Spoofing and Jamming of GNSS Signals: Are They Real and What Can We Do About Them?

R. W. Meggs* CEng, MIMarEST, SMIEEE
R. J. Watson**, MIEEE.
** BMT, UK*
*** University of Bath, UK.*
* Corresponding Author - email: robert.meggs@bmtglobal.com

Synopsis

Put simply, ‘spoofing’ is a means of controlling the reported position and time of a GNSS receiver. Spoofing has now been well demonstrated in the experimental context, but until a few years ago it was regarded as “…a bit like UFOs: much speculation, occasional alarms at suspected instances, but little real-world evidence of its existence” (Ref. 1). In the intervening years spoofing has transformed from a research laboratory into an emerging threat. In this paper we focus on radio-frequency attack as the primary method of spoofing. However there is also the possibility of cyber-attack on GNSS systems, in which there is interception and modification of computed position between the receiver and application. It had perhaps previously been considered that the technology and know-how “barrier to entry” to produce an effective spoofer was itself a significant deterrent. However, the commercial availability of inexpensive (sub £250) software defined radio systems, low-cost computing and open-source GNSS signal generator software has all but eliminated this barrier. This paper will consider various methods of spoofing, means of detecting spoofing through analysis of signal anomalies and also mitigation of spoofing at the physical layer via the antenna and signal processing and at the software application layer through the detection of anomalies.

Keywords: Satellite navigation, jamming, denial of service, radio frequency, ship systems, safety.

1. Introduction

It can be argued that the first Global Navigation Satellite System (GNSS) system was the United States’ Global Positioning System (GPS), development of which began in the late 1960s. GPS became fully operational in 1995. Since then other GNSS have been, or are being, deployed, including GLONASS (Russia), Galileo (Europe) and Beidou (China). Although GPS was originally intended as a military position, navigation and timing (PNT) tool, a substantial civilian user base has grown, not least in the maritime sector.

All GNSS depend on ranging measurements made between the user equipment (receivers) and the satellites. Although the strength of the GNSS signals received at Earth’s surface is very low, in the order of -160 dBW, the codes used to modulate the ranging signals are generally very robust and hence GNSS systems have good immunity to swamping by strong local sources.

Nevertheless, there are certain phenomena, both natural and man-made, that can disrupt the computation of the PNT solution. For example, it has been shown that ionospheric scintillation associated with auroral activity in high latitudes can cause a GNSS receiver to lose signal lock (Ref. 2). Unintended man-made phenomena, such as multipath interference due to the proximity of multiple reflecting surfaces, can also lead to a loss of the PNT solution. The focus of this paper, however, is not on naturally occurring phenomena, but on the intentional and deliberate denial or falsification of GNSS signals for nefarious purposes.

It turns out to be relatively easy to jam the GNSS signals. Jamming is a ‘blunt instrument’ attack that seeks to swamp legitimate GNSS signals so that receivers are unable to compute a valid PNT solution. It is easily achieved by using wide-bandwidth signal, centred on the GNSS carrier frequencies and of a strength that exceeds that of the legitimate signals. A successful jamming attack on a vessel at sea was demonstrated, in controlled circumstances, off Flamborough Head by the General Lighthouse Authority in 2008 (Ref. 3).

Author’s Biographies

Dr Bob Meggs is a Senior Engineer at BMT Defence and Security in Bath, UK. He has a background in both Radio-Frequency (RF) and Electrical Engineering. Before joining BMT in 2009, he was a Research Officer at the University of Bath supporting research into loss of lock in GNSS receivers due to ionospheric phase and amplitude scintillation in high geographic latitudes. He also developed methods to support transionospheric radio propagation studies by forecasting the temporal and spatial evolution of ionospheric electron density over short timescales. In his current role at BMT he has conducted a number of consultancy tasks on emerging technologies for marine power systems and has participated in concept designs for surface ships and submarines. He was also lead electrical engineer for the basic design phase of the UK’s Tide Class fleet tankers for the Royal Fleet Auxiliary.

Dr Robert Watson is a Senior Lecturer (Associate Professor) at the University of Bath, UK. He obtained BEng and PhD degrees in electronic engineering from the University of Essex, in 1992 and 1996 respectively and has since been involved with a number of electromagnetic scattering, radio propagation and radar systems projects. Since 2010 he has been an Associate Editor of the American Geophysical Union’s Radio Science journal. He has also served as the U.K. Commission F representative for the International Union of Radio Science (URSI), 2005–2010 and as external examiner for the Military Electronic Systems Engineering and Guided-Weapon Systems Engineering programmes at the UK Defence Academy, Shrivenham. His current research work is focussed in three main areas: Radio propagation modelling, remote sensing and novel instruments.

https://doi.org/10.24868/issn.2631-8741.2020.005

Spoofing is a more sophisticated attack that seeks to cause GNSS receivers to compute misleading PNT solutions. It had previously been considered that the “barrier to entry” to the technology and the know-how needed to produce an effective spoofer were, in themselves, a significant deterrent. However, the commercial availability of inexpensive (< £250) software defined radio (SDR) systems, low-cost computing and open-source GNSS signal generator software has all but eliminated this barrier. Spoofing has now been well demonstrated in an experimental context. For examples, see Psiaki, et al (Ref. 4), Shepard, et al. (Ref. 5) and Motella, et al (Ref. 6).

Over the past 20 years, concerns have been growing about the impact of malicious interference with GNSS signals (Ref. 7). In particular, there are growing concerns about the integrity of safety-critical ship systems and aids to navigation (AtoN) at sea (Ref. 8). It has been estimated that the economic cost of a 5-day GNSS failure in the maritime sector is in the order of £1.1bn (Ref 9).

In this paper we focus on radio-frequency attack as the primary method of jamming, noting that there is also the possibility of cyber-attack on GNSS systems in which there is interception and modification of computed position between the receiver and application. We shall start by reviewing how GNSS systems work and show where the vulnerabilities lie. We will then consider jamming and various methods of spoofing, means of detecting spoofing through analysis of signal anomalies, and mitigation of spoofing at the physical layer via the antenna, signal processing and at the software application layer through the detection of anomalies.

2. A Review of GNSS Principles

As the ‘first among (GNSS) equals’ GPS has grown to be the principal means of satellite-based position fixing at sea, both coastal and ocean, and also as a timing reference for AtoN in the littoral. Consequently, GPS has been seen as a single point of failure (SPOF). This has led proponents of the emerging GNSS to argue that these new systems will mitigate the SPOF associated with GPS by providing an increase in the number of signals. But all GNSS function on the same principles and use the same carrier frequencies and thus are vulnerable to the same failure modes, including jamming and spoofing.

Broadly speaking, all GNSS offer two levels of service: an open, or standard positioning, service available free of charge to any user, and a closed, or precise positioning, service offering higher accuracy and integrity to military and other authorised users. Access to the closed services is controlled through various levels of encryption.

The open services provided by GPS and Galileo are transmitted on a single carrier frequency of 1575.42 MHz, designated L1 in GPS and E1 in Galileo. It is believed that the Beidou open service will also use this frequency, and the GLONASS open services also use nearby frequency slots. The more precise closed services are also provided on L1/E1 plus one or more other carrier frequencies of between 1176.45 MHz and 1227.6 MHz (GPS L2 frequency).

2.1. GNSS in Marine Systems

The number of ship systems that rely on inputs from GNSS varies greatly from one vessel type to another. At the simplest end of the scale are weekend yachts that may carry a simple single-frequency GPS unit. At the other end of the scale a ship fit may include a large array of interconnected systems, many safety-related, but all deriving inputs from GNSS receivers. Ship navigation systems that may use GNNS include:

- NAVTEX;
- AIS;
- Gyro compass;
- Ship’s Inertial Navigation System (SINS);
- GMDSS;
- Ship’s time server;
- ECDIS/WECDIS;
- Autopilot;
- Differential GPS (DGPS);
- Radar (S-Band and X-Band).

Most of these systems are able to ride through short-duration interruptions in the GNSS signals, but will nonetheless raise alarms. Multiple alarms can lead ship operators into sensory overloads and ‘alarm deafness’.

The main terrestrial AtoN that depend on GNSS are AIS and synchronised lighting. Synchronised lighting is an attempt to overcome the growth of background lighting in harbour approaches and coastal areas that are overwhelming navigation lights. The idea is to time-synchronise multiple lights on buoys or land-based fixtures so that they form a recognisable pattern. For example, a channel may be lit by a two rows of lights that flash in sequence, in a similar manner to a ‘flare path’. Individual lights in such a system are likely to be autonomous and so accurate timing is essential; this is obtained from GNSS signals.

2.2. GNSS Fundamentals

This description applies specifically to GPS, but all GNSS are very similar. A typical GNSS consists of three main segments: a space segment (satellites), a ground-based control segment and a user segment.

The space segment consists of at least 24 satellites, typically arranged in six orbits of four to ensure worldwide coverage. The GPS satellites transmit navigation data on three separate L-Band carrier frequencies known as L1 (1575.42 MHz), L2 (1227.6 MHz) and L5 (1176.45 MHz). Other GNSS use the same or nearby frequencies. The transmitted data includes, among other things, the satellite positions, orbit correction information and a time stamp indicating the time at which the signal left the satellite. Each satellite is uniquely identified by a pseudo-random number (PRN) sequence, which is used to spread the spectrum of the transmitted signal. This also permits simultaneous transmission of all satellite signals on the same frequency at the same time.

The ground-based control segment monitors the tracking, telemetry and control functions of the satellites. It maintains station keeping, issues ephemeris updates and monitors system health. Since the satellite clocks are all free running, an important function the control segment is to maintain the synchronism of the satellite clocks to a common system time, usually referenced to UTC.

The user segment is the community of end users, both military and civil, equipped with GNSS receivers that compute PNT solutions. The simplest receivers access the open services by tracking a single GNSS carrier frequency (L1/E1) to compute the lowest-precision PNT solutions. More sophisticated (and more expensive) receivers can track more than one GNSS carrier frequency and access the higher precision services.

The PNT solution is computed by measuring the path lengths to each satellite in view from the receiver's position. Essentially, the problem is shown in Figure 1. The user’s geographical position (unknown) is represented by the vector **u**, the position of the satellite is represented by the vector **s** (obtained from the navigation message), and the measured range from the user to the satellite is represented by the vector **r**.

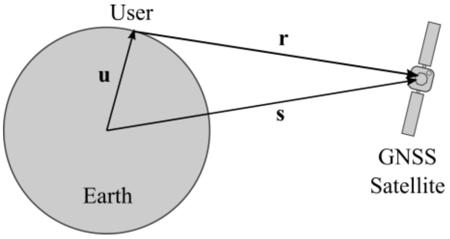

Figure 1 User, range and satellite position vectors.

By differencing the time the signal left the satellite (from the time stamp) and the time it is received (according to the receiver’s clock) the propagation time of the signal can be computed. Knowledge of the velocity of the signal then enables the path length to be determined. A minimum of three range measurements to three different satellites is required for a unique three-dimensional position to be computed.

The satellite and receiver clocks, however, are free running, so they are likely to be offset from the GNSS system time, and by different amounts. This introduces an unknown bias into the range measurement (see Equation 1). It is therefore convenient to refer to the ‘raw’ measured range as the pseudorange (denoted p); this needs to be corrected by eliminating the clock offsets to give the true range (denoted ρ).

$$p = \rho + c(\delta t_r - \delta t_s) \tag{1}$$

The satellite clock offset is not so much of a problem as the satellite clocks are maintained by the control segment. Multiple atomic clocks in each satellite ensure good redundancy and any uncorrected offset is transmitted as part of the satellite’s navigation message. But receiver clocks are often simple quartz devices that can drift significantly over a few hours. In order to resolve the receiver clock offset a fourth measurement is required to another satellite, independently of the other three. This gives a system of four equations in four unknowns (x, y, z and t) which are then solved to yield the PNT solution.

2.3. Signal Integrity and Error Sources

Most receivers are capable of tracking at least 12 satellites. There are (usually) at least four satellites in view from a user’s position so any additional pseudoranges should all be consistent with the computed PNT solution. If, however, one pseudorange differs significantly from the expected value then this may indicate a fault with the associated satellite. This can be detected in receivers that use Receiver Autonomous Integrity Monitoring (RAIM), which is a receiver function that looks for jumps in pseudorange.

The accuracy of the PNT solution also depends on the geometric distribution of the satellites in view. This is quantified by the Dilution of Precision (DOP). A low DOP implies that the satellites are widely distributed and so the geometric uncertainty in the PNT solution is minimised.

There are, of course, other error sources that bias the PNT solution. These include (but are not limited to): ionospheric delay, tropospheric delay, receiver noise, multipath and inter-channel biases. Collectively, these can amount to 20 – 30 metres in the open services, with the most significant contribution being ionospheric delay. The mitigation of these errors sources, however, is complex and is outside the scope of this paper.

3. Jamming and Spoofing

Regardless of their implementation all current GNSS signals are spread-spectrum, meaning that the total occupied bandwidth of the transmitted signal is far more than the bandwidth required to transmit the relatively low rate data.

For example, in the case of the GPS coarse acquisition (C/A) signal, transmitted on the L1 carrier at 1575.45 MHz, the bandwidth is in the order of 2 MHz, whereas the data rate is only 50 bits per second. While this appears to be inefficient use of the radio spectrum, this additional bandwidth provides a “process gain”, which increases the signal-to-noise ratio following de-spreading, reversing the increase in bandwidth performed at the (satellite) transmitter.

3.1. Jamming

Extraction of the signals in the receiver is done on a per-satellite basis using the unique PRN code allocated to each satellite. The consequence of this is that GPS signals can operate well below the thermal noise floor. To effectively jam GNSS signals one needs only to generate a signal that increases the unwanted signal component (noise plus jamming) presented to the receiver. This degrades the signal such that, even with the gain of the dispreading process, it is not possible reliably to recover the data and determine the time offsets required for the PNT solution. That is, when the jammer-to-signal (J/S) ratio threshold is exceeded GNSS reception is denied.

Without de-spreading, the GNSS signal is unobservable simply by measuring the total power within a band at the relevant frequency using a measurement receiver, power meter or spectrum analyser. However, it does mean that jammers are generally readily detectable. Any measured signal that is above the thermal noise floor is a potential threat to GNSS. The J/S ratio required to disrupt GNSS depends on the signal being tracked, the jammer type and the receiver implementation.

The GPS signal power at the Earth’s surface does not exceed -120 dBm (Ref. 10), so depending on the jammer type a signal 15-20 dB larger may typically start to affect reception of weaker low elevation satellites, which may subsequently increase the DOP and degrade the accuracy of the navigation solution. Stronger signals may overwhelm the antenna amplifier and receiver itself completely, preventing the acquisition of new signals and ultimately rendering any legitimate signals unusable.

As noted, any sufficiently strong signal is sufficient to disrupt GNSS signals. Jammers may use a simple narrow bandwidth continuous wave carrier signal, or frequency modulation to occupy a wider bandwidth. In land-based applications, there has been widespread illegal use of low-cost jammer devices sold as “privacy protection devices” designed to defeat tracking devices for vehicle telematics and theft prevention. Such devices typically have output powers anything from 0.1 W to 1 W (20 dBm to 30 dBm). Figure 2 shows an example of the output spectrum of such a device (inset), which produces 0.5 W (27 dBm) on each of GPS and Galileo L1/E1, L2, L5/E5 and E6 frequencies.

https://doi.org/10.24868/issn.2631-8741.2020.005

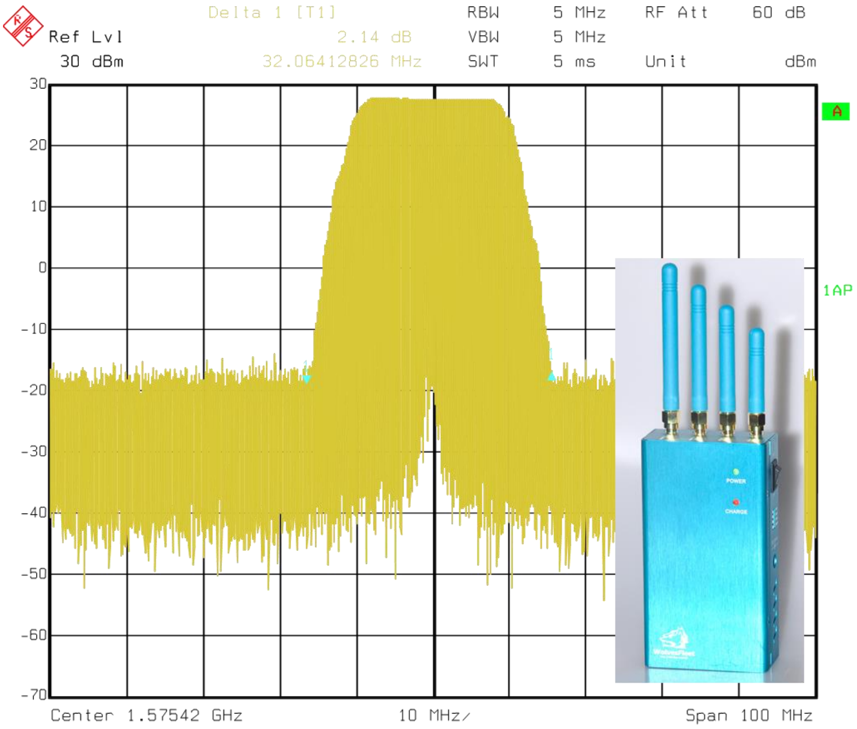

Figure 2 Example output spectrum of a swept frequency GNSS jammer (inset).

By way of illustration of the capability of such a jammer, Figure 3 shows vulnerability of a receiver to a GPS L1 jammer as a function of location, estimated using a radio propagation prediction model (Ref. 11). Here, the "victim" receiver is located in the port of Felixstowe (51.95°N, 1.29° E), corresponding to the map centre. The colour at a given location indicates the jammer power required to exceed a level of -105dBm at the victim receiver location. Although one might expect this to follow a simple inverse square law, strong signal shadowing caused by the topography means that this is often far from the case. Nevertheless it is clear that a low power jammer operated from well outside the port would be able to influence receivers located in the port area.

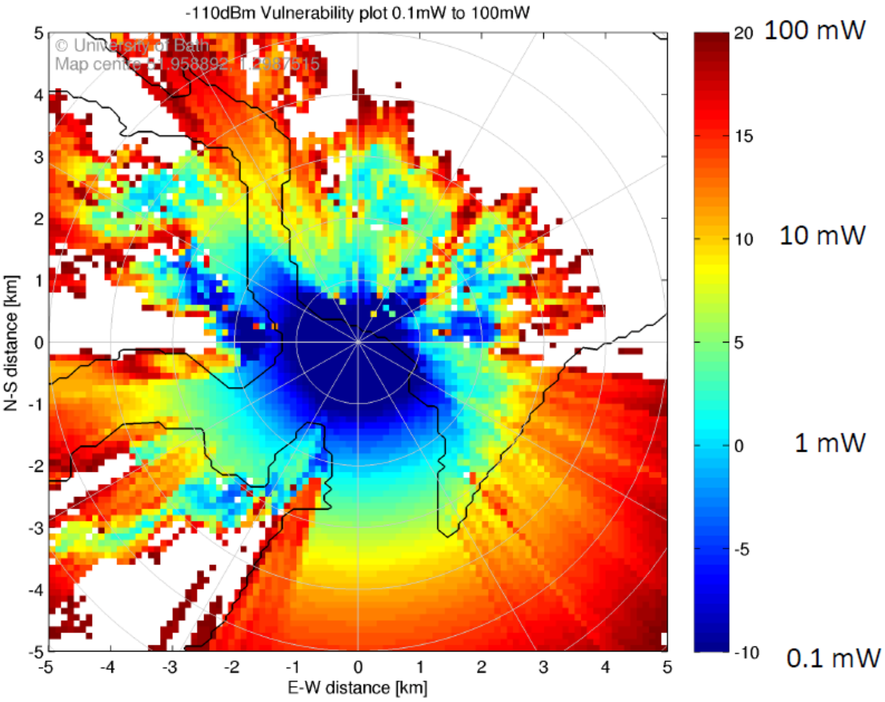

Figure 3 Example GNSS vulnerability plot.

https://doi.org/10.24868/issn.2631-8741.2020.005

Detection and location of jamming is relatively straightforward since any significant power in the protected GNSS radio navigation frequency bands is indicative of interference, whether malicious or not. Several devices are available for the detection, characterisation, location and in some cases mitigation of GNSS jammers. Such devices range from simple handheld power detection devices (e.g., Chronos Technology's CTL3510) to more sophisticated controlled radiation pattern antenna (CRPA) devices. The idea behind a CRPA antenna is to use multiple antenna elements which together can be used to determine the direction of the jamming signal and then form an antenna null in that direction so as to minimise the effect of the jamming on the receiver. A review of the adaptive antenna methods can be found in (Ref. 12). Multi element antenna solutions of this form include the NovAtel GAJT and Raytheon Landshield, using between four and seven elements.

3.2. Spoofing

As previously noted, spoofing is defined as the deliberate transmission of falsified GNSS signals in such a way that the victim receiver reports a time and/or position which is different to its physical location and current time. It has the capacity to create hazardous and potentially dangerous scenarios by causing users to take actions based on incorrect information, e.g., incorrect course corrections that steer vessels into regions with conflicted territorial claims. Spoofing can also be used to alter the course and behaviour of autonomous platforms e.g., aerial vehicles, surface vessels.

Receivers that employ RAIM have some degree of protection against simplistic spoofing attacks such as the broadcasting of a fixed falsified position. RAIM systems are generally able to detect inconsistency in satellite pseudoranges and reject these as false. The hardware and software required to generate a consistent and sufficiently precise set of signals, i.e. the replication of a constellation of satellite signals, was initially a deterrent. The expense of such equipment limited the likelihood of widespread use. However, the availability of software defined radio (SDR) transceivers in the last decade, with capability of generating the required L-band signals, has very significantly altered this situation. In June 2015 source code for a functional software-defined, multi-satellite GPS signal generator was posted to an online software repository. This was tested by the University of Bath with an inexpensive software defined transceiver (the £220 open-source HackRF). With the software compiled and run on £50 Raspberry Pi 3 computer powered from a battery pack, the system was shown to be capable of spoofing the time and position reported by a widely available commercial civilian GNSS receiver module (Ref. 13). For applications in which GNSS receivers are used with little or no integrity monitoring, this unsophisticated and inexpensive attack could easily go undetected.

The first demonstration of spoofing in the open literature was reported by Humphreys, et al (Ref. 14). In this sophisticated attack, a monitoring receiver was first used to determine the true GPS signal from which the spoofing signal was created and transmitted to the victim receiver. The spoofing signal was then deviated away from the true signal in a controlled manner such that the variation in position was followed by the victim receiver.

This method of spoofing is relatively sophisticated. The objective is always to maintain a self-consistent signal from the spoofer in order to maintain lock in the victim receiver's tracking loops. Without causing significant perturbations in the pseudoranges, the spoofing is likely to be undetectable by RAIM. The relatively low-level signals required with this approach also means that detection at the victim receiver by local measurement of spoofed signal power is almost impossible. It should be noted, however, that if the spoofed signal is transmitted far from the victim receiver then it is likely that the spoofed signal could be detected close to the location of its transmitter.

Indications of a spoofing attack depends on its sophistication. In the case of the generation of a falsified complete constellation from a single position, variations in the pre-correlation signal power might be detectable depending on the distance to the spoofer. Such variations can be easily detected by a change in automatic gain control or via sensitive jamming detection equipment. More sophisticated attacks might not cause significant power changes but may still lead to anomalous carrier-to-noise ratios, discontinuities in the reported time outputs, or unexpected variations in the code/doppler tracking space (e.g., unexpected peaks, duplicated satellites). If the spoofing signals are all transmitted to the victim receiver from the same distant location, those signals are likely to suffer from the same multipath and signal variations due to the local propagation environment. Such correlated variations are unlikely if directly received from space.

With a multi-antenna CRPA systems, the angles of arrival of signals can be determined. Instances of multiple signals emanating from the same direction, or multiple inconsistent angles of arrival from the same satellite can all be tell-tale signs. Theoretically, given detailed knowledge of the victim receiver's location it is possible to defeat the spoofing protection of a multi-antenna receiver, by transmitting spoofed signals from multiple locations. This would require the various observable phase differences expected from the true satellite signals to be replicated. Currently, the level of sophistication and synchronisation required would make it prohibitively impractical. While a line-of-sight signal from GPS is right-hand-circularly polarised, an unsophisticated line-of-sight spoofing signal, especially from a ground-based emitter with significant extra multipath, is unlikely to be so.

4. Summary and Conclusions

In summary, we started by noting that the first operational GNSS, GPS, has grown to be the principal satellite-based PNT tool in use in ships and coastal AtoN. More navigation equipment now takes inputs from the ship’s GPS receivers, so that GPS has become a single point of failure (SPOF). While there are natural phenomena that can disrupt the computation of the PNT solution, we have been concerned in this paper with the malicious denial or falsification of GNSS signals.

It is relatively easy to block (jam) GNSS signals in the vicinity of a victim receiver using jamming devices that are readily available at low cost. A more sophisticated attack seeks to spoof the GNSS signals in order to gain control of the victim receiver so that it computes misleading, but superficially plausible, PNT solutions. Simple spoofing is easy and can be done for about £250. Complex spoofing is more difficult but not beyond the capabilities of organised crime or Nation States. Spoofing is particularly worrying as it can lead to a vessel being lured into contested waters.

The increased number of GNSS, such as Galileo and Beidou, while providing greater redundancy in terms of extra GNSS ranging signals, will not mitigate jamming and spoofing as all GNSS constellations use substantially the same carrier frequencies and similar power levels.

Detection and location of jamming is relatively straightforward and there are well-established technologies, ranging from simple power measurement devices to sophisticated multi-antenna devices that determine the direction of the jammer and form a null in the antenna pattern. The same techniques can be used to defeat spoofing attacks.

But these are only part of a wider approach that should include (but not be limited to) digital signatures to enable genuine GNSS signals can be identified, encryption of safety-of-life GNSS services and robust international enforcement of legislation prohibiting intentional interference with GNSS signals, all underpinned by complementary terrestrial PNT services that are immune to spoofing, for example eLoran.

Acknowledgements

The work of RJW was supported by the UK Engineering and Physical Sciences Research Council (Grant: TS/I00257X/1, SENTINEL). We thank Prof Charles Curry of Chronos Technology Limited and the late Prof David Last for numerous useful discussions.

References

1. Scott, Logan: “Spoofing: Upping the Anti”. Interview with Inside GNSS, July/August 2013.

2. Meggs R. W., Mitchell C. N. and Honary, F., “GPS scintillation over the European Arctic during the November 2004 storms”. GPS Solutions, doi: 10.1007/s10291-008-0090-3, March 2008.

3. Williams, P., Grant, A., Ward, N. and Basker, S.: “Reliable GPS: Interference, Jamming and the Case for eLoran”, Proc. of the Royal Institute of Navigation Annual Conference and Exhibition 2008 and 37th ILA Annual Convention and Technical Symposium, London, 28 – 30 October 2008.

4. Psiaki, M. L., Humphreys, T. E. and Stauffer, B.: "Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies," in IEEE Spectrum, vol. 53, no. 8, pp. 26-53, August 2016, doi: 10.1109/MSPEC.2016.7524168.

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

6. Motella, B., Pini, M. and Presti, L. L.: "GNSS interference detector based on Chi-square Goodness-of-fit test," 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing, Noordwijk, 2012, pp. 1-6, doi: 10.1109/NAVITEC.2012.6423070.

7. Volpe, John A.: “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System”, Final Report for the Office of the Assistant Secretary for Transportation Policy, US Department of Transportation, August 2001.

8. Marine Navigation Plan 2016 to 2030, published by The General Lighthouse Authorities. Downloaded from www.trinityouse.co.uk 28 May 2020.

9. Yamada, H. “Navigating the Seas”, GNSS and the Law column in Inside GNSS, September/October 2017.

10. Interface Specification IS-GPS-200: Navstar GPS Space Segment/Navigation User Interfaces, Revision E, dated 8 June 2010. Downloaded from https://www.gps.gov/technical/icwg/IS-GPS-200E.pdf June 2020.

11. N. Dumont, R. J. Watson and S. R. Pennock, "Propagation modelling for white space geo-location databases," 2012 6th European Conference on Antennas and Propagation (EUCAP), Prague, 2012, pp. 2175-2179, doi: 10.1109/EuCAP.2012.6206119.

12. I. J. Gupta, I. M. Weiss and A. W. Morrison, "Desired Features of Adaptive Antenna Arrays for GNSS Receivers," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1195-1206, June 2016, doi: 10.1109/JPROC.2016.2524416.

13. M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1258-1270, June 2016, doi: 10.1109/JPROC.2016.2526658.

14. T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in Proc. ION GNSS, Savannah, GA, USA, 2008, pp. 2314–2325.