VULNERABILITIES OF GLOBAL NAVIGATION SATELLITE SYSTEMS (GNSS) SIGNALS TO JAMMING AND SPOOFING

Dinesh Sathyamoorthy

Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia
Tel: 603-87324431
Fax: 603-87348695
E-mail: dinsat60@hotmail.com

Abstract

Global Navigation Satellite Systems (GNSS) are being increasingly used for a variety of important applications, including public safety services (police, fire, rescue and ambulance), marine and aircraft navigation, vehicle theft monitoring, cargo tracking, and critical time synchronization for utility, telecommunications, banking and computer industries. At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 for the case of GPS, and high precision (HP) for GLONASS) and civilian GNSS signals (L1 coarse acquisition (C/A) for GPS, and standard precision (SP) for GLONASS). Usage of L1 P(Y) and L2, and HP signals are limited to the US and Russian militaries respectively. Other users only have access to civilian GNSS signals. Usage of civilian GNSS signals is growing rapidly due the quality of service provided by GNSS, ease of use and low user cost. However, unlike military GNSS signals, civilian GNSS signals are unencrypted and unauthenticated, making them vulnerable to jamming and spoofing (also known as counterfitting or meaconing). Jamming and spoofing of civilian GNSS signals are surprisingly simple to conduct by even relatively unsophisticated adversaries. Jamming refers to the blocking of GNSS signals, rendering GNSS receivers in the affected areas inoperable, while spoofing refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. Jamming is not surreptitious and affects both civilian and military GNSS signals, while spoofing is surreptitious and primarily affects civilian GNSS signals; military GNSS signals are less affected by spoofing as they are encrypted and authenticated. Due to the increasing reliance of various industries on GNSS, the consequences of GNSS service disruption can be severe, in terms of safety, environmental and economic damage. Hence, GNSS vulnerability mitigations steps should be given emphasis, including navigation/positioning/timing backups, making full use of ongoing GNSS modernization programs, integrity monitoring and augmentation, and anti-jamming and counter-spoofing technologies. This article is aimed at reviewing the vulnerabilities of civilian GNSS signals to jamming and spoofing, and the steps that need to be taken to mitigate these vulnerabilities.

Keywords: *Global Navigation Satellite Systems (GNSS); jamming; spoofing; GNSS vulnerability mitigation.*

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS) are being increasingly used for a variety of important applications, including public safety services (police, fire, rescue, and ambulance), marine and aircraft navigation, vehicle theft monitoring, cargo tracking, and critical time synchronization for utility, telecommunications, banking and computer industries. The US Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS), its Russian counterpart, *Global'naya Navigatsionnaya Sputnikovaya Sistema* (GLONASS), and the upcoming European Galileo system and China’s Compass system transmit GNSS signals bearing reference information from the corresponding constellation of satellites. Any receiving device with the appropriate equipment can decode the signals and utilize the GNSS information to determine its own location (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

Each GNSS receiver is able to receive simultaneously a set of navigation messages, one message from each satellite in the visible satellite constellation. The navigation messages enable each receiver to determine its own position in a Cartesian system, as well as a time correction offset to add to its local clock value in order to maintain the current global time. At least four satellites should be visible so that the receiver can compute the location and time correction offset, with the two quantities together termed as the navigation solution (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

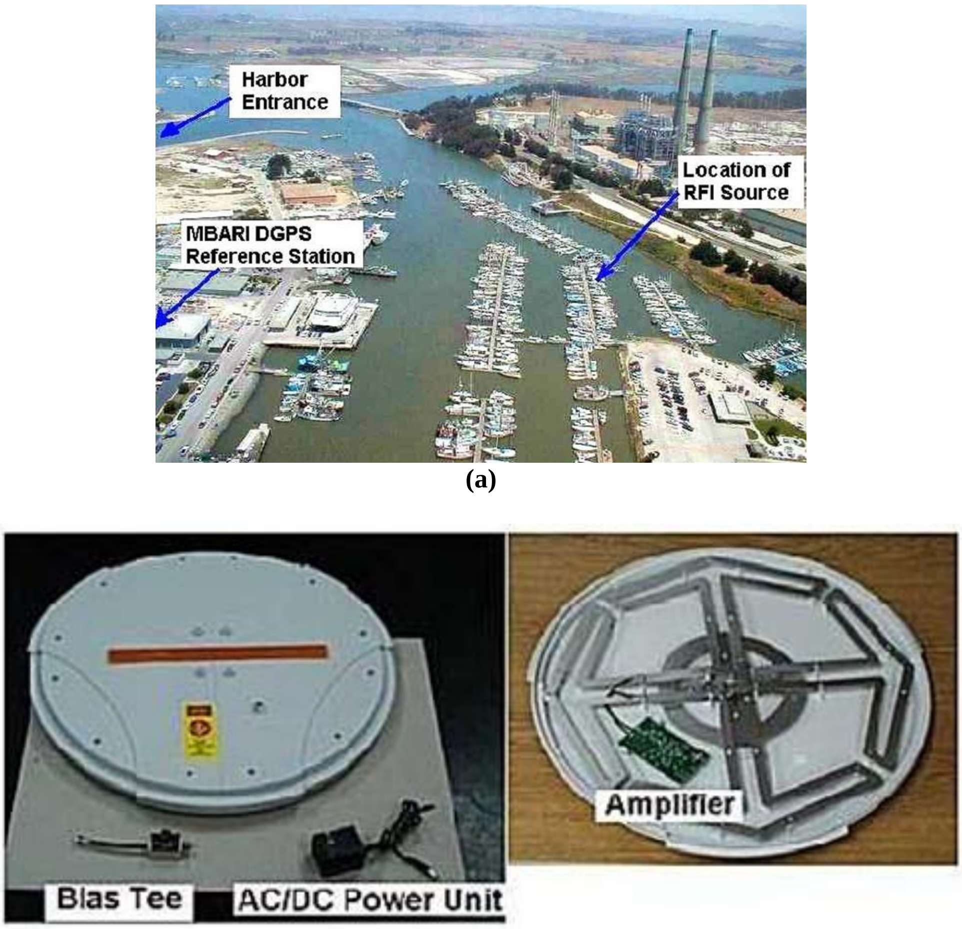
At present, there are two types of GNSS signals; military GNSS signals (L1 P(Y) and L2 for the case of GPS, and high precision (HP) for GLONASS) and civilian GNSS signals (L1 coarse acquisition (C/A) for GPS, and standard precision (SP) for GLONASS). Usage of L1 P(Y) and L2, and HP signals are limited to the US and Russian militaries respectively. Other users only have access to civilian GNSS signals (Kaplan & Hegarty, 2006; Gakstatter, 2008a). Usage of civilian GNSS signals is growing rapidly due the quality of service provided by GNSS, ease of use and low user cost. In addition to obvious positioning and navigation applications, GNSS-based timing synchronization is being increasingly employed, such as timing reference for power station grids, telecommunications systems and digital air-ground communications systems (GAO, 2009; Jewell, 2009). Due to the increasing reliance of various industries on GNSS, the consequences of GNSS service disruption can be severe, in terms of safety, environmental and economic damage.

Unlike military GNSS signals, civilian GNSS signals are unencrypted and unauthenticated, making them vulnerable to jamming and spoofing (also known as counterfitting or meaconing). Jamming and spoofing of civilian GNSS signals are surprisingly simple to conduct by even relatively unsophisticated adversaries. Jamming refers to the blocking of GNSS signals, rendering GNSS receivers in the affected areas inoperable, while spoofing refers to forging and transmission of navigation messages in order to manipulate the navigation solutions of GNSS receivers. Jamming is not surreptitious and affects both civilian and military GNSS signals, while spoofing is surreptitious and primarily affects civilian GNSS signals; military GNSS signals are less affected by spoofing as they are encrypted and authenticated (Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; IDA, 2009). This article is aimed at discussing the vulnerabilities of civilian GNSS signals to jamming and spoofing, and the steps that need to be taken to mitigate these vulnerabilities.

2 JAMMING

Jamming is defined as the broadcasting of a strong signal that overrides or obscures the signal being jammed (DOA, 2009; JCS, 2007; Poisel, 2002). Since GNSS satellites, powered by photocells, are approximately 20,200 km above the Earth surface, GNSS signals that reach the Earth have very low power (10^{-16} W), rendering them highly susceptible to jamming (Pinker & Smith, 2000; Adams, 2001; Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; IDA, 2009). For example, a simple 1 W battery-powered jammer can block the reception of GNSS signals approximately within a radius of 35 km from the jammer (Papadimitratos & Jovanovic, 2008). Even military GNSS signals are susceptible to jamming, as highlighted by the August 2000 Greek tank test incident (discussed in Adams (2001)) and the January 2007 San Diego communications jamming exercise incident (discussed in Jewell (2007)). Furthermore, as GNSS operates on line-of-sight (LOS) propagation between the GNSS satellites and GNSS receiver, blockage of the LOS propagation, such as by trees and buildings, and being indoors, can cause disruption (Volpe, 2001; Forssell, 2005; Kaplan & Hegarty, 2006; Gakstatter, 2008a). Available indoor navigation systems, such as assisted GPS (A-GPS), enhanced GPS (E-GPS) and pseudolites, have unstable accuracy and face difficulty operating in deep indoors (Manandhar *et al.*, 2008).

In 2001, the US Department of Transportation commissioned a report (Volpe, 2001) into the effects of GPS vulnerability on US transport systems. A similar report was commissioned in the United Kingdom (Harding, 2001). Both report that the most common form of GNSS jamming comes from unintentional sources such as broadcast television, fixed and mobile VHF transmitters, personal electronic devices (PEDs), aeronautical satellite communications, mobile satellite services, ultra wideband (UWB) radar and communications, and natural phenomena such as ionospheric distortions, scintillations and solar weather effects. For example, in April – May 2001, GPS coverage in Moss Landing, California, was severely disrupted by a poorly designed television amplifier (Clynch *et al.*, 2003; Last, 2008) (Figure 1). The US Navy reported several occurrences of GPS antenna failures in proximity to high-power radars from nearby ships (Williams, 2006). The current 11-year solar cycle is expected to peak in 2012-2013 (NASA, 2006; Gakstatter, 2009), with expected strong storms that can cause severe GNSS disruptions for several hours (Oberst, 2006; Gakstatter, 2008b, 2009).



(a)

(b)

Figure 1: GPS coverage disruption in Moss Landing, California (April-May 2001):
(a) The location of the jamming source. (b) The poorly designed television amplifier that caused the jamming.
(Source: Last (2008))

Intentional jamming of GNSS signals is not difficult to achieve. The little jammer hidden on the dice shown in Figure 2 radiates 1 kW of power, which is enough to jam GNSS signals throughout a building or across a dock. Some jamming devices/techniques are available on the internet (Figure 3), and proliferation will continue because a single device that could disrupt military and civilian operations would be attractive to malicious governments and groups (Volpe, 2001; Last, 2008; IDA, 2009). In addition, unintentional or natural disruptions, such as produced by the ionosphere or unintentional RF interference, could be used by saboteurs to disguise their intentional disruption, at least to delay government response and warning (Volpe, 2001).

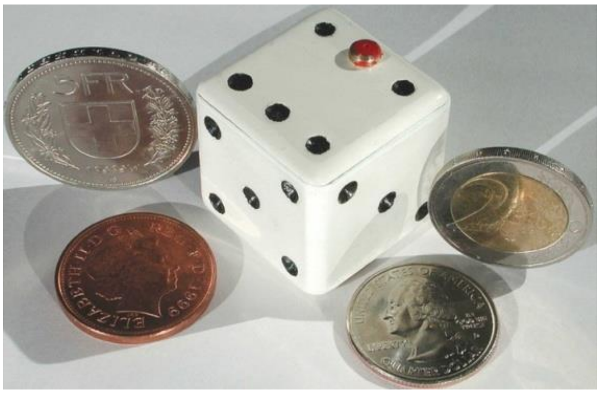


Figure 2: A GNSS jammer hidden on a dice.
(Source: Last (2008))

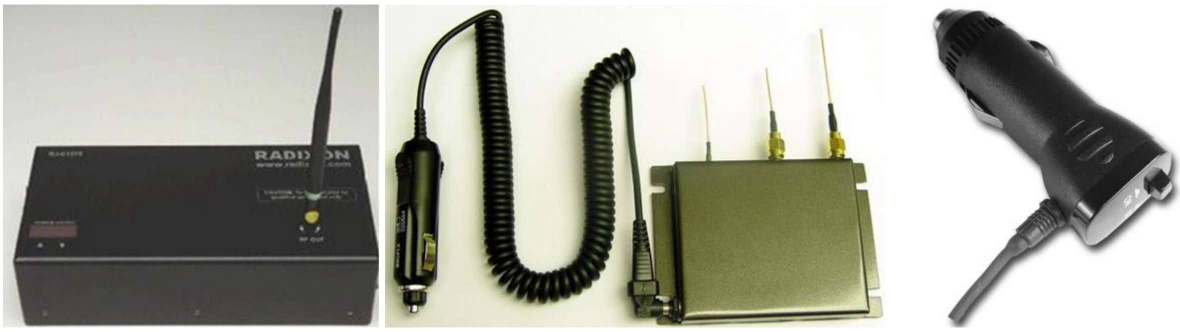


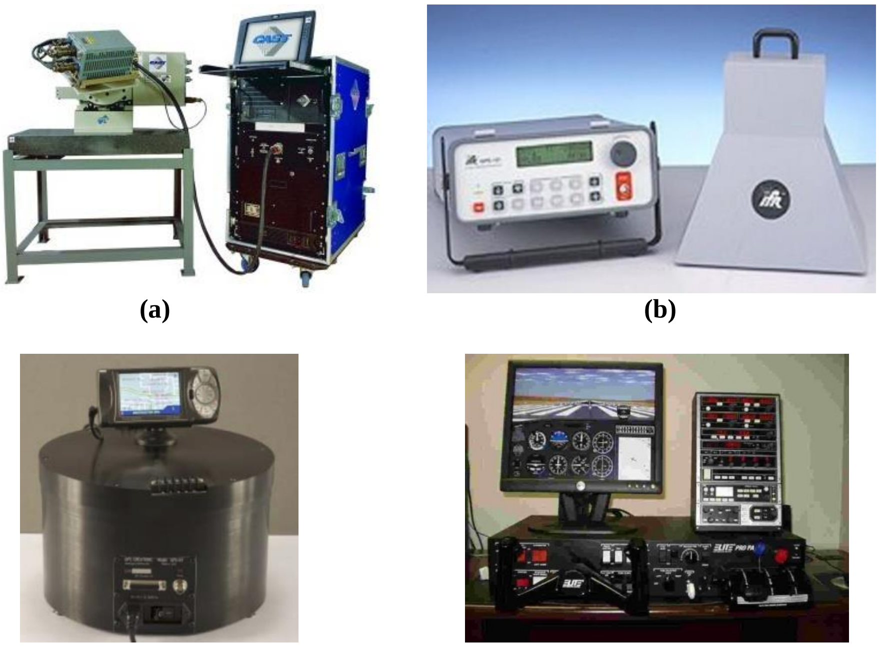
Figure 3: GNSS jammers found during casual browsing of the internet. The sources of the figures are not given for obvious reasons. Readers are reminded that GNSS jamming is illegal.

The accelerating worldwide dependence of various industries on GNSS makes mechanisms to disrupt GNSS signals potent weapons that many militarily sophisticated countries are actively pursuing. For example, the US military has a policy to block potential adversaries' access to the L1 signal while preserving its ability to utilize the L2 signal, without unduly disrupting or degrading civilian GPS applications outside the area of conflict (DOD/DHS/DOT, 2008; Volpe, 2001). The effort to develop GPS disruption systems for this purpose is known as navigation warfare (NAVWAR). From time to time, the US military conducts NAVWAR exercises which disrupt GNSS coverage within the affected areas. However, the US Department of Defense (DOD), Department of Homeland Security (DHS) and Department of Transport (DOT) have developed mechanisms to coordinate times and places for testing, and to notify users in advance (DOD/DHS/DOT, 2008). However, it is apparent that notifications of these tests do not reach enough GNSS user communities, resulting in numerous GNSS disruption incidents (Volpe, 2001; Last, 2008).

3 SPOOFING

Spoofing signals can be generated by GNSS simulators, equipment which is available today. The received power of the spoofing signal should exceed that of the legitimate signal, this being essentially a form of jamming. The receiver then operates with the forged signal as the input and computes the location induced by the spoofer (Johnston & Warner, 2004; Papadimitratos & Jovanovic, 2008; Last, 2008; Humphreys *et al.*, 2009; IDA, 2009). Spoofing is more sinister than intentional jamming because the targeted receiver cannot detect a spoofing attack and hence, cannot warn users that its navigation solution is untrustworthy. While spoofing is more difficult to achieve than jamming, in many cases even if a spoofer is not fully successful, he/she can still create significant errors and jam GNSS signals over large areas (Volpe, 2001; Last, 2008; Humphreys *et al.*, 2009).

A number of GNSS simulators (Figure 4) have been designed for legal purposes such as user training, system maintenance, vehicle motion simulation, and, ironically, anti-jamming testing. However, in the wrong hands, these GNSS simulators can be used to conduct illegal spoofing. Furthermore, GNSS simulators can be built with relatively low cost equipment (Figure 5), as demonstrated by Rogers (1991), Johnston & Warner (2004), Humphreys *et al.* (2008) and Hanlon *et al.* (2009).



(a) **(b)**

(c) **(d)**

Figure 4: Commercially available GNSS simulators: (a) Cast Navigation's CAST EMT3500-3 EGI (b) Areoflex's GPS-101 Global Positioning Simulator (c) GPS Creations' GPS-RT (d) Flightspectrum's Elite Basic Training Device PI-135 makes use of Garmin's G1000 GPS Simulator.

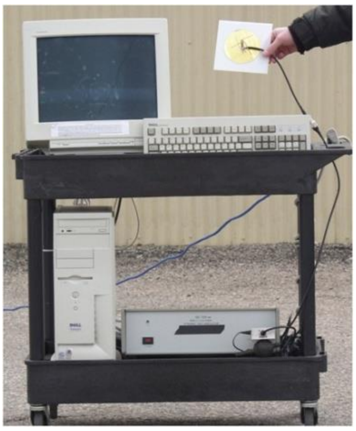


Figure 5: A homemade GNSS simulator.
(Source: Johnston & Warner (2004))

The spoofing threat continuum can be divided into three categories; simplistic, intermediate, and sophisticated (Hanlon *et al.*, 2009; Montgomery *et al.*, 2009) (Figure 6). Simplistic attacks are conducted using standalone GNSS simulators. The menace posed by such attacks are diminished by the fact that most GNSS simulators are heavy and cumbersome, and that it is likely easy to detect because of the difficulty of synchronizing a simulator's output with the GNSS signals in its vicinity. An unsynchronized attack effectively acts like GNSS jamming, and may cause the victim receiver to lose lock and have to undergo a partial or complete reacquisition, raising suspicion of a spoofing attack.

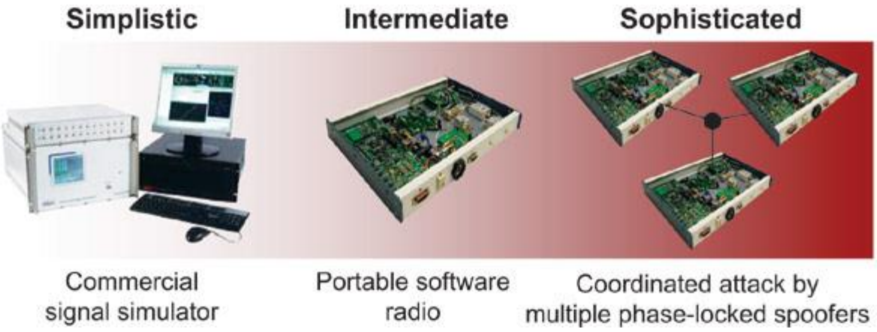

Simplistic
Intermediate
Sophisticated
Commercial signal simulator
Portable software radio
Coordinated attack by multiple phase-locked spoofers

Figure 6: The spoofing threat continuum; simplistic, intermediate and sophisticated spoofing attacks. (Source: Hanlon *et al.* (2009))

Intermediate attacks make use of portable receiver-spoofers, which can be made small enough for inconspicuous placement near the target receiver's antenna. The receiver component draws in genuine GNSS signals to estimate its own position, velocity and time. Based on these estimates, the receiver-spoofer then generates counterfeit signals and generally orchestrates the spoofing attack. The portable receiver-spoofer could even be placed somewhat distant from the target receiver if the target is static and its position relative to the receiver-spoofer had been pre-surveyed. While there are no commercially available portable receiver-spoofer devices, advances in radio frequency (RF) software-defined technologies could see a proliferation of such devices. The only known civilian GNSS equipment based countermeasure that would be completely effective against an attack launched from a portable receiver-spoofer with a single transmitting antenna is multi-antenna angle-of-arrival discrimination. With a single transmitting antenna, it would be impossible to continuously replicate the relative carrier phase between two or more antennas of an appropriately equipped target receiver.

Sophisticated attacks thwart angle-of-arrival defence by a coordinated attack with as many receiver-spoofers as antennas on the target receiver. This type of attack inherits all of the challenges of mounting a single receiver-spoofer attack, with the additional expense of multiple receiver-spoofers and the additional complexity that the perturbations to the incoming signals must be phase-coordinated. Thus, an attack via multiple phase-locked portable receiver-spoofers is somewhat less likely than an attack via single portable receiver-spoofer, but may be impossible to detect with civilian GNSS equipment based spoofing defences, as the only known defence against such an attack is cryptographic authentication.

4 MITIGATION OF GNSS VULNERABILITIES

Given the dependence of various industries on GNSS systems, GNSS disruption could prove to be problematic, if not disastrous, as demonstrated in the incidents highlighted by Adams (2001), Clynch *et al.* (2003) and Jewell (2007). Hence, effective mitigation of GNSS vulnerabilities is required in order to avoid such chaotic scenarios.

The most recommended mitigation step is the application of navigation/positioning backups which can be used in the case of GNSS disruptions (Volpe, 2001; Lilley, 2006; Last, 2008). Navigation backups, such inertial navigation systems (INS), enhanced long range navigation (eLORAN) and VHF omnidirectional range distance measuring equipment (VOR/DME), have the potential to take over seamlessly when GNSS fails, and can be used as a deterrent against spoofing. Recent operational GNSS jamming tests have shown that eLORAN is a highly effective navigation backup in cases of GNSS failure (Basker *et al.*, 2008; GPS World, 2009a; Grant *et al.*, 2009) (Figure 7). An Independent Assessment Team (IAT) report (IDA, 2009), commissioned by the US DOT, recommended that the US government commit to eLoran as the national backup to GPS for the next 20 years. In addition, applications relying on GNSS-based time synchronization should employ suitable timing backups, such as internet time services, network time protocols, and if viable, atomic clocks.

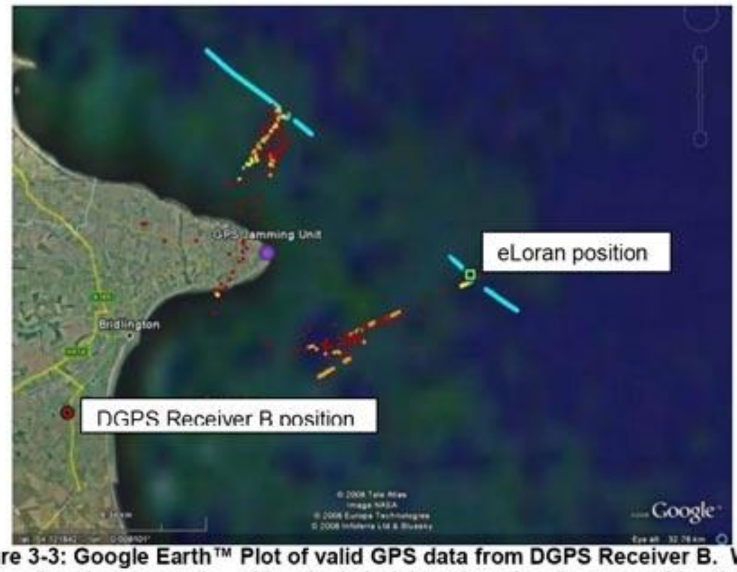
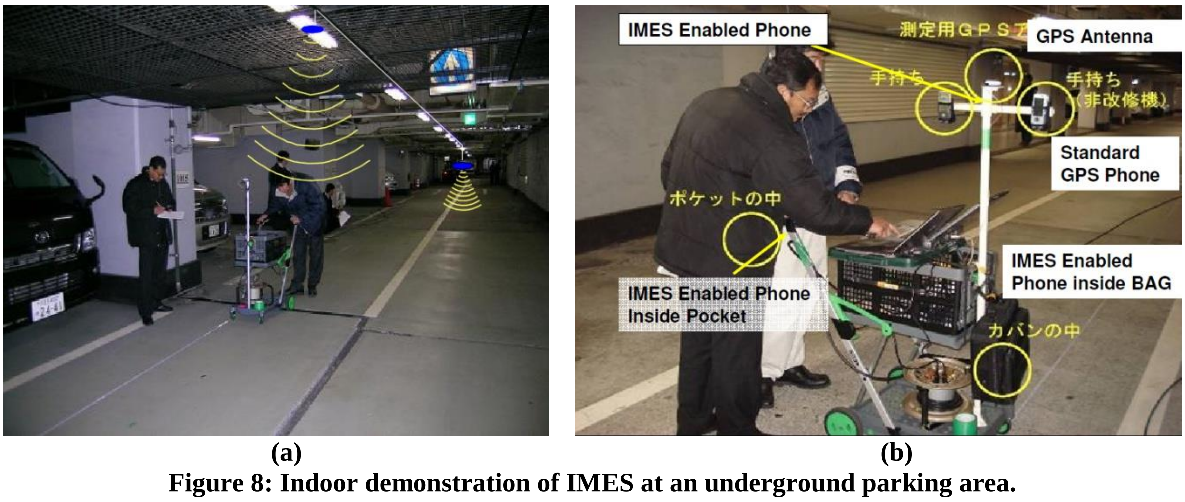


Figure 3-3: Google Earth™ Plot of valid GPS data from DGPS Receiver B. When comparing the reported position (red circle) against the eLoran position (green square) for the same time, one can see an error of 22Km with the reported DGPS Receiver B position being on land. (Colours indicate reported speed: blue <15knts, yellow< 50knts, orange <100knots and red >100knts)

Figure 7: The General Lighthouse Authorities (GLAs) of the United Kingdom and Ireland conducted a GPS jamming exercise from 31st March to 4th April 2008 to investigate the performance of eLoran during GPS service denial. It was reported that eLoran was unaffected by GPS jamming and demonstrated an accuracy of 8.1 m (95%).
(Source: GPS World (2009a))

In order to be able to provide accurate indoor position determination for public and commercial services, such as search-and-rescue, firefighting and location based services (LBS), it has been proposed that indoor positioning transmitters be employed to the solve the GNSS indoor availability issue. The receiver will use GNSS signals outdoors in the usual way, while using signals from transmitters indoors, where GNSS signal quality is strongly reduced. The indoor transmitter signal structure is similar to that of GNSS signals, except for the contents of the navigation message. Thus, the same receiver can be used for both outdoor and indoor applications. Recent indoor positioning technologies include Locata Corporation's LocataNet (Locata, 2003; Barnes *et al.*, 2003), and the Japan Aerospace Exploration Agency's (JAXA) Indoor Messaging System (IMES) (Satoshi *et al.*, 2008; Manandhar *et al.*, 2008) (Figure 8).



(a) **(b)**

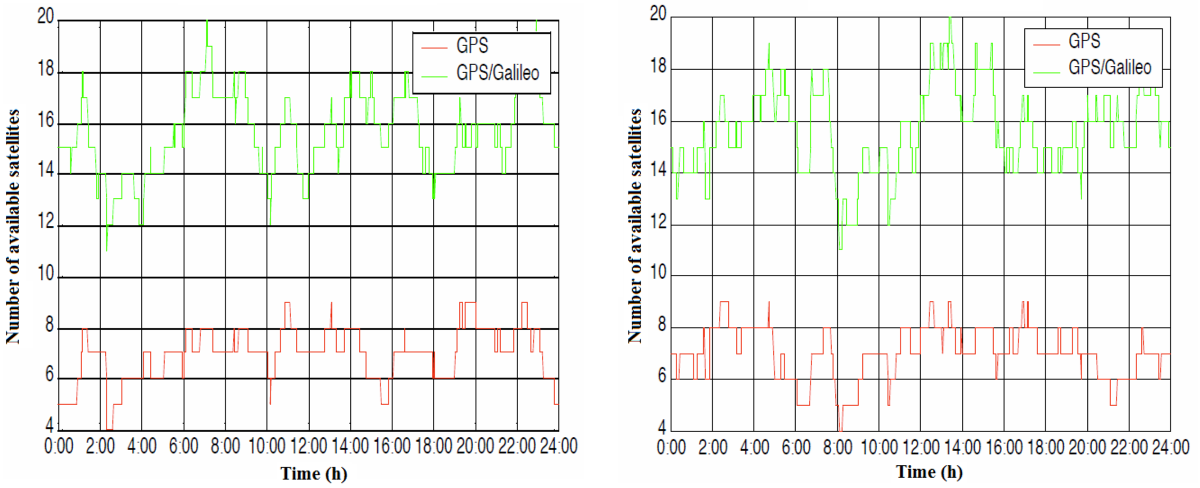
Figure 8: Indoor demonstration of IMES at an underground parking area.
(Source: Manandhar *et al.* (2008))

However, in order for these systems to provide reliable and accurate indoor positioning, the transmitters need to be very densely located in all indoor spaces where location is required, at separations of 20-30 m, requiring large investments in infrastructure (Demspter, 2009). Alternatives that has been proposed to provide cost-effective solutions include RFID (Hähnel *et al.*, 2004; Chang *et al.*, 2008), infrared (Muneyuki *et al.*, 2003; Kemppainen *et al.*, 2006), sensor networks (de Oliveira *et al.*, 2005; Fernandez *et al.*, 2007), and WiFi (Ekahau, 2008; Kawaguchi, 2009).

GNSS users should also take full advantage of the various ongoing GNSS modernization programs (McDonald, 2002; Blomenhofer, 2004; Alkan *et al.*, 2005; Gakstatter & Flick, 2006; Kaplan & Hegarty, 2006; Gibbons, 2006; 2008, 2009; Gakstatter, 2008a,c,d; GAO, 2009; Rizos, 2009). The upcoming new civilian GPS III signals that are to be provided, the L1C, L2C and L5 signals, will be able provide a substantial reduction in the threat of unintentional jamming, and some degree of threat reduction from intentional jamming. With the more robust civil L5 signal (1,176 MHz) being far removed from the L1C ((1,575 MHz) and L2C (1,227 MHz) signals, it is extremely unlikely that unintentional jamming sources can jam all three signals simultaneously, and will be more difficult and costly for intentional jamming. The civilian GPS III signals, in particular the L5 signal, will also have significantly improved code structures that will allow the signals to be acquired and tracked better in tough GPS conditions, such as under tree foliage and extreme solar activity (McDonald, 2002; Gakstatter & Flick, 2006; DOD/DHS/DOT, 2008).

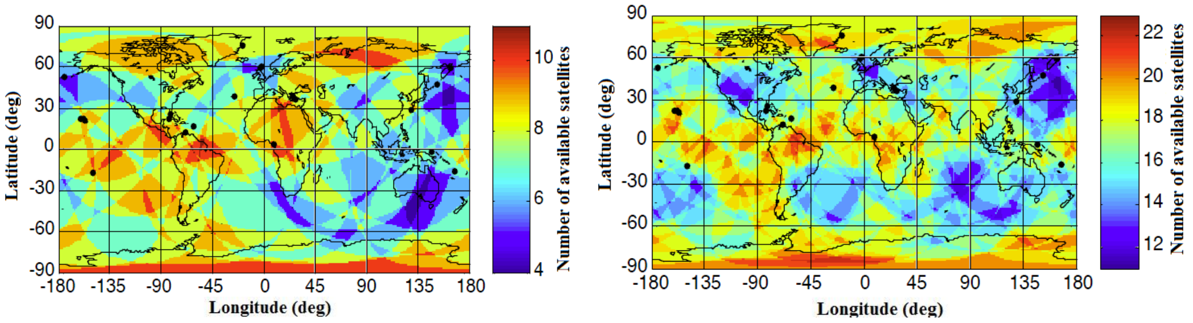
Galileo, which is a GNSS that has been targeted at commercial applications since its inception, is designed to have a 30-satellite constellation (27 operational plus 3 active spares), as well as a complement of groundstation equipment. There are many similarities between the proposed civilian Galileo (L1F, E5a and E5b) and GPS III (L1C, L2C and L5) signals. Galileo's performance is expected to be at least as good as civilian GPS, and some aspects are likely to be superior to GPS (including the onboard atomic clocks). Galileo also has a proposed integrity function that will be much more sophisticated than current GPS (although GPS III will be much improved in this area) (Blomenhofer, 2004; Kaplan & Hegarty, 2006; Gakstatter & Flick, 2006; Gakstatter, 2008c). Studies have also shown that with combined GPS and Galileo constellations, the overall navigation availability in urban areas (where high buildings obstruct the GNSS signals in downtown areas) can be improved from 55% to 95% (Alkan *et al.*, 2005). Using GNSS measurement simulations, Hewitson (2003) demonstrated the increased satellite availability of combined GPS/Galileo over two urban areas in Australia, Sydney and Portland (Figure 9), and worldwide (Figure 10). It can be anticipated that combined GPS/Galileo receivers will be the predominant equipment for critical GNSS applications, and they will also be employed by many massmarket users (Alkan *et al.*, 2005; Gakstatter & Flick, 2006; Gakstatter, 2008a,c,d).

Although GLONASS achieved its full operational capability in January 1996, when 24 GLONASS satellites were available for positioning and timing, its constellation had dropped to just 7 satellites by May 2001 due to decreases in the allocated maintenance budget. In August 2001, the Russian government approved a long-term plan to reconstitute a GLONASS constellation of 24 satellites by 2011 (Revnivykh, 2007, 2008; Sergey et al., 2007). As of 4th November 2009, there are 18 operational GLONASS satellites in orbit, the minimum required to allow for continuous navigation services covering the entire territory of the Russian Federation (GPS World, 2009b). It is expected that the minimum required constellation of 24 satellites will be completed by February 2010 (Inside GNSS, 2009). Due to the difference in signal pattern used by GLONASS (frequency division multiple access (FDMA)) compared to GPS and Galileo (code division multiple access (CDMA)), interoperability between the GNSS systems would require complex and costly receivers. It was reported that during the meeting of the GPS-GLONASS Interoperability and Compatibility Working Group (WG-1) in December 2006, the US and Russian governments made significant progress in understanding the benefits to the user community of changing the GLONASS signal pattern to one that is similar with GPS and Galileo, enabling simply-designed receivers to use the three GNSS systems simultaneously (GPS World, 2007). GLONASS will broadcast CDMA signals beginning with the GLONASS-K generation of satellites which is expected to begin launching in 2010 (Revnivykh, 2007, 2008).



(a) (b)

Figure 9: Satellite availability at (a) Sydney and (b) Portland over 24 hours for GPS and combined GPS/Galileo. The GNSS measurement simulations were carried out at a sample rate of 1 Hz commencing at 0:00 h on 16th January 2003.
(Source: Hewitson (2003))

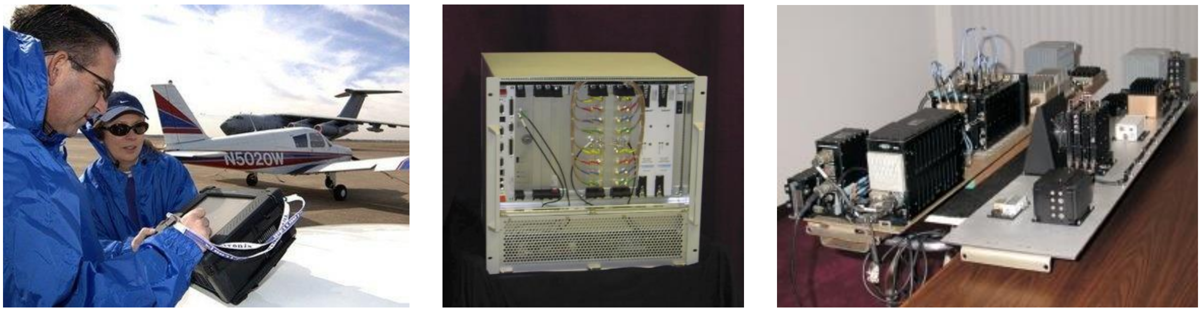


(a) (b)

Figure 10: Worldwide satellite availability for (a) GPS and (b) combined GPS/Galileo. The results were obtained from snapshot simulations for 0:00 h on 16th January 2003 at 1 degree intervals of latitude and longitude and an altitude of 50 m. Snapshot results permit analysis based on spatial variations as time is held constant. The results from the global snapshot scenario are presented as orthographic global colour maps.
(Source: Hewitson (2003))

The incidents discussed in Adams (2001), Clynch *et al.* (2003) and Jewell (2007) indicate a serious inability to effectively identify and locate jamming sources. Systems and procedures to monitor, report and locate intentional and unintentional jamming sources should be put in place, especially for applications for which GNSS disruption is not tolerable. This should be coupled with a prompt field response to remove the jamming source as quickly as possible. Recent technologies in signal tracking and detection, such as Tektronix’s H600 RF Hawk Signal Hunter (Tektronix, 2008) (Figure 11(a)), NAVSYS’ High-Gain Advanced GPS Receiver (HAGR) (Brown *et al.*, 2000) (Figure 11(b)), and the Space and Naval Warfare Systems Center’s (SPAWAR) Location of GPS Interferers (LOCO GPSI) (Simonsen *et al.*, 2004) (Figure 11(c)), should precipitate this.

The application of autonomous integrity monitoring of GNSS signals should also be looked into, such as receiver autonomous integrity monitoring (RAIM) used in the aviation and maritime industries (ION, 1998; Hewitson & Wang, 2006; Dufresne *et al.*, 2008). RAIM is a method which examines the internal consistency of a set of redundant measurements within the GNSS receiver to detect and remove a faulty measurement (a process known as fault detection and exclusion (FDE)). Navigational warning systems, such as Navigational Telex (NAVTEX) and Safetynet can also provide integrity warnings, but there may be delays in delivering such warnings by these methods (IALA, 2004).



(a) (b) (c)

Figure 11: Recent technologies in signal tracking and detection should allow for the fast and effective identification and location of intentional and unintentional jamming sources: (a) Tektronix's H600 RF Hawk Signal Hunter (b) NAVSYS' High-Gain Advanced GPS Receiver (HAGR) (c) Space and Naval Warfare Systems Center's (SPAWAR) Location of GPS Interferers (LOCO GPSI).

GNSS augmentations are required for several reasons, including improvement of accuracy and availability of integrity monitoring. Satellite Based Augmentation Systems (SBAS) determines GNSS integrity and differential correction data on the ground through a network of monitor stations and a central processing facility. Geostationary satellites are then employed to broadcast integrity messages and differential corrections, as well as a navigation message, via the civilian GNSS frequency. Following operational approval, the SBAS signal can then be used to improve GNSS accuracy, availability and integrity (Kaplan & Hegarty, 2006; Gakstatter, 2008a). Publically available SBAS systems, such as the US Federal Aviation Administration's (FAA) Wide Area Augmentation System (WAAS), the European Geostationary Navigation Overlay Service (EGNOS), and Japan's Multi-functional Satellite Augmentation System (MSAS), do not officially provide coverage in Malaysia. India's GPS Aided Geo Augmented Navigation (GAGAN), likely to be operational by May 2011, is expected to provide coverage to Malaysia (Suryanarayana Rao & Pal, 2004; Gakstatter, 2008a) (Figure 12).

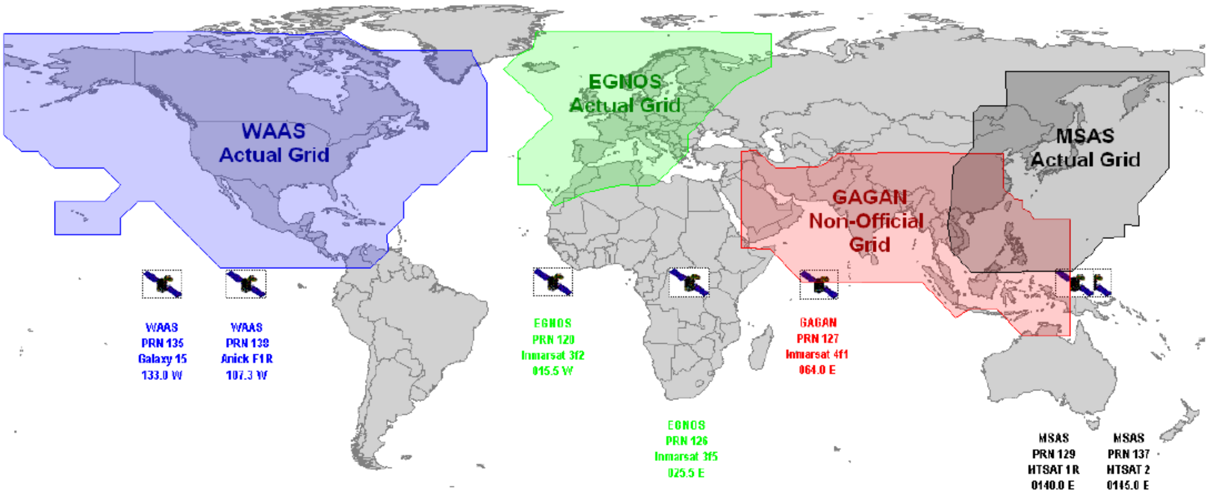

WAAS Actual Grid
EGNOS Actual Grid
MSAS Actual Grid
GAGAN Non-Official Grid
WAAS PRN 135 Galaxy 15 133.0 W
WAAS PRN 138 Anick F1R 107.3 W
EGNOS PRN 120 Inmarsat 3f2 015.5 W
EGNOS PRN 126 Inmarsat 3f5 025.5 E
GAGAN PRN 127 Inmarsat 4f1 064.0 E
MSAS PRN 129 HTSAT 1R 0140.0 E
MSAS PRN 137 HTSAT 2 0145.0 E

Figure 12: Coverages of various publically available SBAS systems.
(Source: Gakstatter (2008a))

Ground Based Augmentation Systems (GBAS), such as the US Local Area Augmentation System (LAAS), and Ground-based Regional Augmentation Systems (GRAS), such as Differential GPS (DGPS) networks available in many countries, consist of multiple reference antennas/receivers, a processing station and VHF/UHF data broadcast equipment. The GNSS signals received by the multiple reference/monitoring antennas are processed to obtain differential correction and integrity information, which are then broadcast via the VHF/UHF data link (Kaplan & Hegarty, 2006; Gakstatter, 2008a).

It should be noted that integrity monitoring and augmentation systems are dependent on GNSS for position indication and are not standalone services. They are therefore subject to interference, jamming and spoofing of GNSS, but may be able to provide a warning of malfunction (Volpe, 2001; IALA, 2004; Last, 2008).

In addition, continuous assessments should be made on the applicability of anti-jamming technologies, including adaptive antenna array, polarization discrimination and spatial-temporal filtering (Casabona & Rosen, 1999; Gustafon *et al.*, 2000; Deshpande, 2004; Loegering, 2006; Meng *et al.*, 2008), and counter-spoofing technologies, including amplitude discrimination, time-/angle-of-arrival discrimination and cryptographic authentication (Key, 1995; Wen *et al.*, 2005; Papadimitratos & Jovanovic, 2008; Humphreys *et al.*, 2009; Montgomery *et al.*, 2009; Ledvina et al., 2009).

5 CONCLUSION

Civilian GNSS signals are vulnerable to jamming, which blocks GNSS receivers from receiving navigation messages, and spoofing, which manipulates the location and time that the receivers compute. With increasing dependence on GNSS for positioning, navigation and timing synchronization, in order to avoid the possible consequences of intentional and unintentional attacks on GNSS signals, GNSS vulnerability mitigations steps should be given emphasis, including navigation/positioning/timing backups, making full use of ongoing GNSS modernization programs, increased ability to identify and locate GNSS jammers, integrity monitoring and augmentation, and anti-jamming and counter-spoofing technologies.

ACKNOWLEDGEMENT

The author is grateful to Dr. Mahdi Che Isa, Head of the Shipping Technology Branch, Science & Technology Research Institute for Defence (STRIDE), Mr. Eric Gakstatter, Principal, Discovery Management Group LLC, and Dr. Panagiotis Papadimitratos, Senior Researcher, Computer Communications and Applications Laboratory 1, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, for their suggestions that have helped improved this article.

REFERENCE

Adams, T.K. (2001). GPS Vulnerabilities. *Mil. Rev.*, **1**: 10-16.

Alkan, R.M., Kamman, H. & Sahin, M. (2005). GPS, GALILEO and GLONASS satellite navigation systems & GPS modernization. *2nd International Conference on Recent Advances in Space Technologies (RAST 2005)*, pp. 390-394.

Barnes, J., Rizos, C., Wang, J, Small, D., Voight, G. & Gambale, N. (2003). High precision indoor and outdoor positioning using LocataNet. *J. GPS*, **2**:73-82.

Basker, S., Grant, A., Williams, P. & Ward, N. (2008). The impact of GPS jamming on the safety of navigation. *Presentation to the Civil GPS Service Interface Committee*, 26th September 2008, Savannah, Georgia.

Blomenhofer, H., 2004. GNSS in the 21st century: The user perspective. *Acta Astronautica*, **5**: 965-968.

Brown, A., Atterberg, S. & Gerein, N. (2000). Detection and location of GPS interference sources using digital receiver electronics. *Proceedings of ION Annual Meeting*, June 2000, San Diego, California.

Casabona, M.M. & Rosen, M.W. (1999). Discussion of GPS anti-jam technology. *GPS Solut.*, **2**: 18-23.

Chang, C.C., Lou, P.C. & Chen, H.Y. (2008). Designing and implementing a RFID-based indoor guidance system. *J. GPS*, **7**: 27-34.

Clynch, J.R., Parker, A.A., Badger, G., Vincent, W.R., McGill, P. & Adler, R.W. (2003). The Hunt for RFI: Unjamming a Coast Harbor. Available online at: http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=43404 (Last access date: 4th November 2009).

de Oliveira, H.A.B.F., Nakamura, E.F., Loureiro, A.A.F. & Boukerche, A. (2005). Recursive position estimation in sensor networks. *Proceedings of the 14th International Conference on Computer Communications and Networks 2005 (ICCCN 2005)*, pp. 557-562.

Dempster, A. (2009). QZSS's indoor messaging system: GNSS friend or foe? *Inside GNSS*, **4**:37-40.

Department of Army (DOA) (2009). Electronic Warfare in Operations. Army Field Manual 3-36, Department of Army, Washington D.C.

Department of Defense (DOD), Department of Homeland Security (DHS) & Department of Transport (DOT) (2008). 2008 Federal Radionavigation Plan. US Federal Government.

Deshpande, S.M. (2004). Study of Interference Effects on GPS Signal Acquisition. Masters thesis, University of Calgary, Calgary, Alberta.

Dufresne, C., Hansen, A., O'Neill, K., Parmet, J. & Volchansky, L. (2008). Global Positioning System (GPS) receiver autonomous integrity monitoring (RAIM) web service to support area navigation (RNAV) flight planning. *Institute for Navigation National Technical Meeting 2008*, 28th-30th January 2008, San Diego, California.

Ekahau (2008). Ekahau RTLS. Ekahau Inc., California.

Fernandez, T.M., Rodas, J., Escudero, C.J. & Iglesia, D.I. (2007). Bluetooth Sensor Network Positioning System with Dynamic Calibration. *4th International Symposium on Wireless Communication Systems 2007 (ISWCS 2007)*, 17th-19th October 2009, Trondheim, Norway.

Forssell, B. (2005). GPS/GNSS indoors: Possibilities and limitations. *GPS/GNSS Seminar of the Swedish National Survey*, March 2005, Gävle, Sweden.

Gakstatter, E. (2008a). Introduction to GNSS. *GNSS Technology Workshop*, 10th-12th December 2008, Institut Tanah Dan Ukur Negara (INSTUN), Behrang, Perak.

Gakstatter, E. (2008b). Solar Activity: Is There Aspirin for This GNSS Headache? Available online at: http://sc.gpsworld.com/gpssc/article/articleDetail.jsp?id=555255 (Last access date: 4th November 2009).

Gakstatter, E. (2008c). Is Dual-Frequency GPS — As We Know It — Becoming Obsolete? Available online at: http://sc.gpsworld.com/gpssc/ArticleStandard/Article/detail/521868 (Last access date: 4th November 2009).

Gakstatter, E. (2008d). So, You've Been Hearing About L5. Available online at: http://sc.gpsworld.com/gpssc/article/articleDetail.jsp?id=517961 (Last access date: 4th November 2009).

Gakstatter, E. (2009). Personal communication.

Gakstatter, E. & Flick, J. (2006). Navigating the World of GNSS. Available online at: http://www.geospatial-solutions.com/geospatialsolutions/Article/Navigating-the-World-of-GNSS/ArticleStandard/Article/detail/318856 (Last access date: 4th November 2009).

Gibbons, G. (2006). GNSS trilogy: Our story so far. Inside GNSS. *Inside GNSS*, **1**: 25-32.

Gibbons, G. (2008). GPS and regime changes: Part 1-The Bush legacy. *GNSS World*, **3**: 20-23.

Gibbons, G. (2009). GPS and regime changes: Part 2-What lies ahead. *GNSS World*, **4**: 20-27.

Grant, A., Williams, P., Ward, N. and Basker, S. (2009). GPS jamming and the impact on maritime navigation. *J. Navigation*, **62**: 173-187.

GPS World (2007). Radical Change in the Air for GLONASS. Available online at:

http://www.gpsworld.com/gnss-system/news/radical-change-air-glonass-4336 (Last access date: 4th November 2009).

GPS World (2009a). Maritime Jamming Trial Shows GPS Vulnerabilities: eLoran shown to be 95 Percent Accurate. Available online at: http://tl.gpsworld.com/gpstl/Latest+News/Maritime-Jamming-Trial-Shows-GPS-Vulnerabilities/ArticleStandard/Article/detail/584318?ref=25 (Last access date: 4th November 2009).

GPS World (2009b). Three GLONASS Satellites Set for October 29 Launch. Available online at: http://www.gpsworld.com/gnss-system/glonass/news/three-glonass-satellites-set-october-29-launch-9034 (Last access date: 4th November 2009).

Government Accountability Office (GAO) (2009). Global Positioning System: Significant Challenges in Sustaining and Upgrading Widely Used Capabilities. Report to the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives, Government Accountability Office (GAO), U.S.

Gustafon, D., Dowdle, J. & Flueckiger, K. (2000). A high anti-jam GPS-based navigator. *Proceedings of the Institute of Navigation*, 28th-30th June 2000, Cambridge, Massachusetts.

Hähnel, D., Burgard, W., For, D., Fishkin, K. & Philipose, M. (2004). Mapping and localization with RFID technology. *International Conference on Robotics & Automation*, April 2004, New Orleans, Louisiana.

Hanlon, B.O., Ledvina, B., Psiaki, M.L., Kintner. P.M. & Humphreys, T.E. (2009). Assessing the Spoofing Threat. Available online at: http://www.gpsworld.com/defence/security-surveillance/assessing-spoofing-threat-3171?page_id=1 (Last access date: 4th November 2009).

Harding, S.J. (2001). Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System. QinetiQ Group, Buckingham Gate, London.

Hewitson, S. (2003). GNSS receiver autonomous integrity monitoring: A separability analysis. *16th International Technical Meeting of the Satellite Division of the U.S. Institute of Navigation*, 9th-12th September, Portland, Oregon.

Hewitson, S. & Wang, J. (2006). GNSS receiver autonomous integrity monitoring (RAIM) performance analysis. *GPS Solut.*, **10**: 155-170.

Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., & Kintner, J. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *ION GNSS 2009*, 16th-19th September 2008, Savannah International Convention Center, Savannah, Georgia.

Humphreys, T.E., Psiaki, M.L. & Kintner, P.M. (2009). GPS Spoofing Threat. Available online at: http://www.telecomasia.net/article.php?id_article=12288&page=4 (Last access date: 4th November 2009).

Inside GNSS (2009). GLONASS Launch Postponed until February. Available online at: http://www.insidegnss.com/node/1718 (Last access date: 4th November 2009).

Institute for Defense Analyses (IDA) (2009). Independent Assessment Team (IAT): Summary of Initial Findings on eLoran. Institute for Defense Analyses (IDA), Alexandria, Virginia.

Institute of Navigation (ION) (1998). RAIM: Requirements, Algorithms, and Performance, Global Positioning System. Papers Published in NAVIGATION, Volume V, Institute of Navigation, Fairfax, Virginia.

International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (2004). IALA Recommendation R-129 On GNSS Vulnerability and Mitigation Measures. International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), Saint Germain en Laye, France.

Jewell, J. (2007). GPS Insights. Available online at: http://www.gpsworld.com/defense/gps-insights-april-2007-8428 (Last access date: 4th November 2009).

Jewell, J. (2009). Time for GPS 101. Available online at: http://mg.gpsworld.com/gpsmg/ArticleStandard/Article/detail/608873 (Last access date: 4th November 2009).

Johnston, R.G. & Warner, J.S. (2004). Think GPS offers high security? Think again! *Business Contingency Planning Conference*, 23rd-27th May 2004, Las Vegas, Nevada.

Joint Chief of Staffs (JCS) (2007). Geospatial Electronic Warfare. Joint Publication 3-13.1, Joint Chief of Staffs, USA.

Kaplan, E.D. & Hegarty, C.J. (2006). Understanding GPS: Principles and Applications, Artech House, Norwood, Massachusetts.

Kawaguchi, N. (2009). WiFi location information system for both indoors and outdoors. *Lect. Notes Comput. Sci.*, **5518**:638-645.

Kemppainen A., Haverinen J. & Röning J. (2006). An infrared location system for relative pose estimation of robots. *16th CISM-IFToMM Symposium of Robot Design, Dynamics, and Control (ROMANSY 2006)*, 20th-24th June, Warsaw, Poland, p. 379-386.

Key, E.L. (1995). Techniques to counter GPS spoofing. Internal memorandum, MITRE Corporation, 17th February 1995.

Last, D. (2008). Navigation satellite systems: The present imperfect. *20th Anniversary Congress of Dutch Pilots (Loodswesen)*, 1st September 2008, Noordwijk, Netherlands.

Lilley, R., Church, G. & Harrison, M. (2006). GPS Backup for Position, Navigation and Timing: Transition Strategy for Navigation and Surveillance. Aviation Management Associates Inc., Alexandria, Virginia.

Locata Corporation (2003). Locata Technology Primer, Version 1.1. Locata Comporation, Australia.

Ledvina, B., Montgomery, P., & Humphreys, T. (2009). A multi-antenna defense: Receiver-autonomous GPS spoofing detection. *Inside GNSS*, **4**: 40-46.

Loegering, G.S. (2006). Dual-resistant antijamming architecture for GPS-guded air vehicle navigation system. *Technol. Rev. J.*, **14**: 1-10.

Manandhar, D., Okano, K., Ishii, M., Asako, M., Torimoto, H., Kogure, S. & Maeda, H. (2008). IMES (Indoor Messaging System): A proposal for new indoor positioning system. *Third Meeting of the International Committee on Global Navigation Satellite Systems*, 8th-12th December 2008, Pasadena, California.

McDonald, K.D. (2002). The modernization of GPS: Plans, new capabilities and the future relationship to Galileo. *J. GPS*, **1**: 1-17.

Meng, D., Feng, Z. & Lu, M. (2008). Anti-jamming with adaptive arrays utilizing power inversion algorithm. *Tsinghua Sci. Technol.*, **13**: 796-799.

Montgomery, P., Humphreys, T.E. & Ledvina, B.M. (2009). A multi-antenna defence receiver-autonomous GPS spoofing detection. *Inside GNSS*, **4**: 40-46.

Muneyuki, S., Yoshihiro, Y., Masataka, I., Yoshitsugu, M. & Kunihiro, C. (2003). Priority roll-call for active IR-tag location system. *Proceedings of the Annual Conference of the Institute of Systems, Control and Information Engineers*, Vol. 47, pp. 301-302.

NASA (2006). Solar Storm Warning. Available online at: http://science.nasa.gov/headlines/y2006/10mar_stormwarning.htm (Last access date: 4th November 2009).

Oberst, T. (2006). Solar Flares Cause GPS Failures, Possibly Devastating for Jets and Distress Calls, Cornell Researchers Warn. Available online at: http://www.news.cornell.edu/stories/Sept06/solar.flares.gps.TO.html (Last access date: 4th November 2009).

Papadimitratos, P. & Jovanovic, A. (2008). Protection and fundamental vulnerability of GNSS. *International Workshop on Satellite and Space Communications 2008 (IWSSC'08)*. 1st-3rd October 2008, Institut Supérieur de l'Aéronautique et de l'Espace (ISAE), Toulouse, France.

Pinker, A. & Smith, C. (2000). Vulnerability of GPS Signal to Jamming, *GPS Sol.*, **3**: 19-27.

Poisel, A.R. (2002). Introduction to Communication Electronic Warfare Systems. Artech House, Boston.

Revnivykh, S. (2007). GLONASS status & development. *Civil GPS Service Interface Committee (CGSIC) Meeting*, 24th-25th September 2009, Fort Worth, Texas.

Revnivykh, S. (2008). GLONASS status & progress. *3rd Meeting of the International Committee on GNSS (ICG)*, 8th-12th December, 2008, Pasadena, California.

Rizos, C. (2009). Generation next. *GIS Dev.*, **13-11**: 20-24.

Rogers, C. (1991). Development of a low cost PC controlled GPS satellite signal simulator. *Proceedings of the 15th Biennial Guidance Test Symposium*, Holloman AFB, New Mexico.

Satoshi. K., Hiroaki, M., Makoto, I., Manandhar, D. & Kazuki, O. (2008). The concept of the Indoor Messaging System. *The European Navigation Conference ENC-GNSS*, April 2008, Toulouse, France.

Sergey, K., Sergey, R. & Suriya, T. (2007). GLONASS as a key element of the Russian positioning service. *Adv. Space Res.*, **39**:1539-1544.

Simonsen, K., Suycott, M., Crumplar, R., & Wohlfiel, J. (2004). LOCO GPSI: Preserve the GPS advantage for defence and security. *IEEE Aerospace Electron. Syst.*, **19**: 3-7.

Suryanarayana Rao, K.N. & Pal, S. (2004). The Indian SBAS system: GAGAN. *India-United States Conference on Space Science, Applications, and Commerce*. June 2004.

Tektronix (2008). H600 RF Hawk Signal Hunter. Available online at: http://www.tektronixcommunications.com/modules/communications/index.php?command=defaultPage&operation=displayDataSheet&catid=3300&id=595 (Last access date: 4th November 2009).

Volpe (2001). Vulnerability Assessment of the Transport Infrastructure Relying on the Global Positioning System. John A. Volpe National Transportation Systems Center, Department of Transport, Washington D.C.

Wen, H., Huang, P.Y.R., Dyer, J., Archinal, A. & Fagan, J. (2005). Countermeasures for GPS signal spoofing. *18th International Technical Meeting of the Satellite Division of the Institute of Navigation ION GNSS 2005*, 13th-16th September 2005, Long Beach Convention Center, Long Beach, California

Williams, S.F. (2006). Radar'd Out: GPS Vulnerable to High-Power Microwaves. Available online at: http://mg.gpsworld.com/gpsmg/article/articleDetail.jsp?id=320030 (Last access date: 4th November 2009).