Smartphone behaviour under sophisticated time synchronized and Record and Replay spoofing attacks and the Role of GNSS Raw Measurements

Ronny Blum, Himanshu Sharma, Thomas Pany

Institute of Space Technology and Space Applications, Universität der Bundeswehr München, Germany

BIOGRAPHIES

Ronny Blum received his M.Sc. in Physics from the University of Basel, Switzerland. After that he worked at Würth Elektronik in the field of signal transmission and later he joined the Forest Research Institute in Freiburg in Breisgau in the field of GNSS reception within the forest. In 2017, he joined the Universität der Bundeswehr München, where he is working in the field of GNSS software receiver with research topics in the field of spoofing, Signal Quality Monitoring and Galileo PRS.

Himanshu Sharma received his M.Sc. in Communications and Signal Processing from Technical University of Ilmenau, Thuringia, Germany. Since 2016, he has been working at the Universität der Bundeswehr München as a research associate. His research interest includes Precise Positioning in Mass Market GNSS Receiver.

Prof. Thomas Pany is with the Universität der Bundeswehr München at Space Systems Research Center (FZ-Space) where he leads the satellite navigation unit LRT 9.2 of the Institute of Space Technology and Space Applications (ISTA). He teaches navigation focusing on GNSS, sensors fusion and aerospace applications. Within LRT 9.2 a good dozen of full-time researchers investigate GNSS system and signal design, GNSS transceivers and high-integrity multi-sensor navigation (inertial, LiDAR) and is also developing a modular UAV-based GNSS test bed. ISTA also develops the MuSNAT GNSS software receiver and recently focuses on Smartphone positioning and GNSS/5G integration. He has a PhD from the Graz University of Technology and worked in the GNSS industry for seven years. He authored around 200 publications including one monography and received five best presentation awards from the US institute of navigation. Thomas Pany also organizes the Munich Satellite Navigation Summit.

ABSTRACT

With more than 70 percent of the world population being the Smartphone user and 77 percent of the smartphone users still rely on the Smartphone positioning for navigation [1], there is no doubt that the Smartphones are amongst the largest Global Navigation Satellite System (GNSS) receiver installed device in the GNSS market, 90 percent of the GNSS receivers in the price segment of less than 5 € are used for smartphones and wearables, which is set to be almost 1.8 billion Smartphones by 2029 [1]. With such a high share in the GNSS market, the threat of GNSS spoofing is no longer limited to the critical infrastructure only. Till date GNSS chip inside the smartphone is a black box providing positioning solution with no access to the baseband processing technique. But, with the availability of GNSS raw measurements through Android API [3], the researcher get access to wide range of measurements, which not only are important for the development of improved positioning algorithms but can also be vital for integrity check.

The vulnerability of smartphones to the spoofing attack and the usage of GNSS raw measurements to counter such attack has been presented in [4] [5]. But, with the availability of newer generation smartphone supporting dual frequency and multi-constellation, it is extremely important to analyze their behaviour under such attack. Considering a L1/L5 spoofing attack to be more complex to generate, the use of L1/L5 frequency for position determination can be a valid indicator against L1 only spoofing. Additionally, the change in pseudorange measurement can alarm against the spoofing detected for one particular constellation type. Other GNSS raw measurements like Automatic Gain Control (AGC), Doppler, Code Minus Carrier (CMC) or Carrier to Noise ratio (C/N_0) are also a good candidates to examine the influence of a spoofing attack. In addition to GNSS

measurements, we also recorded the Inertial Measurement Unit (IMU) data (accelerometer and gyroscope) and have analyzed their contribution as a spoofing indicator. The idea is to compare the acceleration recorded with the smartphone and compare them with the acceleration measured through spoofed GNSS positioning.

In this work we present the results of over the air smartphone spoofing experiments with a repeater in a shielded box. The experiment was conducted with the wide range of smartphones with different manufactures, Operating Systems and different GNSS chipsets to examine their behaviour under the attack. We tested the behaviour under two different types of spoofing, the Record and Replay attack and the more sophisticated approach of a time synchronized signal generator attack. Record and Replay is just the recording of a Global Navigation Satellite System (GNSS) file with a certain bandwidth and retransmitting the recorded file later on with a high power. Signal generator spoofing is the generation and emission of artificial authentic GNSS-signals with a signal generator, which tries to imitate the real satellite signals in terms of code phase, Doppler and navigation bit as good as possible to induce a wrong time and/or position output on the victim receiver. The artificial signals should have ideally a slightly higher amplitude at the target position than the authentic signals in order to get tracked from the receiver. We investigated synchronized attacks with a purchasable Jamming and Spoofing generator from [6], which is able to perform a synchronized spoofing attack to real satellite signals and by now Galileo E1B/C and GPS L1 C/A signals are generated from the spoofing device. Beside the position, some tracking parameters like the Doppler, CMC, C/N_0 and the AGC were analyzed, which changed when the spoofing attack started. These parameters were also analyzed for common receivers and proposed as anti-spoofing parameters in [7]. For the sophisticated attack, all smartphones could be spoofed, meaning the position could be shifted kilometres away from the starting position, which was also the case when the internet was set on in the smartphones. Some smartphones were also set to track L1 and L5 signals, but could still be spoofed, which was unexpected since the spoofing signal only included GPS L1 and Galileo E1 signals. The Record and Replay attack, which is relatively easy to perform and the equipment is also relatively cheap, lead in the most smartphones to a jamming behaviour, meaning that the authentic signals were just overpowered and the spoofing signals were not tracked. But still some could be spoofed as well. The analysis showed that even in the presence of A-GPS (Wi-Fi), it was possible to spoof the smartphone with malicious navigation message transmitted from the spoofer. This gives a firm reason for the need of navigation message authentication in smartphones and will be discussed in the paper. Also the fact that the spoofer did not need to include L5 signals for a successful spoofing, showed the severe vulnerability against spoofing.

Keywords: GNSS, smartphone spoofing, over the air, spoofing defense, anti-spoofing, signal generator attack

Bibliography

[1] Panko, R. "The Popularity of Google Maps: Trends in Navigation Apps in 2018," 2018. [Online]. Available: https://themanifest.com/mobile-apps/popularity-google-maps-trends-navigation-apps-2018.

[2] "GSA GNSS Market Report," GSA, 2019.

[3] GSA, *White Paper : Using GNSS Raw Measurements on Android Devices,* 2018.

[4] Miralles, D. , Levigne, N. , Akos, D.M. , Blanch, J. and Lo, S., "Android Raw GNSS Measurements as a New Anti-Spoofing and Anti-Jamming Solution," in *ION GNSS+*, 2018.

[5] Lo, S., Chen, Y. H., Akos, D., Cotts, B., Miralles, D., "Test of Crowdsourced Smartphones Measurements to Detect GNSS Spoofing and Other Disruptions," *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2019, pp. 373-388.

[6] IGASPIN GmbH, Graz, Austria, "Homepage IGASPIN GmbH," 2020. [Online]. Available: http://www.igaspin.at/products.html.

[7] Blum, R., Dütsch, N., Dampf, J. and Pany,T.(2021). Time synchronized signal generator GNSS spoofing attacks against COTS receivers in over the air tests. Proceedings of the 2021 International Technical Meeting of the Institute of Navigation, January 2021.