHz
-1MHz
0
1MHz
2MHz
Deviation from median frequency

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) (satellite location)
- 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).

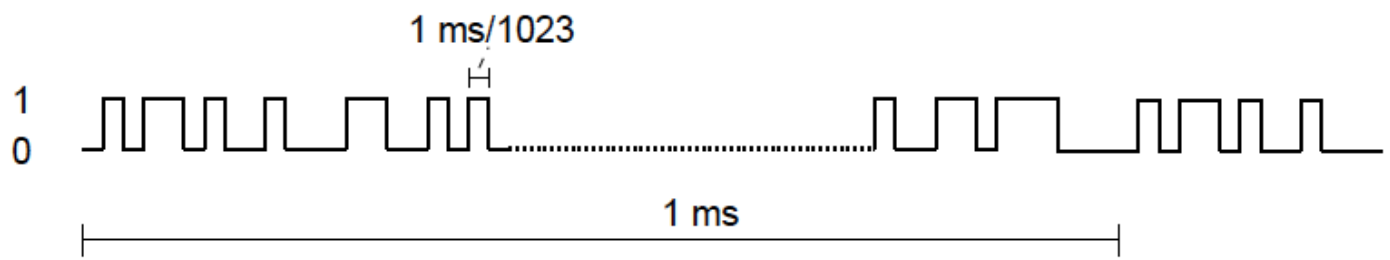


Figure 40: Pseudo Random Noise (PRN)

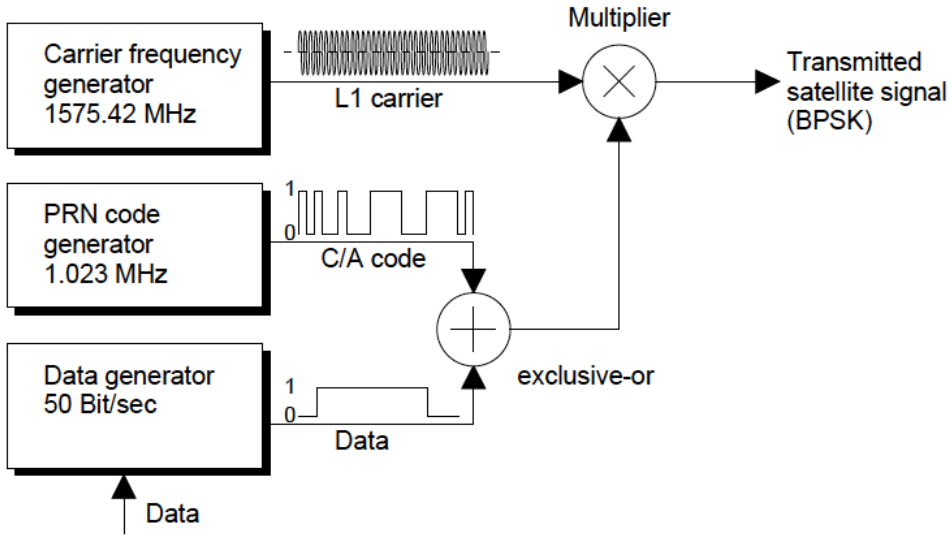


Figure 41: Simplified satellite block diagram

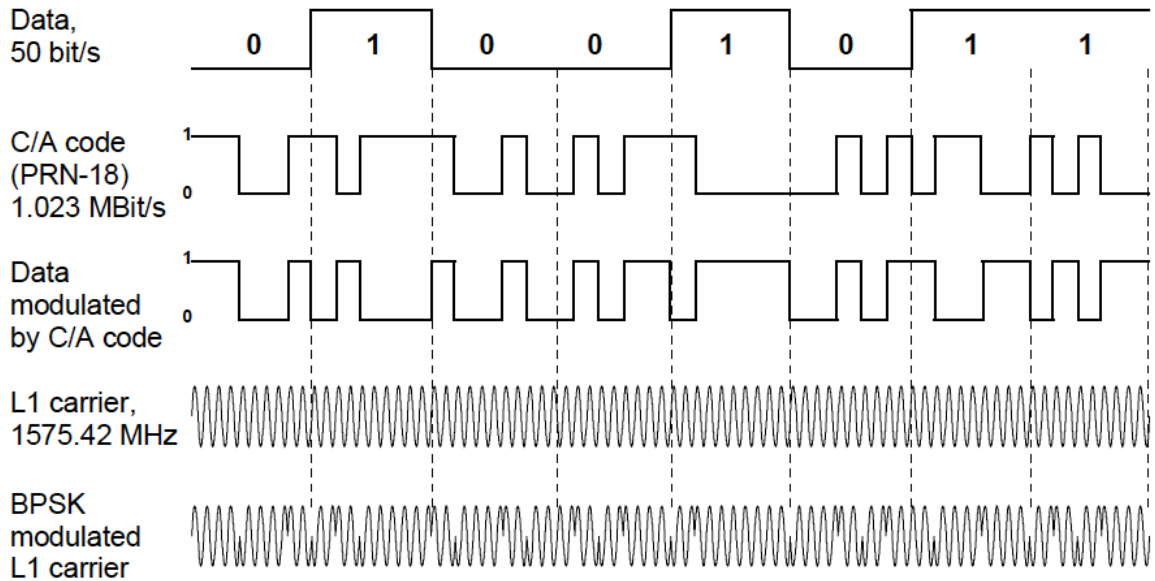


Figure 42: Data structure of a GPS signal

GPS

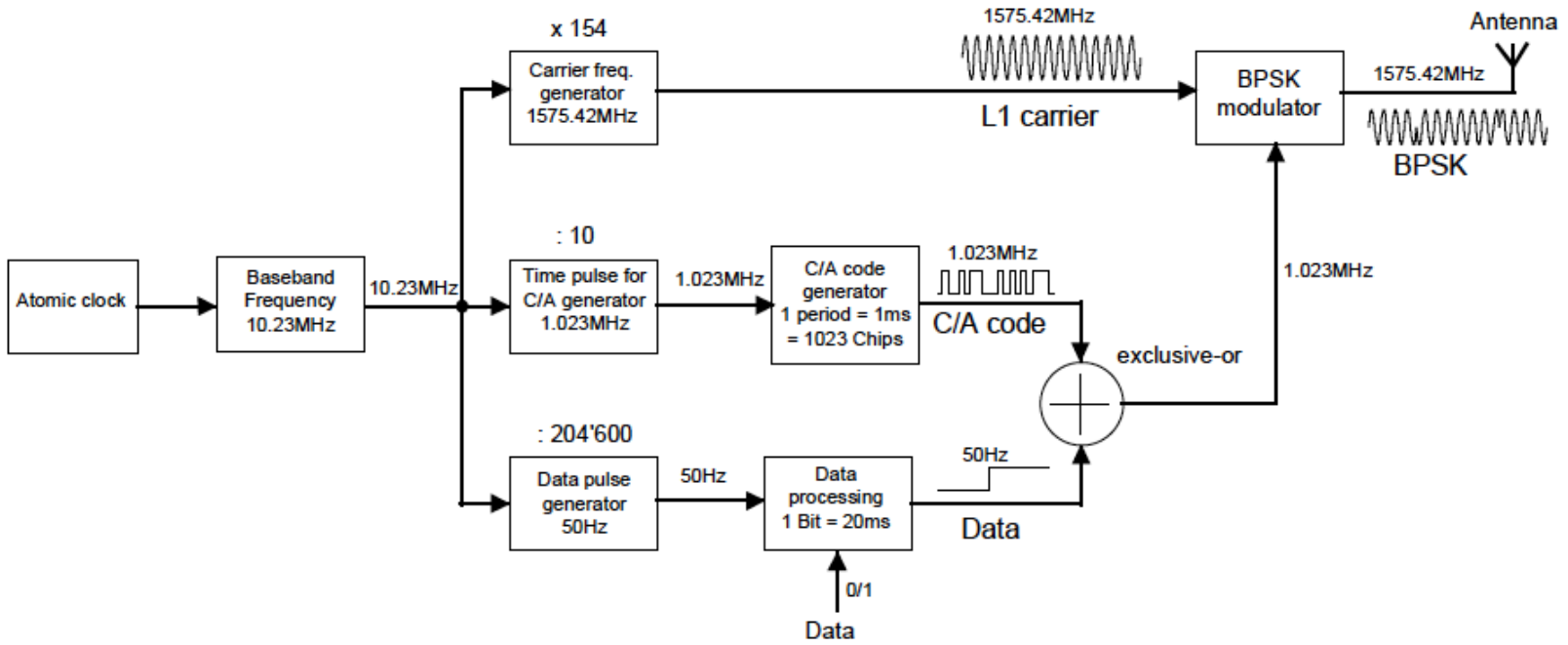


Figure 43: Detailed block diagram of a GPS satellite

GPS: Time of Arrival

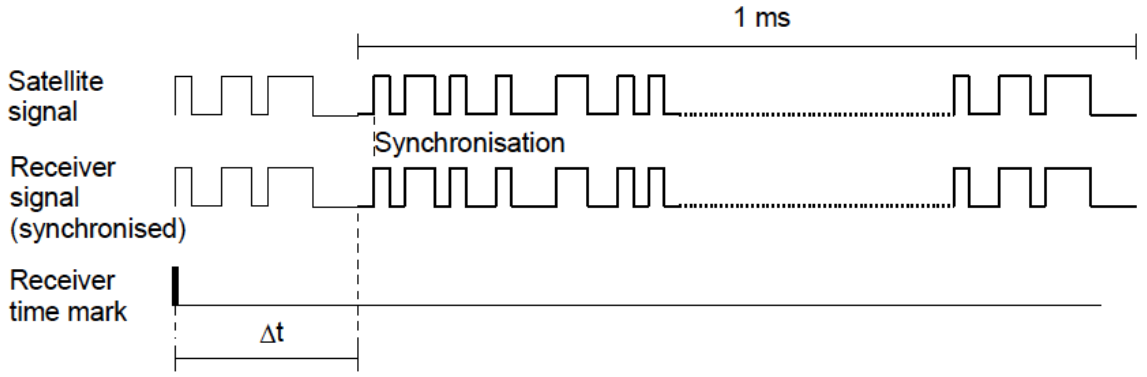


Figure 46: Measuring signal travel time

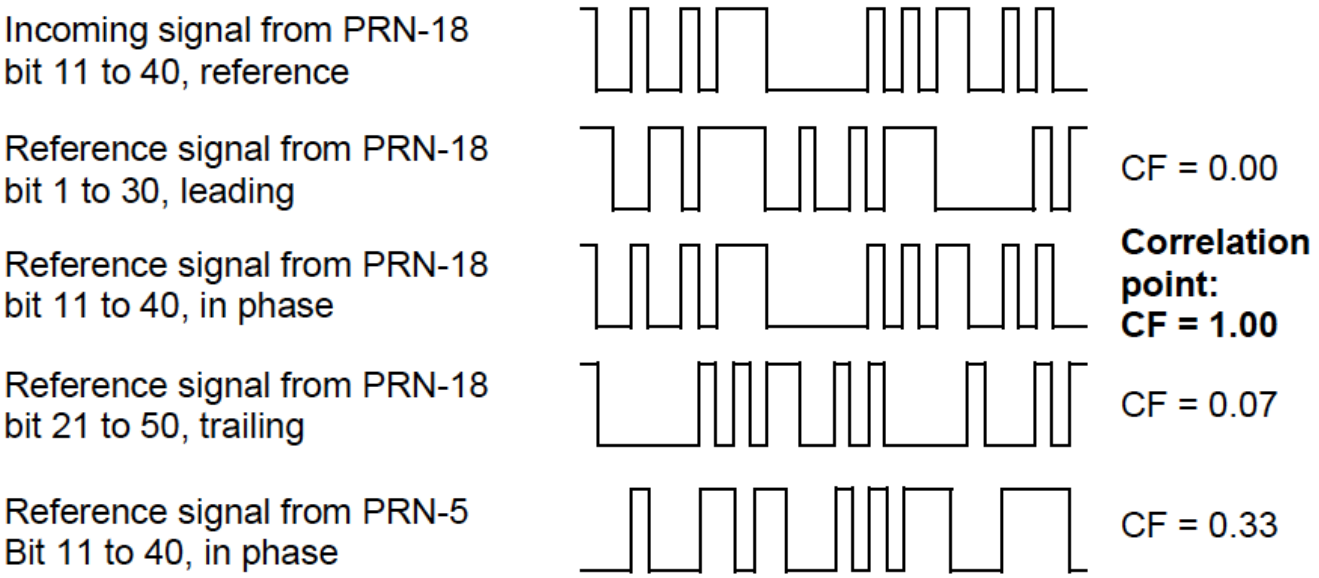
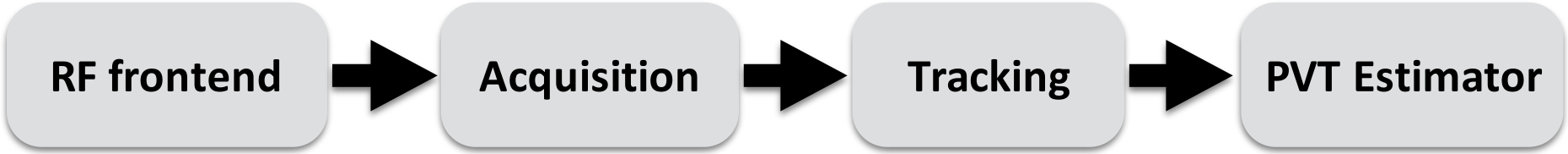
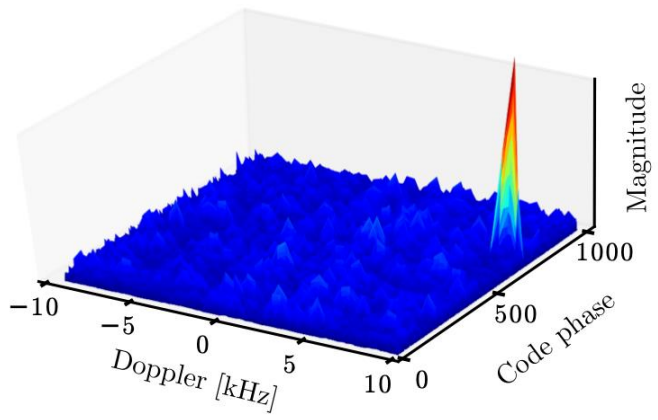
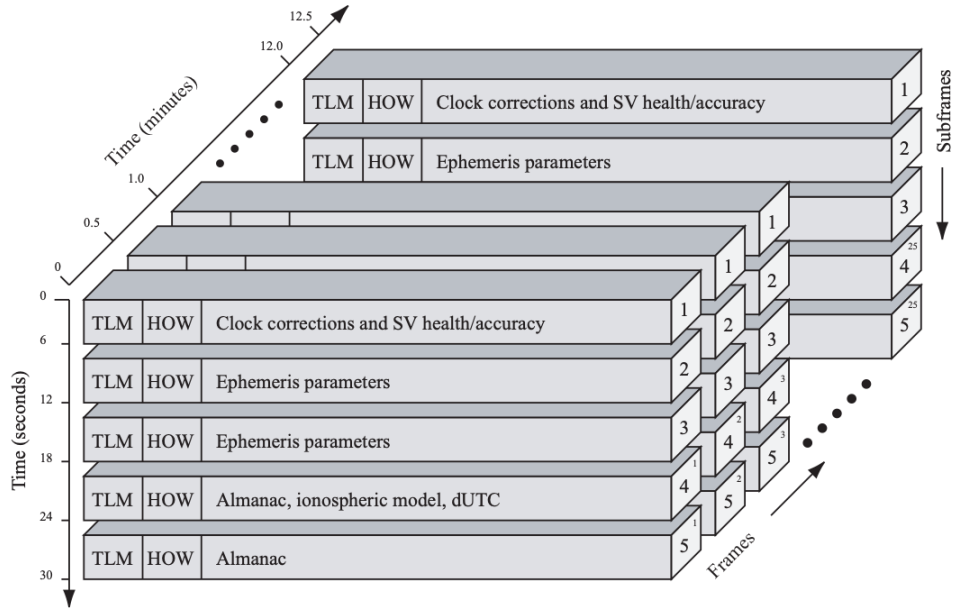


Figure 47: Demonstration of the correction process across 30 bits

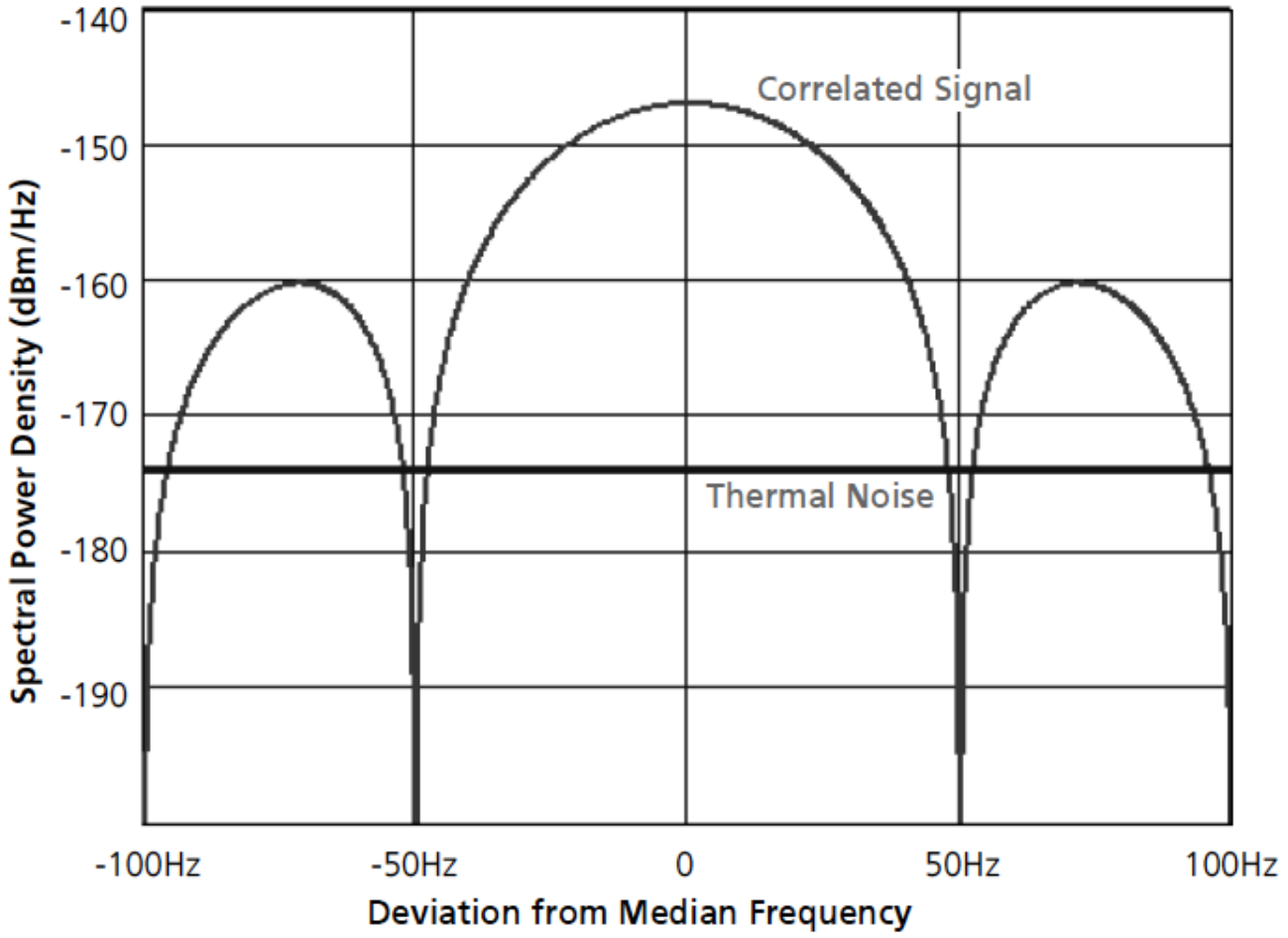
Typical GPS Receiver Architecture



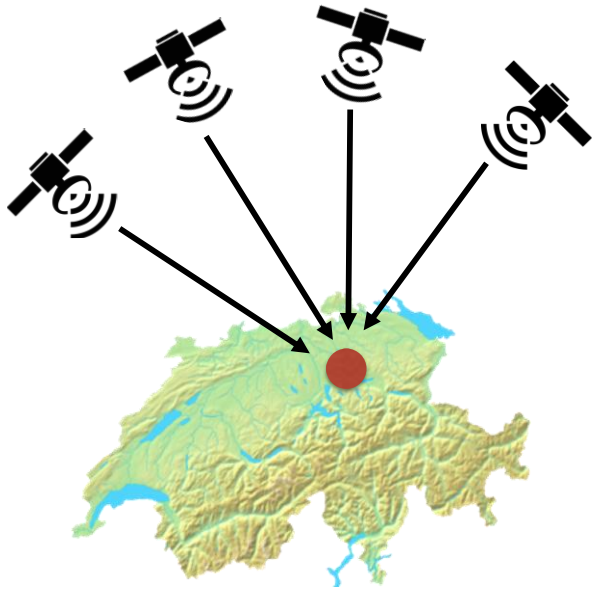


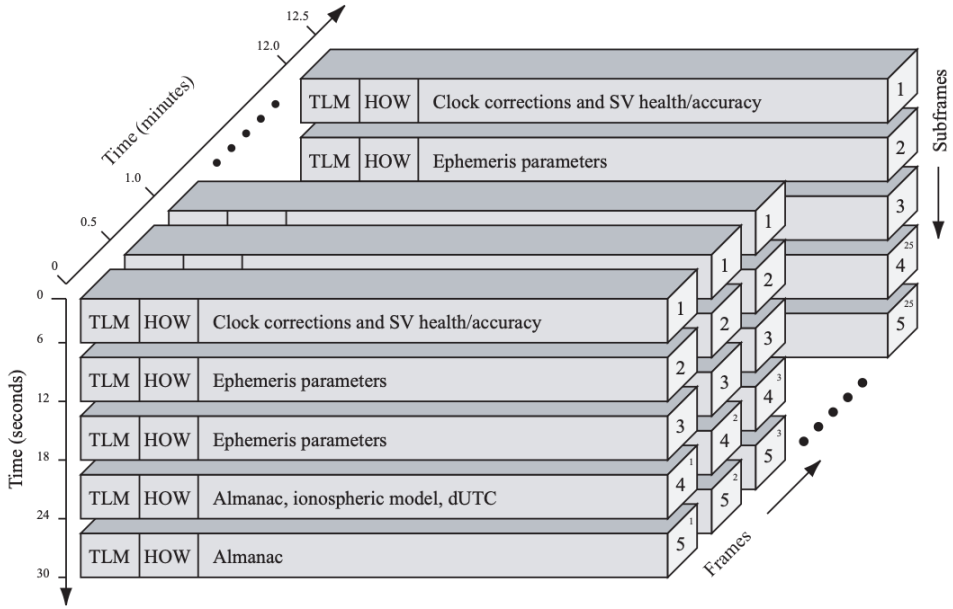


GPS: “Digging the Signal out of the Noise”



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

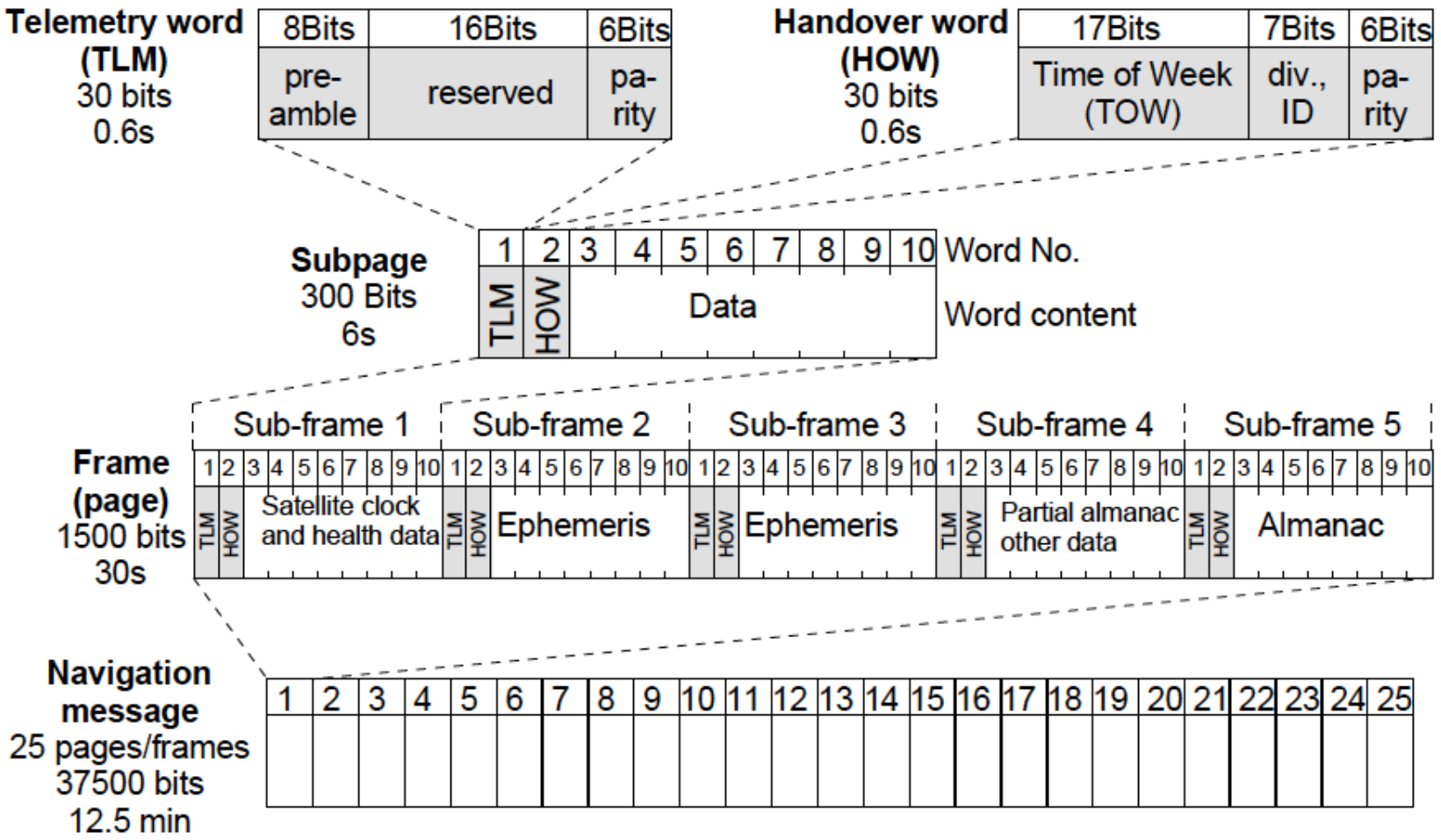


Figure 50: Structure of the entire navigation message

GPS messages

4.6.3 Information contained in the subframes

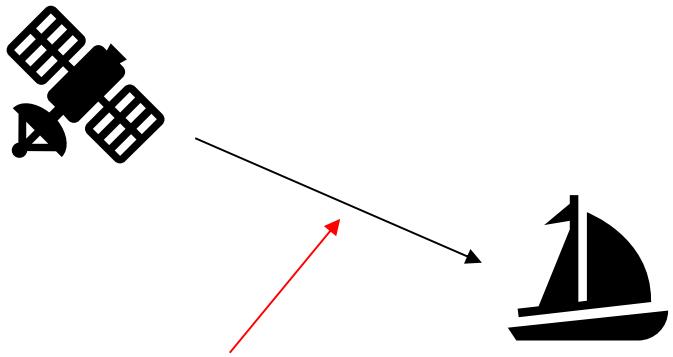
A frame is divided into five subframes, each subframe transmitting different information.

- 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.

That was interesting but…

What about security?

Overview of a big problem…



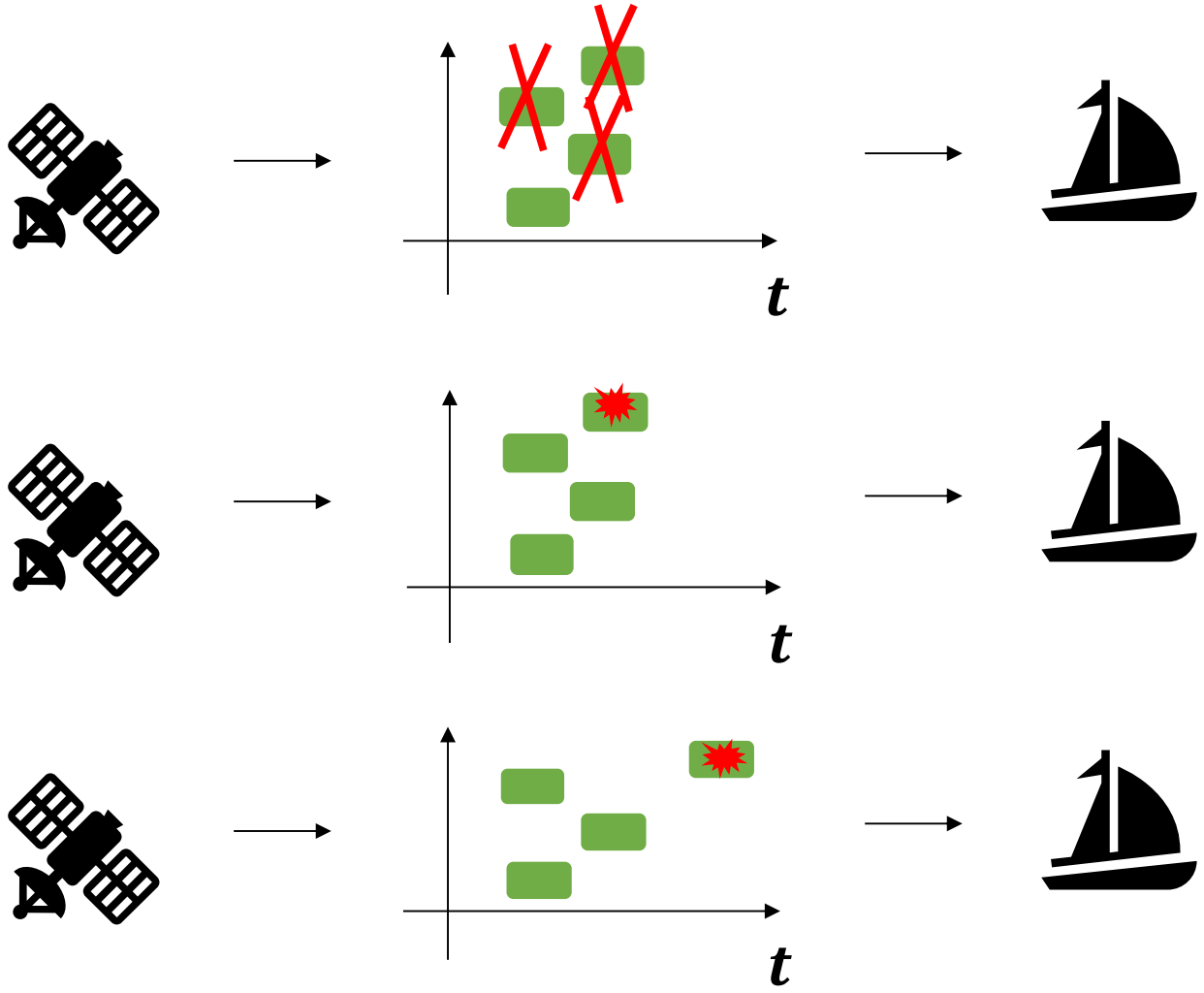
Dolev-Yao Attackers
Can tamper with the signals at their wish…
Because the spectrum is a shared resource and radio hardware is accessible (e.g., SDRs)

Countermeasures?
Countermeasures might restrict the attacker's capabilities

But…
A broadcast system like GNSS cannot be fully secured assuming a DY attacker

You would need…
Secure positioning requires:
Either… bidirectional communication
Or… communication with the infrastructure

High-level attack primitives and their effect



Jam or cancel all or some signals, inducing DoS or assisting other attacks

Change message and/or arrival time, inducing the computation of a rogue PVT solution

Note on the impact

Jamming

DoS is bad, but you know it
You can recover in other ways
(e.g., use inertial systems)

→ Still… it happens that airplanes are grounded because someone forgot a jammer on near the airport parking…

Useful to assist other attacks
(e.g., jam legitimate signal
before injecting a rogue signal)

Rogue position → Bad for (smart, autonomous) vehicles, high-value asset tracking, etc. Especially if you do not detect it and keep trusting the wrong position!

Rogue time → Some systems rely on GPS time for synchronizing over a large area. E.g., phasor measurement units in smart grids. Again, it is important to detect to avoid trusting wrong data

Overview of low-level attack/defense primitives

Add noise or jamming signal to degrade reception

Attack

- Jamming signal
- Signal cancellation
- Spoofing
- Relay/Replay

Subtract a copy of the legit signal to cancel it out

Generate a rogue signal following the specs

"Reuse" a legit signal, but at the wrong time/place

- Early Detection Late Commit
- Forward Error Estimation

Methods to send signals earlier even if you don't know the data bits a priori

Somehow detect inconsistencies at reception, possibly using multiple sources

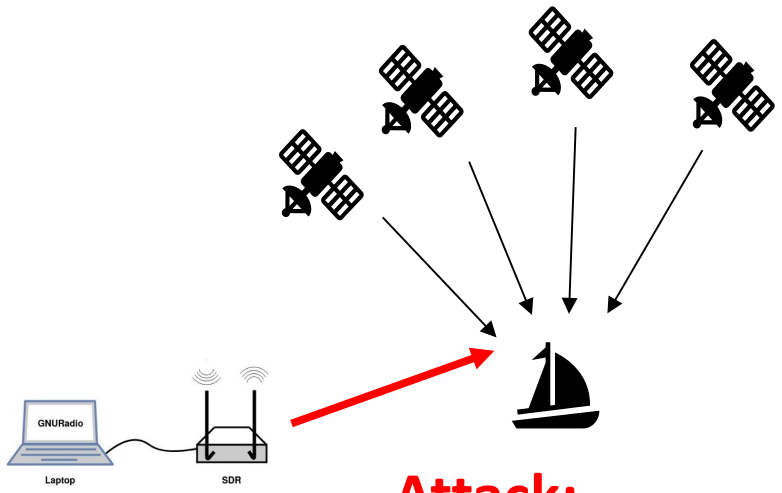
Defense

- Non-cryptographic
  - Signal characteristics
  - Multiple antennas/locations
  - Auxiliary information
- Cryptographic
  - Encrypted code
  - Message authentication

Try to prevent/detect time shifts and non-authentic messages

Let’s go into more detail

Jamming



Note:

- DSSS is hard to jam but… signals arrive on earth at very low power

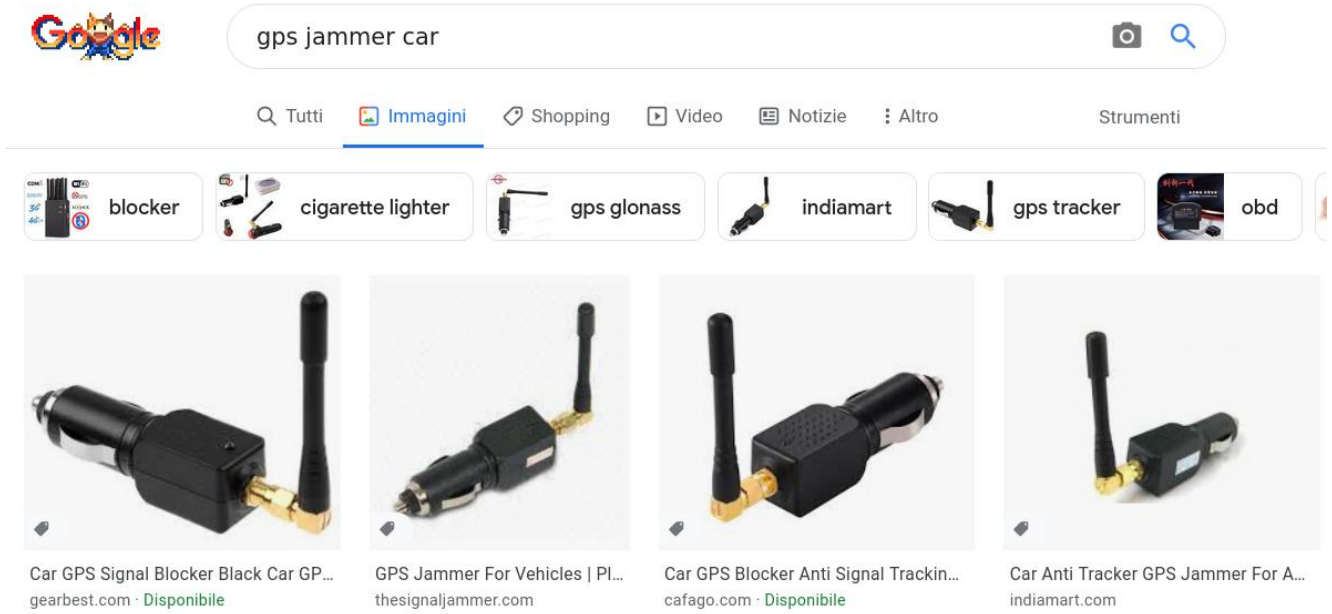
Attack:

- Inject a jamming signal/noise
- The added noise degrades the SNR of the legitimate signal to the point it cannot be received
- If the systems uses CDMA (e.g., GPS but not GLONASS) it jams all satellites at once

Jamming, real-world examples

Jamming devices:

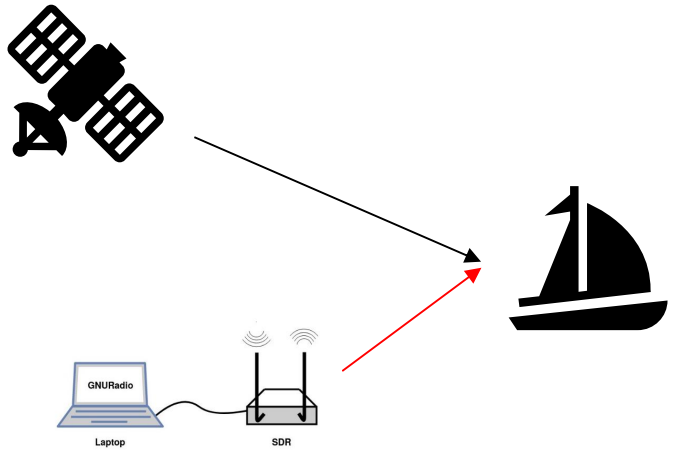
- They are on sale
- But they are illegal!



Someone in big trouble:

- Someone in France forgot a GPS jammer on in a car near the airport...
- https://www.connexionfrance.com/French-news/Forgotten-GPS-jammer-costs-motorist-2-000

Cancellation



Daniel Moser, Vincent Lenders, and Srdjan Capkun

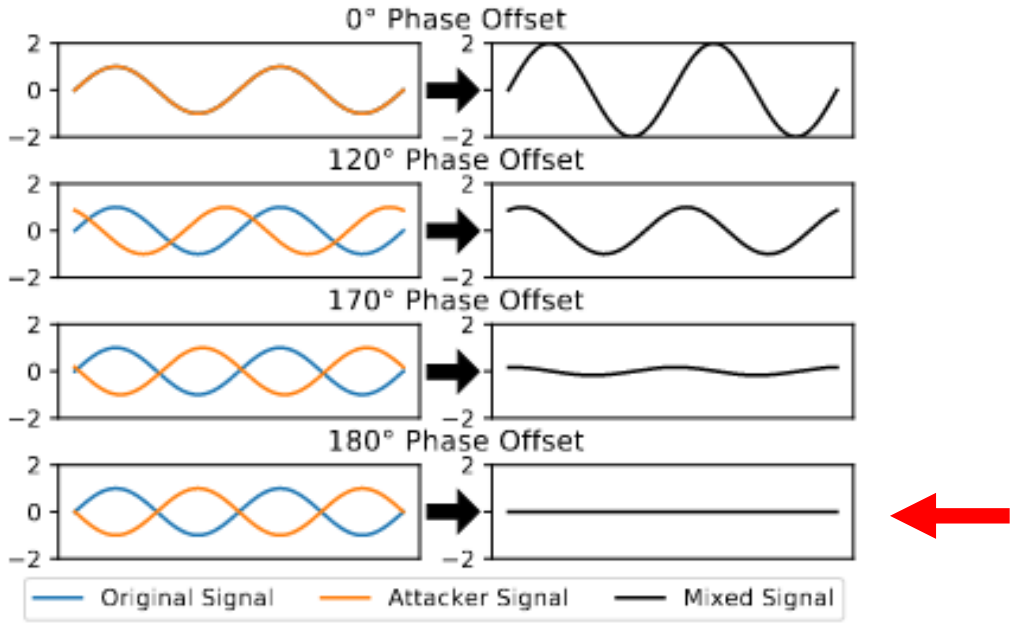


Figure 1: Effect of a signal overlaid with a copy of itself with different phase offsets.

Attack:

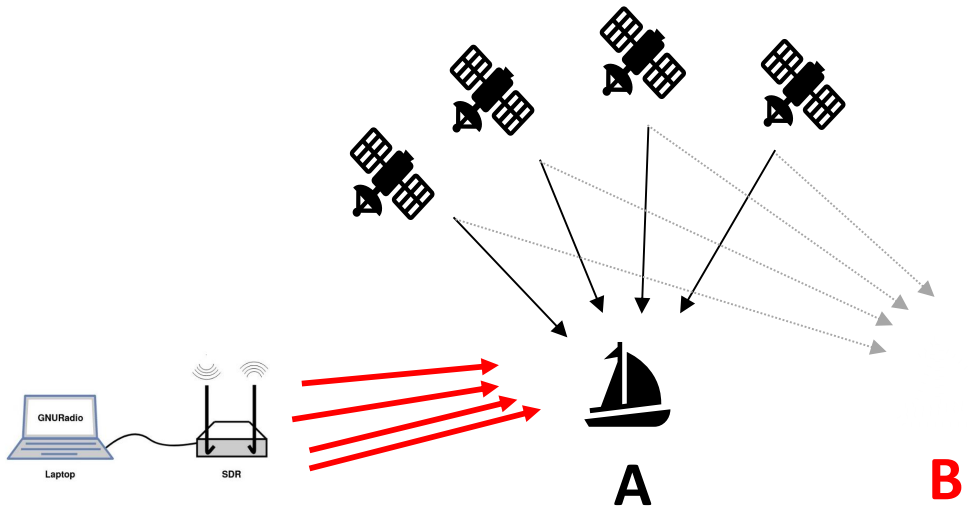
- Overlap a signal that will cancel the original one, a.k.a. “Destructive interference”
- It does not require high power, it is harder to detect compared to adding noise

Daniel Moser, Vincent Lenders, and Srdjan Capkun, “Digital Radio Signal Cancellation Attacks: An Experimental Evaluation,” in WiSec ’19, https://doi.org/10.1145/3317549.3319720.

Spoofing

Premise:

- Public documentation available
- In most cases civilian GNSS signals for a given time/place are fully predictable



Attack part 1:

- Generate valid signals for the desired rogue position/time
- In advance, following the specs

Attack part 2:

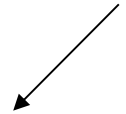
- Get close enough to the victim
- Transmit the valid but rogue signals at higher power
- The receiver locks on the rogue signals and computes the wrong PVT (position B instead of A)

Spoofing in action

https://youtu.be/y4pr5_ea5hw

Spoofing, additional considerations

More on this later



Signals are not always predictable:

- Military service, using a secret unpredictable spreading code
- Galileo Open Service Navigation Message Authentication (which authenticates the messages introducing unpredictability in some portions of the signal)

Attack improvements that facilitate takeover and make detection harder:

- Jam or cancel legitimate signals and force a new cold start
- Smooth “seamless takeover” without loss of lock:
  - First transmit a copy of legitimate signals (you need a way to estimate it)
  - Then slowly increase power until you are sure the receiver is tracking your signal and not the legitimate one anymore
  - Then smoothly start changing the position

Spoofing, (don’t) try it yourself

Gnss-Sdr, n.d., https://gnss-sdr.org/.
osqzss, Gps-Sdr-Sim, 2015, https://github.com/osqzss/gps-sdr-sim.

} Open-source code for RX and TX

Options:

- All in simulation
  - Generate data, store in a file, open in receiver
  - Quick and safe
- Controlled lab equipment
  - Like in the video
  - Requires great care to avoid actually spoofing real GPS!
  - Don’t make mistakes!

Spoofing, bringing hardware to the minimum

https://osmocom.org/projects/osmo-fl2k/wiki
https://github.com/steve-m/fl2k-examples/tree/master/GPS

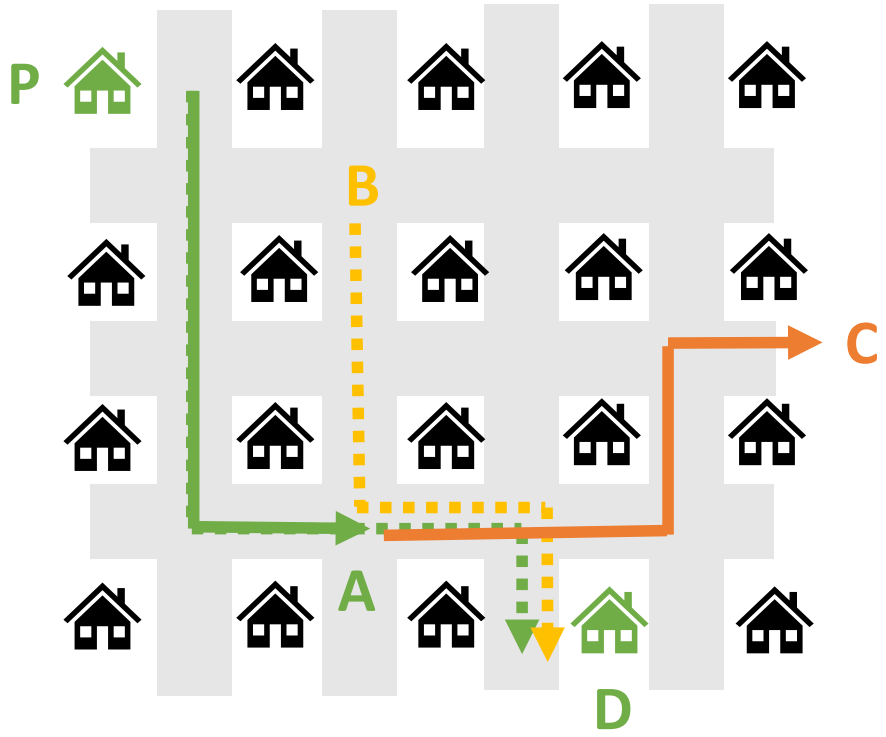
Spoofing in the air or at sea

https://youtu.be/ctw9ECgJ8L0

In the air, at sea, it is harder to have other references (ground, visual, inertial, etc.)

But what about cars in a city?

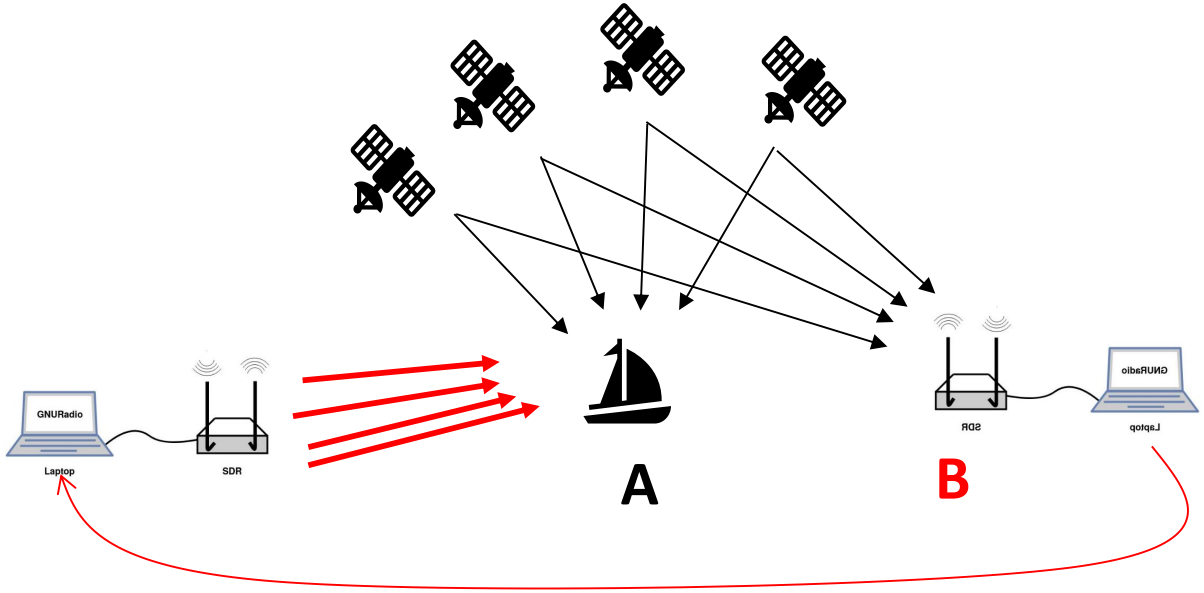
Spoofing, what if you are driving in a city?



Victim's original Route P->D
Victim arrives in A
The attackers spoofs the position so that the victim believes to be in B
The victim's GPS recomputes the road, from B to D
The victim follows the instructions from B to D, but starting from A!
The victim ends up in C!

Kexiong (Curtis) Zeng et al., "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems," 2018, 1527–44, https://www.usenix.org/conference/usenixsecurity18/presentation/zeng.

Relay/Replay



Attack:

- Relay a valid signal (passive cable, digital transmission over the network*, …)
- Record and (selectively) replay
- The victim believes to be in B instead of A
- It generally works also with encrypted/authenticated signals

*Malte Lenhart, Marco Spanghero, and Panagiotis Papadimitratos, “Relay/Replay Attacks on GNSS Signals,” WiSec ’21.

Let’s see some non-cryptographic countermeasures

Monitoring signal characteristics

Examples:

- Check angle of arrival
- Monitor AGC, noise and other physical layer parameters for unexpected changes
- …

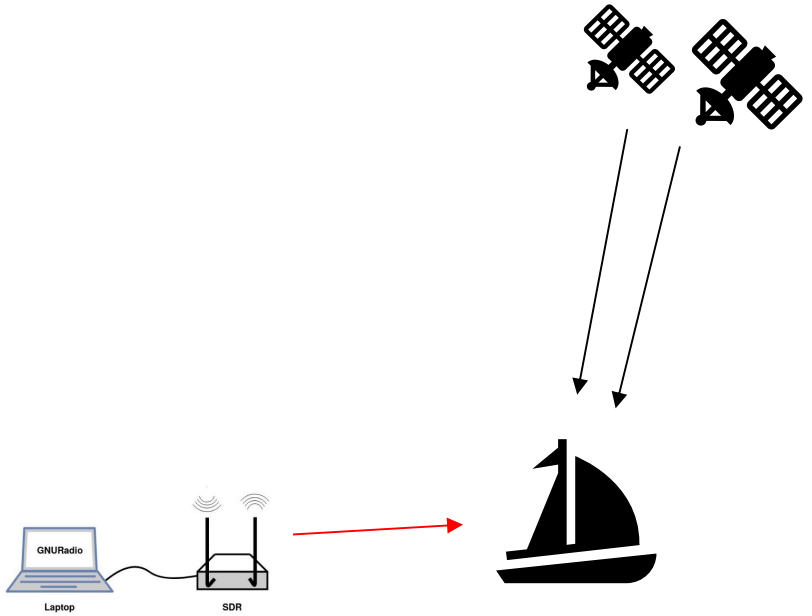
Advantages and disadvantages:

- They do not require changing the GNSS system itself
- They might require changes in the receivers' hardware/software
- It might be hard to distinguish a bad channel from an attack, with the risk of causing disservice if over-conservative for security

Example: Angle of Arrival

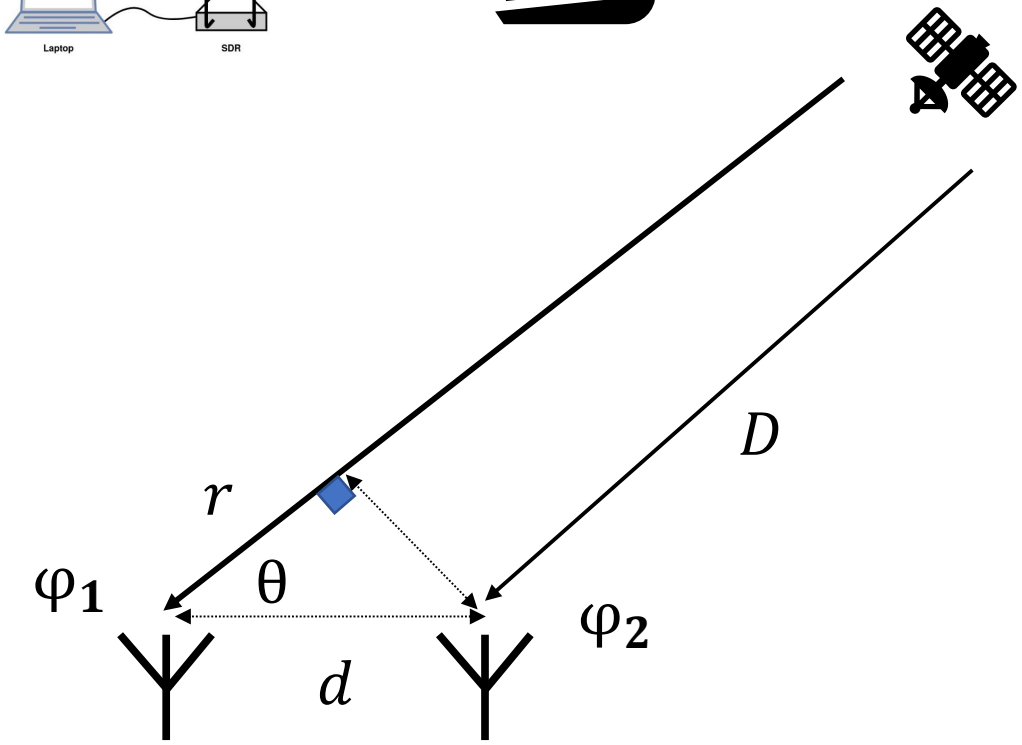
The intuition:

- Satellites have some angle of arrival
- Attackers have a different and strange angle of arrival

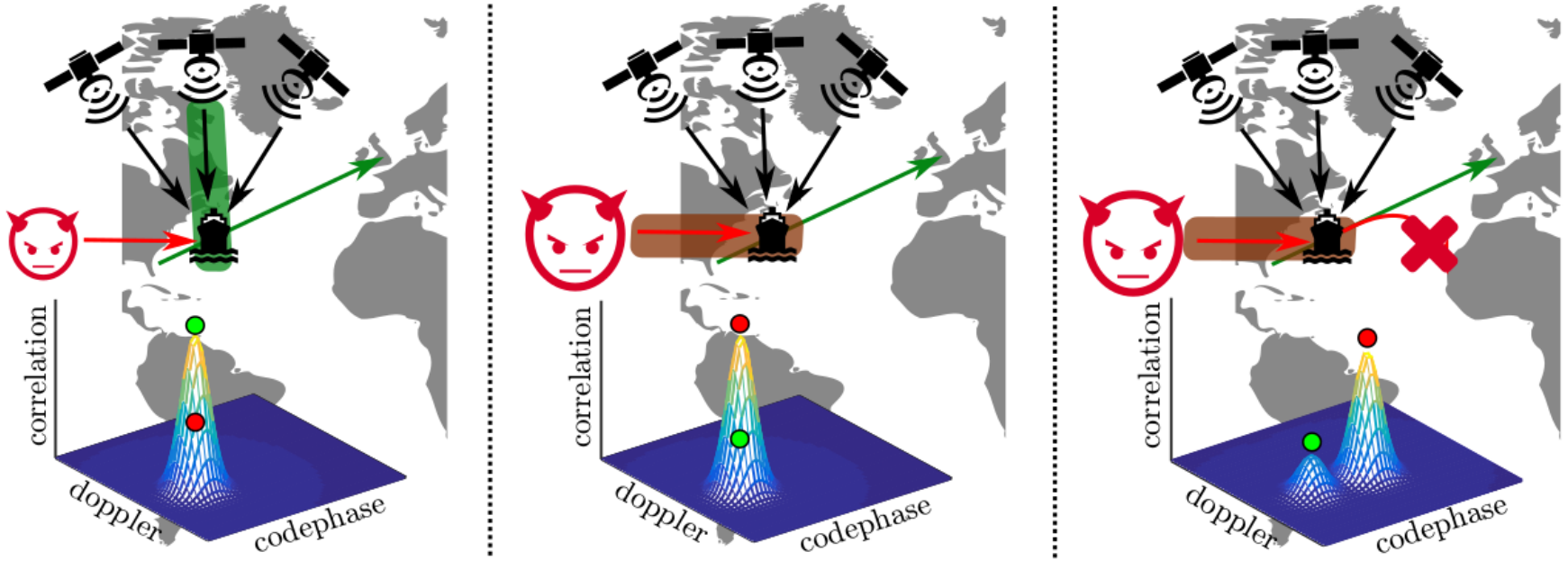


AoA measurement:

- $AoA = f(d, \varphi_1 - \varphi_2)$
- Computationally expensive
- In more detail:
  - $D \gg d$
  - $d < \frac{\lambda}{2}$
  - $r = d \cos\theta$
  - $r = \lambda(\varphi_1 - \varphi_2)/2\pi$



Example: Auxiliary Peak Tracking (SPREE)



Recall: correlation peaks to detect signals, spoofing gradually adds another peak

Intuition: detect a new peak that drifts away, distinguish attack from multi-path

Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun, "SPREE: A Spoofing Resistant GPS Receiver," in MobiCom'16.

https://www.spree-gnss.ch/

The “clock bias” test against replay

Single receiver

The usual equations:

- $\left(t_r^{S_k} - t_s\right)c = |S_k - X| + c\delta t \ \forall k$

Replay attack

- $t_r^{S_k} \rightarrow t_r^{S_k} + t_{delay}^{S_k}$
- $X \rightarrow X'$
- $\delta t \rightarrow \delta t'$

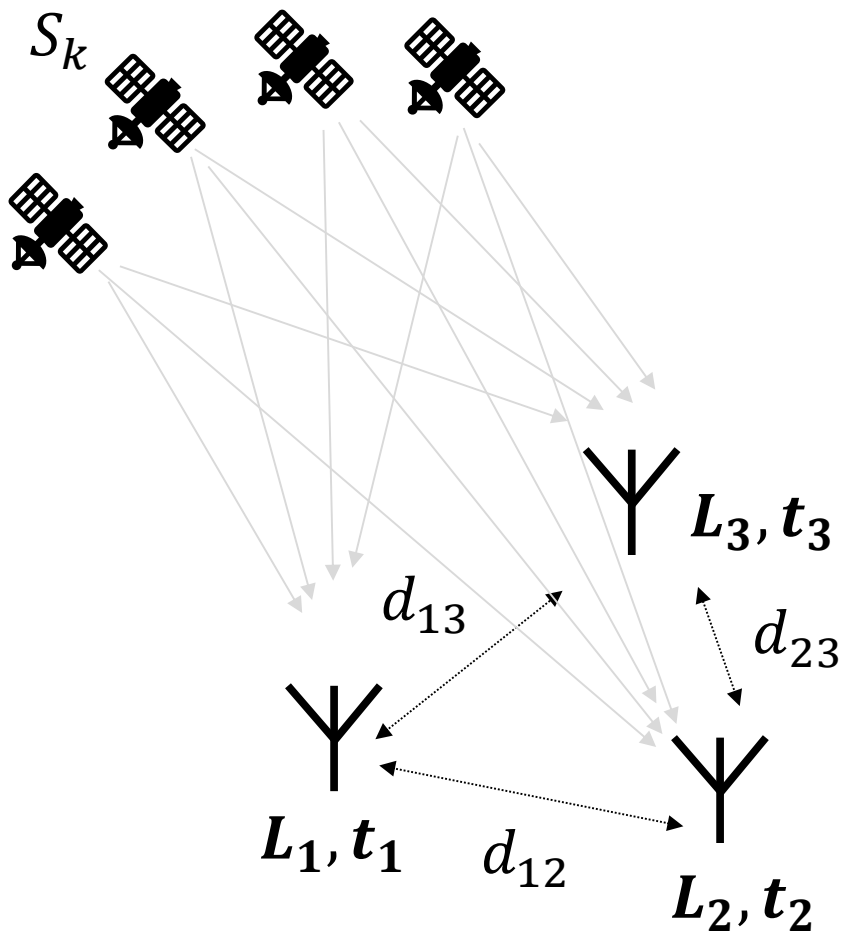
Here the attack delays a signal. More on attacks that can anticipate a signal later

Idea for detection

- $\delta t = \left(t_r^{S_k} - t_s\right) - \frac{|S_k - X|}{c}$
- $\delta t' = \left(t_r^{S_k} + t_{delay}^{S_k} - t_s\right) - \frac{|S_k - X|}{c}$
- $\delta t' > \delta t$
- Detect an attack as a sudden increase in the bias, bigger than a natural clock drift
- Use a stable trusted local clock as a reference

Daniel Marnach et al., “Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers,” Artificial Satellites 48, no. 2 (January 1, 2013), https://doi.org/10.2478/arsa-2013-0006.

Leveraging spatial diversity



Single receiver

The usual equations:

- $\left(t_r^{S_k} - t_s\right)c = |S_k - X_i| + c\delta t_i \quad \forall k$

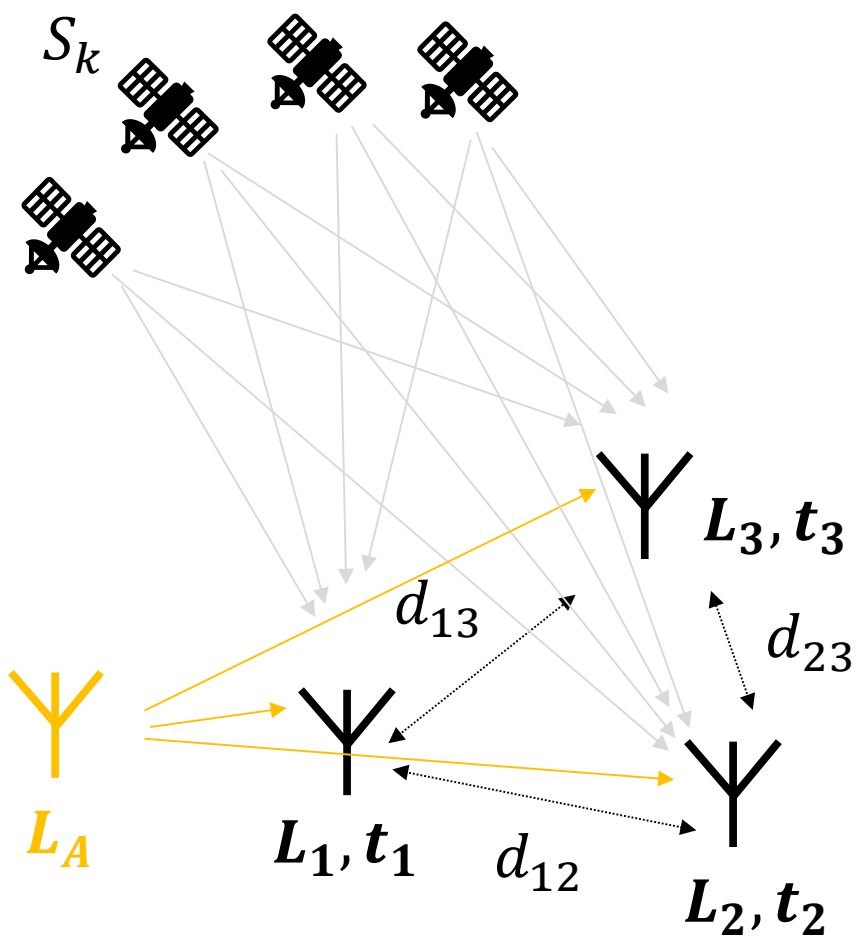
A formation of receivers

Knowledge of distance and time synchronization adds some constraints:

- $t_1 \cong t_2 \cong t_3$
- $|X_i - X_j| = d_{ij} \quad \forall i,j$

Nils Ole Tippenhauer et al., "On the Requirements for Successful GPS Spoofing Attacks," in C CCS'11.

Leveraging spatial diversity

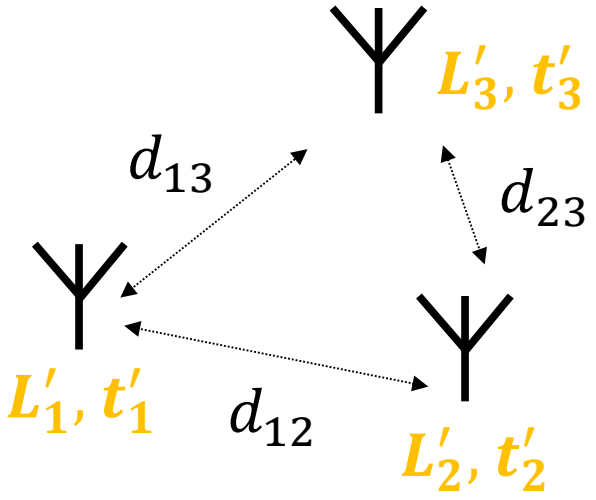


The attacker

From one location with omnidirectional antenna

Chooses claimed satellite position and signal delays

Must respect the additional formation constraints or the receiver could detect the inconsistency



- $t'_1 \cong t'_2 \cong t'_3$
- $|L'_i - L'_j| = d_{12}$

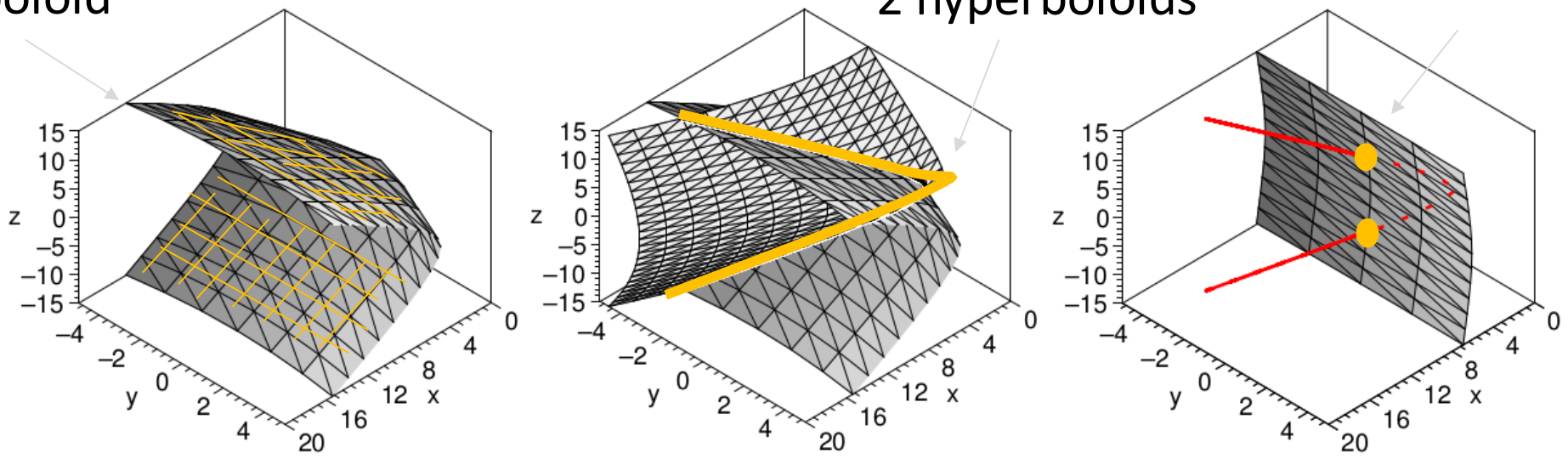
Nils Ole Tippenhauer et al., “On the Requirements for Successful GPS Spoofing Attacks,” in C CCS’11.

Leveraging spatial diversity

hyperboloid

Intersection of
2 hyperboloids

Intersection of
3 hyperboloids
only two points left



2 receivers

3 receivers

4 receivers

The attacker's position is constrained!

- It turns out that respecting the constraints imposed by the formation constrains the position where the attacker can be
- The more receivers, the less possible positions for the attacker

Nils Ole Tippenhauer et al., "On the Requirements for Successful GPS Spoofing Attacks," in C CCS'11.

Some References

Daniel Moser, Vincent Lenders, and Srdjan Capkun, “Digital Radio Signal Cancellation Attacks: An Experimental Evaluation,” in WiSec ’19, https://doi.org/10.1145/3317549.3319720.

Nils Ole Tippenhauer et al., “On the Requirements for Successful GPS Spoofing Attacks,” in Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS ’11 (the 18th ACM conference, Chicago, Illinois, USA: ACM Press, 2011), 75, https://doi.org/10.1145/2046707.2046719.

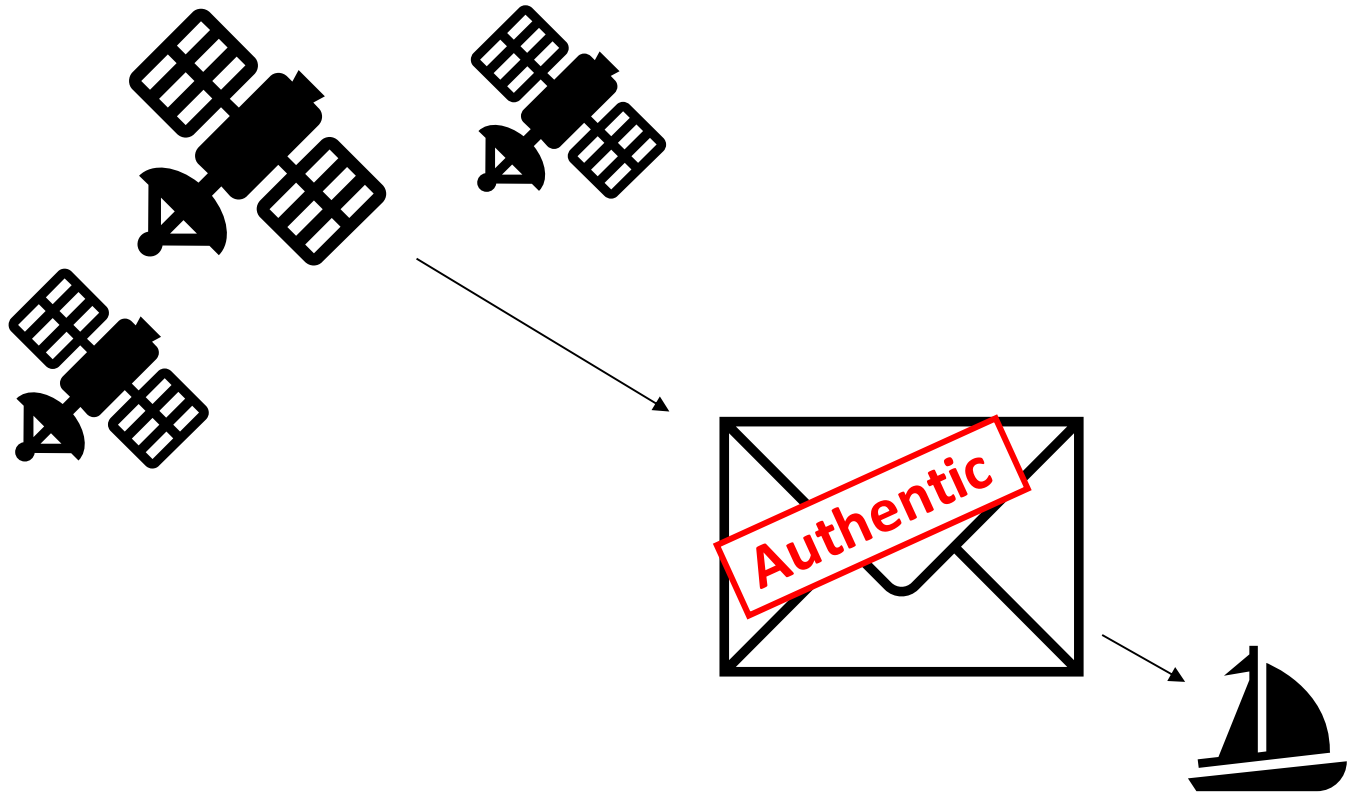
Malte Lenhart, Marco Spanghero, and Panagiotis Papadimitratos, “Relay/Replay Attacks on GNSS Signals,” in Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec ’21: 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Abu Dhabi United Arab Emirates: ACM, 2021), 380–82, https://doi.org/10.1145/3448300.3468256.

Kexiong (Curtis) Zeng et al., “All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems,” 2018, 1527–44, https://www.usenix.org/conference/usenixsecurity18/presentation/zeng.

Malte Lenhart, Marco Spanghero, and Panagiotis Papadimitratos, “Relay/Replay Attacks on GNSS Signals,” WiSec ’21.

Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun, “SPREE: A Spoofing Resistant GPS Receiver,” in MobiCom’16.

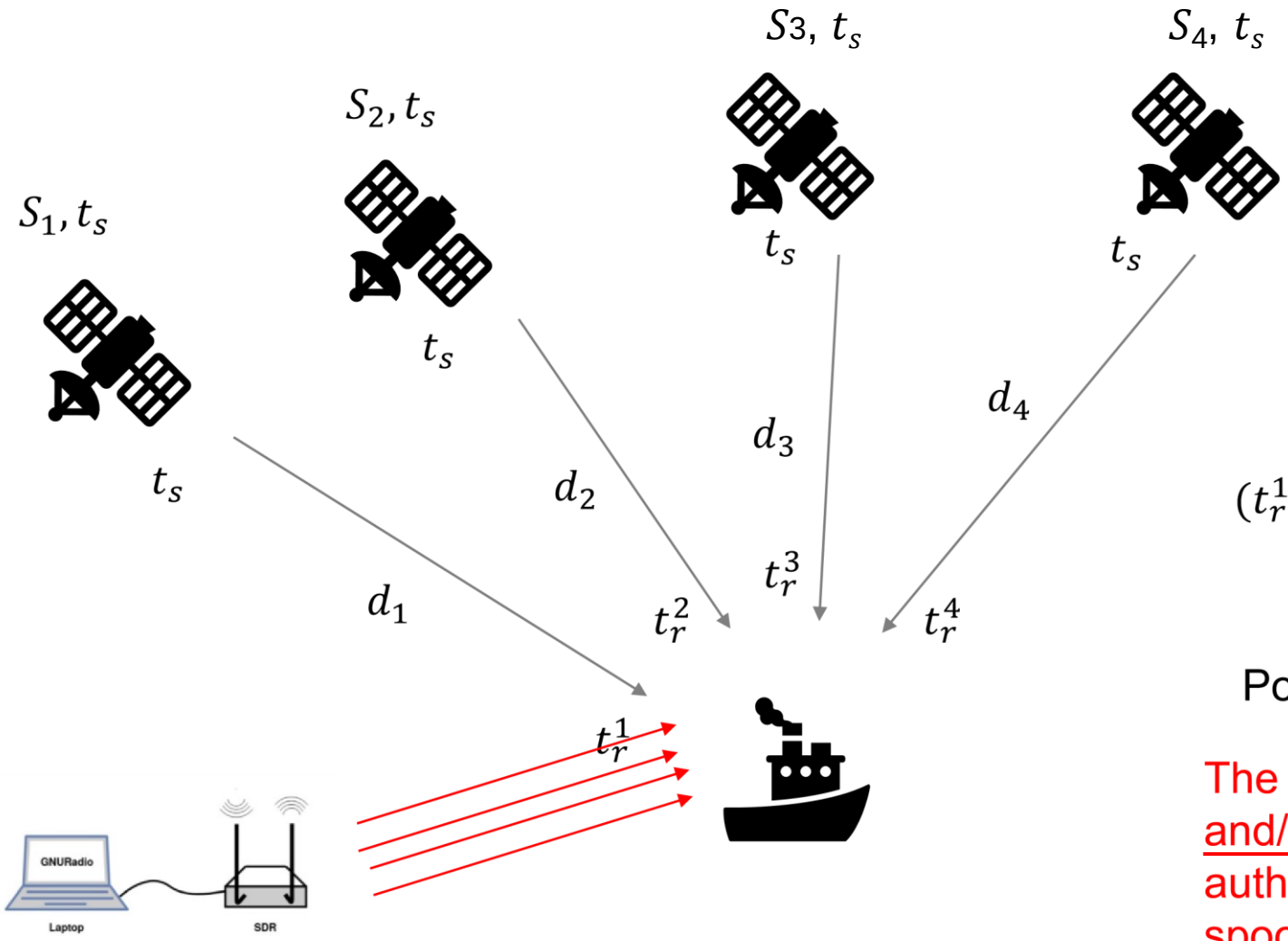
Kewei Zhang, “Secure GNSS-Based Positioning and Timing,” 2021.



Galileo
Open Service Navigation Message Authentication (OSNMA)

The intuition

Quick recap of the problem



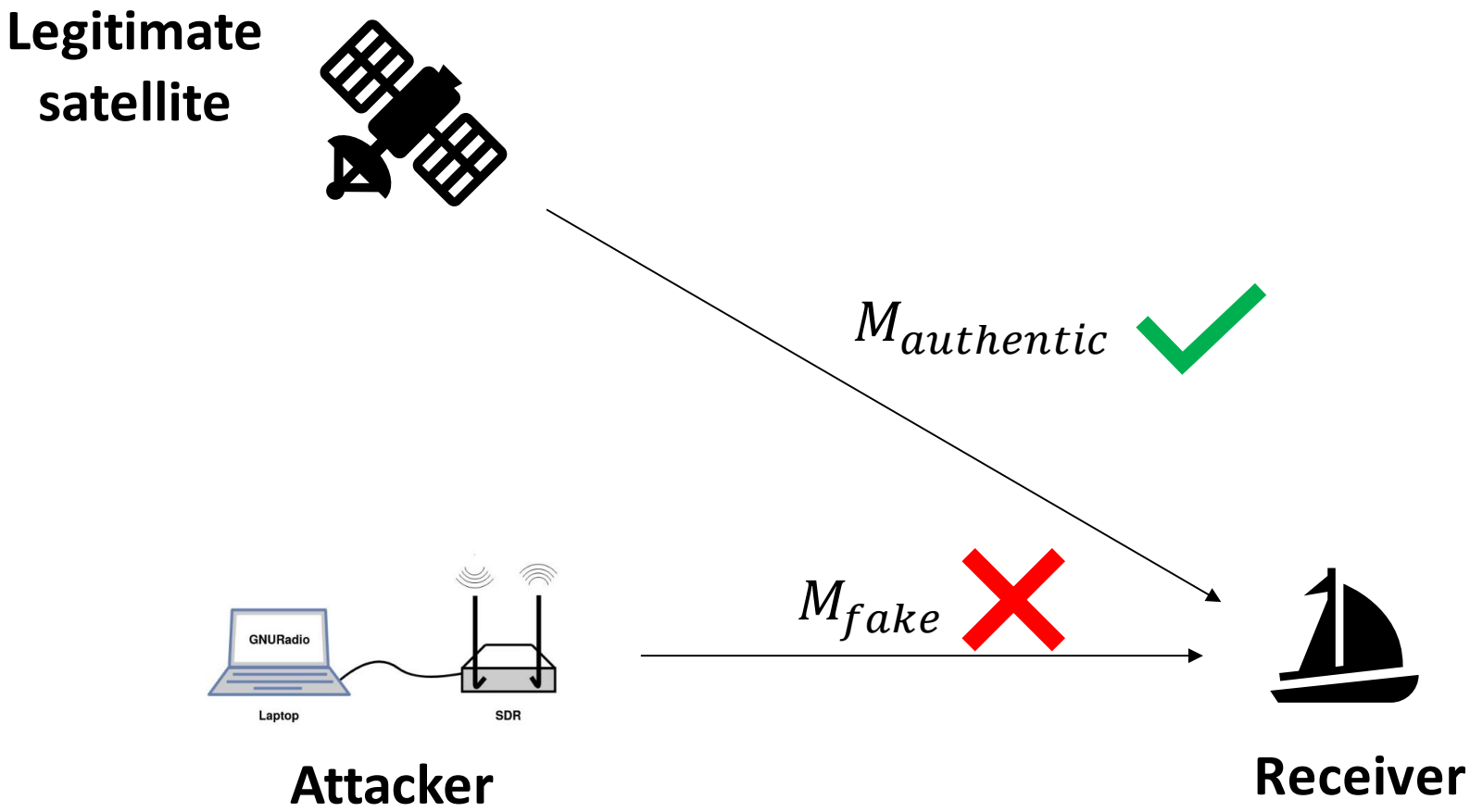
$$(t_r^1 - t_s)c = |S_i - X| + c\delta t$$

↓

Position Velocity Time (PVT)

The attacker can change messages and/or arrival time due to lack of authentication and weak signals (using spoofing, relay, replay, …)

Goal: message authentication



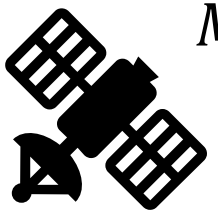
Verify authenticity

How can the receiver verify authenticity and reject fakes?

Naïve solution 1: public key crypto

$K_{private}$

Legitimate satellite



$M_{authentic}$

$DS = Sign(M_{authentic}, K_{private})$

$M_{authentic}, DS$

Good

Well-known and trusted cryptographic solution

Bad

Signature is too long to fit in limited bandwidth

Computationally expensive

K_{public}

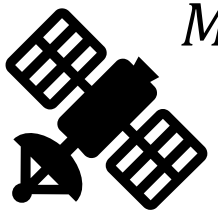
Receiver

$Verify(M_{authentic}, DS, K_{public})$

Naïve solution 2: symmetric crypto

K_{secret}

Legitimate satellite



$M_{authentic}$

$MAC = Encrypt(M_{authentic}, K_{secret})$

$M_{authentic}, MAC$

Good

Light-weight

MAC can be short

Bad

Can you really deploy the same secret key on all receivers and trust it to stay secret?

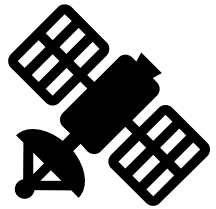
K_{secret}

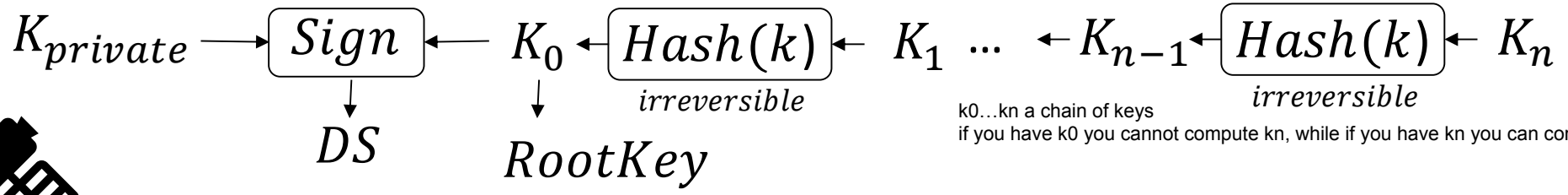
Receiver

$Verify = recompute\ the\ MAC$

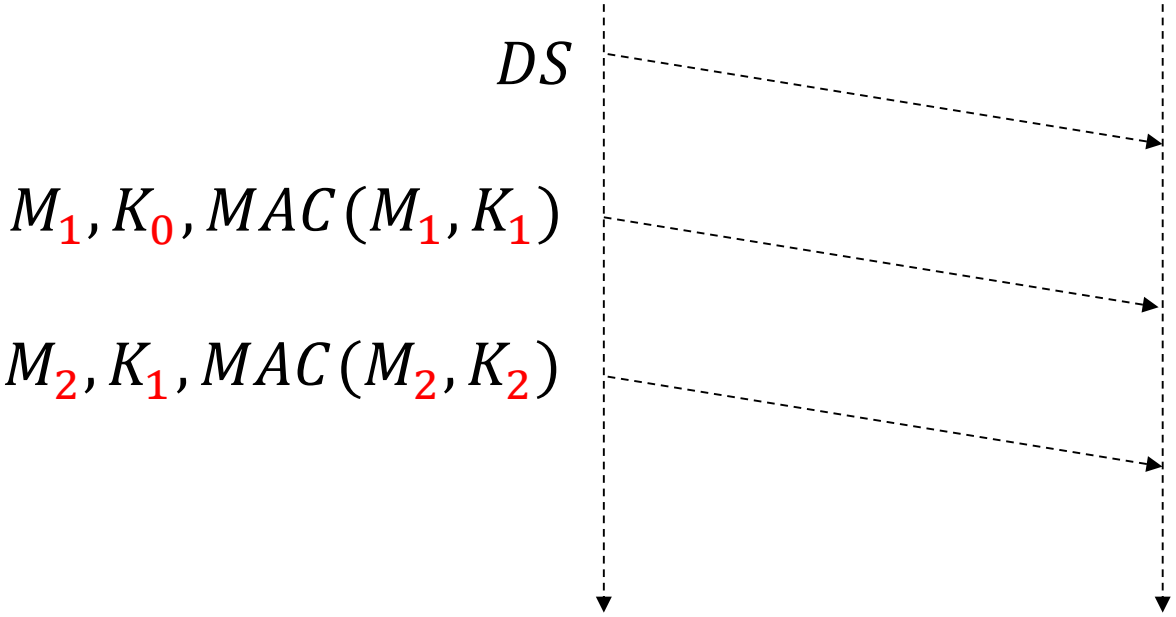
Time-delayed Authentication (Simplified)

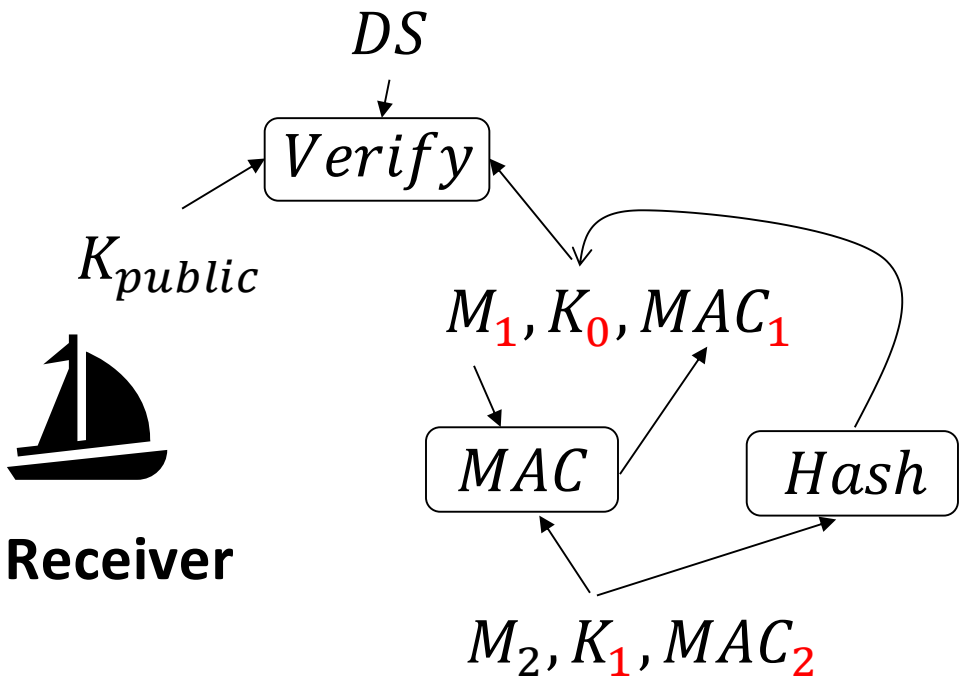
Legitimate satellite





k0…kn a chain of keys
if you have k0 you cannot compute kn, while if you have kn you can compute k0





Receiver

Recap

Irreversible key chain
Generated in reverse order with a hash function
Root key signed with private key

MAC + time-delayed key disclosure
Sign message with next key (not yet known by anyone but the legitimate satellite)
Later in the next message disclose the previous key

Verification
Verify first key against signature using public key
Verify key against previous key (hash, no need to go back to signature every time)
Verify previous message using key disclosed now

Recap

Combined advantages

Long digital signature of root key sent and verified only once (in a while)

Short MAC used all the time

No shared secret thanks to delayed disclosure

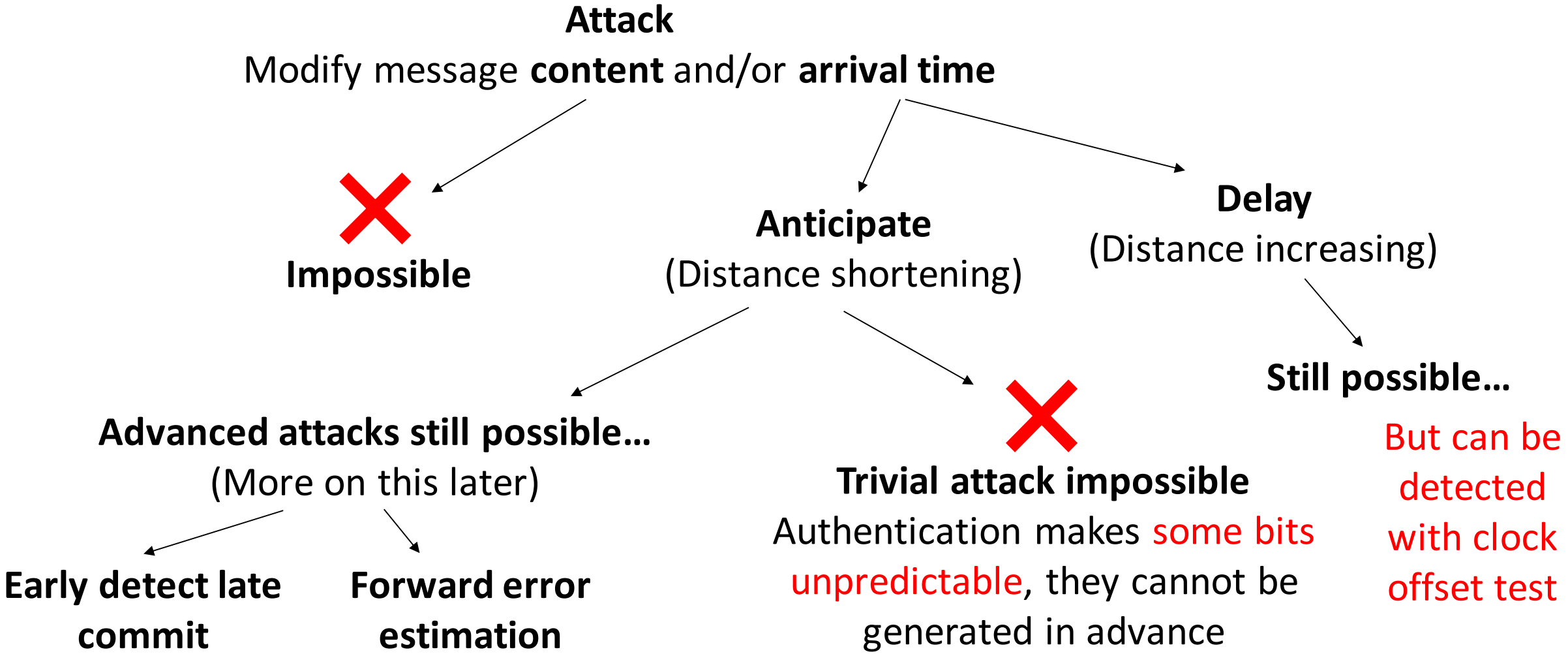
Disadvantages

Time-delayed disclosure is not a well-established crypto method

A lot more details to be secure (e.g., time stamps in hashes)

A lot more to be performant (e.g., truncate MACs)

Security analysis



Conclusion on Galileo OSNMA

A big step forward

For the first time a global protection in the system itself

Many attacks that are now trivial will become hard/impossible

It raises the bar for practical attacks

Still more to do

It is already known that some attack classes are not covered

Some more attacks might be discovered (recent implementation especially at rx)

Additional countermeasures needed when the application is sensitive

Some References (1/2)

Nils Ole Tippenhauer et al., “On the Requirements for Successful GPS Spoofing Attacks,” in Proceedings of the 18th ACM Conference on Computer and Communications Security - CCS ’11 (the 18th ACM conference, Chicago, Illinois, USA: ACM Press, 2011), 75, https://doi.org/10.1145/2046707.2046719.

A. Perrig et al., “Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction” (RFC Editor, June 2005), https://doi.org/10.17487/rfc4082.

Ignacio Fernández-Hernández et al., “A Navigation Message Authentication Proposal for the Galileo Open Service” 63, no. 1 (2016): 18. Implementation details that we simplified

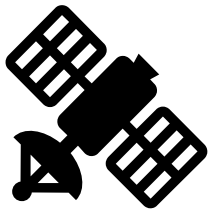
P Walker et al., “Galileo Open Service Authentication: A Complete Service Design and Provision Analysis,” ION GNSS+, 2015. Summary + security analysis

Cillian O’Driscoll and Ignacio Fernández-Hernández, “Mapping Bit to Symbol Unpredictability in Convolutionally Encoded Messages with Checksums, with Application to Galileo OSNMA,” 2020, 3751–65, https://doi.org/10.33012/2020.17715.

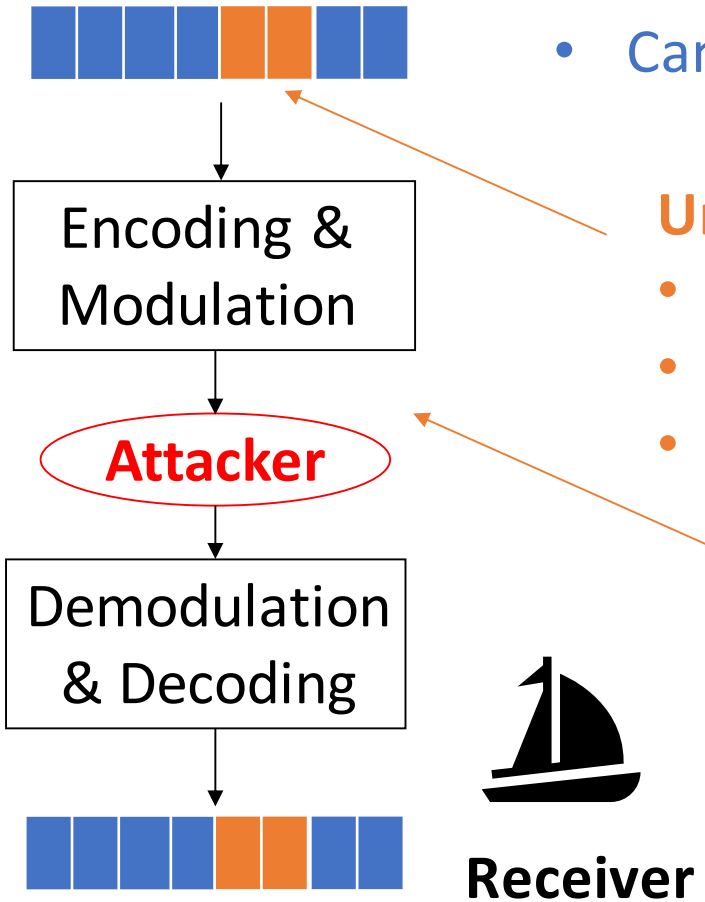
https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf

Distance reduction attacks that can anticipate a signal even if some bits are unpredictable

The problem



Legitimate satellite



Receiver

Predictable bits

- E.g., satellite number
- Known a priori
- Can be generated in advance

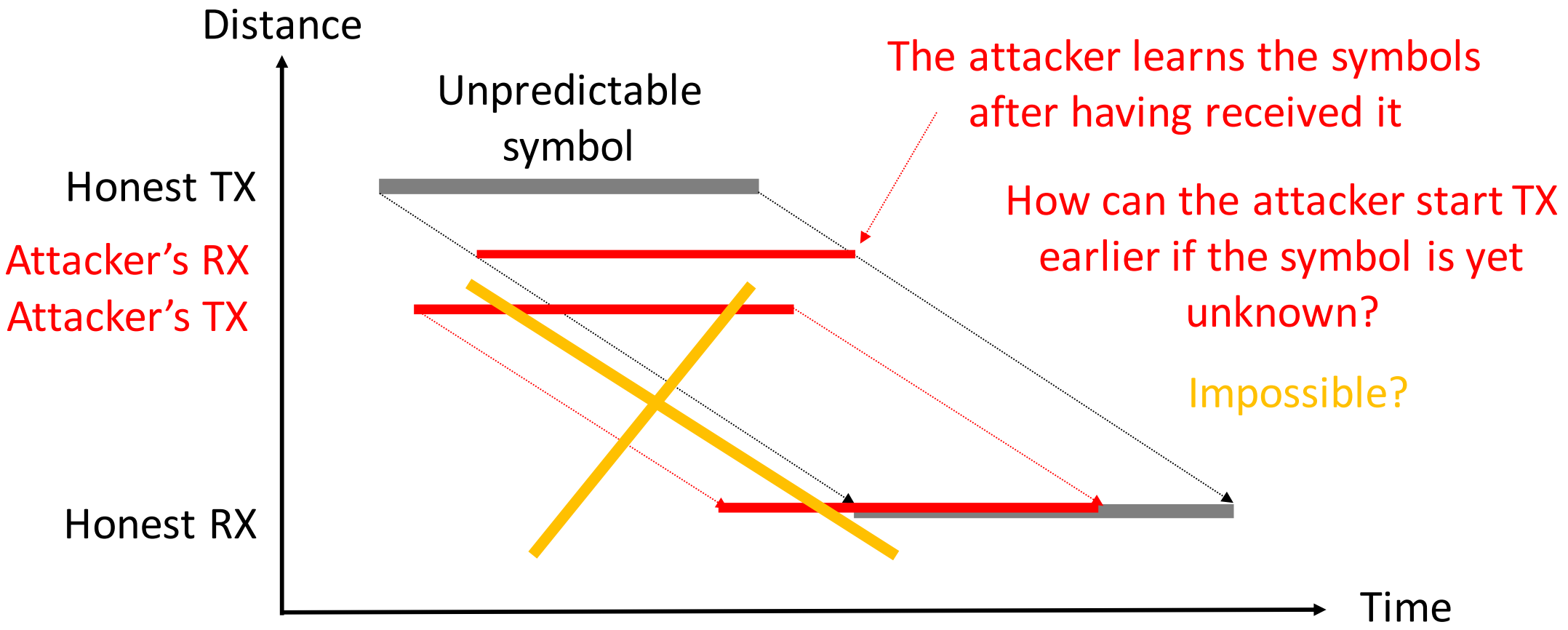
Unpredictable bits

- E.g., bits of the MAC in Galileo OSNMA
- Not known a priori
- Cannot be generated in advance

Unpredictable symbols

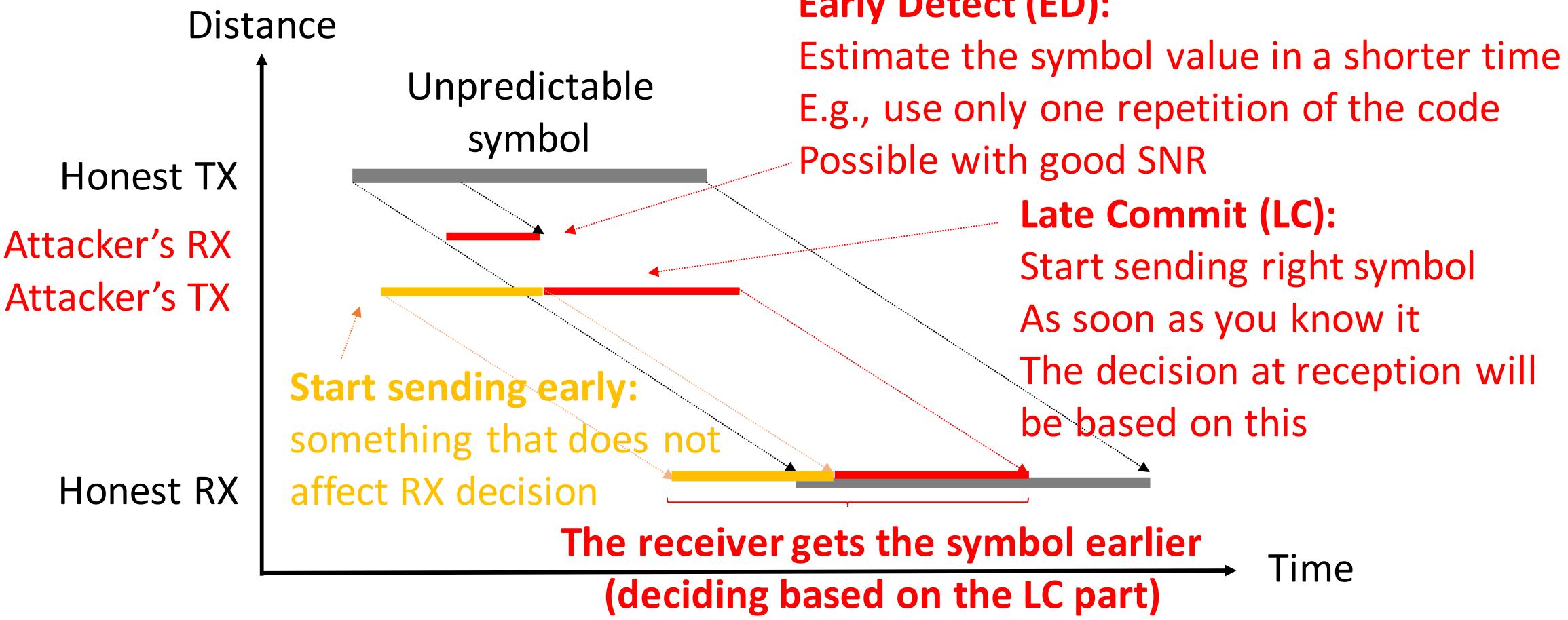
- The attacker can delay them
- The attacker cannot anticipate them

Early Detection Late Commit (Simplified)



Jolyon Clulow et al., "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," in Security and Privacy in Ad-Hoc and Sensor Networks, ed. Levente Buttyán, Virgil D. Gligor, and Dirk Westhoff, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2006), 83–97
Kewei Zhang and Panos Papadimitratos, "On the Effects of Distance-Decreasing Attacks on Cryptographically Protected GNSS Signals," 2019, 363–72.
Kewei Zhang, "Secure GNSS-Based Positioning and Timing," 2021.

Early Detection Late Commit (Simplified)

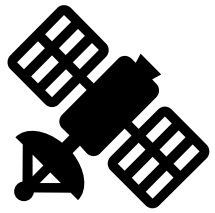


Jolyon Clulow et al., "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," in Security and Privacy in Ad-Hoc and Sensor Networks, ed. Levente Buttyán, Virgil D. Gligor, and Dirk Westhoff, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2006), 83–97

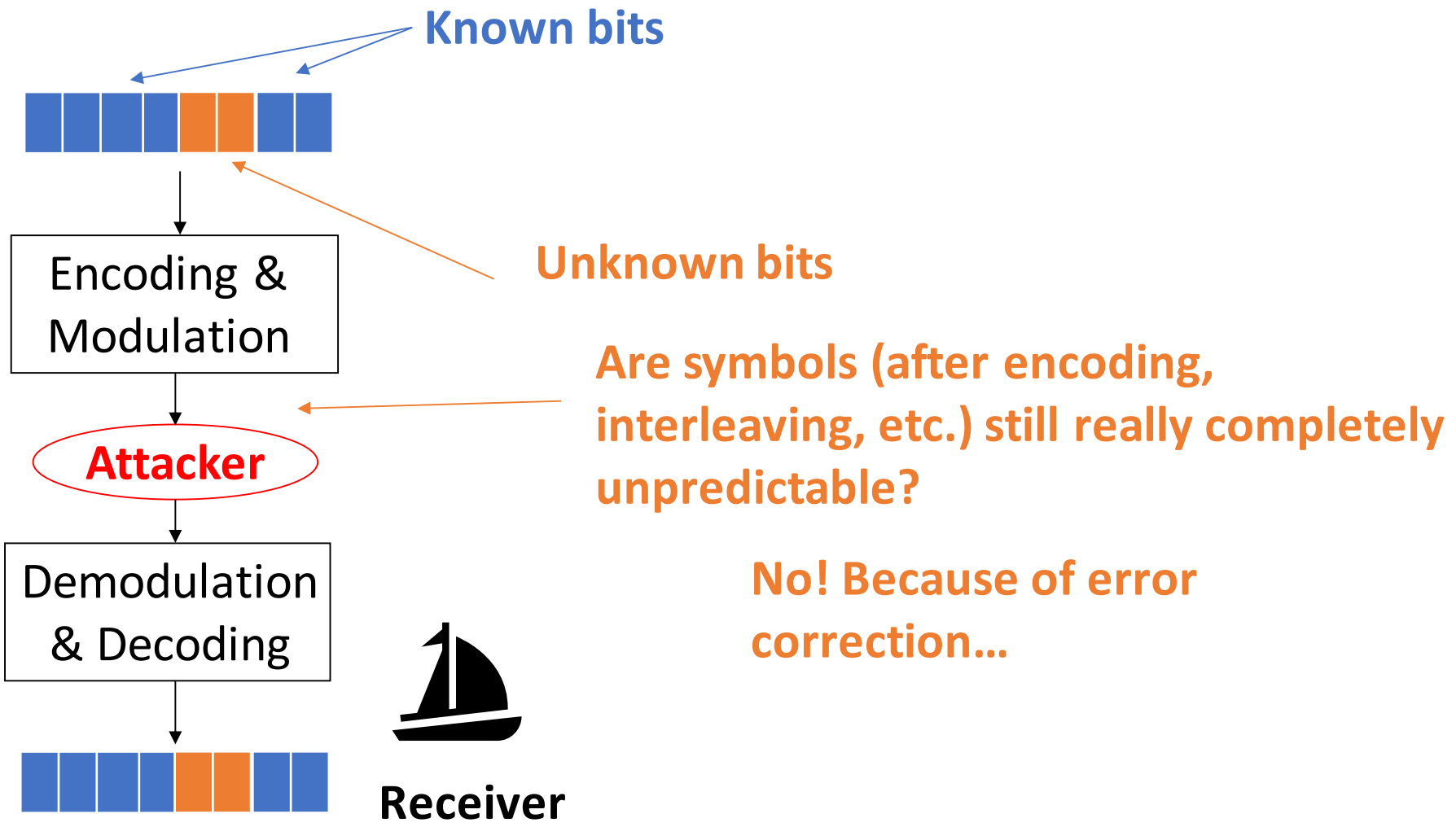
Kewei Zhang and Panos Papadimitratos, "On the Effects of Distance-Decreasing Attacks on Cryptographically Protected GNSS Signals," 2019, 363–72.

Kewei Zhang, "Secure GNSS-Based Positioning and Timing," 2021.

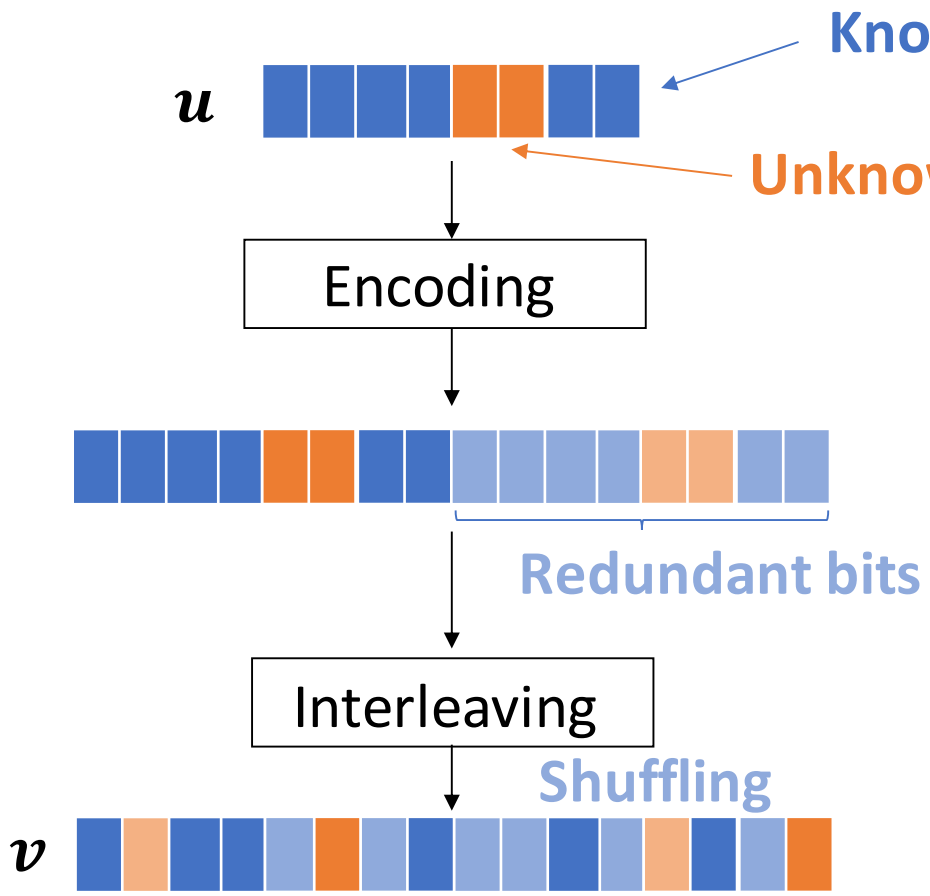
Forward Error Estimation Attack (Intuition)



Legitimate satellite



Forward Error Estimation Attack (Intuition)



Intuitively:

- $u = [d, q], v = f_{enc}(u), u = f_{dec}(v)$
- **Works even with some errors**

Not received yet

Known

Prediction is possible:

- $v' = f_{enc}(f_{dec}(v_0, \dots, v_k, x, \dots, x, d))$

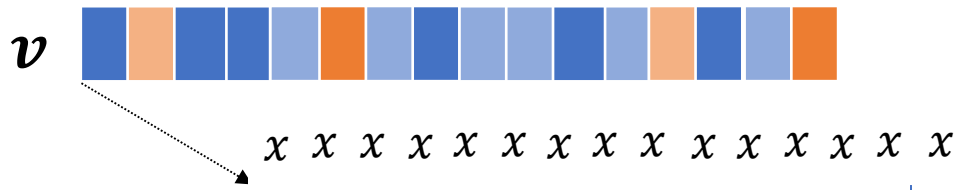
Partial reception of v

James T. Curran and Cillian O'Driscoll, Message Authentication as an Anti-Spoofing Mechanism, 2017.

James T. Curran and Cillian O'Driscoll, "Message Authentication, Channel Coding & Anti-Spoong," 2016.

Cillian O'Driscoll and Ignacio Fernández-Hernández, "Mapping Bit to Symbol Unpredictability in Convolutionally Encoded Messages with Checksums, with Application to Galileo OSNMA," 2020.

Forward Error Estimation Attack (Intuition)



Attacker's RX

Attacker's TX

And so on… Prediction gets more and more accurate

$v_1' v_2' v_3'$

Predict $v_3' = f(v_1, v_2, d)$

Guess

Predict $v_2' = f(v_1, d)$

The signal is accepted by the receiver in advance, despite some errors

James T. Curran and Cillian O'Driscoll, Message Authentication as an Anti-Spoofing Mechanism, 2017.

James T. Curran and Cillian O'Driscoll, "Message Authentication, Channel Coding & Anti-Spoong," 2016.

Cillian O'Driscoll and Ignacio Fernández-Hernández, "Mapping Bit to Symbol Unpredictability in Convolutionally Encoded Messages with Checksums, with Application to Galileo OSNMA," 2020.

Some References

Jolyon Clulow et al., “So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks,” in Security and Privacy in Ad-Hoc and Sensor Networks, ed. Levente Buttyán, Virgil D. Gligor, and Dirk Westhoff, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2006), 83–97, https://doi.org/10.1007/11964254_9.

Kewei Zhang and Panos Papadimitratos, “On the Effects of Distance-Decreasing Attacks on Cryptographically Protected GNSS Signals,” 2019, 363–72, https://doi.org/10.33012/2019.16736.

Kewei Zhang, “Secure GNSS-Based Positioning and Timing,” 2021.

James T. Curran and Cillian O’Driscoll, Message Authentication as an Anti-Spoofing Mechanism, 2017, https://doi.org/10.13140/RG.2.2.28625.12640.

James T. Curran and Cillian O’Driscoll, “Message Authentication, Channel Coding & Anti-Spoong,” 2016, https://doi.org/10.33012/2016.14670.

Cillian O’Driscoll and Ignacio Fernández-Hernández, “Mapping Bit to Symbol Unpredictability in Convolutionally Encoded Messages with Checksums, with Application to Galileo OSNMA,” 2020, 3751–65, https://doi.org/10.33012/2020.17715.

We saw that Galileo OSNMA does not fully protect against shifting signals…

Are there other ways?

Kuhn's proposal (prior to Galileo OSNMA)

Hidden markers & delayed disclosure

- Hide a marker for each satellite
- Low power, hidden in noise
- Secret spreading code
- Satellites reveal their code later, with a signed message, very similar to delayed authentication in Galileo OSNMA

Pros

- It detects signal synthesis AND individual time shifts

Cons

- Relay/replay of all satellites at the same time still possible
- Selective delay still possible if using at least 4 high-gain selective antennas

Markus G. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals," in Information Hiding, ed. Jessica Fridrich, vol. 3200, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer Berlin Heidelberg, 2004), 239–52, https://doi.org/10.1007/978-3-540-30114-1_17.

Some References

Markus G. Kuhn, “An Asymmetric Security Mechanism for Navigation Signals,” in Information Hiding, ed. Jessica Fridrich, vol. 3200, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer Berlin Heidelberg, 2004), 239–52, https://doi.org/10.1007/978-3-540-30114-1_17.

Let’s wrap up

Recap

Add noise or jamming signal to degrade reception

Attack

- Jamming signal
- Signal cancellation
- Spoofing
- Relay/Replay

Subtract a copy of the legit signal to cancel it out

Generate a rogue signal following the specs

"Reuse" a legit signal, but at the wrong time/place

- Early Detection Late Commit
- Forward Error Estimation

Methods to send signals earlier even if you don't know the data bits a priori

Somehow detect inconsistencies at reception, possibly using multiple sources

Defense

- Non-cryptographic
  - Signal characteristics
  - Multiple antennas/locations
  - Auxiliary information
- Cryptographic
  - Encrypted code
  - Message authentication

Try to prevent/detect time shifts and non-authentic messages

Conclusion

An arm's race

The simplest vanilla version of GNSS is vulnerable to simple attacks

Arms race to add non-cryptographic mitigations at the receiver

Arms race to add cryptographic countermeasures in the systems

Still open problems

Secure positioning

A broadcast system like GNSS cannot be fully secured assuming a DY attacker

Secure positioning requires:

Either… bidirectional communication

Or… communication with the infrastructure

Questions?