DEMO: Relay/Replay Attacks on GNSS signals

Malte Lenhart
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
lenhart@kth.se

Marco Spanghero
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
marcosp@kth.se

Panagiotis Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
papadim@kth.se

ABSTRACT

Global Navigation Satellite Systems (GNSSs) are ubiquitously relied upon for positioning and timing. Detection and prevention of attacks against GNSS have been researched over the last decades, but many of these attacks and countermeasures were evaluated based on simulation. This work contributes to the experimental investigation of GNSS vulnerabilities, implementing a relay/replay attack with off-the-shelf hardware. Operating at the signal level, this attack type is not hindered by cryptographically protected transmissions, such as Galileo's Open Service Navigation Message Authentication (OS-NMA). The attack we investigate involves two colluding adversaries, relaying signals over large distances, to effectively spoof a GNSS receiver. We demonstrate the attack using off-the-shelf hardware, we investigate the requirements for such successful colluding attacks, and how they can be enhanced, e.g., allowing for finer adversarial control over the victim receiver.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**; • **Networks → Location based services**.

KEYWORDS

Global Navigation Satellite Systems (GNSS), spoofing, meaconing, replay/relay attack, off-the-shelf hardware

1 INTRODUCTION

Several critical applications rely on GNSS for their functionality, from autonomous navigation to sensitive infrastructure. However, civilian GNSS is inherently vulnerable to attacks against its availability (i.e., jamming) or its integrity (i.e., spoofing, forging GNSS signals to induce a false position or time). Recently, cost-effective tools to mount spoofing attacks increase the risk [2]. Defensive techniques in GNSS receivers are rare [14] and often limited to jamming awareness; thus, potentially leaving millions of devices exposed to adversarial manipulation.

Jamming is directly observable and well documented [4]; spoofing incidents are complex to detect and attribute. Russia reportedly deployed spoofing to prevent drones flying near high ranking officials in safety-critical events [3]. In the research literature, spoofing was used against drones to circumvent geo-fencing and enforce landings [11]. Spoofing a yacht navigation system caused the crew to adjust the course as intended by the researchers [13].

Open-sourcing powerful attack methods is problematic (e.g., misuse of research and development tools lowers the bar for potential adversaries), but such tools are important in evaluating new countermeasures for GNSS receivers. Various detection schemes have been proposed [14, 15]. However, without access to spoofing devices, most works are evaluated by simulation or against a set of well-defined spoofing recordings [9]. Commercial spoofers - if available - constitute a significant investment [5], leaving only high-budget, or knowledgeable and dedicated groups in the position to acquire or build advanced spoofing systems.

Attacks can be carried out through (the misuse of) simulation (spoofing, i.e., creation of GNSS signals from publicly available data) or *meaconing* (replaying recorded signals). Cryptographic protection can thwart spoofed/simulated GNSS transmissions but it cannot alone defend against replay attacks. The attacker can force the victim receiver to lock on to the adversarial signals (and thus control the victim's position/time): it can either cause a loss of lock on the legitimate signals (e.g., by jamming the victim), or by synchronously lifting-off the victim's lock from the legitimate signal. More specifically, the attacker synchronizes forged signals to the legitimate ones and gradually increases power; once both signals match, the victim continues tracking the higher-power adversarial signals [10].

A Global Positioning System (GPS) simulator was released as open source in 2015 [2], providing researchers a tool to test countermeasures. It is limited to GPS signals and cannot act as a synchronized spoofer. We do not expect to encounter it in realistic attacks; even though it has been adopted for self-spoofing [1]. A portable "receiver-spoofer" capable of synchronous lifting-off is presented in [10]. Signals are generated by simulation and synchronized by observation of legitimate signals. A record-and-replay attack investigation is presented in [8]. In principle simpler than spoofing, such an attack is likely to be mounted also by less knowledgeable adversaries, thus increasing its impact. It is however limited in terms of portability and lacks real-time replaying capabilities.

This motivates this work: we investigate the risk posed by real-time capable, long-distance replaying attackers, based on off-the-shelf hardware. We establish the attack feasibility, associated threat, and provide a framework for evaluating countermeasures.

2 NETWORKED REPLAYING SPOOFER

One advantage of meaconing is the ability to operate on encrypted and authenticated signals. Such attacks are relatively simple and potentially agnostic to the future evolution of GNSS signals. Furthermore, by changing the meaconer center frequency we can selectively target a subset of GNSS bands and constellations.

WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates

ACM ISBN 978-1-4503-8349-3/21/06.
https://doi.org/10.1145/3448300.3468256

The networked relay/replay attacker, illustrated in Fig. 1 consists of two colluding adversaries, with one entity (the adversarial sampler) recording legitimate GNSS signals, and the other (the adversarial forwarder) replaying them at a different location. In order for the attack to be successful (i.e., having the victim lock upon the adversarial signals and derives false position and time, due to the attack), the network bandwidth and latency have to be sufficient.

2.1 Network Prerequisites

The network bandwidth required to replay the recorded signal depends on sample rate and quantization bits used by the adversarial sampler ($dataRate = sampleRate * quantizationBits * 2$), taking into account the in-phase and quadrature components. Our preliminary investigation shows that we can achieve the lowest data rate of 31.88 Mb/s at a sample rate of 1 MHz and 16-bit quantization. The adversarial nodes are connected over TCP sockets, as UDP proved too lossy in test transmissions, not allowing a stable replay. Therefore, the choice of sampling parameters needs to be conservative with respect to the network bandwidth.

Sufficient bandwidth to act as an adversarial forwarder, highly dependent on the consumer-grade Internet in the area, is often available [7]. Upload, typically lower than download, is the limiting factor for the adversarial sampler. Such limitations will be increasingly less significant with the roll-out of fast 5G cellular network.

2.2 Experiment Setup

Fig. 2 shows the two colluding adversarial nodes, equipped with *bladeRF 2.0* Software Defined Radios (SDRs) and connected over the Internet. The adversarial forwarder has a second SDR to jam the GPS bands tracked by the victim. The *u-Blox F9P* victim receiver is connected to the the adversarial forwarder and an active antenna to track legitimate signals. The adversarial sampler receives the legitimate GNSS signal, compresses it, and relays it to the adversarial forwarder. The forwarder re-transmits it to the victim, that logs the perceived Position-Velocity-Time (PVT) solution.

To cause our Multi-GNSS receiver victim to loose lock to the legitimate GNSS signals, the adversary jams GPS L1 and L2 bands (by transmitting Gaussian noise) for a time period in which it can be assumed that the victim looses track of all satellites. All bands have to be jammed, so that the victim cannot keep tracking satellites in an undisturbed band, leading to rejection of the replayed signal. At this stage, the replay is limited to one band, therefore the other bands are consecutively jammed after meaconing is initiated.

2.3 Evaluation

To evaluate relaying/replaying over a long distance, the adversarial sampler is located in Stockholm at the KTH Campus in Kista, the adversarial forwarder is positioned in Germany at a distance of 1100 km[1]. We observed that short-term network congestion leads to a brief loss of satellite tracking at the victim, followed by resuming tracking. Such gaps can be compared to natural outages in areas with few or no visible satellites. If the adversarial sampler - adversarial forwarder bandwidth is insufficient for longer periods, the attack fails.

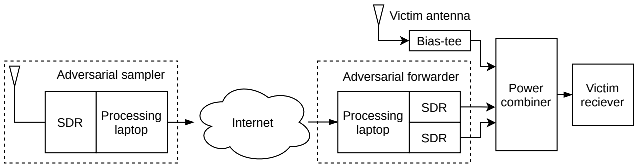
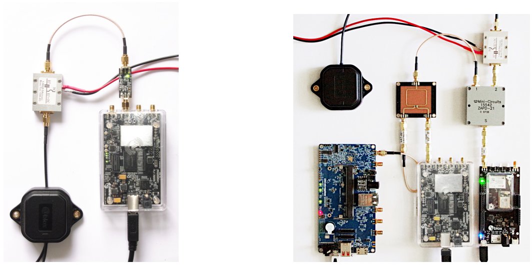


Figure 1: Block diagram of the colluding adversaries. Both adversarial nodes have a SDR, the forwarder is connected to the victim GNSS receiver via a power combiner. To force a loss of lock at the victim receiver, the adversary jams the appropriate frequencies.



(a) Adv. sampler **(b) Adv. forwarder**

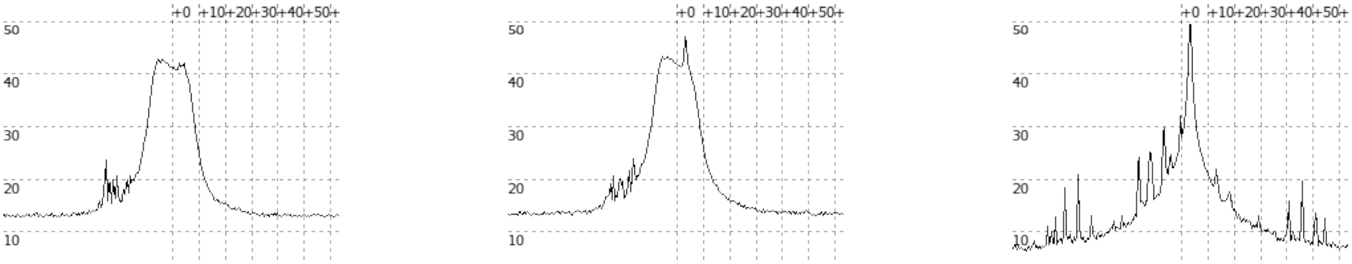
Figure 2: (a) The adversarial sampler SDR is connected to a Low-Noise-Amplifier, a bias-tee and an active GNSS antenna. (b) The victim receives the combination of legitimate GNSS signal, adversarial jamming and replayed signal.

In the first experiment, we attacked the victim receiver that has no prior lock to legitimate signals (i.e., 'cold start'). After a brief interval, the receiver accepted the spoofed signals over the weaker legitimate ones. In the second experiment, the receiver is locked onto legitimate signals, before jamming is initiated. We observe the victim loosing track of all satellites and then we start replaying.

When switching from jamming to replaying in the L1 band, it takes a few minutes until the receiver accepts the replayed signals and is mislead to be at the adversarial location[2]. We observed that in some instances the victim perceives the spoofed satellites but does not lock onto them. In this cases a brief second jamming leads to an immediate lock on in the victim once replaying resumes. Legitimate and relayed/replayed signal spectrograms are depicted in Fig. 3. The addition of replayed signals slightly distorts the power density at center frequency due the bandwidth limitation of the replayed signal. This also explains why the satellites on GPS L2 frequency are missing in the receiver side leading to a larger position error. Jamming changes the perceived spectrum drastically, which among others can be monitored by receivers to detect jamming.

[1] The reverse direction was also tested to assess suitability of consumer grade Internet for this attack. In the first attempt, the upload speed (11 Mb/s) did not suffice, leading to congestion and a non-continuous signal at the victim. A repetition in a place with an upload of 49 Mb/s allowed misleading the Sweden-based victim that its location was in Germany. This shows that a change in location and a Internet provider can determine the success of the attack.

[2] The receiver locks back onto legitimate signals a few minutes after the attack ends.



(a) Legitimate signal spectrum at the victim receiver

(b) Spectrum of combined legitimate and replayed signal

(c) Effect of jamming on legitimate spectrum.

Figure 3: Victim receiver spectrogram. Center frequency is $f_c = 1.575\,42\,\text{GHz}$, power in dB. (a) Legitimate signal. (b) Addition of the replayed signal causes a small spike (top right) in the spectrum, due to higher power and narrow bandwidth of the replayed signal. (c) Jamming changes the perceived spectrum drastically, usable for attack detection.

3 CONCLUSION

This demonstration shows that long-distance replay attacks on GNSS are possible in real-time and with off-the-shelf hardware. As Galileo OS-NMA is currently in testing phase [6], our tests do not include authenticated signals. This is part of future work and we anticipate the relaying/replaying attack effect to be the same. Cryptographic methods do not prevent relaying/replaying attacks, but their combination with other detection schemes, such as drift monitoring or signal distortion [14], can shield GNSS receivers.

Low-rate Internet and expensive hardware made this attack type infeasible in the past, but now it would be possible to setup a network of replayed location sources, streaming legitimate GNSS signals. Such a distributed setup, with several adversarial forwarders and samplers, strengthens the adversarial options. Our experiments involved static adversarial sampler and transmitter; in future work, we will work with mobile nodes, investigating the feasibility of such attack using cellular networks.

Ongoing work: We are working on relaying signals at the message level. For this, we demodulate and analyze the signal at the adversarial sampler and rebuild it, based on signal parameters, at the forwarder. This significantly reduces the required network bandwidth and enables more advanced attack types, such as delaying selected satellite signals. This influences the victim's derived position directly, beyond what is possible with relaying [12].

Replayed signals are hard to be code-phase synchronized with the legitimate signals, due to the processing and network delay. To a certain extend, this can be compensated by sophisticated distance-decreasing attacks [16], with their investigation being part of ongoing work.

4 DEMONSTRATION SETUP

In the scope of the virtual conference, we showcase our networked relay/replay spoofing attack in a pre-recorded video. We introduce the utilized software and hardware, and show the system state shown prior to the attack, with receivers at both ends showing the legitimate derived positions. To start the attack, the adversarial nodes establish the unidirectional sample stream. The adversarial forwarder initiates jamming, and then replays the streamed signals to the victim. After a while, the victim accepts the spoofed position, thus concluding our demo.

ACKNOWLEDGMENTS

This work was supported by the Swedish Foundation for Strategic Research (SSF) SURPRISE project and the KAW Academy Fellow Trustworthy IoT project.

REFERENCES

[1] 2016. *Cheating at Pokémon Go with a HackRF and GPS Spoofing.* Retrieved November 11, 2020 from https://www.rtl-sdr.com/cheating-at-pokemon-go-with-a-hackrf-and-gps-spoofing/

[2] 2018. *Gps-Sdr-Sim: Software-Defined GPS Signal Simulator.* Retrieved Octiober 29, 2020 from https://github.com/osqzss/gps-sdr-sim

[3] 2019. *Above Us Only Stars.* Retrieved November 7, 2021 from https://www.c4reports.org/aboveusonlystars

[4] 2020. *Thousands of GNSS Jamming and Spoofing Incidents Reported in 2020.* Retrieved November 11, 2021 from https://rntfnd.org/2020/12/24/thousands-of-gnss-jamming-and-spoofing-incidents-reported-in-2020-guy-buesnel/

[5] 2021. *Orolia.Com Online Store | GPS/GNSS Simulators, Network Time Servers.* Retrieved January 11, 2021 from https://store.orolia.com/

[6] 2021. *Tests of Galileo OSNMA Underway.* Retrieved May 10, 2021 from https://www.gsa.europa.eu/newsroom/news/tests-galileo-osnma-underway

[7] 2021. *Worldwide Broadband Speed League 2020 | Internet Speed Tests - Cable.Co.Uk.* Retrieved May 13, 2021 from https://www.cable.co.uk/broadband/speed/worldwide-speed-league/

[8] R. Blum, D. Dötterböck, and T. Pany. 2019. Investigation of the Vulnerability of Mobile Networks Against Spoofing Attacks on Their GNSS Timing-Receiver and Developing a Meaconing Protection. In *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation* (Reston, VA).

[9] T. E. Humphreys, J. A. Bhatti, D. Shepard, and K. Wesson. 2012. The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques. In *Proceedings of ION GNSS* (Nashville, TN).

[10] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner. 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *ION GNSS* (Savannah, GA).

[11] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys. 2014. Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics* 31, 4 (2014), 617–636.

[12] P. Papadimitratos and A. Jovanovic. 2008. Protection and Fundamental Vulnerability of GNSS. In *IEEE IWSSC.* Toulouse, France.

[13] M. L. Psiaki and T.E. Humphreys. 2016. Protecting GPS From Spoofers Is Critical to the Future of Navigation. *IEEE Spectrum: Technology, Engineering, and Science News* (Aug. 2016).

[14] M. L. Psiaki and T. E. Humphreys. 2016. GNSS Spoofing and Detection. *Proc. IEEE* 104, 6 (June 2016), 1258–1270.

[15] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren. 2016. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *Comput. Surveys* 48 (May 2016), 1–31.

[16] K. Zhang and P. Papadimitratos. 2019. On the Effects of Distance-decreasing Attacks on Cryptographically Protected GNSS Signals. In *Proceedings of ION ITM* (Reston, Virginia).