Software-Defined-Radio techniques against Jammers for in car GNSS navigation

Antonio Di Fonzo, Mauro Leonardi, Gaspare Galati

Tor Vergata University - Electronic Engineering Department

Via del politecnico, 1 - 00133 Rome Italy

difonzoantonio.87@tiscali.it; mauro.leonardi@uniroma2.it;gaspare.galati@uniroma2.it

Paola Madonna, Luca Sfarzo

Tecnologie nelle Reti e nei Sistemi

TRS spa Via della Bufalotta, 378 - 00139 Roma

paola.madonna@trs.it; luca.sfarzo@trs.it

***Abstract*— It is well know that jamming is an easy and low cost attack method against GNSS-based applications. In the last years these types of attacks have increased significantly due to the availability of GPS jammers that can be easily found, for example, on the internet and due to the constant growth of in-car GNSS-based applications . Usually a jamming device, also called in-car jammer, is a quite simple electronic device which emits a single frequency tone or some type of chirp signal. These types of signal can be considered as an instantaneous narrow band and can be mitigated with very simple processing, based on Short Time Fourier Transform. These considerations lead to the development of an equipment able to reduce the effect of these harmful signals over a generic GNSS receiver through a Software Defined Radio (SDR) equipment. In this paper a brief introduction to the problem is presented and a time-frequency mitigation technique is shown along with some results for a set of in-car jammers.**

Keywords—GNSS, GPS, SDR, Jamming, STFT.

I. INTRODUCTION

In 2009 a satellite-based positioning infrastructure for aircraft landing at Newark airport suffered from brief daily breaks. After two months of investigations by the Federal Aviation Authority it was discovered that a truck passing by on the nearby highway every day had a cheap GPS jammer onboard causing a serious integrity threat to such critical GNSS-based infrastructure.

In 2010 the Guardian wrote: "Criminal gangs have begun using GPS jammers imported from China to help them steal expensive cars and lorries carrying valuable loads and there are fears that terrorists could use more powerful versions to disrupt air traffic…".

Obviously the use of jammers is illegal in most countries but these devices are gaining popularity to avoid road tolling, increase in insurance costs, as well as any tracking and location based monitoring.

Detection and mitigation of interference signals produced by these devices could be one the most challenging and demanding activities in the incoming years of GNSS applied research.

Most of low cost in-car jammers have a very simple hardware and produce simple but still harmful signals. The aim of this work is to analyze the use of an SDR HW to test mitigation techniques for these intentional interferences. The idea is to put a software defined radio between a GNSS antenna and a GNSS receiver to detect and mitigate these interferences.

In Figure 1 two possible implementation schemes for SDR jamming mitigation are shown. The first one is a "retrofit" version that can be put into an already existing antenna-receiver chain. The second scheme represents the implementation of a self-contained SDR equipment in which the GNSS receiver is a SW implementation inside the SDR itself.

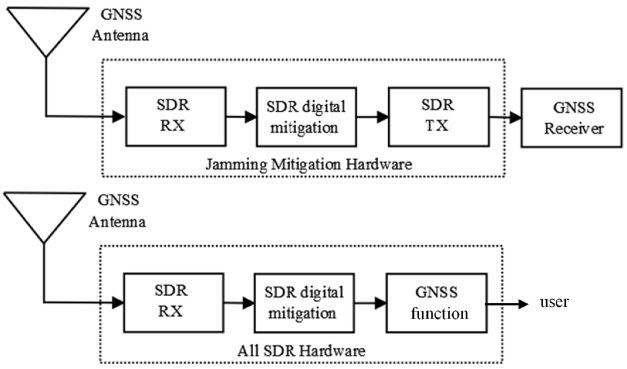

Fig. 1. Possible HW implementation of SDR for jamming mitigation

II. JAMMERS ANALYSYS

Before introducing the HW and SW mitigation techniques an analysis of jammer and signal types is needed. This section deals with some existing in-car jammers; in particular it is divided in two parts: the first refers to the jammers characterized in [1] and the second refers to the jammers available in the TRS (Tecnologie nelle Reti e nei Sistemi) S.p.A. laboratories.

Among the jammers analyzed and classified in [1], this paper focuses on the following three main classes:

- Class I: Continuous Wave Signal
- Class II: Chirp signal with one saw-tooth function
- Class III: Chirp signal with multi saw-tooth functions.

Their characteristic parameters are shown in Table I. They are: sweep time, center frequency, bandwidth and output peak power. Sweep time is the time to accomplish a complete change of frequency (for class II and III jammers); center frequency is the frequency band center.

TABLE I. PARAMETERS OF THE CONSIDERED IN-CAR JAMMERS

N	Class	Center Frequency f_o [GHz]	Bandwidth	Sweep Time [µsec]	P_t [dBm]
1	I	1.5747594	0.92 KHz	-	-12.1
2	I	1.5744400	0.92 KHz	-	-25.6
3	II	1.57507	11.82 MHz	T_{sw}=11.71	-14.4
4	II	1.57194	10.72 MHz	T_{sw} =8.62	-30.8
5	III	1.57130	10.02 MHz	T_{sw1}=8.7 T_{sw2}=34.8	-19.3

The in-car jammers available in TRS S.p.A., shown in Fig. 2, were analyzed in the frequency/time domain with a digital oscilloscope (LeCroy WaveRunner 204MXi-A 2 GHz Bandwidth, 4 Input Channels, 10GS/s Max Sampling Rate) and an RF attenuator to attenuate the input signal to the measuring instrument.

Fig. 2. In-car jammers analyzed

In Figure 2, each jammer has an ID which indicates the model as on the producer's web site; they all produce signals belonging to the category of narrowband interference.

The first jammer (J-0035B) transmits bidirectional chirp signal in the L1 band, as shown in Figure 3, with a multi saw-tooth function which describes the instantaneous frequency. The bandwidth of this signal is about 25 MHz and its sweep time is about 40 µsec with 37 µsec rise time and 3 µsec fall time. The spectrogram, as shown in Figure 3, was performed by recording the signal samples with the digital oscilloscope and processing them with Matlab. In more detail, a spectrogram was computed with a Hamming window of length 2048 samples and an overlap factor between the windows of 100 samples on a signal sampled at a frequency of 5 GHz.

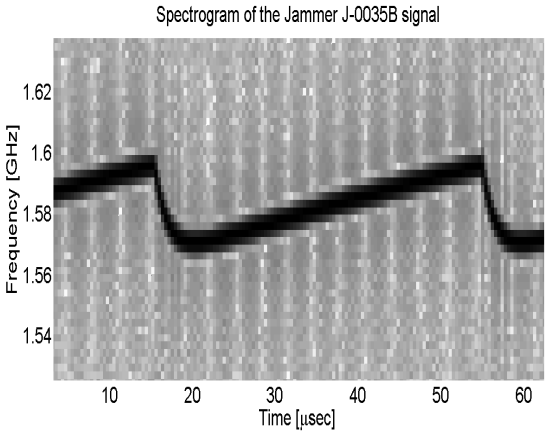

Fig. 3. Spectrogram of jammer J-0035B

The second jammer (J-0035C) transmits a chirp signal on the L1 band, with a 12 MHz signal bandwidth; this is an unidirectional chirp with a sweep time of 20 µsec versus of the bidirectional chirp transmitted by the jammer J-0035C analyzed. The spectrogram is shown in Figure 4.

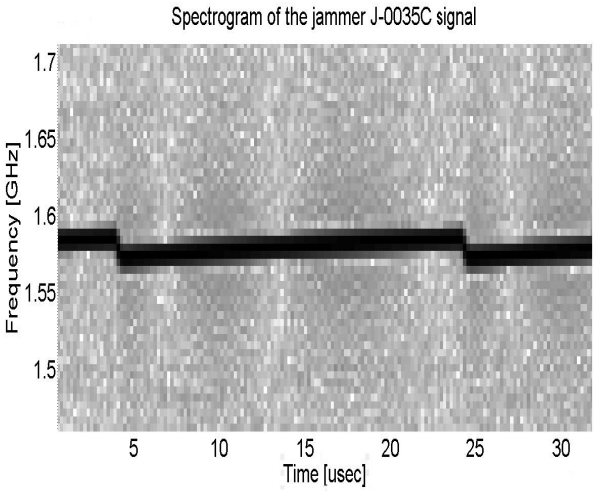

Fig. 4. Spectrogram of jammer J-0035C

Unlike the single frequency jammers (J-0035B and J-0035C, as shown previously) the last jammer analyzed, the J-242G, is a multi-frequency jammer. It has four antennas with a control switch which enables (or not) each transmitting antenna. It transmits bidirectional chirp signals in the L1/L2/L3/L4/L5 bands with a multi saw-tooth function. The fourth antenna is of particular interest because it transmits three chirp signals in the L2, L4 and L5 bands as shown in the spectrogram of Figure 5. The procedure to obtain the spectrogram is the same as the previous case, but the sampling frequency is 10 GHz. The sweep time is the same for the three chirp signals (about 9 µsec).

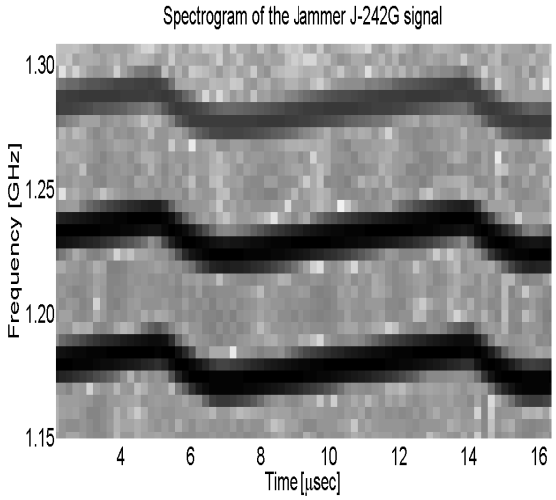

Fig. 5. Spectrogram of jammer J-242

In Table II the measured parameters for these jammers are reported.

TABLE II. PARAMETERS OF THE IN-CAR JAMMERS ANALYZED IN TRS SPA

Name	Class	Antenna	f_0 [MHz]	Band width [MHz]	Sweep-time [µsec]
J-0035B	**III**	**1**	**1581.86**	**25**	**40**
J-0035C	**II**	**1**	**1576.38**	**12**	**20**
J-242G	**III**	**1**	**1573.74**	**15**	**9**
		2	**1202.03**	**15**	
		3	**1277.42**	**15**	
		4	**1227.5**	**15**	
			1279.5	**15**	
			1176	**15**	

III. SDR HW DESCRIPTION

The proposed experimental SDR HW is based on the National Instruments USRP 2920 and is intended to work only in the L1 band for the C/A code. This programmable device has both RX and TX channels capable of working in a frequency range between 50 MHz and 2.2 GHz with a sampling frequency up to 100 MSps [2]. This HW allows to implement both architectures proposed in Figure 1 (thanks to the TX channel). The only additional HW required is an active antenna, a power supply for the antenna and (recommended) an "in-cable amplifier".

The selected antenna is the L1A-GPS that has a low-noise amplifer, with a gain of 33 dB [3]; the selected amplifer is the A11 that has a gain of 30 dB [4]; the amplifier is equipped

with an internal bias-tee that provides the power to the antenna. Within the USPR the signal can be downconverted to an intermediate frequency and sampled. The sampled signal is transferred to the host computer that can be programmed with the desidered algorithms, then the signal can be:

- upconverted to the L1 frequency and transmitted with the USRP TX or
- sent directly to the GNSS receiver algorithms (for example the algorithms proposed by Borre in [5]) to perform the signals acquisition, tracking and PVT estimation.

Knowing the Maximum Input Power (MIP) for USRP-2920, that is 0 dBm [2], and the power trasmitted from the various jammers (Table 1) it is possible to calculate the minimum distance that produces an USRP saturation (D_{SAT}). When the USRP is in saturation it is impossible to implement any mitigation tecnique due to the distortion of the incoming signals. This is the bottom limit under which the jammer cannot be mitigated.

It is also important to define and find the maximum distance (D_{MAX}) at which the jammer still produces a harmful interference on the receiver. In this paper D_{MAX} is the distance at wich the jammer produces 5 over 100 missed acquisition. An acquisition is missed if the peak-to-sidelobe ratio (PSLR) of the correlation function at the receiver is less than 2.5.

In Table III, the effect of the jammers of TABLE I,on the receiver chain in terms of D_{SAT} and D_{MAX} is shown.

TABLE III. MAXIMUM DISTANCE TO DISRUPT ACQUISITION PROCESS (D_{MAX}), AND MINIMUM DISTANCE FOR RECEIVER SATURATION(D_{SAT})

N	Class	D_{MAX} [m]	D_{SAT} [m]
1	I	298.9	5.3
2	I	5.6	1.1
3	II	288.7	4.1
4	II	59.1	0.6
5	III	73.4	2.3

The aim of the mitigation algorithms to be implemented in the mitigation block is to reduce D_{MAX} as much as possible, up to the limit $D_{MAX}=D_{SAT}$.

IV. MITIGATION TECHNIQUES AND RESULTS

Mitigation of narrow band interfering signals can be, in principle, easily done using Short Time Fourier Transform (STFT), by blanking the portion of spectrum in which the interference is located. In particular when the presence of an interfering signal is detected on a part of the signal in the time domain, a blanking of the intefering signal in the STFT domain is applied and then the IFFT is applied to come back to time domain. The performance of this simple approach depends on different parameters such as the frequency resolution of the method used, the time resolution (i.e. sampling time) of the incoming signal, the STFT window length and the blanking logic. In literature some works based on the concept of time-frequency analysis exist: in [6] a mitigation algorithm based on STFT and FrFT (Fractional Fourier Transform) is shown and in [7] this algorithm is examined in depth.

In this work the USRP-2920 is exploited at a sampling frequency of 100 MHz, and a down-conversion to an intermediate frequency of 10 MHz.

The mitigation block performs two preliminary operations:

- Band Pass Filtering with 2 MHz bandwidth
- Undersampling to 25 MSample/sec.

After these operations the Detection Process works and, if neeeded, the Mitigation Process is applied on the acquired signal.

A simulated GPS signal has been produced with a received power level of -158.5 dBm [7], and a noise power level derived by a Band Pass Filter filter of 2 MHz.

The detection technique is based on the detection of a signal with power that exceeds a threshold in the time domain. In particular the Marcum theory is adopted and the detection threshold is determined by fixing the probability of false alarm (to 10^{-6}) and the probability of missed detection to 0.9. In this case the detection of an interference on a GPS signal needs a Jammer-to-Noise-Ratio (JNR) greather than 13.2 dB.. The described detection procedure is implemented on the simulated signal samples; in particular, a sliding window is used to select 32 samples and on these samples the incoming signal power is estimated: if the power is greater than the detection threshold then the presence of a jamming signal is declared.

If no jamming signal is detected then the sliding window is shifted of one sample, and the procedure is repeated.

A window length of 32 samples has been chosen due to the sampling frequency adopted in the algorithm. With a 25 MHz sampling frequency the time window length is 1.28 μs: the sweep time for class II-III jammers is of the order of tens of μsec and it is mandatory to have more than one window on a sweep time, to distinguish the frequency sweep of the jammer.

When a jamming signal is detected, the mitigation process is executed and so a STFT is performed. Initially, a portion of the signal is selected by multiplying the incoming signal with an Hanning window, then the FFT is done and, , the sample with the maximum amplitude is found. The blanking process consists zeroing both the frequency bins where the maximum amplitude has been found and its adjacent frequency bins. So, exploiting an IFFT it is possible to come back to time domain and finally interleaving the examined samples with the samples produced in the previous step; at this point the sliding window is shifted of one sample and the procedure is repeated.

This implementation corresponds with a Short Time Fourier Transform exploiting Hanning windows with an overlap factor of 1 sample, between windows of 32 samples. In Figure 6, a block diagram of the developed algorithm is shown.

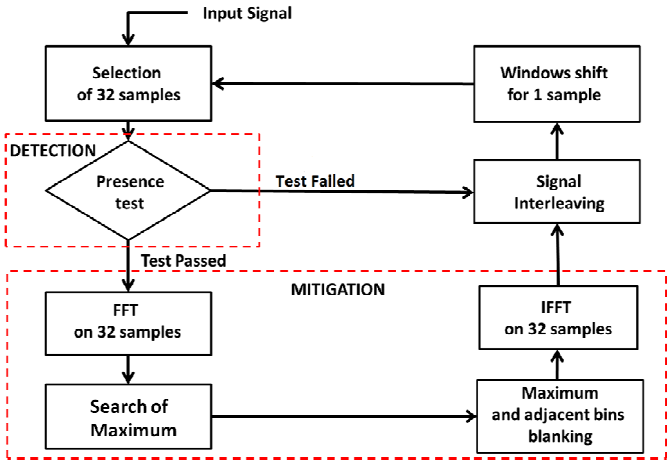

Fig. 6. Algortihm block diagram

In Figure 7 an example is shown of the spectrogram of a GPS jammed signal; in this case the jamming was produced by the jammer number 3 of Table I: this jammer transmits an unidirectional chirp signal with one saw-tooth function that has a sweep time of 11.71 µsec, with a bandwidth of 11.82 MHz. The signal is centered on IF (10 MHz) and GPS signal is between 9 MHz and 11 MHz, due to filtering; the presence of the filter is a hint of mitigation, because when the signal jammer is out of band, it does not disturb the original GPS signal. In this figure, the GPS signal is not visible, since its power level is much lower than the power of the jamming signal.

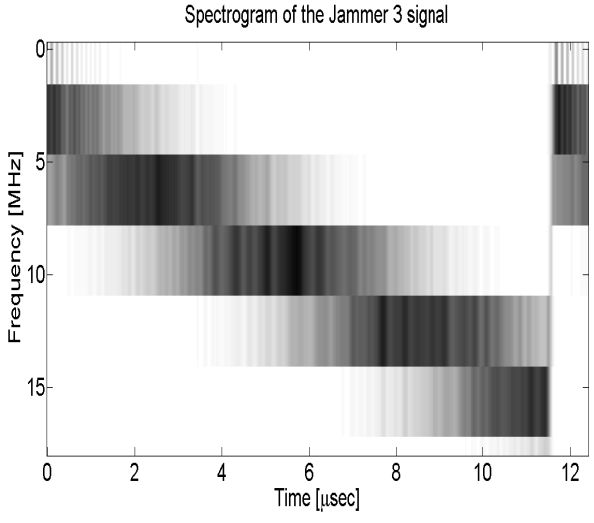

Fig. 7. Spectrogram of the incoming signal (jammer number 3)

In Figure 8 the spectrogram after the aforementioned mitigation technique is shown: in particular the jammer signal has been detected and mitigated and the GPS signal between 9 MHz and 11 MHz is visible.

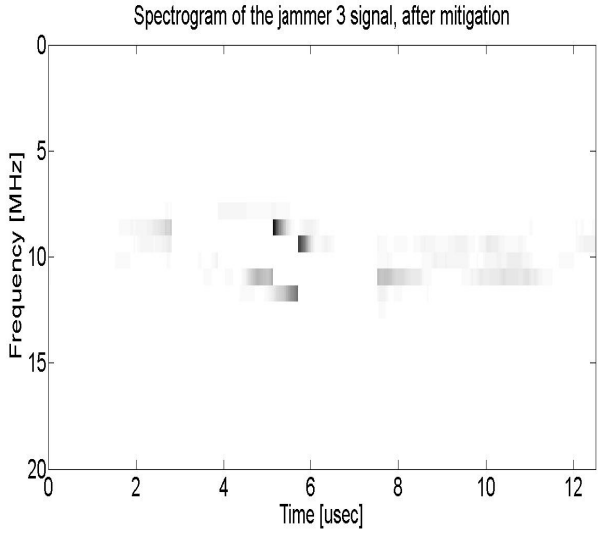

Fig. 8. Spectrogram of the mitigated signal (jammer number 3 case)

In Figure 9 the Peak to Side Lobe Ratio (PSLR) of the correlation function is shown (without and with mitigation). PSLR is performed in order to evaluate the performance of the mitigation algorithm. To obtain a good satellite acquisition a threshold of PSLR of 2.5 has been chosen. This figure is obtained perfoming 10 simulations of the detection and mitigation process. As shown in Figure 9 it is worth nothing that the mitigation algorithm applied has limited the jammer influence by reducing its coverage area from about 300 m to about 80 m. The vertical line in the figure represents D_{SAT} (4.1 m).

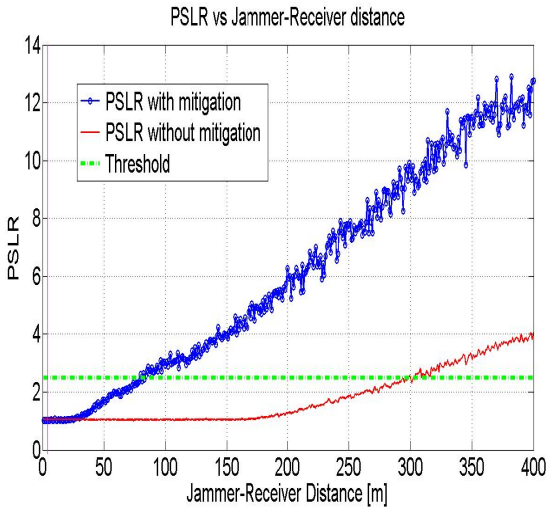

Fig. 9. Mitigation performance. PSLR of the correlation function for an acquisition threshold of 2.5

Table IV shows a summary of the performance improvement for various types of jammer, using this mitigation method, is shown .

The maximum distances within which the jammer disrupts the acquisition process are significantly reduced and the improvements are shown in terms of distance percentage change.

TABLE IV. PARAMETERS OF THE IN-CAR JAMMERS ANALYZED IN THE PAPER AND RESULTS

N	Class	P_T [dBm]	D_{SAT} [m]	D_{MAX} with no mitigation [m]	D_{MAX} with mitigation [m]	Improvement [%]
1	I	-12.1	5.3	298.9	3.5	98.82
2	I	-25.6	1.1	5.6	1	82.23
3	II	-14.4	4.1	288.7	80	72.29
4	II	-30.8	0.6	59.1	26	56
5	III	-19.3	2.3	73.4	14	80.91

V. CONCLUSIONS

A possible detection and mitigation strategy for in-car jamming has been presented. The technique is based on time-frequency analysis through the STFT transformation; the developed algorithm has been applied to signal produced by in-car jammers (transmitting both CW and chirp-signal depending on the specific jammer class).

For jammer number 1 and jammer number 2 (Table IV), that are CW jammers, the problem of missed acquisition vanish after mitigation because the maximum distance for acquisition disrupt (Dmax) becomes smaller than the maximum distance for the receiver saturation (Dsat).

For class II jammers (jammer number 3 and jammer number 4 (Table IV)) and for class III jammer (jammer number 5 (Table IV)), the maximum distance is significantly decreased.

REFERENCES

[1] T. Kraus, R. Bauernfeind, B. Eissfeller, "Survey of In-car jammers-Analysis and modeling of the RF signals and IF samples (suitable for active signal cancellation)", In Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011) September 20 - 23, 2011, pp. 430-435 Oregon Convention Center, Portland, Oregon Portland, OR.

[2] Data Sheet NI USRP-2920, www.ni.com/manuals, February 2014.

[3] Data Sheet L1A, www.gpssource.com/files/ , February 2014.

[4] Data Sheet A11, www.gpssource.com/files/, February 2014.

[5] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, S. H. Jensen, A software defined GPS and Galileo Receiver – A single frequency approach, Birkhauser ed, 2007.

[6] R. Bouernfeind, T. Kraus, A. Sicromoz Ayaz, D. Dotterbock, B. Eissfeller, "Analysis, Detection and mitigation of in car jammer interference in intelligent transport system", German Air and Space Congress 2012, Document ID 281260.

[7] L. Shen, Q. Yin, M. Lu, Q. Zhang, L. Guo, T. Shen, G. Zhao, S. Ning, Linear FM signal parameter estimation using STFT and FRFT, Chinese Journal Of Electronics, April 2013.

[8] Global Navigation Satellite System Manual, second edition, doc 9849 AN457, ICAO, 2012.