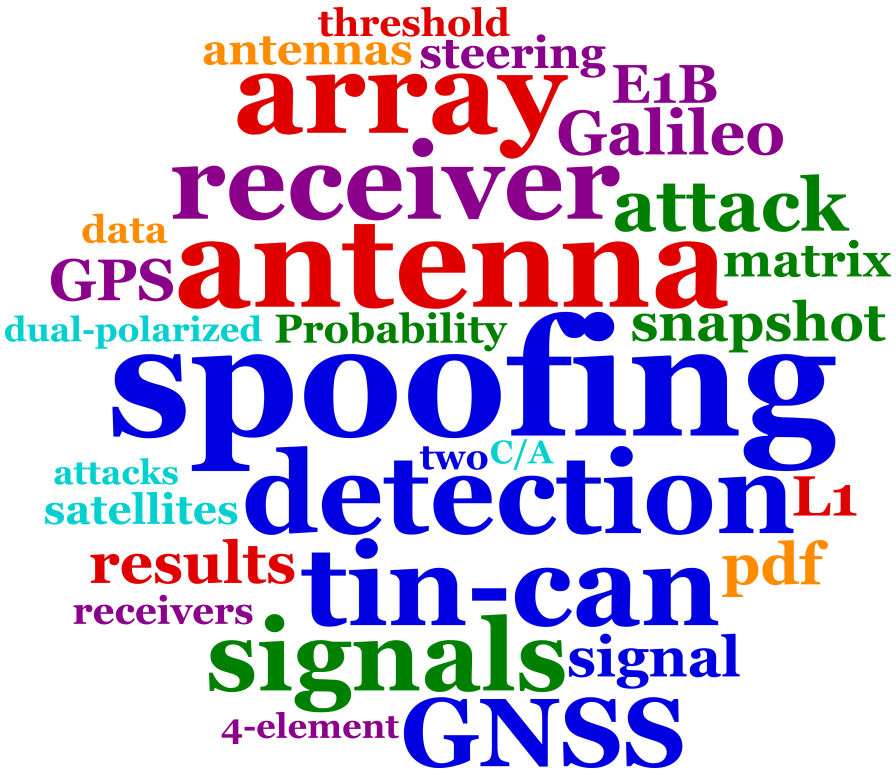
Submitted version of: J. Rossouw van der Merwe, Alexander Rügamer, Alexander Popugaev, Xabier Zubizarreta and Wolfgang Felber, "Cooperative spoofing attack detection using multiple antennas and a snapshot receiver," Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida submitted June 2019, accepted September 2019.

DOI: https://doi.org/10.33012/2019.17112



Cooperative spoofing attack detection using multiple antennas and a snapshot receiver

J. Rossouw van der Merwe, Alexander Rügamer, Alexander Popugaev, Xabier Zubizarreta and Wolfgang Felber
Fraunhofer Institute for Integrated Circuits IIS, Nuremberg, Germany

BIOGRAPHY

J. Rossouw van der Merwe received his B.Eng (Hons) and M.Eng. degrees in Electronic Engineering from the University of Pretoria, South Africa, in 2014 and 2016, respectively. He joined the Fraunhofer Institute for Integrated Circuits IIS in 2016, where his research focuses on signal processing for interference detection, mitigation and array processing.

Alexander Rügamer received his Dipl.-Ing. (FH) degree in Electrical Engineering from the University of Applied Sciences Würzburg-Schweinfurt, Germany, in 2007. Since then he has been working at the Fraunhofer Institute for Integrated Circuits IIS in the Field of GNSS receiver development. He was promoted to Senior Engineer in February 2012. Since April 2013, he is head of a research group dealing with secure GNSS receivers and receivers for special applications. His main research interests focus on GNSS multi-band reception, integrated circuits and immunity to interference.

Alexander Popugaev (M.Sc. and Ph.D in EE) joined Fraunhofer IIS in 2004 and is currently Chief Scientist at the RF and SatCom Systems Department. His main research activities focus on the design of customer-specific GNSS antennas.

Xabier Zubizarreta is currently a researcher at the Fraunhofer IIS in Nuremberg, Germany. He earned his Master of Science on Communication Engineering at the University of Erlangen-Nuremberg 2017, with a work on the assessment of the Open Service Navigation Message Authentication (OS-NMA). His research interests include the design of robust GNSS receivers and the analysis, characterization and mitigation of GNSS interference and spoofing.

Wolfgang Felber received his Dipl.-Ing. degree in Electrical Engineering in 2002 and his doctoral degree Dr.-Ing. in 2006 from Helmut-Schmidt-University of Federal Armed Forces Hamburg, Germany. Since 2014 he is head of the Satellite Based Positioning Systems department of Fraunhofer IIS, division Localisation and Networking in Nuremberg. The main topics in his department is hardware development of satellite navigation receivers for multiple or hybrid precise systems and secure applications. Additionally, since 2016 he is Head of the business field localization at Nuremberg which combines different localization technologies for industrial IoT applications.

ABSTRACT

Cooperative spoofing attacks are difficult to detect and to mitigate. In these attacks the user or owner of the global navigation satellite system (GNSS) receiver is also the attacker, hence, he can ensure ideal spoofing circumstances. Such attacks are associated with criminal activities where the user wants to falsify his own position. A low-cost tin-can spoofing attack against a snapshot receiver is demonstrated in this paper. Such an attack is similar to a cable inject; however, it couples over-the-air via the antenna of the victim GNSS receiver. Methods to detect such tin-can attacks are proposed where an array of antennas or a dual-polarized antenna is used. The detection criteria is based upon the similarity of the spatial properties of the received signals.

The detection metric is analyzed to obtain the analytic detector threshold setting for optimal performance. The results with open service (OS) signals from GPS and Galileo show that with both an array of right-hand circular polarized (RHCP) antennas and a dual-circularly-polarized antenna the spoofing detection is successful. However, the array of antennas has shown superior performance in the detector analysis. This paper practically demonstrates the simplicity and feasibility of a tin-can attack as well as methods to sufficiently detect and counter such attacks. This emphasizes the vulnerability of GNSS receivers, and shows the need for multiple channel operation for robust high-performance receivers.

INTRODUCTION

Spoofing—the illegal transmission of falsified global navigation satellite system (GNSS) signals—is a growing problem for GNSS security. The recent report from C4ADS [1] has shown how common spoofing attacks have become. However, in some instances a GNSS user might also willingly spoof his own equipment: the intent might be to falsify the user's location and its association with criminal activity. Some examples include avoiding GNSS-based highway toll collection systems, falsifying

automatic identification system (AIS) to illegally fish in protected marine areas, evading GNSS-based parole monitoring, or even cheating in mobile games such as "*Pokemon GO!*". Such attacks are cooperative, as the attacker has access to the GNSS hardware and can facilitate ideal spoofing conditions to improve spoofing success.

One method to achieve cooperative spoofing is the "tin-can" method. A conceptual diagram of the tin-can spoofing attack and a snapshot receiver is shown in Figure 1. A tin-can is fitted with an internal monopole antenna and radio-frequency (RF) port. The can is then placed over the antenna of the victim's GNSS receiver. Spoofing signals are transmitted through the can while shielding the antenna from the actual GNSS signals. The tin-can, depending on its dimensions, can enable good coupling between the spoofing-transmitter (internal monopole) and the victim GNSS antenna. This method increases spoofing success, as there are no competing "real" GNSS signals. Further, the user may interfere with the receiver itself, for example by forcing the receiver into a cold start. This makes spoofing detection especially difficult against such an attack, in which only a tin-can and some basic RF components are required. Therefore, it is considered to be a low-cost and simple spoofing scheme. A tin-can attack is characterized by the lack of transmission of any signals outside the can, hence, there is no disruption to other services. This makes it difficult to locate. In this paper, a tin-can attack is executed and methods to detect such an attack using multiple antennas are presented. The spoofing detection metric for the methods are based on the similarity between the spatial properties of the received signals.

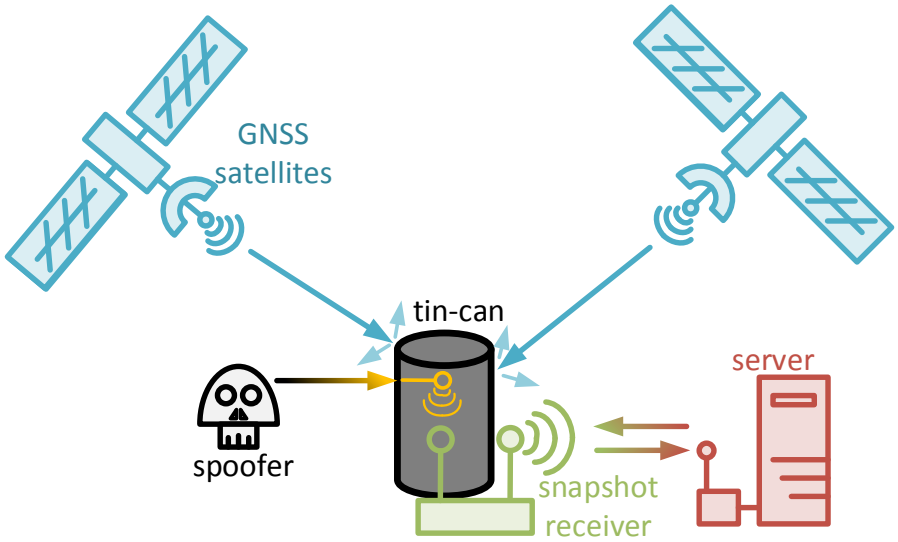


Figure 1. Tin-can concept with a snapshot receiver

A snapshot receiver (also referred to as "cloud based GNSS" [2] or "server based processing" [3]) consists of a recording device (captures the raw RF data), and a server (processes the position, velocity, and time (PVT) solution), as shown in Figure 1. The evaluation of the recorded data, and the associated processing, power requirements and cost are moved to the server [3]. The recorded signal duration is often minimized (typical snapshot lengths of 5 to 20 ms) in order to save power and reduce the data transmission and storage. Therefore, tracking of the signals, like in a conventional GNSS receiver, is not possible. The acquisition output determines the pseudorange estimate. External assistance data provide the ephemeris and GNSS correction. The position is then calculated with the pseudorange and Doppler estimates, as well as assistance data.

Snapshot receivers are gaining more research interest, as this receiver architecture allows off-line processing and authentication. Further, the receiver is not limited by the hardware processing resources (e.g. number of tracking channels). Therefore, more processing opportunities exist in post processing. This receiver architecture is also a relatively recent development, which means that many processing methods that are limited to snapshot processing, have not yet been investigated. Snapshot receivers are especially vulnerable to spoofing, as only a window of data is used for positioning. This limits time-comparative evaluation methods, which are typically used for spoofing detection. As such the need for alternative spoofing detection methods are required for snapshot receivers.

In this paper, a multi-channel snapshot receiver is presented for spoofing detection against a tin-can attack. The benefit of the presented algorithms are that no calibration of the antenna array is required. Furthermore, it shows that beamforming and polarization forming methods could be used in the presence of near-field coupling, even though these methods are traditionally only assumed to be operational in the far-field. Results have shown that a receiver consisting of an array of antennas or a dual-polarized antenna has good potential to detect a spoofing attack.

The paper is structured as follows: Some background to *Snapshot receivers* and *Spoofing attacks* will be presented, followed by the the state of the art *Spoofing detection* methods and the proposed algorithms used in this study. The *Test setup* is described, the *Results* presented, and, finally, the *Conclusion* will be drawn.

SNAPSHOT RECEIVERS

A snapshot receiver operates with only a few milliseconds of raw data obtained by a radio-frequency front-end (RFFE) [3, 4]. This raw data snapshot is sent to a server for remote processing. The server can only achieve signal acquisition, as there are not enough data available for a tracking, nor sufficient data to obtain any information from the navigation message. This means that a snapshot receiver operates fundamentally differently compared to conventional GNSS receivers. Since the navigation data cannot be decoded, information like ephemeris, atmospheric and clock corrections is obtained from a secondary source. The transmission time of the satellite is not available, hence, a direct pseudorange cannot be directly derived. However, given a rough receiver position and time estimate together with the ephemeris data, the pseudorange reconstruction can be achieved [5]. The PVT solution can be verified and might then be sent back to the receiver, depending on the actual use case. Most snapshot receivers only use a single antenna, but the performance with snapshot receivers using multiple antennas has been investigated [6].

SPOOFING ATTACKS

In this section the background to spoofing attacks are presented.

Cooperative spoofing

Spoofing is a term used to describe GNSS deception attacks [7–11]. There are a number of different spoofing types. However, in this paper only cooperative spoofing attacks are considered. In a cooperative attack, the user of the receiver is willingly trying to deceive his own receiver. This increases the difficulty of detecting and countering the spoofing attack, as the user actively influences the attack, thereby, significantly increasing the success-rate of the attack. The user can, for example, decouple any other sensors form the receiver, configure the receiver to only use GNSS signals and systems which are spoofed, deny the use of assistance data, or by forcing a cold-start of the GNSS receiver. Some applications for this attack are: cheating in geo-location based games, like *Pokemon-Go!* [12]; avoiding GNSS based automatic toll collection (ATC) [13]; misuse of car-sharing schemes [14]; infringing on parole monitoring devices [15, 16]; and altering AIS to illegally fish in maritime reserves [17].

Traditionally, cooperative attacks fall into three categories: over-the-air (OTA) spoofing, cable-inject, and application level spoofing [11]. The first two cases alter the input signal to the receiver, and in the third the output solution from the receiver. An OTA spoofing attack has the disadvantage that it can impact all GNSS receivers in the vicinity, which from a electromagnetic spectrum (EMS) point of view is illegal and is possible to locate. In a cable-inject attack, the antenna of the receiver is removed and replaced with a spoofing signal generator. This attack couples the spoofing signal directly to the receiver, thereby, not interfering with the EMS. This makes it difficult to locate but does not interfere with other receivers. In an application level attack, the spoofing is done after the GNSS receiver: the final PVT results are falsified. In such high-level attacks the GNSS receiver is completely bypassed.

Tin-can spoofing

In this paper we present the tin-can spoofing attack, e.g. mentioned by in the GNSS spoofing context [7]. It is similar to the cable-inject, but it assumes that the GNSS receiver incorporates an integrated antenna, or that the user cannot replace the receive antenna with a spoofing signal generator. As a result the spoofing signal can only be coupled electromagnetically to the antenna, using, for example, a tin-can. The tin-can has a transmitting quarter wave monopole antenna on the inside, and in this case it acts like a wave guide between the spoofing transmitter and the GNSS receiver antenna [18]. Further, the metal shell of the tin-can acts like an isolating Faraday cage, thereby reducing the influence of the spoofer to any surrounding GNSS receivers, as well as denying the reception of the actual GNSS signals.

As the GNSS receiver can only observe the spoofing signals, the spoofer does not compete with actual GNSS signals. This results in an improved spoofing take-over. As such, a partial spoofing constellation, where some satellites are spoofed and some are the real GNSS signals, is also not possible. Further, the spoofed signals can be transmitted at lower power, hence, signal power based spoofing detectors are ineffective.

A tin-can antenna (also referred to as a “cantenna”) is simple and cheap to build, and there are many online-guides to do so [19–21]. These antennas are mainly used to boost WiFi signals through increased directionality or to make home radar kits – in either case a quick-and-dirty radio-amateur home project. Therefore, this is a significant risk for GNSS receivers to deal with, as anyone can build it. The simplicity of the method, as well as the efficiency of the spoofing attack, emphasizes the need for adequate detection methods against such attacks.

SPOOFING DETECTION

This sections presents the current methods to detect a spoofing attack, as well as the detection method proposed for tin-can spoofing attacks.

Common detection methods

There are many methods used to detect spoofing [7, 10, 22]. Changes over time, such as the signal power differences— also known as automatic gain control (AGC) based methods [23]— changes in tracking parameters or signal quality [24–27], or discontinuities in the PVT solution [28, 29], are often used as metrics for detection. However, in the case of a snapshot receiver, these methods are not applicable, as only a small portion of data is available and no reference to previous values can be guaranteed. Further, a snapshot receiver does not use tracking, hence, tracking-based spoofing detection methods are not possible.

The tin-can isolates the receiver from the actual GNSS signals. Therefore, the spoofing attack is uncontested, and the spoofing signal do not require higher power than the actual signals to ensure a takeover. As a consequence, power monitoring methods [30–32] for spoofing detection are ineffective. Further, as only the spoofing signals are observed, the interference between the actual signals and the spoofing signals, which cause multipath-like effects, are also not present. Therefore, multipath based spoofing detection [33] is also not possible. As there are only spoofing signals, there is no mix of real or spoofed signals. Hence, mixed PVT solution based, or residual-based spoofing detection methods are futile. The use of other sensors to verify the receiver motion is also limited [28], as the user might disable this functionality in a cooperative spoofing attack. These factors emphasize the limitation in spoofing detection in the event of a snapshot based cooperative spoofing attack.

Spatial spoofing detection methods

Considering all of the aforementioned limitations, only the spatial information can be fully exploited. All of the signals originate from the same direction (i.e. the coupling between the antenna and the tin-can), therefore, all signals will have similar spatial characteristics. This is also true for the polarization of the received signals, as the wave-guide effects of the horizontal and vertical transmission modes are the same for all signals in the tin-can.

Spoofing detection with an array of antennas has already been proven to be successful and reliable [34–37]. However, this requires a calibrated array with known receiver phase offsets and antenna orientation. Further, these methods are direction-of-arrival (DOA) based, and estimate the direction to each satellite. This is a limitation as it requires calibration of the antenna array, which increases the cost of the receiver. In this paper, we asses blind methods, as this reduces system cost and calibration requirements. Further, as the tin-can acts like a near-field coupling device, array calibration is arbitrary to the antenna. Lastly, the tin-can significantly alters the coupling effects between the antenna elements, due to the near-filed operation. Consequently, array calibration and de-coupling methods are no longer useful.

Another method to exploit spatial diversity is to use a dual-circularly-polarized antenna. Spoofing detection methods with polarization have shown good performance in recent studies [38–40]. The dual-polarized antenna can receive both the right-hand circular polarized (RHCP) and left hand circular polarized (LHCP) field components. Usually, only the RHCP component is used, as GNSSs transmit RHCP signals, hence improving the received signal power. Furthermore, when a signal reflects from a conductive surface, it approximately flips polarization from RHCP to LHCP and vice versa (in some cases one polarization component is adsorbed more than the other, resulting in ellipsoidal or linear polarized signals after the reflection). Therefore, all odd-reflected multipath components are LHCP, which further emphasizes the use of RHCP antennas for multipath rejection in GNSS receivers. Low-cost antennas are usually linearly polarized, and can't reject the LHCP components efficiently. In most scenarios, the RHCP will still have more received power than in the LHCP, as multipath components tend to have lower power than the line of sight (LOS) signal (the exception is in severely degraded environments, like urban canyons). In a multipath-free signal, no LHCP component is expected. As the tin-can operates like a wave guide, it is expected that both the RHCP and LHCP components will be significant, making it simple to detect. Further, as all signals originate from the same monopole antenna (linearly polarized) inside the can, the RHCP and LHCP components of all the signals can have comparative magnitudes. Therefore, the similarity test as what was used for the antenna array could simply be adapted. This method shows that this is a simple low-cost option to increase receiver robustness, in comparison to an array antenna. A dual-polarized antenna has the same phase center for both RHCP and LHCP, which is both an advantage (same location) and disadvantage (less spatial diversity).

Tin-can spoofing detection

Spoofing detection with a multi-channel snapshot receiver has been demonstrated [41], and is based estimating the beam-steering values during the acquisition stage of the receiver [6]. This detector uses the array steering vector for each of the received signals. Note that the array steering vector could refer to the beam-steering, the polarization-steering or both, as this depends on the antenna used. From a processing perspective each could be described as a separate "receiver channel". The steering vectors are estimated as part of the acquisition process [41]. The estimated array steering vectors are placed in a matrix $\mathbf{B}$:

$$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_{N_\mathrm{w}}] \ , \tag{1}$$

where $\mathbf{b}_n$ is a column vector containing the array steering vector for the n-th satellite. The constellation consists of a total of N_w received satellites. $\mathbf{B}$ is a number of elements N_e by the number of estimated array steering vectors N_w sized matrix. The matrix is correlated to get a non-normalized correlation matrix $\mathbf{C}$:

$$\mathbf{C} = \mathbf{B}^H \times \mathbf{B} \,, \tag{2}$$

where $(\cdot)^H$ is the Hermitian transpose of the signal, and $\times$ is a matrix multiplication. Each element in the matrix is equivalent to the dot product between each pair of array steering vectors. $\mathbf{C}$ is N_w by N_w Hermitian matrix. To normalize the matrix, the magnitude of the auto-correlations need to be determined:

$$\mathbf{c} = \sqrt{\text{diag}\left(\mathbf{C}\right)} \,, \tag{3}$$

where $\mathbf{c}$ is a column vector containing the magnitude values, and $\text{diag}\left(\cdot\right)$ takes the diagonal of a matrix. The normalized correlation matrix $\mathbf{C}_\text{norm}$ is calculated as:

$$\mathbf{C}_\text{norm} = \Re\left\{\mathbf{C}\right\} \circ \left(\mathbf{c} \times \mathbf{c}^T\right)^{\circ -1} \,, \tag{4}$$

where $\Re\left\{\cdot\right\}$ takes the real component of each value, $\circ$ is the Hadamard product, and $(\cdot)^{\circ -1}$ is the Hadamard inverse. $\mathbf{C}_\text{norm}$ is also a Hermitian matrix. Each element of this matrix has the form:

$$C_\text{norm}(n,m) = \frac{\Re\left\{\mathbf{b}_n^* \cdot \mathbf{b}_m\right\}}{\left\|\mathbf{b}_n\right\| \left\|\mathbf{b}_m\right\|} = \cos\left(\xi_{n,m}\right) \,, \tag{5}$$

where $\left\|\mathbf{b}_n\right\|$ is the magnitude of the n-th beamforming vector. Each correlation can be regarded as the cosine of the angle $\xi_{n,m}$ between two array steering vectors. This is not the spatial angle of the DOA between two satellites (also referred to as the incident angle of the array), but a measure of how similar the two array steering vectors are. For the remainder of this paper, this will be referred to as the steering vector angle. The detector threshold is tuned according to a symbolic steering vector separation angle. This is the steering vector angular threshold ξ_Th:

$$\lambda_\text{Th} = \cos\left(\xi_\text{Th}\right) \,. \tag{6}$$

The threshold is used to detect each value in the matrix $\mathbf{C}_\text{norm}$. If the value is lower than the threshold then the null-hypothesis H_0 of no spoofing is accepted. Otherwise, the alternate hypothesis H_1, where the signals have similar origins and are considered spoofed, is accepted:

$$C_\text{norm}(n,m) = \cos\left(\xi_{n,m}\right) \underset{H_1}{\overset{H_0}{\gtrless}} \lambda_\text{Th} \,. \tag{7}$$

To remove false positives, a similar process is followed; however, the spatial unit vectors $\mathbf{u}_n$ from the receiver position $\mathbf{p}_\text{rx}$ towards each satellite $\mathbf{p}_\text{sat}(n)$ are used:

$$\mathbf{u}_n = \frac{\mathbf{p}_\text{sat}(n) - \mathbf{p}_\text{rx}}{\left\|\mathbf{p}_\text{sat}(n) - \mathbf{p}_\text{rx}\right\|} \,. \tag{8}$$

These are calculated using the PVT solution and the ephemeris information of each satellite. Note that as these vectors are already normalized, no normalization is required. The resultant spatial correlation matrix $\mathbf{U}_\text{norm}$ is defined as:

$$U_\text{norm}(n,m) = \frac{\mathbf{u}_n \cdot \mathbf{u}_m}{\left\|\mathbf{u}_n\right\| \left\|\mathbf{u}_m\right\|} = \mathbf{u}_n \cdot \mathbf{u}_m = \cos\left(\theta_{n,m}\right) \,, \tag{9}$$

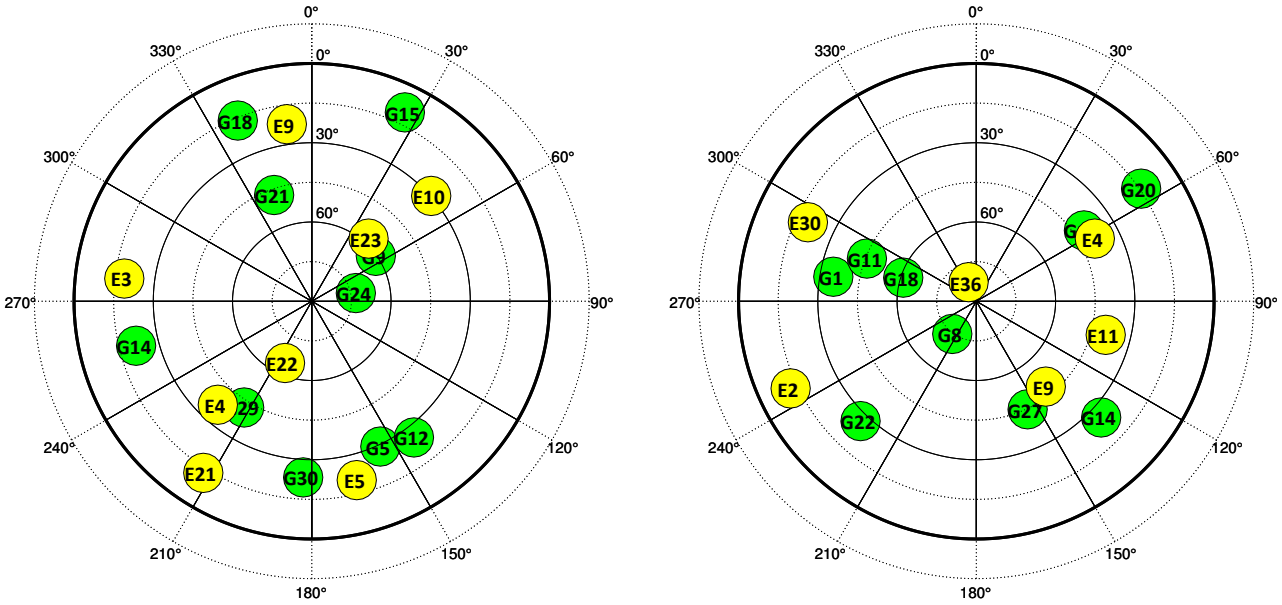
where $\theta_{n,m}$ is the spatial angle between the two satellites. This matrix has the same size and properties as the steering vector correlation matrix $\mathbf{C}_\text{norm}$, i.e it is a symmetric matrix. A threshold that excludes satellites that are close to each other can be set:

$$\lambda_\text{U} = \cos\left(\theta_\text{U}\right) \,, \tag{10}$$

where λ_U is the spatial detection threshold, and θ_U the spatial angular threshold. The detection matrix $\mathbf{D}$ can be determined as:

$$D(n,m) = \left(C_\text{norm}(n,m) \leq \lambda_\text{Th}\right) \cap \left(U_\text{norm}(n,m) > \lambda_\text{U}\right) \,. \tag{11}$$

As the matrices $\mathbf{C}_\text{norm}$, $\mathbf{U}_\text{norm}$, and $\mathbf{D}$ are symmetric (per extension also Hermitian), only the upper triangle needs to be evaluated. The diagonal should also be excluded, as the diagonal measures the similarity of each vector to itself.



(a) Simulated spoofing signal

(b) Open-sky recording

Figure 2. Sky-plot of the received signals

TEST SETUP

Two test setups are used in the evaluation. This first one uses a tin-can to demonstrate the spoofing attack, the second one is the control measurement with an open sky scenario. In the tin-can attack a Spirent GSS9000 signal generator is used to generate the spoofing signals. The generated scenario consists of signals in the L1/E1 band, with realistic carrier-to-noise density ratio (C/N_0) values ranging from 38 to 45 dBHz. A total of 11 visible satellites are simulated for Global Positioning System (GPS) and 10 satellites for Galileo in this scenario. The sky-plot from a GNSS-software-defined radio (SDR) for the generated signal constellation is shown in Figure 2(a).

The output of the Spirent signal generator is passed through an amplifier before it is connected to the tin-can. This is done to ensure sufficient power is received by the antenna: it counters the losses of the tin-can, free space, and any RF mismatches. Different antennas are placed inside the tin-can and connected to a Flexiband RFFE [42]. The recording of the signals is made with 40.5 MHz sampling rate at 4 bit I/Q quantization. A block-diagram of the setup, with the connections between the components, is shown in Figure 3.

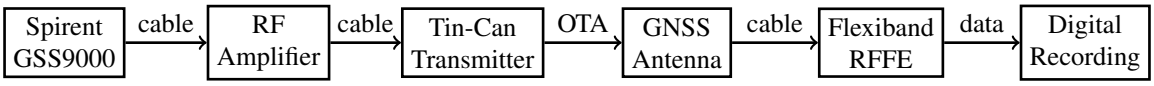


Figure 3. Measurement setup

For the open-sky measurement, the same antennas and receiver hardware is used. The only difference is that the antennas are placed outside to receive the actual GNSS signals. The purpose of this test setup is to have a comparison to an un-spoofed, authentic case. The sky-plot of the open-sky recording is shown in Figure 2(b). In this case the acquired satellite constellation form the GNSS-SDR consists of six GPS and four Galileo satellites. This is lower than the ideal case generated by the signal generator in the tin-can attack.

Two antennas are used for the evaluation. First, to test the validity of polarization, a high-performance dual-polarized antenna [43] is used. This geodetic-grade antenna features RHCP and LHCP with high polarization purity. The second antenna is a commercial four-element controlled radiation pattern array (CRPA) antenna from AntCom (4NC-3.5CG1215A) intended for increasing the receiver robustness. All of the hardware components, including the antennas and the tin-can, are shown in Figure 4.

Two 60 s recordings have been made with the tin-can: one with each antenna. The recordings are evaluated in post-processing with a snapshot based SDR receiver. 10^4 snapshots of 10 ms are extracted from each recording, as this relates to a typical snapshot size [44].

The snapshot based SDR evaluates open service (OS) signals form GPS and Galileo. The acquisition algorithm uses GPS L1 C/A signals with a coherent integration length of 1 ms and 10 incoherently added epochs. This means that an average of 9.5 ms of

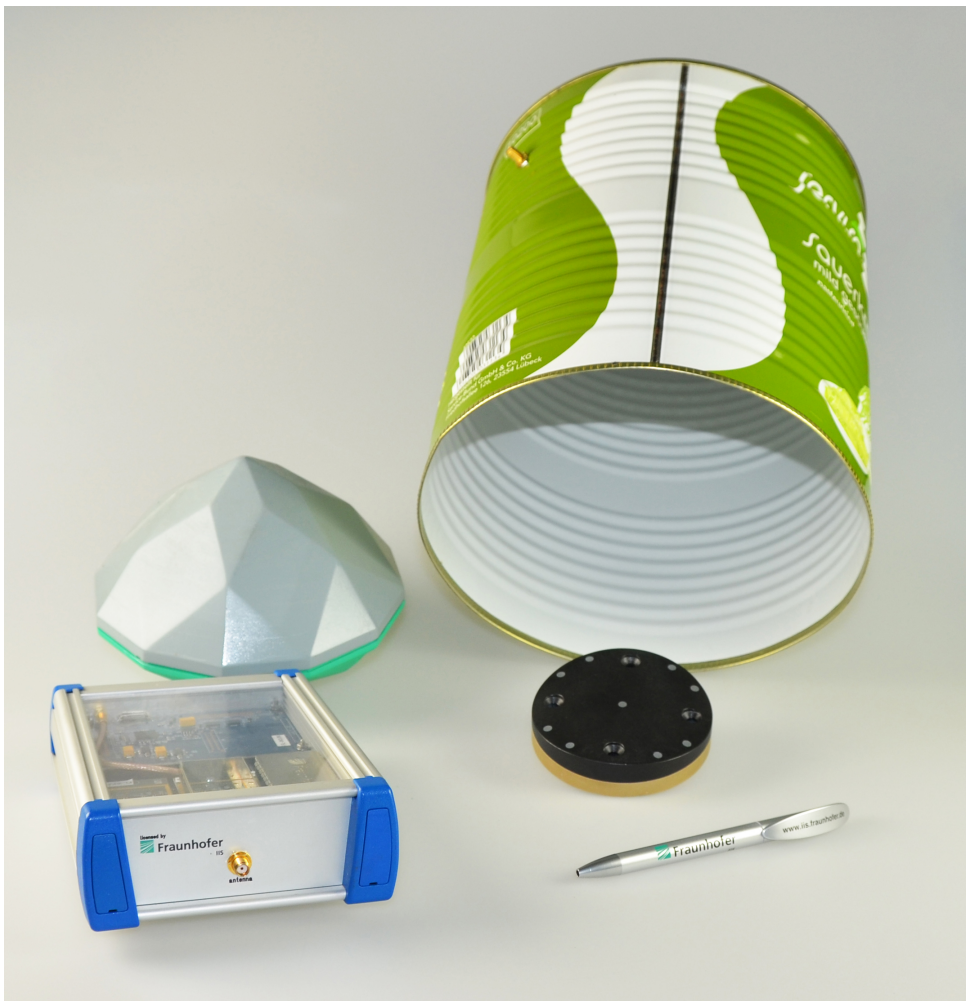


Figure 4. Photo of the system components

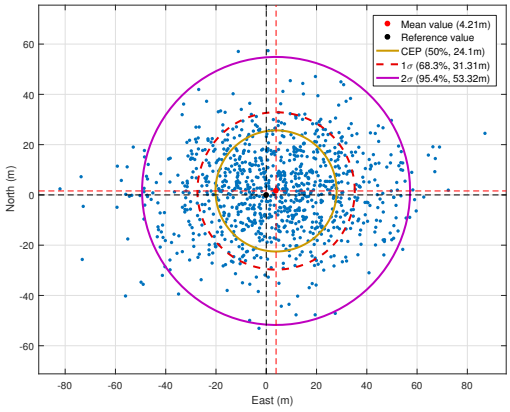
data is used for this configuration, with a Doppler precision of ± 500 Hz. For Galileo, E1B signals with a coherent acquisition of 4 ms and 2 incoherent epochs are selected. This relates to an average of 7 ms of data used, with a Doppler precision of ± 125 Hz. As such, it is expected that for these configurations Galileo E1B will have superior Doppler resolution and coherent integration gain, but inferior overall processing gain. Therefore, overall poorer steering vector estimation is expected for Galileo for this setup.

The acquisition algorithm estimates the array steering vector for each satellite [6]. These array steering vectors are then used for the spoofing detection, according to the algorithm described in the Section: *Spoofing detection*. The detection is done with different values for the steering vector angular threshold ξ_{Th}, as this will indicate for which values the detector can be tuned. Thereafter more analysis of is done to determine the optimal threshold setting for the detectors. In this evaluation the spatial angular threshold θ_{U} is set to 1°. Three sets of evaluations are done:

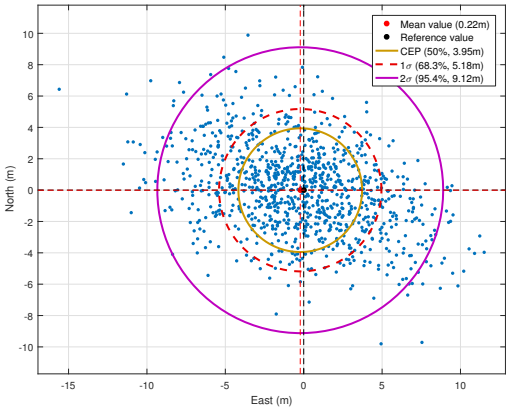
- a two-channel evaluation with the dual-polarized antenna,
- a four-channel evaluation with the CRPA antenna, and
- a two-channel evaluation with the four-element CRPA, where two elements are selected. This allows a fair comparison to the dual-polarized antenna, as the same number of receiver channels are used.

RESULTS

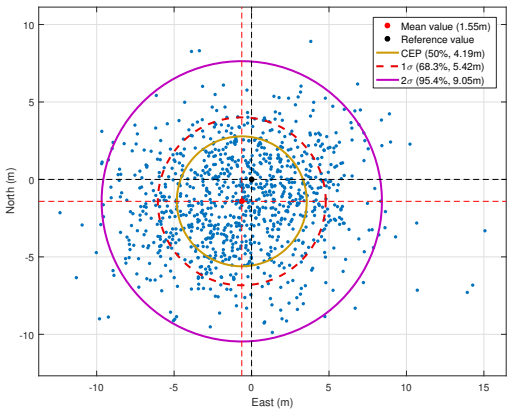
The results are presented in this section. The general results of the snapshot are presented first, followed by individual comparisons of the tin-can and open-sky tests. Finally, the statistics of the tin-can and the open-sky are compared to each other, for a further analysis of the performance.



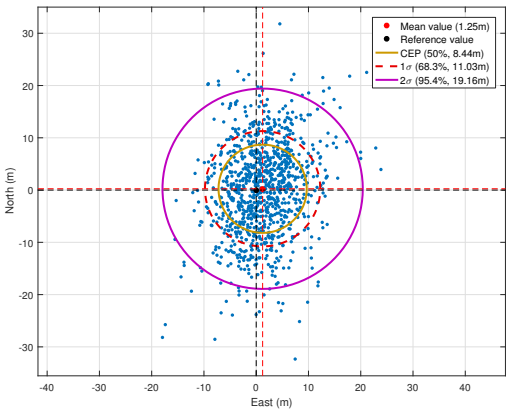
(a) Tin-Can GPS L1 C/A Dual-Pol



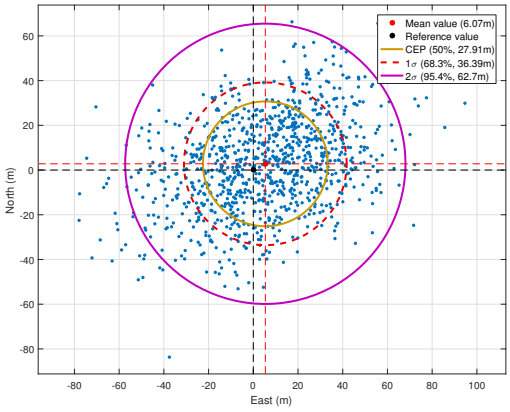
(b) Tin-Can Galileo E1B Dual-Pol



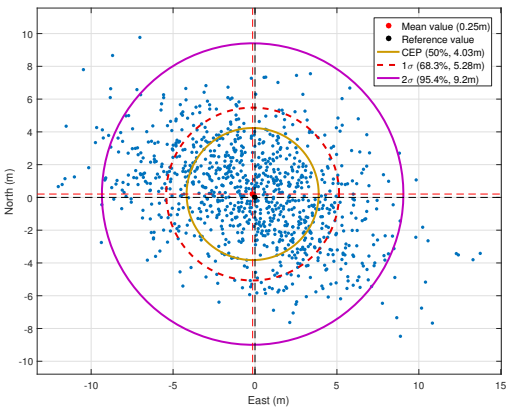
(c) Open-sky GPS L1 C/A Dual-Pol



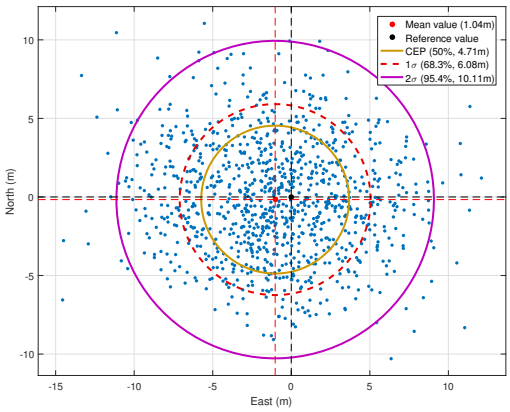
(d) Open-sky Galileo E1B Dual-Pol



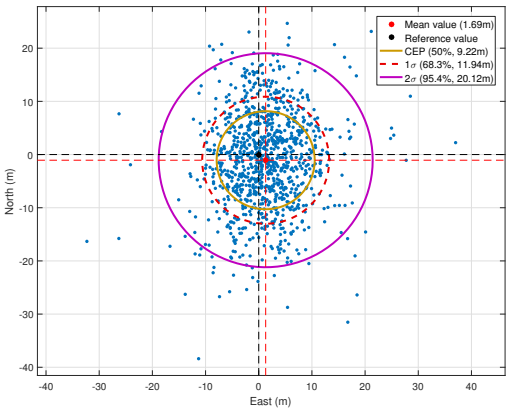
(e) Tin-Can GPS L1 C/A Antenna Array



(f) Tin-Can Galileo E1B Antenna Array



(g) Open-sky GPS L1 C/A Antenna Array



(h) Open-sky Galileo E1B Antenna Array

Figure 5. PVT results for different test setups and signals

General results

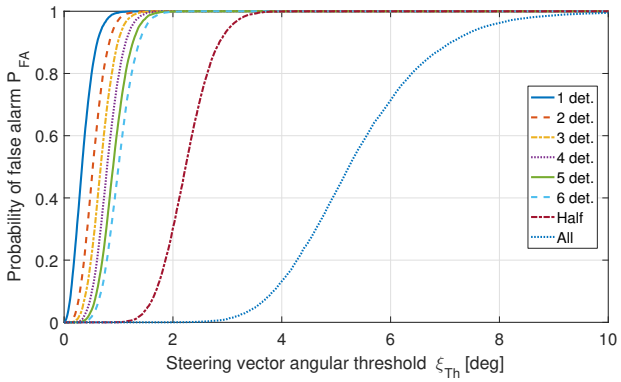
The average number of satellites acquired is shown in Table 1. In both test setups, more GPS satellites are available than Galileo – this is also reflected in the received signals. On average the dual-polarized antenna received more signals than the antenna array.

Table 1. Comparison of the average number of acquired satellites

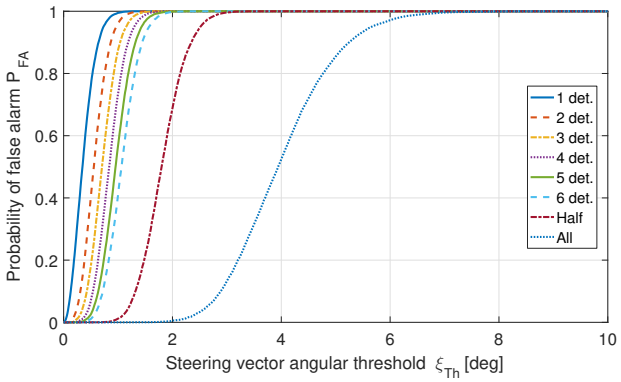
Setup	L1 C/A: dual-polarized	E1B: dual-polarized	L1 C/A: 4-element array	E1B: 4-element array
Tin-can	9.82	7.99	8.86	7.99
Open-sky	8.48	4.93	8.02	5.59

In all of the recordings sufficient satellites where acquired to calculate a PVT solution. The PVT statistic for both the tin-can test and the outdoor measurements are shown in Figure 5.

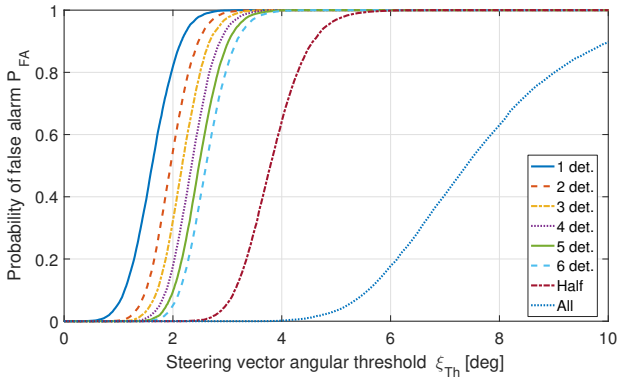
Tin-can results



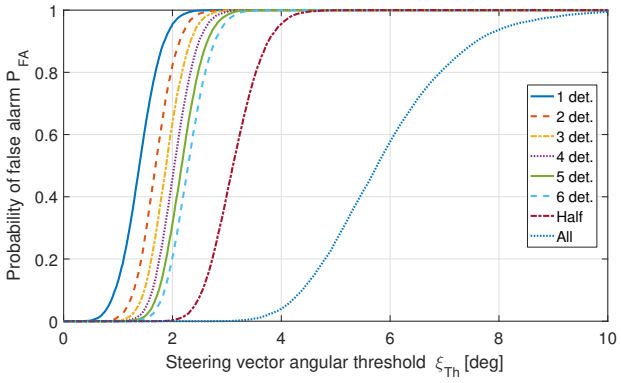
(a) Dual-Pol with GPS L1 C/A



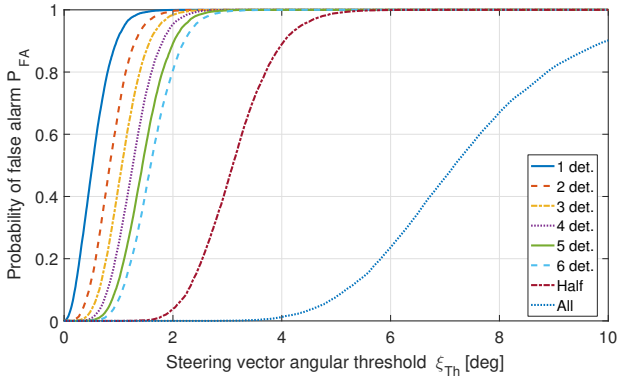
(b) Dual-Pol with Galileo E1B



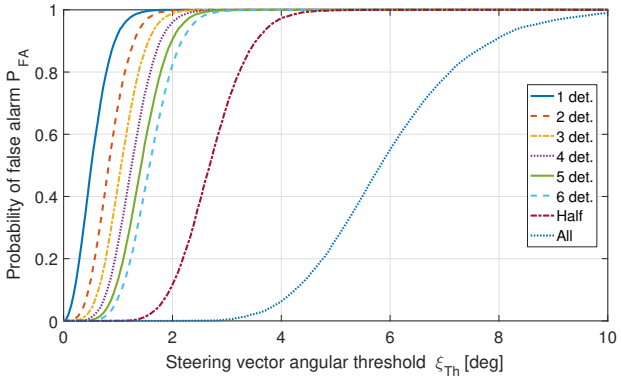
(c) 4-Element array with GPS L1 C/A



(d) 4-Element array with Galileo E1B



(e) 4-Element array using 2 elements with GPS L1 C/A



(f) 4-Element array using 2 elements with Galileo E1B

Figure 6. Probability of spoofing detection P_D for different signals and antennas

The results for the three antenna configurations and the two signal types are shown in Figure 6. In each sub-figure one detection (denoted as "1 det." in the figures) means that only a single value in the upper triangle of the detection matrix **D** was detected, i.e. two satellites are suspected to have similar array steering vectors. Therefore, they are assumed to be spatially coherent and to be from a spoofed source. Likewise, two to six detections indicate how many values are flagged as being detected in the detection matrix **D**.

There are a maximum if 11 satellites, hence, a total of 55 values can be in the upper triangle of the detection matrix **D**. As all signals are spoofed, due to the tin-can, we expect that all values in the matrix **D** to be detected. The case where this is true, is the upper bound to guarantee successful detection (denoted as "All" in the figures). It should be noted that if two satellites happen to be close to each other, the false positive removal will result in this upper bound to be unobtainable. The two satellites which are near to each other will consequently be removed. Further, if dense constellations or multiple systems are considered, then it is likely that near lying satellites will result in multiple detections to be discarded. This highlights why GPS and Galileo are separated from each other in this evaluation. Due to this limitation of having all of the values detected, an alternative method is to see when at least half of the values in the detection matrix **D** is detected (denoted as "Half" in the figures). This represents the median number of detection for a given probability.

Comparing the results from GPS (Figures 6(a), 6(c) and 6(e)) and Galileo (Figures 6(b), 6(d) and 6(f)), the low number of detections (i.e. 1 to 6 det.) are similar. The "All" detection are better for GPS, this is mainly due to the fact that a longer effective integration time is used than with Galileo (better steering vector estimates). Further, as only E1B (data) is used for Galileo, and not the joined E1B/C, a loss of 3 dB signal power is perceived. Thus, lower effective C/N_0s are expected for Galileo. A joint E1B/C acquisition algorithm is a necessary future improvement of the used snapshot SDR.

Open-sky results

The results for the three antenna configurations with an open sky recording for the same configurations are shown in Figure 7.

The detections in the open-sky results (Figure 7) are at significantly larger steering vector angles than in the tin-can results (Figure 6). These detections are also not as smooth, as each pair of satellites have different similarities to each other. This is dependent on the satellite constellation and is more evident with smaller constellations, like with Galileo in this case. Lastly, as Galileo has lower number of acquired satellites, the "Half" detection is in some cases lower than the "6 det.".

Statistical comparison

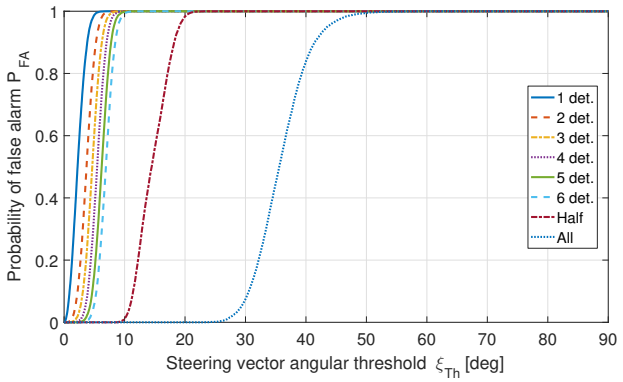
The probability density function (PDF) for the angle of each value in the upper triangle of the normalized correlation matrix $\mathbf{C}_{\text{norm}}$, could be used for optimal threshold setting [45]. This allows better analysis of the underlying statistics to be done. Figure 8 shows the PDFs for the tin-can measurements. These results are the PDF for the probability of detection, i.e. the statistics of the null-hypothesis of Equation 7. In all three cases the results for the GPS and Galileo satellites have similar forms, but are not identical. This shows that the use of the signal type and acquisition have an influence on the correlation values. However, the difference as caused by the antenna type and number of antenna elements is greater, showing the importance of the antenna selection.

The PDF for the open-sky recording is shown in Figure 9. This relates to the PDF for the probability of false alarm (alternative hypothesis of Equation 7). The dual-polarized antenna has a single peak. This shows the coherency of the polarization of real received RHCP signals. In a real scenario the LHCP components would be low, but some components will be visible due to multipath reflections and antenna imperfections. The antenna array in strong contrast as multiple peaks. Each peak is the contribution of each individual satellite, due to its unique DOA. These PDFs are considerable more difficult to classify, as it is a compound distribution.

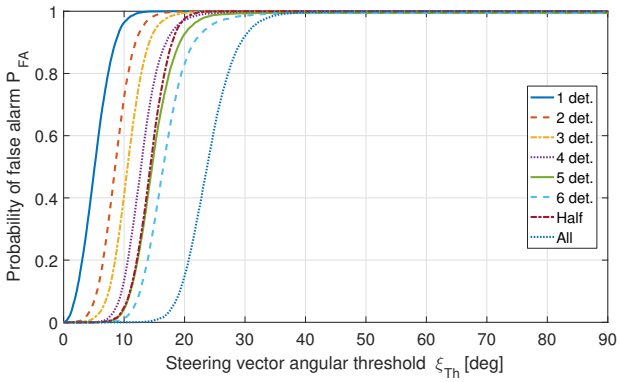
The PDFs can now be used to calculate the probability of detection and the probability of false alarm for a given threshold setting in the detector. A method to do this is the calculate the cumulative distribution function (CDF) for the alternative hypothesis (open-sky) This is also called the "left tail probability" of the PDF [45]. The conjugate cumulative probability (i.e. 1 - CDF), also referred to as the "right tail probability", is calculated for the null hypothesis (tin-can). These two distribution allow the direct determination of the probability of detection, missed detection, false alarm and correct rejection. The plots are shown in Figure 10.

Another method to directly compare the results for the detectors is the receiver operating characteristic (ROC). This directly compares the probability of detection and the probability of false alarm for each set. Figure 11 compares the ROC for the detectors.

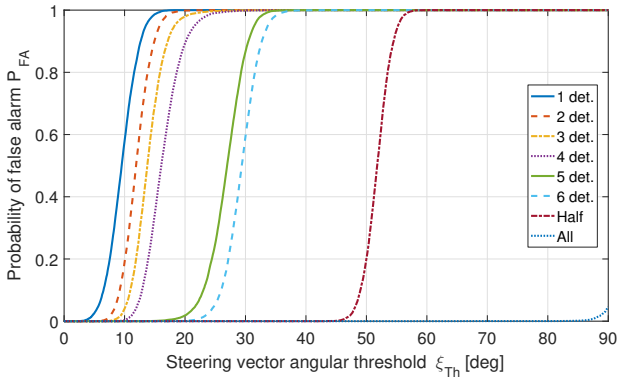
One method to optimize the detector is to select the probability of false alarm to be equal to the probability of missed detection. This minimizes the probability of error for both false decision cases. This is only true under the assumption that a tin-can attack occurring is equally probable to no attack. In the case of the test data, this is a fair assumption; however, in reality the occurrence of a spoofing attack is rather unlikely.



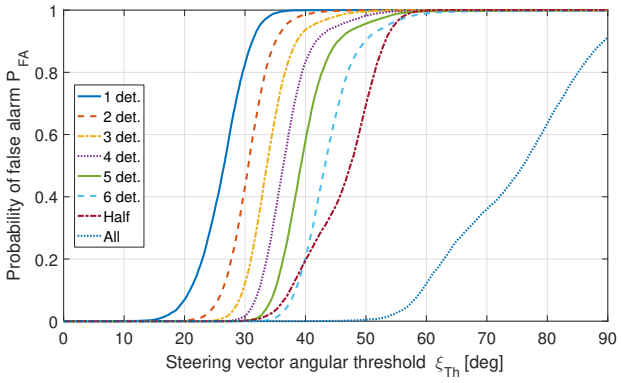
(a) Dual-Pol with GPS L1 C/A



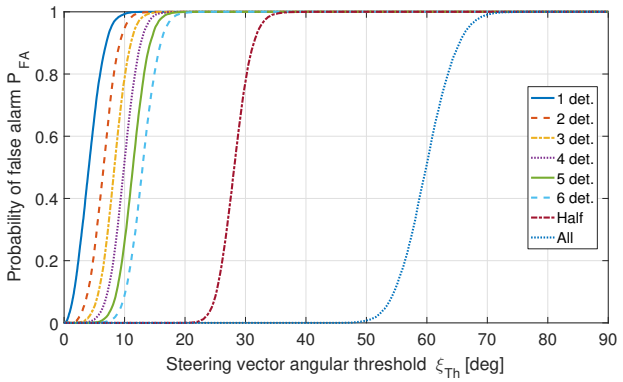
(b) Dual-Pol with Galileo E1B



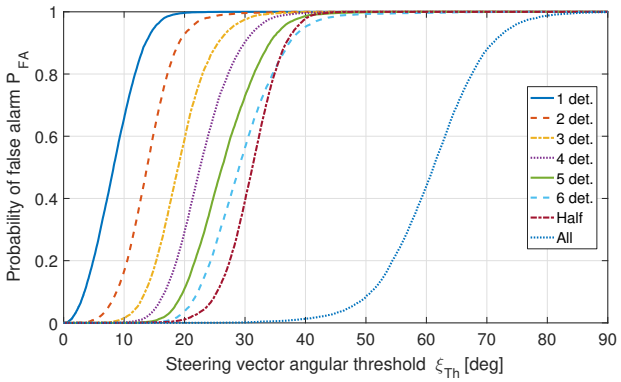
(c) 4-Element array with GPS L1 C/A



(d) 4-Element array with Galileo E1B



(e) 4-Element array using 2 elements with GPS L1 C/A



(f) 4-Element array using 2 elements with Galileo E1B

Figure 7. Probability of false alarm with real signals P_{FA} for different signals and antennas

In the CDF plots of Figure 10, this represents the intersection of the two statistics. This threshold for each scenario is determined, and plotted in the graphs. The error probabilities are also shown in the Figures. For a better one-to-one comparison, these statistics are shown in Table 2.

Table 2. Comparison of optimal detection threshold settings and probabilities

Antenna	Signal	Threshold λ [deg]	Error Probability [%]	Correct Probability [%]
Dual-polarized	L1CA	4.5	7.7	92.3
Dual-polarized	E1B	4.1	3.8	96.2
4-element array	L1CA	8.7	1.56	98.44
4-element array	E1B	11.1	0.005	99.99
2-element array	L1CA	6.7	6.1	93.9
2-element array	E1B	6.4	2.8	97.2

From the table, it can be seen that the 4-element antenna array has the best detection probability. The 2-element array and the

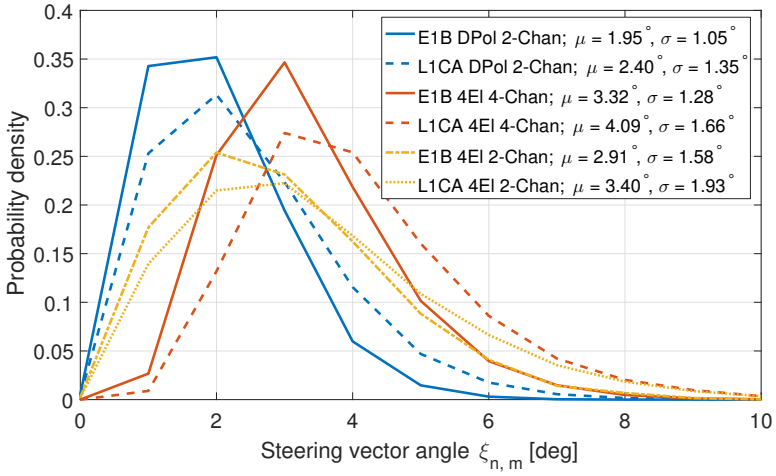


Figure 8. PDF for all combinations of the array steering angles $\xi_{n,m}$ in the tin-can attack

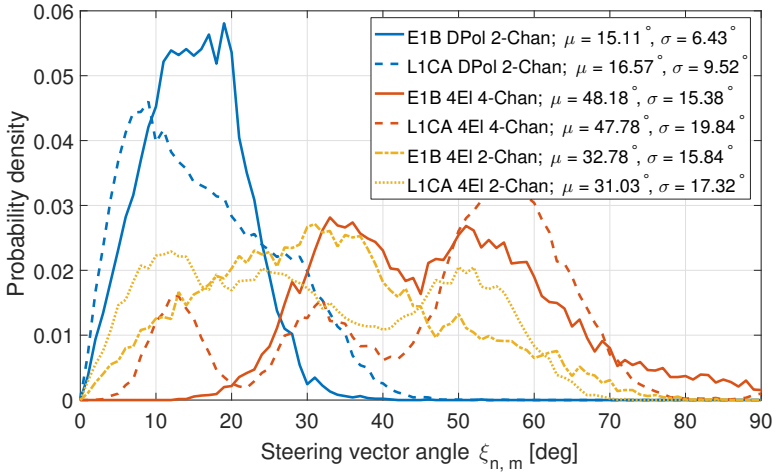


Figure 9. PDF for all combinations of the array steering angles $\xi_{n,m}$ for the open sky

dual-polarized antenna have comparable performance; however this is constellation dependent as a 2-element array has a plane of ambiguities. The differences between GPS and Galileo are visible, but small. This shows the impact that the different coherent and incoherent integration times, as well as the satellite constellations. The detection performance represent the probabilities for a single detection, and will be improved a a system of detection are evaluated.

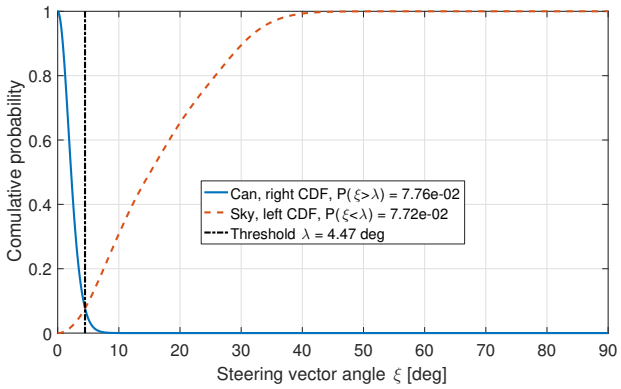
CONCLUSION

A tin-can cooperative spoofing attack has been demonstrated and the current short-comings to deal with such attacks have been highlighted. In the case of snapshot receivers, the difficulty is further increased, hence, emphasizing the need for alternative detection methods. A spoofing detection methods that requires either an array of antennas or a dual-polarized antenna was presented.

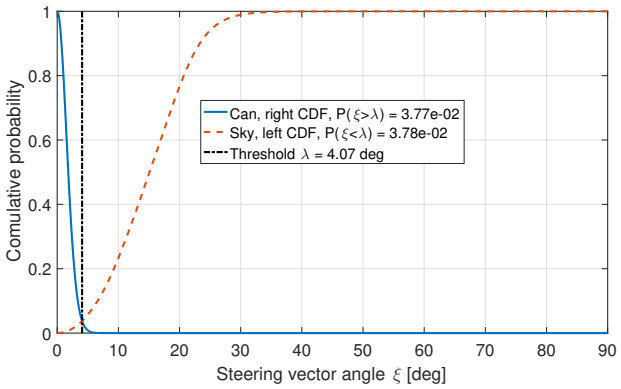
Measurement results of a tin-can attack has shown how simple the attack is as well as how it can be detected. The signal type, C/N_0 of the signals, the effective integration time used in acquisition, and the DOA of each satellite influences the detection performance. The array consisting of four antenna elements showed superior results for the detection metrics, but the dual-polarized antenna and the two-element antenna array also showed adequate performance. The analytic threshold determination showed that for the optimal threshold setting of the poorest performing signal and antenna, only a 7.7 % error probability can be achieved. For the best case it was as low as 0.08 %.

This paper demonstrated a problem and a possible solution to cooperative spoofing attacks. A system of detectors was developed, analyzed, and optimal detector thresholds where determine. As future research it is proposed to investigate further methods to use the system of detectors to improve spoofing detection.

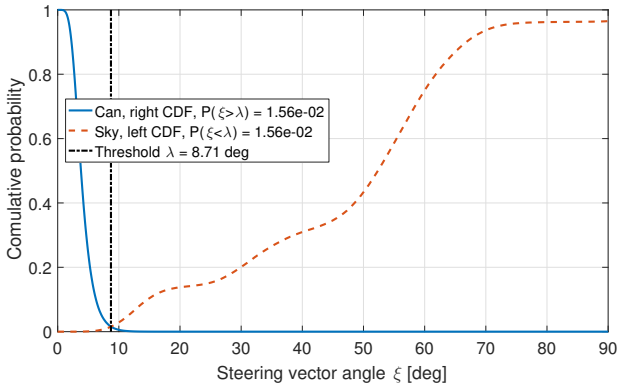
A tin-can spoofing attack is simple and cheap, therefore it is a significant threat. Based on the results of this paper, the authors recommend developers to use of multiple receiver antennas or a dual-polarized receiver antenna to increase the robustness for



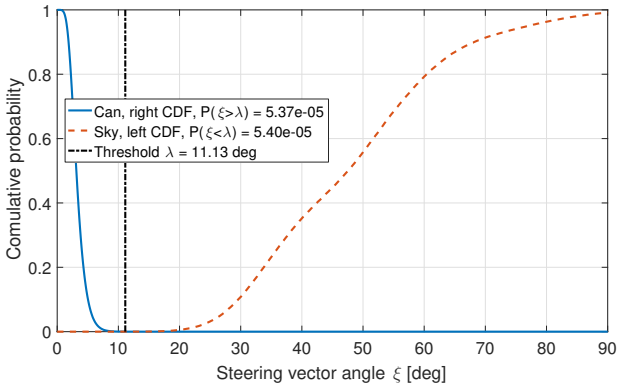
(a) Dual-Pol with GPS L1 C/A



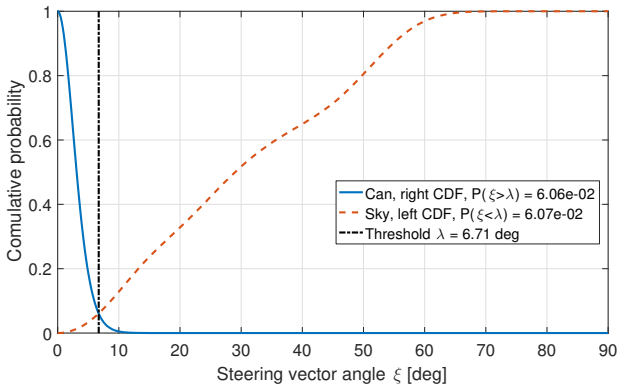
(b) Dual-Pol with Galileo E1B



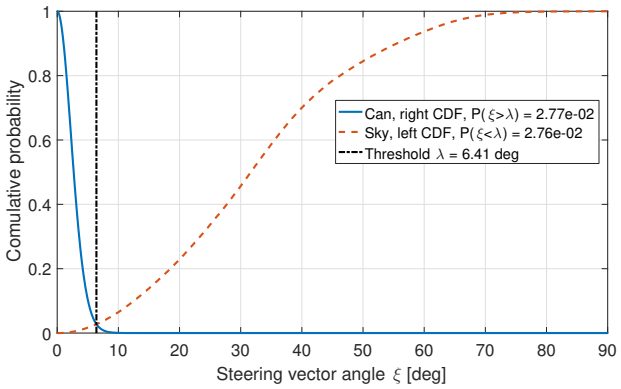
(c) 4-Element array with GPS L1 C/A



(d) 4-Element array with Galileo E1B



(e) 4-Element array using 2 elements with GPS L1 C/A



(f) 4-Element array using 2 elements with Galileo E1B

Figure 10. Statistical evaluation for detector threshold setting

secure GNSS applications. This would increase spoofing detection capabilities above a single RHCP, or even worse a linear-polarized, antenna. Further, the awareness of spoofing threats to security tasked authorities are crucial for improving public GNSS reliability, safety and confidence. Lastly, receiver developers should proactively consider spoofing threats, and implement appropriate counter measures.

REFERENCES

[1] C4ADS, *Above us only stars: Exposing GPS spoofing in Russia and Syria*, 2019.

[2] V. Lucas-Sabola, G. Seco-Granados, J. A. López-Salcedo, J. A. Garcia-Molina, and M. Crisci, "Cloud GNSS receivers: New advanced applications made possible," in *2016 International Conference on Localization and GNSS (ICL-GNSS)*, pp. 1–6, June 2016.

[3] A. Rügamer, D. Rubino, I. Lukčin, S. Taschke, M. Stahl, and W. Felber, "Secure Position and Time Information by Server Side PRS Snapshot Processing," in *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pp. 3002–3017, September 2016.

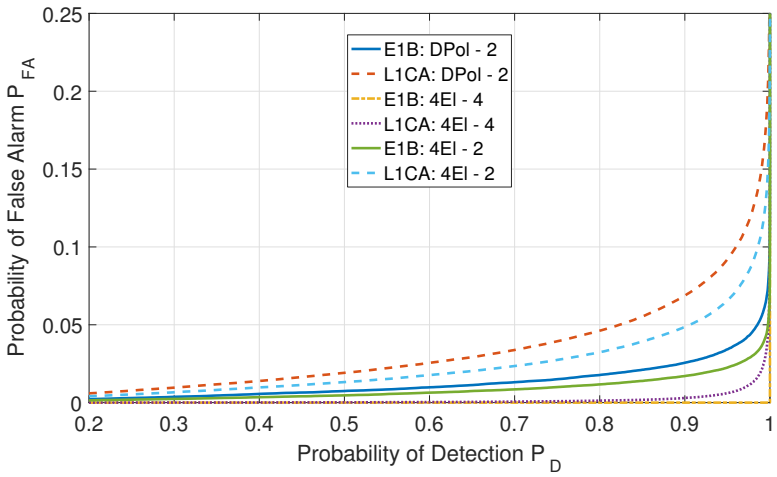


Figure 11. ROC

[4] I. Fernández-Hernández and K. Borre, "Snapshot positioning without initial information," *GPS Solutions*, vol. 20, pp. 605–616, Oct 2016.

[5] F. van Diggelen, *A-GPS: Assisted GPS, GNSS, and SBAS*. Artech House, 2009.

[6] J. R. van der Merwe, A. Fernández-Dans Goicoechea, A. Rügamer, X. Zubizarreta, D. Rubino, and W. Felber, "Multi-antenna snapshot receiver," in *2019 European Navigation Conference (ENC)*, April 2019.

[7] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, pp. 1258–1270, June 2016.

[8] C. Günther, "A survey of spoofing and counter-measures," *Navigation: Journal of the Institute of Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[9] A. Rügamer and D. Kowalewski, "Jamming and Spoofing of GNSS Signals - An Underestimated Risk?!," in *Proceedings, FIG Working Week 2015, May 17 - 21, 2015, Sofia, Bulgaria*, 2015.

[10] 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*, vol. 2012, pp. 1–16, 2012.

[11] J. R. van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*, pp. 91–99, May 2018.

[12] Ajinkya, "How to play Pokemon Go without moving on Android," 2019.

[13] Spy Blog, "Road pricing gps signal jammers? What about cheap GPS position spoofing devices?," 2007.

[14] Resilient Navigation and Timing Foundation, "GPS spoofing a growing problem for Uber - solid driver," 2018.

[15] S. R. Taylor, S. Kandaswamy, T. Evans, and D. Mahaffey, "Market survey of location-based offender tracking technologies, version 1.1," 2016.

[16] R. S. Gable, "Let's stop using ankle bracelets to monitor offenders," 2017.

[17] N. Ungerleider, "Spoofed satellite feeds trouble Google's global fishing watch," 2014.

[18] F. T. Ulaby, E. Michielssen, and U. Ravaioli, *Fundamentals of Applied Electromagnetics*. Pearson Education, 2014.

[19] G. Rehm, "How to build a tin can waveguide WiFi antenna: for 802.11(b or g) wireless networks or other 2.4GHz applications," 2007.

[20] G. Rehm, "How to make a tin can directional WiFi antenna to extend your communication after an EMP," 2017.

[21] G. Charvat, J. Williams, A. Fenn, S. Kogon, and J. Herd, "RES.LL-003 build a small radar system capable of sensing range, Doppler, and synthetic aperture radar imaging," 2011.

[22] M. Psiaki, "Techniques for spoofing and for spoofing mitigation," in *International Symposium on Navigation and Timing, ENAC Toulouse, France* (M. L. Psiaki, ed.), 2015.

[23] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[24] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio, and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, pp. 1888–1896, 2001.

[25] M. Psiaki, S. Powell, and B. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in

Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), 2013.

[26] W. Qi, Y. Zhang, and X. Liu, "A GNSS anti-spoofing technology based on doppler shift in vehicle networking," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 725–729, Sep. 2016.

[27] J. Tu, X. Zhan, X. Zhang, Z. Zhang, and S. Jing, "Low-complexity GNSS anti-spoofing technique based on Doppler frequency difference monitoring," *IET Radar, Sonar Navigation*, vol. 12, no. 9, pp. 1058–1065, 2018.

[28] S. Khanafseh, N. Roshan, S. Langel, F. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, pp. 1232–1239, May 2014.

[29] L. Chen, W. Meng, S. Han, and C. Li, "Subspace projection based anti-spoofing algorithm for GNSS receiver," in *CSNC 2015*, 2015.

[30] J. Nielsen, V. Dehghanian, and G. Lachapelle, "Effectiveness of GNSS spoofing countermeasure based on receiver CNR measurements," 2012.

[31] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements," *International Journal of Satellite Communications and Networking*, vol. 30, no. 4, pp. 181–191, 2012.

[32] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for GPS L1 C/A signals," *Navigation*, vol. 61, no. 1, pp. 1–11, 2014.

[33] A. Broumandan, A. Jafarnia-Jahromi, G. Lachapelle, and R. T. Ioannides, "An approach to discriminate GNSS spoofing from multipath fading," in *2016 8th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pp. 1–10, Dec 2016.

[34] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, pp. 2937 – 2948, 2013.

[35] M. Appel, A. Konovaltsev, and M. Meurer, "Joint antenna array attitude tracking and spoofing detection based on phase difference measurements," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016) September 12 - 16, 2016*, pp. 3018 – 3026, 2016.

[36] E. Pérez Marcos, A. Konovaltsev, S. Caizzone, M. Cuntz, K. Yinusa, W. Elmarissi, and M. Meurer, "Interference and spoofing detection for GNSS maritime applications using direction of arrival and conformal antenna array," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, pp. 2907 – 2922, 2018.

[37] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of spatial processing approaches for GNSS structural interference detection and mitigation," *Proceedings of the IEEE*, vol. 104, pp. 1246–1257, June 2016.

[38] W. De Wilde, J. Sleewaegen, B. Bougard, G. Cuypers, A. Popugaev, M. Landmann, C. Schirmer, D. E. Roca, J. A. López-Salcedo, and G. Gonzalo-Seco, "Authentication by polarization: A powerful anti-spoofing method," in *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*, pp. 3643 – 3658, September 2018.

[39] D. Egea-Roca, A. Tripiana-Caballero, J. A. López-Salcedo, G. Seco-Granados, W. De Wilde, B. Bougard, J.-M. Sleewaegen, and A. Popugaev, "GNSS measurement exclusion and weighting with a dual polarized antenna: The FANTASTIC project," in *2018 8th International Conference on Localization and GNSS (ICL-GNSS)*, pp. 1–6, June 2018.

[40] D. Egea-Roca, A. Tripiana-Caballero, J. A. López-Salcedo, G. Seco-Granados, W. De Wilde, B. Bougard, J.-M. Sleewaegen, and A. Popugaev, "Design, implementation and validation of a GNSS measurement exclusion and weighting function with a dual polarized antenna," *Sensors*, vol. 18, no. 12, 2018.

[41] J. R. van der Merwe, A. Rügamer, A. Fernández-Dans Goicoechea, and W. Felber, "Blind spoofing detection using a multi-antenna snapshot receiver," in *2019 International Conference on Localization and GNSS (ICL-GNSS)*, June 2019.

[42] A. Rügamer, F. Förster, M. Stahl, and G. Rohmer, "A flexible and portable multiband GNSS front-end system," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS 2012, September 17-21, 2012, Nashville, Tennessee, USA*, September 2012.

[43] A. Popugaev, M. Tessema, and W. De Wilde, "A novel broadband dual circularly polarized GNSS antenna," in *European Microwave Conference in Central Europe (EuMCE)*, 2019.

[44] A. Rügamer, D. Rubino, X. Zubizarreta, W. Felber, J. Wendel, and D. Pfaffelhuber, "Spoofing resistant UAVs," in *Proceedings of the International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, 2018.

[45] S. M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, vol. 2 of *Prentice-Hall Signal processing series*. Prentice Hall, 1998.