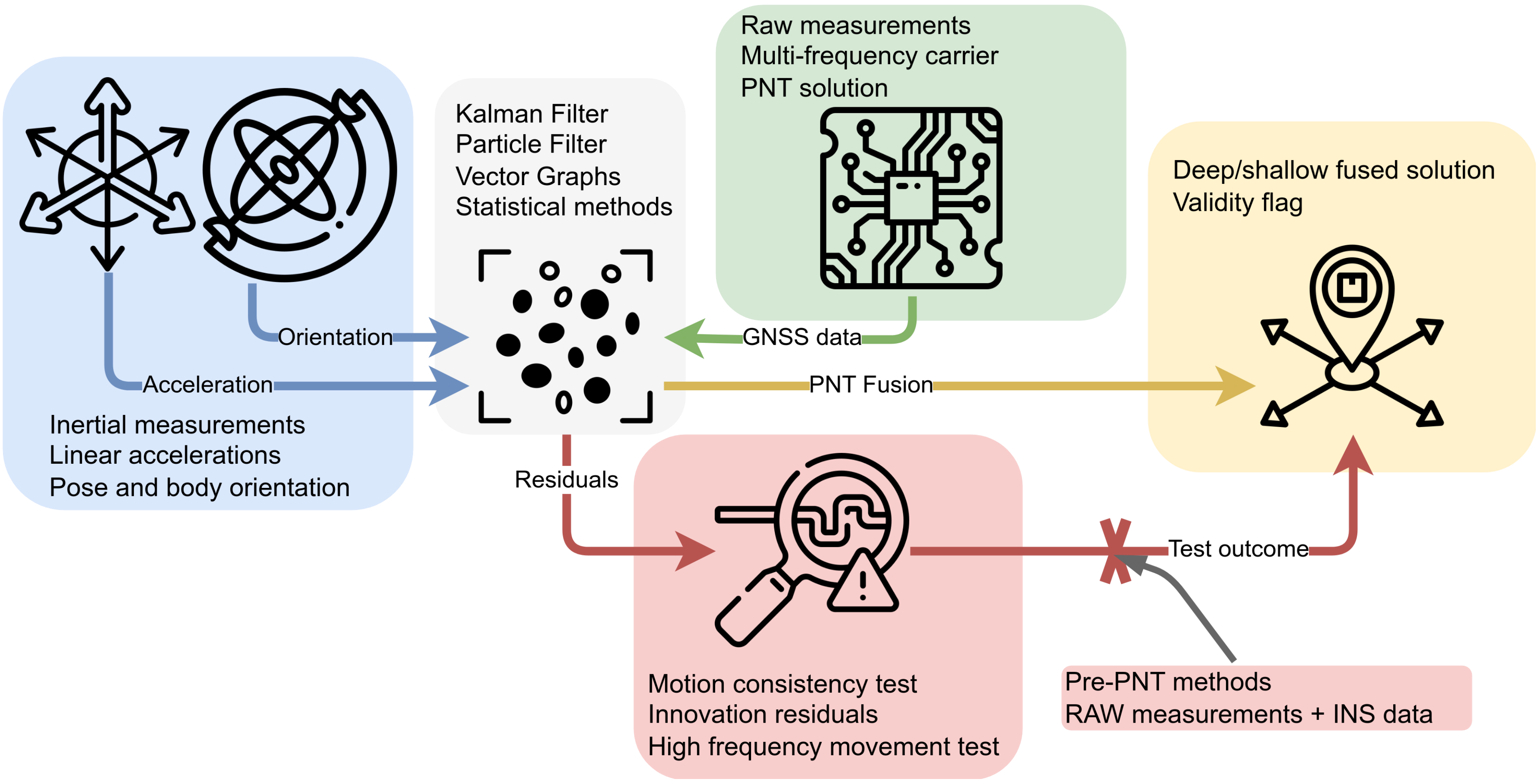
GNSS spoofing detection using carrier phase and consumer INS

Marco Spanghero, Tore Johansson, Panos Papadimitratos
KTH Royal Institute of Technology
Networked Systems Security (NSS) group, www.eecs.kth.se/nss

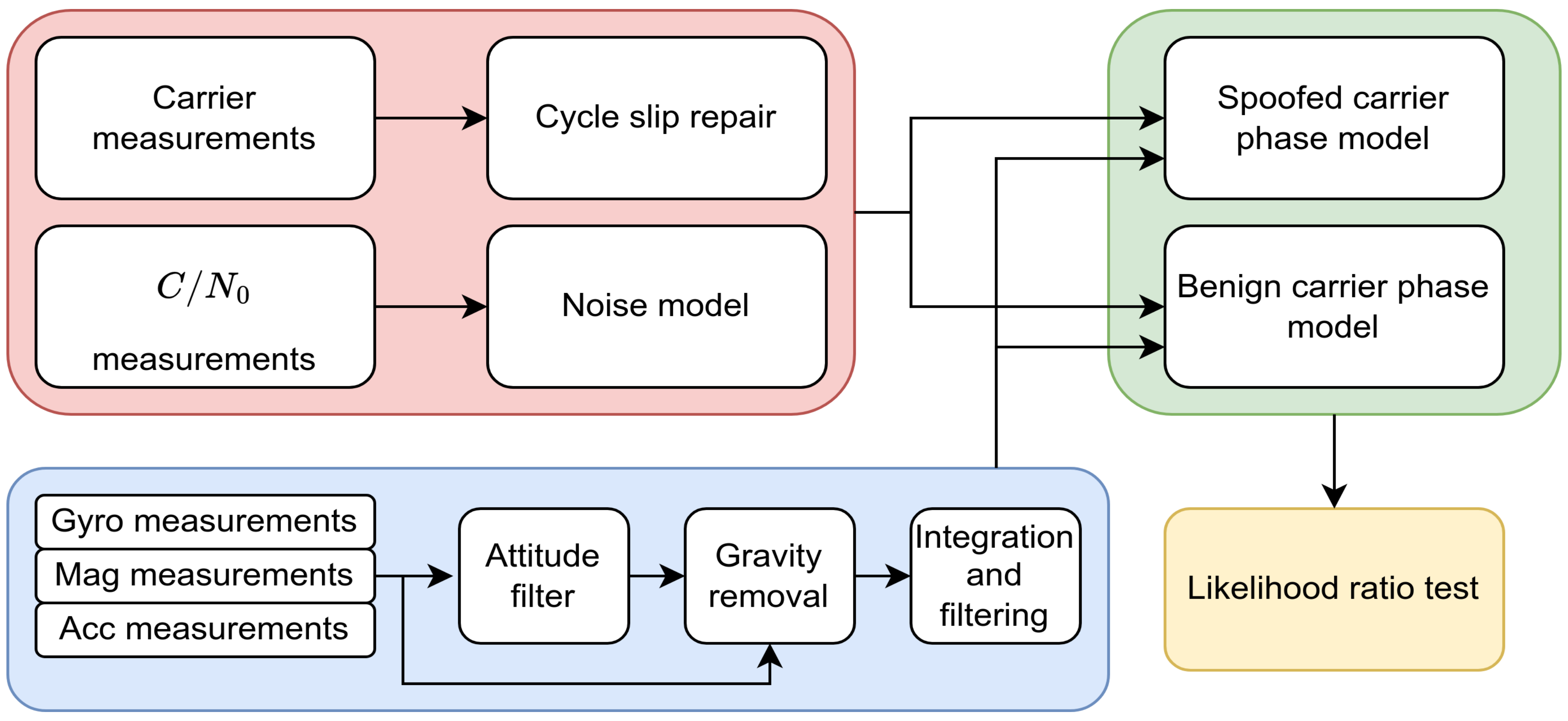
Motivation & Research Goals

Global navigation satellite systems (GNSS) legacy implementations provide only limited support for the new generation of security enhanced signals. Effective inertial navigation requires high-end sensors, but improvements in MEMS technology made possible accurate short-term integration to calculate the displacement of a sensor even at high frequency of motion, specifically with RTK aiding [1]. Identification of legitimate transmitters, based on their geometrical diversity with respect to the antenna system movement [2], is possible even with inexpensive inertial sensors [3]. Results from laboratory evaluation and through field tests at Jammertest 2024 show that the detector is up to 90% accurate in correctly identifying spoofing (or the lack of it), without any modification to the receiver structure and with mass-production grade INS typically used in mobile phones.

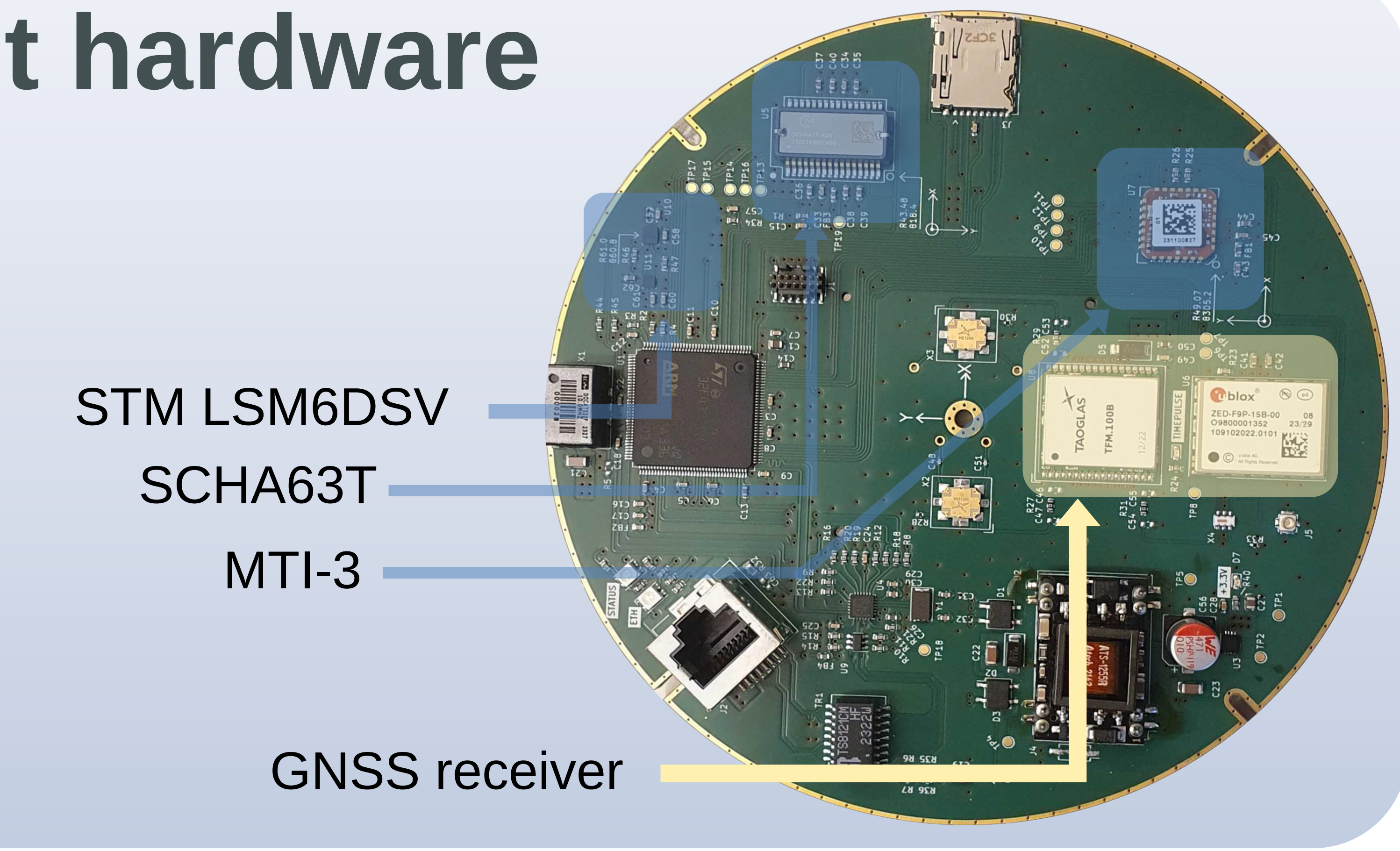
Carrier phase and spoofing



System overview



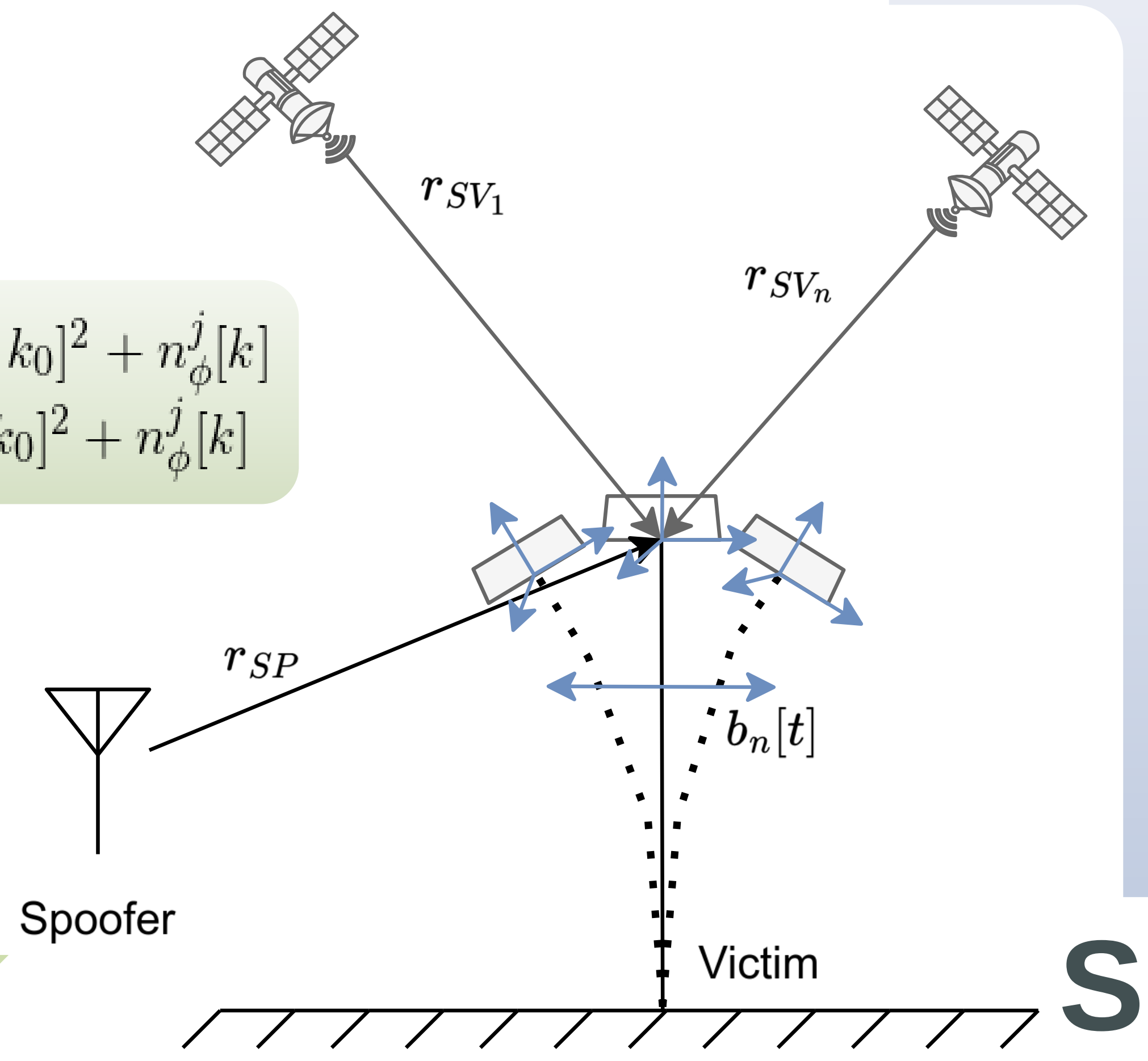
Test hardware



Methodolo

Phase models – polynomial fitting

$$\phi^{sp}[k] \approx \frac{1}{\lambda}(\hat r^{sp})^T A^T b_n[k] + \beta^j_0 + \beta^j_1[k-k_0] + \frac{1}{2}\beta^j_2[k-k_0]^2 + n^j_\phi[k]$$
$$\phi^{j}[k] \approx \frac{1}{\lambda}(\hat r^{j})^T A^T b_n[k] + \beta^j_0 + \beta^j_1[k-k_0] + \frac{1}{2}\beta^j_2[k-k_0]^2 + n^j_\phi[k]$$



Antenna displacement

$$p[k] = -sign\left(\frac{b_n \cdot \hat r_a}{||b_n||||\hat r_a||}\right)||b_n||$$

Per each satellite in view (carrier and noise) [2]

$$\begin{bmatrix}\phi^j_k\\ \phi^j_{k-1}\\ \phi^j_{k-2}\\ \phi^j_{k-3}\\ \vdots\\ \phi^j_{k-N}\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & \frac{1}{\lambda}b^T_{n_k}\\ 1 & 1 & \frac{1}{2}\cdot 1^2 & \frac{1}{\lambda}b^T_{n_{k-1}}\\ 1 & 2 & \frac{1}{2}\cdot 2^2 & \frac{1}{\lambda}b^T_{nk-2}\\ 1 & 3 & \frac{1}{2}\cdot 3^2 & \frac{1}{\lambda}b^T_{nk-3}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & N & \frac{1}{2}\cdot N^2 & \frac{1}{\lambda}b^T_{nk-N}\end{bmatrix}\begin{bmatrix}\beta^j_0\\ \beta^j_1\\ \beta^j_2\\ A\hat r^x\end{bmatrix} + \begin{bmatrix}n^j_{\phi_k}\\ n^j_{\phi_{k-1}}\\ n^j_{\phi_{k-2}}\\ n^j_{\phi_{k-3}}\\ \vdots\\ n^j_{\phi_{k-N}}\end{bmatrix}$$

Factorization

$$\begin{bmatrix}z^j[k]\\ z^j[k-1]\\ z^j[k-2]\\ \vdots\\ z^j[k-N]\end{bmatrix} = \begin{bmatrix}R_{6x6}\\ 0_{6xN}\end{bmatrix}\begin{bmatrix}\beta^j_0\\ \beta^j_1\\ \beta^j_2\\ A\hat r^x\end{bmatrix} + \begin{bmatrix}\eta^j_\phi[k]\\ \eta^j_\phi[k-1]\\ \eta^j_\phi[k-2]\\ \eta^j_\phi[k-3]\\ \vdots\\ \eta^j_\phi[k-N]\end{bmatrix}$$

Minimization of A and r^{sp} under dynamics constraints [2]

$$\mathcal{L}(A, H_0|z^1,\ldots,z^L) = w\exp(-\frac{1}{2}\sum_{j=1}^{L}[R^j A\hat r^j - z^j]^T \cdot [R^j A\hat r^j - z^j])$$
$$\mathcal{L}(\hat r^{sp}, H_1|z^1,\ldots,z^L) = w\exp(-\frac{1}{2}\sum_{j=1}^{L}[R^j \hat r^{sp} - z^j]^T \cdot [R^j \hat r^{sp} - z^j])$$

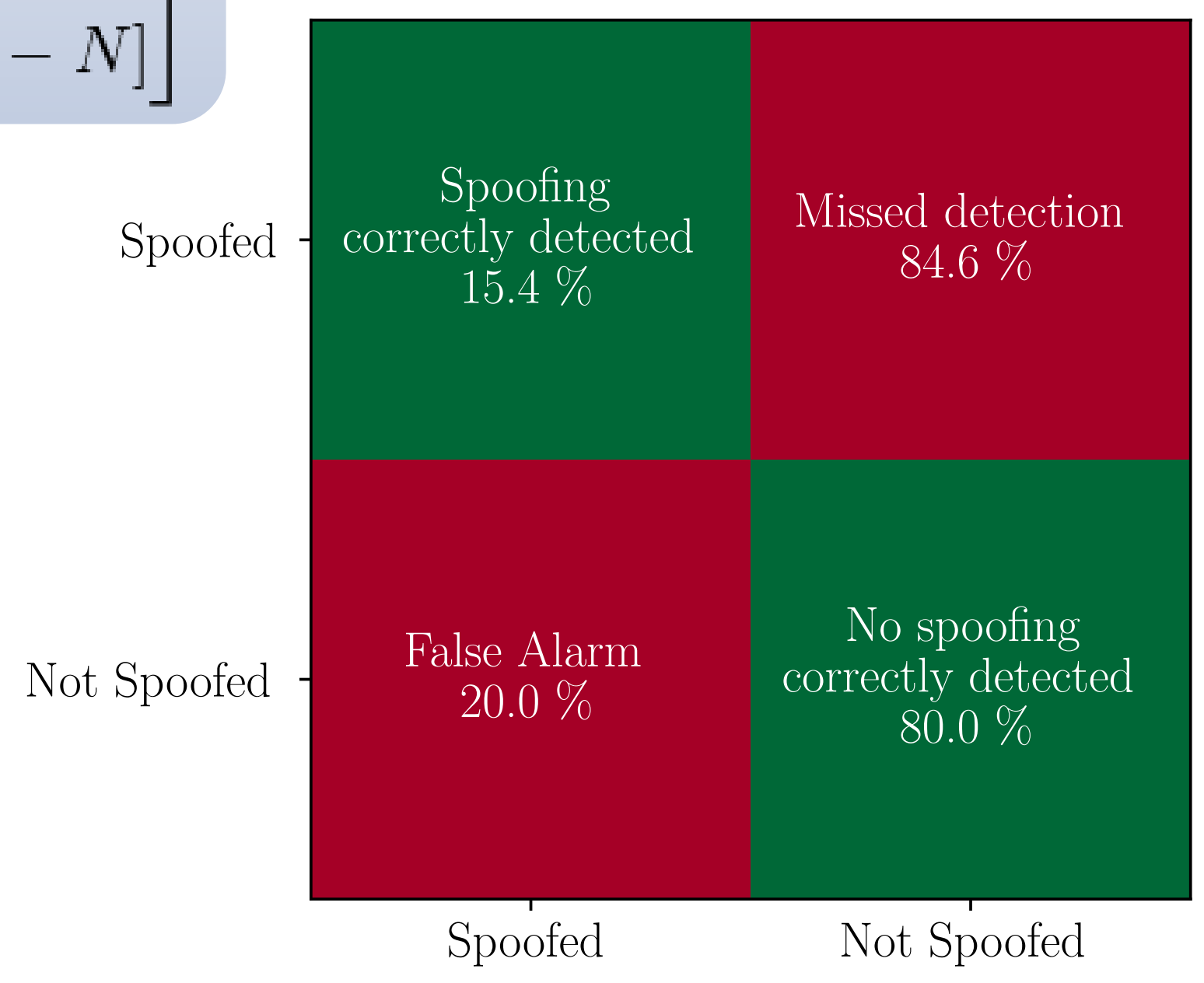
Statistical test

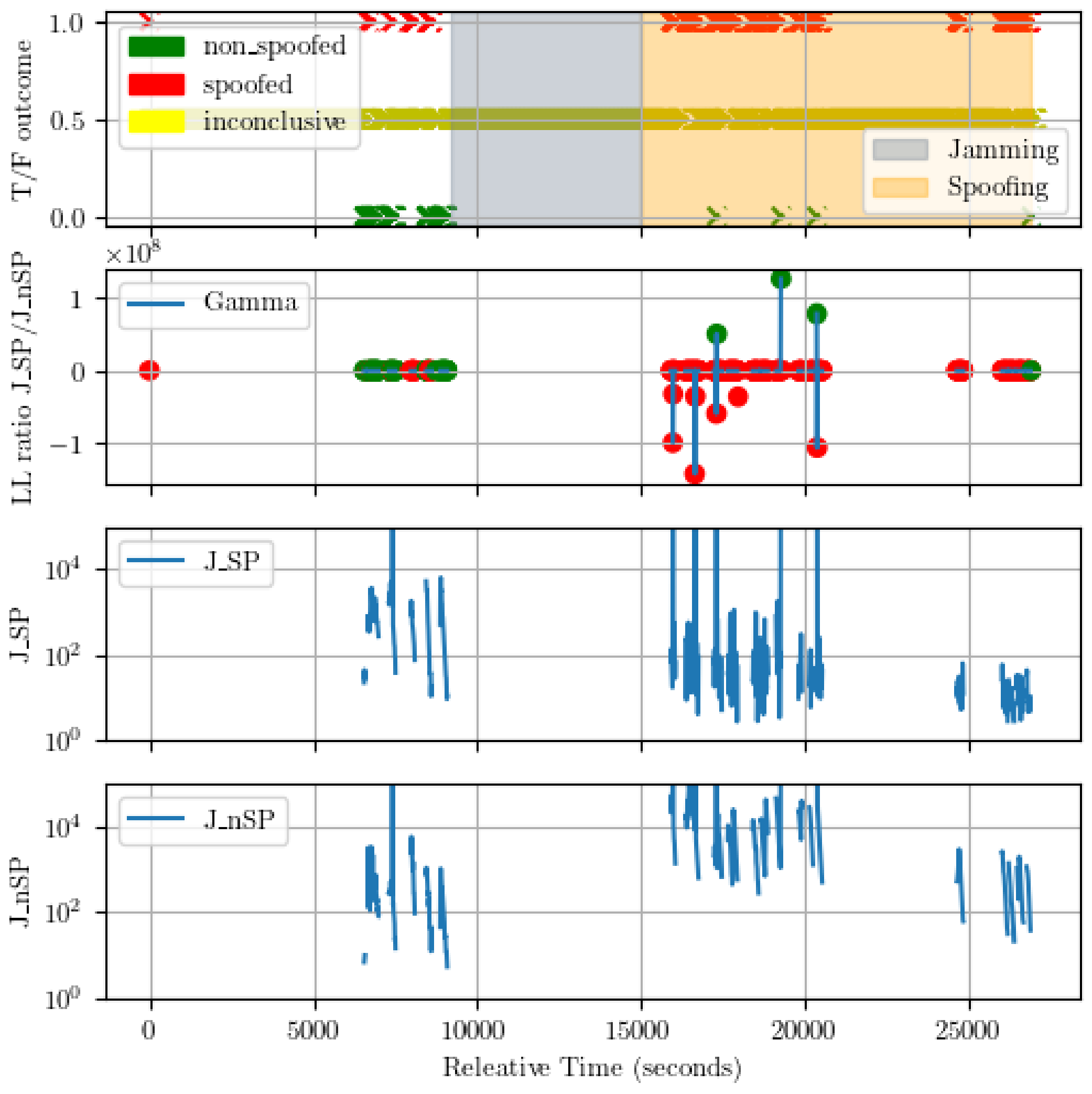
$$\gamma = J_{sp}(\hat r_{opt}) - J_{nonsp}(A_{opt})$$

Spoofing detection results

Live test Jammertest

Control scenarios





Selected results: detection of adversaries in successful in both control tests (fully spoofed and benign) with high accuracy. Live testing at Jammertest 2024 showed that live detection is possible both in static and dynamic cases, for simulation of signals and meaconing. Testing on mobile phones shows the limitations of raw measurements rate in current implementation of Android API (high INS rate, lack of carrier phase data)

References

[1] Clements, Z., Yoder, J. E., and Humphreys, T. E. (2022). *Carrier-phase and imu based gnss spoofing detection for ground vehicles*. Presented at ION ITM/PTTI, Long Beach, CA, USA

[2] Psiaki, M. L., Powell, S. P., and O'Hanlon, B. W. (2013). *Gnss spoofing detection using high-frequency antenna motion and carrier-phase data. In ION GNSS+*, Nashville, TN, USA.

[3] Johannson, T., Spanghero M, and Papadimitratos, P. (2025). *Consumer INS Coupled with Carrier Phase Measurements for GNSS Spoofing Detection*, to appear in ION ITM/PTTI, Long Beach, CA, USA

WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM