The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 2, pp.97-102, Apr. 30, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.2.97
JIIBC 2019-2-14

SDR 수신기를 이용한 위성항법 기만신호 효과도 분석

Analysis on GNSS Spoofing signal effects using SDR receiver

조지행*

Ji-haeng Cho*

요 약 위성항법 시스템은 민간 분야뿐만 아니라 군의 다양한 무기체계에서 위치 및 시각 동기화 등의 중요한 정보를 제공하는 역할을 수행하고 있으며 활용분야와 의존도가 높아지고 있다. 이에 따라, 위성항법 장치를 활용하는 무기체계에 대응하기 위해 전자파를 방사하여 위성항법장치를 기만하고자 하는 연구가 활발히 이루어지고 있다. 위성항법 기만신호는 수신기에 전파 교란신호를 방사하여 항법을 하지 못하도록 하거나 허위 위치와 속도로 오인하도록 유도하는 기술을 의미한다. 그 중 스푸핑 기술은 기만하고자 하는 수신기에서 수신하고 있는 코드 위상/도플러 주파수/항법 메시지와 동기되어 위성항법 신호 대신 기만신호를 획득하고 추적할 수 있도록 신호를 송신해주는 것이다. 본 논문에서는 SDR 수신기를 이용하여 GPS L1 C/A 기만신호에 의한 수신기 추적 알고리즘 영향성을 분석하고 기만 신호에 대한 효과도를 분석하였다.

Abstract The GNSS(Global Navigation Satellite System) provides important information such as Position and Navigation, Timing(PNT) to various weapon systems in the military. as a result, applications that employ satellite navigation systems are increasing. therefore, a number of studies have been conducted to deceive the weapon systems that employ GNSS. GNSS spoofing denotes the transmission of counterfeit GNSS-like signals with the intention to produce a false position and time within the victim receiver. In order to deceive the victim receiver, spoofing signal should be synchronized with GNSS signal in doppler frequency and code phase, etc. In this paper, Civilian GPS L1 C/A spoofing signals have been evaluated and analyzed by SDR receiver.

Key Words : GNSS, PNT, Spoofing, SDR receive

Ⅰ. 서 론

위성항법시스템은 민간 분야의 위치기반 서비스(LSB), 지리정보시스템(GIS), 다양한 방송통신융합기술 분야 뿐만 아니라 군의 다양한 무기체계에서 위치 및 시각 동기화 등의 중요한 정보를 제공하는 역할을 수행하고 있다. 위성항법 신호는 약 20,000 km 상공의 위성으로부터 송출되어 지상 수신기에서는 약 -130 dBm의 매우 미약한 세기의 신호로 수신되어 항법에 사용한다. 한편, 상용 GNSS 신호(GPS L1 C/A, GLONASS G1, BeiDou B1)는 인터페이스 통제문서(ICD)가 공개되어 있어 비의도적 또는 의도적인 교란 신호에 취약한 특성을 가지고 있다.[1][2] 위와 같은 단점을 가졌음에도 위성항법시스템을 활용한 무기체계는 점점 더 다양해지고 있으며 많은 위협으로 자리 잡아가고 있다. 다양한 무기체계 중 근래에 가장 이슈화되고 있는 분야가 무인기를 활용한 무기체계 분야이며 이에 대응하기 위한 기술로 위성항법시스템을 기만하기 위한 다양한 연구가 활발히 이루어지고

*정회원, 국방과학연구소
접수일자 2019년 2월 21일, 수정완료 2019년 3월 21일
게재확정일자 2019년 4월 5일

Received: 21 February, 2019 / Revised: 21 March, 2019 / Accepted: 5 April, 2019
*Corresponding Author: jeniers@naver.com
The 2nd R&D Institute, Agency for Defense Dvelopment, korea

있다. 위성항법 기만기술 중 스푸핑은 실제 위성에서 송신하는 신호와 동일한 신호를 방사하여 수신기가 기존에 추적하고 있는 실 위성 신호 대신 기만신호를 추적하도록 하는 기술이며, 수신기가 항법을 하는 원리대로 항법을 할 수 있는 신호이어야 한다. 따라서 위성항법수신기를 스푸핑하기 위해서는 기만하고자 하는 수신기에서 수신하고 있는 코드 위상/도플러 주파수/항법 메시지 동기가 되어 위성항법 신호 대신 기만신호를 획득하고 추적할 수 있도록 신호를 송신해주어야 한다.[3] 효과적인 기만신호를 생성하기 위해서는 위성항법 기만신호의 특성 및 품질을 분석하고 기만 신호 인가 시 나타나는 수신기의 위성항법 추적 알고리즘에 끼치는 영향성 분석이 필요하다.[4][5] 이를 위해 본 논문에서는 실 위성신호를 이용해 정상항법 신호를 SDR 수신기에 인가하여 이동하는 시나리오를 형성한 후 기만신호를 인가하여 SDR 수신기의 위성항법 추적 알고리즘의 변화와 위성항법 기만신호의 효과도를 분석하고자 한다.

II. SDR 수신기를 활용한 위성항법 기만신호 분석

1. 위성항법 SDR 수신기 설계

본 논문에서는 위성항법 기만신호 효과도 및 수신기 영향성을 분석하기 위해 SDR 수신기를 설계하였다. 위성항법 Upper L-band에는 GPS L1 C/A, BeiDou B1, GLONASS G1 C/A 신호가 존재하며 하나의 wide band RF Fronet-end를 이용하여 신호를 수신하도록 설계하였다. 3가지 신호를 수신하기 위해 다수의 RF front-end를 이용하는 방법보다 wideband RF front-end를 이용할 경우 비교적 적은 데이터 처리량으로도 3가지 신호를 수신할 수 있으며 각 대역별 신호처리에 대한 동기화를 고려할 필요가 없어져 시스템이 간단해진다. 하지만 위성항법 시스템 간 간섭과 대역폭을 최소화 할 수 있는 적절한 IF 주파수 선정이 필요하다. 따라서 본 논문에서 설계한 SDR 수신기는 그림 1과 같이 LO 주파수를 1.584 GHz로 설정하였으며 대역폭 25 MHz, Sampling rate을 50 MHz로 설계하였다.[6]

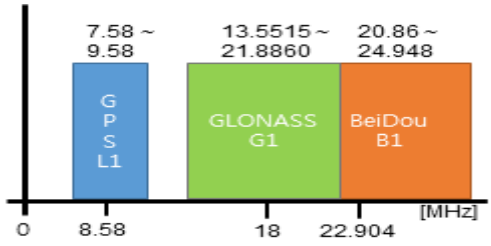

그림 1. SDR 수신기의 IF 주파수 설계
Fig. 1. Plan of IF Frequency for SDR Receiver

그림 2는 SDR 수신기 내부의 데이터 흐름에 대해 나타내며 RF Front-end에서 취득된 신호데이터는 신호 버퍼에 저장되고 상관기에 1ms 단위로 제공되는데, 설정한 Coherent Integration time에 따라 최대 20 ms의 신호를 공급할 수 있다. 신호 획득 단계에서는 상관연산에 필요한 위성신호의 초기정보를 탐색한 다음, 채널정보를 생성 및 갱신하며 신호추적 루프는 상관기/오차측정/채널정보 갱신의 과정을 반복한다. 이때 초기 정보는 신호획득에서 측정된 채널정보를 이용한다. 상관기에서 측정된 Promt 상관값은 비트 추출에 사용되며, 추출된 비트 데이터를 이용해 메시지를 복원하여 궤도력, 송/수신 시간정보 등 항법연산에 필요한 정보를 취득하고 위성위치와 의사거리를 구해 수신기 위치를 추정한다. 신호상관정보, 추적정보, 위성 및 수신기 위치정보, 의사거리, 도플러 맵 등은 IPC 출력 정보에 취합되어 SDR 수신기의 UI 화면으로 출력된다.

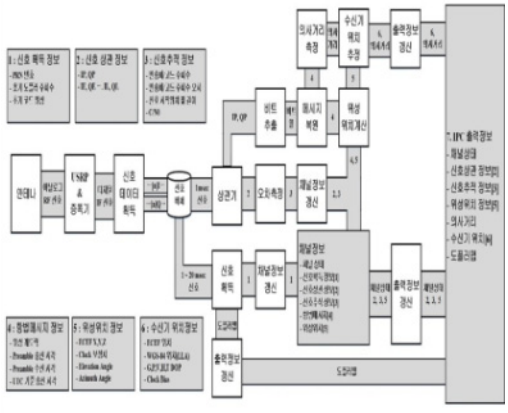

그림 2. SDR 수신기 데이트 흐름도
Fig. 2. Data flow of SDR Receiver

표 1은 SDR 수신기의 신호추적/획득 알고리즘 파라미터를 보여준다. Doppler 탐색 빈도는 Integration time에 따라 달라질 수 있으며, Integration time이 길수록 허용되는 Doppler의 정밀도가 높아져 촘촘한 탐색이 가능하다. Coherent integration time은 신호 추적 및 획득 시 사용할 신호의 길이를 의미하며 길수록 수신감도가 좋아진다. DLL, PLL의 noise bandwidth는 잡음필터에서 통과대역을 의미하며 통과대역이 넓을수록 고주파 성분을 갖게되어 빠르게 변화하는 도플러 및 코드 위상에 적용이 가능하지만, 잡음이 발생하여 정밀도에 영향을 줄 수 있다. 따라서 운용환경에 맞게 적절한 수신기 설정이 필요하다. 한편 DLL chip spacing과 Number of correlators는 다중 상관기와 관련된 정보로 다양한 상관특성을 갖는 수신기를 구현할 수 있다.

표 1. 위성항법 신호 추적/획득 설정 파라미터
Table 1. Parameters of GNSS signal tracking and acquisition

Parameter	Contents	Range
Doppler range	신호 획득시 Doppler freq 탐색 범위	2 ~ 10 kHz
Doppler search bin	신호 획득시 Doppler freq 탐색 빈도	100 ~ 500 Hz
Acquisition threshold	신호 획득 시 Integration 길이	1.0 ~ 20.0
Coherent integration time of acquisition/tracking	신호 추적 시 Integration 길이	1 ~ 20 ms
DLL noise bandwidth	Code tracking loop의 noise bandwidth	2 ~ 10 Hz
DLL chip spacing	Code tracking loop의 Early/Late/Promt 간격	0.1 ~ 1.0 chip
PLL noise bandwidth	Carrier tracking loop의 Noise bandwidth	5 ~ 50 Hz
Number of correlators	Tracking loop의 correlator 수	3/5/7/9

2. 위성항법 기만신호 분석

위성항법 기만신호는 기만하고자 하는 수신기에서 의도된 허위위치로 항법해를 산출하도록 ICD 등을 통해 이미 알려진 위성항법 신호 구조를 모사하여 생성하며 실 위성에서 생성되는 GPS L1 C/A는 다음과 같다.

$$S^i_{L1,C/A}(t^i) = A^i_{L1}(t^i)C^i_{C/A}(t^i)D^i_{L1}(t^i)\sin(2\pi f_{L1}t^i + \phi^i) + \epsilon^i(t^i) \quad (1)$$

수식(1)에서, i는 PRN 번호, t^i는 항법위성의 시각, A^i_{L1}는 신호세기, $C^i_{C/A}$는 C/A PRN 코드, D^i_{L1}은 항법데이터, f_{L1}은 L1 반송파 주파수, ϕ^i는 반송파 초기위상, ϵ^i는 측정 잡음이다. GPS L1 C/A 신호는 정현파 형태의 반송파에 각 위성마다 서로 다른 C/A PRN 코드를 곱하여 생성하며 각 위성의 C/A PRN 코드는 수학적으로 서로 직교하는 특성을 갖는다. 한편, 위성에서 생성된 신호는 공간 상을 전파하면서 매질 변경에 따른 신호의 굴절과 반사, 위성과 수신기의 상대적인 거리와 이동 속도로 인한 관측 시점의 변화 등이 있으며 결과적으로 신호 상에는 코드 지연, 도플러 천이 등의 현상이 반영된다. 따라서 위성항법 기만신호는 기만하고자 하는 수신기에서 수신하고 있는 항법신호의 코드 지연, 도플러 천이, 이온층과 대류층에 의한 지연 뿐만 아니라 기만신호 송신기와 수신기간의 거리 차이에 의한 전파지연까지 고려하여 신호를 생성하여야 하며 수식 (2)와 같이 나타낼 수 있다.

$$J^i_{L1}(T) = S^i_{L1}(T - \tau^i + \tau_{free})I^i(T) + K^i(T) \quad (2)$$

수식(2)에서, $J^i_{L1}(T)$ 는 위성항법 기만신호, τ_{free} 는 기만신호 송신기와 수신기 사이의 거리에 따른 전파 지연, $I^i(\tau)$는 이온층 지연, $K^i(T)$는 대류층 지연을 나타낸다.

3. 위성항법 기만신호 시험 구성 및 결과 분석

위성항법 기만신호의 품질과 효과도를 분석하기 위해 SDR 수신기를 이용하여 그림 3과 같이 시험환경을 구성하였다.

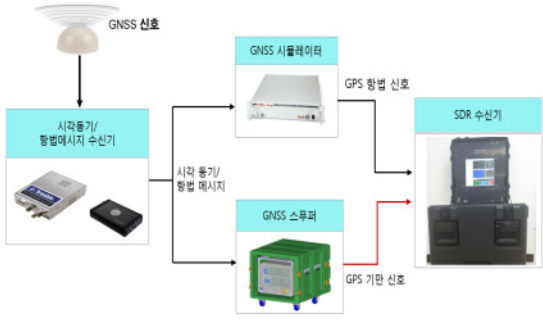

그림 3. 위성항법 기만시험 구성
Fig. 3. Test environtments in Spoofing test

시험방안으로 GNSS 안테나를 통해 실 위성 신호를 수신하고 시각동기 수신기와 항법메시지 수신기를 이용하여 위성항법모의신호 발생기와 위성항법 기만신호 발생기 간의 시각동기(시각 및 1pps)와 항법 메시지 일치화를 수행하였다.

그림 4. 위성항법 기만시험 시나리오
Fig. 4. Scenario for Spoofing test

다음으로 위성항법모의신호 발생기 신호를 인가하여 SDR 수신기가 정상항법을 수행하는지 확인 후 특정방향으로 이동시켰으며 그 이후 위성항법 기만신호를 인가였다. 그림 4는 위성항법 기만시험 시나리오를 보여준다. 그림 4와 같이 위성항법모의신호 발생기를 이용하여 SDR 수신기가 계획경로 방향으로 이동하도록 GPS 신호를 인가하였으며 이동 중 GPS 기만신호를 인가 후 특정 시간이 지난 뒤 기만신호의 경로를 위 방향으로 변경하였으며 SDR 수신기가 기만신호 경로로 이동하는 것을 확인하였다.

그림 5는 GPS 항법 신호와 GPS 기만신호 인가 시 SDR 수신기에서 추적하고 있는 PRN #5 위성신호에 대한 C/No 그래프를 보여준다. GPS 항법 신호를 수신한 SDR 수신기는 PRN #5 위성에 대해 tracking을 하며 항법을 수행 중 약 220 sec 뒤 기만 신호를 수신하여 tracking을 하면서 C/No가 약 6 dB 증가하는 것을 볼 수 있으며 기만신호의 경로가 항법 신호의 경로와 달라지자 C/No가 흔들리다가 기만신호를 tracking 하는 것을 알 수 있다.

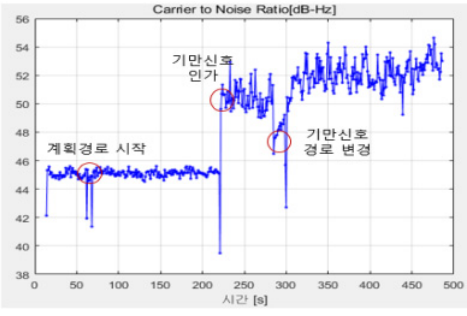

그림 5. PRN #5 신호 C/No 결과
Fig. 5. The results of PRN #5 C/No

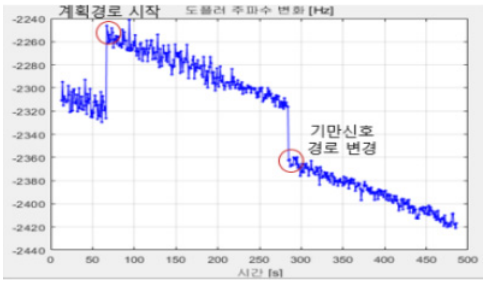

그림 6. PRN #5 신호 도플러 주파수 결과
Fig. 6. The results of PRN #5 Doppler Frequency

그림 6은 PRN #5 위성신호에 대한 도플러 주파수 변화 결과를 보여준다. GPS 항법 신호가 이동하자 일시적으로 PLL 위상이 흔들린 후 고정되는 것을 알 수 있으며 기만신호 인가 후 경로가 변경되자 다시 한번 일시적으로 PLL 위상 추적이 실패되다가 도플러 주파수가 약 50 Hz 변화 후 기만신호를 추적하는 것을 알 수 있다. 한편, 기만신호 인가 시 수신기에서 계산하고 있는 특정 위치보다 거리 이격이 많이 된 기만신호를 인가할 경우 도플러 주파수 변화가 더 커질 것을 예상할 수 있다.

그림 7은 DLL 판별기로부터의 코드 오차를 보여주며 기만신호 인가 시 코드 오차가 증가하였다가 기만 신호를 tracking 하면서 코드 오차가 낮아지는 것을 확인할 수 있다.

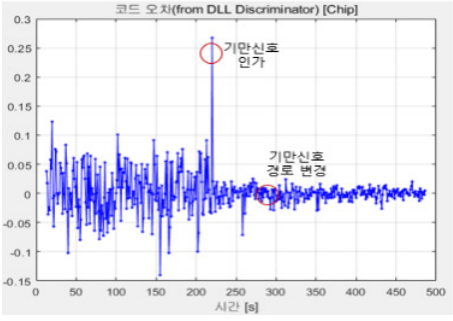

그림 7. PRN #5 신호 코드 오차 결과
Fig. 7. The results of PRN #5 code error

한편, 그림 8은 특정 위성에 대한 상관 결과를 보여주며 SDR 수신기에서 GPS 항법신호와 기만신호 수신 시 전파지연 및 기만신호 위치 오차에 대한 영향성을 분석하기 위해 코드 위상에 대한 상관결과를 분석하였다.

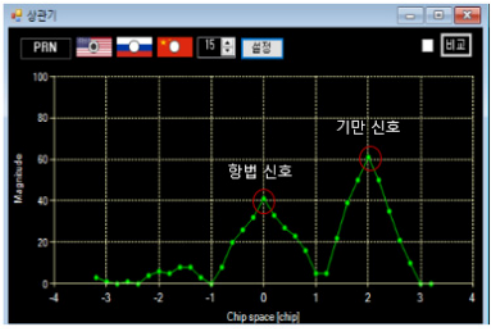

그림 8. 코드 상관 결과
Fig. 8. The results of code correlation

그림 8과 같이 수신기에서 수신하고 있는 항법 신호의 코드 지연 및 전파지연을 고려하지 않고 기만신호 생성 시 수 dB 큰 신호라도 기만신호를 추적하지 않고 항법 신호를 추적하여 항법 해를 도출하는 것을 알 수 있다. 따라서 본 상관 결과를 이용하여 위성항법 기만신호의 품질을 분석할 수 있으며 현재 추적하고 있는 신호 대비 +/- 0.5 chip 범위내의 신호로 인가한다면 수신기에서는 기만신호를 Tracking할 것이다. 따라서 코드 상관 그래프를 이용해 기만신호의 위치 오차 및 전파지연 오차를 확인할 수 있다.

Ⅲ. 결론

본 논문에서는 SDR 수신기를 이용하여 위성항법 기만신호에 대하여 분석하였다. 먼저 다양한 수신기 성능을 구현하기 위해 신호 추적/획득 파라미터를 설정할 수 있도록 SDR 수신기를 구현하였으며 위성항법신호모의 발생기와 위성항법 기만신호 발생기를 이용해 이동 시나리오에 대해 위성항법 기만신호 품질 및 수신기의 신호 추적 알고리즘에 끼치는 영향성을 분석하였다. 한편,대상 수신기를 원하는 위치로 기만하기 위해서는 코드 위상/도플러 주파수/항법메시지/시각 동기 등이 이루어져야 하며 전파지연 특성까지 고려하여야 한다. 따라서 SDR 수신기를 활용하여 기만신호 인가 시 코드 위상/도플러 주파수/신호대 잡음비의 변화를 분석함으로써 유효한 기만신호의 특성을 확인할 수 있다.

References

[1] G. ICD, “Navstar GPS space segment/navigation user interfaces, interface specification, ”IS-GPS-200E E1 Seungdo, CA, USA2010.

[2] Ali Jafarnia-Jahromi, Ali Broumandan, “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques”, International Journal of Navigation and Observation, Vol 2012, Article ID 127072, Feb 2012.
DOI: http://dx.doi.org/10.1155/2012/127072

[3] Nils Ole Tippenhauer, Christina Popper, “On the Requirements for Successful GPS Spoofing Attacks”, In Proceedings of the 18th ACM conference on Computer and communications security, pp. 75-86, Oct 2011.
DOI: https://dl.acm.org/citation.cfm?id=2046719

[4] Mark L. Psiaki, Todd E. Humphreys, “GNSS Spoofing and Detection”, Proceedings of the IEEE, Vol. 104, Issue. 6, pp. 1258-1270, June 2016.
DOI: https://ieeexplore.ieee.org/document/7445815

[5] JOHN W.BETS, KEVIN R. KOLODZIEJSKI, “Generalized Theory of Code Tracking with an Early-Late Discriminator Part I:Lower Bound and Coherent Processing”, IEEE Transactions on Aerospace and Electronic Systems, Vol. 45, Issue. 4, Oct 2009.
DOI: https://ieeexplore.ieee.org/document/5310316

[6] Park, Kwi Woo, Chae, Jeong geun “A Performance Analysis of Multi-GNSS Receiver with Various Intermediate Frequency Plans Using Single RF Front-end”, Journal of Positioning, Navigation, and Timing, Vol. 6, Issue. 1, pp. 1-8, Mar 2017.
DOI: https://doi.org/10.11003/JPNT.2017.6.1.1

[7] Elliott D. Kaplan, “Understanding GPS Principles and Applications”, ARTECH HOUSE, Scond edition

저자 소개

조 지 행(정회원)

- 2010년 8월 : 한밭대학교 전파공학과 공학사
- 2012년 8월 : 전북대학교 전자공학과 공학석사
- 2012년 10월 ~ 현재 : 국방과학연구소 연구원
- 주관심분야 : 위성항법시스템, RF시스템