High Performance SDR for Monitoring System for GNSS Jamming Localization

Filip Šturc
Department of Radio Engineering
Czech Technical University
Prague, Czech Republic
sturcfil@fel.cvut.cz

Tomáš Morong
Department of Radio Engineering
Czech Technical University
Prague, Czech Republic
morontom@fel.cvut.cz

Pavel Kovář
Department of Radio Engineering
Czech Technical University
Prague, Czech Republic
kovar@fel.cvut.cz

Pavel Puričer
Department of Radio Engineering
Czech Technical University
Prague, Czech Republic
puricep@fel.cvut.cz

***Abstract*—This paper presents a basic description of a monitoring system which is designed for the GNSS jamming detection and localization as well as giving the theoretical issue together with specific consequences. The usage of that system is targeted to an aviation safety and space together with general transportation. The system is an extensive project, and this document is mainly about measuring station as an essential part of it. The paper presents specific localization techniques which will be used in digital signal processing. Several tests of the functionality of the measuring station have been made and presented in this paper. The result of the paper comes from the basic test of the measuring station. In that test, functionality - clock synchronization, mutual phase of an antenna array, software-defined radio was proved. The monitoring system is still developing and other important results will be described in the future.**

***Index Terms*—GNSS, jamming, detection, lokalization, receiver, measurement station**

I. Introduction

Global Navigation Satellite System (GNSS) determined for navigation around the world has been widely used for more than 20 years. Although the GNSS is considered as a reliable system in many fields, there is an important issue of vulnerability to radio frequency interference (RFI). Sources of radio frequency interference are classified as unintentional and intentional. Unintentional interference is produced by telecommunication or other wireless systems transmitting their signals on frequencies close to bands of GNSS. On the other hand, intentional interference namely jamming, meaconing and spoofing are due to humans [1].

The most common type of intentional interference is jamming [1], [2]. Jamming is usually a simple signal, which has an appropriate level into the same band or adjacent frequencies to the satellite navigation band of interest. It makes difficult or impossible to process GNSS signal. As a result, it has an adverse impact on the accuracy of position measurement. Devices designed for jamming, which are called jammers, dispose of different types of signals, for instance, narrowband noise, wideband noise, and tones [3], [4]. The most targeted bands are GPS L1 and Galileo E1 whose center frequency is 1575.42 MHz [3]. However, it is not a difficult task for specific jammers to adjust its center frequency or bandwidth of other systems such as BeiDou or GLONASS [4]. Available civil jamming devices and the effects on GNSS receivers were studied in [3], [5]. Meaconing is a more sophisticated type of jamming whose aim is to confuse GNSS users navigation in a particular area. The real GNSS signal is recorded and playback with power higher than the original signal [1]. As a consequence of the signal retransmission, it may be hardly detected [6].

There are two initiatives on why interference techniques are being used. Firstly, it is a defensive of own privacy such as truck drivers who do not want to allow their companies to monitor them on their way. Secondly, the more frequent case is to attack other's use of GNSS. This issue has occurred several times and it is considered as a serious cyber attack [7]. For example, an incident in 2009 at Newark Airport, Newark, USA, Federal Aviation Administration (FAA) revealed intentional jamming coming from a vehicle with low-cost jammer [8]. Other similar example happened in July 2013 in London [7]. Because of a wide range of jamming devices on e-commerce, which can be legally bought, there is a potential risk of using them deliberately in aviation and transportation in general. Based on this fact, it is necessary to propose a functional device in order to characterize, detect and localize interference sources.

To begin with, GNSS interference can be characterized and detected by different approaches as shown in detail in a study [4]. Interference detection can be executed by pre-despreading methods or post-despreading methods. Pre-despreading methods are basically done in frond-end stage whereas post-despreading methods are implemented after the correlation stage [9]. Those methods are based on the knowledge of

978-1-7281-2625-8/19/31.00 ©2019 European Union

the impacts on the individual stages of GNSS receivers. It is described in [4], [9], [10], [11]. One of the simplest non-realtime approaches of interference detection is an evaluation of post-correlation outputs particularly carrier to noise ratio C/No received from navigational data provided by the receiver. In addition, a study [12] exploits this approach for so-called test methods determined for testing of interference immunity of GNSS receivers.

Accurate localization of the interference source can be gained by folowing techniques described in [1], [14]

- Time Of Arrival (TOA)
- Time Difference Of Arrival (TDOA)
- Frequency Difference of Arrivar (FDOA)
- Angle of Arrival (AOA)
- Received Signal Strength (RSS)

In research [13] a concept of GNSS interference detection and localization were investigated. In this case, interference detection was done by Automatic Gain Control (AGC) monitoring concept as a suitable hardware indicator. This method is considered as a pre-despreading method and it was carried out by [4]. Interference localization in the concept presented in [13] is based on a hyperbolic localization with TDOA. The network design consists of a server which is responsible for data collection and processing, and a network of several stations spread in a particular area. As a result, this proposal concept is theoretically capable of localizing a considerable amount of interference sources.

Techniques which are currently suitable for our system are TOA and TDOA. Those techniques are briefly described bellow. Detailed information can be founbd in [14], [15].

A. TOA

Time of Arrival is frequently used and simple method intended to determine the position of electromagnetic radiation. It is based on knowledge of the time when the signal was transmitted, the time when the signal was received, and the speed of signal propagation. Then we are able to calculate distance from the point where the signal was received:

$$d = c * (t_{arrival} – t_{sent}) \tag{1}$$

Where c is the speed of light. While the distance is known set of possible locations can be determined (in two dimensions, it is a circle, in three dimensions, it is a sphere). In two dimensions we can formulate equation:

$$d = \sqrt{(x_{ref} – x)^2 + (y_{ref} – y)^2} \tag{2}$$

where x_{ref}, y_{ref} is the position of receiver. This set has to be calculated for several receivers (at least 3 in 2D, at least 4 in 3D) and the wanted position of the transmitter can be determined as the intersection of those sets [14], [16].

B. TDOA

Time Difference of Arrival is a more robust method than TOA because it does not require information about the exact time when the signal was transmitted from its source. It only needs to know the time when the signal was received and the speed of the signal propagation. When the signal is received by a pair of receivers, the time difference of signal arrivals can be used to determine the difference in distance between the source and the receivers:

$$\Delta_d = c * \Delta_t \tag{3}$$

where c is the speed of light and Δ_t is the time difference of signal arrivals. In two dimensions, the following equation can be formulated:

$$\Delta_d = \sqrt{(x_2 – x)^2 – (y_2 – y)^2} – \sqrt{(x_1 – x)^2 – (y_1 – y)^2} \tag{4}$$

where (x_1, y_1) and (x_2, y_2) are the known positions of receivers . This equation can be converted to the form of a hyperbola. When hyperbolas are calculated the position of the source can be determined by finding the intersection of them. In three dimension, it would be hyperboloids instead [14], [17].

II. The concept of the monitoring system

The system is a distributed network of remote measurement stations for monitoring GNSS interference. The network, which is shown in Figure 1. is based on three measurement stations, central clock synchronization, and a server. The advantage of using SDR is great flexibility allowing new methods for detection and localization of interference. The system support three principles of interference localization, namely Time of Arrival (TOA), Angle of Arrival (AOA) and Time Difference Of Arrival (TDOA). Currently, supported frequency bands are GPS L1 and Galileo E1. However, the hardware is designed universally to enable other GNSS bands. Signals are evaluated in PC in terms of easier programming and fast computing.

The interference detection system can be divided into subparts:

- SDR receiver - Each measurement station is based on a software defined radio (SDR) whose main task is the receiving of GNSS signals, signal digitalization.
- Data Transmission System - It is responsible for the transmission of the sampled data from the ADC converters from individual measuring stations to the server for further processing.
- Antenna array
- SDR Synchronization System – The task of this section is to ensure proper synchronization of the individual measuring station, respectively. SDR receivers, ADC converters and enable basic remote control of stations.
- Server – Server is an HW platform for data collection from individual measuring stations and signal processing.

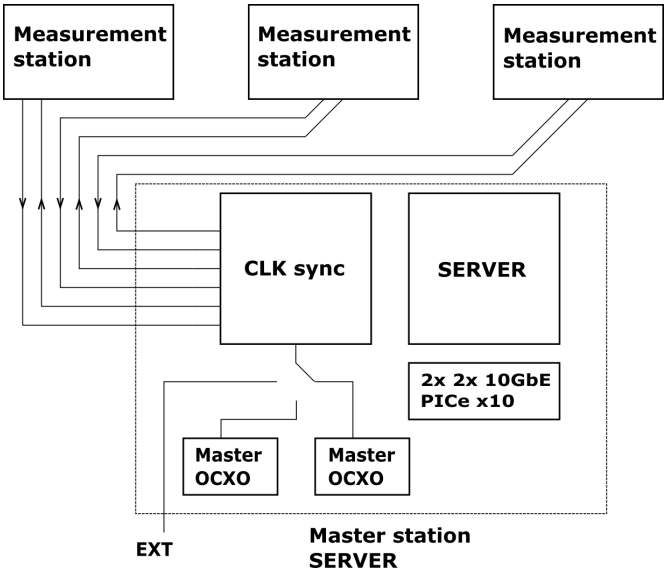

Fig. 1. Monitoring system

- Software block – It includes digital signal processing and evaluation of data from individual measuring stations and display of results.

The aim of the model is to optimize detector placement to achieve the highest level of protection for the protected object. The aim is to find the best location of measurement stations to minimize the likelihood of undetected interference in the protected area. In this case, as interference is considered the presence of a signal that degrades/disables the functionality of the GNSS systems.

A. Measurement station

The measurement station is divided into an analog section and a digital section as shown in Figure 2. The main function of the analog section is a preprocessing of GNSS signals from the antenna array. In each channel, there is a low-noise preamplifier, mixer, and an inter-frequency filter. This is followed by Automatic Gain Control (AGC) to automatically control the signal level before the digitalization.

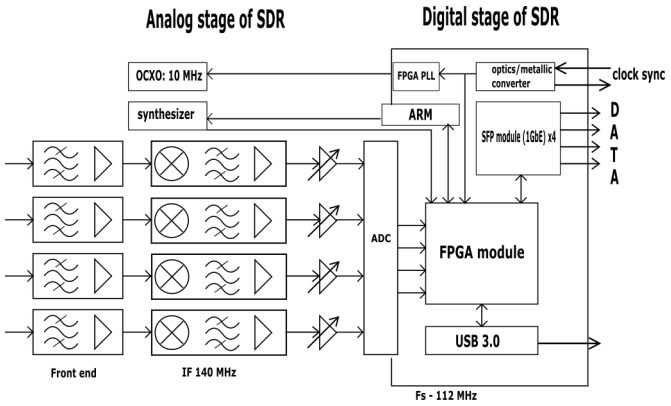

Fig. 2. Masurement station

The digitalization is performed by a four channel ADC converter. A frequency of the reference signal needed for analog mixers, which is derived from a synthesizer, is 336 MHz. It is configured by an ARM processor. Besides, the processor provides its internal temperature measurement and monitors the current consumption of the antenna array. Sampled data is routed to an FPGA module to preprocess it. The connection between the FPGA and the server is made by optical fibers.

B. SDR receiver

It is a receiver with one analog conversion to the intermediate frequency of 140 MHz. The receiver's frequency plan has been optimized so that the receiver can operate without internal interference of any civilian navigational frequency in the L band. The bandwidth of the IF filter has been proposed at 20 MHz from the center frequency. The transfer function is shown in Figure 3. A Surface Acoustic Wave (SAW) is used because of its minimum linear distortion in a passband and high slope of the transition characteristic. The 40 dB attenuation of the filter is achieved at ±26 MHz.

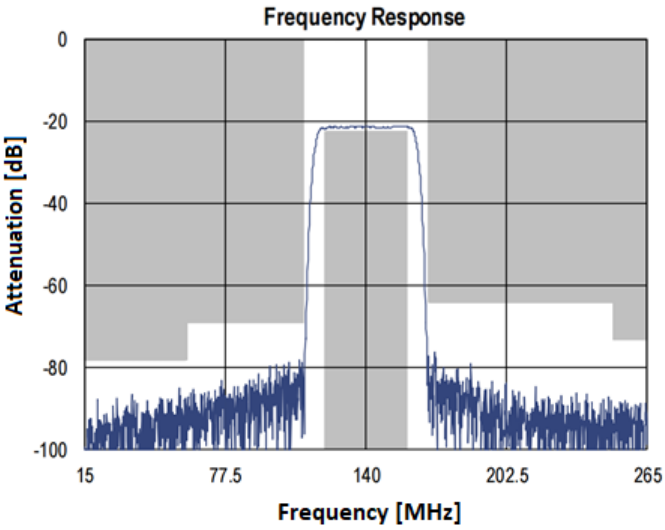

Fig. 3. Frequency response of IF filter

TABLE I
TABLE OF FREQUENCIES

f [MHz]	Label	Pass band		Stop band	
		f1 [MHz]	f2 [MHz]	f3 [MHz]	f4 [MHz]
1575.42	L1,E1	1555.42	1595.42	1549.42	1601.42
1227.6	L2	1207.6	1247.6	1201.6	1253.6
1176,45	L5,E5a	1156.45	1186.45	1150.45	1202.45
1207.14	E5b	1187.14	1227.14	1181.14	1233.14
1278.75	E6	1258.75	1298.75	1252.75	1304.75
1602	GL L1	1582	1622	1576	1628
1249	GL L2	1229	1269	1263	1275

C. Clock synchronization

Clock synchronization ensures the proper functionality of the entire system, and it is directly related to the achievable ac-

curacy of determining the arrival time of the TDoA signal and a directional targeting based on the interferometric principle. Synchronization sampling of all four channels (GNSS signals) from all measurement channels is required. A reference signal is distributed through electro-optical fiber optic converters on the server side and through the optoelectronic converter to the FPGA on the side of individual measuring stations. A phase discriminator, which is implemented in FPGA, measures the phase difference between the reference clock, the local clock signal, and converts it to a pulse-width modulation signal. This signal is modified by a low-pass filter so that its output voltage matches the range of the oscillator control input. The moment at which the reference and local signals are in phase is indicated by the output signal of a Locked phase generator.

D. Remote control of SDR receiver via synchronization channel

In order to remotely access the basic parameters of the SDR receiver a method of data communication among the server, the reference clock source and the measuring stations were integrated into the synchronization channel. The communication is based on a control of reference clock pulse width.

III. Testing of the Measurement Station

As it was mentioned above the whole monitoring system is comprehensive. Furthermore, it is necessary to verify each part individually. The first test, which has been made is based on collecting data from all four channels of the one measurement station. As a result, the functionality of the SDR receiver has been verified, and the Data Transmission System.

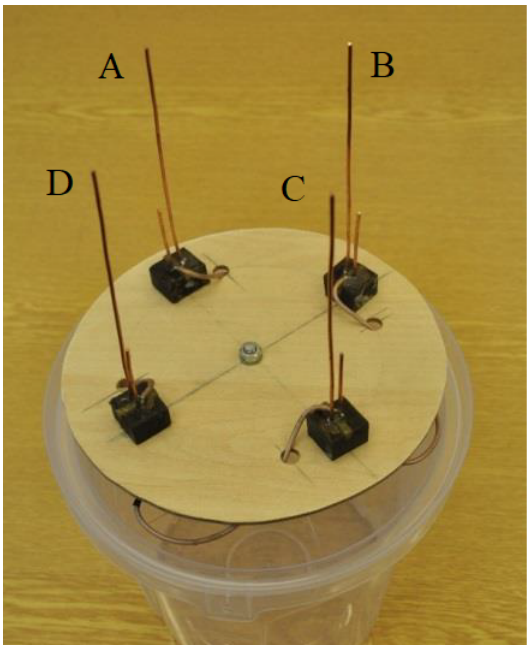

Fig. 4. The antenna array of the measurement station

Before using algorithms for localization mutual phases between individual antennas in the antenna array have to be processed. The antenna array used in the measurement station is shown in Figure 4. Data from different channels are received via optical fibers and evaluated in Matlab. The mutual phase is calculated via the following equations:

$$E_{AB} = \int_{-\infty}^{\infty} s_A(t) * s_B{}^*(t)dt \tag{5}$$

$$\varphi_{AB} = \frac{180}{\pi} arg\{E_{AB}\} \tag{6}$$

where E_{AB} is a mutual energy of signals $s_A(t)$ and s_B. Value φ_{AB} is the mutual phase. Te result of it is shown in Figure 5.

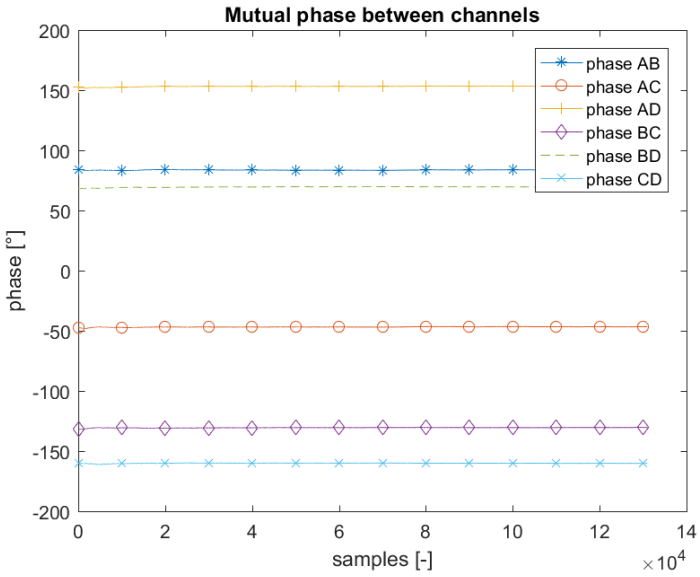

Fig. 5. Mutual phase

IV. Conclusion

We have presented a concept of the monitoring system, which is determined for GNSS interference detection and localization. The system is still developing, so only basic features and information were presented in this paper. The main object was a description of one measuring station with localization methods. Currently, the measurement station has been tested. The test of the measurement station is sufficient for verification of the functionality. The importance of a mutual phase, which is a result of an essential measurement, is a determination of a signal delay among channels. The future work will be focused on the final development of the entire monitoring system and advanced localization techniques.

Acknowledgment

This research is supported by the grant Strategic infrastructure protective system detecting illegal acts intentionally affecting GNSS signals No. VI2VS/439 of Ministry of Interior of the Czech Republic

REFERENCES

[1] A. G. Dempster and E. Cetin, "Interference Localization for Satellite Navigation Systems," Proc. IEEE, vol. 104, no. 6, pp. 1318–1326, 2016.

[2] M. Psiaki and T. Humphreys, "GNSS spoofing and detection," Proc. IEEE, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[3] R. H. Mitch et al., "Know your enemy: Signal characteristics of civil GPS jammers," GPS World, vol. 23, no. 1, pp. 64–72, 2012.

[4] D. R. DE SOUZA, ," IOSR J. Econ. Financ., vol. 3, no. 1, p. 56, 2016.

[5] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, "Impact and detection of GNSS jammers on consumer grade satellite navigation receivers," Proc. IEEE, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[6] D. Marnach, S. Mauw, M. Martins, and C. Harpes, "Detecting Meaconing Attacks by Analysing the Clock Bias of Gnss Receivers," Artif. Satell., vol. 48, no. 2, 2018.

[7] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS Receivers from Jamming and Interference," Proc. IEEE, vol. 104, no. 6, pp. 1327–1338, 2016.

[8] D. Guenter and J. Dennis, "Initial operational experience with CAT i Ground Based Augmentation System (GBAS)," ICNS 2015 - Innov. Oper. Implement. Benefits Integr. CNS Infrastructure, Conf. Proc., no. September, pp. S11–S114, 2015.

[9] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers," Proc. IEEE, vol. 104, no. 6, pp. 1233–1245, 2016.

[10] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," Proc. 2015 Int. Conf. Localization GNSS, ICL-GNSS 2015, pp. 1–6, 2015.

[11] F. D. Nunes and F. M. G. Sousa, "Jamming detection in GNSS signals using the sample covariance matrix," 6th ESA Work. Satell. Navig. Technol. Multi-GNSS Navig. Technol. Galileo's Here, NAVITEC 2012 Eur. Work. GNSS Signals Signal Process., 2012.

[12] T. Morong, P. Puričer, P. Kovář, "Study of the GNSS jamming in real environment", International Journal of Electronics and Telecommunications, vol. 65, no. 1, pp. 65–70, 2019.

[13] V. Pellegrini, F. Principe, A. Tomei, M. Mori, M. Natali, and R. Cioni, "The GNSS operative monitoring equipment (GNOME): An SDR-based solution for integrity assurance," 6th ESA Work. Satell. Navig. Technol. Multi-GNSS Navig. Technol. Galileo's Here, NAVITEC 2012 Eur. Work. GNSS Signals Signal Process., pp. 1–8, 2012.

[14] D. P. Young, C. M. Keller, D. W. Bliss, and K. W. Forsythe, "Ultra-wideband (UWB) transmitter location using time difference of arrival (TDOA) techniques," presented at Signals, Systems and Computers, 2003 The Thrity-Seventh Asilomar Conference on, 2003.

[15] G. Shi, Y. Ming, "Survey of Indoor Positioning Systems Based on Ultra-wideband (UWB) Technology" in Wireless Communications Networking and Applications, Springer, pp. 1269-1278, 2016.

[16] S. Bartl, P. Berglez and B. Hofmann-Wellenhof, "GNSS interference detection, classification and localization using Software-Defined Radio," 2017 European Navigation Conference (ENC), Lausanne, 2017, pp. 159-169.

[17] J. A. Bhatti, T. E. Humphreys and B. M. Ledvina, "Development and demonstration of a TDOA-based GNSS interference signal localization system," Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, Myrtle Beach, SC, 2012, pp. 455-469.