POLITECNICO DI TORINO
Repository ISTITUZIONALE

Detecting Single-antenna Spoofing Attacks by Correlation in Time Series of Raw Measurements

Original
Detecting Single-antenna Spoofing Attacks by Correlation in Time Series of Raw Measurements / Minetto, Alex; Rustamov, Akmal; Dovis, Fabio. - ELETTRONICO. - (2023), pp. 73-84. (Intervento presentato al convegno 36th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2023) tenutosi a Denver, Colorado (USA) nel September 11 - 15, 2023) [10.33012/2023.19205].

Availability:
This version is available at: 11583/2983005 since: 2023-10-17T08:55:47Z

Publisher:
Institute of Navigation (ION)

Published
DOI:10.33012/2023.19205

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
GENERICO -- per es. EPJ (European Physical Journal) : quando richiesto un rinvio generico specifico per

(Article begins on next page)

16 May 2024

Detecting single-antenna spoofing attacks by correlation in time series of raw measurements

Alex Minetto, Akmal Rustamov, Fabio Dovis
Politecnico di Torino, Turin, Italy

BIOGRAPHY

Alex Minetto received the B.Sc. and M.sc. degrees in Telecommunications Engineering from Politecnico di Torino, Turin, Italy and his Ph.D. degree in Electrical, Electronics and Communications Engineering, in 2020. He joined the Department of Electronics and Telecommunications of Politecnico di Torino in 2021 as researcher and assistant professor. His current research interests cover navigation signal design and processing, advanced Bayesian estimation applied to Positioning and Navigation Technologies (PNT) and applied Global Navigation Satellite System (GNSS) to space weather and space PNT.

Akmal Rustamov is a PhD candidate at the Department of Electronics and Telecommunications of Politecnico di Torino. His research is focused on the implementation and resilience test of GNSS positioning systems for road applications. He received his MSc degree in the field of Mechanical Engineering in 2016 at Turin Polytechnic University in Tashkent.

Fabio Dovis received his M.Sc. degree in 1996 and his Ph.D. degree in 2000, both from Politecnico di Torino, Turin, Italy. He joined the Department of Electronics and Telecommunications of Politecnico di Torino as an assistant professor in 2004 and as associate professor in 2014. Since 2021 he is a full professor. He coordinates the Navigation Signal Analysis and Simulation (NavSAS) research group. His research interests cover the design of GPS and Galileo receivers, advanced signal processing for interference and multipath detection and mitigation, as well as ionospheric monitoring.

ABSTRACT

Global Navigation Satellite System (GNSS) receivers are vulnerable to intentional radio frequency interferences, posing significant risks to their performance and reliability. Among these threats, it has been widely argued that modern GNSS-equipped Android™ smartphones are resilient to non-coherent spoofing attacks. This study challenges such a perception by highlighting the vulnerability of GNSS-equipped Android™ smartphones to single-antenna, non-coherent spoofing attacks and proposing a novel, application-level detection technique solely based on raw GNSS observables, i.e., carrier-to-noise-density time series. The analysis demonstrated the capability of successfully detecting such attacks by observing the cross-correlation among Global Navigation Satellite System (GNSS) measurements time series. Cross-correlation quantified by Pearson's correlation coefficients shows a relevant increment during harmful spoofing attacks. Under these conditions, the proposed methodology allows to rise a spoofing alarm in about 5 seconds with a false alarm probability of 1.5%. Furthermore, the proposed technique does not require low-level signal access, making it suitable for implementation at the application layer in a large number of smart devices with limited knowledge of their low-level system architecture. A validation campaign has been performed by testing 18 different Android™ devices and chipsets, thus demonstrating the applicability of the proposed method independently from the device under test.

I. INTRODUCTION

With the rapid development of positioning and navigation technology based on the GNSS, mass-market applications have significantly increased with a demand for more accurate and reliable Positioning, Navigation and Timing (PNT) services. In May 2016, Google announced the availability of raw GNSS data starting for the devices running Android™ 7. For the first time, developers could access carrier and code measurements, internal clock information, and eventually, also to the decoded bit of the navigation messages. Several applications have been developed relying upon raw GNSS measurement availability as in the context of high-accuracy positioning applications (Lachapelle and Gratton, 2019; Minetto et al., 2022) as well as in collaborative navigation (Minetto et al., 2021). Besides these applications, since they provide, to a certain extent, an insight into the processing taking place inside the chipset, raw GNSS measurements can be used to analyze the effects of Radio Frequency Interference (RFI) affecting the GNSS received signals.

Detection strategies for anthropogenic RFI, such as jamming and spoofing threats, have been extensively discussed in the literature(Dovis, 2015). However, many of the proposed spoofing detection techniques require the implementation of sophisticated algorithms requiring to access low-level signal processing stages of the GNSS receiver to be effective against simplistic to advanced spoofing attacks (Humphreys et al., 2008). Others are suitable only in specific experimental conditions and lack generality. A classical technique for spoofing detection based on the carrier-to-noise ratio (C/N_0) is proposed in (Jafarnia-Jahromi

et al., 2012), where the measured C/N_0 of received GNSS signals is compared to a threshold or expected value. If its measured C/N_0 is significantly lower than the expected value, it could indicate that jamming or spoofing is ongoing, and the signal should be discarded. A classical technique for detecting spoofing attacks involves comparing the measured carrier-to-noise ratio C/N_0 of received signals to an expected value to identify unspecified RFI. Unexpected increments of the C/N_0 can be easily associated with spoofing threats. A significantly lower measured C/N_0 may indicate the presence of RFI, and the signal should be discarded, as proposed by (Jafarnia-Jahromi et al., 2012).
However, if a counterfeit signal is correctly tracked and unspread, it can show a C/N_0 value within a nominal range, even though jamming or spoofing is performed. Detection of such malicious actions can be difficult in this case, as the C/N_0 measurement may not show any abnormalities. In such cases, other techniques operating at signal level, i.e., over frequency or time domains, or the use of integrity messages from augmentation systems, have to be considered in conjunction with C/N_0 monitoring to provide a more robust spoofing detection. An early proposal to investigate the cross-correlation between raw GNSS data under spoofing was proposed by (Broumandan et al., 2012) for kinematic receivers. It leveraged spatial correlation introduced in the Doppler shift observations by the movement of the receiving antenna. Such a technique seems not applicable to static receivers and it has been surprisingly neglected in recent research. A recent work by (Spens et al., 2022) proposed an effective strategy to detect and discriminate jamming and spoofing threats in mass-market devices that is based on Automatic Gain Control (AGC) and C/N_0 observations. The proposed methodology leverages the following assumptions from (Lee et al., 2021; Manfredini et al., 2018), i.e., i) if AGC value decreases and C/N_0 decreases, jamming is likely, ii) if AGC value decreases and C/N_0 is relatively constant, spoofing is more likely than jamming.

Unfortunately, depending on the different Android™ versions, AGC values are not granted for outdated devices and, if available, they are not as reliable as other classes of raw GNSS measurements, as discussed in (Spens et al., 2022). Besides, the discrimination of anomalous C/N_0 values requires the non-trivial definition of a threshold and the identification of a transient in the observed data. Therefore, the proposed algorithm also combines several controls over different metrics, i.e., it compares i) GNSS estimated location and estimates from other location providers (e.g., network), ii) checks for the Android™ mock location flag, and compares GNSS and Android™ system times. An extended literature review on these methods can be found in (Rustamov et al., 2023)
In this study, we show how statistical characterisation of the C/N_0 can indeed reveal that a spoofing attack is being performed, and to a certain extent also discriminate between counterfait and legitimate signals among the tracked GNSS signals at the receiver. By assuming Android smartphones as a reference framework, we present a performance assessment of a technique for the detection of single-antenna spoofing attacks. The proposed solution exploits the spatial and temporal correlation of the spoofing signals, and it is validated through an extensive, experimental campaign based on the analysis of the correlation of the raw output data provided by various Android™ smartphones.

The rest of the paper is organized as follows: Section II recalls the fundamentals on GNSS and spoofing signals as well as their effects on the observed GNSS raw measurements. By targeting C/N_0 time series, Section III introduces the methodology for a spoofing detection strategy exclusively based on those class of raw GNSS data. A performance assessment is then presented in Section IV and, eventually, conclusions are drawn in Section V.

II. BACKGROUND

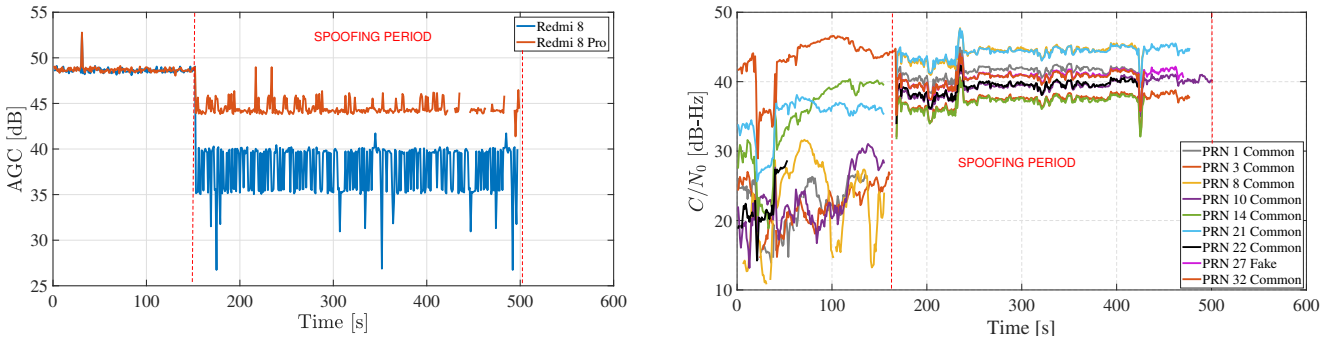
In absence of interference, a real GNSS signal at the receiving antenna can be modelled as the sum of N_s satellites' signals

$$x_{f_c}(t) = \sum_{i=1}^{N_s-1} \sqrt{2P_{R,i}} D_i\left(t-\tau_i\right) C_i\left(t-\tau_i\right) \cos\left(2\pi\left(f_c + f_{d,i}(t)\right) t + \triangle\theta_i\right) + n(t) \tag{1}$$

where $P_{R,i}$ is the received signal power of the in-phase and quadrature ensemble, $D_i(t)$ is the navigation data bit stream, $C_i(t)$ is the pseudo-random code sequence, f_c is the carrier frequency shifted by the observed Doppler shift $f_{d,i}$, τ_i is the propagation delay, and $\triangle\theta_i$ is the phase offset. Eventually, $n(t)$ is the thermal noise contribution. It is worth remarking that the term $D_i(t-\tau_i)C_i(t-\tau_i)$ can be BPSK, BOC, CBOC or AltBOC modulated. The unique characterisation of the satellite-to-receiver signal propagation path affects the received power $P_{R,i}$ of each GNSS signal and in turn it may condition the observables generated by the receiver.

1. Non-coherent spoofing

An ideal spoofing attack would emulate satellites' signals incldued in (1) while altering their characteristics to fake the state estimation of a victim receiver. A smooth signal takeover requires a coherent signal transmission by the spoofer that is typically hard to achieve. Indeed, simplistic spoofing attacks are often referred to as *non-coherent*, as the code and carrier phase as well as the time reference in the navigation message are not kept consistent with the legitimate ones.



(a) AGC **(b)** C/N_0

Figure 1: Examples of AGC and C/N_0 behaviours under effective spoofing attack on Android™ smartphones. Spoofing effectiveness was declared upon spoofed position was estimated by the device under test.

The model for the sum of N_{sp} single frequency, single constellation spoofed signals is

$$x_{f_c}^{(S)}(t) = \sum_{i=1}^{N_{sp}} \sqrt{2P_{R,i}^{(S)}}\hat{D}_i\left(t-\tau_i^{(S)}\right)C_i\left(t-\tau_i^{(S)}\right)\cos\left(2\pi\left(f_c+f_{d,i}^{(S)}(t)+f_d^{(S)}(t)\right)t+\triangle\theta_i^{(S)}\right)+n(t) \tag{2}$$

where the apex $(\cdot)^{(S)}$ identifies the altered signal properties w.r.t. to (1). In particular a further Doppler shift term, $f_d^{(S)}(t)$, is introduced by the relative kinematics of the spoofer and victim antennas. Under spoofing threat, both the signals in (1) and (2) reach the receiver antenna and the overall received signal can be modeled as

$$x_{tot}(t) = \bar{x}_{f_c}(t) + \bar{x}_{f_c}^{(S)}(t) + n(t) \tag{3}$$

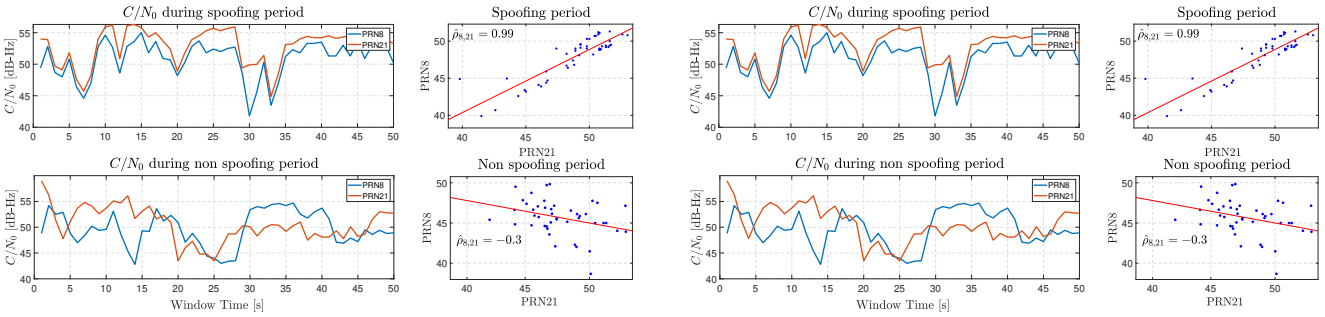
where $\bar{x}$ indicates noiseless, legitimate and spoofing signals derived from (1) and (2) by neglecting the respective noise terms. The overall received power is naturally increased by the spoofed signals thus typically inducing the feedback of the AGC in GNSS receivers, as discussed by (Bastide et al., 2003).

2. Effects of signal propagation on raw GNSS measurements

Unless satellite-based spoofing actions are considered, legitimate and spoofed GNSS signals are subject to different propagation paths. Legitimate GNSS signals are mostly conditioned by the free space path loss, ionospheric signal scattering and multipath. Such impairments rarely affect all the received signals power at the same time. Furthermore, different attenuation and impairments affecting each signals return heterogeneous behaviours of the raw measurements, i.e., AGC, C/N_0 and pseudorange measurements. On the contrary, the propagation path travelled by spoofed signals in case of single antenna attacks, is common to all the received signals and reflects the channel properties of spoofer-to-receiver line-of-sight or reflected paths. As anticipated in Section I, previous works discussing spoofing detection methods for mass-market devices have rarely leveraged such a temporal and spatial correlation of raw measurements. They have usually analysed short-term observations of single-value metrics or peculiar transients in their time evolution. In Figure 1, we observe that state-of-the-art approaches reviewed in Section I seems valuable to classify the spoofing event. Indeed, as shown in 1a on spoofing action the AGC quickly reacted to the additional received power at the receiver by reducing the gain in two different devices, i.e., a Xiaomi Redmi 8 and a Xiaomi RedMi 8 Pro. Similarly, in Figure 1b we observe a quick reaction of C/N_0 which generally improves for all the signals that are both available as legitimate and counterfeit, i.e., common. However, some limitations have to be noticed about these observations:

- AGC value drops under spoofing depends on the device, this makes difficult to generalize a threshold for the spoofing detection
- AGC value is an aggregated metric that may not be able to sense few spoofed signals especially when spoofer acts with calibrated power levels.
- C/N_0 increment may vary depending on the tracked signal and it may fail in case of power-calibrated spoofers.

However, in Figure 1b, we can observe that spoofing introduces a remarkable similarity in the C/N_0 time series that appears poor before the spoofing period. Such a similarity seems not related to the magnitude of the C/N_0 and is further verified in the



(a) PRN 1 and PRN 3

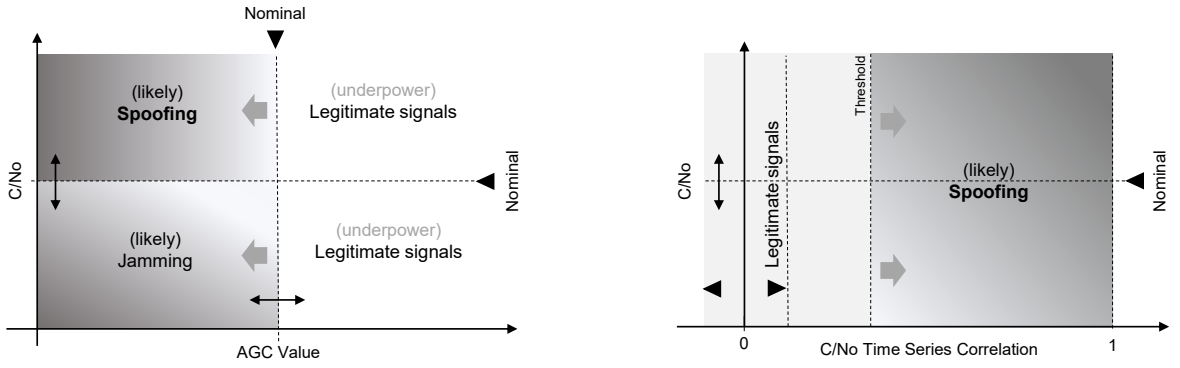
(b) PRN 8 and PRN 21

Figure 2: comparison of C/N_0 time series for different PRNs during the spoofing (upper panels) and non spoofing period (lower subplots), and associated linear correlation plot (right subplots). Discontinuities in the time series are mapped to null values in the correlation plots. Observation window of duration $T_n = 50$ s.

examples of Figure 2. A simple linear regression performed on pairs of C/N_0 time series quantify the correlation introduced by the spoofed signals w.r.t. the correlation between the legitimate ones.

3. Single value observations vs. C/N_0 correlation index

Figure 3a shows how the positive or negative variations of C/N_0 and AGC value are effectively exploited by (Lee et al., 2021), (Manfredini et al., 2018), and (Spens et al., 2022). By relying on the observed correlation, Figure 3b shows our target methodology by highlighting its independence on the C/N_0 variations. The idea is to extract a reliable correlation index constrained in the range $[0, 1]$ to discriminate those signals which are being transmitted through the same physical channel.Intermediate variations in the range can be exploited to establish a certain level of severity of an occurring attack.



(a)

(b)

Figure 3: Pictorial view of current state-of-the-art approach for spoofing detection through raw GNSS measurments observations and the proposed approach.

III. METHODOLOGY

1. Retrieving correlation coefficients from raw measurements time series

Let us consider the pairwise cross-correlation between two time series X_i and X_j

$$R_{XY}(t_1, t_2) = E\left[X_i(t_1)X_j^*(t_2)\right] \tag{4}$$

where $E(\cdot)$ is the mean operator, t_1 and t_2 identifies two generic time instants, and the $(\cdot)^*$ indicates the complex conjugate of the argument. By subtracting the mean to each series, the cross-covariance function is obtained as

$$C_{XY}(t_1, t_2) = E[(X_i(t_1) - \mu_{X_i}(t_1)) \left(X_j(t_2) - \mu_{X_j}(t_2)^*\right)]. \tag{5}$$

Assuming X_i and X_j being C/N_0 data series observed over short timespans (less than 1 minute) we can reasonably neglect any long-term trends and assume them as wide-sense stationary processes. In light of this, (5) is changed as

$$C_{XY}(\tau) = E\left[(X_i(t) - \mu_{X_i}(t)) \left(X_j(t+\tau) - \mu_{X_j}(t+\tau)\right)^*\right] \tag{6}$$

where $\tau = t_1 - t_2$ highlights the independece on the choice of the time instants t_1 and t_2. To remove the scaling factor of the correlation, we normalize (6) through the Pearson correlation function

$$\rho_{X_i,X_j}(\tau) = \frac{C_{XY}(\tau)}{\sigma_{X_i}\sigma_{X_j}} \tag{7}$$

The maximum value assumed by (7) corresponds to the *Pearson correlation coefficient* (Fisher, 1925; Kendall et al., 1948), and is computed as

$$\rho_{X_i,X_j} = \max\left\{\rho_{X_i,X_j}(\tau)\right\} = \frac{\text{cov}\left(X_i, X_j\right)}{\sigma_i\sigma_j}. \tag{8}$$

In case the size and values assumed by X_i and X_j are identical, the argument of (8) which maximizes ρ_{X_i,X_j} is $\tau = 0$. Pearson correlation coefficients assume values in the range $[-1, 1]$, where $\rho_{X_i,X_j} = \pm 1$ indicates a perfect positive or negative relationship, respectively, and $\rho_{X_i,X_j} = 0$ denotes absence of any linear relationship between the processes. By considering its absolute value, we can define a metric in a the range $[0, 1]$. We assume ergodicity of the observed processes so that we can estimate sample means μ_{X_i} and μ_{X_j} through the time average of X_i and X_j. By following the steps described so far, the Pearson correlation coefficient in (8)is approximated over a time span T_n through

$$\hat{\rho}_{a,b}^{T_n} = \frac{\sum_{n=1}^{Tn}\left(x_i[n] - \overline{X_i}\right)\left(x_j[n] - \overline{X_j}\right)}{\sqrt{\sum_{n=1}^{Tn}\left(x_i[n] - \overline{X_i}\right)^2}\sqrt{\sum_{t=1}^{Tn}\left(x_j[n] - \overline{X_j}\right)^2}} \tag{9}$$

where T_n is the window size, $x[n]$, $x[n]$ are the time series samples observed at the n-th instant, and $\overline{X_i}, \overline{X_j}$ are the sample means. Equation (9) is applicable to any pair of time series to highlight pairwise correlation associated to different satellites. It is worth recalling that a trade-off between estimation accuracy and latency has to be considered for the implementation of (9). By performing an exhaustive computation of (9), we define a $K \times K$ Pearson matrix that includes correlation information about any pair of tracked GNSS signals

$$P^{T_n} = \begin{bmatrix} 1 & \hat{\rho}_{1,2} & \hat{\rho}_{1,3} & \cdots & \hat{\rho}_{1,K} \\ \hat{\rho}_{2,1} & 1 & \hat{\rho}_{2,3} & \cdots & \hat{\rho}_{2,K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \hat{\rho}_{K,1} & \hat{\rho}_{K,2} & \hat{\rho}_{K,3} & \cdots & 1 \end{bmatrix} \tag{10}$$

where K is the number of tracked signals for which C/N_0 time series are actually available. The correlation information included in (10) can be used to infer possible spoofing attacks on subset of tracked signals. However, we propose an aggregated metric to quantify the severity of the attack by gathering all the pairwise information

$$\mu_\rho^{(K)} = \frac{2}{K(K-1)}\sum_{i,j}\hat{\rho}_{i,j} \quad \forall i > j,\ i \in (1, K) \tag{11}$$

where i and j defines rows and columns indices, respectively.

2. Spoofing detection: decision logic

We can detected an ongoing spoofing attack based on the binary hypothesis that either the GNSS receiver tracks legitimate satellite signals, $\mathcal{H}_0$, or spoofed signals, $\mathcal{H}_1$. Under $\mathcal{H}_0$, μ_ρ is typically close to zero, thus denoting a poor cross-correlation

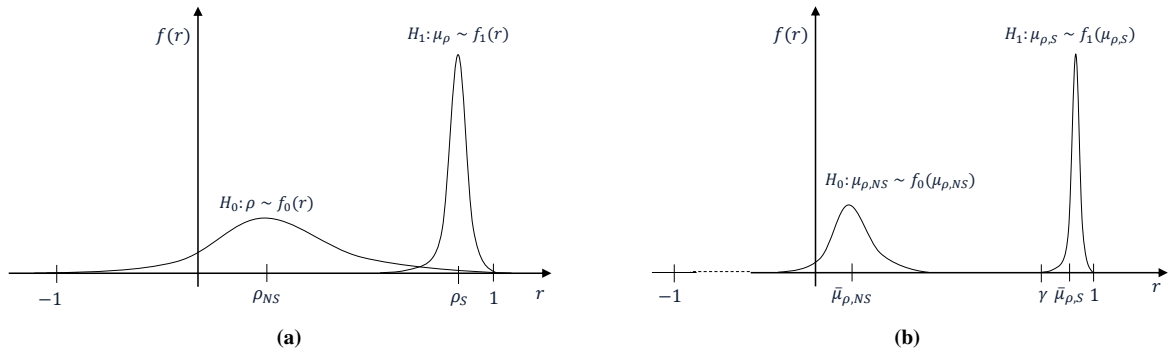


Figure 4: Pictorial view of the Neyman-Pearson criterion applied to spoofing detection based on the Pearson correlation coefficients of C/N_0 time series. PDFs of single Pearson's correlation coefficients (a) and of aggregated data, i.e. average Pearson correlation coefficient (b).

among the C/N_0 time series, and its distribution follows a given PDF, $f_0(r)$. On the contrary, under $\mathcal{H}_1$, μ_ρ is expected to be as closer to 1 as many spoofed satellites are tracked by the receiver, with a PDF distributed according to $f_1(r)$. As anticipated in Section II, the magnitude of (11), provide a feedback on the harmfulness of the ongoing attack. We can approximate the PDFs $f_0(r)$ and $f_1(r)$ by means of

$$f(r) \simeq \frac{2^{n-3}(1-\rho^2)^{\frac{n-1}{2}}(1-R^2)^{\frac{n}{2}-2}}{\pi\Gamma(n-2)} \times \sum_{k=0}^{\infty}\left[\Gamma\left(\frac{n-1+k}{2}\right)\right]^2 \frac{(2R\rho)^k}{k!} \tag{12}$$

where r is a variable defined in the range $(-1, 1)$, $\Gamma(\cdot)$ is the Gamma function, n is the number of Pearson's correlation samples in a given observation, and ρ is the known level of correlation, according to (Muirhead, 2009). The skewness of (12) increases with ρ. However, according to the Central Limit Theorem, (12) can be transformed through the Fisher transformation

$$z = \frac{1}{2}\ln\left(\frac{1+r}{1-r}\right) = \tanh^{-1}(r) \tag{13}$$

such that (12) approaches a normal distribution as the number of Pearson samples, n, increases. The transformed PDF is characterised by a standard deviation

$$\sigma_z = \frac{1}{\sqrt{n-3}}. \tag{14}$$

These analytical steps are depicted by the plots of Figure 4. Single correlation coefficient will define the distribution of Figure 4a while averaging n Pearson coefficients will shift the decision problem to the Gaussian-like distributions defined through (13) and centered at the average correlation coefficient, as in Figure 4b. A decision threshold, γ, can be established by expressing the probability of a false alarm as

$$P_F \simeq \int_{\gamma'}^{1} f_0'(z)\, dz = \alpha \tag{15}$$

where $f_0'(z)$ is the transformed PDF according to (13), and α is the design parameter for the decision logic. The threshold γ' is computed by fixing the probability of a false alarm, α, as

$$\gamma' = Q^{-1}(\alpha) \tag{16}$$

where $Q(\cdot)$ is the the Marcum Q-function and γ' must be reverted to γ by inverting (13). As an example, by fixing a probability of false alarm of $1.5\,\%$ through $\alpha = 0.015$, we obtain $\gamma' \simeq 2.17$. This value corresponds to a threshold $\gamma \simeq 0.5$ for the original PDF (12) of Figure 4b. The value $\gamma \simeq 0.5$ is used as a reference for the validation of the technique through the experimental campaign to assess the spoofing detection with a probability of false alarm of $1.5\,\%$.

a) Implementation of the decision logic

The proposed algorithms is described through the pseudocode in Algorithm 1. It is worth recalling that the *mean correlation threshold*, γ, can be heuristically determined under $\mathcal{H}_0$ and $\mathcal{H}_1$ hypothesis. As an alternative, γ can be estimated by an arbitrary false alarm probability, according to Section III. We then compare the current mean Pearson correlation coefficient $\mu_\rho^{(K)}$ estimated through real-time data over a window of T_W s, with the Selected threshold. Eventually we establish $\mathcal{H}_1$ (spoofing) or $\mathcal{H}_0$ (non-spoofing) conditions within the observed time window by accepting or rejecting $\mathcal{H}_1$ according to the Neyman-Pearson criterion.

Data: $Th = \lambda$, $\mathbf{C} = C/N_0$
for $i \leq K$ **do**
  for $j < i$ **do**
    $\mathbf{P}(i,j) \leftarrow pears(\mathbf{C}(i,:), \mathbf{C}(j,:))$
  end
  $\mu_\rho^{(K)} \leftarrow \frac{2}{K(K-1)} \sum_{i,j} P(i,j)$
  if $\mu_\rho^{(K)} \geq Th$ **then**
    $\mathcal{H}_1$ accepted over T_n
  else
    $\mathcal{H}_1$ rejected over T_n
  end
end

Algorithm 1: Spoofing detection algorithm based on the correlation of C/N_0 time series

3. Experimental setup

Spoofing tests were executed by means of a low-cost portable spoofer based on a Great Scott Gadgets™ HackRF One™ platform and a Raspberry™ PI 4B. The HackRF One™ front-end is a low-cost, open-source SDR allowing for a cost-effective RF signal transmission from binary files (.bin) including Intermediate Frequency (IF) or baseband signal samples.

The front-end can receive and transmit signals from 1 MHz to 6 GHz with adjustable power and channel bandwidth. The software used to numerically generate the spoofed Global Positioning System (GPS) signal is GPS-SDR-SIM, an open GPS L1 C/A signal generator toolbox distributed with a MIT license. The attack was planned to simulate a static position, and all the visible satellites belonging to the GPS constellations and their signals were transmitted through the SDR equipment. An optional reference 10 MHz Oven Controlled Crystal (Xtal) Oscillator (OCXO) was connected to the front end to discipline the signal generation. The power supply can be provided through a mass-market, 10000 mAh battery pack compliant to the supply specification of the Raspberry™ PI 4B. The HackRF One™ can be then supplied by the Raspberry PI itself through its USB 3.0 interface. Spoofing attacks were performed through the portable spoofer according to the following steps:

1. *Numerical fake signal generation*. The fake static location coordinates were chosen and configured to the GPS-SDR-SIM. The software also requires in input the daily GPS broadcast ephemeris file (i.e., RINEX v2 brdc file). Once the input are provided, it generates the simulated pseudorange and Doppler shifts for the GPS satellites in view. This simulated range data was used to produce a binary file with In-phase(I)/Quadrature(Q) samples of the complex baseband GNSS signal, ready to be reproduced by the SDR front-end (i.e., HackRF One™).
2. *A .bin file transmission*. The .bin file is read by the HackRF One through the USB interface of the Raspberry™ PI 4B.
3. *Digital to analogue conversion*. The transmitting module of the front-end (HackRF One™) is in charge to perform the digital-to-analog conversion by mixing the baseband signal provided at step 2 to the carrier frequency generated through the Voltage-Controlled Oscillator (VCO) (i.e. GPS L1 C/A), thus, transmitting I/Q modulated GNSS signals in L1 band.
4. *RF signal transmission*. After baseband signal samples are generated, HackRF One™) transmits .bin file through an antenna of the SDR platform at L1 frequencies. Specifically, the transmission command is used to spread the samples using HackRF One™), at 1575.42MHz, repeatedly.

a) Devices under test

A variety of Android™ smartphones with multi-frequency GNSS chipsets were chosen to test the effect of the simplistic spoofing attack performed through the portable spoofer described above. The list of devices under test is reported in Table 1. These devices are all equipped with Google Android™ Operating System (OS) and the GNSS Logger Android application provided by Google™ was installed for the procurement of GNSS raw measurements. Additionally, the devices' Position, Velocity, Timing (PVT) solutions were logged through the Android™ National Marine Electronics Association (NMEA) Tools application, which

provides the GNSS standalone position of the smartphone in standard NMEA format.

b) Test methdology

Experiments on smartphones were carried out in a dedicated test campaign. Each test foresaw about $500\,\mathrm{s}$ data collections for two complementary scenarios, in controlled environmental conditions. The scenarios included i) devices waking on nominal GNSS signals and then being subject to spoofing after $150\,\mathrm{s}$ and ii) devices waking on under spoofing attack switched off after $350\,\mathrm{s}$ The range of the spoofer was kept at about $3\,\mathrm{m}$, and, in order to prevent any RFI disturbances beyond the range of the experimental setupcontrolled environment, a $30\,\mathrm{dB}$ attenuator was applied at the coaxial cable to reduce transmitting signal power levels and limit the spoofer coverage. The actual locations of the smartphones, i.e., the test site, were at N 45°3'52.4711" E 7°39'42.7179", 2022-06-14 at 14:50 UTC +00:00 while the portable spoofer broadcast spoofing signals over GPS L1 band with a fake location at N 45°09'28.5" E 7°34'47.9", 2022-06-14 at 14:00 UTC +00:00 which was approximately 12 km away from the test location. Based on the results of the previous test campaigns (Rustamov et al., 2020b,a), we modified the test settings to achieve the most vulnerable conditions under which an Android™ smartphone could be spoofed by a simplistic attack. To this aim, the test has been executed in both normal and pilot/airplane modes. Normal operational modes in smartphone foresees wireless data connectivity that allows smartphones to download updated GNSS ephemeris. Such a data can be used for cross-checking the time-consistency of the received navigation message in rudimentary anti-spoofing techniques. However, in (Rustamov et al., 2023) it has been shown that no relevant differences have been observed by operating the devices under test in the two modes. For a conservative and more realistic approach, all the results presented in this article have been obtained in normal operational modes.

Table 1: Android™ devices under test and embedded GNSS chipsets with supported frequency bands.

Model	System on chip (SOC)	GPS Bands
Samsung A30	Qualcomm Exynos 7904 Octa	L1
Samsung A32	Qualcomm Snapdragon 720G	L1
Samsung S6	Qualcomm Exynos 7420 Octa	L1
Samsung A20	Qualcomm Exynos 7884 Octa	L1
Samsung Note 8	Qualcomm Snapdragon 835	L1
Samsung Note 20	Qualcomm Exynos 990	L1
Samsung A21s	Qualcomm Snapdragon 720G	L1
Samsung Note 22	Qualcomm Snapdragon 8	L1
Samsung A72	Qualcomm Snapdragon 720G	L1
Xiaomi Redmi 6	Mediatek MT6762 Helio P22	L1
Xiaomi Redmi 6 Pro	Qualcomm Snapdragon 636	L1
Xiaomi Redmi 8	Qualcomm Snapdragon 845	L1+L5
Xiaomi Redmi 8 Pro	Qualcomm Snapdragon 845	L1+L5
Xiaomi Note 9	MediaTek Helio G85	L1+L5
Xiaomi Note 11	Qualcomm Snapdragon 680 4G	L1+L5
Xiaomi 12x	Qualcomm Snapdragon 870	L1+L5
Huawei Y9	Octacore HiSilicon Kirin 710	L1
Honor X8	Qualcomm Snapdragon 680	L1

IV. RESULTS AND DISCUSSION

1. Correlation Matrix and Average Pearson Coefficients

We discuss hereafter the Pearson correlation matrices under both legitimate and spoofing signals of three representative datasets for three different devices. As it can be observed, in the Samsung A30 dataset Figure 5b, one of the highest correlations corresponding to the pair PRN 1 and PRN 3 ($\hat{\rho}_{1,3} = 0.99$). Similarly, PRN 1 and PRN 3 were highly correlated for the Samsung A30, Samsung S6 and Xiaomi 8 dataset, as shown in Figure 5d ($\hat{\rho}_{1,3} = 0.98$), Figure 5f ($\hat{\rho}_{1,3} = 0.99$) and Figure 5h ($\hat{\rho}_{1,3} = 0.97$). In both the datasets, the C/N_0 time series increases the value of the Pearson coefficient of $\delta\bar{\mu}_\rho = 92.94\,\%$, $\delta\bar{\mu}_\rho = 95.75\,\%$, $\delta\bar{\mu}_\rho = 79.31\,\%$ and $\delta\bar{\mu}_\rho = 89.31\,\%$ during the spoofing time period, with respect to the non-spoofed one where lower or negative correlation coefficients, $\hat{\rho}_{1,3} = -0.76$, $\hat{\rho}_{1,3} = 0.18$, $\hat{\rho}_{1,3} = -0.30$ and $\hat{\rho}_{1,3} = -0.30$ are observed in both Figure 5a, Figure 5c, Figure 5e and Figure 5g populations. A summary of the experimental campaign is given in Figure 6 for different devices under test. It can be seen that the Pearson correlation increment varies depending on the dataset but the spoofing alarm is always correctly raised by realying on a threshold $\gamma = 0.5$. The complete analysis of all the datasets confirms how a significant increment on the correlation between the time series can be observed for all the pairs of the PRNs, and thus the mean of the Pearson coefficient defined in (11) is a suitable metric for the detection of a single-antenna spoofing attack based exclusively on the observation of raw GNSS measurements.

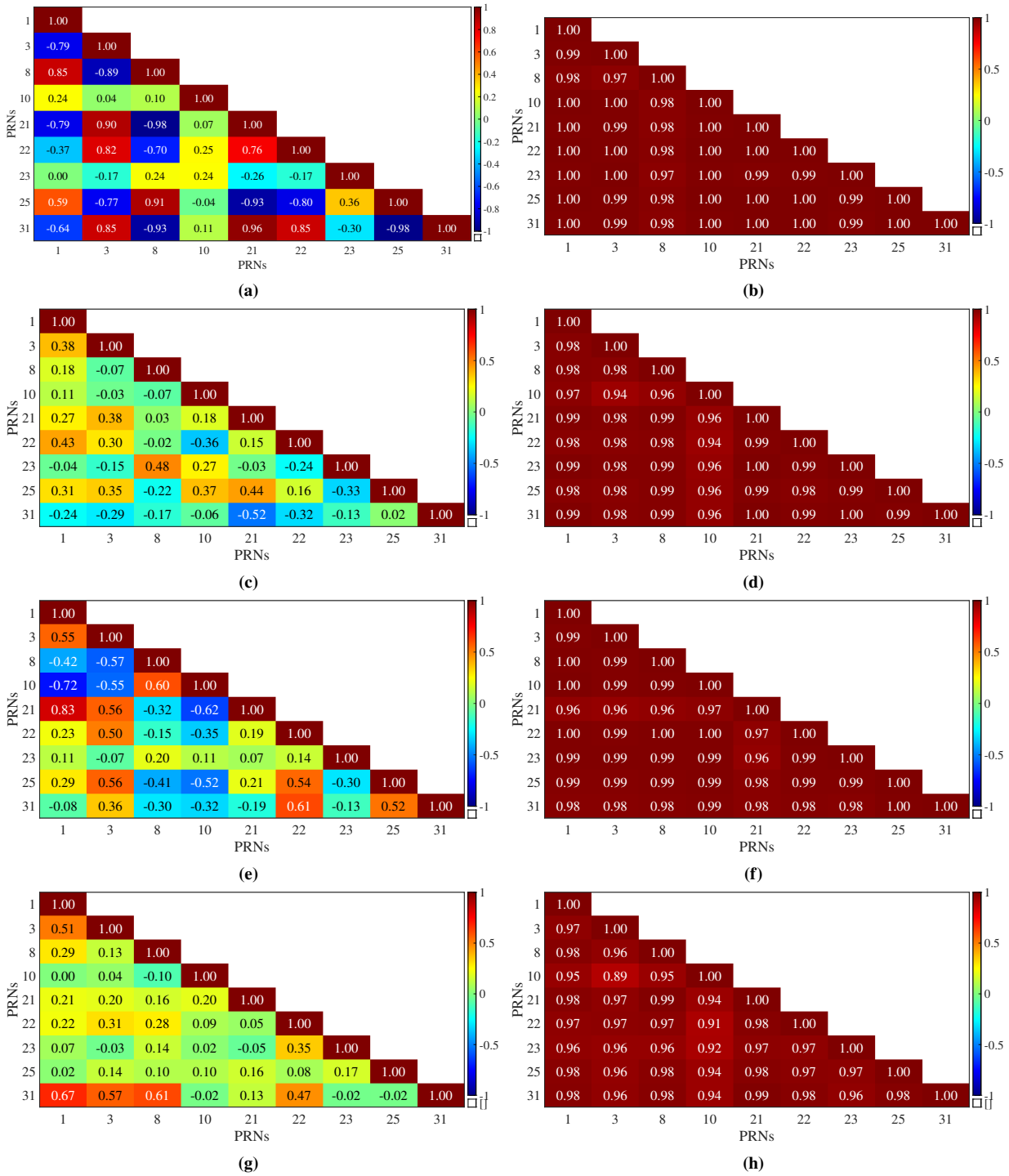


Figure 5: Sample heatmaps showing Pearson correlation coefficients between available PRNs according to (10). Results were computed over an observation window of duration $T_n = 50$ s during the spoofing (a,c,e,g) and non spoofing periods (b,d,f,h) for the Scenario 1.

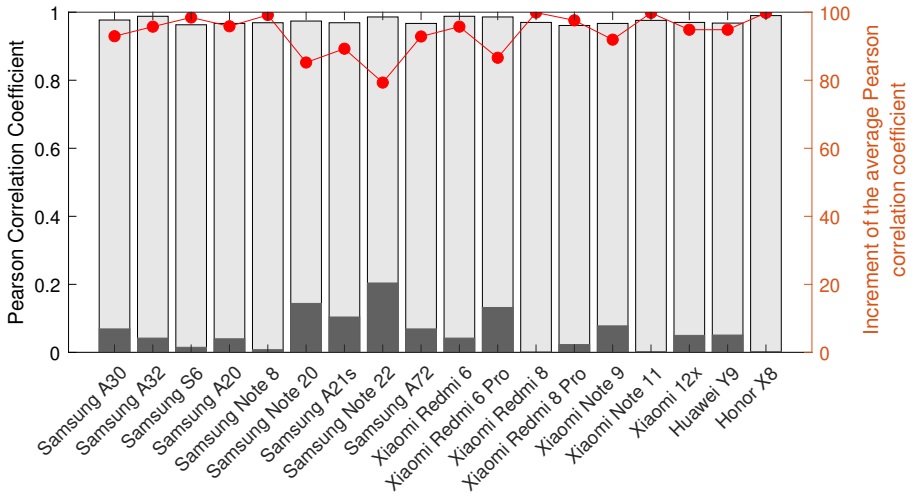


Figure 6: Mean Pearson correlation coefficients and average correlation increment evaluated under $T_n = 50\,\text{s}$ for each dataset under non-spoofed and spoofed conditions.

2. Observation window length and detection latency

The results presented in a Subsection II.2 were obtained using a predetermined observation window length of $T_n = 50\,\text{s}$. However, it is natural to explore the relationship between the window length and the reliability of the threshold in detecting possible spoofing attacks. To determine the minimum latency required for such detection, we evaluated the average Pearson correlation coefficients, denoted as $\mu_\rho^{(K)}$, for different window lengths ranging from $5\,\text{s}$ to $400\,\text{s}$.

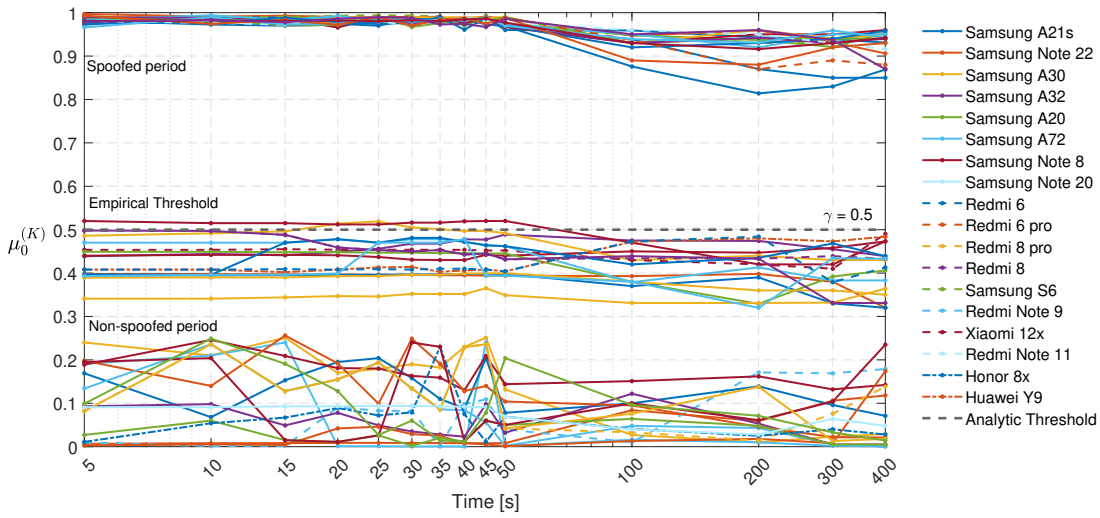


Figure 7: Mean Pearson correlation coefficients computed for all the devices under test by varying the duration of the observation time window in 5-400 s.

Figure 7 depicting the behavior of $\mu_\rho^{(K)}$ and the estimated threshold, γ, was generated by varying the observation window lengths for all devices under test. In the range of $5\,\text{s}$ to $50\,\text{s}$, the coefficients were reported with a step size of $5\,\text{s}$. It can be observed that the observation windows can be adjusted, either shortened or extended, without significantly affecting the performance of the proposed method. Shorter windows reduce decision logic latency and data buffering requirements but may result in unreliable output coefficients, as exemplified by the case of the Samsung A32 in a particular scenario. Conversely, increasing the window length introduces a longer latency and increases vulnerability to environmental variability within the observation period. Considering these findings, a window length of $T_n = 50\,\text{s}$ was selected as a valuable and safe trade-off

between latency and reliable correlation coefficients for this study.

V. CONCLUSIONS

In this study, it was observed that while smartphones are generally considered resilient to spoofing attacks, properly designed malicious actions can still pose a threat to these devices. We focused on single-antenna spoofing attacks and their impact on the raw GNSS measurements reported by GNSS receivers. The study demonstrated that single-antenna spoofing attacks induce a distinct correlation pattern in the raw GNSS measurements, specifically targeting the C/N_0 parameter. Leveraging this correlation, the researchers developed a method to detect simplistic spoofing attacks and formalized the estimation of a correlation index. This correlation index serves as an indicator of the occurrence of a single-antenna spoofing attack against a GNSS receiver. To assess the practicality of their approach, the study provided a theoretical background on the analysis of Pearson correlation coefficients and their applicability to spoofing detection on mass-market Android™ devices. The researchers suggested an observation window ranging from $T_n = 5 - 50$ s to estimate pairwise correlation indices. This window size aimed to achieve a false alarm probability of 1.5 %. Overally, this research highlights the importance of considering the potential vulnerabilities of smartphones to spoofing attacks, even though they are generally considered resilient. By identifying and leveraging the correlation induced by single-antenna spoofing attacks, the study provides a method to detect spoofing attacks and offers insights into their impact on GNSS receiver measurements. These findings contribute to the ongoing efforts to enhance the security and resilience of smartphones against spoofing attacks.

ACKNOWLEDGEMENTS

A. Minetto acknowledges funding from the research contract no. 32-G-13427-5 DM 1062/2021 sustained by the Programma Operativo Nazionale (PON) Ricerca e Innovazione of Italian Ministry of University and Research.

REFERENCES

Bastide, F., Akos, D., Macabiau, C., and Roturier, B. (2003). Automatic Gain Control (AGC) as an Interference Assessment Tool. In *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pages 2042–2053, Portland, OR.

Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., and Lachapelle, G. (2012). Gnss spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium*, pages 479–487.

Dovis, F. (2015). *GNSS interference threats and countermeasures*. Artech House.

Fisher, R. (1925). *Statistical Methods for Research Workers*. Biological monographs and manuals. Oliver and Boyd.

Humphreys, T., Ledvina, B., Psiaki, M., O'Hanlon, B., and Kintner, J. (2008). Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pages 2314–2325.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., and Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012.

Kendall, M. G. et al. (1948). The Advanced Theory of Statistics. Vols. 1. *The advanced theory of statistics. Vols. 1.*, 1(Ed. 4).

Lachapelle, G. and Gratton, P. (2019). GNSS Precise Point Positioning with Android Smartphones and Comparison with High Performance Receivers. In *2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP)*, pages 1–9.

Lee, D.-K., Spens, N., Gattis, B., and Akos, D. (2021). Agc on android devices for gnss. In *Proceedings of the 2021 International Technical Meeting of the Institute of Navigation*, pages 33–41.

Manfredini, E. G., Akos, D. M., Chen, Y.-H., Lo, S., Walter, T., and Enge, P. (2018). Effective gps spoofing detection utilizing metrics from commercial receivers. In *Proceedings of the 2018 International Technical Meeting of The Institute of Navigation*, pages 672–689.

Minetto, A., Bello, M. C., and Dovis, F. (2022). DGNSS cooperative positioning in mobile smart devices: A proof of concept. *IEEE Transactions on Vehicular Technology*, 71(4):3480–3494.

Minetto, A., Nardin, A., and Dovis, F. (2021). Modelling and Experimental Assessment of Inter-Personal Distancing Based on Shared GNSS Observables. *Sensors*, 21(8).

Muirhead, R. J. (2009). *Aspects of multivariate statistical theory*. John Wiley & Sons.

Rustamov, A., Gogoi, N., Minetto, A., and Dovis, F. (2020a). Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices. In *2020 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6.

Rustamov, A., Gogoi, N., Minetto, A., and Dovis, F. (2020b). Gnss Anti-Spoofing Defense Based on Cooperative Positioning. In *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, pages 3326–3337.

Rustamov, A., Minetto, A., and Dovis, F. (2023). Improving GNSS spoofing awareness in smartphones via statistical processing of raw measurements. *IEEE Open Journal of the Communications Society*, 4:873–891.

Spens, N., Lee, D.-K., Nedelkov, F., and Akos, D. (2022). Detecting gnss jamming and spoofing on android devices. *NAVIGATION: Journal of the Institute of Navigation*, 69(3).