A Design of Anti-jamming Method Based on Spectrum Sensing and GNSS Software Defined Radio

Kwi Woo Park[1], *Min Joon* Lee[2], and *Chansik* Park[1,*]

[1]Chungbuk National University, Dept. of Electronics Eng., 28644 Cheongju, Republic of Korea
[2]Agency for Defense Development, 34186 Deajeon, Republic of Korea

Abstract. This paper presents result of new approach for anti-jamming using a method based on cognitive radio. To detect and get center frequency and bandwidth of jamming, a spectrum sensing based on multi-channel energy detector is implemented on the SDR. The SDR and a universal software radio peripheral is used to support real-time channel reconfiguration. And detected center frequency and bandwidth is used to select LO frequency to avoid jamming and receive GNSS signal. Then the receiver is reconfigured by the selected LO frequency. To verify the feasibility of the proposed anti-jamming process, position, carrier to noise ratio of each channel are measured using a test scenario that is consist of GPS and Beidou with a CW jamming. As a results, by switching of LO frequency, GNSS signal that is not affected by jamming can be received with the same performance as non-jamming.

1 Introduction

The GNSS signal is vulnerable to intentional and unintentional jamming, due to the extremely low receiving power of the satellite signal. To mitigate jamming, notch filter, pulse blocking, array antenna based nulling techniques were applied to many GNSS receivers [1]. However, when jamming mitigation method is used for GNSS receiver, signal power of the GNSS will be decreased. Sometimes, it may be efficient to receive GNSS signals in other bands that are not affected by jamming rather than when the jamming mitigation method was applied. The method can be realized using spectrum sensing and reconfigurable receiver based on SDR.

Recently, the GNSS software defined radio (SDR) has been widely used to develop and verify performance of GNSS signal processing algorithms for anti-jamming, multipath mitigation, multi-constellation and so on [2]. Because various algorithms can be applied easily in SDR without hardware modification. Furthermore, real-time operation of the SDR has been become possible with GPU-based signal processing. When the jamming is occurred in a GNSS band, the jamming status can be detected by spectrum sensing [3-4]. And the results are used to change channel of receiver to get other band signal which is not affected by jamming. This is an application of cognitive radio (CR) for GNSS anti-jamming. And we think this approach has been not attempted for GNSS anti-jamming.

This paper presents result of new approach for anti-jamming using a method based on cognitive radio. GNSS SDR is implemented using PC based on GPU and multi-core CPU. And a universal software radio peripheral is utilized as RF front-end. To detect jamming and check spectrum quality, a spectrum sensing based energy detector is implemented on the SDR. And estimated center frequency and bandwidth is used to select LO frequency for GNSS reception. To verify the feasibility of proposed method a test-bench was implemented. Using the test-bench, precision of position, carrier to noise ratio (C/N0) were observed on test scenario.

2 The SDR and spectrum sensing

2.1 Spectrum sensing

The concept of CR was proposed for efficient utilization of frequency in RF communication system [1-2]. When a primary user did not use a band, a secondary user can use the band for communication until that primary user re-use. To detect primary signal, the spectrum sensing technique is required for secondary user.

The energy detection (ED), matched filter, cyclostatio -nary, and so on are widely applied to spectrum sensing [3]. Among these technique, the energy detection is most suitable for the jamming signal detection of GNSS receiver that the jamming signal is assumed unknown signal. Because ED does not require prior information of jamming signal such as center frequency, bandwidth, modulation method, and so on.

$$H(t) = \begin{cases} h_1 & |s(f)|^2 > \lambda \\ h_0 & |s(f)|^2 \le \lambda \end{cases} \tag{1}$$

[*] Corresponding author: chansp@cbnu.ac.kr

https://doi.org/10.1051/e3sconf/20199403004

The concept of ED is that state of band is divided into jamming or non-jamming by energy measurements of spectrum. The concept can be expressed in Eq. (1). Where, h_1 means that jamming exist on band f, h_0 means non-jamming. And λ is threshold.

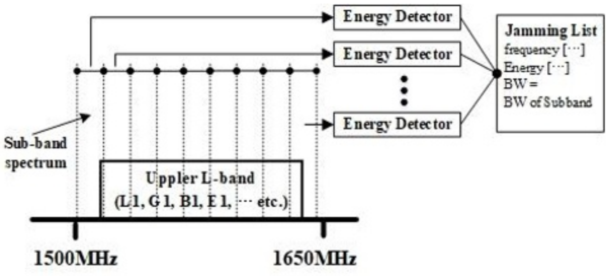

Fig.1. Multi-channel joint energy detector for GNSS receiver

The ED can be expand as multi-channel joint detection to detect jamming signal on wide-band spectrum for multi-channel receiver [4]. In the multi-channel joint method, an acquired wide-band spectrum is divided into several sub-band spectrum that size is smaller than original spectrum like figure 1. Then each sub-band spectrum is inputted to each energy detector. In the other research [4], each output of many energy detectors are combined some method such as OR rule.

In proposed anti-jamming process, each outputs are not integrated. Each output has center frequency and average of energy for sub-band spectrum. This information is useful to find frequency and bandwidth of the jamming signal. And the information is utilized to find another band that is not affected by jamming. In this method, accuracy of the estimated frequency and bandwidth of detected jamming signal will be depend on size of sub-band spectrum.

2.2 The implemented SDR software

In the receiver based on CR, channel flexibility is very important specification to change reception channel according to result of spectrum sensing in real-time. The SDR has been known that is most suitable for CR application. Because, most signal processing of the SDR is designed based on software using general purpose processor.

In our laboratory, a SDR has been designed and implemented to utilize development of anti-jamming, analysis of receiving environment, and multi-constellation positioning algorithms [5] since 2013. The SDR has been operated on high performance PC based on CPU and GPU. And the signal processing can be performed by parallel processing in real-time with 65 GNSS channels. The GUI of implemented SDR software is shown figure 2. Currently, GPS L1 C/A, Beidou B1I, B2I, GLONASS L1 and L2 signal can be received in our SDR. And navigation solution is determined by single GNSS measurements or all measurements of enabled-GNSS in SDR.

In this paper, the proposed anti-jamming process based on CR is implemented on the SDR to support channel reconfiguration. In the SDR, receiver channel can be switched using local oscillator (LO) frequency which is used to convert RF to intermediate frequency (IF). If the LO was changed, correlator, bit extractor, replica generator, and so on are auto adapted to receive GNSS signal that IF is changed. Then we can obtain useful results for performance analysis such as correlation output, C/N0, navigation solution, bit sequence, and so on from the SDR.

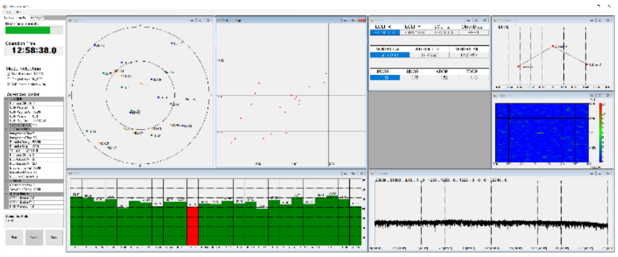

Fig. 2. GUI of implemented GNSS SDR

2.3 Reconfigurable RF front-end

By the implementing based on SDR approach, many signal processing module have been high flexibility. But because of most RF front-end will be fixed to fit a special band, implementation of CR-based receiver was difficult. Where, the RF front-end means a hardware part that down conversion, analog to digital conversion, and filtering such as image rejection is performed in the receiver.

Fortunately, a general purpose RF front-end with high flexibility was researched and developed along with the progress of SDR research and development. There is a Universal Software Radio Peripheral (USRP) that made by Ettus[6] as a typical general purpose RF front-end. The USRP can modify LO frequency of down converter, sampling rate of ADC, and gain of amplifier. In addition, the reception band can be changed without hardware modification. The reconfigurable parameters are set by function based on software such as USRP hardware driver (UHD) or GNURadio [6]. As the utilization of USRP and UHD, the implemented SDR software can get digital IF signal in real-time. And the reception channel of the SDR can be reconfigured in real-time.

3 A proposed method of anti-jamming

3.1 A process of anti-jamming based on CR

The concept of proposed anti-jamming is selection of LO frequency to reject bands that is occupied by jamming and to protect other GNSS bands that is not affected by jamming. For the proposed method to be realized, the information of the jamming must be measurable using the spectrum at the receiver. To do this, we added a spectrum acquisition and spectrum sensing to the anti-jamming process.

The GNSS services have been distributed and operating over a wide range of 500MHz bandwidth from GLONASS G1 (1602MHz) to GPS L5 (1175MHz). To scan all services requires a wide-band spectrum of 500MHz bandwidth. However, this spectrum cannot be obtained at once from a typical receiver. Because reception bandwidth of receiver should be limited to tens MHz. In this paper, sweeping the LO frequency and combining each spectrum were applied to obtain the wide-band spectrum. When each spectrum was combined, the overlap method was applied to improve accuracy of wide-spectrum [7]. The execution time and accuracy of implemented wide-band spectrum acquisition will be vary depending on the LO frequency sweep interval and the overlap ratio. The sweep interval is determined by sampling rate of receiver or reception bandwidth.

The spectrum sensing is performed based on multi-channel energy detection method mentioned in section 2. If the obtained wide-band spectrum includes one or more signal that have higher energy than threshold, by the spectrum sensing, number of sub-bands, the center frequency of each sub-band, and the average energy are measured. These information are considered to frequency bandwidth, and number of the jamming signals.

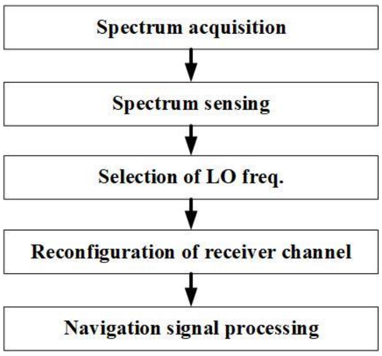
Spectrum acquisition
Spectrum sensing
Selection of LO freq.
Reconfiguration of receiver channel
Navigation signal processing

Fig. 3. Flow chart of proposed anti-jamming.

Based on the jamming information obtained from spectrum sensing, the LO frequency that can minimize the impact of jamming and receive GNSS signals can be selected by proposed method. Then receiver channel is reconfigured. The receiver performs signal processing operations for the available GNSS satellite signals in accordance with the reconstructed parameters. If more than four satellite signals are acquired, the navigation solution is also calculated. The proposed anti-jamming process can be summarized as shown in figure 4.

Using this method, the minimum power of the jamming signal that can be avoided is dependent on the performance of the spectrum sensing. Also, the maximum power of the jamming signal that can be avoided will be determined by the dynamic range of receiver. And in this process, the receiver must find the optimum LO frequency for continuous navigation. We propose a method to find the appropriate LO frequency using the LO frequency range model that determines which GNSS is available and the LO frequency range model that determines not to receive jamming signals.

3.2 Selection of LO frequency

Eq. (2) means range of LO frequency to receive GNSS signal. We get the LO frequency range using Eq. (2), when center frequency of GNSS signal and bandwidth was given. The signal information is known for anyone. In Eq. (2), f_{Gx} is center frequency of a GNSS signal, B_{G} is bandwidth of a GNSS signal, and B_{R} is bandwidth of receiver that is determined by sampling rate and pass band of filter. By the Eq. (2), if the LO frequency is included in range which is defined by a signal's frequency and bandwidth, the signal can be received.

$$\begin{gathered} f_{Gx}+B_{Gx}/2-B_R < \; f_{LO,Gx} \; < f_{Gx}-B_{Gx}/2 \\ f_{Gx}+B_{Gx}/2 < \; f_{LO,Gx} \; < f_{Gx}-B_{Gx}/2+B_R \end{gathered} \qquad (2)$$

The LO frequency range model is applied to make a function that can output 1 or 0 according to probability of the GNSS reception. The function (W_{Gx}) can be shown Eq. (3). Where, Gx means name of GNSS service such as GPS, Beidou, GLONASS, and so no. hat of f_{LO} is selected LO frequency.

$$W_{G_x}(\hat{f}_{LO}) = \begin{cases} 1 & (\hat{f}_{LO} \in f_{LO,G_x}) \\ 0 & (\hat{f}_{LO} \notin f_{LO,G_x}) \end{cases} \qquad (3)$$

If there are two or more GNSS were considered to select LO frequency, several W_{Gx} will be defined with its center frequency and bandwidth. Then all W_{G} are integrated by weighting sum. At this time, the weight values can be designed by a parameter of each GNSS system's performance such as error variance, visible number of satellites. And sum of weight values should be 1. If the weight values are determined by visible number of satellites of each GNSS, The product of integrated W_{G} and sum of all expected number of satellites means an estimation model for the number of satellites that can be received according to the LO frequency.

$$\begin{gathered} f_{LO,n} < f_{J,n} - (B_R + B_{J,n}/2) \;\; or \\ f_{LO,n} > f_{J,n} + (B_R + B_{J,n}/2) \end{gathered} \qquad (4)$$

To reject jamming signal, a range of LO frequencies can be obtained by Eq. (4). Where, $f_{\mathrm{J,n}}$ and $B_{\mathrm{J,n}}$ are center frequency and bandwidth of *n*th jamming signal, respectively. And a function that outputs 1 or 0 according to the probability that the jamming signal is excluded is derived as shown in Eq. (5).

$$W_{J,n}(\hat{f}_{LO}) = \begin{cases} 0 & (\hat{f}_{LO} \in f_{LO,n}) \\ 1 & (\hat{f}_{LO} \notin f_{LO,n}) \end{cases} \qquad (5)$$

When two or more jamming exists, all W_J be combined by OR rule to obtain a range of LO frequencies that do not receive all jamming signals.

$$f'_{LO} = mean(\arg\max[W(\mathrm{f}_{LO})]) \qquad (6)$$

Finally, the production W_G and W_J is a function (W) that can find LO frequency to get GNSS signal and to reject jamming signal. When all LO frequency candidates

($\mathbf{f}_{\mathrm{LO}}$) are inputted to W, The LO frequency that the highest value is calculated by the function is the optimal LO frequency. If there are two or more optimal LO, the final value is calculated by average.

4 Experiment

4.1 Test-bench

The test-bench was implemented using the LabSat, USRP, Signal generator, and a combiner. Figure 4 shows the implemented test-bench. We used the test-bench to verify the performance and validity of proposed anti-jamming based on CR.

To monitor performance changes as the LO frequency changes, repeated experiments with the same RF signal are required. The LabSat records live GNSS signal and then replay them as RF GNSS signals. Therefore, GNSS signals are supplied from LabSat. The jamming signals were generated using HSG-D2000A, a signal generator made by HP. This signal generator can generate signals such as CW, FM, and AM with power of -135dm to -15 dBm in 250 kHz to 2GHz.

The jamming signal and the GNSS signal are combined by the combiner, and the combined signal is entered into the USRP. USRP sends IF digital signals to PCs in real time, and SDR software receives these signals and performs GNSS signal processing. The proposed anti-jamming method is also implemented in this process.

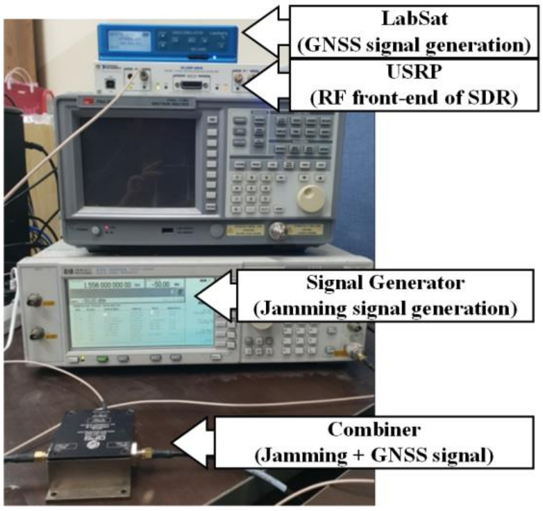

Fig. 4. A **c**onfiguration of test-bench.

4.2 The result of a test scenario using GPS and Beidou with a jamming

A test scenario was defined using GPS L1 C/A, Beidou B1I and a single jamming signal. This scenario is used to confirm the validity of the proposed anti-jamming process. GPS L1 C/A exists at 1575.42 MHz and assumes approximately 2 MHz bandwidth. Beidou B1I exists at 1561.098 MHz and assumes approximately 4 MHz bandwidth. On the other hands, the jamming will be occurred in 1561.098 that is same to Beidou B1I signal. The jamming method is CW type is used, and the signal power is set to 50dB jamming to signal ratio. It means that power of jamming signal is higher than noise power over 30dB. Directly affected by this jamming signal, the GNSS is not available.

The parameters of wide-band spectrum acquisition, spectrum sensing, and SDR are summarized in Table 1. The range of wide spectrum is set to 1540 to 1580MHz, and overlap ratio is 0.5. Because the sampling rate is 20MHz, bandwidth of receiver is determined as 10MHz. In this case, wide-band spectrum is obtained by the LO frequency sweep eight times and computation of narrow spectrum. A spectrum of 40MHz bandwidth is divided into 1MHz units to perform multi-channel energy detection.

Table. 1 The parameters for the test scenario

Parameter name	value
Range of spectrum[MHz]	1540 to 1580
Overlap ratio	0.5
Bandwidth of sub-band of ED[MHz]	1
Threshold of ED[dB]	-170
Sampling rate[MHz]	20
Quantization bit	16

The scenario was replayed for about three minutes. We tested three situations repeatedly when there was no jamming (Non-jamming), when jamming existed, when the anti-jamming method was applied (Anti-jamming turn on), and when anti jamming was not applied (Anti-jamming turn off).

First, we introduce the results of spectrum sensing. Figure 5 shows the results of spectrum sensing based on multi-channel energy detection when jamming is exist. Because 40MHz bandwidth is divided into 1MHz intervals, a total of 40 energy measurements can be obtained. Each energy measurement corresponds to the respective center frequency. The threshold value is -170 dB. As a result, a jamming signal was detected in the sub-band spectrum with a central frequency of 1560.5 MHz. At this point, the energy measurement is -160.7 dB, about 20 dB higher than the other sub-band spectrum, which is not affected by jamming. This result means that even 40 dB jamming to signal ratio can be found without false alarms.

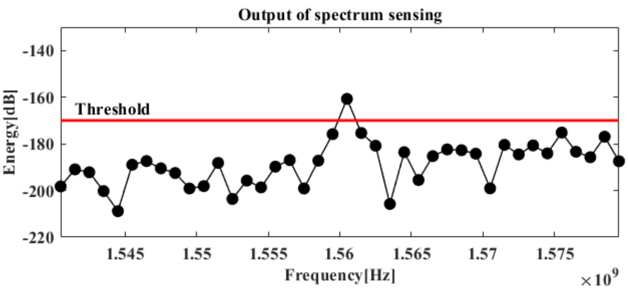

Fig. 5. A result of spectrum sensing

Figure 6 shows the appropriate LO frequency found based on the spectrum sensing results. In figure 6, red dot means that LO frequency is selected by proposed Eq. (6).

Where the y-axis is the output of function W, which means that it is capable of receiving GNSS signals. A value of 0.5 means that only one system of two systems, GPS and Beidou, can be received. And y value of different LO frequencies from 1572MHz to 1584MHz are equal. The average of these values is the final LO frequency, it is 1578 MHz.

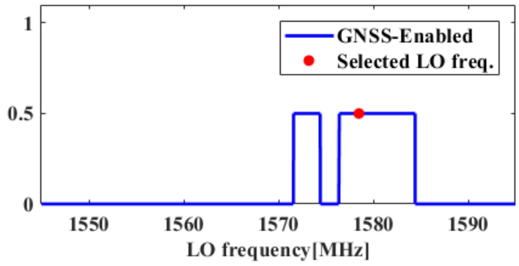

Fig. 6. A result of LO frequency selection

In non-jamming situations and situations where Anti-jamming does not apply, the LO frequency is set to 1568MHz. In this case, GPS and Beidou signals can be received simultaneously at 10 MHz bandwidth. Figure 7 shows that when there is no jamming, a total of 15 satellite signals are received by successfully receiving both GPS and Beidou. However, in the situation that jamming is occurred, keeping the LO frequency will make loss most satellites signal such as yellow bar in figure 7.

On the other hands, a case of that the selected LO frequency was applied to receiver channel by the proposed method can provide navigation solution using only GPS signal. This is because the LO frequency with only GNSS signals is properly found except for the band affected by jamming. As a result, 8 GPS satellite signals were received. At this time, C/N0s of each signal were only 0.3 dB different from the non-jamming situation. It is not possible to eliminate the jamming effect of a Beidou signal, but simply changing the LO frequency makes the GPS signal available.

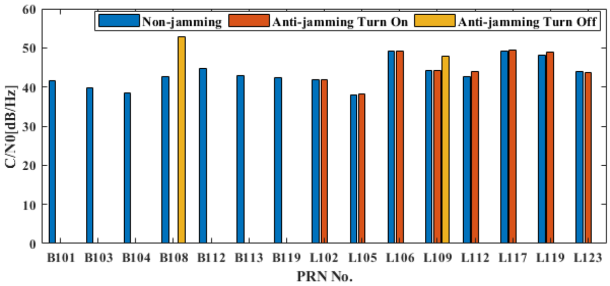

Fig. 7. C/N0 of all received signals for three situations: non-jamming, anti-jamming turn on or off

Table 2 summarizes the precision of navigation solution measured in each situation. The receiver position was calculated in the two situations of non-jamming and anti-jamming turn on. The precision is measured based on CEP. As a result, precision of non-jamming situation that GPS and Beidou is used to calculate position of receiver is 3.3m, and in the other case only GPS is used is 3.45m.

The CR-based anti-jamming that we proposed does not mitigate the jamming effect of Beidou. But just switching of LO frequency, GPS signal can be received with the same performance as non-jamming.

Table. 2 The position precision (CEP) in each situation

Situation	Precision [m]
Non-jamming(GPS/Beidou)	3.3
Anti-jamming On(Only GPS)	3.45
Anti-jamming Off	-

5 Conclusion

This paper presents result of anti-jamming based on CR. The process of anti-jamming is consist of 5 step such as spectrum acquisition, spectrum sensing, selection LO frequency, receiver channel reconfiguration, and navigation. The spectrum acquisition was implemented based on sweeping and overlap method, and the multi-channel energy detector is used for spectrum sensing.

The LO frequency selection method is proposed in this paper, the method can determined a LO frequency that GNSS can receive and jamming can reject. The receiver channel reconfiguration was implemented using SDR software and USRP. And the navigation signal processing for GPS, Beidou, and GLONASS be supported in SDR.

A test-bench was implemented using the LabSat, USRP, Signal generator, and a combiner. The proposed anti-jamming process was verified based on a test scenario using GPS and Beidou with a jamming signal. As a result of the experiments, the proposed method does not mitigate the jamming effect of attacked GNSS. But just switching of LO frequency, GNSS signal that is not affected by jamming can be received with the same performance as non-jamming.

Acknowledgments

This work has been supported by the National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

References

1. Septentrionv, "Septentrio white paper GNSS Interference", www.septentrio.com, (2012)
2. S. Söderholm, M. Bhuiyan, S. Thombre, L. Ruotsalainen, & H. Kuusniemi, A multi-GNSS software-defined receiver: design, implementation, and performance benefits, Annals of Telecommunications, **71**, 399-410 (2016)
3. M. Ben R Z. Quan, S. Cui, A. Sayed & H. Poor, Optimal multiband joint detection for spectrum sensing in cognitive radio networks. IEEE Transactions on Signal Processing, **57**, 1128-1140 (2009)

4. T. Yucek, & H. Arslan, A survey of spectrum sensing algorithms for cognitive radio applications, IEEE communications surveys & tutorials, **11** (2009)
5. K. Park, J. Chae, S. Song, S. Son, S. Choi, & C. Park, A Performance Analysis of Multi-GNSS Receiver with Various Intermediate Frequency Plans Using Single RF Front-end, Journal of Position, Navigation, and Timing, **6**, 1-8 (2016)
6. Ettus research, USRP Hardware Driver and USRP Manual[Internet], cited 2018 Sep 12, available from: http://files.ettus.com/manual/index.html
7. W. Liu, O. Yaron, I. Moerman, S. Bouckaert, B. Jooris, Real-time wide-band spectrum sensing for cognitive radio, *In Communications and Vehicular Technology in the Benelux* (SCVT), 1-6 (2011)