ISSN 1797-3457 (verkkojulkaisu)
ISBN (PDF) 978-951-25-2525-6

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, Salomon Honkala
Department of Navigation and Positioning
Finnish Geodetic Institute
*laura.ruotsalainen@fgi.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 due to the severe threat they pose to many applications relying on satellite positioning, especially to applications for safety-critical purposes, but also for public services and consumer products. Jammers may cause serious damage if their signals are not properly detected and the effects mitigated. 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/COMPASS and in future 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. The extent of the damage caused by jamming was perceived at Newark airport in United States in 2009, as discussed in e.g. (The Economist, 2011) and (Pullen & Gao, 2012). The satellite-positioning receivers for navigation aiding in airplane landings were suffering from brief daily breaks. After investigation it was found out that the outages were caused by a driver who passed by on the nearby highway each day. He had a cheap GPS (Global Positioning System) jammer in his truck for preventing his employer to track the location and speed of his vehicle. Probably unknowingly he also disrupted GPS signals for others nearby and ended up causing substantial danger to the whole airport.

Deliberate deception in form of spoofing signals on the other hand totally cripples satellite navigation, but more sophisticatedly and, therefore, more expensively. In 2012, Todd Humphreys' research team at the University of Texas at Austin demonstrated the first successful civil GPS spoofing of an unmanned aerial vehicle (Inside GNSS, 2012), indicating the potentially hazardous risks associated with spoofing when critical infrastructure is concerned.

Interference, whether it is unintentional or deliberate, will incur loss of accuracy resulting into noisy position, velocity and time (PVT) solution, severely erroneous position information with significant “jumps” in the PVT solution, total loss of signal resulting to no PVT solution, or appearance of hazardous misleading information.

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 develop and compare various methods for interference analysis, detection, and mitigation in order to accomplish robust satellite navigation. The FGI-GSRx bases on an open-source software radio platform (Borre et al, 2007) that was modified to be Galileo-compatible and include interfaces to various commercial radio front-ends. On the second year of the project, 2013, the FGI-GSRx was modified to be also BeiDou/COMPASS compatible. 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 followed by detection scenarios of jammer presence. Thereafter, methods for detection of interference, both jamming and spoofing, were developed. Finally a method integrating GNSS with Inertial Navigation system (INS) for mitigating the effect of jamming was developed. Test data from live space-based signals were utilized as well as hardware-simulated data from a Spirent signal simulator.

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. 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, demonstrated in Figure 1. The usage permission of these jammers within the laboratory of the Finnish Geodetic Institute was obtained from the Finnish Communications Regulatory Authority (Ficora).

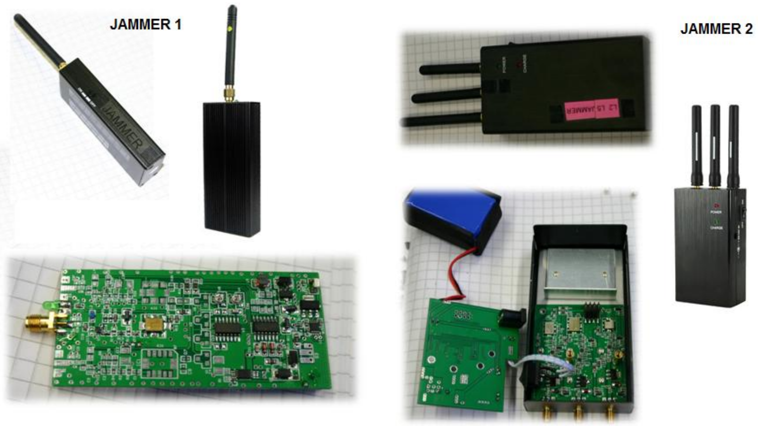


Figure 1 Jammers analysed in the DETERJAM-project

Civilian in-car jammers typically transmit chirp signals, as also the ones shown in Figure 1. A chirp signal (also termed as sweep signal) is a signal in which the frequency increases ('up-chirp') or decreases ('down-chirp') with time. The output power of online-available jammers varies, but is typically over 10 dBm. High-power jammers may not only hinder the usage of GNSS in the vicinity of the jammer but paralyze GNSS usage over a large coverage area.

4. Results and discussion

The project assesses aspects of especially intentional interference on civilian GNSS positioning. Both interference consequences and methods for detection and mitigation are addressed.

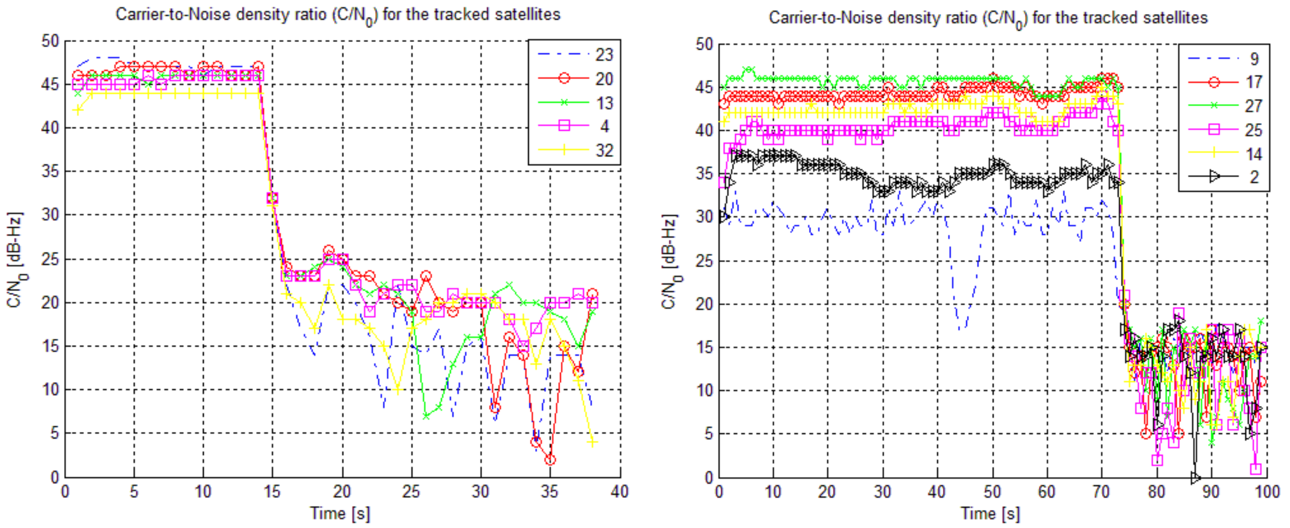
4.1 Impact of jamming on commercial mass-market receivers

In-car, civilian jammers have a threatening effect on the performance of consumer grade GPS receivers as reported in Kuusniemi et al (2012). All the consumer-grade receivers suffer from performance degradation in the vicinity of a jammer. The higher the jamming power, the more degradation it causes. The tests conducted during the first year of the project and presented in Kuusniemi et al (2012) with two different J/S ratios (i.e., max 15 dB and 25 dB, respectively) illustrated the fact that accuracy and signal availability was considerably compromised when jamming was present.

4.2 Interference Detection

In order to guarantee the reliability of the received GNSS signal, the receiver should either be able to function in the presence of Radio Frequency Interference (RFI) without generating misleading information (i.e., offering a navigation solution within an accuracy limit), or the receiver must detect RFI so that some other means could be taken into action as a countermeasure in order to ensure robust and accurate navigation. One major objective of this project is to investigate the effect of interference on different GNSS receiver observables. 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 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, as is shown on Figure 2. However, the same phenomenon is observed when the GNSS receiver is transferred from outdoors to indoors, also shown in the figure. A method called Running Digital Sum (RDS) is proposed to overcome this challenge.

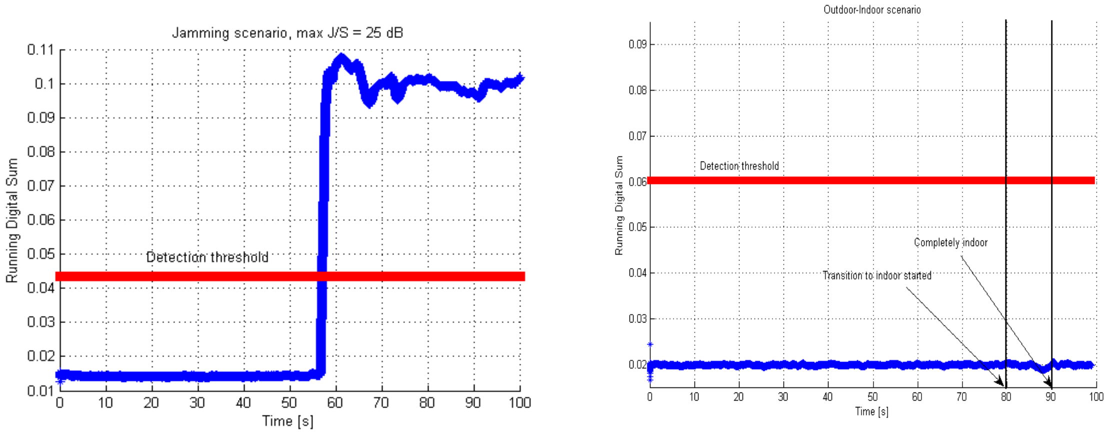


(a) a jamming scenario

(b) an outdoor-indoor scenario

Figure 2 C/N_0 values cannot separate a malicious interference occurrence of transition from outdoors to indoors

A new Running Digital Sum (RDS) -based interference detection method is proposed in this project that can be used as an alternate to AGC-based interference detection. Its advantages compared to the AGC-based detection are that it is available at the signal processing level as AGC is a hardware component and it uses data that is readily available in the GNSS processes. It was also shown in Bhuiyan et al (2013) that it is not at all wise to consider certain receiver observables for interference detection (i.e., C/N_0); rather it is beneficial to utilize certain specific observables, such as the RDS of raw digitized signal levels or the AGC-based observables that can uniquely identify a critical malicious interference occurrence. Figure 3 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 3 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 objective of jamming is to simply interrupt the availability of the signal at the receiver. The effect of jamming is to cause the received signal to be corrupted so that no valid GNSS signal can be decoded by the receiver. On the other hand, 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 (2013) for civilian GPS L1 C/A receivers. The spoofing indicators, namely Carrier-to-noise-density ratio (C/N_0), running DLL variance, running PLL variance, and running multi-correlator RMSE indicators were implemented at the tracking stage along with a navigation consistency check in the navigation stage in a software-defined receiver platform utilizing an off-the-shelf single-frequency GNSS radio front-end. Two hardware signal-simulation spoofing scenarios were presented and the results of the potential spoof-detection indicators were shown. The results illustrate that the tracking signal quality indicators are capable of revealing the spoofer attack whereas the simple navigation domain consistency checking did not efficiently reveal the spoofing incident. Figure 4 shows the results for the running multi-correlator RMSE indicator based spoofing detection. Also commercial receivers were heavily affected in terms of degraded accuracy of the spoofing. Future work will include implementation of spoofing mitigation technique based on multi-correlator tracking structure in the presence of any malicious spoofing attack. In addition, a consistent Receiver Autonomous Integrity Monitoring (RAIM) technique will be implemented based on the receiver tracking observables.

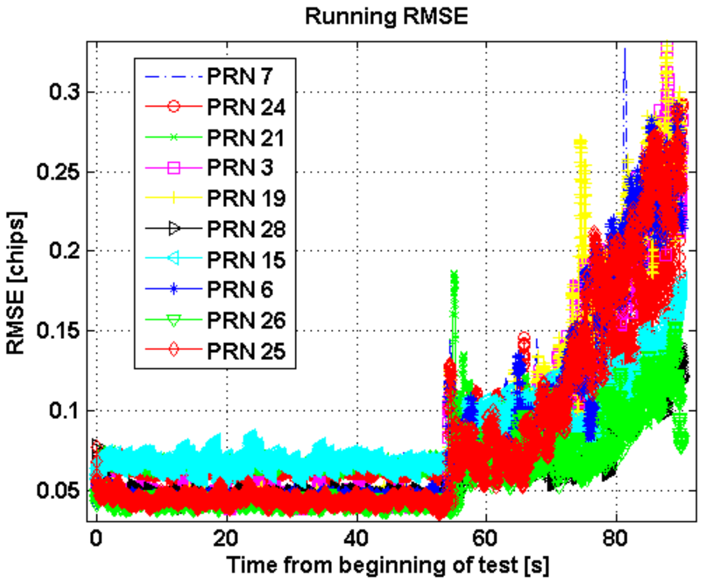
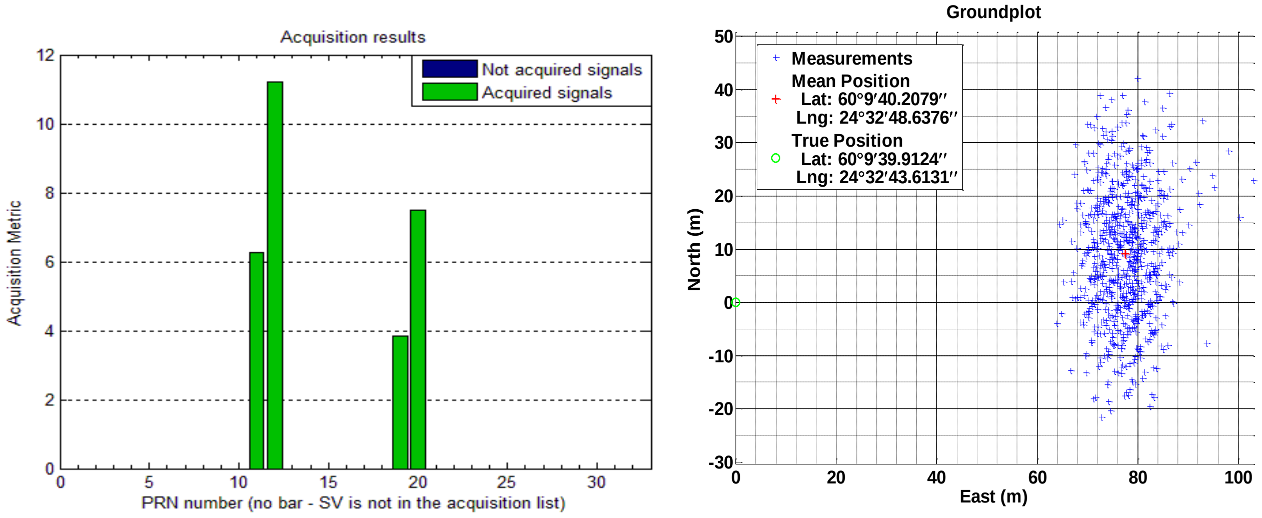


Figure 4 Spoofing detection via a running RMSE check of the received signal

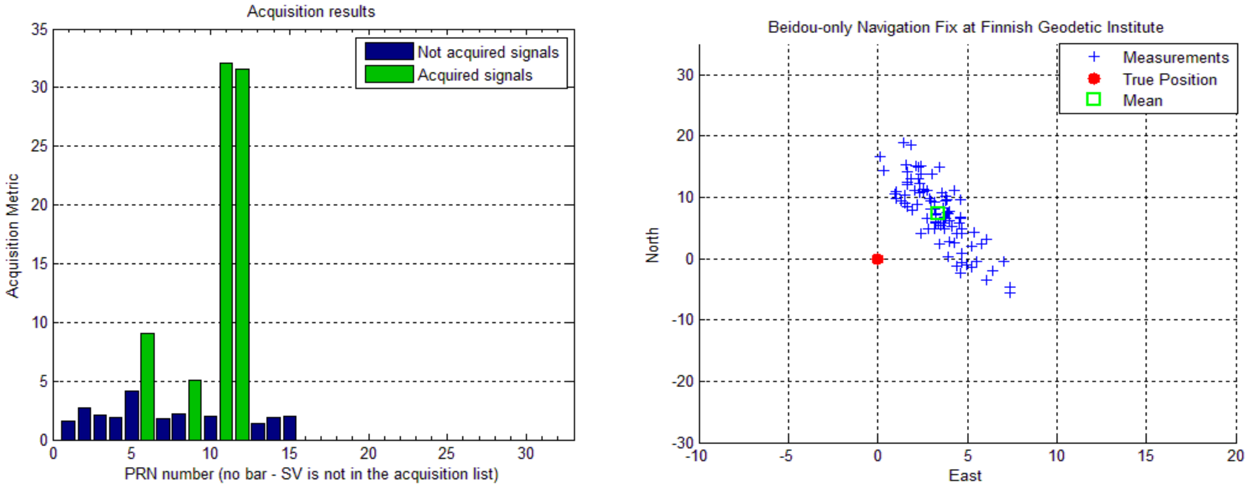
4.4 Multi-GNSS receiver development

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. During the recent months, the FGI-GSRx successfully achieves a position fix with two new global navigation satellite systems, namely the European Galileo and the Chinese BeiDou navigation systems (Kuusniemi et al (2013)). Finnish Geodetic Institute is the first within Finland to claim Galileo-only and BeiDou-only position fix with its own software-defined receiver FGI-GSRx. A dual-frequency front-end from Nottingham Scientific Limited (NSL) was used to collect GNSS signals (Nottingham Scientific Limited (2012)). A significant effort has now been dedicated to offer a multi-GNSS position fix with GPS, Galileo and BeiDou constellations. In addition, the FGI-GSRx is being developed to receive signals from the Russian GLONASS navigation system. This will eventually make the FGI-GSRx a true multi-GNSS software receiver platform, capable of offering a position fix with all four global navigation systems. Figures 5 and 6 show the results of successful acquisition and position solution with Galileo and BeiDou satellite navigation systems, respectively. There is an inexplicable bias of more than 70 meters in the Galileo-only position fix; the reason for the bias is under examination. At present, the 2D mean error for the BeiDou-only position fix is 9.3 meters.



(a) (b)

Figure 5 (a) Acquisition of 4 IOV Galileo satellites (b) Galileo-only position fix with 4 IOV satellites



(a) (b)

Figure 6 (a) Acquisition of BeiDou satellites (b) BeiDou-only position fix with a 2D mean error of 9.3 meters

4.5 Interference mitigation

Integrating GNSS with Inertial Navigation System (INS) provides enhanced robustness against interference and jamming. Inertial sensors provide a solution for position, velocity and attitude autonomously. Their measurements are obtained with high rate and bandwidth and they are not affected by interference disturbing GNSS. Therefore, the use of a combination of inertial sensors and GNSS is beneficial mainly due to their different error characteristics. An advanced integration method called deeply-coupling (Serant et al. (2012)) uses information obtained from self-contained sensors to aid the signal processing algorithms and therefore enhances the robustness of GNSS to interference.

A deeply-coupled Kalman filter integrating GNSS and INS was developed in the DETERJAM project (Ruotsalainen et al. (2013)). 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 7. On left, the C/N_0 values for GPS-only tracking are shown. The C/N_0 values decrease immediately to around 29 t o30 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. The method was found to be an efficient method for jamming mitigation based on the behaviour of the C/N0 values in the presence of jamming signals.

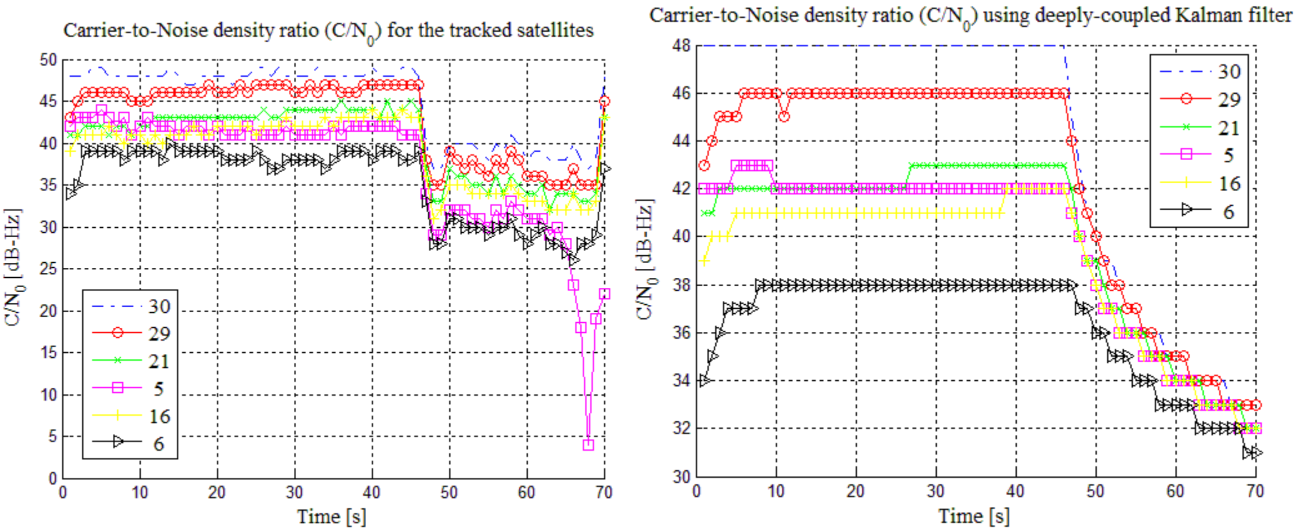


Figure 7. C/N0 values before and during jamming of the GPS L1-signals, on left using GPS-measurements only and on right using deeply-coupled INS/GPS integration

The drawback of the method was found to be the incapability of the method to completely recover from the jamming situation, i.e. the C/N_0 values did not get back to the correct value after the jamming was interrupted. Future research will consist of tuning parameters for the Kalman filter for an improved performance and finding methods for recovering from the jamming situation. Also, means for spoofing mitigation will be addressed.

5. Conclusions

In-car, civilian jammers have a threatening effect on the performance of consumer grade GNSS receivers, as demonstrated in DETERJAM so far. 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, namely multi-correlator based running RMSE, running DLL variance and running PLL variance 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 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 future research in DETERJAM will focus on developing the FGI-GSRx software GNSS receiver to offer a multi-GNSS position fix with GPS, Galileo and BeiDou constellations. In addition, the FGI-GSRx will be developed to receive signals from the Russian GLONASS navigation system. Also, the future research will focus on implementing a spoofing mitigation technique based on multi-correlator tracking structure in the presence of any malicious spoofing attack. A consistent Receiver Autonomous Integrity Monitoring (RAIM) technique based on the receiver tracking observables will be implemented for interference detection and for isolating defective GNSS measurements. The research for jamming mitigation by deeply-coupled INS/GNSS method will continue by tuning parameters for the Kalman filter for an improved performance and by proposing methods for recovering from the jamming situation. The DETERJAM project is planned for the years 2012-2014.

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

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.

Bhuiyan, M.Z.H., Kuusniemi, H., Soderhölm, S. and Airos, E. (2013). “The Impact of Interference on GNSS Receiver Parameters - A Running Digital Sum Based Simple Jammer Detector”, submitted to Radioengineering, ISSN 1805-9600 (Online), November 2013, 9 p.

Kuusniemi, H, Bhuiyan, M.Z.H. and Kröger, T. (2013) “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. (2013) “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., 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, in press

7. References

Bhuiyan M. Z. H., H. Kuusniemi, S. Soderhölm, E. Airos (2013). “The Impact of Interference on GNSS Receiver Parameters - A Running Digital Sum Based Simple Jammer Detector”, submitted to Radioengineering, ISSN 1805-9600 (Online), November 2013, 9 p.

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

11(2):12-19.

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.

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

Kuusniemi H, Airos E, Bhuiyan MZH, 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 M. Z. H. Bhuiyan (2012c). "Signal Barred", Geospatial World, The Geospatial Industry Magazine, November 2012: 31-33.

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

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

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

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