POLITECNICO DI TORINO
Repository ISTITUZIONALE

Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices

Original
Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices / Rustamov, A., Gogoi, N., Minetto, A., Dovis, F.. - ELETTRONICO. - (2020). (2020 International Conference on Localization and GNSS (ICL-GNSS) Tampere, Finland, Finland 2-4 June 2020) [10.1109/ICL-GNSS49876.2020.9115489].

Availability:
This version is available at: 11583/2839032 since: 2020-07-08T17:57:09Z

Publisher:
Institute of Electrical and Electronics Engineers

Published
DOI:10.1109/ICL-GNSS49876.2020.9115489

Terms of use:

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

Publisher copyright
IEEE postprint/Author's Accepted Manuscript

©2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

19 November 2026

Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices

Akmal Rustamov*†, Neil Gogoi*, Alex Minetto*, Fabio Dovis* *Department of Electronics and Telecommunications, Politecnico di Torino, Turin, Italy †Turin Polytechnic University in Tashkent, Tashkent, Uzbekistan

***Abstract*—In this paper, we investigate the effects of spoofing attacks on the mass-market positioning and navigation units integrated in modern day Android™ smartphones. In order to operate spoofing in a real environment, we designed and implemented a portable, configurable, low-cost GPS spoofer exploiting a software-defined radio (SDR) implementation and a low-cost front-end. Such a tool has been exploited to set up a test campaign trying to mislead the Position, Velocity and Time computation of different Android™ smartphones. The effects of such simplistic spoofing attack on the smartphone GNSS has been assessed observing raw measurements and the evaluated positions and time. The main findings of this work showed that modern Android™ devices have a remarkable resilience to simplistic spoofing attacks, highlighting in parallel further potential weaknesses to be protected by means of practical defence mechanisms and countermeasures to spoofing.**

***Index Terms*—Global navigation satellite system, Global Positioning System, Smart devices, Radiofrequency interference**

I. Introduction

With the use of Global Navigation Satellite Systems (GNSS) in many applications and services, a constantly growing attention is being devoted to the security and safety of the technologies needed to process navigation signals and estimate the positions. Current GNSS signals used for mass-market applications (e.g. GPS L1 C/A, E1 Galileo and GLONASS) do not provide any means to ensure the authenticity of the transmitting source or to protect the receiver against possible spoofing attacks [1], [2], [3]. Galileo is planning the use of the Open Service Navigation Message Authentication Signal (OSNMA) and the Commercial Authentication Service (CAS), with the aim of allowing users to calculate Position, Time and Velocity (PVT) solution based on trusted signals. Nevertheless, currently, GNSS receivers are vulnerable to intentional interference and this opens opportunities for attackers who want to impair or mislead them [4]. This constitutes a threat to many applications based on GNSS receivers, thus, making them vulnerable and in some cases can also have a cascading effect onto interconnected systems and critical infrastructures. From a general perspective, the GNSS receiver plays a core role providing the only absolute estimation of the position in most positioning units. Such units may also include several exteroceptive and proprioceptive sensors like Inertial Measurement Units (IMUs), Barometers, Ultra-Wide Band (UWB) ranging and proximity sensors, etc. aiding or refining the positioning solution. In the general scheme of a positioning unit which is typically interfaced to an application layer, the position information is exchanged to other services or stored in remote databases. Such an architecture is prone to a wide range of spoofing attacks, especially if it is based on products which are low-cost, Commercially available and Off-The-Shelf (COTS). These use the aforementioned satellite-based positioning services and standard unencrypted communication services. As a consequence, it is worth examining the potential effects of intentional interference on the low-cost GNSS units embedded in mass market receivers as well as assessing the resilience of the receiver itself. Many studies are available on defence against civil GNSS spoofing attacks. In [5], Unicorn Team showed the spoofing technology using MATLAB® to Record GPS signal by a USRP™ B210 and Replay the signal by a SDR BladeRF™ to spoof PVT of a smartphone. The team presented the vulnerability of smartphones even if the trial regarded a limited number of devices. In addition, work developed in [6] showed how easy it is to spoof the navigation solution in the phone using software radios and additional equipment. A study of spoofing in road navigation, developed in [7], presents a spoofing attack under practical constraints with a fake road map. In [8], a technique based on monitoring the correlation peaks of the Carrier-to-Noise density ratio (C/N_0) is suggested in order to reduce the effect of the threats. In [9], the authors proposed a detection method based on low-cost Inertial Measurements Units (IMUs) for spoofing detection. In the spoofing scenario, the coherence between IMU and GNSS measurements is evaluated using acceleration and rotation rate vectors. In [10], mitigation countermeasures at hardware level are proposed, such as multi-antenna receivers [11], [12]. Similarly, in [13], [14], the impact of spoofing attacks on mobile phones is analysed and specific techniques are suggested to enhance security such as the use of cheap acceleration sensors. In [15], inertial navigation sensors such as magnetometer, accelerometer, and barometer are used for triggering possible spoofing events in smartphones. Several countermeasures are still at research stages and most low-cost commercial devices are yet to implement even basic detection mechanisms [16]. Despite the proposed solutions, there is as yet no fully proven defence against GNSS spoofing and no extensive investigation carried out on Android™ domain. Smartphones account for almost 80% of the global installed base of GNSS devices [17] and in 2020 the number of smartphone users is forecast to reach almost 3.5 billion [18]. In light of this, a comparative analysis of the resilience of Android™ domain to intentional disturbances is performed in this paper. The experimental work presented hereafter provides one of the

first investigations on the use of a portable spoofer to threaten Android™ smartphones. The portable low-cost spoofer has been developed, based on open source signal generator and low-cost electronics and radio-frequency equipment and then used to carry out spoofing attacks on different Android™ smartphones. The rest of the paper is organised as follows: In Section II, background of a spoofing attack, spoofing techniques and the state of vulnerability of receivers are explained. Section III provides a methodology of 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. Background

A. Spoofing attacks

Spoofing methodologies are typically classified on the basis of the difficulty in inducing the attack and on the possibility to detect it from a receiver point of view. Compared to a jamming disturbance to a GNSS receiver, which could significantly impair the receiver at a signal processing stage, thus, allowing easy detection, a spoofing disturbance challenges potential detection as the receiver operation is not interrupted. Depending on the features of the spoofing and the complexity of the attack, it is possible to classify these disturbances into three categories: simplistic, intermediate and sophisticated [19], [20].

a) Simplistic spoofing: It is characterised as a transmission of locally generated RF signals forcing receivers to compute a fake PVT solution. A lack of synchronisation between spoofers and GNSS timescale can be often used to detect occurring attacks. This type of spoofer can be also built by using a signal simulator which re-transmit fake signal or SDR low-cost components.

b) Intermediate spoofing: the spoofer has a built-in receiver that collects and tracks the satellite signal parameters in order to generate a new signal that is consistent with real GNSS signals. It receives real time GNSS signals, changes the signal properties based on its need and transmits GNSS signals synchronised with real GNSS time to the targeted victim receiver. An intermediate spoofing hardware might have GNSS receiver integrated with front-end or conventionally designed for spoofing purposes. A drawback of Intermediate spoofing attack, is that it require certain target information which is difficult to implement. For successfully misleading the target, different factors must be theoretically evaluated and combine with experimental verification. Some implementations of intermediate spoofing scenario is made of civilian GPS with modified software defined receiver integrated with front-end [4].

c) Sophisticated spoofing: also referred to as 'nulling' transmits a destructive interference signal along with fake spoofed signals. Sophisticated spoofing is the most dangerous because it takes control of the target receiver without being detected. As described in [21], the attack principle is soft-take-over or time-synchronised transmission. It starts with a low level of power which is increased slowly till the receiver has acquired and started to track the spoofed signals. In [22], research conducted sophisticated spoofing scenarios in a multi-layered processing architecture. However, this type of spoofing uses multiple antennas to broadcast GNSS signals to overcome standard anti-spoofing techniques. Thus, it is rarely used due to its high cost and complexity.

B. Spoofing attacks to integrated GNSS receivers in smartphones

Some demonstrations of spoofing against Google Android™ OS are presented in [23] with realistic spoofing and fake Google Maps™ integration. This work demonstrated that spoofing might impact the device's navigation unit affecting in turn a popular Location Based Service (LBS). Since the version 7 onwards of Android™ OS gives access to raw GNSS measurements, it can be exploited to study and detect the effect of spoofed signals in applicable smartphones. The raw GNSS measurements may include internal clock measurements like the time of signal reception, clock drift, clock discontinuities, etc. and the GNSS receiver measurements such as received GNSS satellite time, Doppler frequency, carrier phase measurements, constellation status, navigation messages, etc. [24] . More recently, the Google Service Framework™ also provides Automatic Gain Control (AGC) measurements in its Android™ location modules with the release of Android™ Android Application Program Interface (API) 9.0. However, not all the GNSS chipsets or software of the different Android™ devices are compatible with such measurements and the quality of the raw GNSS measurements vary between device to device [25], [26].

III. Methodology

A. A low-cost, portable spoofer

In our experiment we used a low-cost spoofer based on a Great Scott Gadgets™ HackRF One™ platform and a Raspberry™ PI 4B. The 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 [27], an open GPS L1 C/A signal generator toolbox distributed with a MIT licence [28]. A scheme of the device is provided in Figure 1.

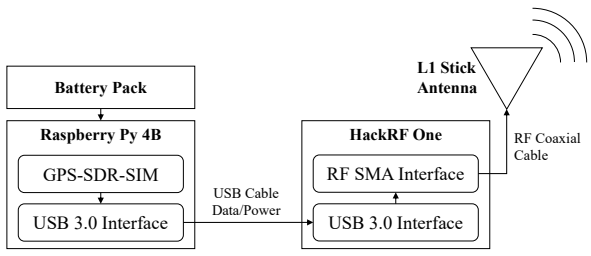


Fig. 1. High-level schematic of the low-cost portable spoofer.

The attack was planned simulating a static position and all the visible satellites belonging to GNSS constellations and their

TABLE I
DEVICES UNDER TEST.

ID	Model	System on cheap (SOC)	GNSS chipset
S1	S 8	Qualcomm Exynos 8890	BCM 4774
S2	MI 8	Qualcomm Snapdragon 845	BCM 47755
S3	MI 8 PRO	Qualcomm Snapdragon 845	BCM 47755

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 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 Py4.
2) *Numerical signal generation*. The trajectory is then injected to the GPS-SDR-SIM. The software generates a file with In-phase/Quadrature (I/Q) samples of the baseband signal complex envelope that is ready to be injected to the SDR front-end (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), thus, offering quadrature modulation in L1 band.

B. Test devices

Following the direction of testing the chosen simplistic portable spoofing methodology on consumer GNSS devices, three different commercial smartphones were chosen among those equipped with Google Android™ 8 Operating System (OS). These are detailed in Table I and are referred to as S1, S2 and S3 respectively in the following analysis. In order to identify and procure GNSS raw measurements, the GNSS Logger Android application provided by Google™ was installed in the android devices. The devices PVT solutions were logged through the Android application NMEA tools, which provides the GNSS raw position of the smartphone in standard NMEA format. Figure 2 shows the set-up of different Android™ devices and the transmitting antenna of the developed spoofer. Additionally, a commercial GNSS receiver was also used as a benchmark for data collection and PVT estimation.

The raw GNSS measurements of the smartphones were processed on the MATLAB®® GPS measurement-tools software[1]

[1]Apache Licence 2.0 (http://www.apache.org/licenses/LICENSE-2.0)



Fig. 2. Experimental setup consisting of a HackRF One, (1) equipped with an L1 stick antenna, (2), a Raspberry PI 4B, (3) a u-blox™ Neo-M8N GNSS, (4) with an active GNSS antenna, (5) and a set of smartphones, (6) listed in Table I.

[29]. For the purpose of this paper, the following raw measurements are mainly analysed to test the effects of spoofing:
a) Carrier-to-Noise Density Ratio (C/N_0): : It is a basic indicator of received satellite signal quality. Abrupt variations to it can indicate the presence of interference while an unnaturally high value could also indicate presence of a fake satellite signal.
b) Automatic Gain Control (AGC): : The AGC implementation in a smartphone acts as a variable gain amplifier adjusting the power of the incoming signal. Changes in the value are typically indicative of power fluctuations of the input signal in the frequency band foreseen this measurement [24]. AGC is extremely useful in detecting spoofing attacks and has been used in the past to detect defective signals [30].
c) Time of Signal Transmission and Reception: : The GPS Time of signal Transmission, t_{TX}, is demodulated from the received signal and used to compute the pseudorange from the particular satellite along with The Time of signal Reception, t_{RX}, which is taken either from the cellular or Wi-Fi network in the smartphone. A remarkable difference in the two timestamps could indicate an altered t_{TX} data coming from a spoofed signal or a faulty satellite. Generally, it is in the range of $60 - 100$ ms.

C. Spoofing scenario

A 15-minutes spoofing scenario was tested in a controlled outdoor environment with open sky conditions. By acting on the HackRF One transmitting power, the range of the spoofer antenna was kept to within 1-3 m to not provide any disturbance beyond the range of the controlled environ-

TABLE II
SATELLITE SUBSETS

Subset	SV ID Number
Real	24,25,28,19,17,15,13,12
Fake	8,16,27
Common	10,20,32

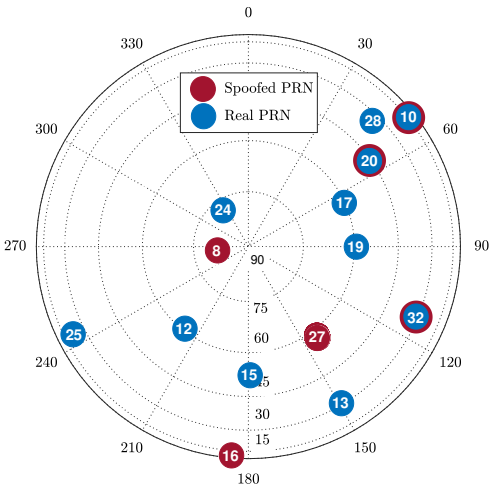


Fig. 3. Sky-plot showing real and spoofed satellite signals.

ment. The smartphones were positioned at a location with coordinates 45.064406 N, 7.661922 E (Turin, Italy) starting UTC time of February 11, 2020, 14.21.41 and for the first 5 minutes, they received live GNSS signals without any other interference. Then the portable spoofer was switched on, broadcasting spoofing signals over GPS L1 band with coordinates 45.470111 N, 9.179874 E (Milan, Italy) and UTC time February 10, 2020, 12.00.00 which was 144 km away from the test location. The spoofing signals were broadcasted for 5 minutes after which the spoofer was switched off. For the remaining duration, the smartphones received only live GNSS signals. The u-blox™ Neo-M8N GNSS receiver was used for cross validation of the test measurements. 14 GPS satellites were considered in the overall scenario. As seen in Table II, the satellites could be divided into three different subsets. The first subset (Real) consists of the real in-view Satellite Vehicle Identifiers (SV IDs) which were received by each device and not part of the satellites transmitted by the spoofer. The second subset (Fake) consists of the SV IDs which were transmitted by the spoofer and visible to all the smartphones, but their real counterparts were not in view during the test period [8, 16, 27]. The third subset (Common) consists of the overlapping Satellite Vehicle (SV) IDs which were both in-view real time and transmitted by the spoofer as well [10, 20, 32]. The overall satellite skyplot during the test is shown in Figure 3.

IV. RESULTS AND ANALYSIS

This section is roughly divided based on the effect of the spoofing described in Section III-C on GPS L1 GNSS raw measurements of the three different subset of satellites. The data analysed is from smartphone S3 but similar results were also achieved with S2. GNSS raw measurement could not be retrieved from S1 after the spoofer was turned on. The effect on position computation of the smartphone as retrieved from the Android location API was also analyzed, as reported in the following. The u-blox™ Neo-M8N receiver position shifted to the coordinates provided by the spoofer within 1 minute from the start of the spoofing action, thus, validating the effectiveness of the attack.

A. Effect on Real satellites

Figure 4 compares the C/N_0 and pseudoranges of two real SV IDs during the entire test period with SV ID 24 and 25 being at high and low elevations respectively. Naturally this will affect their signal strength and pseudorange distance as seen in the Figure 3. It is clear that the spoofer acts as a source of interference over the L1 frequency band disturbing the healthy satellites during the spoofing timespan and tracking of low elevation satellites being lost. This effect is seen for the L1 signals of constellations as well.

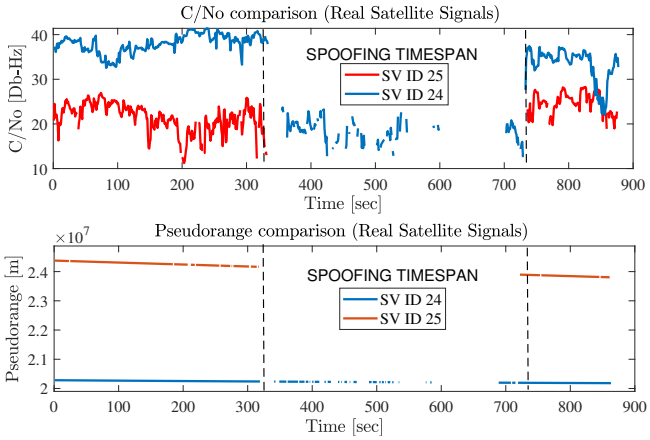


Fig. 4. Effect on real satellites (SV ID 24 and 25) during the test duration.

B. Fake and Real satellites comparison

Figure 5 plots the AGC dB values of the S3 GNSS receiver 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 C/N_0 of a fake (SV ID 16) and real signal (SV ID 24) in Figure 6. An important difference captured between the two satellite signals is the t_{TX}, whose values in a real signal was within the standard 100 ms of the t_{RX} throughout the test, while fake signals had t_{TX} and t_{RX} difference values over 10^5 seconds. This naturally gives a hugely and unrealistic pseudorange value for the fake satellite. Nevertheless, it has to be remarked that no effect is experienced on the time provided, since the connected device is kept synchronised to the communication network infrastructure (cellular or Wi-FI).

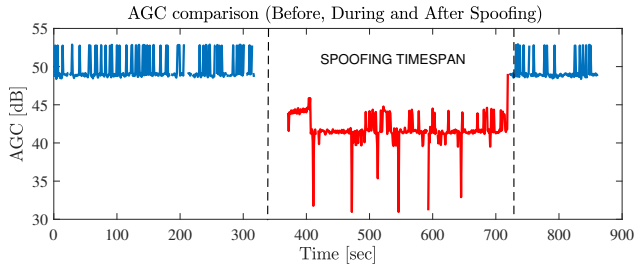


Fig. 5. Effect of Spoofing on AGC.

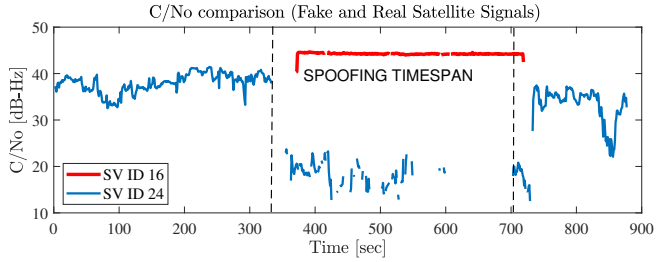


Fig. 6. Comparison of Fake (SV ID 16) and Real (SV ID 24) satellite's C/N_0 .

C. Effect on Common satellites

Figure 7 plots the effect of spoofing on the C/N_0, Pseudorange and Carrier phase measurements of a Common satellite (SV ID 10) present among the live satellites and in the set of spoofed signals. It can be seen that the receiver does not acquire the fake satellite signal with the same SV ID during the spoofing timespan and only looses acquisition of the real signal. It reacquires the real satellite after spoofing stops as also seen by the carrier phase measurement.

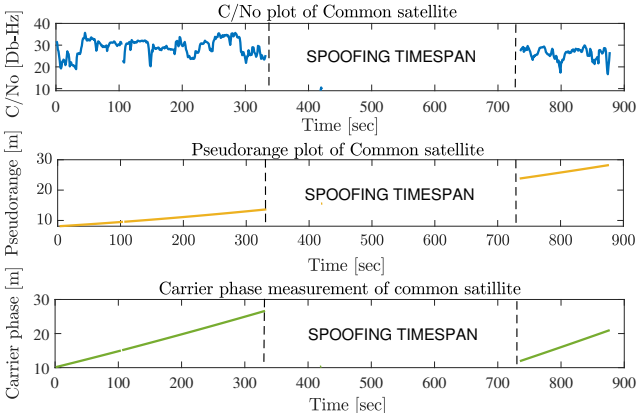


Fig. 7. Common Satellite (SV ID 10) analysis.

D. Effect on smartphone GNSS position estimation.

Figure 8 shows the error in position of the ECEF coordinates of the three different smartphones during the test. The spoofing time span is delayed compared to the previous plots as NMEA Tools app was initialised before GNSS Logger app. It can be seen that spoofing achieves only a few metres of deviation in the position output of the GNSS receiver which can be attributed to the loss of some satellites due to interference. 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 interesting to notice that S1 carries the Broadcom™ BCM 4774 chipset without dual frequency GNSS capabilities and it is affected the most, comparatively.

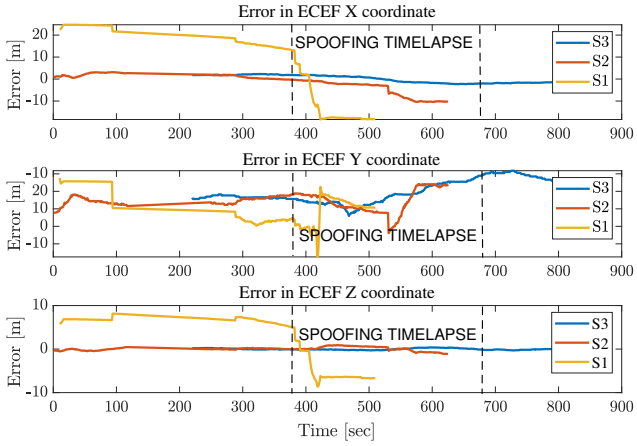


Fig. 8. Effect on Smartphone GNSS Position.

V. Conclusion and Further Research

In this work, a portable GPS L1 spoofer was implemented and a spoofing strategy was proposed for the calculation of intentionally misleading PVT solution on a GNSS receiver. Comparative analysis is addressed on the performance of modern commercial smartphones and it is comprehensively seen that a simplistic spoofing attack is not fully successful on such smartphones in open-sky conditions. Spoofer transmitted satellites though acquired, are not used by the smartphone GNSS receivers except in the case of overlapping satellites where they are not present in the set of already acquired signals. The spoofer acted more as an interference agent to the smartphones in the L1 band and their GNSS receiver clocks are not affected by it. The effect of a longer duration of spoofing than presented in this paper and multi-frequency (L1 and L5) spoofer implementation are to be seen. This suggests that a proper attack should implement as well an initial jamming phase before presenting the fake signals to the receiver for acquisition. An important follow up of this work is the development of an intermediate portable spoofer to gain success in spoofing modern day smartphones and then develop proper counter measures since such spoofers are already a reality today.

References

[1] European Space Agency (ESA), "Galileo open service, Signal-In-Space Interface Control Document (OS SIS ICD)," 2008.

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

[3] K. Linux, "Penetration testing and ethical hacking linux distribution," 2018.

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

[5] L. Huang and Q. Yang, "Low-cost GPS simulator GPS spoofing by SDR," in *Proceedings of DEFCON*, 2015.

[6] S. Lo, Y. H. Chen, T. Reid, A. Perkins, T. Walter, and P. Enge, "The benefit of low cost accelerometers for GNSS anti-spoofing," in *Proceedings of the ION 2017 Pacific PNT Meeting*, 2017, pp. 775–796.

[7] K. Wang, S. Chen, and A. Pan, "Time and position spoofing with open source projects," *black hat Europe*, vol. 148, 2015.

[8] J. Nielsen, V. Dehghanian, and G. Lachapelle, "Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[9] J. T. Curran and A. Broumendan, "On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications," in *Proceedings of ITSNT*, 2017.

[10] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A low-complexity GPS anti-spoofing method using a multi-antenna array," *a a*, vol. 2, p. 2, 2012.

[11] S. Han, L. Chen, W. Meng, and C. Li, "Improve the security of GNSS receivers through spoofing mitigation," *IEEE Access*, vol. 5, pp. 21 057–21 069, 2017.

[12] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium*, April 2012, pp. 479–487.

[13] D. Miralles, N. Levigne, D. M. Akos, J. Blanch, and S. Lo, "Android raw GNSS measurements as a new anti-spoofing and anti-jamming solution," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida*, 2018, pp. 334–344.

[14] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, and S. Tomasin, "Exploiting side-information for resilient GNSS positioning in mobile phones," in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. IEEE, 2018, pp. 1515–1524.

[15] D. M. S. L. D. A. Dong-Kyeong Lee, Matthias Petit, "Analysis of raw gnss measurements derived navigation solutions from mobile devices with inertial sensors," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida*, 2019, pp. 3812 – 3831.

[16] L. Dobryakova and E. Ochin, "On the application of GNSS signal repeater as a spoofer," *Zeszyty Naukowe/Akademia Morska w Szczecinie*, 2014.

[17] European GNSS Agency. GSA GNSS market report issue 5. [Online]. Available: https://www.gsa.europa.eu/market/market-report

[18] GSA. Gsa gnss market report issue 6. [Online]. Available: https://www.gsa.europa.eu/market/market-report

[19] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver," *Gps Solutions*, vol. 19, no. 3, pp. 475–487, 2015.

[20] J. R. v. d. Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*, 2018, pp. 91–99.

[21] C. Gunther, in *A Survey of Spoofing and Counter-Measures*. Navigation, 2014, pp. 159–177.

[22] J. N. A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," in *International Journal of Navigation and Observation, vol.2012*, 2012, pp. 1–16.

[23] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A practical GPS location spoofing attack in road navigation scenario," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, 2017, pp. 85–90.

[24] Google Developers. GNSSmeasurement. [Online]. Available: https://developer.android.com/reference/android/location/GnssMeasurement

[25] N. Gogoi, A. Minetto, N. Linty, and F. Dovis, "A controlled-environment quality assessment of android GNSS raw measurements," *Electronics*, vol. 8, no. 1, p. 5, Dec 2018. [Online]. Available: http://dx.doi.org/10.3390/electronics8010005

[26] G. Galluzzo, M. Navarro-Gallardo, and M. Sunkevic, "Using GNSS raw measurements on android devices-tutorial part i," 2017.

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

[28] "MIT licence," https://opensource.org/licenses/mit-license.php, accessed: 2020-02-10.

[29] "Google GNSS logger," https://github.com/google/gps-measurement-tools/, accessed: 2020-02-10.

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

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 is a 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.