The Need for GNSS Position Integrity and Authentication in ITS: Conceptual and Practical Limitations in Urban Contexts*

Davide Margaria, Emanuela Falletti, Member, IEEE, and Tankut Acarman, Member, IEEE

Abstract—This tutorial paper highlights possible issues related to the integrity and authentication of the GNSS position in road applications. In fact, the Global Navigation Satellite System (GNSS) community is already aware of the conceptual and practical problems related to the availability of the position integrity (i.e., position confidence, protection level) and authentication in urban scenarios. However, these issues seem not to be widely known in the Intelligent Transportation Systems (ITS) domain. These limitations need to be carefully considered and addressed in the perspective of deploying reliable and robust systems based on positioning information.

I. INTRODUCTION

Position and time plays crucial role in all aspects of Intelligent Transport System (ITS) and Intelligent Vehicle (IV) technologies. Many emerging applications such as active safety, advanced driver assistance, road tolling, digital tachograph, are dependent on the position of the ego vehicle. As a near future technology, autonomous driving is strongly dependent on the position and localization [1]. To deploy IV technologies, only a portion of the sensors may be available, and some related measurements may be estimated by data processing (dead reckoning, building observers, Kalman or Particle filters [2]). Vehicle-to-Vehicle (V2V) communication is mainly deployed to disseminate time-critical safety messages on the road. To maximize dissemination range, multi-hoppings are used. In this scheme, the vehicular nodes at the maximum distance with respect to the sender must be known and access immediately to the media [3].

In any IV, accuracy and reliability of position information need to be known a priori to assure active safety. Although nowadays active safety systems in vehicles (e.g., emergency braking) only loosely depend on satellite data and vehicular communications, because of the uncertainty of positioning error, but also of signal delays and quality-of-service issues, on the other hand future applications are expected to better exploit the potentialities offered by modern GNSS and vehicular communications.

This trend is witnessed by the number of European funded projects that in the last years have addressed cooperative vehicular systems among their research topics (e.g., PRE-DRIVE-C2X, DRIVE-C2X, SIM TD, SAFESPOT, CVIS, COOPERS, GEONET, CoVeL, GAIN, etc.). Data quality was always an important topic in these projects, but most of them focused on vehicular applications, ranging from the integration aspects to on-field operational tests. Limited research effort has been devoted to the improvement of the integrity and authenticity of the positioning information provided by GNSS receivers.

The number of GNSS signals openly available for civil uses is continuously growing. Beyond the celebrate GPS, the arrival of the European Galileo, the Chinese Compass, the Indian IRNSS, the Japanese QZSS, and the modernization of GPS and GLONASS bring a lot of new signals being available in the next years. In parallel, the number of commercial applications that assume to rely on wireless positioning, including satellite positioning, is also increasing fast [4]. Current mass-market applications based on the knowledge of the user’s position (and time) can be conceptually partitioned in two groups, depending on their requirements [4]:

- **Location Based Services (LBS)**, software applications for mobile devices that require knowledge about where the mobile device is located. For example, LBS could provide the user with information about the nearest points of interest (restaurants, ATMs, drugstores etc.), or they could deliver coupons or other advertising information to customers who are in a specific geographical area. By nature, LBSs are more concerned about the continuity of the service (to be available anywhere, anytime), while the accuracy of the user's position information is not a big issue. This requirement for seamless and ubiquitous positioning clearly includes urban and indoor scenarios.

- **Liability-critical vehicular applications**, in which the information about the user’s position or velocity is used at the basis for legal decisions or economic transactions, so that large positioning error probability cannot be tolerated. Examples of such applications are road charging, pay-as-you-drive insurance, etc. Such family of applications are principally focused on the reliability (i.e., integrity and authentication) of the estimated position/time, especially in order to avoid misleading information (leading to mischarging or intentional frauds), while continuity is typically less critical.

Of course, the principal source of position information that enables such services/applications is the GNSS receiver integrated in the user’s smartphone or tablet. However, common commercial GNSS receivers are known to be potentially vulnerable in urban scenarios, where their positioning capability can be degraded by the limited satellite visibility, multipath effect, interferences, and other impairments. In addition, commercially-sensitive LBS applications become even more an attractive target for illicit

---

*Research supported by the European GNSS Agency in the framework of GLOVE, a project co-funded under the 7th Framework Program.

D. Margaria is with the Navigation Technology Research Area, ISMB, 10138, Torino, Italy (corresponding author, e-mail: margaria@ismb.it).

E. Falletti is with the Navigation Technology Research Area, ISMB, 10138, Torino, Italy (e-mail: falletti@ismb.it).

T. Acarman is with the Computer Engineering Department, Galatasaray University, 34349, Istanbul, Turkey (e-mail: acarman@ieee.org).
exploitation by terrorists and hackers, increasing the risk of intentional alteration of the GNSS signals (by means of jamming, meaconing or spoofing attacks) [5] [6].

The GNSS community has become aware of these problems and limitations, so that specific effort has already been spent to address these issues. The integrity framework has been developed in the aeronautical field for safety critical applications, whereas the introduction of a position authentication concept is motivated by the growing number of liability critical applications. Nonetheless, such awareness seems not completely mature yet within the ITS community. The aim of this paper is then to provide some general insight in the concepts of GNSS integrity and authentication, tailored to the vehicular field.

A general overview of the position integrity and authentication concepts is then provided in the following sections, highlighting their importance and their benefits in the vehicular domain. Their conceptual and practical limitations in urban contexts are also pointed out, discussing the currently available solutions.

II. THE GNSS INTEGRITY INFORMATION

The “integrity concept” is defined as the measure of the trust that can be placed in the correctness of the information supplied by a navigation system and it includes the ability of the system to provide timely warnings to users when the system should not be used for navigation [7].

The GNSS integrity framework, as currently provided by Satellite-Based Augmentation Systems (SBAS, for example EGNOS in Europe), Wide Area Augmentation Systems (WAAS) and Local Area Augmentation Systems (LAAS), was principally defined in the past fifteen years in the aviation context for Safety-of-Life applications [8] [9].

It has become evident that the concept of GNSS integrity and, especially, the concept of Protection Level (PL) is of interest not only in the aviation field, but also in other transportation fields which lately discovered the potential of a “reliable” (i.e., integer and possibly certified) positioning information [10] [11]. In fact, the availability of a PL associated to the position/time estimated by a GNSS receiver is of the utmost importance for all those applications which require a certain level of trust in the positioning information before deciding to use it (i.e. safety critical or liability critical applications). Examples of such newcomers are the maritime field (e.g. aiming to an increased safety for in-harbor operations), the rail field (with the potential passage from the traditional “fixed block” track management system based on balises to the new “moving block” system based on GNSS), and especially the vehicular field, with applications such as law enforcement, Pay As You Drive insurance and electronic toll collection [10].

A short overview of the integrity framework, as developed and validated for the aeronautical field, is provided in the following paragraphs, summarizing the general definitions and the related practical aspects. For further details, the interested reader may refer to [12].

Next, Section III will discuss its major limitation factors related to non-aeronautical applications.

A. The Concept of Expected Position Confidence

From a user perspective, it is interesting to have an estimation of the confidence in the positioning information produced by the GNSS receiver. Such a confidence is a statistical measure related to the errors between estimated positions and the true (unknown) position of the receiver, as illustrated in Fig. 1.

Such position confidence depends on:

- the quality of the measurements performed by the GNSS receiver, and
- the user-satellite geometry, expressed by means of the so-called Geometric Dilution of Precision (GDOP).

The GNSS measurements are essentially the distances (ranges) of the satellites in view from the receiver; they theoretically enable the computation of the user’s position via trilateration [13][14]. Because of the incertitude in the temporal reference affecting the range measurements, the time has to be resolved as an additional unknown of the problem and the distance measurements affected by this temporal uncertainty are called pseudo-ranges. The other errors affecting the pseudo-ranges are essentially due to non-idealties in the RF signal propagation and are compactly expressed in terms of the User Equivalent Range Error (UERE, i.e. \( \sigma_{UERE} \)), an expected standard deviation of all the non-recovered errors in the pseudo-range determination.

The simplest expression for the so-called expected position confidence represented in Fig.1 can be written as [13] [14]:

\[
\sigma_{pos} = \sigma_{UERE} \cdot GDOP
\]

where \( \sigma_{UERE} \) represents the standard deviation of the error affecting the pseudorange measurements and GDOP is a geometrical parameter dependent on the reciprocal positions of the user and the satellites in view (user-satellite geometry) which relates the pseudorange measurements errors to the errors in the estimated Position, Velocity and Time (PVT). Both these factors, \( \sigma_{UERE} \) and GDOP, are discussed in next subsections.

Figure 1. The concept of Position Confidence.
B. The User Equivalent Range Error

The User Equivalent Range Error represents a statistical indication of the quality of the pseudorange measurements performed by the GNSS receiver: it is usually expressed in the form of standard deviation ($\sigma_{\text{UERE}}$) of the pseudorange measurements errors.

The UERE is defined at the system design level, taking into account the different GNSS error sources: it represents the residual error on the measured pseudo-ranges after the removal of all the predictable error components (e.g. by using the correction models in single frequency GPS receivers). Such a residual error is modeled as an additive Gaussian random variable with zero mean and standard deviation $\sigma_{\text{UERE}}$ [14].

For modeling purposes, the standard deviation of the pseudorange measurement error is typically and simplistically assumed equal for all the in view satellites. The value of such aggregated $\sigma_{\text{UERE}}$ is obtained as the Root Sum Square (RSS) of the standard deviation of the individual error components, obtained by properly modeling the different error sources [14].

However, more detailed error models are based on the more realistic assumption of different standard deviation values for each $i$-th satellite in view ($\sigma_{\text{UERE},i}$), depending at least on the satellite elevation (e.g. see [15]). In fact, the $\sigma_{\text{UERE},i}$ values can significantly vary also depending on the receiver configuration (e.g., single/dual frequency, single/multi GNSS constellation, SBAS enabled/disabled) and on the operative environment (especially in urban scenarios). For these reasons, for the same system geometry, the obtainable position confidences can be significantly different.

In general, a proper characterization of $\sigma_{\text{UERE},i}$ to reliably take into account all the possible residual errors is a difficult task, which requires continuous monitoring of the global and local system performance [12].

It is worth noticing here that in the airports the monitoring of the local system performance (to get rid of interference, multipath shadowing and signal blockage, for example) is a complex task, for which, nevertheless, solutions have been developed [12][26][27]. On the contrary, the monitoring of local effects for vehicular applications is necessarily different: since the terrestrial surface that has to be monitored could have a continental extension, the airport-native solution is not scalable and another approach must be developed.

C. The Geometric Dilution of Precision

As already shown in (1), the GDOP represents the amplification of the standard deviation of the measurement errors onto the positioning solution and it is a function solely of the satellites-receiver geometry. It depends on the geometry of the constellation as seen by the receiver: the better is the relative geometrical positions between satellites and user, the lower is the GDOP. A larger number of satellites in nearly open-sky view usually leads to lower GDOP values, thus to better accuracy on the estimated position (lower $\sigma_{\text{pos}}$). For example, GDOP values higher than 4 are symptom of a possibly bad geometry.

GDOP can also be decomposed in its Horizontal (HDOP), Vertical (VDOP), and Time (TDOP) components; their analytical definitions can be found for example in [14].

D. Vertical and Horizontal Position Confidences

It is known that the GNSS accuracy along the vertical direction ($V$) can be significantly worse than the accuracy over the 2-dimensional horizontal plane ($H$) [16]. Furthermore, in many applications the accuracy required along the $V$ direction is different than that required on the $H$ plane (e.g., for an aircraft in any phase of its flight). For these reasons, it is typical to separately assess the accuracy performance along the $V$ and $H$ directions (e.g. see Fig. 2), so that also the position confidence previously defined in (1) may be separately addressed as:

- Vertical position confidence ($\sigma_V$);
- Horizontal position confidence ($\sigma_H$).

Furthermore, since the position domain error can be considered as a linear combination of pseudorange errors used in the navigation solution [17], the error variance in the position domain can be written as a linear combination of the error variances associated to each pseudorange measurement ($\sigma_{\text{UERE},i}^2$) from each $i$-th GNSS satellite in view. If all the individual pseudorange errors can be assumed to be independent, zero-mean, normally distributed, then also the position error is representative of a zero-mean normal distribution [17]. Evidently, the coefficients of such a linear combination depend on the algorithm used for determining the navigation solution, i.e., for combining the pseudorange measurements. Different analytical expressions are available for the computation of the Vertical and Horizontal position confidences in case of Least Squares (LS) or Weighted Least Squares (WLS) navigation solutions. In detail, in the case the differential corrections provided by a SBAS are applied for correcting the pseudoranges before using them in the navigation solution, the expressions for computing the standard deviation in the position domain residual errors can be found for example in [17].

Figure 2. Example of vertical and horizontal position confidences (shown in terms of ellipsoidal iso-probability contours [16]).
E. From Position Confidences to Protection Levels

In the context of GNSS, the so-called Protection Level (PL) descends from the expected position confidence and is intended as a measure of a confidence interval (one- or two-dimensional) around the estimated position/time in which the true receiver position/time stays with a certain pre-defined probability. The PL is formally defined as follows:

**Definition 1:** The PL is a statistical error bound computed so as to guarantee that the probability of the absolute position error exceeding said number is smaller than the target integrity risk.

In this definition the concept of integrity risk is equivalent to a measure of the acceptable probability that an error exceeds the PL bound during the mission or operation.

As for the position confidence, also a measure of the PL is typically given in a separate way for the horizontal plane (Horizontal Protection Level, HPL) and for the vertical direction (Vertical PL, VPL). As shown in Fig. 3, this means that the HPL and the VPL are referred to the horizontal plane tangent the Earth ellipsoid at the true receiver position or the direction orthogonal to that plane, respectively.

Protection levels are equivalently defined in the aviation domain by the Radio Technical Commission for Aeronautics (RTCA), specifically for a GNSS airborne equipment operating with a SBAS service [8], as follows:

**Definition 2:** the HPL is the radius of a circle in the horizontal plane (the plane tangent to WGS-84 ellipsoid), with its center being at the true position, that describes the region assured to contain the indicated horizontal position (within the required missed alert and false alarm). It is a horizontal region where the missed alert and false alarm requirements are met for the chosen set of satellites when autonomous fault detection is used.

Notice that the second definition is conceptually equivalent to the first one, although it introduces the missed alert and false alarm probabilities, as specifications of the integrity risk and continuity risk, respectively.

It also introduces the concept of fault detection, referred to a subset of significant errors which exceed the statistics included in $\sigma^2_{UERE,i}$. Operatively, the following definition can be written:

**Definition 3:** the PL defines the smallest position error that must be detected with the required probabilities of false alert and missed detection.

An error exceeding the PL is a misleading information (see Fig. 4); in case the application also defines an Alarm Limit (AL), the misleading information becomes hazardous as long as the error exceeds also the AL. However, as the errors are not known by nature, the two integrity events are not observable, unless in case of static surveys. Fig. 4 graphically represents the concepts of PL and AL, including the conventional nomenclature for the related integrity events (misleading information, hazardous misleading information).

It is worth pointing out that the PL is a function of the satellite/user geometry and the expected error characteristics: it is not affected by actual measurements. Its value is predictable given reasonable assumptions regarding the expected error characteristics and thus by proper modeling possible error sources.

The step from positioning confidence to protection level is represented by the following relationship:
where the multiplicative dimensionless factors \( k_H \) and \( k_V \) are necessary to propagate the position confidences (\( \sigma_H \) and \( \sigma_V \)) to a level compatible with the required integrity risk \([17]\), i.e., to guarantee the desired level of probability of missed detections, \( P_{md,X} \): \( k_X = k_X(P_{md,X}) \), where \( X \) stands for the \( H \) or the \( V \) dimension. In practice, such computation can be cumbersome, because the distribution of the position errors can be non-trivial.

### III. LIMITATIONS OF THE CLASSIC INTEGRITY

It is important to remark that the “classic” GNSS integrity framework introduced above was principally defined and developed in the aeronautical context. Being a strictly Safety-of-Life context, the development of a strong system integrity framework has been of the utmost importance. Therefore extensive studies focused on various aspects of the GNSS integrity in the aeronautical field have been conducted and the literature addressing such approaches is almost exterminated (see for example \([12]\) and references therein).

However, as briefly anticipated in the previous section, the applicability of the aviation-born integrity concepts to other transportation fields is far from being straightforward: it has been argued that a deep reconsideration of the approach is necessary in order to effectively exploit GNSS integrity in non-aviation operations \([10]\) \([11]\). In fact, the classic integrity is known to be affected by the following conceptual and practical limitations:

- The conventional analytical models used to predict the pseudorange error variances (assuming an open-sky satellite visibility and diffuse ground multipath) may be no more consistent for mass-market automotive receivers. In fact, the aviation-born error models do not explicitly account for impairments difficult to be predicted, such as limited satellite visibility, multipath, non-line-of-sight signals, deep fast fading, whose probability of occurrence is high in urban scenarios \([10]\);
- The typical values associated to the integrity risk in aviation operations (in order to bound maximum plausible positioning errors) could be too conservative with respect to the requirements of vehicular applications, especially in non-Safety-of-Life cases \([11]\);
- The limited availability of the SBAS satellite signal in space in typical urban canyons can impair the applicability of the classic integrity concept to the vehicular context, where either the SBAS satellites can be not in visibility or the obtained PLs can result extremely large (unusable) due to a poor satellite geometry (as demonstrated for example by the measurement campaigns reported in \([18]\));
- The classic integrity approach does not take advantage of possible additional information potentially available from multiple receivers, as for example from a Vehicular Ad-Hoc Network (VANET) infrastructure. In fact, the growing interest on connected vehicles, smart cities, and related applications allows foreseeing an extensive deployment of VANETs in the medium term, paving the way for new distributed services and technologies based on cooperative network connectivity between vehicles. In this context, additional services based on GNSS-related data exchange between vehicles and/or road-side units could be implemented among other VANET-based services.

The investigation of possible solutions, aiming to overcome the major limitations of the classic SBAS integrity concept, is an active research topic, which is gaining attention in the GNSS community.

Some promising approaches, based on collaborative positioning and/or sensor fusion (i.e. the fusion of positioning information from multiple sensors, e.g. by means of a particle filter \([2]\)), allow to improve the positioning performance in terms of accuracy, the precision and the availability in harsh environments. However, these hybrid approaches do not usually provide information about the trustfulness of the obtained positioning solution (i.e. protection levels).

An interesting proposal for re-tailoring the classic integrity concept to urban and road environments has been presented in \([10]\). Nonetheless the implementation of this autonomous integrity method (patented by GMV Aerospace and Defense S.A. \([19]\)) is quite complex and of course it does not exploit any potentiality of a VANET.

As an alternative solution, the novel concept of “local integrity” is proposed in \([20]\). The idea is to exploit the potentialities offered by the VANET infrastructure to cope with the highlighted problems and limitations of the “classic” SBAS integrity approach in urban vehicular scenarios. In detail, the potential availability of multiple observations of GNSS signals, taken by different vehicles participating to a VANET, can be shared and combined in order to implement a collaborative spatial/temporal characterization and continuous monitoring of the local degradations of the GNSS signals. This idea is being investigated within the EU FP7 “GLOVE” project (joint Galileo Optimization and VANET Enhancement \([21]\)\([22]\)).

### IV. THE NEED FOR POSITION AUTHENTICATION

The growing penetration of liability critical applications and services is pushing the demand for authentication solutions, in order to guarantee the correctness and fairness of decisions which depend on the GNSS positioning (for example, in case of road charging). In general, the position authentication could be used by applications that are sensitive to possible frauds, because current GNSS receivers (e.g. those using the GPS L1 C/A signal) can be spoofed to avoid being charged \([5]\). On top of this, some applications, as law enforcement and dangerous goods transportation, may need a strong authentication service, possibly based on cryptographically secure signals.

Unfortunately, the position authentication cannot be ensured by current standalone receivers, which solely exploit civil GNSS signals. Some solutions are already available, based on a client-server approach, in which for example the hidden/unknown attributes of military GNSS signals (i.e. GPS L1 P(Y) codes) are cross-compared between different locations in order to authenticate the civil signals \([23]\).
Other approaches aim to increase the security of civil receivers by adding countermeasures against jamming, meaconing or spoofing attacks, for example double-checking the PVT result of the GNSS receiver with other sensors (e.g. IMU, compass, Wi-Fi or cellular network positioning) [5].

Furthermore, some interesting proposals have already been made for the implementation of authentication services based solely on GNSS signals. In detail, simple modifications of the current civil signal-in-space (or at least of the navigation message content) have been proposed both for the modernized GPS [24] and the Galileo Open Service signals [25]. Thus, in the near future the position authentication will be provided as an added value by the GNSS system itself, for example by the Galileo Commercial Service: this will allow the receivers to perform a standalone assessment of the authenticity of the computed position, decreasing the need of costly additional sensors or other countermeasures to spoofing attacks.

V. CONCLUSIONS

The importance and the benefits motivating the dissemination of position integrity and authentication information have been discussed, aiming to increase the awareness on the current problems and limitations in vehicular applications. Possible solutions, suitable to ITS applications based on mass-market GNSS receivers, have been mentioned.

As a final remark, it is possible to forecast that future GNSS-based applications will increase their reliability and robustness exploiting added value services offered by GNSS systems and collaborative or client-server architectures, especially feasible with an extensive deployment of VANETs. This trend will allow reducing the cost and the implementation complexity currently required for ensuring the continuity and the integrity of the services (e.g. additional countermeasures against jamming and spoofing attacks).

ACKNOWLEDGMENT

This article presents some ideas and results of GLOVE [21], a project co-funded under the 7th Framework Program, in the context of “Exploiting The Full Potential- GALILEO-2011-GSA-1”, Grant Agreement n. 287175. The article reflects the views only of the authors and the EU cannot be held responsible for any use that may be made of the information contained therein.

REFERENCES

[22] GLOVE project’s official web site: http://www.glove-fp7.eu/