2014 / 2500M-006

ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-2631-4

SUMMARY REPORT

DETERJAM
Detection, analysis, and risk management of satellite navigation jamming (Satelliittipaikannuksen häirinnän tunnistaminen, analysointi ja riskinhallinta)

Laura Ruotsalainen*, Heidi Kuusniemi, Mohammad Zahidul H. Bhuiyan, Stefan Söderholm, Martti Kirkko-Jaakkola, Sarang Thombre, Salomon Honkala
Department of Navigation and Positioning, Finnish Geospatial Research Institute FGI
***laura.ruotsalainen@nls.fi**

Abstract
Satellite navigation signals are very weak after travelling from the satellite transmitter to the user receiver antenna on the Earth and are extremely vulnerable to unintentional and intentional, malicious interference. A serious concern nowadays is the increase in the amount of jammer devices as well as the emergence of spoofing events, due to the severe threat they pose to many applications relying on satellite positioning. This project analyses the effects of intentional interference on satellite based positioning and investigates methods for interference detection and mitigation. The project also aims to develop advanced signal acquisition and tracking techniques as well as reliability enhancement algorithms suitable for situations when interfering signals are present.

1. Introduction

Reliable navigation and positioning as well as robust timing reference from Global Navigation Satellite Systems (GNSS) are becoming imperative in more and more applications for safety-critical purposes, public services and consumer products. GNSS, such as the American Global Positioning System (GPS), the Russian GLONASS, the Chinese BeiDou and the European Galileo, are particularly prone to unintended and malicious interference due to the extremely low power level of the signal at the user receiver after travelling from the satellite transmitter to the user receiver antenna on the Earth.

A serious concern nowadays that has gained a lot of attention is the increase in the amount of illegal jammer devices on the civilian field due to the brutal threat they pose to many applications fully relying on satellite positioning. Jammers may cause severe damage if their signals are not properly detected and the effects mitigated in user receivers as perceived e.g. at Newark airport in United States in 2009 (The Economist, 2011) and (Pullen & Gao, 2012). A continuously growing concern is the more sophisticated form of intentional interference, spoofing. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver to use these fake signals, which ultimately results in a misleading position solution. The severeness of the matter was perceived in 2011 when a classified U.S. drone was captured by Iran who afterwards made unsubstantiated claims to have spoofed its GPS receiver (Psiaki et al., 2014). Thereafter, Psiaki et al. have simulated various spoofing scenarios and thereby shown its drastic consequences.

This research aims to determine the risks and analyze the associated effects of especially intentional interference sources on civilian GNSS receivers and applications. Also, the goal is to increase satellite navigation robustness against interference by implementing various advanced receiver signal processing techniques and reliability assessment algorithms for interference detection and mitigation.

2. Research objectives and accomplishment plan

The DETERJAM project started in the year 2012 with the acquisition of software-defined radios in the GNSS frequency band, GNSS signal repeaters for the navigation laboratory testing facilities, and jammer devices with the related authorization from the Finnish Communications Regulatory Authority (Ficora). Thereafter, a software-defined GNSS platform, the FGI-GSRx, was developed in the Matlab programming environment to implement and compare various methods for interference analysis, detection, and mitigation in order to accomplish robust satellite navigation. The FGI-GSRx constitutes an important, flexible tool to assess and consequently publish the research progress obtained within the interference detection and mitigation research. In DETERJAM, civilian jammer effects on consumer grade receivers were first investigated. Thereafter, methods for detection of interference, both jamming and spoofing, were developed. Also, two sophisticated methods for mitigating the effects of interference were implemented, the first one using an adaptive multi-GNSS position solution formation and the other integration of GNSS with Inertial Navigation system (INS) and visual sensors. As well, methods for acquiring signals in weak signal conditions, namely indoors, in urban canyons and under jamming, were developed. Test data from live space-based signals were utilized as well as hardware-simulated data from Spirent and Spectracom signal simulators to verify the feasibility of the developed methods.

3. Materials and methods

Both real-life data and simulated data from a hardware simulator are used in the project. Though hardware simulators are useful in providing a confined testing scenario with known errors and repeatability, they rarely fully realistically depict real-life interference sources and effects. Thus, real-life data provide an important means for method validation in reality. The research platform for this project is an open source based GNSS software receiver, the FGI-GSRx, which will be described in detail below. Generic GNSS radio front-ends can be used in conjunction with the software GNSS receiver. The FGI-GSRx can process raw IF (intermediate frequency) data samples in post-mission. The FGI-GSRx is a Matlab-based software receiver in which various receiver design algorithms can be implemented and their performances evaluated with the real-life GNSS data from any suitable radio front-end. Two different radio front-ends (SiGe GN3S sampler V3 and the Stereo V2) from Sparkfun Electronics and Nottingham Scientific Limited (NSL), respectively, have been used to capture real or hardware-simulated GNSS signals throughout the project. The flexible software defined architecture also enables the implementation of inertial-augmented signal acquisition and tracking in GNSS-denied environment (for example, interference or spoofing scenario). The XSENS MTi-G-700 Inertial Navigation System (INS) was used for providing the measurements for inertial augmenting in the project. It is a consumer grade INS composed of micro-electro-mechanical (MEMS) sensors, making the system small, light and reasonable prized. Its accelerometer and gyroscope measurements were integrated by deeply-coupling procedure with GNSS measurements to aid the GNSS signal processing algorithms and thereby mitigate the effect of interference.

The navigation laboratory at the Finnish Geodetic Institute is also equipped with a single- and a dual-frequency jammer transmitting chirp signals. The usage permission of these jammers within the laboratory of the Finnish Geodetic Institute was obtained from the Finnish Communications Regulatory Authority (Ficora).

4. Results and discussion

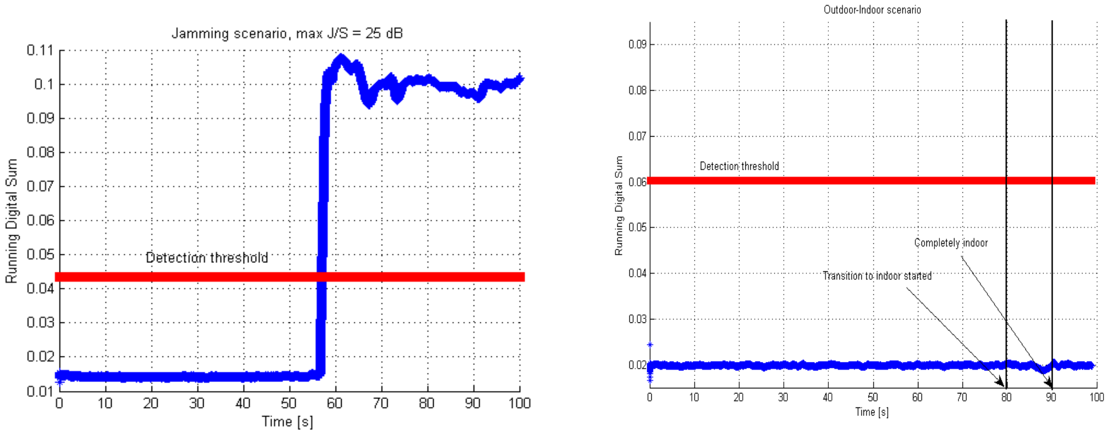
The project assesses aspects of especially intentional interference, jamming and spoofing, on civilian GNSS positioning. Both interference consequences and methods for detection and mitigation are addressed and the main results presented below.

4.1 Impact of jamming on commercial mass-market receivers

In-car, civilian jammers have a threatening effect on the performance of consumer grade GPS receivers. All the consumer-grade receivers suffer from performance degradation in the vicinity of a jammer which was shown in tests conducted during the first year of the project and presented in Kuusniemi et al (2012).

4.2 Jamming Detection

In order to guarantee the reliability of the received GNSS signal, the receiver should be able to detect interference so that some other means could be taken into action as a countermeasure in order to ensure robust and accurate navigation. The impact of interference on a number of different receiver observables was investigated in Bhuiyan et al (2013). The investigated observables include the Automatic Gain Control (AGC) measurements, the digitized IF (Intermediate Frequency) signal levels, the Delay Locked Loop and the Phase Locked Loop discriminator variances, and the Carrier-to-noise density ratio (C/N_0) measurements. The investigations showed that the substantial drop of the (C/N_0) measurements in a jamming situation appears to be an effective indicator for the presence of a jamming device. However, the same phenomenon is observed when the GNSS receiver is transferred from outdoors to indoors, and therefore the C/N_0 measurements were not alone sufficient for interference detection. A new Running Digital Sum (RDS) -based interference detection method was proposed in this project (Bhuiyan et al. 2014) to overcome the above mentioned shortcoming. Figure 1 demonstrates the fact that the proposed Running Digital Sum –based Interference Detection (RDS-ID) method can uniquely identify an intentional interference occurrence as it is unaffected due to weak GNSS signal condition indoors.



(a) a jamming scenario

(b) an outdoor-indoor scenario

Figure 1 RDS of the digitized IF samples can uniquely identify a malicious interference occurrence

4.3 Spoofing Detection

Spoofing is completely a different phenomenon than jamming. The goal of spoofing is to provide the receiver with a misleading signal, fooling the receiver to use fake signals for positioning calculations, which ultimately result in a misleading position, velocity and time solution. While the GPS P(Y)-code (precise) is heavily encrypted and thus, is hard to spoof, the civilian GNSS signal, for example, the GPS L1 C/A signal, is easy to spoof because the signal structure, the spread spectrum codes, and the modulation types are open to the public. A number of potential spoofing detection indicators are investigated in Kuusniemi et al (2013a), the results illustrating that the tracking signal quality indicators are capable of revealing the spoofer attack. However, the simple navigation domain consistency checking does not efficiently reveal the spoofing incident as may be deduced from Figure 2 representing position error obtained using a static GNSS receiver and a simulated spoofer. Spoofing signal deludes the receiver to observe motion as the position slowly changes despite the receiver in reality is static.

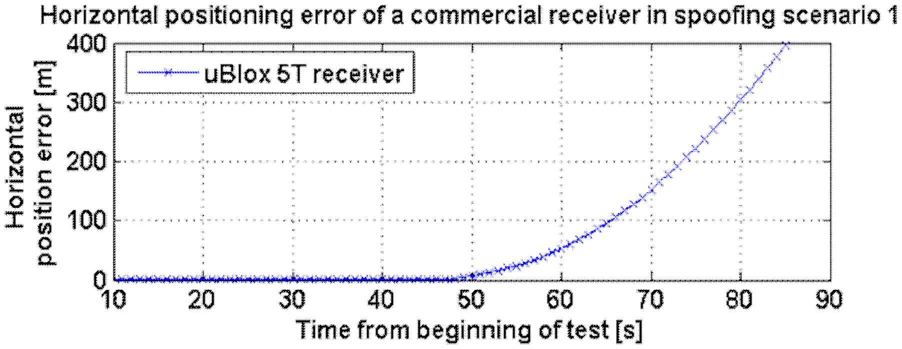


Figure 2 Spoofing is not detected from the position solution, the receiver observes motion when in reality it is static

4.4 Multi-GNSS receiver development

A software defined GNSS receiver platform, the FGI-GSRx, has been under continuous development for the analysis and validation of novel algorithms for an optimized GNSS navigation performance. The FGI-GSRx bases on an open-source software radio platform (Borre et al, 2007) developed for processing GPS signals. In the beginning of the DETERJAM project FGI-GSRx was first modified to be Galileo-compatible. On the second year of the project, 2013, the FGI-GSRx was modified to be also BeiDou compatible and then on successfully achieving a multi-GNSS position fix using the European Galileo, the Chinese BeiDou and the US GPS navigation systems (Kuusniemi et al (2013b)). Finnish Geodetic Institute was recognized by the European Space Agency (ESA) in 2014 for being within the first 50 entities in the world to claim Galileo position fix with its own software-defined receiver FGI-GSRx. During the third project year FGI-GSRx was developed to form a multi-GNSS solution incorporating signals also from the Russian GLONASS system and the Indian IRNSS. In addition, the receiver was elaborated to have a dual-frequency capability, namely being able to process both BeiDou B1 and B2 signals. The dual-frequency capability may further be easily expanded for other signals also, e.g. Galileo E5 and E6.

Figures 3 shows the results of a multi-GNSS position solution. At present, the 50% Circular Probable Error (CEP) for the GPS-only position fix is 2.94, BeiDou-only 3.14, Galileo 4.5 and multi-GNSS 1.43 meters (Söderholm et al., 2014).

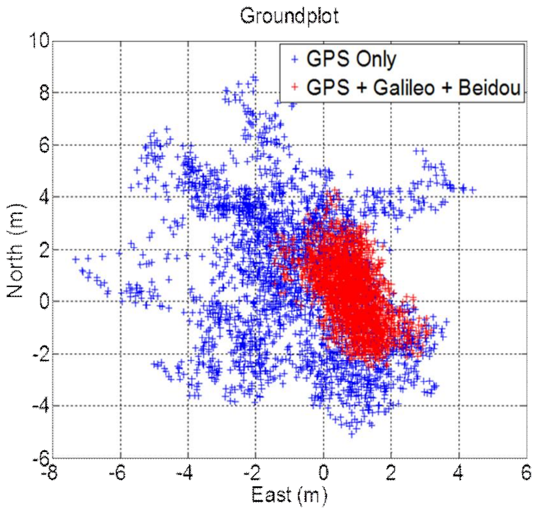


Figure 3 Position errors obtained using a GPS-only and a multi-GNSS position solution

4.5 Interference mitigation

Interference mitigation research in DETERJAM has concentrated on two approaches feasible for the task; utilizing two or more GNSS interoperable for forming a multi-GNSS position solution and deeply-coupled integration of GNSS and inertial sensors, lately also complemented with visual sensors to mitigate the inertial sensor errors as discussed below.

4.5.1 Multi-GNSS

The impact of a cheap commercial GPS jamming device on the BeiDou signal was assessed to evaluate the benefits of using modern GNSS systems (Ruotsalainen et al. 2014a). The effects were monitored by examining the C/N$_0$ values and the obtained position solution. The results were compared to the corresponding results obtained using GPS. The impact of the jammer was significant on GPS, as was known from previous research, but surprisingly it deteriorated the BeiDou performance slightly too. However, the impact was not as drastic as on GPS, the increase of the position errors was in the range of meters, as for GPS there was an increase of hundreds of meters, as is shown in Figure 4.

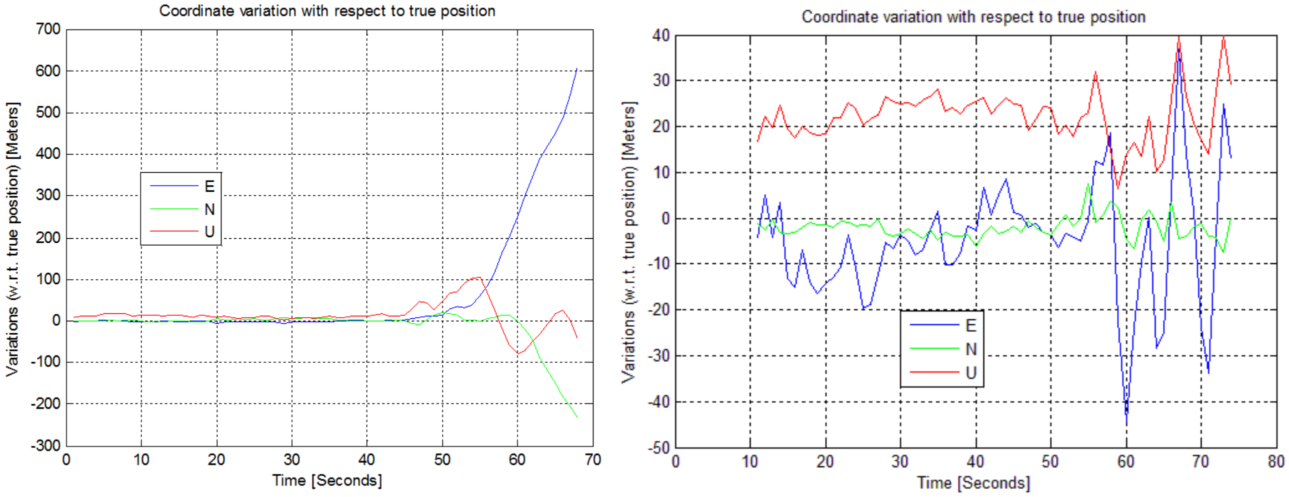


Figure 4 Position errors obtained using GPS (on left) and BeiDou (on right) under jamming

A multi-GNSS solution using both GPS and BeiDou interoperable was computed. The position accuracy was worse with respect to GPS only, but much better compared to BeiDou only solution, when no jamming was encountered. However, when the jamming device was turned on, the accuracy was improved with respect to GPS solution, both on the horizontal and vertical components as may be seen from Figure 5. BeiDou only position solution was still better than the multi-GNSS solution on both position components when jamming device was used.

The degraded performance of the multi-GNSS solution compared to GPS only, when no jamming was present, was a result from the use of all satellites available, and therefore the signals with poor quality deteriorated the solution. Thereafter, the receiver autonomous integrity monitoring (RAIM) algorithms were implemented into the software defined receiver, FGI-GSRx. Using RAIM the best combination of satellites, regarding the quality of signals and geometry could be selected for use and therefore a much better position accuracy obtained. Initial results obtained using RAIM algorithms in a GPS/GLONASS jamming scenario show that in addition to the improvement of the position solution, the availability of the solution also increases from 75% of the test duration up to 91% in this certain scenario.

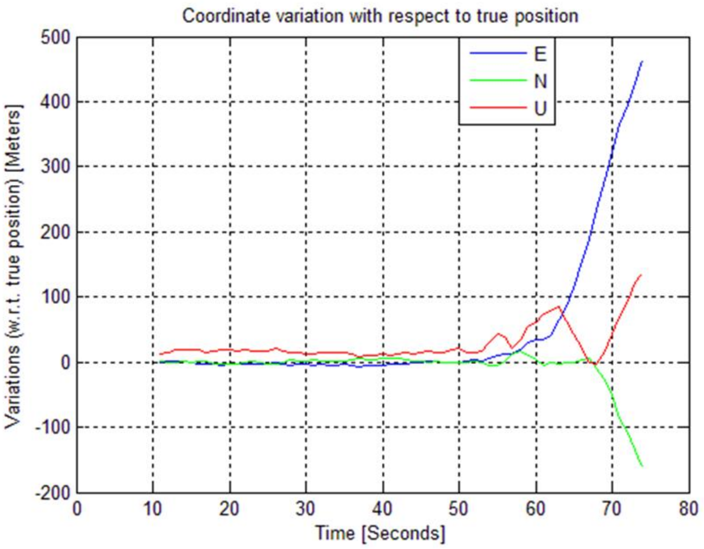


Figure 5 Position errors obtained using a multi-GNSS solution under jamming

4.5.2 Deeply-coupled GNSS/INS integration

Deeply-coupled, also referred to as ultra-tight, integration of GNSS and Inertial Navigation System (INS) uses information obtained from the inertial sensors, namely angular rotation from gyroscopes and acceleration from accelerometers, to aid the GNSS signal processing algorithms. The measurements obtained using INS are not affected by jamming and therefore the integration results in a system with enhanced robustness to interference.

A deeply-coupled Kalman filter integrating GNSS and INS was developed in the DETERJAM project (Ruotsalainen et al. 2013, Kirkko-Jaakkola et al. 2014). Its performance was assessed using real GPS signals and a consumer grade MEMS IMU XSens MTi-G-700. After 46 seconds from the start of the experiment the signals were interfered using the low-cost single frequency jamming device discussed above. The results are shown in Figure 6. On left, the C/N_0 values for GPS-only tracking are shown. The C/N$_0$ values decrease immediately to under 20 dB-Hz when the jamming is started jeopardizing the navigation solution computation. The figure on right shows the C/N$_0$ values for the same GNSS data when the tracking is performed using the deeply-coupled Kalman filter integrating GNSS and INS. Although the values start decreasing when the jamming device is turned on, the decrease is slower compared to the situation when the GPS-only tracking is used and the C/N$_0$ values stay above 30 dB-Hz for almost twenty seconds. The method was found to be an efficient method for jamming mitigation based on the behaviour of the C/N$_0$ values in the presence of jamming signals.

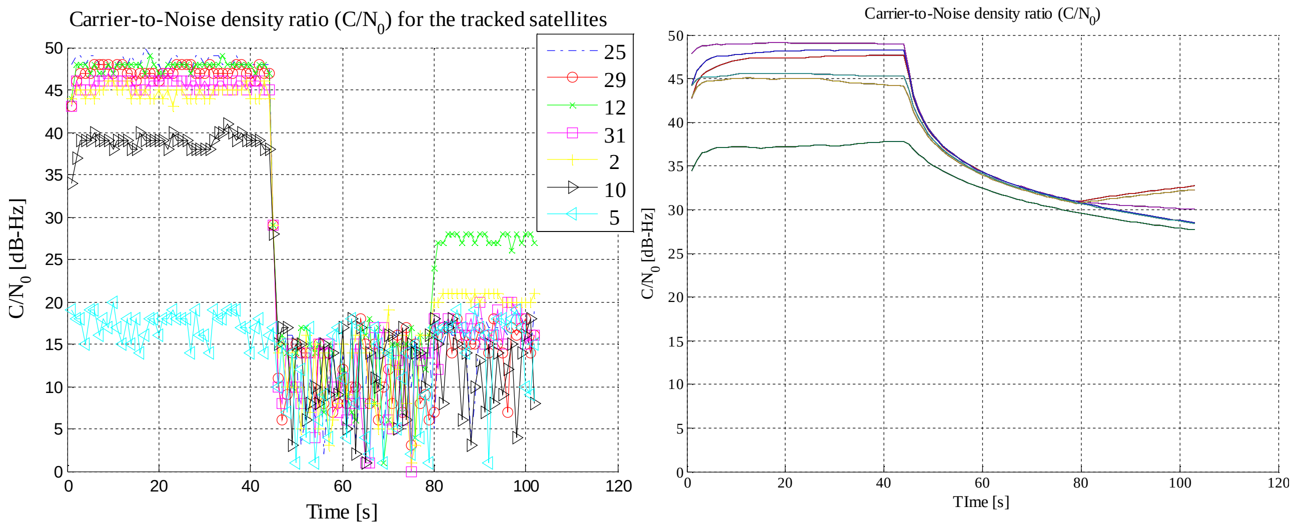


Figure 6. C/N0 values in a jamming scenario using only GPS measurements (on left) and using deeply-coupled GNSS/INS integration (on right)

4.5.3 Deeply-coupled GNSS/INS/Visual sensor integration

However, despite the encouraging results seen above, the performance of INS suffers from measurement biases that accumulate to large position errors with time. Typically deep-coupling corrects the above mentioned INS errors using the GNSS signals, but if the jamming continues for a longer time forestalling the use of proper GNSS signals, degradation of the position solution will incur after some period. Visual sensors, i.e. cameras, are feasible instruments for constricting the growth of the INS errors and are resistant to GNSS jamming. In favorable environments and special camera configuration, camera attitude and translation between consecutive images may be detected. Virtual features, called vanishing points, arising from parallel straight line in the scene, may be detected from images. The motion of vanishing points in consecutive images provides means for observing the attitude change, the developed method is called a visual gyroscope, Figure 7 shows an image used in the method. With a particular configuration of the camera and the positioning platform the translation of the system between the consecutive images may also be resolved (Ruotsalainen 2013); the concept is called a visual odometer. These measurements may further be used for mitigating the errors in INS observations, which may be seen from the observed velocity error of the receiver, shown in Figure 8. Integration of the visual measurements decreases the maximum velocity error observed using the deeply-coupled integration from 8 m/s to 2 m/s. Deeply-coupled integration of the visual measurements, INS and GNSS will further improve the robustness of the positioning accuracy in situations where the jamming is not only momentary (Ruotsalainen et al. 2014b). By providing valuable information about the receiver dynamics, the method would be feasible for spoofing mitigation also.

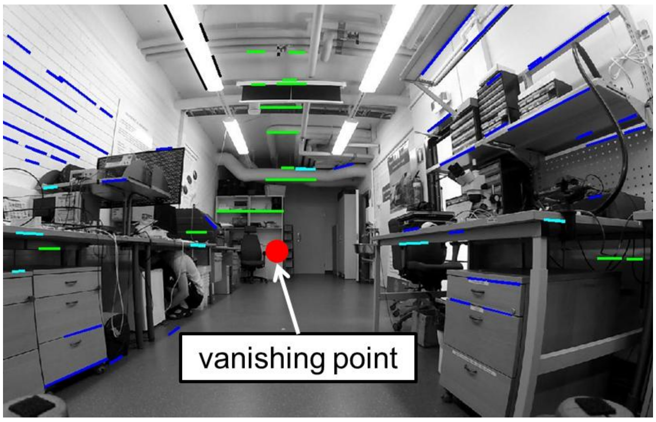


Figure 7. Formation of the visual gyroscope

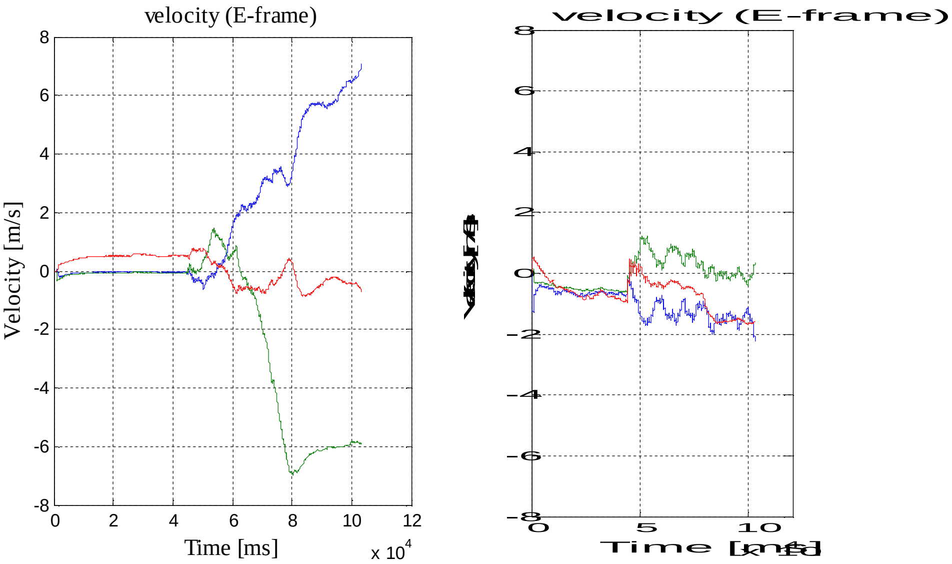


Figure 8. Velocity error of the receiver in GNSS/INS (on left) and GNSS/INS/visual sensor (on right) deeply-coupled integration

4.6. Jammer localization

A literature survey on jammer localization research was done during the project. Traditionally the jammer localization methods are based on utilizing multiple receivers at monitoring stations and resolve the location of the jammer by using triangulation based on AGC voltage (Lindström et al. 2007), or receivers in ad-hoc networks and signal angle-of-arrival (AOA) or time-difference-of-arrival (TDOA) measurements (Fontanella et al. 2013), both claiming the accuracy of the observed jammer location to be few tens of meters, probably being enough to find the jamming source. Recently also more advanced antenna configurations are being used allowing the jammer localization using only one receiver (Navtechgps).

5. Conclusions

In-car, civilian jammers have a threatening effect on the performance of consumer grade GNSS receivers, as demonstrated in DETERJAM. The higher the jamming power, the more degradation it causes. The developed RDS-ID method can successfully be utilized for jamming detection. Also spoofers have devastating effects on the GNSS receiver performance if not properly detected and mitigated. Spoofer detectors capable for identifying a spoofing situation were proposed and implemented in the project. Integration of GNSS and inertial sensors has proven to be an efficient method for jamming mitigation and therefore a deeply-coupled GNSS/INS integration method, augmented with visual sensors to restrict the errors in INS measurements, was proposed and implemented in the project. Modern satellite navigation systems have novel features making them less vulnerable for interference, especially when using signals merged from several systems. Therefore the research in DETERJAM focused on developing the FGI-GSRx software GNSS receiver to offer a multi-GNSS position fix with GPS, Galileo, GLONASS and BeiDou constellations. A consistent Receiver Autonomous Integrity Monitoring (RAIM) technique based on the receiver tracking observables was implemented for interference detection and for isolating defective GNSS measurements. The DETERJAM project was in operation during the years 2012-2014.

6. Scientific publishing and other reports produced by the research project

Bhuiyan, M.Z.H., Söderholm, S., Thombre, S., Ruotsalainen L. and H. Kuusniemi (2014). Overcoming the Challenges of BeiDou Receiver Implementation, Sensors, MPDI.

Bhuiyan, M.Z.H., Kuusniemi, H., Söderholm, S. and Airos, E. (2014). The Impact of Interference on GNSS Receiver Parameters - A Running Digital Sum Based Simple Jammer Detector, Radioengineering, 23(3).

Bhuiyan, M.Z.H., Söderholm, S., Thombre, S., Ruotsalainen, L., and Kuusniemi, H. (2014). First Studies of BeiDou in Finland, Poster presentation, ICL-GNSS 2014, Helsinki, Finland, June 2014.

Bhuiyan M.H.Z., Kuusniemi H., Söderholm, S., Thombre, S., Ruotsalainen L. (2014).Tracking the BeiDou Satellites with a Software-defined Receiver, Geospatial World - the Geospatial Industry Magazine, 21 April, Magazine.

Bhuiyan M.H.Z., Söderholm, S., Thombre, S., Ruotsalainen L. and H. Kuusniemi (2014). Implementation of a Software-defined BeiDou Receiver, Lecture Notes in Electrical Engineering (ISSN: 1876-1100).

Bhuiyan M.Z.H., Söderholm, S., Thombre, S., Ruotsalainen L., Kirkko-Jaakkola M. and H. Kuusniemi (2014) Performance Evaluation of Carrier-to-Noise Density Ratio Estimation Techniques for BeiDou B1, in Proceedings of UPINLBS 2014.

Kirkko-Jaakkola M.,Ruotsalainen L., Bhuiyan, M.H.Z., Söderholm, S., Thombre S., Kuusniemi, H. (2014). Performance of a MEMS IMU Deeply Coupled with a GNSS Receiver under Jamming, in Proceedings of UPINLBS 2014

Kuusniemi, H., Airos, E., Bhuiyan, M.Z.H., Kröger, T. (2012a). Effects of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. European Navigation Conference (ENC) 2012, Gdansk, Poland, 25-27 April, 2012, 13 p.

Kuusniemi, H., Airos, E., Bhuiyan, M.Z.H., Kröger, T. (2012b) “GNSS jammers: how vulnerable are consumer grade satellite navigation receivers?,” European Journal of Navigation 08/2012; 10(2):14-21.

Kuusniemi, H. and Bhuiyan, M.Z.H. (2012c). “Signal Barred“, Geospatial World, The Geospatial Industry Magazine, November 2012: 31-33.

Kuusniemi, H, Bhuiyan, M.Z.H. and Kröger, T. (2013a) “Signal Quality Indicators and Reliability Testing for Spoof-Resistant GNSS Receivers,” European Journal of Navigation 08/2013; 11(2):12-19.

Kuusniemi, H, Bhuiyan, M.Z.H., Liu, J., Ruotsalainen, L. and Honkala, S. (2013b) “Tracking the First Satellites of the European Galileo and the Chinese BeiDou Systems,” Finnish National

Committee on Space Research Conference 2013, Metla, Vantaa, August 29-30, 2013

Ruotsalainen L., Bhuiyan M.Z.H., Thombre S., Söderholm S., Kuusniemi H. (2014a). Impact of cheap commercial jammer on BeiDou signals, In proceedings of ENC, 14-16 April, Rotterdam.

Ruotsalainen L., Kirkko-Jaakkola, M., Bhuiyan, M. Z. H., Söderholm, S., and Thombre, S., and H. Kuusniemi (2014b). Deeply-coupled GNSS, INS and visual sensor integration for interference mitigation, Proceedings of ION GNSS.

Ruotsalainen, L., M.Z.H. Bhuiyan, H. Kuusniemi, S. Söderholm (2013). Preliminary Investigation of Deeply-Coupled Galileo and Self-Contained Sensor Integration for Interference Mitigation. ESA/GSA 4th International Colloquium: Scientific and Fundamental Aspects of the Galileo Programme, 4-6 December 2013, Prague, Czech Republic.

Söderholm, S., Bhuiyan, M. Z. H., Thombre, S., Ruotsalainen L. and H. Kuusniemi (2014). An L1 CDMA multi-GNSS software receiver, GPS Solutions, Springer, in press

S. Thombre, M. Z. H. Bhuiyan, S. Söderholm, M. Kirkko-Jaakkola, L. Ruotsalainen, H. Kuusniemi (2014). 'Tracking IRNSS Satellites for Multi-GNSS Positioning in Finland', InsideGNSS, Nov/Dec.

7. References

Borre, K., D.M. Akos, N. Bertelsen, P. Rinder, S.H. Jensen (2007). A Software Defined GPS and Galileo Receiver - A Single-Frequency Approach. Birkhäuser, 198 p., 2007.

Fontanella D., Bauernfeind R., Eissfeller B. (2013), Inside GNSS May/June, 70-80.

Inside GNSS (2012), UAVs Vulnerable to Civil GPS Spoofing, July/August 2012, http://www.insidegnss.com/node/3131, accessed 23 November 2012

Jonas Lindström, Dennis M. Akos, Oscar Isoz and Marcus (2007), GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules, ION GNSS.

Navtechgps, http://www.navtechgps.com/assets/1/7/CTL3520_DS.pdf

Nottingham Scientific Limited (2012) http://www.nsl.eu.com/primo.html#, accessed 12 August, 2012.

Psiaki, M.L., O' Hanlon, B.W., Powell, S.P., Bhatti, J.A., Humphreys, T.E., Schofield A. (2014), "GNSS Lies, GNSS Truth, Spoofing Detection with Two-Antenna Differential Carrier Phase", GPS World, vol 25. no 11.

Pullen, S., G. Gao, "GNSS Jamming in the Name of Privacy, Potential Threat to GPS Aviation", Inside GNSS, March/April 2012, 34-43.

Ruotsalainen L., (2013). Vision-Aided Pedestrian Navigation for Challenging GNSS Environments. Doctoral Dissertation, Suomen geodeettisen laitoksen julkaisuja - Publications of the Finnish Geodetic Institute; 151.

Serant D., Kubrak D., Monnerat M., Artaud G. and L. Ries, (2012), Field test performance assessment of GNSS/INS ultra-tight coupling scheme targeted to mass-market applications, Navitec 2012, 5-7 December, Noordwijk, The Netherlands.

Sparkfun Electronics (2012) SiGe GN3S sampler v3. http://www.sparkfun.com/products/10981, accessed 08 June 2012.

The Economist, "GPS jamming: No jam tomorrow", 2011, http://www.economist.com/node/18304246