Positioning, 2013, 4, 169-182
http://dx.doi.org/10.4236/pos.2013.42017 Published Online May 2013 (http://www.scirp.org/journal/pos)

Analysis of GNSS Interference Impact on Society and Evaluation of Spectrum Protection Strategies

Do Alexis Sanou, René Jr. Landry

Department of Electrical Engineering, École de Technologie Supérieure (ÉTS), Université du Quebec, Montreal, Canada.
Email: do-alexis.sanou.1@ens.etsmtl.ca

Received January 9th, 2013; revised February 12th, 2013; accepted March 3rd, 2013

ABSTRACT

Global Navigation Satellite System (GNSS) technology is growing fast in our society and new applications are being introduced at an unprecedented pace. The GNSS products provide worldwide and real-time services using precise timing information, positioning and synchronization technologies. Within years, GNSS applications are becoming more accurate and their precision opens doors to a wide range of applications. Nevertheless, these applications are susceptible to disruption in the operation of GNSS receivers when malfunctions, failures or interference occur. This paper's objective is to make an overall analysis of GNSS failure impact on society and therefore make a review of GNSS spectrum protection strategies. In the first three sections of this analysis, we survey GNSS applications, their importance and their criticality. While questioning the criticality of GNSS applications, we evaluate their impact on main critical infrastructures and particularly the risks of critical dependencies in case of failure or interference. In the last two sections, we investigate GNSS spectrum interference in relation to its effects on crucial infrastructures. We review the principal Radio Frequency Interference (RFI) sources leading to GNSS and satellite communications (SATCOM) spectrum issues. Alongside, we study various ways to mitigate RFI. This process is essential to further develop and standardize mitigation techniques and to ensure GNSS spectrum immunity against RFI.

Keywords: Critical Applications; Critical Infrastructures; GNSS; Mitigation Strategies; RFI; SATCOM

1. Introduction

The goal of this paper is to investigate the importance of GNSS civilian applications in our society. The acronym GNSS (Global Navigation Satellite Systems) is nowadays a common term used to point out current and future satellite-based navigation systems. GNSS can be described as a service based on satellite signals that enable high accuracy positioning and navigation.

While some systems (US-built GPS and the Russian GLONASS) are fully operational, others systems are still in development (European Galileo and Chinese Compass/BeiDou). These global navigation systems are backfilled with regional navigation systems (Indian IRNSS and Japanese QZSS) and augmentation systems like US WAAS, European EGNOS, Japanese MSAS and Indian GAGAN.

GNSS receivers are integrated in numerous applications and therefore they are increasingly forming part of human habits. They provide a strong impact for countries development. Applications using GNSS cover a large array of sectors including any kind of transport (road, air, maritime and rail), energy production and distribution, advanced technologies (timing, scientific survey, earth observation, network synchronization), safety of life (surveillance, defense, emergency and location-based services) and even social networking and recreation. GNSS technology is important in real-time prediction of real or possible critical situations and natural disasters. Moreover, GNSS applications are linked with all levels of human security in our society.

Satellite navigation is becoming an important part of everyday life. Every year, the whole market of GNSS products and services increases at an annual rate of about 25% [1]. Some previsions expect that in 2020 [2] more than 1 billion of satellite navigation units will be operating driven by growth in emerging economies. Some factors are facilitating the growing of GNSS applications: receivers are becoming more powerful, smaller, cheaper and easier to handle, emerging economies are growing,

etc.

In first section, we will precise the large array of GNSS applications. Our approach is to perform an analysis of GNSS applications and their criticality. In second and third sections, we will discuss the impact of GNSS critical applications on society via critical infrastructures. This investigation will show how deeply our society is becoming more dependent to GNSS applications. One of GNSS systems problems is its reliability. GNSS systems cannot work completely without fail. So in fourth section, we will highlight the principal sources of SATCOM and GNSS spectrum interference, the effect of its outage and its consequences. In fifth section, we will review current and new mitigation techniques capable of resolving SATCOM and GNSS spectrum interference issues.

2. Criticality of GNSS Applications

Nowadays, it is hard to find systems or structures that have not yet used the benefits of GNSS technology. GNSS can serve many applications or purposes. We choose to categorize GNSS applications in five main domains (refer to **Figure 1**).

2.1. Transportation Applications

The GNSS technology provides many applications useful for navigation purposes. These applications are divided into air transport, terrestrial transport and maritime transport.

Air transport applications are basically those dedicated to aviation and aeronautical. The majority of commercial aircrafts use GNSS units to assist pilot crew in every flight phase, from taxing, to take-off, en-route flying, precision and non-precision approaches. There are also applications coupled to radio navigation equipment to determine attitude, altitude, speed, distance, air traffic control, etc. The GNSS technology can be used in almost every climatic condition while reaching a safety level required. These performances can be reached thanks to GNSS accuracy, integrity and service continuity. Furthermore, the aviation applications are the ones which led to the development of satellite augmentation systems such as Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS).

Figure 1. Main categories of GNSS applications.

Terrestrial transport applications gather every application useful for road and railway guidance. Nowadays, the majority of GNSS users are dedicated to road applications such as in-car navigation, fleet management, urban traffic control, dynamic route guidance, collision avoidance, automated highway, lane control, etc. These applications provide the position of land vehicles to control its course, drive it until destination or locate it. Among railway applications, there are signaling and control for train, infrastructure data collection, train location, passenger information systems, train integrity and level crossing approach, etc. These applications are used to locate the position of the train and its wagons, to control its speed and position, to know the distance between wagons when they are separated, to control the cargo transport, to manage the itinerary of a fleet of trains and to provide the train location service to passengers.

The most important maritime transport applications are those dedicated to both coastal and open-sea navigation, inland waterway navigation, tugs and pushers, icebreakers, automatic collision avoidance, vessel traffic, cargo handling, traffic hydrography, dredging and construction, etc. In these applications, we can say that GNSS is used to determine the distance between ships, maritime trade routes and ports, weather conditions, water level, depth, avoid collisions between vessels, the dredging of rivers, perform underwater construction, and develop hydrographic charts of the seas and rivers.

2.2. Energy and Food Supply Applications

At present, many companies use GNSS technology for the survey of energy related fossil (oil, gas, etc.). These applications are useful for energy supply (fuel extraction, construction and mining) and food supply (fisheries, precise agriculture).

For energy supply, there are basically those applications dedicated to oil and gas production. These are exploration, appraisal drilling, field development, and support to production and post-production such as distribution, transportation, etc. These applications are used to locate oil deposits, synchronize sensors for drilling offshore assessment, identify hazards and delineate borders and pipelines. Industrial applications are dedicated to mining, civil engineering and construction.

As regards food supply applications, there are basically those useful to precise agriculture and fisheries. The precise agriculture applications include the positioning for yield monitoring, weed and pest control, soil sampling, and robotic agriculture. These applications are

used to control the application of fertilizers, pesticides, to guide the seeding and harvesting machines in an automated way to collect soil samples, to locate the position of the sample and to evaluate the performance of the floor. Among fisheries applications, we can mention the location of fishing grounds and fishery monitoring. These applications help locating rich fishing grounds, monitoring fishing activities, combat illegal fishing and monitor the amount of fish caught by fishermen. All these applications are excellent support to increase the food safety.

2.3. Advanced Technologies Applications

The GNSS technology provides many advanced technologies applications. These applications include timing applications and scientific applications.

Timing applications include telecommunications and network synchronization functions to control parameters, to locate faults and to adjust their time clocks. GNSS technology can provide synchronous and asynchronous technologies, using a time source (atomic clock) with appropriate accuracy, stability and reliability to operate effectively. Then, they impact communications, digital broadcasting, satellite monitoring, maintenance of international time standards and time calibration services.

Scientific applications of GNSS are widespread and include primarily land surveying, environmental and atmospheric monitoring, geodesy, precise time reference, geodynamics, geographic information systems, climate research and meteorology. They also include applications to support animal behavior studies, botanical specimen location. They are important to detect and interpret ground movement and deformation.

The GNSS is useful for monitoring of unmanned vehicles includes unmanned aerial vehicle, and autonomous vehicles.

2.4. Safety of Life Applications

The safety of life services have been tremendously increased with the support of GNSS technology in the domain of emergency, security, protection and defense.

Security and protection applications include tracking of vehicles and valuable cargoes, and covert tracking of suspects.

Emergency services include applications to monitor and track calls, search and rescue operations, personnel protection, dynamic route guidance for emergency vehicles (ambulances, fire workers, etc.).

2.5. Recreational Applications

This last part of GNSS applications gathers applications which are useful for personal and recreational hobbies. They played a key role in smartphones functions, in social networking, etc.

For example, there are recreational purposes such as location based services by using mobile phones to locate restaurants, cinemas, or other point of interest. GNSS recreational enable-devices come in many shapes and sizes to serve a variety of purposes. Commonly, they are low-cost units, less precise technology, user friendly and are integrated in small personal devices. For example, hikers, campers and outdoorsmen will require a portable system, while those who do a lot of driving will opt for a mounted unit. GNSS fitness systems designed for the wrist, capture distance and speed data, while mapping favorite routes for cyclists and runners. Mariners can rely on marine GNSS devices for onshore/offshore maps, and chart-plotting functions.

2.6. GNSS and Critical Applications

We can summarize the GNSS impact on services and activities and the minimal degree of performance needed to perform them properly. In reviewing GNSS main applications, they can be classified in different criticality categories [3]: Safety of life applications and Mission applications.

By definition, safety of life applications are those whose failures or errors may directly cause harm, injury or death to humans: aviation, rail, maritime, emergency management (ambulance, fire, police, search and rescue), traffic surveillance, personal protection, etc. Basically, these applications are vital to people health and integrity. Their main characteristics are the following: They must be error-free (high integrity) in any circumstances. They also need high availability and high continuity. At the end, because of their criticality, the devices intended for safety of life applications need strictly to be certified.

By definition, mission applications are those whose failures or errors may indirectly affect people integrity or health by causing destruction of system, damage property external to the system, or damage the environment. These applications are deemed vital to an organization's business success or existence. They need to be highly accurate, highly reliable and highly available. They regroup exhaustively industries such as: Oil and gas, mining, environment, space, construction/civil, fisheries, precision survey, precision agriculture, forecasting, geodesy, timing, fleet management, engineering, vehicle control and robotics. These kinds of services need high accuracy, high precision and high reliability GNSS receivers to perform.

GNSS technology can be related to numerous types of accidents. They are involved in distracted driving. For example, GPS devices being fallible, some errors can lead to outdated or inaccurate information for driving guidance and navigation. Because of these factors, GNSS devices can increase the risk of accidents and take brain

out of the driving equation or awareness. For example, it is estimated that GPS units have directly been involved in 300,000 car accidents only in the United Kingdom in 2008 [4]. In addition, virtually hundreds of thousands of civil aircrafts rely on GNSS devices.

GNSS applications can be classified as mission critical or safety critical, as it is shown in **Figure 2**. These two classes are not mutually exclusive, and several GNSS applications can be considered both mission and safety of life applications, as indicated by the intersection region of those ones. It is important to mention that a third category of criticality can be distinguished: business critical [5]. However, we believe that this eventual third part falls in the category of mission critical.

3. GNSS Impact on Critical Infrastructures

3.1. Critical Infrastructures

In society, a critical infrastructure is an area composed of equipment and systems that require support of critical functions (applications) to satisfy basic societal needs and provide public safety. The critical infrastructures are vital to the nation's security, economy, and survival. There are 8 categories of critical infrastructures (Thomas, 2011), which include the following sectors (refer to **Figure 3**):

- Information and communications services: This sector is an integral component of economy underlying the operations of all businesses, public safety organizations, and government. It provides critical control systems and services, physical architecture and Internet infrastructure. Over years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. GNSS technology is central to network synchronization, encryption, positioning and time transfer. The information and communications sector is closely linked to other sectors: Energy (power to run cellular towers, central offices, and other critical communications facilities), finance (transmission of transactions and operations of financial markets), emergency (directing resources, coordinating response, alerting the public, and receiving emergency 911 calls) and transportation (control systems, tracking shipments, and regular communications requirements).
- Financial services: also known as banking and finance, this sector represents a vital component of nation's critical infrastructure. Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyber-attacks demonstrate the wide range of potential risks the sector faces. GNSS timing application is well used for encryption, legal time traceability, and internet timing. These functions allow financial institutions to provide a broad array of products from the largest institutions to the smallest community banks and credit unions.
- Water supply and environmental protection: the water sector is vulnerable to a variety of attacks, including contamination with deadly agents, physical attacks such as the release of toxic gaseous chemicals and cyber-attacks. There is no apparent direct involvement nowadays but in the future, with the water resources question becoming more crucial, GNSS tracking-capabilities will be needed. GNSS technology also uses code and carrier phase measurements for botany, geomorphology, geology, and hydrology. GNSS observations play a key role to perform real-time weather predictions such as change of sea level, tsunami alerts, etc.
- Transportation and shipping: GNSS is used in virtually every mode of transportation; many include safety

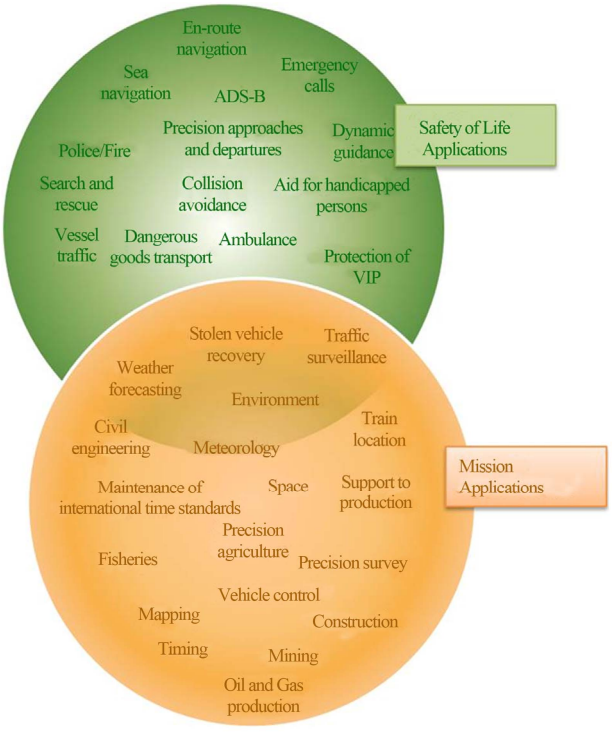

Figure 2. Classification of GNSS applications by criticality.

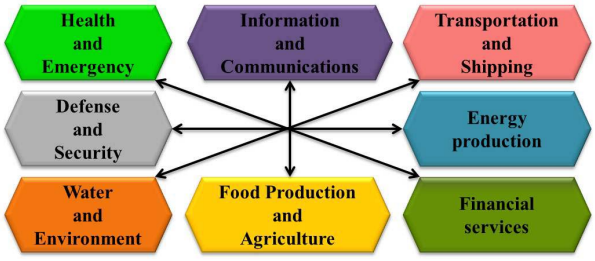

Figure 3. Social Critical Infrastructures.

of life. The transportation system quickly, safely, and securely moves people and goods through the country and overseas. The transportation sector consists of eight key subsectors, or modes: aviation, maritime, pipeline systems, freight rail, mass transit, passenger railway, motor carrier and highway infrastructure. The shipping sector moves messages, products, and financial transactions each day. Every sector of the economy depends on service providers in the transportation and shipping sector to deliver time-sensitive letters, packages, and other shipments. In particular, the banking and finance, commercial facilities, government facilities, and healthcare and public health sectors rely heavily on the shipping sector for the shipment and delivery of critical documents and packages. Major interdependencies with other sectors include those with the communications, energy, information technology, and transportation sectors.

- Health and emergency services: systems of prevention, preparedness, response, and recovery elements, the health and emergency sector represents the first line of defense in the prevention and mitigation of risks from terrorist attacks, man-made incidents, infectious disease outbreaks, and natural disasters. GNSS timing is becoming important for telemedicine, critical for the location of downed aircraft, car accidents, and maritime rescue. Also it is used in the dispatch and control of public safety vehicles for more efficiency in emergency cases management. This sector also serves in a unique capacity as the primary protector for all critical infrastructure sectors. While healthcare tends to be delivered and managed locally, the public health component of the sector, focused primarily on population health, is managed across all levels from national, state to local level. Encompassing a wide range of emergency response functions, the primary mission of emergency services is to save lives, protect property and the environment, assist communities impacted by disasters, and aid recovery from emergencies. These functions are defined by five areas (law enforcement, public works, emergency monitoring, medical services, and fire services).
- Energy production: the energy infrastructure is divided into three interrelated segments, including electricity, oil and natural gas. GNSS timing synchronizes electric power grid. It detects and precisely locates grid faults. For fossil energy (oil and gas) production and storage, GNSS is critical for monitoring large oil tankers in narrow waterways. The energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare are threatened, and the economy cannot properly function.
- Defense and security services: this sector includes local defense (police), national defense (army) and foreign intelligence. For internal defense, GNSS timing and positioning is becoming essential for Enhanced 911, precise incident location and reporting, emergency dispatch, encrypted communications, search and rescue operations, tracking dangerous people. For national defense, GNSS is essential in matters of war in order to mobilize, deploy, sustain military operations, improve the targets of attack and direct the troops in field operations. This sector also covers the industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapon systems, subsystems, and components or parts, to meet military requirements. For foreign intelligence, GNSS positioning and timing is used to spy hostile communications, to control systems, to geo-locate and to plan missions.
- Food and agriculture production: This sector has the capacity to feed and clothe people well beyond country boundaries. It has critical dependencies with many sectors, but especially with water, transportation systems, energy, banking and finance.

3.2. Connection between Applications and Infrastructures

The relationship between GNSS services and society can be explained by the following steps, graphically described by **Figure 4**:

- We know that a society is composed of many institutions. Some of them are critical, as we said previously. An example of critical infrastructure is health and emergency services with ambulances.
- We know that many elderly people in our society use health and emergency services for assistance or for public care. Some of these services use GNSS signals to track patient health via wireless devices (hearth, blood pressure, temperature, etc.). These services are critical, ambulances tracking, etc.
- So we can make the assumption that GNSS has an impact on critical health and emergency services (critical infrastructures) in our society.
- Knowing that GNSS is embedded in health services, emergency services, defense, transportation, financial, food production, energy production, environment

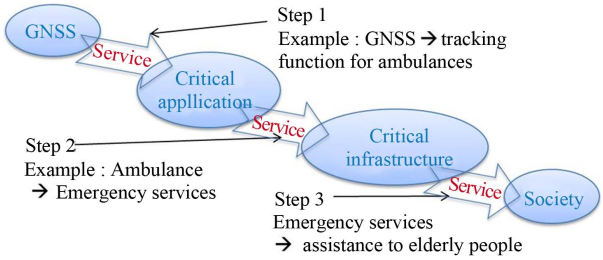

Figure 4. GNSS Impact on Society.

surveying, all sectors vital for society, we can conclude that GNSS services impacts the society via crucial infrastructures.

We must know the modifications generated by the GNSS system in society in order to understand the impact that society will suffer if the reception of GNSS signals is of poor quality due to interferences, if the GNSS system is disrupted or attacked by jamming, spoofing or meaconing.

3.3. GNSS Effects on Critical Infrastructures

Critical infrastructure, seeking the increased efficiencies made possible by GNSS, has also developed a reliance on GNSS that can lead to serious consequences if the service is disrupted and the applications are not prepared with mitigating equipment and procedures. There is a real dependency on GNSS services. If crucial infrastructures are affected (as it is described in **Table 1**), the people's confidence towards the systems will gradually lower.

Table 1. GNSS effects description on infrastructures.

Infrastructure	Effects description
Impact on Economy	Overreliance on GNSS signal is rampant for financial operations, inter-bank communications, transactions tracking, etc.
Impact on Health services	Failure in GNSS can disable search and rescue operations, prevent helping people who are in danger due to accidents, crimes, etc.
Impact on Communications	Failure of GNSS timing can provide desynchronization for internet and mobile networks.
Impact on Transportation	GNSS failure can affect air traffic control, highway navigation, monitoring of cargos traffic, etc. For example in aviation, safety can be put in jeopardy due to misinformation brought by GNSS signal to terrain awareness (EGPWS), ADS-B, map displays, traffic applications, alerting systems, etc.
Impact on Energy	GNSS failure can bring desynchronization into phasor measurement units and therefore affect precision and real-time measurements for power grids.
Impact on Environment	GNSS failure can disable alerts systems essential for natural disasters prevention. The errors can lead to injury, death, material losses and systems destructions. GNSS systems are used to forecast the weather. People follow a schedule depending on weather.
Impact on Defense	GNSS device error can prevent tracking emergency vehicles, tracking dangerous people wearing electronic bracelet, etc.
Impact on Agriculture	GNSS failure can lower farming equipment efficiency for planting, maintaining and harvesting fields. With lower efficiency, yields become worst, leading to lower monetary payback.

4. Sources of Space Spectrum Interference

The radio navigation by satellites technology is becoming more and more precise and accurate with years. But under some circumstances, GNSS receivers may fail to work properly. So what are the main sources of failure or malfunction a GNSS user can encounter?

4.1. Source No. 1: System Malfunction

GNSS system malfunction, without human interfering, can take place either in space segment or control segment. The space segment consists of the constellation satellites. These satellite or space vehicles emit radio signals. The main problem that could be potentially related to the space segment is the drop of operational satellites and a lack of backups (spare satellites). According to US Government Accountability Office reports, the failure of old space vehicles combined at a lack of sufficient backups could potentially reduce service, lead to disastrous accuracy in positioning and provoke more position outages. Another malfunction is related to the diffusion of bad navigation data. This problem can lead to misinformation about orbits prediction, clock predictions and affect severely the positioning accuracy. They are also some jumps or drifts of clock, bad signals shape, loss of satellites or interruption of satellite service [6]. The control segment installations (network of tracking stations and Masters Control facilities) can suffer physical attacks leading to the loss of satellite timing and controlling.

4.2. Source No. 2: Hazardous in Propagation Channel

The vulnerabilities at environment-level are related to the properties and characteristics of the signal. The GNSS signals powers are weak and have to be transmitted from great distance (about 20,000 km). For example, the GPS minimum power level at reception is usually between −150 dBW and −160 dBW. Also, the spectrum of received signal is below the noise level. For that purpose, the signal acquisition requires higher signal-to-noise ratio (SNR) than tracking. Before reaching the receiver, the GNSS signal is affected by reflections, scattering and diffraction in the propagation channel. The signals are affected by atmospheric disruption introduced by solar activity, magnetic storms, and scintillations in ionosphere or climatic conditions.

The atmospheric errors are separated in two categories: the ionospheric effect and the tropospheric delay. While the ionospheric effect is frequency dependent and caused by the region of the atmosphere between 50 and 1000 km above the surface of the Earth, the tropospheric delay is frequency independent, and it is caused by the lower part of the atmosphere, between the surface and 50 km.

Another main source of errors is multipath. Multipath

interference is caused by the phase difference between direct and reflected signals, or among reflected signals which cause confusion to the recipient at the time of recognition of information. Multipath causes gross errors in position accuracy.

4.3. Source No. 3: Unintentional Interference

The vulnerabilities introduced by accidental interference are created by external sources. We have harmonic emissions from high power transmitters, mobile satellite services, television, ultra wideband radar and personal electronic devices.

Another accidental interference is the saturation of the spectrum. Sometimes frequencies are over-used. New frequencies are allocated to newcomers in the same band of operation of GNSS. So they compete in the same spectrum as GNSS services. This can lead to interference situations.

4.4. Source No. 4: Intentional Interference

This kind of interference corresponds to the case of interference caused intentionally by sources impeding the receiver to receive the correct message. The three kinds of intentional interference that could occur are spoofing, meaconing and jamming. Of these ones, spoofing and meaconing are more dangerous because they can replace true information by false information.

Jamming is the intentional emission signal with enough power and characteristics to prevent the receiver to acquire and track the information within the area covered. The jammers can be simple or elaborated as those that sweep a frequency band. Mostly the military are the main responsible of GNSS signals disruption. They drive the research of jamming techniques, the design of jamming devices, the same we can obtain easily after in the black market. The jammers are too easily available and the risks related to them will increase within years. There are three classes of jammers: tones (single, continuous wave), pulses (e.g. Gaussian shaped from DME) and chirps (most commercial jammers).

Spoofing is a deceptive signal transmission in the same frequency as the real signal. The receiver treats the signal as real, when it is not. These false signals are intended to deceive or to saturate the receiver without it recognizing the effect.

The meaconing consists of receiving, delaying and broadcasting the signal in the same frequency as the real signal to confuse the navigation system and user. The meaconing implies knowledge of the victim receiver position. It is more sophisticated than jamming.

4.5. Source No. 5: Human Factors

The human factor can be divided into two parts: those from consumers and those from manufacturers or operators. They also regroup the user segment that consists of the association of GNSS receiver's users. According to [6], the vulnerabilities of GNSS user segment include the entire phenomenon that can affect the receiver device or the signals propagation. It is complex to review the vulnerabilities at this segment due to the large variety of devices and their functions (civil, military, scientific, alone or built-in other device, etc.). Also, the problem can affect one kind of manufacturer (software bugs, systems upgrades, etc.), or a specific area (jamming, interference, etc.). Generally, the receivers can encounter occasional roll-overs, overlay systems due to the variety of constellations (GPS, Galileo, Compass, GLONASS, etc.), second leaps, etc.

As said previously, the diversity of functions and the variety of GNSS receivers' devices introduce some complexity to vulnerabilities listing at this level. They extend from conception errors of design (user equipment, satellite design) to user mishandling (lack of knowledge, lack of tracking). In major cases, most people can't stand receiver interruptions or/and performance reduction because they basically don't understand GNSS vulnerability. In few cases people cannot handle GNSS receivers properly.

5. Space Spectrum Interference Mitigation Strategies

There is no magic bullet for cancelling undesired Radio Frequency Interference (RFI) from satellite communication and GNSS signals. The protection of satellite communications and GNSS requires a package of measures to deal with the various aspects of RFI: regulatory protection and efficient mitigation techniques.

5.1. First Strategy: Space Spectrum Protection

This proactive strategy allows avoiding RFI before their occurrence. Theoretically it is the best option, but it needs a strong discipline and organization to set up. The best strategies include negotiation, laws and regulations, radio quiet frequencies or zones, observatory modes and users crowdsourcing. For that purpose, RF spectrum management regulatory and standards bodies (agencies and authorities with local, federal and international jurisdiction) such as United States Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), and the International Telecommunications Union (ITU) would play a crucial role in keeping satellite communication immunity against intentional interference (jamming and spoofing).

5.1.1. Negotiation Options

Regulatory and standard bodies with private stakeholders

must set up new spectrum management approaches focusing on spectrum efficiency and receivers performance. In facts, the deployment of new services and technologies can negatively impact existing services. To conduct negotiation strategy about satellite spectrum issues, three kinds of solutions are proposed: Establishing new regulations for new entrants and incumbents, modifying existing regulations between incumbents, or reinforcing existing regulations between interferers and victims.

For that purpose, some spectrum interference standards must be driven to reduce conflicts between legacy stakeholders and new entrants. This option must anticipate and solve interference issues between new cellular radio systems and public safety radio systems, between unlicensed wireless systems and radar systems, between terrestrial networks services and mobile satellite spectrum (including GNSS).

5.1.2. Standardization Options

Regulatory bodies and manufacturers must strengthen technical standards and certifications for electronic equipment working on frequencies close to those used by GNSS.

Technically, some adjacent bands can be redefined and added to mobile satellite spectrum to protect signals and ensure that any further services can be safely implemented without affecting existing services. This should include protection bands of frequency in order to define the bandwidth needed for an optimal performance. This alternative would reduce the necessity to involve regulators, lead to win-win solutions and avoid past examples such as LightSquared cases on GPS L1 band [7].

Also, regulatory bodies can map out the allowable power limits for those electronic devices. The power limit determinations would take into account how far away the working frequency is from the GNSS band. The goal is to maintain current protections for GNSS receivers while building more interference-tolerant receivers. This alternative would ensure compatibility among satellite spectrum users and minimize the occurrence of RFI or EMI (Electromagnetic interference).

5.1.3. Legal Measures Options

In a civil society, the role of laws is to protect individual and common interests. Official authorities should reinforce regulations and laws in order to discourage spectrum intentional interference. Monetary penalties or material seizure can be raised against illegal violation, especially for those that put safety-of-life systems at risk. Laws are needed at the highest level and must become stricter against intentional interference to discourage jamming/spoofing devices selling, advertising and casual operations. This option is mandatory because the use of jamming/spoofing devices affects crucial infrastructures (airports, 911 emergency calls, vehicle navigation and tracking, aircraft navigation, etc.) and can place people life in danger [8].

5.1.4. Radio Quiet Zones (or Frequencies) Options

To establish radio-quiet zones, a call for protection from many levels is required from global regulatory protection (ITU Radio Regulations), local protection (regulations at national level), and self-protection (computers, electronics associated with telescope control, signal processing).

A radio quiet zone is made of two zones [9]: An exclusion area in which all radio emissions are prohibited, with restrictions on housing and industrial developments; and a larger coordination area where the power of radio transmissions is limited. The electronic and electrical equipment that is used inside the radio quiet zone themselves can also potentially interfere with our own observations. To prevent this, computers and electronic devices can be enveloped in a Faraday cage, or in rooms or even in entire buildings shielded against radio noise that may leak out.

The aim is to establish an area (or a spectrum band) within which any electrical installation or equipment is subject to control or coordination. This alternative would obviously decrease unintentional interference by a selection of the most suitable locations or spectral bands frequencies. Priority should be directed towards critical infrastructures services in order to protect public safety. Today, satellite signals can be easily masked by local signals due to their lower power. To fulfill satellite spectrum protection, satellite communications and GNSS require a greater allocation of spectrum for their services, more advanced radio telescopes, and more protection. Some remote areas can be set up locally using local regulations to restrict housing and industrial developments in the vicinity of a radio observatory and to restrict the use of electrical equipment [9].

5.1.5. Customers Crowdsourcing Options

According to reports [2], GNSS chipsets are expected to approach 1 billion units by 2020. Thus, many customer devices can be used as a jamming/spoofing detector. Some intelligent networks and receivers (e.g. smartphones) can interact to report RFI events to customers and ensure protection against hazardous misleading information. [10] describes the J911 system concept that is an anti-jamming technique using crowdsourcing approaches. These approaches use a multitude of opportunistic observers based on cellphones to provide time and location specific alerts. Even though the individual measurements have poor accuracy, the crowd community offers reasonably good accuracy and wide geographic coverage to detect jamming source and determine jammer location.

5.2. Second Strategy: Spectrum Interference Monitoring

5.2.1. Geo-Location Techniques

The techniques for achieving location of RFI sources exploit the characteristics of radio wave propagation and multi-rate digital signal processing methods to determine the geographical origin source of RFI in satellite communications.

- Time-of-Arrival (TOA) technique is the one-way propagation time of the signal travelling at speed of light between a source and a receiver. TOA estimation allows the measurement of distance, thus enabling localization. These location techniques exploit time delays and are based are based on the estimation of the cross-correlation peak of the received signal and locally generated replicas [11,12].
- Time-Difference-of-Arrival (TDOA) techniques estimate the difference in arrival times of the emitted signal received at a pair of antennas, implying that clock synchronization is required. It is the time difference between two received signals from a single transmitter, each propagated through a different satellite. The two signals travel two different path lengths, so they arrive at different times. More accurate and much simpler than TOA techniques, TDOA choose for a single-emitter the delay that maximizes the time-domain cross-correlation function. However, for multiple emitters, analysis of the cross-power spectral density offers better resolution because of powerful subspace methods [11,13].
- Power-of-Arrival (POA) techniques exploit variations in power radio wave characteristics as signal propagates. They use the relative power of arrival of a signal, and measure the strength of the received signal via the path attenuation loss. Combined with signal propagation modeling and historical calibration data, radio signal power-of-arrival can be normalized at the receiver, leaving only the path-loss between the device and the receiver [11].
- Power-Difference-of-Arrival (PDOA) techniques also exploit variations in power radio wave characteristics as signal propagates. These techniques use the absolute differences in received radio power at multiples receivers to compute a position. However, these techniques require that receiver locations must be known a priori. Signal propagation modeling or historical calibration data can be used to improve the location estimate [11].
- Angle-of-Arrival (AOA) techniques measure the direction from which a source of RF energy appears to originate. They permit to point to the direction from which the RF energy originated. A unique location can be estimated by determining the AOA by drawing two or more lines of bearing from different receivers [11].
- Frequency-Difference-of-Arrival (FDOA) techniques exploit radio waves frequency shifting and Doppler effects. They use the difference in received frequency between two signals from a single transmitter propagated through two different satellites. FDOA is the result of differences in the satellites' oscillator frequency offset and drift, and different Doppler shifts caused by satellite motion [11,14].
- Ephemeris Error Compensation (EEC) Algorithms:

Ephemeris error also contributes to location error, so location techniques can exploit Ephemeris Error Compensation (EEC) Algorithms. EEC algorithms use above-the-noise-floor communications waveforms as calibrators to calculate improved satellite ephemeris.

5.2.2. Characterization Techniques

The following are main techniques used to detect and characterize RFI. The list below is not exhaustive:

- Fast Fourier Transform (FFT), which directly transforms a signal into its spectral representation. It is a powerful method in narrowband and continuous wave Interference mitigation.
- Short Time Fourier Transform (STFT), based on the Fourier Transform (FT), which gives information about frequency and time of the signal.
- Welch's Method is used to estimate the power of a signal at different frequencies: that is, it is an approach to spectral density estimation.
- Karhunen-Loève Transform (KLT) technique [15] has very high potential and can outperform the classical signal detection methods that are used today. The KLT is equally capable of detecting both narrowband and wideband signals, which deserves close attention if we think of future applications in the field of GNSS.
- Analysis of the instantaneous phase [16] is a classic method for automatic modulation classifiers in the field of Signal Intelligence (SIGINT) for military applications. Based on the dependence of phase statistical properties on the signal modulation, this method proposes to measure some statistics of the signal and perform the signal characterization according to an ad hoc hierarchical decision tree.

5.3. Third Strategy: Receiver Interference Mitigation

The **Figure 5** describes the main points of interference mitigation in a generic GNSS receiver. There are:

5.3.1. RFI Detection (1)

Detection techniques can be classified into two categories: detection techniques based on deterministic methods that exploit known properties of the signals such as

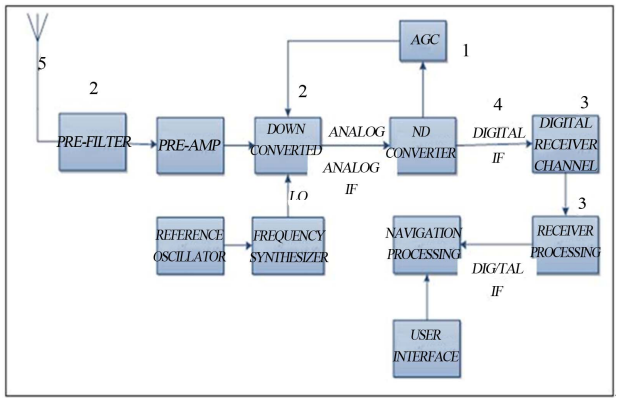

Figure 5. Generic GNSS receiver and points of interference reduction.

modulation type or certain periodicities, and detection techniques based on statistical models with unknown parameters.

- Jammer-to-noise power ratio (J/N) meter: Implemented at the automatic gain control (AGC) area, the J/N meter sensor provides a measure of the level of RF interference that passes through the antenna and the receiver amplifier. GNSS signals are below the thermal noise, so the J/N meter will detect an RFI which energy levels are above normal [17].
- ADC/AGC monitoring technique: Automatic Gain Control (AGC) is an adaptive variable gain amplifier which aims to minimize the quantization losses. AGC is required anytime multi-bit quantization is implemented. It is driven by thermal noise rather than GNSS signal energy. The AGC system provides an accurate estimate of Jammer-to-noise power ratio (J/N), and based on this value we can estimate the relationship Jammer-to-noise power ratio (J/N) [17]. Adaptive Analog-to-Digital (A/D) conversion can reduce constant envelope interference effects. The GNSS receiver can have an adaptive A/D to improve its performance under CWI. The adaptive A/D can adjust its signal threshold according the receiver power.
- Time domain techniques: These techniques are based on statistical tests on useful measurements (power, jitter variance, etc.) at the output of correlation unit.
- Frequency domain techniques: These techniques are based on spectral estimation and a threshold determination on the estimated power spectral density. There are Kurtosis detection, cross-frequency detection and more.
- Transformed domain techniques: These techniques are implemented in order to represent the received signal in a different domain where the useful part can be split from the RFI. There are Time-Frequency domain and Time-Scale domain such as Karhunen-Loève Transform (KLT). The KLT is a data mining procedure to convert a set of observations of correlated variables into a set of values of linearly uncork-related variables called principal components [15].

5.3.2. Front-End Filtering Techniques (2)

- Passive filtering is a pre-correlation technique. Front-end filtering protects GNSS receivers from high-powered emissions that are out-of-band. The disadvantage of installing a passive filter between the antenna and the pre-amplifier is that for every 1 dB of insertion loss, it adds 1 dB to noise figure. This, in turn, reduces the tracking threshold by 1 dB.
- PIN diodes before pre-amplifier: To limit the high-energy pulses which can generate harmonics that could be within the range of GPS, PIN diodes can be implemented before the pre-amplifier. A PIN diode will act as a limiter and cut high energy pulses.
- Additional filters at LO stage: In addition to the above pre-filtering, filtering can also be applied before and after each stage of the local oscillator (LO), increasing the narrow band filtering.

5.3.3. Code/Carrier Tracking Loop Techniques (3)

These techniques improve the lock threshold in the code and tracking loops and are post-correlation techniques. They are implemented in the digital receiver channels and the receiver processor. The threshold of lock improvement reduces the carrier phase tracking and code loop filter bandwidth. This also reduces the dynamics of the line of sight that each channel can tolerate. This reduction in the dynamics can be mitigated by increasing the loop filter order or providing support from an external system to the tracking loops [18].

- Adaptive Tracking Loop bandwidth: The in-band interference can be reduced by decreasing the carrier-tracking loop bandwidth and thus improving the tracking threshold. If the tracking loop bandwidth is properly adjusted, according to the interference power, higher anti-jam margins can be obtained, but the consequence it's a lower performance to Doppler effects [18].
- Loop Aiding techniques are used to narrow loop bandwidths of GNSS receiver thereby increasing its robustness in presence of RFI and when GNSS signal carrier-to-noise C/N0 is reduced.
- Vector Tracking techniques combine the outputs of the tracking loops, in such a way that each tracking loop update is also based on information from the other tracking loops. The information from several satellites can be used to recover the information of the weaker signals. The GNSS receiver can also use the combined information of the satellites to compute the dynamics of the receiver, and then it can be used to help the tracking loops, reducing the bandwidth of the tracking loop [19].

- Data Wiping technique consists in removing the navigation data from the received signal so that longer coherent integration times are enabled in order to improve the receiver sensitivity. This technique is more effective when the GNSS receiver has already a high anti-jamming immunity. The data wiping can improve the tracking threshold of GNSS receivers by up to 6 dB [20].
- Code Tracking Loop techniques are part of internal navigation aiding enhancements. The carrier loop helps the code loop to reduce its bandwidth and the thermal noise on the pseudo-range measurements, which in turn enhances the navigation accuracy [20].
- Carrier Tracking Loop techniques are part of internal navigation aiding enhancements. They can provide accurate velocity aiding to the closed carrier tracking loop, thereby removing dynamics from the carrier tracking loop. The carrier tracking loop, in turn, aids the code tracking loop [18].
- Open Carrier Tracking Loop Aiding: The receiver carrier tracking loop can be opened while the carrier numerically controlled oscillator (NCO) being maintained with external velocity aiding. Using external velocity aiding in the code tracking loop, the code loop filter bandwidth decreases and the improvement against wideband (Gaussian) jammers is achieved [18].

5.3.4. Signal Processing Techniques (4)

- Pulse Blanking techniques and data flagging techniques can also remove RFI from signal by blanking some parts of its spectrum. This reactive strategy excises the RFI data from corrupted/degraded bands of signal spectrum.
- Adaptive filtering techniques often need to be adaptive because of the dynamic or changing characteristics of interference and propagation channel. A filter designed in hardware or software device is applied to a set of satellite data stream to extract statistical parameters. The goal of this method is to find some statistical characteristics signatures that discriminate RFI from signal-of interest. Among adaptive filtering algorithms, there are amplitude domain filtering in time (ADP) and frequency (FADP), filters based on Wiener algorithms, filters based on Least Mean Squared (LMS) algorithms, and more.
- FFT/Temporal Domain Filters (Notch Filters): These filters notch narrowband interferences in the frequency domain without disturbing too much the GPS signals. The notch filter implementations are classified in FFT based filters (Overlapped FFT based, filter bank) or in temporal domain filters (Finite Impulse Response, FIR, or Infinite Impulse Response, IIR). Some examples of algorithms are: the sign algorithm, the plain gradient algorithm, the normalized gradient algorithm, the recursive prediction algorithm, the lattice algorithm, the P-Power algorithm and the memory-less non-linear gradient algorithm.

5.3.5. Antenna Enhancements (5)

Antennas based techniques, mainly beam forming and null steering, belong to the field of adaptive spatial processing and are the only effective means against broadband interference. These techniques require however multi-element antenna arrays. A dual polarization antenna is another innovate technique that can achieve best anti-inference margins against interference waveforms [21] while requiring only a single antenna device. It belongs to the class of the spatial filtering techniques. Antenna enhancements techniques can be classified in antenna pattern enhancement and antenna polarization techniques.

- Reception pattern enhancement techniques are composed of more than one radiating element and they can reject broadband interferences. This technique changes the radiation pattern of the antenna according to the needs of cancelling jammers.
- Beamforming techniques: This general approach for cancelling interfering signals is also known as a nulling antenna system. In this technique, the spatial filter uses an antenna array connected to a single beamformer whose output is fed into a GNSS receiver. We can imagine the antenna array and the beamformer as a single antenna element with an adjustable beam pattern.

5.4. Fourth Strategy: Space Weather Mitigation

5.4.1. GPS Modernization

The main alternatives are to add new frequencies (such as GPS L2C) to enhance both scintillation and Total Electron Content (TEC) monitoring. For that purpose, GPS will add open-coded L2C (at L2) and L5 (1176.45 MHz) signals as satellites are replenished (L2C on 8 block IIR-M satellites, L2C and L5 on all subsequent Block IIF satellites). Also, future SBAS GEOs will broadcast at L1 and L5. Similarly, Galileo will have open-coded signals at L1 and at L5 frequencies. Another alternative is to add new payloads with more significant power [22].

5.4.2. Enhancement of GNSS Signal Tracking

This solution seeks to perform the three stages of signal tracking in receivers where they are not implemented. The first stage is to perform a re-acquisition of signal if signal not detected. If the signal is detected, in second stage, the frequency lock loop must be enhanced (amplitude measurements). If the code is locked then, in third stage, the phase lock loop (phase measurements) must be

enhanced [22].

5.5. Fifth Strategy: Spoofing and Meaconing Mitigation

There are several techniques to counter spoofing and meaconing. [23] seems to have investigated spoofing and spoofing countermeasures in detail in a internal memorandum for he MITRE Corporation. Some antispoofing techniques are being used to detect GNSS spoofers based on signal simulator: amplitude monitoring, time-of-arrival discriminator and consistency checks among different measurements [24].

5.5.1. Angle-of-Arrival Discrimination

For spoofing different approaches have been studied of which the angle-of-arrival discrimination is probably the most efficient. Matching the angle-of-arrival of the satellite signal is almost impossible for the spoofer. This technique requires however a multi-element antenna. The phase difference between the two antennas is monitored over time. It can be observed that the phase difference changes due to the satellite motion and the rate of phase difference is proportional to the baseline length. The expected carrier phase differences can be calculated and compared to the measured delta phases. The carrier phases did not change over time, indicating the presence of a malicious transmitter.

5.5.2. Inertial Measurement Unit (IMU) Cross Check

It is basically a consistency cross check with IMU navigation. GNSS Navigation data are cross-checked and corrected in real-time with IMS data.

5.5.3. Polarization Discrimination

This technique requires only a single antenna aperture and belongs to the class of the spatial filtering techniques. In comparison, post-correlation methods on the other hand comprise enhanced signal processing techniques and the use of additional sensoring.

5.5.4. Cryptographic Authentication

This technique requires a change of the GNSS signal structure, which again, is very unlikely to happen. There are:

- Navigation Message Authentication denotes the authentication of satellite signals by signing digitally the navigation message.
- Navigation Message Encryption uses a symmetric system to encrypt the data modulated on the satellite ranging signals. This system can provide authentication if the user community is trustworthy or by encapsulating the symmetric encryption key in tamper-resistant hardware.
- Spreading Code Encryption can accomplish user and signal authentication. Yet, the process is far more complex.

5.6. Sixth Strategy: Space Systems Enhancements

The advantage to enhance space systems is to add redundancy and provide an over determined solution for position, velocity or time problem. Meanwhile, these strategies increase systems size and overall costs. Below are listed some alternatives to enhance space systems:

- Development of augmentation systems,
- Addition of pseudolites,
- Use of advanced antennas (smart, polarized, etc.),
- Use of more backup systems,
- Use of external navigation aids.

5.7. Evaluation Metrics of Interference Mitigation

The evaluation of interference mitigation techniques is required to assess techniques efficiency by the definition of quantitative and qualitative metrics.

The first category of metrics will be to measure the degree (or level) of RFI signal suppression. For example, the Interference-to-Noise Ratio (INR) describes how much RFI dominates the noise. The INR is also known as the JNR (Jamming-to-Noise Ratio) in the specific case of jamming. Also, there is the intensity of RFI signal which can be performed by a ratio of system-noise variance and RFI variance. Another metric can be the ratio of occupied bandwidth (or bandwidth corruption). This method can be described by a ratio of the signal-of-interest bandwidth and RFI bandwidth.

The second category of metrics will be to define the amount of information lost from signal-of-interest as a result of RFI mitigation process. For example the processing gain after RFI suppression can describe the ratio of SNR (after mitigation) and SNR (before mitigation). Also, the loss from RFI processing can be described by a ratio of SNR (after mitigation) and SNR (with no implementation of RFI mitigation). With these metrics, one can quantify the amount of data loss from signal-of-interest after the implementation of a RFI mitigation technique.

The third category of metrics will be to evaluate the degree of complexity of the RFI mitigation techniques and their overall impact on the transmission chain (speed, performance, etc.). For that, the complexity of RFI mitigation can be described by a number of computations induced by the mitigation process.

The fourth category of metrics will be to evaluate the additional cost, resulting of RFI mitigation implementation (hardware and/or software) inside a space communication based system.

6. Conclusions

GNSS civilian applications are an asset which has changed our society. This technology allows unlimited possibilities to change working conditions in a vast range of applications.

The disruption of the GNSS service in critical applications that are used by these infrastructures has a critical impact in society. The most vicious effects are condensed around the sectors on transportation, financial services, public health, Search and rescue. In final, the sources of GNSS failures or errors reduce the efficiency of GNSS devices to solve a problem, leading to decrease reliance in GNSS and affecting directly or indirectly people's habits.

It is complex to classify or compare mitigation techniques. On the one hand, some specific techniques can be applied similarly in different domains and in various combinations. On the other hand, some mitigation techniques can be effective or ineffective under certain conditions. What is certain is that the effectiveness of any given technique depends on the RFI characteristics (its source, its nature, persistent or intermittent), the RFI scenario of occurrence (accidental or unintentional, interaction with terrestrial networks, human factors, etc.) and the device or systems impairments.

This paper outlines questions for debate about the degree of vulnerability our society can be exposed in case of a potential GNSS failure or interference. In the future, the main axes for improving GNSS technology will be driven by GNSS main performance metrics (accuracy, availability, continuity, and integrity), alongside robustness to interferences and system failures tolerances.

REFERENCES

[1] D. Hook, "For Want of a Nail: An Assessment of Global Positioning System Satellite Replenishment," United States Army Command and General Staff College, Fort Leavenworth, 2004, p. 99.

[2] GSA, "GNSS Market Report Issue 2," European GNSS Agency (GSA) Publications, Brussels, 2012.

[3] H. T. Ltd., "System and Policy Inventory: Development of the European Radio Navigation Plan," European Commission DG TREN, 15 March 2004.

[4] T. Carey, "SatNav Danger Revealed: Navigation Device Blamed for Causing 300,000 Crashes," *The Mirror*, 2008. http://www.mirror.co.uk/news/top-stories/2008/07/21/satnav-danger-revealed-navigation-device-blamed-for-causing- 300-000-crashes-89520-20656554/

[5] M. Thomas, J. Norton, A. Jones, A. Hopper, N. Ward, P. Cannon, N. Ackroyd, P. Cruddace and M. Unwin, "Global Navigation Space Systems: Reliance and Vulnerabilities," The Royal Academy of Engineering, London, 2011.

[6] B. Forssell, "The Dangers of GPS/GNSS," Coordinates Magazine, Dehli, 2004.

[7] L. Strickling, "NTIA Light Squared Recommendation to the FCC," National Telecommunications & Information Administration, Washington DC, 2012.

[8] N. P. A. Boards, "Jamming the Global Positioning System: A National Security Threat: Recent Events and Potential Cures," *National Space-Based Positioning*, *Navigation*, *and Timing*, Washington DC, 4 November 2010.

[9] H. Schwarz, "Light Pollution: The Global View," Kluwer Academic, Dordrecht, 2003.

[10] L. Scott, "J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches," 24*th International Technical Meeting of Satellite Division of the Institute of Navigation*, Portland, 20-23 September 2011, pp. 1931-1940.

[11] J. Bull and M. Ward, "Interference Detection, Characterization and Location in a Wireless Communications or Broadcast System," United States Patent No. US 81389 75B2, 2012.

[12] D. Humphrey, "Interference Mitigation for Time of Arrival Estimation," *IEEE Wireless Communications and Networking Conference* (*WCNC*), Sydney Australia, 18-21 April 2010, pp. 1-6.

[13] J. Bhatti, "Development and Demonstration of a TDOA-Based GNSS Interference Signal Localization System," *IEEE/ION Position Location and Navigation Symposium* (*PLANS*), Myrtle Beach, 23-26 April 2012.

[14] D. Musicki, "Geolocation Using TDOA and FDOA Measurement," 11*th International Conference on Information Fusion*, Cologne, 30 June-3 July 2008, pp. 1-8.

[15] L. Musumeci, "A Comparison of Transformed-Domain Techniques for Pulsed Interference Removal on GNSS Signals," *International Conference on Localization and GNSS* (*ICL-GNSS*), Starnberg, 25-27 June 2012, pp. 1-6.

[16] E. Azzouz and A. K. Nandi, "Automatic Modulation Recognition of Communication Signals," Kluwer Academic, Dordrecht, 1996, p. 235.

[17] R. Thompson, E. Cetin and A. Dempster, "Detection and Jammer-to-Noise Ratio Estimation of Interferers Using the Automatic Gain Control," *International Global Navigation Satellite Systems Society* (*IGNSS*) *Symposium*, Sydney, 15-17 November 2011.

[18] M. Trinkle and D. Gray, "GPS Interference Mitigation: Overview and Experimental Results," *Proceedings of the 5th International Symposium on Satellite Navigation*, Canberra, Sydney, July 2001.

[19] E. D. Kaplan and C. J. Hergaty, "Understanding GPS: Principles and Applications," Artech House, Boston, 2005, p. 726.

[20] R. J. Landry, "New Technique to Improve GPS Receiver Performances by Acquisition and Tracking Thresholds Reduction," 6*th Saint Petersburg International Conference on Integrated Navigation Systems*, St. Petersburg, Russia, 24-26 May 1999.

[21] M. Rosen and M. Braasch, "Low Cost GPS Interference Mitigation Using Single Aperture Cancellation Tech-

niques," *National Technical Meeting of The Institute of Navigation* (*ION NTM*), Long Beach, 21-23 January 1998, pp. 47-58.

[22] A. Coster, "Webinar: Space Weather & GNSS: Sources, Characteristics, and Mitigation Effects," *InsideGNSS & Novatel*, Eugene, 31 October 2012.

[23] E. Key, "Techniques to Counter GPS Spoofing. Internal Memorandum," MITRE Corporation, Bedord, 1995.

[24] A. Jafarnia-Jahromi and A. Broumandan, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation*, Cairo, 2012.

