



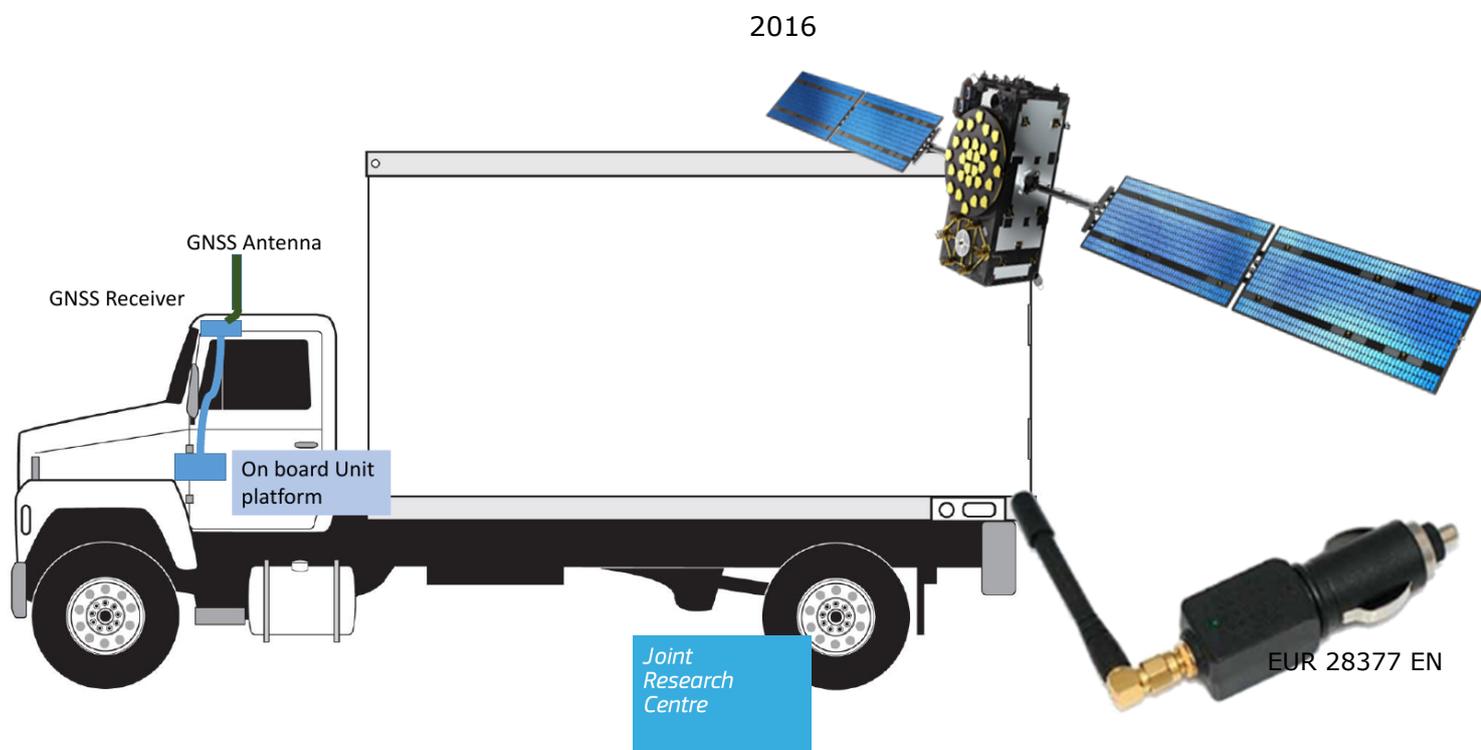
European  
Commission

## JRC TECHNICAL REPORTS

# Robust GNSS Services for Road Transportation

*Analysis and studies to  
mitigate GNSS threats in  
the road transportation  
sector*

Gianmarco Baldini,  
Daniele Borio,  
Ciro Gioia,  
Raimondo Giuliani,  
Eduardo Cano-Pons



This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

#### Contact Information

Name: Gianmarco Baldini  
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 360, 21027 Ispra (VA), Italy  
E-mail: gianmarco.baldini@jrc.ec.europa.eu  
Tel.: +39 0332 78 6618

#### JRC Science Hub

<https://ec.europa.eu/jrc>

JRC104649

EUR 28377 EN

PDF	ISBN 978-92-79-64803-8	ISSN 1831-9424	doi:10.2788/953749
Print	ISBN 978-92-79-64802-1	ISSN 1018-5593	doi:10.2788/301839

Luxembourg: Publications Office of the European Union, 2016

© European Union, 2016

The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted. The European Commission shall not be held liable for any consequences stemming from the reuse.

How to cite: Gianmarco Baldini, Daniele Borio, Ciro Gioia, Raimondo Giuliani and Eduardo Cano Pons; *Robust GNSS Services for Road Transportation*, EUR 28377 EN, doi 10.2788/953749

All images © European Union 2016

#### Robust GNSS Services for Road Transportation

This report provides an overview of the activities carried on in 2016 in the JRC.E in the context of GNSS for road transportation.

# Robust GNSS Services for Road Transportation

Gianmarco Baldini,

Daniele Borio,

Ciro Gioia,

Raimondo Giuliani,

Eduardo Cano-Pons



**Contents**

Abstract ..... 1

1. Introduction ..... 2

2. GNSS Jamming ..... 5

3. Augmented GNSS with IMU ..... 7

4. Galileo Open Service (OS) Authentication ..... 11

5. GNSS Receiver Fingerprinting for White List Authentication ..... 13

6. Conclusions ..... 16

7. Annex 1 - Jammer Localization: from Crowdsourcing to Synthetic Detection ..... 17

8. Annex 2 - Trapping the Jammer: the Slovenian Experiment ..... 18

9. Annex 3 - GNSS Receiver Fingerprinting for Security-Enhanced Applications ..... 25

References ..... 26

List of abbreviations and definitions ..... 27

List of figures ..... 28

## Abstract

The application of Global Navigation Satellite System (GNSS) services in the road transportation sector has substantially increased in recent years. Position Velocity and Time (PVT) information is playing and will play even more in the future a crucial role in all aspects of Intelligent Transportation System (ITS) technologies. There are many ITS applications which benefit from the use of GNSS services like active safety, advanced driver assistance, road tolling, digital tachograph, fleet management. In the near future, autonomous driving and Cooperative Intelligent Transport Systems (C-ITS) will strongly depend on the position and localization technologies.

In comparison to other domains where GNSS is used, road transportation applications often include safety or regulatory aspects where the accuracy and reliability of position information need to be known a priori to assure active safety. For example, the new version of the digital tachograph defined in regulation EC 165/2014 requires the use of GNSS to record the start and end location of the activity of a driver of a commercial vehicle. In addition, the user location must be recorded every three hours of accumulated driving time. There are significant economical gains for malicious parties to falsify the data calculated from GNSS. The unavailability of GNSS services can also have a significant negative impact in the above mentioned regulated applications. While current safety related applications in the road transportation sectors are loosely dependent on satellite data due to the uncertainty of positioning errors, to data/signal delays and quality-of-service issues, future applications are expected to better exploit the potential offered by modern and future GNSS signals and services. For example, autonomous driving could benefit from GNSS services if they will be able to provide accurate and precise location data in a timely manner. As a consequence, it is important to mitigate threats (both intentional or unintentional) which could negatively impact the provision of GNSS services and to investigate complementary means which could be used to make more robust and accurate the calculation of PVT information in the road transportation sector.

In addition to Radio Frequency (RF) threats, the provision of PVT information from a GNSS receiver can be impaired through the manipulation of the data output by the receiver itself. In a vehicle, the GNSS receiver may be integrated in a network where PVT information is used by several devices. A malicious entity may falsify the information provided by the GNSS receiver in the internal in-vehicle network compromising the operations of the devices connected. In this context, the authentication of the source of information (e.g., the GNSS receiver) to the on board platform is also important.

The goal of this report is to provide an overview of the activities carried on in 2016 in the unit E.2 and E.3 in the context described above. In particular, the following activities were carried out:

1. Experimental campaigns of jamming of GNSS signals in a road transportation context.
2. Analysis and experimental evaluation of authentication of a GNSS receiver using the physical properties of the GNSS receiver itself.
3. Experimental evaluation of augmented GNSS using Inertial Mounted Unit (IMU) systems with Extended Kalman Filterings (EKFs) and Particle Filterings (PFs).
4. Preliminary evaluation of the authentication of the Galileo OS.

In some cases, the analysis was performed and published in the form of a scientific paper submitted to a journal or a conference. While this report provides a summary of the results from the scientific papers, the details of the analysis are in the papers themselves. The papers are provided as annexes.

# 1. Introduction

The application of Global Navigation Satellite System (GNSS) to the road transportation sector has steadily increased in recent years. In fact, the road transportation sector has been one of the early adopter of GNSS technology to track vehicles, support the user driving and facilitate the delivery of goods and persons.

There are many applications, which benefited from the application of GNSS:

1. *Fleet Management*: where the location of the fleet vehicles at any given time is very important for the fleet manager to monitor the status of the delivery and to improve the route selection.
2. *Driving support*: where the location of the vehicle can support the driver to identify more efficiently the best route to reach the destination.
3. *Traffic management*: where road authorities can use the vehicle locations to assess the traffic conditions and improve the road management.
4. *Tolling*: where the information needed to calculate tolling can be based on the position recorded and transmitted by GNSS receivers installed in the vehicle rather than using Dedicated Short Range Communications (DSRC) systems
5. *Specific regulated applications*: where the Position Velocity and Time (PVT) information provided by the GNSS receiver is used to satisfy policy needs. Examples are the eCall and the digital tachograph.
6. *Pay as you drive insurance schemes*: where the insurance fee is based on the driving activity rather than on a flat yearly fee.

This list is only a subset of a wider list of Intelligent Transportation System (ITS) applications, which benefited from the application of GNSS and which are already quite familiar to the general user. Future applications can also benefit from GNSS. For example, autonomous vehicles could use the PVT provided by GNSS to improve the cognitive driving process. Cooperative Intelligent Transport Systems (C-ITS) could use the same PVT information, which exchanged among the vehicles and the roadside systems (called C-ITS stations) to improve vehicle coordination, safety and traffic efficiency.

To support current and future applications, the PVT information should be reliable, precise and accurate. More specifically, the following high level requirements should be satisfied:

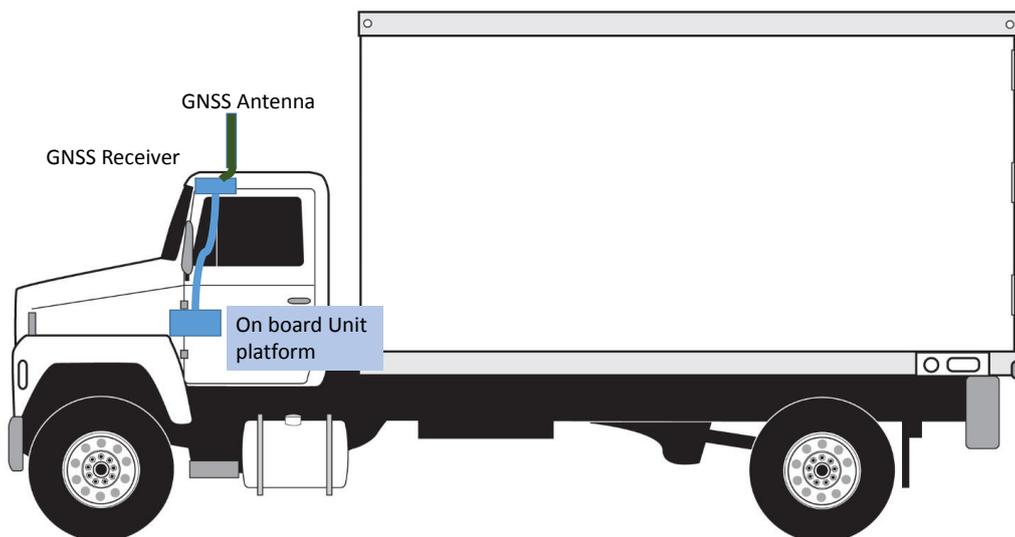
1. *Availability*: GNSS signals and services should be available to the vehicle at any time. This may not be always possible, because physical obstacles (e.g., buildings in an urban environment) or wireless interference either intentional (e.g., jamming) or unintentional which could degrade or block the GNSS signals before they reach the GNSS receiver.
2. *Reliability*: the provided information (i.e., PVT) should be reliable. In other words, it should be resistant against attacks, which could change the content transmitted by the GNSS signal. An example is the spoofing attack, which changes the content of the GNSS data.
3. *Accuracy*: the PVT provided by the GNSS receiver should be accurate. There is an extensive bibliography on the analysis of the factors, which contribute to the accuracy of the PVT solution. These factors may include physical obstacles (as for availability) or other conditions. Accuracy could be improved if the GNSS data are complemented by other sources such as accelerometers and gyroscopes which could be installed in the vehicle.
4. *Timeliness*: the provided information should be processed in time so that the user applications can exploit it. For example, in the C-ITS context, the safety messages are transmitted and received quite frequently (e.g., many times in a second). Because a safety message contains PVT information, the GNSS signals should be processed by the telematics systems in the vehicle in short time.

In this report, we will focus on the requirements 1), 2) and 3) as timeliness is often a performance aspect addressed by the producer of the GNSS receiver. In particular, we investigated:

1. what is the impact of an intentional attack on GNSS signals through jamming in a road transportation context to address requirement 1).
2. how the accuracy of the position provided by a GNSS receiver can be improved exploiting the information provided by additional accelerometers and gyroscopes installed in the vehicle. This is to address requirement 3).
3. if new authentication mechanisms could be used. In particular, we investigated the authentication of the open service of Galileo to address requirement 2).

Another aspect is related to the distribution of GNSS information. When the GNSS receiver is external to the processing platform, i.e. the On Board Unit (OBU) of the vehicle, it is important to protect the data provided by the GNSS receiver. A view of the possible architecture where the GNSS receiver is external to the OBU is shown in Figure 1. This architecture has been considered for applications such as the digital tachograph.

**Figure 1:** Architecture where the GNSS receiver is external to the OBU. In this case, the connection used to provide GNSS data should be secured.



The link between the GNSS receiver and the OBU must be protected. This can be achieved through cryptographic means, but the distribution of cryptographic keys could be complex to implement or the keys could be compromised. Even with this potential shortcomings, this is the used approach to secure the link between the motion sensor and the vehicle unit of the digital tachograph and it is also the one implemented for standard ISO 16844.

In our research work, we have also investigated the possibility to authenticate the sensor through the physical properties of the GNSS receiver itself and the way it processes the GNSS data. In this way, the authentication can be based on the intrinsic physical features of the GNSS receiver.

The report provides the results and the investigation carried on in the areas described previously on the basis of the following structure:

- Section 2 describes the analysis on the impact of GNSS jamming. The analysis is extracted from published papers presented at conferences at journals by the authors of this report.

- Section 3 describes the algorithms and the results of the experimental campaigns to improve GNSS accuracy using Inertial Mounted Unit (IMU) integration.
- Section 5 describes the potential use of GNSS fingerprinting to support multi-factor authentication of the GNSS receiver. The analysis is extracted from published papers presented at conferences by the authors of this report.
- Section 4 describes the activities carried on in 2016 by the DG JRC E.2 and E.3 units in the context of the Galileo Open Service (OS) authentication.

## 2. GNSS Jamming

GNSS jamming consists in the emission of a powerful electromagnetic wave towards a victim GNSS receiver with the ultimate goal of preventing the computation of the user PVT. Jamming can be perpetrated using low-cost portable devices called jammers. The proliferation of such devices is expected to grow along with the development of GNSS-based services.

In the road transportation sector, a malicious entity can have a commercial interest to implement jamming to deny the collection of PVT data from the GNSS receiver. For example, electronic tolling based on GNSS or the new version of the digital tachograph (i.e., smart tachograph based on European regulation 165/2014) are dependent on GNSS. A dishonest user can obtain an unfair advantage because the tolling manager or the law enforcer would not be able to get the needed specific positions of the vehicle to ensure conformance to regulations.

There is an extensive literature on the implementation of GNSS jamming attacks and on possible countermeasure. A recent special issue of the IEEE Proceedings (June 2016, Vol. 104, Issue 5) investigated different GNSS threats and mitigation approaches. In particular, possible solutions to address GNSS jamming include

1. jamming detection (Borio et al., 2016)
2. mitigation of the jamming effects (Gao et al., 2016)
3. localization of the jamming source (Dempster and Cetin, 2016).

Although the first two solutions have been extensively investigated, jammer localization has recently received significant attention from the scientific community and research groups have devoted their efforts to the design of localization techniques. The fast and accurate identification of the location of the jammer source is a very effective way to stop jamming. In fact, jamming localization could become a powerful tool used by law enforcers to identify in the road infrastructures the presence of a non-compliance related to the use of GNSS. For example, a jammer localization system used by a law enforcer could identify the presence of a GNSS jammer on a commercial vehicle, which is used to deny the collection of position information for the smart tachograph. Beyond road transportation, the usage of GNSS jammers is considered illegal in most countries because it could interfere with needed services in other domains (e.g., synchronization of the smart grids or telecommunication infrastructures) and the availability of reliable localization techniques will simplify the operations of authorities trying to stop this phenomenon.

To investigate the technical feasibility to identify GNSS jammers, some of the authors of this report have conducted experimental campaigns in a realistic road environment.

The experimental campaigns were performed in Slovenia and they were authorized by the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS). The experimental activities were conducted in collaboration with the University of Ljubljana and its branch in Portorož, Slovenia. The experiments were conceived to evaluate the size of the area affected by a GNSS jammer installed on a vehicle driving at different speeds on the road. Different detection approaches were considered by using both GNSS receivers (even included in consumer grade smartphones) and low cost Software Defined Radio (SDR) platforms, with the objective to reveal the presence of the GNSS jammer and identify its location. Two experimental campaigns were conducted: the first in July 2015 and the second in November 2015.

A detailed description of the experimental settings and the results obtained in the experimental campaigns are provided in the following two papers:

- the paper presented at the ION GNSS+ 2016 conference in Portland Oregon 'Jammer Localization: from Crowdsourcing to Synthetic Detection' registered in the JRC PUBSY systems with identifier JRC100806.
- the paper published in the magazine Coordinates 'Trapping the Jammer: the Slovenian Experiment' registered in the JRC PUBSY systems with identifier JRC103329.

Both papers are available in the JRC PUBSY system and they are also reproduced in Annex 1 of this report. Both papers demonstrate the possibility of detecting and localizing

jammers using low-cost Commercial Off-The-Shelf (COTS) components and  $C/N_0$  measurements provided by commercial GPS receivers and by smartphones.

### 3. Augmented GNSS with IMU

In this section, we describe the work done to improve the accuracy of the the position calculated using GNSS on the basis of the fusion with IMU data. GNSS is not the only available positioning technology. Wireless Communication technologies based on ranging can also provide accurate position depending on the environment and the features of the wireless communication technology (e.g., bandwidth, power). Another class of positioning systems is based on IMU, i.e the combination of accelerometers and gyroscopes.

In 2014 and 2015, the JRC has conducted a project on the use of IMU to improve accuracy of the GNSS reported position in the context of road transportation. The idea was to combine GPS measurements with additional information coming from various vehicle sensors and, in particular, from an IMU installed in a vehicle. Unluckily, solving the data fusion problem may entail a formidable complexity mainly due to a) the intrinsic nonlinearity of the involved measurement and state models, and b) the large dimensionality of the system state. A theoretical model was implemented by Prof. Vitetta from Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT) to address these issues and it was published as report JRC93775. In the report, the problem of navigation is analysed from a theoretical viewpoint and it is shown that methods for mixed linear/nonlinear systems, like Particle Filtering (PF) and Extended Kalmann Filtering (EKF), can be exploited to solve this problem at an acceptable complexity. The problem of embedding map information in the filtering process was also analysed. The theoretical model was then implemented in MATLAB and tested with real data collected in measurement campaigns where the GNSS receiver and the IMU were installed on a vehicle.

A microcomputer connected to a DAISY 7 board with an IMU and a GNSS receiver was installed in a vehicle and it was used to collect data in a specific route in the JRC campus. The setup and the car used in the experiment are shown respectively in Figures 2 and 3.

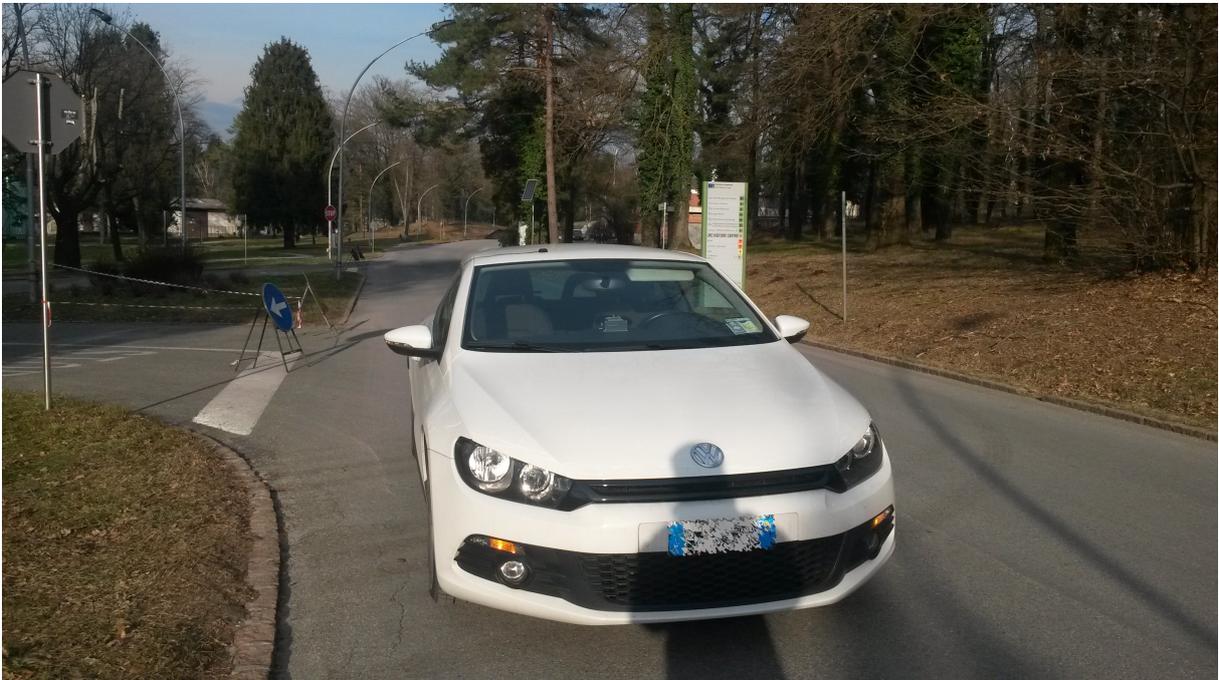
**Figure 2:** View of the experimental platform used to collect GNSS and IMU data.



The path selected for the experiment is shown in Figure 4.

The three approaches used to estimate the user location are compared in Figure 5. The three approaches considered are GPS alone and EKF and PF with IMU data fusion. From the figure, we note that the combination of GPS with PF provides a better accuracy than with the other sensors (GPS and IMU).

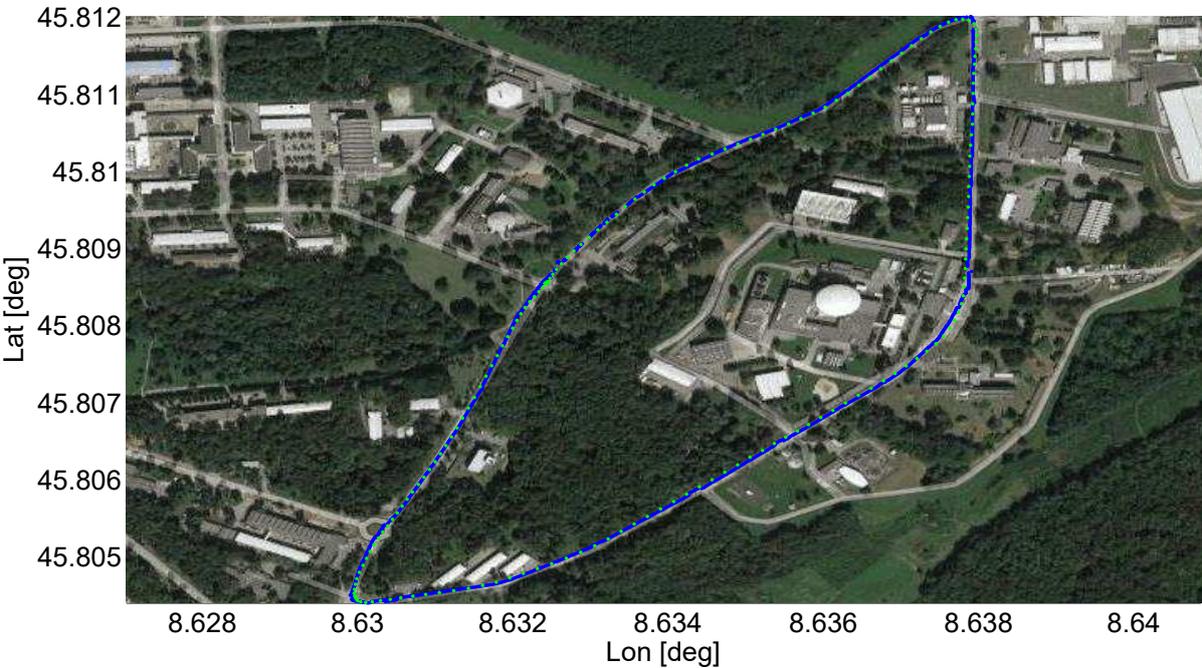
**Figure 3:** The car used in the GNSS/IMU experiment.



**Figure 4:** Path selected for the experimental campaign involving GNSS and IMU data.



**Figure 5:** Trajectories estimated using the GPS only solution and the PF. Map information has been added to the data fusion process.



## 4. Galileo OS Authentication

As described in the introduction, there is the need to mitigate various threats to the provision of PVT through GNSS in road transportation. In particular spoofing attacks where the PVT data can be modified. If implemented successfully, a spoofing attack can be a more serious threat than jamming because a false information can directly create a safety hazard (as in the case of C-ITSS) or indirectly by tampering with correct operations of regulated application like the digital tachograph.

Several techniques have been proposed to mitigate GNSS vulnerabilities like spoofing. Adding cryptographic features to GNSS signals is one of them. This is the case of the Commercial Service (CS) of Galileo, which is not free.

Another possibility has been proposed recently in (Fernández-Hernández et al., 2016), where it is described the authentication of the Galileo OS, the Navigation Message Authentication (NMA) used to protect the Galileo navigation message. NMA can make the Galileo OS more resilient against spoofing attacks, and therefore protect Galileo signals against certain threats.

The proposed Galileo authenticated services may provide major benefits to users at a very low additional cost to the programme. It is planned that Galileo will start to transmit the OS NMA as of 2018, and it will be included in the full operational capability in 2020.

The OS NMA is very useful for the new smart tachograph where it is specifically requested by regulation 165/2014 that the used GNSS service is free of charge, which forbids the use of the commercial service of Galileo.

DG.JRC.E.2 and DG.JRC.E.3 worked together with DG GROW and European GNSS Agency (GSA) on the OS NMA. E.2 supported the definition of OS NMA, while E.3 has worked on the application of OS NMA to the digital tachograph.

In August 2016, representatives from E.2 and E.3 have met Ignacio Fernandez Hernandez from DG GROW to discuss how to support DG GROW for the assessment of OS NMA in prevision of its future deployment.

As Dr Fernandez Hernandez explained in a series of slides at the GNSS summer school organized in Ispra in August 2016, the OS NMA will be based on TESLA which is briefly summarized in Figure 6. The main service drivers for the definition of OS NMA are:

- Open access: it requires the uses of asymmetric cryptography.
- One-to-many: satellites provide a one way communication channel.
- Noise tolerance: the GNSS channel is noisy and has a low bandwidth.
- Commensurate receiver requirements: CPU, memory, connectivity, protection.
- Long-term security: OS NMA should provide long-term cryptographic security.
- Backward compatibility: the introduction of OS NMA should not affect users not interested.

While OS NMA is a very important key differentiator for Galileo in comparison to other GNSSs (i.e. GPS, Glonass, Baidu), it does not guarantee security against all types of attacks. This is predictable because CS and Public Regulated Service (PRS) are designed for higher level of security. Still, it is quite important to support DG GROW and evaluate against which types of attacks OS NMA can be used. This will be the main objective of the collaboration between E.2, E.3 and DG GROW in 2017.

**Figure 6:** Schematic representation of the OS NMA scheme based on TESLA protocol. From the presentation of Dr. Fernandez Hernandez, Ispa, Italy, July 2016.

## TESLA PROTOCOL

Achieving asymmetry through the **delayed symmetric key disclosure**:

- Generate **chain of keys** from a seed key through a 1-way function

$$K_0 = F^n(K_n)$$

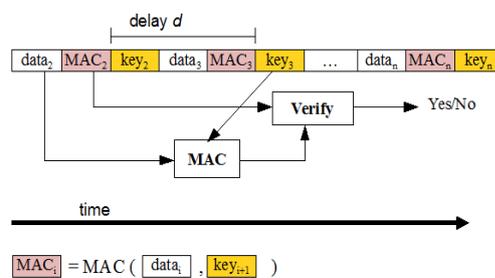
$$F(K_m, GST_j) = trunc(K_{len}, hash(K_m || GST_j))$$

- **Transmit root key** signed (public-private scheme; receiver has public key)
- Generate and transmit **Message Authentication Code (MAC)** authenticating nav data with a key of the chain, not yet disclosed.

$$MAC_{j,i,l} = trunc(n, mac(K_{j,MAC}, (i || l || CTR || P_{j,l})))$$

(j=key index; i=tx sat index; l=auth sat index)

- **Transmit key**  $K_j$  after some delay.
- **Authenticate key** with  $K_0$  by 1-way function
- **Authenticate data** (n) with received MAC and  $K_j$



## 5. GNSS Receiver Fingerprinting for White List Authentication

As described in Sections 2 and 4, the processing of GNSS signals by a GNSS receiver can be negatively impacted by jamming and spoofing attacks and potential countermeasures (e.g., detection and location of the jammer) have been presented. In this section, we describe another potential threat to the use of GNSS in the road transportation sector, i.e. GNSS data faking.

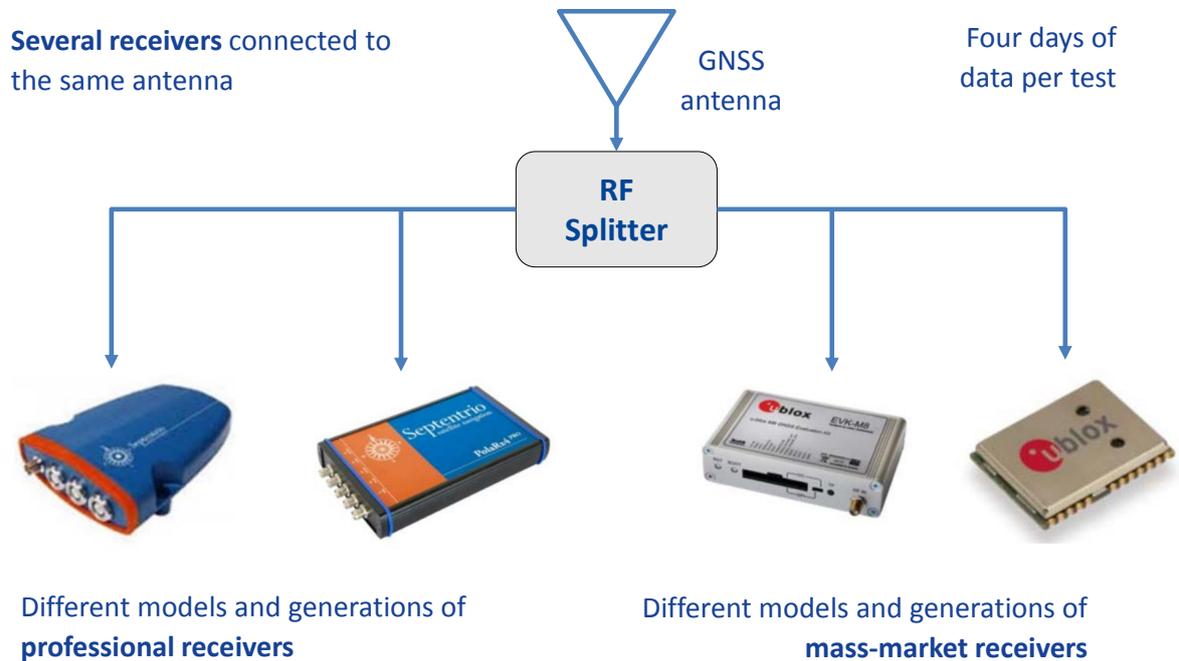
Even if the GNSS receiver is able to mitigate jamming and spoofing, the processed PVT information must still be provided to other platforms and to components present in the commercial vehicle. As shown in Figure 1, a road transportation application like fleet management could require the installation of an OBU in a vehicle, which must be connected to an external GNSS receiver. Even if an OBU could be installed with an internal GNSS receiver, it could be more practical to have one external GNSS receiver which could serve different applications present in the vehicle platform (there could also be different OBUs). The connection between the GNSS receiver and the OBU could be *paired* or *coupled* through cryptographic means, where the OBU and the GNSS receiver mutually authenticate each other. While this solution is technically feasible and there are many low cost cryptographic components, which could be used for this purpose, it may be organizationally complex because the OBU and the GNSS receiver should be equipped with symmetric or asymmetric keys. These keys should be installed in the initial deployment of the commercial vehicle or during the installation of equipment required by specific application. The keys should be protected from external attacks. One possible way would be to make the GNSS receiver and the OBU tamper-proof. In addition, the cryptographic material should be updated when the underlying cryptographic algorithm is not considered secure any longer or in case of its public disclosure.

We investigated another potential solution, which could be used to support the authentication of the GNSS receiver by the OBU. This solution is based on the exploitation of the unique physical or software features of the GNSS receiver. These characteristics are difficult to be cloned or modified because they are part of the device itself. There is an extensive research literature on the exploitation of the physical properties of an electronic device to authenticate it. In most cases, this can be achieved because each electronic component has tiny differences generated in the manufacturing process or due to the materials which composes it. This produces a unique fingerprint which plays a role similar to that of DNA in human beings. Similarly to the DNA, a fingerprint can unequivocally identify a device. Fingerprints can be determined using the digital output generated or emitted by the electronic device. For example, there is an extensive literature on the exploitation of the Radio Frequency (RF) emissions of consumer mass market mobile phones, which can be used to uniquely identify the phone itself with high accuracy (Hasse et al., 2013). In other cases a phone can be identified by its digital camera (Li, 2010) or by the digital output of its accelerometers (Baldini et al., 2016). To the knowledge of the authors of this report, there is no research record on the possibility to fingerprint a mobile phone by using its internal GNSS receiver. The identification of the GNSS receiver through its digital output could be used to pair it to the OBU or the OBUs in the commercial vehicle. In a potential deployment scenario, OBU could record the specific fingerprint of the paired GNSS receiver in the installation phase of the application and the OBU. If the GNSS receiver is replaced by another device by a malicious entity the OBU could compare the different fingerprints and understand that the device has been replaced. In other words, the fingerprint is used to authenticate the legitimate GNSS receiver and mitigate the risk of its replacement with another device, which could provide false data. Note that the fake GNSS receiver will have difficulties to provide data leading to a fingerprint similar to that of the original device. The fingerprint can be based and represented with many different statistical features which have to be intrinsically robust to forgery. The selection of appropriate features is a key aspect which makes data forgery difficult.

To investigate this approach, some of the authors of this report have performed experimental campaigns with a significant number of GNSS receivers in different conditions and they have collected the data generated by the GNSS receivers. The test setup adopted for this purpose is schematically shown in Figure 7.

The analysis performed on the data collected from GNSS receivers, the identification of fingerprints on the basis of the selected features and the classification results were presented at the ION GNSS+ conference in September 2016 at Portland, Oregon, USA. The conference paper is presented in Annex 3.

**Figure 7:** Different types of GNSS receivers used for fingerprinting.



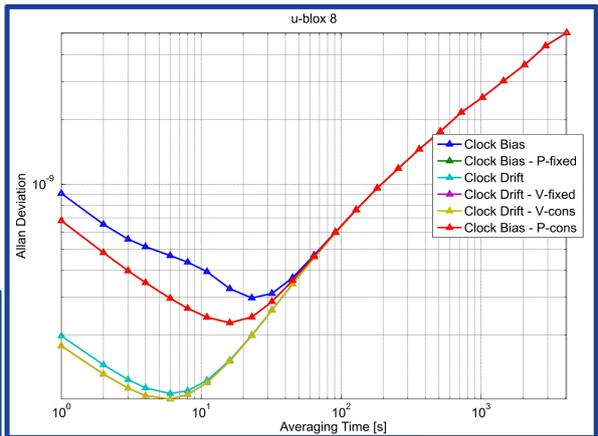
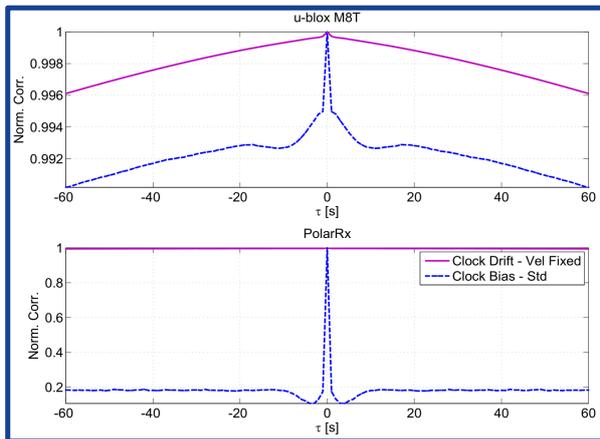
Statistical features were derived from the raw data of the GNSS receiver. This output includes pseudoranges and Doppler measurements. Some of the basic features considered in the paper are briefly illustrated in Figure 8. The features selected are based on the behavior of the GNSS receiver under test. GNSS receivers naturally provide the bias of their local clock with respect to a stable GNSS time scale. The clock bias characterizes the GNSS receiver and clock-related features can be derived considering parameters such as the Allan Deviation (ADEV) and the correlation between the samples of the clock bias time series. These parameters are illustrated in Figure 8. The statistical features are evaluated at period of time in order to assess their variability. The stability of the features is an important requirements for the definition of a fingerprint which should be stable over time. As described in detail in the Annex, the best statistical features were selected based on their capacity to distinguish the different GNSS receivers. The best set of statistical features was used to generate the fingerprints for the GNSS receivers. As seen from Figure 9, which provides the final results, it is possible to distinguish the GNSS receivers of different models but it is not possible to distinguish in a effective way GNSS receivers of the same model. This may be a limitation for the application of this approach for authentication because different GNSS receivers are not distinguishable. On the other side, a malicious device, which replaces a valid GNSS receiver, may have a very different hardware structure (it may not even be a GNSS receiver) and it could be considered a different model, so this approach could be valid in this context.

Short-term clock-derived features are the most effective with features derived from Doppler measurements more stable to environmental changes. From Figure 9, the possibility of distinguishing professional and mass-market receivers clearly emerges. Future work will use a wider set of statistical features and a larger number of GNSS receivers.

**Figure 8:** Clock-derived metrics used for the selection of statistical features used for fingerprinting.

**Allan Deviation:**

$$\sigma_A(\tau) = \sqrt{\frac{1}{2(N_\tau - 1)} \sum_{i=1}^{N_\tau-1} (\tilde{f}_{e,K}[i] - \tilde{f}_{e,K}[i-1])^2}$$



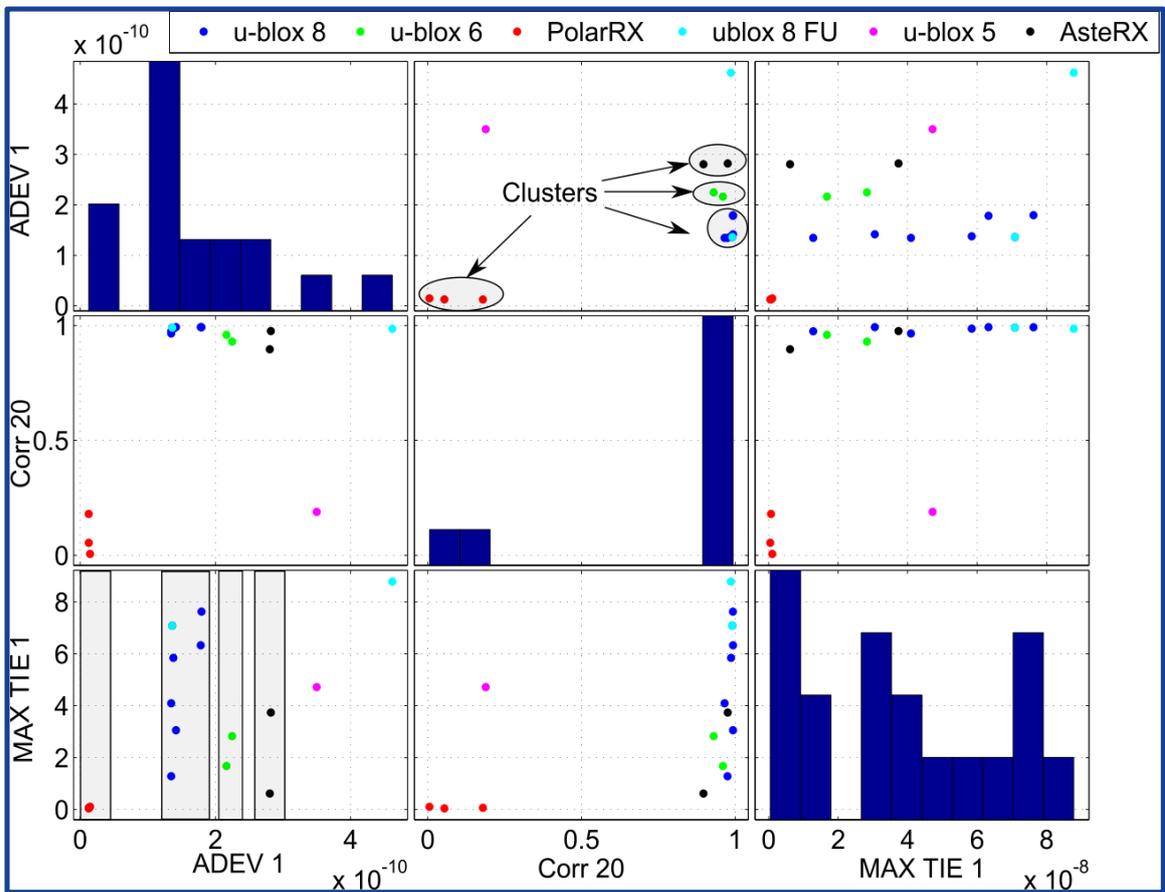
**Correlation:**

$$\tau = KT_s$$

$$R(\tau) = \frac{1}{\sigma_f^2(N-K)} \sum_{n=K}^{N-1} (f_e[n] - \bar{f}_e)(f_e[n-K] - \bar{f}_e)$$

Average freq. error

**Figure 9:** Sample classification results for different GNSS receivers.



## **6. Conclusions**

In this report, we have described the main activities of DG JRC.E.2 and DG JRC.E.3 in the area of the application of GNSS to road transportation. In particular, we investigated the possible threats to GNSS like jamming and spoofing. The work will continue in 2017 with specific focus on Galileo OS NMA and research in improving the accuracy of GNSS using data fusion with IMU systems installed in a vehicle.

## **7. Annex 1 - Jammer Localization: from Crowdsourcing to Synthetic Detection**

The paper *Jammer Localization: from Crowdsourcing to Synthetic Detection* is available at <http://www.ion.org/publications/abstract.cfm?jp=p&articleID=14689>

The paper should be cited as:

Borio, Daniele, Gioia, Ciro, Štern, Andrej, Dimc, Franc, Baldini, Gianmarco, "Jammer Localization: From Crowdsourcing to Synthetic Detection," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, September 2016, pp. 3107-3116.

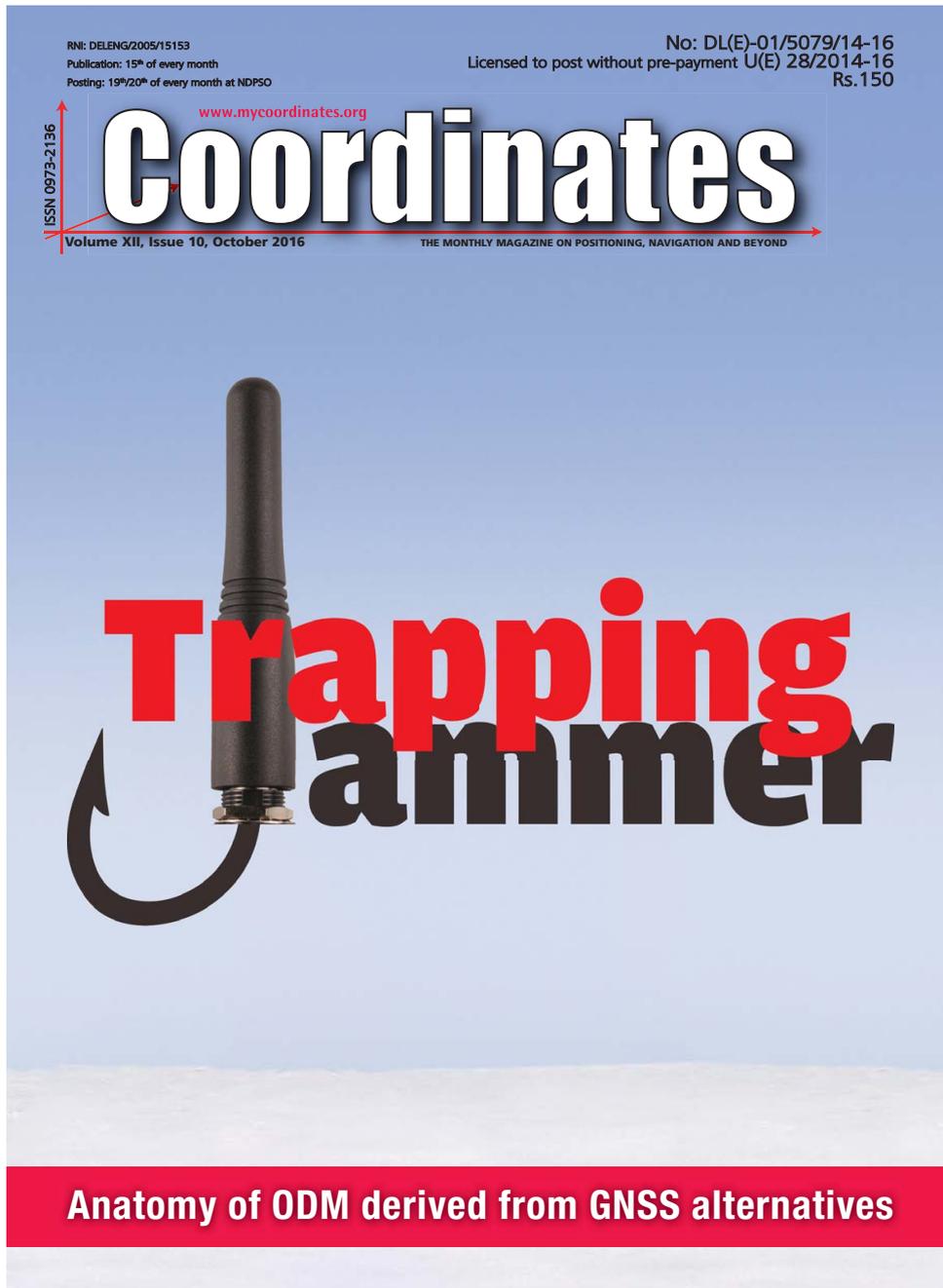
## 8. Annex 2 - Trapping the Jammer: the Slovenian Experiment

A copy of the article "Trapping the Jammer: the Slovenian Experiment" is provided in this annex. The paper has been published in the magazine "Coordinates" (<https://mycoordinates.org/>). The paper has been published in the October 2016 issue of the magazine and it can be retrieved at the following url:

<http://mycoordinates.org/pdf/oct16.pdf>

The paper deserved the journal cover which is reported in Figure 10.

**Figure 10:** Cover of the October 2016 issue of "Coordinates". The cover is devoted to the concept of trapping a GNSS jammer.



# Trapping the jammer: the Slovenian experiment

This paper provides a comprehensive account of the activities jointly conducted by the European Commission Joint Research Centre, the University of Ljubljana and Agency for Communication and Services of Republic of Slovenia to characterize and ultimately mitigate the jamming threat

**D**uring the last decade, the number of applications relying on Global Navigation Satellite System (GNSS) has experienced an exponential growth. Nowadays, GNSS positioning is fundamental in different fields including avionics, Location Based Services (LBSs), road and maritime transportation. Moreover, GNSS technologies are key-enabler for several regulated and

safety-critical applications, such as the Digital Tachograph (DT), the Automatic Identification System (AIS) and time distribution infrastructures. Hence, GNSS should provide reliable and continuous services. These services, however, can be easily disrupted by several interference sources including intentional attacks such as spoofing and jamming. Jamming, in particular, is the voluntary emission of

powerful electromagnetic waves towards a victim GNSS receiver which will be prevented to operate [1]. Jamming can be perpetrated using low-cost portable devices called jammers. The proliferation of such devices is expected to grow along with the development of GNSS-based services. Possible solutions to address GNSS jamming include jamming detection [2] and jammer localization [3]. This paper presents the joint efforts of the European Commission Joint Research Centre (JRC), of the University of Ljubljana and of the Agency for Communication and Services of Republic of Slovenia (AKOS) towards the development of reliable and affordable techniques for jamming detection and localization. The activities performed have a strong experimental component and two extensive data collections were carried out with the ultimate goal to design effective jamming countermeasures. The principle is similar to that adopted to fine drivers not respecting speed limits: a speed trap is used to identify and fine the law transgressor. In a similar way, “jammer traps” should be developed to allow authorities to reliably identify the presence of jammers on-board vehicles and fine the jammer user. It is noted that the usage of GNSS jammers is considered illegal in most countries and the availability of reliable localization techniques will simplify the operations of authorities trying to stop this phenomenon.



**Gianmarco Baldini**  
European Commission, Joint Research Centre (JRC), Directorate for Space, Security and Migration, Italy



**Franc Dimc**  
University of Ljubljana, Faculty of Maritime Studies and Transport, Ljubljana, Slovenia



**Matej Bažec**  
University of Ljubljana, Faculty of Maritime Studies and Transport, Portoroz, Slovenia



**Niko Gaberc**  
Agency for Communication and Services of Republic of Slovenia (AKOS), Slovenia



**Ales Blatnik**  
Agency for Communication and Services of Republic of Slovenia (AKOS), Slovenia



**Ciro Gioia**  
European Commission, Joint Research Centre (JRC), Directorate for Space, Security and Migration, Italy



**Daniele Borio**  
European Commission, Joint Research Centre (JRC), Directorate for Space, Security and Migration, Italy



**Andrej Stern**  
University of Ljubljana, Faculty of Electrical Engineering, Portoroz, Slovenia

The first data collection was organized in July 2015 and it was followed by a second campaign that took place in November 2015. The second campaign benefited from the experience gained during the experiments conducted in July and several additional tests were

designed and performed to evaluate possible jammer localization approaches.

Different experiments were conducted and, in particular, the following approaches were considered:

1. *Spectrum monitoring and sentinel receivers*: a portable Rhode & Schwarz PR100 spectrum analyser was used to fingerprint the signal broadcast by jammers. A sentinel GPS receiver was also used to assess the impact of jamming on GPS devices.
2. *Software Defined Radio (SDR)-based detection*: several detection approaches were implemented using the samples provided by a low-cost TV tuner used as agile front-end operating in the GNSS bands.
3. *Receiver-based detection*: detection techniques based on the measurements provided by a GNSS receiver have been considered. This included the use of  $C/N_0$  measurements provided by victim GPS receivers.
4. *Jammer localization using  $C/N_0$  measurements*: two approaches for jammer localization were attempted using a single moving GPS receiver and a grid of static smartphones.

These four types of tests were performed in parallel considering two scenarios: in the first case, a static jammer was used while the detection unit was mounted on a moving vehicle. In the second scenario, the role of jammers and detection units was inverted: the jammer was installed on a moving vehicle while the detection unit was static on the road side. The two scenarios are complementary and provide insights on the effects caused by a jammer.

For jammer localization, a third scenario was also considered where a grid of Android phones was used to simultaneously collect  $C/N_0$  measurements. This last type of tests was implemented only during the second data collection.

The two measurement campaigns took place in the proximity of the village of Črnotiče in Slovenia and provided valuable data for the evaluation of the jamming threat.

The experimental results show that low-power car jammers can be effectively detected in a road environment using commercial devices such as portable spectrum analysers

This paper provides an account of the experimental and analysis activities originated from the experiments conducted in Črnotiče. More details on specific aspects of the experiments conducted can be found in the references provided at the end of the paper.

### The Slovenian campaigns

The first scenario considered during the two Slovenian campaigns is described in Figure 1. In this case, jammers were kept static whereas the detection unit was mounted on a car as schematically represented in Figure 1 b). The vehicle with the detection units moved, with an almost constant velocity, back and forth between the two way-points (A and B) shown in Figure 1 a). The tests were repeated considering different jammers (three jammers were used) and

different speeds (50 and 90 km/h). The measurement units employed included a Realtek RTL2832U front-end, used to collect In-phase/Quadrature (I/Q) samples and implement experiments of type 2, a u-blox LEA-6T, GPS single frequency receiver, used to collect GNSS measurements and implements techniques of type 3 and 4. The Ljubljana Interference Monitor (LIM), a composite detection unit based on a Raspberry Pi platform, a GPS receiver and a RTL2832U front-end was also adopted for testing real-time SDR approaches.

As mentioned above, a second scenario was also performed where the detection unit was static and the jammer was mounted on a vehicle. In this case, a portable Rhode & Schwarz PR100 spectrum analyser was used to fingerprint the jamming signal.

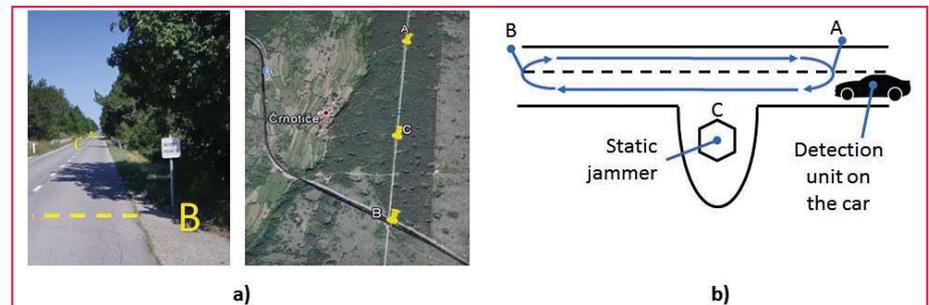


Figure 1: Jammer test performed in a remote area close to Črnotiče. a) View of the road environment selected. b) Schematic representation of the tests carried out considering a static jammer and detection units mounted on a car.

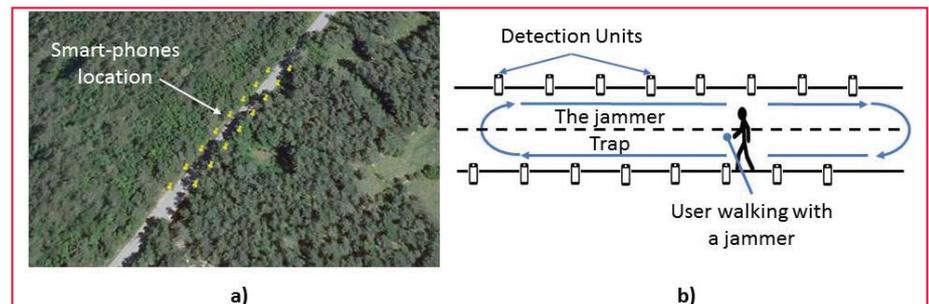


Figure 2: Smartphone-based test: a) test environment and location of the smartphones. b) schematic representation of the tests carried out considering a user walking through the smartphones with a jammer. The tests also considered the vehicular case.

The tests performed in the two scenarios provided similar results. The usage of a static jammer however allows one to establish a reference position for the jammer, and thus it allows the performance analysis of jammer localization techniques. For this reason, more emphasis is provided here to the results obtained for the first scenario.

The third scenario developed for the techniques of type 4 is illustrated in Figure 2. In this case, sixteen Android smartphones were placed over a regular grid along a straight section of the road. The location of the phones is shown in Figure 2 along with a schematic representation of the tests performed. A vehicle equipped with a jammer passed several times between the phones at different speeds. Also in this case, the test was repeated considering three different jammers and different speeds. The experiment was also repeated considering a pedestrian user slowly moving through the phones. During the experiments, the phones continuously

collected  $C/N_0$  measurements which were used for jammer localization.

### Trapping the jammer

This section provides a summary of the results obtained for the different techniques tested and for the different scenarios considered.

### Spectrum monitoring and sentinel receivers

The usage of portable spectrum analysers, such as the Rhode & Schwarz PR100 device, allows one to obtain a clear fingerprint of the signal broadcast by a jammer. This approach not only allows one to detect the jammer presence but it also provides specific signatures which, in principle, can be used to identify the specific jammer type. During the experiments conducted, it was possible to clearly distinguish the three jammers adopted: each device has its Radio Frequency (RF) signature with a characteristic spectral shape.

Sample results obtained during the Slovenian campaign are shown in Figure 3 which provides the RF signature of one of the three jammers considered. The jamming signal spans a 32 MHz frequency interval which is significantly larger than the bandwidth of GPS and Galileo open signals.

The data were collected with the equipment positioned on the road side with the jammer placed on a car passing closely to the observation station. The minimum distance between jammer and spectrum analyser was about 5 m. The colour variations in the spectrogram in Figure 3 b) reflect the received power variations due to the approaching and distancing of the jammer.

### SDR-based detection

The availability of the I/Q samples provided by a SDR front-end enables sophisticated detection techniques with performance similar to that achieved using a commercial spectrum analyser. In particular, I/Q samples can be used to compute metrics such as the histogram and the Power Spectral Density (PSD) of the input samples. The histogram and the PSD provide a signature of the jamming signal, and thus enable jammer identification.

The time-varying histogram and PSD obtained considering the same jammer discussed in the previous section are provided in Figure 4. When the jammer is in the close proximity of the RTL device, the jamming signal saturates the front-end and the input samples assume significant values. This fact is reflected by the multi-coloured bands present in Figure 4 a). A similar effect can be observed in PSD: when the jammer is closed to detection unit significant power is present in all the frequencies captured by the SDR front-end.

From the histogram and the PSD, it is possible to derive summary statistics which can be used for jamming detection. Metrics derived from the histogram are the signal mean, variance and kurtosis whereas metrics derived from the PSD are the total power and the spectral entropy.

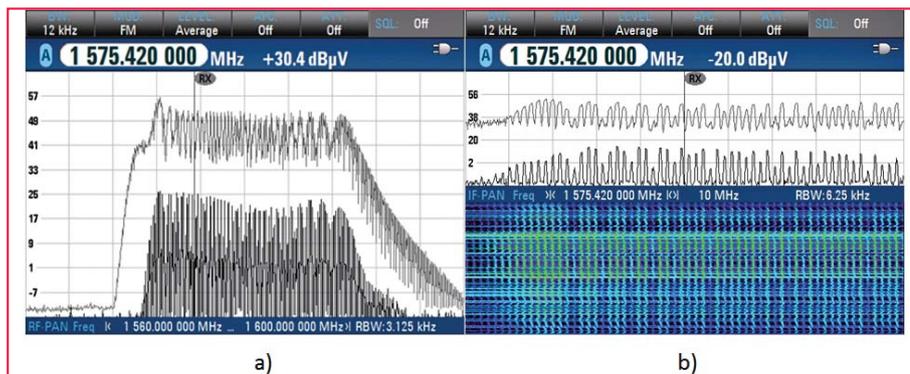


Figure 3: RF fingerprint of a wideband jammer: a) RF spectrum measured in 40 MHz bandwidth b) Spectrogram evaluated in a 10 MHz bandwidth.

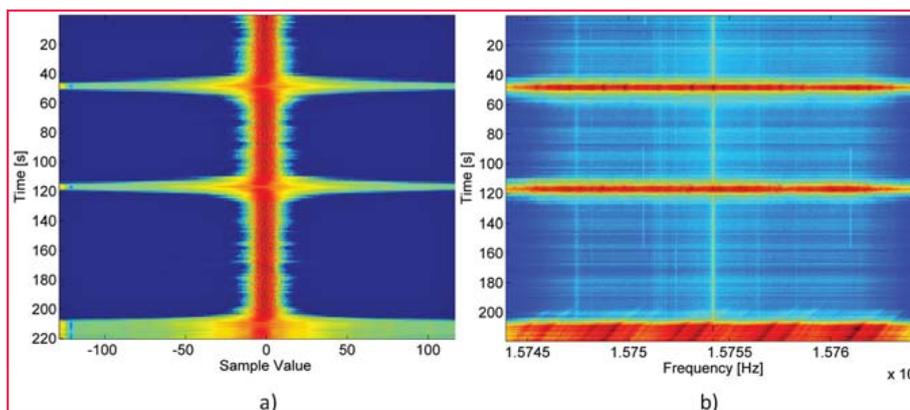


Figure 4: Time-varying histogram (a) and PSD (b) of the signal collected in the presence of a jammer. The same jammer considered in Figure 3 is analysed.

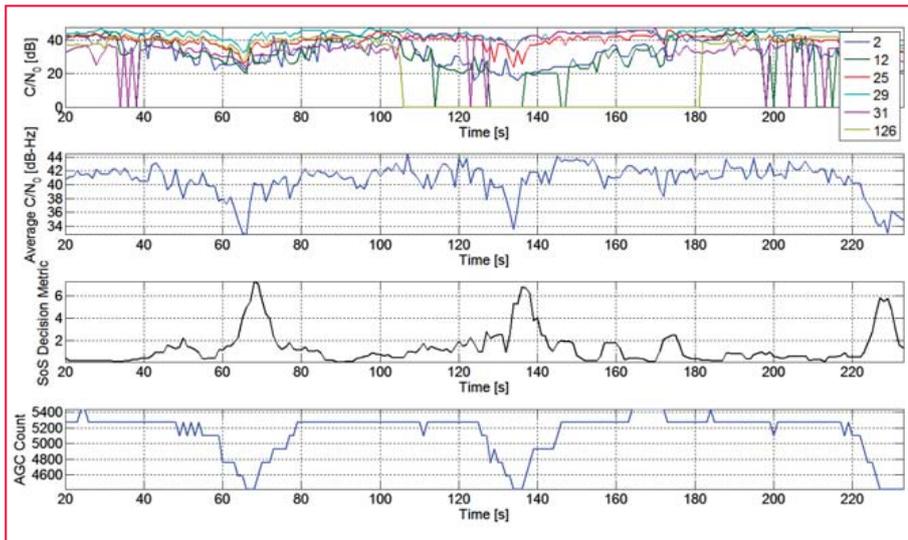


Figure 5: Sample results obtained using the measurements provided a GPS receiver in the presence of jamming. Notches and peaks are observed in the correspondence of the jammer passages.

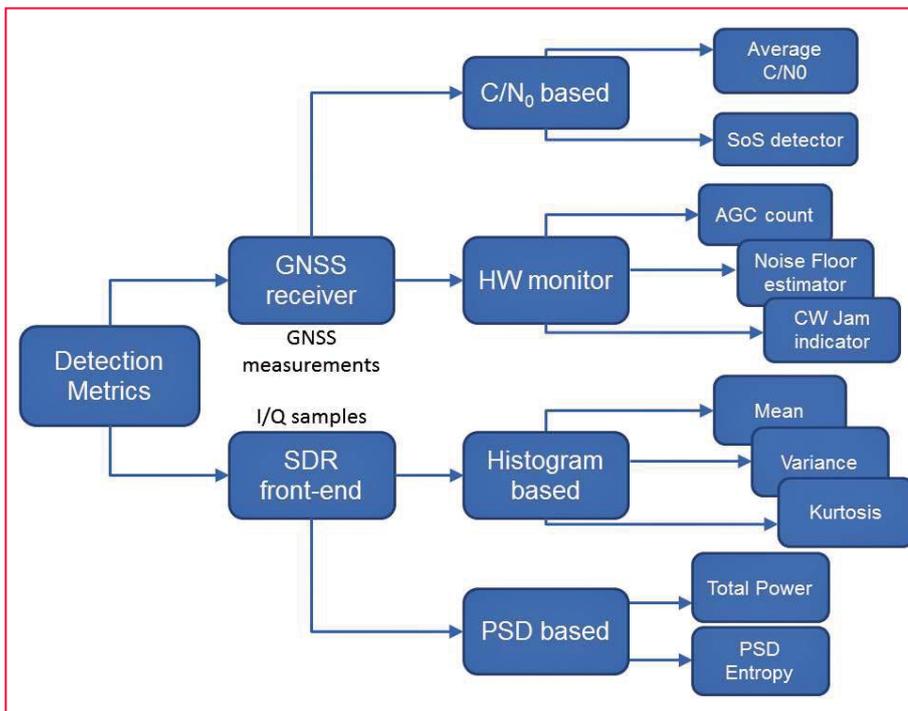


Figure 6: Detection metrics considered in this work

### Receiver-based detection

GNSS receivers provide several measurements which are significantly affected by a jamming signal.  $C/N_0$  measurements, for example, reflect the presence of interference: a significant drop in all  $C/N_0$  values is experienced in the presence of jamming.  $C/N_0$  values are “naturally” provided by most GNSS receivers and are, for example, directly accessible in smartphones. Thus, jamming detection can be implemented exploiting  $C/N_0$  measurements.

In addition to  $C/N_0$  values, several receivers provide the Automatic Gain Control (AGC) count, a noise floor estimator and dedicated interference indicators. All these measurements have been used for jamming detection.

Sample results obtained using receiver-based metrics are provided in Figure 5: the average  $C/N_0$  reflects the reduction in performance caused by the proximity of the jammer. The Sum-of-Squares (SoS) approach suggested by [5] has also been considered: the SoS detection

metric clearly reflects the jammer presence. Finally, Figure 5 shows the AGC count as a function of time: when the car with the jammer passes closely to victim receiver, the AGC count drops significantly, revealing the presence of an interference source.

A summary of all the detection metrics considered in this work, with both SDR- and receiver-based techniques is shown in Figure 6. All these techniques have been analysed and compared using the data collected during the Slovenian campaigns. A detailed analysis of these detection approaches can be found in [4].

Note that more complex approaches can be developed by combining the information provided by both SDR platforms and GPS receivers. An example is the LIM platform developed by the University of Ljubljana which integrates different sensors using the Raspberry Pi micro-computer. More details on LIM can be found in [6].

### Localization technique

Finally, jammer localization techniques have been implemented using  $C/N_0$  measurements. Two approaches, namely synthetic and crowdsourcing localization, have been considered. The two approaches are both based on the usage of  $C/N_0$  values: in the first case, measurements are taken by the same device at different locations and at different time instants. In the second case, a grid of Android phones is used to simultaneously collect the  $C/N_0$  measurements.

As indicated above,  $C/N_0$  estimates are affected by the presence of interference and the  $C/N_0$  provided by a receiver can be expressed as [7]:

$$\frac{C_i}{N_0}_{eff} = \frac{C_i}{N_0 + k_\alpha J} = \frac{C_i}{N_0} \frac{1}{1 + k_\alpha \frac{J}{N_0}} \quad (1)$$

where  $C_i$  is the power received for the  $i$ th satellite,  $N_0$  is noise power spectral density and  $J$  is the received jamming power.  $k_\alpha$  is the Spectral Separation Coefficient (SSC) [7] and models the filtering effect of the receiver on the jamming signal. From Eq. (1), it emerges the  $C/N_0$  is a function

of the received jamming power which can be related to the jammer/receiver distance using a simple path-loss model:

$$J_{dBW} = J_{0,dBW} - 10\alpha \log_{10}\left(\frac{d}{d_0}\right) \quad (2)$$

where  $J_{0,dBW}$  is the jammer reference power measured at distance  $d_0$ .  $\alpha$  is the path loss exponent and can be assumed equal to 2 for rural open environments.  $d$  is the distance between the jammer and the victim GNSS receiver. Eq. (2) is expressed in logarithmic units. By expressing (1) in logarithmic scale and combining it with (2) it is possible to obtain a simple model valid when the jammer is in the proximity of the victim receiver. In particular,

$$\left. \frac{C_i}{N_0} \right|_{eff,dB-Hz} = \beta_i + 10 \log_{10} d \quad (3)$$

where  $\beta_i$  is an unknown parameter which absorbs several factors such as the un-interfered  $C/N_0$ , the SSC and the transmitted jamming power.  $\beta_i$  can be obtained through calibration. Synthetic localization is based on (4) where  $C/N_0$  measurements are combined in a cost function whose minimum corresponds to the location of the jammer. In particular, it is possible to consider  $C/N_0$  measurements taken at different time instants and in different positions as equivalent to simultaneous observations from different receivers. In order to obtain more robust measurements, the average  $C/N_0$  can be used and (4) can be rewritten as:

$$\begin{aligned} \left. \frac{C_a[n]}{N_0} \right|_{eff,dB-Hz} &= \beta + 10 \log_{10} d[n] \\ &= \beta + 5 \log_{10} [(x[n] - x_{jam})^2 + (y[n] - y_{jam})^2] \end{aligned} \quad (4)$$

where notation ' $[n]$ ' is used to indicate quantities measured at the instant  $n$ . In particular,  $(x[n], y[n])$  and  $d[n]$  are the receiver position and the receiver distance from the jammer at the instant  $n$ .  $\beta$  is the average of the  $\beta_i$  terms which refer to a single satellite. Using (4), it is possible to construct the cost function:

$$J(x_{jam}, y_{jam}) = \sum_{n=0}^{N-1} \left[ \left. \frac{C_a[n]}{N_0} \right|_{eff,dB-Hz} - \beta - 5 \log_{10} [(x[n] - x_{jam})^2 + (y[n] - y_{jam})^2] \right] \quad (5)$$

where  $N$  is the number of instants during which a jamming event is detected. The jammer position is computed minimizing (5).

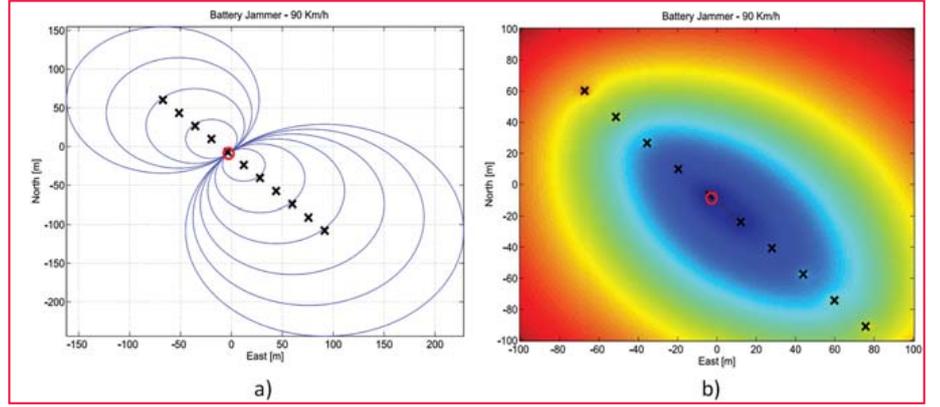


Figure 7: Jammer localization using a moving detection unit. a) Geometric interpretation of the cost function and of the estimated jammer position. b) Cost function evaluated using  $C/N_0$  measurements collected at the points indicated by black crosses.

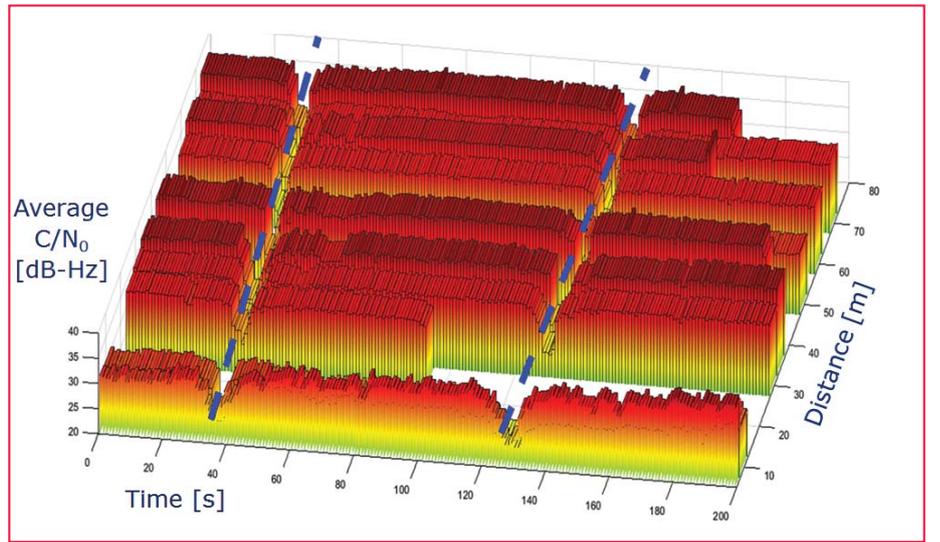


Figure 8: Average  $C/N_0$  as a function of the receiver position (distance from the first device) and time.

Sample results obtained using the approach described above are shown in Figure 7. A geometric interpretation of the cost function and of the estimated jammer position is provided in Figure 7 a): the jammer is localized at the intersection of different circles. Each circle is centred at the location of the vehicle hosting the detection unit and its radius is defined by the average  $C/N_0$  observed.

In Figure 7 b), the cost function is plotted with respect to the estimated jammer location expressed in a local frame centred in the true jammer position. Thus, the coordinates estimated for the jammer correspond to the actual localization error which, in this case, is less than 10 meters. This level of accuracy was consistently observed among the different tests performed.

For the crowdsourcing approach, it was not possible to use the same principle described for synthetic localization. In particular, each phone involved in the experiment was characterized by a different  $\beta$ . Since the calibration of all phones was not feasible, a different approach was adopted.  $C/N_0$  measurements are first used to detect the jamming presence: jammer localization is then achieved by combining detection results from different smartphones. For localization, it was assumed that GNSS receivers are sufficiently far from the jamming source to obtain a valid position solution and sufficiently close to be affected by the jamming signal and observe a reduction in  $C/N_0$ . Jamming detection was implemented using the SoS approach mentioned above and the jammer position was finally obtained as

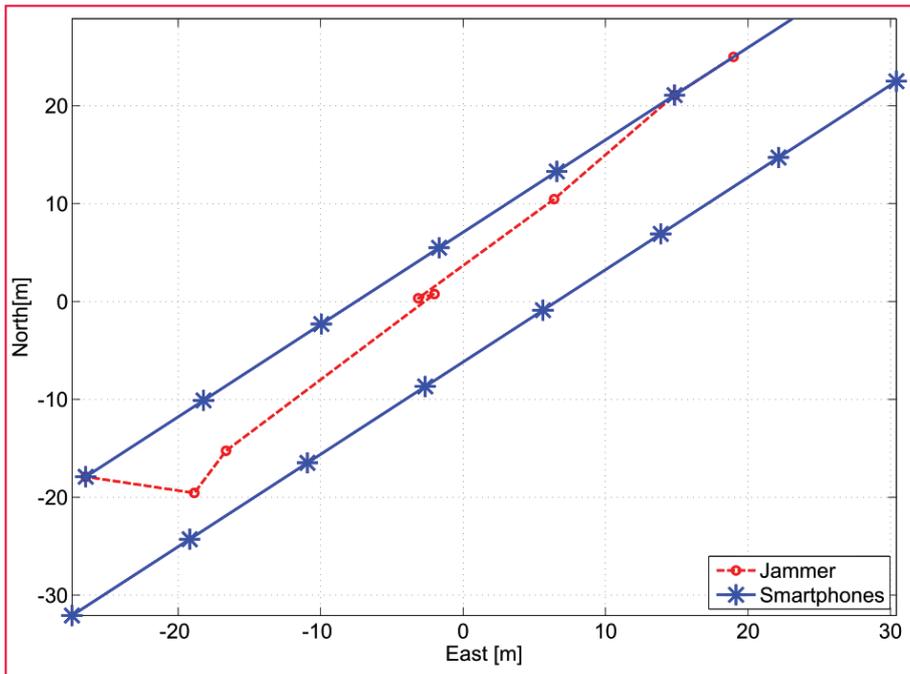


Figure 9: Estimated jammer position, obtained considering a single passage of the jammer. The positions of the jammer and of the smartphones are plotted in a local EN frame centred in the mean of the smartphone coordinates.

$$\begin{aligned} x_{jam} &= \frac{1}{\#\mathcal{D}} \sum_{k \in \mathcal{D}} x_k \\ y_{jam} &= \frac{1}{\#\mathcal{D}} \sum_{k \in \mathcal{D}} y_k \end{aligned} \quad (6)$$

where  $\mathcal{D}$  is the set of receivers detecting a jammer.  $\#\mathcal{D}$  is the number of receivers detecting the jammer and  $(x_k, y_k)$  is the position of the  $k$ th receiver. The jammer location is thus identified as the centroid of the positions of the receivers which detect the jammer. If  $\mathcal{D}$  is empty, the jammer is not detected and localization is not performed. Sample results obtained using the crowdsourcing approach are presented in Figure 8. Specifically, the average  $C/N_0$  is provided as a function of the phone location and time. The average  $C/N_0$  describes a “spatial wave” which clearly shows the passages of the jammer. Although few devices malfunctioned, the direction of motion and velocity of the jammer can be easily identified.

The estimated jammer positions together with the smartphones locations are shown in Figure 9. The red trajectory is the jammer trajectory obtained considering a single passage of the jammer. The positions of the jammer and of the smartphones are plotted in a local East North (EN) frame centred in

the mean of the smartphone coordinates. From the figure, it emerges that the trajectory of the jammer was correctly identified even if some of the devices were not properly working during the experiment. This demonstrates the robustness of the proposed approach in the presence of malfunctions of some detection units. Additional results on the jammer localization techniques described can be found in [8].

## Conclusions

This paper provides a comprehensive account of the activities jointly conducted by the European Commission JRC, the University of Ljubljana and AKOS to characterize and ultimately mitigate the jamming threat. Two unique measurement campaigns have been conducted and several experiments have been conducted to evaluate different detection and localization approaches. The experimental results show that low-power car jammers can be effectively detected in a road environment using commercial devices such as portable spectrum analysers. Effective and affordable detectors can be obtained using SDR platforms and measurements

directly provided by commercial GPS receiver including smartphones. The results obtained are promising and encourage additional work towards the development of effective jammer traps.

## References

- [1] T. Economist, “GPS jamming: No jamming tomorrow,” *Technology Quarterly*, Mar. 2011.
- [2] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, “Impact and detection of GNSS jammers on consumer grade satellite navigation receivers,” *Proc. IEEE*, vol. 104, pp. 1233–1245, June 2016.
- [3] A. G. Dempster and E. Cetin, “Interference localization for satellite navigation systems,” *Proc. IEEE*, vol. 104, pp. 1318–1326, June 2016.
- [4] F. Dimc, D. Borio, C. Gioia, G. Baldini, M. Bazec, and M. Basso, “An experimental evaluation of low-cost GNSS jamming sensors,” *NAVIGATION, Journal of the Institute of Navigation*, pp. 1–14, Accepted for Publication, Sep. 2016.
- [5] D. Borio and C. Gioia, “Real-time jamming detection using the sum-of-squares paradigm,” in *Proc. of the International Conference on Location and GNSS (ICL-GNSS)*, pp. 1–6, June 2015.
- [6] M. Bažec, B. Luin, F. Dimc. “GPS jamming detection with SDR“, *Proc. of the 24th International Symposium on Electronics in Transport (ISEP 2016)*, ITS for efficient energy use, Electrotechnical Association of Slovenia, Ljubljana, Slovenia, Mar., pp.1-4.
- [7] J. W. Betz, “Effect of partial-band interference on receiver estimation of  $C/N_0$ : Theory,” in *Proc. of the 2001 National Technical Meeting of The Institute of Navigation*, Long Beach, CA, pp. 817–828, Jan. 2001.
- [8] D. Borio, C. Gioia, A. Štern, F. Dimc and G. Baldini “Jammer Localization: From Crowdsourcing to Synthetic Detection” *Proc. of 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, Sep. pp. 1-10 ▽

## **9. Annex 3 - GNSS Receiver Fingerprinting for Security-Enhanced Applications**

The paper *GNSS Receiver Fingerprinting for Security-Enhanced Applications* is available at: <http://www.ion.org/publications/abstract.cfm?jp=p&articleID=14688>

The paper should be cited as:

Borio, Daniele, Gioia, Ciro, Baldini, Gianmarco, Fortuny, Joaquin, "GNSS Receiver Fingerprinting for Security-Enhanced Applications," *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, Oregon, September 2016, pp. 2960-2970.

## References

Baldini, G., Steri, G., Dimc, F., Giuliani, R. and Kamnik, R., 'Experimental identification of smartphones using fingerprints of built-in micro-electro mechanical systems (mems)', *Sensors*, Vol. 16, No 6, 2016, p. 818.

Borio, D., DAVIS, F., Kuusniemi, H. and Presti, L. L., 'Impact and detection of GNSS jammers on consumer grade satellite navigation receivers', *Proc. IEEE*, Vol. 104, No 6, June 2016, pp. 1233–1245.

Dempster, A. G. and Cetin, E., 'Interference localization for satellite navigation systems', *Proc. IEEE*, Vol. 104, No 6, June 2016, pp. 1318–1326.

Fernández-Hernández, I., Rijmen, V., Seco-Granados, G., Simon, J., Rodríguez, I. and Calle, D., 'A navigation message authentication proposal for the galileo open service', *Navigation*, Vol. 63, No 1, 2016, pp. 85–102.

Gao, G. X., Sgammini, M., Lu, M. and Kubo, N., 'Protecting GNSS receivers from jamming and interference', *Proc. IEEE*, Vol. 104, No 6, June 2016, pp. 1327–1338.

Hasse, J., Gloe, T. and Beck, M., 'Forensic identification of GSM mobile phones', In 'Proc. of the first ACM workshop on Information hiding and multimedia security', ACM, pp. 131–140.

Li, C.-T., 'Source camera identification using enhanced sensor pattern noise', *IEEE Transactions on Information Forensics and Security*, Vol. 5, No 2, 2010, pp. 280–287.

## **List of abbreviations and definitions**

**ADEV** Allan Deviation

**AKOS** Agency for Communication Networks and Services of the Republic of Slovenia

**C-ITS** Cooperative Intelligent Transport Systems

**CNIT** Consorzio Nazionale Interuniversitario per le Telecomunicazioni

**COTS** Commercial Off-The-Shelf

**CS** Commercial Service

**DSRC** Dedicated Short Range Communications

**EKF** Extended Kalman Filtering

**GNSS** Global Navigation Satellite System

**GSA** European GNSS Agency

**IMU** Inertial Mounted Unit

**ITS** Intelligent Transportation System

**IV** Intelligent Vehicle

**NMA** Navigation Message Authentication

**OBU** On Board Unit

**OS** Open Service

**PF** Particle Filtering

**PRS** Public Regulated Service

**PVT** Position Velocity and Time

**RF** Radio Frequency

**SDR** Software Defined Radio

**TESLA** Timed Efficient Stream Loss-tolerant Authentication

## List of figures

<b>Figure 1.</b> Architecture where the GNSS receiver is external to the OBU. In this case, the connection used to provide GNSS data should be secured. . . . .	3
<b>Figure 2.</b> View of the experimental platform used to collect GNSS and IMU data. . .	7
<b>Figure 3.</b> The car used in the GNSS/IMU experiment. . . . .	8
<b>Figure 4.</b> Path selected for the experimental campaign involving GNSS and IMU data.	9
<b>Figure 5.</b> Trajectories estimated using the GPS only solution and the PF. Map information has been added to the data fusion process. . . . .	10
<b>Figure 6.</b> Schematic representation of the OS NMA scheme based on TESLA protocol. From the presentation of Dr. Fernandez Hernandez, Ispa, Italy, July 2016.	12
<b>Figure 7.</b> Different types of GNSS receivers used for fingerprinting. . . . .	14
<b>Figure 8.</b> Clock-derived metrics used for the selection of statistical features used for fingerprinting. . . . .	15
<b>Figure 9.</b> Sample classification results for different GNSS receivers. . . . .	15
<b>Figure 10.</b> Cover of the October 2016 issue of "Coordinates". The cover is devoted to the concept of trapping a GNSS jammer. . . . .	18

***Europe Direct is a service to help you find answers  
to your questions about the European Union.***

**Freephone number (\*):**

**00 800 6 7 8 9 10 11**

(\* ) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (<http://europa.eu>).

## **HOW TO OBTAIN EU PUBLICATIONS**

### **Free publications:**

- one copy:  
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:  
from the European Union's representations ([http://ec.europa.eu/represent\\_en.htm](http://ec.europa.eu/represent_en.htm));  
from the delegations in non-EU countries ([http://eeas.europa.eu/delegations/index\\_en.htm](http://eeas.europa.eu/delegations/index_en.htm));  
by contacting the Europe Direct service ([http://europa.eu/europedirect/index\\_en.htm](http://europa.eu/europedirect/index_en.htm)) or  
calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (\*).

(\* ) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

### **Priced publications:**

- via EU Bookshop (<http://bookshop.europa.eu>).

## JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**

[ec.europa.eu/jrc](https://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



Joint Research Centre



EU Science Hub

