

ANALYSIS, DETECTION AND MITIGATION OF INCAR GNSS JAMMER INTERFERENCE IN INTELLIGENT TRANSPORT SYSTEMS

R. Bauernfeind, T. Kraus, A. Sicramaz Ayaz, D. Dötterböck and B. Eissfeller
Institute of Space Technology and Space Applications, University FAF Munich, Germany

Abstract

Satellite navigation signals have interference protection to some degree due to their spread spectrum code structure. However, since signals transmitted from satellites reach the receiver antenna with a very low signal power, buried in noise, they are vulnerable to interference. Interference sources like in-car jammers block the navigation signal reception in their vicinity and degrade positioning performance, proportional to the distance, over a wide area. As novel and innovative transport systems rely on a precise and reliable position determination, the threat of interference should not be underestimated. The work presented in this paper analyses the interference caused by malicious use of in-car jammers and proposes techniques to mitigate the jammer. After detection of the jammer signal within the GNSS receiver, the jammer can be mitigated in a first step at the receiver by excision of the jamming signal from the IF sample stream and further initiating the mitigation of the interference at the source by means of reporting of the interference event to authorities.

1. INTRODUCTION

An Intelligent Transport System (ITS) is defined by vehicles and transport infrastructure applying information and communication technology to improve transportation efficiency, sustainability and safety. The primary information, enabling ITS, is the location information of vehicles provided by Global Navigation Satellite System (GNSS) measurements. Awareness of the vehicle locations at all time in an absolute frame is mandatory for advanced application like

- eCall, a pan-European location based emergency call, which in case of an accident will automatically communicate the vehicle position based on GNSS to the next public safety answering point,
- for the European Electronic Toll Service (EETS) where it is recommended to use GNSS for distance based road user charging like the German Toll Collect system,
- cooperative ITS (C-ITS) which will enable vehicles to establish a vehicular ad-hoc network (VANET) and communicate based on their current position, determined by GNSS.

Even if short GNSS positioning outages can be bridged through dead reckoning algorithms based on odometer and gyroscope measurements or driver assistance systems use additional sensors like automotive radars for relative measurements. GNSS interference can cause serious interruption to the vehicle positioning system.

The most harmful interference sources are so called in-car jammers, used intentionally to prevent GNSS receivers from position determination. GNSS jammers are openly advertised online as personal protection devices (PPD). They are relatively easy to purchase from abroad over the Internet and to operate by plugging into the cigar lighter of a vehicle. The usage may be motivated by criminal intentions such as disabling a vehicle theft protection system, a fraud attempt against a distance-based road user charging system or distance-based vehicle insurance, or by privacy concerns, to escape monitoring

by a fleet-management or other tracking system. Since nowadays most GNSS receivers carry a communication link, it is hard to keep full control of the data flow.

Due to their high transmission power, these jammers are not only affecting the targeted receiver, but also GNSS receivers in far distance. To guarantee the robustness and safety of ITS applications it is necessary that their GNSS receivers have interference detection capabilities and are able to mitigate their effect. In order that authorities can take action on detected events it is necessary that detected interference events are also communicated to authorities.



FIG 1. Privacy GNSS Jammer

The paper is structured as follows. First the transmitted signals of the jammers, depicted in FIG 1, are analyzed followed by an analysis of the effect on the GNSS receiver. The second part describes how the jamming signal is detected and characterized within the GNSS receiver. After detection, techniques are presented to mitigate the jammer signal at the source by reporting the event and mitigation of the signal within the GNSS receiver. The last part presents an evaluation of the algorithms, implemented and tested with the ipex Software Receiver.

2. JAMMER SIGNAL ANALYSIS

Seven jammers were purchased and analyzed in the frequency domain with a spectrum analyzer (Will'tek 9102B) as well as in the time-domain by recording the

signal with a software defined radio card (GE ICS-572B). The jammers as depicted in FIG 1 from left to right are referred to as jammer no. 1 to jammer no. 7. Based on the signal characteristics as described in the following, the jammers were grouped in four classes [1], namely

- **Class I:** Continuous wave (CW) jammer
Jammer No. 1 and 4
- **Class II:** Chirp jammer with one saw-tooth function
Jammer No. 2, 3 and 7
- **Class III:** Chirp jammer with multi saw-tooth functions
Jammer No. 5
- **Class IV:** Chirp jammer with frequency bursts
Jammer No. 6

Most of the in-car jammers belong to the class II. These jammers have a uni-directional chirp signals, which means that they have just one positive saw-tooth function for describing the instantaneous frequency.

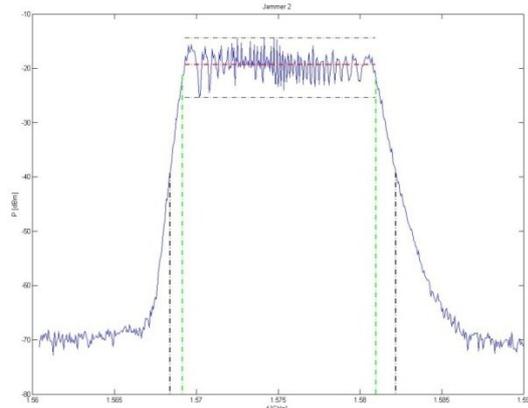


FIG 2. Power spectrum of jammer 2 (Class II)

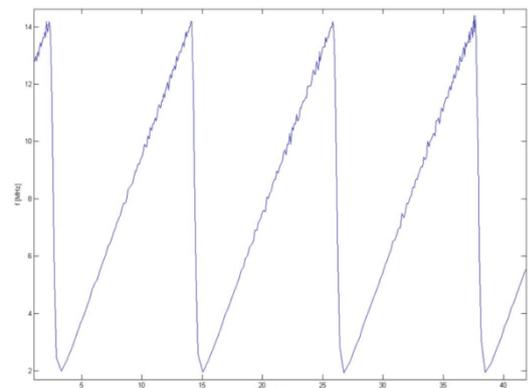


FIG 3. Instantaneous frequency of jammer 2 (Class II)

There is also a negative slope in reality, but this slope is high compared to the positive one so that it can be neglected for modeling. The power spectrum is shown in FIG 2 and the instantaneous frequency over three sweep time cycles in FIG 3. The bandwidth of class II jammers are between 10.72 and 44.9 MHz and the sweep times are between 8.62 and 18.97 µsec. In the class III we found just one jammer (number 5). Additional to the class II, where only one saw-tooth function was used for the VCO input, a class III in-car jammer has a second saw tooth function. The second one has a sweep time, which is four times longer than the first one. Both oscillators are bi-directional saw-tooth functions. In FIG 4, the instantaneous frequency of the second oscillator is printed in red color. Due to this second oscillator the total bandwidth is higher than for each single saw tooth (10.02 MHz and 8.97 MHz, respectively).

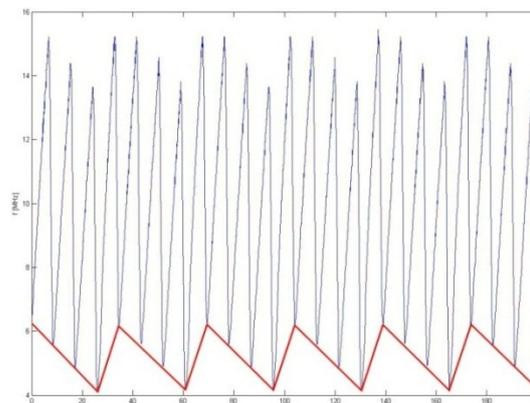


FIG 4. Instantaneous frequency of jammer 5 (Class III) with the second saw-tooth function (red line)

The in-car jammer 6 is the most complex one, with four oscillators controlling the VCO. The signal is similar to class III but with the difference that the fourth one is causing frequency bursts, which almost double the bandwidth for a very short time frame. Thereby jammer 6 defines a separate class IV. These frequency bursts, which occurs every 1.12, 1.35, or 2.28 milli seconds, can be seen in the power spectrum in FIG 5 and in the time analysis in FIG 6. The third oscillator is again a saw-tooth function, but compared to the previous jammers this one has variant sweep times between 139.9 and 183.7µs (see the red line in FIG 7). The analysis of the first and second oscillator showed that the sweep times are constant again, but no synchronization to each other could be derived. An overview on the parameters of the jammers is given in TAB 1.

TAB 1. Overview on Jammer Signal Parameter

No.	Class	Center frequency	Bandwidth	Sweep time(s)	P _{Peak} [dBm]
1	I	1.5747594 GHz	0.92 kHz	-	-12.1 dBm
2	II	1.57507 GHz	11.82 MHz	T _{SW} = 11.71µs	-14.4 dBm
3	II	1.58824 GHz	44.9 MHz	T _{SW} = 18.97µs	-9.6 dBm
4	I	1.5744400 GHz	0.92 kHz	-	-25.6 dBm
5	III	1.57130 GHz	10.02 MHz	T _{SW1} = 8.7 µs (T _{SW1,up} = 6.8µs, T _{SW1,down} = 1.9µs) T _{SW2} = 34.8µs	-19.3 dBm
6	IV	1.57317 GHz (1.57723 GHz)	11.31 MHz (- 19.43 MHz)	T _{SW1} = 8,7408µs T _{SW2} = 43.78µs T _{SW3} = 139.9–183.7µs T _{SW4,1} = 1.1215 ms T _{SW4,2} = 1.3557 ms T _{SW4,3} = 2.2825 ms	-9.5 dBm
7	II	1.57194 GHz	10.72 MHz	T _{SW} = 8.62µs	-30.8 dBm

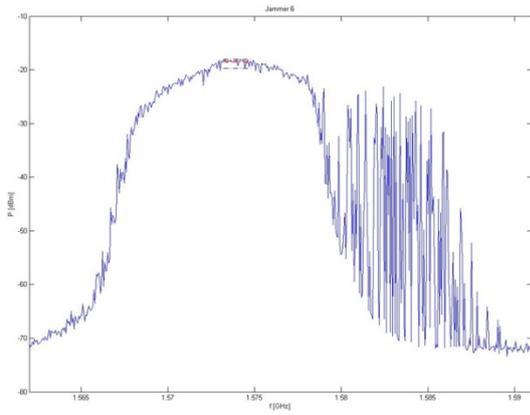


FIG 5. Power spectrum of jammer 6 (Class IV)

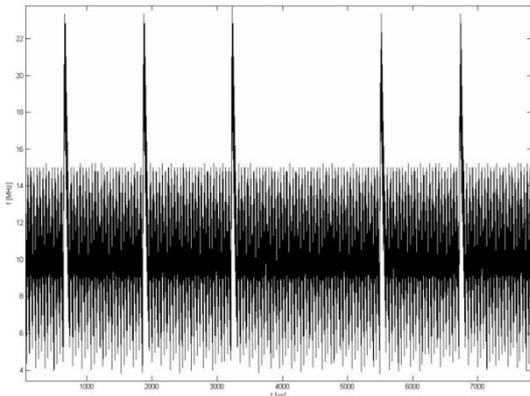


FIG 6. Instantaneous frequency of jammer 6 (Class IV) plus frequency bursts

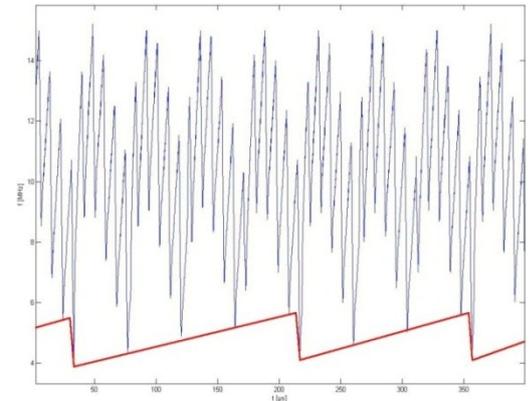


FIG 7. Instantaneous frequency of jammer 6 (Class IV) with the third saw-tooth function (red line)

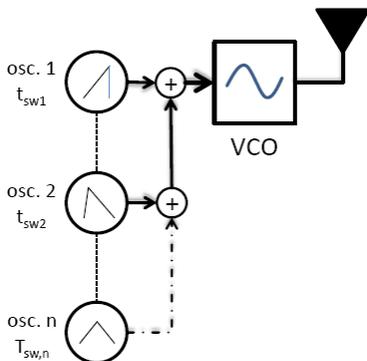


FIG 8. Schematic for the internal structure of a jammer

The construction of an in-car jammer chirp signal is usually done by a voltage controlled oscillator (VCO) with an input voltage of at least one saw tooth function. The instantaneous frequency is equivalent to the voltage input for the VCO within the in-car jammers. FIG 8 shows a general schematic of the internal structure of a jammer. The instantaneous frequency of one oscillator (saw tooth function) can be described generally by

$$f_{osc,n}(t) = \begin{cases} f_{0,n} + k_{up,n}t, & \text{for } 0 \leq t < T_{up,n} \\ f_{0,n} + (k_{up,n} - k_{down,n})T_{up,n} + k_{down,n}t, & \text{for } T_{up,n} \leq t < T_{sw,n} \end{cases} \quad (\text{EQU 1})$$

Together with this equation the signal of all in-car chirp jammers can be formulated as

$$x(t) = a \cdot \sin \left(2\pi \sum_{h=0}^{+\infty} \left(\int_0^t f_{osc,1}(t' - h \cdot T_{sw,1}) \cdot dt' + \dots \dots + \int_0^t f_{osc,n}(t' - h \cdot T_{sw,n}) dt' \right) \right) \quad (\text{EQU 2})$$

where $f_{osc,n}$ is the saw tooth function of oscillator, $f_{0,n}$ the start frequency of the oscillation stage $k_{up,n}$ and $k_{down,n}$ the positive and negative slope of the oscillators saw tooth function, $T_{up,n}$ the time for the increasing part of the saw tooth function and $T_{sw,n}$ the sweep time of the saw tooth function oscillator stage.

3. EFFECT ON THE GNSS RECEIVER

With an exceptional permission, open field measurements were performed at GATE, using the Institute's PC based Experimental Software Receiver (ipexSR) [2]. The frontend parameters and tracking loop settings are summarized in TAB 2. With the ipexSR a NovAtel GPS-704-X antenna was used. For comparison an additional NAVILock GPS mouse with SiRFstarIII chip and a patch antenna was installed to record the carrier-to-noise density ratio (C/N₀). During the measurements, the receivers were static while the jammers approached the receiver, starting from 1200 m distance.

TAB 2. ipexSR configuration

Frontend Parameter	
Bandwidth	10.24 MHz
Sample Rate	20.48 MHz
IF Frequency	5.00 MHz
Quantization	8 bit

The ipexSR outputs are shown with the measurement of jammer 2 which is online the most available and probably most sold and used jammer.

3.1. Received Power Measurements

While moving the jammer towards the receivers, the received interference power $C_{i,received}(r)$ increases in respect of the distance according to the free space loss as

$$C_{i,received}(r) = C_{Jammer} \left(\frac{c}{4\pi r f} \right)^2 \quad (\text{EQU 3})$$

where C_{Jammer} is the radiated jammer signal power. FIG 9 shows the received interference power, estimated after the frontend's analog-to-digital converter (ADC), compared with the theoretical curve of a jammer with -10 dBm transmission power. The curves show good alignment for the interval where the received interference power is noticeable above the noise floor until a certain point, indicated by the dashed red line, from where on the received signal strength converges to an upper limit. This is due to saturation of the frontend which limits the received interference signal amplitude.

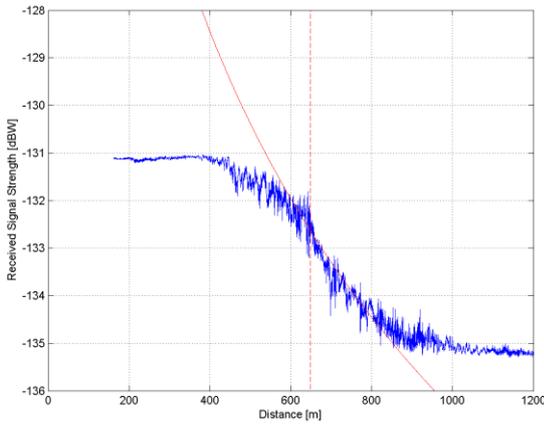


FIG 9. Received signal strength

The frontend used with ipexSR comprises no automatic gain control (AGC), hence for the measurements the gain is set externally in the receivers configuration file. When setting the gain it is considered to distribute the non-interfered samples over the entire ADC bins. The gain setting for the interference free samples distributed over the entire ADC bins is optimal when no interference is present, whereas with interference the ADC is immediately at its limit. The saturation effect can also be seen in FIG 10 where the actual C/N_0 degradation is compared with the theoretical effective C/N_0 curve. As soon as the frontend ADC is saturated it causes severe degradation which exceeds the pure degradation caused by the increased interference power until loss-of-lock on the signal. The theoretical degradation of the receiver performance is expressed by the effective carrier-to-noise density ratio $(C/N_0)_{eff}$ derived by [5] as

$$\left(\frac{C}{N_0} \right)_{eff} = \frac{1}{\frac{C_i}{C_s} + \frac{1}{QR_c}} \quad (\text{EQU 4})$$

where Q is the spectral separation gain adjustment factor and C_i the received interference power.

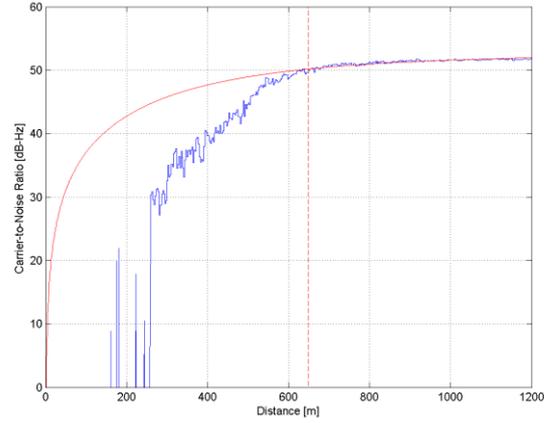


FIG 10. Comparison of theoretical $(C/N_0)_{eff}$ and ipexSR measured C/N_0

The SiRFstarIII receiver has an AGC to compensate for the rising interference power level, which results in better performance under interference conditions. The C/N_0 curve of the SiRFstarIII receiver (FIG 11) shows good alignment with the theoretical curve over the whole measurement range. For this measurement jammer 6 has been used with an in the lab determined peak power of -9.5 dBm (TAB 1). Via C/N_0 matching of the measured C/N_0 in the receiver of PRN12 and EQU 1 the effective jammer "noise" power equals -11.5 dBm. The difference of 2 dB can be explained because of uncertainties, like antenna loss of the jammer and the unclear filter parameters of the receiver frontend. In any case, it approves that the measurements of the lab are correct, which showed that the maximum power of a jammer is 0.1 mW.

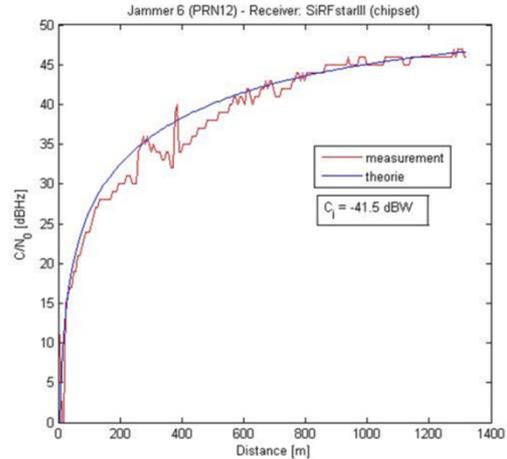


FIG 11. Comparison of theoretical $(C/N_0)_{eff}$ and SiRFstarIII measured C/N_0

One way to determine the effect of interference on a receiver is the definition of harmful interference (HI). HI within the GPS community is usually defined as a degradation of 1 dB in the effective C/N_0 . With jammer 6 this occurs already in a distance of approximately 1000 meters. For another example, LightSquared defined HI as a 6 dB change in C/N_0 [3]. This level of degradation occurs in a distance of 500 meters. The loss-of-lock in the tracking loop started in a distance of 23 meters, which results in a C/N_0 of 15 dBHz.

3.2. Tracking Performance

Until saturation of the frontend the interference degrades the correlation process by raising the noise floor. FIG 12 shows the multicorrelator output in an interference free environment whereas the multicorrelator output in FIG 13 is distorted by the received interference signal.

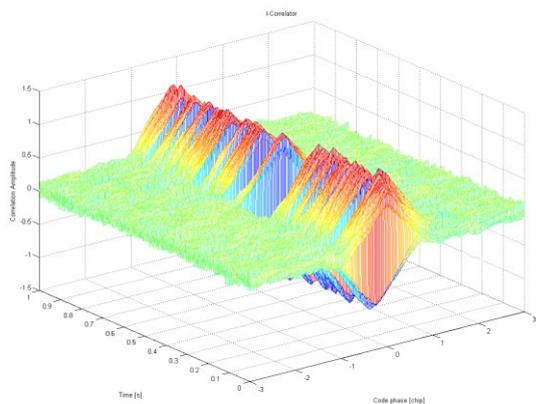


FIG 12. Multicorrelator without interference

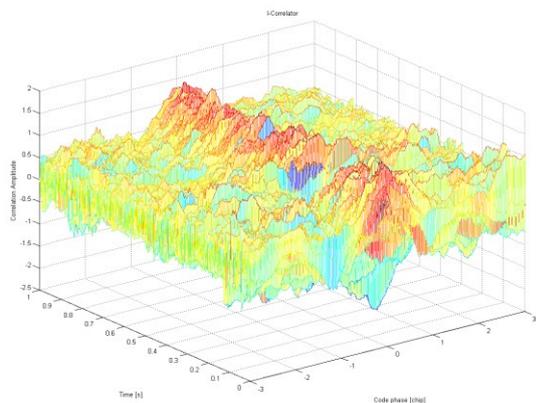


FIG 13. Multicorrelator output with interference present

FIG 14 shows the distortion of the punctual code correlation output over the whole measurement range. The inphase correlator output is degraded until loss-of-lock on the navigation signal occurs.

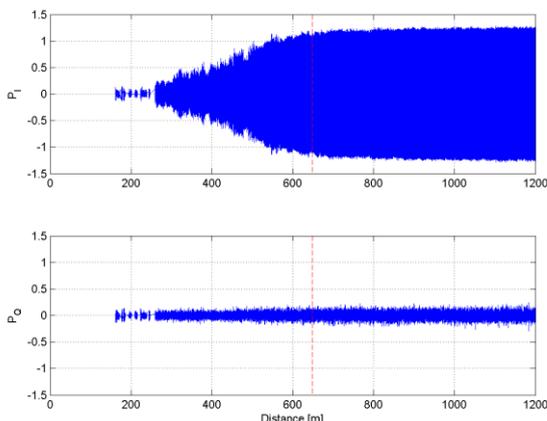


FIG 14. Prompt I/Q correlation outputs

Degradation of the correlation output has a direct effect on the performance of the tracking loops and their discriminator outputs as shown in FIG 15.

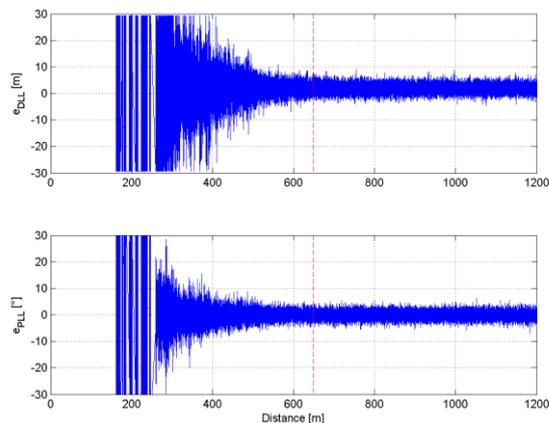


FIG 15. DLL and PLL discriminator outputs

The tracking loop error rises until it is out of the pull in range of the discriminator functions which causes loss-of-lock on the PLL. Degradation of DLL performance causes degraded position accuracy (FIG 16) until less than four PRNs can be tracked and consequently no more position determination is possible.

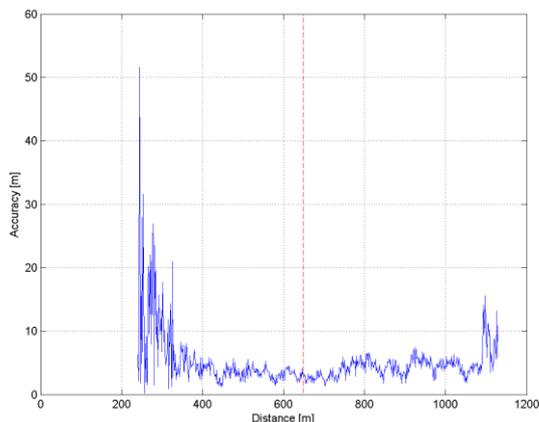


FIG 16. Measured position error

The measurements have shown that currently available in-car jammer degrade the receiver performance approximately in a radius of 1 km and prevent receivers from position determination within a radius of about 200 m.

4. JAMMER DETECTION

Detecting interference is the first step in the mitigation process. Upon detection, the interference event can be reported to the authorities to initiate the mitigation of the interference at its source as well as to enable interference mitigation techniques at the receiver. State of the art receivers like the u-blox 6 receiver are able to detect interfering signals by monitoring the background noise and looking for significant changes. To take appropriate measures against jammers, it is not only necessary to detect the presence of interference but also to characterize the interfering signal.

In the following, a two-sample t-test was used to detect interference in the time domain. Upon detection, the signal is analyzed in the time-frequency domain by applying a short-time Fourier transformation to determine the interference signal parameters.

4.1. Detection and Signal Transformation

For detection of GNSS interference signals in the receiver, a non-parametric large sample t-test is used as introduced by Marti [4] and evaluated later by Balaei [5]. The algorithm incorporates an assessment window which is supposed to be interference free and an evaluation window which is shifted over the incoming data stream. The t-test then performs a hypothesis test of the null hypothesis that the data in the assessment window and evaluation window are independent random samples from normal distributions with equal means and equal but unknown variances, against the alternative hypothesis that the means and variance are not equal. For the case where the variances of the two populations are not equal (Smith-Satterthwaite test [6]) the test statistic is given by

$$t = \frac{\bar{x} - \bar{y}}{\sqrt{\frac{S_x^2}{N} + \frac{S_y^2}{M}}} \quad (\text{EQU 5})$$

where \bar{x} and \bar{y} are the sample means, s_x and s_y are the sample standard deviation. To detect interference by revealing fluctuations of the received signal power, the test is performed on the second moment energy estimator \hat{U} given by

$$\hat{U} = E[X^2] = \frac{1}{N} \sum_{n=0}^{N-1} X_n^2 \quad (\text{EQU 6})$$

It is shown by Marti [4] that \hat{U} converges to a normal distribution and is over bound by the Berry-Esseen theorem.

After detection of the interference signal in the time domain, the one-dimensional function $x(t)$ is mapped into a two-dimensional function of time and frequency $T_x(t, f)$ to allow a temporal localization of the interfering signals spectral components [7]. Among others, the Short-Time Fourier Transform (STFT) was chosen for the initial analysis of the detected interference signal. It has poor localization properties but is favorable for its low computational load. The discrete STFT of a discrete signal $r[n]$ is defined as

$$STFT(\tau, f) = \sum_{i=0}^{N-1} r[i]w[i - \tau]e^{-i2\pi n f} \quad (\text{EQU 7})$$

where $w[n]$ is the analysis window.

For the implementation with ipexSR, a Hanning window with 2^5 samples length and 50 % overlapping was applied to achieve the required time-frequency (TF) resolution. The input IF sample stream and five successive STFT plots are shown in FIG 17 and FIG 18 respectively. Assembling STFT plots for each time step results in the TF representation shown in FIG 19. In the TF plane, the instantaneous frequency of the chirp signal can be observed to move linearly over the entire frontend bandwidth (0 to 10.24 MHz).

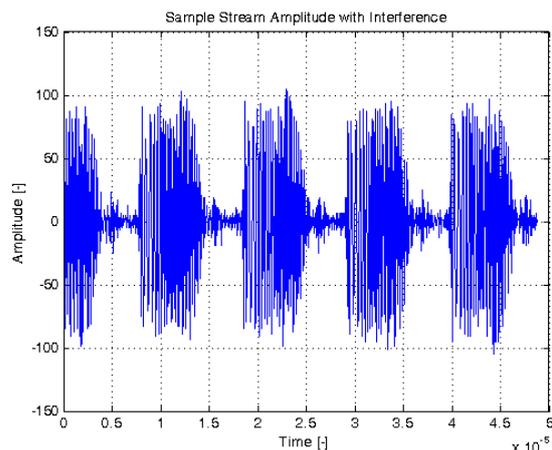


FIG 17. IF sample stream

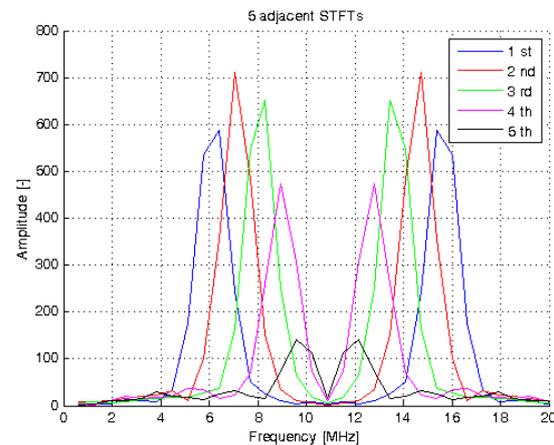


FIG 18. Five successive STFT plots

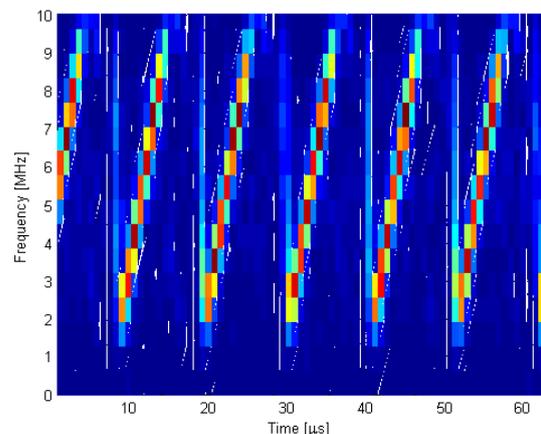


FIG 19. Time-Frequency representation of the jammer signal

Based on the TF representation, a characterization of the interference signal parameters is possible.

4.2. Parameter Estimation

To characterize the interference signal it is necessary to determine the instantaneous frequency of the signal. The instantaneous frequency is estimated through a peak tracking algorithm. For each time instance it searches for the maxima in the STFT representation. FIG 20 shows the output of the algorithm with the instantaneous frequency at

IF when no interference signal is present within the bandwidth of the frontend.

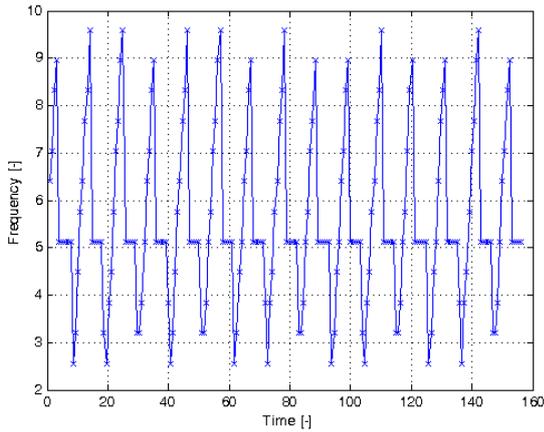


FIG 20. STFT peak tracking for jammer signal

From the output of the peak tracking algorithm, the coarse frequency rate of the chirp signal can be estimated. The coarse frequency rate can be taken as input to estimate the frequency rate more accurately with a fractional Fourier Transform (FrFT). The FrFT is a generalization of the ordinary Fourier transformation [8] where the signal is rotated in the TF plane. A discrete-time approximation of the continuous form was used [9] with gives negligible loss. The continuous form of the FrFT is described as

$$FrFT_{\alpha}(u) = \int_{-\infty}^{\infty} r(t)K_{\alpha}(t,u)dt \quad (EQU 8)$$

with $K_{\alpha}(t, u)$ representing the kernel function defined as

$$K_{\alpha}(t, u) = \begin{cases} \sqrt{\frac{1 - icot \alpha}{2\pi}} e^{i\frac{u^2}{2}cot \alpha} \\ \times e^{i\frac{t^2}{2}cot \alpha - iutcsc \alpha}, & \alpha \neq n\pi \\ \delta(t - u), & \alpha = 2n\pi \\ \delta(t + u), & \alpha = (2n + 1)\pi \end{cases} \quad (EQU 9)$$

and $\delta(t)$ representing the Dirac function. The order parameter α specifies the frequency rate of the chirp signal in the TF plane and can be derived as shown in [10] by

$$\dot{f} = \frac{f_s^2}{2N} \tan \alpha \quad (EQU 10)$$

where f_s is the sampling frequency and N the FrFT length. Chirp signals generate at their optimum FrFT order an impulse. Using the coarse chirp rate as an input and searching for the maximum peak iteratively allows to derive the exact chirp rate as shown in FIG 21.

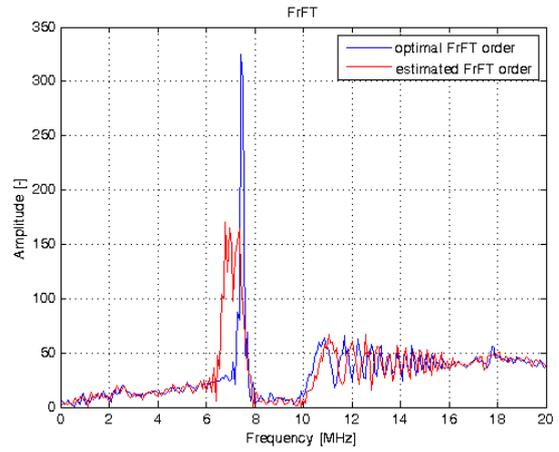


FIG 21. FrFT output with the estimated and optimal FrFT order

The data from the detection will be used in the next steps to mitigate the jammer at the source by reporting the interference event to authorities and to mitigate the jammer effect at the receiver by excision of the interfering signal from the intermediate sample stream.

5. JAMMER MITIGATION AT THE SOURCE

In the United States the Department of Homeland Security is working on a sensor system called Patriot Watch to protect GPS users from interference. It envisions an open architecture to allow for the integration of various sensors using a common data exchange format [11].

Here we envisage to use the infrastructure of future cooperative ITS (C-ITS) which is currently under standardization [12]. C-ITS will increase the performance of road traffic management activities through improved quality of traffic and road conditions monitoring. Different ITS sub-systems as illustrated in FIG 22 are intended to combine vehicles as floating sensors with existing road side equipment to monitor its environment cooperatively. GNSS receivers connected within the C-ITS architecture establishes a comprehensive GNSS sensor network.

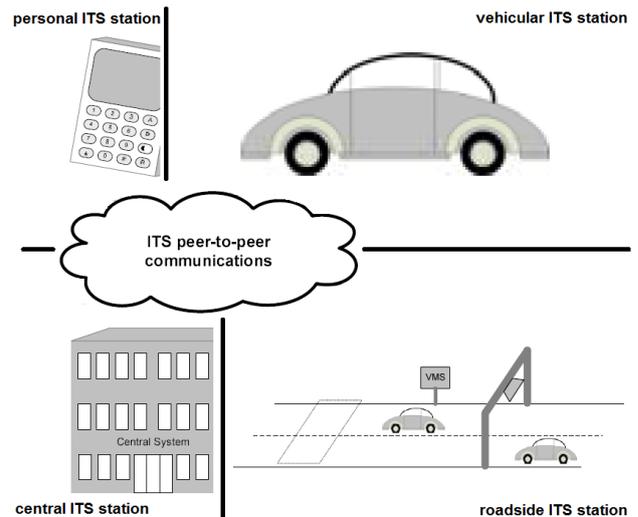


FIG 22. Sub-systems of the C-ITS network [13]

Automotive positioning systems have the advantage of boundaries on their movement, possibility of map matching and additional sensors which they can use for

position determination in case of blocked GNSS signals. By reporting detected interference events and the vehicle position, based on the additional sensors, to the central ITS station, a coarse localization of jammers is possible.

5.1. Message Structure

In the C-ITS architecture, unexpected roadway conditions ahead, such as accidents, hazardous weather conditions, etc. corresponding to a Road Hazard Warning (RHW) use case are communicated in real-time by a Decentralized Environmental Notification Message (DENM) to enhance driver awareness. The DENM is used to distribute and to evaluate information related to road events. It is a basic message to support the event based exchange of information. In case the GNSS sensor detects an interference event, the vehicular ITS station generates a DENM containing the measured interference signal power and optional additional parameters and sends it via point-to-point communication to the back-end (central ITS station). DENMs are broadcast as long as the event exists at a given frequency. It consists of three containers as depicted in FIG 23.

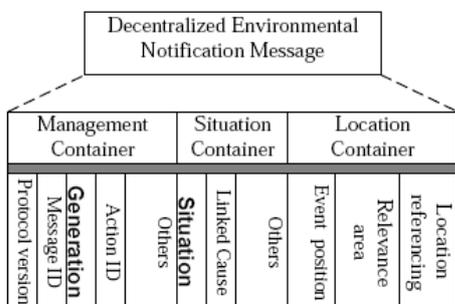


FIG 23. General structure of the DENM [14]

Each container is composed of a sequence of data elements and data frames. To code the cause and the severity of an event the Situation Container has three parameters CauseCode, SubCauseCode and Severity. A new ID for the cause has to be added indicating a disturbed infrastructure. This ID links to another category specifying what kind of signal is affected, e.g. GNSS L1, GNSS L5 or even other communication links like GSM. To indicate the severity level an enumeration ranging from 1 (informative level) to 4 (danger level 3: highest danger) already exists. As the severity of degraded or missing GNSS may differ in each vehicle, it is proposed to set the ID = 1 informative and let the in-vehicle application decide how to deal with it. For example: A dangerous goods transport may decide to drive slower or even take an alternative route, a private vehicle may simply follow its original track. To code the location of an event, the location container has 3 parameters for the position and one parameter for the relevance area. In the basic implementation the relevance area can be used to code the received interference power. In the advanced implementation where the receiver also characterizes the interference the DENM has to be extended to contain the parameters for interference type and signal parameters.

5.2. Message Flow

If sufficient evidence has been collected, a local control team may be informed about the incidence which than can take action to find the suspected interference source. The message flow and the participating communication peers

are depicted in a general way in the sequential diagrams in FIG 24. The ITS station operated in the vehicle is capable of communicating via the WiFi standard IEEE 802.11p for vehicular communication. To keep the diagrams as simple as possible, only one vehicle starts the communication. In reality it is expected that more than one device will be in the range of the interference source and therefore more than one vehicle reacts to the interference event. Nevertheless this assumption does not change the message flow described, it affects however timing and processing behavior of the units.

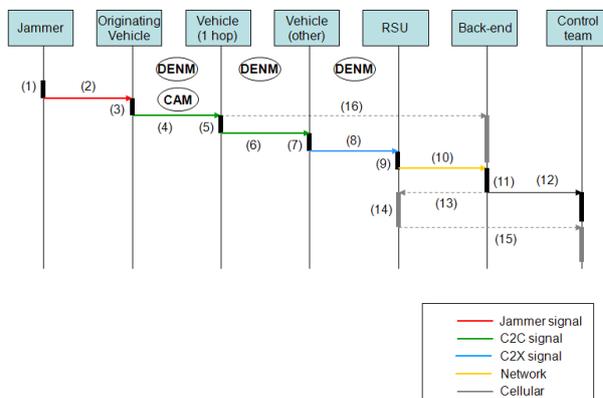


FIG 24. Control team communication

The legal entity that could process the data necessary for interference localization would be the local Traffic Management Center (TMC). A TMC is operating as a kind of public authority, closely linked to police and road operators. Information about road safety, hazards, construction sites and weather conditions amongst others are processed and communicated there. In Germany, the following entities are involved in fraud and frequency issues

- The BAG (Bundesamt für Güterverkehr) acts as the control entity for “Toll Collect”.
- The authority responsible for frequency management is the BNetzA (Bundesnetzagentur). As a civil authority it controls the availability of radio frequencies, civilian as well as military. The BNetzA is also the authority which prosecutes interferers and is supported by civil and military police.
- Civil police acts on directive of the BNetzA.
- In severe cases the military police can also prosecute by itself supported by the intelligence corps due to the military assignment of the GNSS band.

In case of a detected interference the best solution would be the TMC reporting directly to the civil police. The TMC generates and broadcasts the DENM interference warning, informs involved toll system operators and the police which is then tracking down the interference source in real-time. For example the Munich TMC is operated in the domain of the local police forces. It therefore demonstrates that a close link between TMC and local police already exists and an effective infrastructure to build on is in place. For back office communication between TMC and toll operator to exchange information on possible fraud attempts, bi-lateral agreements may be sufficient.

6. JAMMER MITIGATION AT THE RECEIVER

After detection and characterization of the interfering signal in the time-frequency domain as described before, the interference can be mitigated by clipping or zeroing of

bins containing interference and applying an inverse signal transformation [15]. The operation is illustrated in FIG 25. Since for the STFT transformation an overlapping of 50 % was used, for the inverse STFT and signal synthesis the overlap-add method is applied [16]. In FIG 26 the input and output IF sample streams are compared.

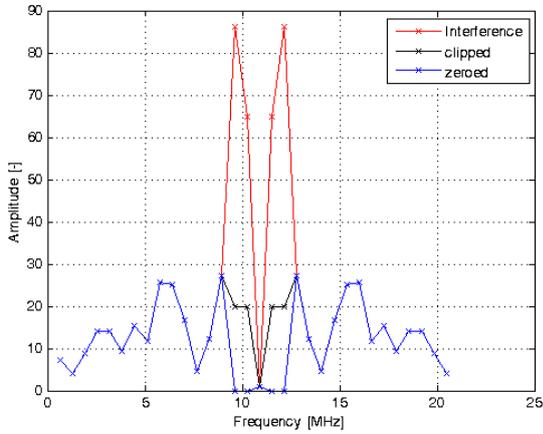


FIG 25. Zeroing or clipping of bins containing interference

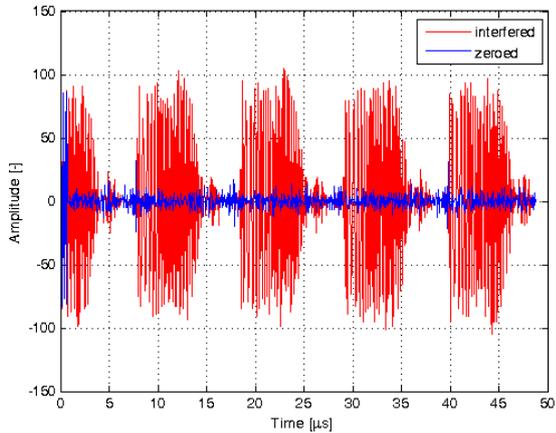


FIG 26. IF sample stream before (red) and after (blue) mitigation

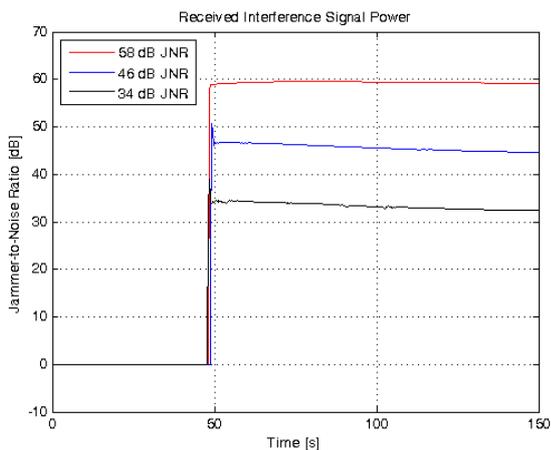


FIG 27. Jammer-to-Noise Ratio of received interference signal

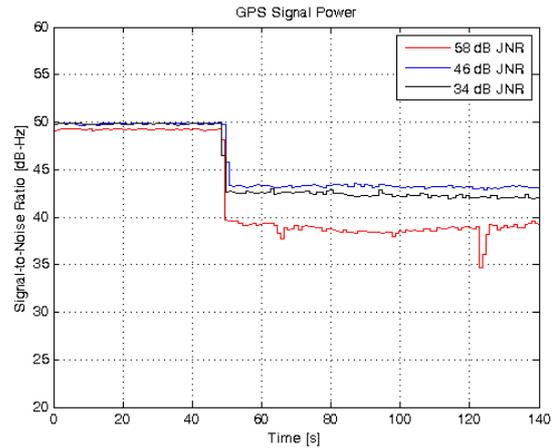


FIG 28. Carrier-to-Noise Ratio for GPS when applying STFT based zeroing

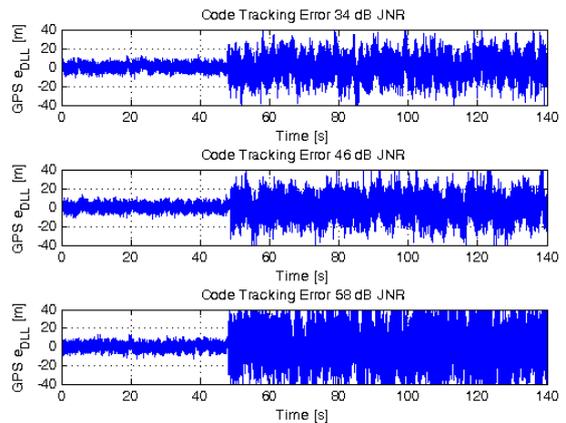


FIG 29. DLL tracking error

In a GNSS receiver the signal is correlated with a local replica of the PRN code. When filtering techniques are applied for interference mitigation, the received PRN sequence and the original sequence will no longer be identical. The interference mitigation increases the C/N0 in respect to the interfered signal but it also decreases the C/N0 in respect to the interference free signal. FIG 27 shows the jammer-to-noise ratio (JNR) profiles for 3 measurements. The interference source is turned on after approximately 50 seconds. Without applying any mitigation techniques, after the interference is turned on, it is not possible to continue tracking of the navigation signal in all three cases. FIG 28 shows for GPS the improved tracking performance by means of the C/N0 measurements. The tracking loop error for an early-minus-late correlator with 20 ms coherent integration time is shown in FIG 29. The GNSS receiver enabled mitigation algorithms shows an apparent superior performance then the receiver without any mitigation techniques.

7. CONCLUSION

The InCarITS project presented in this paper attempts to counter the interference threat at three sides. First, it created public awareness of the problem. The initial characterization of in-car jammers and evaluation of the effects on the receiver helps to understand the problem. Second, reporting of interference shall enable authorities to take action on detected malicious interference events.

By relying on vehicular communication and existing infrastructure it is possible to simultaneously warn advancing vehicles but also to inform local authorities about strength, coarse location and movement of the interference source. Given the safety relevance of the threat, detection and reporting of interference events should be subject of safety related vehicular communication and its standards should be able to handle this in the same way as other safety related issues. Third, the project showed techniques to mitigate the interference signal at the receiver by excision of the high power interference signal from the IF sample stream. Altogether the results of the project contribute to make nowadays GNSS relying traffic infrastructure more robust and safer.

8. ACKNOWLEDGMENTS

The results presented in this paper were developed during the InCarITS Project (Analysis, Detection and Mitigation of In-Car GNSS Jammer Interference in Intelligent Transport Systems), funded by the Federal Ministry of Economics and Technology (BMW) and administered by the Project Management Agency for Aeronautics Research of the DLR in Bonn (project/grant no. 50 NA 1001).

9. REFERENCES

- [1] T. Kraus, R. Bauernfeind and B. Eissfeller, *Survey of In-Car Jammers - Analysis and Modeling of the RF signals and IF samples (suitable for active signal cancellation)*, Portland, OR, USA: ION GNSS 2011 Conference, 2011.
- [2] C. Stöber, "ipexSR: A Real-Time Multi-Frequency Software," in *IEEE ELMAR*, Zadar, Croatia, 2010.
- [3] Working Group (FCC Ordered), "GPS/LightSquared Final Report of FCC-Ordered Working Group," 30.06.2010.
- [4] L. M. Marti, *Global Positioning System Interference and Satellite Anomalous Event Monitor*, Athens, Ohio, US: Ohio University, 2004.
- [5] A. T. Balaei, *Detection, Characterization and Mitigation of Interference in Receivers for GNSS*, Sydney, Australia: University of New South Wales, 2007.
- [6] D. D. Wackerly, *Mathematical statistics with applications*, Belmont, CA, US: Thomson Higher Education, 2008.
- [7] D. Borio, *A Statistical Theory for GNSS Signal Acquisition*, Torino, Italy: Politecnico di Torino, 2008.
- [8] E. Sejdic, I. Djurovic and L. Stankovic, "Fractional Fourier transform as a signal processing tool: An overview of recent developments," *Signal Processing*, no. 91, pp. 1351-1369, 2011.
- [9] C. Candan, A. Kutay and H. Ozaktas, "The Discrete Fractional Fourier Transform," *IEEE TRANSACTIONS ON SIGNAL PROCESSING*, 2000.
- [10] C. Capus and K. Brown, "Short-time fractional Fourier methods for the time-frequency representation of chirp signals," *Journal of the Acoustical Society of America*, no. 113, 2003.
- [11] D. A. Divis, "Homeland Security Steps Up to Protect GPS (But Not from LightSquared)," *Inside GNSS*, no. May/June, 2011.
- [12] C. Weiß, "V2X communication in Europe - From research projects towards standardization and field testing of vehicle communication technology," *Computer Networks*, vol. 55, pp. 3103-3119, 2011.
- [13] ETSI, "EN 302 665; Intelligent Transport Systems (ITS); Communications Architecture," France, 2010-09.
- [14] ETSI, "TS 102 637; Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications," France, 2010-09.
- [15] X. Ouyang and M. G. Amin, "Short-Time Fourier Transform Receiver for Nonstationary Interference Excision in Direct Sequence Spread Spectrum Communications," *IEEE Transactions on Signal Processing*, vol. Vol. 49, no. No. 4, pp. 851-863, 2001.
- [16] B. Yang, "A Study of Inverse Short-Time Fourier Transform," *ICASSP*, pp. 3541-3544, 2008.