POSTER: Testing network-based RTK for GNSS receiver security

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 (GNSS) provide precise location, while Real-time Kinematics (RTK) allow mobile receivers (termed rovers), leveraging fixed stations, to correct errors in their Position-Navigation-Time (PNT) solution. This allows compensating for multi-path effects, ionospheric errors, and observation biases, enabling consumer receivers to achieve centimeter-level accuracy. While network distribution of correction streams can be protextect with common secure networking practices, the reference stations can still be attacked by GNSS spoofing or jamming. This work investigates (i) the effect RTK reference station spoofing has on the rover's PNT solution quality and (ii) the potential countermeasures towards hardening the RTK infrastructure.

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS) are ubiquitous and provide localization and timing for a wide gamut of often strategic location-based services. For precision navigation, RTK leverages multiple receivers to correct GNSS measurements at the mobile station (rover) using differential ranging and a known baseline with a reference station (base). Specifically, network-based RTK is established as an open-source, collaborative system to achieve centimeter-level accuracy with consumer-grade receivers.

Nevertheless, the current unencrypted and public nature of the GNSS signals make GNSS receivers a relatively easy target for manipulation, via spoofing, meaconing (e.g. replay/relay), or jamming [3–5]. Although cryptographic countermeasures to the spoofing problem exist, adopting such methods will take time especially when they require modifications to the signal in space or the receiver structure [6].

Generally, a rover connects to the closest reference station to the area it operates in, and the GNSS corrections are considered meaningful within a 10 km radius of the reference station. While the network-based correction stream can effectively be protected using secure internet protocols, to avoid manipulation of the information during transfer, e.g., see [8], these methods fall short if the adversary can directly manipulate the GNSS signals at the reference station. Even low-sophistication spoofing attacks are possible with low-cost hardware and open-source implementation, in particular, if simulation or replay/relay-based and can effectively control a GNSS receiver [2].

In this work, we evaluate the effects of different types of interference, from simplistic barrage jamming to sophisticated synchronous lift-off on an RTK base station, and how such manipulation reflects on the victim receiver. We attack our reference station, to avoid causing disturbance to potentially other users obtaining corrections from the station. The evaluation is performed by analyzing the state of the RTK baseline and the error under different adversarial conditions and receiver configurations.

2 SYSTEM AND ADVERSARY MODEL

Two GNSS receivers communicate over a Networked Transport of RTCM via Internet Protocol (NTRIP) interface [1]. The communication link is secured and the adversary cannot change data in transit, impersonate the reference (source of the stream), or in any way tamper with the NTRIP provided correction stream. The adversary can cause a Denial of Service (DoS), effectively making the rover unable to connect to the station but this is beyond the scope of this work as we assume the rover can at any moment connect, disconnect, and receive corrections from any available station. Additionally, we assume that the base station is honest and, unless adversarial manipulation is present, it provides legitimate, trustworthy corrections to any connected rover.

As the GNSS signal structure is known, the attacker can craft signals for any constellation or frequency (not cryptographically protected) that match the legitimate signals (modulation, frequency allocation, and data content). In addition, the adversary can generate signals so that the resulting PNT solution at the station matches the attacker's objective. Given that stations are mounted at precise locations, the adversary has full knowledge of the type of receiver, antenna, and position of the phase center of the antenna to centimeter-level accuracy. With this knowledge, the attacker can control the GNSS receiver via spoofing or meaconing or cause denial of service by jamming.

3 EXPERIMENT SETUP

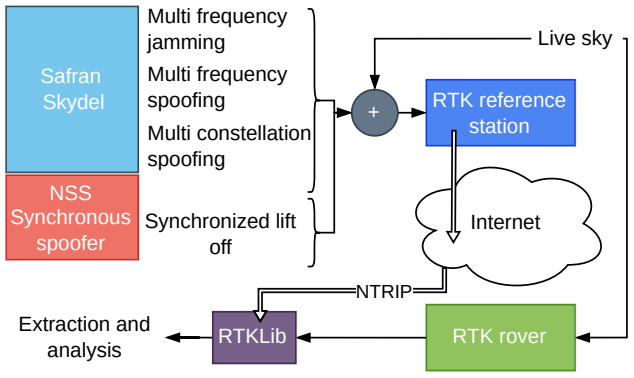

Figure 1: RTK test bed: implementation of station, rover and attacker.

The system setup considers two u-Blox ZED-F9P multi-frequency, high-precision GNSS receivers, each connected to a platform capable of providing connectivity and computation. One device is configured to broadcast RTK corrections over a secure channel using a standard NTRIP provider to all connected clients. In Fig. 1, this device is defined as *station*. For the purpose of the demonstration in this work, it is not important how the rover and the reference station exchange information in a secure, authenticated way (e.g., this can be implemented with secure network transport). The rover receiver provides raw GNSS measurement data to an implementation of RTKLib (open source, at [7]) that processes the RTK solution based on the correction stream obtained from the NTRIP server.

The adversary is implemented in two ways. First, we use a custom-made GPS L1 spoofer capable of code-phase-aligned and time-frame-aligned constellation coherent spoofing. This allows controlling the pseudorange of each satellite, by extending or shrinking it in a coordinated fashion and changing the time offset of the GNSS victim receiver. Additionally, this forces the station GNSS to produce fake pseudorange corrections at the NTRIP server. If the capture is successful, the adversary obtains full control of the RTK station GNSS receiver.

Second, we use Safran Skydel to generate a set of different scenarios, including jamming with different signals and spoofing. Multiple constellations and frequency bands can be simulated and spoofed at the same time, showing that even multi-constellation and multi-frequency RTK stations can be manipulated to produce valid but degraded correction streams.

The experiments are conducted without radiating power in the GNSS frequency bands, following the local interference avoidance regulations - all tests are conducted either in a shielded environment or via cable.

4 EVALUATION AND CONCLUSIONS

We evaluate three scenarios: synchronous spoofing, asynchronous spoofing and jamming of the reference station. The most interesting and advanced case is shown in Fig. 2. During synchronous multi-constellation spoofing with overpower, the reference station is captured during the multiple attempts (marked in red in Fig. 2). During the attack, the degradation is severe with a 3D-RMS error of more than 50 m and significantly degraded altitude. The rover reaches convergence quickly after the spoofing action stops and rapidly recovers from the attack. Nevertheless, neither the GNSS receiver nor the RTKLib implementation seems to be aware of the spoofed reference station and instead of rejecting meaningless corrections, tries to reach convergence degrading the RTK solution quality which goes from full RTK fix (where the carrier phase information is fully resolved) to Differential GNSS (considering only double differences on the pseudoranges). Instead, the receiver should reject any correction that does not improve the accuracy achievable in stand-alone positioning mode. Additional investigations in these regards are ongoing.

Further results and test cases are shown in the graphical poster, analyzing the convergence ratio, other types of attacks and potentially a proposal for a countermeasure aiming at mitigating misbehaving reference stations.

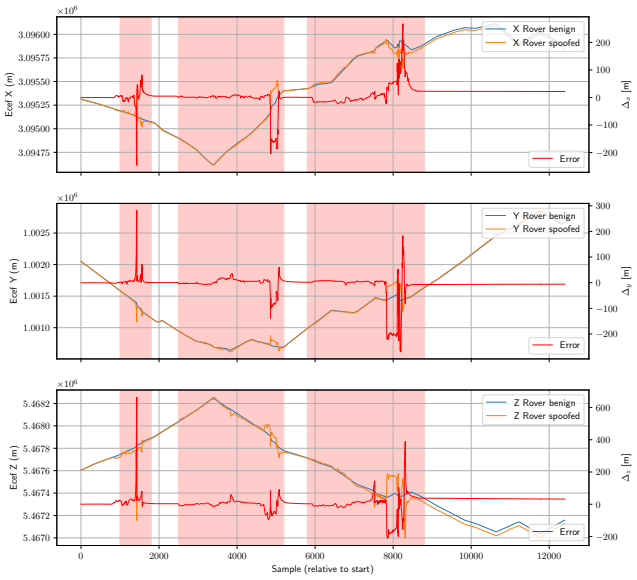

Figure 2: RTK degradation at the rover during synchronous multi-constellation spoofing.

ACKNOWLEDGMENTS

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

REFERENCES

[1] European Space Agency (ESA). 2021. *Networked Transport of RTCM via Internet Protocol (Ntrip).* Retrieved March 11, 2024 from https://gssc.esa.int/wp-content/uploads/2018/07/NtripDocumentation.pdf

[2] GPSPatron. 2021. *How Non-Coherent Spoofing Affects GNSS Base Stations.* Retrieved March 11, 2024 from https://gpspatron.com/how-non-coherent-spoofing-affects-gnss-base-stations/

[3] 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, USA).

[4] M. Lenhart, M Spanghero, and P. Papadimitratos. 2022. Distributed and Mobile Message Level Relaying/Replaying of GNSS Signals. In *International Technical Meeting of The Institute of Navigation (ITM).* Long Beach, CA, USA.

[5] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan. 2023. Location-independent GNSS Relay Attacks: A Lazy Attacker's Guide to Bypassing Navigation Message Authentication. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks.* Guildford, UK.

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

[7] RTKLibExplorer. 2021. *A version of RTKLIB optimized for single and dual frequency low cost GPS receivers, especially u-blox receivers.* Retrieved March 11, 2024 from https://github.com/rtklibexplorer/RTKLIB

[8] Pepijn van Tol. 2020. *RTK-GNSS augmentation data spoofing.* Master's thesis. Delft University of Technology, The Netherlands.