International Global Navigation Satellite Systems Association
IGNSS Symposium 2018

Colombo Theatres, Kensington Campus, UNSW Australia
7 – 9 February 2018

Vulnerabilities in SBAS and RTK Positioning in Intelligent Transport Systems: An Overview

Davide Imparato
Department of Spatial Sciences, Curtin University,
Perth, Australia
Tel: +61 8-92663403, Email: davide.imparato@curtin.edu.au

Ahmed El-Mowafy
Department of Spatial Sciences, Curtin University,
Perth, Australia
Tel: +61 8-92663403, Email: a.el-mowafy@curtin.edu.au

Chris Rizos
School of Civil and Environmental Engineering, UNSW,
Sydney, Australia
Tel: +61 2 93854205, Fax: +61 2 9385 6139, Email: c.rizos@unsw.edu.au

Jinling Wang
School of Civil and Environmental Engineering, UNSW,
Sydney, Australia
Tel: +61 2 93854203, Fax: +61 2 9385 6139, Email: jinling.wang@unsw.edu.au

ABSTRACT

As Intelligent Transport Systems (ITS) become more automated and more demanding, ITS positioning integrity is becoming a key performance parameter. ITS relies on GNSS technology for absolute positioning. In order to develop efficient models and methods that can provide high levels of integrity, it is necessary to study the vulnerabilities of the GNSS-based positioning systems intended for use in ITS applications, in particular those which require positioning accuracy at the sub-metre level. These vulnerabilities are attributed to several sources and include biases and errors in the GNSS measurements, and in the corrections applied to the measurements for augmented performance, as well as those induced by the operating environment. The vulnerabilities also comprise possible anomalies that may affect each component of the system, including disturbances or disruption in the communications between the service provider and users, data latency, to name a few. In this paper a preliminary overview of possible vulnerabilities is presented for two widely-used GNSS positioning techniques envisioned for ITS applications: the Satellite-Based Augmentation System (SBAS) and low-cost RTK. Some examples are given, including the source of these errors, e.g. satellite or receiver hardware, environment, external communications, the error magnitude, temporal and spatial behaviour, their deterministic and stochastic characteristics, and their impact on estimated positions. Furthermore, some of the corresponding mathematical models that can be used to describe these vulnerabilities in the integrity monitoring

algorithms are presented.

KEYWORDS: ITS, GNSS, SBAS, RTK, vulnerabilities.

1. INTRODUCTION

The lane-level accuracy required in most urban ITS applications is deemed out of reach of the Standard GNSS Positioning Service (SPS). It is thus necessary to augment the SPS with other techniques, like V2V and V2I communication (Cooperative ITS), INS and SBAS, or employ more precise positioning techniques, such as PPP or RTK (Austroads 2013). As the level of vehicle automation increases, requirements on the positioning accuracy become more demanding, possibly reaching the centimetre level that is prerogative of RTK. Recent studies suggested that, with the advent of new GNSS systems as Galileo and BeiDou, low-cost RTK will be possible even in the urban environment (Pesyna et al. 2014, Murrian et al. 2016, El-Mowafy and Kubo, 2017).

Among the most demanding ITS applications are the safety applications (e.g. collision warnings and emergency brake), which require a highly trustworthy positioning. For these applications there is a need to monitor the integrity of the system and be aware of all possible anomalies that can affect it.

This work provides an overview of the vulnerabilities affecting the positioning by SBAS and RTK techniques, with a focus on their application in ITS. As most of ITS users will be located in metropolitan areas, the critical cases will be related to vulnerabilities in the urban environment: multipath, Non-Line-Of-Sight (NLOS) and radio-frequency interference. Therefore major interest is on the characterisation of these threats and on related mitigation techniques.

The vulnerabilities are categorised on the basis of their source (i.e. GNSS, environment, user, positioning method and service).A general description of their temporal/spatial behaviour, deterministic and stochastic characteristics and their impact on the positioning is provided. Section 2 gives an outline of the positioning methods used in SBAS and RTK. Section 3 provides a description of the main vulnerabilities affecting these methods and a table summarising the main anomalies that may affect the systems. Next conclusions are given.

2. POSITIONING TECHNIQUES

As mentioned above we restrict focus in this paper on two GNSS positioning techniques, satellite based augmentation system (SBAS) and real-time kinematic (RTK). They are summarised in the following sections.

2.1 SBAS

Any SBAS system is constituted by a ground segment, i.e. a network of reference stations and master stations, and a space segment, i.e. a set of GEO satellites (Enge et al. 1996; Roturier et al. 2001). The SBAS system augments the GNSS systems in three ways:

- providing user differential corrections to improve the positioning accuracy,
- providing extra ranging navigation signals, from the GEO satellites, and
- providing the integrity service, i.e. performing quality control of measurements and

parameters that facilitate computing the Protection Levels used in integrity monitoring.

The measurements taken at the ground reference stations allow the computation of the user corrections. These corrections are computed for the satellites' clock and ephemerides, ionosphere, troposphere and satellite hardware delays. The general GNSS code and phase observations can be expressed as:

$$\begin{aligned} p_j &= ||x_S - x_r|| + c\,\delta t_r - c\,\delta t_S + \imath j + \tau + m + c\,d_r + c\,d_S + e \\ \varphi_j &= ||x_S - x_r|| + c\,\delta t_r - c\,\delta t_S - \imath j + \tau + \lambda j a + \mu + c\,\delta_r + c\,\delta_S + \varepsilon \end{aligned} \qquad (1)$$

where p_j and φ_j are the code and phase observables on the *j*th frequency (in metres), x_S and x_r are the positions of satellite and user receiver respectively, c is the speed of light in vacuum, δt_r and δt_S are receiver and satellite clock offsets respectively, $\imath j$ is the slant ionospheric delay, τ is the slant tropospheric delay, m and μ are the multipath error on code and phase measurements respectively, d_r, d_S and δ_r, δ_S are systematic hardware delays, at receiver and satellite, on code and phase measurements respectively, λj is the *j*th carrier wavelength, a is the constant carrier phase integer ambiguity in cycles, e and ε are the random code and phase measurements noise, respectively. x_r and δt_r are to be solved for. The other terms are sources of error in the positioning.

SBAS positioning is code observations based, though in most applications both user and reference stations employ carrier-phase observation smoothing. In the standard civil aviation SBAS applications the user relies only the observations on the civil frequencies, e.g. in US and Europe till now only on single-frequency L1 observations. Reference stations instead make use of geodetic multi-frequency receivers to estimate the ionospheric delay and increase the accuracy of the network corrections. Future SBAS may include L1/L5 double-frequency observations, as in the current Australian SBAS testbed

With the application of SBAS corrections, most of the error terms are reduced in size, in particular the clock and ephemeris errors, and the ionospheric delay. The total pseudorange variance is generally computed as (e.g. in the WAAS and EGNOS systems):

$$\sigma^2_{code} = \sigma^2_{UDRE} + \sigma^2_{GIVE} + \sigma^2_{tropo} + \sigma^2_{multi} + \sigma^2_{noise} \qquad (2)$$

where σ_{UDRE} is the STD of the User Differential Range Error, σ_{GIVE} is the STD of the Grid Ionospheric Vertical Error, σ_{tropo} is the STD of the differential tropospheric delay, σ_{multi} is the STD of the (differential) multipath error, and σ_{noise} is the STD of the combined corrections-user thermal noise. The UDRE includes satellite clock and ephemeris errors, and satellite hardware delays. In integrity monitoring satellite and receiver hardware delays are treated separately and added as nominal biases in the computation of the Protection Levels (Blanch et al. 2015). Table 1 provides common values of the different error components in (2).

Table 1: SBAS range accuracy components.

Source	L1-only	L1/L5 iono-free comb.
σ_{UDRE}	0.3-0.6m	0.3-0.6m
σ_{GIVE}	0.2-0.8m	0
σ_{tropo}	0.05-0.3m	0.05-0.3m
σ_{noise}	0.2-0.6m	2.6 x $\sigma_{noise\ L1}$

In Table 1 we distinguish between single-frequency (L1) SBAS service and dual-frequency (L1/L5) SBAS, which makes use of the iono-free combination. Dual-frequency SBAS, which isnot yet officially operative, permits the complete cancellation of the first order error term of the ionospheric delay. However, if no ionosphere model is used, the thermal noise and multipath error terms will be inflated by the factor 2.6 (Walter et al. 2010b). It is expected that in the aviation sector the elimination of the ionospheric threat will outweigh the increase of noise and multipath errors, and the ionosphere-free combination will be employed without need for additional corrections. However, in ITS environment the multipath error constitutes likely the most critical error component. Therefore, further studies are needed to quantify the dual-frequency SBAS errors in ITS – studies planned within our contribution in the Australian SBAS testbed – and evaluate the need/opportunity of coupling the dual-frequency observation with ionospheric models.

Performance analysis reports, e.g. by the NSTB/WAAS T&E Team (2015), show results on WAAS performance over time. Range error variance smaller than 1m, positioning horizontal accuracy 0.5m to 1.4m, and vertical accuracy of 0.8m to 1.7m are typically reported. The improvement in accuracy, compared to single point positioning (SPS), is generally over 33% (Ali et al. 2012). Current SBAS integrity services are meant for use in the aviation sector. The multipath term is coupled with the receiver noise and assumed to be of the order of 0.3-0.5m. This is of course not representative of a typical urban environment, where multipath and NLOS effects can generate errors of several metres (Ali et al. 2012).

2.2 RTK

RTK is also a differential positioning method, but relies on carrier-phase observations to achieve better positioning accuracy. In RTK, the significant reduction in spatially-correlated measurement errors, due to the use of shorter baselines, allow for ambiguity resolution, with a resulting increase in positioning precision to achieve a few cm accuracy. Fast ambiguity resolution has so far relied on the use of high-quality multi-frequency receivers, but the availability of observations from new systems such as Galileo and BeiDou is making it possible also with low-cost single-frequency receivers (Pesyna et al. 2014, Murrian et al. 2016).

In RTK, most of the terms in equation (1) that represent error sources in SBAS, such as x_S, δt_S, ι_j, τ, d_r, d_S, δ_r, δ_S mostly cancel by differentiation or are lumped with the unknowns to be solved for. As a result, when ambiguity resolution is possible the positioning error can decrease to the level of the carrier-phase observation noise (i.e. centimetre-level and smaller). Recent studies suggest that fast ambiguity resolution is possible in urban environment with a low-cost multi-GNSS receiver as long as the atmospheric delay uncertainty is kept in the order of 2mm – requirement that could be met with RTK baseline shorter than 20km (Murrian et al. 2016).

Even though the impact of the above mentioned sources of errors and threats is reduced in size, because of the high level of accuracy that is necessary for correct ambiguity resolution, small anomalies or faults that would have only little impact on the measurements will still have a significant impact on the position estimation. Cycle-slips may in fact lead to incorrect ambiguity fixing and therefore constitute a threat to reliable positioning. Furthermore, while constant integer ambiguities leads to cm accuracy, float ambiguities can lead to deci-metre accuracy, which could be acceptable for ITS.

3. VULNERABILITIES

We categorise the GNSS vulnerabilities in four groups: GNSS system, medium/environment, user, and overlay service (including the positioning method). Figure 1 shows the categorisation employed. The mentioned GNSS anomalies are summarised in Tables 2 and 3. Fault modes are classified in Table 4, where approximate mathematical models are given.

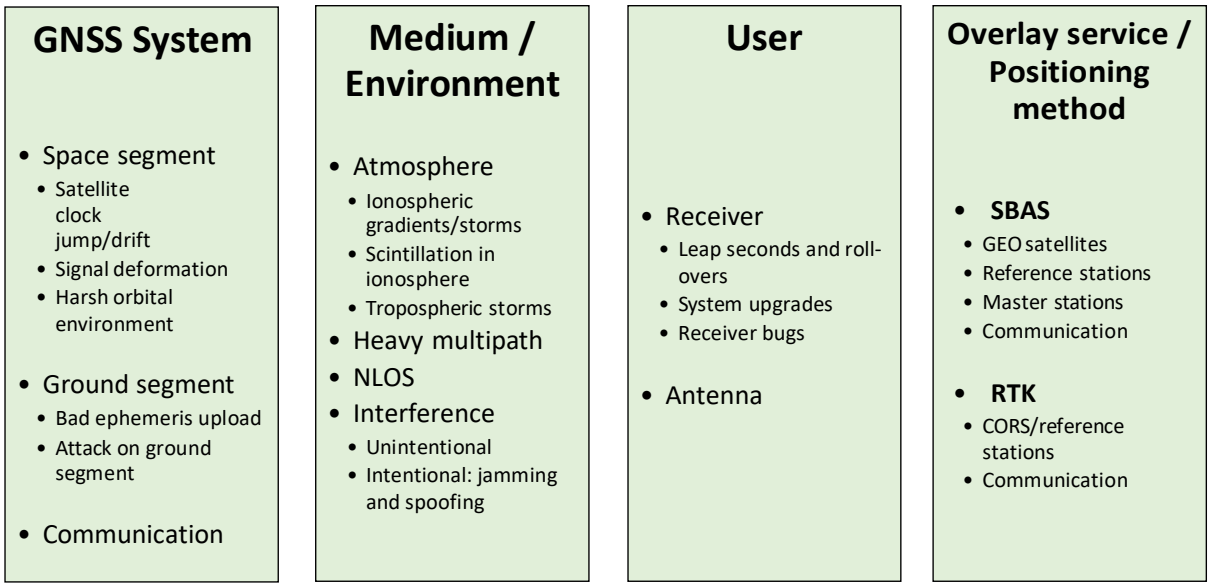

Figure 1: GNSS vulnerabilities

Table 2: GNSS anomalies (Bhatti and Ochieng 2007; Ochieng et al. 2003; The Royal Academy of Engineering 2011).

Cause	Characteristics	Impact	Model	Likelihood
GNSS system				
Satellite clock jump	Clock misbehaviour that results in an abrupt change in the transmitted signal.	Range error of up to kilometres.	Step error	~ 10^{-5}/hr per satellite
Satellite clock drift	Clock misbehaviour that introduces a slow ramp type error in the transmitted signal.	Range errors can grow gradually to few kilometres.	Ramp error	~ 10^{-5}/hr per satellite
Ephemeris information error	Increases with the time lapse between two consecutive uploads.	Range errors of up to 40 metres (Ochieng et al. 2003).	Step/Ramp error	~ 10^{-5}/hr per satellite
Incorrect modelling of Earth Orientation Parameters (EOP)	Increases with the time lapse between two consecutive uploads.	Constellation-wide fault, positioning error up to hundreds of metres (Perea Diaz et al. 2014).	Step/Ramp error	< 10^{-5}/hr per system
Signal deformations	Deformation of signal correlation function.	Range errors of few metres.	Step error / Random noise	~ 10^{-5}/hr per satellite
Low signal power / Power fluctuations	May be due to satellite attitude instability or hardware wear.	Increased random noise (errors of few metres). Could result in loss of lock.	Random noise	~ 10^{-5}/hr per satellite
Code-carrier incoherence	Failure to maintain coherence between broadcast code and carrier (Simili and Pervan 2006). Observed only on GEO satellites and GPS L5 signals.	Range errors up to few metres.	Ramp error	~ 10^{-5}/hr per satellite
Harsh space weather	Can cause ionisation of payload silicon material, or satellite attitude instability.	Range errors of few metres or increased random noise.	Step error / Random noise	UI[1] (low)
Non-standard code (NSC)	NSC is a warning not to use the observation. Possible anomaly in the oscillator of Time Keeping Systems (TKS), see Wu (1999).	Unusable observation (for a proper receiver).	Step error	UI
RF filter failures	There can be sudden jumps or slow fluctuation in signal frequencies.	Loss of lock.	Step error	UI
Single-string Failure Mode	Either satellite bus or the navigation payload are operating without backup capacity.	At any time, 16 satellites may be operating in single string failure mode. Threat to continuity.	Step error	UI
Leap Second Anomaly	Error in UTC offset parameters broadcast. Occurred in November 2003 and January 2016, with no impact on positioning performance.	Some receivers may temporarily lose lock.	Step error	UI (low)
Medium/Environment				
Unintentional interference	Vicinity of an installation that generates radio frequencies in the GPS frequency range.	Increased noise up to complete loss of lock.	Random noise	UI

[1] Under Investigation.

Cause	Characteristics	Impact	Model	Likelihood
Jamming/Spoofing	Intentional interference to cause loss of lock (jamming) injection of spurious GPS or corrections like signal (spoofing).	Unbounded.	Step error	UI
Ionospheric gradients	During high solar activity large errors in signals can be introduced due to large spatial or temporal gradients.	Range errors of up to 100m (single-frequency case).	Step/ramp error	$\sim 2 \cdot 10^{-4}$/hr per satellite
Ionospheric scintillation	Due to small-scale irregularities in electron density in the ionosphere.	Cycle slips, increased noise. In severe cases, loss of lock.	Random noise	$\sim 2 \cdot 10^{-4}$/hr per satellite
Tropospheric errors	Tropospheric storms may cause large spatial/temporal gradients of tropospheric delay.	Range errors of up to several metres.	Random noise	Within Gaussian model bounds
Multipath	Reflection/diffraction of the signal by surrounding surfaces.	Dependent on operational environment. Range errors up to several metres (Van Nee 1995). Can result in loss of lock.	Random noise	Environ-ment dependent
Non Line of Sight (NLOS)	Reception of NLOS signal through reflection by surrounding surfaces.	Dependent on operational environment. Range errors up to hundred metres.	Step error / Random noise	Environ-ment dependent
User				
Receiver problems	Leap seconds and rollovers, system upgrades, software bugs, components failures and replacements, wear, over-heating, etc.	Receiver dependent.	Step error / Random noise	Receiver dependent
SBAS specific				
GEO satellites faults	Same as GNSS satellites.	Comparable to GNSS Satellites.	Any	Service dependent
Reference receiver faults	As user's receiver.	Service dependent.	Step error / random noise	Service dependent
Master stations errors	Errors in estimation of the corrections.	Service dependent.	Step error	Service dependent
Incorrect information up-link	Communication or broadcast errors between reference stations, master stations, GEO satellites and user.	Service dependent.	Step error	Service dependent
RTK specific				
Carrier-phase multipath	Reflection/diffraction of the carrier by surrounding surfaces.	Dependent on operational environment. Range errors up to 5-6cm.	Random noise	Environ-ment dependent
Cycle-slips	Discontinuity in the receivers continuous phase lock on a satellite's signal.	Range errors up to several metres.	Step error	Environ-ment & elevation dependent
Reference receiver faults	As user's receiver.	Service dependent.	Step error / random noise	Service dependent
Incorrect information up-link	Communication or broadcast errors between reference stations and user.	Service dependent.	Step error	Service dependent

Table 3: Error models (Bhatti and Ochieng 2007).

Error type	Failure Model
Step Error	$f(t) = A\ u(t-t_0)$ where A is the magnitude of the fault, $u(t)$ is the unit step function and t_0 is the onset time of the error
Ramp Error/Drift	$f(t) = R(t - t_0)\ u(t - t_0)$ where R is the slope of the error, $u(t)$ is the unit step function and t_0 is the onset time of the error
Random noise	$f(t) = B\ u(t-t_0)$ where $B \sim N(\eta, Q)$ is the normally distributed magnitude of the error, with mean η and variance Q, $u(t)$ is the unit step function and t_0 is the onset time of the error

In the following sections the above errors are briefly discussed.

3.1 GNSS System

- *SV Clock/Ephemeris Estimation Errors.* Nominal clock and ephemeris errors affect GNSS observations even when no fault affects the system (Amarillo-Fernandez et al. 2008; Heng et al. 2011; Montenbruck et al. 2015; Warren and Raquet 2003). Hardware fault or erroneous navigation message upload can induce significant errors in the broadcast GNSS clock and ephemeris information. Errors can be caused by switching between clocks on board the satellite, unannounced manoeuvring of the satellite, or clock malfunctions. Ephemeris information may be incorrectly decoded either by the system or by the user (Gratton et al. 2007; Heng et al. 2010). By design, GPS failure rate should be at most 1.43×10^{-5} events/hr per satellite, where a failure occurs in case of UERE >4.42 x URA, corresponding to a significance level of 10^{-5} and UERE > 5.73×URA for GPS block III satellites (Walter et al. 2010a, El-Mowafy and Yang 2016). Current integrity monitoring algorithms use the conservative value of 1×10^{-5} events/hr per satellite. An actual empirical conservative estimate, by Pullen et al. (2006), is 2.4×10^{-6} events/hr per satellite. The history of outages in LAAS (Pullen and Enge, 2013) shows that failure probabilities are different depending on age and history of faults of each satellite.

- *Signal Deformations.* Signals on all frequency may be affected by distortions that change the correlation function shape and may lead to biases, dependent upon the correlator spacing and bandwidth of the receivers. These biases cannot be detected by a network of identically configured receivers, but require the use of specialised receivers. When using the ionosphere-free combination (e.g. dual-frequency SBAS), the effects are magnified compared to L1-only. This threat could constitute the largest source of uncertainty in the ionosphere-free combination (Walter et al. 2012).

- *Code-Carrier Incoherency.* A satellite may fail to maintain the coherency between the broadcast code and carrier. This threat causes either a step or a rate of change between the code and carrier broadcast from the satellite. This threat has never been observed on the GPS L1 signal, but has been observed on SBAS geostationary satellite signals and on the GPS L5 signal (Gordon et al. 2010; Montenbruck et al. 2010). This threat is relevant in SBAS only if carrier smoothing of the code is used. A fault can create

sensible errors in the smoothed code estimate.

3.2 Medium/Environment

- *Ionosphere*. The ionosphere represents a threat mainly for single-frequency users. In SBAS (single-frequency), ionospheric delay is estimated and bounded using a simple local planar fit, which is reasonably accurate most of the time at mid-latitudes. However, periods of ionospheric instability and disturbances occasionally occur, which can add significant errors to the observations. The steepest ionospheric gradients occur at high and low latitudes, though gradients larger than three metres of vertical delay over a ten kilometre baseline have been observed even at mid-latitudes (Datta-Barua et al. 2010). In addition, rates of change as large as four vertical metres per minute have been observed. Nevertheless, at mid-latitudes severe storms are quite rare, as they are registered less than 0.5% of the time. The probability of occurrence of a threatening storm, in a day, is estimated at 0.0026 (Pullen et al. 2006) for mid latitudes.

  It was also observed that usually the ionosphere gradient wave moves quickly, and specific areas are affected briefly; i.e. 2.2×10^{-4}/hr. In current SBAS, the Grid Ionospheric Vertical Error (GIVE) describes the residual ionospheric estimation errors, and must be able to protect against the worst possible ionospheric disturbance that may occur in the user's region. Scintillation also can constitute a threat (SIW Group 2010), but is also not frequent at mid-latitudes, as it is linked to ionosphere disturbances, e.g. storms. Scintillations can cause cycle-slips and loss of lock, as well as increased noise, and affect few satellites at a time. It is most concerning for L2 and L5 frequencies.
  GNSS Loss of Lock Characteristics under Ionosphere Scintillation has been investigated (Liu et al, 2017) and statistical analysis of the risks due to the loss of GNSS signals during a day is yet to be further carried out. Scintillations may affect also the satellite data link (not only the ranging information) – satellites may be unusable for a minute or longer. There is a risk of disruption for the data-link of SBAS GEO satellites as well – this may cause loss of integrity messages and therefore unavailability. However, the SBAS integrity message is usually very robust, and there is redundancy of GEO satellites (SBAS Ionospheric Working Group 2003). When dual-frequency observations are available, the first order term of the ionospheric delay is eliminated. Higher order terms are about two orders of magnitude smaller (Datta-Barua et al. 2008). The main concern in dual-frequency would be scintillation (Kintner et al. 2009).

- *Tropospheric Errors.* Tropospheric errors are typically small compared to ionospheric errors or satellite faults. Models based on historical observations have been formulated to describe the troposphere behaviour, and deviations from these models have been extensively studied (Collins and Langley 1998). Conservative bounds can be applied to the distribution of those deviations, ensuring protection against the propagated tropospheric errors. Of some concern are the statistical properties of this type of errors: tropospheric errors are correlated for long periods, and produce correlated errors at user and reference stations.

- *Multipath and NLOS.* Multipath is the most significant source of measurement error in ITS applications. It limits the ability to estimate the satellite and ionospheric errors and may change error statistical distribution, and thus will need changes in the standard methods used in integrity monitoring in aviation. Multipath depends upon the environment surrounding the antenna and the satellite trajectories. When using the

L1/L5 ionosphere-free combination, as multipath exist on L1 and L5, the net effect is an increase of approximately 2.6 times the L1-only multipath error. Multipath is especially intense in dense urban areas due to the presence of high rise buildings, which block, reflect and diffract the signals. Buildings and other obstacles degrade the positioning in three ways: 1) signals may be completely blocked, and be unavailable for positioning, 2) direct signals are blocked, but the signals are still received via a reflected path, with the NLOS reception, 3) both direct Line-Of-Sight (LOS) and reflected signals are received, causing multipath interference. NLOS code signals can exhibit positive ranging errors of tens of metres magnitude in dense urban areas.

Many approaches exist for multipath and NLOS mitigation (Groves 2013). Good quality antenna are more sensitive to right-hand circularly polarised (RHCP) signals, rather than left-hand circularly polarized (LHCP): most reflected signal have LHCP or mixed polarisation, and therefore their impact on the observations would be reduced. One of the main drawbacks of cheap antennas is that they guarantee much less polarisation discrimination – smartphone antennas none at all. Monitoring the Signal-to-Noise Ratio (SNR) can also be helpful in detecting NLOS, as they are usually characterised by reduced signal power. There is a large literature on receiver-based signal-processing techniques apt to mitigate multipath effects (Bhuiyan and Lohan 2012).

Over the past seven years, there has been a lot of interest in 3D-map-aided (3DMA) GNSS, a range of different techniques that use 3D mapping data to improve GNSS positioning accuracy in dense urban areas. The simplest form of 3DMA GNSS is terrain height aiding. 3D models of the buildings can be used to predict which signals are blocked and which are directly visible at any location (Bradbury et al. 2007; Suh and Shibasaki 2007; Wang et al. 2012). A technique that determines position by comparing the measured signal availability and strength with predictions made using a 3D city model over a range of candidate positions is the shadow matching technique (Groves et al. 2015). 3D models of the buildings can also be used to aid conventional range-based GNSS positioning. Where the user position is already approximately known, it is straightforward to use a 3D city model to predict the NLOS signals and eliminate them from the position solution (Bourdeau and Sahmoudi 2012; Obst et al. 2012; Peyraud 2013). However, for most urban positioning applications, especially when based on SPS, there is significant position uncertainty.

Different approaches have been proposed in the literature which define search areas centred on the conventional GNSS position solution and attribute weights to hypotheses of NLOS or LOS signals (Adjrad and Groves 2016a,b; Suzuki 2016). Several groups have extended 3D-mapping-aided GNSS ranging by using the 3D city model to predict the path delay of the NLOS signals across an array of candidate positions (Betaille et al. 2013; Hsu et al. 2015; Kumar and Petovello 2014, 2016; Suzuki and Kubo 2013). Multipath and NLOS prediction with advanced ray tracing algorithms is proposed by Fuschini et al. (2008). A single-epoch positioning accuracy, for 3DMA SPS technique, of 4m has been reported by Hsu et al. (2015). Dominguez et al. (2014) reported pseudo-range errors of 4-6m on motorways, and 6-7m in the urban environment. As the position errors (for SPS) appear to follow Gaussian distributions with heavy tails, Bin Ahmad et al. (2014) has proposed the use of a Pareto distribution to model the distribution of position errors due to multipath and NLOS errors.

- *Unintentional and intentional interference.* Accidental interference can occur in presence of harmonic emissions from high power transmitters, ultra-wideband radar, televisions, VHF, mobile satellite services and portable electronic devices. In the worst case, interference can cause the complete loss of lock of the receivers. Numerous studies evaluated the effects of interference on GNSS receivers (e.g. De Bakker et al. 2006, Jost et al. 2008). Deliberate interference can be categorised in jamming (disruption of the GNSS signal), spoofing (broadcast of false signals) and meaconing (delaying and rebroadcast of the signal). Jamming is the most common form of deliberate interference – the GNSS signals are weak and easy to jam by broadcasting noise-like signals at the specific frequencies. Spoofing threats and anti-spoofing techniques are reviewed by Jafarnia-Jahromi et al. (2012), Psiaki and Humphreys (2016). The risk of interference is hard to quantify and likely not negligible in urban environment.

3.3 User

- *Antenna Bias.* Look-angle dependent biases in the code phase on all frequencies are present at the user's antenna, as well as at the GPS satellite antennas (Haines et al. 2005; Shallberg and Grabowski 2002). These biases constitute nominal errors (as such are not included in Table 2), and may be several tens of centimetres in magnitude. These biases are observable in an anechoic chamber, but more difficult to characterise in operation. They may result from intrinsic antenna design as well as manufacturing variation, and they are different for each GNSS system (included in the inter-System Biases).

- *Inter-frequency Bias Estimation Errors.* The hardware differential delay between the L1 and L2 frequencies is referred to as Tau group delay (Tgd) for the bias on the satellite and Inter-Frequency Bias (IFB) for the user's (or reference station) receiver. Knowledge of this delay is needed in the correction algorithms of current L1-only SBAS services. These biases are part of the nominal errors and are typically estimated in tandem with the ionospheric delay (Wilson et al. 1999). They are nominally constant, but they may vary in special conditions: in case of component switching, when a receiver or antenna is replaced, or if different components or paths are made active on a satellite; in case of thermal variation, either at the reference station or on the satellite as it goes through eclipse; or as a consequence of aging, which may induce a slow variation. These biases are eliminated in dual-frequency SBAS.

- *Receiver Faults.* Errors can occur at the receiver through false lock or other mechanisms, including hardware failure (GNSS receiver, antenna, atomic frequency standard), software bugs (tracking loop implementation), components replacement, and manned operations. These may be mitigated through components redundancy, e.g. redundant receivers, antennas and/or clocks, as described in Haines et al. (2005).

3.4 Positioning method specific vulnerabilities

3.4.1 SBAS specific vulnerabilities

SBAS is developed primarily to address threats to GNSS; however, it may introduce additional risks (Walter et al. 2012):

- *Reference Station Position Errors.* Errors in the surveyed position of the antenna at the

reference stations affect users in the same way as antenna biases, although they are smaller in magnitude and affect all frequencies identically. These errors are constant in time, although changes may occur with new surveys. They are usually lumped together with the antenna biases.

- *Reference Stations Receiver Clock Estimate Errors.* The time offsets between the reference station receivers is an unknown to be estimated by the SBAS algorithms. These offsets are nominally linear over time, but this behaviour may change following components replacement or failure in the receiver. The estimation of time offsets can be jeopardised by reference station clock failures and/or satellite ephemeris errors.

- *Satellite Segment (GEO satellites).* Same threats as for the GNSS satellites.

- *Reference Stations Receiver Faults.* As for the user receiver, faults or anomalies can occur at the reference receivers due to component replacement, component failure, overheating, software bugs, inadequate manned operations, and site displacement. These risks are usually mitigated by using redundant systems (e.g. multiple receivers per reference station).

- *Master Stations Errors.* Errors can occur during data processing and estimation of the corrections to be up-linked.

- *Communication.* Errors can occur in the broadcast of the range corrections and integrity information to the GEO satellites and to the user. The risk is mitigated by using robust data-link messages and the redundancy of GEO satellites.

3.4.2 RTK-specific vulnerabilities

Most of the GNSS anomalies discussed so far constitute threats also for RTK. Even if in RTK most error terms are estimated (or cancelled for the most part by differentiation), mathematical models (e.g. dynamic models) are adopted to describe their expected temporal behaviour. The anomalies discussed may disrupt the validity of those models, and as such they still represent a threat to correct positioning. Furthermore, additional threats to RTK positioning are:

- *Reference Station Position Errors.* Surveyed positions of the reference station antennas are important in RTK as much as in SBAS. As the precision required in RTK applications is higher, corrections for effects as of the solid tides, ocean/atmospheric loading also become important.

- *Reference Stations Receiver Clock Estimate Errors.* As in SBAS, the satellite correction algorithm must estimate and remove the time offsets of the reference station receivers.

- *Reference Stations Receiver Faults*. Reference stations receivers may be affected by faults, as much as user and SBAS receivers.

- *Carrier-phase Multipath.* Multipath affects carrier-phase observations with the same mechanism as code observations (Rost and Wanninger 2009). Carrier-phase multipath is one of the critical elements in determining the Time to Ambiguity Resolution (TAR). The amount of multipath error experienced is also related to the quality of receiver employed – low-cost receivers have generally poor multipath suppression capabilities

(Pesyna et al. 2014).

- *Cycle-slips.* Cycle-slips constitute the main RTK-specific threat, as they can cause wrong ambiguity fixing and result in large errors in the positioning. Cycle-slips are mainly consequence of: 1) signal obstruction, 2) low signal power or 3) receiver software failure (Hofmann et al. 2001). There is a vast literature on cycle-slip detection (e.g. Kim and Langley 2001, Lee et al. 2003). Availability of multi-frequency measurements is expected to strengthen the cycle-slip detection capabilities (Dai et al. 2009). Carrier-phase measurement quality in urban environments was also assessed in recent studies. Frequent cycle-slips are reported at low elevations of the satellites, but tracking becomes generally good at elevations larger than 40° (Deambrogio and Julien 2013).

- *Communications.* As in SBAS, errors can occur in the broadcast of information between reference stations and user. Standard RTK infrastructure and messages are generally less robust than SBAS.

4. CONCLUSIONS

A preliminary overview of the vulnerabilities affecting SBAS and RTK with focus on their use in ITS applications has been provided. The threats affecting the positioning techniques have been categorised on the basis of their source – thus distinguishing the threats that are inherent to the GNSS system and threats that depend on the operational environment or on the specific tools and services employed. Assessment of the probability of occurrence and impact on observations/estimated position in the literature has been given where possible, and general mathematical models have been provided to characterise the behaviour of the different anomalies.

Acknowledgment

This study is supported by an Australian Research Council project number DP170103341.

REFERENCES

Adjrad, M. and Groves, P. D. (2016*a*), Enhancing least squares GNSS positioning with 3D mapping without accurate prior knowledge, *NAVIGATION* **64**(1), 75–91.

Adjrad, M. and Groves, P. D. (2016*b*), Intelligent urban positioning using shadow matching and GNSS ranging aided by 3D mapping, in *Proceedings of the ION GNSS+ 2016*, Portland, Oregon, September 12-16, pp. 534–553.

Ali, K., Pini, M. and Dovis, F. (2012), Measured performance of the application of EGNOS in the road traffic sector, *GPS Solutions* **16**(2), 135–145.

Amarillo-Fernandez, F., Crisci, M., Ballereau, A., John Dow, J., Hollreiser, M., Hahn, J. and Gerner, J. (2008), The Galileo ground mission segment performances, in *International GNSS Service Workshop IGS*, 2-6 June 2008, Miami Beach, Florida, USA.

Austroads, Vehicle Positioning for C-ITS in Australia (Background Document), Technical Report, Project No. NT1632, Austroads Publication No. AP-R431-13, 2013.

Betaille, D., Peyret, F., Ortiz, M., Miquel, S. and Fontenay, L. (2013), A new modeling based on

urban trenches to improve GNSS positioning quality of service in cities, *IEEE Intelligent Transportation Systems Magazine* **5**(3), 59–70.

Bhatti, U. I. and Ochieng, W. Y. (2007), Failure modes and models for integrated GPS/INS systems, *The Journal of Navigation* **60**(2), 327–348.

Bhuiyan, M. Z. H. and Lohan, E. S. (2012), Multipath Mitigation Techniques for Satellite-Based Positioning Applications, Jin, Second Edition, *Global Navigation Satellite Systems: Signal, Theory and Applications*, pp. 405–426.

Bin Ahmad, K. A., Sahmoudi, M. and Macabiau, C. (2014), Characterization of GNSS Receiver Position Errors for User Integrity Monitoring in Urban Environments, in *ENC-GNSS 2014, European Navigation Conference*, 14-17 April 2014, Rotterdam, Netherlands.

Blanch, J., Walter, T., Enge, P., Lee, Y., Pervan, B., Rippl, M., Spletter, A. and Kropp, V. (2015), Baseline advanced RAIM user algorithm and possible improvements, *IEEE Transactions on Aerospace and Electronic Systems* **51(1)**, 713–732.

Bourdeau, A. and Sahmoudi, M. (2012), Tight integration of GNSS and a 3D city model for robust positioning in urban canyons, in *Proceedings of the ION GNSS 2012*, 17-21 September, Nashville, Tennessee.

Bradbury, J., Ziebart, M., Cross, P. A., Boulton, P. and Read, A. (2007), Code multipath modelling in the urban environment using large virtual reality city models: Determining the local environment, *Journal of Navigation* **60**(1), 95–105.

Collins, J. P. and Langley, R. (1998), The residual tropospheric propagation delay: How bad can it get?, in *Proceedings of ION GPS*, Vol. 11, Institute of Navigation, 15-18 September 1998, Nashville, Tennessee, pp. 729–738.

Dai, Z., Knedlik, S. and Loffeld, O. (2009), Instantaneous triple-frequency GPS cycle-slip detection and repair. *International Journal of Navigation and Observation*, Article ID 407231.

Datta-Barua, S., Lee, J., Pullen, S., Luo, M., Ene, A., Qiu, D., Zhang, G. and Enge, P. (2010), Ionospheric threat parameterization for local area global-positioning-system-based aircraft landing systems, *Journal of Aircraft* **47**(4), 1141–1151.

Datta-Barua, S., Walter, T., Blanch, J. and Enge, P. (2008), Bounding higher-order ionosphere errors for the dual-frequency GPS user, *Radio Science* **43**(5).

Deambrogio, L. and Julien, O. (2013), Characterization of Carrier Phase Measurement Quality in Urban Environments, in *EWGNSS 2013, 6th European Workshop on GNSS Signals and Signal Processing*, 7-10 February 2013, Munich, Germany.

De Bakker, P. F., Samson, J., Joosten, P., Spelat, M., Hoolreiser, M., and Ambrosius, B. (2006). Effect of radio frequency interference on GNSS receiver output. In *ESA workshop on satellite navigation user equipment technologies NAVITEC, ESA/ESTEC*, 11-13 December 2006, Noordwijk, NL.

Dominguez, E., Seco-Granados, G., Salcedo, J., Egea, D., Aguado, E., Lowe, D., Naberezhnykh, D., Dovis, F., Boyero, J. and Fernandez, I. (2014), Characterization of integrity threats in terrestrial applications using real signal captures, in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*, Vol. 2, Institute of navigation, 8-12 September 2014, Manassas (VA), pp. 954–966.

Enge, P., Walter, T., Pullen, S., Kee, C., Chao, Y.-C., and Tsai, Y.-J. (1996), Wide Area Augmentation of the Global Positioning System, *Proceedings of the IEEE* **84**(8), 1063–1088.

El-Mowafy, A., Kubo N. (2017). Integrity Monitoring of Vehicle Positioning in Urban Environment Using RTK-GNSS, IMU and Speedometer. *Measurement, Science and Technology*, **28**(5), 055102, 1-12.

El-Mowafy, A., Yang, C. (2016). Limited Sensitivity Analysis of ARAIM Availability for LPV-200 over Australia using real data. *Advances in Space Research*, **57**(2), 659–670.

Fuschini, F., El-Sallabi, H., Degli-Esposti, V., Vuokko, L., Guiducci, D. and Vainikainen, P. (2008), Analysis of multipath propagation in urban environment through multidimensional measurements and advanced ray tracing simulation, *IEEE Transactions on Antennas and Propagation* **56**(3), 848–857.

Gordon, S., Sherrell, C. and Potter, B. (2010), WAAS offline monitoring, in *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, 21-24 September 2010, Portland, Oregon, pp. 2021–2030.

Gratton, L., Pramanik, R., Tang, H. and Pervan, B. (2007), Ephemeris failure rate analysis and its impact on category 1 LAAS integrity, in *Proceedings of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2007)*, 25-28 September 2007, Fort Worth, TX,pp. 386–394.

Groves, P. D. (2013), *Principles of GNSS, inertial, and multi-sensor integrated navigation systems*, Artech House, Second Edition.

Groves, P. D., Wang, L., Adjrad, M. and Ellul, C. (2015), GNSS shadow matching: The challenges ahead, in *Proceedings of the ION GNSS+ 2015*, 14-18 September 2015, Tampa, Florida, The Institute of Navigation.

Haines, B., Bar-Sever, Y., Bertiger, W., Byun, S., Desai, S. and Hajj, G. (2005), GPS antenna phase center variations: New perspectives from the grace mission, *Dynamic Planet* 2005.

Heng, L., Gao, G. X., Walter, T. and Enge, P. (2010), GPS Signal-in-Space Anomalies in the Last Decade, in *Proceedings of the International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010)*, 21-24 September 2010, Portland, OR.

Heng, L., Gao, G. X., Walter, T. and Enge, P. (2011), Statistical characterization of GPS signal-in-space errors, in *Proceedings of the 2011 International Technical Meeting of the Institute of Navigation (ION ITM 2011)*, 24-26 January 2011, San Diego, CA, pp. 312–319.

Hofmann, B., Lichtenegger, H., & Collins, J. (2001). GPS theory and practice. *Springer Wien NewYork*.

Hsu, L.-T., Gu, Y. and Kamijo, S. (2015), 3D building model-based pedestrian positioning method using GPS/GLONASS/QZSS and its reliability calculation, *GPS Solutions* **20**(3), pp. 413-428.

Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation, 2012*.

Jost, T., Weber, C., Schandorf, C., Denks, H., & Meurer, M. (2008). Radio interference effects on commercial GNSS receivers using measured data, in *Position, Location and Navigation Symposium, 2008 IEEE/ION*, 6-8 May 2008, Monterey, CA, US, pp. 459-467.

Kim, D. and Langley, R. B. (2001) Instantaneous real-time cycle-slip correction of dual frequency GPS data, in *Proceedings of the international symposium on kinematic systems in geodesy, geomatics and navigation*, 5-8 June 2001, Banff, Alberta, Canada, pp. 255–264.

Kintner, P., Humphreys, T. and Hinks, J. (2009), GNSS and ionospheric scintillation. How to survive the next solar maximum, *Inside GNSS* **4**(4), 22–30.

Kumar, R. and Petovello, M. G. (2014), A novel GNSS positioning technique for improved accuracy in urban canyon scenarios using 3D city model, in *Proceedings of the ION GNSS+ 2014*, 8-12 September 2014, Tampa, Florida, pp. 2139-2148.

Kumar, R. and Petovello, M. G. (2016), Sensitivity analysis of 3D building model-assisted snapshot positioning, in *Proceedings of the ION GNSS+ 2016*, 12-16 September 2016, Portland, Oregon, pp. 12-16.

Lee, H. K., Wang, J. and Rizos, C. (2003), Effective cycle slip detection and identification for high precision GPS/INS integrated systems. *The Journal of Navigation* **56**(3):475–486.

Liu, Y., Fu L., Wang J., and Zhang, C. (2017), Study of GNSS Loss of Lock Characteristics under Ionosphere Scintillation with GNSS Data at Weipa (Australia) During Solar Maximum Phase, *Sensors (Switzerland)*, **17**(10), 2205; doi:10.3390/s17102205

Montenbruck, O., Hauschild, A., Steigenberger, P. and Langley, R. (2010), Three's the challenge: A close look at GPS SVN62 triple-frequency signal combinations finds carrier-phase variations on the new L5, *GPS World* **21**(8), 8–19.

Montenbruck, O., Steigenberger, P. and Hauschild, A. (2015), Broadcast versus precise ephemerides: a multi-GNSS perspective, *GPS Solutions* **19**(2), 321–333.

Murrian, M. J., Gonzalez, C. W., Humphreys, T. E., Pesyna, K. M. Jr, Shepard, D., and Kerns, A. J. (2016), Low-cost precise positioning for automated vehicles, *GPS World* **27**(9), 32-39.

NSTB/WAAS T&E Team (2015), Wide-Area Augmentation System performance analysis report, Technical report, October 2015, FAA/William J. Hughes Technical Center.

Obst, M., Bauer, S. and Wanielik, G. (2012), Urban multipath detection and mitigation with dynamic 3D maps for reliable land vehicle localization, in *Proceedings of the IEEE/ION PLANS 2012*, 23-26 April 2012, Grande Dunes Myrtle Beach, SC, USA, pp. 685-691.

Ochieng, W. Y., Sauer, K., Walsh, D., Brodin, G., Griffin, S. and Denney, M. (2003), GPS integrity and potential impact on aviation safety, *The Journal of Navigation* **56**(1), 51–65.

Perea Diaz, S., Joerger, M., Pervan, B., Rippl, M. and Martini, I. (2014), Analysis of ARAIM against EOP GPS-Galileo faults on LPV-200 precision approach, in *27th International Technical Meeting of the Satellite Division of The Institute of Navigation*, The Institute of Navigation, 8-12 September 2014, Tampa, Florida, pp. 3575–3586.

Pesyna Jr, K. M., Heath Jr, R. W., & Humphreys, T. E. (2014, September). Centimeter positioning with a smartphone-quality GNSS antenna, in *Proceedings of the ION GNSS+ Meeting*, 9-12 September 2014, Tampa, FL, pp. 1568-1577.

Peyraud, S. e. a. (2013), About non-line-of-sight satellite detection and exclusion in a 3D map-aided loca ization algorithm, *Sensors* **13**, 829–847.

Psiaki, M. L., and Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE*, **104**(6), pp. 1258-1270.

Pullen, S. and Enge, P. (2013), Using outage history to exclude high-risk satellites from GBAS corrections, *Navigation* **60**(1), 41–51.

Pullen, S., Rife, J. and Enge, P. (2006), Prior probability model development to support system safety

verification in the presence of anomalies, *Proceedings of IEEE/ION PLANS 2006*, 25-27 April 2006, San Diego, CA, pp. 24–27.

Rost, C. and Wanninger, L. (2009), 'Carrier phase multipath mitigation based on GNSS signal quality measurements, *Journal of Applied Geodesy* **3**(2), 81–87.

Roturier, B., Chatre, E. and Ventura-Traveset, J. (2001), The SBAS integrity concept standardised by ICAO. Application to EGNOS', *Navigation-Paris* **49**, 65–77.

SBAS Ionospheric Working Group (2003), Ionospheric research issues for SBAS — A white paper, Technical report.

SBAS Ionospheric Working Group (2010), Effect of ionospheric scintillations on GNSS — A white paper, Technical report.

Shallberg, K. and Grabowski, J. (2002), Considerations for characterizing antenna induced range errors, in *ION GPS 2002: 15th International Technical Meeting of the Satellite Division of The Institute of Navigation*, 24-27 September 2002, Portland, Oregon.

Simili, D. V. and Pervan, B. (2006), Code-carrier divergence monitoring for the GPS local area augmentation system, in *Position, Location, And Navigation Symposium*, 2006 IEEE/ION, IEEE, 25-27 April 2006, San Diego, California, pp. 483–493.

Suh, Y. and Shibasaki, R. (2007), Evaluation of satellite-based navigation services in complex urban environments using a three-dimensional GIS, *IEICE* **E-90**(B), 1816–1825.

Suzuki, T. (2016), Integration of GNSS Positioning and 3D Map using Particle Filter, in *Proceedings of the 29th International Technical Meeting of the ION Satellite Division*, ION GNSS+ 2016, Portland, Oregon, September 12-16, pp. 1296–1304.

Suzuki, T. and Kubo, N. (2013), Correcting GNSS multipath errors using a 3D surface model and particle filter, in *Proceedings of the ION GNSS+ 2013*, 16-20 September 2013, Nashville, TN.

The Royal Academy of Engineering (2011), Global Navigation Satellite Systems: reliance and vulnerabilities, Technical report, The Royal Academy of Engineering, 3 Carlton House Terrace, London.

Van Nee, D. J. R. (1995), *Multipath and multi-transmitter interference in spread-spectrum communication and navigation systems*, Ph. D. thesis,TU Delft.

Walter, T., Blanch, J. and Enge, P. (2010*a*), Evaluation of signal in space error bounds to support aviation integrity, *Navigation* **57**(2), 101–113.

Walter, T., Blanch, J. and Enge, P. (2010*b*), Vertical protection level equations for dual frequency SBAS, *in* Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010), 21-24 September 2010, Portland, OR, pp. 2031–2041.

Walter, T., Blanch, J., Eric Phelts, R. and Enge, P. (2012), Evolving WAAS to serve L1/L5 users, *Navigation* **59**(4), 317–327.

Wang, L., Groves, P. D. and Ziebart, M. K. (2012), Multi-constellation GNSS performance evaluation for urban canyons using large virtual reality city models, *Journal of Navigation* **65**(3), 459–476.

Warren, D. L. and Raquet, J. F. (2003), Broadcast vs. precise GPS ephemerides: a historical perspective, *GPS Solutions* **7**(3), 151–156.

Wilson, B., Yinger, C., Feess, W. and Shank, C. (1999), New and improved-the broadcast interfrequency biases, *GPS World Magazine 10(9), pp. 28-34*.

Wu, A. (1999), Investigation of the GPS Block IIR time keeping system (TKS) anomalies caused by the voltage-controlled crystal oscillator (VCXO), Technical report, AEROSPACE CORP EL SEGUNDO CA, December 1999