Multi-Receiver GPS Spoofing Detection: Error Models and Realization

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

Nils Ole Tippenhauer
Singapore University of Technology and Design
nils_tippenhauer
@sutd.edu.sg

Christina Pöpper
New York University
Abu Dhabi
christina.poepper@nyu.edu

ABSTRACT

Spoofing is a serious threat to the widespread use of Global Navigation Satellite Systems (GNSSs) such as GPS and can be expected to play an important role in the security of many future IoT systems that rely on time, location, or navigation information. In this paper, we focus on the technique of multi-receiver GPS spoofing detection, so far only proposed theoretically. This technique promises to detect malicious spoofing signals by making use of the reported positions of several GPS receivers deployed in a fixed constellation.

We scrutinize the assumptions of prior work, in particular the error models, and investigate how these models and their results can be improved due to the correlation of errors at co-located receiver positions. We show that by leveraging spatial noise correlations, the false acceptance rate of the countermeasure can be improved while preserving the sensitivity to attacks. As a result, receivers can be placed significantly closer together than previously expected, which broadens the applicability of the countermeasure. Based on theoretical and practical investigations, we build the first realization of a multi-receiver countermeasure and experimentally evaluate its performance both in authentic and in spoofing scenarios.

CCS Concepts

•**Security and privacy** → *Mobile and wireless security;*
•**Information systems** → Global positioning systems;

Keywords

GPS, spoofing, countermeasure, localization security

1. INTRODUCTION

In recent years, the Global Positioning System (GPS) has become a ubiquitous source of location, time, and navigation information for devices such as navigation units, mobile phones, industrial control systems, financial trading platforms, trains, ships, and ankle bracelets for criminals. Localization services such as GPS are also expected to play an important role in the context of the upcoming Internet of Things (IoT) and cyber-physical systems as they often involve mobile or time-dependent components, e. g., for autonomous driving. Unfortunately, Global Navigation Satellite Systems (GNSSs) are susceptible to *spoofing* attacks, in which a malicious transmitter emits manipulated signals imitating real satellites. A spoofing attack can cause a victim's GNSS receiver to compute a wrong location and/or time solution. As a result, an attacker may remotely inject fake data into security- and safety-relevant systems.

In response to this threat, increasingly sophisticated methods for spoofing detection have been developed and were analyzed to enable the real-time identification of ongoing spoofing attacks, e. g., [1,2,5,8,12–14,16,20–22]. These countermeasures can be categorized in two classes. The first set of countermeasures is based on receiver observables [12, 33] such as the number of visible satellites, clock and date information, received signal strength measurements from the satellites, and verification of digital signatures (if available). In [8], these countermeasures are classified as *data-bit level* detection techniques. The second type of countermeasures focuses on the *signal-processing level.* These countermeasures require custom receivers with elaborate signal processing techniques and enhanced hardware. With custom receivers, spoofing attacks can be detected, e. g., by estimating the angle-of-arrival of navigation signals [13], their carrier phases [20, 21], random antenna motion [14, 22], or automatic gain control on the radio frontend [1].

However, the attacker model used in many of these countermeasures considers single-antenna attackers that may not make use of elaborate signal processing and mixing techniques. We argue that an attacker with, e. g., an adaptable GPS simulator, can generate spoofing signals with arbitrary precision in data and signal characteristics such as the imitation of satellite constellations, transmission power, and other physical-layer characteristics. In addition, public GPS data is not protected by signatures, so an equipped attacker can also spoof the data content of the navigation messages.

We therefore advocate the use of a detection measure that leverage signal properties which are *impossible* to spoof correctly for nearby or terrestrial attackers. In this work, we focus on *multi(ple)-receiver GPS spoofing detection* [29] and perform its first practical evaluation. The detection is based on the location reported by two or more commercial-off-the-shelf (COTS) receivers mounted in a fixed formation. During an attack, a single-antenna attacker would spoof receivers to the exact same position solution, which can be

ACSAC '16, December 05 - 09, 2016, Los Angeles, CA, USA

ISBN 978-1-4503-4771-6/16/12. . . $15.00

DOI: http://dx.doi.org/10.1145/2991079.2991092

used to detect the attack. It has been shown that—from a certain number of receivers onwards—even a multi-antenna attacker cannot succeed in maintaining a fixed formation, respectively the relative distances, during the attack [29]. This leads to the fact that this detection technique is principally unspoofable as long as the attacker signals are received at all receiving devices (which is hard to prevent if the receivers are positioned close enough together).

A benefit of the multi-receiver detection mechanism is that it can be realized with COTS receivers without changes to the GPS infrastructure. The performance of the countermeasure is expected to depend on the chosen distances between the receivers, as in practice the location is influenced by noise. Based on a rough estimation of required distances, the authors of [29] suggested application settings such as cargo ships or trucks. Following theoretic investigations [5, 26], performance values for distances between 10 m to 50 m were derived analytically. As a result, the countermeasure does not seem suitable for most moving vehicles, but can only be applicable for large stationary installations.

To the best of our knowledge, the multi-receiver countermeasure has not been practically investigated and validated against real spoofing setups. In this work, we analyze the models used in [5] and [26] and show that (*i*) nearby real-world GPS receivers have correlated noise on their location estimates, (*ii*) previous error models over-estimate the location error in the attack case, and (*iii*) considering correlated errors can drastically reduces the expected false detection rate of the countermeasure while preserving the sensitivity to attacks. As a result, a distance of 3 m to 5 m can be expected to be sufficient (in contrast to 10 m to 50 m) as we show by simulations and experiments (for the same performance criteria).

We validate our theoretical predictions using an experimental setup with several receivers and a GPS satellite signal generator as spoofer, and we provide in-depth insights on parameters and setups for a reliable operation of the countermeasure. In summary, our work contains the following contributions:

- We extend previous theoretical work on multi-receiver spoofing countermeasures by modeling distance-related errors with the goal to differentiate between error distributions during normal operation and under attack.
- We experimentally provide estimates of practical localization noise in normal operation as well as in spoofing scenarios showing that the noise is spatially correlated.
- We leverage these insights to show that the multi-receiver spoofing countermeasures can be used reliably in formations which are almost an order of magnitude smaller than previously proposed (area of formation).
- We experimentally demonstrate that our countermeasure prototype can reliably detect real spoofing signals utilizing four receivers in a mutual distance of 5 m.

Our investigations and results demonstrate the applicability of the countermeasure and will help users or engineers to set it up accordingly. The countermeasure may be used in static setups, e. g., in factories to prevent time spoofing, as well as in mobile settings, e. g., on vehicles such as trucks or airplanes to prevent location and navigation spoofing. As an extension, we also envisage its use for highly mobile setups such as drone formations. The evaluation framework can serve as baseline for further investigations.

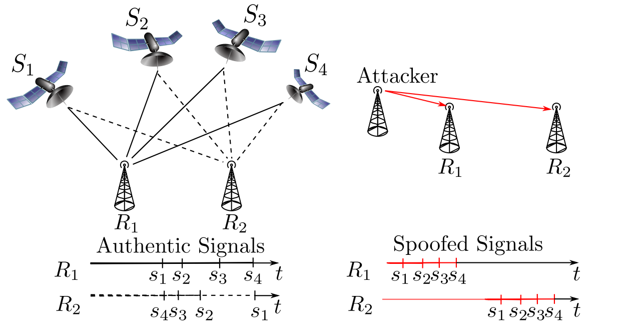

Figure 1: ToA of satellite signals. Left: The relative ToA determines the localization result, exemplary for two receivers and four satellites. Right: An attacker generates spoofed signals for all four satellites with some relative ToA. At each victim, the spoofed signals have identical relative ToAs, but are overall offset due to victims' distances to the attacker.

2. GPS SPOOFING AND DETECTION

We start by briefly introducing GPS, errors in GPS, the considered attacker model, and the concept of multi-receiver spoofing detection. In general, the spoofing attacks and our countermeasure should apply to any GNSS. In the context of this work, we focus on GPS as its receivers and signal generation devices are readily available. For a detailed description of GPS we refer to [6, 11, 25].

2.1 GPS and GPS Spoofing

GPS is based on measurements of the time of arrival (ToA) of signals sent by four or more satellites from medium earth orbit. Based on the ToA of the individual satellite signals, a pseudo-distance to each satellite can be computed. Based on these pseudo-distances and the periodically embedded satellite positions, a receiver can use multilateration to find its local position and time (see Figure 1). The ToA measurement for each signal is affected by a range of errors, which we discuss in more detail in Section 2.2.

GPS provides two types of signals: (*i*) public GPS signals that can be received (and generated) by everyone with suitable equipment, and (*ii*) military GPS signals that are protected by (at least) secret spreading codes. In this work, we focus on attacks and countermeasures for civilian signals, but we note that the underlying spoofing problem of falsifying ToA of signals cannot be fully prevented by secret spreading codes alone.

Spoofing attacks are based on the broadcast of false GNSS signals in order to change the localization and time result of a victim [7, 26, 29]. In this work, we focus on spoofing attacks that target the ToA of signals and use otherwise the same data content as real signals. These signals can be generated by replaying previously recorded GPS signals or by using a satellite simulator. Attacks that also change the data content of the signals are discussed in [15].

2.2 GPS Error Sources

As GPS errors take a critical role in our countermeasure, we discuss them in more detail. While the GPS localization accuracy is sufficient to estimate a position within a few meters radius, the system suffers under errors affecting the deviation from the actual location. Due to the signal gener-

Table 1: L1 C/A Error Sources and UERE [6], [18]

Type	Error Source	Total [m]
Satellite	Ephemerides data	2.1
	Satellite clock	2.1
Channel	Ionosphere	4.0
	Troposphere	0.7
	Multipath	1.4
Receiver	Measurement	0.5
UERE [m]		**5.3**

ation in space and a travel distance of more than 20,000 km, GPS signals are affected by various error sources that can be categorized into three groups [6]: satellite, propagation medium, and receiver errors (see Table 1).

Satellite errors. Errors can arise from the satellite itself in regard to clock biases and orbital drifts. For error mitigation the adjustable ephemeris data sent out by each satellite include an estimation of the error characteristics.

Signal propagation errors. Environmental effects such as ionospheric or tropospheric refractions are dependent on the physical conditions on the propagation path. When GPS signals reach the earth's surface they are potentially reflected at obstacles leading to multipath effects that decrease the signal-to-noise ratio (SNR).

Receiver errors. In addition to normal receiver noise (e. g., thermal noise in components), the receiver can suffer under clock biases and center phase variations.

The combined error of all presented sources is summarized in the User Equivalent Range Error (UERE) [25, p. 298]. A quantifying analysis is conducted in [18]; its results in terms of total error are given in Table 1. The given values are based on a 1σ-probability level relating to the deviation in meter. In order to evaluate the quality of the position solution, error contributions can be estimated and periodically embedded in the navigation message [18].

2.3 System and Attacker Model

We consider the following attacker model. The goal of the attacker is to change the localization or time result of one or more victims. The attacker is capable of generating fake GPS signals with the same signal characteristics as authentic GPS signals. We distinguish between two scenarios for the attacker antennas: (*i*) a single-antenna attacker and (*ii*) a multi-antenna attacker. In the first case, the attacker is restricted to a single-antenna setup, where all spoofing signals are sent from the same source. In the second case, the attacker can utilize multiple antennas to have more freedom for the transmission of signals and can send potentially different signals from various locations.

In this work, we assume that all receivers obtain signals from the same sources, i. e., receivers are not shielded from the reception of signals seen by other receivers. We generalize our approach to protect against a single-antenna attacker as well as a multiple-antenna attacker. As shown in related work [29, 32], a single-antenna attacker can successfully spoof individual victims to an arbitrary location and time by sending spoofing signals that have constant relative ToA with respect to each other, independently of the location of the receiver (see Figure 1). As a result, multiple receivers in range of the attacker all compute the same localization result (with minor time differences due to their respective distances to the attacker).

For the multi-antenna adversary model, spoofing individual position solutions for less than four receivers becomes theoretically possible. We would like to stress that such an attacker was only theoretically proposed in [29], but no practical implementations are known. Theoretically, an attacker can generate and synchronize its antennas to adjust the ToA of signals at each victim receiver. Practically, implementing such an attack successfully is expected to be very challenging, as there are tight constraints on signal power and alignment [29]. We discuss the resilience of our countermeasure to a multi-antenna attack in Section 8.

The problem of taking over an established lock, i. e., the problem of taking over a victim's fix to authentic GPS signals, is out of scope of this work. In order to induce a new fix onto the spoofed signals (i. e., to replace legitimate signals), an attacker needs to force a lock loss of the establish fix, e. g., by prior jamming or high spoofing power [31]. Since our countermeasure is based on the position information, we can give the attacker the power to overcome prominent signal-based countermeasures such as RAIM [12], signal power [33], or angle-of-arrival [13] discrimination.

2.4 Multi-Receiver Spoofing Detection

Conceptually, a multi-receiver spoofing countermeasure detects GPS spoofing attacks based on the location reported by two (or more) COTS receivers at fixed known positions. The receivers periodically compare their distances of the calculated locations, e. g., using wired connections. In case of authentic signals, the computed distances are expected to be rather stable and close to the physical distances of the given formation. In case of an attack, the computed distances will shrink to values close to zero, as the receivers would report the same location during a single-antenna spoofing attack. Two receivers in appropriate distance to each other are sufficient to detect single-antenna attacks; a multi-receiver countermeasure with at least four receivers can also detect attacks from multiple locations (Section 8). As it only uses the localization result, a beneficial property of this countermeasure is that it does not require any modification of standard COTS receivers.

In this work, we provide detailed theoretical models and experimental validation to find the required distances and detection thresholds for bringing the multi-receiver countermeasure to practice (see Figure 2). Being able to deploy the receivers closer together has two advantages: (*i*) it broadens the number of possible application scenarios and (*ii*) it makes attacks based on individual spoofing (separate signals for each receiver and shielding other receivers from reception) harder to achieve.

3. PRACTICAL SPOOFING DETECTION

We now introduce our detection mechanism and argue that its performance depends on (*i*) the physical formation of the receivers, and (*ii*) on the position solution noise experienced by the receivers. We then discuss both factors in more detail. In particular, we predict that authentic signals and attacker signals have different noise characteristics, which can be used to improve the performance of the countermeasure.

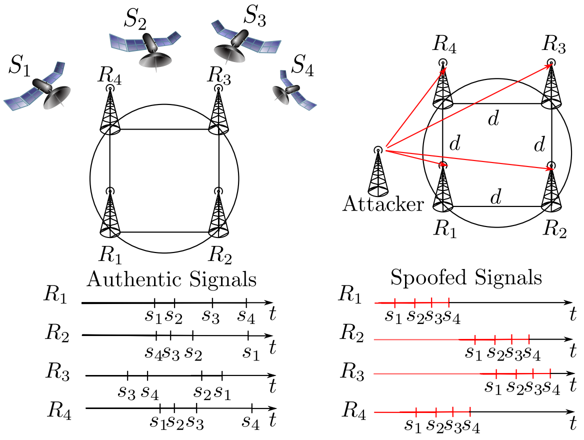

Figure 2: Multi-receiver spoofing detection system set up in a fixed formation. All receivers periodically compare their mutual distances. Normal operation: Distances will be constant (with minor variations due to noise). Spoofing: Locations will coincide (again, with some noise).

3.1 Detection Mechanism

We assume that two (or more) GPS receivers are set up in a known static formation. All receivers are continuously obtaining their location via GPS, and a central controller uses the locations to detect spoofing cases. Basically, our detection mechanism compares the reported receiver locations in order to perform a binary classification into authentic/spoofed situations. This decision is probabilistic and considers the predefined receiver formation, its fixed relative distances, and the noise characteristics of the receivers. The detection model is based on work in [26–28]; it distinguishes between two potential detection outcomes based on the presence of an attack. The considered hypotheses H_0 and H_1 are:

H_0: No spoofing occurred.
H_1: Spoofing is performed.

The decision making is based on the preservation of known receiver distances. If the system detects significant anomalies, the test should indicate a spoofing attack. In contrast to the absolute positions in [27], our detection is based on *relative distances* between all pairs of receivers. The mechanism is a function of the reported position information and a comparison against a decision threshold λ to be defined. The adapted test can be formally expressed as:

$$f\left(\mathrm{P}_1, \ldots, \mathrm{P}_m\right) \underset{\mathrm{H}_1}{\overset{\mathrm{H}_0}{\gtrless}} \lambda, \tag{1}$$

where m denotes the number of receivers and their respective position is P_i, $i \in \{1, \ldots, m\}$ and $f()$ is a function on the distances. Each position P_i consists of a latitude and a longitude component. The position also contains altitude information, which is neglected here due to the low precision of GPS altitude. To simplify the discussion, we assume that for our countermeasure all receivers are placed at approximately the same height. We analyze possible functions (e. g., minimal, maximal, or weight-based approaches) and their effects on attack detection in more detail in Appendix A.

Since we only consider the relative distances between receivers, we can detail (1) to directly take the set of distances $d_{i,j}$ as input:

$$f(d_{i,j}) := f\left(\left\{d_{i,j}\right\}_{i<j}^{1\leq i,j\leq m}\right) \underset{\mathrm{H}_1}{\overset{\mathrm{H}_0}{\gtrless}} \lambda. \tag{2}$$

If the result of function f on the distances between the receivers falls *below* the threshold λ, the test indicates a spoofing attack (H_1). However, if the result is *above* the threshold λ, the test decides for no spoofing (H_0). Notably, since the absolute positions contained in (1) are not crucial for our spoofing detection, there is no information loss from (1) to (2). Hence, we can safely use (2), which contains all distances clearly defining the underlying formation.

On the basis of (2), we can define two important probabilities in regard to the detection and the false alarm ratio. The probability of detection p_d describes the chance that an actual spoofing attack is indeed detected. Thus, the result of f needs to be *below* the threshold λ:

$$p_\mathrm{d} = \Pr\{f\left(d_{i,j}\right) < \lambda \mid \mathrm{H}_1\},$$

with $1 \leq i < j \leq m$. On the other hand, the false alarm probability p_fa describes the chance of triggered alarms when no spoofing occurs. The result of f needs to be *above* the threshold λ, which can be described as:

$$p_\mathrm{fa} = \Pr\{f\left(d_{i,j}\right) < \lambda \mid \mathrm{H}_0\}.$$

Considering both equations, we need to optimize λ with the purpose of achieving high detection rates while maintaining a low probability of false alarms. If the receivers were to obtain their position solution without any error, they could perfectly detect spoofing attacks even if their mutual distances are very small (e. g., a few centimeters). Unfortunately, GPS receivers have a non-negligible position-solution error in practice (as discussed in Section 2.2).

3.2 Countermeasure Formation

The general receiver formation for our countermeasure considers a virtual center, around which the receivers are placed. In particular, receivers are placed equidistantly on the edge of a virtual circle with the aforementioned center. With this constellation, a multi-receiver setup can be realized in a compact way and the setup is extendable while keeping the same radius of the circle.

We denote the number of receivers as m and the radius of the circle is defined as r, while the resulting distance between neighbors is d. For instance, for $m = 2$ each receiver is placed on the opposing side of the circle. As a result, for a given radius r the distance becomes $d = 2r$. For $m = 3$ we obtain a triangle and for $m = 4$ the formation becomes a square with equal edge lengths. The relationship between m, r, and d can be formulated as:

$$d = 2r \cdot \sin\left(\frac{2\pi}{2m}\right).$$

Notably, the more receivers we use, the more different distances between all possible receiver pairs are obtained and are used by the function f. While for $m = 2$ we only have one single distance, for $m = 4$ we already have six (partially dependent) distances. For the actual detection system, we mostly consider a setup with $m = 4$ receivers. That is the least amount of receivers required while protecting against the multiple-antenna attacker [29].

3.3 Leveraging Environmental Errors

The noise of the position solution experienced by the receivers is a determining factor for the performance of our countermeasure. We introduced general GPS errors in Section 2.2, and we now apply the general error model to our spoofing scenario.

In prior work [26], the position solution error (UERE) was modeled to be identical for authentic and spoofing signals. We now argue that this is not the case in practice, and a more realistic model can improve the countermeasure performance. On closer inspection, the UERE is a composition of two components. The satellite system-intrinsic User Range Error (URE) includes environmental errors, whereas the User Equipment Error (UEE) is caused by the receiver design [30]. This is particularly relevant for two reasons:

(a) We claim that the environmental errors are *to a certain degree* location-specific—i. e., several receivers at the same location will experience correlated environmental errors. The intuition is that this will make our countermeasure more reliable in normal operating conditions, as position shifts are partially correlated.

(b) During a location spoofing attack, an attacker has potentially large influence on the environmental error, but this error will be roughly the same for multiple victims. In particular, the attacker has control over the ephemerides data and satellite clock offsets in the spoofing signals. In addition, the attacker is comparably close to the receivers, so that multipath effects are greatly reduced. As a result, our intuition is that in an attack scenario, the location differences of several victims are *less noisy* than under normal operation (i. e., their UERE is expected to develop a stronger correlation).

In order to get a better understanding of the impact of correlation, we have a look at the calculation of a (noised) 1D distance:

$$d\left(\mathrm{P}_i + n_i, \mathrm{P}_j + n_j\right) = d\left(\mathrm{P}_i, \mathrm{P}_j\right) + n_i - n_j,$$

where n_i and n_j is the noise for P_i and P_j, respectively. The actual distance $d\left(\mathrm{P}_i, \mathrm{P}_j\right)$ is impacted by the combined noise $n_i - n_j$. If both noise sources are independent, there is no tendency on how the calculated (noised) distance will behave. However, when the sources are correlated they will compensate each other to a certain degree, which can be calculated by:

$$\sigma_d = \sqrt{\sigma_i^2 + \sigma_j^2 - 2\rho_{i,j}\sigma_i\sigma_j} \overset{\sigma_i=\sigma_j}{=} \sqrt{2}\sigma \cdot \sqrt{1-\rho_{i,j}},$$

where σ_d is the standard deviation of the distance, σ_i and σ_j the standard deviation of P_i and P_j (assumed to be roughly equal), and ρ is the Pearson correlation coefficient given as:

$$\rho_{X,Y} = \frac{\mathrm{cov}(X,Y)}{\sigma_X \sigma_Y}, \qquad (3)$$

with X and Y being two datasets of the same length. In particular, the correlation coefficient is a measure of linear dependence between these two datasets. A value of 0 indicates no correlation, whereas +1 and −1 represent total positive, respectively total negative, correlation. As a result, the stronger the correlation between the experienced noise, the less *noisy* are the mutual distances. Similar considerations apply to the cases of 2D latitude and longitude components as well as multidimensional points.

3.4 Error Modeling and Distribution

In addition to our model of the receiver formation and the general error sources, we also need a more detailed model to describe the error distribution. Based on those models, we can perform simulations to determine suitable distances between the receivers and optimal decision thresholds. According to the GPS performance standard [30], we assume that the receiver's position errors are Gaussian distributed in latitude and longitude. If mean and standard deviation for each direction are known, we can compute probability functions and make predictions for the error distribution.

However, our scheme is based on relative distances and thus combines both directions. Following [26], we assume that *distance-related* errors are Gaussian distributed with approximately the same standard deviation in latitude and longitude. We also assume that the correlation between changes in each direction exhibits similar characteristics. By making these simplifications, the error distribution of the Euclidean distance of *two* 2D-Gaussian distributed points can be formulated in a closed form. Notably, we use the distance projected on a two-dimensional plane neglecting the curvature of the earth for small distances.

The resulting mathematical model, which describes the distribution of the distances between *one* 2D-Gaussian distributed point and a *fixed point*, is a Rician distribution. We extend the model by replacing the fixed point with a second 2D-Gaussian distributed point. If the standard deviation and the correlation are the same, the adjusted distribution maintains its Rician property.

The probability density function (PDF) for a Rician distribution is given by:

$$f(x) = \begin{cases} \frac{x}{\sigma^2} e^{-\frac{x^2+s^2}{2\sigma^2}} I_0\left(\frac{xs}{\sigma^2}\right), & x > 0, \\ 0, & x \leq 0, \end{cases} \qquad (4)$$

with noncentrality parameter s reflecting the distance to the center and scale parameter σ as the standard deviation of the Gaussian distribution. I_0 denotes the zero-order modified Bessel function of the first kind.

The cumulative distribution function (CDF) is defined as:

$$F(x) = \begin{cases} 1 - Q_1\left(\frac{s}{\sigma}, \frac{x}{\sigma}\right), & x > 0, \\ 0, & x \leq 0, \end{cases} \qquad (5)$$

where Q_1 is the first order Marcum Q-function.

Due to our adaptions and the addition of a second Gaussian distributed point, the noncentrality parameter s and the scale parameter σ of the resulting distribution are not equivalent to the distance nor the standard deviation (but are very close to the actual scales).

For the special case of *two* 2D-Gaussian distributed points with the *same center*, s becomes 0. As a result, a Rayleigh distribution is obtained, which is only dependent on the scale parameter σ.

Thus, the PDF simplifies as follows:

$$f(x) = \begin{cases} \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, & x > 0, \\ 0, & x \leq 0. \end{cases} \qquad (6)$$

The corresponding Rayleigh CDF is:

$$F(x) = \begin{cases} 1 - e^{-\frac{x^2}{2\sigma^2}}, & x > 0, \\ 0, & x \leq 0. \end{cases} \qquad (7)$$

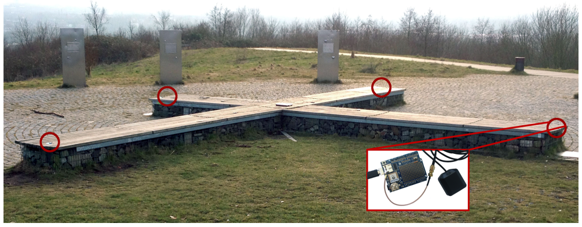

Figure 3: Setup of a central laptop connecting four receivers positioned on each end of a wooden bench (red circles).

Table 2: Receiver Placement and Relative Distances

Rec.	Side	d_C[m]	d_{R1}[m]	d_{R2}[m]	d_{R3}[m]	d_{R4}[m]
R1	East	7	-	8.06	13.00	9.90
R2	South	4	8.06	-	7.21	11.00
R3	West	6	13.00	7.21	-	9.22
R4	North	7	9.90	11.00	9.22	-

In order to evaluate the CDFs, we first need to determine the parameters s and σ. However, the parameter estimation for both distributions is a non-trivial problem in mathematical analysis. Therefore, we use the numeric solution calculated by the distribution fitting function `fitdist` provided by MATLAB. Note that these error models are not taking correlations into consideration. We therefore expect distances to be more dense around the mean and that our model is a pessimistic approximation.

4. ERROR FOR AUTHENTIC SIGNALS

In this section, we present a series of experiments we conducted to obtain real-world GPS localization errors. The experiments were executed with a set of co-located receivers, which allows us to determine temporal and spatial correlations between the localization errors. As a result, we were able to identify suitable parameters for our spoofing detection mechanism.

4.1 Experimental Setup

For our experimental setup we deployed four standalone Arduino UNOs, rev. 3. Each Arduino is extended with a GPS logger shield including a GPS module in order to process incoming GPS signals. Furthermore, an external active antenna with an additional 28 dB gain is coupled with each GPS shield. The external antenna not only provides more stable solutions but also increases the flexibility of the setup due to an additional 5 m cable length. The combination of these components is hereafter referred to as a *receiver*.

For the initial measurements, four receivers were arranged in a cross-like formation with side lengths of approx. 4 m to 7 m as depicted in Figure 3. Each receiver generates NMEA 0183 data sentences from the received signals. The data is constantly stored on a controlling laptop connected via USB, which also powers the receivers. With a total of four receivers, we obtain six distinct distances matching each device with each other. For the specific relative distances we refer to Table 2, in which d_C is the distance to the center (as measured by hand), and d_{Ri} is the calculated distance to the other receivers. The overall formation is aligned to the cardinal directions North, South, East, and West; it is illustrated in the position map shown in Figure 4, which was set up for approx. 2.5 h at a place with clear line of sight to the sky.

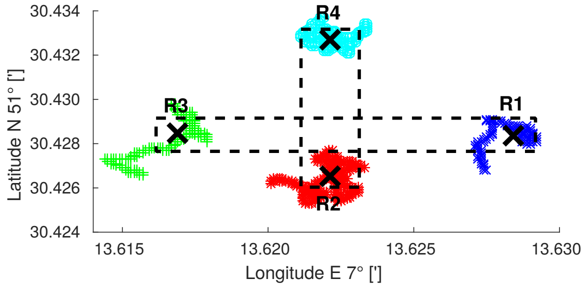

Figure 4: Illustration of the receiver placement including reported positions, where "X" indicates the mean position over the measurement duration.

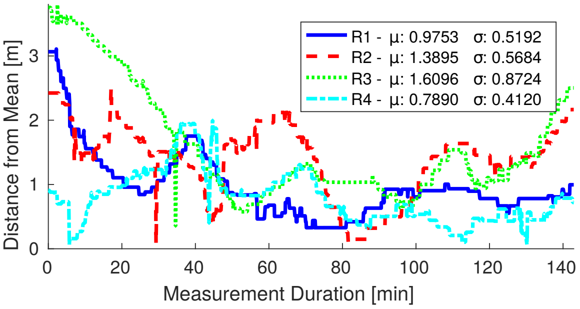

Figure 5: The calculated distances between the reported positions and their respective mean (close to the actual positions).

4.2 Measurement Analysis

We next evaluate the recorded data and derive suitable parameters for the subsequent simulations. The position map indicates that the reported positions are scattered around four points, which in our case closely reflect the actual receiver placement. However, the deviation from the interim positions to the actual placement can reach several meters. Figure 5 shows the development of these distances over the course of the experiment. While the average distance error μ ranges from approx. 0.79 m for R4 to 1.61 m for R3, the standard deviation σ varies between approx. 0.41 m for R4 and 0.87 m for R3. In comparison to the values reported in Table 1, the positions measured during the experiment are very stable.

Since our spoofing detection mechanism takes the relative distances into account, we calculate the distances between the reported positions. The results including the average distances μ are depicted in Figure 6. The histogram uses a bin width of 1 m. The average distances are all within 1 m from the actual distances noted in Table 2. In Section 3.4, we concluded that the underlying distribution is Rician. We try to align the respective PDF from (4) with the measurements. The solid (red) line represents a normalized best fit based on a Rician distribution. The gap between the theoretical distribution and the recorded data is mainly due to

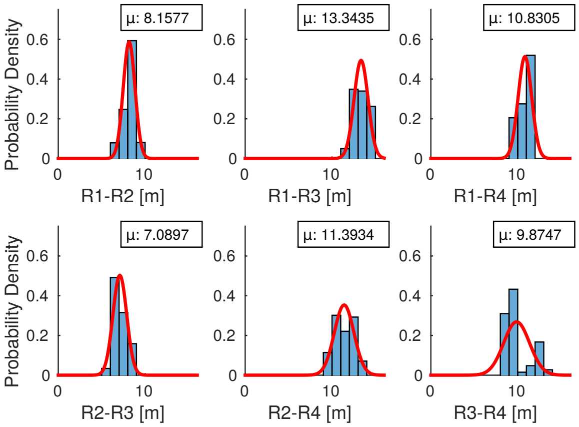

Figure 6: The distribution of calculated distances between each pair of receivers, with fitted Rician distributions.

Table 3: Error Distribution Parameters

Distance	s	σ	d_{99}[m]	ρ_{LAT}	ρ_{LON}
R1-R2	8.129	0.681	6.576	0.045	0.399
R1-R3	13.319	0.809	11.464	0.490	0.779
R1-R4	10.802	0.779	9.020	0.509	0.472
R2-R3	7.045	0.796	5.244	0.721	0.654
R2-R4	11.337	1.132	8.768	0.511	0.462
R3-R4	9.760	1.495	6.423	0.351	0.719

correlations of position errors (distances tend to be smaller) and limitations of the measurement setup. In other setups, we obtain results that fit the Rician distribution better (Appendix B). The parameters of the distributions are included in Table 3. In particular, the noncentrality parameter s closely reflects the average distance μ, whereas the scale parameter σ reflects the standard deviation of the dataset.

As an illustrative example, we focus on a single distance. Considering the CDF of the Rician distribution from (5), we are able to calculate the probability that a certain threshold λ is exceeded. In particular, we can determine the point at which 1 % of the distribution is accumulated. According to the CDF, we expect that 99 % of the distances exceed this fix point such that

$$\Pr\{d \leq d_{99}\} = 1 - Q_1\left(\frac{s}{\sigma}, \frac{d_{99}}{\sigma}\right),$$

where d_{99} represents the distance that is *shorter* than 99 % of all distances. With this equation we can calculate thresholds that belong to different probabilities. The distances corresponding to the 99 % threshold for each pair of co-located receivers are shown in Table 3. For instance, the distance R3-R4 ($\mu = 9.875$ m) is expected to be below 6.423 m in only 1 % of the cases and is calculated to be maintained 99 % of the times, which is approx. 3.4 m less than the actual distance based on the initial measurements.

A further aspect of our measurement analysis is how position changes correlate spatially. Since we assumed that the system-intrinsic URE is an environment-dependent error, we expect to detect a certain correlation between the position deviations for co-located receivers. To identify the extent of correlation, we compute Pearson's correlation coefficient ρ from (3) between the reported positions. The coefficients for our measurements are listed in Table 3. For better clarity ρ is partitioned in a latitude and a longitude component. We recognize a positive correlation. Even though the amount of correlation differs between the respective receivers due to noise effects (ρ_{LAT} for R1-R2 is an outlier), the magnitude of correlation is considerable and throughout positive.

Conclusion for Authentic Signals. In conclusion, the localization precision of the utilized COTS receivers is within typical standard deviations of $\sigma \approx 0.5, \ldots, 3$. The correlation between the position shifts is significantly positive and stabilizes at $\rho \approx 0.4, \ldots, 0.6$ for long-term measurements. To validate our findings, we conducted further experiments in different environments between August 2015 and May 2016, which are discussed in Appendix B.

5. ERROR FOR SPOOFED SIGNALS

In the previous section, we investigated the localization error for authentic signals. We now present experimental results on the localization error for spoofed signals, using the same receivers as in the previous experiment.

5.1 Experimental Setup

In our measurement setup, the spoofing attack is realized via a GPS signal simulator that is capable of generating arbitrary civilian GPS signals (LabSat 3). These signals can be composed with attacker-chosen parameters such as signal power or position solution. With the supplied software tools, we are able to generate scenarios, which emulate similar conditions as were present during our measurements for the authentic signals. In particular, the simulator uses the ephemeris data for that specific place and time period.

Since the satellite simulator aggregates a mix of satellite signals into a signal that is resolvable to one specific location, we choose the coordinates of one of the receivers from our initial measurements as the spoofed position. The spoofing signal was sent wirelessly during limited time periods. Thus, all receivers obtained the same signal at similar power levels. In order to imitate the authentic scenario as closely as possible, we adapted the external antennas inclination to the new angles-of-arrival due to the ground-level simulator. A sophisticated attacker is assumed to send out signals from higher positions avoiding the antenna adjustments. During the (indoor) experiment, the receivers were shielded from real GPS signals in order to acquire a quick fix to the spoofing signals as well as to prevent signal leakages to the outside. In less than one minute, the receivers locked onto the spoofing signal and kept tuning to process all available satellites from the signal. The spoofing attack was performed with the same GPS time and for the same duration as for the outdoor measurement.

5.2 Measurement Analysis

The analysis of the recorded measurements reveals the following insights. All receivers report positions, which closely reflect the preconfigured location for which the GPS signals were generated. Within the given precision, the mean of the reported positions is the same for all receivers. Notably, this is independent of the actual positioning or formation.

All four traces exhibit similar patterns over the course of the experiment. Across all receivers, we can recognize periods in which the distance to the mean positions increases, respectively decreases as shown in Figure 7. In these periods,

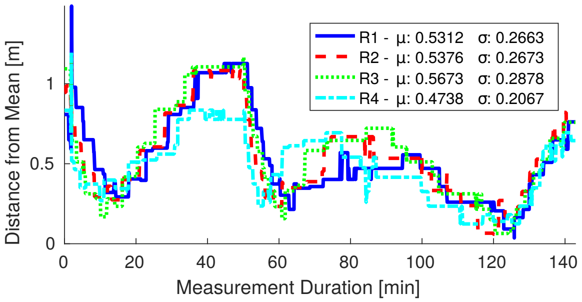

Figure 7: The progression of the distance to the respective mean reveals a close spatial correlation.

we assume that the simulator imitates the changing signal quality at that location during that time by adjusting the impact of system-intrinsic UREs. The average distance μ from the means varies between approx. 0.47 m for R4 and 0.57 m for R3, whereas the standard deviation σ ranges from approx. 0.21 m for R4 to 0.29 m for R3. In comparison to the outdoor measurements, both quantities are roughly halved. Thus, the reported positions are less affected by errors.

In consideration of the relative distances, the resulting distribution is depicted in Figure 8. To increase the resolution, the applied bin width is refined to 0.1 m. As analyzed in Section 3.4, the distances follow a Rayleigh distribution, for which the noncentrality parameter s becomes 0 due to overlapping center points. The solid (red) curve represents the best fit on the basis of the respective PDF from (6). Note again that, due to correlations between the position errors, distances tend to be smaller than the distribution suggest. Measurement limitations prevent a perfect fit with the distribution, see Table 4 for the determining scale factor σ.

According to Figure 8, the relations involving R4 feature less distinct peaks such that the red curve drops slower towards the right side. Taking the CDF of the Rayleigh distribution from (5) into consideration, we can determine the probability that a certain threshold λ is exceeded. This can be described as

$$\Pr\{d > d_{99}\} = e^{-\frac{{d_{99}}^2}{2\sigma^2}},$$

where d_{99} is expected to be *larger* than 99 % of the distances. In contrast to the authentic measurements, the role of d_{99} is swapped representing a threshold towards the upper limit. For each receiver pair, the value of d_{99} is stated in Table 4. Due to the very small deviations in the reported position solution, the calculated thresholds are less than 1 m. Even for the most diversified distance R1-R4, the relative distance exceeds approx. 0.655 m in only 1 % of the cases.

Finally, we evaluate the correlation between position deviations on the basis of the correlation coefficient. The calculated coefficients for latitude and longitude directions are included in Table 4. Across all receivers, the values illustrate a strong positive correlation with a minimal coefficient of 0.870 for R1-R4 and a maximal coefficient of 0.986 for R2-R3, both in latitude direction. Compared to the correlation for the outdoor measurements, the correlation in the spoofing scenario is constantly higher. Each receiver is faced with the same GPS signals and thus the same embedded system-intrinsic errors. Receiver-specific errors only take a minor role, which is reflected by high coefficients close to 1.

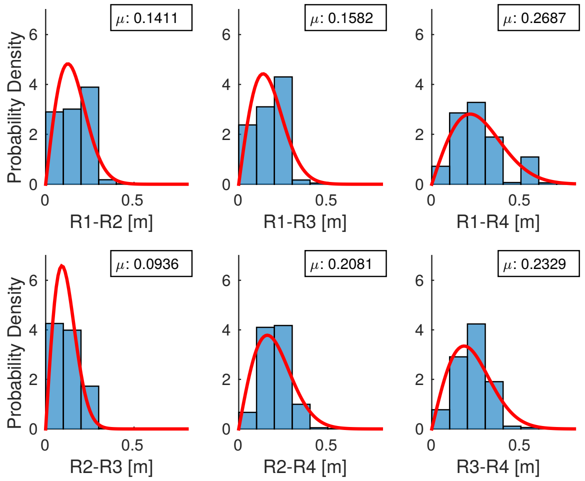

Figure 8: The distribution of relative distances under spoofing.

Table 4: Error Distribution Parameters - Spoofing

Distance	σ	d_{99}[m]	ρ_{LAT}	ρ_{LON}
R1-R2	0.126	0.381	0.970	0.932
R1-R3	0.137	0.416	0.975	0.916
R1-R4	0.216	0.655	0.870	0.898
R2-R3	0.092	0.279	0.986	0.969
R2-R4	0.160	0.487	0.932	0.964
R3-R4	0.181	0.550	0.927	0.959

Conclusion for Spoofed Signals. In conclusion, the receivers maintain a position accuracy of $\sigma \approx 0.2, \ldots, 1$. The typical correlation coefficient for position shifts is strong positive in the range of $\rho \approx 0.5, \ldots, 0.9$. In comparison to the performance for authentic signals, the position solutions are more stable and the correlation is higher. Results from additional spoofing experiments investigating the impact of different environments are presented in Appendix B.

6. COUNTERMEASURE EVALUATION

We now use the noise parameter ranges learned from our real-world experiments to instantiate the detection mechanism and evaluate its performance through simulations.

6.1 Evaluation Metric

We developed a simulation framework using MATLAB in order to calculate the expected performance of different receiver positioning. In addition, the framework finds optimal decision thresholds λ with respect to corresponding detection probabilities p_{d} and false alarm probabilities p_{fa}.

Within the simulation framework, we pursue two goals: (i) Simulate the countermeasure for m receivers (we focus on $m = 4$) considering different distribution parameters including distance, standard deviation, and correlation. (ii) Evaluate different instantiations of the function f, which is the determining function in the decision mechanism (2). For the analysis with $m = 4$ receivers we chose a normalized majority voting, where longer distances (diagonal in a square) are more significant. The reasoning behind the selection is given in Appendix A.

Table 5: Simulation Parameter Sets

Case	σ_{legit}	ρ_{legit}	σ_{spoof}	ρ_{spoof}
1	4	0.5	2	0.5
2	2	0.5	1	0.5
3	1	0.5	1	0.5
4	1	0.5	1	0.7
5	1	0.5	0.5	0.9

Based on real-world measurements, we consider five different error models representing different scenarios and measurement environments, see Table 5. The first scenario considers high noise from our worst case measurements (Case 1). On the other hand, the fifth scenario includes the most stable position solutions that we measured (Case 5). The other scenarios are intermediate steps between the two extremes (Cases 2,3,4). Notably, the third scenario represents an error model for which authentic and spoofing signals suffer from the same extent of errors.

The simulation covers varying receiver distances given as the radius r, which is step-wise increased from 0 m to 15 m with a step size of 0.01 m. The amount of generated measurements is 10,000,000 for each receiver position and each simulation run. The standard deviation is modeled by Gaussian distributions and we use correlations between generated datasets.

As the first measure of performance, we consider equal error rates (EER), i. e.,

$$1 - p_{\text{d}} \overset{!}{=} p_{\text{fa}}. \tag{8}$$

In other words, our decision threshold λ is chosen in such a way that the probability of a false alarm p_{fa} is equal to the probability of a missed detection p_{d}. However, we notice that spoofing and non-spoofing scenarios are not equally distributed. In most cases, the receivers operate with authentic signals, whereas an actual attack is very unlikely. False alarms are generally more likely to occur than false detections and thus need to be weighted more than missed detections. The usage of the EER gives us a worst case estimation with a stronger focus on reliable detection; the receivers distances may be decreased further if we allow poorer detection probabilities. At the same time, missed detections typically incur a larger security risk than false detections. To account for these considerations, we later additionally report results individually for the probabilities of false alarms p_{fa} and missed detection p_{d}.

6.2 Simulation of the Countermeasure

We examine the detection performance of our detection mechanism for $m = 4$ receivers. The results under consideration of the noise scenarios from Table 5 are depicted in Figure 9. The required receiver distances differ substantially for each of the simulated cases. For example, a radius of approx. 11 m is needed for an EER of 10^{-6} in the worst measured scenario (Case 1). An EER of 10^{-6} equals only one triggered alarm on a sample size of 1,000,000 measurements under normal operation, whereas only one instance of spoofing remains undetected. For our best noise model the required radius is reduced to approx. 2 m (Case 5). The radii for the other scenarios vary from approx. 6 m (Case 2), and approx. 4 m (Case 3), to approx. 3.5 m (Case 4).

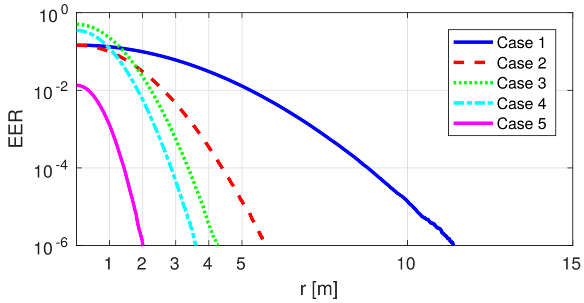

Figure 9: EER for different radii ($m = 4$).

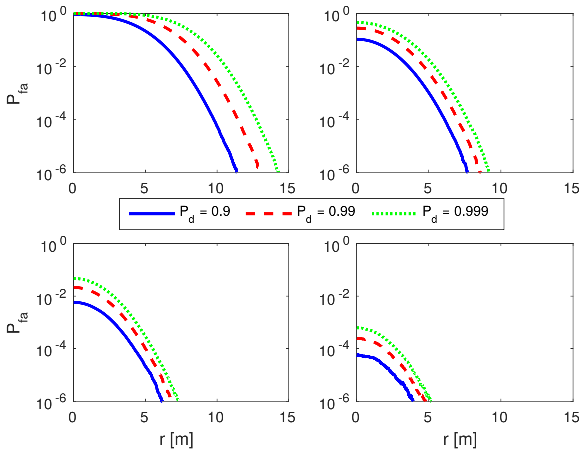

Figure 10: Detection performance ($m = 4$): without considering our proposed improvements (top left), considering correlation (top right), lower standard deviation under spoofing (bottom left), and the combination of both (bottom right).

To integrate our results with theoretic prior work [26–28], we take $\sigma = 4$ (assumed by Swaszek et al. [27]) as a starting point to show the effect of our measurement-based improvements. Note that the official performance standard [30] only gives typical ranges for the standard deviation from $\sigma \approx 1$ to $\sigma \approx 8$. Figure 10 shows the performance improvements as we introduce our assumptions. The top left curves are generated with a standard deviation of $\sigma = 4$ and a correlation of $\rho = 0.5$ between position changes for both normal operation and spoofing. A more realistic assumption on the standard deviation is introduced in the bottom left figure, where we keep $\sigma_{\text{legit}} = 4$ and change $\sigma_{\text{spoof}} = 1$ emulating the reduced position shifts under spoofing. At the top right corner, we introduce the effect of higher correlation during a spoofing attack by adjusting $\rho_{\text{spoof}} = 0.9$. The bottom right figure combines both effects, i. e., $\sigma_{\text{legit}} = 4$, $\sigma_{\text{spoof}} = 1$, $\rho_{\text{legit}} = 0.5$, and $\rho_{\text{spoof}} = 0.9$.

In particular, the (red) dashed line in Figure 10 represents the resulting false alarm rate as a function of the radius by fixing the detection probability to $p_{\text{d}} = 0.99$. Without considering reduced error characteristics under spoofing, we obtain $p_{\text{fa}} = 10^{-5}$ for a radius of approx. 12.31 m. Using our derived parameter set, the required radius is reduced to approx. 3.63 m for the same false alarm rate. The resulting square has edges of length approx. 5.13 m.

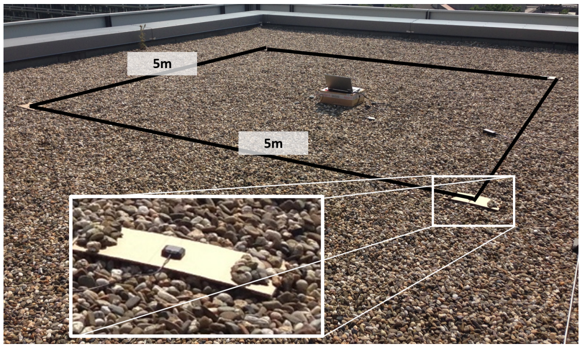

Figure 11: The outdoor measurement environment for our GPS spoofing detection prototype.

Summary of Results. We conclude that our proposed improvements reduce the required area for the countermeasure from $200\,\mathrm{m}^2$ in [27] to approx. $(5.13\,\mathrm{m})^2 \approx 26.32\,\mathrm{m}^2$, which is almost an order of magnitude smaller (square area). For this comparison, we picked the same UERE values as in [27]. If we use the UERE we measured in our experiments instead, the performance would be increased even further.

7. PROTOTYPE IMPLEMENTATION

To demonstrate the applicability of our proposed multi-receiver spoofing detection mechanism, we developed a prototype implementation. We deployed an experimental setup with $m = 4$ receivers positioned in a square with edge length $d = 5.00\,\mathrm{m}$, which is equivalent to a circle with $r \approx 3.54\,\mathrm{m}$. Two receivers are placed in close vicinity to a metal wall introducing signal shielding and additional multipath components. Figure 11 shows the measurement environment (the metallic wall is close to the right hand side).

We tested this formation in two different environments: (i) We recorded measurements under authentic conditions, see Figure 11. (ii) We targeted the same formation with an indoor spoofing attack. Notably, we used the indoor setup to prevent—in particular illegal—interference with surrounding devices. We captured data for spoofing and normal operation for close to three hours. For this specific setup we utilized the normalized majority voting approach for the receiver distance analysis. The threshold, which is represented by the horizontal line, is an estimation that optimizes both the detection and the false alarm probability.

Within the entire measurement period, we encountered no false alarms while under spoofing our countermeasure detected the spoofing attack reliably as depicted in Figure 12. More than 80,000 GPS measurements were recorded during the experiments. The normalized majority distance for the authentic measurements is constantly above the threshold, whereas in the spoofing case it is always below. If any of the measurements cross the threshold line, either a false alarm or a missed spoofing would occur. A sliding-window approach could compensate single threshold under- or overcuts.

Summary. With our prototype implementation we have demonstrated that the detection mechanism is applicable to $m = 4$ receivers positioned in a square of edge length $d = 5.00\,\mathrm{m}$ or a circle with radius $r \approx 3.54\,\mathrm{m}$. For the duration of the experiment we encountered no false alarms and no missed spoofing events.

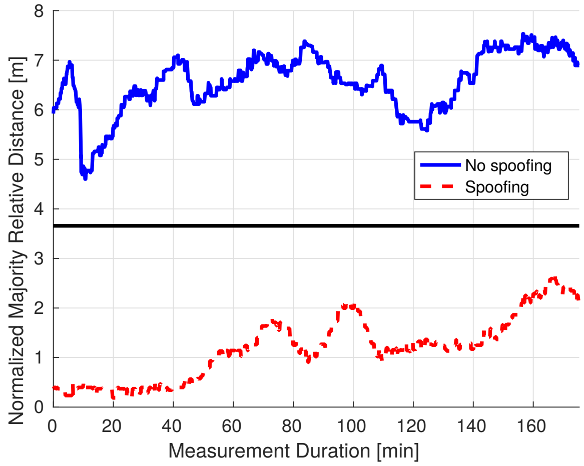

Figure 12: The normalized majority relative distance for authentic GPS signals (top) and under spoofing (bottom). The horizontal line represents an estimation for the threshold λ.

Outlook on Future Work. This investigation of multi-receiver GPS spoofing detection leaves promising studies for future work. Before the countermeasure is deployed on a larger scale, more investigations regarding the stability of GPS errors and their correlation for different locations, environmental conditions, and time intervals are desirable. Recently, Pesyna et al. [19] presented the potentiality of centimeter positioning, which would greatly improve our detection performance. Our investigations provide an evaluation framework that facilitates extended measurements and evaluations. We leave the evaluation of overlapping legitimate and spoofing signals for future work.

8. MULTI-ANTENNA ATTACKER

We now discuss the multi-antenna attacker with respect to our GPS spoofing countermeasure. To the best of our knowledge, this type of attacker has only been proposed theoretically [29]; practical realizations do not exist in the public literature. Implementing and realizing this multi-antenna attacker is challenging as we will explain in the following. Comprehensive results as well as extensive descriptions and evaluations are beyond the scope of this paper.

The multi-antenna attacker utilizes (at least) four antennas each sending out a different satellite signal. These signals arrive at the receivers as individual signals with certain attacker-chosen time offsets. If chosen properly, the signals can be resolved to a position that is determined by the actual satellite positions included in the ephemeris data and the corresponding ToA. Per receiver, this is identical to what a single-antenna attacker would achieve. However, if we position the antennas such that the ToA at an adjacent receiver can be correctly resolved to a position that is a configurable distance apart, we can realize a distance-preserving multi-antenna attack.

Our test setup uses two receivers and four USRPs N210 [3] each transmitting a GPS satellite signal realizing an attacker with four antennas. The signal samples were generated using the software project gps-sdr-sim [4] and are synchronized using a control laptop. In order to spoof a single receiver, the four USRPs are positioned equidistantly around the targeted receiver. The correct ToA (as under normal operation) is already considered during the signal generation. When we extend the countermeasure to $m = 2$ receivers, we need to rearrange the antennas such that the relative ToA for both receivers corresponds to the actual relative ToA for that specific time frame.

For instance, for a co-located receiver at a distance of 5 m the differences in the pseudoranges are in the range of -5 m to $+5$ m. Consequently, the antennas need to be moved based on the second receiver position and the emitted satellite signal. Additionally, the setup needs to be adapted to the current ephemeris data and spoofed GPS time since differences in the pseudoranges change over time.

Implementation Challenges. Under normal operation, GPS signals have roughly the same signal power. For the single receiver with equidistant senders we achieved a GPS lock by using four separated signal sources. However, when we rearrange the antennas to simultaneously fulfill the ToA at an adjacent receiver, the distances to the second receiver now varies from 0.5 m to 7 m in contrast to 5 m to the first receiver. This results in substantially different power levels which leads to a very unstable lock. Unfortunately, for a realistic attacker that is located, e. g., at a distance of about 100 m from the receivers, however, the differences in power levels are getting less and less since the relative differences shrink as well.

Our Countermeasure. For settings with $m \geq 4$ receivers, a multi-antenna attack (with the attacker trying to adjust the ToAs) cannot preserve the relative distances of all receivers [29]. As a result, our proposed multi-receiver countermeasure with four receivers is expected to be resilient against multi-antenna attacks by design. With our limited multi-antenna attacker implementation, we were only able to spoof single receivers, and even our most basic countermeasure with $m = 2$ is already complicating the attack significantly.

9. RELATED WORK

First experimental work on the topic of GPS spoofing was published by Warner et al. [32, 33]. The authors demonstrated that GPS spoofing attacks were feasible using a GPS satellite simulator. They proposed countermeasures mostly based on signal strength differences for spoofed signals.

A rich set of related work on GPS spoofing was published by Humphreys et al. [7, 10, 13, 20, 21]. In [7], a spoofer was constructed that would use legitimate GPS signals to obtain correct GPS data, and then re-transmit this data with selectively applied time offsets, causing the victim's receiver to compute a wrong location. In [13], physical-layer signal characteristics such as phase shifts between two antennas were used to detect ongoing spoofing attacks. This countermeasure required a custom two-antenna receiver setup.

In [24], Scott proposed changes to the GPS signals to introduce data-level authentication based on a public-key infrastructure. Another authentication signal-based scheme was proposed in [11]. In [20], the (encrypted) military GPS signal was used to authenticate the civilian signal received at the same time. In [10], a practical GPS spoofing attack on a UAV was conducted.

Spoofing detection based on different signal characteristics (e. g., angle-of-arrival, signal power, etc.) was discussed in [2, 16, 17]. In contrast to these detection schemes focusing on physical-layer characteristics, we focus on the navigation message information itself. In other words, instead of using pseudoranges [23] we use the position solution for our countermeasure, which is easy to obtain, process, and store on a high abstraction level.

The multi-receiver countermeasure was analyzed theoretically in [5, 26–28]. The authors of [5] derived performance values for mutual distances of 20 m achieving a false rejection rate of less than 0.1 and a false detection rate of 0.01 (location noise $\sigma = 5$ m). Therefore, the countermeasure seems hardly applicable to most moving vehicles, but instead only suited toward large stationary installations. Swaszek et al. theoretically investigated the countermeasure, using statistical models [26,28] extended by bias in the 2D noise distribution of the localization result [27]. For a four-receiver countermeasure, they suggest that a square setup with 14 m edge distance would achieve a false acceptance rate of $\approx 10^{-5}$ and a detection rate of ≈ 0.99 (location noise $\sigma = 4$ m). Such a formation would require an area of 200 m^2.

Other recent works consider GPS spoofing attacks on the time and phase synchronization in smart power grids [9, 34]. In [34], the authors propose to use a set of modified static GPS receivers with tight time synchronization to determine the exact time of arrival of spoofed signals at each locations with 1 ns precision. Based on that information, multilateration can be used to locate the attacker.

10. CONCLUSION

In this work, we thoroughly investigated a multi-receiver-based GPS spoofing detection technique and performed its first practical implementation. We started by revising the underlying assumptions of previous theoretical work, in particular the error models, and proposed that there is a correlation between errors at co-located receiver positions. We experimentally validated that the predicted error correlation is present in authentic signal scenarios, as well as under a spoofing attack. By leveraging the correlated noise of co-located receivers, we were able to lower the false acceptance rate of the countermeasure, while preserving the sensitivity to attacks.

As result, a formation covering an area of 26 m^2 is sufficient (for a detection rate of 99 % and a false detection rate of approx. 10^{-5}), in contrast to the previously proposed 200 m^2 [27] or even larger area in [5]. We realized the *first* multi-receiver-based GPS spoofing detection system based on low-cost COTS devices. Using that implementation, we were able to validate our theoretical findings through a range of experiments using single-antenna and multi-antenna attackers. For an experiment over the course of roughly 3 h, we observed no false positive or false negatives.

For future work, promising avenues based on our experimental measurements include further reductions of the required distance between receivers (e. g., in scenarios with rather stable signals due to direct line-of-sight) or due to receiver dynamics. Additionally, the detection threshold could be subject to dynamic adaptation.

11. ACKNOWLEDGMENTS

The research in this work was supported in parts by the DFG Research Training Group GRK 1817/1 and by SUTD's startup grant SRIS14081.

12. REFERENCES

[1] D. M. Akos. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *NAVIGATION, Journal of the Institute of Navigation*, 59(4):281–290, Dec. 2012.

[2] A. Cavaleri, B. Motella, M. Pini, and M. Fantino. 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, Dec. 2010.

[3] Ettus. Universal Software Radio Peripheral (USRP). https://www.ettus.com.

[4] Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim.

[5] L. Heng, J. J. Makela, A. D. Domínguez-García, R. B. Bobba, W. H. Sanders, and G. X. Gao. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture. In *Power and Energy Conference at Illinois*, PECI '14. IEEE, Feb. 2014.

[6] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins. *Global Positioning System: Theory and Practice*. Springer, 5th edition, 2001.

[7] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr. 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, pages 2314–2325, Savannah, GA, USA, Sept. 2008.

[8] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, 2012, May 2012.

[9] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Transactions on Power Systems*, 28(3):3253–3262, Feb. 2013.

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

[11] M. G. Kuhn. An Asymmetric Security Mechanism for Navigation Signals. In *International Conference on Information Hiding*, IH '04, pages 239–252, Toronto, Ontario, Canada, May 2004. Springer.

[12] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. In *International Technical Meeting of The Institute of Navigation*, ION '10, pages 698–712, San Diego, CA, USA, Jan. 2010.

[13] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina. 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, pages 124–130, Anaheim, CA, USA, Jan. 2009.

[14] J. Nielsen, A. Broumandan, and G. Lachapelle. GNSS Spoofing Detection for Single Antenna Handheld Receivers. *NAVIGATION, Journal of the Institute of Navigation*, 58(4):335–344, Dec. 2011.

[15] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley. GPS Software Attacks. In *ACM Conference on Computer and Communications Security*, CCS '12, pages 450–461, Raleigh, NC, USA, Oct. 2012. ACM.

[16] P. Papadimitratos and A. Jovanovic. GNSS-based Positioning: Attacks and Countermeasures. In *IEEE Military Communications Conference*, MILCOM '08, pages 1–7, San Diego, CA, USA, Nov. 2008. IEEE.

[17] P. Papadimitratos and A. Jovanovic. Protection and Fundamental Vulnerability of GNSS. In *IEEE International Workshop on Satellite and Space Communications*, IWSSC '08, pages 167–171, Toulouse, France, Oct. 2008. IEEE.

[18] B. W. Parkinson, J. J. Spilker Jr., P. Axelrad, and P. Enge. *Global Positioning System: Theory and Applications*, volume I. American Institute of Aeronautics and Astronautics, 1996.

[19] K. M. Pesyna Jr., R. W. Heath Jr., and T. E. Humphreys. Centimeter Positioning with a Smartphone-Quality GNSS Antenna. In *International Technical Meeting of The Satellite Division of the Institute of Navigation*, ION GNSS+ '14, pages 1568–1577, Tampa, FL, USA, Sept. 2014.

[20] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys. Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals. In *International Technical Meeting of The Satellite Division of the Institute of Navigation*, ION GNSS '11, pages 2619–2645, Portland, OR, USA, Sept. 2011.

[21] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield. GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase. In *International Technical Meeting of The Satellite Division of the Institute of Navigation*, ION GNSS+ '14, pages 2776–2800, Tampa, FL, USA, Sept. 2014.

[22] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon. 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, pages 2949–2991, Nashville, TN, USA, Sept. 2013.

[23] D. S. Radin, P. F. Swaszek, K. C. Seals, and R. J. Hartnett. GNSS Spoof Detection Based on Pseudoranges from Multiple Receivers. In *International Technical Meeting of The Institute of Navigation*, ION '15, pages 657–671, Dana Point, CA, USA, Jan. 2015.

[24] L. Scott. Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. In *International Technical Meeting of the Satellite Division of The Institute of Navigation*, ION GPS/GNSS '03, pages 1543–1552, Portland, OR, USA, Sept. 2003.

[25] G. Seeber. *Satellite Geodesy: Foundations, Methods, and Applications*. de Gruyter, 2nd edition, 2003.

[26] P. F. Swaszek and R. J. Hartnett. 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, pages 2921–2930, Nashville, TN, USA, Sept. 2013.

[27] P. F. Swaszek and R. J. Hartnett. A Multiple COTS Receiver GNSS Spoof Detector – Extensions. In *International Technical Meeting of The Institute of Navigation*, ION '14, pages 316–326, San Diego, CA, USA, Jan. 2014.

[28] P. F. Swaszek, R. J. Hartnett, M. V. Kempe, and G. W. Johnson. Analysis of a Simple, Multi-Receiver GPS Spoof Detector. In *International Technical Meeting of The Institute of Navigation*, ION '13, pages 884–892, San Diego, CA, USA, Jan. 2013.

[29] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun. On the Requirements for Successful GPS Spoofing Attacks. In *ACM Conference on Computer and Communications Security*, CCS '11, pages 75–86, Chicago, IL, USA, Oct. 2011. ACM.

[30] U.S. Department of Defense. *Global Positioning System Standard Positioning Service Performance Standard*, 4th edition, Sept. 2008.

[31] J. A. Volpe. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. Technical report, National Transportation Systems Center, Aug. 2001.

[32] J. S. Warner and R. G. Johnston. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. *Journal of Security Administration*, 2003.

[33] J. S. Warner and R. G. Johnston. GPS Spoofing Countermeasures. *Homeland Security Journal*, 25(2):19–27, 2003.

[34] D.-Y. Yu, A. Ranganathan, T. Locher, S. Čapkun, and D. Basin. Short Paper: Detection of GPS Spoofing Attacks in Power Grids. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '14, pages 99–104, Oxford, United Kingdom, July 2014. ACM.

APPENDIX

A. SELECTION OF FUNCTION F

We consider four different functions, which represent a *minimal*, *maximal*, *majority*, and *normalized* approach. The minimal and the maximal functions only consider the minimal, respectively the maximal, measured distance from the set of all distances. The majority approach performs a type of voting mechanism which decides for spoofing when the majority of distances, i. e., four out of six, fall below the decision threshold. The normalized approach makes some distances more significant than others, e. g., the diagonal in a square is $\sqrt{2}$ times longer than the edges and then performs a majority voting.

For $m = 4$ receivers there are six distances in total. We evaluate the detection performance of different instantiations of the function f, which operate on the distances. Exemplary, we present results considering the error model with the same error distributions for spoofing and non-spoofing conditions (Case 3). We are able to identify the best choice for the function f for this specific model and give hints towards the impact of changing error models.

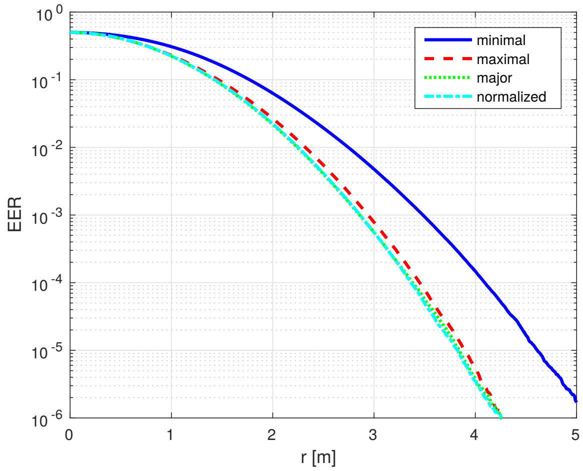

Figure 13: EER for different radii considering different functions f ($m = 4$) (Case 3).

Table 6: Function f Performance (Lower is Better)

Function f	Relation 1	Relation 2	Relation 3
Minimal	≥ 7	≥ 9	≥ 10
Maximal	1.0000	1.2049	1.2344
Majority	0.8457	1.0000	1.0224
Normalized	0.8320	0.9820	1.0000

Figure 13 compares performance values for the chosen types of the function f, i. e., minimal, maximal, majority, and normalized. As one can see, the choice of a minimal function offers the worst performance from the analyzed set. The other three types, namely maximal, majority, and normalized, all perform pretty similar.

In order to quantitatively compare the performances, we compute the relative difference in EER over all radii and average it by means of normalizing the results. Results are given in Table 6. We can state that the normalized approach performs approx. 2 % better than the (non-normalized) majority voting and approx. 17 % better than the maximal function. The majority function has an approx. 15 % better average performance than the maximal function. In conclusion, the normalized approach is the best choice for the selected error model.

We also conducted simulations for the other error models with similar results. For the scenarios with more stable and more correlated signals, we notice that the differences of maximal, majority, and normalized functions is decreasing and eventually the maximal distance performs as good as the others within negligible margins. The usage of the maximal distance can be beneficial for setups with restricted computational resources since this function requires less comparisons. Nevertheless, the (normalized) majority voting approach is the optimal choice for all considered error models.

B. FURTHER MEASUREMENTS

We conducted further measurements between August 2015 and May 2016 to confirm our error modeling approach in

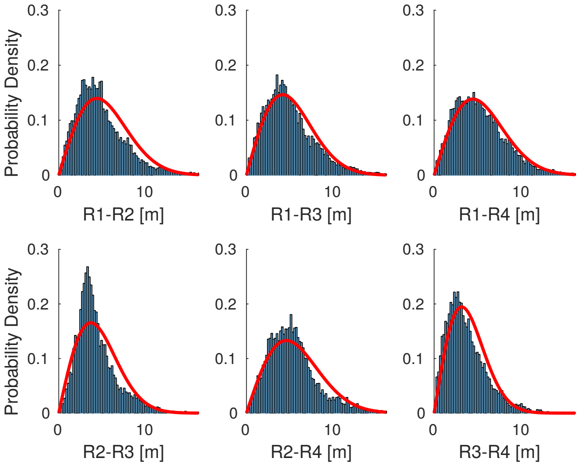

Figure 14: Distribution of distances from a three-day measurement with $m = 4$ receivers and a bin width of $0.2\,\mathrm{m}$.

different environments. For instance, receivers were placed close to metallic walls or near other noise sources. Over different time periods (up to three days non-stop) measurements were collected to assess the effects of signal reflections and changing meteorological conditions. For the sake of clarity, we only present resulting parameters for the standard deviation and the correlation here.

Authentic. For receivers with clear line-of-sight, but under multipath effects, we experienced typical position noise in the range of $\sigma \approx 0.746$ to $\sigma \approx 3.063$, where the latter was measured close to a reflecting metallic wall. Similar degradations can be observed for the correlation between position changes. Additional noise sources can decrease the correlation to $\rho \approx 0.265$ for direct wall reflections. However, correlations of $\rho \approx 0.820$ were still measured for receivers affected by multipath signal components but with clear line-of-sight.

Spoofed. For our spoofing experiments we also varied the antenna inclination due to the different angle-of-arrival of spoofing signals due to a ground level satellite simulator. We tried establish similar power levels at the receiver to imitate conditions under normal operation. In all our experiments, the spoofer was in close vicinity to the receivers. We obtained the following typical results for the standard deviation and the correlation. For unfavorable environments, the individual receiver's position inaccuracy can increase to $\sigma \approx 0.882$ under spoofing. The correlation coefficients across several measurements maintained a comparably high level of $\rho \approx 0.981$ to $\rho \approx 0.463$ in a worst case scenario.

3-day Experiment. This experiment was run over the course of three days with $m = 4$ receivers and changing weather conditions. Over 1,000,000 data points for each receiver were recorded. Figure 14 shows a histogram of all relative distances. We note that the real distances between the receivers were relatively small to shelter the devices from rain. Outliers are still visible and could be caused by changing temperature and weather conditions.