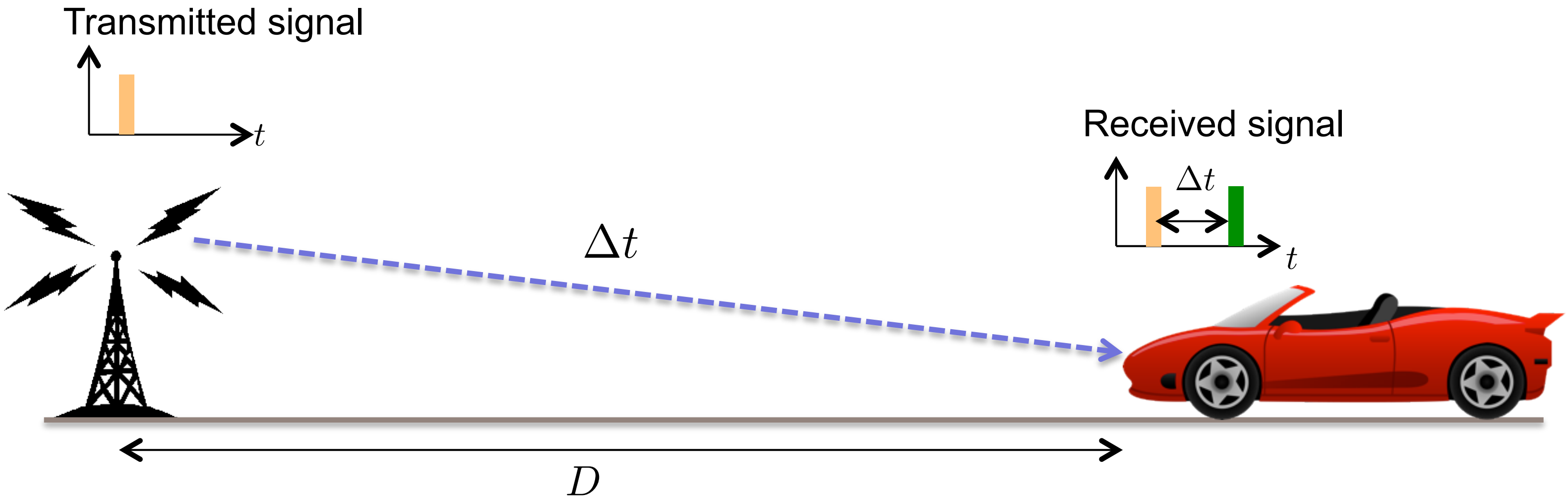
Security of Global Navigation Satellite Systems (GNSS)

GPS Fundamentals
GPS Signal Spoofing Attack
Spoofing Detection Techniques

Global Navigation Satellite Systems (GNSS)

- Umbrella term for navigation systems using satellite data for their operation
- Major systems
  - GPS (USA)
  - Galileo (Europe)
  - GLONASS (Russia)
- Differs in carrier frequency and data modulation methods.
- Navigation solution estimation methods are similar.

Time-of-flight (ToF) based Distance Estimation



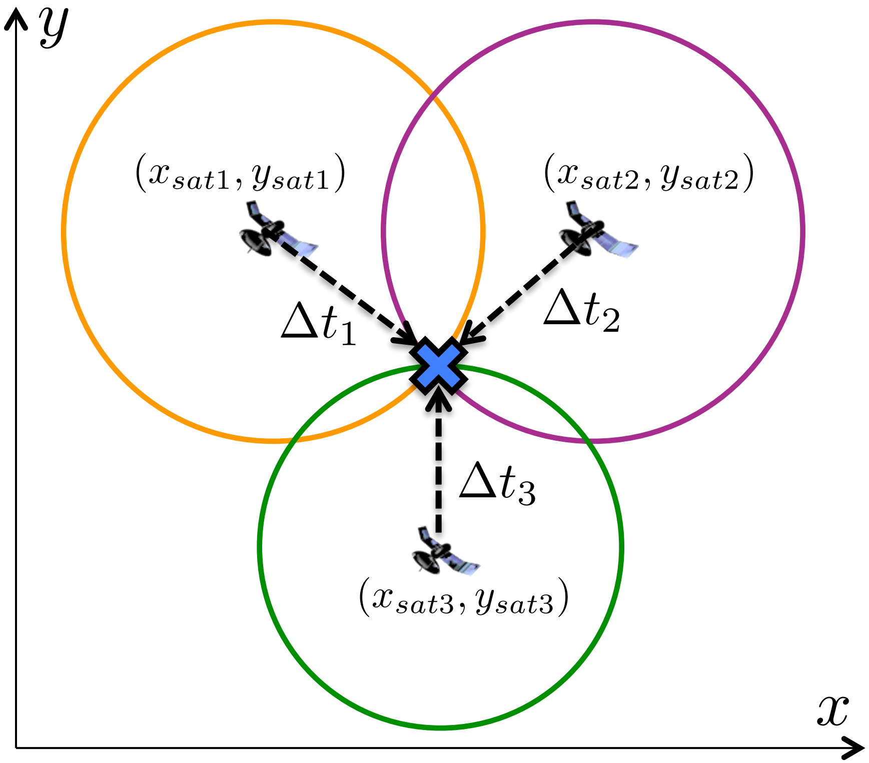
$D = c \cdot \Delta t$, where c is the speed of light (3x10^8 m/s)

The clocks at both the transmitter and receiver needs to tightly in sync. Sync error of 1us between the Tx and Rx results in distance estimation error of ~300 m.

* Adapted from uBlox GPS manual

2D Trilateration

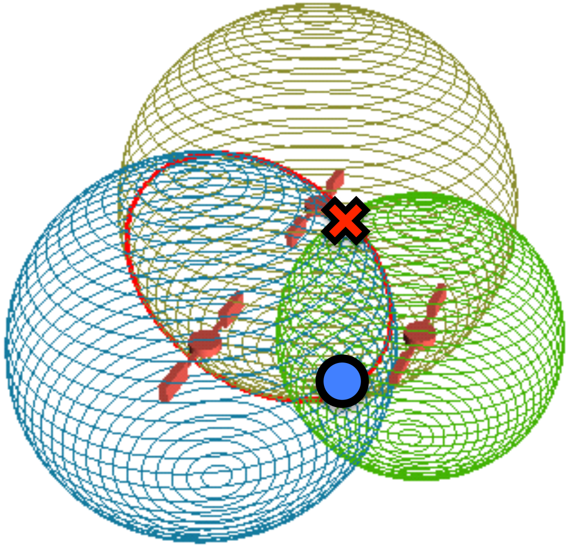
- User location determined based on distances
  - Not to be confused with *triangulation* (which involves measurement of angles)



(x_{sati}, y_{sati})	Known transmitter locations
Δt_i	Signal transit times
$R_i = c \cdot \Delta t_i$	Distance from the transmitter
(x, y)	Receiver location

$$R_1 = \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y)^2}$$
$$R_2 = \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y)^2}$$
$$R_3 = \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y)^2}$$

Trilateration in GPS

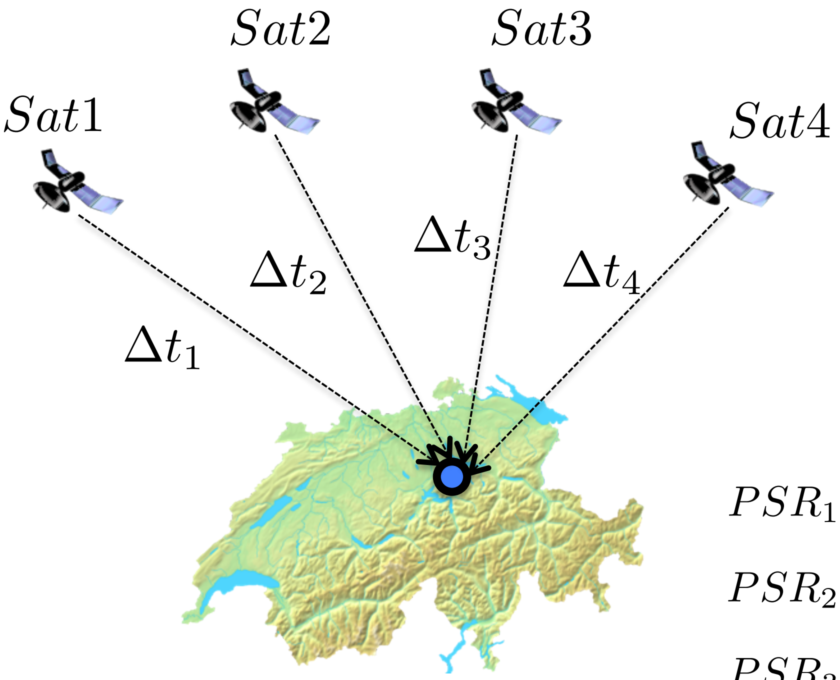


- 3 spheres intersect at 2 distinct points.
- One of the points is usually discarded since it will be far away from earth.

But, we require four satellites to determine an user's location. Why? *Hint: Time*

- Satellites have atomic clocks on-board and hence, the time of transmission of the GPS signal is known precisely.
- The receiver clocks are not atomic and not tightly synced to that on the satellites which introduces error in the TOA measurement at the receiver.
  - ✧ 1 us → 300 m error in position estimation
- Hence, a fourth pseudorange (truerange+clock error) measurement is used to determine the correct user location.

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

$$PSR_1 = \sqrt{(x_{sat1} - x)^2 + (y_{sat1} - y) + (z_{sat1} - z)^2} + c \cdot \tau$$

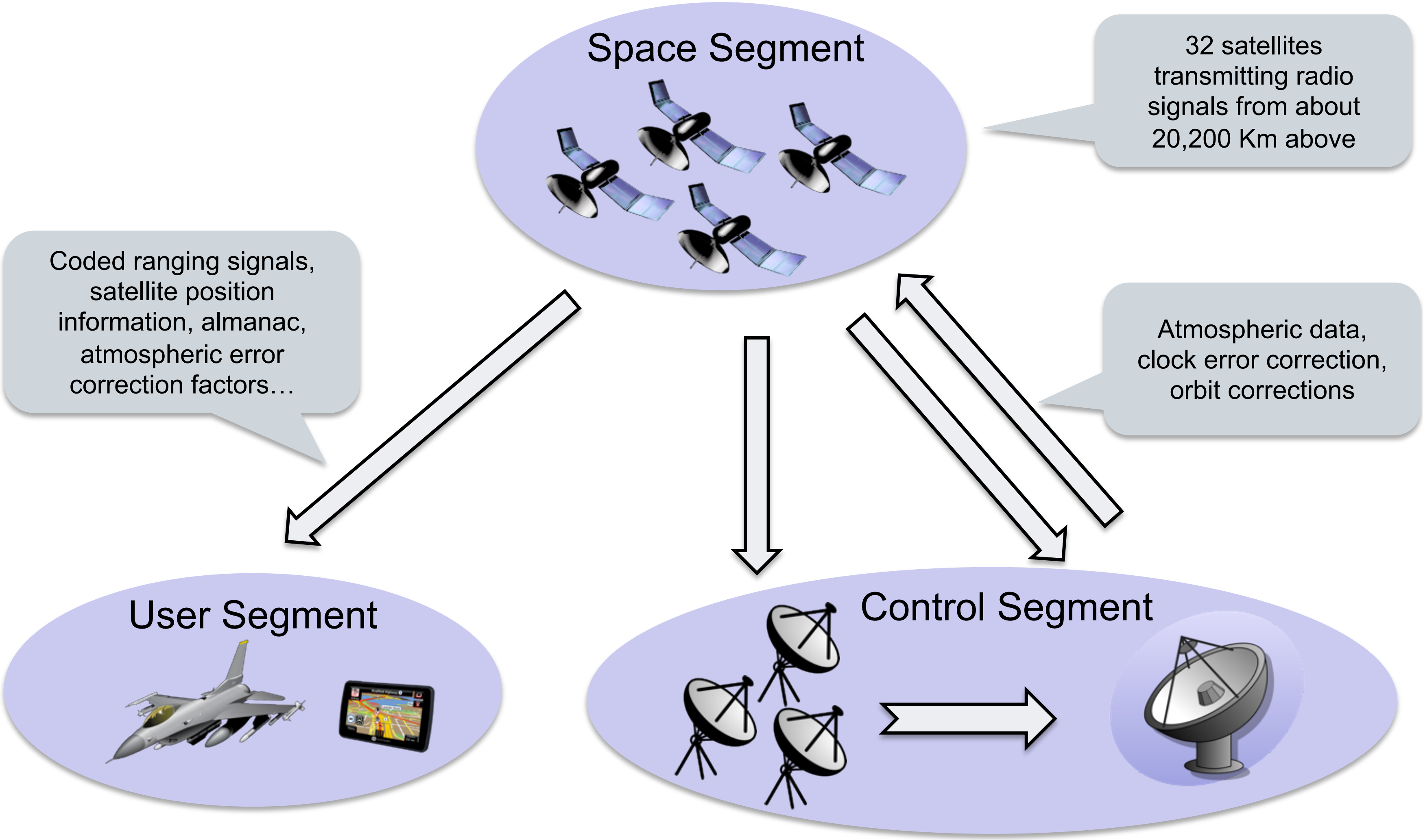
$$PSR_2 = \sqrt{(x_{sat2} - x)^2 + (y_{sat2} - y) + (z_{sat2} - z)^2} + c \cdot \tau$$

$$PSR_3 = \sqrt{(x_{sat3} - x)^2 + (y_{sat3} - y) + (z_{sat3} - z)^2} + c \cdot \tau$$

$$PSR_4 = \sqrt{(x_{sat4} - x)^2 + (y_{sat4} - y) + (z_{sat4} - z)^2} + c \cdot \tau$$

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

Global Positioning System (GPS)



Space Segment

32 satellites transmitting radio signals from about 20,200 Km above

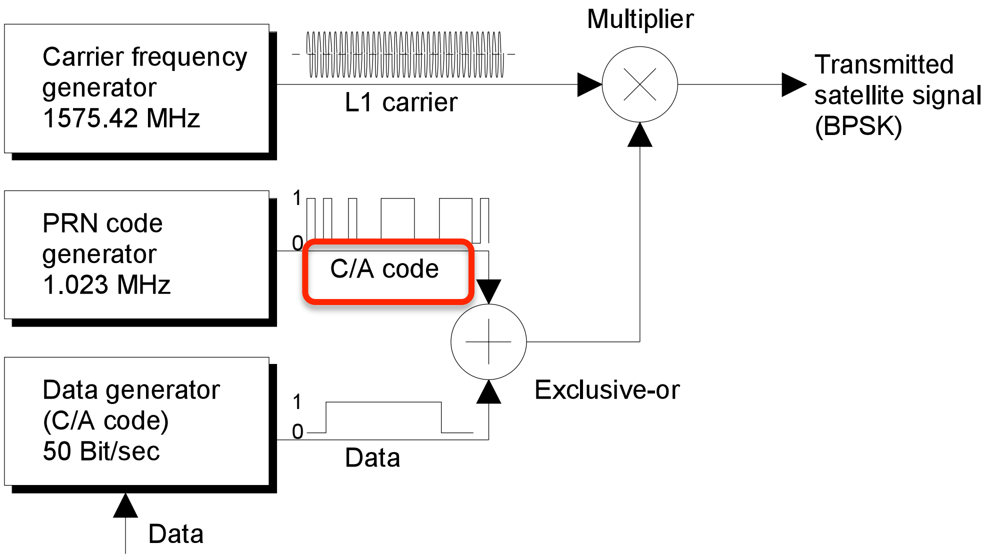
Coded ranging signals, satellite position information, almanac, atmospheric error correction factors…

Atmospheric data, clock error correction, orbit corrections

User Segment

Control Segment

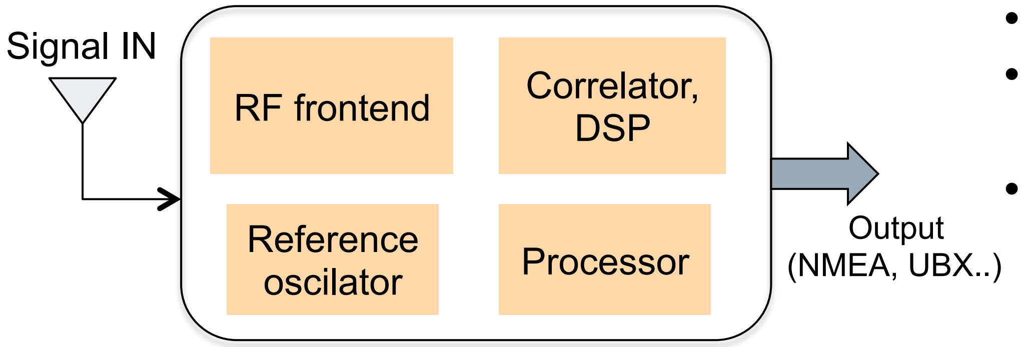
GPS Satellite Signal Structure and Generation


Carrier frequency generator 1575.42 MHz
L1 carrier
Multiplier
Transmitted satellite signal (BPSK)
PRN code generator 1.023 MHz
1
0
C/A code
Exclusive-or
Data generator (C/A code) 50 Bit/sec
1
0
Data
Data

- Civilian GPS data is transmitted on the 1575.42 MHz carrier.
- Each satellite uses a unique pseudorandom code (C/A code) to spread its data (DSSS).
- Each civilian C/A code is 10,230 bits long and is public.
- Military uses 767,250 bits long secret pseudorandom code for spreading.

Data is transmitted at 50 bps and contains information such as orbital data for all satellites (ephemeris and almanac), atmospheric error correction factors, satellite health…

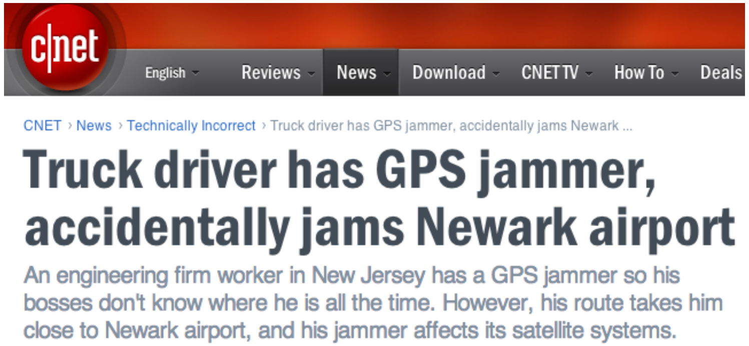
Typical GPS Receiver



- The GPS signal travels ~20,000 Km.
- Typical received signal power is -130 dBm (100x10^{-18} Watts).
- RF Frontend: Pre-amplification, filtering, intermediate frequency conversion.

- Correlating the received signal with each of the pseudorandom (PRN) code ascertains the signal transit time.
- Correlation additionally improves the signal to noise ratio ("amplifies") the signal above the standard noise level.
- Processor calculates the position and time and outputs the information in different formats (NMEA, UBX,SiRF etc.)

Physical-layer Security of GPS Systems

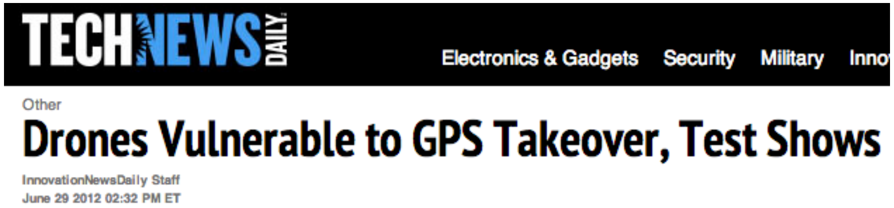


CNET › News › Technically Incorrect › Truck driver has GPS jammer, accidentally jams Newark ...

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

University of Texas team takes control of a yacht by spoofing its GPS



Other

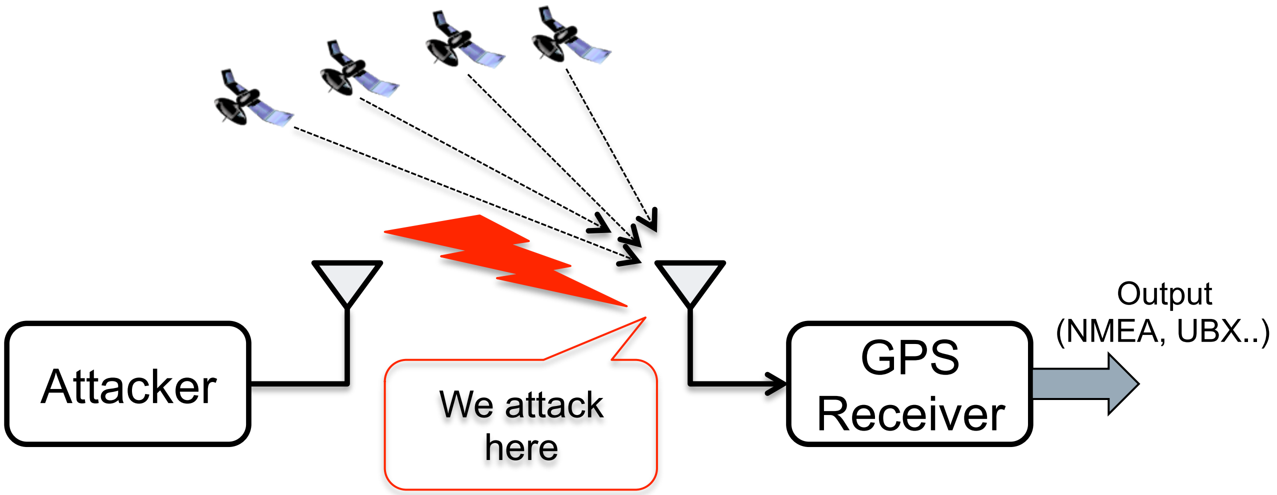
Drones Vulnerable to GPS Takeover, Test Shows

InnovationNewsDaily Staff
June 29 2012 02:32 PM ET

Security of GPS Systems

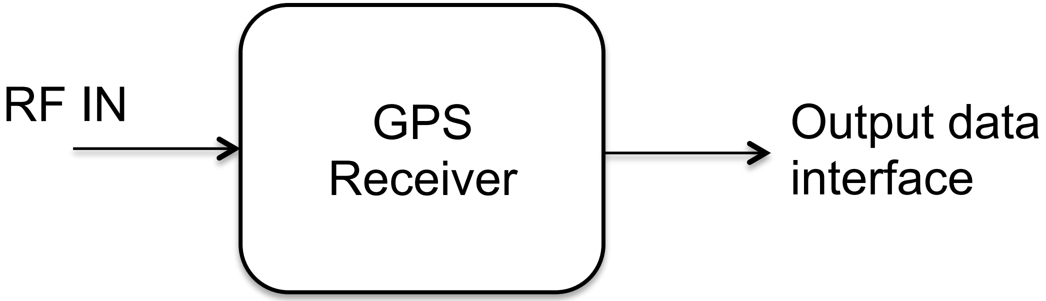
- The pseudo code used by the satellites to transmit data are public.
- No means of authenticating GPS signal.
  - Galileo offers authentication to “premium” users
- Commercial GPS signal simulators are available.
  - Typically used for development and testing of GPS modules
  - Capable of record and replay, real time GPS signal generation for static and dynamic (route simulation) scenarios, configurable power levels and so on..

Signal Spoofing Attack on GPS



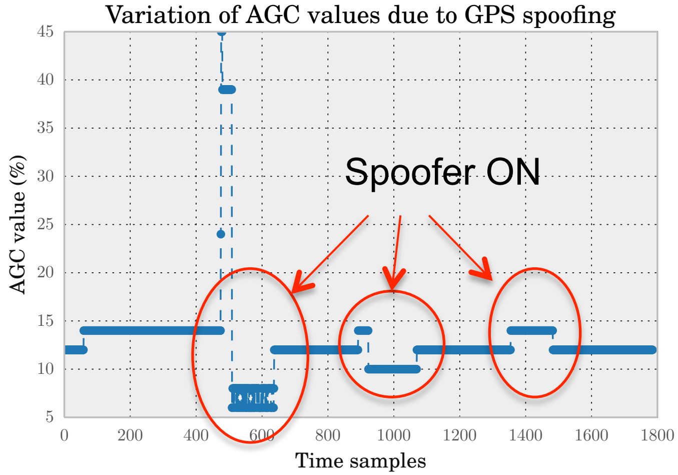
- **GPS signal spoofing**
  - Attack is at the physical layer (not a software/application layer attack).
  - Fake GPS signals are transmitted at a higher power.
  - The signals are crafted such that they are identical to the satellite signals potentially received at the spoofed location.
  - The GPS receiver processes the spoofed signals and computes the location (which will result in a new spoofed location different from the actual location of the receiver.

GPS Spoofing Detection Methods

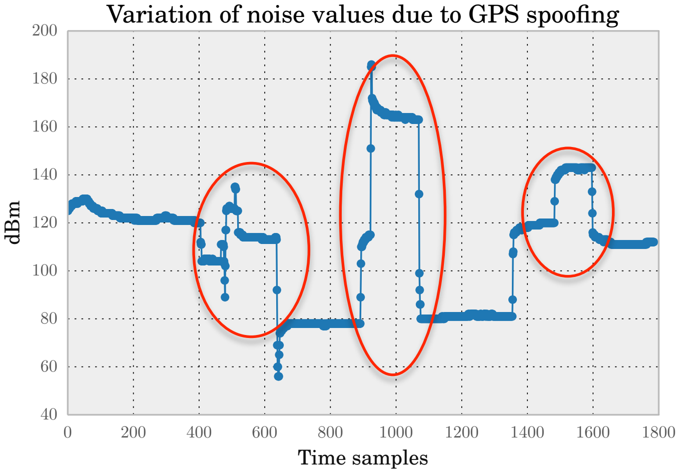


- **Common receiver observables based**
  - Standardized data exchange format (e.g., NMEA) outputs information such as geographic position (lat, long, alt), #visible satellites, time and date, received signal strength from each of the visible satellite etc.
  - Several detection schemes based on the above have been proposed.
  - No modifications to the receiver required.
- **RF signal physical characteristics based**
  - Estimating Angle of arrival, carrier phase based detection (introducing random antenna motion)…
  - Requires modification to the receiver signal processing hardware.

Receiver Observables Based Spoofing Detection Schemes



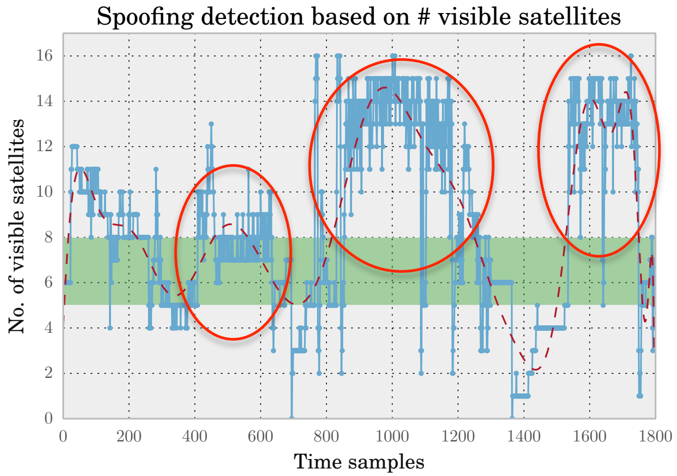
Automatic Gain Controller* varies the gain of the internal amplifier so as to account for the dynamic nature of GPS input signal.
Gain is increased for weak input signals and reduced for stronger signals (to prevent saturation)



Typical **noise floor level** is around -120 dBm. Presence of a nearby spoofer could cause distinct changes to the observed noise level.

* ***Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC)***, *Dennis M Akos., Journal of Navigation.*

Receiver Observables Based Spoofing Detection Schemes



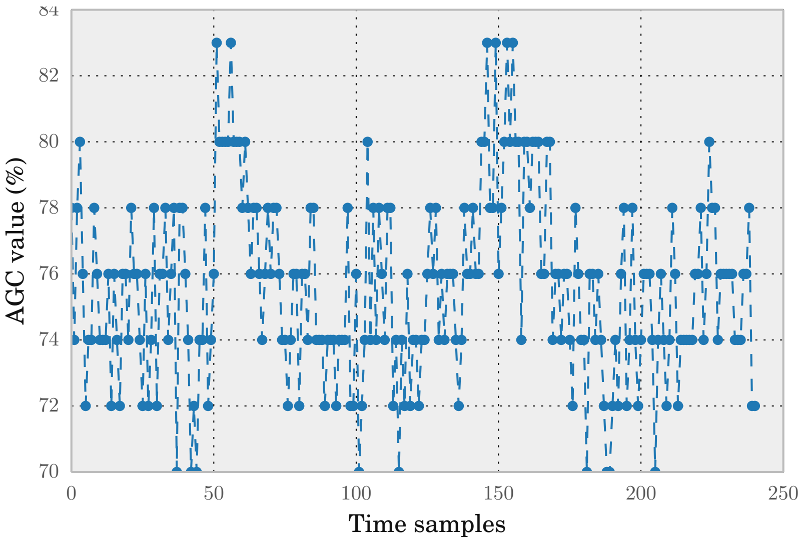
During spoofing, the number of visible satellites can increase beyond a certain threshold. Typically, 4-8 satellites are visible.

Is GPS spoofing still a threat? Drawbacks?

GPS Spoofing: Dynamic Scenario

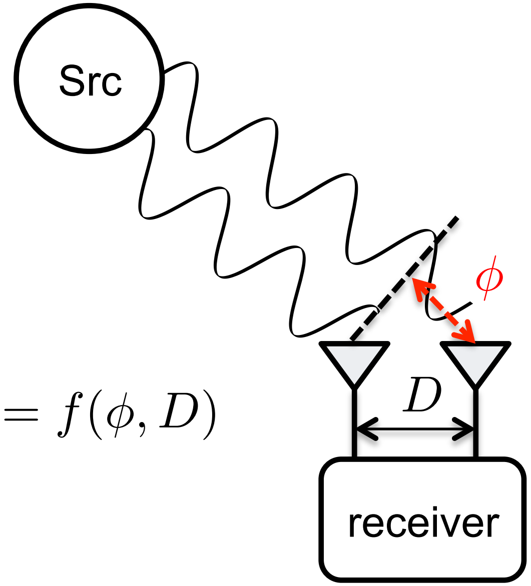
- **Previous Experimental Setup**
  - Receiver was static (no movement)
  - No external interference
  - Little disturbance from the environment

In a real-world dynamic scenario…

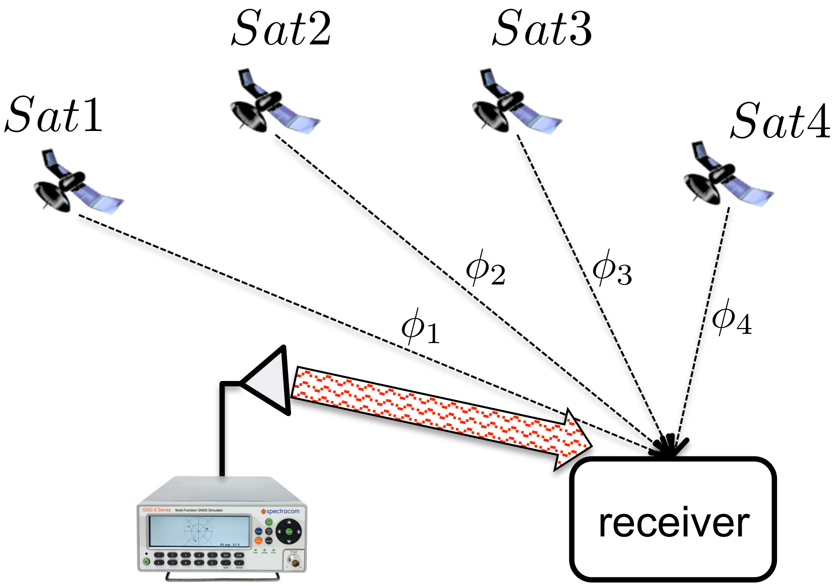


Multipath reflections, other radio interferences, weather changes (cloudy vs clear skies)

Angle of Arrival based GPS Spoofing Detection



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



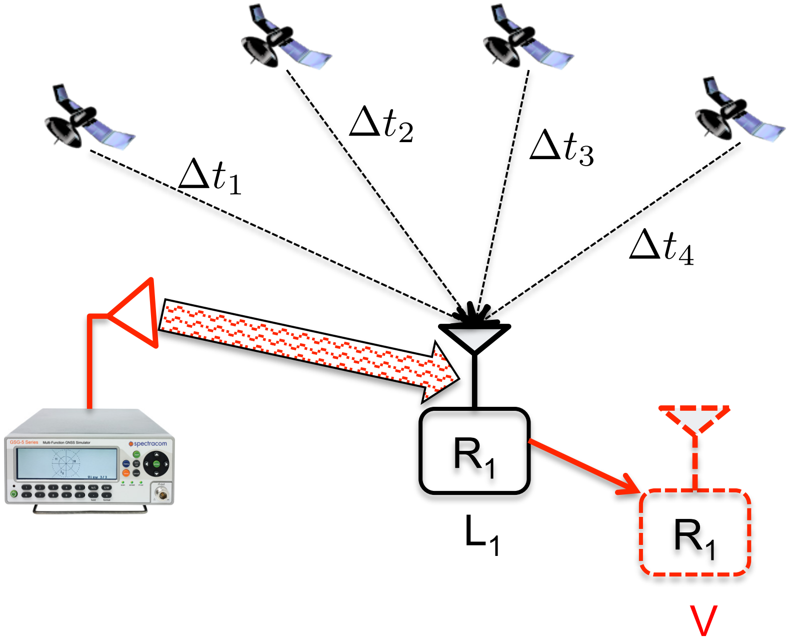
Angle of arrival is a function of the measured signal phase difference (Φ) at both the antennas and their separation D.

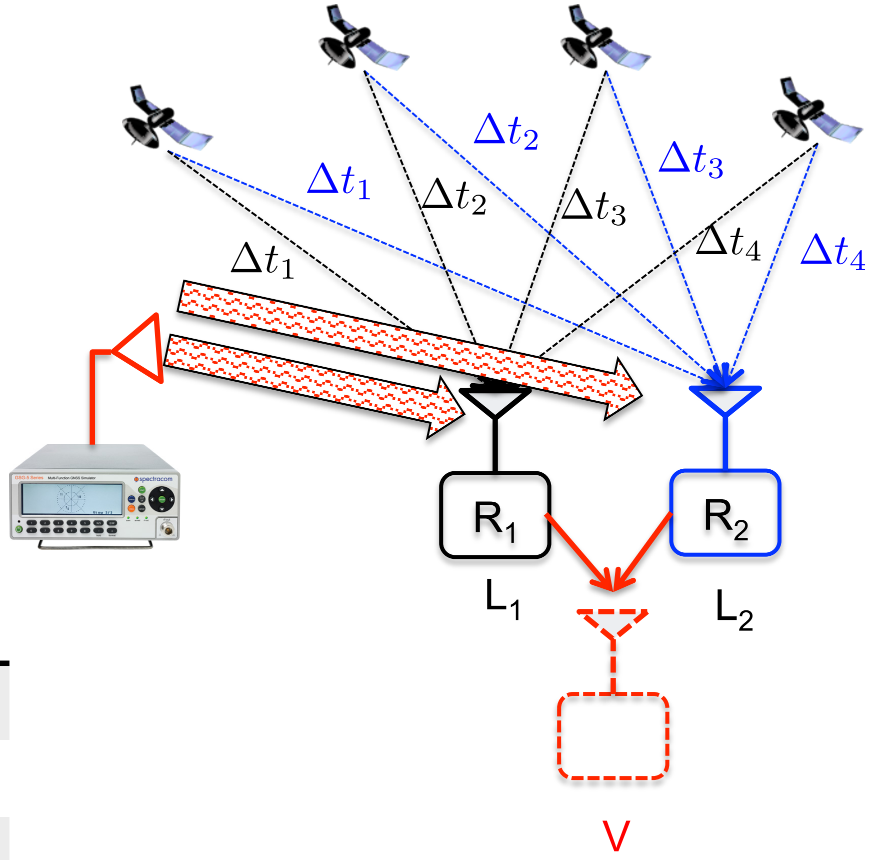
Spoofed scenario: $\phi_1 \sim \phi_2 \sim \phi_3 \sim \phi_4$

Phase measurement is computationally expensive and requires receiver hardware modifications.

*Montgomery, P.Y., T.E. Humphreys, B.M. Ledvina, "**A Multi-Antenna Defense Receiver-Autonomous GPS Spoofing Detection**," InsideGNSS, 2009.*

A Multi-Receiver Approach



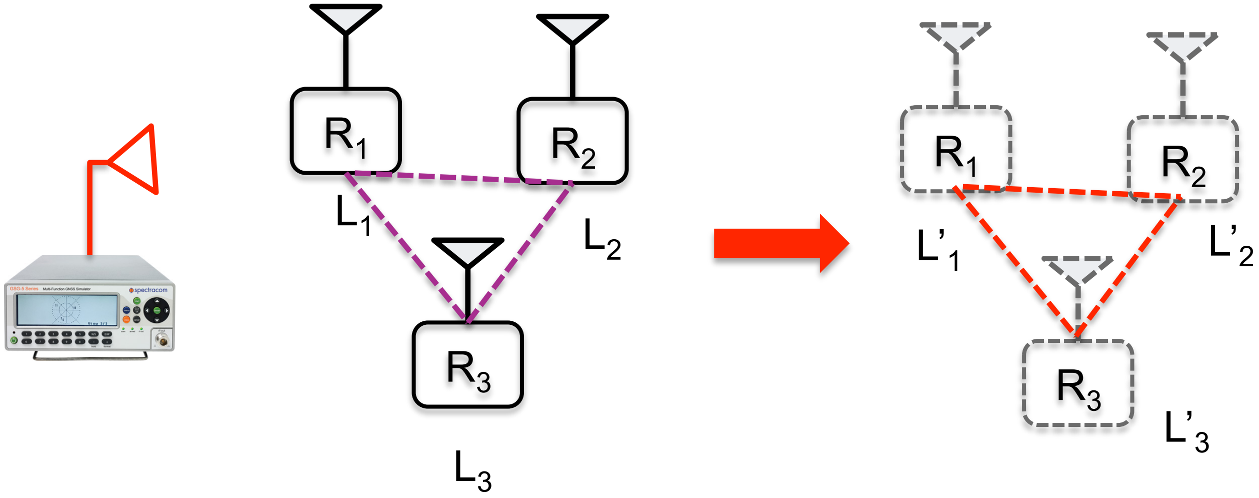


Δt_i	Signal transit times
L_i	Receiver locations
V	Spoofed location

Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, Srdjan Capkun, “**On the Requirements for Successful GPS Spoofing Attacks**”, In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2011

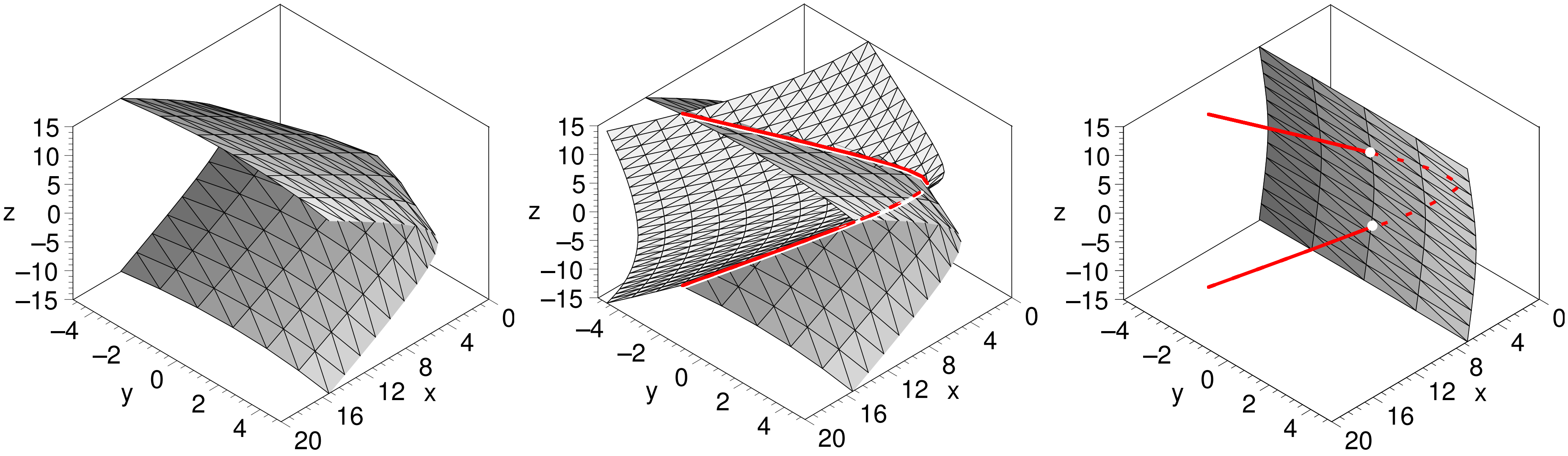
Group Spoofing Problem

“The GPS Group Spoofing Problem is the problem of finding combinations of GPS signals (sent by the attacker), transmission times (when the spoofing signals are sent), and physical transmission locations (from where the attacker transmits) such that the location or time of each victim is spoofed to the desired location.”



L’$_l$ are spoofed locations

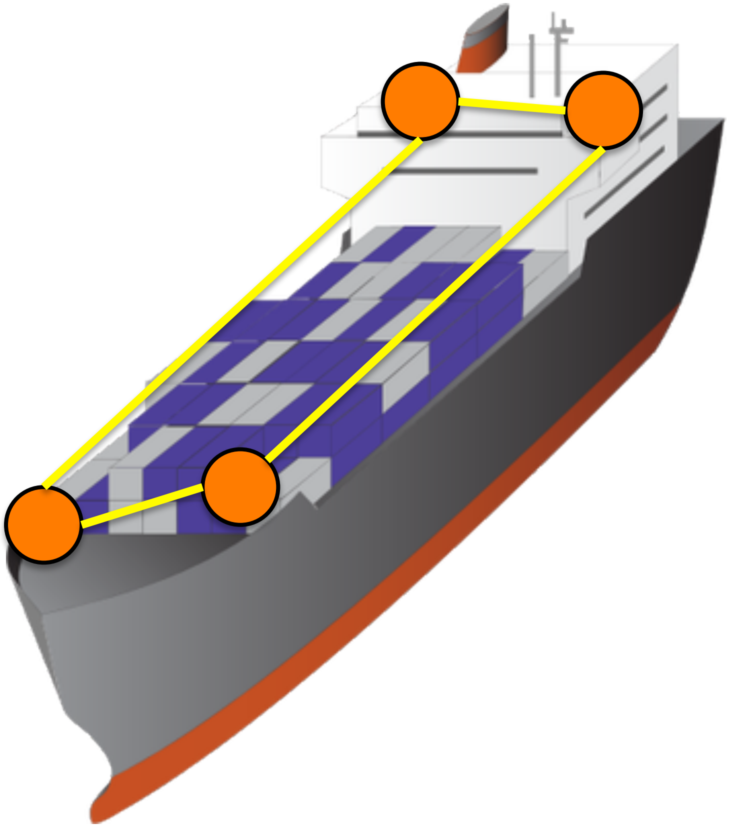
Group Spoofing: Possible Attacker Positions



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

	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

Multi-receiver Spoofing Countermeasure



The GPS receivers are setup on a cargo ship with a known formation and the receivers exchange their location information between them. If the reported individual locations do not match the known formation then a possible spoofing attack can de detected.

● GPS Receivers

Ongoing Work

- Effectiveness of the multi-receiver countermeasure in real-world high multipath environment.
- Feasibility of group spoofing using multiple spoofers
- Effectiveness of receiver observable based spoofing detection schemes in various environmental conditions.
- Generalization of the group spoofing problem for ‘n’ receivers.