JPNT 7(4), 227-233 (2018)
https://doi.org/10.11003/JPNT.2018.7.4.227

JPNT Journal of Positioning, Navigation, and Timing

Design and Analysis of Switching Timing for High Power GPS Meaconing Jammer

Byung-Hyun Lee†, In-Geun Oh, Sung-Il Kim

EW R&D Center, Hanwha Systems, Seongnam-si 13524, Korea

ABSTRACT

The purpose of satellite navigation meaconing jamming is to make the target GPS receiver calculate false navigation by meaconing the received satellite signals. At this time, since the received and transmitted signals have the same frequency, the back-lobe reduction level of antenna should be -160 dB when the Effective Radiated Power (ERP) is 1 Watt (30 dBm). Therefore, meaconing jamming is impossible by merely reducing the back-lobe level of antenna when the transmitter and receiver are in proximity to each other. In general, the transmitter and receiver are isolated by the time division method to eliminate such transmission/reception interference. This paper studied the optimal switching timing between transmitting and receiving when isolating the time division transmission and reception for GPS meaconing jamming.

Keywords: meaconing, GPS, jamming, RF switching timing, time division

1. INTRODUCTION

Recently, as the interest in unmanned systems such as unmanned surveillance vehicles and unmanned vehicles has increased, the importance of absolute positioning systems such as the Global Positioning System (GPS) is also increasing for reliable navigation systems. As the fields that use Unmanned Aerial Vehicles (UAV) or drones become more diverse, drones in unauthorized areas are becoming a threat (Meurer 2017). Therefore, GPS jamming is one of the methods to address the issues related to drones. The automatic flight of UAV uses GPS location information and the signal strength is weak, making it very vulnerable to unintended radio interference. Therefore, GPS jamming can be used to cope with UAV threats (Shepard et al. 2012, Seo et al. 2015).

GPS jamming techniques include noise, spoofing, and meaconing jamming techniques. Noise jamming refers to the application of a stronger signal than the authentic GPS signal to the receiver, which interferes with normal navigation functions. In terms of spoofing and meaconing jamming, which is being studied recently, the jammer generates an intended navigation solution by applying GPS-like signals to the receiver, thereby hindering the normal navigation functions of the receiver (Humphreys et al. 2008). The jamming signals generated by each jamming technique are radiated at high power using a High-Power Amplifier and an antenna (Psiaki & Humphreys 2016). Noise and spoofing jamming generate and radiate signals through the jammer's internal signal generator. However, in the case of meaconing jamming, since the actual satellite signal is received and re-transmitted, the signal receiver and transmitter are both inside a single jammer. This structure allows the radiation signal to be applied to the jammer's receiver when the jamming signal is radiated at high power, causing the jammer to malfunction.

Therefore, the receiver and transmitter must be isolated for successful meaconing jamming. The isolation techniques include physical isolation and isolation through digital signal processing. For physical isolation, the jamming transmission antenna and reception antenna should be separated over a long distance or special equipment is required to prevent radiation jamming signals from reaching the reception antenna. Since the typical GPS reception signal strength is about -130 dBm (Parkinson et al. 1996, Kaplan & Hegarty 2006), the signal strength at which the radiation jamming

Received Sep 12, 2018 **Revised** Nov 18, 2018 **Accepted** Nov 23, 2018
†**Corresponding Author**
E-mail: byunghyun.lee@hanwha.com
Tel: +82-31-8091-7709 Fax: +82-31-8091-7193

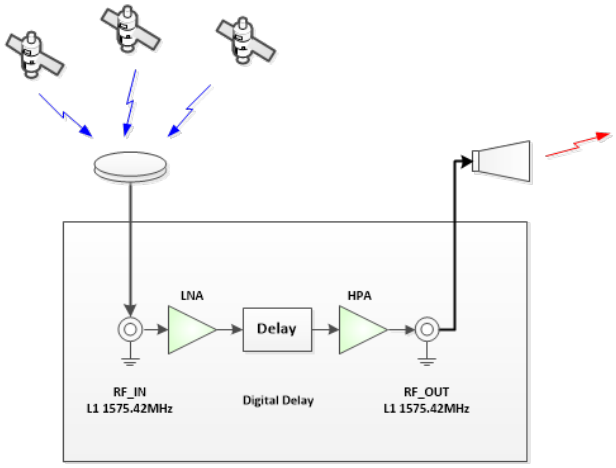


Fig. 1. Structure of conventional meaconing jamming system.

signal reaches the reception antenna should be canceled to less than -130dBm.

The isolation through digital signal processing is performed by implementing Self-Interference Cancellation for full duplex communication to reduce the power of the radiation signals introduced to the receiver (Bharadia et al. 2013) or by applying the time division method to block the receiver during transmission through transmission/reception switching and isolating the transmission and reception so that the radiation signals are not transmitted during reception (Shairi et al. 2011). The purpose of meaconing jamming is to coerce the target GPS receiver to calculate false navigation solutions or cause the receiver to operate abnormally. This paper studied the transmission/reception switching timing which can cause the target receiver to generate false navigation solutions by receiving the meaconing jamming signal.

2. STRUCTURE OF MEACONING SYSTEM

Fig. 1 shows the structure of meaconing jamming. The horn antenna was applied as the jamming signal transmitting antenna to withstand an ERP of hundreds of watts. When the transmitter and the receiver are in one system as shown in Fig. 1, the system does not operate normally because of the infinite self-interference caused by the application of the antenna's back-lobe signals and reflected signals from the surrounding environment to the reception antenna. Antennas with back-lobe reduction functions are used to address this problem, and the HA 9251-12 (SCHWARZBECK MESS-ELEKTRONIK) has a Front-to-Back Ratio (FBR) of 27 dB and the horn antenna designed by Shin et al. (2018) has an FBR of 47 dB. When the ERP is 1 Watt (40 dBm) and the distance between the transmission and reception antennas

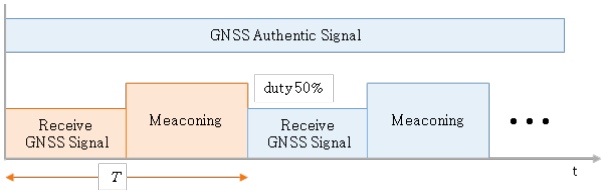


Fig. 2. Concept of TDD based TX/RX isolation.

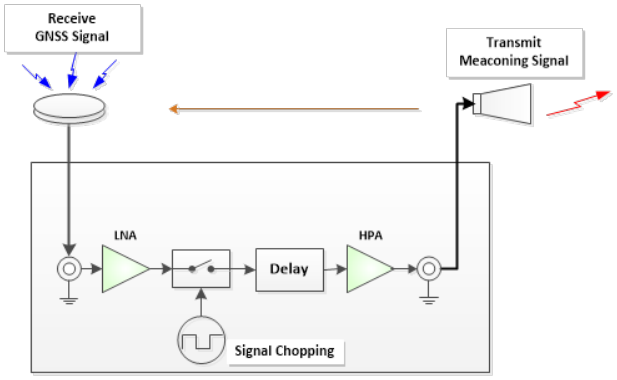


Fig. 3. Structure of TDD applied meaconing jamming system.

is 10 m, a signal attenuation is 57 dB by the free space path loss model, thus the meaconing jamming back-lobe signal strength applied to the receiption antenna becomes -64 dBm. That is, a meaconing jamming signal which is about 66 dB stronger than the nominal GPS reception signal power of -130 dBm is applied. This means meaconing jamming is impossible with the back-lobe reduction function solely.

3. TIME DIVISION DUPLEX BASED TX/RX ISOLATION

As described in Chapter 2, transmission and reception isolation of the Time Division Duplex (TDD) concept is required to successfully perform meaconing jamming. Fig. 2 shows the concept of transmission/reception isolation in terms of the TDD method.

The RF switch is used to isolate the reception and transmission signals. The receiver receives GPS signals and uses the pre-designed chopping signals to prevent the jamming signals from being transmitted while receiving the GPS signals. The transmitter is designed not to receive GPS signals while transmitting the jamming signals (Fig. 3).

The switch timing for transmission and reception isolation is an important design parameter for successful meaconing. In order to completely isolate the transmission and reception signals, the signal delay time at each end of the meaconing jamming equipment and the signal delay time according to the separation distance between the transmission and

Table 1. Switching Timing of each signal characteristics.

Level	Signal	Frequency (MHz)	Successful switching time (1/2*frequency, nsec)	Note
Carrier	L1	1575.42	0.32	GPS L1
Code (chip)	P	10.23	48.88	Military
	C/A	1.023	488.76	Civil
Correlation	C/A	0.001	0.5 (msec)	Civil

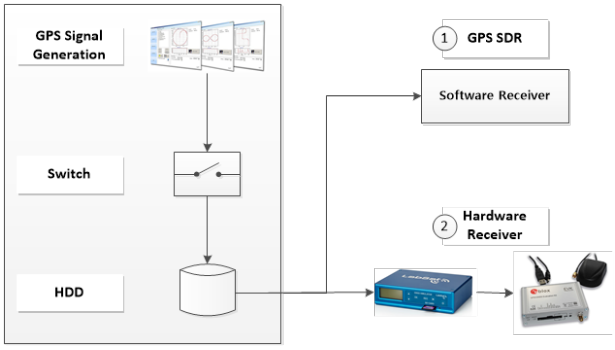


Fig. 4. Simulation setup.

reception antenna must be accurately measured and calibrated. The convenience and isolation performance of the actual implementation is determined according to the switching timing. Slow switching timing improves the ease of implementation and the isolation performance depending on the characteristics of the device. However, if the switching timing is too slow, the target GPS receiver may operate like noise jamming when receiving the meaconing jamming signals. This paper used Digital Radio Frequency Memory (DRFM) to control the delay. The digital sampling performance of the DRFM is determined depending on the delay time according to the switching interval for successful meaconing and the separation distance between the transmission/reception antennas, and the required memory size of the DRFM is determined according to the delay time set as the design parameter.

For successful meaconing, switching must be performed at twice the speed according to the Nyquist theory (Table 1). Switching can be considered in 3 levels as shown in Table 1. First, in order to avoid signal loss in carrier frequency level, switching must be performed in units of 0.32 nsec. In this case, calibration becomes very sensitive and difficult to implement depending on the separation distance between the transmission and reception antennas. The second is code level switching. In terms of C/A code, switching needs to be performed in 0.48 μsec because the switching is performed within 1 chip. The last parameter that can be considered is correlation level switching. General GPS signal processing correlates signals of 1 msec, which is 1 cycle of C/A code. When the switching timing is determined by considering these 3 parameters, meaconing is possible for the target GPS receiver.

Table 2. Summary of simulation results.

CST	Acquisition	Tracking	Navigation	Position error (m)	Height error (m)
No	○	○	○	2.66	6.42
0.5	○	○	○	2.68	5.99
1 (chip level)	○	○	○	2.54	6.44
2	○	○	○	2.52	6.31
4	○	○	○	2.56	6.08
8	○	○	○	2.54	6.09
511.5	○	○	○	2.58	6.32
1023 (correlation level)	○	○	○	2.65	6.14
2046	○	○	×	-	-

4. SIMULATION RESULTS

4.1 Simulation Setup

In this chapter, simulations was performed to evaluate the switching timing in theory as mentioned in chapter 3. The simulation generated IF signals for each switching timing of the GPS signal generated by the SatGen simulator. The performance evaluation was performed by signal processing using the ① GPS software receiver platform SoftGNSS v3.0 (Borre et al. 2007) and was evaluated using ② the U-Blox EVK-M8N receiver by replaying the IF signals generated by LabSat3 (Fig. 4).

Figs. 5 and 6 are the results of processing GPS signals with a software receiver and hardware receiver without switching. GPS signals that can be processed normally as shown in the figures are switched to various switching timings to verify whether signal processing is possible. Fig. 5a shows the acquisition result of the software receiver, and Fig. 5b presents the scatter plot, navigation message bit, raw Phase Locked Loop (PLL) discriminator output, Early-Prompt-Late correlation output, filtered PLL discriminator output, raw Delay Locked Loop (DLL) discriminator output, and filtered DLL discriminator output from the top left. Fig. 6 is the GUI of a U-Blox receiver, which shows the satellite sky plot, receiver status, and C/N0 for each satellite.

4.2 Simulation Results

In order to verify chip level switching, we generated 1 CST (chip switching timing, 1 CST: 1 chip duty 50% on/off) signal which gives one cycle of on/off to 1 chip and analyzed the performance. The software receiver confirmed that the discriminator values of each tracking loop, the navigation message, and the navigation result were calculated normally. In addition, the hardware receiver confirmed that the navigation solution was calculated normally, despite C/N0 attenuation (Figs. 7 and 8).

Next, in order to verify correlation level switching, this

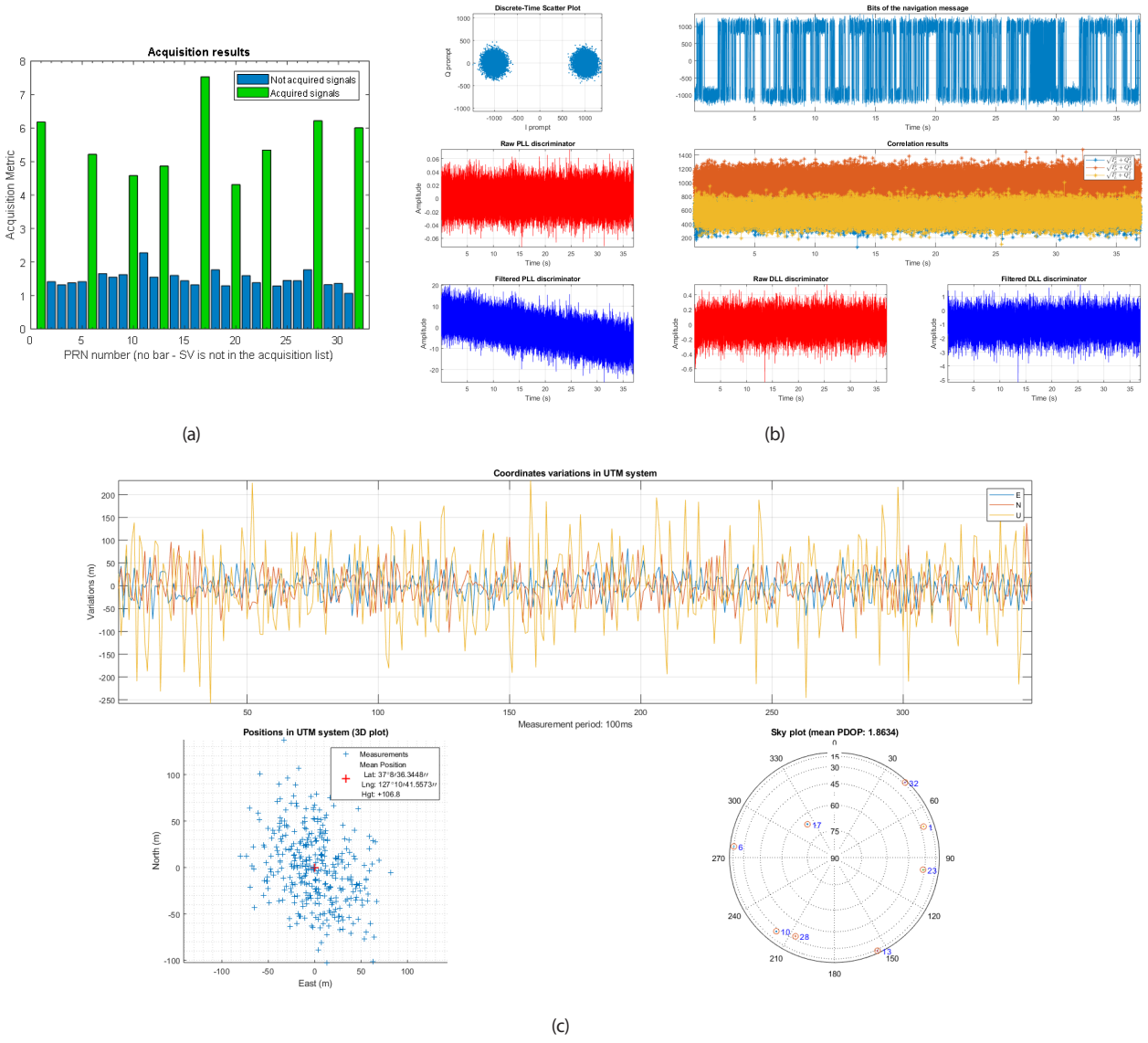


Fig. 5. (a) Acquisition, (b) Tracking, (c) Navigation results of software receiver (no switching).

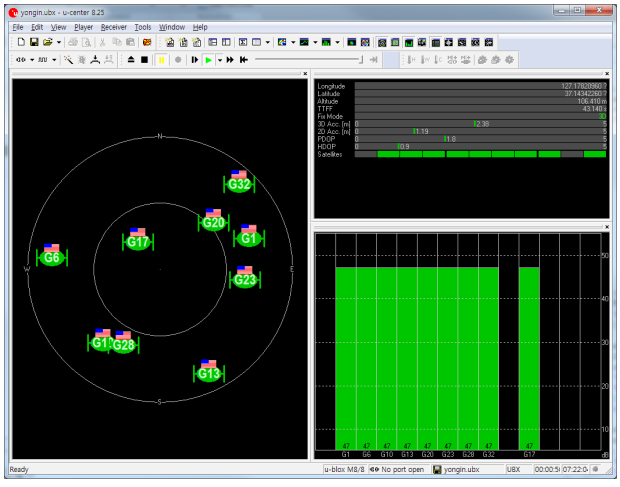
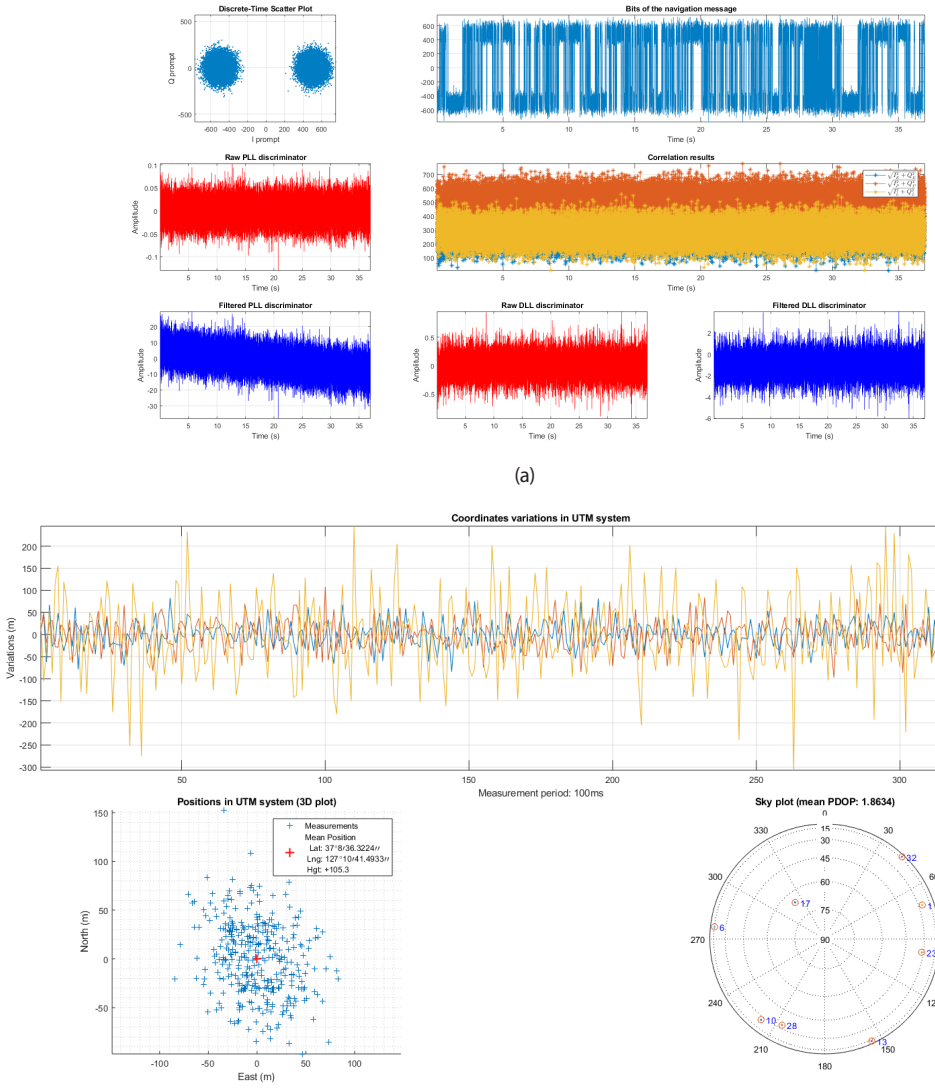


Fig. 6. Result of hardware receiver (no switching).

study generated signals of 1023 CST switching, which is the C/A code cycle, and analyzed the performance. The result was the same as 1 CST. This means that meaconing jamming can be successfully performed by determining the switching timing at the chip level and correlation level.

The signal processing does not operate normally when exceeding correlation level CST. When generating simulated GPS signals, stationary signals with no dynamic characteristics are generated, which allows continuous signal tracking because the tracking loop does not miss the signals. However, since the navigation bit is not normal, the subframe of the navigation message cannot be decoded because the preamble cannot be detected. Therefore, it is impossible to calculate navigation solutions (Figs. 9 and 10).

To verify chip level switching, this study generated from



(a)

(b)

Fig. 7. (a) Tracking (PRN 17) and (b) navigation result (1 CST switching).

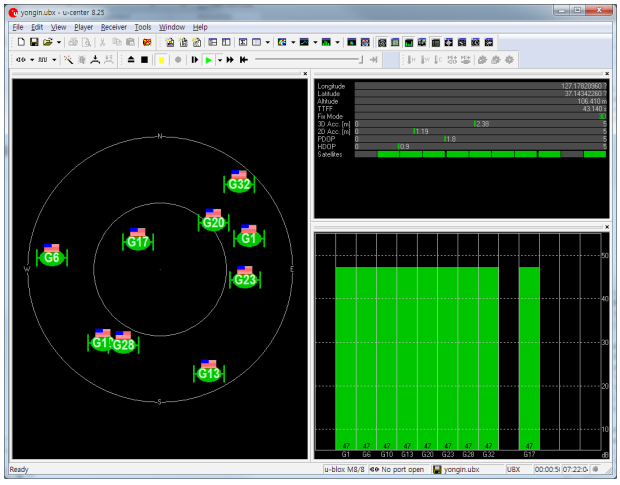


Fig. 8. Result of Hardware receiver (1 CST switching).

1 CST to 1023 CST signals in order to verify correlation level switching, and 2046 CST signals to verify cases that exceed the above. The simulation results are summarized in Table 2.

5. CONCLUSIONS

In order for meaconing jamming function to operate successfully, the jammer's transmission signals must not affect the receiver. This paper studied the switching timing to apply the time division method to isolate transmission and reception. Since GPS uses CDMA signals, switching timing should be considered as the meaconing jamming design parameter. The simulation results confirmed normal operation even when time division was performed with

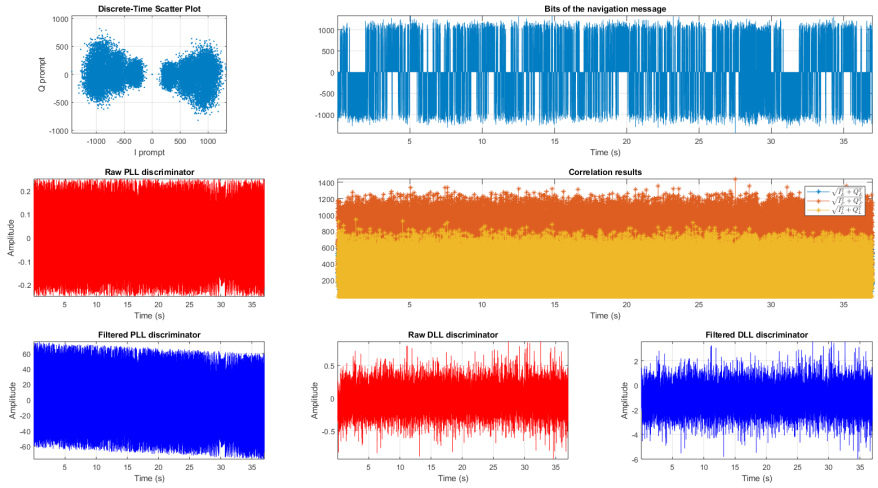


Fig. 9. Tracking result (PRN 17, 2046 CST switching), no navigation result.

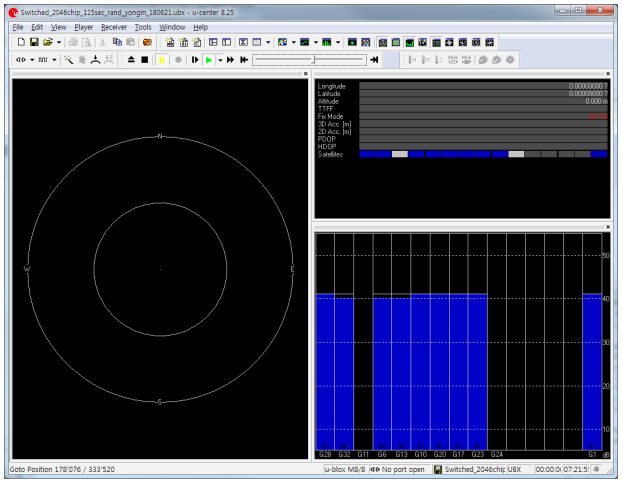


Fig. 10. Result of Hardware receiver (2046 CST switching).

chip level and correlation level switching timing. In order to implement actual meaconing jamming equipment, the total delay inside the equipment and the delay according to the separation distance between the transmission and reception antennas need to be measured to determine the delay for transmission and reception isolation. Based on the simulation results, a meaconing jamming device can be implemented by applying an RF switching device of less than 1023 CST and determining the CST unit according to the accuracy of the delay device for transmission/reception isolation. In the future, additional research is needed to analyze the receiver's anti-jamming characteristics and signal tracking loop characteristics according to the CST in order to derive the optimal CST timing for meaconing jamming in reality.

REFERENCES

Bharadia, D., McMilin, E., & Katti, S. 2013, Full duplex radios, in ACM SIGCOMM Computer Communication Review, 12-16 Aug 2013, Hong Kong, China, pp.375-386

Borre, K., Akos, D. M., Bertelsen, N., Rinder, P., & Jensen, S. H. 2007, A software-defined GPS and Galileo receiver: a single-frequency approach (Berlin: Springer Science & Business Media)

Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, Jr. P. M. 2008, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in Proceedings of the ION 21st International Technical Meeting of the Satellite Division of The Institute of Navigation, Savannah, GA, 16-19 Sep 2008, pp.2314-2325

Kaplan, E. D. & Hegarty, C. J. 2006, Understanding GPS: Principles and Applications, 2nd ed. (Boston: Artech House Inc.)

Meurer, M. 2017, Hostile MAVs – An introduction to threats and countermeasures, in Proceedings of the ION GNSS+ 2017, Portland, Oregon, 25-29 September 2017

Parkinson, B. W., Spilker Jr, J. J., Axelrad, P., & Enge, P. 1996, Global Positioning system: Theory and Applications, vol.1 (Washington, D.C: AIAA)

Psiaki, M. L. & Humphreys, T. E. 2016, GNSS Spoofing and Detection, in Proceedings of the IEEE, 104, 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658

Seo, S. H., Lee, B. H., Im, S. H., & Jee, G. I. 2015, Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal, Journal of Positioning, Navigation, and Timing, 4, 57-65. https://doi.org/10.11003/JPNT.2015.4.2.057

Shairi, N. A., Ahmad, B. H., & Khang, A. C. Z. 2011, Design and analysis of broadband high isolation of discrete packaged PIN diode SPDT switch for wireless data communication, in Proceedings of IEEE International RF and Microwave Conference (RFM), Seremban, Malaysia, 12-14 Dec 2011. https://doi.org/10.1109/RFM.2011.6168703

Shepard, D. P., Bhatti, J. A., Humphreys, T. E., & Fansler, A. A. 2012, Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks, in Proceedings of ION GNSS 2012, Nashville, TN, 17-21 Sep 2012

Shin, J. Y., Shim, H. S., Lee, B. H., Lee, J. R., & Woo, J. M. 2018, Front-to-Back Ratio Improvement of a High-Power Horn Antenna, The Journal of Korean Institute of Electromagnetic Engineering and Science, 29, 389-392. http://dx.doi.org/10.5515/KJKIEES.2018.29.5.389

Byung-Hyun Lee is a senior researcher in the Hanwha Systems. He received the Ph.D degree in Electronics Engineering from Konkuk University in 2016. He is interested in GNSS software receiver, precise positioning, anti-jamming/spoofing, autonomous vehicles and navigation sensor integration.

In-Geun Oh is a senior researcher in the Hanwha Systems. He received the Bachelor's degree in Electronics Engineering from Sungkyunkwan University in 2009. He is interested in GNSS software receiver, precise positioning, anti-jamming/spoofing and autonomous vehicles.

Sung-Il Kim is a senior researcher in the Hanwha Systems. He received the Bachelor's degree in Electric and Electronics Engineering from Yonsei University in 2009. He is interested in GNSS software receiver, software engineering, jamming/spoofing and radar system.