GNSS Cloud-Data Processing Technique For Jamming Detection And Localization

Jung-Hoon Lee, Hyeong-Pil Kim, Jong-Hoon Won

GNSS cloud-data processing technique for jamming detection and localization

Jung-Hoon Lee, Hyeong-Pil Kim, Jong-Hoon Won, *Inha University*
Email: jh.won@inha.ac.kr

BIOGRAPHIES

Jung-Hoon Lee is currently in the Master's Course in the Department of Electrical Engineering at Inha University, Korea. He received B. S. degree at the same department in 2017. His research interests include GNSS receiver signal processing, Cospas-Sarsat system, Anti-Jamming technology, and A-GPS.

Hyeong-Pil Kim is currently in the Master's Course in the Department of Electrical Engineering at Inha University, Korea. He received B. S. degree at the same department in 2017. His research interests include GNSS receiver signal processing, and Anti-Jamming technology.

Jong-Hoon Won received the Ph.D. degree in the Department of Control Engineering from Ajou University, Korea, in 2005. After then, he had worked with the Institute of Space Technology and Space Applications at University Federal Armed Forces (UFAF) Munich, Germany. He was nominated as Head of GNSS Laboratory in 2011 at the same institute, and involved in lectures on advanced receiver technology at Technical University of Munich (TUM) since 2009. He is currently an assistant professor of the Department of Electrical Engineering at Inha University. His research interests include GNSS signal design, receiver, navigation, target tracking systems and self-driving cars.

ABSTRACT

In this paper, assuming that a jammer is located in an area where a large number of low-cost GNSS receivers are densely distributed over and their received signals are gathered into a central processing unit like a cloud-data, we propose a 2-dimensional time-frequency correlation method for the cloud-data which can determine the type of jamming signal and estimate the jammer's position. This method is applied for examining the similarity between arbitrary two signals acquired from different receivers, thereby discriminating the presence and the type of a jamming signal in the time-frequency domain and also estimating the jammer's position. The availability of the proposed method is examined by a numerical simulation, where 15 GNSS receivers are randomly placed at the certain distances that range from 100 [m] to 300 [m] from the jammer, so that the jamming to signal ratio(J/S) at the receiver varies as distance increases. Finally, we analyze the results of the time-frequency correlation method to confirm that the jamming signal can be detected and the position of the jammer can be estimated.

1 INTRODUCTION

For the modern human life, the Global Navigation Satellite System (GNSS) is an essential element to provide accurate location-based services with worldwide coverage. However, the satellite signal used in GNSS is vulnerable to jamming because intrinsically it has a very low signal power level on the surface of the earth by being transmitted from satellites at an altitude of about 20,000 [km]. In order to solve this problem, a lot of research has been performed, and recently, as the price of the GNSS receiver gradually decreases due to the development of technology, methods using data acquired from a large number of GNSS receivers have been proposed.

In [1] and [2], researchers proposed an idea for detecting the interference signal and estimating the location of the interference source through a number of independent monitoring stations consisting of low-cost antennas and front-end modules distributed over a certain region. Here, the interference signal was detected based on the automatic gain control (AGC) measurement, and the position of the interference source was estimated using the AGC output and the time difference of arrival (TDOA) between the signals of the monitoring stations. Experiments using 4 monitoring stations showed that the result of the TDOA based localization had an about 80% reduced estimation error than that of the AGC output-only based method.

In [3] and [4], the author proposed so-called J911 system that refers to the U.S. E911 system that connects 911 calls to the appropriate public safety answering point (PSAP) including location information. The J911 system was described to identify the constant envelope (CE) type jamming signal and estimate the jammer's location by using jamming-to-noise (J/N) observations and location infor-mation acquired from a large number of smartphones. Here, through the simulation of cloud situation with 1,000 smartphones distributed per 1km^2 area, it was shown that the higher the density of the smartphone that provides the measurements in a certain space, the higher the accuracy of the jammer localization increased.

In [5], authors proposed cloud sourcing based method that used carrier-to-noise density (C/N_0) and AGC information obtained from many smartphones to distinguish between the jamming and the spoofing signals and estimate the jammer position. In the experiment to verify the method, satellite information from 15 smartphones was acquired using the self-developed android application software, and the AGC level was measured via the SiGe GN3S Sampler. Then they estimated the moving jammer position through the TDOAs.

In this paper, we propose a cloud-data based jamming detection and localization method. This method uses a 2-dimensional time-frequency correlation technique that is in between 2 of cloud-data. It is assumed that we can gather and utilize the intermediate frequency (IF) signal data from many low-cost GNSS receivers distributed in a certain region. Discrimination of jamming signal type uses the fact that the result of the correlation between the cloud-data shows different characteristics with respect to power, TDOA, and frequency variation. Then the position of the jammer is estimated using the obtained TDOA information. The availability of the proposed method is verified by a numerical simulation. It is noted that in this paper the AGC effect that may induces the saturation for high power jamming signal at the RF front-end is assumed to be not existed.

2 JAMMING SCENARIO

2.1 Schematic depiction of jamming scenario

Figure 1 is a schematic depiction of a scenario in which a jammer transmitting weak jamming signals is located between a number of low-cost GNSS receivers distributed in a dense density over a large area, and a processing procedure of the receiver data. The area where the jammer interferes with the receiver is set within a radius of 300 [m], so that in the jamming area, we assume that the amplitude of the jamming signal is larger than the amplitude of the satellite signal. All receivers distributed over a large area continuously transmit the data of the received signal to the cloud server and the server monitors the jamming signal via the time-frequency correlation between the specific data. If the jamming signal is detected, the type of jamming signal, received jamming power, and TDOA information between the two signals are obtained by analyzing the result of the correlation method in the time-frequency domain. As a result, we estimate the position of the jammer by applying a position estimation method suitable for the type of specific jamming signal.

2.2 Types of jamming signals applied to the scenario

The jamming signal blocks the reception of the GNSS signal by deliberately emitting electromagnetic radiation to disrupt user receivers by reducing the signal-to-noise level at the user's receiver [6]. Therefore, various types of signals can be classified as jamming signals.

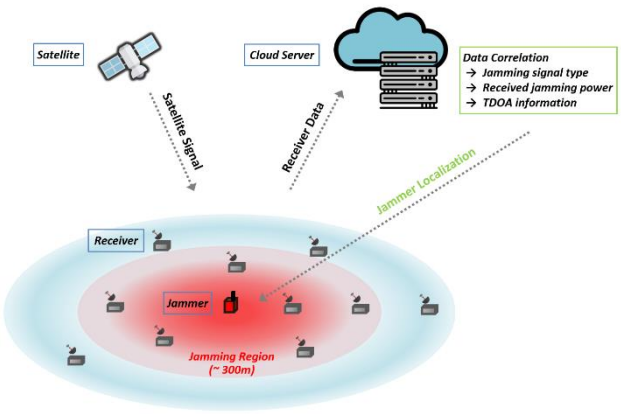

Figure 1 – Schematic depiction of jamming scenario and processing procedure of the receiver data

Table 1 – Modeling of jamming signals

Type	Signal Modeling	Note
CWI	$\sqrt{2P_i}cos(2\pi f_i t + \theta_i)$	P_i : Jamming power f_i : Jamming signal frequency θ_i : Jamming signal phase $C(t)$: Spreading code $n(t)$: White gaussian noise $rect(t,d,r)$: Pulse with duration d, repetition frequency r at time t f_0 : initial frequency k : Chirp rate t_{chirp} : $0 \le t_{chirp} \le T_{sw}$ (T_{sw} : sweep time)
MSI	$\sqrt{2P_i}C(t)cos(2\pi f_i t + \theta_i)$	
BLWI	$\sqrt{2P_i}n(t)cos(2\pi f_i t + \theta_i)$	
Pulse	$\sqrt{2P_i}rect(t,d,r)cos(2\pi f_i t + \theta_i)$	
Chirp	$\sqrt{2P_i}cos\left[2\pi\left(f_0 + \frac{k}{2}t_{chirp}\right)t\right]$	

In this section, we explain 5 types of jamming signals dealt with in this paper and present the modeled equations in Table 1.

• Types of jamming signals

(1) Continuous Wave Interference (CWI)
- It is a sinusoidal wave, single-tone frequency signal within the GNSS frequency band.

(2) Matched Spectrum Interference (MSI)
- It uses the same spreading code as the GNSS signal and shows the same frequency characteristics.

(3) Band-Limited White Gaussian Noise Interference (BLWI)
- It has the white gaussian noise characteristic within the limited band, ideally the power spectral density is constant in frequency domain.

(4) Pulse Interference (Pulse)
- It has a large power in a very short time, and the form of pulse signal is generated according to the duty cycle, the pulse repetition frequency, and the pulse width.

(5) Chirp Interference (Chirp)
- As a continuous waveform signal with time-varying frequency modulation, it is technically easy to

implement and has good jamming characteristics, so it is mainly used in In-car Jammer.

3 JAMMING DETECTION AND LOCALIZATION USING TIME-FREQUENCY CORRELATION METHOD

Correlation is generally applied between two data acquired from different receivers. Therefore, in this section, we explain the time-frequency correlation method for two receivers located at different location as shown in Figure 2.

3.1 Time-frequency correlation method

In order to detect jamming signals and estimate the jammer's position, the time-frequency correlation method proposed in this paper consists of two correlations as follows

- 2-D image correlation in the time-frequency domain
- Signal correlation in the time domain

• 2-D image correlation in the time-frequency domain

This correlation is to compare the 2-D images of the time-frequency domain generated with the IF signal data acquired at each receiver. Figure 3 outlines the method of generating a 2-D image in the time-frequency domain for a single receiver. If the current time is 0, the preset signal length is n samples, and 10 samples of signal correspond to time T_s, the 2-D image can be obtained by applying fast fourier transform (FFT) to the IF signals over time. At this time, the frequency bin is expressed in other colors according to the magnitude of the amplitude.

• Signal correlation in the time domain

This method means the correlation between the two IF signals received at two different receivers. Referring to Figure 2, the equation representing this correlation is given as follows

$$\begin{aligned} \mathrm{R}(\tau) &= r_A * r_B \\ &= \{S(t-\tau_{S,A}) + J(t-\tau_{J,A}) + \eta_A\} \\ &\quad * \{S(t-\tau_{S,B}) + J(t-\tau_{J,B}) + \eta_B\} \end{aligned} \quad (1)$$

where r_A and r_B are received signal for receiver A and B, respectively, $\tau_{S,A}$ and $\tau_{J,A}$ are time delay of satellite and jamming signal for receiver A, respectively, $\tau_{S,B}$ and $\tau_{J,B}$ are time delay of satellite and jamming signal for receiver B, respectively, and η_A and η_B are noise component for receiver A and B, respectively.

3.2 Jamming detection using time-frequency correlation method

If the center frequency of the jamming signal differs from the satellite signal or continuously changes like the chirp signal, the frequency value with the largest amplitude will be different from the center frequency of the satellite signal in the time-frequency domain 2-D image. Frequency variation can also occur for fast-moving jammers, so the

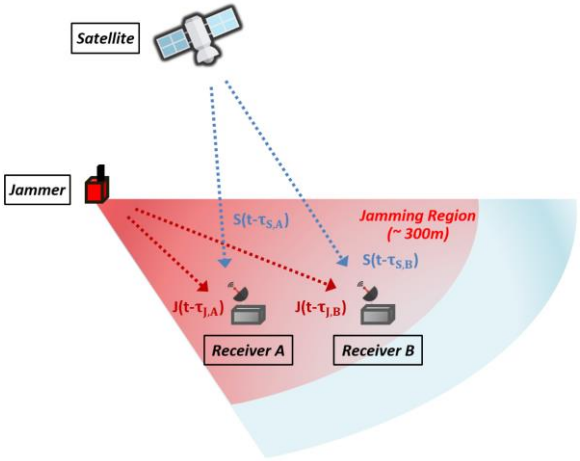

Figure 2 – Jamming scenario for two receivers in another location

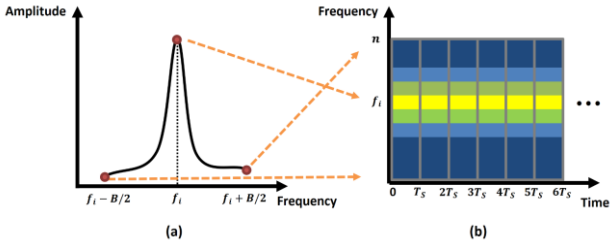

Figure 3 – Method of generating a 2-D image in the time-frequency domain for a single receiver. (a) FFT result of n sample length IF signal at any one time (b) Generated 2-D image

presence and type of jamming signal can also be determined by monitoring them. But, we assume that the jammer and receivers are almost static or slowly moving in this paper.

It is also possible to detect the jamming signal by using signal correlation in the time domain. When the two IF signals in which the satellite signal and the jamming signal have different time delays are correlated in the time domain, the two correlation peaks exist at the index having $\tau_{S,B} - \tau_{S,A}$ and $\tau_{J,B} - \tau_{J,A}$. Although the correlation form of the satellite signal is well known, the correlation form of the jamming signal shows different characteristics depending on the jamming signal type. By analyzing this feature, it is possible to discriminate the presence and the type of jamming signal. Jamming signal detection using correlation method is verified for availability through the simulation in Section 4.2.

3.3 Jamming source localization using time-frequency correlation method

In the jamming scenario covered in this paper, the correlation peak value of the jamming signal is generally larger than that of the satellite signal for receivers placed in or near the jamming region. It is possible to obtain the TDOA information of the jamming signal between the receivers by analyzing the correlation peak. If we acquire this TDOA information from a large number of receivers, the position of the jammer can be estimated. It is also

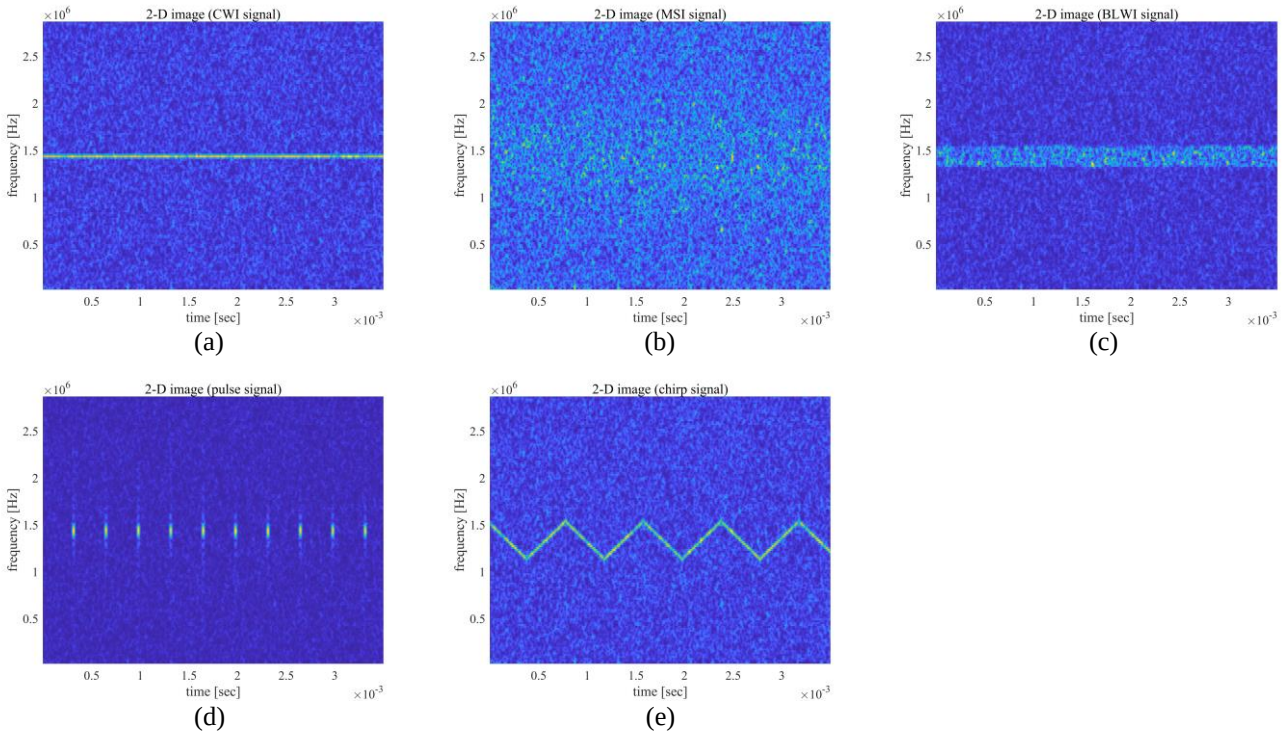

Figure 4 – Generated 2-D images for jamming signals. (a) CWI (b) MSI (c) BLWI (d) Pulse (e) Chirp

possible to estimate the jammer position roughly by using the correlation of time-frequency domain 2-D images obtained from a lot of receivers. This exploits the fact that the 2-D image obtained from a receiver close to the jammer has a higher amplitude than a far-away receiver. For example, if a large number of cloud-data obtained from region 'A' shows a 2-D image having a higher amplitude than that of region 'B', it can be seen that the jammer is located in the vicinity of region 'A'.
Jamming source localization using correlation method is verified for availability through simulation in Section 4.3.

4 SIMULATION RESULTS ANALYSIS

4.1 Jamming scenario implementation

In the simulator, we assume that jammer can generate the aforementioned five jamming signals. In order to implement cloud-data, multiple receivers were arbitrarily placed at the certain distances that range from 100 [m] to 300 [m] from the jammer. Considering the free space propagation loss, we set the J/N to 0 [dB] at 100 [m] from the jammer. Thus, all receivers in the jamming region indicate the certain values of the J/N that are smaller than 0, while J/S of receivers are positive values. In order to process IF signal data, the sampling frequency is set to 28.57 [MHz] and the integration time of signal correlation is set to 1 [ms] for receivers. In addition, the center frequency of IF signal is 1.4 [MHz]. Besides this for simplicity, we assume that the setting and time of all receivers are synchronized.

4.2 Simulation result analysis of jamming detection

Figure 4 shows the plots of the generated 2-D images of received signals for the five jamming signal types. As mentioned in Section 3.2, jamming can be detected using the characteristics of the FFT result. In order to generate each vertical slice of the 2-D image, we use FFT result of 285 samples of IF jamming signal. The FFT result is filtered by the hamming-window and there is 10 samples delay between two adjacent vertical slices.

In Figure 4(a), the yellow point which is the peak amplitude stays on the 1.4 MHz because the CWI jamming signal is a continuous sinusoidal signal of constant frequency.

In Figure 4(b), since the MSI jamming signal is the signal that uses the same spreading code as the existing GNSS signals, the FFT result is also spread. Therefore, in order to detect jamming signal through the 2-D image of received signal, we should note that the amplitude of combined signal containing jamming signal and satellite signal with noise is slightly greater than that of satellite signal with noise. Thus, the 2-D image of combined signal would be colored more brightly than that of satellite signal. However, it cannot be easy to sense the change of 2-D image color.

In Figure 4(c), the 2-D image show random color with constant bandwidth because the BLWI jamming signal is white noise having a limited bandwidth. This makes the color of 2-D image discontinuous, which is different from the 2-D image with no jamming signal.

In Figure 4(d), since the pulse jamming signal radiates a signal of high power during a short period of time, the FFT

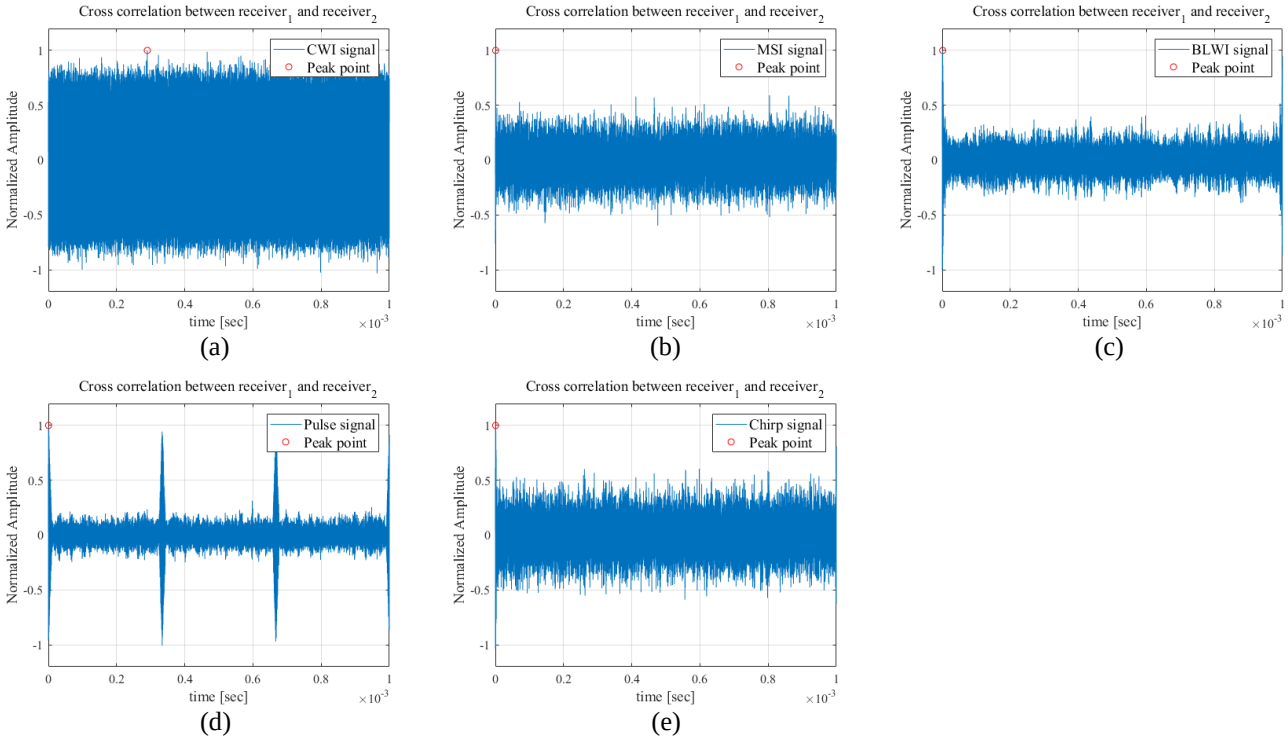

Figure 5 – Correlation results of two received signals. (a) CWI (b) MSI (c) BLWI (d) Pulse (e) Chirp

results have the peaks sparsely over a certain time. As can be seen, the yellow point stays on the 1.4 MHz.

The chirp jamming signal is a continuous sinusoidal signal like CWI, but frequency changes according to time elapse. Therefore, in Figure 4(e), the peak amplitude of the FFT result also varies with time. Fortunately, this remarkable characteristics of 2-D image of chirp help us to detect jamming signal easily.

As described in Section 3.2, we can also detect jamming signal by using signal correlation in the time domain. Figure 5 shows the correlation results of two received signals from different receivers for the five jamming signal types respectively. The peak point means the highest value of the correlation result.

In Figure 5(a), the correlation result according to time comes out in the form of period, because the CWI jamming signal is a continuous sinusoidal signal. The result can help us to distinguish the CWI jamming signal from the various types of jamming signals. According to this characteristic, the estimation result of the jammer's position obtained by using the correlation of CWI signals can be easily wrong compared to the true jammer's position. It will be explained in Section 4.3.

In Figure 5(b), since MSI is very similar to the existing GNSS signal, it is difficult to detect jamming signal through the correlation in the time domain for MSI. However, assuming that the difference of doppler effect between two receivers is large for the satellite signals and also the amplitude of jamming signal is greater than that of satellite signal, the correlation result between the satellite signals may have small peak. Under these assumption, we can only obtain the correlation peak of MSI, and then detect it.

In Figure 5(c), the correlation result of the BLWI signals has a sharp peak compared to the result of spreading code correlation of GNSS signal.

In Figure 5(d), as mentioned earlier, since pulses radiate a signal of high power during a short period of time, the correlation value of the time domain has a large peak at a constant period.

In Figure 5(e), the correlation result of the chirp signals shows similar pattern as that of the MSI signals. However, if the time used for correlation is longer than the sweep period, the correlation result has one main lobe with side lobes that has smaller peak than main lobe. This can be similar to the result of the pulse signals in which peaks of the same size are periodically displayed.

As can be seen, plots in Figure 5 do not present much information relative to the type of jamming signal. We can only find that CWI and pulse signal have specific correlation results. However, since the correlation peak of jamming signals exists at certain time index that is different from that of correlation peak of satellite signals, we can recognize not only the presence of jamming signal, but also TDOA information. This information will be explained in Section 4.3 for jammer localization.

It is determined whether or not a jamming signal is present through correlation between IF signals collected from a large number of receivers. Signal correlation can be performed regardless of the presence and type of jamming signal because it uses two received signals.

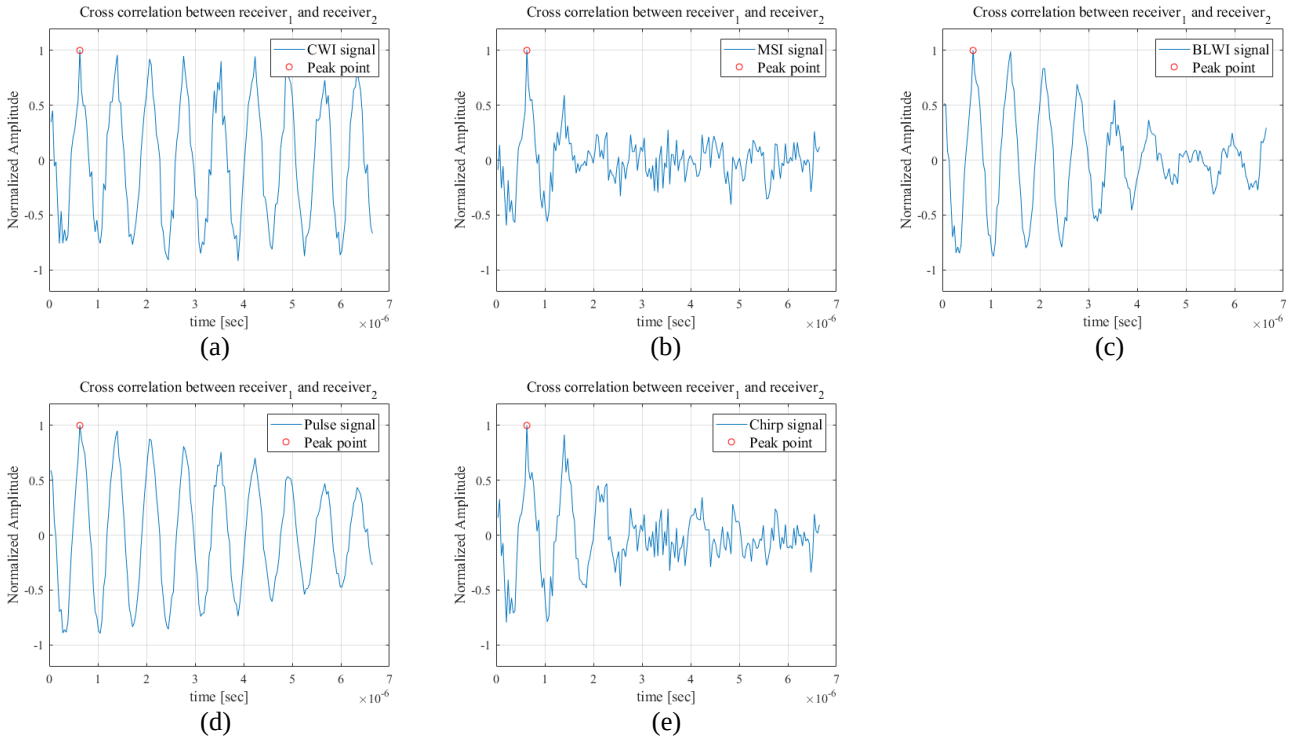

Figure 6 – TDOA information of signal correlation results. (a) CWI (b) MSI (c) BLWI (d) Pulse (e) Chirp

4.3 Simulation result analysis of jamming position estimation

In this section, we show the simulation results performed to prove that position estimation is possible through the proposed correlation method.

We use the TDOA information that is estimated from the correlation result of two received signals to estimate the jammer position. This information is presented in Figure 6 by plotting Figure 5 with limited time scale (7 micro-seconds) for the five jamming signal types respectively. The limited time scale is really short because the sampling frequency of receiver is high enough to obtain high resolution of TDOA.

In Figure 6, every jamming signal except CWI has one main peak that contains TDOA information on the time axis. However, in case of CWI, the sinusoidal wave characteristic prevent the correlation result from containing the true main peak with true TDOA information. Thus, it can be hard to estimate the jammer position with signal correlation result of CWI signals, while other types can be used for jammer localization.

In simulation, the true jammer position was set to be located at the coordinates (0, 0), and the 15 receivers were randomly placed at the certain distances that range from 100 [m] to 300 [m] from the jammer. With the TDOA information, the position was estimated by using the nonlinear least squares estimation (NLSE) method. As a result of the simulation that is summarized in Figure 7, the estimated position of the jammer had about 10.2 [m] error from the true jammer location.

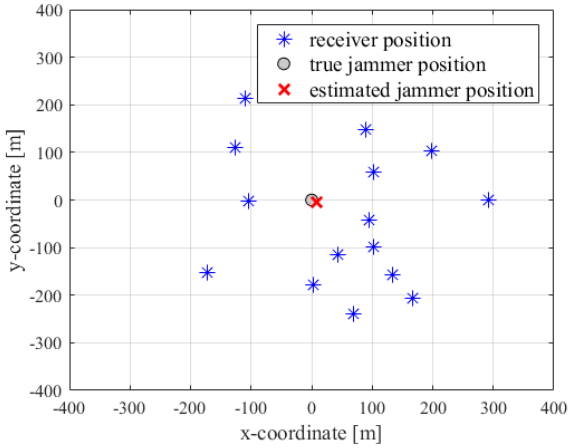

Figure 7 – The results of jammer position estimation by using proposed method

We proved that it is also possible to estimate the position of the jammer by using the proposed method. If we generate more receivers and the amount of cloud-data increases, the accuracy of jammer position estimation will increase.

5 CONCLUSIONS

In this paper, assuming that a jammer with a weak jamming signal power is located in between a large number of low-cost GNSS receivers distributed at dense density in a wide area, we proposed a 2-dimensional time-frequency correlation method that is to ideally applied to detect and localize the jamming source by using data obtained from multiple receivers through cloud-data computing. The availability of the proposed method was examined by simulation.

By applying the time-frequency correlation method composed of two correlations, it is proved that different characteristics can be seen according to the type of jamming signals, therefore five jamming signals can be detected and classified.

Through the jamming scenario where 15 receivers were arranged, it was proved that the jammer position estimation is possible by using the TDOA information of the jamming signals obtained as the result of the signal correlation between the data of receivers.

As a result, by using the time-frequency correlation method which was proposed in this paper, we can discriminate the presence and the type of jamming signal, and estimate the position of the jamming signal source. Furthermore, if we could monitor a huge amount of the cloud-data simultaneously, it will be helpful for the jamming signal monitoring for a wide area.

ACKNOWLEDGMENTS

This research was supported by a grant of Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B03031787)

REFERENCES

[1] Lindstrom, J., Akos, D. M., Isoz, O., and Junered, M. (2007), *GNSS Interference Detection and Localization using a Network of Low-cost Front-End Modules*, Proceedings of the 20th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2007), pp.1165-1172

[2] Isoz, O., Balaei, A. T,, and Akos, D. M. (2010), *Interference Detection and Localization in the GPS L1 Band*, Proceedings of the 2010 International Technical Meeting of The Institute of Navigation, pp.925-929

[3] Scott, L. (2010), *J911: Fast Jammer Detection and Location Using Cell-Phone Crowd-Sourcings*, GPS World 21, no. 11.

[4] Scott, L. (2011), *J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches*, Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), pp.1931-1940

[5] Strizic, L., Akos, D. M., and Lo, S. (2018), *Crowdsourcing GNSS Jammer Detection and Localization*, Proceedings of the 2018 International Technical Meeting of The Institute of Navigation, pp.626-641

[6] Dovis, F. (2015), *GNSS Interference Threats and Countermeasures*, 1st ed. Artech House Inc.