A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures

DESMOND SCHMIDT, KENNETH RADKE, SEYIT CAMTEPE and
ERNEST FOO, Queensland University of Technology (QUT)
MICHAŁ REN, Adam Mickiewicz University

Detection and prevention of GNSS “spoofing” attacks, or the broadcast of false global navigation satellite system services, has recently attracted much research interest. This survey aims to fill three gaps in the literature. First, to assess in detail the exact nature of threat scenarios posed by spoofing against the most commonly cited targets. Second, to investigate the many practical impediments, often underplayed, to carrying out GNSS spoofing attacks in the field. Third, to survey and assess the effectiveness of a wide range of proposed defences against GNSS spoofing. The conclusion lists promising areas of future research.

1. INTRODUCTION

GNSS (global network satellite system) receivers have become extremely cheap and compact [U-blox 2013]. They are now used ubiquitously in active tracking systems for people, animals and vehicles [Dimino 1999; Michael et al. 2006], in RTUs (remote terminal units) in SCADA (supervisory control and data acquisition) systems [Paolone et al. 2009], in mobile phones and in many other consumer products. GNSS is attractive because it provides a precise location of any receiver with a clear view of the sky with an accuracy of around ± 4 metres [DOD 2008; GPS.GOV 2014], and time up to about ± 10 nanoseconds [Lombardi et al. 2001].

This widespread use of GNSS has recently fuelled much research into the vulnerabilities of GNSS receivers [Nighswander et al. 2012]. The ability to spoof modern GNSS timers and navigation devices has been demonstrated in the laboratory many times [Warner and Johnson 2002; Humphreys et al. 2008; Humphreys and Ledvina 2010; Motella et al. 2010; Shepard et al. 2012; O’Hanlon et al. 2013].

But ubiquity of use does not equate to ubiquity of risk. In spite of several surveys of the GNSS spoofing threat [Volpe 2001; RAoE 2011; NERC 2012], what is still lacking is enough detail to assess the true nature of the vulnerabilities exposed by individual threat scenarios, the difficulty of carrying out the attacks, their likelihood, and hence what their overall impact will be. This approach is in line with the risk assessment guidelines published by national bodies such as NIST (U.S.) [NIST 2012] and ENISA [ENISA 2006] (Europe).

The first contribution of this survey, developed in Section 4, is a reassessment of the main attack scenarios mentioned in the research literature. The result is a downgrading of the often-cited GNSS spoofing threats against aircraft, taxis and trucks, and mobile phone networks. In their place, the spoofing threats against shipping, future Smart Grid control and management, and to a lesser extent train-collision-avoidance and secure criminal tags, emerge as the most vulnerable targets of GNSS spoofing in the future. Although the focus of this paper is on GNSS spoofing, many of the threat scenarios described in this section also involve jamming, whether because they form part of the spoofing attack itself, or because the assessment requires a comparison between spoofing and jamming.

The second contribution, in Section 5, is to provide a practical grounding to GNSS spoofing attacks. The possibility of spoofing GNSS devices under laboratory conditions has often been demonstrated, but this does not address the many practical difficulties in carrying out the same attacks in the field. These limitations have occasionally been hinted at (e.g. [Humphreys et al. 2008; Shepard and Humphreys 2011]), but never described in any detail.

An assessment of the broad range of defence strategies against spoofing forms the third contribution in Section 6. A great variety of strategies, from physical devices, cryptographic techniques, signal processing, and alternative sources for verifying timing and navigation solutions have been proposed. But so far no one seems to have ranked a broad selection of the proposals against each other, on the basis of generally applicable criteria such as cost, effectiveness, practicality, and whether the proposal is theoretical or proven. (Jafarnia's survey [Jafarnia-Jahromi et al. 2012] focuses on signal-processing, and Günter's on mostly cryptographic techniques [Günter 2014].)

Finally, Section 7 discusses the remaining gaps in the literature on GNSS spoofing, and which areas may still require further investigation.

Before any of these points can be made, however, Section 2 first describes the necessary background of the technology of GNSS, and Section 3 describes how spoofing and jamming attacks work. The points explained here will be necessary to understand the various attack scenarios, defences, and the practical difficulties of mounting attacks as explored in later sections.

2. GNSS

GNSS is an umbrella term for any "global navigation satellite system", of which there are currently only two fully working examples: GPS (US) and GLONASS (Russia), and two others in the process of becoming global: the European Galileo and the Chinese Beidou-2 systems. Each system of satellites maintained by one organisation is termed a "constellation". The overall designs of all forms of GNSS are remarkably similar. All transmit three basic messages:

a) A ranging signal for position, velocity and timing (PVT),
b) Precise ephemeris data, which specifies the exact location of the individual satellite, and
c) An almanac, which specifies the locations and orbits of *all* satellites in the constellation, along with status information [GPS 1995; Glonass 2008; Galileo 2010; BeiDou 2013], used to select satellites for tracking.

This basic degree of interoperability allows GNSS receivers to read signals from the four main satellite constellations and so avoid blackouts in "urban canyons" or other areas of poor reception by taking into consideration satellites from other constellations that may be visible [Ji et al. 2010]. It has been estimated that by 2020 around 100 GNSS satellites will be available, with 30-40 visible at any one time [Verhagen and Teuissen 2013]. All types of GNSS satellites transmit on at least two bands: using the predominant GPS terminology, on frequency L1 an encrypted military code, called P(Y), and an unencrypted civilian code, called C/A, while on the L2 band the P(Y) code is repeated.

2.1. Signal characteristics

At the lowest level a GNSS navigation signal can be seen as an analog sinusoidal wave at a frequency that varies roughly between 1.2 and 1.6 GHz. In order to carry digital information, segments of this basic signal are phase-shifted, in the case of GPS or GLONASS L1 by π radians. The usual method is BPSK (binary phase shift keying), which encodes 1 bit per phase-shift [Betz 2002]. Other variations are QPSK (quad phase), which uses four phase shifts to encode 2 bits per shift, as used in Beidou-2 [BeiDou 2013, p.4], and MBOC (multiplexed binary offset carrier), as used in Galileo E1 [Hein et al. 2006], which is designed to interoperate with the existing GPS L1 signal.

The information transmitted on a given frequency is composed of two separate signals: the in-phase (I) and quadrature (Q) components. These are phase-shifted by 90°

with respect to each other. In the case of GPS L1 (1575.42 MHz) the in-phase signal carries the civilian C/A code and the Q component the military P(Y) code.

In all cases what is encoded onto the analog carrier wave is a PRN (pseudo random number) sequence. The PRN is transmitted at an order of magnitude slower than the carrier, in the case of GPS L1, at 1 megabits per second. The length of the civilian PRN sequence is 1023 bits, which lasts for 1 millisecond, then it repeats [GPS 1995, p.9]. The W-code used in GPS L2, on the other hand, is 6.1871×10^{12} bits long and takes a week to transmit [Navstar 2006, p.6]. The length of PRN sequences used in other GNSS services varies considerably.

The GPS, Galileo and Beidou-2 signals are transmitted using CDMA (code division multiple access), which spreads the signal around a nominal frequency [Olenewa 2014, Ch.3]. This allows multiple signals, one from each satellite, identified by their PRN codes, to be transmitted at the same frequency. GLONASS, on the other hand, uses FDMA, which dedicates a separate frequency to each satellite, but also uses PRN sequences to encode the signal [Glonass 2008, p.15].

These PRN codes are what the satellite receiver locks onto. They are added modulo 2 to the actual navigation message transmitted at a very much lower rate, typically at only 50 bits per second.

The signal is transmitted by satellites at an altitude of between 19,100 (Glonass) [Glonass 2008] to 35,786 km (Beidou-2, inclined geosynchronous orbit) [BeiDou 2013]. On its way to Earth it has to pass through various distortions, such as the ionosphere, which delays the signal, particularly during the day, by as much as 300 nanoseconds [Dana 1997, p.17]. Since light travels about 90cm every 3 nanoseconds this effect alone amounts to a possible position error of 90 metres. The encrypted military signal can be used to compensate for this delay by correlating the two versions of the P(Y) code, which are delayed by differing amounts due to their different frequencies. However, it is possible even for civilian receivers to align the two P(Y) signals, using codeless techniques, and so derive the same ionospheric delay to correct the C/A code [Wright et al. 2011].

2.2. Augmentation

In addition to the main GNSS signals there are also local corrective signals which use a variety of techniques. Differential GPS uses ground-based receivers in precisely-determined locations that measure the delay between the time reported by local GNSS receivers and true time. These differences are then rebroadcast either using ground-based or satellite transmitters on a different frequency, which may be picked up by GNSS receivers and used to refine the navigational and timing solutions [Jinping 2012]. When combined with the main GNSS signals, these methods can provide positional accuracy up to 10-15cm. The drawback with all augmentation systems is that they only provide useful information for the area in which the augmentation system is located. For the continental U.S. and Hawaii there is the WAAS, for Europe EGNOS, in Japan MSAS, in India GAGAN, and in China the 2 geostationary satellites in the Beidou-2 system transmit augmentation data [BeiDou 2013]. In Australia DGPS services are provided by marine beacons [AMSA 2013] or by OmniSTAR satellites.

2.3. Position Solution

The calculations performed by a GNSS receiver to compensate for various forms of signal delay, such as relativistic effects or tropospheric delay [Dana 1997], end up as corrections to the difference between the time stamped on the packet and the time it was received, but do not affect the basic nature of the position calculation. When a GNSS receiver reads a time and location signal from a single satellite, it cannot compute the actual range because its local clock will be offset from the satellite clock

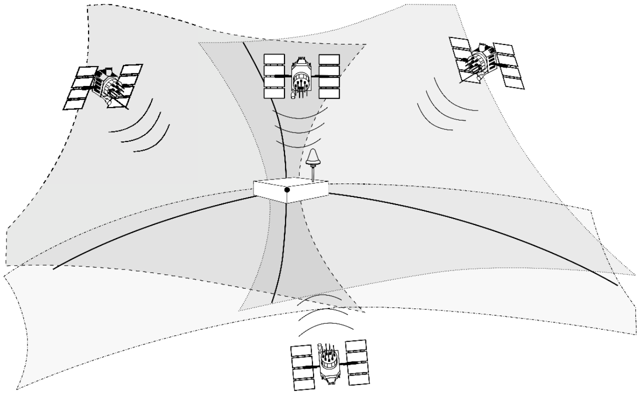

Fig. 1. Position solution

by an unknown amount. Even a difference of 1 millisecond equates to a range error of 300 *kilometres*. Representing this offset as ΔT, and c as the speed of light, the distance or *pseudo*-range p_0 to satellite 0 is:

$$p_0 = \sqrt{(x_0 - x)^2 + (y_0 - y)^2 + (z_0 - z)^2} + c\Delta T$$

The pseudo-ranges for four satellites $p_i,\ i \in [0, 3]$ represent four non-linear equations with four unknowns (the x, y, z coordinates of the receiver and ΔT). Subtracting p_0 from the other three equations eliminates the term $c\Delta T$ and produces three range differences $d_i,\ i \in [1, 3]$ [Kleusberg 2003]:

$$\begin{aligned} d_i = {} & \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} \\ & - \sqrt{(x_0 - x)^2 + (y_0 - y)^2 + (z_0 - z)^2} \end{aligned} \qquad 1)$$

These equations correspond to three hyperboloids, whose intersection, or simultaneous solution, is the location of the receiver, as shown in Figure 1.

2.4. Time Solution

Having worked out its position (x, y, z) in space, the receiver can also now compute the local time t_l using the transmitted time t_n and position x_n, y_n, z_n of satellite n:

$$t_l = t_n + \sqrt{(x_n - x)^2 + (y_n - y)^2 + (z_n - z)^2}/c \qquad 2)$$

A moving receiver, say in a car, must recompute its position each time it wants to derive local time. But if the receiver is in a fixed location, it only needs to solve the navigation problem a few hundred times, average the results, and then simply solve Equation 2 for a *single* satellite [Dana 1997, p.31]. The Arbiter GPS timer, for example, may take 24 hours worth of position fixes before entering “position hold mode”, at which point all timing calculations utilize that position fix. When computing time, usually only 1–4 satellites are used (those highest in the sky) and the results averaged [Trimble 2013, pp.45,119], but only one is required to provide a time fix [Dana 1997, p.25], [Warner and Johnston 2003].

Timing error is quoted very variously by different manufacturers as between ± 4 and ± 100ns [Symmetricom 2014; Trimble 2013]. These variations have less to do with the true accuracy of the timer, and more with the way that accuracy is quoted: as 1σ or as 2σ deviations, whether the figure includes augmentation, whether it is the accuracy of the receiver, or that of the time transmitted by the clock. Also the absolute accuracy of the atomic clocks in the satellites depends on the frequency of their updating. For example, the accuracy of the GNSS signal at the satellite end is variously quoted as “not worse than” 8 nanoseconds for GLONASS-M satellites [Glonass 2008, p.22], < 40ns for GPS [DOD 2008, p.24] and < 20ns for Beidou-2 [Chengqi 2012]. These are likely to be conservative estimates, since commercial timers often report, and provide evidence of, accuracies as high as ±4–15ns [Symmetricom 2014; Trimble 2013; Meinberg 2015].

3. SPOOFING/JAMMING VULNERABILITIES

Jamming needs to be described in order to distinguish it from spoofing, because the two are often confused. Sometimes it may even be legitimate to describe a tracking device as “spoofed” if it has been jammed, and reports a false location. Jamming may also be used as a prelude to a spoofing attack by forcing the receiver out of lock [Papadimitratos and Jovanovic 2008b; Humphreys 2013a; Kerns et al. 2013].

3.1. Jamming

GNSS signals at the earth’s surface varies from a minimum of -163dbW [BeiDou 2013, p.5] to -152dbW [Galileo 2010, p.10]. This has been likened to the strength of a 25W light bulb seen from 16,000 kilometres away [Warner and Johnston 2003]. Therefore a local noise signal, transmitted at an appropriate frequency, can easily overpower the legitimate satellite signals. The frequencies for all four constellations are on 15 bands ranging from 1164 MHz (Galileo E5a) to 1602 MHz (Glonass L1) [Hein et al. 2002; Glonass 2008; GPS.GOV 2013b; BeiDou 2013]. Even in countries where the GPS jammers are illegal (e.g., Australia [ACMA 2013], the United States [GPS.GOV 2013a] and the UK [RAoE 2011, p.6]), simple jammers can be bought on the Internet for as little as $15 [Chronos 2014, p.30]. Jammers are used to dodge tolls on motorways or to hide from employers the actual route taken by company vehicles [Marks 2013; Collier and Harris 2013]. When a GNSS tracking device is jammed, most devices report their last known location, rather than raise an alarm [Chronos 2014; Juneo 2015], although some do [MeitrackUSA 2015]. Loss of lock occurs so often for legitimate reasons: e.g. going through a tunnel, in heavily built-up areas etc., that sending an alarm signal at such times would be more of an annoyance than a help. This weakness can also be exploited to falsify the whereabouts of a truck with valuable cargo [Economist 2011; ABC 2013], and can have an impact on vehicles in the vicinity, including emergency vehicles.

The most common jamming technique is to transmit a continuous or ‘chirping’ (sawtooth pattern) noise signal at the known GPS frequencies, especially L1 [Kar et al. 2014]. Alternatively the GNSS PRN codes can themselves be used as noise, without any data, to pass through anti-jamming filters [RAoE 2011, p.20].

Jamming is also a serious threat to aircraft navigation, and networks and monitoring systems are now being set up to detect illegal GPS jammers on a national scale in countries like USA and UK [PNT 2010; Economist 2011; Chronos 2014; Kar et al. 2014]. Jamming events detected by the UK Sentinel system reported hundreds of incidents at a single provincial airport in its first three months of operations (October-December 2013) [Chronos 2014]. Isoz also reported hundreds of GPS/Galileo interference events per day at Kaohsiung International Airport, Taiwan [Isoz et al. 2011], and similar interference events have been detected at several airports in the U.S. [Dierendonck 2012], and in the London financial district [Weiss 2013].

3.2. Spoofing

Spoofing is more subtle than jamming, and relies on the generation of a counterfeit signal with just the right strength to “lift” a timer or navigation receiver from the legitimate signal. This can be done because, depending on the position of the satellite in the sky and atmospheric conditions, GPS signal strength may vary legitimately between -160dbW and -153dbW [GPS 1995, p.18], and the latter is five times the power of the former. A power ratio (spoofed versus authentic signal) of just 1.1 is sufficient to lift the receiver onto the spoofed signals [Shepard and Humphreys 2011].

The only detectable differences between legitimate satellite signals and spoofed ones may be in discrepancies in timing, signal direction, strength, doppler shift (relative speed between satellite/spoofer and receiver), and signal to noise ratio, which are all discussed in Section 6 below.

Most modern receivers are not equipped to detect these differences. The widespread implementation of AGC (automatic gain control) in GNSS receivers adjusts the signal gain to compensate for fluctuating signal strength (see Section 6.1 below), but also makes receivers more vulnerable to spoofing [Borowski et al. 2012; Jafarnia-Jahromi et al. 2013]. Also, crucially, since the receiving antenna is typically located at one point in space, a receiver has no way of telling whether the signal is coming from a locally generated spoofing source, or a legitimate satellite.

If the receiver is not secured, the spoofing signal can even be directly injected by replacing the antenna cable with the spoofing source. Or, if the spoofer knows the precise location of the target receiver he/she may more easily superimpose the authentic signals with the spoofed ones. This will be necessary if the receiver is already in operation and locked onto legitimate signals [Günter 2014]. Alternatively, if precise synchronization with legitimate signals is impractical, then stronger unsynchronized signals may be used to overwhelm the legitimate ones. However, this will only be effective if the receiver is starting up or is first knocked out of lock by a jamming attack.

3.2.1. Meaconing. The simplest form of spoofing is meaconing, which is the capture and retransmission of legitimate GNSS signals after a delay. Meaconing, however, is difficult in the case of the encrypted military signal, such as the GPS P(Y), because it is modulated onto a far longer PRN sequence. Since receivers have their own clock they could easily detect the out of phase alignment of the W code [Humphreys 2013a]. Also, because the P(Y) GPS signal is transmitted well below the background noise level, retransmitting it would require an accurate estimation of the secret W code, which can be achieved via "semi-codeless" techniques [Jung et al. 2003].

For the civilian signals, however, no such difficulty of spoofing arises. Since the *relative* arrival times of the four signals are unchanged by the meaconing process, the navigation solution will be that of the meaconer [Papadimitratos and Jovanovic 2008a; Wesson et al. 2012]. The timing solution will likewise be that of the meaconer, plus the time taken to retransmit the signals to the victim [Wesson et al. 2012].

However, meaconing does not seem suitable for attacks against timers. The first stage of an attack is to substitute the spoofed signal for the real one. Since a timer already knows its own location, it would read the delayed time being transmitted by the meaconer, resulting in a sudden shift in the timing solution equal to the time required to retransmit the signal. This would clash with the known local time maintained by the clock, and could be used to raise an alarm. However, meaconing could also be performed initially with a zero-delay, by predicting the signal values in advance and synchronising with the true signals [Wesson et al. 2012].

3.2.2. SCER. A variation of meaconing called SCER (security code estimation and replay) or "selective delay" [Kuhn 2004] involves the rebroadcast of individual satellite signals after a delay [Wesson et al. 2012]. This can modify both the position and/or timing solutions. An attacker could then manipulate the position solution only and so avoid a time jump when starting an attack [Pozzobon 2011]. SCER is described more fully in [Papadimitratos and Jovanovic 2008a].

3.2.3. Other forms of spoofing. Other forms of spoofing are categorized by the level of sophistication. Humphreys and Motella divide these into "simplistic" (broadcast of arbitrary GNSS signals without synchronization with legitimate signals), "intermediate" (spoofing synchronized with legitimate signals) and "sophisticated" (using multiple phase-locked intermediate spoofers) [Humphreys et al. 2008; Motella et al. 2010].

A spoofing device, called as "limpet spoofers" [Lo and Enge 2010], can be attached to the vehicle or timer it is intended to spoof. These devices overcome many of the practical limitations on spoofing described in Section 5 below, but require both compromise of the physical security of the receiver, and in practice also a level of miniaturization that has not yet been achieved.

4. SPOOFING/JAMMING SCENARIOS

A wide variety of spoofing threat scenarios are mentioned in the literature. This section examines the main ones in sufficient depth to assess the seriousness of the vulnerabilities in practical scenarios. However, this must be combined with an assessment of the practical limitations on carrying spoofing attacks, which is explored in the following Section 5. The overall assessment of the vulnerabilities will be made at the end of that section, summarized in Table I.

Jamming threats are also described only when they overlap with spoofing. Where appropriate, a critical assessment of work done in each field will be made. However, most of these threats remain unexplored as separate research topics.

4.1. Power distribution networks

Power distribution networks are among the most often cited potential targets of GNSS spoofing attacks [Humphreys and Ledvina 2010; Shepard et al. 2012; Jiang et al. 2013; Garofalo et al. 2013; Akkaya et al. 2013; Heng et al. 2014]. However, they are currently not particularly susceptible to such attacks, because controls over centralized distribution and fault control are managed by electronic devices and manual monitoring techniques. At the moment GNSS timers are used mostly for passive logging or telemetry [NERC 2012]. However, as will be shown below, the emergence of the Smart Grid and distributed power generation will greatly increase the susceptibility of power distribution to GNSS spoofing.

4.1.1. The time-critical nature of power generation. The roots of this dependency lie in the time-regulated nature of power generation and transmission. Alternating current (AC) is an oscillating voltage transmitted over long or short distances at a constant frequency: 50 or 60 Hz. Modern power systems use triphase, three separate signals separated in phase by $120°$. Generators must maintain their phase and frequency to agree with the grid, and this requirement is under constant stress. For example, increased electrical load tends to slow down the generator by increasing the electrical torque T_{elec}, forcing it out of synchronization with the mechanical torque T_{mech}. This results in a change in frequency, which must be compensated for by the use of mechanical governors to increase T_{mech} [Wood et al. 2014, p.468f].

Likewise, when first connected to the grid, the phase and frequency of a mechanical generator must match that of the grid; otherwise the generator will suffer excessive torque as it is pulled into alignment, which may result in the destruction of the generator [Williston and Finney 2011; Thompson 2012]. This is because the magnetic fields of the generator are in opposition to those induced by the grid, resulting in sheering forces that cause rapid acceleration and increased energy consumption. The degree of tolerance depends on the size of the rotor: the larger it is the less tolerance. For generators up to 10,000kVA the maximum tolerance is 10° [IEEE 2002, Table 5]. This process is currently handled automatically by programmable logic controllers (PLCs) [ASKA 2012].

4.1.2. PMUs. The advent of distributed power generation, such as local smaller generators, wind-turbines and home-scale solar panel systems, have greatly complicated the older centralized power distribution scenario [Giri et al. 2009]. As part of the "Smart Grid" this more complex system requires an improvement in the monitoring, protection, and operation that can only be provided by real-time sensing and reaction to dynamic power system phenomena [IEEE 2011].

A key component of the management of the Smart Grid is the phasor measurement unit, or PMU. This is a monitoring device which reports current, phase and voltage at anything from once per second to one or two times per 50-60Hz cycle [IEEE 2011]. The synchronization provided by a GNSS timer is essential to the function of the PMU because timing with an accuracy of around ± 1 microseconds is required [Hurtgen and Maun 2012]. Although this level of accuracy could be provided by PTP (precision time protocol), this requires specialized routing equipment [Schweizer 2015], and is thought not to scale to the size of a national grid [Yu et al. 2014].

A "phasor" is a numerical quantity that describes the synchronization of the measured voltage wave form with the rest of the network. They can be seen as a compact way to represent the phase and magnitude of the current, voltage and rate of change of frequency (ROCOF) at a particular point in the network [IEEE 2011]. Each measurement is precisely time-stamped using a local GNSS clock, which is not part of the PMU, and is then transmitted back to a management point, via a series of "phasor concentrators", which aggregate and time-align readings from multiple PMUs. Real time control of the network is provided via "synchrophasor vector processors", which can be programmed to take remedial actions such as reclosing (reconnection after separation of part of the network) and tripping, when instability in the line threatens equipment, or bringing into phase geographically separate parts of the power network [Schweitzer 2014; Hurtgen and Maun 2012].

The synchronization between the PMU's internal clock and its time reference must be within $\pm 31\mu$secs for a 50 Hz system, or the PMU will report loss of synchronization [IEEE 2011]. This is independent of any error in the time reference source itself, and damage to the electrical system is unlikely until a time error of 2 milliseconds is reached.

PMUs offer a much more detailed picture of grid stability that requires automated control, both because of the amount of data and the speed at which events happen [Giri et al. 2009]. The international survey by Hurtgen and Maun in 2012 shows that usage of PMUs is already widespread globally, and growing rapidly [Hurtgen and Maun 2012]. Typically countries have around a dozen PMUs in total, but they are used for controlling national and even international grids. They identify 16 main applications of PMUs, many of them involving time-critical management.

There is currently little mention in the literature on the development of PMU applications of any threat from GNSS spoofing (although see [Yu et al. 2014]). Arbiter Systems, for example, claim that although their clock 1094B is vulnerable to GPS spoofing it is unlikely to happen in practice and they know of no case where it has actually happened [US-Cert 2015]. In spite of this, Shepard and Humphreys have shown that the kinds of timers usually coupled with PMUs can be easily spoofed [Shepard and Humphreys 2011; Shepard et al. 2012]. The development of PMU applications may still be in its infancy, but their development is comparable to that of GNSS spoofers themselves. Several models of portable GNSS simulators, such as the GPSG-1000 or the hand-held Cast SGX, which could be used as spoofers at close range, are already available [Cobham 2015; CAST 2013]. Further miniaturisation may conceivably lead to the development of limpet-spoofers “the size of a pack of cards” [Humphreys et al. 2008]. The growth of the Smart Grid, the possibility of inducing cascading failures by spoofing timers [Shepard et al. 2012], and the proven ease of spoofing substation timers, together imply that a significant threat to power grid management on a national scale may develop in future, unless the spoofing threat is adequately addressed [Akkaya et al. 2013].

4.1.3. Fault detection. Another possible target in power system management is fault detection. When a fault occurs in a long transmission line, due to lightning strikes, overload, ageing etc., a crew must be dispatched to repair the fault. When the fault occurs, a travelling wave (TW) is transmitted in both directions. Detectors are usually set to monitor the lines and to detect the TW [Elhaffar 2008]. One of the best methods compares the arrival times of a TW at both ends of a line where the fault occurred [Elhaffar 2008]. But this requires precise synchronization of the two clocks at either end. Since electricity travels at 9/10ths the speed of light, the timing error must be kept well below 1 μsec. The Finnish power management system has only five detectors, and faults are located by comparing the time of arrivals of the TW at the nearest two detectors. Hence even a small timing error in one of the GNSS clocks might result in a measurement error of hundreds of kilometres [Elhaffar 2008, p.81]. The losses here are in the increased time required to fix a fault, and the consequent cost to business and inconvenience to domestic users.

4.2. Shipping

As Humphreys has demonstrated, spoofing the navigation receiver of a large ship is relatively easy [Humphreys 2013c]. This could be accomplished either from another boat shadowing the target, or simply by covert broadcast of spoofed signals from the deck of the target vessel. One use of spoofing can be to hide the true location of a fishing vessel in forbidden waters [Humphreys et al. 2008; Motella et al. 2010]. Since 2002, ships over 300 tons are required by international agreement to carry AIS (automatic identification system) transponders, which transmit the GNSS-determined position to AIS satellites in orbit [IMO 2004, V.2.4]. In 1995 the Royal Majesty, a passenger cruiser carrying 1,509 people, grounded near Nantucket after veering off course, causing $7 million in damage, because of the failure of a GPS navigation system [NTSB 1997]. Although not a spoofing attack, the effect of this incident is similar to Humphreys' steering of a yacht off course [Humphreys 2013c; 2013b]. DGPS is also used for precision steering of ships during harbor approach, which requires 8-20 metre positional accuracy [Volpe 2001, p.15]. Spoofing of GNSS signals would thus be a relatively easy way for terrorists to sink a ship, which is a high value target.

Ship-based GNSS receivers also react badly to jamming signals, reporting erroneous locations without warning [PNT 2010].

Swaszek [Swaszek et al. 2014] describes a promising technique applicable to ships in which an IMU (inertial measurement unit) is used to correlate the pitch and roll of the vessel against the GNSS calculated position. In the spoofed scenario the pitch and roll are not detected by the GNSS receiver and so spoofing is easily detected.

4.3. Aircraft

Kerns [Kerns et al. 2013] examines the difficult task of spoofing the GNSS receiver of a small rotor-powered drone in flight. Both altitude (12m) and speed (10m/sec) are far less than a real world target, such as a fast high-flying commercial jet aircraft. Even so, having to precisely track the target, and estimate Doppler-shift in real time, and controlling signal strength, are all challenging problems. Kerns admits that in commercial aircraft the shadowing effect of the underside of aircraft would make it very difficult for a spoofer to estimate the correct signal strength [Rao et al. 2006] [Kerns et al. 2013, p.25]. Hence the only possible way to spoof the GNSS receiver of a commercial aircraft would appear to be to fly alongside it, matching it for speed and power.

The use of GNSS in landing and takeoff, however, reveals a far greater vulnerability. Most commercial aircraft still use ILS (instrument landing system). However, increasingly GBAS (ground based augmentation system) is becoming something of an international standard. The US NextGen aircraft landing system is critically dependent on GPS. In Australia flight path approaches to major airports are governed by Smart Tracking, a GNSS-based guidance system. Australian airports currently use enhanced ILS (instrument landing system) for approaches, which can only guide a plane down to 60 metres before the pilot takes over. However, the plan is to eventually move to GBAS [Airservices 2014], although so far this has only been done at Sydney airport. GBAS has the advantage of being potentially a "CAT III" system, that is, one that can land a plane entirely automatically. Worldwide usage is growing, particularly in Europe and Russia [GBAS Working Group 2013]. Concerns about the vulnerabilities of GBAS to interference and reliance on GPS alone has so far held back widespread deployment. GBAS is currently unauthenticated, and so could be spoofed [Lo and Enge 2010].

Since most of the GNSS receivers used in GBAS reside on the ground at an airport, the height of an individual aircraft could conceivably be spoofed, leading to a crash [Becker et al. 2009]. Jamming part or all of a GBAS installation, or the approaching/departing aircraft's GNSS receiver would be relatively simple, or could easily happen accidentally, and may result in significant loss of life.

4.4. Trucks and Taxis

GNSS jamming devices are easy to obtain from overseas suppliers, and retail from $300 to as little as $15, and an effective range from 1–500 metres [PNT 2010; JFC 2014; Chronos 2014]. Vehicle tracking devices work by using the GNSS position fix in the conventional way, then transmitting via a mobile phone band (GSM or 3G) to a service run by the tracking company [Pozzobon 2004]. The owner of the fleet then logs in to the service and reviews tracking information for company vehicles. When a tracking device is disabled by a jammer it usually reports its last known location, since loss of lock is common in areas of poor reception [Chronos 2014, p.25] [Juneo 2015]. Some of the more expensive trackers, however, do now raise an alarm if they are jammed, e.g. the Meitrack MVT100 [MeitrackUSA 2015].

Truck drivers use GNSS jammers to disable tracking so they can use a truck for unauthorized routes. They can also be used by thieves to steal valuable cargo or the vehicles themselves [Chronos 2014].

Taxi drivers use them to disable tracking while taking on extra fares; they then respond when offered a job by the control centre, allowing them to steal extra work [ACMA 2014].

Warner used a GNSS simulator to spoof a truck's navigation system [Warner and Johnson 2002]. However, limitations on signal strength meant that they had to follow 15 feet behind the spoofed vehicle, and the initial lock took several minutes' standing right next to the vehicle. However, these difficulties may be overcome in the future if miniature spoofers [Humphreys et al. 2008, p.4] become as freely available as miniature jammers.

4.5. Trains

The American positive train control (PTC) system utilizes GPS position and velocity information as the primary means to track train movements, enabling the prevention of accidents particularly at road crossings, but also collision avoidance and speeding detection at lower cost than alternatives such as ATC (automatic train control) [Volpe 2001]. The system is now mandated to be implemented on all US rail services by December 2015 [GPO 2008], although most report they will miss the deadline [Fleming 2013]. Similarly the Russian train system uses KLUB-U, which is based on GLONASS [NIIAS 2015]. But the majority of automatic train control systems used worldwide are based on the European ATP/ERTMS (automatic train protection/European rail traffic management system). The Volpe report assessed the dangers to PTC as slight, because the GPS information is correlated with many other sources of positional and timing information. In the event of a severe GPS outage rail services would continue to run at reduced efficiency [Volpe 2001, p.61]. But it still seems possible to spoof the location of a train that uses PTC or KLUB-U, using an on-board spoofer, which may lead to serious loss of life. However, the exact nature of GNSS vulnerabilities to the KLUB-U and PTC collision-avoidance systems is currently unknown.

4.6. Securely-tagged criminals

Ankle monitors that exploit the accurate positioning provided by GPS (or GNSS) to limit the wearer to a geographically-defined boundary, have existed since 1999 [Grillo and Veschi 1999]. Today in the USA around 200,000 criminals are regulated in this way [Payne et al. 2014]. PLS (personal location services) ankle monitors cost around $500 per item, and around $700 a year to run [MightyGPS 2009]. This is a fraction of the cost of incarceration. Most modern ankle monitors operate within the home by direct transmission over mobile phone bands, to a monitoring service. Active tracking is where the location of the criminal is checked at intervals, usually about 15 minutes, whereas passive tracking allows the wearer more freedom to move, and their whereabouts are downloaded at the end of the day to a base station for checking [Koshima and Hoshen 2000].

If the GPS signal lock is lost one of two things happens: either the monitor sends an alarm to the monitoring service, or it falls back to using GSM location. However this is far less accurate, and can only provide an approximation of the wearer's location to within about 2 miles [Landoni 2011]. Some ankle monitors claim to be able to detect the presence of a GPS jammer, and all attempts to block the signal, for example, by wrapping it in foil, will produce an alarm [Blutag 2012]. In none of the models examined via their online manuals, however, is there any mention of resistance to GPS *spoofing,* and this would likely be undetectable. Theoretically, a limpet-spoofer worn by the offender could falsify his/her whereabouts. Manufacturers could respond to this threat by correlating the GPS position with the GSM-computed one, and raising an alarm if there was a mismatch, but offenders could still wander outside the tight confines of their legally fenced position with the aid of a spoofer.

4.7. Mobile phones

The practical difficulties of spoofing individual mobile phones make them unlikely targets. Mobile phones, like their owners, are mostly found in cities. But cities are full of buildings that can easily block signals from a spoofer located at ground level. Many mobile phones are also on the move, in cars or moving with their walking owners in built-up areas, making it difficult to maintain a spoofed signal lock (see Sections 5.2, 5.3, 5.5 below). Although occasionally mobile phones have reported an erroneous location that threatened life [Hyde 2012], the difficulty of carrying out such an attack and the low recompense for the attacker make this a highly unlikely scenario.

On the other hand, mobile phone networks are often, though not always, dependent on precise timing. The Volpe report notes that, in 2001 GPS timers were used in PCS, GSM (also [Carroll and Montgomery 2008]), TDMA, CDMA (also [Jafarnia-Jahromi et al. 2012]), and Wideband CDMA mobile telephony systems [Volpe 2001]. GNSS timing is also used in 4G networks, such as LTE-TDD (time division multiplexing). Timing requirements for LTE-TDD range from 5-1μ seconds [Weiss 2012]. CDMA requires $\pm 10\mu$sec accuracy between basestations [Carroll and Montgomery 2008; Humphreys and Ledvina 2010; Shepard and Humphreys 2011]. Carroll reports that a GPS jamming incident in San Diego 2007 caused a mobile phone outage [Carroll and Montgomery 2008].

The older phone technology, GSM, which uses TDMA (time division multiple access), paradoxically doesn't require precise synchronization between base stations. This is because it has a protocol to synchronize the handset with the current basestation and also during handover [ETSI 1996].

However, the recent development of alternative timing systems, independent of local GNSS timers, has largely made this spoofing vulnerability moot. For CDMA Wheatley proposed using the CDMA network itself to distribute accurate time from a small number of timer-equipped base stations [Wheatley 1999]. But the most popular method is PTP (precision time protocol), standardized in IEEE-1588-2008 [Antonova et al. 2013], which is suited to modern 4G networks that use an IP network. LTE is purely packet-based and benefits from a centralized precision timing service [Broadcom 2008]. However, CDMA, a 3G technology, appears to still be susceptible because local GPS time receivers are used on each base station [Chronos 2014]. This is expensive, and the tendency now is to move to packet-based IP synchronization via PTP for all LTE services in future [Ferrant et al. 2013, Ch.6]. Hence the GNSS spoofing threat against mobile phone networks, although high in certain vulnerable networks that are in decline, is also declining with it.

5. PRACTICAL DIFFICULTIES OF SPOOFING

No one has yet assessed the numerous impediments to carrying out spoofing attacks in the field. Taken together, these considerations make attacks against the most common types of receivers, such as mobile phones and cars, impractical, by raising the bar of difficulty too high in relation to the benefit that would accrue to the attacker. On the other hand, higher value targets such as ships, planes, secure tagging and power stations may still present worthwhile targets.

5.1. Cost and labor

Cost depends on the type of spoofer being constructed, and the type of target. In accordance with with the types of spoofer described in Section 3.2.3 above, practical costs associated with simplistic simulation, meaconing and receiver-spoofer devices will now be assessed. "Sophisticated" spoofers seem thus far to be only theoretical.

5.1.1. Simulator costs. Broadcasting at least one constellation without synchronization with legitimate signals is the cheapest option in terms of labour. The software to generate one or more constellations is provided by the simulator manufacturers. There are two types: analogue and digital [Petrovski and Ebinuma 2010]. The analogue ones tend to be very expensive, up to $500,000, because a separate transmitter is needed to represent each satellite [Petrovski and Ebinuma 2010, p.54]. Digital simulators, on the other hand, use a single transceiver to broadcast at multiple frequencies. A complete digital simulator with multi-GNSS capability would cost around $20,000–50,000, depending on the make and number of constellations. With digital simulators the main cost is the simulator software. Smaller portable simulators by Aeroflex and CAST offer simulation of a few constellations only, with the possibility of creating custom scenarios [CAST 2013; Cobham 2015].

5.1.2. Meaconing costs. The literature is largely silent on the subject of building a meaconer. However, it would be relatively easy to build a meaconer based on a software-defined radio, such as the Ettus USRP N210, which retails for $2,300, plus a wideband transceiver, which would cost an extra $700. This could be combined with a signal captured from a GPS antenna, then replayed after a delay [Brown et al. 2013]. But to introduce a variable delay or to separate out the various satellite signals for SCER would require custom software development, and the final cost would probably approach that of the cheaper full simulators. A multi-constellation meaconer, however, would be difficult due to limitations on commercial DSP chips [Humphreys et al. 2006].

5.1.3. Intermediate-level spoofer costs. In Humphreys' receiver-spoofer design, the receiver's signals are used to compute an accurate simulated constellation under the control of the operator [Humphreys et al. 2008]. Currently only the GPS constellation has been successfully spoofed under laboratory conditions [Humphreys et al. 2008; Motella et al. 2010; Shepard and Humphreys 2011; Shepard et al. 2012]. The cost of creating a GNSS simulator nowadays is often claimed to be low [Motella et al. 2010; Shepard et al. 2012], but this ignores the considerable costs of in-field deployment. The simulator part of Humphrey's design is readily available commercially. As a result, a basic digital simulator are similar to the cost of building a meaconer. However, many extras are needed to turn this basic device into a simulator for use in the field. The software can be a combination of GNU Radio and Matlab [Motella et al. 2010; Brown et al. 2013], both of which would require a PC to run the software (at least $1,000), a vehicle for transporting the equipment (hired for $80/day), and a parabolic antenna ($80) to avoid spoofing unintended victims and to concentrate the signal. Also, if the target is a timer or PMU, in order to be effective, the attack should first be practised on an example of the relevant model of receiver in the laboratory, to gauge signal strength, speed and acceleration at which the navigation and time solutions can be skewed. For these purposes an rf-shielded tent would be needed (ca. $10,000), and suitable substation timers cost at least $3,000, and much more for one with an atomic clock.

The amount of labor and expertise required to put together a complete receiver-spoofer is also quite high. Humphreys reports that his spoofer took “four Ph.D. students several years” to build [Humphreys 2013b]. Raising the bar still further, GNSS timers are already using multiple constellations for increased precision [Dicom 2014; Trimble 2013], and so a multi-constellation simulator would be needed. This increases the difficulty and cost of developing an intermediate-level spoofer significantly [Humphreys et al. 2008, p.12].

5.2. Covert operations

Knowledge of the exact location of the relevant antenna and make and model of the GNSS receiver it is connected to, and its spoofability, would be essential for the attack to have any realistic chance of success [Shepard and Humphreys 2011].

If an off-the-shelf simulator was chosen, police forces could use the record of purchase to track down the offender if the attack was detected [Ledvina et al. 2010]. This could result from simultaneous disruption of mobile GNSS services in the vicinity, through mobile jamming detectors [Chronos 2013], or through direct detection by sensor networks [Gabelli et al. 2013; Chronos 2014].

5.3. Inverse square law

One of the major problems faced by the would-be spoofer is the simple inverse square law [Jafarnia-Jahromi 2013, p.28]:

$$P_r = \frac{P_t}{4\pi d^2}$$

Where P_t is the transmitted power, P_r the received power, and d the distance between the receiving and transmitting antennas. As the distance between spoofer and target varies even by a small amount, for example, when spoofing a navigation receiver in a vehicle, the received signal strength P_r varies more widely, in accordance with the d^2 term. As a result the spoofer must either maintain a precise distance to the target or vary signal strength to compensate [Tippenhauer et al. 2011]. Otherwise, the receiver may detect the unexpectedly strong signal and report loss of lock [Jafarnia-Jahromi 2013, p.103f] [Shepard et al. 2012, p.7], or will fall back onto the legitimate signals [Shepard and Humphreys 2011]. In either case the spoofer would have to start all over again, but would not know that the attack had failed.

The signals from legitimate satellites also vary with the inverse square law, but their distance from the receiver doesn't vary significantly for distances of several kilometres on the earth's surface, but such variations make a very big difference in the spoofing case because the transmitter and receiver are much closer together. Some of the variations that do occur in the legitimate signals depend on known factors such as satellite elevation, but received power can also vary by as much as ±6dbW due to the orientation of the transmitting antenna and changes in altitude of the SV [Glonass 2008, pp.16,47]. All of the cited spoofing experiments carried out in the laboratory have emphasized this need for closely controlling signal strength for a spoofing attack to succeed.

5.4. Moving targets

One consequence of the inverse square law is the difficulty of spoofing a moving target such as a ship, aeroplane or car. In order to maintain correct signal strength it would be necessary for the spoofer also to be moving with the target, unless it was on-board, as in the case of Humpheys' spoofing demonstration with the yacht [Humphreys 2013b; Zaragoza 2013]. Similarly, in order to spoof a truck's navigation system, Warner had to follow 15 feet behind the target truck after first disabling the its GPS satellite lock and establishing a fake one at close proximity for several minutes [Warner and Johnson 2002]. Kerns notes the need for accurate tracking of aircraft for spoofing to succeed, requiring the use of the aircraft's own ADS-B broadcasts [Kerns et al. 2013]. Jafarnia and Wesson note that for a synchronous spoofing attack (the precise alignment of the legitimate and spoofed PRN sequences) to avoid detection through the vestigal signal defense (Section 6.1.4 below) requires precise "centimetre level knowledge" of the position of the spoofer in relation to its target [Wesson et al. 2011; Jafarnia-Jahromi 2013, p.20]. Ideally, a spoofing device needs to be either physically on the receiving antenna or at a fixed distance from it. Although these were experiments, or theoretical scenarios, these kinds of limitations make the remote spoofing of vehicles very difficult in many cases, and in the case of ground-based vehicles jamming is often easier, more reliable and far cheaper.

5.5. Direct line of sight

The most common GNSS signals are transmitted around 1.5 GHz (GPS L1, etc.), which has a wavelength of just 20cm. As a result, GNSS signals do not bend much around obstacles. Hence a spoofer would have to be in direct line of sight with the target's antenna. Aircraft are already considered immune from ground-based GNSS interference when in flight, because of the shielding effect of the aircraft underside, while the antenna is typically situated on the top of the aircraft [Rao et al. 2006]. Terrestrial broadcasting of spoofing signals inside a city or in uneven terrain would also likely fail because of shielding from buildings and hills.

5.6. The need for multiple simulators

It is hard for a spoofer to attack more than one GNSS receiver at once. Because of the inverse square law, the correct signal strength at one receiver would likely be too weak or too strong for a second receiver, and the correlation peaks between authentic and spoofed signals would not be aligned [Jafarnia-Jahromi 2013, p.150], unless they were close together. To affect multiple receivers over a wide area the simulator would have to broadcast a general, powerful signal from a mountain top or tower, which would cause denial of GNSS services over a wide area, making discovery virtually certain. So, in practice, a spoofing attack against multiple navigation receivers or timers would require multiple phase-locked intermediate GNSS spoofers, situated close to each target [Tippenhauer et al. 2011]. This greatly increases the logistical effort required, as well as the expense of mounting an attack. It also requires that each of the targets has an identical GNSS receiver.

5.7. Speed of attack

In the laboratory failure in a spoofing attack can be corrected by seeing the result and adjusting the speed and strength of the attack for a particular brand of receiver, but in the field such feedback would be lacking. The type of receiver being attacked may not be known, and attacks typically take anything between two minutes and an hour. Variations in the speed at which the position solution may be skewed from its true value vary enormously, anything from 2 m/sec to 1,300 m/sec [Shepard and Humphreys 2011]. Exceeding this speed limit would result in loss of lock, and the spoofer having to start again. When used with atomic clocks, time receivers can tightly control the rate at which time may drift, and hence require much more patience on the part of the attacker [Ledvina et al. 2010], or even render such an attack impossible.

5.8. Compromise of antenna security

Several types of attack require spoofing transmitters to first overcome the physical security of the antenna. An example mentioned by Kuhn requires the isolation of the antenna through RF-shielding and the placement inside the enclosure of a simulator with full control over the receiver's inputs [Kuhn 2004]. Humphreys makes a similar point about the placement of hypothetical spoofers "the size of a pack of cards" on the individual antennas of a multi-antenna array [Humphreys et al. 2008, p.4]. Although these were just experiments or proposals, the feasibility of such attacks against high value targets such as large ships, aeroplanes and power stations is at least questionable.

5.9. Rarity of GNSS Spoofing Attacks

The only successful GNSS spoofing attacks reported in the field have been planned experiments against GPS-only navigational receivers. The yacht steered off course in international waters [Humphreys 2013c], the smaller drone controlled by spoofing in a football stadium [Humphreys 2012], and the attack on a truck by Warner [Warner and Johnson 2002] are all of this type. According to the account of the Iranian perpetrators, the US military drone reportedly brought down by "spoofing" in Iran was actually a case of simple jamming, along with the compromise of "unencrypted drone data streams", i.e. *not* the military GPS signal [Peterson and Faramarzi 2011]. The "spoofing" attacks claimed by Lo [Lo et al. 2009] were also just jamming incidents [Forssell 2009]. In spite of the fact that the GNSS spoofing threat was first acknowledged 20 years ago [Hartman 1996], none of the research papers, monitoring experiments or risk assessment studies surveyed mention a *single* confirmed case of hostile GNSS spoofing in the field, although accidental spoofing by GNSS repeaters is known to have occurred at European airports [Günter 2014]. This rarity of spoofing may be either because it is hard to discriminate between jamming and spoofing, or equally because it is hard to carry out a successful spoofing attack in the field [Jafarnia-Jahromi et al. 2013].

5.10. Summary of Spoofing Vulnerabilities

The considerations arising from Sections 4 and 5 above suggest that GNSS spoofing is mostly a potential, rather than a current threat. The dangers posed by spoofing to secure tagging, shipping, aircraft landing systems and power stations remain theoretical, and as yet there have been no confirmed reports of their exploitation. This contrasts with the very real threat, and many documented cases of, GNSS jamming. However, the numerous practical limitations on deployment of intermediate level spoofers in the field can mostly be overcome by the use of small, locally attached "limpet" spoofing devices. The ready availability of cheap GNSS jamming devices today suggests that manufacturers may soon develop such limpet-spoofers, which would seriously compromise the security of many of these targets. The current and potential threats to individual GNSS applications from both spoofing and jamming are summarized in Table I.

Table I. GNSS Spoofing and Jamming Vulnerabilities in Applications

Application	Spoof (now)	Spoof (future)	Jam
Ship navigation	High	High	Med.
Aircraft landing/takeoff	Low	Low	High
Aircraft navigation	Negligible	Negligible	Negligible
Train collision-avoidance	Low	Med.	Negligible
Power system PMUs	Low	High	Negligible
Delivery trucks	Negligible	Med.	Med.
Mobile phones	Negligible	Negligible	Negligible
Mobile phone networks	Med.	Low	Low
Secure criminal tags	Low	Med.	Low

In most devices, having no protection against spoofing is an adequate response, since no one is likely to spoof low-value targets like mobile phones, animal tracking devices, bush-walkers or in-car navigators. Not only are attacks against these targets exceptionally difficult, the consequences of any such an attack are mostly trivial. Hence, adding extra software "security" to mitigate the spoofing threat would paradoxically increase vulnerability by increasing the attack surface [Manadhata and Wing 2010]. Research into spoofing countermeasures should focus instead on high value targets, such as power distribution networks (in the future), ship navigation, train collision-avoidance and secure criminal tags, and on anti-jamming technologies for aeroplane landing systems and vehicles.

6. SPOOFING COUNTERMEASURES

Many countermeasures, as summarized in Table II, have been proposed to protect against GNSS spoofing. These can be divided into four basic categories:

(1) Signal processing defenses
(2) Cryptographic defenses
(3) Correlation with other timing sources
(4) Radio spectrum and antenna defenses

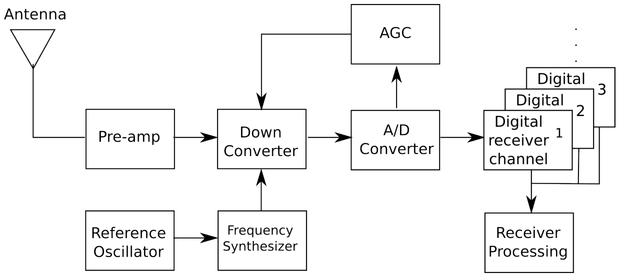

Fig. 2. Generic Digital GNSS receiver (adapted from Ward [Kaplan 1996, p.122])

6.1. Signal processing based defenses

As shown in Figure 2, there are several stages to signal processing by a digital GNSS receiver before the navigation and time solutions can be computed [Kaplan 1996]. The incoming analog RF signal from the antenna is first amplified, then down-converted to a lower frequency, and its signal strength adjusted via AGC (automatic gain control). After digital conversion, a replica PRN code, plus the computed Doppler shift (caused by the relative motion of the receiver and the satellite vehicle), is used to separate the individual satellite signals. The digital data of the individual channels, including their in-phase (I) and quadrature (Q) components (see Section 2.1) is then available for computing the navigation and time solutions. As discussed in the following sections, at various stages in this process it is possible to monitor the acquisition and tracking of signals for anomalies that may indicate a spoofing attack is in progress. These approaches differ from cryptographic and physical defences, in that they do not require physical modifications to existing equipment or signal protocols, but only the updating of the device firmware.

6.1.1. RAIM. Receiver autonomous integrity monitoring (RAIM) is the oldest and most widely used anti-spoofing strategy in GNSS receivers [Volpe 2001; Ledvina et al. 2010]. This checks all available GNSS signals for spatial consistency, and can exclude aberrant satellites [Kaplan 1996, p.306]. For example, the ephemeris data predicts the location of satellites in advance, and should closely agree with their reported position in the navigation message and external sources [Heng et al. 2014]. In the case of authentic signals, the frequency changes due to the Doppler effect, and the PRN code is delayed to maintain signal lock. A low quality spoofer might not be able to keep this correlation [Jafarnia-Jahromi 2013, p.40]. Another RAIM-like check is for clock consistency between times of other satellites not currently being tracked [Heng et al. 2014].

The basic weakness of RAIM is that it assumes any spoofing attack will be confined to one or two aberrant satellites, not an entire constellation. The owner of a timer also has no detailed knowledge of which sanity checks are performed, and hence cannot assess the degree of protection they provide [Volpe 2001; Scott 2011, p.38]. The effectiveness of RAIM can be deduced by the fact that, although RAIM countermeasures were first proposed in 1997 [Dana 1997], 20 years later several researchers reported that GNSS timers and navigation receivers could be easily spoofed [Humphreys et al. 2008; Motella et al. 2010; Shepard and Humphreys 2011].

6.1.2. Signal to interference plus noise ratio (SINR/SNR). The signal to noise ratio after processing of a given satellite signal is the ratio of the received signal strength to the noise power plus other signal interferences:

$$SINR_l^a = \frac{p_l^a}{|I_{\text{Auth}}|^2 + |I_{\text{Spoof}}|^2 + (\sigma^2/N)}$$

where I_{Auth} and I_{Spoof} are the interference components of the authentic and spoofed signals respectively, p_l^a is the authentic power of channel l and (σ^2/N) is their variance. Since the receiver has no way to distinguish interference from thermal noise, SINR is usually referred to simply as "SNR". It is used, for example, in the Sentinel network to detect jamming events [Chronos 2014]. The effectiveness of this measure for spoofing detection, however, has been questioned by McDowell [McDowell 2007] and Jafarnia [Jafarnia-Jahromi et al. 2012]. Their objection is that, although the SNR of the authentic signals increases as the spoofed signal increases in strength, once the receiver has locked onto the spoofed signals, the SNR appears normal, because the increase in noise from the legitimate signals is balanced by the greater strength of the spoofed signal [Jafarnia-Jahromi 2013, p.12].

6.1.3. Absolute Power. Absolute power monitoring [Jafarnia-Jahromi et al. 2013] involves monitoring the received signal strength (RSS) versus expected signal levels. Jafarnia [Jafarnia-Jahromi 2013] argues that using absolute power level rather than SNR considerably reduces receiver vulnerability to spoofing. Heng also concludes that raw received power, as provided by the AGC, provides a reliable means of spoofing detection with low computational complexity [Heng et al. 2014]. However, signal levels vary due to atmospheric and solar interference. They may also be changed by the AGC in the receiver (unless the changes are detected in the AGC controller itself [Akos 2012]), and only moderately increased signals levels of +1-2dB are required to execute a "lift". Also, the risk of false alarms would be a serious problem for this technique, which would be therefore limited to detecting only highly elevated signals.

6.1.4. Doppler shift detection. Due to satellites' high orbital speeds relative to a receiver, the Doppler effect: the shortening of wavelengths when moving towards, or lengthening when moving away, induces detectable effects in the received frequency of GNSS signals. These effects are normally corrected for in the receiver, and vary in a predictable way for each satellite. Hence a defence based on detecting anomalies in Doppler shift between real and simulated constellations, might be an effective spoofing detection technique. In the Volpe report [Volpe 2001] detection of such anomalies was listed as a defence, but it was also observed that simulators regularly provide control over Doppler shift. However, such simulation might leave tell-tale traces that could be used as the basis for detection, even in the case of a sophisticated spoofer [Papadimitratos and Jovanovic 2008a]. Humphreys identified two kinds of Doppler simulation: consistent Doppler attacks, where the spoofer keeps the code delay rate and frequency consistent with one another, and attack where the spoofer locks the Doppler frequency of the spoofing signal to that of the authentic signal [Humphreys 2012]. Both scenarios, however, leave strong traces of an attack such as fluctuation in signal strength caused by interactions between the spoofed and authentic signals [Jafarnia-Jahromi 2013]. This form of signal analysis, therefore, already tested in the laboratory by several researchers, seems one of the most promising detection techniques.

6.1.5. Correlation Peak Monitoring. Cavaleri investigated the feasibility of using this technique as a means of spoofing detection [Cavaleri et al. 2010]. Under the name "vestigal signal defense" (VSD) it has also been evaluated by Wesson et al. [Wesson et al. 2011] and Jafarnia [Jafarnia-Jahromi et al. 2013]. They note that to avoid detection a spoofer would require "centimeter-accurate knowledge" of the victim's antenna position, and

"100-picosecond-accurate knowledge of its processing and transmission delay". However, authentic GNSS signals frequently suffer from multipath signals reflected off buildings in a similar way to spoofed signals [Shepard and Humphreys 2011]. Wesson concludes that it is probably too difficult to distinguish the two effects in practice, and hence the risk of false alarm seems to weaken the effectiveness of this technique.

6.1.6. Clock bias monitoring. Jafarnia proposes "clock bias monitoring", or "time of arrival" (TOA) monitoring, based on the assumption that a spoofed PVT solution transmitted to a distant receiver will induce a time-offset equal to the time required to transmit the solution to the target. Even if the spoofer adds a time-offset to coincide with the target's local time, tell-tale variations in the clock bias will reveal the presence of a spoofer whenever the target receiver moves. This delay can be observed in the PRN code offset and in unusual data bit transition boundaries [Jafarnia-Jahromi 2013, p.151]. But this will only work if the target is moving in relation to the spoofer. If a limpet-spoofer is used, or the target is a fixed location receiver, such as a PMU clock, this defence will be ineffective.

6.2. Cryptographic techniques

Cryptography has often been proposed as a solution to the threat of GNSS spoofing. However, because billions of devices worldwide already use the unencrypted civilian signals, adding any form of encryption to those public protocols is not possible. As a result, the focus of research has shifted to new services, such as the GPS CNAV format, currently broadcast on L2C and L5 frequencies, and the Galileo PRS on $E6_A$ and $L1_A$ [Hein et al. 2002]. Another serious limitation is that, because of the possibility of replay attacks such as plain meaconing or SCER, cryptographic methods alone will never completely protect civilian signals.

6.2.1. Spreading code encryption (SCE). The only cryptographic technique currently in widespread use is spreading code encryption [Pozzobon 2011; Hein et al. 2007; Wullems et al. 2005], which is used exclusively in military applications. In the GPS case, the L2 and L1 frequencies are used to transmit wholly encrypted navigation data. Similar services are provided for GLONASS in the VT signal, similarly broadcast on L1 and L2, [Glonass 2008], on the Beidou2 Q code on B1 and B2 [BeiDou 2013], and in Galileo on $E6_{A,B,C}$ [Wullems et al. 2005]. Although the details of these encryption techniques are secret, and almost nothing is publicly known about the GLONASS, Beidou-2 and Galileo schemes, over the years details of how the GPS P(Y) signal is secured have emerged.

In GPS each of the 34 pre-generated W codes are 15,345,000 chips in length. Since this takes a week to transmit, a delayed meaconing or SCER attack (see Sections 3.2.1–3.2.2 above) could easily be detected. The encrypted P(Y) signal is also transmitted about 28dB below the thermal noise level of a typical receiver [Becker et al. 2009], and in order to be replayed in a SCER attack it would first have to be extracted from the noise, which requires knowledge of the secret W code [Becker et al. 2009]. The encrypted Y code is apparently modulo-2 added to the W code after encryption by a symmetric cipher [Pozzobon 2011, p.50]. The key to this cipher is changed regularly, and is transmitted to each receiver after being encrypted via the secret key contained in each military receiver. In this way lost receivers can be blacklisted, rendering them useless [Hein et al. 2007]. All of these measures, although providing a very high level of resistance to spoofing, are impractical for a civilian receiver, due to the required level of secrecy, expense, and scalability.

However, a modification of the SCE approach for civilian signals was proposed by Scott [Scott 2003], and another by Kuhn [Kuhn 2004], in which *short* sequences of spread spectrum security codes (SSSCs) are used to modify the navigation signal. In

Kuhn's scheme the key to unlock the SSSC was transmitted after a delay, designed to thwart replay attacks. However, this approach requires change to the standard signal protocols, and is thus generally regarded as impractical.

6.2.2. Navigation message authentication/encryption (NMA/NME). Most of the schemes proposed to date are based on a similar strategy of embedding a signed digest of the navigation message into the navigation message itself – the so-called navigation message authentication (NMA) [Wullems et al. 2005; Hein et al. 2007; Pozzobon 2011; Wesson et al. 2012]. NMA uses public key infrastructure (PKI) techniques to verify that the GNSS signal is genuine by embedding a signature periodically in the otherwise unencrypted navigation message. This signature is a signed digest of the ephemeris and time of week (TOW) components [Wesson et al. 2012].

The alternative NME (navigation message encryption) encrypts the entire navigation message [Hein et al. 2007]. But since this requires changes to the interface specification of GNSS signals it is thought to be impractical [Wesson et al. 2012].

NMA, on the other hand, has the advantage of allowing an uncertified receiver to read the navigation message without verification, and for a certified receiver to provide added security for a fee [Wullems et al. 2005]. For this to work, the proportion of the navigation message that contains the signature must be relatively small – no more than 10%. This places constraints on the types of algorithms used, favoring the shorter outputs of elliptic curve over the longer outputs of the DSA and RSA algorithms [Wesson et al. 2012]. Another consideration is that the computational cost of decrypting the signature cannot place too great a burden on the receiver. Since GNSS navigation signals are transmitted at a slow rate of only 25–50 bits/sec, and authentication would be required every 5 minutes or so to prevent replay attacks [Wesson et al. 2012, p.11], a short signature is needed. Wesson [Wesson et al. 2012] and Wullems [Wullems et al. 2005] suggest ECDSA or elliptic curve signature algorithm, as this has a signature size of 466 bits, when using the 233-bit Koblitz curve. A 5-bit salt transmitted along with the signed message digest makes the signature unpredictable. Although this could be replayed by an attacker after a delay, the digest is computed like a CRC over the navigation message and its embedded time data. Hence the receiver could identify that the local time offset had suddenly shifted.

A time-jump at the receiver end can, however, be avoided with a carefully crafted SCER attack. NMA encryption schemes can thus be fully circumvented [Papadimitratos and Jovanovic 2008a], although this requires sophisticated and powerful spoofing equipment [Hein et al. 2007].

Another weakness of all versions of NMA is that the loss of a single bit would lead to failure to verify. So a robust error-correction scheme would be needed.

Even the fastest authentication schemes are slow in critical safety of life (SoL) situations, such as CAT-1 landing requirements for aircraft. Wesson's signature would require 96 seconds to transmit, but in such cases 6–10 seconds is considered a suitable response time [Wullems et al. 2005].

For these reasons, although NMA is the most often preferred technique (e.g. [Wullems et al. 2005; Hein et al. 2007; Wesson et al. 2012]) it is usually recommended to be used together with direct spoofing detection techniques such as SNR, absolute received power monitoring [Hein et al. 2007; Wesson et al. 2012], or an antenna array.

6.2.3. TESLA. Other cryptographic schemes have also been suggested, most often TESLA [Perrig et al. 2002; Wesson et al. 2012], in which a sequence of MACs (message authentication codes) is encrypted by a one-way chain of keys $s_0, s_1, \ldots s_{\ell-1}, s_\ell$ such that for any intermediate key s_i:

$$F^i(s_i) = s_0$$

where F^i is the one-way function F applied i times. This has been used in the eLoran augmentation signal [Becker et al. 2009], but lacks an application in mainstream GNSS authentication. It has the advantage of small key size (around 80 bits). However, one weakness of TESLA is that the first key, s_0 could be generated by a spoofer, in which case the chain of keys derived from it would provide no protection [Lo and Enge 2010].

6.3. Correlation with Other GNSS Sources

The civilian code is usually transmitted in phase quadrature with a military code (e.g. on GPS L1), which cannot be easily spoofed. During a spoofing attack the P(Y) signal would thus be out of phase with the civilian signal, and this difference should be detectable through reference with another receiver. This approach has the advantage that it does not require modification of the signal protocols or the satellites that transmit them [Psiaki et al. 2011; Heng et al. 2013].

Psiaki [Psiaki et al. 2011], O'Hanlon [O'Hanlon et al. 2013] and Lo et al. [Lo et al. 2009; Levin et al. 2011] propose the use of a small number of secure reference receivers to verify GNSS receivers in the field. But the amount of traffic originating in the signal snapshots being sent for verification might overwhelm the references. And network-based verification might be vulnerable to common types of cyber-attack, such as man-in-the-middle, which could turn the trusted reference receiver into a spoofing source for multiple receivers. Heng varies the theme by proposing ad hoc verification via peers [Heng et al. 2013]. But this would require agreement by receiver manufacturers on the verification protocol. Also, since it involves the sending of around 1 megabit of data to each of five peers, every time a verification request is made, the threat of denial of service by misbehaving peers would be hard to prevent.

6.3.1. Correlation with Alternative Position/Timing Sources. External sources of position and timing information such as IMUs (inertial measurement units) have sometimes been suggested as a possible source for verification of the GNSS position solution [Volpe 2001; Warner and Johnston 2003; Ledvina et al. 2010], [Jafarnia-Jahromi 2013, p.9]. But such devices are often less accurate than GNSS, and tend to quickly drift from the correct values, due to accumulated errors, for them to be used to detect the slow skewing of position induced by a spoofing attack [Papadimitratos and Jovanovic 2008b]. The exception is Swaszek's successful use of an IMU in ship-based spoofing, as described in Section 4.2 above.

A general problem in providing only one form of backup is that, if GNSS and the backup disagree, which of the two should be followed? The principle of external backup works well if one solution fails outright, but not if one of them simply produces a false reading. A case in point is the grounding of the Royal Majesty mentioned above in Section 4.2, where the erroneous GPS solution was preferred by the crew over the correct eLoran one [NTSB 1997]. The same objection can be raised against the use of NTP [Garofalo et al. 2013], PTP [GAO 2013, pp.21–22] or eLoran [Carroll and Montgomery 2008] as a backup for GNSS timers. At least two additional technologies with comparable accuracies and stability would be needed for such backups to work, and that is usually impractical. The only case where it might work would be if a highly accurate local time source, such as a Caesium clock, were available [Volpe 2001], but that would be too expensive to be generally viable.

6.4. Radio Spectrum and Antenna Defences

The advantages of antenna-based defences is that they are immune to software attack, are inherently resistant to spoofing, and can be used to improve the security of existing receivers.

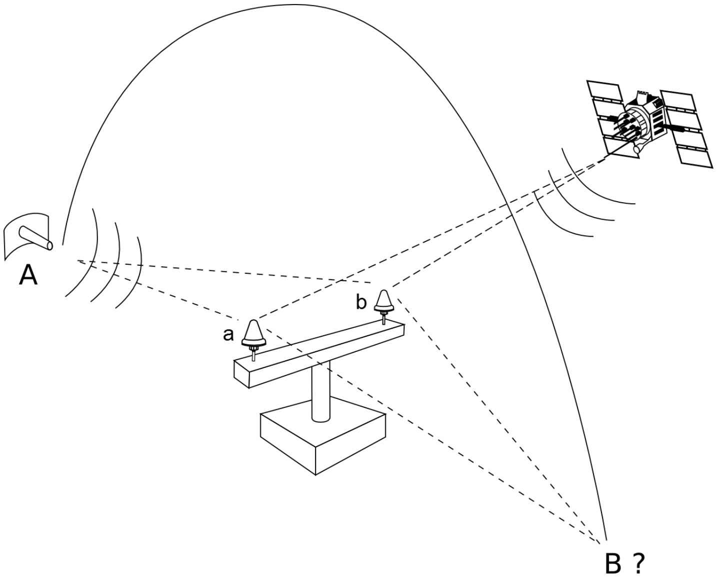

Fig. 3. The twin antenna defence

6.4.1. Angle of Arrival Discrimination. The idea of using an antenna array to distinguish spoofed from genuine GPS signals was patented by Honeywell in 1996 [Hartman 1996], and has been recently revived by Montgomery et al. [Montgomery et al. 2009]. Usually called "angle of arrival" (AOA) discrimination, it uses two antennas a short distance apart (around $10w$, where w is the wavelength), the pseudo range difference $\Delta\rho$ between the two signals received by the antennas a and b in Figure 3 is given by:

$$\Delta\rho = \frac{\Delta\phi}{2\pi}w$$

where $\Delta\phi$ is the phase difference. This allows the determination of the pointing-angle of the satellite source. The position of the spoofer at A in Figure 3 can only be estimated as being along the arc from A to B; and even assuming he/she is on the surface of the Earth, the location can still be either A or B. But all spoofed signals will likely have the same pointing angle, and not the various ones broadcast in the ephemeris. In this way a spoofing attack can be easily detected, causing an alarm to be raised to disregard readings from that timer, or a reliable backup can be used instead.

The AOA defence may only be circumvented by the placement of individual synchronized limpet-spoofers on the two antennae and controlling them via software to simulate the correct angle of arrival for all satellites in view [Humphreys et al. 2008; Ledvina et al. 2010]. This can be made more difficult by locating them on a high mast or in a secure area. Such requirements raise the bar very high for the would-be spoofer, and hence the AOA defence is regarded as very strong.

One variation of this defence is the placement of a number of detectors 20-50 metres apart at known locations, and then comparing their navigation solutions [Tippenhauer et al. 2011; Swaszek et al. 2013; Heng et al. 2014; Yu et al. 2014]. This requires more investment into defence methods that can use location information collected from multiple, preferably commercial-of-the-shelf, receivers with fixed locations. In another variation, more than two antennas may be used [Magiera and Katulski 2015].

6.4.2. Moving antennas. Various moving antennas that perform the same role as an antenna array with a single antenna [Nielsen et al. 2011], and the rapidly moving antenna [Psiaki et al. 2013] have the advantage of a simpler antenna structure to physical antenna arrays, but require mechanical motion, which may fail under stress or repeated use, and take up as much space as a static array.

Jafarnia considers various moving antenna scenarios including arbitrary movement, circular (radius less than 1.5m), random walk, constant linear speed and completely unknown motion, which are all effective, allowing not only detection of the spoofing source but also the determination of its location, revealed through exaggerated oscillations in the PVT solution [Jafarnia-Jahromi 2013].

6.4.3. Use of two different antenna types. Zhang et al. [Zhang et al. 2012] have proposed a spoofing detection technique that takes advantage of a patch and a monopole antenna. These two antennas are assumed to have complementary reception patterns, i.e. the patch antenna has a maximum at the zenith while the monopole has a minimum at that angle. But its effectiveness in detecting spoofing attacks remains unproven.

6.5. Transmitting a null back to the spoofing source

Multi-element antenna arrays have been proposed for military anti-jamming. These work by using the antennas in a closely packed array with a separation between antennas of just $\lambda/2$, where λ is the wavelength (19cm for GPS L1) [Daneshmand 2013; Magiera and Katulski 2015, p.163]. Using a matrix processing technique to filter out the jamming or interference signals from the expected legitimate signals they are able to null out the interference using the beam-forming capabilities of the array [McDowell 2007; Jafarnia-Jahromi 2013]. However, these require exact synchronization of the null signal with the incoming spoofing signal, and would appear to be illegal in many countries that regulate transmissions in the civilian GNSS bands. Also the null signal would need to have the same amplitude as the spoofing signal and would be hard to precisely focus on the spoofing source. Alternatively, multi-element antenna arrays may be used to passively filter out the jamming signal as a more viable countermeasure without any legal concerns.

7. CONCLUSION

The conclusions of this survey are first that GNSS spoofing is a *nascent* threat, not yet observed in real life situations. Nevertheless, significant potential threats exist against shipping and future Smart Grid power management systems, and lesser threats against secure criminal tags and train control systems, with some residual threat to existing mobile phone infrastructure. GNSS jamming is currently a threat to some current and future aircraft landing systems, and to truck and taxi tracking systems.

In terms of practicality, GNSS spoofing is currently hard to carry out in the field. But it is likely that, as has been seen in the development of very low-cost GNSS jammers, that eventually similarly low-cost GNSS spoofers will be developed. This may seem far-fetched, given the far greater complexity of an intermediate-level spoofer, but the complexity is largely in the software [Humphreys et al. 2008], and hand-held GPS simulators like the Cast and Aeroflex products are growing smaller [CAST 2013; Cobham 2015]. If so, our growing dependence on GNSS applications in key areas, such as the Smart Grid, may come under serious threat.

The spoofing countermeasures surveyed in Section 6 above are summarized in Table II with qualitative assessments using values ranging from low to high. However, different methods will appeal depending on the individual applications that need protecting. Where signal processing is the main line of defence, Doppler shift testing is the

Table II. Summary of Spoofing Countermeasures

Technique	**Cost**	**Effective**	**Practical**	**Tested**
Signal processing	—	—	—	—
RAIM	Low	Low	High	Yes
SNR	Low	Low	High	No
Abs. Power	Low	Med.	High	No
Doppler Shift Test	Low	High	High	Yes
Correlation Peak	High	Low	Low	Yes
Clock bias	Med.	Low	Low	No
Encryption	—	—	—	—
SCE	High	High	High	Yes
NMA	Med.	Med.	Med.	No
NME	High	Med.	Low	No
TESLA	High	Low	Low	No
Correlation	—	—	—	—
Other GNSS	Med.	High	Low	No
Non-GNSS	High	Low	Low	No
Antenna based	—	—	—	—
AOA	Med.	Very High	High	Yes
Moving	Med.	Med.	Low	No
Two different	Med.	Low	Low	No
Transmit null	High	Low	Low	No

most highly rated and has been tested. RAIM or consistency checks on GNSS signals no longer suffice, and although they should not be discontinued, the spoofing threat has now moved on from the forgery of individual satellites to entire constellations. Cryptographical defences mostly do not suffice for civilian use; they remain unproven and incomplete, although the military grade SCE technique is highly effective. Among the remaining defences the angle of arrival (AOA) defence is assessed highest on practicality and effectiveness, and recent work suggests that this approach is undergoing a something of a revival [Montgomery et al. 2009; Daneshmand 2013; Magiera and Katulski 2015].

7.1. Future work

One of the main functions of a survey is to determine the best directions for future research. The areas least covered and most significant are firstly the development of sensor networks to detect spoofing and jamming events. But these must be redesigned to locate spoofers and jammers in real time, which would make them a very effective defence in their own right. Other areas that have not received much attention include the spoofing threats against shipping, secure criminal tags and train guidance systems. Finally, crucial to the development of the field is the development of low-cost, portable, multi-GNSS receiver-spoofers. These are needed to test existing and new equipment for spoofing resistance. Currently attacks in the laboratory are only possible against GPS receivers, and increasingly the GNSS market is moving rapidly towards multi-constellation receiver design to take advantage of the increasing variety and stability of modern GNSS services. Without these further developments critical infrastructure and safety of life situations will be vulnerable to GNSS spoofing attacks.

ACKNOWLEDGMENTS

This work was supported in part by Australian Research Council Linkage Grant LP120200246, Practical Cyber Security for Next Generation Power Transmission Networks.

REFERENCES

ABC. 2013. GPS System Monitors Parolees 24/7. (May 2013). http://abcnews.go.com/Primetime/story?id=132116

ACMA. 2013. Mobile phone & GPS jamming devices FAQ. (November 2013). http://www.acma.gov.au/theACMA/ACMAi/Complants/iFAQS/faqs-mobile-phone-and-gps-jamming-devices-acma

ACMA. 2014. Taxi driver convicted. (2014). http://www.acma.gov.au/Citizen/Consumer-info/All-about-spectrum/High-risk-devices/taxi-driver-convicted

Airservices. 2014. GBAS implementation program. (2014). http://www.airservicesaustralia.com/projects/ground-based-augmentation-system-gbas/gbas-implementation-program/

Ilge Akkaya, Edward A. Lee, and Patricia Derler. 2013. Model-Based Evaluation of GPS Spoofing Attacks on Power Grid Sensors. In *Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. IEEE, Berkeley CA, 1–6.

Dennis M. Akos. 2012. Who's Afraid of the Spoofer? GPS/GNSS Spoofing Detection via Automatic Gain Control (AGC). *Journal of Navigation* 59, 4 (Winter 2012), 281–290.

AMSA. 2013. Differential Global Positioning System. (2013). http://www.amsa.gov.au/navigation/services/dgps/

Galina S. Antonova, Alex Apostolov, Doug Arnold, Stephan Bedrosian, and Christoph Brunner. 2013. Standard Profile for Use of IEEE Std 1588-2008 Precision Time Protocol (PTP) in Power System Applications. In *66th Annual Conference for Protective Relay Engineers*. IEEE, College Station, TX, 1–6.

ASKA. 2012. Parallel Generators and Synchronization, Generator Power System Design. Electronic. (2012). http://www.aksapowergen.com/pdf/other/Parallel+Generators+Synchronization.pdf

George T. Becker, Sherman Lo, David Di Lorenzo, Di Qiuand Christof Paar, and Per Enge. 2009. Efficient authentication mmechanism for navigation systems – a radio-navigation case study. In *Proceedings of the ION GNSS Meeting*. ION, Savannah, GA, 901–912.

BeiDou. 2013. *BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal (Version 2.0)*. Technical Report. China Satellite Navigation Office.

John Betz. 2002. Binary Offset Carrier Modulations for Radionavigation. *Journal of the Institute of Navigation* 48, 4 (2002), 227–246s.

Blutag. 2012. How to bypass House Arrest Ankle Monitor. Electronic. (2012). http://www.digitaltechnologies-2000.com/how-to-bypass-house-arrest-ankle-bracelet/

Holly Borowski, Oskar Isoz, Fredrik Marsten Eklöf, Sherman Lo, and Dennis Akos. 2012. Detecting False Signals With Automatic Gain Control. *GPS World* April 1 (2012), online.

Broadcom. 2008. *Ethernet Time Synchronization*. White paper. Broadcom. http://www.broadcom.com/collateral/wp/StrataXGSIV-WP100-R.pdf.

Alison Brown, Jarrett Redd, and Michael Dix. 2013. *Open Source Software Defined Radio Platform for GNSS Recording and Simulation*. Technical Report. NAVSYS Corporation. http://www.navsys.com/Papers/13-09-001_Open_Source_SDR_Platform_for_GNSS_Recording_and_Simulation.pdf.

James Carroll and Kirk Montgomery. 2008. Global Positioning System Timing Criticality Assessment – Preliminary Performance Results. In *40th Annual Precise Time and Time Interval (PTTI) Meeting*. John A. Volpe National Transportation Systems Center, Cambridge, MA, 484–505.

CAST. 2013. CAST-SGX GPS Satellite Simulator. (2013). http://www.castnav.com/cast_pdf/CASTSGX.pdf

Antonio Cavaleri, Beatrice Motella, Marco Pini, and Maurizio Fantino. 2010. Detection of Spoofed GPS Signals at Code and Carrier Tracking Level. In *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE, Noordwijk, 1–6.

Ran Chengqi. 2012. *Global Navigation Satellite Systems*. The National Academies Press, Washington, D.C., Chapter Development of the Beidou Navigation Satellite System, 28–33.

Chronos. 2013. *CTL3520 GPS Jammer Detector & Locator*. GPS World. http://www.chronos.co.uk/files/pdfs/ctl/ctl3520.pdf

Chronos. 2014. *Sentinel Project Report on GNSS Vulnerabilities*. Technical Report. Chronos Technology. http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf.

Cobham. 2015. GPSG-1000 GPS/Galileo Portable Positional Simulator. (2015). http://www.arsitec.com.br/pdfs/GPSG-1000is.pdf

Karen Collier and Amelia Harris. 2013. Taxi cheats using GPS jammers to steal fares. (November 2013). http://www.heraldsun.com.au/news/law-order/taxi-cheats-using-gps-jammers-to-steal-fares/story-fni0fee2-1226756138559

Peter H. Dana. 1997. Global Positioning System (GPS) Time Dissemination for Real-Time Applications. *Real-Time systems* 12 (1997), 9–40.

Saeed Daneshmand. 2013. *GNSS Interference Mitigation Using Antenna Array Processing*. Ph.D. Dissertation. University of Calgary, School of Engineering.

Dicom. 2014. *GTR51 - Time and frequency transfer GNSS receiver*. Dicom. http://www.dicom.cz/en/product/1650-time-and-frequency-transfer-gnss-receiver

A.J.Van Dierendonck. 2012. *Global Navigation Satellite Systems*. The National Academies Press, Washington, D.C., Chapter Impact of International, Low Power, In-Band, Personal Privacy Device (PPDs) on Aviation, 147–152.

Michael Dimino. 1999. Telephone operable global tracking system for vehicles. Patent US 5918180 A. (1999).

DOD. 2008. *Global Positioning System Standard Positioning Service Performance Standard 4th Edition*. Technical Report. U.S. Department of Defense. http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

Economist. 2011. No jam tomorrow. *The Economist* Q1 (March 2011), 1–6. http://www.economist.com/node/18304246.

Abdelsalam M. Elhaffar. 2008. *Power Transmission Line Fault Location Based on Current Traveling Waves*. Ph.D. Dissertation. Helsinki University of Technology.

ENISA. 2006. *Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs) Deliverable 2 Final version Version 1.0*. Technical Report. ENISA. http://www.enisa.europa.eu/act/rm/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes/at_download/fullReport.

ETSI. 1996. *GSM Technical Specification GSM 05.10*. Technical Report. European Telecommunications Standards Institute. http://www.etsi.org/deliver/etsi_gts/05/0510/05.00.00_60/gsmts_0510v050000p.pdf.

Jean-Loup Ferrant, Mike Gilson, Sebastien Jobert, Michael Mayer, Laurent Montini, Michel Ouellette, Silvana Rodrigues, and Stefano Ruffini. 2013. *Synchronous Ethernet and IEEE 1588 in Telecoms*. Wiley, Hoboken, NJ.

Susan A. Fleming. 2013. Positive Train Control: Additional Authorities Could Benefit Implementation. (Sept 2013). http://www.gao.gov/products/GAO-13-720

Börje Forssell. 2009. The dangers of GPS/GNSS. *Coordinates* V, 2 (February 2009), 6–8.

Giulio Gabelli, Ediz Cetin, Ryan J. R. Thompson, Andrew G. Dempster, and Giovanni E. Corazza. 2013. GNSS Signal Cancellation for Enhanced Interference Detection and Localization. In *International Global Navigation Satellite Systems Society IGNSS Symposium*. IGNSS, Gold Coast, 1–15.

Galileo. 2010. *European GNSS (Galileo) Open Service Signal in Space Interface Control Document*. Technical Report. European Union and European Space Agency.

GAO. 2013. *Report to Congressional Requesters: GPS Disruptions*. Technical Report. United States Government Accountability Office. http://www.gao.gov/assets/660/658792.pdf

Alessia Garofalo, Cesario Di Sarno, Luigi Coppolino, and Salvatore D'Antonio. 2013. A GPS Spoofing Resilient WAMS for Smart Grid, In EWDC 2013, M. Vieira and J.C. Cunha (Eds.). *LNCS* 7869 (2013), 134–147.

GBAS Working Group. 2013. GBAS approach and landing systems. Electronic. (2013). http://flygls.net/

Jay Giri, David Sun, and Rene Avila-Rosales. 2009. Enhancing Grid Reliability and Stability with a Better, Smarter, Faster Control System Is the Key to Avoiding Total System Collapse. *IEEE power & energy magazine* March/April (2009), 35–40.

Glonass. 2008. *Global Navigation Satellite System GLONASS Interface Control Document Navigational Radiosignal in Bands L1, L2*. Technical Report. Russian Institute of Space Device Engineering, Moscow.

GPO. 2008. FEDERAL RAIL SAFETY IMPROVEMENTS PUBLIC LAW 110–432OCT. 16, 2008. GPO. (2008). https://www.fra.dot.gov/eLib/Details/L03588.

GPS. 1995. *Global Positioning System Standard Positioning Service Signal Specification*. Technical Report. Global Positioning System. http://www.gps.gov/technical/ps/1995-SPS-signal-specification.pdf.

GPS.GOV. 2013a. Information About GPS Jamming. (2013). http://www.gps.gov/spectrum/jamming/

GPS.GOV. 2013b. New Civil Signals. (2013). http://www.gps.gov/systems/gps/modernization/civilsignals/

GPS.GOV. 2014. GPS Accuracy. (18 September 2014). http://www.gps.gov/systems/gps/performance/accuracy/

Anthony Grillo and John P. Veschi. 1999. GPS restraint system and method for confining a subject within a defined area. US Patent 6232916 B1. (Aug 1999). http://www.google.com.au/patents/US6232916

Christoph Günter. 2014. A Survey of Spoofing and Counter-Measures. *Navigation* 6, 3 (2014), 159–177.

Randolph G. Hartman. 1996. Spoofing Detection System for a Satellite Positioning System. (17 Sept. 1996).

Gunter W. Hein, Jose-Angel Avila-Rodríguez, Stefan Wallner, John W. Betz, Chris J. Hegarty, Joseph Rushanan, Andrea L. Kraay, Anthony R. Pratt, Lt Sean Lenehan, John Owen, Lean-Luc Issler, and

Thomas A. Stansell. 2006. MBOC: The New Optimized Spreading Modulation Recommended for Galileo L1 OS and GPS L1C. *Inside GNSS* May/June 2006 (May/June 2006), 57–66.

Günter W. Hein, Jeremie Godet, Jean-Luc Issler, Jean-Christophe Martin, Phillipe Erhard, Rafael Lucas-Rodriguez, and Tony Pratt. 2002. Status of Galileo Frequency and Signal Design. In *Proc. ION GPS*. ION, Portland, Oregon, 34–37.

Gunter W. Hein, Felix Kneissl, Jose-Angel Avila-Rodriguez, and Stefan Wallner. 2007. Authenticating GNSS Proofs against Spoofs Part 2. *Inside GNSS* September/October 2007 (September/October 2007), 71–78.

Liang Heng, Jonathan J. Makela, Alejandro D. Dominguez-Garcia, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao. 2014. Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture. In *IEEE Power and Energy Conference at Illinois*. IEEE, Champaign, IL, USA, 1–7.

Liang Heng, Daniel B. Work, and Grace Xingxin Gao. 2013. Cooperative GNSS Authentication Reliability from Unreliable Peers. *Inside GNSS* Sept/Oct (2013), 70–75.

Todd Humphreys. 2012. Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV. (2012). http://www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav

Todd Humphreys. 2013a. Detection Strategy for Cryptographic GNSS Anti-Spoofing. *IEEE Trans. Aerospace Electron. Systems* 49, 2 (April 2013), 1073–1090.

Todd Humphreys. 2013b. Researchers Steer Off Course to Show Potential Power of 'GPS Spoofing'. (August 2 2013). http://www.pbs.org/newshour/bb/science-july-dec13-gps_08-02/

Todd Humphreys. 2013c. UT Austin Researchers Spoof Superyacht at Sea. (2013). http://www.engr.utexas.edu/features/superyacht-gps-spoofing

Todd Humphreys and Brent M. Ledvina. 2010. The GPS Assimilator Upgrading Receivers via Benign Spoofing. *InsideGNSS* June (2010), 50–58.

Todd E. Humphreys, Brent M. Ledvina, Mark L. Psiaki, Brady O'Hanlon, and P. M. Kintner Jr. 2008. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *Proceedings of ION GNSS Conference*. ION, Savanna, GA, 2314–2325.

Todd E. Humphreys, Mark L. Psiaki, and Paul M. Kintner. 2006. GNSS Receiver Implementation on a DSP: Status, Challenges, and Prospects. In *Proceedings ION GNSS Conference Fort Worth, TX, September 26–29*. ION, Fort Worth, TX, 2370–2382.

Michaël Hurtgen and Jean-Claude Maun. 2012. *Applications of PMU measurements in the Belgian electrical grid*. Technical Report. Belgian Federal Government. http://economie.fgov.be/nl/binaries/20120420_PMU_Final_Report_tcm325-200078.pdf.

Nick Hyde. 2012. Apple Maps gets drivers lost in Australian outback, police warn. (11 December 2012). http://www.cnet.com/au/news/apple-maps-gets-drivers-lost-in-australian-outback-police-warn/

IEEE. 2002. *IEEE P1547/ D10 Draft Standard for Interconnecting Distributed Resources with Electric Power Systems*. Technical Report. IEEE. http://dg.raabassociates.org/Articles/Draft_IEEE_\%20P1547.pdf.

IEEE. 2011. IEEE Std C37.118.2-2011 IEEE Standard for Synchrophasor Data Transfer for Power Systems. (7 December 2011).

IMO. 2004. International Convention for the Safety of Life at Sea. Online. (1 July 2004). http://www.imo.org/Publications/Documents/Newsletters\%20and\%20Mailers/Mailers/IF110E.PDF

Oscar Isoz, Denis Akos, Tore Lindgren, Chih-Cheng Sun, and ShauShiun Jan. 2011. Assessment of GP L1/Galileo E1 Interference Monitoring System for the Airport Environment, In Proceedings of Institute of Navigation GNSS. *ION GNSS* (Sept. 19-23 2011), 1920–1930.

Ali Jafarnia-Jahromi. 2013. *GNSS Signal Authenticity Verification in the Presence of Structural Interference*. PhD Thesis. Department of Geomatics Engineering, University of Calgary.

Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, and Géard Lachapelle. 2012. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation* 2012 (2012), 1–16.

Ali Jafarnia-Jahromi, Saeed Daneshmand, and Gérard Lachapelle. 2013. Spoofing Countermeasure for GNSS Receivers – a Review of Current and Future Research Trends. In *4th International Colloquium on Scientific and Fundamental Aspects of the Galileo Programme European Space Agency, Prague, 4-6 December*. ESA, Prague, 1–8.

JFC. 2014. Jammer from China. Electronic. (2014). http://www.jammerfromchina.com/categories/GPS_Jammers/

Shengyue Ji, Wu Chen, Xiaoli Ding, Yongqi Chen, Chunmei Zhao, and Congwei Hu. 2010. Potential Benefits of GPS/GLONASS/GALILEO Integration in an Urban Canyon – Hong Kong. *The Journal of Navigation* 63 (2010), 681–693.

Xichen Jiang, Brian J. Harding, and Alejandro D. Domínguez-García. 2013. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Transactions on Power Systems* 28, 3 (2013), 3253–3262.

Chen Jinping. 2012. *Global Navigation Satellite Systems*. The National Academies Press, Washington, DC, Chapter Analysis of the GNSS Augmentation Technology Architecture, 139–144.

Shenzen Juneo. 2015. Shenzen Juneo Technology Limited TK106. (2015). http://www.tkstargps.com/ProductShow.asp?ID=181 Accessed 24/8/2015.

Hee Jung, Mark L. Psiaki, and Stephen P. Powell. 2003. Kalman-Filter-Based Semi-Codeless Tracking of Weak Dual-Frequency GPS Signals. In *ION GPS / GNSS*. ION, Portland, Oregon, 2515–2523.

Elliot D. Kaplan. 1996. *Understanding GPS Principles and Applications*. Artech House, Norwood, Mass.

Gorkem Kar, Hossen Mustafa, Yan Wang, Yingying Chen, Wenyuan Xu, Marco Gruteser, and Tam Vu. 2014. Detection of On-Road Vehicles Emanating GPS Interference. In *CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Scottsdale, Arizona, USA, 621–632.

Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. 2013. Unmanned Aircraft Capture and Control via GPS Spoofing. (2013). http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf

Alfred Kleusberg. 2003. *Geodesy – The Challenge of the Third Milennium*. Springer, Heidelberg, Chapter Analytical GPS Navigation Solution, 93–96.

Hiroaki Koshima and Joseph Hoshen. 2000. Personal locator services emerge. *Spectrum, IEEE* 37, 2 (2000), 41–48.

Marcus G. Kuhn. 2004. An Asymmetric Security Mechanism for Navigation Signals. *LNCSS* 3200 (2004), 239–252.

Boris Landoni. 2011. Mini GSM Localizer with GPS. Electronic resource. (June 2011). http://www.open-electronics.org/mini-gsm-localizer-without-gps/.

Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Isaac Miller. 2010. *An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers*. Technical Report. Institute of Navigation ITM. http://www.coherentnavigation.com/~ledvina/wp-content/uploads/2012/07/inline_antispoofing.pdf.

Peter Levin, David S. De Lorenzo, Per K. Enge, and Sherman C. Lo. 2011. Authenticating a Signal Based on an Unknown COmponent Thereof. United States Patent 7,969,354 B2. (June 2011).

Sherman Lo and Per Enge. 2010. Authenticating Aviation Augmentation System Broadcasts. In *Proceedings of IEEE / ION Position Location and Navigation Symposium (PLANS)*. IEEE, Palm Springs, CA, 708–717.

Sherman Lo, David De Lorenzo, Per Enge, Dennis Akos, and Paul Bradley. 2009. Signal Authentication A Secure Civil GNSS for Today. *Inside GNSS* September/October (September/October 2009), 30–39.

Michael A. Lombardi, Lisa M. Nelson, Andrew N. Novick, and Victor S. Zhang. 2001. Time and Frequency Measurements Using the Global Positioning System. *The International Journal of Metrology* 8, 3 (Jul.-Sept. 2001), 26–33.

Jaroslaw Magiera and Ryszard Katulski. 2015. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology* 131, 1 (2015), 45–57.

Pratyusa K. Manadhata and Jeanette M. Wing. 2010. An Attack Surface Metric. *IEEE Transactions on Software Engineering* XX, X (2010), 1–17.

Paul Marks. 2013. Radar gun spots vehicles with illegal GPS jammers. (August 2013). http://www.newscientist.com/article/dn23984-radar-gun-spots-vehicles-with-illegal-gps-jammers.html

Charles E. McDowell. 2007. GPS Spoofer and Repeater Mitigation System Using Spatial Nulling. Patent. (July 2007).

Meinberg. 2015. Manual LANTIME NTP Server (FW LTOS 6.16). (2015).

MeitrackUSA. 2015. Meitrack MVT100. (2015). http://www.meitrackusa.com/trackers/gps-vehicle-trackers/mvt100 Accessed 24/8/2015.

Katina Michael, Andrew McNamee, and MG Michael. 2006. The Emerging Ethics of Humancentric GPS Tracking and Monitoring. In *Proceedings of the International Conference on Mobile Business (ICMB'06)*. IEEE, Copenhagen, 34.

MightyGPS. 2009. Ankle Bracelet GPS Tracker. Online. (2009). www.mightygps.com/Ankle_GPS_tracker.htm

Paul Y. Montgomery, Todd E. Humphreys, and Brett M. Ledvina. 2009. A Multi-Antenna Defense Receiver-Autonomous GPS Spoofing Detection. *Inside GNSS* March/April (2009), 40–46.

Beatrice Motella, Marco Pini, Maurizio Fantino, and Paolo Mulassano. 2010. Performance Assessment of Low Cost GPS Receivers Under Civilian Spoofing Attacks. In *Proceedings of Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop*. IEEE, Noordwijk, 1–8.

Navstar. 2006. *Navstar Global Positioning System Interface Specification IS-GPS-200 Revision D*. Technical Report. GPS Joint Program Office. http://www.losangeles.af.mil/shared/media/document/AFD-070803-059.pdf.

NERC. 2012. *Extended loss of GPS Impact on Reliability*. Technical Report. North American Electric Reliability Corporation. http://www.nerc.com/docs/escc/PNT\%20-\%20Power\%20Systems\%20V19.pdf.

John Nielsen, Ali Broumandan, and Gérard Lachapelle. 2011. GNSS Spoofing Detection for Single Antenna Handheld Receivers. *Navigation* 58, 4 (2011), 335–344.

Tyler Nighswander, Brent Ledvina, Johnathan Diamond, Robert Brumley, and David Brumley. 2012. GPS Software Attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. ACM, Raleigh, NC, 450–461.

JSC NIIAS. 2015. JSC NIIAS Research & Design Institute for Information Technology, Signalling and Telecommunications on Railway Transport. (2015). http://www.vniias.ru/en/images/stories/docs/niias_brochure_en.pdf

NIST. 2012. *Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1*. Technical Report. National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NTSB. 1997. *Grounding of the Panamanian Passenger Ship Royal Majesty on Rose and Crown Shoal near Nantucket, Massachusetts June 10, 1995*. Technical Report. National Transportation Safety Board. http://www.ntsb.gov/doclib/reports/1997/mar9701.pdf.

Brady W. O'Hanlon, Mark L. Psiaki, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. 2013. Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals. *Navigation* 60, 4 (2013), 267–278.

Jorge L. Olenewa. 2014. *Guide to Wireless Communications, Third Edition*. Cengage Learning, Boston, USA.

Mario Paolone, Alberto Borghetti, and Carlo A. Nucci. 2009. Development of an RTU for Synchrophasors Estimation in Active Distribution Networks. In *IEEE BucharestPower Tech Conference*. PowerTech, Bucharest, 1–6.

Panagiotis Papadimitratos and Aleksander Jovanovic. 2008a. GNSS-based Positioning: Attacks and Countermeasures, In IEEE Military Communications Conference (MILCOM 2008), San Diego, CA,. *CoRR* (Nov 16-19 2008), 3168–3174.

Pangiotis Papadimitratos and Aleksander Jovanovic. 2008b. Protection and Fundamental Vulnerability of GNSS. In *IEEE International Workshop on Satellite and Space Communications (IWSSC), Toulouse, France, October 1-3*. IEEE, Toulouse, 167–171.

Brian K. Payne, David C. May, and Peter B. Wood. 2014. The 'pains' of electronic monitoring: a slap on the wrist or just as bad as prison? *Criminal Justice Studies* 27, 2 (2014), 133–148.

Adrian Perrig, Ran Canetti, Doug Tygar, and Dawn Song. 2002. The TESLA Broadcast Authentication Protocol. *CryptoBytes* 5, 2 (Summer/Fall 2002), 2–13.

Scott Peterson and Payam Faramarzi. 2011. Iran hijacked US drone, says Iranian engineer. (December 11 2011). http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video

IIvan Petrovski and Takuji Ebinuma. 2010. Everything You Always Wanted to Know About GNSS Simulators But Were Afraid to Ask. *Inside GNSS* September (2010), 48–58.

PNT. 2010. *National PNT Advisory Board comments on Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures*. White paper. National Space-Based Positioning, Navigation, and TIming (PNT) Advisory Board. http://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf

Oscar Pozzobon. 2004. Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services. *Journal of Global Positioning Systems* 3, 1–2 (2004), 200–207.

Oscar Pozzobon. 2011. Keeping the Spoofs Out Signal Authentication for Future GNSS. *Inside GNSS* May/June (2011), 48–56.

Mark L. Psiaki, Barry W. O'Hanlon, Jahshan A. Bhatti, Daniel P. Shepard, and Todd E. Humphreys. 2011. GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals. *Transactions on Aerospace and Electronic Systems* 49, 4 (2011), 2250–2267.

Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon. 2013. Correlating Carrier Phase with Rapid Antenna Motion. *GPS World* June 1 (2013), online. http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

Rama Rao, Eddie N. Rosario, and Robert J. Davis. 2006. Radiation pattern analysis of aircraft mounted GPS antennas and verification through scale model testing. In *Proceedings of the IEEE/ION PLANS Meeting*. IEEE/ION, Coronado, CA, 306–318.

RAoE. 2011. *Global Navigation Space Systems: reliance and vulnerabilities*. Technical Report. The Royal Academy of Engineering. http://www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf.

Schweitzer. 2014. SEL-3378 Synchrophasor Vector Processor. Web page. (2014). www.selinc.com/sel-3378

Schweizer. 2015. Dependable Communications for Critical Infrastructure. Electronic. (2015). https://www.selinc.com/ICON/

Logan Scott. 2003. Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems. In *Proceedings of the Institute of Navigation GPS/GNSS Conference*. ION, Portland, OR, 1543–1552.

Logan Scott. 2011. Receiver Certification: Making the GNSS Environment Hostile to Jammers & Spoofers. Electronic. (2011). http://www.gps.gov/governance/advisory/meetings/2011-11/scott.pdf

Daniel P. Shepard and Todd E. Humphreys. 2011. Characterization of Receiver Response to Spoofing Attacks. In *Proceedings of the ION GNSS Meeting Portland, Oregon*. ION, Portland, Oregon, 2608–2618. http://radionavlab.ae.utexas.edu/images/stories/files/papers/spcharION2011.pdf.

Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. 2012. Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks. *International Journal of Critical Infrastructure Protection* 5, 3–4 (2012), 146–153.

Peter F. Swaszek, Richard J. Hartnett, Matthew V. Kempe, and Gregory W. Johnson. 2013. Analysis of a Simple, Multi-Receiver GPS Spoof Detector . In *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*. ION, San Diego, California, 884–892.

Peter F. Swaszek, Scott A. Pratz, Benjamin N. Arocho, Kelly C. Seals, and Richard J. Hartnett. 2014. GNSS Spoof Detection Using ShipboardIMU Measurements. In *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (IONGNSS+)*. ION, Tampa, Florida, 745–758.

Symmetricom. 2014. *XLi Time and Frequency System Data Sheet*. Symmetricom. http://www.microsemi.com/products/timing-synchronization-systems/time-frequency-distribution/gps-instruments/xli.

Michael J. Thompson. 2012. Fundamentals and Advancements in Generator Synchronizing Systems. In *65th Annual Conference for Protective Relay Engineers*. IEEE, College Station, TX, 203–214. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6201234

Nils Ole Tippenhauer, Christina Pöpper, Kaspar B. Rasmussen, and Srdjan Capkun. 2011. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS '11)*. ACM, Chicago, Illinois, 75–86.

Trimble. 2013. *Resolution SMT GG Multi-GNSS Timing Module User Guide*. Trimble Navigation Limited, Sunnyvale, CA.

U-blox. 2013. AMY-5M: world's smallest GPS receiver module. (2013). http://www.u-blox.com/en/amy-5m.html

US-Cert. 2015. Advisory (ICSA-14-345-01) Arbiter Systems 1094B GPS Clock Spoofing Vulnerability. (January 2015). https://ics-cert.us-cert.gov/advisories/ICSA-14-345-01

Sandra Verhagen and Peter J.G. Teuissen. 2013. Ambiguity resolution performance with GPS and BeiDou for LEO formation flying. *Advances in Space Research* 54, 5 (2013), 830–839.

Volpe. 2001. *Vulnerability assessment of the transportation infrastructure relying on the global positioning system. Final Report, 2001*. Technical Report. John A. Volpe National Transportation Systems Center.

Jon S. Warner and Roger G. Johnson. 2002. A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing. *The Journal of Security Administration* 25 (2002), 19–28.

Jon S. Warner and Roger G. Johnston. 2003. GPS Spoofing Countermeasures. Electronic. (2003). http://www.ne.anl.gov/capabilities/vat/pdfs/GPS-Spoofing-CMs-\%282003\%29.pdf

Marc Weiss. 2012. Telecom Requirements for Time and Frequency Synchronization. Electronic. (2012). http://www.gps.gov/cgsic/meetings/2012/weiss1.pdf

Mark Weiss. 2013. GPS Vulnerability in Mobile Networks. Electronic. (2013). http://www.gps.gov/multimedia/presentations/2013/12/MNSS/weiss.pdf

Kyle Wesson, Mark Rothlisberger, and Todd Humphreys. 2012. Practical Cryptographic Civil GPS Signal Authentication, In Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation. *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation* (September 2012), 3335–3345.

Kyle Wesson, Daniel Shepard, Jahshan Bhatti, and Todd E. Humphreys. 2011. An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing. In *ION GNSS Conference Portland, OR, September 21–23*. ION, Portland, Oregon, 1–11.

Chuck Wheatley. 1999. Self-synchronizing a CDMA cellular network. *Microwave Journal* May 1 (1999), 320–328.

Dale Williston and Dale Finney. 2011. *Consequences of Out-of-Phase Reclosing on Feeders With Distributed Generators*. Technical Report. Schweitzer Engineering Laboratories, Inc. http://grouper.ieee.org/groups/scc21/1547.8/email/pdfX2pEArHjt0.pdf.

Allen J. Wood, Bruce F. Wollenberg, and Gerald B. Sheblé. 2014. *Power Generation, Operation and Generation, Third Edition*. Wiley, Hoboken, NJ.

Willian Wright, Michael Russell, and John Brockhaus. 2011. Myth Busted: Civilian receivers actually do have access to the L2 Frequency. *Army Space Journal* Fall/Winter (2011), 46–47. http://www.dtic.mil/dtic/tr/fulltext/u2/a538975.pdf

Chris Wullems, Oscar Pozzobon, and Kurt Kubik. 2005. Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems. In *Proceedings of the European Navigation Conference GNSS*. EUGIN, Munich, 1–10.

Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, and David Basin. 2014. Short Paper: Detection of GPS Spoofing Attacks in Power Grids. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*. ACM, Oxford, 99–104.

Sandra Zaragoza. 2013. Spoofing a Superyacht at Sea. (July 2013). http://www.utexas.edu/know/2013/07/30/spoofing-a-superyacht-at-sea/

Zhenghao Zhang, Matthew Trinkle, Lijun Qian, and Husheng Li. 2012. Quickest Detection of GPS Spoofing Attack. In *Military Communications Conference*. IEEE, Orlando, FL, 1–6.