# SPREE: A Spoofing Resistant GPS Receiver

Aanjhan Ranganathan, Hildur Ólafsdóttir, Srdjan Capkun
aanjhan@inf.ethz.ch, ohildur@inf.ethz.ch, capkuns@inf.ethz.ch
Department of Computer Science
ETH Zurich, Switzerland

## ABSTRACT

Global Positioning System (GPS) is used ubiquitously in a wide variety of applications ranging from navigation and tracking to modern smart grids and communication networks. However, it has been demonstrated that modern GPS receivers are vulnerable to signal spoofing attacks. For example, today it is possible to change the course of a ship or force a drone to land in a hostile area by simply spoofing GPS signals. Several countermeasures have been proposed in the past to detect GPS spoofing attacks. These countermeasures offer protection only against naive attackers. They are incapable of detecting strong attackers such as those capable of seamlessly taking over a GPS receiver, which is currently receiving legitimate satellite signals, and spoofing them to an arbitrary location. Also, there is no hardware platform that can be used to compare and evaluate the effectiveness of existing countermeasures in real-world scenarios.

In this work, we present SPREE, which is, to the best of our knowledge, the first GPS receiver capable of detecting all spoofing attacks described in the literature. Our novel spoofing detection technique called auxiliary peak tracking enables detection of even a strong attacker capable of executing the seamless takeover attack. We implement and evaluate our receiver against three different sets of GPS signal traces: (i) a public repository of spoofing traces, (ii) signals collected through our own wardriving effort and (iii) using commercial GPS signal generators. Our evaluations show that SPREE constraints even a strong attacker (capable of seamless takeover attack) from spoofing the receiver to a location not more than 1 km away from its true location. This is a significant improvement over modern GPS receivers that can be spoofed to any arbitrary location. Finally, we release our implementation and datasets to the community for further research and development.

## CCS Concepts

**•Security and privacy → Mobile and wireless security; •Computer systems organization → Embedded and cyber-physical systems; •Information systems → Global positioning systems;**

## Keywords

GPS Spoofing; Receiver Architecture



*MobiCom'16, October 03 - 07, 2016, New York City, NY, USA*



ISBN 978-1-4503-4226-1/16/10…$15.00

DOI: http://dx.doi.org/10.1145/2973750.2973753

## 1. INTRODUCTION

Today, a number of security- and safety-critical applications rely on Global Positioning Systems (GPS) [26] for positioning and navigation. A wide-range of applications such as civilian and military navigation, people and asset tracking, emergency rescue and support, mining and exploration, atmospheric studies, smart grids, modern communication systems use GPS for localization and timing. GPS is a satellite-based navigation system that consists of more than 24 satellites orbiting at more than 20,000 km above the earth. Each satellite continuously broadcasts data called *navigation messages* containing its precise time of transmission and the satellite's location. The GPS receiver on the ground receives each of the navigation messages and estimates their time of arrival. Based on the time of transmission that is contained in the navigation message itself and its time of arrival, the receiver computes its distance to each of the visible satellites. Once the receiver acquires the navigation messages from at least four satellites, the GPS receiver estimates its own location and precise time using the standard technique of multilateration.

However, the civilian GPS navigation messages that are transmitted by the satellites lack any form of signal authentication. This is one of the prime reasons GPS is vulnerable to *signal spoofing* attacks. In a GPS spoofing attack, an attacker transmits specially crafted signals identical to those of the satellites but with a power that is sufficient to overshadow the legitimate GPS satellite signals. The GPS receiver then computes a false location and time based on the stronger spoofing signal transmitted by the attacker. As a result, today, it is possible to spoof a GPS receiver to any arbitrary location. For example, researchers have demonstrated the insecurity of GPS-based navigation by diverting the course of a yacht using spoofed GPS signals [9]. A similar hijack was also successfully executed on a drone using a GPS spoofer that costs less than $1000. More recently, researchers demonstrated a GPS signal generator that can be built for less than $300 [3]. The increasing availability of low-cost radio hardware platforms [1] make it feasible to execute such attacks with less than few hundred dollars worth of hardware equipment. More advanced attacks were demonstrated in [28,33] in which the attackers *takeover* a target re-

ceiver that is already locked onto (i.e., continuously receiving navigation messages) authentic satellite signals without the receiver noticing any disruption or loss of navigation data. It was shown that a variety of commercial GPS receivers were vulnerable and in some cases even caused permanent damage to the receivers. It is thus evident that these threats are real and it is important to secure GPS from such signal spoofing attacks.

Although spoofing attacks can be, to a certain extent, mitigated by adding cryptographic authentication to the navigation messages (e.g., military GPS systems where the spreading codes are secret), their use requires distribution and management of shared secrets, which makes them impractical for majority of applications. Even with cryptographic authentication, the system is not protected against relay attacks where an attacker simply records and replays the radio signals to the receiver [29]. Several countermeasures that do not require cryptographic authentication were proposed in recent years either to detect or to mitigate signal spoofing attacks. They rely on detecting anomalies in certain physical characteristics of the signal such as received satellite signal strength, ambient noise floor levels, automatic gain control [10] values and other data that are readily available as *receiver observables* on modern GPS receivers. Some other countermeasures leveraged the signal's spatial characteristics [27, 32] such as the received GPS signal's direction or angle of arrival. All the above mentioned countermeasures are ineffective against attackers capable of manipulating navigation message contents in real time or a seamless takeover attack [28, 33]. Additionally, majority of these solutions are not reliable in an environment with strong multipath (signal copies that reach the receiver with a time delay due to reflections in the environment etc.) or in the case of a mobile receiver. Moreover, today there is no receiver platform that can be used to compare and evaluate the effectiveness of these countermeasures in real-world scenarios.

In this work, we present a novel GPS receiver which we refer to as SPREE and make the following contributions: SPREE is to the best of our knowledge, the first commercially off the shelf, single-antenna, receiver capable of detecting or significantly limiting all known GPS spoofing attacks described in the literature. SPREE does not rely on GPS signal authentication and therefore can be used to detect both civilian and military GPS spoofing attacks. Additionally, it is designed to be standalone and does not depend on other hardware such as antennas, additional sensors or alternative sources of location information (like maps or inertial navigation systems). In SPREE, we introduce a novel spoofing detection technique called auxiliary peak tracking that limits even a strong attacker (e.g., seamless takeover) from being able to move (spoof) a receiver to any arbitrary location or time. We leverage the presence of authentic signals in addition to the attacker's signals to detect spoofing attacks. We implement SPREE by modifying an open source software-defined GPS receiver [17] and evaluate it against different signal data sets including the de-facto standard of a publicly available repository of GPS signal spoofing traces (Texas Spoofing Battery (TEXBAT) [19]). Furthermore, we evaluate SPREE against COTS GPS simulators, and our own traces obtained through an extensive wardriving effort of over 200 km. Our analysis shows that SPREE can reliably detect any manipulations to the navigation message contents. Also, SPREE severely limits even strong attackers capable of taking over a receiver that is currently locked (receiving and decoding) on to legitimate satellite signals without being noticed. Our evaluations showed that such a strong attacker could offset the SPREE's location to a maximum of 1 km away from its true location. As a result, with SPREE deployed, an attacker will not be able to deviate the course of a ship or force an unmanned aerial vehicle to land in areas more than 1 km away from its safe landing zones. This is a significant improvement over modern GPS receivers that can be trivially spoofed to any arbitrary location in the world. Finally, we release our implementation and a set of recorded GPS signal traces used for evaluating SPREE to the community for further research and development [7].

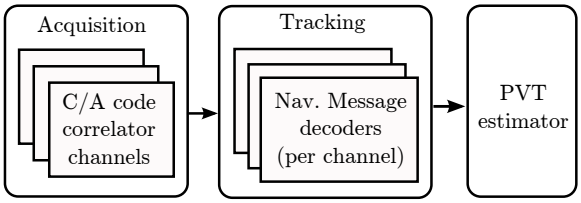


Figure 1: GPS receiver architecture. The RF front-end (not shown in the figure) preprocesses the received satellite signals. The acquisition module searches for any visible satellite signals and if detected forwards it to the tracking module. The tracking module decodes the navigation data which is used in estimating the position, velocity and time.

# 2. GPS OVERVIEW

## 2.1 GPS Satellite System

GPS consists of more than 24 satellites orbiting the earth at more than 20,000 km above the ground. Each satellite is equipped with high-precision atomic clocks and hence the timing information available from all the satellites are in near-perfect synchronization. Each satellite transmits messages referred to as the *navigation messages* that are spread using pseudorandom codes that are unique to a specific satellite.

The navigation data transmitted by each of the satellites consists of a 1500 bit long data frame which is divided into five subframes [12]. Subframes 1, 2 and 3 carry the same data across each frame. The data contained in subframes 4 and 5 is split into 25 pages and is transmitted over 25 navigation data frames. The navigation data is transmitted at 50 bps with the duration of each subframe being 6 seconds. Each frame lasts 30 seconds and the entire navigation message, containing 25 such frames, takes 12.5 minutes to be received completely by a receiver. The first subframe mainly includes satellite clock information. The second and third subframes contain the ephemeris, i.e., information related to the satellite's orbit and is used in computing the satellite position. Subframes 4 and 5 contain the almanac data, i.e., the satellite orbital and clock information with reduced precision for all satellites.

## 2.2 GPS Receiver

A typical GPS receiver consists of four main building blocks: (i) RF front-end, (ii) Acquisition module, (iii) Tracking module and (iv) Position, Velocity, Time (PVT) estimator module. The RF front-end block pre-processes the

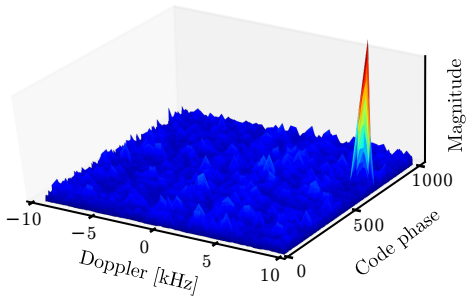


Figure 2: GPS Signal Acquisition. The result of the correlation for a real satellite signal acquisition.

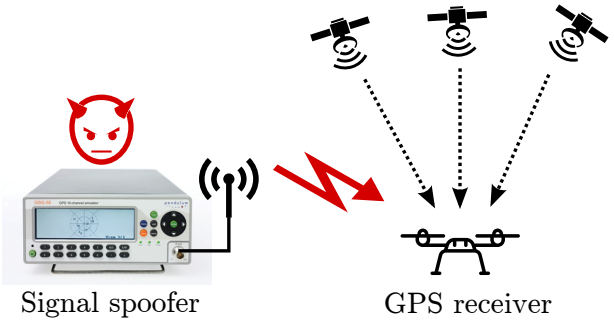


Figure 3: Spoofing attack. The attacker uses a commercial GPS signal simulator to transmit signals identical to legitimate satellite signals but with a higher power to overshadow the legitimate signals. The receiver computes a false location and time based on the spoofing signals.

received satellite signals and forwards it to the acquisition module. The acquisition module is responsible for searching for any satellite signals and forwarding the signal to the tracking module when a visible satellite signal is detected. The tracking module decodes and extracts the navigation data from the acquired signal and sends it to the PVT estimator module for computing the receiver's location and time.

The acquisition module searches for satellite signals by correlating its own replica of the pseudorandom code corresponding to each of the satellites. In addition, the carrier frequency of the satellite signals can differ from its true value due to the relative motion of the satellite and the receiver itself (Doppler effect). Thus, in order to detect any visible satellite signal, the receiver performs a two-dimensional search. First, it has to search through all possible delays (phase) of the pseudorandom code. Second, the receiver must account for frequency errors that occur due to the Doppler effect and other environmental interferences. Figure 2 shows the output of a signal acquisition phase. If the code and Doppler searches result in a peak above the acquisition threshold, the GPS receiver then switches to tracking and demodulating the navigation message data. The decoded data is used to estimate the receiver's range or distance from each of the visible satellites. In order to determine the range, the receiver needs the satellite signal's transmission and reception time. The navigation message contains the transmission time of each subframe, and the receiver estimates the reception time. It is important to note that the satellite clocks are in tight synchronization with each other while the receiver's clock (not using atomic crystals) contain errors and biases. Due to the receiver's clock bias, the estimated ranges are referred to as *pseudoranges*. The receiver requires at least four pseudoranges to determine its position after eliminating the effect of receiver clock bias.

## 3. GPS SPOOFING ATTACKS

A GPS signal spoofing attack is a physical-layer attack in which an attacker transmits specially crafted radio signals that are identical to authentic satellite signals. Civilian GPS is easily vulnerable to signal spoofing attacks due to the lack of any signal authentication and the publicly known spreading codes for each satellite, modulation schemes, and data structure. In a signal spoofing attack, the objective of an attacker may be to force a target receiver to (i) compute a false geographic location, (ii) compute a false time or (iii) disrupt the receiver by transmitting unexpected data. Due to the low power of the legitimate satellite signal at the receiver, the attacker's spoofing signals can trivially overshadow the authentic signals. During a spoofing attack, the GPS receiver locks onto (acquires and tracks) the stronger signal i.e., the attacker's signals, ignoring the legitimate satellite signals. This results in the receiver computing a false position, velocity and time based on the spoofing signals.

An attacker can influence the receiver's position and time estimate in two ways: (i) manipulating the contents of the navigation messages (e.g., location of satellites, navigation message transmission time) and/or (ii) modify the arrival time of the navigation messages. The attacker can manipulate the arriving time by temporally shifting the navigation message signals while transmitting the spoofing signals. We classify the different types of spoofing attacks based on how synchronous (in time) and consistent (with respect to the contents of the navigation messages) the spoofing signals are in comparison to the legitimate GPS signals currently being received at the receiver's true location.

*Non-Coherent and Modified Message Contents:* In this type of an attack, the attacker's signals are both unsynchronized and contain different navigation message data in comparison to the authentic signals. Attackers who use GPS signal generators [2, 4] to execute the spoofing attack typically fall under this category. An attacker with a little know-how can execute a spoofing attack using these simulators due to their low complexity, portability and ease of use. Some advanced GPS signal generators are even capable of recording and replaying signals, however not in real-time. In other words, the attacker uses the simulator to record at one particular time in a given location and later replays it. Since they are replayed at a later time, the attacker's signals are not coherent and contain different navigation message data than the legitimate signals currently being received.

*Non-Coherent but Unmodified Message Contents:* In this type of an attack, the navigation message contents of the transmitted spoofing signals are identical to the legitimate GPS signals currently being received. However, the attacker temporally shifts the spoofing signal thereby manipulating the spoofing signal's time of arrival at the target receiver.

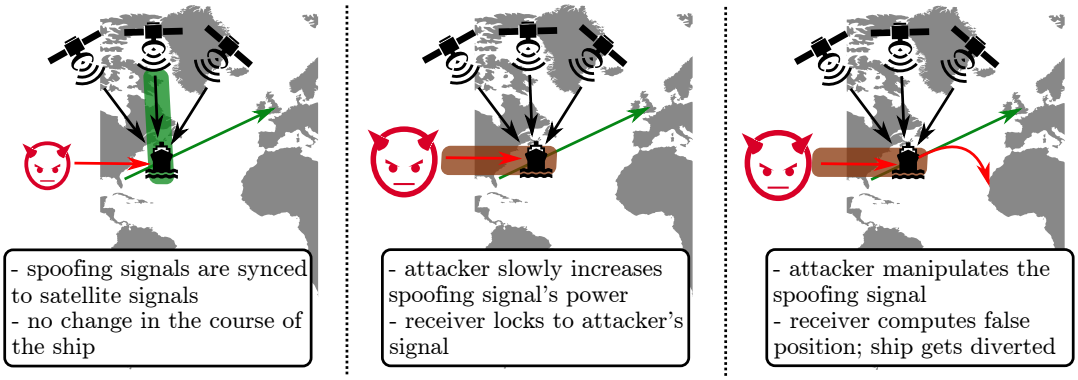


Figure 4: Seamless takeover attack. The receiver is locked onto the legitimate satellite signals. The spoofing signal is synchronized to the legitimate signal and contains the same navigation message contents. Next, the attacker slowly increases the power of the spoofing signal. The receiver stops tracking the legitimate signals and locks on to the attacker's signal. Finally, the attacker shifts the spoofing signal temporally causing the receiver to compute a false location and thereby altering the course of the ship.

For example, attackers capable of real-time record and replay of GPS signals fall under this category as they will have the same navigation contents as that of the legitimate GPS signals, however, shifted in time. The location or time offset caused by such an attack on the target receiver depends on the time delay introduced both by the attacker and due to the propagation time of the relayed signal. The attacker can precompute these delays and successfully spoof a receiver to the desired location.

*Coherent but Modified Message Contents:* The attacker generates spoofing signals that are synchronized to the authentic GPS signals. However, the contents of the navigation messages are not the same as that of the currently seen authentic signals. For example, attacks such as those proposed in Nighswander et al. [28] can be classified under this category. Nighswander et al. [28] present a Phase-Coherent Signal Synthesizer (PCSS) that is capable of generating a spoofing signal with the same code phase as the legitimate GPS signal that the target receiver is currently locked on to. Additionally, the attacker modifies the contents of the navigation message in real-time (and with minimal delay) and replays it to the target receiver. A variety of commercial GPS receivers were shown to be vulnerable to this attack and in some cases, it even caused permanent damage to the receivers.

*Coherent and Unmodified Message Contents:* In this type of an attack, the attacker does not modify the contents of the navigation message and is completely synchronized to the authentic GPS signals. Even though the receiver locks onto the attacker's spoofing signals (due to the higher power), there is no change in the location or the time computed by the target receiver. Therefore, this is not an attack in itself but is an important first step in executing the seamless takeover attack.

## 3.1 Seamless Lock Takeover Attack

The seamless lock takeover attack is considered one of the strongest attacks in the literature. In a majority of applications, the target receiver is already locked on to the legitimate GPS satellite signals. The goal of an attacker is to force the receiver to stop tracking the authentic GPS signals and lock on to the spoofing signals without causing any signal disruption or data loss. This is because the target receiver can potentially detect the attack based on the abrupt loss of GPS signal. Consider the example of a ship on its way from the USA to the UK as shown in Figure 4. The GPS receiver on the ship is currently locked onto the legitimate satellite signals. In a seamless lock takeover attack, the attacker first transmits spoofing signals that are synchronized with the legitimate satellite signals and are at a power level lower than the received satellite signals. The receiver is still locked on to legitimate satellite signals due to the higher power and hence there is no change in the ship's route. The attacker then gradually increases the power of the spoofing signals until the target receiver stops tracking the authentic signal and locks on to the attacker's spoofing signals. Note that during this takeover, the receiver does not see any loss of lock, in other words, the lock takeover was seamless. Even though the target receiver is now locked on to the attacker, there is still no change in the route as the spoofing signals are both coherent with the legitimate satellite signals as well as there is no modification to the contents of the navigation message itself. Now, the attacker begins to manipulate the spoofing signal such that the receiver computes a false location and begins to alter its course. The attacker can either slowly introduce a temporal shift from the legitimate signals or directly manipulate the navigation message contents to slowly deflect the course of the ship to a hostile destination. Tippenhauer et al. [33] describe the requirements for an attacker to execute a seamless takeover and move the target receiver towards the intended location.

## 3.2 Performance of Existing Countermeasures

In this section, we discuss existing countermeasures and describe their effectiveness against various types of spoofing attacks. Many countermeasures were based on detecting anomalies in the physical-layer characteristics of the received signal. In addition to the estimated position, velocity and time, modern GPS receivers output information pertaining to particular physical-layer characteristics directly as *receiver observables*. Modern GPS receivers can be con-

figured to output, e.g., automatic gain control (AGC) values, received signal strength (RSS) from individual satellites, carrier phase values, estimated noise floor levels, etc. Many previous works [10, 11, 35] proposed using some of the receiver observables mentioned above to realize spoofing awareness in a GPS receiver. For example, in [35] the authors suggest monitoring the absolute and relative signal strength of the received satellite signals for anomalies, the number of visible satellites (should not be high), simultaneous acquisition of satellite signals, etc. Other countermeasures such as detecting sudden changes to the AGC values were also proposed for detecting GPS spoofing attacks. Automatic Gain Controller (AGC) is a hardware module that varies the gain of the internal amplifier depending on the strength of the received signal. Such a countermeasure is at best capable of detecting attackers who transmit their spoofing signal at very high power. They are ineffective against attackers who have better control over their spoofing signal.

Several spoofing detection strategies based on analyzing the distortions present in the output of the receiver's correlation function [30, 38] have been proposed in the literature. In an ideal noise-free environment, the correlation output has minimal distortions. The authors argue that during a spoofing attack, the attacker's signal would distort the output of the correlators, which can be used to detect the attack itself. However, the correlation output is also distorted due to multipath signals that arrive a few nanoseconds later than the direct signal. Wesson et al. [38] showed that it is indeed difficult to distinguish between the distortions caused due to a spoofing attack and a legitimate multipath signal. Spoofing detection techniques based on the differences in the inherent spatial characteristics of the received signal such as direction or angle of arrival [15, 27, 31] also face the same challenge of reliably distinguishing between legitimate multipath signals and a spoofing attack. Additionally, they also require additional hardware modifications to the GPS receiver. To summarize, although several countermeasures have been proposed in the literature to detect spoofing attacks, no countermeasure today is effective in detecting strong attackers such as a seamless lock takeover attack. Moreover, no platform can be used to compare and evaluate the effectiveness of existing countermeasures in real-world scenarios. Today, it is still possible to spoof a victim receiver to any arbitrary location without being detected.

# 4. SPREE – A SPOOFING RESILIENT GPS RECEIVER

The design of SPREE is primarily motivated by the lack of a GPS receiver capable of detecting or constraining all the spoofing attacks known in the literature. In this section, we present the design of SPREE, the first GPS receiver capable of detecting or limiting all known spoofing attacks. Our receiver design consists of two key components: (i) Auxiliary Peak Tracker (APT) and (ii) Navigation Message Inspector (NAVI) module. First, we describe the auxiliary peak tracking module, a novel countermeasure which plays a vital role in constraining even a strong attacker capable of a seamless lock takeover. The key feature of APT is that it acquires and tracks not only the strongest received satellite signal but also the weaker signals that may be present in the environment. Second, we introduce a navigation message inspector (NAVI) which inspects the decoded contents

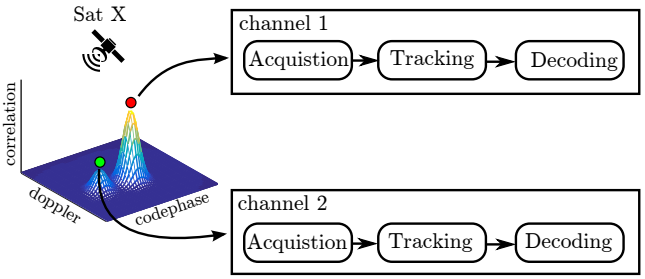


Figure 5: Auxiliary Peak Tracking (APT) module. SPREE uses more than one channel to acquire, track and decode each satellite's signal. This enables tracking of signals that produce weaker acquisition correlation peaks.

of the navigation message from every satellite and reports any discrepancies. We show that NAVI is capable of detecting attackers who modify the contents of the navigation message. The Auxiliary Peak Tracker protects SPREE from attackers who are not synchronized (non-coherent) to the legitimate GPS signals currently being received and the Navigation Message Inspector prevents attackers from modifying the contents of the navigation message. The combination of auxiliary peak tracking and the navigation message inspector enables SPREE to detect all types of spoofing attacks reliably.

## 4.1 Auxiliary Peak Tracking (APT)

In this section, we describe the details of our proposed Auxiliary Peak Tracking technique, which is one of SPREE's key features that makes it resilient to spoofing attacks. Typically, GPS receivers have multiple acquisition and tracking modules to search and track simultaneously different satellites. Each set of acquisition and tracking module is called a *channel* and each satellite signal is acquired and tracked by only one channel. For example, a 24-channel GPS receiver can simultaneously search for 24 satellites thereby shortening the time to acquire a position fix when compared to a 4-channel receiver. In other words, the receiver searches for a satellite by allocating each channel to one specific satellite. The receiver searches for a particular satellite signal by correlating its own replica of that specific satellite's pseudo-random code with the received signal. If the search results in a correlation value above the acquisition threshold, the receiver switches to tracking and demodulating the navigation message data. *It is important to note that GPS receivers acquire and track only the satellite signal that produces the strongest correlation peak and ignores any weaker correlation peaks as noise.*

In SPREE, we allocate *more than one* channel to the same satellite. This means that in addition to tracking the signal that results in the strongest correlation, SPREE can also track weaker correlation peaks (if present) for the same satellite. In other words, SPREE does not restrict itself to the satellite signals that produces the maximum correlation, but it also detects and tracks signals that produce weaker correlation (Figure 5).

**Spoofing detection by tracking auxiliary peaks:** The Auxiliary Peak Tracker protects SPREE from attackers who are not synchronized to the authentic GPS signals. Recall that the attacker transmits higher power spoofing signals

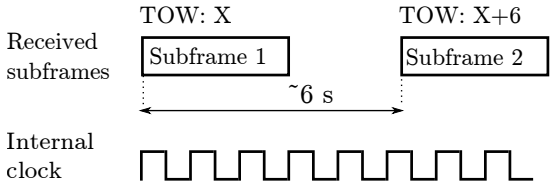


Figure 6: Time of Week (TOW) and Receiver's Clock. SPREE compares the received TOW to its internal clock and validates whether TOW is increased at 6 s intervals.

to overshadow the authentic GPS signals. Even though the spoofing signals have successfully overshadowed the authentic signals, they are still present in the environment and it is difficult for an attacker to completely annihilate them. In order to completely annihilate the authentic GPS signals, the attacker first needs to know the target receiver's precise location (cm-level). Furthermore, he needs to annihilate all the multipath components of the GPS signal at the receiver. This means that the attacker should be able to transmit nulling signals such that they cancel both the direct GPS signal and *all* the possible multipath components at the receiver. In case the receiver is in motion, the attacker must be able to predict the *exact* trajectory of the receiver. Given the difficulty of completely annihilating the authentic satellite signals, they will appear as auxiliary peaks when the attacker's spoofing signals are non-coherent or in other words not synchronized with the authentic satellite signals. We provide a more detailed analysis on how SPREE's APT module enables detection of even the strong seamless lock takeover attackers in Section 6.

## 4.2 Navigation Message Inspector (NAVI)

The Navigation Message Inspector module inspects the decoded navigation data for consistency and sanity and is key to protecting the GPS receiver from attackers who modify the contents of the navigation message.

**Time of Week (TOW) and Receiver's Clock:** One of the key parameters that an attacker can modify in order to spoof a target receiver's location or time is the transmission time of the navigation messages. The navigation data transmitted by each of the satellites contains five subframes. Each subframe begins with a handover word which includes a truncated version of the time of week (TOW) at which the satellite transmitted that particular subframe. Each subframe lasts for about 6 seconds, and since the TOW is transmitted once every subframe, it can only increase in steps of 6 seconds. We leverage the internal clock of SPREE's hardware and the fact that the TOW can only change in steps of 6 s to detect spoofing attacks (Figure 6). SPREE records the received GPS week and time of week with its internal clock count and raises an alarm if the difference in the time elapsed internally doesn't match the newly received GPS time of week.

**Satellite Orbital Positions:** In addition to the transmission time of the navigation message, an attacker can also modify the satellite's position in the orbit. The GPS receiver estimates the satellite's position from the ephemeris data. For example, Nighswander et al [28] demonstrated that it is possible to modify the ephemeris data such that the receiver estimates the satellite to be in the middle of the earth. The authors executed such an attack by setting the square root of the semi-major axis of the satellite's orbit to 0. In our design, an attacker cannot execute such manipulations as SPREE continuously monitors and evaluates any changes to the orbital parameters.

**Almanac & Ephemeris Data:** SPREE continuously monitors the decoded navigation data from all the visible satellites and performs a number of consistency checks. The almanac and ionospheric model data should be the same across all the navigation frames received from all the satellites. Also, whenever feasible SPREE leverages the availability of navigation data such as ephemeris, almanac and the ionospheric models from third-party sources to compare the data decoded by the GPS receiver. This data is then compared against the information received from the satellites and is used to detect spoofing attacks.

Thus, SPREE's navigation message inspector independently protects the receiver from attackers capable of modifying the navigation message. By combining the NAVI and APT modules, SPREE detects or constraints all types of attacks capable of spoofing the receiver's location and time.

# 5. IMPLEMENTATION

We implemented SPREE based on GNSS-SDR [17], an open source software-defined GPS receiver. GNSS-SDR is written in C++ and can be configured to process signals received directly from a radio hardware platform such as USRP [1] or from a file source. GNSS-SDR works with a range of hardware platforms and signal recorders such as USRP, SiGe GN3S Sampler, NSL Primo [6], IFEN's NavPort [8], etc. The architecture of GNSS-SDR mostly resembles the design of a typical GPS receiver as described in Section 2. It consists of a signal source and a conditioner module which are responsible for interfacing with the underlying receiver hardware or file source. Similar to typical GPS receivers, GNSS-SDR also consists of several *channels*; each channel managing all the signal processing related to a single satellite. In GNSS-SDR, the *channel* is a software module that encapsulates the functions of acquisition, tracking and navigation message decoding blocks. All the channels then report to a module that estimates the pseudoranges and a number of other observables. Finally, if enough information is available, the receiver calculates a position, velocity, and time. A configuration file allows the user to chose operational parameters such as the sampling frequency, the algorithms to use for each processing block, signal source etc. We modified the acquisition and tracking modules of GNSS-SDR to realize SPREE. First, we implement the auxiliary peak tracking system within the GPS receiver's acquisition module. Recall that the auxiliary peak tracker enables the receiver to track multiple signals of the same satellite instead of limiting it to the strongest component only. We implement the navigation message inspector which checks the consistency and sanity of the extracted navigation data within the tracking module of the receiver.

**Auxiliary Peak Tracking (APT):** In SPREE, when a particular satellite is assigned to a channel, all local peaks of the acquisition correlation function, which are above the acquisition threshold are collected and stored for processing.

This is in contrast to the modern receivers only choosing the highest correlation peak. Each local peak is then assigned to a different channel in descending order of magnitude for tracking. The maximum number of channels that can track the same satellite is made configurable at run time. The number of channels that can be assigned to track the same satellite will influence the number of peaks that can be evaluated at the same time.

If SPREE is successful in acquiring more than one peak, it records the differences in their arrival times i.e., the separation between two peaks. If the difference is more than the maximum acceptable time difference, $\tau_{max}$, SPREE detects a spoofing attack. The value $\tau_{max}$ is set in the configuration file. This check is done each time a new navigational message is received. The arrival time is computed by the tracking module, where it is estimated based on the sample counter of GNSS-SDR and fine tuned based on the code phase of the satellite signal. After an auxiliary peak has been acquired, tracked and evaluated for signs of spoofing and none are found it is dropped and the channel is free to acquire another auxiliary peak to evaluate. If the peak is still present, it will be evaluated again when a channel is free *and* all other peaks have been assessed.

**Navigation Message Inspector (NAVI):** In GNSS-SDR, a telemetry decoder is responsible for decoding the contents of the received navigational message. First, SPREE records the time of week decoded from each of the received navigation message subframes. If the difference in time of week present in consecutive subframes does not match with its internal clock count (more than 6 s difference due to the minimum resolution), SPREE raises an alarm. Next, the stored navigation data for each of the visible satellites is compared with the contents of the preceding navigation message for that particular satellite. If there is a discrepancy between these two values, SPREE notes it as a possible spoofing attack. Also, SPREE compares the navigational data from all satellites with each other for any discrepancies in the almanac and ephemeris data. Recall that, the almanac and ionospheric model data should be the same across all the navigation frames received from all the satellites. If configured to do so and if possible, it can also compare the time, almanac, ephemeris and the ionospheric model data received from the satellites to data received from third-party sources using the Secure User Plane Location (SUPL) protocol. These checks are done each time a new navigation message is received.

In addition to the above modules, we also implement several existing countermeasures described in Section 3 to facilitate real-world performance evaluations. However, we restrict our discussion to our main contributions, the APT and NAVI module as they enable reliable detection of all known spoofing attacks in literature. It is important to note that SPREE adds no additional requirements on the underlying hardware and supports all the platform and file sources supported by GNSS-SDR.

# 6. SECURITY EVALUATION

In this section, we evaluate SPREE and present its security guarantees. Figure 7 shows our evaluation setup. A configuration file is used to select SPREE's parameters including those needed by the spoofing detection module. In

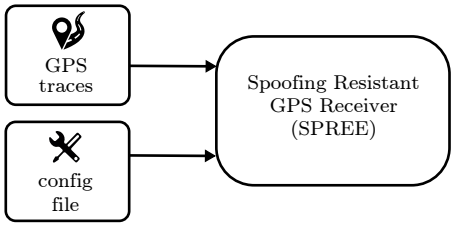


Figure 7: Evaluation Setup. A configuration file specified vital system parameters such as the input source, signal sampling rate and the configuration of the spoofing detection module.

our evaluations, the GPS signal traces (spoofing and clean) were recorded and stored in files and later input to SPREE. We evaluated SPREE against three different sets of GPS signals: (i) a public repository of spoofing traces (TEXBAT) [19], (ii) signals recorded through our own wardriving effort and (iii) spoofing signals generated using COTS GPS simulators.

## 6.1 GPS Traces

**GPS Simulator:** First, we evaluated the performance of SPREE against our own spoofing signals generated using commercially available GPS simulators. Specifically, we used Spectracom's GSG-5 Series advanced GPS simulator [2] in order to generate our spoofing signals. One of the key features of the simulator is its ability to generate multipath signals for any satellite. It is even possible to configure the multipath's power levels and time offset i.e., the extra distance traveled by the multipath relative to the original line-of-sight (LOS) signal. The GPS simulator traces were mainly used to evaluate the ability of SPREE to detect auxiliary peaks robustly. In addition, we used the GPS simulator traces to simulate attackers capable of manipulating the content of the navigation messages.

**Texas Spoofing Test Battery (TEXBAT):** The Texas Spoofing Battery (TEXBAT) [19] is a set of digital recordings containing GPS spoofing tests conducted by the University of Texas at Austin. TEXBAT is the only publicly available dataset and the de-facto standard for testing spoofing resilience of GPS receivers. TEXBAT includes two clean (spoofing free) data sets in addition to spoofing scenarios based on the location and time of the clean GPS traces. The set of spoofing traces contains a wide variety of scenarios including take-over attacks where either the time or position of the target receiver is spoofed. The spoofing signals are closely code-phase aligned with the authentic signals. Furthermore, the carrier phase of the seamless lock takeover scenarios is aligned with the authentic GPS signals during the takeover.

**Wardriving:** In addition to using the TEXBAT traces, we collected our own GPS signal traces through an extensive wardriving effort. We used the wardriving dataset to evaluate SPREE's behavior in a non-adversarial (only legitimate GPS signals present) scenario and determine how reliable SPREE is concerning false alarms. The setup used for recording the GPS signals during the wardriving effort is shown in Figure 8. The front end of the setup consists of an

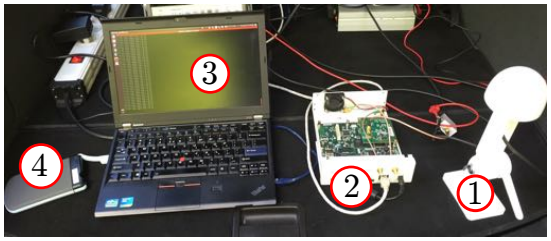


Figure 8: Our wardriving setup. The setup consists of (1) an active conical GPS antenna and (2) a USRP N210. The signals were recorded using (3) a laptop. The recordings were periodically moved to (4) an external hard disk.

active conical GPS antenna and a bias-tee. During the drive, we set up the antenna using magnetic holders onto the car's roof and drove for more than 200 km across a wide variety of geographic landscapes. We used a USRP N210 and recorded raw GPS signals on an external hard disk. The signals were sampled at 10 MHz and stored in complex data format. The entire setup was powered using the car's power outlet. We recorded the GPS signals at various locations: (i) An open field, (ii) parking lot of a small village, (iii) driving on a highway at the speed limit of 100 km/h, (iv) driving inside a city, (v) inside a city with neighbouring tall buildings and (vi) inside a forest with dense tree cover.

## 6.2 Security Evaluation

Recall that an attacker can influence the receiver's estimates by either manipulating the contents of the navigation messages or temporally shifting the navigation message signals while transmitting the spoofing signals.

**Detecting Non-coherent Attackers:** Recall that a non-coherent attacker's spoofing signal is not synchronized with the authentic satellite signals. Even though the receiver might be locked on to the attacker's spoofing signals, the authentic signals will appear as auxiliary peaks due to the Auxiliary Peak Tracking module. The effectiveness of detecting such non-coherent spoofing attacks depends on the ability of the APT module to detect and track auxiliary peaks. First, using our GPS simulator traces, we tested the ability of the APT module to detect and track multiple acquisition correlation peaks. Specifically, we leveraged the ability of the simulator to generate duplicate copies of a satellite signal at different time intervals away from the original signal. We generated signal copies spaced between 50 ns and 1000 ns. SPREE was able to reliably detect and track auxiliary peaks that were spaced 500 ns or more. In some scenarios, it was able to track peaks much closer, however not reliably (over multiple runs). Thus, we configured APT module to track auxiliary peaks that are separated by more than 500 ns. The choice of 500 ns separation between two peaks for spoofing detection is supported by two additional reasons: (i) During signal acquisition (searching for satellite signals), GPS receivers shift their correlator typically by half a chip[1] period i.e., 500 ns. This means that most modern receivers can reliably track peaks that are separated by 500 ns and no additional hardware changes are required to implement SPREE in modern receivers. (ii) Several prior works on modelling

[1]A chip is one bit of the pseudorandom code

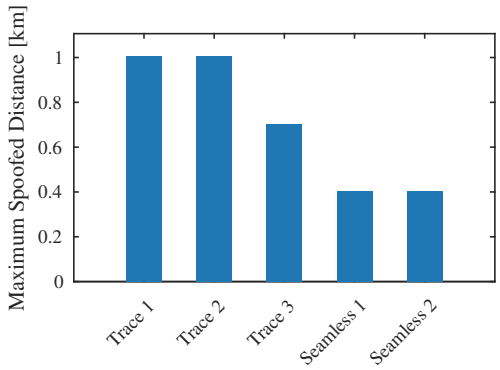


Figure 9: Spoofing detection in TEXBAT dataset. SPREE detected auxiliary peaks in all the spoofing traces. The maximum location offset the attacker could cause before being detected was less than a kilometer. Refer Appendix for the mapping of traces to the TEXBAT dataset.

GNSS multipath signals [13, 20, 23, 25] show that most GPS multipath are delayed by less than $300-400$ ns. This means that it is highly unlikely to observe an auxiliary peak caused due to legitimate multipath signals occurring at more than 500 ns away from the line-of-sight signal peak. Moreover, the attenuation and polarization shift introduced in the legitimate signals due to reflections that are a few hundred meters away would make the signal untrackable. We proceeded to evaluate SPREE against the TEXBAT set of GPS spoofing signal traces described previously. SPREE detected auxiliary peaks in all the traces containing spoofing signals and failed to detect any auxiliary peaks for the clean non-spoofing traces. Based on the separation of auxiliary peaks at the time of detection, we evaluated the maximum possible location offset an attacker could have caused without being detected and present it in Figure 9. In the case of the seamless takeover attacks, the maximum deviation an attacker could introduce in SPREE was about 400 m. It is important to note that traces 1, 2 and 3 contain spoofing signals that are not as closely synced as the seamless takeover traces and hence the larger values for maximum spoofed distance. For completeness, we processed our wardriving traces that represent clean, non-spoofing scenarios for any false alarms. SPREE did not detect any auxiliary peaks. Furthermore, SPREE is not vulnerable to multiple GPS spoofing attackers. Note that SPREE can track multiple peaks of the same satellite by modifying the number of channels allocated to each satellite. Therefore, multiple attackers will cause multiple auxiliary peaks which will trigger SPREE to raise an alarm.

**Detecting Navigation Message Modifications:** We will now analyze SPREE's resilience against attackers who modify the contents of the navigation message. The key parameters that an attacker can manipulate the navigation data are the time of transmission of the navigation subframe and the satellite's orbital information present in the almanac and ephemeris.

*Modifying TOW:* As described in Section 4.2, the value of TOW can be altered only in steps of 6 seconds. SPREE leverages the internal clock of the hardware receiver to com-

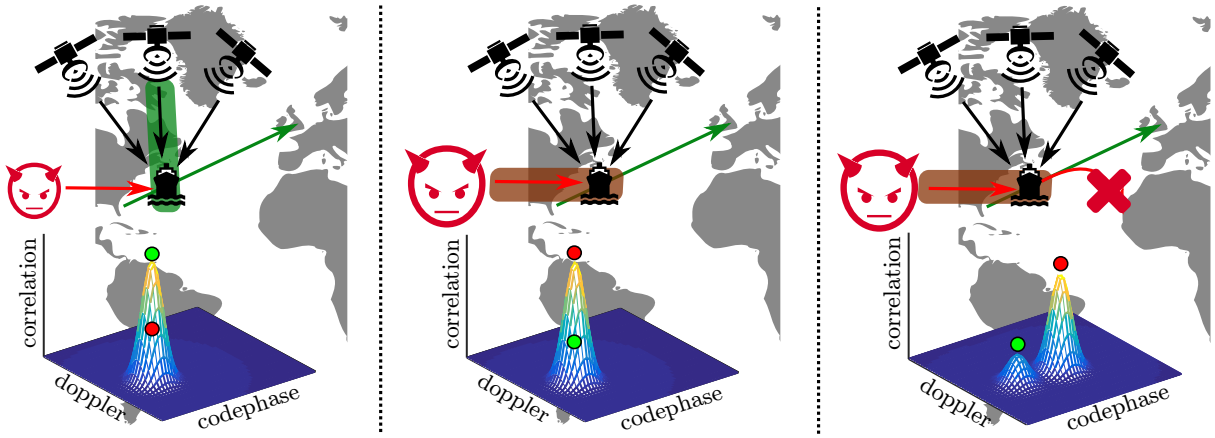


Figure 10: Detecting Seamless Lock Takeover Attack. As the attacker begins to drift the spoofing signal away with the intention of changing the course of the ship, SPREE will detect the auxiliary peak produced by the legitimate satellite signal and raise an alarm.

pare the received TOW data against its internal clock count continuously. SPREE raises an alarm if the difference in the time elapsed internally doesn't match the newly received GPS time of week information. We note that even a watch crystal today has an error rating of approximately 10 ppm which is a drift of less than a second in one day. Therefore a drift of 6 s can be easily detected even without a thermally controlled crystal oscillator (TCXO[2]) that is present in modern hardware receiver platforms. We evaluated SPREE against such an attack using two GPS simulators each spoofing the same satellite however with different TOW data and SPREE successfully detected the attack. Both the simulators were synchronized to the same reference clock signal. We used this setup to evaluate SPREE's resilience to attacks described in [28] such as arbitrary manipulation of week numbers and date desynchronization attacks.

*Modifying Ephemeris Data:* The attacker can also manipulate the ephemeris data to force the receiver to malfunction. Ephemeris data gets updated once every two hours and contains precise satellite orbital information including satellite clock biases. However, it was shown in [28] that it is trivial to force a receiver to accept ephemeris changes whenever possible. Since SPREE's NAVI module keeps track of the elapsed time using the receiver's internal clock, it can be configured to ignore any ephemeris updates within the 2-hour time interval. It is also important to note that any changes to the satellite orbital information or in general the ephemeris data can be compared against ephemeris data available from third-party sources [5]. Additionally, SPREE is capable of recording the ephemeris data received from all satellites in the past and notify if there is any unexpected change in the ephemeris data values.

Alternatively, an attacker can slowly manipulate the ephemeris data, but this would involve causing minute changes to the ephemeris data over the course of many hours (ephemeris data only changes every two hours). Also, legitimate changes to the ephemeris data are typically error corrections. Hence, these changes are quite minimal and don't result in significant changes to the receiver's location estimates itself. In SPREE, the current ephemeris data is compared to previously received information, and the alarm is triggered if there is a change in the ephemeris data more frequently than every two hours. Furthermore, we analyzed ten years of ephemeris data from NASA's archive of space geodesy data [5] and compare every change to the ephemeris against the maximum possible change that can legitimately occur. Thus, SPREE severely constrains the attacker from manipulating the ephemeris data.

**Detecting Seamless Lock Takeover Attack:** As described previously, a seamless takeover attack is an attack in which the attacker takes control of the victim receiver without any disruption to its current state. The seamless lock takeover attacker is one of the strongest attackers known in the literature, and no existing countermeasure is effective in detecting the seamless takeover attack. We will now see how SPREE enables detecting a seamless takeover attack. Consider the same example of a ship on its way from the USA to the UK, currently locked onto legitimate satellite signals. The attacker begins a seamless lock takeover by transmitting spoofing signals that are synced to the legitimate satellite signals but at a lower power level. The output of the acquisition module is shown in Figure 10. Notice that the legitimate satellite signal (shown in green) is stronger than the spoofing signal but they are synchronized to each other. Now the attacker, increases the spoofing signal's power and takes over the receiver's lock. Note that, even though the receiver is locked on to the attacker, there is still no change in route yet. This is because the attacker is both synchronized to the legitimate GPS signals and is transmitting the same navigation message. Now, the attacker begins to drift the spoofing signal away with the intention of changing the course of the ship. At this point, a typical GPS receiver will ignore any weaker correlation peaks that exist and compute its new location based on the attacker's signal. However, SPREE will detect an auxiliary peak and raise an alarm thereby alerting the ship from being diverted.

**Maximum position offset:** Recall that SPREE detects any modifications to the contents of the navigation message

[2]Modern TCXOs have error ratings between $1-100$ ppb and are available for under $10

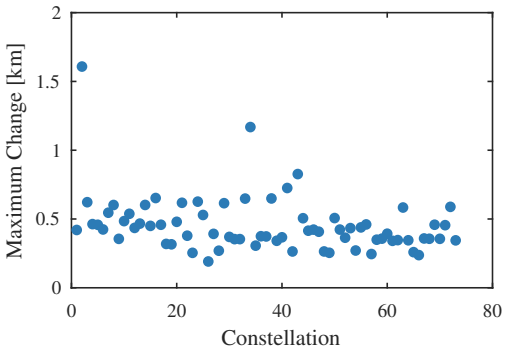


Figure 11: Maximum location offset. An analysis of 73 satellite constellations (as observed during wardriving) show that a strong attacker can cause a maximum location offset of less than 1 km in the majority of the scenarios before being detected.

and tracks peaks of the same satellite that are separated by more than 500 ns. This value was setup after extensive experiments using signals from GPS simulators and our own wardriving efforts as described previously. This means that the attacker is limited to temporally shift the spoofing signals by at most 500 ns which results in a 150 m change in the pseudorange estimated by the receiver for that specific satellite. It is important to note that the effect of this change in pseudorange caused by the attacker on the receiver's final position estimate depends on the constellation of the satellites. We collected all the different constellations observed during our wardriving and evaluated the effect of temporally shifting the satellite pseudoranges by 150 m. Our analysis accounted for all possible pseudorange changes an attacker can introduce on all combinations of visible satellites. We analyzed over 73 different satellite constellations, each one with four satellites, and calculated the maximum possible location offset an attacker could introduce. Our results are shown in Figure 11. On an average, the maximum position deviation was 455 m. This means that e.g., in the ship hijack scenario, it would not be possible for an attacker to deflect the course of the ship by more than 455 m. Note that, we limited our analysis to constellations consisting of only four visible satellites, which is the most favourable for an attacker. In most environments, more than four satellites will be visible, which will further constrain how much the attacker can change the victim's position. Furthermore, we observed that the constellations that allow the attacker to spoof the receiver more than 1 km away, comprised satellites at very low elevation angles. Therefore, configuring SPREE only to accept satellite signals with a minimum elevation angle will potentially constrain the attacker further.

# 7. DISCUSSION

**Integrating SPREE into commercial receivers:** One of the main differences between SPREE and a commercial GPS receiver is that unlike commercial receivers which track one satellite per channel, SPREE uses multiple channels to track the same satellite. This means that without any hardware changes i.e., for the same number of acquisition and tracking channels, our spoofing-aware receiver will track less number of satellites than its capable of. In order to do this, two changes are necessary: (i) allocate a minimum of two channels for every visible satellite signal (one for the authentic GPS signal and one that keeps searching for a potential spoofing signal) and (ii) search the entire range of time delays for weaker acquisition peaks. The number of channels allocated per visible satellite signal can be easily modified in the firmware. However, as mentioned before, this will limit the number of satellites that the receiver can simultaneously acquire and track. Modern receivers typically have $32-128$ channels capable of tracking $32-128$ satellites simultaneously[3] and allocating two channels for each satellite will reduce the number of satellites that can be tracked by half. In reality, this is not a problem since the typical number of visible satellites at any time instant is not more than 10 or 11. In order to track auxiliary peaks, we keep a list of all auxiliary peaks found during the acquisition in a float array. The number of floats stored is $2 \cdot \frac{F_s}{1000}$ for each acquisition, where $F_s$ denotes the sampling rate. This means that for a sampling rate of 10 MHz each acquisition requires an additional $\approx 19.5$ kB of storage. We believe this to be negligible when compared to the available RAM in most of the modern receivers today. There is practically no performance overhead in detecting changes to the contents of the navigation message by an attacker. The only waiting time is the time ($\approx 6$ s) needed to receive and decode the new subframe completely. Hence, our design modifications can be easily integrated into a modern GPS receiver with only a firmware upgrade and does not require any changes to the underlying hardware. We note that the power consumed by SPREE will be similar to current GPS receivers with all the channels actively acquiring satellite signals. However, more analysis is required in the scenarios where the receivers optimize the usage of the acquisition and tracking channels.

**Probability of False Alarms:** False alarms are caused due to an event that forces SPREE to believe it is being spoofed. In the case of SPREE, the arrival of a legitimate multipath signal with a delay of more than 500 ns and with a signal strength greater than the acquisition threshold will result in SPREE raising a spoofing alert. The value of 500 ns was selected for the following reasons. GPS signals are typically right-hand polarized and any reflections causes a change in the polarization of the signal. The majority of GPS receiver antennas are configured to received the direct right-hand circularly polarized signals and attenuate other reflected signals. Additionally, since the multipath signals travel a few hundred meters more than the direct line-of-sight signal, the signals undergo more attenuation due to propagation path loss. Also, reflections from surfaces themselves may cause the GPS signal to attenuate and therefore, given the received power levels of the direct line of sight GPS signals on the ground, multiple reflections would eventually only make the signal untrackable.

Furthermore, auxiliary peaks caused by legitimate multipath tend to be momentary and untrackable in contrast to a peak resulting from a spoofing attack. Several prior works on modelling GNSS multipath signals [13, 20, 23, 25] show that most GPS multipath are delayed by less than $300-400$ ns. Additionally, we independently confirmed the results mentioned above with our own wardriving effort (details in Section 6). In our wardriving effort, we set up the

[3]sometimes used in receiver's capable of using more than one satellite navigation system such as GLONASS

antenna on the roof of the car (using magnetic holders) and drove for more than 200 km across a wide variety of geographic landscapes as described in Section 6. We did not observe any auxiliary peak separated by more than 500 ns in any of our collected GPS traces.

**Applications of SPREE:** Recall that SPREE restricts even a strong attacker capable of a seamless lock takeover from spoofing SPREE to a maximum of 1 km away from its true location. This means that, with SPREE deployed, the course of ships and trucks carrying cargo or other security-critical assets cannot be diverted by more than 1 km. Drones and unmanned aerial vehicles cannot be forced to land in hostile areas that are more than 1 km away from their safe landing zones. Thus, in the scenario of an attack, SPREE significantly reduces the search space while modern GPS receivers allow the attacker to spoof the receiver to any arbitrary location in the world. We also note that the 1 km estimation is an upper bound calculated based on the scenarios in which the GPS receiver acquires the minimum needed amount of satellite signals (four). Typically, there are more than four satellites visible to the GPS receiver which reduces the maximum spoofing distance significantly. For example, an analysis of the wardriving constellations with more than four satellites shows that an attacker could not spoof the victim receiver more than a few hundred meters away from its actual location.

**Limitations:** One of the limitations of SPREE is it is only capable of detecting a spoofing attack. Even though detecting all existing spoofing attacks is a significant improvement over the state of the art, the ability to annihilate or neutralize the attacker's spoofing signal will enable the receiver to continue operation even in the scenario of an attack. In the case of SPREE, the significant challenge in canceling the spoofing signal is the ability to determine the source of the auxiliary peak. For example, SPREE will raise an alarm once it detects an auxiliary peak. Note that, even after detecting auxiliary peaks, it is currently difficult to distinctly identify the peak caused by the spoofing signal and that caused by the legitimate signal. An analysis of the temporal behavior of multipath signals against spoofing signals can potentially enable distinct identification of peaks caused due to a spoofing signal. The results of the analysis can help the receiver to ignore or internally cancel the spoofing signal and thereby building better resilience to GPS signal spoofing attacks.

Another limitation is that in order to detect manipulations to the navigation message's ephemeris data, SPREE assumes the availability of legitimate navigation messages before the start of the spoofing attack. SPREE will not detect navigation message manipulations in scenarios where the receiver does not have a prior navigation message to compare against, i.e., the receiver is in cold or factory start mode. However, to avoid being detected throughout the course of the receiver's use, the attacker must always be synced with the legitimate GPS signals while transmitting spoofed navigation messages. Such an attack might corrupt the contents of both the legitimate and spoofing navigation messages resulting in decoding errors. Therefore, the attacker will not be able to control the location to which he is trying to spoof the receiver. There is no way other than cryptographic authentication of navigation messages [21] or a challenge-response based ranging scheme such as distance-bounding [14] to prevent such cold-start attacks. We note that cryptographic authentication would be still vulnerable to message replay attacks and a challenge-response based ranging scheme is not scalable or feasible with global satellite-based navigation systems.

The only scenario that can result in the failure of SPREE in detecting a spoofing attack is as follows. In order to execute the seamless lock takeover, the attacker transmits spoofing signals that are synchronized to the legitimate GPS signals. Simultaneously, to avoid creating auxiliary peaks during the takeover process, the attacker needs to transmit nulling signals to annihilate the legitimate GPS satellite signals. The annihilating signals must be transmitted such that the attacker eliminates *only* the legitimate signals but not his own spoofing signals. Note that, since the attacker's spoofing signals are also synchronized to the legitimate GPS signals, the annihilation signals will cancel the attacker's spoofing signal as well. This makes it difficult for the attacker to execute the seamless lock takeover while ensuring that the victim receiver is continuously locked on to one of the GPS signals. We believe this is the only way to defeat SPREE. Today, it is trivial to execute spoofing attacks on GPS receivers and therefore with SPREE, we raise the bar for an attacker significantly.

# 8. RELATED WORK

The work that comes closest to SPREE is the design of an inline anti-spoofing device [22]. The device connects to the GPS antenna and a GPS receiver, and uses complex correlation peak distortion techniques to identify spoofing signals. As demonstrated in [38], such countermeasures face the challenge of distinguishing spoofing signals from real-world channel effects and are ineffective against seamless takeover attackers. Also, the device is incapable of detecting attackers who modify the contents of the navigation messages. Several works [21, 24, 37] propose solutions that are cryptographic in nature and therefore require modifications to the GPS infrastructure. Incorporating cryptographic authentication into civilian GPS, similar to military GPS, could to an extent mitigate spoofing attacks. However, this would require distribution and management of shared secrets which makes it infeasible for a large set of applications. Additionally, cryptographic authentication does not protect against signal replay attacks where an attacker simply records legitimate GPS signals at one location and replays it to the victim receiver [29]. Some other proposals depended on additional hardware such as additional receivers, alternative navigation systems, sensors, etc. Tippenhauer et al. [33] proposed the use of multiple synchronized GPS receivers to detect spoofing. They show that spoofing a set of synchronized GPS receivers, with known relative distances or geometrical constellation restricts the number of locations from where an attacker can transmit the spoofing signals. Cross-validation of the position estimates against alternate navigation systems such as Galileo [18] were also proposed. However, a simulator that can spoof both GPS and Galileo will easily defeat this countermeasure. Data from other sensors can also be used to cross validate GPS navigation solutions. For example, inertial measurement units (e.g., accelerometer, gyroscope, compass) have already been proposed as alternative ways to navigate during temporary GPS outages [16, 34, 36]. The main drawback of inertial navigation units is the accu-

mulating error of the sensor measurements. These accumulated sensor measurement errors affect the estimated position and velocity over a longer duration of time and hence limit the maximum period an IMU can act independently.

## 9. CONCLUSION

In this paper, we presented SPREE, the first GPS receiver that detects all known spoofing attacks. We designed, implemented and evaluated SPREE against different sets of GPS signal traces and showed that even a strong attacker capable of a seamless lock takeover cannot spoof the receiver more than 1 km away from its true location. This is a vast improvement over current GPS receivers that can be spoofed to any arbitrary location in the world. Finally, we release our implementation and the GPS dataset used in our evaluations to the research community.

## 10. ACKNOWLEDGMENTS

This work was partially supported by the Zurich Information Security and Privacy Center. It represents the views of the authors.

## 11. REFERENCES

[1] Ettus research llc. http://www.ettus.com/.

[2] GSG-xx Series Multi-channel advanced GNSS simulator. http://www.spectracomcorp.com/.

[3] Hacking A Phone's GPS May Have Just Got Easier. http://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/.

[4] LabSat GPS Simulator. http://www.labsat.co.uk/.

[5] NASA's archive of space geodesy data. http://cddis.gsfc.nasa.gov/.

[6] NSL Primo GNSS SDR Front End. http://www.nsl.eu.com/primo.html.

[7] SPREE Source Code. `http://www.spree-gnss.ch/`.

[8] SX3 GNSS Software Receiver. http://www.ifen.com.

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

[10] Akos, D. M. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Navigation* (2012).

[11] Bastide, F., Akos, D., Macabiau, C., and Roturier, B. Automatic gain control (AGC) as an interference assessment tool. In *ION GPS/GNSS 2003, 16th International Technical Meeting of the Satellite Division of The Institute of Navigation* (2003).

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

[13] Braasch, M. S. Performance comparison of multipath mitigating receiver architectures. In *Proceedings of the Aerospace Conference* (2001), IEEE.

[14] Brands, S., and Chaum, D. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology* (1993).

[15] Broumandan, A., Jafarnia-Jahromi, A., Dehghanian, V., Nielsen, J., and Lachapelle, G. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the IEEE Position Location and Navigation Symposium (PLANS)* (2012).

[16] Farrell, J., and Barth, M. *The Global Positioning System and inertial navigation.* McGraw-Hill New York, 1999.

[17] Fernández–Prades, C., Arribas, J., Closas, P., Avilés, C., and Esteve, L. GNSS-SDR: An open source tool for researchers and developers. In *Proceedings of the ION GNSS Conference* (2011).

[18] Hofmann-Wellenhof, B., Lichtenegger, H., and Wasle, E. *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more.* Springer Science & Business Media, 2007.

[19] Humphreys, T. E., Bhatti, J. A., Shepard, D. P., and Wesson, K. D. The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques. In *Proceedings of the ION GNSS Meeting* (2012).

[20] Kong, S.-H. Statistical analysis of urban GPS multipaths and pseudo-range measurement errors. *IEEE Transactions on Aerospace and Electronic Systems* (2011).

[21] Kuhn, M. G. An asymmetric security mechanism for navigation signals. In *Information Hiding* (2005).

[22] Ledvina, B. M., Bencze, W. J., Galusha, B., and Miller, I. An in-line anti-spoofing device for legacy civil GPS receivers. In *Proceedings of the International Technical Meeting of the Institute of Navigation* (2010).

[23] Lehner, A., and Steingass, A. The land mobile satellite navigation multipath channel–a statistical analysis. In *Proceedings of the 2nd Workshop on Positioning, Navigation and Communication (WPNC) & 1st Ultra-Wideband Expert Talk (UET)* (2005).

[24] Lo, S. C., and Enge, P. K. Authenticating aviation augmentation system broadcasts.

[25] Manandhar, D., Shibasaki, R., and Torimoto, H. GPS reflected signal analysis using software receiver. *Journal on Positioning* (2006).

[26] Misra, P., and Enge, P. *Global Positioning System: Signals, Measurements and Performance Second Edition.* Lincoln, MA: Ganga-Jamuna Press, 2006.

[27] Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In *Proceedings of the ION International Technical Meeting* (2009).

[28] Nighswander, T., Ledvina, B. M., Diamond, J., Brumley, R., and Brumley, D. GPS software attacks. In *Proceedings of the ACM Conference on Computer and Communications Security* (2012).

[29] Papadimitratos, P., and Jovanovic, A. GNSS-based Positioning: Attacks and countermeasures. In *Proceedings of the IEEE Military Communications Conference, MILCOM.* (2008).

[30] Phelts, R. E. *Multicorrelator techniques for robust mitigation of threats to GPS signal quality.* PhD

thesis, Stanford University, 2001.

[31] Psiaki, M. L., O'Hanlon, B. W., Bhatti, J. A., Shepard, D. P., and Humphreys, T. E. Civilian GPS spoofing detection based on dual-receiver correlation of military signals. *Institute of Navigation GNSS (ION GNSS)* (2011).

[32] Psiaki, M. L., Powell, S. P., and O'Hanlon, B. W. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In *Proceedings of the ION GNSS+ Meeting* (2013).

[33] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., and Capkun, S. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM Conference on Computer and communications security* (2011).

[34] Titterton, D., Weston, J., et al. *Strapdown Inertial Navigation Technology. 2nd Edition.* IET, 2004.

[35] Warner, J. S., and Johnston, R. G. GPS spoofing countermeasures. *Homeland Security Journal* (2003).

[36] Wendel, J., Meister, O., Schlaile, C., and Trommer, G. F. An integrated GPS/MEMS-IMU navigation system for an autonomous helicopter. *Aerospace Science and Technology* (2006).

[37] Wesson, K., Rothlisberger, M., and Humphreys, T. Practical cryptographic civil GPS signal authentication. *Journal of Navigation* (2012).

[38] Wesson, K., Shepard, D., Bhatti, J., and Humphreys, T. E. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *Proceedings of the ION GNSS Meeting* (2011).

# APPENDIX

**TEXBAT Spoofing Traces as mapped in Figure 9**

| Trace Set | Description |
|---|---|
| Trace 1 | (ds3) Static Matched Time Push |
| Trace 2 | (ds2) Static Overpowered Time Push |
| Trace 3 | (ds4) Static Matched Position Push |
| Seamless 1 | (ds7) Seamless Carrier Phase Aligned |
| Seamless 2 | (ds8) Security Code Estimation Replay |