A Demonstration of Spoofing an Android Mobile Phone with Low-Cost Signal Generator

フレデルセス　エラリザ　　久保　信明
Ellarizza Fredeluces　　Nobuaki Kubo

東京海洋大学学術研究院
Tokyo University of Marine Science and Technology

1. Introduction

Spoofing is an interference where the receiver is fooled to track the fake signal coming from an external transmitter, usually on ground, instead of a true signal coming from GNSS satellites. Spoofing attacks are usually classified as simplistic, intermediate, and sophisticated spoofing. Simplistic spoofing is commonly implemented with signal simulator and front end to transmit the signals. Intermediate and sophisticated spoofing are more complex because it needs to synchronize with incoming GNSS signals. In this paper, we implemented simplistic spoofing of two Android mobile phones, Xiaomi POCO M3 and Google Pixel 7a, with LimeSDR USB and modified version of GPS-SDR-SIM of Professor Takuji Ebinuma. We demonstrated that it is possible to spoof modern Android devices with just low-cost and open-source signal generator.

2. Methodology

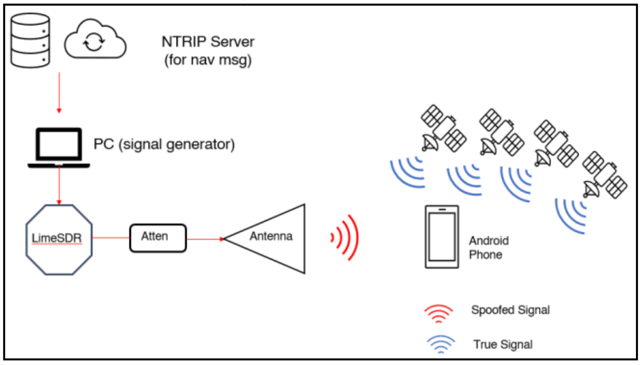

Figure 1. General Methodology

Figure 1 shows the general methodology. We prepared all the hardware components including LimeSDR USB as front end, attenuators, and transmitting antenna. The PC environment we used has 11th Gen. Intel i7 as CPU since generating and transmitting signals requires big CPU power. We downloaded orbit information from free NTRIP streams of rtk2go.com using STRSVR. The data is formatted in RTCM so we converted it to RINEX v3 by using RTKCONV. To generate the spoofed signals, we used a modified version of GPS-SDR-SIM for LimeSDR by Mr. Kaito Kobayashi which is called LimeGNSS. Using LimeGNSS, we created a static spoofing scenario with target location and time as 35.665701,139.793850,100 and 2023/09/28 08:00:00 (UTC), respectively. The downloaded navigation message will also be an input in LimeGNSS as this will be the basis for GPS and QZSS satellite ephemeris. We did the experiment indoors and outdoors with Xiaomi POCO M3 and Google Pixel 7a.

3. Results

Table 1 below shows a summary of results for indoor experiment setup. For indoor experiment, we only used LTE antenna for transmitting signals. Both devices were spoofed, and the time to spoof is indicated in Table 1. Although Google Pixel 7a was spoofed very quickly, lock to spoofed signal in this time is still unstable. After waiting around 2 minutes, the lock became continuous. When WiFi was on while spoofer was on, POCO M3 remained spoofed. Google Pixel 7a appears to still be spoofed based on Google Maps, but it was able to recover its true position.

Table 1. Summary of Results for Indoor Experiment

Android Device	Spoofer on (Spoofed?)	Time to Spoof	Spoofer on + WiFi on (Spoofed?)	Was position recovered?
Xiaomi POCO M3	Yes	2.5 minutes	Yes	No
Google Pixel 7a	Yes, but time is not spoofed	20s but unstable, after 2 minute more stable	Yes, but did not lock continuously to spoof signal	Yes

Table 2 below shows the summary of results for outdoor experiment where we used a GNSS Passive Antenna. Both devices were spoofed. However, we were not able to test when the WiFi was on because of lack of mobile data during the experiment.

Table 2. Summary of Results for Outdoor Experiment

Android Device	Spoofer on (Spoofed?)	Time to Spoof
Xiaomi POCO M3	Yes	1.5 minutes
Google Pixel 7a	Yes	4 minutes

4. Conclusion

For indoor experiment, the time to spoof for Xiaomi POCO M3 is 3.5 minutes while it is around 2.5 minutes for stable spoofing in Google Pixel 7a. We were not able to spoof time of Google Pixel 7a in indoors. For the outdoor experiment, it took 25 seconds and 70 seconds to lock on spoofed signals for Xiaomi POCO M3 and Google Pixel 7a, respectively. When WiFi is turned on during spoofing for indoor experiment, Xiaomi POCO M3 remained in the spoofed position and time. For Google Pixel 7a, it remained in the spoofed position, and then recovered its position after waiting some time.