Detection of GNSS jamming and spoofing using smartphones

Emile GHIZZO, PhD student
supervised by C. MILNER, J. LESOUPLE and C. MACABIAU

ENAC, TELECOM-SIGNAV, Toulouse, France

Context

Jamming and spoofing are growing threats for GNSS receivers, especially for civil aviation which requests not only a high level of accuracy but also of availability, continuity and integrity. Different models and detection techniques have been defined in function of the interference properties, such as cryptographic detection, signal-geometry-based detection [4] or detection based on drift monitoring [3] [2]. Since the introduction of raw GNSS measurements in android devices in 2016, smartphones have become a point of interest in GNSS related study including jamming and spoofing detection. In fact, smartphones provide an accessible GNSS receiver, coupled with numerous systems such as sensors, networks or telecommunication services which allow providing environment information. If low quality components are selected in smartphones, the diversity of environment information and the number of devices could increase performance detection. This thesis explores a smartphone crowd-source based jamming and spoofing detection techniques using machine learning algorithms. Machine learning is increasingly effective considering complex problems with numerous parameters, if GNSS reception and PVT computation is a well-defined problem, machine learning is already used in GNSS for multipath detection [1] [5] or atmosphere scintillation.

Main objectives

- Implementation of an Android application to collect smartphone data
- Review of the state of the art about GNSS structure and jamming/spoofing interference
- Review of the stae of the art about Machine learning
- Analysis of the collected data using machine learning and estimation algorithms
- Creation of a controlled jamming/spoofing broadcast in test smartphones
- Development of machine learning algorithm for single and centralized phones

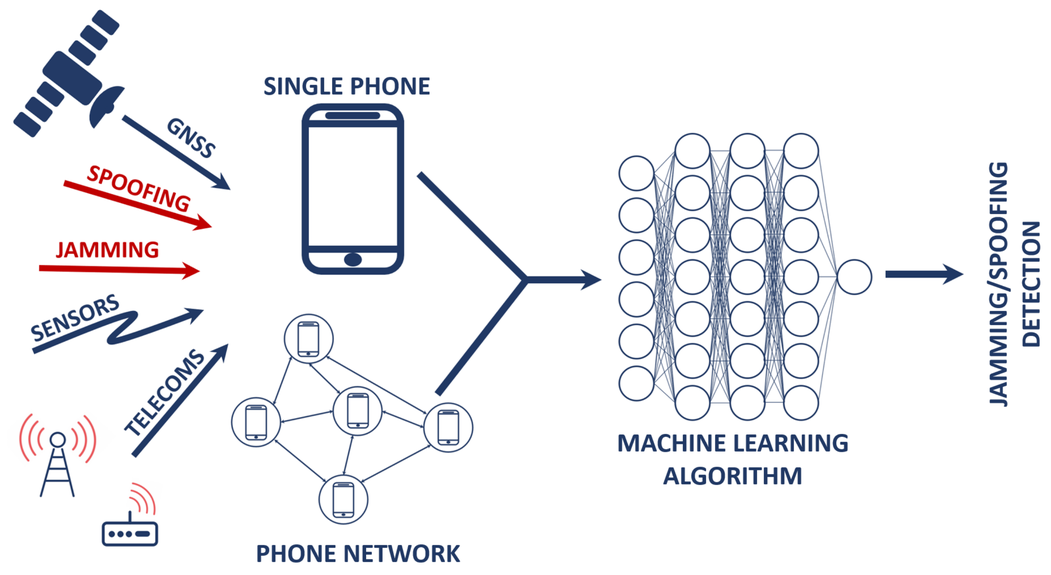

Figure 2: Thesis objectives diagram

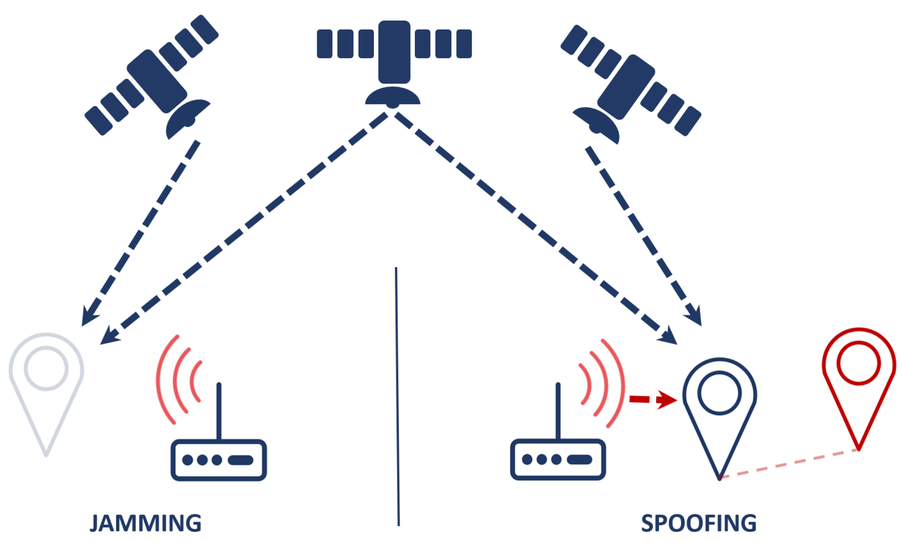

Figure 1: Jamming and spoofing illustration

GNSS jamming/spoofing definition

GNSS positioning uses trilateration to compute the receiver location from 4 received signals. GNSS signals have low power, which means that a weak interference source can cause the receiver to fail or to produce hazardously misleading information.

Jamming

In jamming situation, the GNSS signal is masked by another emitted signal (intentional or not). The receiver is then unable to decode the signal and compute location.

Spoofing

Spoofing consists in broadcasting a false GNSS signal which confuses the receiver.

Data collection

Machine learning uses training examples to build patterns and then predict future data with the uncovered patterns. A main objective of this study is thus to collect environment data from smartphones. This data collection is performed in implementing an Android application, which collects in background several types of information and saves them in a database.

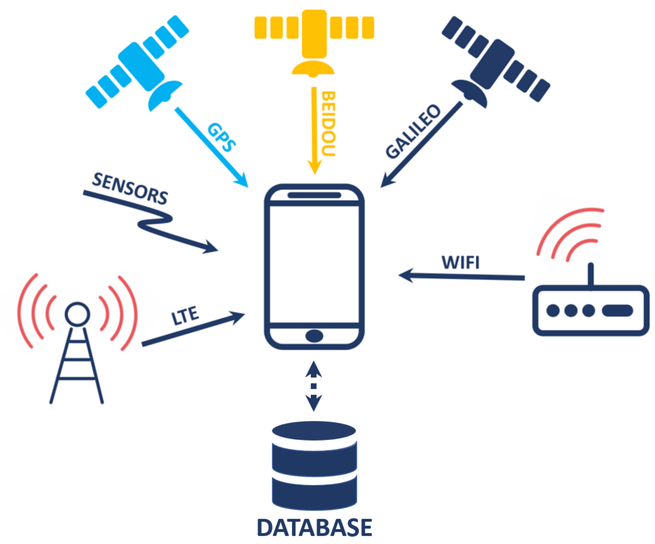

Figure 3: Data collection principle

References

[1] Ashwin V Kanhere et al. “Improving GNSS Positioning using Neural Network-based Corrections”. In: *arXiv preprint arXiv:2110.09581* (2021).

[2] Dong-Kyeong Lee et al. “Analysis of Raw GNSS Measurements Derived Navigation Solutions from Mobile Devices with Inertial Sensors”. In: *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)* (2019).

[3] Damian Miralles et al. “Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution”. In: Oct. 2018, pp. 334–344. DOI: 10.33012/2018.15883.

[4] Mark L. Psiaki and Todd E. Humphreys. “GNSS Spoofing and Detection”. In: *Proceedings of the IEEE* 104.6 (2016), pp. 1258–1270. DOI: 10.1109/JPROC.2016.2526658.

[5] Yan Xia et al. “Anomaly detection for urban vehicle GNSS observation with a hybrid machine learning system”. In: *Remote Sensing* 12.6 (2020), p. 971.