ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

XXXV Cycle

Implementation and resilience test of a GNSS positioning system for road application

Akmal Rustamov

Supervisor: Prof. Fabio Dovis

Research context and motivation

- Due to the low received power of Global Navigation Satellite Systems (GNSS) signals, the performance of GNSS receivers can be disrupted by anthropogenic radio frequency interferences, with intentional jamming and spoofing activities being among the most critical threats. It is reported in the literature that modern, GNSS-equipped Android smartphones are generally resistant to simplistic spoofing, and many recent contributions support such a biased belief. It is more malicious than jamming, the false signals take control of the target receiver, and the victim is fooled without any notice and spoofing becoming easier:
  - Navigation signals properly designed to force the receiver to estimate a wrong fix;
  - Easy access to open-source software, that can implement a using a €200 hardware;
  - Mass market devices such as smartphones can be subject to spoofing since no specific countermeasures are implemented;
- Does android smartphone be actually spoofed, can it be used as a monitor of the spoofing attack implementing proper detection algorithms?

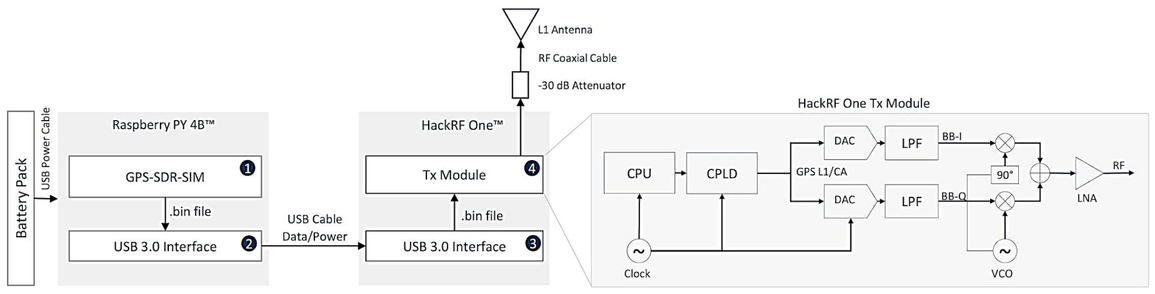
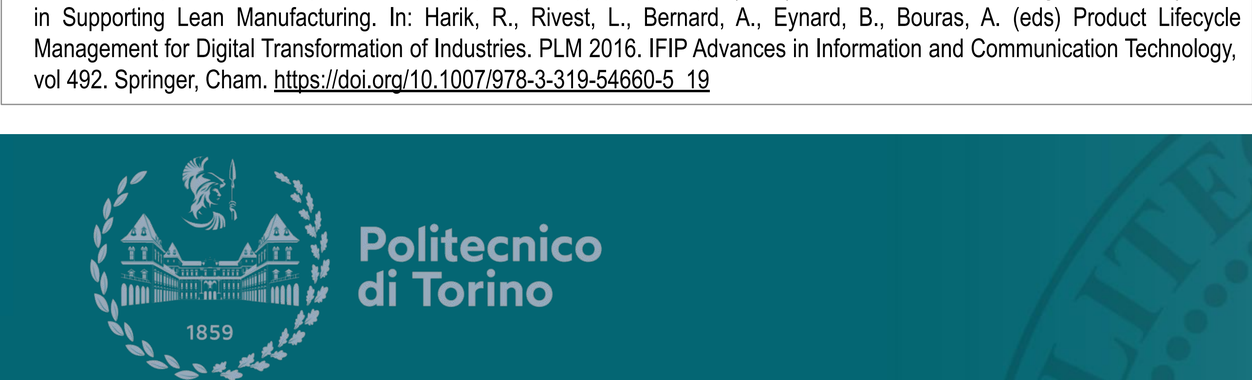


Fig. 1. High-level schematic of the low-cost portable spoofer.

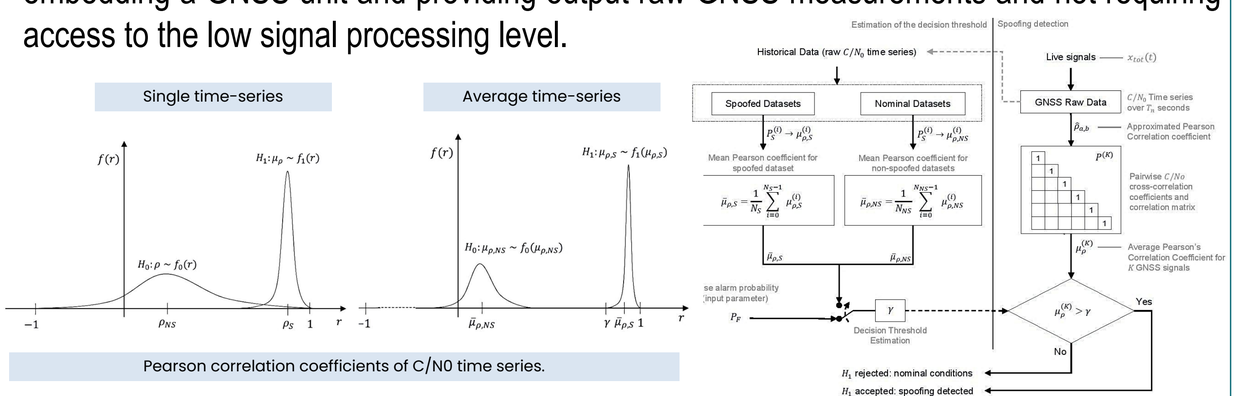
Addressed research questions/problems

- In our research, we take the smartphone platform as a reference case study, we propose and assess the performance of a technique for detecting single-antenna spoofing attacks. The proposed solution exploits the spatial and temporal correlation of the spoofing signals, and it is validated through an experimental campaign based on the analysis of the correlation of the raw output data provided by various Android smartphones. However, the same methodology can also, be applied to raw measurements provided by another kind of mass-market receivers;
- Vulnerability analysis and validation of the proposed technique were conducted in a controlled environment by transmitting realistic, fake Global Positioning System (GPS) L1/CA RF signals to a variety of Android smartphones. In the process, we show that, under proper conditions, the devices were vulnerable to the attacks and that the effects were visible through their raw measurements, i.e., Carrier-to-noise ratio (C/N0), pseudo-range measurements, and position estimates. In particular, the study demonstrates that cross-correlation between C/N0 time series provided by each device about different GNSS satellites increases under spoofing conditions, thus constituting a proper metric to detect the attacks.



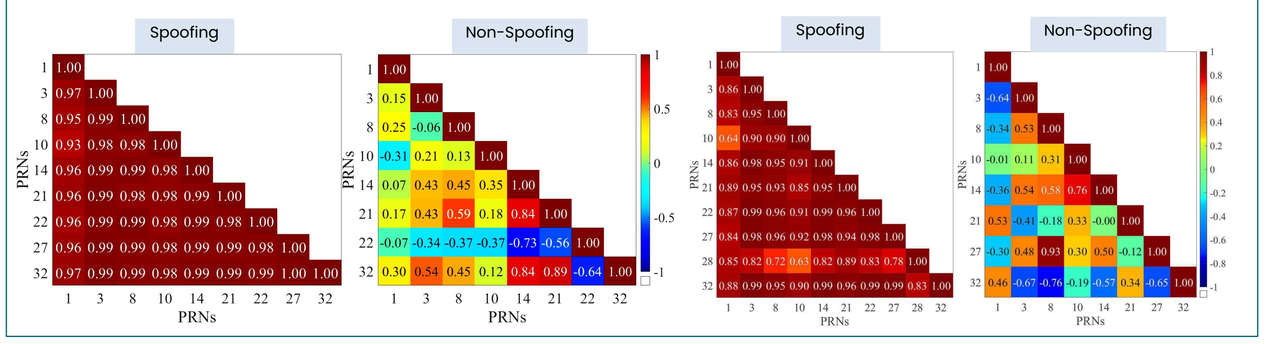
Novel contributions

- We presented resilience of devices to simplistic spoofing attacks and highlight their actual vulnerability. We then proposed an effective spoofing detection technique, that exploits the spatial and temporal correlation of the counterfeit signals by leveraging the statistical analysis of raw GNSS measurements. The proposed solution applies to devices embedding a GNSS unit and providing output raw GNSS measurements and not requiring access to the low signal processing level.



Adopted methodologies

- Implementation of the decision logic get main steps of the proposed algorithm are:
- 1) determining the correlation threshold, γ, under H0 and H1 hypothesis. γ can be estimated by fixing the false alarm probability;
- 2) comparing the current mean correlation coefficient μ (K) ρ estimated through real-time data over a window of TW s, with the threshold γ;
- 3) deciding for spoofing or non-spoofing conditions within the observed time window by accepting or rejecting H1 according to the Neyman-Pearson criterion.
- Pearson correlation increment varies depending on the dataset but is always experimentally verified which summarizes the remarkable difference between correlation coefficients under spoofed and non-spoofed time periods.



Future work

- We analyzed of the effects that single-antenna, simplistic spoofing has on the GNSS receivers embedded in Android™ smartphones, a spoofer detection technique based on the processing of raw measurement was proposed. The most relevant observation is that raw GNSS measurements.
- The estimation of the C/N0 for spoofed signals was indeed sensitive to the spatial and temporal correlation introduced by the spoofer transmission of multiple signals over a single propagation channel. Such a peculiar feature of single-antenna spoofing attacks made the difference w.r.t. received legitimate GNSS signals. It has been shown as the estimation of a mean Pearson correlation coefficient considering all the PRNs pairs provides a suitable metric for the detection of the attack.
- Future works will investigate the applicability of the technique to different classes of GNSS devices, exploring different conditions of the attacks and optimizing the size of the observation window to reduce spoofing detection latency.

Submitted and published works

- A. Rustamov, N. Gogoi, A. Minetto and F. Dovis, "Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices," 2020 International Conference on Localization and GNSS (ICL-GNSS), 2020, pp. 1-6, . https://doi.org/10.1109/ICL-GNSS49876.2020.9115489
- Rustamov, Akmal, Gogoi, Neil, Minetto, Alex, Dovis, Fabio, "GNSS Anti-Spoofing Defense Based on Cooperative Positioning," Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), September 2020, pp. 3326-3337. https://doi.org/10.33012/2020.17565
- A. Rustamov, A. Minetto and F. Dovis, “Improving GNSS spoofing awareness in smartphones via statistical processing of raw measurements”, in IEEE Sensors Journal, under review.
- D’Antonio, G., Sauza Bedolla, J., Rustamov, A., Lombardi, F., Chiabert, P. (2016). The Role of Manufacturing Execution Systems in Supporting Lean Manufacturing. In: Harik, R., Rivest, L., Bernard, A., Eynard, B., Bouras, A. (eds) Product Lifecycle Management for Digital Transformation of Industries. PLM 2016. IFIP Advances in Information and Communication Technology, vol 492. Springer, Cham. https://doi.org/10.1007/978-3-319-54660-5_19

List of attended classes

- 02LWHRV – Communication (23/01/2020)
- 01RISRV – Public speaking (25/01/2020)
- 01SWPRV – Machine learning for pattern recognition (25/01/2020)
- 01SYBRV – Research integrity (25/01/2020)
- 01SFURV – Programmazione scientifica avanzata in matlab (25/05/2020)
- 01TAGIU – Ubiquitous computing (03/06/2020)
- 01UJVRS – IoT platforms for spatial analytics in smart energy systems (19/05/2020)
- 01UOFRV – LabView-based programming toolchains for Power Electronics (19/02/2020)

Politecnico di Torino

PhD program in
Electrical, Electronics and Communications Engineering