Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Alexander RÜGAMER, Fraunhofer IIS, Germany
Dirk KOWALEWSKI, NavXperience GmbH, Germany

Keywords: Jamming, Spoofing, Interference Mitigation, Galileo PRS

SUMMARY

GNSS technology is used for many applications: The surveying industry uses GNSS for monitoring the continental drift, stakeout fixed-points, measuring maps of areas and many other location based services. The construction industry uses GNSS for machine control and logistics, agriculture for precise farming, power steering assists and other tasks like bringing out manure, harvesting and plowing. Over the last 10 years GNSS has also entered many daily life applications like car navigation and location based services (Google Maps, Facebook). But GNSS is also used as a sensor for many safety-critical applications: the example of guided lading approach of airplanes is well known, but it is less known that GNSS – and here specifically the Open Service of the US NAVSTAR GPS – is used as a crucial sensor for timing and synchronization of reference stations for telecommunication, electrical power supplies, exchange markets and banks.

For many years, the availability and faultless function of GNSS has been taken for granted. Jamming (intentional interference targeting the unavailability of the system) as well as spoofing (faking of a false position/time towards a target GNSS receiver) was no concern for nearly all users except the military.

But recent events started a gradual paradigm shift: the unintentional jamming of Newark Airport, NY, USA by an UPS driver with a US $ 100 device available on eBay; the capturing of a US drone using a GPS spoofer by Iran; the demonstration of students from the University of Austin, Texas, US, to hijack a US$ 80 million dollar Yacht with a self-made spoofer as well as their laboratory demonstration to use this spoofer to tamper the phase measurement units used for energy network synchronization and control.

In this paper we review these events and show how our currently used GNSS technology was attacked and affected. Then we discuss different measures to detect and even mitigate these threats on the algorithmic, receiver, antenna and system level. Finally, we conclude with providing solutions and recommendations for hardening and protecting GNSS receivers by e.g. using array antennas and/or services like the Galileo Public Regulated Service (PRS) with civilian anti-spoofing guaranteed by the strong encryption used there.

Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Alexander RÜGAMER, Fraunhofer IIS, Germany
Dirk KOWALEWSKI, NavXperience GmbH, Germany

1. INTRODUCTION

Originally intended to be military only global navigation satellite systems (GNSS), the American NAVSTAR GPS as well as its Russian counterpart GLONASS started a revolution in localization and navigation worldwide. Although it is often forgotten that the civilian use of these systems is merely tolerated – without any legal basis or control if these GNSSs become unavailable – according to [1], the GNSS core market worldwide is expected to be around $ 70 billion, and over $ 200 billion if also GNSS enabled revenue is included, in 2015. An annual growth rate of 9% is predicted. Consequently, the European Galileo will be the first GNSS under civilian control where – next to the Open Service (OS) and the Public Regulated Service (PRS) for government authorized users – for the first time especially a Commercial Service (CS) is included for certain professional applications. The worldwide GNSSs are completed with the Chinese BeiDou Navigation Satellite System (BDS), comprised of regional coverage and worldwide receivable satellite constellations.

GNSS technology is used for many applications: The surveying industry uses GNSS for monitoring the continental drift, stakeout fixed-points, measuring maps of areas and many other location based services. The construction industry uses GNSS for machine control and logistics, agriculture for precise farming, power steering assists and other tasks like bringing out manure, harvesting and plowing. Over the last 10 years, GNSS has also entered many daily life applications like car navigation and location based services (e.g. Google Maps, Facebook). But GNSS is also used as a sensor for many safety-critical applications: the example of guided landing approach of airplanes is well known, but it is less known that GNSS – and here specifically the publicly available Coarse/Acquisition (C/A) service of GPS – is used as a crucial sensor for timing and synchronization of reference stations for telecommunications, electrical power supplies and the financial sector.

For many years, the availability and faultless function of GNSS has been taken for granted. Jamming (intentional interference targeting the unavailability of the system) as well as spoofing (faking of a false position/time towards a target GNSS receiver) was no concern for nearly all users except the military.

In this paper, we introduce the threat of GNSS jamming with practical examples of commercially available GNSS jammers and continue with the threat of spoofing. We review some more or less known GNSS jamming and spoofing events and show how our currently used GNSS technology can be attacked and affected. Then we discuss different measures to detect and even mitigate these threats on the algorithmic, receiver, antenna and system level. Finally, we conclude with providing solutions and recommendations for hardening and protecting GNSS receivers.

2. GNSS INTERFERENCE

Due to the inherently low power of GNSS signals (approx. -130 dBm received signal power on earth), the GNSS bands are dominated by white Gaussian noise. The noise is about a hundred to a few thousand times stronger than the GNSS signals themselves. As a consequence, GNSS signals are extremely susceptible to all types of interference. These interferences can be unintentional, e.g. the harmonics of certain oscillators that translate into single or multi-tones in the GNSS spectrum, co-operation in bands with radio amateurs, co-operation with distance measurements equipment (DME) near airports, etc. However, there are also more and more intentional interferers readily available on the Component-off-the-self (COTS) market, mostly sold over the internet, even if their use is illegal in most countries. Whereas jammers are used for denial-of-service attacks, spoofers pose an even bigger threat, since they can intentionally cause a receiver to estimate a fake position and/or time without recognizing it.

2.1 Jamming

Jamming is the act of intentionally directing electromagnetic energy towards a communication (and navigation) system to disrupt or prevent signal transmission [2]. Thus GNSS jammers broadcast their interference signal in the frequency band used for satellite navigation. A jammer attack can be categorized as a denial of service – the GNSS is still available but its broadcast signals are totally exceeded by the jammer power. One should distinguish military and civil jammers.

2.1.1 Military Jammers

In crisis situations, the military or the government is authorized to intentionally – typically locally – jam civilian signals. The objective is to restrict the positioning service to authorized and therefore military users only in order to weaken the enemy's tactical possibilities.

Although the idea of "friendly" jamming to prevent civilian GNSS usage is straightforward, there are rumors that it can be quite challenging in practice. It is said that e.g. in the Iraq war, the US military carried out intentional GPS C/A jamming, but realized soon that their own troops also wildly used civilian GPS receivers for their own purposes because due to their classified nature, military receivers are much bulkier, slower, less accurate and less user-friendly than their commercial civilian counterparts.

A commercial military jammer is e.g. available from *NovAtel* with its *NEAT* product "... a small hand-held GPS jammer developed to train allied forces to recognize and adapt to GPS jamming. With provision for remote operation, NEAT can be pre-programmed with customizable waveforms for simple field use." [3]. Of course, even friendly jammers may only be used in a protected area. Examples of these specially protected test ranges are, e.g. the missile test range Vidsel, Sweden, [4] or the White Sands Missile Range *JAMFEST* in New Mexico, USA [5].

2.1.2 Civilian Jammers

Over the last few years commercial jammers – so-called Personal or Privacy Protection Devices (PPD)s – have become increasingly popular, but have also gained public attention due to several incidents of abuse. These PPD devices can be bought e.g. over the internet starting from 30 € for a plain car cigarette lighter powered jammer to very sophisticated GPS-all-bands (including GSM, WiFi) jammers with external antenna connectors and configurable operation modes for over several hundred Euros.

There are many different motivations for PPD usage, most of which are bordering on illegality, like turning off of the Anti-Theft-System in a car that would communicate the GPS position of the vehicle to the central unit, or bypassing read toll systems and pay-as-you-drive insurance, or withdrawing from a Fleet Management System; or switching off the Automatic Identification System of vessels; or to protect the privacy of parcel delivery agents from their employers. Even though some of the motivations may be reasonable, the impact of the PPDs usage is often not clear for the users. They do not realize that such a tiny PPD can disrupt or distort the GNSS integrity over a range of several kilometers.

Nearly all commercially available jammers transmit chirp signals, a continuous wave (CW) tone with constantly changing frequency over time. Their bandwidth often also cover military GPS signals. Unfortunately, a chirp jammer is also the type of jammer that is most difficult to mitigate: For pulse jammers, the interference signal can be blanked. CW jammers can be efficiently mitigated by applying a notch-filter. But there is no real practical signal processing approach against chirps. And to make mitigation even harder, due to the low quality design of the commercial chirp jammers, their chirp characteristics change over time e.g. due to heating of the circuit and aging. Having an unpredictable interference source can be regarded as the worst case.

For demonstration purposes, Fraunhofer IIS bought three different kinds of GNSS jammers from an internet shop located in the UK, see Figure 1. This also shows the simplicity of purchasing COTS jammers via the internet. The blue jammer at the left side allows the user to choose which signal band to jam: L1, L2, L5, GSM900, or any combination of these. For each band, a chirp interference signal is generated as described in the following. The overall measured output power (directly measured at the jammer's output ports - without the antennas) is +33 dBm. The jammer has a rechargeable battery back and comes with a convenient leather holster. The price is approx. 170 €. According to its leaflet, this jammer can be used to "... protect the privacy of its user in a radius of at least 15 m... ", even though it might be several kilometers due to its relatively high output power.

The other two jammers are typical cheap cigarette lighter jammers for the GPS L1 band. Again, a chirp-like interference output signal is used with an output power of approx. +12 dBm. They cost between 40 to 80 € and are advertised to "... Prevent car of government, intelligence agency, famous person, principal etc. from being tracked. This device doesn't affect navigation device which installed on other cars.", and "If you are sales personnel and delivery drivers, this GPS tracking jammer is a very popular item for you to take lunch or make a personal stop outside of your territory or route 'off the radar'."

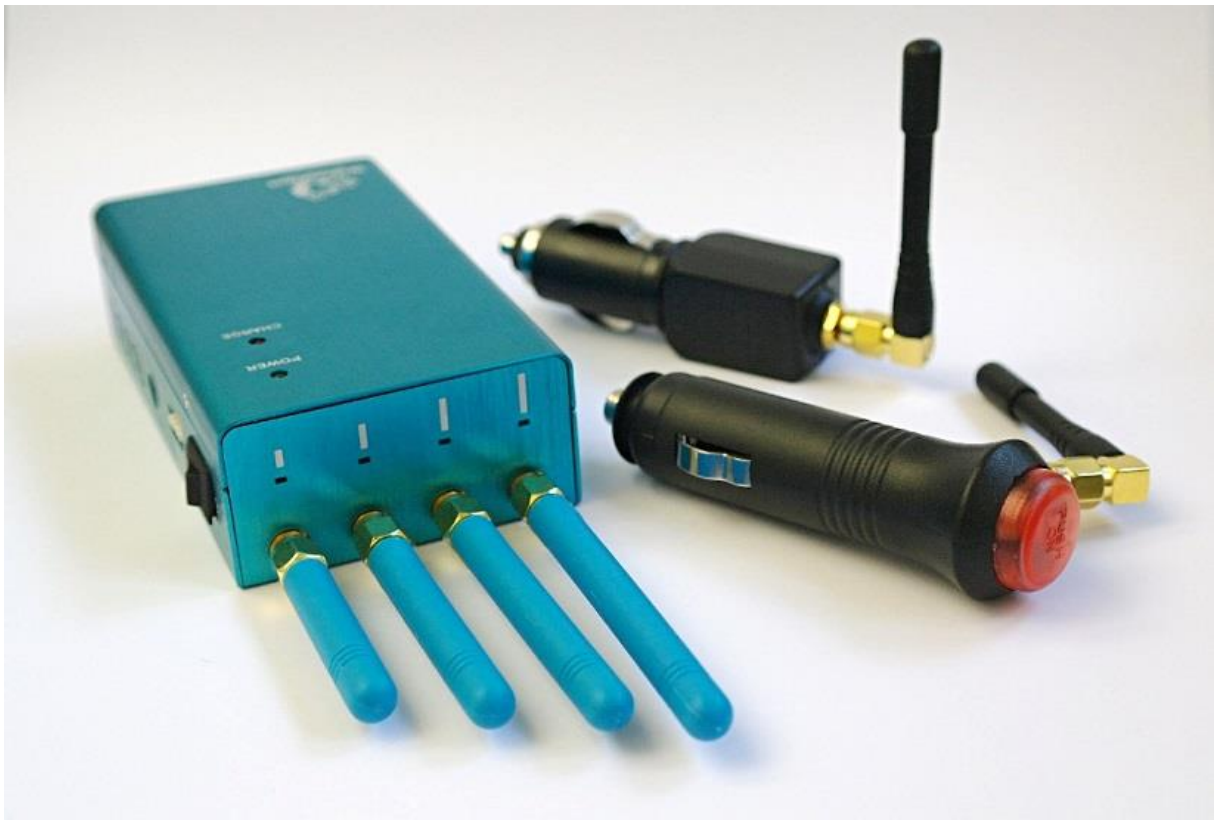

Figure 1: Commercial jammers acquired by Fraunhofer IIS

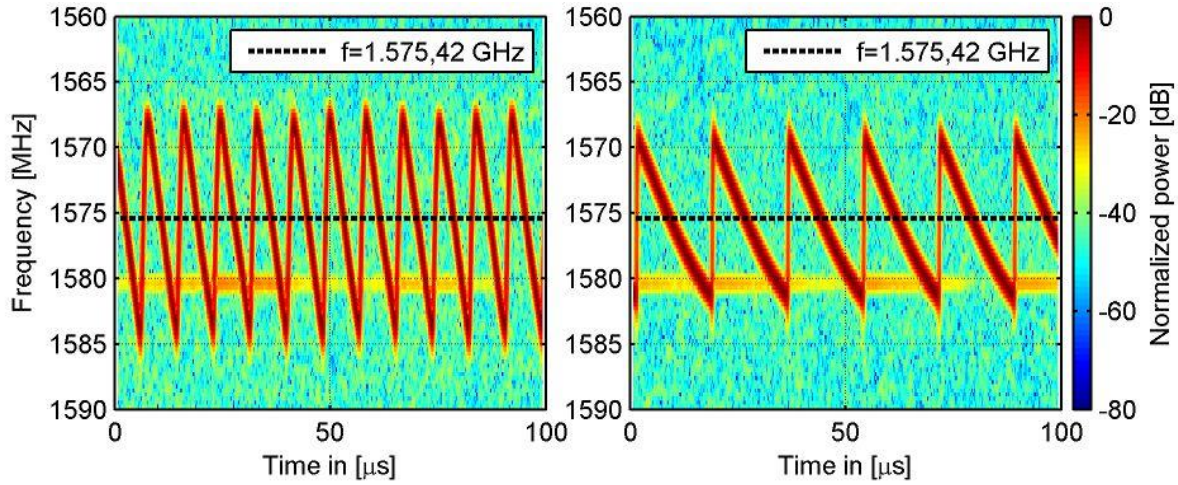

Figure 2: Measured spectrogram of GPS L1 Jammer signals for two different jammer models

Figure 2 shows spectrograms of these two jammers. Both are jamming the GPS L1 band at 1575.42 MHz with a chain-saw chirp. The black dotted line shows the center frequency of the GPS L1 band. The continuous power at 1580 MHz is caused by a DC-offset of the measurement device (intermediate frequency at 4.795 MHz). An extensive investigation on the properties of different commercial jammers was conducted in [6] and [7].

2.2 Spoofing

Spoofing is a deliberate transmission of fake GNSS signals with the intention of fooling a GNSS receiver into providing false Position, Velocity and Time (PVT) information. The goal of spoofing is to secretly force a GNSS receiver to track the spoofed signal (or deceptive signals) with the objective to provide or at least to induce a wrong position solution.

Spoofing of classified signals using cryptographic signal protection like the military GPS P(Y) or the Galileo PRS is practically impossible. However, even classified signals are not safe from meaconing attacks: Meaconing means recording and rebroadcasting of authentic GNSS signals. If the receiver tracks the signals generated by meaconing hardware without noticing it, the receiver will not get its correct position, but instead the position of the meaconing hardware or a slightly changed version of it.

2.2.1 Spoofing Attacks

Humphreys et al. [8] classify spoofing attacks into three categories: Simplistic attack, intermediate attack and sophisticated attack.

In the *simplistic attack*, a commercial GNSS simulator is used to broadcast GNSS signals for the spoofed position, to the GNSS receiver under attack. It is a quite simple attack and no knowledge of the victims original PVT is used. The attack can be detected relatively easily since pseudorange, C/N0 and Doppler jumps will occur, which can be monitored in the receiver.

An *intermediate attack* is carried out with the spoofer first gaining information on the victim's PVT and using this information to generate a similar spoofed composite GNSS signal broadcast via the spoofer's antenna towards the victim. Gradually, the spoofed signals' power is increased till the attacked receiver locks onto the spoofed signal without noticing. Then the spoofer can gradually change the victim's PVT to an arbitrary value.
Since the attack starts with the victim's actual PVT, such an attack is hard to detect with standard GNSS receiver processing. One way to detect intermediate attacks is e.g. by

monitoring the Doppler/pseudorange variations when moving the victim's receiver's antenna: Since all spoofed signals are transmitted from a single antenna, the Doppler/pseudorange variations are correlated [9].
In the *sophisticated attack*, a similar attack as described before is carried out, but now using several coordinated spoofers to also emulate the spatial signal domain, making both the attack itself very difficult to carry out as well as very hard to detect for a conventional single antenna receiver.

2.2.2 Types and Characteristics of Commercial Spoofers

The most common type of commercial spoofer does not attack the GNSS signal itself but just inserts the spoofed information directly at the receiver's output. Obviously, physical or software access to the victim's receiver is required for that. Such commercial spoofers are e.g. used to fog fishing in waters where it is forbidden or to dump wasted oil in the sea where the vessel's Automatic Identification System (AIS) position would otherwise be related to the incident. Another field of application is e.g. toll collect fraud. "Simple GPS fraud kits" that can feed spoofed PVT information into the receiver's NMEA RS-232 output port are available for approx. 2,000 €.

RF-signal spoofers are much less common. Commercial GNSS RF-signal generators start at about 100,000 €. They cannot directly be used to perform an intermediate spoofing attack but can certainly disturb a standard GNSS receiver significantly. Shepard et al. [10] describe the capabilities of the real-time GPS RF-signal spoofer developed by the University of Texas at Austin's (UT) Radionavigation Lab. They successfully demonstrated spoofing attacks on civilian unmanned aerial vehicles (UAV), GPS time-reference receivers used in "smart grid" measurement devices, as well as spoofing of Yachts, as described in the following section.

The first ready-to-buy commercial GNSS spoofer is probably Spirent's SimSAFE software together with a Spirent GNSS RF-signal generator [11]. SimSAFE supports two different modes: in the pure "fully simulated" mode, a real-scenario as well as the spoofed one are simulated within one common Spirent signal simulator scenario. The second "live" mode is much more interesting since it could be used in a real spoofing attack. A commercial GNSS receiver tracks the current signals from the sky and uses this information to generate an appropriate spoofing signal out of the GNSS RF simulator. SimSAFE supports spoofing attacks on GPS L1 and Galileo E1. In principle, multi-frequency-attacks are also possible but not yet implemented.

3. PRACTICAL USE OF JAMMERS AND SPOOFERS

Various jamming and spoofing events have already occurred and made their way into mainstream press reports:

In the so called “Iran - U.S. RQ - 170 incident” [12], a Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle (UAV) was captured by the Iranian military using a GPS spoofer in December of 2011. Having first been denied, this incident was confirmed a few days later by US military sources. The attack was successful because no military GPS was used.

Another famous jamming incident happened at the airport of Newark, New York, US. A UPS driver was using a PPD on the highway right next to the airport leading to regular alarms in the airport's ground based augmentation system (GBAS), resulting in the unavailability of GPS assisted landing approaches [13]. Even though the UPS driver (who was unaware of jamming also the airport's GBAS) was arrested, it is reported that there are still several similar incidents at Newark Airport a day.

According to [14], South Korea is considering to turn away from GNSS and back to eLoran for maritime navigation due to heavy GPS jamming from North Korea. It is reported that within 16 days of jamming from North Korean forces, over 1.000 airplanes and over 250 ships experienced GPS disruption.

GNSS jamming attacks are increasing in frequency also in Europe: A jammer monitoring campaign at two highway gantries around Munich, Germany reported approx. 6 jamming incidents a week [15], whereas one monitored carriageway outside London, UK is reported with 10 jamming incidents a day [16].

In 2013 and 2014, US researchers from the University of Austin, Texas, used their self-built spoofer to successfully demonstrate an intermediate spoofing attack on a drone [17] and on an $ 80 million Yacht. The Yacht holds its course according to its GPS controlled autopilot. Using their spoofer, the researchers caused the Yacht to go zigzag, even though the autopilot still reported the original straight course [18]. In theory, this kind of spoofing attack could also have been used to hijack cargo containers, or even spoof the global financial system where financial transactions are GPS time tagged, as reported in [19], with potentially disastrous consequences for the global markets.

Many critical resources rely on absolute and accurate GNSS time. The availability of a worldwide nanosecond-accurate clock distribution thanks to GNSS is used for many synchronization purposes: For example, phasor measurement units (PMU) in distributed electric power grids are used to monitor voltage, currents and their respective phase angle to

provide feedback for the grid's power management. A spoofing attack on these GPS time tagged measurement data might easily lead to a black-out. Such an attack was already successfully carried out in a protected environment [20]. Also critical timing networks like LTE communication or IT infrastructure relay on an accurate GNSS timing source. Obviously, while relatively simple to carry out, a successful attack on these services would have significant effects.

4. INTERFERENCE DETECTION AND MITIGATION

Interference detection and mitigation can be carried out in the time, frequency and spatial domains. The detection and mitigation techniques can be implemented in various parts of a GNSS receiver like the antenna, the front-end, the baseband processing stage pre- or post-correlation, as well as in the positioning domain. Cryptographically protected GNSS signals can be a very effective spoofing defense.

4.1 Jamming Detection and Mitigation

4.1.1 Antenna Techniques

Professional GNSS antennas reject low elevation signals to mitigate multipath but have no explicit protection against jammers. So do array-antennas, which consist of several, individual GNSS antennas from typically two to seven, ordered in a distance of approx. half the signals' reception wavelength. The individual antennas are combined in a way to form a combined radiation pattern towards a desired direction to suppress all others. That is why they are often called CRPA: controlled reception pattern antenna. Such array antennas can detect and mitigate jammers in the spatial domain and have been used for decades together with certain military receivers. For a few years, their application has also been considered for certain non-military safety critical applications, like GBAS or reference receiver stations.

Moreover, array antennas can be used to improve the reception performance: since they can concentrate the reception field of the antenna towards the satellite, they increase the signal-to-noise ratio and therefore the C/N0 while at the same time attenuating unwanted signals (interference, jamming, multipath) from all other directions. Taking into account their known structure and behavior, they can also be used to estimate both Direction of Arrival (DoA) and/or Direction of Interference (DoI).

Typical applications of array processing algorithms are:

- Beamforming, i.e. increasing the signal strength in the direction of interest while simultaneously attenuating the unwanted reception direction
- Nullsteering, i.e. suppressing undesired signals in their direction of appearance
- Determining the signal of interest's DoA by exploiting information available from spatial separation
- Determining the source of interference and spoofing (DoI)

The array processing algorithms can be implemented pre- or post-correlation, depending on the application and the receiver design [21]:

In case of a pre-correlation implementation, the GNSS signal is not yet despread and interference and noise are dominant. This fact can be used to directly estimate the DoI. For beamforming, it is only possible to steer a single beam towards one satellite, making pre-correlation array processing techniques unattractive for conventional beamforming receiver applications. Therefore pre-correlation processing is mostly used for nullsteering and DoI, for which the GNSS receiver implementation does not have to be modified.

In case of a post-correlation implementation, the GNSS singles are despread and therefore over the noise floor. DoA algorithms can estimate the azimuth and elevation of the GNSS satellites. DoI is challenging since the interference signals after the correlator are spread and cannot be detected as easily as before the correlation. Post-correlation implementations are mainly used for beamforming, where individual beams can be steered towards each satellite to be tracked – with the downside that the required number of receiver channels is multiplied by the number of array-antennas used. Moreover, special beamforming receiver designs are required for this kind of implementation.

Finally, it should be noted that when using general adaptive beamforming or nullsteering algorithms, the phase center of the array antenna will typically vary with the interference/satellite constellation. Special algorithms have to be selected and constrained if the phase center stability is important for the application.

4.1.2 Front-end Techniques

The GNSS receiver front-end connects to the analog RF output of the antenna, and filters, amplifies and downconverts the analog signals to an intermediate frequency or baseband domain, where the signal is digitized by an analog to digital converter (ADC).

The received, undisturbed GNSS signals are buried under the thermal noise floor with only a few dB of signal power dynamics. Therefore, the expected gain is approximately known. Monitoring the front-end's automatic gain control (AGC), variations may be used for interference detection if a gain much bigger than the expected one is suddenly detected.

When no interference is present, the raw data ADC samples are normally distributed. Consequently, with a raw samples test for normal distribution, interference can be detected. Moreover, these raw samples can also be used for time-frequency detection methods like short time Fourier transforming. Since interferences are typically sparse regarding the received undisturbed noise-like GNSS signal, it might also be possible to apply detection techniques based on Compressed Sensing as proposed and described in [22].

4.1.3 Pre- and Post-Correlation Receiver Techniques

Pre-correlation techniques are applied before the signal reaches the receiver's correlators and tracking loops. Therefore, they remove impairments common to all GNSS signals. Examples of pre-correlation techniques are: filtering, pulse blanking and nullsteering (in case of array antennas).

A very efficient way to mitigate the disturbance effect powerful pulses have on the GNSS tracking correlation process is to use a pulse blanker. A pulse blanker detects and nulls signals exceeding a certain threshold and being shorter than a certain time period. Since most pulses are normally much shorter than the minimum integration time used in GNSS processing, the implementation loss of such a pulse blanking mitigation approach is negligible. Without blanking, the pulse power would considerably increase the noise in the correlation process and therefore degrade the overall reception performance.

CW signals can either be mitigated in the time domain by using e.g. an adaptive notch-filter, or in the frequency domain by means of a frequency domain adaptive filter (FDAF) implementation. In FDAF, the raw data is transferred to the frequency domain using a fast Fourier transformation (FFT). Frequency bins over a certain threshold are categorized as interferences and nulled in the spectrum before the signal is transformed back into the time domain by an inverse FFT operation. The FDAF approach is especially powerful if non-stationary multi-tone interferers are present, but it is computationally complex and suffers from FFT leakage effects [21].

Post-correlation techniques are applied at the correlator outputs. They allow detection and mitigation techniques for each individual tracked signal. Since jamming attacks are generally not GNSS signal specific, post-correlation techniques for interference mitigation are restricted to e.g. array processing beamforming. The detection of interference can, however, also be carried out by monitoring the correlation functions, even though the correlators despread and therefore inherently mitigate the jammer effects, which makes detection at this stage harder.

4.2 Spoofing Detection and Mitigation

4.2.1 Antenna Techniques

Since most spoofing attacks are carried out using a single transmitter antenna, array processing methods are perfectly suited to detect and mitigate spoofing attacks by utilizing its spatial dimension. Using an array antenna, the individual DoA of the GNSS satellites can be estimated together with the receiver's attitude. By comparing the transmitted satellite position information in the GNSS message to the estimated one, a spoofer can easily be detected and suppressed afterwards using beamforming techniques [24].

4.2.2 Receiver Techniques

As one pre-correlation detection method, monitoring the receiver's front-end AGC can be used as an indication for a spoofing attack. But in contrast to jamming detection, post-correlation methods for spoofing detection are much more suited. Methods like cross-checks between code and carrier-phase measurement as well as range measurements from different frequency bands, C/N0 monitoring of the individual satellites, and step-detections on the raw measurements of all tracked signals can be used as direct indicators for spoofing attacks. Moreover, Receiver Autonomous Integrity Monitoring (RAIM) can be used to detect and exclude inconsistencies in the pseudorange measurements.

Especially if the receiver's antenna is moved – and assuming the movement is known to the receiver – powerful techniques exist that exploit the emerging correlations in a receiver's raw data output within a spoofing attack using a single transmitter antenna. In [25] a moving antenna uses the fact that spoofed signals from a single antenna are spatially correlated while authentic signals from the real satellites distributed in the sky are not. In a similar way, [9] is doing spoofing detection using intentional high-frequency antenna motion and the correlation of carrier phase data.

Since an inertial measurement system (INS) inherently cannot be jammed or spoofed, such a sensor can assist to harden a GNSS receiver. One technique described in [26] is based on fusing GNSS observables with inertial sensors measurements. The proposed method uses residual-based Receiver Autonomous Monitoring and comprises the INS and GPS solutions for successful spoofing detection.

4.2.3 Cryptographic Techniques

Spoofing is only possible because most GNSS signals do not use any cryptographic protection. There are no reported spoofing weaknesses with military signals which rely on cryptographically generated codes and encrypted messages. The downside is that the processing of these very well protected signals needs special security modules and a certain key infrastructure.

However, certain cryptographic techniques are discussed that do not impose any additional hardware or infrastructure costs [27], [28]. The idea is to add additional elements to the GNSS signals and/or their messages, like public key infrastructure (PKI) authentication elements or digital signatures. This is currently discussed for the GPS civilian navigation message (CNAV). Anyway, these ideas are still proposals and it might take a decade until some of them are finally realized and used in GNSS receivers.

Right now, with Galileo two cryptographically protected services available for non-military user groups are introduced for the first time. Even though the Galileo Commercial Service (CS) is not yet fully defined, ideas about providing additional correction data over an encrypted message for which the user has to pay are currently realized in an early demonstration project [29], [30].

The Galileo Public Regulated Service (PRS) features two encrypted signals on two frequency bands and targets both governmental and authorized users, e.g. police, border control, emergency, armed forces, Search and Rescue, and also operators of critical infrastructures like telecommunication and energy networks as well as critical transports. It is important to highlight that in contrast to GPS and GLONASS, Galileo is a civilian GNSS under civilian control. Consequently, PRS is not a military service, even though it is comparable to the military signals like the GPS P(Y) in terms of access control and the strong encryption used. The access to the PRS is controlled by the Galileo Member States through an encryption key system. The first Galileo PRS pre-operational receivers are currently under development in the P3RS-2 project for the successful demonstration of PRS services for pilot users beginning in 2016 [31]. There are also ongoing projects to use the protected and non-spoofable Galileo PRS signals for applications without having to use a dedicated PRS receiver at the end-user side by relying on offline PRS processing in an authorized environment [32]. These methods could be a door opener for mass-market applications with Galileo PRS

5. CONCLUSION

GNSS interference, both jamming and spoofing, is still an underestimated risk to many users of critical and/or even safety-relevant applications of GNSS, despite the reported events and demonstrations that showed the weaknesses of the current GNSSs and receivers. Most professional high-end receivers already incorporate some of the interference detection and mitigation techniques outlined in this paper. Unfortunately, many receivers – even certified ones – still do not provide any detection or mitigation features. Operators of critical infrastructure depending on GNSS usage should critically review their GNSS devices and upgrade to jamming and spoofing resilient receivers and consider using new spoofing resistant services like the Galileo Public Regulated Service (PRS). This, and in addition using array antennas with appropriate array processing techniques, seems to be the best protection against intentional GNSS interference available.

REFERENCES

[1] GNSS Market Report – Issue 3, October 2013

[2] A. Graham. Communications, Radar and Electronic Warfare. John Wiley & Sons, 2011

[3] Military & Defense NAVWAR Positioning Technology, April 2014. http://www.novatel.com/assets/Documents/Manuals/NovAtel-Defense-Brochure2.pdf

[4] FMV. Vidsel, ”The Natural Frst Choice for Real-world Testing in Europa”, http://www.vidseltestrange.com/.

[5] Eric Lagier, Desiree Craig, and Paul Benshoof. ”JAMFEST - A Cost Effective Solution to GPS Vulnerability Testing”, In Journal of Global Positioning Systems, 3:40–44, 2004.

[6] T. Kraus, R. Bauernfeind, and B. Eissfeller. ”Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation)”. In Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, 2011.

[7] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O’Hanlon, J. A. Bhatti, and T. E. Humphreys. ”Signal Characteristics of Civil GPS Jammers”. In Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, 2011.

[8] Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady W. O’Hanlon, and Paul M. Kintner Jr. ”Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.” In Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 2008.

[9] M.L. Psiaki, S.P. Powell, and B.W. O'Hanlon, "GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data," In Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2949-2991.

[10] Daniel P. Shepard, Jahshan A. Bhatti, T. E. Humphreys, and Aaron A. Fansler. ”Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks”. In Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 3591-3605., 2012.

[11] K. von Hünerbein and W. Lange. ”A New Solution of Generation of Spoofing Signals for GNSS Receivers” In Proceedings of International Symposium on Certification of Gnss Systems and Services (CERGAL) 7-8. Juli 2014

[12] http://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident

[13] http://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/

[14] J. Seo and M. Kim ”Loran in Korea – Current Status and Future Plans”, European Navigation Conference, ENC 2013, 23 – 25. April 2013, Vienna, Austria

[15] R. Bauernfeind and B. Eissfeller, ”Software-Defined Radio Based Roadside Jammer Detector: Architecture and Results”, In IEEE/ION Position Location and Navigation Symposium (PLANS), May 5-8, 2014, Monterey, California, 2014

[16] http://www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks

[17] Daniel P. Shephard, J Bhatti, T Humphreys, “Drone Hack: Spoofing Attack Demonstration On a Civilian Unmanned Aerial Vehicle”, GPS World, Aug 2012, vol. 23, no. 8, pp. 30-33

[18] http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[19] http://www.foxnews.com/tech/2012/02/23/gps-emerging-threat/

[20] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. ”Going up Against Time: The Power Grid’s Vulnerability to GPS Spoofing Attacks” GPS World, 2012.

[21] A. Rügamer, I. Suberviola, F. Förster, G. Rohmer, A., Konovaltsev, N. Basta, M. Meurer, J. Wendel, M. Kaindl, and S. Baumann, ”A Bavarian Initiative towards a Robust Galileo PRS Receiver”. In Proceedings of the 24th International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GNSS 2011, September 19-23, 2011, Portland, Oregon, USA

[22] A. Rügamer, I. Lukcin, G. Rohmer, and J. Thielecke, ”GNSS Interference Detection using a Compressed Sensing Analog to Information Converter Approach.”, In Proceedings of the 2013 International Technical Meeting of The Institute of Navigation – ION ITM 2013, January 28 - 30, 2013, San Diego, CA

[23] A. Rügamer, P. Neumaier, P. Sommer, F. Garzia, G. Rohmer, A. Konovaltsev, M. Sgammini, S. Caizzone, M. Meurer, J. Wendel, F. Schubert, S. and Baumann, ”BaSE-II: A Robust and Experimental Galileo PRS Receiver Development Platform.” In Proceedings of the 27th International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GNSS+ 2014, September 8-12, Tampa, Florida, USA

[24] A. Konovaltsev, S. Caizzone, M. Cuntz, M. Meurer, ”Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array”, In Proceedings of the 27th International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GNSS+ 2014, September 8-12, Tampa, Florida, USA

[25] A. Broumandan, A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen, and G. Lachapelle. ”GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation.”, In IEEE/ION Position Location and Navigation Symposium (PLANS), April 24-26, 2012, Myrtle Beach, South Carolina

[26] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. M. Joerger, and B. Pervan. ”GPS Spoofing Detection using RAIM with INS Coupling” In IEEE/ION Position Location and Navigation Symposium (PLANS), May 5-8, 2014, Monterey, California, 2014

[27] L. Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," In 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.

[28] T. E. Humphreys. ”Detection Strategy for Cryptographic GNSS Anti-Spoofing.” In IEEE Transactions on Aerospace and Electronic Systems, volume 49, april 2013.

[29] I. Rodríguez, G. Tobías, D. Calle, J.M. Martín, O. Pozzobon, M. Canale, D. Maharaj, P. Walker, E. Göhler, P. Toor, I. Fernández ” Preparing for the Galileo Commercial Service – Proof of Concept and Demonstrator Development” In Proceedings of the 27th International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GNSS+ 2014, September 8-12, Tampa, Florida, USA

[30] J. David Calle, Enrique Carbonell, Irma Rodríguez, Guillermo Tobías, Eckart Göhler, Oscar Pozzobon, Matteo Cannale, Ignacio Fernández, ”Galileo Commercial Service from the Early Definition to the Early Proof-of-Concept”, In Proceedings of the 27th International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GNSS+ 2014, September 8-12, Tampa, Florida, USA

[31] http://www.selex-es.com/-/pioneer-ii

[32] A. Rügamer, M. Stahl, and G. Rohmer. ”Privacy Protected Localization and Authentication of Georeferenced Measurements using Galileo PRS”. In IEEE/ION Position Location and Navigation Symposium (PLANS), May 5-8, 2014, Monterey, California, 2014.

BIOGRAPHICAL NOTES

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

Dirk Kowalewski

1987 – 1991 Technische Fachhochschule Berlin Dipl.-Ing. for Geodesy

1991 – 1993 sales manager Schikora GmbH

1993 – 2001 Head of branch office Rothe Berlin

From 2001 Founder and director of the Geo.IT Systeme GmbH

From 2009 Founder and director of the navXperience GmbH

2009 – 2012 Research project: MoDeSh with GL and HSVA: Motion and Deformation of Ships

From 2010 developing precise GNSS antennas

From 2011 Member of the working group AK 3 “Measurement method and Systems” DVW Germany

From 2014 Research project: Goose developing precise GNSS Receiver with an open Interface

CONTACTS

Alexander Rügamer

Fraunhofer IIS

Nordostpark 93

90411 Nuremberg

GERMANY

Tel. +49 911 58061-6379

Fax + 49 911 58061-6398

Email: alexander.ruegamer@iis.fraunhoer.de

Web site: www.iis.fraunhofer.de

Dirk Kowalewski

navXperience GmbH

Querweg 20

13591 Berlin

Tel.: +49 (30) 375 896 7-0

Fax : +49 (30) 375 896 7-1

Email: dirk.kowalewski@navXperience.com

Web site: http://www.navXperience.com