DEMO: RTKiller - controlling GNSS rovers by RTK base spoofing

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 global positioning and timing. Multiple receivers with known reference positions (stations) can assist mobile receivers (rovers) in obtainin Global Navigation Satellite System (GNSS) corrections and achieve centimeter-level accuracy on consumer devices. However, GNSS spoofing and jamming, nowadays achievable with off-the-shelf devices, are serious threats to the integrity and robustness of public correction networks. In this demo, we show how manipulation of the Position-Navigation-Time (PNT) solution at the reference station is reflected in the loss of baseline fix or degraded accuracy at the rover. Real Time Kinematics (RTK) corrections are valuable but fundamentally vulnerable: attacking the reference stations can harm all receivers (rovers) that rely on the targeted reference station.

1 INTRODUCTION

GNSS services are commonly used to provide precise timing and localization, globally, to a wide set of applications. Standalone GNSS can achieve sub-meter accuracy, but RTK is necessary in high-accuracy contexts. RTK allows using multiple GNSS receivers to obtain centimeter-level accuracy correcting measurement errors by comparing a moving receiver (rover) with a static one (station). RTK is commonly used for Unmanned Aerial Vehicle (UAV) navigation, autonomous driving, robotics, and precision agriculture applications, as it is simple and cost-effective. Modern RTK infrastructure relies on network-based RTK, unlike traditional RTK with short-range radios connecting the rover and the station receiver. This simplifies both the extension of and the accessibility to correction services. Several reference stations are connected to the Internet and any device can leverage network connectivity to obtain out-of-band GNSS corrections; inversely, a single reference station can provide corrections to multiple receivers, usually within 10 km from the station location.

RTK reference stations are mounted at precisely surveyed points, whose location is accurately determined. This way, the reference receiver can calculate precise carrier phase measurements referenced to its static position and distribute this information to the connected rovers, which ultimately use them to calculate precise positions. The corrections are meaningful only if the rover can securely access the reference station (e.g., via an authenticated and encrypted link as in [4]), and the reference station itself is not under adversarial control. Nevertheless, each RTK reference receiver, even if otherwise trusted, can be jammed or spoofed: cryptographical protocols safeguarding the network-based correction distribution system cannot contain this problem.

Spoofing any mobile GNSS receiver, in this context the rover, is complex, but it is much simpler and straightforward to smoothly capture a GNSS receiver whose location is well-determined and fixed. By attacking the RTK reference, the attacker is capable of causing significant degradation of the PNT solution at the rover, resulting in potentially infeasible trajectory control or outright denial of service. This is specifically true in cases where RTK corrections are necessary to obtain the required accuracy and any rover that obtains corrections from a reference station under adversarial control data will be affected.

This is exactly the aim of this demo: under different GNSS constellation configurations and attack methods, we show that a strategically placed attacker can degrade the PNT solution quality at the rover simply by tampering with the reference station receiver. We demonstrate three adversarial settings (synchronous single constellation lift-off, multiconstellation asynchronous spoofing, and jamming), and the effects they have on the rover's PNT solution.

2 SYSTEM AND ADVERSARY MODEL

Two GNSS receivers, one configured as RTK rover and the other as RTK station, are connected over a network link. The RTK station is mounted in a fixed point with known coordinates, which are included in the correction stream that is provided over the network. The network link between the rover and the station is protected by standard network practices (e.g., authenticated link). Practically, the adversary can only control the reference GNSS receiver by simulation, co-simulation, or replay-relay of GNSS signals. The attack setup is simplified in Fig. 1, where the attacker causes a reduction of accuracy at the rover by the transmission of interference to the reference station.

Due to the open structure of the GNSS signal the adversary can craft signals with valid modulation, frequency, and data content that match the position of the RTK station and, jointly, the adversarial action. This usually consists of (but is not limited to) modifications in the navigation data information, code-carrier modification, and selective replacement of specific signals [1, 2]. Specifically, the adversary can match and synchronize the spoofing signals to the legitimate ones and slowly force its adversarial action. It is important to notice here that the attacker aims to disrupt and degrade the RTK solution quality at the rover. In a regular spoofing scenario, the adversary usually cannot measure the effect of its action on the victim receiver. Due to the broadcast nature of the network-based RTK, the attacker can monitor the degradation caused to the correction stream by tampering with the GNSS signals simply by connecting its own rover receiver to the connection stream.

3 EXPERIMENT SETUP

The RTK rover implementation relies on RTKLIB for the baseline calculation and RTK corrections, providing the user with a 3D

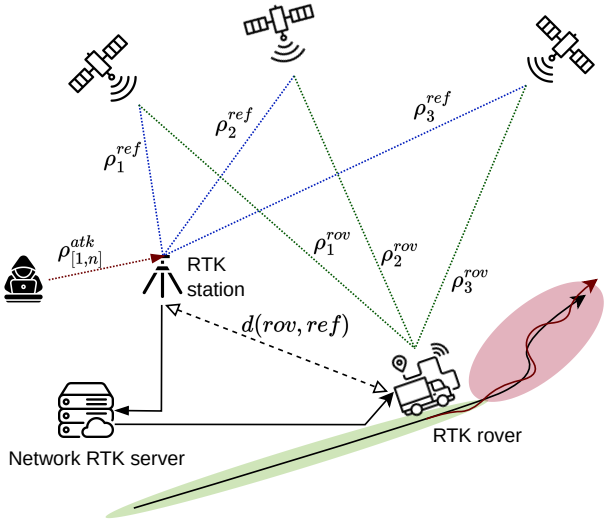

Figure 1: Typical network RTK scenario with an attacker spoofing the reference station

corrected PNT solution. The receivers on each GNSS-enabled node are u-Blox ZED-F9P high precision RTK receivers.

The adversary is implemented in two different ways. First, a custom-made synchronous signal simulator targeting L1 is used. This implementation allows the adversary to generate code phase-matched GPS L1 signals for each satellite consistent with the RTK station's live sky view and transmit them synchronously to the beginning of the GPS frame at the victim receiver. The attacker can modify the pseudoranges at the victim receiver while maintaining the victim's fixed position consistent with the operational conditions of the RTK station. Second, an asynchronous spoofing attack is mounted against the RTK station, targeting multiple constellations and forcing the RTK station into a different position. The second adversarial setting allows the transmission of different jamming signals and conditions detrimental to the station PNT solution quality. The experimental setup of the demo is shown in Fig. 2. This demonstration will showcase the implementation of the attack using both our in-house simulator and Safran Skydel to generate a legitimate constellation and a spoofing signal for a station and a rover receiver. The attendees will have the possibility of directly interacting with the setup and testing our live-sky spoofer.

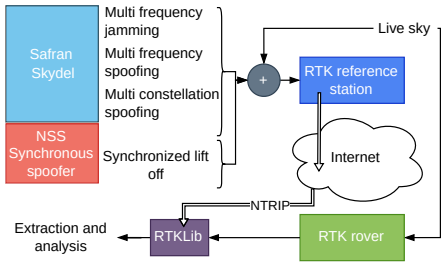

Figure 2: Demo setup.

4 EVALUATION AND CONCLUSIONS

The experiment shows that the 3D error under spoofing is 30 m, with peaks of several 100s of meters and the baseline calculation fails in 47.12% of the cases (where the GNSS receiver and RTKLib default to a differential solution, instead of a fixed RTK one). The investigation is ongoing to explore whether the manipulation of the reference could cause predictable adversary-induced behavior at the rover. Results of this work are presented also in [3]

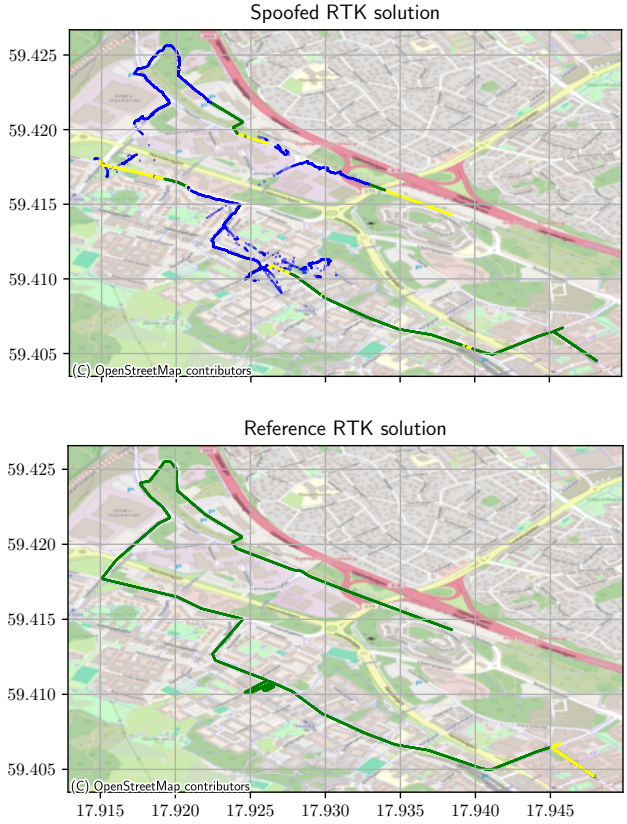

Figure 3: RTKiller in action causing degraded DGNSS solution at the rover.

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] 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).

[2] 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.

[3] Spanghero M and P. Papadimitratos. 2024. Poster: Testing network-based RTK for GNSS receiver security. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*. Seoul, Korea.

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