POLITECNICO DI TORINO
Repository ISTITUZIONALE

GNSS Anti-Spoofing Defense Based on Cooperative Positioning

Original
GNSS Anti-Spoofing Defense Based on Cooperative Positioning / Rustamov, Akmal; Gogoi, Neil; Minetto, Alex; Dovis, Fabio. - ELETTRONICO. - (2020), pp. 3326-3337. ((Intervento presentato al convegno Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020) [10.33012/2020.17565].

Availability:
This version is available at: 11583/2854538 since: 2020-12-03T11:04:39Z

Publisher:
Institute of Navigation

Published
DOI:10.33012/2020.17565

Terms of use:
openAccess

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

Publisher copyright

(Article begins on next page)

18 October 2022

GNSS Anti-Spoofing Defense Based on Cooperative Positioning

Akmal Rustamov, Neil Gogoi, Alex Minetto and Fabio Dovis
Department of Electronics and Telecommunications (DET), Politecnico di Torino, Italy
e-mail: name.surname@polito.it

BIOGRAPHY

Akmal Rustamov is a PhD candidate at the Department of Electronics and Telecommunications of Politecnico di Torino. His research is focused on implementation and resilience test of a 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. He involved in teaching assistant part of the course "Electrical Machines and Circuit theory" at Polytechnic University of Turin in Tashkent.

Neil Gogoi completed his 1st and 2nd Level Masters at the University of Nottingham, U.K and Politecnico di Torino, Italy respectively in the field of Navigation technology. His past work includes Multi-Constellation GNSS performance investigation and GNSS deformation monitoring. Currently he is pursuing a PhD at Politecnico di Torino within the NavSAS group with the support of PIC4SeR. His aim is developing effective navigation systems for robotic vehicles with current focus on the feasibility of Android smartphones and cooperative algorithms towards it.

Alex Minetto has finished his PhD candidate at the Department of Electronics and Telecommunications of Politecnico di Torino within the Navigation Signal Analysis and Simulation (NavSAS) group. His research is focused on GNSS based cooperative positioning algorithms. He developed his Master Thesis at European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) in Darmstadt (Germany), addressing the development of a new precise detection algorithm for radar pulses sent from Metop satellites during their calibration campaign.

Fabio Dovis is an associate professor at the Department of Electronics and Telecommunications of Politecnico di Torino as a member of the Navigation Signal Analysis and Simulation (NavSAS) group. His research interests cover the design of GPS and Galileo receivers and advanced signal processing for interference and multipath detection and mitigation. He has a relevant experience in European projects in satellite navigation as well as cooperation with industries and research centers.

ABSTRACT

Radio navigation is of utmost importance in several application fields. Nowadays, many civil and professional applications massively rely on the Global Navigation Satellite System (GNSS) and related technologies to accurately estimate position and time. Existing GNSS-based systems are threatened by malicious attacks among which spoofing and meaconing constitute severe challenges to the receiver. Several of such GNSS systems constitute mass market applications and devices, and a threat to the GNSS receiver could have cascading effects at application levels and for interconnected systems. Networked GNSS receivers are in general ubiquitous because any receiver embedded in a complex system such as a smart device or smart connected cars can exploit network connectivity. This novel generation of valuable-performance GNSS receivers are prone both to standard RF spoofing attacks and to cyber-attacks conceived to hijack complex network based services such as DGNSS-based cooperative positioning. By means of a set of experimental tests, this paper highlights possible metrics to be checked to identify malicious attacks to the positioning and navigation systems in mass market connected devices. The network-based exchange of GNSS data such as GNSS raw measurements recently disclosed in Android smart devices is conceived in this work to offer the possibility to compare or combine such metrics to better identifies spoofing and meaconing attacks.

I. INTRODUCTION

The presence of the Global Navigation Satellite System (GNSS) technology in modern life has been constantly growing in the recent years, supporting the use of GNSS receivers in diverse fields of applications involving civilian, military, leisurely, safety of life and financial sectors. A constantly growing attention is being devoted to the security and safety of GNSS related technologies with one of the threats being malicious attack such as spoofing and meaconing. The terms refer to an unauthorized transmission of locally generated Radio Frequency (RF) signals forcing receivers nearby to compute a fake Position Velocity Time (PVT) solution. From the perspective of GNSS signals, according to the current version of the Interface Control Documents (ICDs) [1], GNSS signals (e.g. GPS L1 C/A, E1 Galileo and GLONASS) do not provide any means to the receivers by default in order to ensure the authenticity of the source of the satellite signals or to improve the robustness of

the receiver against possible spoofing attacks [2]–[4]. The European Galileo is planning the use of Open Service Navigation Message Authentication Signal (OSNMA) and the Commercial Authentication Service (CAS) for allowing users to calculate PVT solution based on trusted signals in the near future. While these countermeasures are being implemented at system level to provide a minimum level of protection also on signals exploited by mass-market applications, there is a widespread debate if even by means of a simplistic spoofing attack it would be possible to threaten GNSS receivers with a cascading effect at application level and for interconnected systems [5]. It is known that, a lack of synchronisation between spoofers and GNSS timescale can be theoretically used to detect such spoofing attacks with a small effort. On the other hand, specific dedicated detectors are not implemented in most positioning units in the consumer field such as simple unmanned aerial vehicles (UAVs), smartphones and other personal devices, making them vulnerable to spoofing attacks. From a general perspective, the GNSS receiver plays a core role as being usually the only one providing an absolute estimation of the position. However, in mass-market devices it is part of a positioning unit that is comprised of GNSS technology, along with Inertial Measurement Units (IMUs), electronic compasses, etc., which helps in aiding or refining the positioning solution. Furthermore, in several cases the positioning unit is typically interfaced to an application layer (i.e. Location-Based Services), and the position information or related measurements are exchanged to other services or remotely processed in remote servers such as for snapshot positioning. Such an architecture is prone to any of common spoofing attacks at signal and non-signal level (cyberattacks) especially if it is based on low cost commercially available off-the-shelf (COTS) products which use standard positioning services (GPS C/A, Galileo Open Service, GLONASS, etc.), and standard unencrypted communication services. Consequently, it is worth examining the impairment of intentional interferences to the low-cost GNSS units embedded in the mass market receivers and further assessing the resilience of the overall device or platform. Many researchers have utilized different methods to measure spoofing attacks in recent years. A GNSS satellite simulator was firstly used to a GNSS spoofing experiment in [6]. In [7], researchers at the University of Texas at Austin developed a portable low-cost GPS spoofer. Similarly, in [8] a commercial super yacht was successful spoofed with intermediate spoofing techniques, with it being one of the most well-known assessment of the threat of spoofing. A number of techniques have been developed since then to mitigate spoofing for GNSS security. Despite these remarkable results, they require additional hardware or changes to the interface specification. The complete work aims to develop an anti-spoofing detection and coping mechanism in connected COTS GNSS devices, but what is presented in this paper are the assessment of parameters and metrics to understand the occurrence of a spoofing attack taking advantage of the cooperative paradigm of networked GNSS receivers. This approach is particularly interesting to explore because of the appealing application of Cooperative positioning (CP) in short range communication networks such as Vehicle to vehicle (V2V) in vehicular navigation field and distributed ad hoc infrastructures. In order to demonstrate the potential of CP techniques, a popular COTS GNSS receiver and different commercial Android smartphone devices and are used for the assessment. The latter can be considered as ultra-low cost COTS GNSS receivers when considering only their GNSS units [9]. An advanced experiment was conducted considering a real-time-oriented collaborative framework using combination of raw measurements to determine inter-agent distances and improve the position estimation accuracy. A low cost portable spoofer platform able to place simplistic attacks is developed and experimental tests are performed on selected COTS devices.

The rest of the paper is organised as follows: In Section II, methodology, background of a spoofing attack, CP techniques and the state of vulnerability of receivers are explained. Section III provides the experimental setup and test. Results and analysis on the performance of the smartphones under the spoofing attack is discussed in Section IV. Conclusions and further research are then drawn in Section V.

II. Methodology

A. RF Spoofing attacks

We developed a low-cost portable spoofer based on a Great Scott Gadgets™ HackRF One™ platform and a Raspberry™ PI 4B. The used front-end HackRF One™ is a low-cost, open-source Software Defined Radio allowing fast and accurate RF signal transmission from binary files. This front-end can receive and transmit signals from 1 MHz to 6 GHz with adjustable power and channel capacity. The software used to numerically generate the spoofed GPS signal is GPS-SDR-SIM [10], an open GPS L1 C/A signal generator toolbox distributed with a MIT license [11]. The attack was planned simulating a static position and all the visible satellites belonging to GNSS constellations and their signals were transmitted to the SDR equipment. An optional reference clock can be used to discipline the signal generation at an increased cost of the overall equipment. For the scope of the paper, reference oscillator was not connected to the front-end. Power supply can be provided through a mass-market, 10000 mAh battery pack according to the supply specification of the Raspberry™ PI 4B. The HackRF One™can be then supplied by the Raspberry PI itself through the USB 3.0 interface. The spoofing attack can be performed through the portable spoofer according to the following steps:

1) *Trajectory generation*. The fake trajectory was generated in Linux OS implementing the daily GPS broadcast ephemeris Receiver Independent Exchange Format (RINEX) file, a National Marine Electronics Association (NMEA) GGA stream and a `.csv` file containing the Earth-centered Earth-fixed (ECEF) position with a 10 Hz sampling rate. The file is transmitted through the USB interface of the Raspberry™ PI 4B.

2) *Numerical signal generation*. The trajectory is then injected to the GPS-SDR-SIM. The software generates the simulated pseudorange and Doppler for the GPS satellites in view. This simulated range data was used to produce a file with In-phase / Quadrature (I / Q) samples of the complex baseband signal envelope ready to be inserted into the front end of the SDR (i.e. HackRF One™).
3) *Digital to analogue conversion and RF signal transmission*. The front-end (HackRF One™) is in charge to perform the digital-to-analogue conversion mixing the baseband signal provided at step 2 to the carrier frequency (i.e. GPS L1 C/A), thus, offering quadrature modulation in L1 band.

RF signal model: Low-power received signal makes GNSS receiver vulnerable to any kind of interference. In order to take control GNSS receivers a portable spoofer need to replicate satellite spreading code, radio frequency carrier and navigation date bits of selected GPS L1 satellite signal. When there is no present spoofing interference, the typical GPS L1 signal can be expressed as follows:

$$x_{L1,i}(t) = \sum_{i=1}^{N_s-1} \sqrt{P_C} D_i(t-\tau_i) C_i(t-\tau_i) cos(2\pi \triangle f_i t + \triangle\theta_i) \tag{1}$$

where $x_{L1,i}(t)$ is the L1 C/A authentic signal received by i th satellite signal, N_s is the number of visible satellites. P_C is the signal power carrying C/A code, $D_i(t)$ is the navigation data bit stream, $C_i(t)$ is the C/A spreading code sequence(BPSK PRN), $\triangle f_i t$ is the frequency difference, τ_i is the i th signal code phase and $\triangle\theta_i$ is phase offset. A simplistic portable spoofer generate and broadcast GPS L1 C/A code like signals but it is not able to make them consistent and time-synchronized with real signals. Generated fake signals have a similar structure compare to an authentic one, with the only differences being the Doppler shift, time shift and higher power level. In order to capture the victim receiver's tracking loop, the fake signal must be phase and Doppler matched to the authentic signal.

$$x_{L1,si}(t) = \sum_{i=1}^{N_s-1} \sqrt{P_C} \hat{D}_i(t-\tau_{si}) C_i(t-\tau_{si}) cos(2\pi \triangle f_i t + \triangle\theta_{si}) \tag{2}$$

A simplistic portable spoofer broadcasts estimated code, carrier phase and data bit stream (τ_{si}, $\triangle\theta_{si}$, $\hat{D}_i$) for $i = 1, 2, 3, ...N$. Taking into account that the spoofing signal $x_{L1,si}(t)$ is generated through older ephemera data, this causes rough discrepancies in the navigation message and is inconsistent with respect to real authentic $x_{L1,i}(t)$ signals. Due to the lack of time synchronization, counterfeit signals $x_{L1,si}(t)$ are typically affected by non-negligible residual modulation effect where $\triangle f_i \neq 0$ and $\triangle\theta_i \neq 0$.

When GNSS receiver under the simplistic spoofing attack, it accepted both real authorized signals and spoofing signals. During the RF attack total signal at victim receiver is:

$$x_{tot}(t) = x_{L1,i}(t) + x_{L1,si}(t) + n(t) \tag{3}$$

where $n(t)$ is Gaussian noise. Thus in our experiment we started the spoofing signal with low power and increased it gradually. Moreover, for a successful spoofing strategy, the spoofed code phase $\tau_{s1}, ..., \tau_{si}$ and carrier phase $\theta_{s1}, ..., \theta_{si}$ needed carefully design.

B. Cooperative Positioning and Spoofing

CP framework can encapsulate additional monitoring to avoid current and next-gen-type attacks to the positioning and navigation units. The work presented in [12] opened the investigation to the DGNSS-CP based on the inter-device range from GNSS raw measurements between two Android devices within a communication framework. The availability of cooperative algorithms applied to the GNSS pushed researchers to design new framework to cope for the limitations of traditional PNT approaches. The DGNSS-CP framework investigated in this work ideally supports the exchange of raw GNSS measurements among multiple receivers interconnected by 4G LTE or Wi-Fi connectivity executed through an Android application. The measurements are hence synchronized through a Doppler compensation technique [13] and the inter-agent distance is computed through a differential GNSS approach [14].

The DGNSS-CP framework presented by the authors acts according to the following steps for each PVT epoch, t_k

1) Agent $\mathbf{A}$ sends to $\mathbf{T}$ its set of raw pseudorange measurements $\boldsymbol{\rho}_A(t_k)$ and the estimated position $\hat{\mathbf{x}}_A(t_k)$ with an associated timestamp t_k
2) Agent $\mathbf{A}$ aligns the external set of measurements retrived from $\mathbf{T}$ $\boldsymbol{\rho}_A(t_k)$, to the closest set of measurements locally dumped.

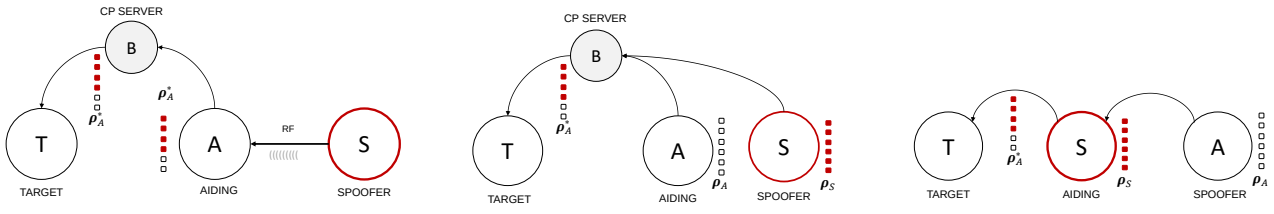
3) Agent **A** combines the local and external pseudorange measurements through differential method to determine the inter-agent distance between **A** and **T**
4) Agent **A** integrates such **A**-**T** inter-agent distance w.r.t. the position of **T** (consistent) along with local pseudorange measurements within its navigation algorithm (i.e. Extended Kalman Filter (EKF))
5) The position estimation of **A** is generally improved by the additional information carried by the set of pseudorange measurements shared by other receivers and it is not expected to show any particular drift [15].

Technical details concerning the implementation of the framework can be found in [16]–[18] and a proof-of-concept applied to Android smartphones was developed within the ESA project HANSEL.

The aforementioned DGNSS-CP framework is prone to be fooled by malicious attacks at different stages of the GNSS processing chain

- **Signal domain**: performed through the transmission of RF signals, according to the description provided in II-A. This approach induces the tracking of the fake signals to an aiding receivers, thus the computation of fake pseudorange measurements, and in turn, of a fooled PVT estimation of both aiding and aided receivers. A scheme of the attack is provided in Figure 1a.
- **Measurements domain** This approach acts by replacing the measurements transferred to the server of a CP client-server architecture, as in Figure 1b, or performing a man-in-the-middle attack, to ideally perform a "virtual" spoofing/meaconing attack as shown in Figure 1c.

An attack pursued in any of this domains induces similar effects on the final positioning estimation but a proper distinction is worth to distinguish the typology of attack between *classical spoofing/meaconing* and *cyber-attack*. The latter are indeed less related to the receiver architecture and mostly focused on the system/network. With the control over sharing of specific information between the devices and availability of synchronization strategy, some strategies will be proposed to detect the presence of spoofing in one or multiple networked GNSS receivers devices. Therefore, the possibility to imprint such an algorithm to COTS GNSS receivers on other networked operating platforms can open several possibilities oriented to spoofing attacks such as in networked Unmanned Aerial Vehicles (UAVs) and Unmanned Ground Vehicles (UGVs).



(a) (b) (c)

Fig. 1: Schemes of possible attacks performed through a GNSS-based CP framework. Filled squares represent fake measurements provided by S while white squares are nominal measurements provided by A.

III. Experimental Tests

The following scenarios were defined to investigate potential countermeasures to the malicious attacks against GNSS.

A. Scenarios 1: Test on static Android Smartphones

For the primary test, two different commercial smartphones (with Broadcom® BCM47755 GNSS chipsets) were chosen for testing the effect of a simplistic spoofing attack performed through the portable spoofer described in Section II on consumer GNSS receivers. Both of the devices, denoted as S1 and S2 respectively further in this work are equipped with Google Android™ 9 Operating System (OS) and the GNSS Logger Android application provided by Google™ was installed in them for identification and procurement of GNSS raw measurements. A 800 seconds spoofing scenario was tested in a controlled outdoor environment with open sky conditions. During the test, the devices were located at a distance of 10 meters apart, where S1 was places next to the spoofer to explore the effect of interference and S2 was kept 10 meters away to avoid the risk of spoofing under open sky conditions. The range of the spoofer was kept to around 2 meters and in order to prevent any radio-frequency interference (RFI) disturbances beyond the range of the controlled environment a 10 dB attenuator was used and inserted to the coaxial cable to reduce transmitting signal power levels. Both smartphones actual locations were around the coordinates 45.06 N, 7.66 E (Turin, Italy). During the first 120 seconds of the test, both devices received live GNSS signals without any other interference. Then the portable spoofer was switched on, broadcasting spoofing signals over GPS L1 band

with coordinates 45.755664 N, 4.831035 E (Lione, France) with S1 in its range. The spoofing signals were broadcasted for 500 seconds after which the spoofer was switched off. For the remaining duration, both devices received only live GNSS signals. In general, 16 GPS satellites were considered during the test. The satellites could be divided into three different group. The first subgroup (Real) consists of real-time Satellite Vehicle Identifiers (SV IDs) received by each device and not part of the satellites transmitted by the spoofer. The second subgroup (Fake) consists of SV IDs that were broadcasted by the spoofer and available to all smartphones, but their real equivalents were not displayed during the test [15, 19, 24]. The third subgroup (Common) consists of concurrent Satellite Vehicle (SV) IDs which were both in-view in real time and transmitted by the spoofer [10, 14, 32].

B. Scenarios 2: Simulated meaconing attack in multi-agent vehicular scenario

This section presents a preliminary investigation of a simulated meaconing attack affecting one agent being part of a multi-agent network. The meaconing aims at forcing the computation of the inter-agent distance (a.k.a. baseline length) by using fake pseudorange measurements provided by a spoofer chosen among the available agents. The simplistic scenario is composed of 3 agents within a multi-agent network:

- The target ($\mathbf{T}$) (the kinematic agent which is expected to benefit from cooperation)
- The aiding agent $\mathbf{A}$ (a further kinematic agent providing pseudorange measurements)
- The spoofer ($\mathbf{S}$) (an agent generating pseudorange measurements related to its own position but to be used to fake the contribution of $\mathbf{A}$ to $\mathbf{T}$).

According to the nominal steps recalled about the cooperative framework in Section II-B, the following considerations about this specific attack hold if $\mathbf{S}$ overwrites the pseudorange measurements transmitted by $\mathbf{T}$ but not its reference position. Formally

- Agent $\mathbf{A}$ simply receives a packet composed by the position of $\mathbf{T}$ and the measurements of $\mathbf{S}$
- Agent $\mathbf{A}$ aligns the external set of measurements of $\mathbf{S}$ to the closest (in time) set of measurements dumped locally
- Agent $\mathbf{A}$ combines the local and external pseudorange measurements through some differential method (i.e. DD) to determine the inter-agent distance between $\mathbf{A}$ and $\mathbf{S}$
- Agent $\mathbf{A}$ integrates this inter-agent distance A-$\mathbf{S}$ w.r.t. the position of $\mathbf{T}$ (inconsistent) along with local pseudorange measurements within its navigation algorithm
- The position estimation of $\mathbf{A}$ is "generally degraded" by the additional information and it diverges from the standalone GNSS solution

IV. Results and Analysis

After presenting a validation of the spoofing scenario at Section III-A, the results and analysis section is roughly split into following parts. The first part Section IV-A and IV-B deals with the comparison of GNSS raw measurements between the two connected and synchronized devices in order to build up an effective anti-spoofing strategy. The second part Section IV-C firstly presents the results of a meaconing test on the CP framework chosen for this work and then the advances to the framework which could be made to identify spoofing attacks.

A. Validation of Spoofing Attack

The u-blox™ Neo-M8N GNSS receiver was used for cross validation of the test measurements during the primary test. Figure 2 shows the change in geodetic coordinates of the u-blox GNSS receiver during the test . It can be seen that the receiver has no defence against the simplistic spoofing attack with the latitude, longitude and altitude changing to that of the spoofed coordinates hence validating the spoofing mechanism employed on a regular COTS device.

In another tertiary test replicating the same spoofing attack methodology on S1, S2 and an added smartphone S3, it was seen that the positions of the smartphones were not spoofed by the spoofer broadcasted signals. It has to be noted that the equipment and RF spoofing signal is identical in this test and could not be carried out along with the main tests due to logging problems of NMEA and GNSS raw measurements data simultaneously.There was a slight meter of deviation in the positions during the spoofing period, displayed on the left of Figure 3 which shows the variation in the Earth-Centered Earth-Fixed (ECEF) Z coordinate from the reference chosen, as an example. These few metres of deviation in the position output of the Android devices can be attributed to the loss of some satellites due to interference as will be seen later and it can be roughly visualized on the right of the Figure 3 which shows number of satellites acquired during the time period. The vertical doted line in the figure corresponds to the start of the spoofing period. It can be speculated that the smartphones maintain their true position with the help of multi-constellation, multi-frequency GNSS capabilities along with network positioning and other sensors. It is also interesting to notice that S3 carries the Broadcom™ BCM 4774 chipset without dual frequency GNSS capabilities and it is affected the most, comparatively. This is seen to be due to the spoofing signals acting as an interference on the L1 band, hence hampering reception of low-quality signals. The smartphones hence inherently have a robustness to such simplistic spoofing

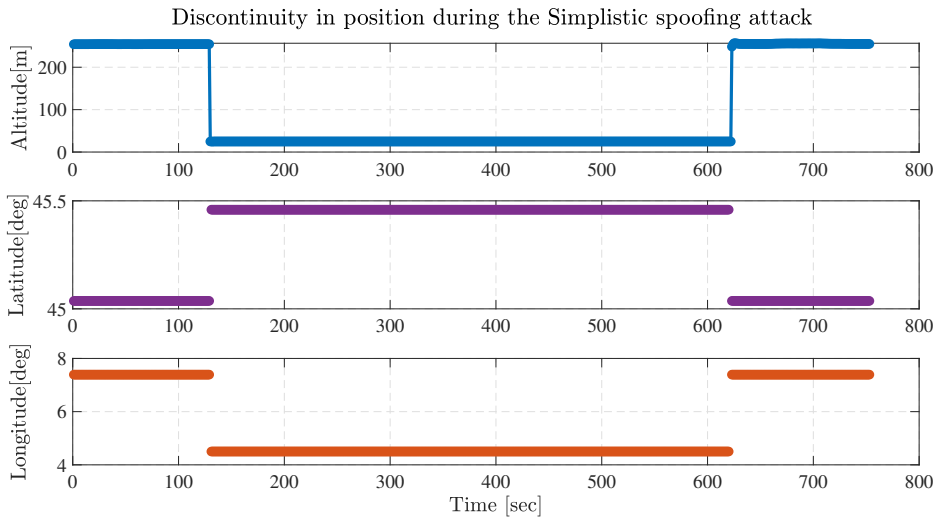


Fig. 2: Effect of spoofing interference on u-blox™ Neo-M8N receiver.

attacks due to it being an accumulation of multiple sensors, connected networks and complicated positioning algorithms. This however does not mean that the spoofed signals aren't acquired, but only that the PVT computation of Android location API ignores the spoofed signal measurements. With a multitude of Android applications being developed in recent times utilizing GNSS raw measurements directly, the simplistically spoofed signals being acquired and tracked in Android devices pose a significant threat. Therefore, an analysis of the acquired Android Raw GNSS Measurements of smartphones under and without a spoofing attack simultaneously follows.

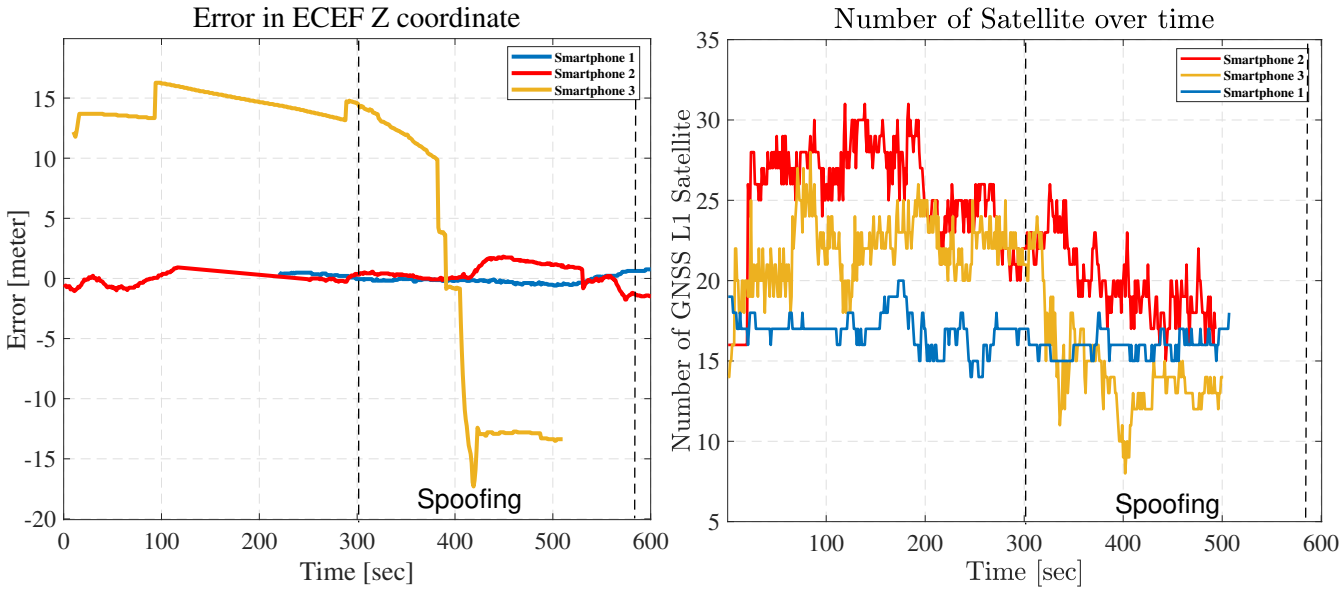


Fig. 3: Effect of spoofing on: a) Earth-Centered Earth-Fixed (ECEF) Z coordinate (left) and b) GNSS L1 satellite availability in Android smartphones (right).

B. Analysis of Android Raw GNSS Measurements of the two devices

1) Time and Ephemeris considerations: In Android Smartphones, the GNSS time of signal transmission of each satellite is demodulated from the received signal and presented as a raw measurement used to compute the pseudorange for that particular satellite along with the time of signal reception. However, the latter is taken either from the cellular or Wi-Fi network in the smartphone and hence it has not been possible to affect the reception time with GNSS spoofed signals. Considering the clock biases, since the general difference between the two time stamps falls in the range of 60 - 100 ms, a remarkable difference in the

two timestamps could directly indicate the possibility of a spoofed signal. To generate real time spoofed signals consistent with GNSS time, the scope of the work goes beyond simplistic spoofing. A few of the current Android GNSS devices also support demodulation of the GPS navigation message and present them as a string of numbers to be converted into a binary form. Processing this message for the two different phones showed a clear distinction between satellites of the different subgroups in terms of GPS Time of Week (TOW) and this can be an alternate check to time inconsistency between two devices to detect a simplistic spoofing attack. The resistance of the spoofed device to not acquire the Common subgroup of spoofed satellites as presented in [19] meant however that the same satellite ID could not be compared between two devices at the same time where one device tracks the spoofed satellite and the other tracks the real one. Further, the limitation of most commercial Android phones to not provide the navigation message and the inability to provide navigation messages of other constellations makes this approach very narrow and situational.

2) C/N_0 and AGC comparisons: Figure 4 compares the S1 (under spoofing attack) and S2 (without spoofing attack) GNSS receiver C/N_0 values of various SV IDs during the spoofing test duration. The SV IDs are represented by their PRN numbers on the plot. On the left side of the figure, looking at the C/N_0 time trend of the Real and Common subset of satellites over time (SV ID), it can be seen that it is affected drastically during the spoofing period between 120-620 seconds. It is clear that the spoofer acts as a source of interference over the L1 frequency band disturbing healthy satellites during the spoofing time span with tracking of low elevation satellites being lost at times (PRN 27). This effect is seen for the L1 signals of other constellations as well. The Fake subgroup of satellites appear as expected when the spoofing starts and has a consistent high C/N_0 value corresponding to the static nature of both the spoofer and the Android device. In contrast, the right side of the figure presents the normal behavior of C/N_0 values in the Android device under no spoofing attack. This introduction of noise by the spoofer results in the disturbance of the PVT solution of the GNSS receiver in the device, as seen in the test of Figure 3 regardless of the spoofed satellites not being included in the solution computation. Figure 5 plots the AGC amplification/attenuation value (in dB) of the S1 (left) and S2 (right) devices during the test period. It is observed that the effect of turning on the spoofer is similar to what in-band jamming or interference would do. Due to the presence of powerful spoofing signals, the receiver reduces the amplification of the incoming sign which, while disturbing real signals, allows fake signals to be easily acquired. This is clear when comparing the S1 and S2 of a fake and real signal.

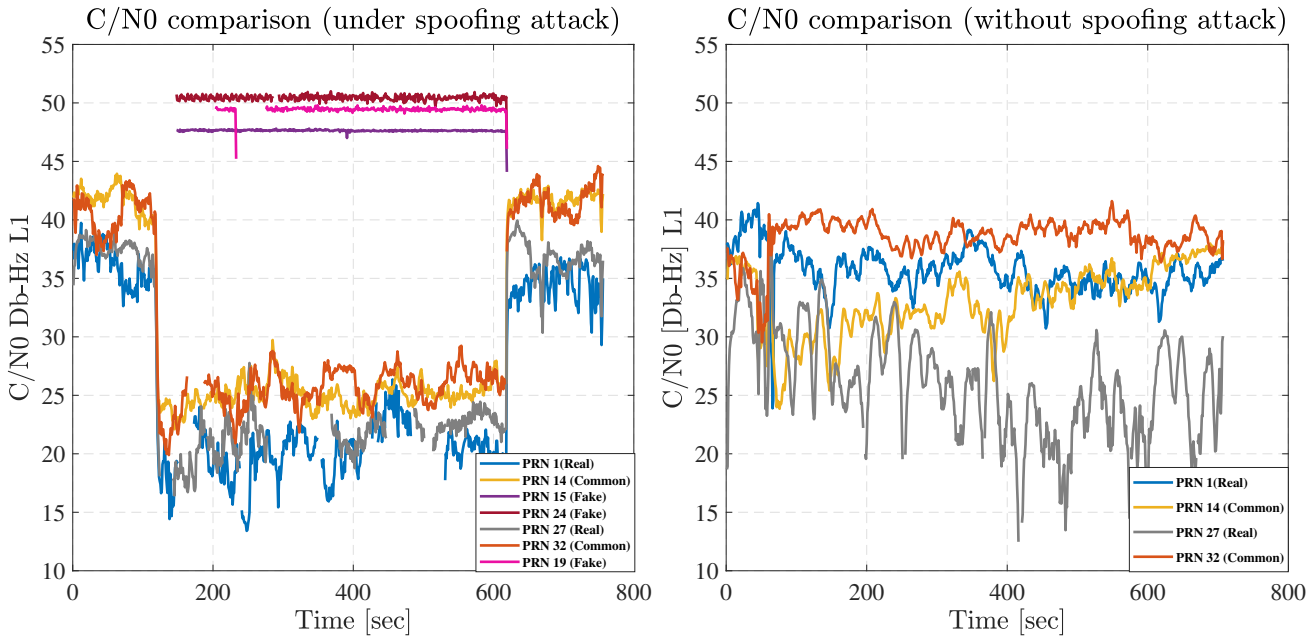


Fig. 4: Effect spoofing on Signal-to-noise ratios with (left) and without (right) spoofing during the test duration.

3) AGC to C/N_0 Ratio: In [20] [21] analyzed correlation between various metrics such as power monitoring, multiple-correlation tap, maximum-likelihood multipath estimator for distinguishing GNSS spoofing, jamming or multipath effects. To build towards a simpler anti-spoofing strategy an attempt is made to narrow the dimension of GNSS raw observations. For AGC, depending on the front-end quantization of a receiver it affects the C/N_0 with different sensitivities [22] and COTS receivers generally have lower bit quantizations. Hence building on the correlation, a parameter equating to the AGC to C/N_0 ratio of its absolute values is observed. Across different Android smartphones, slightly different levels of AGC and C/N_0 are observed depending on the front-end and digital signal processing blocks on similar test conditions. Hence this parameter standardizes the power of a signal at the receiver to an extent taking into account the only variable available in Android devices currently to consider the front-end stage. Identifying the AGC to C/N_0 response of the receiver's front-end to RFI events, we could be able to draw a threshold that will allow us to discriminate between jamming events and spoofing attacks. While

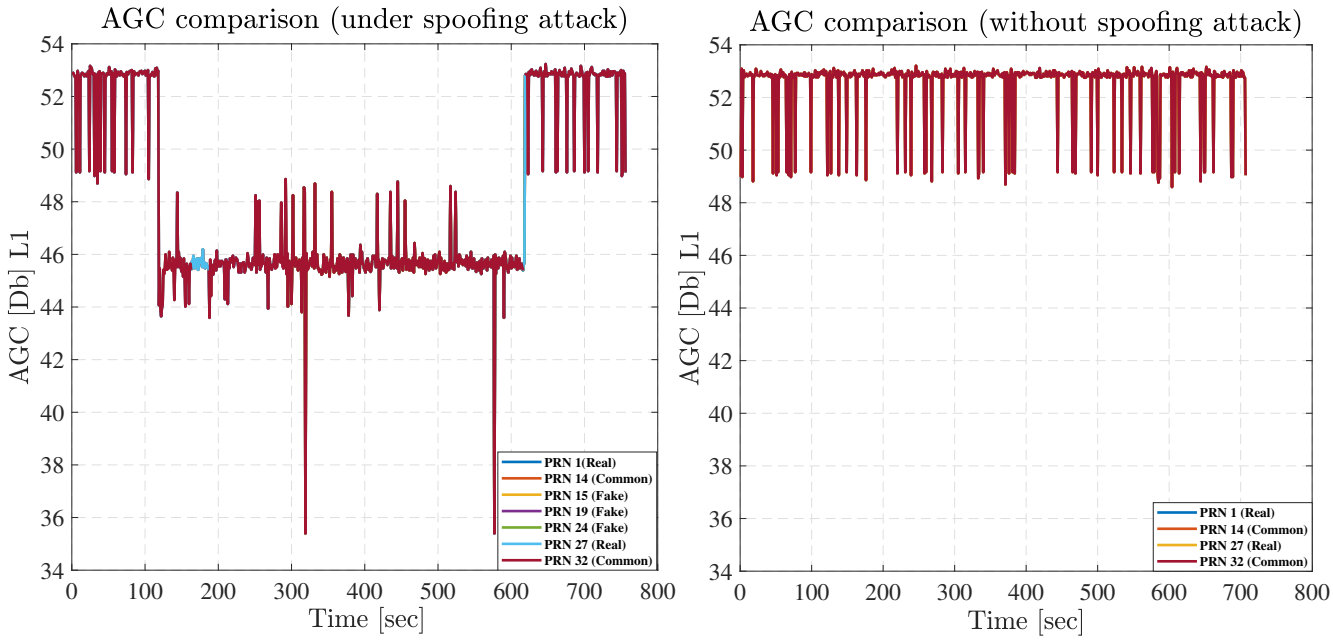


Fig. 5: Effect spoofing on AGC with (left) and without (right) spoofing during the test duration.

spoofing attack lead to a drop of the AGC when they appear within the band, the way they are generated are different because of their respective nature. For a non-intentional RFI attack, the signal is not consistent with the satellite and noise is added to the targeted GPS band, which leads to a drop of the C/N_0 of the tracked signal. Conversely, during a spoofing attack the signal is generated to look like a GPS signal. Thus, it increases the power of the carrier signal and so, it leads to a raise of the C/N_0 value. Figure 6 displays this ratio parameter in the phones S1 and S2 on the left and right respectively. The nature of this parameter can be seen to be similar during periods of non interference in both devices and upon the spoofing period, there is a stark contrast between spoofed and non spoofed PRNs. The parameter is put to test for different test datasets as well considering jamming and multipath conditions (on the left and right respectively) in Figure 7. A threshold considering either the direct value or its change with respect to time between different PRNs is to be presented as future work. Considerations will have to be made for utlizing a wider range of Android devices as well as interference power levels.

There are further metrics to be explored as well which will be presented in future works. For example, GNSS signal authenticity verification technique using carrier phase double differences as presented in [23] was considered but due to poor quality of results and limitation to experiment datasets, it could not be presented in this paper.

C. Spoofing Attacks in a Cooperative Positioning Framework

1) Meaconing attack in multi-agent vehicular scenario: Spoofing Attacks in a CP Framework are referred to the spoofing scenario of Figures 1b and 1c discussed in Section II-B. This test is presented to highlight the potential effects of a meaconing attack and to propose potential countermeasures against this novel threats to positioning and navigation for next-gen networked receivers. A realistic simulation over a Bernoullian trajectory was performed through a MATLAB Software receiver named NavSAS SWRx on top of IFEN-generated signals. We can see that cooperative positioning of the meaconed solution, in Figure 8b is remarkably altered w.r.t. the GNSS standalone estimation, in Figure 8a. It is worth noticing that the trajectory shape is roughly preserved when measurements are faked and additional measurements from exteroceptive or proprioceptive sensors are required to inform the user that a different trajectory is followed. By comparing GNSS standalone and cooperative solutions, the receiver of agent **A** can detect an anomaly in the navigation solution because the the collaborative PVT diverges w.r.t. to the GNSS standalone estimation, still preserving a considerable precision. The navigation system cannot trust the cooperative submodules and it can inhibit the use of auxiliary measurements.

In order to design robust CP algorithm using ranging measurements the target **T** (or the server, if a client-server architecture is considered) has first to assess the consistency of reference position and pseudorange measurements to exclude the contribution of Agent T (which is faked by S) and inhibit the **A**-**T** cooperation which could limit the reliability of the solution.

2) Attack and detection through collaborative measurements combination: An advanced detection method can be designed by looking through the processing chain of the collaborative measurements to look at the effect of combining a set of locally-estimated pseudorange with a set of "spoofed" measurements retrieved from a further receiver. In this case only inter-agent distances between the two receivers are computed by relying on their pseudorange measurements, thus the effects of attack

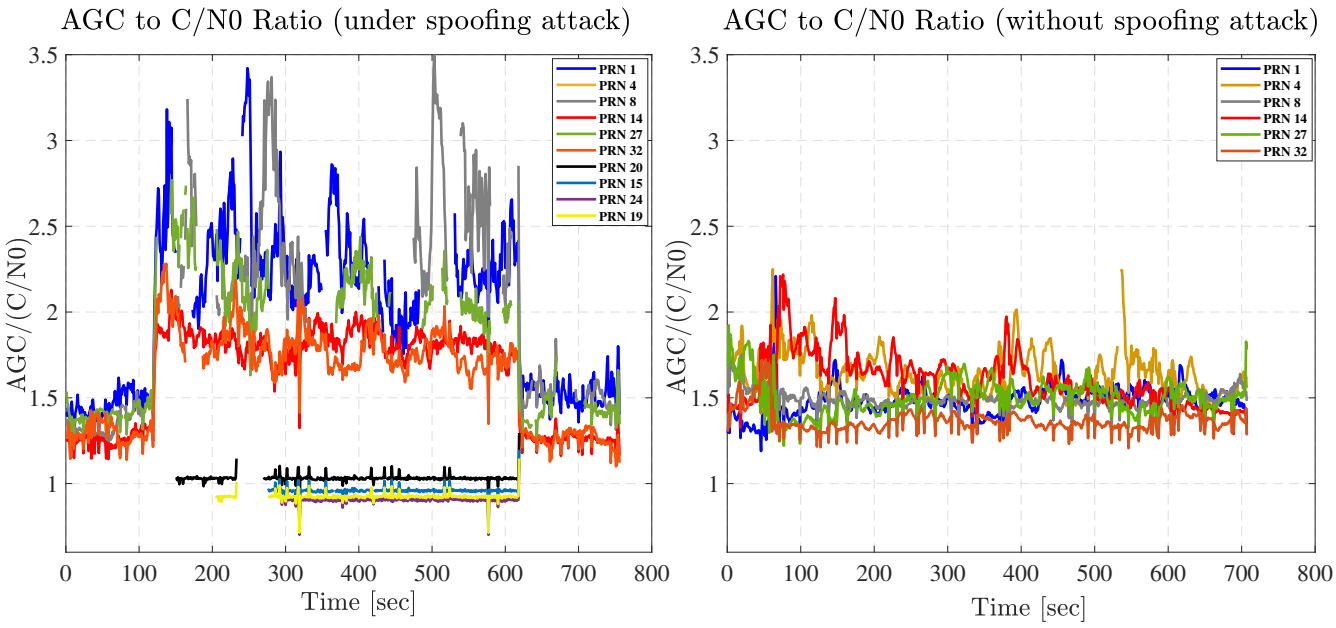


Fig. 6: AGC to C/N_0 ratio values with (left) and without (right) spoofing during the test.

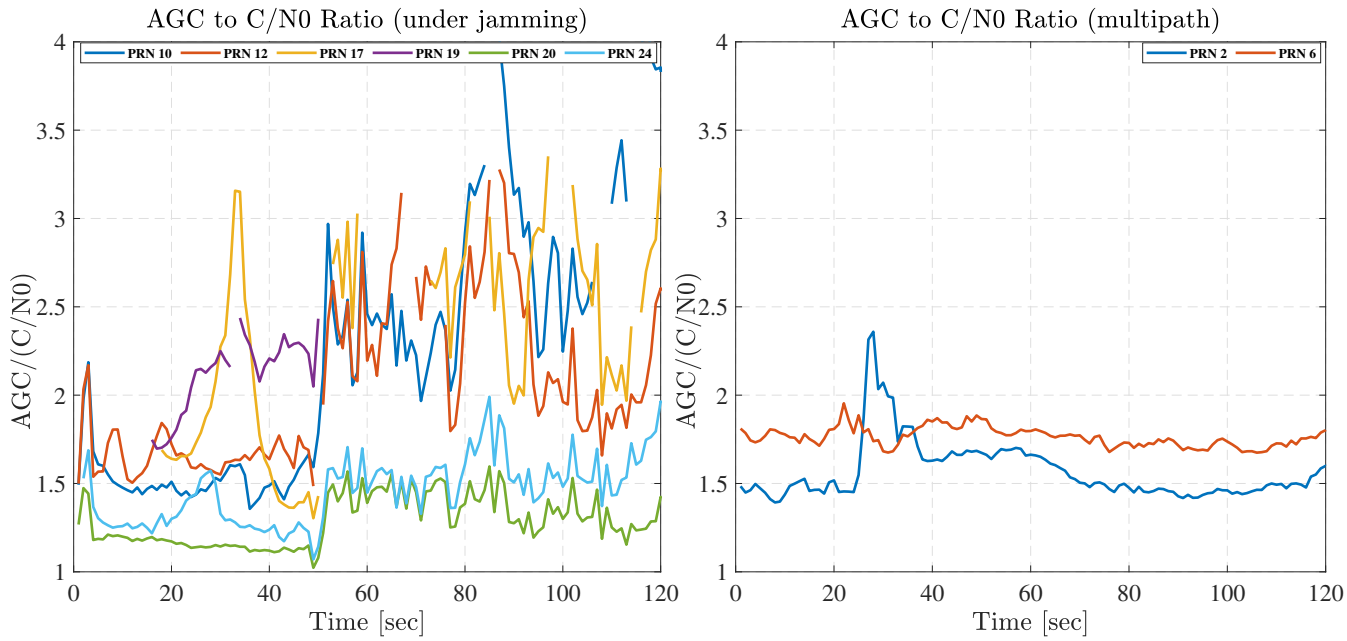
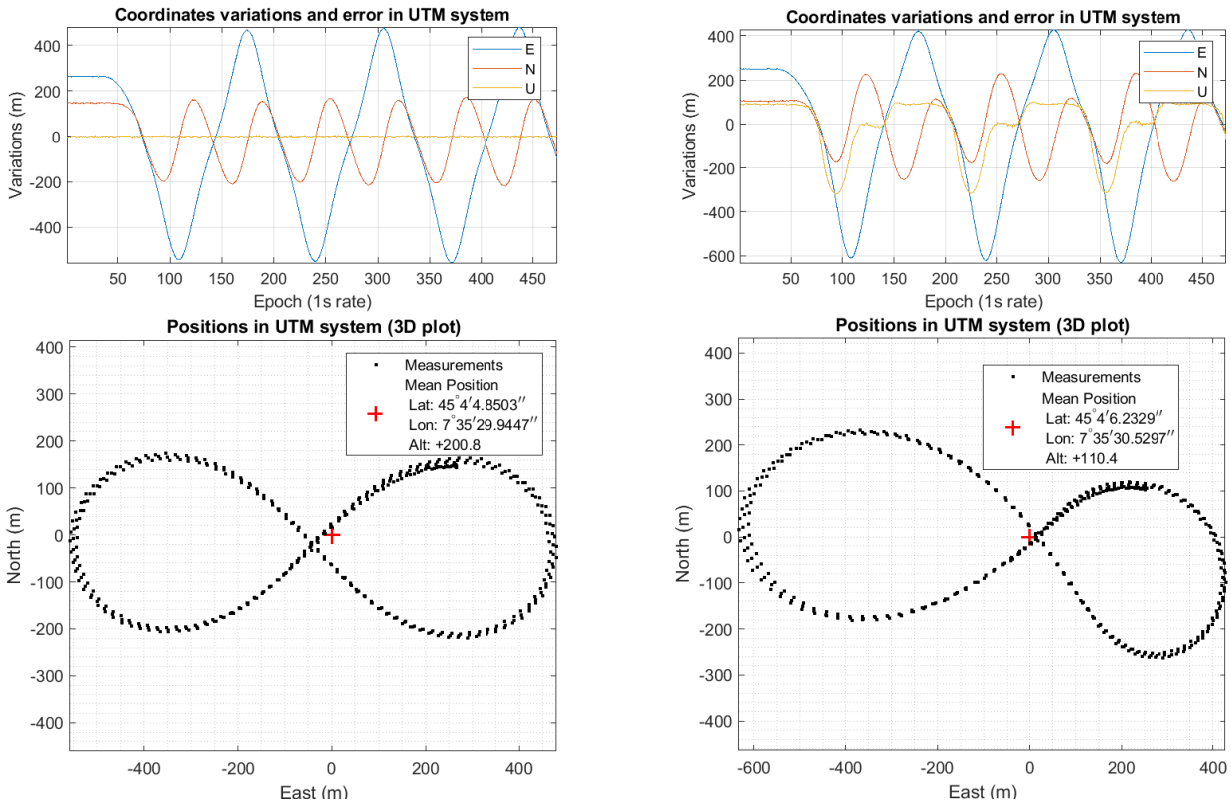


Fig. 7: Effect of different RFIs: a) jamming effect (left) and b) multipath (right) in Android smartphones.

on the positioning solution are not discussed. It is worth stressing that in the current CP framework, receivers cooperate at measurements level, Therefore, there is no control on earlier signal processing stages. $\mathcal{N}$ is the set of cardinality N including the satellites being simulated by the IFEN NavX RFCS to be acquired, tracked and exploited for the PVT of all the receivers. $\mathcal{S}$ is instead the set of cardinality S including faked measurements provided by the agent **S** to replace the measurements of agent **A**.

The test was conducted according to the following steps:

- A set of receivers locally retrieves a set of $N = 10$ pseudoranges and Doppler independently, in nominal conditions.
- Receiver **A** got $N - S$ nominal pseudorange and Doppler measurements and S "spoofed" measurements (injected by an agent which is moving hundred meter ahead on the same path).
- A set of receivers **T** uses the full measurements set provided by **A** to build inter-agent distances via WLS-DD.



(a) (b)

Fig. 8: Nominal cooperative PVT estimation 8a and the distortion effect of a *promiscuous cyber-attack* performed by inducing the overwriting the measurements of a generic aiding agent A, 8b

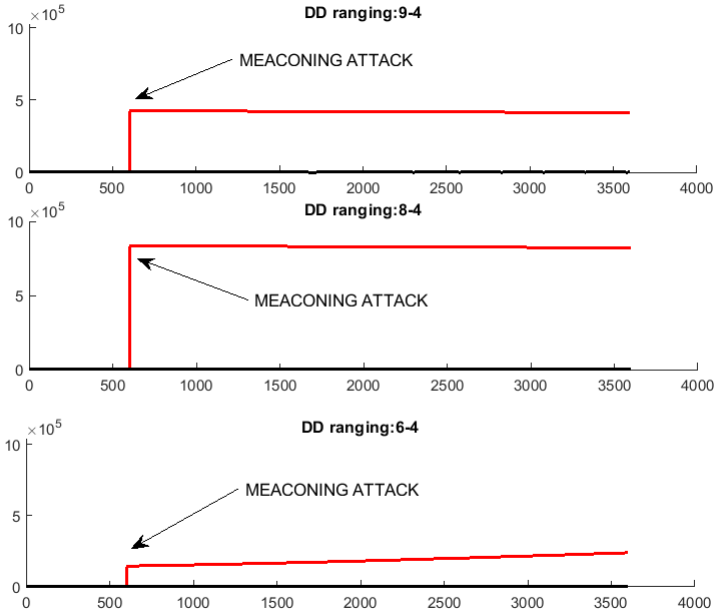


Fig. 9: Meaconing detection By raw measurements

Three different combinations of possible attacks can be identified according to the cardinality of the satellite sets:

- a) $S \subseteq N$, and only agent $\mathbf{A}$ is under attack. All the other agents interacting with $\mathbf{A}$ are expected to be indirectly affected.
- b) $S \subset N$ and also measurements of receivers $\mathbf{A}$ are spoofed such that $S_A \cup S_B = S_A$.
- c) $S \subset N$ and also measurements of receivers $\mathbf{T}$ are spoofed $S_A \cap S_B = \emptyset$ (different subsets of satellites).

In the case a, the attack is performed against a single receiver, while in b and c, the attack aims at damaging the whole cooperative network by acting on "cooperating pairs". A full-set attack (all the visible satellites are actually spoofed) was covered in the previous section. The aforemention list is provided for the sake of completeness and the following results are referred to the preliminary investigation of mode a. Considering a scenario including kinematic car platooning composed of 9 vehicles moving on a round trajectory, a discontinuity in the range measurement is shown for all the agents collaborating with agent $\mathbf{A}$. In Figure 9 a relevant discontinuity in the computation of the inter-agent distance via DD is shown under a spoofing attack starting after a given amount of epochs using $S = 7$ such that the amount of visible satellites is high enough to find a non-empty set of common satellites to solve for DD). In this case, spoofing lasts up to the end of the simulation. Such a discontinuity is quite easy to be detected through any threshold-based edge-detection algorithms [24]. The identification of the most effective technique to identify the discontinuity is out of the scope of this paper and it will be addressed in future contributions. A further test was performed by limiting the meaconing attack to 400 epochs, by approaching an ON/OFF attack to check whether anomalies in the measurements can be properly detected through differential measurements. In Figure 10b and Figure 10a two independent examples are provided. In the first case, agent 4 (agent $\mathbf{A}$) was meaconed by agent 5 (through the transmission of its own GNSS measurements) and this induced a sever discontinuity in the range measurements computed by agent 6 (agent $\mathbf{T}$). Similarly the computation of the inter-agent distance is altered in the pair 4-9. All the agents collaborating with agent 4 showed similar discontinuity.

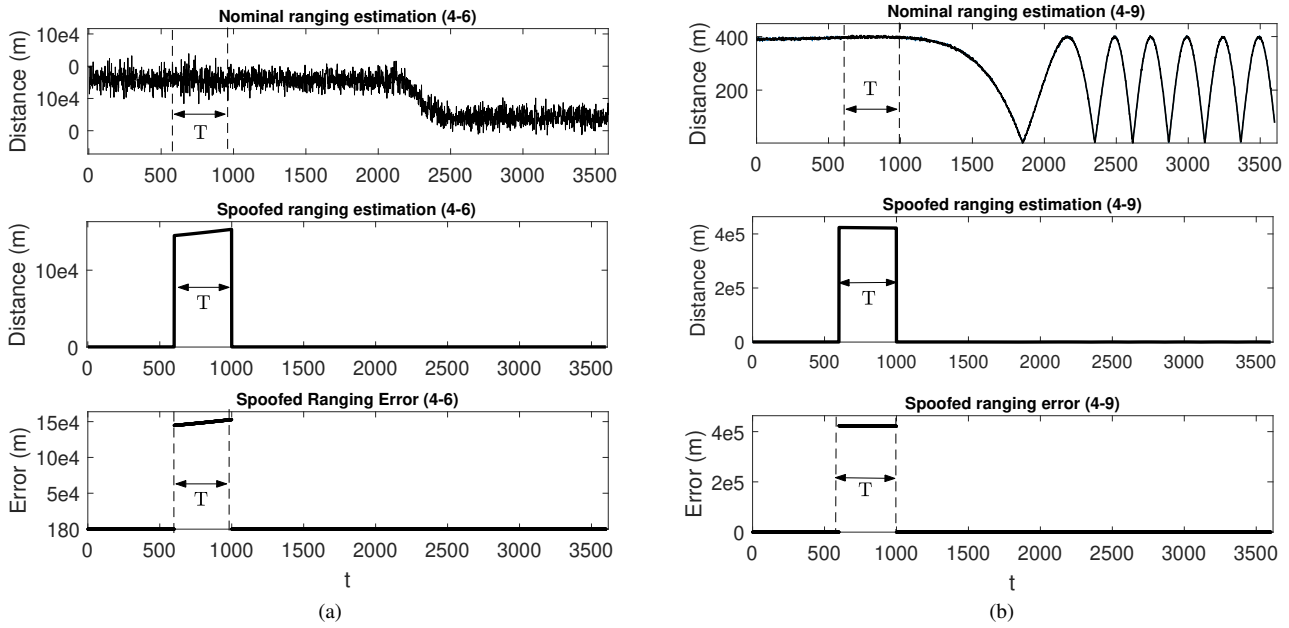


Fig. 10: Time-limited meaconing attack to a cooperative network: effects of measurements inconsistency on the differential ranging. The upper plots show the behaviour expected in nominal conditions.

These findings provide an indirect strategy to detect measurement anomalies in a network of cooperating agents. Collaborating agents can rise alarms in the network to identify possible outliers due to malicious attacks. Potentials countermeasures to such a kind of cyber-attacks are strategical to make CP frameworks more reliable and robust.

A set of further points must be considered as guidelines for future works:

- The observed behaviour in the DGNSS-CP framework is not related to a an actual RF spoofing, it discloses indeed potential weaknesses to the cooperative frameworks relying on the exchange of raw GNSS measurements.
- The measure of the divergency in the nominal and affected positioning solutions must be provided to properly rise a potential flag when dangerous values are observed.
- A check of the consistency of the measurements and reference position of the aiding agent, agent A has to perform a PVT using the retrieved measurements when attack detection is implemented at PVT level. Alternatively, a strategy can be performed at measurements level at which the PVT of the aiding agent is not necessary.

V. Conclusion

In this paper, we perform a set of experimental tests and presents the analysis towards devising an anti spoofing strategy in connected GNSS devices. One part of the work is related to a classical spoofing approach (simplistic RF attack) and its effects on the raw GNSS observables. With two synchronized devices in a cooperative framework, possible metrics are highlighted to identify a spoofing attack to one of the device by observing anomalies in them. The other part addresses the simulated meaconing of an already developed collaborative positioning framework based on the exchange of raw GNSS measurements through the network. The different approaches of an attack to the framework are laid down and the anomalies to be considered to detect an attack in a network of cooperating devices are presented.

This paper represents a part of a larger goal to develop an anti-spoofing detection and coping mechanism in connected COTS GNSS devices. With restrictions to perform further experiments due to the COVID-19 emergency, the analysis part of the goal is presented. Therefore future work would include developing the mechanism and putting it to test under different spoofing approaches.

References

[1] M. J. Dunn, "The navstar GPS space segment/user segment L5 interfaces," *Global Positioning Systems Directorate (24 September 2013).* [Online]. Available: http://www. gps. gov/technical/icwg/IS-GPS-705D. pdf

[2] European Commission, "European GNSS (Galileo) Open Service Signal In Space Interface Control Document," OS SIS ICD, Issue 1.1. September 2010.

[3] Coordination Scientific Information Center, "Global Navigation Satellite System GLONASS Interface Control Document (ICD)," 2002.

[4] K. Linux, "Penetration testing and ethical hacking linux distribution," 2018, accessed: 2020-02-10.

[5] F. Dovis, *GNSS interference threats and countermeasures*. Artech House, 2015.

[6] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, P. Kintner, and Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the Proceedings of the ION GNSS International Techniqueal Meeting of the Satellite Division, Savannah, GA, USA)*, 01 16–19 September 2008, pp. 2314–2325.

[7] W. Sterling and J. Roger, "A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing," *The Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[8] J. Bhatti and T. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," vol. 64, 03 2017, pp. 51–66.

[9] GSA. GSA GNSS market report issue 6. Accessed: 2020-02-10. [Online]. Available: https://www.gsa.europa.eu/market/market-report

[10] "Software-defined GPS signal simulator," accessed: 2020-02-10. [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[11] "MIT Licence," accessed: 2020-02-10. [Online]. Available: https://opensource.org/licenses/mit-license.php

[12] N. Gogoi, A. Minetto, and F. Dovis, "On the cooperative ranging between android smartphones sharing raw gnss measurements," *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pp. 1–5, September 2019.

[13] B. Wang, X. Liu, B. Yu, R. Jia, and X. Gan, "Pedestrian dead reckoning based on motion mode recognition using a smartphone," *Sensors*, vol. 18, p. 1811, June 2018.

[14] D. Yang, F. Zhao, K. Liu, H. Lim, E. Frazzoli, and D. Rus, "A GPS pseudorange based cooperative vehicular distance measurement technique," 07 2012.

[15] A. Minetto and F. Dovis, "On the information carried by correlated collaborative ranging measurements for hybrid positioning," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2019.

[16] A. Minetto, G. Falco, and F. Dovis, "On the trade-off between computational complexity and collaborative GNSS hybridization," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Sep. 2019, pp. 1–5.

[17] A. Minetto, A. Nardin, and F. Dovis, "Tight integration of GNSS measurements and GNSS-based collaborative virtual ranging," in *31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, September 2018, pp. 2399–2413.

[18] A. Minetto, A. Nardin, and F. Dovis, "GNSS-only collaborative positioning among connected vehicles," in *Proceedings of the 1st ACM MobiHoc Workshop on Technologies, models, and Protocols for Cooperative Connected Cars*, ser. TOP-Cars '19. New York, NY, USA: ACM, 2019, pp. 37–42.

[19] A. Rustamov, N. Gogoi, A. Minetto, and F. Dovis, "Assessment of the vulnerability to spoofing attacks of gnss receivers integrated in consumer devices," in *2020 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2020, pp. 1–6.

[20] J. Gross and T. Humphreys, "Gnss spoofing, jamming, and multipath interference classification using a maximum-likelihood multi-tap multipath estimator," 03 2017, pp. 662–670.

[21] E. Manfredini, D. Akos, Y.-H. Chen, S. Lo, T. Walter, and P. Enge, "Effective gps spoofing detection utilizing metrics from commercial receivers," 02 2018, pp. 672–689.

[22] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, "Automatic gain control (agc) as an interference assessment tool," 2003.

[23] A. J. Jahromi, A. Broumandan, and G. Lachapelle, "Gnss signal authenticity verification using carrier phase measurements with multiple receivers," in *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE, 2016, pp. 1–11.

[24] N. Linty, A. Minetto, F. Dovis, and L. Spogli, "Effects of phase scintillation on the gnss positioning error during the september 2017 storm at svalbard," *Space Weather*, vol. 16, no. 9, pp. 1317–1329, 2018.