Designing of SDR Based Malicious Act: IRNSS Jammer

Priyanka L. Lineswala(✉) and Shweta N. Shah

Department of Electronics and Communication, SVNIT, Surat, India
plineswala@gmail.com, snshah@eced.svnit.ac.in

Abstract. Indian Regional Navigation Satellite System (IRNSS) is the regional navigation system designed by India which is identical to well-known Global Position System (GPS). The system promises to provide accurate Position, Velocity and Time (PVT) estimations. In future different applications of Internet on Things (IoT) like smart power distribution grids, sensor networking, vehicular network and airplane navigation systems will be depend on IRNSS. To provide reliable and faithful navigation service, IRNSS is developed by India. But it is highly susceptible to a range of threats like jammer. Here, the different types of jammers are classified in detail based on user, structure and signal. Such jammers are developed by Software Define Radio (SDR) just for experimental purpose. The empirical results are compared with jammer which is available in market.

Keywords: IRNSS · Jammer · Software Define Radio

1 Introduction

Precise location as well as accurate timing information is provided by Global Navigation Satellite System (GNSS). The usage of GNSS is not only for personal car and air craft navigation but, they can be employed for the tracking of birds and animals, to provide automation in different transport agency (like railway, ships) and defense applications. But accuracy and reliability (authority based permission) of such system are very important issues. To solve such issues, Indian Regional Navigational Satellite System (IRNSS) is developed by India. IRNSS from India and Quasi-Zenith Satellite System (QZSS) from Japan is independent and autonomous regional navigation system which provides accurate Position, Velocity and Time (PVT) same as GNSS.

In addition to this, new IRNSS applications are currently under development [1]. For example, IRNSS Satellites are launched and functioning of system is under observation. Some type of applications like "toll collection unit" needs to collect information of IRNSS users, which introduces privacy issues. This motivates the development and use of devices like jammer which can deny IRNSS signal reception.

Jammers are illegal but still in the market different types of jammer are easily available. Analyzing jammer is prerequisite to design detection and mitigation techniques of such intentional interference [2]. It is very smooth to analyze jammer if it is simulated on software. As software based simulations are easy to develop with low cost. Also, the major studies are carried out on software, provide flexibility and controllability.

Z. Patel and S. Gupta (Eds.): ICFITT 2017, LNICST 220, pp. 237–246, 2018.
https://doi.org/10.1007/978-3-319-73712-6_25

Here, the paper is focused on intentional interference like jammer for IRNSS L5 band [3]. The detail classification of jammer is also included. SDR based different experimental jammers are created using GNU and their signal characteristics are compared with original jammers [4]. From the analysis it emerges that the use of mitigation techniques, significantly improves the performance of satellite receivers even in the presence of strong malicious signals. This study is useful to develop mitigation technique by proper realize characteristics of jammer. Software based jammer provides the flexibility in parameters setting to prove the efficiency of any mitigation technique.

The rest of this paper is organized as follows. The classifications of jammers are mentioned in Sect. 2. The results of different SDR based jammers are described in Sect. 3. Also all of them are analyzed with the help of spectrum analyzer and parameters are compared in Sect. 4. Finally the result performance of the different jamming signal and future scopes are summarized.

2 Classification of Jammer

As mentioned in Fig. 1, the detail classification of jammers are done with different ways like based on user, based on physical structure and based on signal characteristics. Based on user, military jammers are available with larger size and civilian jammers are hand

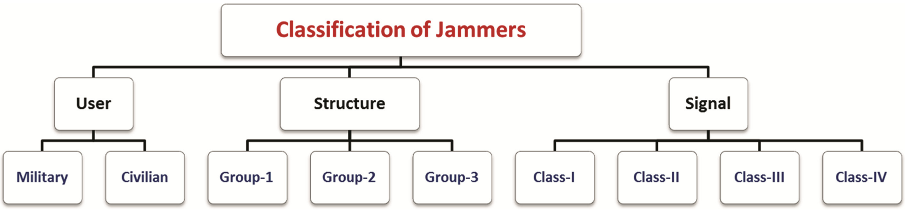


Fig. 1. Classification of jammers

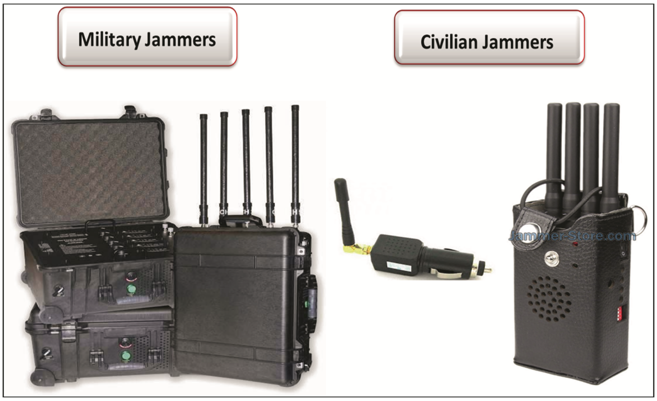


Fig. 2. User based jammer [6]

held device. The Fig. 2 shows the pictorial view of the military based jammers and civilian based jammers.

The requirement of structure depends on the complexity and quality of jammers. Such types of jammers are as shown in Fig. 3. Jammers with auxiliary power supply fall under group 1, jammers with rechargeable battery and external antenna known by group 2. The jammers with rechargeable battery and without external antenna are under group 3 which looks like mobile phone [5].

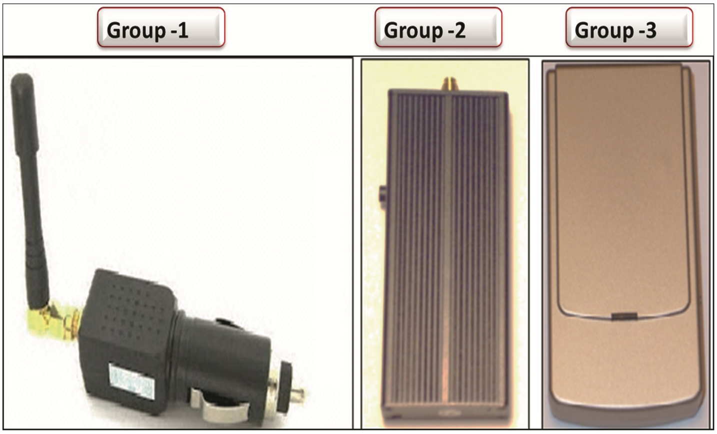


Fig. 3. Structure based jammer [7]

Based on signal, jammers can be classified as (i) Class I: Continuous Wave (ii) Class II: Chirp Signal with Single Saw Tooth (iii) Class III: Chirp Signal with Multiple Saw Tooth (iv) Class IV: Jammers with Frequency Burst. These all types of jammers can be implemented using hardware as well as software [8].

To analyze the jammer it is better to implement these jammers based on software compare to hardware. As software based implementation provides more flexible parameter like power level, frequency value, sweep rate etc. In general as per [9], different signals of jammer can be represented in time and frequency domain as shown in Fig. 5. Figure 4 shows different types of interference signals discussed and implemented here. The left hand side plots show the time domain signals while the right hand side plots refer to frequency domain representation of each signal.

Figure 4(a) illustrates a narrowband CW interference whose frequency is constant within the observation interval. It is a simple CW can be generated easily. Figure 4(b) is a multi-tone interference signal which consists of three frequency components. This type of signal can be generated using multiple signal waveforms with different frequencies. Figure 4(c) is a chirp interference signal whose instantaneous frequency linearly changes over time. Figure 4(d) is a sinusoidal pulse jammer with a 50% duty cycle. The frequency response of this jammer is wider than that of the narrowband CW signal. This type of interference can be generated by simple multiplication of CW with 50% duty cycle pulse or square wave.

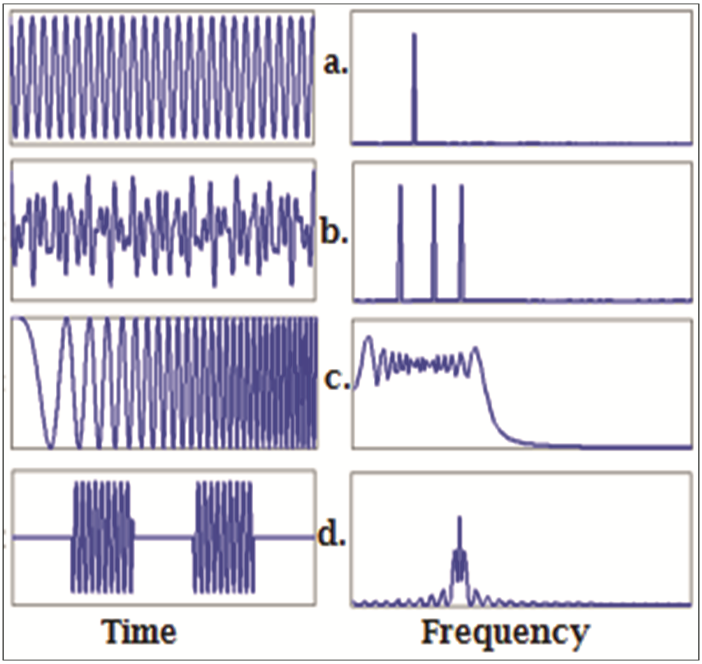


Fig. 4. Characteristics based jammer [9]

3 Implementation of Jammer Using SDR

The different jammers discussed in previous section are implemented by combination of GNU radio software [10] and Amitec SDR hardware [11]. The laboratory set up which was used to implement different class of jammer is as shown in Fig. 5. GNU radio generates jammer signal (laptop) whereas Amitec SDR hardware is transmitting these signals through the antenna. The jammer signal bandwidth and received power were measured by spectrum analyzer CXA N9000A of Agilent Technologies.

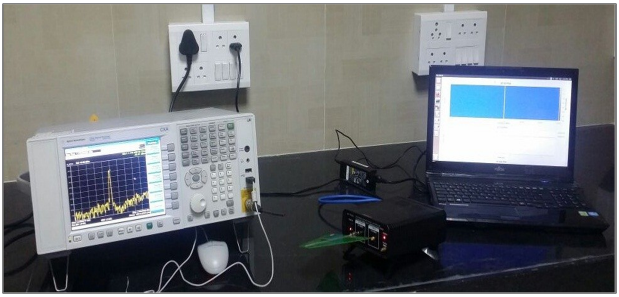


Fig. 5. Experiment setup in laboratory

The objective of this study is to use the GNU Radio Companion (GRC) tool to configure the SDR for generating different types of jammers of the IRNSS L5 band and then transmit these signals through the SDR transceiver into or nearer to IRNSS receiver. The SDR connections and settings should be correctly configured for the specified task. More details about SDR implementation is shown in process steps of Fig. 6.

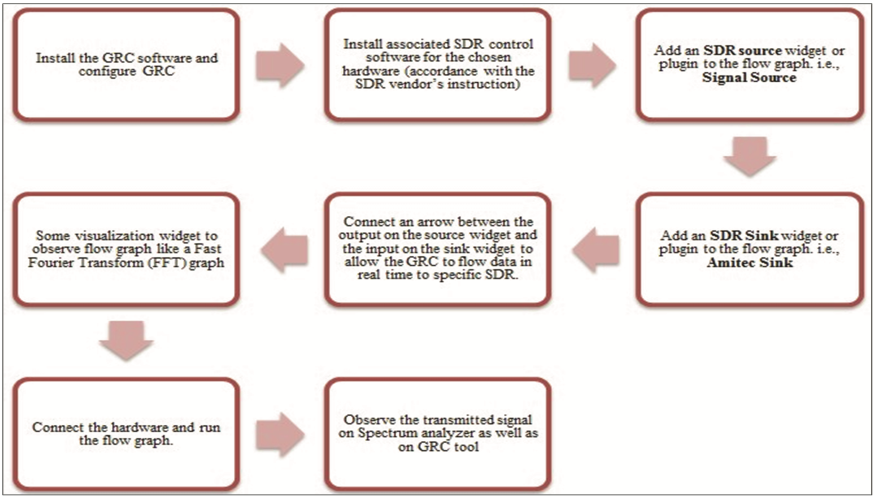
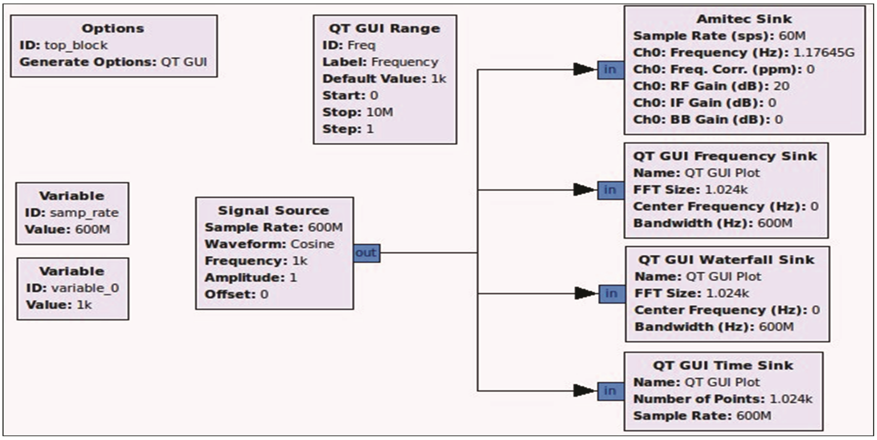

Install the GRC software and configure GRC
Install associated SDR control software for the chosen hardware (accordance with the SDR vendor's instruction)
Add an **SDR source** widget or plugin to the flow graph. i.e., **Signal Source**
Add an **SDR Sink** widget or plugin to the flow graph. i.e., **Amitec Sink**
Connect an arrow between the output on the source widget and the input on the sink widget to allow the GRC to flow data in real time to specific SDR.
Some visualization widget to observe flow graph like a Fast Fourier Transform (FFT) graph
Connect the hardware and run the flow graph.
Observe the transmitted signal on Spectrum analyzer as well as on GRC tool

Fig. 6. SDR implementation process flow

3.1 Class I: Continuous Wave Jammer

Simple continuous wave and multi tone jammers are implemented using GNU and SDR which transmit a signal frequency nearer to carrier frequency of IRNSS L5 band. The



Options
ID: top_block
Generate Options: QT GUI

QT GUI Range
ID: Freq
Label: Frequency
Default Value: 1k
Start: 0
Stop: 10M
Step: 1

Amitec Sink
Sample Rate (sps): 60M
Ch0: Frequency (Hz): 1.17645G
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 20
Ch0: IF Gain (dB): 0
Ch0: BB Gain (dB): 0

Variable
ID: samp_rate
Value: 600M

Variable
ID: variable_0
Value: 1k

Signal Source
Sample Rate: 600M
Waveform: Cosine
Frequency: 1k
Amplitude: 1
Offset: 0

QT GUI Frequency Sink
Name: QT GUI Plot
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 600M

QT GUI Waterfall Sink
Name: QT GUI Plot
FFT Size: 1.024k
Center Frequency (Hz): 0
Bandwidth (Hz): 600M

QT GUI Time Sink
Name: QT GUI Plot
Number of Points: 1.024k
Sample Rate: 600M

Fig. 7. SDR based single tone continuous wave jammer

flow graph for simulated jammer is shown in Fig. 7. Signal source generating cosine wave and transmit that signal with RF gain 20 dB and frequency 1.17645 GHz. As shown in Fig. 8, the jammer signal bandwidth and received power is measured by signal analyzer from jammer power spectrum. The measured signal bandwidth is around 1 kHz and received power is approximately −34 dBm. The value of bandwidth and power can be changed using GNU flow graph settings.

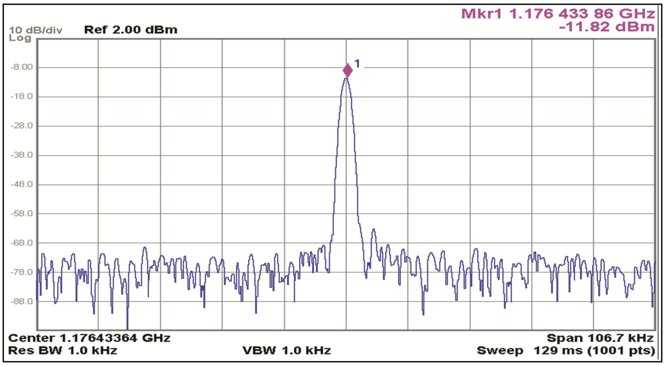


Fig. 8. Single tone CW jammer signal spectrum of IRNSS L5 band

As per [12] Fig. 9 shows same class I narrow band L1 jammer signal spectrum. The frequency of the class I cigarette lighter type PPDs jammer is very close to L1 whereas frequency of generated by SDR jammer is close to L5 based on IRNSS L5 band. The multi tone CW jammer is implemented same as the Fig. 7 but four signal sources are generating cosine wave compare to above single tone CW jammer. From the measured

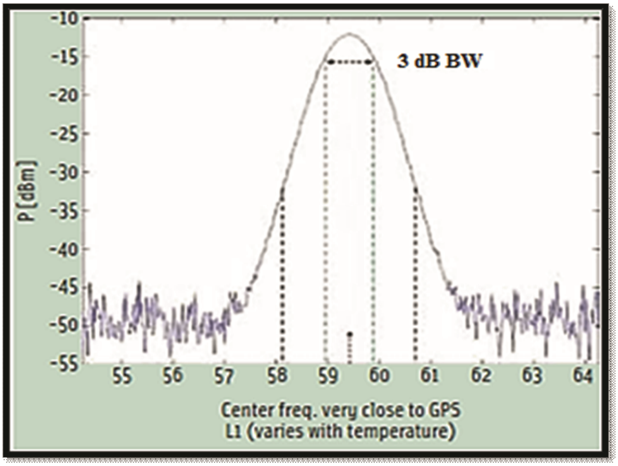


Fig. 9. Single tone CW jammer signal spectrum of GPS L1 band [12]

power spectrum of Fig. 10 power range from −60 dBm to −26 dBm with different peak level of multi tone jammer.

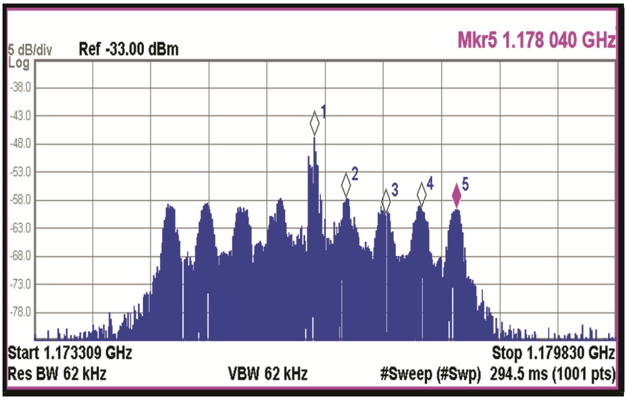
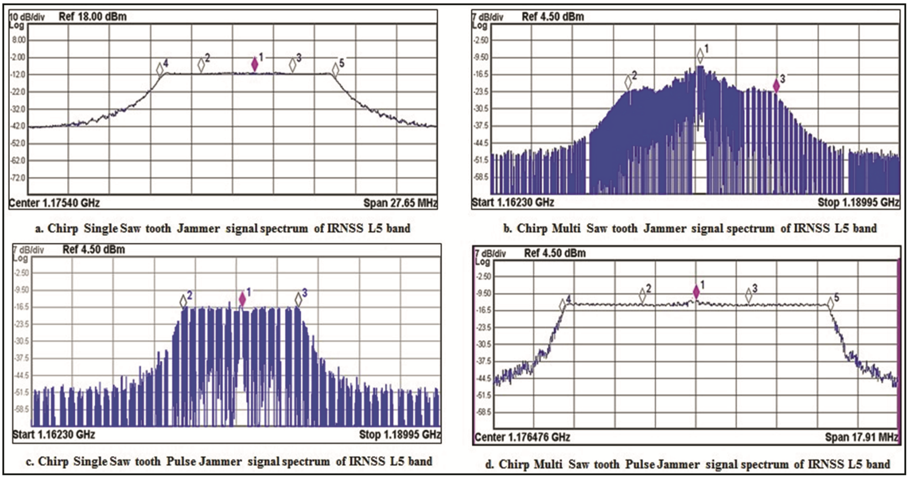


Fig. 10. Multi tone CW jammer signal spectrum of IRNSS L5 band

3.2 Class II: Chirp Signal with Single Saw-Tooth Jammer

This type of jammer signals are made up using Voltage Controlled Oscillator (VCO). Input voltage of VCO varies with a single saw tooth function and the frequency of saw tooth function decides the sweep rate of the resulting signal. However, the upper and lower voltage values decide the bandwidth of the jamming signal. Frequency components of these signals resonate between the higher and lower frequency value with a fix rate of change in frequency [8]. So, chirp signal are much more effective to interfere the navigation signals compare to class I jammer.



a. Chirp Single Saw tooth Jammer signal spectrum of IRNSS L5 band

b. Chirp Multi Saw tooth Jammer signal spectrum of IRNSS L5 band

c. Chirp Single Saw tooth Pulse Jammer signal spectrum of IRNSS L5 band

d. Chirp Multi Saw tooth Pulse Jammer signal spectrum of IRNSS L5 band

Fig. 11. Power spectrums of Class II, III, IV types of jammer

Here, the saw-tooth signal source is given to VCO and then VCO generates signal frequency of jammer in GNU flow graph. The measured signal bandwidth and power level is shown in power spectrum of Fig. 11(a).

3.3 Class III: Chirp Signal Multi Saw-Tooth Jammer

These signals are same as signal of chirp single saw tooth signals. So, this jammer is implemented same as single saw-tooth jammer using GNU and SDR. However, the multiplication of two saw-tooth signal sources are given to VCO and then VCO generates signal frequency of jammer. In the case of chirp single saw tooth signal it may be possible to detect it and mitigate through a proper technique. Whereas it is very difficult to mitigate multiple saw tooth chirp signals because one cannot predict the newer sweep rate and newer upper and lower value of the frequency [13]. The measured power spectrum of this implemented jammer is shown in Fig. 11(b).

3.4 Class IV: Chirp Signal with Frequency Burst Jammer

These types of jammers are made up of the same signals as it is of Class II or Class III jammers but such generated signals are multiplied with square wave of 10–15 kHz frequency. This multiplication provides burst of frequency and appears like on and off pattern of jammer signal. Also, the chirp signals gets on and off for limited time, in one second more than 10,000 times. These makes nearly impossible to mitigate jammer signals [13].

Square wave for the generation of burst signal is developed in a square wave generator and chirp signals generated independently. The multiplication of both signals is done which implement such jammer as shown in Fig. 12.

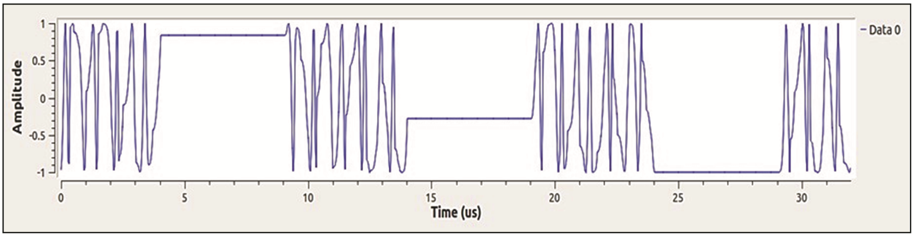


Fig. 12. Implemented chirp signal multi saw-tooth burst jammer

The measured power spectrum shown in Fig. 11(c) and (d) is used to analyze signal bandwidth and power level for the chirp single saw-tooth and chirp multi saw-tooth burst jammer respectively.

4 Analysis of Jammer Parameters

The interference suppression techniques are more beneficial to make reliable and accurate navigation receiver. The examination of these techniques with applications depends on the jammer class. Part of work focuses on implementation of several well-known class of jammer using GNU based SDR. To implement the different jammer support of mathematical equations are considered from reference [9]. In reference [8] jammer parameters are measured values of actual jammer.

So, validation of the work is shown in Table 1 by comparing the parameters of generated SDR jammer signal with reference [8]. The bandwidth values are closer to actual and also the power level controlled by GNU software provides more realistic for consideration.

Table 1. Validation of generated jammer signal parameters with reference [8]

Class	Name	Bandwidth	Power level [8]	Power level
I	Continuous Wave Jammer	~1 kHz	−12.1 dBm	−11.8 dBm
II	Chirp Signal with Single Saw tooth Jammer	~10 MHz	−14.40 dBm	−13 dBm
III	Chirp Signal with Multiple Saw tooth Jammer	~10 MHz	−19.3 dBm	−16.5 dBm
IV	Chirp Signal with Frequency Burst Jammer	~10 MHz	−9.5 dBm	−12.5 dBm

5 Summary

This paper has presented the development of SDR based all type of IRNSS jammers. The importance of navigation signal is based on their application. It is prerequisite to study jammer signal to make the navigation signal receiver robust and more secure against intentional interference like jammer. The brief examples were given to generate jammer based on SDR. Further, such implemented jammer provides parameter wise flexibility for further exploration of intentional interference in laboratory. This work is more useful to make advance research on effective real time mitigation technique for jammer.

Acknowledgements. The author would like to express their thanks to the scientist of SAC, ISRO and Amitec Pvt. Ltd. for their support provided to information about IRNSS and SDR respectively. Special thanks to Mrs. Darshna and Mr. Rutvij for the support provided during measurement campaign.

References

1. Indian Regional Navigation Satellite System: Signal in space ICD for Standard Positioning Services, Version 1.0, ISRO, IRNSS, June 2014
2. Ruparelia, S.M., Lineswala, P.L., Jagiwala, D.D., Desai, M.V., Shah, S.N., Dalal, U.D.: Study of L5 band interferences on IRNSS. In: Proceeding on International GNSS (GAGAN-IRNSS) User Meet, p. 45 (2015)
3. Dovis, F.: GNSS Interference Threats and Countermeasures. Artech House, Norwood (2015)
4. Mitch, R.H., Dougherty, R.C., Psiaki, M.L., Powell, S.P., O'Hanlon, B.W.: Signal characteristics of civil GPS jammers. In: ION GNSS, pp. 1–13 (2011)
5. Grabowski, J.C.: Personal privacy jammers. GPS World **23**, 28–37 (2012)
6. Military Convoy VIP Jammer. http://www.thesignaljammer.com/products/TSJ85W-Vehicle.html
7. Bauernfeind, R., Krmer, I., Beckmann, H., Eissfeller, B., Vierroth, V.: In-car jammer interference detection in automotive GNSS receivers and localization by means of vehicular communication. In: IEEE Forum on Integrated and Sustainable Transportation Systems, 29 June–1 July 2011, Vienna, Austria, pp. 376–381 (2011)
8. Bauernfeind, R., Kraus, T., Sicramaz Ayaz, A., Dtterbck, D., Eissfeller, B.: Analysis, detection and mitigation of InCar GNSS jammer interference in intelligent transport systems, ID: 281260, pp. 1–10. Deutscher Luft- und Raumfahrt kongress (2012)
9. Jahromi, A.J., Broumandan, A., Daneshmand, S., Lachapelle, G.: Vulnerability analysis of civilian L1/E1 GNSS signals against different types of interference. In: ION GNSS, Tampa, FL, pp. 1–10, 14–18 September 2015
10. GNU Radio. http://www.gnuradio.org/redmine/projects/gnuradio.html, http://www.gnuradio.org/redmine/projects/gnuradio/wiki/InstallingGR.html
11. SDR Lab. http://www.sdrlab.com/applications.htmlDd
12. Pullen, S., Gao, G.I.: GNSS jamming in the name of privacy- potential threats to GPS aviation, Inside GNSS Magazine, pp. 34–43, March–April 2012
13. Bauernfeind, R., Eissfeller, B.: Software-defined radio based roadside jammer detector: architecture and results. In: IEEE/ION Position Location and Navigation Symposium (PLANS), California, pp. 1–7, 5–8 May 2014