Live GPS L1 재방송 기만신호 생성 분석

김태희*, 신천식*

Analysis of the GPS Meaconing Signal Generator for the Live GPS L1 Signal

Taehee Kim*, Cheonsig Sin* *Regular Members*

요 약

본 논문에서 Live GPS L1 신호에 대하여 재방송 기만신호를 생성하기 위한 하드웨어 신호생성기를 구현한 후 실험을 통하여 성능을 분석하였다. 재방송과 같은 기만 신호는 사용자가 정확한 시각 및 위치정보를 수신하지 못하도록 거짓된 정보를 전달하는 것을 목적으로 한다. 또한 재방송 기만신호는 안테나를 통해 수신된 신호를 신호처리 없이 지연을 통하여 수신기를 쉽게 기만할 수 있는 특징이 있다. 본 논문에서는 이러한 재방송 기만신호를 생성하기 위한 하드웨어를 설계 제작하였으며 수신된 Live GPS신호를 재 송출함으로써 수신기의 영향을 확인하였다. 최대 지연시간은 약 2.6msec까지 가능하며 또한 이격된 안테나를 통하여 수신기의 위치를 재방송 기만기 안테나의 위치로 이동하는 시험을 성공하였다.

Key Words : GPS, 재방송, 재방송기만, 동기화, 항법해

ABSTRACT

In this paper, we developed the hardware GPS signal generator for generating a GPS L1 meaconing signal with Live GPS signal signals and analyzed the performance of meaconing signal generator thorough the experiment. Deception of the signal, such as a re-broadcast, it is an object of the user to provide false information so as not to receive location information and accurate time. The signal just rebroadcast has the features that can be easily deceive the receiver via a delay of no received signal to the signal processing through an antenna. In this paper, the hardware for generating a signal only these rebroadcast designed and manufactured, by re-sending the received Live GPS signals, to confirm the effect of the receiver. The maximum delay time is possible up to about 2.6msec, also, has been successfully tested to be moved to the position of re-broadcasting based on maturity antenna the position of the receiver through a spaced antenna.

I. 서 론

GPS(Global Positioning System 글로벌 포지셔닝 시스템) 또는 범지구 위치결정시스템은 현재 GLONASS와 함께 완전하게 운용되고 있는 범지구 위성항법시스템이다. 미국 국방부에서 개발되었으며 공식 명칭은 NAVSTAR GPS (NAVSTAR)이다.[1] 무기 유도, 항법, 측량, 지도제작, 측지, 시각동기 등의 군용 및 민간용 목적으로 사용되고 있다.

각각의 GPS 위성은 위성에 탑재된 시계의 시각 및 오차와 위성의 상태 정보, 모든 위성과 관련된 궤도 정보와 상태(almanac), 각각의 궤도정보와 이력(ephemeris), 오차 보정을 위한 계수 등이 포함된 항법메시지(navigation message)를 50 bps의 속도로 지속적으로 방송한다.

이와 같은 항법메시지는 C/A 코드(Coarse/Acquisition code 또는 Standard code)와 P 코드(Precision code)와 함께 반송파(carrier wave)에 실려 송신된다. C/A 코드와 P 코드는 각각 비트율 1.023 Mbps, 10.23 Mbps로 위성마다 고유한 의사잡음부호(PRN, Pseudo-Random Noise)가 담긴다. C/A 코드는 민간에 개방되어 있으나 P 코드는 군사 목적으로 전용하기 위해 공개되지 않은 W 코드를 이용해 암호화되는데, 암호화된 P 코드를 Y 코드 또는 P(Y) 코드라고 한다. P(Y) 코드를 해독하기 위해서는 특별한 장비가 필요하다.[2]

이렇듯 위성항법신호는 군사적 목적으로 사용되었으나 점차 사회전반에 걸쳐 시각동기 및 항법해를 이용한 다양한

*ETRI 위성항법레이더연구실 (thkim72@etri.re.kr)

※ 본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2014-044-052-001 , GNSS전파혼신 검증플랫폼 기술개발 사업]

접수일자 : 2016년 11월 14일, 최종게재확정일자 : 2016년 12월 22일

응용분야에 적용되고 있다.[3] 그러나 항법신호가 가지는 특성으로 해당 항법신호에 대한 전파교란 공격이 증가추세에 있다. 예로 항법수신기가 정상동작을 방해하는 재밍과 항법수신기가 잘못된 항법해를 산출하도록 하는 기만과 같은 공격이 행해지고 있다. 본 논문에서는 단순히 항법위성에서 송출하는 항법신호를 재방송함으로써 암호화된 코드를 사용하는 군용 서비스까지도 기만이 가능한 공격 형태인 재방송 기만기를 구현하고 이에 대한 성능을 분석하였다.

Ⅱ. GNSS 전파혼신 검증플랫폼

■ GNSS 전파혼신 검증플랫폼 개요

GNSS(Global Navigation Satellite System) 전파혼신이 점차 다양화, 고도화(단순 재밍 → 스마트 재밍(Spoofing 및 Meaconing) 추세이고 또한, 전파혼신신호 발생 장치가 판매되고 있다는 점을 고려하여 다양한 전파혼신 신호를 발생하고, 항법수신기 대응특성 측정을 위한 전파혼신 신호 모사, 시험할 수 있는 검증플랫폼 기술을 개발하고 있다. 검증 플랫폼 기술개발에는 GNSS 전파혼신 신호 발생장치 기술, GNSS 전파혼신 신호 측정장치 기술, GNSS 전파혼신 영향평가 기술개발 등이 포함되며 GNSS 전파혼신 신호발생장치는 아래와 같이 3가지 특성을 가지고 있다.[4,5]

- GNSS 전파혼신 신호 발생장치는 7종의 재밍신호를 생성하고 이를 RF로 송출하며 수신 안테나 입력단 기준, 0~ 100 dB까지 J/S(Jamming to Signal Ratio) 레벨 제공
- GPS 신호와 0.1 usec 이내로 동기된 신호를 생성하여 상용수신기들이 이를 감지하지 못해 잘못된 위치 및 시각정보를 산출하는 Spoofing 형태의 전파혼신 신호를 검출하고 이에 대응할 수 있는 알고리즘 개발에 활용할 수 있는 신호 생성
- 또한 생성된 전파혼신 신호를 일정시간 만큼 지연 후, 재전송할 경우 이를 수신하는 수신기들이 산출하는 위치정보가 현재의 자신의 위치가 아닌 신호를 재전송하는 장치의 위치가 되도록 하는 Meaconing에 대한 항법수신기에서의 알고리즘 개발 등에 활용하는데 필요한 재방송 신호(Meaconing signal)생성

본 논문에서는 GNSS 전파혼신 신호 발생장치를 개발하고 GPS L1 신호에 대한 재방송 기만 신호 생성에 대한 성능검증을 수행하였다.

■ GNSS 전파혼신 신호 발생장치 하드에어 구성

GPS신호와 동기된 항법신호를 생성할 수 있도록 구성하였다. GPS신호와 동기된 항법신호를 생성하기 위한 하드웨어 구성도는 다음 그림 1과 같다.

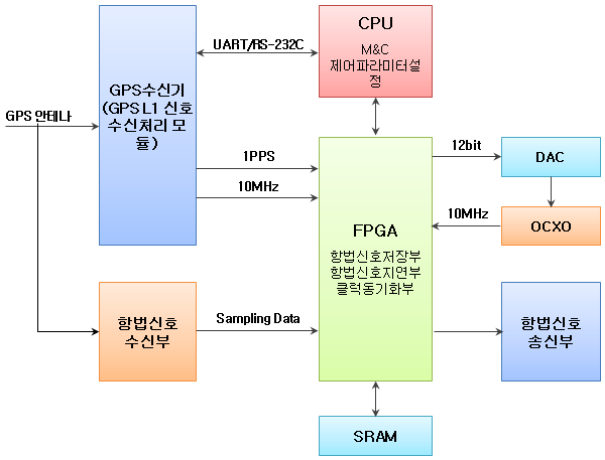


그림 1. GNSS 전파혼신 신호발장치 구성도

하드웨어 기반의 GPS와 동기된 항법신호 생성기는 크게 4가지 모듈로 구성된다. Live GPS신호를 수신하여 항법 정보를 제공할 수 있는 GPS수신모듈, GPS수신모듈에서 GPS 신호처리로 생성한 클럭정보를 이용하여 하드웨어 신호생성기에 기준클럭을 제공하고 GPS수신모듈에서 제공되는 정보를 이용하여 GPS와 동일한 항법신호를 생성하는 신호생성모듈, 신호생성모듈에서 생성한 IF신호를 RF신호로 변환하는 RF변환모듈, 마지막으로 재방송 기만신호생성을 위하여 항법신호를 수신하여 저장한 후 다시 항법신호를 송출하는 재방송모듈로 구성된다.

그림 2는 GNSS 전파혼신 신호발생장치의 하드웨어 구현 형상이며 재방송 기만신호 생성모듈에 대한 보드 형상을 보여주고 있다.

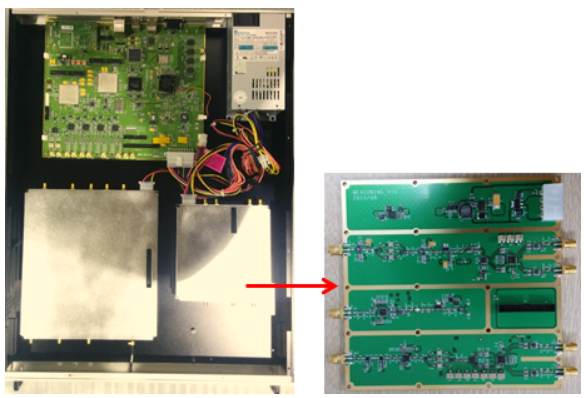


그림 2. GNSS 전파혼신 신호발장치 하드웨어 형상

■ 재방송 기만 신호수신 및 송신부

재방송 기만신호 수신부는 안테나를 통해 수신된 RF 신호를 처리하여 저장 가능한 형태의 신호로 변환하는 기능을 수행한다. 이때 주파수 별로 독립적으로 구성되면 사용자의 선택에 따라 해당 주파수를 처리한다. 재방송 기만신호 수신부는 다음 그림과 3같이 RF 주파수를 하향주파수 변환하기 위한 DC(Down converter), 하향주파수 변환된 아날로그 신

호를 디지털 변화하기 위한 ADC(Analog to Digital Converter), 주파수 대역폭을 제어하기 위한 BPF(Bandpass Filter)로 구성되어 있다.

재방송 기만신호 송신부는 신호생성보드에 저장된 디지털 항법신호를 다시 아날로그 신호로 변환하여 RF로 송출하는 기능을 수행하며 이를 위하여 DAC(Digital to Analog Converter), 상향주파수변환기(UC : Up converter)를 이용하여 안테나로 송출한다.

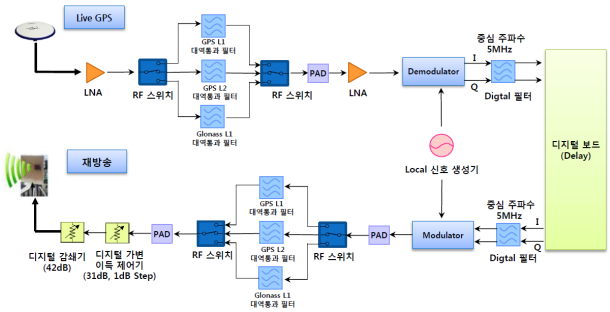


그림 3. 재방송기만 송수신 블럭도

■ 재방송 기만 신호지연부

재방송 기만 신호지연부는 FPGA내에 구현되어 있으며 FIFO를 이용하여 지연에 대한 제어를 수행한다. 재방송 기만 신호지연부에서는 수신된 항법신호의 최종 지연(D)을 위하여 내부적으로 시간 지연값(T)을 이용한다. 다음 그림은 신호지연 알고리즘을 나타낸 것이다.

재방송 기만 신호지연부에서는 GNSS RF 수신부에서 수신한 양자화 된 신호데이터를 수신하여 내부 저장공간에 데이터를 저장한다. 데이터 저장 공간은 신호의 지연값과 양자화 비트수, 샘플링률에 따라 결정된다. 만약 데이터를 저장할 공간이 부족한 경우 가장 먼저 수신한 데이터를 삭제하고 현재 입력된 데이터를 저장한다. 데이터를 저장한 후 사용자로부터 입력된 재방송 기만 지연시간값(D)에 따라 저장된 데이터를 추출하여 RF 생성모듈로 데이터를 전송하게 된다.

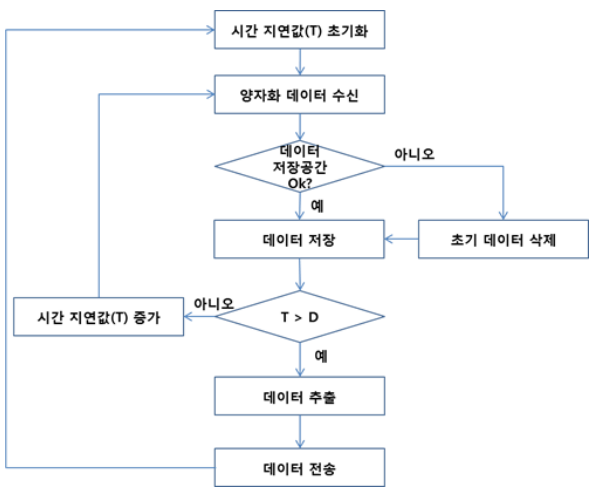


그림 4. 재방송 기만신호 지연 알고리즘

재방송 기만의 성능 목표치인 5usec 신호지연을 위해 필요한 데이터 정장공간은 다음과 같이 계산될 수 있다. GPS L1 및 L2 신호의 경우 2M 대역에서 신호의 95%이상 존재하기 때문에 샘플링률을 2M의 2배 이상으로 설정해야 하며 GPS L1/L2 신호를 수신하기 위한 샘플링률을 5.714MHz로 설정할 경우 5usec 동안 저장되어야 할 데이터는 28.57 바이트가 된다. 그러나 GLONASS L1의 경우 FDMA 방식을 사용하기 때문에 중심주파수인 1602MHz를 중심으로 0.5625MHz 단위로 14개의 채널이 존재하며 약 8M의 대역에 신호가 분포하게 된다. 따라서 샘플링률은 적어도 16M 이상으로 설정해야 한다. 샘플링률이 16M일 때 5usec에 해당하는 저장 공간은 80 바이트가 된다. 샘플링률 결정은 RF 신호를 양자화된 IF 신호로 변환한 후 다시 RF 신호로 변환할 때 원래의 RF 신호와 동일하게 생성될 수 있는 값으로 결정해야 한다. 만약 샘플링률이 너무 낮으며 원래의 신호로 복원할 수 없기 때문이다. 따라서 이론상으로 결정된 값을 기반으로 실제 실험을 통하여 적정한 값을 선택하여 적용하여야 한다.

III. 성능평가

1. 실험 환경

GPS L1 신호에 대한 재방송 기만시험을 두 가지 형태로 진행하였다. 첫 번째는 재방송 기만기의 최대 시간지연을 측정하기 위한 실험을 수행하였고 두 번째로 수신기의 위치가 재방송 기만기의 위치로 이동하는 시험을 진행하였다.

재방송 기만기의 최대 재방송 지연 신호 송출을 검증하기 위하여 다음 그림 5와 같이 실험 환경을 구축하였다.

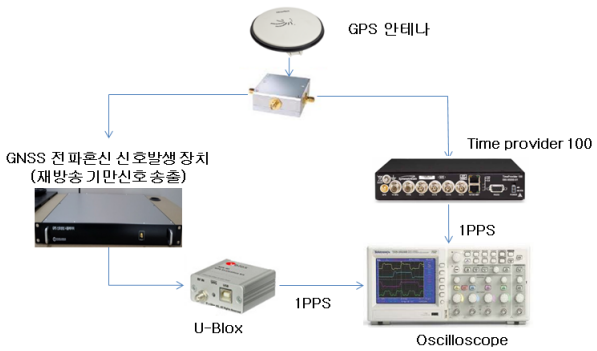


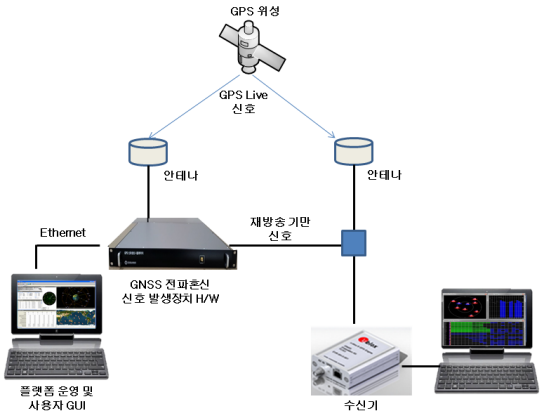
그림 5. 재방송 기만신호 시간 지연 실험 환경

동일한 안테나로부터 수신된 GPS 신호를 정상적으로 신호를 처리하는 수신기(Timeprovider100:TP100)와 재방송 기만기로부터 재방송된 지연신호를 수신하는 수신기(U-Blox Evaluation kit)의 1PPS를 오실로스코프를 통하여 비교 측정하였다. 재방송 기만기에서 안테나로부터 수신한 신호를 재방송하기 위한 파라메터는 표1과 같다.

표 1. 신호 생성 파라메터

Item	Value
Sampling Rate	50 Mbps
IF Frequency	5 Mhz
Quantization Bit	16bit

재방송 기만신호에 의한 수신기 위치변화 영향을 실험하기 위하여 남북으로 약 15m 이격되게 안테나를 위치하고 각 안테나로 수신된 신호를 재방송 기만기와 U-Blox 수신기의 입력으로 인가하였다. 재방송 기만기로부터 출력된 신호는 U-Blox 수신기로 인가되는 신호와 결합하여 재방송 기만신호의 영향을 분석하였다. 재방송 기만신호에 의한 위치변화 확인 실험환경은 그림 6과 같다.



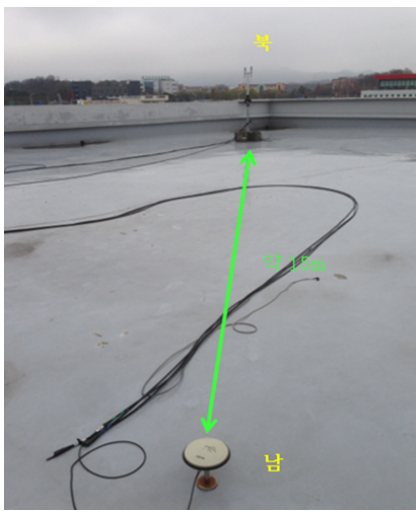


그림 6. 재방송 기만신호 위치 이동 실험 환경 및 안테나 배치

재방송 기만신호 생성 실험을 위한 파라메터는 다음 표2와 같다. 실험 시작 후 약 38초 되는 시점에 재방송 기만신호를 약 1분 44초 동안 지속 생성하여 안테나로부터 수신되는 신호와 결합하여 U-Blox 수신기로 인가하였다.

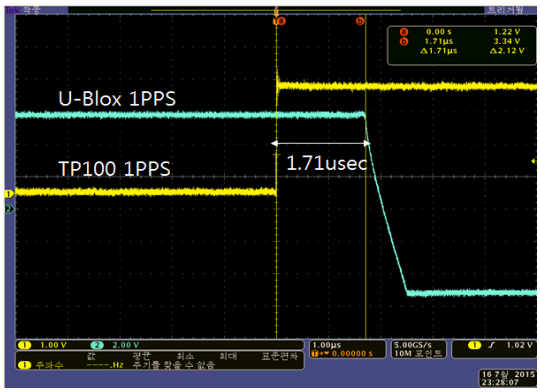
표 2. 신호 생성 파라메터

Item	Value
총 실험 시간	5분 20초
재방송 기만신호 생성 시점	38초
재방송 기만신호 지속시간	1분 44초

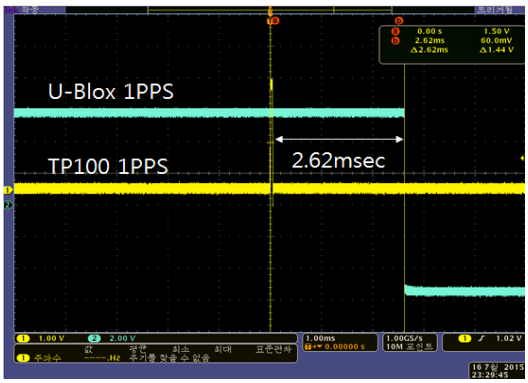
2. 실험 결과

그림 7의 (a)는 GNSS 전파혼신 발생장치에서 재방송 기만신호 생성 시 최소 시간 지연값을 U-Blox 수신기와 TP100 수신기를 이용하여 측정한 것이며 (b)는 최대 지연시간값을 측정한 것이다. GNSS 전파혼신 발생장치에서 재방송 기만신호를 생성하기 위하여 재방송 기만 RF보드에서 Live GPS 신호를 수신하여 샘플링률에 따라 신호를 양자화하여 신호처리보드의 FPGA의 FIFO 메모리에 저장 후 일정 시간지연 후 다시 재방송 기만 RF보드를 통하여 송출함으로써 재방송 기만신호를 생성할 수 있다. 이때 GPS신호가 수신되어 FIFO에서 지연을 주지 않고 바로 GPS신호를 재방송 송신할 때까지의 하드웨어적 지연을 측정한 것이 그림 의 (a) 의 시간 지연이 된다. 이렇게 측정된 값은 GNSS 전파혼신 발생장치에서 재방송 신호를 생성하여 수신기에 영향을 주기위한 시간 옵셋값(t')으로 사용된다. 즉 재방송 기만 공격을 수행하기 위한 목표 수신기에서 수신하는 신호의 시간값을 정확하게 일치하기 위해서는 이렇게 측정된 시간 옵셋을 반영하여 FIFO에서 지연을 인가한 후 신호를 송출해야 한다. 수신기와의 시간을 일치하는 것은 현재 수신기가 수신하고 있는 코드위치를 일치하는 것과 동일하다. 이를 위하여 FIFO에서 재방송 기만을 위하여 시간을 지연할 때 GPS L1 신호가 1msec의 코드주기를 갖는 특성을 이용하여 지연시간을 결정해야 한다. 예를 들어 재방송 기만을 위하여 재방송 기만기와 동일한 위치의 수신기를 기만하기 위해서는 1msec 단위로 동일한 코드위치에 해당하는 신호를 송출해야 한다. 즉 재방송 기만기에서 1msec 지연을 위해서는 FIFO에서 1msec - t'의 시간 지연 후 송출하면 된다.

그림 7의 (b)는 GNSS 전파혼신 발생장치의 FIFO에서 최대 신호 지연을 할 수 있는 시간값이다. 현재 GNSS 전파혼신 발생장치에서 재방송 기만을 위한 샘플링이 50Mbps로 설정된 상태에서 약 2.62msec의 지연이 가능하다. 최대 지연시간값은 FIFO에 저장할 수 있는 공간의 크기와 비례한다. 또한 샘플링률이 낮을수록 더 많은 샘플데이터를 저장할 수 있기 때문에 지연 시간값 또한 증가할 수 있다.최대 지연시간으로 수신기에 영향을 줄 수 있는 것은 수신기의 시각을 변화시킬 수 있게 된다.



(a) 재방송 기만신호 최소 지연



(b) 재방송 기만신호 최대 지연
그림 7. 재방송 기만신호의 시간 지연 비교

그림 8은 그림 에서와 같이 서로 이격된 안테나를 이용하여 GPS수신 신호를 수신하여 생성한 재방송 기만신호에 의해 수신기의 위치가 이동하는 현상을 측정한 것이다.

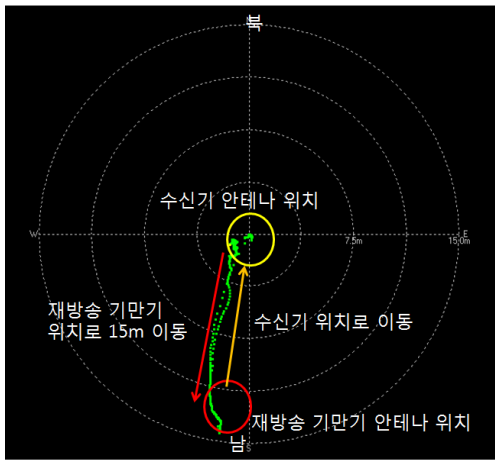
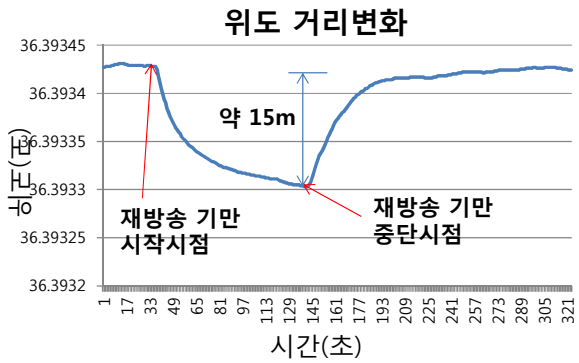


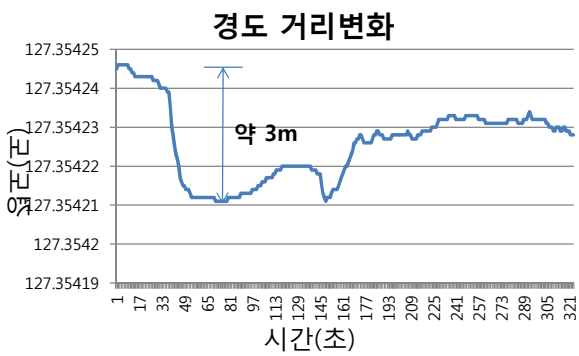
그림 8. 재방송 기만신호의 위치변화 비교

GNSS 전파혼신 발생장치로 수신되는 안테나의 위치는 공격 목표 수신기의 위치에서 남쪽으로 약 15m 위치시켰다. 정상적으로 GPS Live 신호를 수신하고 있는 수신기에 재방송 기만신호를 생성하여 수신기에 인가할 경우 수신기의 위치가 재방송 기만신호 생성기의 위치로 이동하였으며 재방송 기만신호 생성을 중단할 경우 다시 원래의 수신기위치로 이동하는 것을 확인하였다. 두 안테나의 위치에서 위성 신호를 수신할 경우 거의 동일한 시간으로 신호를 수신할 수 있기 때문에 GPS Live 신호를 1msec 신호를 지연시켜 같은 위성별 코드위치를 동기시켜 재방송 기만신호를 생성하였다. 재방송 기만신호를 수신기에 인가할 경우 신호의 끊김없이 수신기의 위치좌표가 이동하였고 재방송 기만신호를 중지할 경우에도 마찬가지로 신호 끊김없이 원래 수신기 위치좌표로 이동하였다.

그림 9의 (a)(b)는 그림 에서 보여준 재방송 기만신호에 의해 수신기의 위치좌표가 이동한 결과를 시간의 흐름에 따른 수신기의 위도 및 경도좌표를 그래프로 나타낸 것이다. 그림 의 (a)는 시간에 따른 위도 거리변화를 나타낸 것이다. 위도 36도에서 1도에 해당하는 거리는 약 110979m에 해당한다. 따라서 재방송 시작 전의 위도에서 재방송 시작하여 재방송 안테나로 수신기의 위도 좌표가 약 0.00015도 이동하였으므로 거리로 환산하면 약 15m에 해당한 값이 나온다. 또한 재방송 기만신호의 인가로 인하여 수신기의 위치좌표가 끊김없는 현상은 재방송 기만신호의 코드위치와 수신기에서 수신하고 있는 코드위치가 1칩 이내로 동기가 유지된 것으로 판단된다. 그림 의 (b)는 시간에 따른 경도 좌표를 그래프로 나타낸 것이다. 그림 의 (a)와 동일하게 재방송 기만신호가 생성된 시점부터 값의 변화가 발생하며 재방송 기만신호 중단 후 수신기의 원래 좌표로 이동하고 있다. 위도 36도 지점에서 경도 1도에 해당하는 거리는 약 90111m 가 되므로 재방송 기만신호에 의한 경도좌표의 이동거리는 약 3m가 되며 그림에서 측정된 값과 유사하게 나타나고 있다.

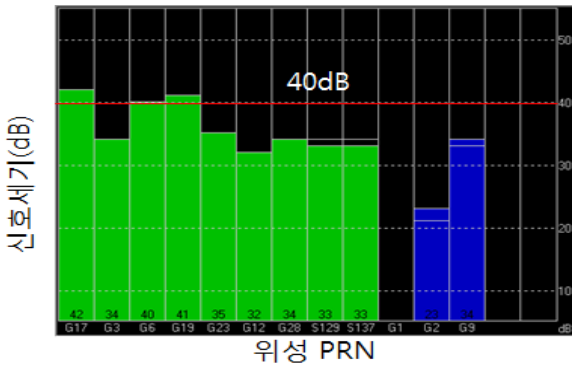


(a) 재방송 기만신호에 의한 동서방향 거리변화

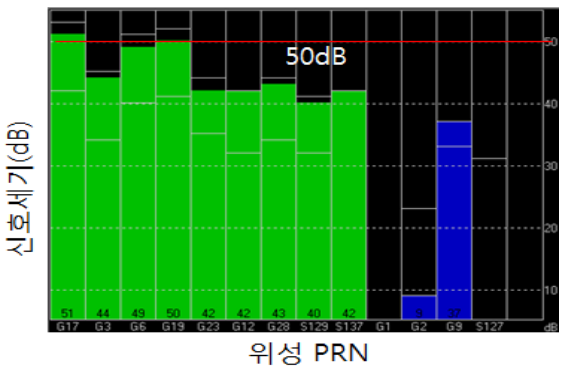


(b) 재방송 기만신호에 의한 남북방향 거리변화
그림 9. 시간에 따른 항법해 오차 영향

그림 10의 (a)는 정상적으로 GPS신호를 수신하였을 때 위성별 신호세기를 나타낸 것이고 (b)는 재방송 기만신호를 인가하였을 때 위성별 신호세기를 나타낸 것이다. 정상적인 GPS 신호를 수신하였을 경우 약 40dB 이하로 신호세기가 측정되는 반면 재방송 기만신호를 인가하였을 때 동일한 위성 PRN의 신호세기가 약 10dB 증가된 것을 확인할 수 있다. 이는 정상적인 신호를 수신하는 수신기를 기만하기 위해서는 수신되고 있는 신호의 세기보다 높게 송출해야지만 수신기가 송출된 재방송 기만신호의 영향을 받을 수 있게 된다. 따라서 실험을 위해 재방송 기만신호의 송출 출력을 GPS 신호보다 약 10dB 높게 설정하였다.



(a) 정상 GPS 수신 신호세기



(b) 재방송 기만신호 영향에 의한 신호세기
그림 10. 재방송 기만신호에 의한 신호세기 비교

IV. 결론

본 논문에서는 GNSS 전파혼신 검증 플랫폼 과제에서 개발 중인 GNSS 전파혼신 신호발생장치를 구현하고 GPS Live 신호에 대한 재방송 기만신호 생성에 대한 성능을 실험을 통하여 시각과 위치변화 측면에서 분석하였다. 재방송 기만신호의 위치변화에 대한 영향을 분석하기 위하여 GNSS 전파혼신 신호발생장치에서 Live GPS RF 신호를 수신한 후 저장하고 공격대상 수신기와 동기를 위한 시간만큼 지연한 후 저장된 신호를 다시 RF신호로 변환하여 송출하여 수신기에 인가한 경우 수신기의 위치가 재방송 기만기의 우치로 이동하는 것을 확인하였다. 이는 Live GPS 신호를 신호처리하지 않고 단지 디지털 신호를 샘플링하고 일정 시간만큼 지연하여 수신기를 기만할 수 있는 것을 확인하였고 상용수신기 뿐만 아니라 군용수신기에도 손쉽게 영향을 줄 수 있음을 의미한다. 또한 샘플링률을 주파수별로 개별 할당할 경우 현재의 2.6ms 이상의 지연을 인가할 수 있을 것으로 판단된다. 향후 해당 GNSS 전파혼신 신호발생장치를 이용하여 GPS L2/GLONASS L1 신호에 대해서도 재방송 기만을 위한 실험을 진행할 예정이다.

참 고 문 헌

[1] Parkinson, B.W. (1996), Global Positioning System: Theory and Applications, chap. 1: Introduction and Heritage of NAVSTAR, the Global Positioning System. pp. 3-28, American Institute of Aeronautics and Astronautics, Washington, D.C.

[2] 신미영, 조성룡"GPS 신호기만의 특성 및 수신기에 미치는 영향 분석", 한국군사과학기술학회지 제13권 제2호, pp. 296~303, 2010년 4월

[3] SCOTT, L. "Anti-spoofing & authenticated signal architectures for civil navigation systems" In Proceedings of the ION GNSS International Technical Meeting of the Satellite Division (2003).

[4] 김태희, 신천식,"복합혼신 신호생성 방안 설계"2015 KGS conference 374-377

[5] 김태희, 신천식, "Live GPS L1과 동기된 항법신호 생성 분석", 통신위성우주산업연구회논문지 제10권 제1호 PP 71-76

저자

김 태 희 (Taehee Kim)

- 1999년 2월 : 전북대학교 컴퓨터공학과 학사졸업
- 2001년 2월 : 전북대학교 컴퓨터공학과 석사졸업
- 2001년1월 ~ 현재 : 한국전자통신연구원 선임연구원

<관심분야> : 위성항법, 통신프로토콜, 소프트웨어 기반 실시간 위성항법 수신기 및 신호생성기

신 천 식(CheonSig Sin) **정회원**

- 1990년 2월 : 한양대학교 전자공학과 학사졸업
- 2000년 2월 : 충남대학교 전자공학과 석사졸업
- 2005년 3월 ~ 현재 : 한양대학교 전자컴퓨터 통신공학과 박사과정
- 1990년 2월 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야> : 위성통신, 위성항법, 위성궤도 주파수