POSTER: SemperFi: A Spoofer Eliminating Standalone GPS Receiver

Harshad Sathaye
Northeastern University
Boston, USA
sathaye.h@husky.neu.edu

Aanjhan Ranganathan
Northeastern University
Boston, USA
aanjhan.ranganathan@northeastern.edu

ABSTRACT

With the advent of autonomous cyber-physical systems such as self-driving cars and unmanned aerial vehicles, the use of Global Positioning System (GPS) for positioning and navigation has become ubiquitous. It is well-known that GPS is vulnerable to signal spoofing attacks. There is a need to design and develop a standalone GPS receiver capable of autonomous recovery during a spoofing attack. In this work, we present SemperFi, a single antenna, standalone, GPS receiver that is capable of tracking legitimate GPS satellite signals and estimating the true location even during a spoofing attack. Unlike majority of wireless systems where data contained in the wireless signals is important, GPS relies on the time of arrival of satellite signals. This presents a unique challenge and to address this challenge, SemperFi consists of specially designed algorithms and modules based on successive interference cancellation that are capable of recovering legitimate GPS signals that are overshadowed completely by a powerful adversary. We implement our design using SoftGNSS and evaluate its performance against a variety of GPS datasets. Our evaluations show that SemperFi can recover from a seamless takeover attack with an accuracy of 100 m and power advantage of an attacker up to 15 dB. SemperFi can also be incorporated as a pluggable module capable of generating a spoofer free GPS signal for processing on any COTS GPS receiver available today. Finally, we release the implementation of our receiver design to the community for further development.

1 INTRODUCTION

Global Positioning System (GPS) is used ubiquitously to estimate location and time in a wide variety of applications such as positioning, navigation, asset and personnel tracking, communication systems, power grids, emergency rescue and support, and access control. With the advent of unmanned vehicular systems such as self-driving cars, the use of GPS in safety- and security-critical applications is only increasing. GPS is one of the Global Navigation Satellite Systems (GNSS)[1] comprising of a constellation of satellites. Each satellite continuously broadcast data called navigation messages that contain various information such as the satellite's location and time of transmission. A receiver on the ground receives these navigation messages and calculates a *pseudorange* to each of the visible satellite based on the time of transmission contained in the navigation message and the time of arrival estimated at the receiver. The receiver then proceeds to estimate its location and time using multilateration once pseudoranges of at least four satellites have been acquired. Due to the lack of any form of authentication in civilian navigation messages, GPS is vulnerable to signal spoofing attacks. In a signal spoofing and cancellation attacks, the attacker transmits specially crafted signals that imitate satellite signals with power high enough to overshadow the legitimate signals as shown in [2–4, 16] or cancel the signals as seen in [14].

Several countermeasures to GPS spoofing based on cryptographic and physical-layer signal properties have been proposed. Cryptographic countermeasures [6, 10, 11, 19] prevent attackers from generating arbitrary false GPS signals. However, they do not protect against replay attacks. Other countermeasures rely on detecting anomalies in the physical characteristics of the received GPS signal such as received signal strength [18], noise levels, direction or angle of arrival [12], and other data that are readily available. Some countermeasures [15] exploit the difficultly in canceling out legitimate GPS signals completely to detect stealthy, seamless takeover attackers. A few countermeasures propose the use of additional sensors [8], receivers [13, 17] and even crowdsourced network [9] to detect spoofing attacks. The majority of the above schemes only detect GPS spoofing, i.e., raise an alarm in case of a spoofing attack and often require manual intervention. Moreover, existing spoofing mitigation techniques are ineffective against strong adversaries capable of completely overshadowing the legitimate signals and

[1] GLONASS, Beidou, Galileo are some other GNSS

WiSec '20, July 8–10, 2020, Linz (Virtual Event), Austria

ACM ISBN 978-1-4503-8006-5/20/07…$15.00
https://doi.org/10.1145/3395351.3401703

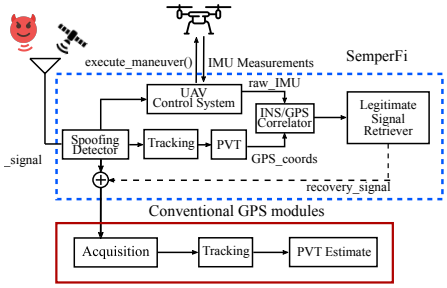

Figure 1: Schematic of SemperFi with Adversarial Peak Identifier and legitimate Signal Retriever

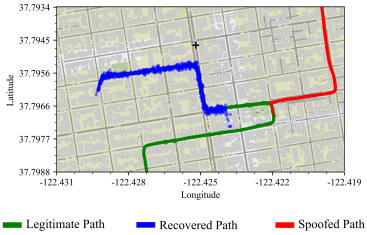

Figure 2: This figure shows the legitimate path, the spoofed path and the recovered path. The '+' mark shows the reference point for UTM plots

are incapable of uninterrupted operation during a spoofing attack.

2 DESIGN OF SemperFi

A block diagram of SemperFi's various components is shown in Figure 1. Two modules work together to enable fully-autonomous spoofing resistance: i) Adversarial Peak Identifier, ii) legitimate Signal Retriever (LSR). In this work, we use the design of a prior work [15].

The adversarial peak identifier (API) is implemented in SemperFi to detect spoofing and identify which of the detected peaks needs to be attenuated. API correlates accurate inertial measurement unit data and calculated position velocity and time (PVT) solution to accurately detect spoofing and provide SemperFi with the necessary information to attenuate adversarial signals. The LSR is responsible for generating a replica of the adversarial signal that is used to perform successive interference cancellation (SIC). The LSR module uses the tracking parameters output by the spoofing detector to track the adversary signal for a specific duration and extract navigation bits. Then, the amplitude and phase of the adversarial signal are estimated, and a recovery signal (an estimate of adversary signal) is generated with the extracted bits as the navigation message contents. The replica is then fed back to execute SIC and then passed for acquisition. If necessary, this process is repeated until an alarm is not triggered by the spoofing detector module. At this stage, the spoofing signal is eliminated or significantly attenuated, and therefore the receiver starts tracking the legitimate signals. There are scenarios where either due to the spoofing signal's strength or synchronization with respect to the legitimate signals, the navigation messages contents and its time of arrival are hard to track and introduce ambiguities in the PVT estimates. The pseudorange rectifier corrects these ambiguities by rectifying the arrival times, which are otherwise overshadowed. Finally, we designed SemperFi as a plugin module that can be configured to act as a spoofing signal filter, where the filtered signal can be directly fed to any commercial GPS receiver. This prevents significant hardware design changes to existing deployments.

3 EVALUATION OF SemperFi

A complete functional SemperFi was implemented on Soft-GNSS [5] an open-source single-frequency GPS and Galileo receiver written in MATLAB. It allows granular control over various processes incorporated in a typical receiver. Soft-GNSS support can be extended to data recorded by a plethora of software-defined radio frontends. In our implementation and evaluation, we use sophisticated software-defined radios manufactured by Ettus Research [1], specifically, USRP B210 and N210 with SBX-40 daughterboard for recording and providing raw data. SemperFi is implemented as a feedback system separate from the acquisition. The spoofing detection module is implemented as a configurable module inside the acquisition block. We evaluate SemperFi and showcase its performance in recovering legitimate GPS signals under a variety of attack settings and traces. Specifically, we use three different datasets that contain both spoofing and legitimate signals: i) Synthetic GPS signals generated using COTS GPS simulators, ii) Recorded real-world GPS signals and iii) a public repository of GPS spoofing signals (TEXBAT) [7]. The signals were captured, stored, and used as input to SemperFi. Figure 2 shows the recovery of simulated GPS signal.

4 CONCLUSION

We presented SemperFi, a stand-alone, single-antenna spoofer signal eliminating, GPS receiver that is capable of providing uninterrupted legitimate locations even in the presence of a strong adversary. We designed, implemented and evaluated SemperFi against various GPS signal traces. We showed that SemperFi can fully recover from a seamless takeover attack with an accuracy of 100 meters and power advantage of an attacker up to 15 dB. Finally, we release the implementation of our receiver design to the community for further development.

REFERENCES

[1] Ettus Research. https://www.ettus.com/products/.

[2] UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, 2013. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.

[3] Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria, 2019. https://www.c4reports.org/aboveusonlystars.

[4] Ghost ships, crop circles, and soft gold: A gps mystery in shanghai, 2019. https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/.

[5] Borre, K., Akos, D. M., Bertelsen, N., Rinder, P., and Jensen, S. H. *A software-defined GPS and Galileo receiver: a single-frequency approach*. Springer Science & Business Media, 2007.

[6] Cheng, X.-j., Xu, J.-n., Cao, K.-j., and Wang, J. An authenticity verification scheme based on hidden messages for current civilian gps signals. In *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology* (2009), IEEE, pp. 345–352.

[7] Humphreys, T. E., Bhatti, J. A., Shepard, D., and Wesson, K. The texas spoofing test battery: Toward a standard for evaluating gps signal authentication techniques. In *Radionavigation Laboratory Conference Proceedings* (2012).

[8] Jafarnia-Jahromi, A., Lin, T., Broumandan, A., Nielsen, J., and Lachapelle, G. Detection and mitigation of spoofing attacks on a vector-based tracking gps receiver. *Proc. ION ITM* (2012), 790–800.

[9] Jansen, K., Schäfer, M., Moser, D., Lenders, V., Pöpper, C., and Schmitt, J. Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks. In *2018 IEEE Symposium on Security and Privacy (SP)* (2018), IEEE, pp. 1018–1031.

[10] Kuhn, M. G. An asymmetric security mechanism for navigation signals. In *International Workshop on Information Hiding* (2004), Springer, pp. 239–252.

[11] Lo, S. C., and Enge, P. K. Authenticating aviation augmentation system broadcasts. In *IEEE/ION Position, Location and Navigation Symposium* (2010), IEEE, pp. 708–717.

[12] Meurer, M., Konovaltsev, A., Appel, M., and Cuntz, M. Direction-of-arrival assisted sequential spoofing detection and mitigation.

[13] Montgomery, P. Y. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil gps spoofer. In *Radionavigation Laboratory Conference Proceedings* (2011).

[14] Moser, D., Lenders, V., and Capkun, S. Digital radio signal cancellation attacks: An experimental evaluation. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (2019), ACM, pp. 23–33.

[15] Ranganathan, A., Ólafsdóttir, H., and Capkun, S. Spree: A spoofing resistant gps receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking* (2016), pp. 348–360.

[16] Shepard, D. P., Bhatti, J. A., and Humphreys, T. E. Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle.

[17] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security* (2011), pp. 75–86.

[18] Warner, J. S., and Johnston, R. G. Gps spoofing countermeasures. *Homeland Security Journal 25*, 2 (2003), 19–27.

[19] Wesson, K., Rothlisberger, M., and Humphreys, T. Practical cryptographic civil gps signal authentication. *NAVIGATION: Journal of the Institute of Navigation 59*, 3 (2012), 177–193.