UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Detecting Spoofing Events by Comparing Reconstructed Positions of E1b and E5a Galileo Signals

Giulio Scattolin

Stefano Tomasin

Smartphone vulnerability

- Leakage of GNSS signals at ION GNSS+2017 Conference:
  - abnormal behaviors on numerous smartphones
  - detecting and understanding of the incident took hours

- Undetected attacks against current Android and iOS devices:
  - spoofing to very remote locations (a continent away)
  - corruption of the navigation signal

- Now - warfare spoofing affecting other regions: navigation in the Caspian sea affected by the war in Syria
- Future - possible use of spoofing by criminals

- Many applications in smartphone are based on GNSS information: we need to protect them from such vulnerability

Spoofing detection

- Protection against spoofing: detect its presence

- Multiple solutions:
  - Authenticate the GNSS signal (e.g., using the Galileo Open Service Navigation Message Authentication)
  - Checking the integrity of the GNSS signal
  - Cross-checking with other signals providing localization (e.g., cellular and WiFi signals)
  - Cross-checking all GNSS signals (e.g., consistency of satellites in view)

- **Integration** is the key: multiple solutions should be explored and possibly integrated in order to make attacks harder to go undetected

Nougat on the rescue

- 2016: GNSS raw measurements available to smartphone users since Android release 7 (Nougat)
- 2018: First dual-frequency GNSS smartphone
- Galileo has the majority of satellites with dual frequency capabilities
- Raw measurements already exploited for detection of spoofing attacks

Use-case scenario

- Attacker
  - Transmitting spoofed GNSS signals on a single carrier frequency at a time (i.e., Galileo E1b and / or GPS L1)
  - Not able to null the legitimate signals at the user device

- User device
  - Dual-frequency enabled (i.e., Galileo E1b / E5a + GPS L1 / L5 support)
  - Optimal signal reception on both carriers

- **NOTE** : We assume that the attacker does not transmit the fake satellite signals on ALL the bands, but only on some bands.
- Therefore, we can detect the attack by observing both fake and legitimate signals (on different bands).

Detection criteria #1

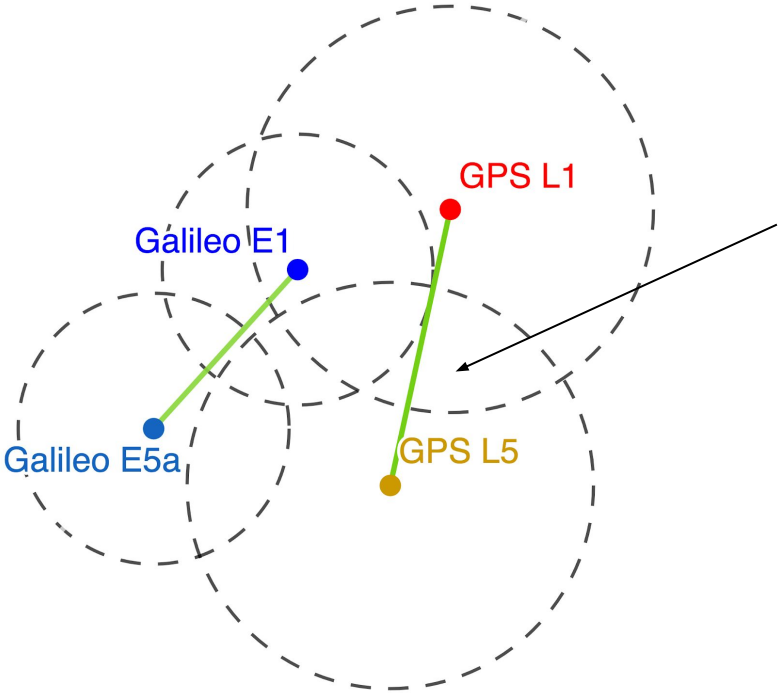


Fig.1 - Genuine scenario (no spoofing attack is undergoing).

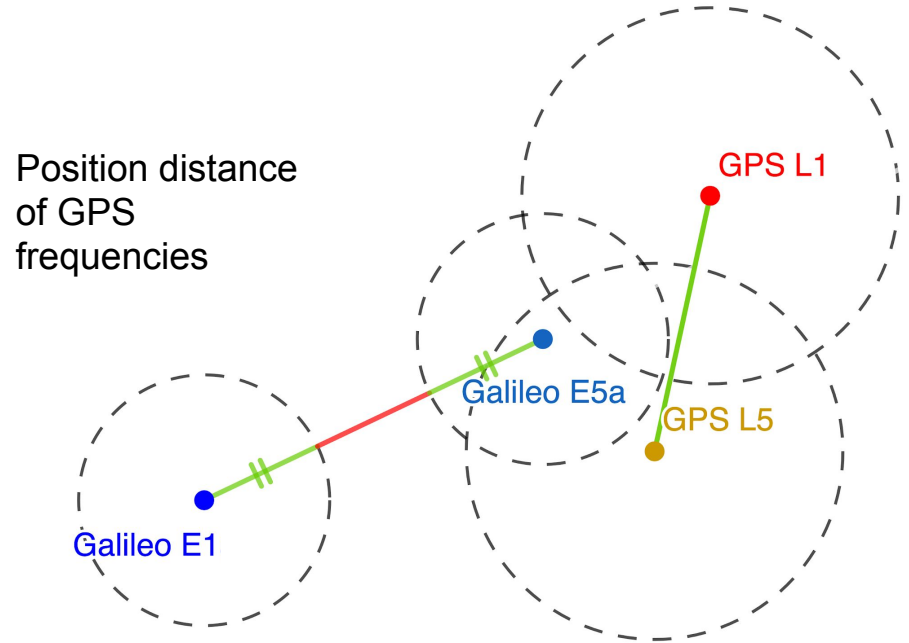
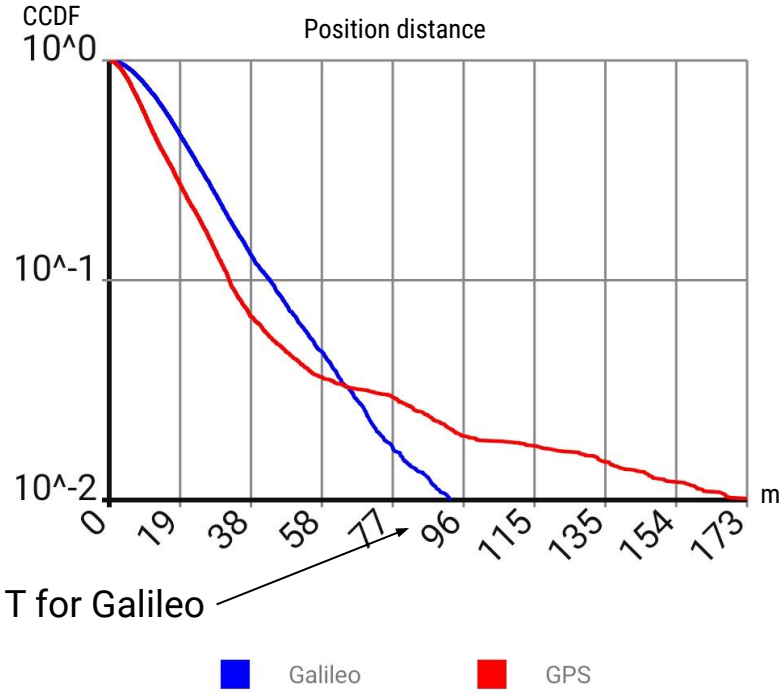


Fig.2 - Spoofing attack on Galileo E1b carrier frequency.

Threshold criterion

- Trigger a spoofing alarm when the position distance is larger than a threshold T
- Among possible criteria for the choice of T:
  - choose T such that the alarm is activated at most 1% of the tests in the absence of spoofing



Detection criteria #2

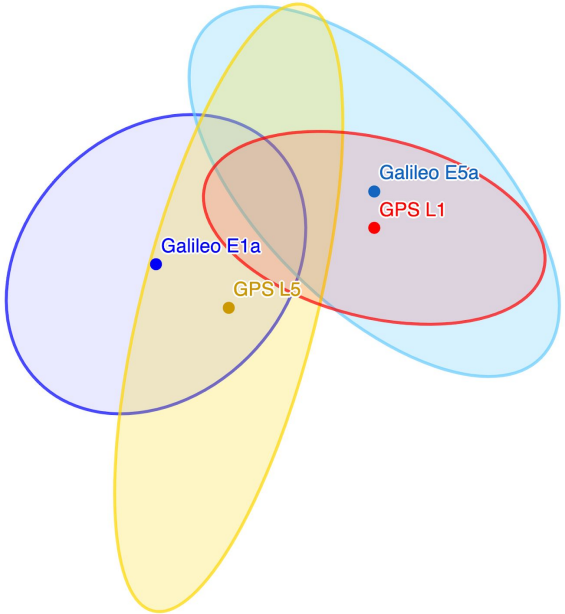
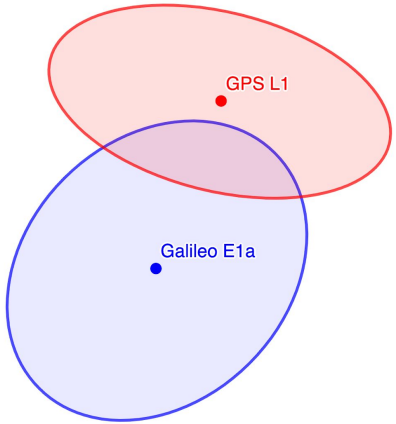


Fig.3 - Genuine scenario (no spoofing attack is undergoing).



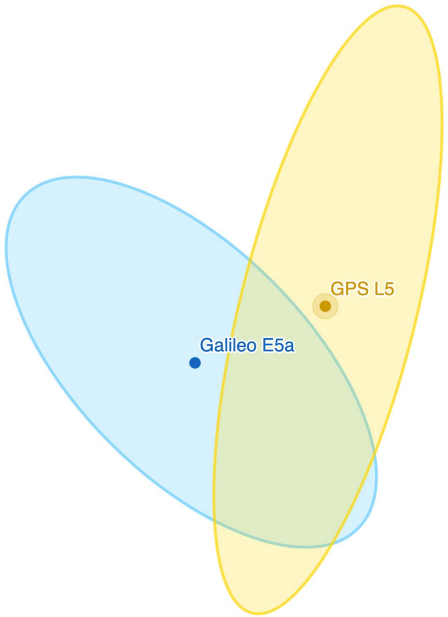


Fig.4 - Spoofing attack on both L1 and E1b carrier frequencies.

Detection algorithm

1) Reconstruct positions using subsets of satellites

2) Trigger an alarm if consistency criteria fail more than a fixed rate in a constant window

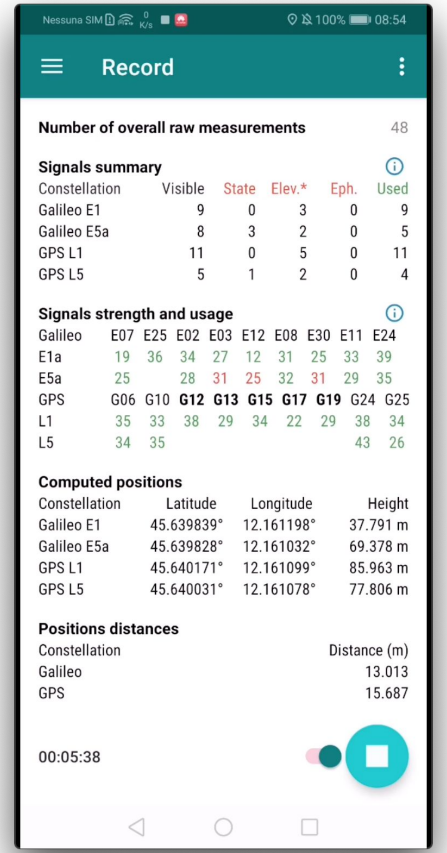
   a) For every system, reconstructed positions must be closer than an estimated threshold

   b) For every reconstructed position, all the confidence ellipses must overlap a common region

Android application

- An *all-in-one* app
  - records measurements and computed positions
  - estimates threshold parameters to guarantee a chosen confidence
  - runs detection algorithm
  - integrates ESA *GNSS Compare* application to compute positions and DOP matrices

Application footage



Features

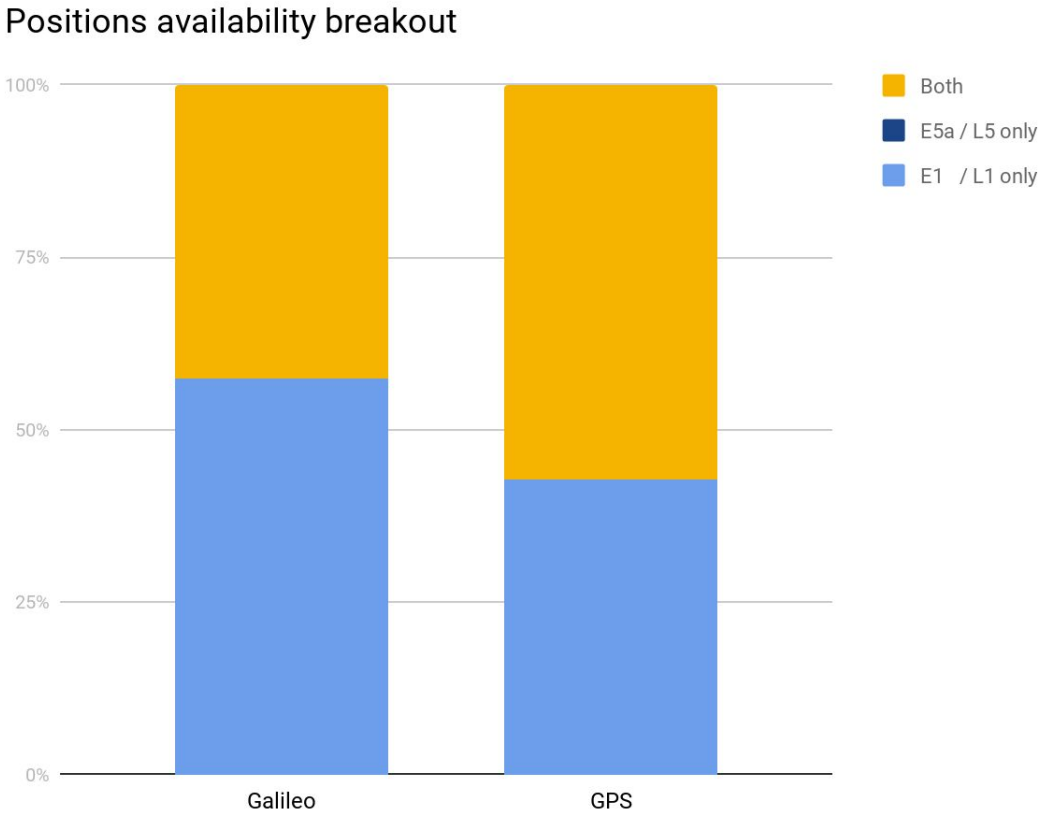
1) User must handle the situation manually, dismissing the alarm.

2) The user is warned a few seconds later the attack begins.

3) One or more legitimate positions may be still available.

4) Parallel evaluation of metrics for Galileo and GPS computed positions increase reliability.

Availability



Conclusions

- New spoofing detection app for smartphones
- Detection based on the consistency of estimated positions using set of satellite signals on different bands
- Criteria: distance between the reconstructed positions or overlapping of DOP ellipses
- Design criterion: ensuring a chosen false alarm probability
- App integrates *GNSS Compare* calculation modules to compute positions
- Future activity: integration with other spoofing detection techniques based on raw measurements

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Thank you.

giulio.scattolin@studenti.unipd.it
stefano.tomasin@unipd.it