Journal of Institute of Control, Robotics and Systems (2013) 19(2):113-118
http://dx.doi.org/10.5302/J.ICROS.2013.19.2.113 ISSN:1976-5622 eISSN:2233-4335

실시간 GNSS 기만 시뮬레이터를 이용한 위성항법수신기에서의 기만 영향 분석

An Analysis of Spoofing Effects on a GNSS Receiver Using Real-Time GNSS Spoofing Simulator

임 성 혁, 임 준 혁, 지 규 인*, 허 문 범
(Sung-Hyuck Im[1], Jun-Hyuck Im[2], Gyu-In Jee[2], and Mun-Beom Heo[1])
[1]Korea Aerospace Research Institute
[2]Konkuk University

Abstract: In this paper, spoofing effects on a GNSS receiver were analyzed. The spoofer (spoofing device) was classified to two categories. One is an active spoofer and the other is a passive spoofer. The active spoofer was considered for analysis. For the analysis of spoofing effects on a GNSS receiver, a real-time GNSS spoofing simulator was developed. The simulator was consisted with two parts which are a baseband signal generation part and a RF up-conversion part. The first GNSS baseband signal was generated according to spoofing parameters such as range, range rate, GNSS navigation data, spoofing to GNSS signal ratio, and etc. The generated baseband signal was up-converted to GNSS L1 band. Then the signal transmitted to a GNSS signal. For a perfect spoofing, a spoofer knew an accurate position and velocity of a spoofing target. But, in real world, that is not nearly possible. Although uncertainty of position and velocity of the target was existed, the spoofer was operated as an efficient jammer.

Keywords: GNSS, spoofing, software defined GNSS simulation

I. 서론

근래에 미국은 2006년 10월까지 새롭게 편성되는 DoD (Department of Defense) GPS 시스템에 SAASM (Selective Availability and Anti-Spoofing Module)을 탑재할 것을 권고하였다. 그만큼 기만(spoofing)은 재밍(jamming)과 더불어 GPS에 심각한 타격을 줄 수 있는 방해형태이다. 기만은 기만 신호를 이용한 위성항법(GNSS) 수신기에 대한 교란을 행하는 장치로써 각 위성으로부터 도달하는 GNSS 신호를 추적하는 과정을 효과적으로 기만하여 잘못된 신호추적을 수행하도록 유도하여 GNSS 수신기가 잘못된 위치해를 도출하도록 만드는데 그 궁극적인 목적이 있다. 또한 기존의 재밍신호는 고출력의 전파를 이용하여 GNSS 신호를 교란하는데 반해 기만은 GNSS 신호와 유사한 출력인 -160 dBW 정도의 소량의 출력으로 GNSS 신호를 교란하는데 있어 기존 재밍의 지속시간이 짧은데 비해 장시간의 교란이 가능하다는 특징이 있다. 최근 ION GNSS 2008 학회에서 휴대용 GPS 기만 장비가 1,000불 정도에 제작이 가능하다는 논문이 발표됨으로써 저가의 휴대형 GPS 기만장비의 생산이 가능함이 보여 졌다[4]. 또한 동일한 저자에 의해 무인 헬기의 기만에 성공함을 보임으로써 그 위협 가능성이 점차 높아지고 있다. 따라서 기만에 대한 위협이 현실화됨으로써 정밀도를 생명으로 하는 GNSS를 이용하는 유도장치에 대한 항-기만 기능의 탑재가 절실히 요구되고 있는 상황이다.

현재까지의 국내 연구에서는 단일 채널 위성항법 신호를 대상으로 기만신호에 의한 영향이 분석되었다[7]. 하지만 위성항법 신호는 단일 위성에 대한 신호만을 복제해서는 기만에 성공할 수 없고 완전한 기만을 위해서는 가시위성 전체에 대한 위성 신호를 복제하여야만 기만이 가능하다. 그러므로 기존의 단일채널 기만 모의실험 장치를 확장하여 전체 가시위성에 대한 기만 모의실험이 가능한 실시간 소프트웨어 기만의 기만 모의실험 장치를 사용하여 위치결정 관점에서의 기만에 의한 영향 분석을 수행해야만 한다.

본 논문에서는 상용 위성항법 수신기가 기만신호에 의해서 기만될 수 있는 가능성에 대해서 모의실험을 통하여 확인하였다. 모의실험을 위해서 위성항법 신호와 기만신호를 생성하는 RF 레벨의 실시간 기만재현 시뮬레이터를 개발하였다. 개발된 시뮬레이터는 기저대역의 위성항법 및 기만 신호를 생성하여 RF 신호 발생기를 이용한 주파수 천이를 통하여 L1 대역으로 송출한 후 위성항법 수신기의 안테나 입력에 신호를 인가할 수 있도록 제작되었다.

논문은 총 VI 장으로 구성되어 있으며, II 장에서는 위성항법신호의 특징에 대해 설명하였고 III 장에서는 기만신호의 종류와 특징에 대해서 설명하였고 IV 장에서는 실시간 위성항법 기만 시뮬레이터의 구현에 대해 기술하였으며 V 장에서는 두 종류의 기만실험에 대해서 기술하였고 VI 장에서 논문의 결론을 맺었다.

II. 위성항법 신호의 특징

GPS L1 C/A 코드는 PRN(pseudo-random noise)을 이용한 대

* 책임저자(Corresponding Author)
논문접수: 2012. 12. 3., 수정: 2012. 12. 26., 채택확정: 2012. 12. 31.
임성혁, 허문범: 한국항공우주연구원
(ish@kari.re.kr/hmb@kari.re.kr)
임준혁, 지규인: 건국대학교 전자정보통신공학과
(junhyuck@konkuk.ac.kr/gijee@konkuk.ac.kr)
※ 본 연구는 국토해양부 교통체계효율화사업의 연구비지원(06교통핵심A03)에 의해 수행되었음.

Copyright© ICROS 2013

역확산 신호이다. 잡음(noise)과 유사하게 설계된 2진의 의사 잡음(pseudo random noise) 확산 시퀀스(sequence)는 잡음과 거의 유사하다. 생성된 확산 시퀀스는 그림 1(a)와 같고 그림 1(b)에서와 같은 자기상관 함수를 갖는다.

GPS 기만신호는 위성으로부터 전파된 GPS 신호와 코드 지연이 약 1μs(C/A code chip length) 이하인 경우에 GPS 신호를 교란할 수 있다. 그림 2는 기만신호에 의해서 GPS 신호의 상관함수가 왜곡됨을 나타낸다.

그림 3에서와 같이 GPS 신호와 기만신호 사이의 코드 지연이 1μs 이상인 경우에는 기만신호에 의해서 영향을 받지 않는다.

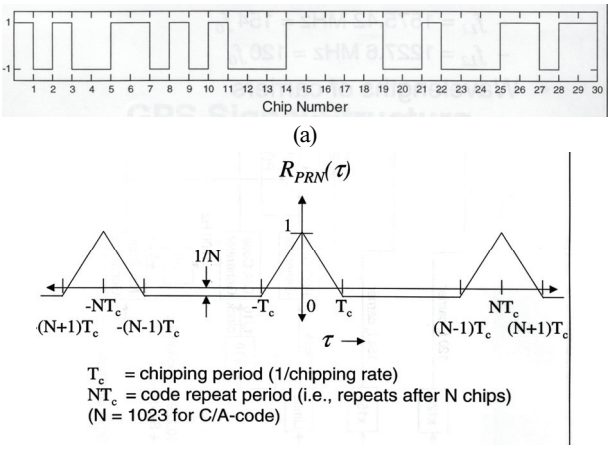

그림 1. PRN 열(a)과 자기상관 함수(b).

Fig. 1. PRN sequences(a) and auto-correlation function(b).

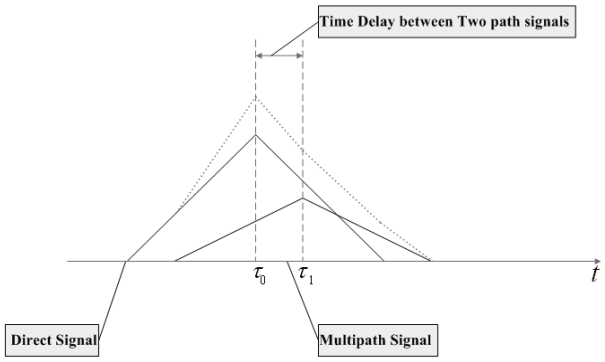

그림 2. 기만신호를 포함한 상관 형태 (지연 < 1 μs).

Fig. 2. Cross-correlation with spoofing signal (delay < 1 μs).

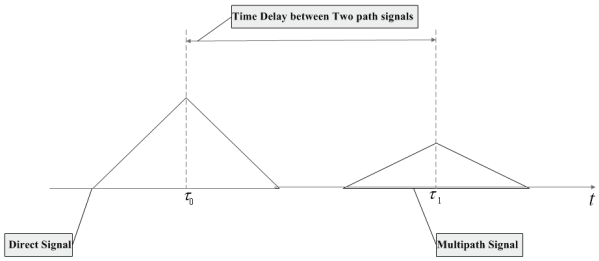

그림 3. 기만신호를 포함한 상관 형태 (지연 > 1 μs).

Fig. 3. Cross-correlation with spoofing signal (delay > 1 μs).

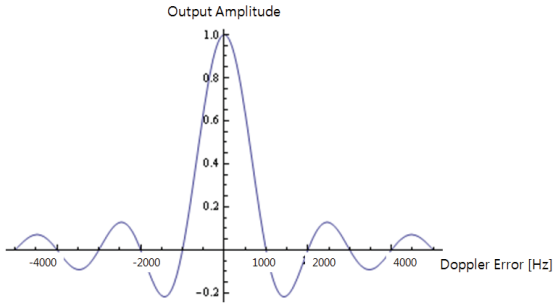

그림 4. 도플러 오차에 따른 전력 세기.

Fig. 4. Output power according to Doppler error.

그림 4는 도플러 오차에 따른 출력 세기를 도식한 것이다. 그림에서와 같이 도플러 오차의 증가에 따라 출력 세기는 급격히 감소하게 된다. 특히 1000 Hz에 가까워지게 되면 출력 세기는 '0' 이 된다.

그러므로 GPS 수신기를 탑재된 항체를 기만 영향을 주기 위해서 기만장치는 항체의 위치에 대한 정보를 최소한 약 300미터 (1μs=1chip) 이내로 추정하여야 하며, 도플러는 1000 Hz 이내로 추정하여야 한다. 신호 대 잡음비를 고려하는 경우 기만장치는 항체의 위치 및 도플러에 대하여 보다 높은 추정 정확도를 필요로 하게 된다.

III. 기만신호의 종류 및 특징

위성항법 신호에 대한 기만을 수행하기 위한 장치는 기만기(spoofer)라고 지칭하며 표 1에서와 같이 능동형(active) 기만기와 수동형(passive) 기만기로 분류할 수 있다. 능동형 기만기는 목표물에 대한 추적기능(레이더 장비 이용)을 포함하여 정해진 목표물에 대한 기만을 가하는 기만형태이고 수동형 기만기는 정해진 목표물에 대한 정보 없이 목표물의 예상 진로를 예측하여 예상 지역을 대상으로 기만을 가하는 기만형태이다. 일반적으로 능동형 기만기는 물체추적 장비의 추적 정확도의 낮음으로 인하여 실제적인 구현이 쉽지 않으므로 특정 지역을 대상으로 위성항법 기만 신호를 생성하여 기만하는 수동형 기만기가 많이 사용될 수 있으며 유도미사일, 비행체 또는 지상차량과 같이 개별적인 기만이 가능한 경우에 한해서 능동형 기만기의 사용이 용이할 수 있다. 마찬가지로 기만기의 형태를 고정형과 이동형 기만기로 분류할 수 있다. 고정형의 경우에는 지상으로부터 위성항법 기만 신호를 발사하여 목표물을 기만하는 형태이며 이동형은 비행체

표 1. 기만기 구분.

Table 1. The caption comes before the table.

구분			장점	단점
기만기	추적기능	능동형 Spoofer	효과적인 기만 가능 (모든 위성신호 기만)	기만지역 협소, 구현이 어려움 (추적장비 필요)
		수동형 Spoofer	광역 기만 가능	인지 및 제거 용이
	이동여부	고정형 Spoofer	고출력 가능	기만지역 제한
		이동형 Spoofer	광범위지역 기만가능	출력 제한

표 2. 기만 전략.
Table 2. The caption comes before the table.

구분	내용
경로/동특성 탐색형 Spoofing	- 유도무기가 지나가는 모든 경로를 찾기 위해서 코드 및 도플러를 변경하며 탐색하여 기만한다. - 일반적으로 Spoofing 신호의 탐지가 쉽고 모든 위성신호를 기만할 수 없지만 넓은 지역에 대한 기만이 가능하다.
경로/동특성 대기형 Spoofing	- 특정 동특성을 가진 유도무기가 지나가는 특정 경로를 지정하여 코드 및 도플러 값을 설정하여 그 지역을 지나가는 유도무기가 기만되도록 함 - Spoofing 탐지가 쉽지 않으며 모든 위성신호에 대해서 기만이 가능하지만 좁은 지역에 대한 기만이 가능하다.

(또는 이동체)나 Buoy 등을 이용하여 기만 신호를 방사하는 형태이다.

수동형 기만기의 경우에는 기만전략(spoofing strategy)이 중요하다. 그 이유는 위성항법 신호의 특성과 기만 목표의 움직임에 의해서 특정시간 및 특정지역에서의 의사거리와 도플러가 결정되게 된다. 그러므로 효과적인 기만을 위해서는 고도로 설계된 기만전략을 필요로 한다. 기만전략을 크게 두 가지로 나누면 표 2와 같이 정리할 수 있다.

결과적으로 위성항법 신호의 기만은 위성항법 신호를 사용하는 장치를 기만하기 위해서는 위성항법 신호와 가장 유사한 신호를 사용하는 것이 기만효과를 극대화하는 방법이다. 그러므로 위성항법 신호의 기만을 위해서는 앞의 2장에서 설명한 위성항법 신호의 일반적인 특성에 대하여 정확한 이해가 필요하며 바꾸어 말하면 기만대응을 위해서는 위성항법 신호의 특성에 대한 이해를 통해서 기만가능성에 대해 연구한 후 취약부분을 보완함으로써 기만을 피할 수 있다.

IV. 실시간 기만 시뮬레이터

위성항법 수신기에 대한 기만신호에 의한 영향을 분석하기 위해서 RF레벨(위성항법 수신기에 직접 인가를 목적으로 함)의 위성항법 및 기만 신호생성 및 처리 장치의 개발이 필수적이다. 따라서 실제 위성항법 신호와 동일한 수준의 신호를 생성할 수 있는 소프트웨어 기반의 위성항법 신호 생성기와 National Instrument사의 RF 신호 발생기와의 결합을 통하여 소프트웨어 기반의 위성항법 신호 생성기를 통해 발생된 기저대역 위성항법/기만 신호를 RF 대역으로 변환하여 송출한다.

그림 5는 기만실험을 위한 GPS/Spoofing 신호 발생장치의 구조를 나타낸 것이다. 기만신호 발생장치는 목표물의 위치/속도와 기만기의 위치 정보를 이용하여 위성항법 신호 기저대역 신호를 생성한 후 National Instrument사의 PXIe-5673(RF Genenrator)로 인가하여 위성항법 RF 신호를 생성한다.

그림 6은 위성항법/기만 신호 발생기의 성능 평가를 위해서 기만 신호가 존재하지 않는 상황에서 상용 수신기인 Novatel사의 OEM-V3와 Ublox사의 LEA-4T에 인가하여 사용된 위성항법 수신기가 개발된 시뮬레이터를 통해 생성된 위

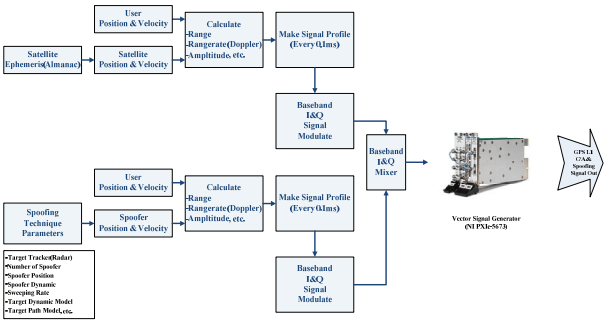

그림 5. 위성항법/기만 신호 발생기 구조.
Fig. 5. Structure of GNSS/Spoofing signal generator.

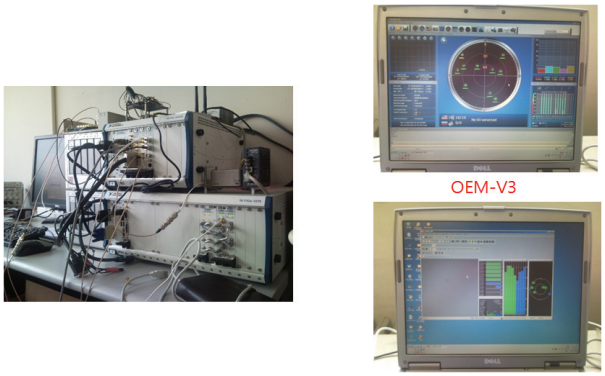

그림 6. 위성항법/기만 신호 발생기 성능 평가.
Fig. 6. Performance evaluation of GNSS/Spoofing signal generator.

성항법 신호에 대한 위치해 정확도를 평가하는 실험 사진이다. 그림을 통해서 생성된 신호를 위성항법 수신기가 정상적으로 추적 및 위치해를 제공함을 확인할 수 있다.

V. 기만 모의 실험

1. 기만기가 목표물의 위치를 정확히 알고 있는 기만상황

위성항법 신호를 기만하기 위해서는 기만하고자 하는 대상의 위치에 대한 정보가 필수적이다. 모의실험을 위해서 최초 기만신호는 기만대상의 위치를 탐지하지 못한 상태에서 시작하여 위치 탐지가 완벽하여 기만신호를 기만대상으로 접근시킨 후 일정시간이 경과한 다음 기만기가 원하고자 하는 위치에 대한 정보를 담은 기만신호를 생성하여 항체에 탑재된 위성항법 수신기의 위치해 출력을 벗어나도록 유도한다.

그림 7은 기만대상(항체)의 목표 궤적을 나타낸다. 약 10 km 고도에서 약 300 m/s의 속도로 북쪽으로 활공하는 물체이다.

항체가 출발한 후 기만기는 항체 경로의 진행방향(along track)과 교차방향(cross track)으로 각각 750미터의 오차를 갖는 위성항법 기만 신호를 생성하여 150초가 되는 순간 항체와 일치하는 위치에 대한 기만 신호를 생성하고 250초부터 기만기는 위성항법 기만 신호를 항체의 진행 경로의 교차방향 우측으로 위치해를 도출하도록 기만 신호를 생성한다.

기만신호와 위성항법 신호의 전력비(JSR)는 0 dB와 5 dB 각각에 대해 모의실험을 실시하였다.

기만신호가 인가되지 않는 경우에는 그림 8에서와 같이 실제 목표 궤적과 수신기가 출력하는 궤적의 정보가 일치함을 확인 할 수 있다.

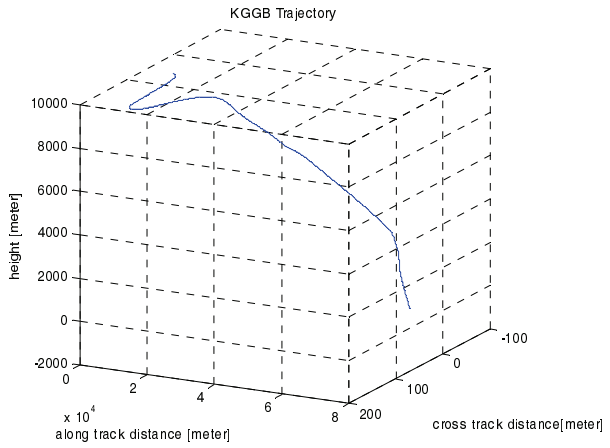

그림 7. 항체의 진행 경로.

Fig. 7. Trajectory of vehicle.

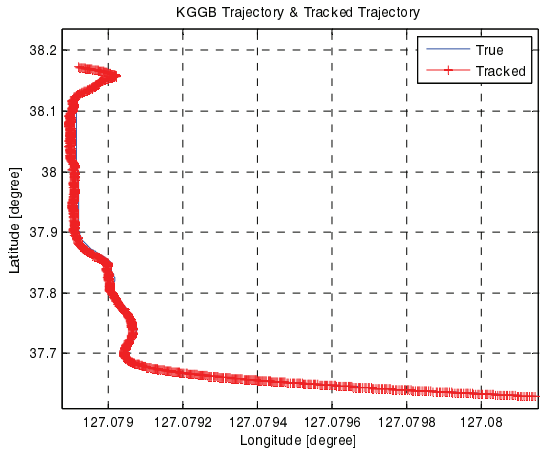

그림 8. 항체 및 수신기 출력 수평면 위치 (기만 없는 경우).

Fig. 8. Horizontal position of target and receiver output (without spoofing).

그림 9~12는 기만신호를 인가한 후 각각의 위성항법 수신기가 출력한 결과를 비교한 것이다.

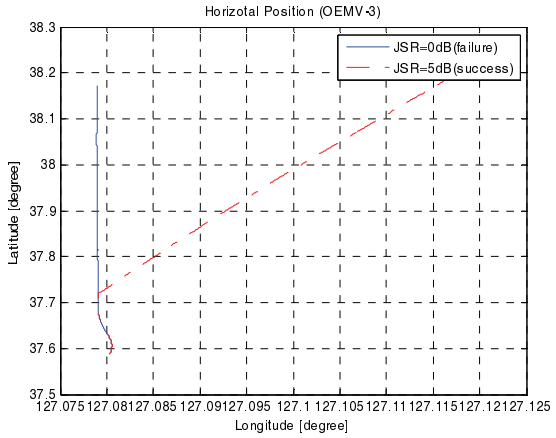

그림 9. 수평면 위치해(OEMV-3): 파란색 실선-기만실패, 붉은색 점섬-기만성공.

Fig. 9. Horizontal position (OEMV-3): blue line-fail spoofing, red dot-successful spoofing.

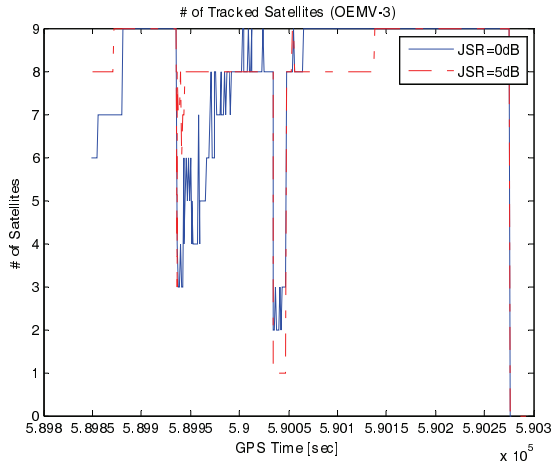

그림 10. 추적 위성 수(OEMV-3): 파란색 실선-기만실패, 붉은색 점섬-기만성공.

Fig. 10. Number of tracked satellites (OEM-V3): blue line-fail spoofing, red dot-successful spoofing.

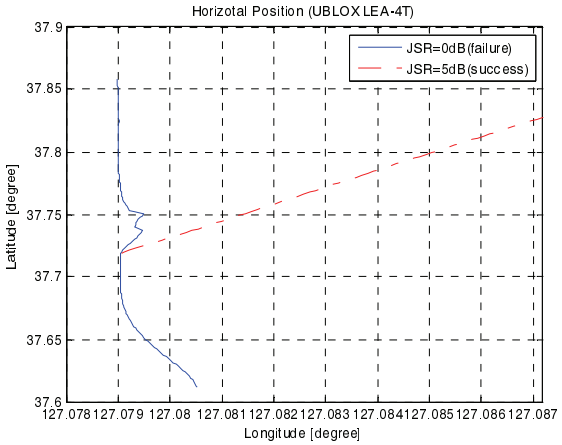

그림 11. 수평면 위치해(LEA-4T): 파란색 실선-기만실패, 붉은색 점섬-기만성공.

Fig. 11. Horizontal position (LEA-4T): blue line-fail spoofing, red dot-successful spoofing.

그림 10과 12에서와 같이 기만신호가 위성항법 신호에 영향을 주는 시점과 영향이 사라지는 시점에서 급격한 신호의 산란(fading)에 의해서 위성항법 신호를 잃는 경우가 발생하게 된다. 이는 기만 성공 여부와 상관없이 발생하며, 기만신호 대 위성항법 신호의 비가 같은 경우 위성신호를 잃은 후에 다시 위성항법 신호를 추적하게 되고 기만신호가 위성항법 신호보다 5 dB가 큰 경우에는 위성신호를 잃은 후에 기만신호를 추적하여 완전히 기만되는 것을 확인할 수 있다.

그림 9와 11은 기만신호에 의해 영향을 받은 위성항법 수신기가 출력하는 수평면 궤적을 나타낸 것이다. 기만신호가 위성항법 신호보다 5 dB 큰 경우에는 완전히 기만되어 붉은 점선과 같이 기만궤적을 출력하는 것을 확인할 수 있다. 또한 기만이 되지 않더라도 그림 11의 파란색 실선과 같이 기만신호에 의한 다중경로오차 발생으로 인하여 저가형 상용 위성항법 수신기는 위치오차가 증가하는 것을 확인할 수 있다.

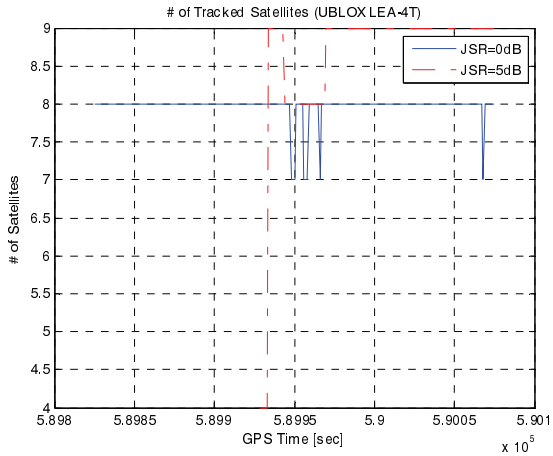

그림 12. 추적 위성 수(LEA-4T): 파란색 실선-기만실패, 붉은색 점섬-기만성공.

Fig. 12. Number of tracked satellites (LEA-4T): blue line-fail spoofing, red dot-successful spoofing.

2. 기만기가 알고 있는 목표물의 위치에 오차가 존재하는 기만상황

현실적으로 목표물의 위치와 속도를 정확히 추정하는 것은 어렵다. 그러므로 위치에 대한 오차가 존재하는 기만상황에 대해 모의 실험을 실시하였다. 위치는 3차원이지만 3차원에 대해 모두 모른다고 가정하는 경우 기만할 수 있는 경우는 복잡해지므로 단순화를 위하여 항체의 진행방향에 대해서는 정확이 안다고 가정하고 항체의 진행방향의 교차방향으로 각각 ±600미터의 기만기의 목표물에 대한 위치추정 오차가 존재한다고 가정하였다.

그림 13은 2대의 기만기가 목표물의 진행방향에 대한 교차방향에 대해서 지그재그로 기만신호를 인가하는 교차방향 위치에서 나타낸 것이다.

그림 14와 15는 각각 수평면 위치 오차와 고도 오차를 나타낸 그림이다. 두 대의 기만 신호는 그림 13과 같이 항체의 진행방향의 교차방향에 대해서 초당 300미터로 진행하게 된다. 그러므로 수초마다 위성항법 신호는 기만 신호에 노출되게 된다. 기만에 의해서 일부 위성이 영향을 받음에 따라 수평면과 수직 위치오차가 발생하게 된다. 표 3은 기만신호에 영향을 받은 전 구간 동안의 평균 위치 오차를 나타낸 것이다.

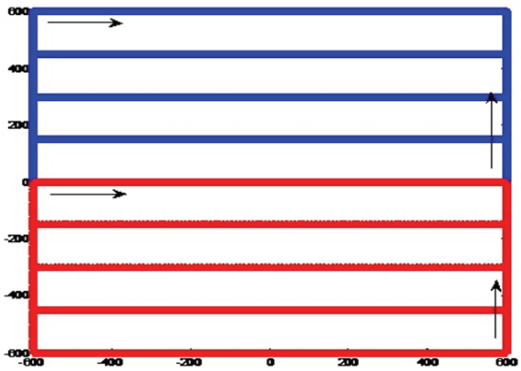

그림 13. 기만 신호 인가 형태.

Fig. 13. Pattern of spoofing signal.

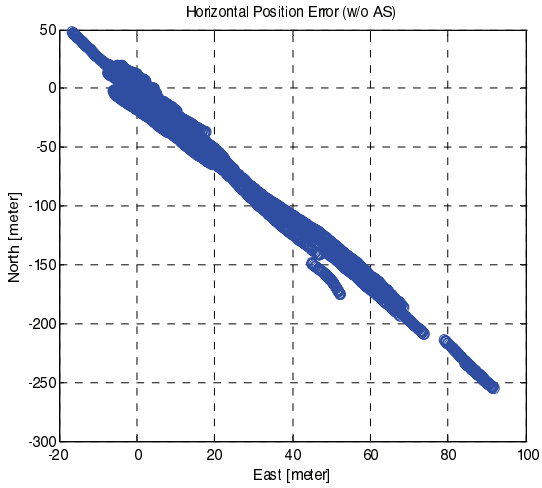

그림 14. 수평면 위치 오차.

Fig. 14. Horizontal position error.

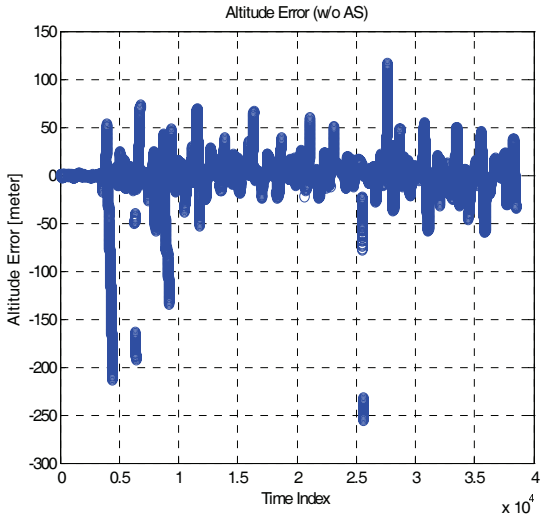

그림 15. 수직 위치 오차.

Fig. 15. Vertical position error.

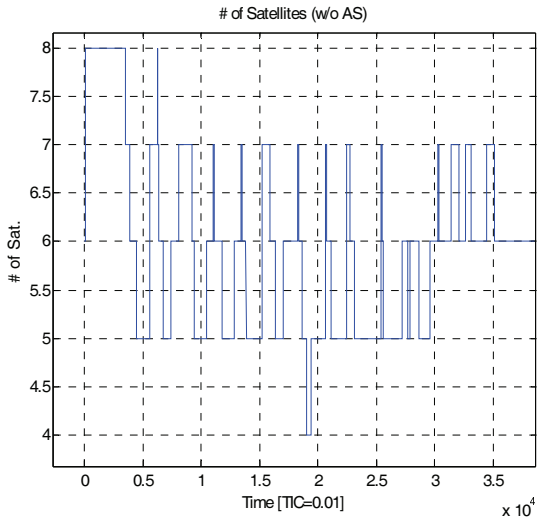

그림 16. 추적된 위성 수.

Fig. 16. Number of tracked satellites.

표 3. 위성항법 수신기 위치 오차.
Table 3. Position error of GNSS receiver output.

구분	East [meter]	North [meter]	Altitude [meter]
오차	8.96	24.66	23.86

VI. 결론

본 논문에서는 실시간 GNSS 기만 시뮬레이터를 이용하여 위성항법 수신기에 대한 기만신호에 의한 영향을 분석하였다. 위성항법 수신기를 기만하기 위해서는 위성항법 수신기의 정확한 위치와 속도정보를 알고 있어야 하며, 위성 항법 데이터를 정확하게 만들 수 있어야 한다. 우선 실시간 GNSS 기만 시뮬레이터를 개발하여 위성항법 수신기에서의 성능 평가를 통해 위성항법 신호를 정확하게 생성함을 확인하였으며 2가지의 기만 모의 실험을 통하여 완전한 기만 또는 위성항법 신호의 부분적 기만이 위성항법 수신기에 미치는 영향을 분석하였다. 완전한 기만을 위해서는 위성항법 수신기가 수신하는 위성항법 신호를 완벽하게 재현하여야 가능함을 확인하였고 부분적 기만을 통해서는 위성항법 수신기가 기만신호에 의해서 특정 위성의 신호를 순간적으로 잃거나 다중경로오차로 인한 오차와 같이 위치해 오차가 증가하도록 만들 수 있음을 확인하였다.

결론적으로 위성항법 수신기를 완전히 기만하기 위해서는 많은 제약조건을 충족시켜야 한다. 하지만 현실적으로 이와 같은 제약조건을 충족시키는 것은 어렵지만 부분적 기만신호는 위성항법 수신기의 위치해 오차를 증가시켜 효과적인 교란신호로 사용될 수 있음을 확인하였다.

참고문헌

[1] B. W. Parkinson and J. J. Spilker Jr, *GPS Positioning System: Theory and Application*, AIAA, 1996.

[2] E. D. Kaplan, *Understanding GPS: Principles and Applications*, Artech House Publisher, Norwood, MA, 1996.

[3] J. B.-Y. Tsui, *Fundamentals of Global Positioning System Receivers : A Software Approach*, John Willey&Sons INC., 2000.

[4] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: development of a portable GPS civilian spoofer," *ION GNSS 2008*, 2008.

[5] S.-H. Im, G.-I. Jee, S.-D. Cho, and S.-J. Ko, "A novel software GPS receiver architecture using partial down conversion," *ION 2007 National Technical Meeting*, 2007.

[6] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, Dec. 2003.

[7] S.-H. Im, J.-H. Im, G.-I. Jee, S.-W. Baek, Y.-W. Lee, and D.-Y. Lee, "Susceptibility of spoofing on a GPS L1 C/A signal tracking loop" *Journal of The Korean Navigation Institute (in Korean)*, vol. 15, no. 1, pp. 32-38, 2011.

[8] S.-H. Im and G.-I. Jee, "A GNSS signal correlation using map-based partial-time common intermediate frequency removal method," *Journal of Institute of Control, Robotics, and Systems (in Korean)*, vol. 14, no. 7, pp. 695-701, 2008.

[9] S.-H. Im and G.-I. Jee, "A implementation of software-based GNSS IF (Intermediate Frequency) signal and IMU (Inertial Measurement Unit) data generator," *12th GNSS Workshop (in Korean)*, 2005.

임 성 혁

2003년 건국대학교 전자정보통신공학과 졸업. 2005년 건국대학교 전자정보통신공학과(공학석사). 2011년 건국대학교 대학원 전자정보통신공학과(공학박사). 2011년~현재 한국항공우주연구원 선임연구원. 관심분야는 실시간 고성능 컴퓨팅기반 GNSS 수신기 신호 처리 및 생성, GNSS anti-jamming/spoofing, GNSS 신호처리, 복합센서 결합 항법.

임 준 혁

2008년 홍익대학교 전자전기공학부 졸업. 2010년 건국대학교 전자정보통신공학과(공학석사). 2011년~현재 건국대학교 전자정보통신공학과 박사과정 재학 중. 관심분야는 무인자동차, Loran-C, 소프트웨어 GNSS, 무선 실내측위.

지 규 인

1982년 서울대학교 제어계측공학과(공학사). 1984년 서울대학교 제어계측공학과(공학석사). 1989년 Case Western Reserve Univ. System and Control Engineering(공학박사). 1992년~현재 건국대학교 전자정보통신공학과 교수. 관심분야는 GPS/INS 결합항법, GPS 수신기 신호처리, 무선측위, 소프트웨어 GPS, GPS anti-jamming.

허 문 범

1992년 경희대학교 기계공학(공학사). 1997년 Illinois Institute of Technology(공학석사). 2004년 Illinois Institute of Technology(공학박사). 2005년~현재 한국항공우주연구원 선임연구원. 관심분야는 위성항법 정밀위치결정, 위성항법시스템고장검출, 위성항법 보강항법시스템.