Opinion: Advancing Attacker Models of Satellite-based Localization Systems—The Case of Multi-device Attackers

Kai Jansen
Ruhr-University Bochum
Bochum, Germany
kai.jansen-u16@rub.de

Christina Pöpper
New York University Abu Dhabi
Abu Dhabi, United Arab Emirates
christina.poepper@nyu.edu

ABSTRACT

In this paper, we report on recent advancements in attacking satellite-based positioning systems and on shortcomings of proposed countermeasures. Applications based on satellite positioning and navigation systems make use of a deployed infrastructure that is challenging to protect and secure against attacks. Many of the proposed protection mechanisms and solutions in the wild are based on and analyzed with respect to single-antenna attacker models that should in the meantime be considered outdated as they are no longer appropriate. Due to a significant drop in complexity and cost to perform multi-device attacks on these systems, the attacker models need to be adjusted to comprise more powerful adversaries that have recently become a reality. By demonstrating the implementation of a simple yet effective multi-antenna setup, we outline possible attacks against systems that are otherwise considered secure.

CCS CONCEPTS

•**Security and privacy** →*Mobile and wireless security;* •**Information systems** →Spatial-temporal systems;

KEYWORDS

localization security, attacker model, multi-device attack

ACM Reference format:
Kai Jansen and Christina Pöpper. 2017. Opinion: Advancing Attacker Models of Satellite-based Localization Systems—The Case of Multi-device Attackers. In *Proceedings of WiSec '17, Boston, MA, USA, July 18-20, 2017,* 4 pages.
DOI: 10.1145/3098243.3098270

1 INTRODUCTION

Localization systems based on multiple reference points such as satellites allow the positioning of entities by determining the individual distances to those references. However, distance-based localization systems are challenging to protect and are usually prone to spoofing attacks, e. g., fake GPS signals can be specifically generated to confuse the localization procedure of a targeted receiver to inject false position or time information.

When the first affordable GPS spoofing systems became available, the research community began proposing countermeasures against spoofing attacks. These solutions were designed to defend against attackers that use one spoofing system to generate a mixture of false signals transmitted over a single antenna. Proposed countermeasures against these attackers were mainly based on signal characteristics that could not be correctly emulated by single-antenna systems such as geometric features [17, 23–25], signal correlations [3, 8, 12], relative carrier phases [4, 13, 16], angle of arrival [28], Doppler effects [21], or signal arrival times [20].

Part of these works assume that an attacker can only utilize single-antenna spoofing systems and that using multiple devices is deemed too complex or too expensive. Concerning technical advancements and significant cost reductions to deploy several spoofing devices simultaneously, these assumptions need to be considered outdated. However, today's security solutions are still based on the single-antenna attacker model and neglect the fact that the multi-device attacker has become a reality. As a result, systems with this outdated attacker model need to be considered potentially insecure.

For instance, a multi-device attacker can successfully attack systems that use a distributed sensor infrastructure such as two proposals to secure air traffic from Schäfer et al. [20, 21]. While the former system is based on unspoofable time offsets [20], the latter builds on the integrity of the Doppler Frequency [21]. Nevertheless, a multi-device attacker can adjust both properties at different locations accordingly to, e. g., inject fake aircraft remaining undetectable by the respective system. Furthermore, anti-spoofing systems based on signal characteristics such as the angle of arrival [12] or spatial correlation [3] can be circumvented by deploying multiple antennas sending from different directions. Such systems could also emulate realistic multipath propagation.

2 ATTACK ADVANCEMENTS

The GPS spoofing threat was first brought to a wider attention of the public by the Volpe report [1] in 2001. The report states that malicious parties could be able to deploy attacks against systems relying on GPS with respect to the system's inherent lack of confidentiality and authentication. The spoofing threat became a reality in 2008 when Humphreys et al. [9] presented a self-built portable GPS spoofer to generate fake satellite signals with which they demonstrated the vulnerability of GPS-dependent systems.

In the meantime, GPS satellite simulators—mainly designed for developing and testing purposes—dropped significantly in cost from approx. $100,000 [12] to a few thousand dollars. However, these devices can also be turned into spoofing systems, limited only by the accompanying software tools. Eventually, at DEFCON 2015,

WiSec '17, Boston, MA, USA

978-1-4503-5084-6/17/07…$15.00
DOI: 10.1145/3098243.3098270

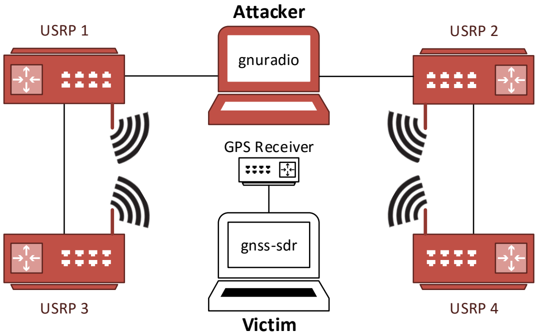

Figure 1: A simple experimental multi-antenna attacker setup consisting of four USRPs synchronized and operated by *gnuradio* targeting a victim's GPS receiver.

a software-defined radio GPS spoofer was presented [15] that is fully customizable and only requires off-the-shelf USRPs such as a HackRF [7], which lowers the costs for a single spoofing system to approx. $400. Several systems of this type can be utilized to transmit different signals realizing a multi-antenna attacker.

As a result, we conclude that, during the last decade, the cost and complexity to build a GPS spoofing system lowered significantly. While the threat of facing a multi-antenna attacker could be considered minimal ten years ago, nowadays we need to factor the deployment of such an attacker into our attacker models as it has become feasible, thus changing our security assumptions.

3 IMPLEMENTATION OF A MULTI-ANTENNA ATTACKER

To illustrate the advancement in attacker capabilities, we deploy a simple yet effective setup to generate multiple spoofing signals (Fig. 1). Each spoofing signal constitutes a different satellite signal, all of which are then recombined at the targeted receiver who uses them to compute the corresponding position solution. Note that this is different from the standard attacker setup, where a mix of satellite signals is emitted from the same source [3, 4, 9, 11–13, 16–19, 26, 28]. The implementation of a multi-antenna attacker allows us to be more flexible and to attack systems that assume that the attacker cannot leverage these many degrees of freedom.

In particular, we deploy a setup of four USRPs N210 from Ettus Research [6], each transmitting a different satellite signal. These signals are generated by the software tool *gps-sdr-sim* [15] for four random satellites that were visible at the position and time to be spoofed. All USRPs are connected via a network switch and a standard laptop running *gnuradio*. A *gnuradio* block was designed that synchronously provides the USRPs with the necessary precomputed data samples. The USRPs are coupled with standard off-the-shelf passive GPS antennas. The targeted GPS receiver is another USRP N210 device connected to a second laptop running *gnss-sdr* [5] to analyze the capability of our multi-antenna attacker.

We performed this experiment in an indoor environment shielded from the outside to minimize potential signal leakages to the outside. With this simple test environment, we gathered the following three insights. (i) We were able to spoof the receiver with four spoofing devices each emitting a different satellite signal. By placing the spoofers equidistant to the receiver and a time synchronization via *gnuradio*, we achieved a stable position lock on the spoofed signals. (ii) The targeted receiver acquired a lock on the spoofed signals after 50 s, which is in the range of a normal warm start. (iii) The achieved position accuracy was within an error of 20 km.

Notably, the time synchronization between the spoofing signals is a crucial requirement for a stable lock and for yielding the desired position. For instance, a time offset of 1 ms causes an offset in the pseudorange of approx. 300 km. This can lead to unstable calculations and high position errors. Considering the high dependency on the time synchronization, we were able to preliminarily achieve a good accuracy that was also reproducible. Moreover, all results have been gathered in a non-laboratory environment, and we plan to significantly increase the accuracy in future experiments by implementing an external time pulse reference [2].

As a result, we were able to successfully spoof the targeted receiver with a setup that uses four antennas that each emit a different satellite signal. This setup allows us to dynamically adjust single satellite signals separately from each other. Hence, we obtain the complete freedom of how to manipulate the target, i. e., we can change individual pseudoranges, signal amplitudes, Doppler frequencies, angle of arrivals, or time delays in order to trigger a desired behavior. This can either be achieved by adjusting the transmitted signals or by changing the geometric setup. This allows attacking systems that are based on the assumption that signals are transmitted as a mixture and cannot be changed individually.

It is noteworthy that the costs of the deployed attacking setup are moderate and can be further decreased by using cheaper SDRs such as a HackRF One [7], which is expected to perform equally good. The required knowledge can also be considered low as most software is freely available online and the *gnuradio* block can be generated by automated tools. This setup implements a fully customizable multi-antenna attacker that can be used to target present secure localization systems.

4 RELATED WORK AND MULTI-ANTENNA ATTACKER IMPACT

While there is a multitude of related work on how to protect localization systems, the assumptions made on the attacker model differ significantly. For instance, several countermeasure proposals only consider a single-antenna attacker and state that a multi-antenna attacker is too complex, too costly, or too impractical [3, 4, 8–10, 12, 13, 16–18, 23–25]. The presented solutions are shown to be secure against the single-antenna attacker model, but considering a more realistic attacker, they need to be re-evaluated. Table 1 contains an overview of related work on localization systems that consider the multi-antenna attack model and the resistance of the proposed solutions to multi-antenna attacks.

Moreover, countermeasure solutions assuming the outdated single-antenna attacker model [3, 4, 8, 10, 12, 13, 16, 20, 21, 28] can be deemed vulnerable against a stronger attacker. In particular, we need to consider those works as potentially insecure and to fall victim to more sophisticated attackers. As a special case, solutions based on multiple receivers monitoring the satellite pseudoranges [17, 18, 23–25] can be shown to be secure using four or more receivers according to Tippenhauer et al. [26].

Table 1: Related work on wireless localization security and related fields that consider a multi-antenna (MA) attacker as a potential threat.

Ref.	Year	MA Attacker Too Complex	Potentially Vulnerable	Attack Resistant
[9]	2008	✓	—[1]	—[1]
[13]	2009	✓	✓	✗
[12]	2010	✓	✓	✗
[4]	2010	✓	✓	✗
[26]	2011	✗	—[1]	✓[2]
[3]	2012	✓	✓	✗
[28]	2012	✗	✓	✗
[10]	2012	✓	✓	✗
[16]	2013	✓	✓	✗
[23–25]	2013/14	✓	✓[3]	✓[4]
[8]	2014	✓	✓	✗
[27]	2014	✗	✗	✓
[17, 18]	2015	✓	✓[3]	✓[4]
[22]	2015	✗	—[1]	—[1]
[20, 21]	2015/16	✗	✓	✗
[14]	2016	✗	—[1]	—[1]
[19]	2016	✗	✗[5]	✓[5]
[11]	2016	✗	✗	✓

[1] focus on attacks rather than countermeasures
[2] and provide a proof for the security of four and more receivers
[3] with three or less receivers
[4] with four or more receivers
[5] secure according to the authors, but we argue that using more antennas as available channels in the receiver can also circumvent this countermeasure

As a consequence, countermeasures that were already designed with an extended attacker model in mind exhibit better security against the multi-antenna attacker [11, 19, 27]. However, while Ranganathan et al. [19] state that their system is secure against any currently known attacker, the countermeasure makes use of a limited number of channels. Raising the number of attacking devices above the number of channels, the countermeasure could potentially be circumvented.

Recently, the first works that specifically put the focus on a multi-device attacker model were published. These publications do not necessarily analyze localization systems but evaluate the capabilities of multi-device attackers on, e. g., sensor systems or physical-layer key exchange. For instance, Moser et al. [14] presented insights on how to attack an air traffic control sensor system by using a multi-device attacker. Furthermore, Steinmetzer et al. [22] outlined an attack using a multi-antenna setup to eavesdrop on a physical-layer key exchange. This attacker can successfully reconstruct the secret key, which was deemed impossible considering the outdated single-antenna attacker. We want to highlight that these publications are an exception to the standard security models.

Table 2 shows related work—not limited to localization systems—that already consider multi-device attackers and present either theoretical, simulation, or experimental results. As a summary, only a few works exist that analyze stronger attacker models and the minority actually performed simulations or experiments.

Table 2: Selected publications that already provide results with respect to a multi-antenna adversary model.

Domain	Ref.	Theory	Simulation	Experiment
Localization	[9]	✓	✗	✗
	[11]	✓	✗	✗
	[19]	✓	✗	✗
	[26]	✓	✗	✗
Power Grids	[27]	✓	✗	✗
Physical Layer Key Establishment	[22]	✓	✓	✓
Air Traffic Control	[14]	✓	✓	✓

5 CONCLUSION AND DESIRED DIRECTIONS

We conclude that the majority of security solutions for satellite-based localization systems are based on an outdated single-antenna attacker model. Our simple yet effective multi-antenna setup demonstrates that today adversaries have access to affordable and moderately complex tools to deploy multiple-device spoofing systems. These systems can be used to attack localization systems that were considered secure in the single-antenna adversary model. Even more critical, the systems are falsely shown to be secure without factoring in that stronger attackers already became a reality and may completely break the security.

Taking these insights into consideration, we advocate a better understanding of present attacker models, i. e., the multi-antenna attacker. In general, proposals for countermeasures should be based on the most recent advancements in attacker capabilities and should faster react on future progressions of available tools. We want to highlight again that the multi-device attacker—often deemed as too complex—needs to be considered as a feasible attack vector and countermeasures need to be developed accordingly.

For the future, we demand designs and security solutions that are resistant against the multi-antenna attacker to guarantee their integrity. First works already considered stronger adversary models, however, this is still an exception. Following their approach, this gives a good direction for future work that needs protection even against strong but realistic attackers.

ACKNOWLEDGMENTS

The authors would like to thank David Rupprecht for helping to conduct the experiments by providing useful insights into synchronized attacks. This work was supported in parts by the DFG Research Training Group GRK 1817/1 and the BMBF SysKit project.

REFERENCES

[1] Anon. 2001. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.* Technical Report Final Report. John A. Volpe National Transportation Systems Center.

[2] Marco Bartolucci, José A. del Peral-Rosado, Roger Estatuet-Castillo, José A. García-Molina, Massimo Crisci, and Giovanni E. Corazza. 2016. Synchronisation of Low-Cost Open Source SDRs for Navigation Applications. In *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC '16).* IEEE, Noordwijk, Netherlands.

[3] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. 2012. GNSS Spoofing Detection in Handheld Receivers based

on Signal Spatial Correlation. In *IEEE/ION Position, Location and Navigation Symposium (PLANS '12)*. IEEE, Myrtle Beach, SC, USA, 479–487.

[4] Antonio Cavaleri, Beatrice Motella, Marco Pini, and Maurizio Fantino. 2010. Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. In *ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC '10)*. IEEE.

[5] Centre Tecnológic de Telecomunicacions de Catalunya (CTTC). 2017. An open source Global Navigation Satellite Systems software-defined receiver. (2017). Retrieved March 18, 2017 from http://gnss-sdr.org

[6] Ettus. 2017. Universal Software Radio Peripheral (USRP). (2017). Retrieved March 18, 2017 from https://www.ettus.com

[7] Great Scott Gadgets. 2017. HackRF One. (2017). Retrieved March 18, 2017 from https://greatscottgadgets.com/hackrf/

[8] Liang Heng, Jonathan J. Makela, Alejandro D. Domffinguez-Garcffia, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao. 2014. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture. In *Power and Energy Conference at Illinois (PECI '14)*. IEEE, Champaign, IL, USA, 196–202.

[9] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon, and Paul M. Kintner, Jr. 2008. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '08)*. Savannah, GA, USA, 2314–2325.

[10] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Gérard Lachapelle. 2012. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation* 2012 (May 2012).

[11] Kai Jansen, Nils Ole Tippenhauer, and Christina Pöpper. 2016. Multi-Receiver GPS Spoofing Detection: Error Models and Realization. In *Annual Computer Security Applications Conference (ACSAC '16)*. ACM, Los Angeles, CA, USA, 237–250.

[12] Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Isaac Miller. 2010. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. In *International Technical Meeting of The Institute of Navigation (ION '10)*. San Diego, CA, USA, 698–712.

[13] Paul Y. Montgomery, Todd E. Humphreys, and Brent M. Ledvina. 2009. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer. In *International Technical Meeting of The Institute of Navigation (ION '09)*. Anaheim, CA, USA, 124–130.

[14] Daniel Moser, Patrick Leu, Vincent Lenders, Aanjhan Ranganathan, Fabio Ricciato, and Srdjan Čapkun. 2016. Investigation of Multi-device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. In *Annual International Conference on Mobile Computing and Networking (MobiCom '16)*. ACM, New York, USA, 375–386.

[15] osqzss. 2017. Software-Defined GPS Signal Simulator. (2017). Retrieved March 18, 2017 from https://github.com/osqzss/gps-sdr-sim

[16] Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon. 2013. GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data. In *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ '13)*. Nashville, TN, USA, 2949–2991.

[17] David S. Radin. 2015. *GPS Spoofing Detection Using Multiple Antennas and Individual Space Vehicle Pseudoranges*. Master's Thesis. University of Rhode Island.

[18] David S. Radin, Peter F. Swaszek, Kelly C. Seals, and Richard J. Hartnett. 2015. GNSS Spoof Detection Based Upon Pseudoranges from Multiple Receivers. In *International Technical Meeting of The Institute of Navigation (ION '15)*. Dana Point, CA, USA, 657–671.

[19] Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Čapkun. 2016. SPREE: A Spoofing Resistant GPS Receiver. In *Annual International Conference on Mobile Computing and Networking (MobiCom '16)*. ACM, New York, USA, 348–360.

[20] Matthias Schäfer, Vincent Lenders, and Jens Schmitt. 2015. Secure Track Verification. In *IEEE Symposium on Security and Privacy (SP '15)*. IEEE, San Jose, CA, USA, 199–213.

[21] Matthias Schäfer, Patrick Leu, Vincent Lenders, and Jens Schmitt. 2016. Secure Motion Verification using the Doppler Effect. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '16)*. ACM, Darmstadt, Germany, 135–145.

[22] Daniel Steinmetzer, Matthias Schulz, and Matthias Hollick. 2015. Lockpicking Physical Layer Key Exchange: Weak Adversary Models Invite the Thief. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '15)*. ACM, New York, USA.

[23] Peter F. Swaszek and Richard J. Hartnett. 2013. Spoof Detection Using Multiple COTS Receivers in Safety Critical Applications. In *International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ '13)*. Nashville, TN, USA, 2921–2930.

[24] Peter F. Swaszek and Richard J. Hartnett. 2014. A Multiple COTS Receiver GNSS Spoof Detector – Extensions. In *International Technical Meeting of The Institute of Navigation (ION '14)*. San Diego, CA, USA, 316–326.

[25] Peter F. Swaszek, Richard J. Hartnett, Matthew V. Kempe, and Gregory W. Johnson. 2013. Analysis of a Simple, Multi-Receiver GPS Spoof Detector. In *International Technical Meeting of The Institute of Navigation (ION '13)*. San Diego, CA, USA, 884–892.

[26] Nils Ole Tippenhauer, Christina Pöpper, Kasper B. Rasmussen, and Srdjan Čapkun. 2011. On the Requirements for Successful GPS Spoofing Attacks. In *ACM Conference on Computer and Communications Security (CCS '11)*. ACM, Chicago, IL, USA, 75–86.

[27] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Čapkun, and David Basin. 2014. Short Paper: Detection of GPS Spoofing Attacks in Power Grids. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '14)*. ACM, Oxford, United Kingdom, 99–104.

[28] Zhenghao Zhang, Matthew Trinkle, Lijun Qian, and Husheng Li. 2012. Quickest Detection of GPS Spoofing Attack. In *IEEE Military Communications Conference (MILCOM '12)*. IEEE, Orlando, FL, USA.