A Survey of Spoofing and Counter-Measures

Christoph Günther
Deutsches Zentrum für Luftfahrt (DLR), Oberpfaffenhofen, and
Technische Universität München (TUM), Munich, Germany

Received November 2013; Revised April 2014

ABSTRACT: *The growing economic importance of Global Navigation Satellite Systems (GNSS) makes it rewarding for malevolent people to aim at misleading receivers in their position and time estimation. This can be achieved by replacing or superposing signals to the authentic GNSS satellite signals and is called spoofing. Most current receivers are not designed to detect spoofing. The present article aims at a systematic exposition of threats. In many cases, they can be addressed by comparing the received signals, the estimated states, and their respective dynamics against models. A cryptographic signature of the navigation message would furthermore improve the detectability of fake synthetic signals, and should be implemented in the definition of new GNSS signals. In general, the analysis of spoofing should receive the same attention as the analysis of natural impairments. We hope that the present paper will contribute to achieve this.* Copyright © 2014 Institute of Navigation.

INTRODUCTION

Spoofing is the intentional manipulation of GPS signals by a so-called "spoofer" to mislead one or several target receivers in their position or time estimation. The Volpe report analyzed potential vulnerabilities of GPS and identified spoofing as a critical threat [1]. Very few cases are known today. A prominent but contested one is Iran's claim to have forced the landing of an American drone "RQ-170 Sentinel" in December 2011 by spoofing its GPS receiver. Humphreys demonstrated the feasibility of the capture of a UAV with unencrypted signals in 2012 [2]. He took control of a civil drone by spoofing its GPS receiver and successfully landed it. One year later, in 2013, he controlled the course of a yacht at sea [3]. This shows that the threat is real in a certain context. In Europe, unintentional spoofing by GPS repeaters occurred at an international airport. In one configuration, airborne receivers locked on a repeater and caused ground proximity warnings during take-off [4].

The understanding of GPS as well as the skills needed to mount an intentional spoofing attack are becoming more widely available. The threat is similar for all current Global Navigation Satellite Systems (GNSS). The potential motivations for spoofing attacks are rather diverse, reaching from terrorism, through fraud, to avoiding traceability by the employer. In all cases, spoofing is or should be illegal. Each possible exemplary motivation has a different target and requires a different amplitude of the induced error:

- A terrorist who wants to send a vehicle onto a collision path must induce an error of a few tens of meters - this corresponds to a fraction of a microsecond in propagation time
- Drivers who want to evade toll need to displace their position by a few kilometers, i.e., delays in the order of tens of microseconds
- Fishermen who want to catch fish outside of the permitted areas need displacements in the order of tens of kilometers, i.e., delays up to a fraction of a millisecond, and
- Criminal organizations who want to manipulate the timing of financial transactions need errors at the millisecond-level.

The range of delays that must be induced in signals thus varies from fractions of a microsecond to several milliseconds. In general, shorter delays are more difficult to discover.

The limited spread of know-how in the early phase of satellite navigation made spoofing unlikely. Thus it was not publicly discussed. The situation changed with time and the Volpe report raised the issue in 2001. In the same year, Scott published his paper [5] on anti-spoofing and authentication, which became the root paper for later research. He addressed most of the techniques with respect to their harming potential and proposed specific counter-measures. He also triggered awareness in the scientific community. Recent overview papers were written by Hein, Kneissl, Avila-Rodriguez, and

NAVIGATION: *Journal of The Institute of Navigation*
Vol. 61, No. 3, Fall 2014
Printed in the U.S.A.

Wallner [6, 7], Kröner and Dimc [8], as well as Wesson, Shepard, and Humphreys [9]. The introductory statements to other papers also include overviews, see for example the paper by Pozzobon, Wullems and Kubik [10].

The present article further develops this prior art by providing a systematic description of options for manipulating the position and clock-offset estimated by GNSS receivers and describes associated counter-measures. The second section introduces the options for misrepresenting position and time in a target receiver by forging navigation messages or by manipulating the phasing of signals. This requires injecting a spoofed signal into the target receiver. Different options for injecting the signal, as well as for the onset of spoofing are discussed in that same section. The third section presents counter-measures based on signal- and state-analysis, on the consistency of signals, on the conformance of signals and states to models, as well as on the authentication of the navigation messages and navigation signals. The section concludes with the description of a generic monitoring approach. The article addresses structural aspects in some depth but does not attempt to propose any dimensioning of specific solutions. The complete discussion is focused on over-the-air threats and specifically on modifications of the GNSS signals themselves. It does not cover receiver modifications, or manipulations in the infrastructure of GNSS systems, or augmentation systems.

We believe that spoofing should be taken as seriously as any natural threat to GNSS position and time estimation. Much of the defense is implemented in the receiver, but it also relies on support from the GNSS system itself. Galileo is currently redefining its navigation messages. Message authentication is discussed in this context, but not yet decided upon. We recommend the implementation of authentication on E1 and at least one E5 signal for all Galileo satellites in order to improve the protection against spoofing in the future.

SPOOFING

Spoofers aim at misrepresenting the position and/or time estimation of a target receiver by manipulating the signals processed by the target receiver. For convenience, we group the position $\vec{r}$ and clock-offset δ of the receiver in a state denoted by $\xi^T = (\vec{r}^{\,T}, c\delta)$, with c being the velocity of light. If the user has a model on how this state changes over time, this restricts the possibilities of a spoofer. The same applies for the satellite clocks and orbits, as well as for the atmospheric and multipath delays. A smart spoofer must aim at staying within the boundaries of such models. Spoofers are assumed to be smart and assume themselves that the defending receiver is smart as well. Additional sensors, such as accelerometers, gyroscopes or an external clock can support the target receiver in discovering spoofers. The focus of the present paper is, however, on using GNSS measurements for this purpose. The term "spoofer" denotes both the person conceiving the attack and the device used for it. In order to improve the readability, and more specifically the distinction of the spoofer from the receiver, we shall refer to the spoofer as "he" and to the receiver as "it."

Satellite navigation receivers can be categorized into snap-shot and tracking receivers (see Misra and Enge [11] for a general discussion of receivers). Snap-shot receivers sample the signal and subsequently process these samples from memory. The frequency offset, delay and phase are not tracked continuously. *A priori* knowledge about the frequency offset and delay are either used from one measurement to the next or are obtained from a mobile telephony network in the form of so-called assistance data (see van Diggelen [12] for a discussion of assisted GNSS). The time span between two measurements varies widely. It is chosen in a tradeoff of functional requirements and power consumption. This type of receivers is used in most consumer products. Tracking receivers, on the contrary, continuously estimate the frequency, delay, and phase of the signal, i.e., they extensively use prior knowledge about the signal. Prior to tracking, these receivers must search for the signal. This happens during the so-called acquisition phase. In the tracking phase, receivers are rather robust to signal impairments and achieve an improved accuracy. If they lose tracking, they perform a reacquisition using their knowledge about the latest values of the code phase and frequency offset. Tracking receivers are used in many professional applications. The presentation in this paper focusses on *tracking receivers*. With respect to their vulnerability to spoofing, snap-shot receivers behave like tracking receivers, which perform reacquisition for every measurement.

Time Dimension

Satellite navigation receivers are susceptible to spoofing attacks rather differently during the acquisition and the tracking phase. Spoofers will aim at taking advantage of this dependency. The first step during initial acquisition is a search through all plausible codes, all plausible combined Doppler shifts and oscillator frequency offsets, and all delays. If a signal is detected with a sufficient probability the tracking loops for the delay (DLL) and the frequency offset (FLL) are initiated. In a next step phase synchronization is acquired and a loop for phase (and frequency) tracking (PLL) is started.

The DLL, FLL, and PLL for a given carrier are often coupled. However, in a classical receiver, the loops of different satellites or carriers run independently. This changes with the Vector Tracking Delay Locked Loop (VDLL) introduced by Spilker [13], and extended by Zhodzishsky, Yudanov, Veitsel, and Ashjaee to include joint delay and frequency tracking [14]. In these cases, the tracking of the signals takes advantage of the fact that all satellite signals are received by the same antenna located at $\vec{r}$ and moving with velocity $\dot{\vec{r}}$. The approach was further extended to include carrier phase tracking by Giger and Günther [15]. These schemes have simple internal models for the time evolution of all state variables, including atmospheric delays. They can bridge periods of signal loss on individual satellites, e.g., due to jamming, and are difficult to dislodge from tracking the GNSS satellite signals. A spoofer who wants to mislead such a receiver needs to act very cautiously on all signals at once.

In the present paper we focus on independently tracked signals. The spoofer has the option to capture one signal at a time, and to do this while the receiver is in different states:

CS *Spoofing starts before acquisition and the receiver has no a priori knowledge*: This situation occurs after a receiver is switched on (cold start). It provides a maximum of options to the spoofer who wants the receiver to capture his signal first. The receiver cannot distinguish the spoofer's signal from an authentic GNSS signal unless the signal is somehow authenticated. The receiver's clock might have drifted substantially and the position might be completely different at power-up than it was at power-down.

Ra *Spoofing starts before acquisition but the receiver has a priori knowledge*: This occurs if the receiver has lost one or all satellites for a short while, or acquires satellites that have newly raised above the horizon. Snap-shot receivers are in this situation for every estimate that they perform once they have prior knowledge. In all these cases, the spoofer has to be aware that the receiver combines knowledge about its state, the environment, and their evolution to detect spoofer activity. Changes that a receiver might analyze against models include position, clock-offsets, and atmospheric delays.

Tr *Spoofing during tracking*: This is the most demanding situation for the spoofer, since the signals now have to change in a manner compatible with the detailed physical movement of the receiver, as well as with the changes in its environment. Vector tracking can be used to further harden the receiver in this state.

The above description provides a characterization with respect to the relative timing of spoofing and acquisition. The naming of these states is CS for "Cold Start," Ra for "Reacquisition," and Tr for "Tracking." The first situation, i.e., "Cold Start," gives the largest freedom to the spoofer. The last situation, "Tracking" (Tr), is easiest to defend by the receiver. The spoofer might thus aim at provoking a "Reacquisition" by jamming the receiver before initiating the spoofing procedure. Although such jamming creates a signature, the latter signature could also have a natural cause. If the target receiver uses this signature as a sole trigger for detecting the spoofer, this might reduce service availability to an unacceptably low level. The spoofer has the final option to willingly cause a denial of service if he feels that he cannot deceive the receiver otherwise.

Generating Position and Clock Errors

GNSS receivers estimate their position and clock-offset using pseudoranges. A pseudorange is the time between the transmission of the signal by the satellite measured by the satellite's clock and the time of arrival of the signal at the receiver measured by the receiver's clock. For the signal transmitted by satellite k on the carrier frequency with index m, the pseudorange thus is:

$$\tilde{\rho}^k_m = c\left(t^k_{RX,m} - t^k_{TX,m}\right), \tag{1}$$

with $t^k_{RX,m}$ being the time of reception, as measured by the code- or potentially the carrier-phase of the received signal, and with $t^k_{TX,m}$ being the time of transmission as encoded in the navigation message. The free electrons in the ionosphere are one cause for the m-dependency of the receive time. The group delay variations in the transmit and receive hardware, respectively, are other causes. They influence the receive time $t^k_{RX,m}$ and the transmit time $t^k_{TX,m}$, respectively. A spoofer has the possibility to modify the transmit time information used by the receiver or to manipulate its receive time estimate. In order to understand the latter option, we assume that a spoofer located at $\vec{r}\,'$ measures the time of arrival $t'^k_{RX,m}$, then his pseudorange $\tilde{\rho}'^k_m$ becomes

$$\tilde{\rho}'^k_m = c\left(t'^k_{RX,m} - t^k_{TX,m}\right).$$

Assume that the spoofer transmits a spoofing signal with a delay $\tau^k_{S,m}$. If the target receiver locks onto it, and if the spoofing signal does not interfere with the satellite signal, the target receiver determines the spoofed pseudorange:

$$\begin{aligned}\tilde{\rho}^k_{S,m} &= ct^k_{RX,S,m} - ct^k_{TX,S,m} + c\left(\delta - \delta'\right)\\ &= \left(\|\vec{r} - \vec{r}^{\,\prime}\| + c\tau^k_{S,m} + ct'^k_{RX,m}\right) - ct^k_{TX,S,m} + c\left(\delta - \delta'\right)\\ &= \left(\|\vec{r} - \vec{r}^{\,\prime}\| + c\tau^k_{S,m} + \tilde{\rho}'^k_m + ct^k_{TX,m}\right) - ct^k_{TX,S,m}\\ &\quad + c\left(\delta - \delta'\right),\end{aligned} \tag{2}$$

with $c\left(\delta - \delta'\right)$ being the difference in the clock-offset of the target receiver and of the spoofer receiver. In this expression, the spoofer manipulates the receive time $t^k_{RX,S,m}$ by adapting the delay $\tau^k_{S,m}$ and modifies the transmit time $t^k_{TX,S,m}$ by substituting the content of the navigation message. This gives him several options for influencing the pseudorange, which he might combine for reducing the likelihood of being detected.

The option of manipulating the received signal is realized by

- delaying the GNSS satellite signals (called meaconing),
- by replacing the GNSS satellite signal by a synthetic signal, or
- by superimposing synthetic signals to the GNSS satellite signals.

Changing the content of the navigation message is easier with synthetic signals but can also be implemented with stream encrypted signals if the content of the navigation message transmitted by the satellite is known. Since information about the orbits and clock-offset are transmitted on both open and encrypted signals, this is a weakness of stream encrypted systems such as GPS P(Y) and presumably all other military, public regulated, and authorized services.

The pseudorange is related to the state ξ through the equation:

$$\begin{aligned}\tilde{\rho}^k_m &= \left(\vec{e}^{\,k}\right)^T\left(\vec{r} - \vec{r}^{\,k}\right)\\ &\quad + c\left(\delta - \delta^k\right) + m\left(E^k\right)T_z + q^2_m I^k + \eta^k_m,\end{aligned} \tag{3}$$

with

- $\vec{r}^{\,k}$ and $c\delta^k$ denoting the known position and the clock-offset of the k-th satellite at the time of transmission,
- $\vec{e}^{\,k}$ being the unit vector pointing from the k-th satellite to the receiver,
- T_z and $m(E^k)$ being the tropospheric zenith delay and the associated mapping function, and E^k being the elevation of the k-th satellite,
- I^k being the ionospheric slant delay for satellite k, with $q^2_m = f^2_1/f^2_m$ being the ratio of the squared carrier frequencies relative to $f_1 = 154 \cdot 10.23$ MHz, and
- η^k_m being the noise associated with the measurement of $\tilde{\rho}^k_m$, which is modeled as zero-mean Gaussian.

Equation (3) is the basis for understanding the options relating to modifications of the navigation message. Let $\xi_S = \xi + \Delta\xi_S$ denote the state that the spoofer wants the target receiver to estimate, then he can cause the receiver to estimate ξ_S by modifying the satellite clock corrections $c\delta^k$ and/or the satellite orbits and thus $\vec{r}^{\,k}$ for all satellites in the following manner:

$$\begin{aligned}\vec{r}^{\,k}_S &= \vec{r}^{\,k} + \alpha\left(\Delta\vec{r}_S + \vec{e}^{\,k}c\Delta\delta_S\right) \quad \text{and}\\ c\delta^k_S &= c\delta^k + \beta\left(\left(\vec{e}^{\,k}\right)^T\Delta\vec{r}_S + c\Delta\delta_S\right).\end{aligned} \tag{4}$$

All choices of α and β with $\alpha + \beta = 1$ lead to the desired value ξ_S. The relative weighting of α and β depends on the known stability of the clocks and orbits. With $\beta = 1$, the spoofer only modifies the satellite clock-offsets, and with $\alpha = 1$ only the satellite orbits. Additionally, the spoofer can modify the tropospheric and ionospheric parameters. The estimation of the troposphere by the receiver is typically based on models. In Satellite Based Augmentation Systems (SBAS) the associated parameters are provided in the augmentation message and can be modified there. In other systems these parameters are internal to the receiver and are therefore not available to the spoofer. In carrier phase positioning the tropospheric zenith delay is sometimes co-estimated from measurements. Throughout the paper, we shall assume that the tropospheric delay is obtained from a model. The estimation of the ionosphere is radically different in receivers that process single or multiple carrier frequencies. In single frequency receivers, the atmospheric parameters must be provided externally, either through a global ionospheric model (Klobuchar for GPS [16], NeQuick for Galileo [17]) whose parameters are transmitted in the navigation message or through a regional map (SBAS) transmitted in an augmentation message. With this information, the receiver computes the corrected "pseudoranges":

$$\rho^k_m = \tilde{\rho}^k_m + \left(\vec{e}^{\,k}\right)^T\vec{r}^{\,k} + c\delta^k - m\left(E^k\right)T_z - q^2_m I^k,$$

and solves the system of equations:

$$\rho^k_m = \left(\vec{e}^{\,k}\right)^T\vec{r} + c\delta + \eta^k_m, \tag{5}$$

for the state $\xi^T = \left(\vec{r}^{\,T}, c\delta\right)$ by least squares estimation, a Kalman filter or a more general Bayesian

estimator. A shifted state ξ_S can be obtained by modifying the ionospheric delay as follows:

$$I_S^k = I^k - \gamma \left(\left(\vec{e}^{\,k} \right)^T \Delta \vec{r}_S + c \Delta \delta_S \right),$$

with $\alpha + \beta + \gamma = 1$. This is more easily achieved using an SBAS map than through a model which always shows a certain rigidity. The latter rigidity may force the spoofer to eliminate some satellites from the receiver's solution, which he cannot adapt sufficiently. This might be achieved by transmitting a navigation bit sequence that is sufficiently far from a codeword to be rejected or by setting the health flag to "unhealthy." Modifying the ionospheric delay is often more plausible than modifying the clock-offset or the orbits but it is also limited as shall be seen below. In a multi-frequency scenario, the receiver computes the corrected "pseudoranges" in a different manner:

$$\rho_m^k = \tilde{\rho}_m^k + \left(\vec{e}^{\,k} \right)^T \vec{r}^{\,k} + c\delta^k - m \left(E^k \right) T_z,$$

and estimates the extended state, consisting of position, clock-offset and the ionospheric parameters, i.e., $\xi^T = \left(\vec{r}^{\,T}, c\delta, I^1 \ldots I^K \right)$ by solving the system of equations:

$$\rho_m^k = \left(\vec{e}^{\,k} \right)^T \vec{r} + c\delta + q_m^2 I^k + \eta_m^k \tag{6}$$

as before. In this case, the spoofer modifies the delay of the pseudoranges on each carrier individually, to reach his target.

In conclusion, a spoofer can misrepresent the state ξ:

- by modifying $t_{TX,m}^k$, $\vec{r}^{\,k}$, $c\delta^k$, and I^k in the navigation message, or any auxiliary message used by the receiver (augmentation, assistance,...), or
- by manipulating $t_{RX,m}^k$ itself, through a time delay $\tau_{S,m}^k$.

This completes the list of ways for a spoofer to misrepresent the state ξ by acting on the GNSS signals and navigation messages. If the target receiver uses assistance or augmentation data, a spoofer can also influence ξ by manipulating this data. Assistance data are typically transmitted through mobile radio systems. Some of them apply cryptographic protection to user data. Satellite Based Augmentation Systems (SBAS) provide their data on GNSS carriers broadcast by geostationary satellites. They show the same vulnerabilities on the path "satellite to receiver" as the GNSS signals themselves. The path "ground segment to satellite" must be considered as well. Finally, differential augmentation systems provide their corrections to code and carrier phase measurements using a large variety of typically unprotected air-interfaces. The vulnerability of satellite navigation receivers to the manipulation of augmentation data must be addressed with the same depth in all these cases. In the case of Ground Based Augmentation Systems (GBAS) measures have been taken to protect the VHF-links. They are implemented in the corresponding standards of the Radio Technical Commission for Aeronautics (RTCA) and the International Civil Aviation Organization (ICAO), see also Lo and Enge [18]. The latter authors further propose an authentication scheme for GBAS and SBAS that relies on cryptographic methods developed later in this paper, as well as on multiple independent sources of keys in the large area visited by an aircraft during its flight. Using the latter property forces the spoofer to act globally.

Manipulation attempts in the GNSS ground and satellite segment must be prevented as well. This is within the responsibility of the system operator. It is addressed by strict isolation of the control centers (access of individuals, absence of data links to the external world, and shielding of electromagnetic radiation) as well as by cryptography used for protecting the links to the satellites. On the receiver side, potential manipulations of the hardware and of the interface to the application must be avoided as well. This is addressed by Pozzobon, Wullems, and Detratti [19] (hardware) and by Pozzobon, Wullems, and Kubik [10] (interface). In some applications global system aspects must finally be considered to prevent an auxiliary device from collecting raw data at the location at which the receiver should be and replaying it to the front-end of the actual receiver while it is at another location. Such aspects are beyond the scope of the present paper which focuses on the prevention of local manipulations of signals.

Type of Spoofing Signals - Meaconing

There are two fundamentally different types of spoofing signals. The first one is a (local) replay of authentic GNSS satellite-generated signals - this form of spoofing is called meaconing. For the spoofer it is attractive since any form of signal authentication is maintained, including the encryption used in military and Public Regulated Signals (PRS), such as GPS P(Y) and GPS M-code as well as Galileo PRS. The spoofer is, however, limited to delay signals. The second form of spoofing uses fully synthetic signals. Since the current open services do not include any cryptographic protection, these open GNSS signals can be synthesized by everyone. A receiver locked onto synthesized signals has no means to distinguish them from authentic GNSS satellite signals. This statement assumes that the spoofer

generates realistic signals, with a plausible signal to noise ratio, multipath, and ionospheric propagation as well as a realistic dynamic of the associated parameters. Excellent GNSS simulators are commercially available for tests during receiver development and receiver manufacturing. They can be used for spoofing operations. This provides spoofers with much freedom in choosing the phasing of the signals and in injecting signals in a receiver without being detected.

In the simplest version of meaconing, the spoofer captures the signals at position $\vec{r}'$ and retransmits them with a delay τ_S. Assuming that the receiver is at position $\vec{r}$, and that the receiver locks on the spoofed signal, this leads the target receiver to determine the following pseudoranges:

$$\rho_S^k = \left(\vec{e}^{\,k}\right)^T \vec{r}' + c\left(\delta + \tau_S\right) + \|\vec{r} - \vec{r}'\| + \eta_S^k, \qquad (7)$$

and to estimate the state $\xi^T = \left(\vec{r}'^T, c\left(\delta + \tau_S\right) + \|\vec{r} - \vec{r}'\|\right)$, i.e., a position that is the spoofer's position and a clock-offset $\delta + \tau_S + \|\vec{r} - \vec{r}'\|/c$. The noise and multipath interference are increased by the spoofer receiver. It is subsumed in a zero-mean Gaussian term η_S^k. With Equation (7), the spoofer must be able to place his antenna in the location, which he intends the user to estimate. This is impractical in many scenarios. It happened unintentionally in aeronautics, with receivers locking on GNSS repeaters [4]. Such repeaters are used in hangars for testing purposes after maintenance.

In a second more sophisticated approach, the spoofer delays the signals from different satellites individually. In obvious notations:

$$\rho_S^k = \left(\vec{e}^{\,k}\right)^T \vec{r}' + c\left(\delta + \tau_S^k\right) + \|\vec{r} - \vec{r}'\| + \eta_S^k. \qquad (8)$$

For this purpose, he must first separate the signals. Assuming that the orbits of the satellites are known, both an array of antennas or a set of reflectors can isolate the individual signals to a certain degree. The isolated signals are then replayed with a delay τ_S^k in order to make the receiver believe that it is in the spoofed position $\vec{r}_S$ rather than in the true position $\vec{r}$. The position $\vec{r}_S$ is now arbitrary and no more the spoofer's location. The spoofer induces the desired displacement $\Delta\vec{r}_S = \vec{r}_S - \vec{r}'$ with respect to his position by choosing:

$$c\tau_S^k = \left(\vec{e}^{\,k}\right)^T \Delta\vec{r}_S + c\tau_S$$

with

$$c\tau_S = -\min_k \left(\vec{e}^{\,k}\right)^T \Delta\vec{r}_S,$$

which implies

$$\rho_S^k = \left(\vec{e}^{\,k}\right)^T \vec{r}_S + c\left(\delta + \tau_S\right) + \|\vec{r} - \vec{r}'\| + \eta_S^k.$$

Note that the noise includes components from the directional reception at the spoofer and from the reception at the target receiver, as well as from their respective propagation and interference environments. The choice of the delay τ_S ensures that

$$c\tau_S^k \geq 0,$$

i.e., that all delays are positive and thus realizable. The spoofed receiver estimates $\xi^T = \left(\vec{r}_S^T, c(\delta + \tau_S) + \|\vec{r} - \vec{r}'\|\right)$. The position is as intended by the spoofer, but the clock-offset is changed. The latter provides a signature that can be used by the target receiver. This generalized form of meaconing provides more flexibility to the spoofer but is rather complex. We do not believe that it will be broadly applied in the near future.

Injecting the Spoofed Signals

In the earlier discussion of the *Time Dimension*, different possibilities for the timing of the onset of spoofing were introduced. Similarly, the spoofer has different options for injecting the signal:

Cab *Cable inject:* In this case, the spoofer directly injects his signal into the receiver front-end either by unplugging the antenna cable and by connecting it to the spoofing source or by significantly attenuating the GNSS signals and injecting the spoofing signal at the same time. This option gives the spoofer the maximum control possible. It can be implemented whenever the receiver is under the spoofer's control, typically for tracking his movement (control road toll, manage fleets, follow stolen cars, enforce fishing limitations, track criminals,...).

Coh *Spoofing by coherent superposition:* In this case, the spoofer knows the precise location of the receiver's antenna, as well as the phasing of the signal. In the coherent case, the spoofer suppresses the main component of the authentic satellite signal by subtracting a synthesized copy of that component for a time long enough to capture the receiver to his signal. Reference receivers provide the kind of information needed for such an approach.

NCo *Spoofing by non-coherent superposition:* In this case the spoofer has lesser control. He must hide the authentic signal in noise. This option is more widely applicable but is easier to defend.

In order to discuss these cases, we consider a generic GNSS signal $s(t)$, composed of a navigation message $b(t)$ modulated on a spread spectrum signal $u(t)$:

$$s(t) = b(t)u(t).$$

Both components $b(t)$ and $u(t)$ depend on the satellite index k and the carrier index m. The n-th bit of the navigation message $b^k_{m,n}$ is transmitted in the interval $\left[\left(n-\frac{1}{2}\right)T_b, \left(n+\frac{1}{2}\right)T_b\right)$:

$$b^k_m(t) = \sum_n b^k_{m,n}\left(\theta\left(t-\left(n-\frac{1}{2}\right)T_b\right) - \theta\left(t-\left(n+\frac{1}{2}\right)T_b\right)\right),$$

with $\theta(t)$ being the Heaviside function, i.e., $\theta(t) = 1$ for $t \geq 0$ and 0 otherwise. The spread spectrum signal is given by $u^k_m\left(t; \omega_m + \omega^k_D\right)$, with

$$u^k_m(t,\omega) = \sum_n c^k_{m,n}\, p_m(t - nT_c)\cos(\omega t + \phi^k_m),$$

and with

- $c^k_{m,n}$ being the n-th chip of the spreading code,
- p_m being the pulse form used on the m-th carrier,
- ω_m and ω^k_D being the carrier and Doppler frequencies, respectively, and
- ϕ^k_m being the phasing of the signal.

For simplicity, the following considerations are limited to the single carrier frequency case, which allows us to drop the index m. The extension to the multi-frequency case is straight-forward. Due to multipath, the receiver and the spoofer see superpositions of several copies of the above signals, which are delayed and phase rotated. The resulting signal is additionally degraded by noise, leading to:

$$y(t) = \sum_k \sum_i h^k_i b^k\left(t - t^k_{RX}\right) u^k\left(t - t^k_{RX} - \tau^k_i; \omega + \omega^k_{D,i}\right) + n(t),$$

with h^k_i, τ^k_i, and $\omega^k_{D,i}$ being the complex amplitude, phase, and Doppler-shift associated with the i-th multipath component of the signal from satellite k. The direct path always has zero delay, i.e., $\tau^k_0 = 0$, and a Doppler-shift that only depends on the relative movement of the receiver and of the satellite. The impact of τ^k_i on the bits of the navigation message is neglected. A spoofer would like the target receiver to track his signal:

$$s_{S,\omega_{S,D},\tau_S}(t) = \sum_k \sum_i h^k_{S,i} b^k_S\left(t - t^k_{RX,S}\right) u^k\left(t - t^k_{RX,S} - \tau^k_{S,i}; \omega + \omega^k_{S,D,i}\right),$$

with

- $b^k_S(t)$ being the spoofed navigation message of satellite k,
- $t^k_{RX,S}$ being the receive time of the spoofer's signal with satellite-index k chosen to induce the desired state estimation error $\Delta\xi_S$. It is related to the receive time at the spoofer t'^k_{RX}, to the extra delay τ^k_S used to tune the estimate, and to the propagation time from the spoofer to the target receiver through the equation:

$$t^k_{RX,S} = t'^k_{RX} + \tau^k_S + \|\vec{r} - \vec{r}\,'\|/c. \tag{9}$$

- $h^k_{S,i}$, $\tau^k_{S,i}$, and $\omega^k_{S,D,i}$ finally are the complex amplitude, delay, and Doppler-shift of the artificial multipath component i for the satellite signal k.

If the spoofer has direct access to the antenna interface (Option Cab) he does effectively replace the signal $r(t)$ by

$$s_{S,\omega_{S,D},\tau_S}(t) + n_S(t),$$

with $n_S(t)$ being noise inserted to make the signal appear more realistic. This is the first and most impacting option. Nearly any choice of $\omega_{S,D}$ and τ_S are possible with this option. A meaningful choice for these parameters is closest to the authentic GNSS signal.

In cases where the spoofer has no access to the antenna interface, the next best he might aim for is to cancel the direct path and to superimpose it with the spoofing signal:

$$-h^k_0 b^k\left(t - t'^k_{RX} + \|\vec{r} - \vec{r}\,'\|/c\right) u^k\left(t - t'^k_{RX} + \|\vec{r} - \vec{r}\,'\|/c\right) + s_{S,\omega_{S,D},\tau_S}(t) + n_S(t). \tag{10}$$

The first term in this expression cancels the direct path and the second term inserts the spoofing signal. This option requires that the phase of the receiver be known by the spoofer. For this reason it is called "Spoofing by coherent superposition" (Coh). In order to remain undiscovered, the spoofer starts with $\omega^k_{S,D,0} = \omega^k_{S,D}$, $\tau^k_{S,0} = 0$, and

$$t^k_{RX,S} = t'^k_{RX} + \|\vec{r} - \vec{r}\,'\|/c,$$

as well as values of $h^k_{S,i}$, $\tau^k_{S,i}$, and $\omega^k_{S,D,i}$ that are as close as possible to a realistic multipath. Furthermore, the spoofer transmits the authentic navigation message. He then tunes $t^k_{RX,S}$ to the desired value as described by Equation (9), and smoothly ramps up the strength of the signal h_0 and $h_{S,0}$. Furthermore, he adds the other multipath components ($i > 0$) in a manner compatible with models, such as those proposed by Lehner, Steingaß, and Schubert [20]. Ideally, he also phases-in an offset $\Delta\omega = \omega_{S,D,0} - \omega_{S,0} = 2\pi/T_u$ in the carrier-frequency,

with T_u being the period of the spreading sequence. Since the integration time T_i is typically a multiple of T_u this implies that the sinc-factor in the correlation of the received signal and the local replica

$$\mathrm{sinc}\left(\Delta\omega\, T_i/2\right)$$

is zero or near to zero. Obviously, there is a transient in which the two signals are superposed, which the spoofer must make appear realistic. His aim is that the phasing of his signal is earlier than the phasing of the satellite signal since receivers track the earliest path. The spoofer succeeds if the receiver stays locked on his signal and thus estimates the pseudorange to be $\tilde{\rho}_S$. In this scenario, a short transient during which the receiver decodes a superposition is unavoidable. This is the chance for the receiver to discover the spoofer. If the spoofer increasingly offsets his frequency, the satellite signal successively disappears, and the receiver tracks the spoofer's signal in a stable manner. If the frequency offset is the same for all satellites on a given carrier, and strictly proportional for different carriers, the receiver interprets the offset as being due to its own oscillator. In GPS the necessary shift for separating the spoofed and authentic satellite signals is 1 kHz, which corresponds to 1 ppm of the carrier frequency and is thus within the specifications of most oscillators. Any departure from strict proportionality can be detected by the target receiver if it analyzes the frequency offsets. These latter offsets are due to the known movement of the satellites relative to the receiver. After having locked onto the spoofer's signal, the receiver decodes the spoofed navigation message b_S. At this stage, the spoofer will switch from the authentic to the spoofed navigation message. He will do this in line with the applicable GNSS specifications.

In the coherent injection mode, the spoofer must know the location of the phase center of the antenna of the target receiver to an accuracy of a fraction of the wavelength. This information is sometimes available if there is no relative movement between the spoofer and the receiver. Reference and monitoring receivers for carrier phase positioning are a critical example. Such receivers provide the necessary information with a very high level of accuracy since this is necessary for them to fulfill their task. Implementing Equation (10) is rather difficult in most other situations, especially if several receivers are used in one location and if carrier phase measurements are not provided, like in current Ground Based Augmentation Systems (GBAS). In such cases, the spoofer superposes the following signal at the receiver's antenna:

$$h_n^k u_n^k\left(t - t_{RX}^{\prime k} + \|\vec{r} - \vec{r}^{\,\prime}\|/c\right) + s_{S,\omega_{S,D},\tau_S}(t) + n_S(t), \quad (11)$$

with $u_n^k(t)$ being a noise-like signal that correlates well with $u^k(t)$. An example is $\alpha^k(t)u^k(t)$ with $\alpha^k(t)$ being a random complex-valued process, with a bandwidth $\sim 1/T_u$. The power of this process reduces the processing gain associated with $u^k(t)$ and increases the likelihood of the receiver to acquire the spoofing signal. The noise power spectral density of $n_S(t)$ is a tradeoff between ensuring the acquisition of the spoofed signal and at the same time making the presence of the noise-like signal $u_n^k(t)$ plausible. This is the last option in our list, it is called "spoofing by non-coherent superposition" (NCo). The details of the ramp up of h_n and $h_{S,0}$ depend on the initial state of the receiver. The spoofer will chose a fast enough ramp up to prevent the receiver from having a sufficient processing gain in order to find the satellite signal covered by $u_n^k(t)$. When it believes that the receiver has acquired the signal, the spoofer will tune the values of τ_S and increase the frequency offset $\Delta\omega$ to $1/T_u$.

With both coherent and non-coherent superposition, the success of the spoofer depends on the traces of the satellite signal left in the superposition of the spoofing and the satellite signals, as well as on the sophistication of the analysis by the target receiver. From the above exposition, it is obvious that this analysis should also consider the frequency domain, which to our knowledge has not been done so far. Several criteria for finding residual signals in the time domain have been proposed. Wesson, Shepard, Bhatti, and Humphreys [21] are providing an overview of options and an analysis.

A spoofer has a different chance of success with the three injection methods depending on the state of the receiver described earlier. Table 1 summarizes our perception of the level of difficulty for the spoofer or equivalently the level of threat for the user. We proceed column by column. The first column corresponds to cable injection (Cab). In a cold start situation (CS), a spoofer generating realistic signals will capture the receiver. This is a situation where cryptography plays an important role. If the signal sources are switched during reacquisition (Ra), the spoofer will capture the receiver if he manages

Table 1 — Difficulty for a spoofer to succeed in different scenarios characterized by the Case CS (cold start), Case Ra (reacquisition), Case Tr (tracking), and the Option Cab (inject into the antenna interface), Option Coh (cancel the GNSS satellite signal by coherent superposition), Option NCo (hide it in noise). The target receiver is assumed to be maximally smart in all cases.

	Cab	Coh	NCo
CS	very easy	-	less difficult
Ra	easy	-	very difficult
Tr	very difficult	very difficult	very difficult

to synthesize a close reproduction of the signal. Switching the sources during tracking (Tr) would require phase coherence, which is hardly feasible. We now turn to the second column, signal injection by coherent superposition (Coh). This cannot be initiated during cold start (CS) or reacquisition (Ra), since the spoofer cannot know the internal phase offsets of the receiver. The latter is only provided by some reference receivers in the tracking phase (Tr). Still, under this most favorable situation, the spoofer has to ensure the observability of his phasing without being discovered. The non-coherent superposition (NCo), i.e., the cases listed in the last column, are slightly more difficult to detect than those with cable injection. Contrary to the latter Cab-case, the authentic satellite signal is present in the NCo-Case, which provides at least some means for detecting the spoofer. Amongst these options, the spoofer will most easily capture the receiver during cold start (CS). A well designed receiver may discover the noisy screening signal if it is used for a longer period of time. A spoofer may not need much screening if he knows the acquisition strategy of the receiver, e.g., acquiring satellites in a certain order. He could then construct the spoofing signal to ensure that the target receiver acquires his signals first. In the reacquisition mode (Ra), the receiver has a clear expectation about the signal it is looking for. In the case that it does not reacquire a signal whose parameters are compatible with the changes permitted by the movement of the user or changes in the environment it will discard the signal. The analysis of the noise spectrum may also provide hints about the presence of a spoofer. In the tracking mode (Tr), the situation is further improved for the receiver, which tracks the plausibility of all changes against models. All of the above statements only apply for receivers which aim at a maximum of protection. Most current receivers can be fooled in all scenarios described in Table 1.

COUNTER-MEASURES

A spoofer was found to be capable of modifying the pseudoranges and under certain circumstances also the content of navigation messages in the previous sections. In this section we will develop options for detecting the presence of a spoofing signal. This includes the analysis of the measurements and of the state evolution, as well as the use of cryptographic authentication.

Detecting Modified Navigation Messages

Synthetic or manipulated navigation messages can be detected by analyzing

- the scheduling of changes in the navigation message,
- the conformance of changes in the parameters with models,
- the consistency of measurements with the navigation solution, and
- the signature of the navigation message.

The first three options can and should be applied immediately. The last one needs a modification of the current navigation message format or an external authentication channel. This is discussed in the next section.

Today navigation messages are updated on a regular basis. In GPS the update interval is in multiples of one hour with the exception of the first update after the upload of a new data set (see [22], Section 20.3.4.4). Additional changes might be due to setting the "Alert" flag in the Handover Word (HOW) but are extremely seldom. Whatever the pattern is, it can be used to detect changes that are unlikely to be caused by the GNSS system itself.

Satellite orbits are constrained by physics. Operational satellites are currently not maneuvered intentionally. Correspondingly, an orbit propagator can be implemented in the receiver to verify the conformance of changes from one message to the next. The stability of modern rubidium clocks limits changes in the clock to less than 1 ns from one message to the next (up to 120 minutes), which makes larger changes unlikely. A further characterization of clocks (Cs, Rb, H-Maser and their different implementations) would be beneficial for taking best advantage of this test without unduly reducing availability.

The ionosphere provides some freedom during solar maximum. The variability in the navigation message is, however, rather limited even in that case. A model of possible changes seems not to have been developed so far but could be worked out rather easily. It would limit the possibilities for a spoofer to influence the state via this degree of freedom.

With coherent (Coh) and non-coherent signal injection (NCo), the receiver's antenna captures a superposition of the authentic and spoofed signal. This provides an opportunity for the receiver to detect the spoofer. The superposition of signals is difficult to distinguish *a priori* from multipath. The paper by Wesson, Shepard, Bhatti, and Humphreys [21], mentioned previously, studied a number of tests for detecting the spoofer on that basis. Their results show that the dynamic of the metrics are different in the presence of multipath or of a spoofer. In some environments, large multipath contributions are so unlikely, that such a test can potentially be used. This is the case whenever the reduction in availability due to false alarms is low enough. In more general situations, we recommend estimating the multipath. A number of different methods have been developed for this

purpose with Bayesian estimation being the most advanced one. It was analyzed by Lentmaier, Krach, and Robertson [23] (see also the references to other simpler methods in that paper). The estimated multipath components associated with the signals transmitted by the visible satellites on all carrier frequencies are then used to discriminate the spoofer from multipath. Clearly, more intricate models are making this complex but they also very much restrict the options of the spoofer if he wants to stay undiscovered.

Finally, the receiver must also analyze the consistency of its solution with Equations (5) and (6). The latter equations can both be written in the form

$$\rho = H\xi + \eta,$$

with obvious definitions of ρ, H, and η. Given its estimate $\hat{\xi}$, the receiver analyzes the statistics of the difference

$$\rho - H\hat{\xi},$$

with respect to their conformance to multipath and noise models. This is what Receiver Autonomous Integrity Algorithms (RAIM) do, see, e.g., [24] and [25]. Additionally, the receiver should also consider the corresponding equations for the rates:

$$\dot{\rho} = H\dot{\xi} + \upsilon,$$

with

$$\dot{\rho}_m^k = \lambda_m \dot{\varphi}_m^k + \left(\vec{e}^{\,k}\right)^T \dot{\vec{r}}^{\,k} + c\dot{\delta}^k,$$

and

- $\dot{\varphi}_m^k$ being the frequency measurement - derived from the PLL - as well as
- $\dot{\vec{r}}^{\,k}$, and $\dot{\delta}^k$ being the velocity of the satellite and the drift of its clock as derived from the navigation message,
- $\dot{\xi}$ being the velocity of the target receiver and the drift of its clock.

With these variables, the receiver analyzes the statistics of

$$\dot{\rho} - H\dot{\hat{\xi}}.$$

This metric is very sensitive due to the low noise of carrier phase measurements and their low susceptibility to multipath. Thus, in the presence of *a priori* information, the options of the spoofer become rather limited both with respect to the timing and the size of the state changes that can be induced if the receiver performs the above types of verifications.

Navigation Message Authentication (NMA)

The situation changes if the spoofer starts transmitting before the receiver has acquired the signal and if the receiver only has aged *a priori* information or none at all (Cold Start CS). In this case, the spoofer can generate an almost arbitrary synthetic signal and the target receiver will not be able to distinguish it from a signal transmitted by a GNSS satellite. On the contrary, the receiver is likely to reject a leaking-in satellite signal as fake. The cryptographic authentication of navigation messages is an effective counter-measure for preventing this situation. Scott suggested such an approach in [5] and a number of authors have developed it subsequently see [6, 7, 26–29].

An important boundary condition to cryptographic methods is that most users are unlikely to be targeted by spoofers. They shall thus not be affected by the associated counter-measures, i.e., navigation messages shall in particular remain readable in open form. This excludes the use of message encryption. A first option uses symmetric cryptographic signatures, i.e., a key-dependent compressed form of the message, which can only be produced and verified by the owner of the key K. Authentication is ensured if all legitimate users have obtained the key in a trusted manner but no spoofer has access to it. Such a distribution process seems infeasible, even in a limited community such as aeronautics. A single malevolent user would compromise the whole system. Any information distributed before-hand must be assumed to be known to both legitimate users and spoofers.

A second option is to use the timing of uncovering knowledge: specifically, the control center could insert random information in future messages and use this information for signing the current message. In this case, the function (or equivalently a key which parametrizes it) could be known to everyone. The scheme is based on one-way functions, i.e., functions f that can be efficiently computed, using a Probabilistic Polynomial Time (PPT) algorithm, but whose inversion by any PPT-algorithm is unlikely to succeed (see Goldwasser and Bellare [30] for a precise formulation). One-way permutations are one-way functions that are one-to-one. The existence of one-way functions and one-way permutations in a strict sense is open. A number of functions are believed to have the desired property, and are used in today's information and payment systems. This shows the high level of trust in the difficulty of inverting functions that are currently believed to be one-way. In the following, "one-way" shall thus mean such a level of trust. Let f be such a one-way permutation and g be such a one-way function, then the processing center chooses a seed X_ℓ and computes the sequence

of keys $X_0 \ldots X_{\ell-1}$, and the sequence of signatures $Y_0 \ldots Y_\ell$:

$$X_0 = f(X_1) = f^2(X_2) = \ldots = f^\ell(X_\ell),$$
$$Y_i = g(M_i, X_{i+1}), \text{ for } i \in 0 \ldots \ell\text{-}1.$$

The satellite then transmits triples (M_i, Y_i, X_i) and from time to time a signed copy of X_0. The receiver verifies the validity of X_i and the correctness of the signature Y_i. Under the assumption that the function f is a one-way permutation, the computational uncertainty about X_i is essentially equal to the length of X_ℓ. Note that its information theoretical uncertainty (entropy) is 0, since f is a permutation. The unpredictability of X_{i+1} also makes Y_i unpredictable. If the lengths of Y_i and X_{i+1} are the same, the computational uncertainty of Y_i is essentially equal to the length of X_ℓ. This scheme and variants were proposed by Perrig, Canetti, Tygar, and Song [26], and discussed by Wullems, Pozzobon, and Kubik [27] as well as Lo and Enge [18]. Since computer memories with sizes of terabytes are widely available, the minimum length of X_ℓ needs to be significantly larger than $\lceil \log_2 10^{12} \rceil \geq 40$. Otherwise, f could be tabulated. The navigation message channel typically has a data rate of 50 bps (250 bps in some cases), and since the relative allocation to authentication shall be small - a common assumption is 10% or less - such an authentication is at best available after seconds. One element in the chain of X's must furthermore be authenticated, e.g., by providing X_0 while the aircraft is on the ground. Without such an additional authentication, the spoofer could create his own chain with his initial seed $X_{\ell,S}$, and the target receiver could not distinguish the forged chain from the authentic chain.

In 1976 Diffie and Hellman introduced public key cryptography [31], and something that today would be called a trapdoor one-way function. They defined a pair of families of functions E_{K_P} and D_{K_S} with the property:

$$D_{K_S}\left(E_{K_P}(M)\right) = M,$$

i.e., the decryption function D_{K_S} inverts the encryption function E_{K_P}. Both transformations are parametrized by different keys K_S and K_P. Important properties are that it is computationally infeasible to invert E_{K_P} without knowing K_S. Rivest, Shamir, and Adleman introduced an example of such functions [32] with the additional property that:

$$E_{K_P}\left(D_{K_S}(M)\right) = M.$$

These functions are:

$$E_{K_P}(M) = M^{K_P} \mod n, \quad \text{and}$$
$$D_{K_S}(M) = M^{K_S} \mod n$$

with n being a product of two large primes, and with K_P being none of these primes. The primes are kept secret, since they allow one to compute the secret key K_S through the equation $K_S K_P \equiv 1 \mod (p-1)(q-1)$. By the Fermat-Euler theorem, this choice implies (see Theorem 72 in [33]):

$$D_{K_S}\left(E_{K_P}(M)\right) = E_{K_P}\left(D_{K_S}(M)\right) = M^{K_P K_S} \mod n$$
$$= M^{K_P K_S \mod (p-1)(q-1)} \mod n = M.$$

If the control center now publishes n and K_P, and if users can identify (n, K_P) as having originated from the control center, and if the control center decrypts the navigation message or a hash of M:

$$Z = D_{K_S}(M)$$

then this is a signature that can be verified by everyone, through the test:

$$M \stackrel{?}{=} E_{K_P}(Z)$$

but that no one can forge, at least not if it is computationally infeasible to compute D_{K_S} without knowing K_S.

Since the length of the signature grows in parallel to the size of the key, this size is an issue. The National Security Agency (NSA) considered keys with 1024 bits as being secure until 2010 [34], which would mean at least 200 seconds for the transmission on our channel utilizing 10% of its 50 bps rate. This inconvenience can be somewhat reduced by using another public-key system based on elliptic curves introduced by Miller [35] and Koblitz [36]. This system is particularly interesting when the keys have to be further extended due to future increases in computing power. The National Institute of Standards and Technology (NIST) provides a number of recommended curves with key lengths as shown in Table 2. The delays are somewhat reduced but remain critical. As stated earlier, the navigation message changes only rarely. Thus the delay in message authentication mainly impacts the initial acquisition. In a consumer context, the signature could be supplied via a mobile radio channel, which has a much larger bandwidth. Schemes using

Table 2 — Size of keys in bits recommended by NIST to achieve a nearly equivalent security, see [34] for details.

Symmetric key	RSA	Elliptic Curves
80	1024	163
112	2048	224
128	3072	256
192	7680	384
256	15360	521

digital signatures have been proposed for Galileo by Hein, Kneissl, Avila-Rodriguez, and Wallner in 2007 [7] and for GPS by Wesson, Rothlisberger, and Humphreys in 2012 [29]. It appears meaningful to choose a flexible system. This allows one to increase the key length or even to change the trapdoor one-way function should its inversion becomes computationally feasible at some time in the future.

Due to the possibility of transmission errors, signatures are protected by error correcting codes. The associated codes are typically used both for correcting and detecting errors. The receiver performs a trade-off between the two. Let d be the minimum distance between two codewords, let $d' \geq 1$ be the minimum distance between the decoding spheres, which is a receiver parameter, and let t be the distance between the received word and the closest codeword, then different outcomes of the decoding process are possible, see Table 3. A large value of d' increases the probability of correct decoding at the price of a reduced probability of decoding (no output). By design the spoofer is unlikely to guess the signature and thus cannot achieve the first or third option/line in Table 3. If the signal is received with a large Signal-to-Noise Ratio (SNR), errors are unlikely. In this case, the second option occurs with a very high probability, and the spoofer is discovered. Thus, the spoofer must generate a word that is far from any codeword and at the same time inject a level of noise that makes this level of errors plausible (fourth option). The receiver will then not be able to decide whether the received signal is spoofed. A frequent occurrence of cases marked as unlikely should be used by the receiver as an indication of the presence of a spoofing signal.

Partially Authenticated Messages

The tests described in the previous section and the authentication of navigation data using cryptographic signatures make it difficult to spoof a cautious user by modifying authenticated navigation messages. In the case that some signals continue to be broadcast without authentication, the spoofer's next option is to manipulate the navigation message and or phasing of these remaining non-authenticated signals. The different options for initiating such a spoofing attack were described previously. The options for manipulating the signals were described in Equations 10 and (11).

In GPS, the navigation message on the L1 carrier is at least not authenticated initially. For simplicity, we first assume that all signals of the L5 carrier are authenticated. In this case, the processing in the receiver could be restricted to the measurements on L5. The ionospheric delays would then be obtained from a model, e.g., Klobuchar for the ionospheric delay or an authenticated SBAS message, which implies that the position accuracy is then driven by the accuracy of the latter model. Alternatively, the receiver could perform dual frequency processing on L1 and L5. Let

$$g^k = \left(\vec{e}^{\,k}\right)^T \vec{r} + c\delta + m\left(E^k\right) T_z$$

denote the relation between the "geometric" state variables and their contribution to the pseudorange, then the equations for the corrected pseudoranges on carrier L1 and L5 become:

$$\begin{aligned} \rho_1^k &= g^k + I_1^k + \eta_1^k, \\ \rho_5^k &= g^k + q_5^2 I_1^k + \eta_5^k. \end{aligned} \tag{12}$$

Since

$$g^k = \frac{\rho_5^k - q_5^2 \rho_1^k}{1 - q_5^2} + \text{noise}$$

a spoofer who aims at causing an error in state estimation $\Delta\xi^T = \left(\Delta\vec{r}_S, \Delta\delta_S\right)$, would inject an L1 signal with a phasing such that:

$$\rho_{1,S}^k = \rho_1^k - \frac{1 - q_5^2}{q_5^2}\left(\left(\vec{e}^{\,k}\right)^T \Delta\vec{r}_S + c\Delta\delta\right).$$

This shifts the receiver's state estimate according to the spoofer's intention. The shift can, however, be detected if the receiver jointly estimates all state variables including the ionospheric delay. This is easily recognized by inspecting the following ionosphere-preserving geometry-free linear combination (noise not included):

$$\frac{\rho_1^k - \rho_5^k}{1 - q_5^2} = \begin{cases} I_1^k & \text{in the absence of spoofing} \\ I_1^k - \frac{1}{q_5^2}\left(\left(\vec{e}^{\,k}\right)^T \Delta\vec{r}_S + c\Delta\delta\right) & \text{in the presence of spoofing} \end{cases}, \tag{13}$$

and by verifying the plausibility of these values using ionospheric models. The options for the spoofer are thus limited to induce errors that are

Table 3 — Decoding and Signature Verification

Number of errors	Signature Verif.	Conclusion, SNR large	Conclusion, SNR small
$t \leq \lfloor (d - d')/2 \rfloor$	OK	authenticated	unlikely
	wrong	probably spoofed	unlikely
$\lfloor d/2 - 1 \rfloor \geq t > \lfloor (d - d')/2 \rfloor$	OK	unlikely	authenticated?
	wrong	unlikely	undecidable

consistent with ionospheric models. In the presence of a spoofer, the user thus loses the benefit of estimating the ionospheric delay from dual-frequency measurements. Errors of this magnitude are still critical in the context of some safety of life applications, such as the landing of aircraft, and should thus be prevented.

Next, we assume that Galileo authenticates signals on all relevant carriers. Even in this context, there have been some discussions on whether the navigation messages on all satellites need to be authenticated. In order to answer this question, we reconsider Equation (6) with K satellites. The state vector associated with this equation is $\xi^T = \left(\vec{r}^{\,T}, c\delta, I \ldots I^K\right)$. It can be reduced in special situations (known location, on-board atomic clock,...) or when using models for the ionospheric delays. The length of ξ is $\kappa + K$, with $\kappa = 4$ in the above case. In a least squares approach, the solution is completely determined and cannot be forged, if the receiver sees signals authenticated on two frequencies from at least $K \geq \kappa$ satellites. The associated accuracy and integrity are limited by the geometry of this subset of satellites. If the receiver comes to the conclusion that it is not under attack with a sufficient confidence, it can include additional measurements as well. A smart spoofer will jam the authenticated signals in order to make positioning impossible (denial of authenticated service) or to make it very inaccurate. He controls this through the position-related upper 3×3-submatrix of $\left(H^T C^{-1} H\right)^{-1}$. In this expression H is the (multi-frequency) measurement matrix and C the noise (and interference) covariance matrix at the receiver. This means that the spoofer does not control the error but the uncertainty. Since constellations are typically designed to provide an accurate state estimation to users but no more, there is no real slack for leaving some signals unauthenticated. We thus recommend that the navigation message of *all* satellites be authenticated on at least two frequencies. If authentication is only to be available to dual-frequency receivers, the authentication of two carriers can be obtained without additional overhead. The navigation messages on both carriers are simply signed together. This keeps the length of the signature unchanged without weakening it. The signature of the second carrier is obtained at no extra cost.

In order to reduce the authentication delay, the navigation messages may additionally be signed using a different asymmetric cryptosystem in the Internet. This requires that the receiver has access to the Internet, which most receivers do.

The analysis for multiple constellations is very similar. Every constellation which contributes at least two satellites visible at the user's location can be included. The state vector then needs to be expanded with one receiver clock-offset for each constellation. This improves the availability of authenticated position and time estimates.

Detection of Delayed Synthesized Signals

If the GNSS system uses authenticated signals, the spoofer can aim at gaining an advantage over the target receiver in the estimation of the signature bits. With these estimates, the spoofer can then synthesize a forged signal with an arbitrary positive delay but with an unchanged navigation message. In certain combinations of spoofing architectures and receiver processing, this is more promising for the spoofer than the generalized meaconing approach.

One possibility for the spoofer is to introduce a delay. This option can be used after a cold start of the target receiver (Case CS), provided that the target receiver does not use a stable clock. In this scenario, the spoofer delays his synthetic signals by roughly one bit (20 ms for GPS, 4 ms for Galileo), which gives him the possibility to estimate that bit and to reuse it in his synthesized signal.

A second option for the spoofer is to increase his SNR as compared to the target receiver. He might achieve this by array processing. The required gain can be smaller than in generalized meaconing since the spoofer only needs to speed-up his estimation of the signature bits as compared to the target receiver. He does not need to extract clean signals anymore. A smart spoofer continuously estimates the values of the navigation bits. He starts transmitting random chips covered by noise and then increases the SNR of the transmitted signal successively as his estimates of the bit become more reliable. As a counter-measure, the receiver analyzes the SNR of the chips as a function of the chip-phasing n within the signature bits, i.e., it computes partial correlations:

$$C_n^k = \frac{1}{L} \sum_{\ell=0}^{L-1} r_{BB}^k \left(n \frac{T_c}{2} + \ell \frac{T_b}{2} \right) \hat{b}_\ell^k c_n^k,$$

with r_{BB} being the baseband version of the received signal, sampled in the middle of the chip (the delay and phase tracking have been subsumed in r_{BB}):

$$r_{BB}^k \left(n \frac{T_c}{2} + \ell \frac{T_b}{2} \right) \simeq \begin{cases} h_0^k b_\ell^k c_n^k + n_{\ell,n}^k & \text{for the GNSS satellite signal} \\ h_{S,0}^k b_{S,\ell,n}^k c_n^k + n_{\ell,n}^k & \text{for a spoofed signal,} \end{cases}$$

with

- $b_{S,\ell,n}^k$ being the spoofer's estimate of the ℓ-th bit of the k-th signal after having seen n chips,
- $\hat{b}_\ell^k$ being the receiver's estimate of the ℓ-th bit assumed to be mostly correct, i.e., $\hat{b}_\ell^k = b_\ell^k$,

- c_n^k being the known n-th chip of the spreading code,
- h_0^k and $h_{S,0}^k$ being the estimates of the amplitude of the direct path by the receiver and the spoofer, respectively,
- $n_{\ell,n}^k$ denoting the noise and interference contributions from other satellites and multipath, and with
- L being the duration of the summation.

For simplification, the noise is assumed to be zero-mean Gaussian with a covariance

$$\mathcal{E}\left[n_{\ell',n'}^k n_{\ell,n}^k\right] = \frac{\mathcal{N}_0}{2}\delta_{\ell'\ell}\delta_{n'n}.$$

In this expression $\mathcal{E}[.]$ denotes the expectation with respect to the Gaussian probability distribution. The duration L is chosen long enough to detect the spoofer. With perfectly tracking loops, the expectation of the correlation output is

$$\mathcal{E}\left[C_n^k\right] = \begin{cases} h_0^k \frac{1}{L}\sum_{l=0}^{L-1} b_\ell^k \hat{b}_\ell^k \simeq h_0^k & \text{for the GNSS satellite signal,} \\ h_{S,0}^k \frac{1}{L}\sum_{l=0}^{L-1} b_{S,\ell,n}^k \hat{b}_\ell^k = h_0^k \alpha_n^k & \text{for a spoofed signal.} \end{cases}$$

In the presence of a spoofer, the crosscorrelation of the early estimates of the navigation bit by the spoofer with its actual value α_n^k is very small (random walk). The covariance of C_n^k is easily determined to be diagonal with the value $\mathcal{N}_0/2L$. Thus, the receiver can choose a threshold T_n and perform the test

$$C_n^k < T_n h_0^k$$

on the n-th chip to detect the spoofer. The probability of missed detection then is

$$p_{\text{md}} = \prod_{n=1}^{n_0} Q\left(\sqrt{\frac{2L(h_0^k)^2}{\mathcal{N}_0}}\left(T_n - \alpha_n^k\right)\right)$$

and the probability of false alarm

$$p_{\text{fa}} = 1 - \prod_{n=1}^{n_0} Q\left(\sqrt{\frac{2L\left(h_0^k\right)^2}{\mathcal{N}_0}}\left(T_n - 1\right)\right)$$

$$= 1 - \prod_{n=1}^{n_0}\left(1 - Q\left(\sqrt{\frac{2L\left(h_0^k\right)^2}{\mathcal{N}_0}}\left(1 - T_n\right)\right)\right).$$

In obvious notations, this can be written as $p_{\text{md}} = \prod_n Q_n$ and $p_{\text{fa}} \sim \sum_n Q$. For small n_0 a value of $T_n = 1/2$ seems thus reasonable. The value of L is determined by the choice of p_{md}. In the scheme proposed by Wesson, Rothlisberger, and Humphreys, the length of the signed message is 446. Since the receiver has to wait for 466 bits before being able to verify the signature, it is reasonable to chose $L = 466$. The probability of correctly decoding the bits by the spoofer after having seen n_0 chips is given by

$$p_{\text{corr}} = 1 - Q\left(\sqrt{\frac{2n_0 g\left(h_0^k\right)^2}{\mathcal{N}_0}}\right),$$

with g being the ratio of the antenna gain of the spoofer to the antenna gain of the target receiver. The latter antenna gain is included in $(h_0^k)^2$. The spoofer could hide his estimation errors if $p_{\text{wrong}} = 1 - p_{\text{corr}} \simeq p_{\text{fa}}$. This means that the gain g must thus be of the same order of magnitude as L. Thus, message authentication not only makes it difficult to forge satellite navigation messages but also to synthesize forged signals. With this understanding, it is necessary that the combined signature on two carriers introduced in the previous section is split into two segments, and that each segment is transmitted on a different carrier. This reduces the authentication delay by a factor of two as compared to single carrier authentication if the same transmission rate is used on both channels in dual-frequency authentication as is used in single carrier authentication. The only disadvantage of this approach is that the receiver must be a dual-frequency receiver, and that the signals on both carriers must be available. The capability of authenticating signals and not only messages is an important argument for providing authentication in the data stream of the satellite and not only in the Internet. It also explains why the cryptosystem used in the Internet must be "different" than the one used over the air. The verification of the authenticity of the signal would not be possible if the signature was communicated to the spoofer through the Internet ahead of time. "Different cryptosystem" may thereby just mean "using another key."

More sophisticated schemes of authentication for signals have also been proposed. In these schemes the GNSS satellites transmit a spreading code which is disclosed in an authenticated manner at a latter stage. The estimation of these chips is more difficult for the spoofer than the estimation of the bits in the signature - they force the spoofer to use an even larger antenna than in the previous case. This scheme was first proposed by Scott [5] and later refined in [37]. A similar approach was

also considered by Pozzobon, Canzian, Danieletto, and Della Chiara [38]. As in the previous situation, the primary problem is the delay after which the authenticity can be established, since the complete code and its complete signature must have been received before a decision about authenticity can be made. Furthermore, it also requires a modification of the system. An interesting alternative, which does not require such a modification, is the use of sequences of samples of the signal including the P(Y)-code. Since the P(Y) code is not available publicly, it can only be predicted by legitimate users of that code, mainly US and allied military personnel. Lo, de Lorenzo, Enge, Akos, and Bradley [28] proposed the scheme. Psiaki, Hanlon, Bhatti, Shepard, and Hanson [39] analyzed its performance for a narrow-band front-end. In this scheme it is crucial that the sequence of samples is authenticated, since a spoofer could otherwise substitute the C/A component of the signal, and thus control the user's position and clock offset.

Reducing the delay caused by a cryptographic signature scheme to a minimum is an important goal but will often not be sufficient to fulfill the delay requirements imposed by applications. This is especially the case in a safety of life context such as the landing of aircraft. A promising approach in such situations is to use inertial measurements for propagating the GNSS measurements from the past instant at which they can be authenticated to the present. On aircraft, the propagation can be implemented using a navigation grade INS. In other situations, Micro-Electro-Mechanical-Systems (MEMS) are a possible alternative. They are improving continuously and achieve rather low drift rates already. Besides being a propagator for authenticated positions, they can also be used to cross-check the GNSS navigation solution and further restrict the options for the spoofer by forcing him to remain within the error models of the gyros and accelerometers.

Detection of Meaconing

Meaconing and generalized meaconing were introduced earlier as options for manipulating cryptographically secured signals. The verification of authentication from the previous two sections will thus not discover a meaconing attack. Other methods must be used. Meaconing with a signal injection mode Coh and NCo may be detected by tracking the position. The latter jumps if the spoofer is not located at the spoofer's intended location at the time at which the target receiver locks on the spoofer's signal. Additionally, meaconing and generalized meaconing can be detected through the clock jump $c\tau_S$, which is positive whenever the target receiver is not collocated with the spoofer at the time of lock. The clock jump is easily detected if the receiver is in tracking or reacquisition mode. The cold start is the more critical situation. Depending on the acceptable spoofing error and on the affordable cost, this may be addressed by using a stable clock and/or a continuously running inertial system.

Antenna Arrays at the Receiver

Typical spoofers transmit their signals using a single antenna. Thus the spoofed signals all arrive from one single direction. The authentic satellite signals, on the other side, arrive from different directions. This may be used to detect and even localize the spoofer. It requires a receiver capable of estimating directions of arrival, e.g., by evaluating the phases of the signals received by a set of antennas. With four antennas, a receiver generates 4K measurements that are used to estimate the position, the attitude, the clock offset, and the ionospheric delays. Cuntz, Denks, Konovaltsev, Hornbostel, Dreher, and Meurer [40] built such a receiver. The directions of arrival estimated by such a receiver are compared with the values derived from the navigation message. This approach was first proposed and demonstrated by Montgomery, Humphreys, and Ledvina [41]. Meurer, Konovaltsev, Cuntz, and Hättich further developed methods for the automated detection of spoofers as well as for their isolation, see [42] and [43]. In the presence of a sufficient number of satellites with directions of arrival sufficiently different from the spoofer, the spoofing signals can be suppressed. Array processing at the target receiver thus forces the spoofer to generate a three dimensional wave-field using several tightly synchronized transmitters. This is a very complex task, which nevertheless deserves a detailed analysis.

Vulnerability and Monitoring

The analysis described in the previous sections confirms that spoofing is a real threat. At the same time, it shows that this threat can be controlled to a significant extent by receiver design. If the GNSS system provides authentication, and if the receiver includes a stable clock or proper antenna processing, this threat can be essentially mitigated.

The design of receivers used for critical applications should include a detailed spoofing analysis. Ideally, the receiver incorporates a spoofing monitor, which was previously suggested in [29]. The basic architecture for such a monitor is shown in Figure 1. We assume that the receiver processes the signals on at least two carriers and estimates the ionospheric slant delays. The received signals are first analyzed in the left part of the drawing while the state variables are compared to models and checked for consistency in the right part. The

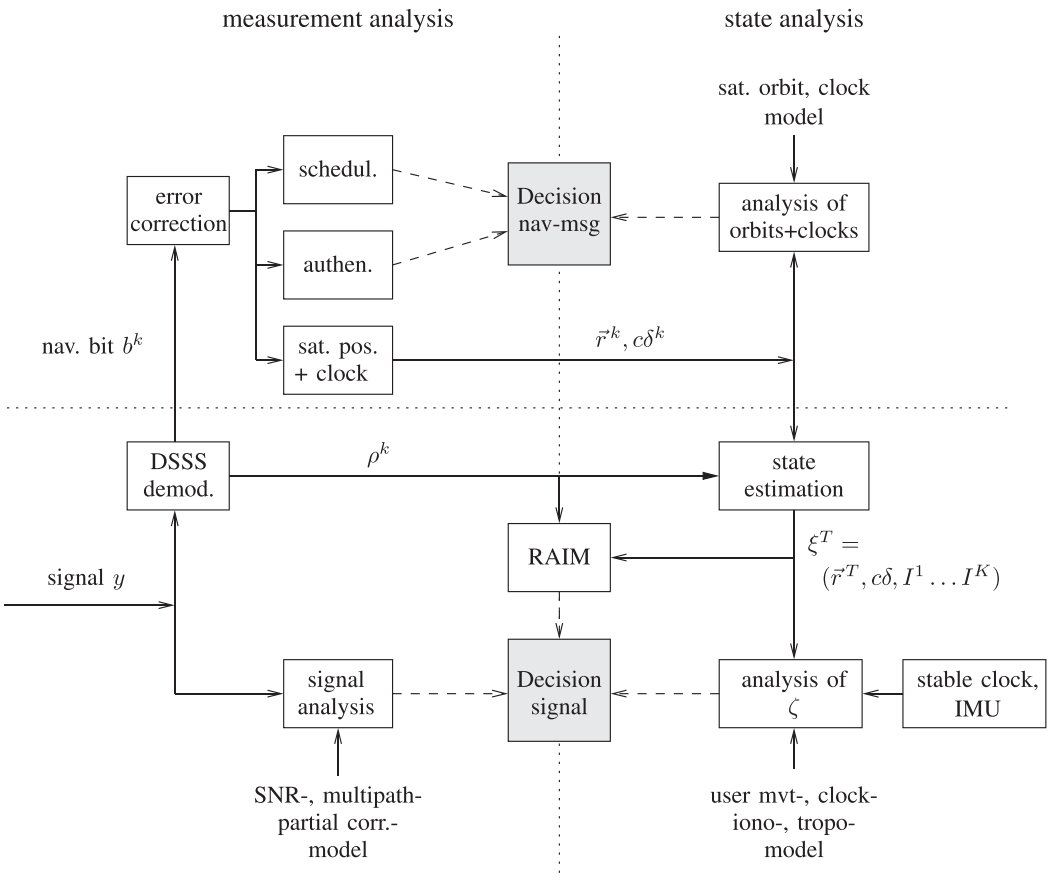

Fig. 1–The spoofing monitor shown in this figure consists of a number of estimation and evaluation units. The plain lines show signal flows and the dashed lines information flows. The state $\xi(t)$ estimated by the receiver is compared against models for the user movement $\vec{r}(t)$ and clock stability $\delta(t)$, as well as for the ionospheric slant delays $(I^1 ... I^k)(t)$. The sampled signal is analyzed with respect to its conformance to models describing the signal and the multipath. "RAIM" finally establishes the consistency of the measurements amongst themselves. Additional explanations are provided in the text.

"Direct Sequence Spread Spectrum (DSSS) demodulator" estimates the pseudoranges ρ^k, the carrier-phases φ^k, and the bits of the navigation message b^k. The monitor performs an analysis of the navigation message (upper part) and of the phasing of the signals (lower part). Signals are tested for SNR, multipath, and partial correlations (signal analysis). The navigation message is tested for unexpected scheduling (schedul.) and for its cryptographic signature (authen.). The orbits and clock-offsets are computed (sat. pos.+clocks) and tested against models (analysis of orbits+clocks). The navigation message and pseudoranges are used to determine the state $\xi = \left(\vec{r}, c\delta, I^1 \dots I^k\right)$, e.g., by least squares estimation (state estimation). The components of the state include the position $\vec{r}$, the clock-offset δ, as well as the ionospheric delays $I^1 \dots I^K$ or potentially a subset of them. The plausibility of these components is tested against models describing the components and their change (analysis of ξ). A clock and inertial measurement unit (IMU) provide references that cannot be spoofed. They drift, however, which needs to be taken into account in the tests. The residuals $\rho - H\hat{\xi}$ are furthermore used to verify that the measurements are consistent with the solution (RAIM). This might be the basis for eliminating selected measurements. To our knowledge the theory for selecting an optimal set of measurements in the presence of natural biases and spoofing has not yet been developed. The thresholds used in the tests are determined by the acceptable probability of not detecting the spoofer. The latter probability depends on the application considered. The resulting thresholds determine the probability of false alarms. A high probability of false alarm is undesirable since it reduces the availability of positioning. A proposal for testing the implementation of such monitors has been made by Pozzobon et al. [44].

In an alternative approach, not shown in the present figure, the clock and the inertial measurement unit provide their measurements to the state estimation unit. The state estimation is then performed using a Kalman filter or a Bayesian estimator. The associated state needs to include the orientation of the platform, as well as biases relating to clock-, gyro-, and accelerometer-imperfections. Both Kalman and Bayesian estimates assume a model for the time evolution of the state. In this

approach, both clock and the inertial measurements are part of the solution. They are thus no more available for an independent comparison. The former test against the clock and IMU becomes part of the RAIM processing. The model describing the dynamics of the state is also used in the estimation of the state. Corresponding inconsistencies must also be detected through RAIM processing. The associated theory is again to be developed.

In the latter approach and in the approach of Figure 1, the counter-measures to spoofing may reduce the availability of position and time and/or may degrade their accuracy in the case that measurements are eliminated or de-weighted in the processing. On the other hand, the counter-measures fulfill their purpose by strongly limiting the error in position and time that a spoofer may intentionally induce.

CONCLUSION

The analysis presented in this paper follows the usual approach of a threat analysis. It aims at identifying all relevant threats and at protecting the user against them. This has led to the identification of a number of weak points that could be exploited by a spoofer. Many of them were individually known before, but not addressed in a common context.

The main conclusions are that:

- Without authentication, a spoofer who captures a receiver during initial acquisition can mislead the estimate of the receiver's position and clock-offset to nearly every value.
- After acquisition, the stability of the receiver's clock combined with models for that clock, for the receiver movement, and for changes in the ionospheric slant delays greatly constrain the position errors that a spoofer can induce without being discovered. This requires that the receiver analyzes the signals and the state variables as well as their evolution using models.
- Spoofers who cannot shield the satellite signals find it difficult to inject their signals in a manner that does not leave traces of the authentic satellite signals. Receivers should exploit this to detect the presence of spoofing signals.
- Message authentication greatly improves the situation for the receiver. The spoofer is forced to perform complex manipulations of authentic satellite signals, such as the one associated with generalized meaconing to deceive the receiver. The delay associated with cryptographic authentication is large, however.
- An inertial system can be used to mitigate the effect of authentication delay. For this purpose, the authenticated position at an earlier time is propagated to present time. The same applies to time, which may be propagated using a stable clock. Such external systems can additionally be used to verify the plausibility of changes in position and time, and to thus further constrain the maneuvering range of a spoofer to the stability of the inertial system and of the clock used.
- Generalized meaconing is complex but possible. Since the spoofer can only delay signals, he can at least in principle be detected using a stable clock. A continuously running inertial system may also detect him. This, however, amounts to having another independent navigation system of sufficient accuracy.
- In the absence of authentication, the receiver may incorporate an antenna subsystem, which estimates the direction of arrival of the satellite signals. This forces the spoofer to either generate a wave field or to have access to the antenna interfaces for injecting the signals with the right phases. The former approach is rather complex; the latter one is unlikely to be relevant. Thus, the estimation of the direction of arrival may provide the necessary protection in a number of situations.

In order to protect a broad user community, we recommend including message authentication in updates of GNSS. In the case of Galileo, the joint authentication of E1 and E5a is very attractive. It causes the same overall overhead as the authentication of a single carrier but halves the authentication delay. Authentication allows us to detect modified messages and often also to detect manipulated signals. We strongly recommend that all receivers used in a sensitive context undergo a detailed threat analysis which addresses spoofing. In particular, these receivers should incorporate a monitor which constantly verifies the conformance of measurements and estimates with their expected values - and issues an alert in the case of non-conformance.

ACKNOWLEDGEMENTS

It is my pleasure to acknowledge the helpful comments of the anonymous reviewers. Their valuable suggestions sharpened selected aspects of the paper and improved its readability.

REFERENCES

1. "Vulnerability Assessment for the Transportation Infrastructure Relying on the Global Positioning System," John A. Volpe National Transportation System Center, 2001.
2. "Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV," 2012, Available: http:// www.ae.utexas.edu/news/archive/2012/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav, [accessed 6-10-2013].

3. "Spoofing a Superyacht at Sea, 2013," Available: http://www.utexas.edu/know/2013/07/30/spoofing-a-superyacht-at-sea/, [accessed 22-03-2014].
4. Steindl, E., Dunkel, W., Hornbostel, A., Hättich, C., and Remi, P., "The Impact of Inteference Caused by GPS Repeaters on GNSS Receivers and Services," *Proceedings of the European Navigation Conference*, Vienna, Austria, 2013.
5. Scott, L., "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, September 2003, pp. 1543–1552.
6. Hein, G. W., Kneissl, F., Avila-Rodriguez, J.-A., and Wallner, S., "Authenticating GNSS, Proofs against Spoofs, Part 1," *Inside GNSS*, July/August 2007, pp. 58–63.
7. Hein, G. W., Kneissl, F., Avila-Rodriguez, J.-A., and Wallner, S., "Authenticating GNSS Proofs against Spoofs, Part 2," *Inside GNSS*, September/October 2007, pp. 71–78.
8. Kröner, U., and Dimc, F., "Hardening of Civilian GNSS Trackers," *Proceedings of the 3rd GNSS Vulnerabilities and Solutions Conference*, Baška, Krk Island, Croatia, 2010, Available: http://www.researchgate.net/publication/236631022_Hardening_of_civilian_GNSS_trackers, [accessed 6- 10-2013].
9. Wesson, K., Shepard, D., and Humphreys, T., "Straight Talk on Anti-Spoofing," *GPS World*, Vol. 23, No. 1, 2012, pp. 32–39.
10. Pozzobon, O., Wullems, C., and Kubik, K., "Requirements for Enhancing Trust, Security and Integrity of GNSS Location Services," *Proceedings of the 60th Annual Meeting of The Institute of Navigation*, Dayton, OH, June 2004, pp. 65–75.
11. Misra, P., and Enge, P., *Global Positioning System: Signals, Measurements and Performance*, Second ed., Massachusetts: Ganga-Jamuna Press, 2006.
12. Van Diggelen, F. S. T., *A-GPS: Assisted GPS, GNSS, and SBAS,* Artech House, Boston and London, 2009.
13. Spilker, J. J., "Fundamentals of Signal Tracking Theory," *Progress in Astronautics and Aeronautics*, Vol. 163, 1996, pp. 245–328.
14. Zhodzishsky, M., Yudanov, S., Veitsel, V., and Ashjaee, J., "Co-Op Tracking for Carrier Phase," *Proceedings of the 11th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1998)*, Nashville, TN, September 1998, pp. 653–664.
15. Giger, K., and Günther, C., "Position-Domain Joint Satellite Tracking," *Proceedings of ESA NAVITEC*, Noordwijk, Netherlands, 2010.
16. Klobuchar, J. A., "Ionospheric Time-Delay Algorithm for Single-Frequency GPS Users," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 3, 1987, pp. 325–331.
17. Radicella, S. M., "The NeQuick Model Genesis, Uses and Evolution," *Annals of Geophysics*, Vol. 52, No. 3/4, 2009, pp. 417–422.
18. Lo, S. C., and Enge, P. K., "Authenticating Aviation Augmentation System Broadcasts," *Proceedings of IEEE/ION PLANS 2010*, Indian Wells, CA, May 2010, pp. 708–717.
19. Pozzobon, O., Wullems, C., and Detratti, M., "Security Considerations in the Design of Tamper Resistant GNSS Receivers," *Proceedings of ESA NAVITEC*, Noordwijk, Netherlands, 2010.
20. Lehner, A., Steingaß, A., and Schubert, F., "A Location and Movement Dependent GNSS Multipath Error Model for Pedestrian Applications," *Atti dell'Istituto italiano di Navigazione*, Vol. 189, 2009, pp. 108–119.
21. Wesson, K. D., Shepard, D. P., Bhatti, J. A., Humphreys, T. E., and An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing, *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland, OR, September 2011, pp. 2646–2656.
22. GPS-ICD, "Navstar GPS Space Segment / Navigation User Interfaces," Available: http://www.gps.gov/technical/icwg/ #is-gps-200, [accessed 4-10-2013].
23. Lentmaier, M., Krach, B., and Robertson, P., "Bayesian Time Delay Estimation of GNSS Signals in Dynamic Multipath Environments," *International Journal of Navigation and Observation,* Article ID 372651, 2008.
24. Lee, Y. C., "Analysis of Range and Position Comparison Methods as a Means to Provide GPS Integrity in the User Receiver," *Proceedings of the 42nd Annual Meeting of the Institute of Navigation*, Seattle, WA, 1986, pp. 1–4.
25. Pervan, B. S., Pullen, S. P., and Christie, J. R., "A Multiple Hypothesis Approach to Satellite Navigation Integrity," *NAVIGATION*, Vol. 45, No. 1, Spring 1998, pp. 61–71.
26. Perrig, A., Canetti, R., Tygar, J. D., and Song, D., "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *Proceedings of IEEE Symposium on Security and Privacy*, Berkeley, CA, 2000, pp. 56–73.
27. Wullems, C., Pozzobon, O., and Kubik, K., "Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems," *Proceedings of European Navigation Conference GNSS*, Munich, Germany, 2005.
28. Lo, S., De Lorenzo, D., Enge, P., Akos, D., and Bradley, P., "Signal Authentication: A Secure Civil GNSS for Today," *Inside GNSS*, Vol. 4, No. 5, 2009, pp. 30–39.
29. Wesson, K., Rothlisberger, M., and Humphreys, T., "Practical Cryptographic Civil GPS Signal Authentication," *NAVIGATION*, Vol. 59, No. 3, Fall 2012, pp. 177–193.
30. Goldwasser, S., and Bellare, M., "Lecture Notes on Cryptography," *Summer Course Cryptography and Computer Security,* MIT, Cambridge, MA, 1996.
31. Diffie, W., and Hellman, M., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. 22, No. 6, 1976, pp. 644–654.
32. Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120–126.
33. Hardy, G. G. H., and Wright, E. M., *An Introduction to the Theory of Numbers,* Oxford University Press, Oxford, UK, 1979 (First Ed. 1938).
34. NSA, "The Case of Elliptic Curve Cryptography," Available: http://www.nsa.gov/business/programs/elliptic_curve.shtml, [accessed 28-9-2013].
35. Miller, V. S., "Use of Elliptic Curves in Cryptography," *Proceedings of CRYPTO'85*, Santa Barbara, CA, Springer, 1985, pp. 417–426.
36. Koblitz, N., "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, 1987, pp. 203–209.
37. Scott, L., "Proving Location Using GPS Location Signatures: Why it is Needed and A Way to Do It," *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation*

(ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2880–2892.
38. Pozzobon, O., Canzian, L., Danieletto, M., and Della Chiara, A., "Anti-Spoofing and Open GNSS Signal Authentication with Signal Authentication Sequences," *Proceedings of ESA NAVITEC*, Noordwijk, Netherlands, 2010.
39. Psiaki, M., O Hanlon, B., Bhatti, J., Shepard, D., and Humphreys, T., "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 49, No. 4, 2012, pp. 2250–2267.
40. Cuntz, M., Denks, H., Konovaltsev, A., Hornbostel, A., Dreher, A., and Meurer, M., "GALANT - Architecture Design and First Results of A Novel Galileo Navigation Receiver Demonstrator With Array Antennas," *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, September 2008, pp. 1470–1477.
41. Montgomery, P., Humphreys, T. E., and Ledvina, B. M., "A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection," *Inside GNSS*, Vol. 4, No. 2, 2009, 40–46.
42. Meurer, M., Konovaltsev, A., Cuntz, M., and Hättich, C., "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 3007–3016.
43. Konovaltsev, A., Cuntz, M., Haettich, C., and Meurer, M., "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," *Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, September 2013, pp. 2937–2948.
44. Pozzobon, O., Sarto, C., Della Chiara, A., Pozzobon, A., Gamba, G., Crisci, M., and Ioannides, R. T., "Status of Signal Authentication Activities within the GNSS Authentication and User Protection System Simulator (GAUPSS) Project," *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 2894–2900.