GPS L1 신호에서 코드지연에 따른 기만신호 영향 분석

김태희*, 신천식*, 이상욱*

Analysis of Effect of Spoofing Signal According to Code Delay in GPS L1 Signal

Taehee Kim*, Cheon Sig Sin*, Sanguk Lee* *Regular Members*

요 약

본 논문에서는 기만신호의 영향을 분석하기 위하여 기만신호의 코드지연에 따른 코드 및 반송파 추적에 대한 결과를 분석하였다. 기만신호의 특성 및 방어 방법에 대한 조사를 통하여 현재 GPS 신호와 동기를 유지할 수 있는 중급기만을 고려하여 기만신호생성기를 이용하여 시뮬레이션을 수행하였다. 기만신호생성기에서 생성한 정상신호 및 기만신호가 합성된 신호를 소프트웨어 수신기를 통하여 신호처리를 수행하였다. 본 논문에서는 코드추적루프(DLL) 및 위상추적루프(PLL)의 출력값을 비교분석하여 기만신호의 영향을 파악하였으며 또한 기만신호 인가 시 잘못된 의사거리에 따른 항법해의 영향을 분석하였다. 결과적으로 기만신호의 영향은 신호추적 단계에서는 1칩 이내의 코드지연을 갖는 기만신호의 영향을 받으며 신호획득에서는 코드 지연에 상관없이 영향을 받는 것을 확인하였다.

Key Words : 위성항법, 기만, GPS

ABSTRACT

In this paper, we analysis the effect of error of code tracking and frequency tracking according to the chip delay of spoofing signal through the simulation. Firstly, we investigate the type of spoofing signal and defense technical of spoofing attack. For simulation, we generated the intermediate spoofing signal using the software GNSS signal generator simulator(SGGS), the intermediate spoofers synchronize its counterfeit GPS signals with the current broadcast GPS signals. The software GPS receiver simulator(SGRS) received the spoofing signal and normal signal from SGGS, and process the signals. In paper, we can check that the DLL and PLL tracking loop error are generated and pseudo-range is changed non-linear according to chip delay of spoofing signal when the spoofing signal is entered. As a result, we can check that navigation solution is incorrectly effected by spoofing signal.

I. 서 론

위성항법 시스템은 초기 미국의 군사적 목적인 GPS로부터 최근 유럽의 Galileo, 중국의 Compass 등 다양한 위성항법시스템이 개발되고 있다. 이러한 항법시스템은 사회 전반적인 분야에서 활용되고 있다. 흔히 우리가 접할 수 있는 분야는 차량용 항법 시스템이고 더 나아가 인명구조, 화제진화 등의 사회 안전 및 이동통신 분야에서 시각동기, 금융 시스템의 동기 등의 기간 분야의 활용도가 높아지고 있다.

이렇듯 사회 전분야에서 위성항법 시스템의 활용도가 높아지고 있는 상황에서 항법시스템의 장애야 말로 사회적 혼란을 야기할 수 있다.[1]

최근 북에서 GPS 혼신원을 발생하여 경기도 북부지역 및 강원도 지역에서 정상적인 항법신호를 수신 처리할 수 없는 상황이 발생하였다. 이는 북에서도 항법시스템의 교란도 하나의 공격무기가 됨을 인지하고 새로운 형태의 도발을 감행하고 있는 상황이다.

위성항법신호의 교란의 형태는 크게 두 가지로 나누어 볼 수 있다. 첫째 재밍(Jamming)신호 송출에 의한 항법 단말기의 무력화 기능이다. 이는 항법신호와 동일한 RF 주파수 대역에 신호세기가 큰 톤(tone) 신호, 협대역 신호 또는 광대역 신호를 발생하여 GPS수신기가 신호추적을 수행할 수 없도록 하는 것이다. 재밍신호는 일반 항법신호세기(-163dBW)보다 훨씬 큰 고출력의 신호를 전송해야하므로 장시간 사용

※ 본 연구는 방송통신위원회 및 정보통신연구진흥원의 IT 연구개발사업 프로그램의 일환으로 수행하였음.
*ETRI 위성항법연구팀 (thkim72@etri.re.kr)
접수일자: 2012년 6월 13일, 수정완료일자: 2012년 6월 19일, 최종게재확정일자: 2012년 6월 25일

이 어려운 단점이 있으나 간단하게 재밍신호가 도달하는 광범위한 지역의 항법단말기 동작을 방해할 수 있는 장점이 있다. 또한 최근 지능적인 형태의 재밍신호로 톤 신호를 스위핑(Sweeping)하는 방법을 사용하는데, 이는 협대역 또는 광대역 신호보다 낮은 신호출력을 이용한 톤 신호를 항법주파수 대역에서 주파수를 이동하며 톤 신호를 발생하는 것이다. 해당 재밍신호를 수신하는 입장에서 대응이 어렵다는 장점이 있다. 위성항법 신호의 두 번째 교란형태는 기만신호 송출에 의한 항법 단말기의 오동작을 유도하는 것이다. 기만신호의 경우 재밍신호와 달리 항법 단말기에서 파악하기 어려우며 정상적으로 동작하는 것으로 인지하며 동작하기 때문에 재밍신호 형태보다 위험한 공격방법이다. 기만신호는 기존의 위성항법 신호세기와 유사한 신호세기(-160dBW)를 이용하여 위성항법 신호를 교란하게 된다. [2]

Ⅱ. 기만신호 형태 및 대처 방안

기만신호의 형태는 크게 3가지로 나누어 볼 수 있다.

1. 초급기만

초급기만은 GNSS 신호생성 시뮬레이터를 이용하여 RF 신호를 송출하는 형태의 기만이다. 초급기만신호 생성기는 현재 GPS위성과 시각 동기없이 기만신호를 생성하여 기만대상 수신기에게 신호를 전송하게 된다. 기만신호 대상 수신기에서 새로운 신호획득을 수행할 경우 기만신호에 따라서 비정상적인 위치를 산출하지만, 새로운 신호획득이 아니라 현재 추적된 수신 채널에 영향을 미칠 확률은 현저히 떨어지게 된다. 따라서 초급 기만의 형태는 단순한 형태의 기만신호를 생성하여 불특정 다수의 기만 대상을 목적으로 하고 있다.

이러한 기만에 대한 대처방안은 현재 기만대상 수신기에서 처리하고 있는 가시위성 이외의 PRN에 대하여 제거하는 방법이 있다.

2. 중급기만

중급기만은 현재 GPS 위성에서 전송하는 신호와 동기를 맞춰 기만신호를 생성하는 형태이다. 이와 같은 중급기만 신호생성기는 현재 GPS신호를 처리하기 위한 GPS 수신기 및 GPS 정보를 이용하여 기만신호를 생성하기 위한 기만신호 생성기로 구성된다. 중급기만 신호생성기는 현재 GPS 신호를 처리하기 때문에 위성별 도플러 쉬프트, 항법데이터 비트, 신호세기 등의 정보를 추출하여 기만대상 수신기로 GPS 신호와 동일한 형태의 기만신호를 송출하게 된다. 기만대상 수신기에서는 해당 기만신호를 수신할 경우 현재 수신하고 있는 정상적인 신호 대신 기만신호를 처리하여 잘 못된 위치를 산출하게 된다. 이렇듯 현재 GPS 신호와 동기를 유지하기 때문에 보다 쉽게 기만대상 수신기를 기만할 수 있게 된다.

중급 기만신호에 대한 간단한 대처방안은 신호처리를 통한 해당 기만된 PRN의 신호세기, 측정값, 항법메시지, 항법해등의 값을 이용하여 기만신호 PRN을 검출하고 해당 PRN을 제거하는 방법이 있다. [3,4]

3. 고급기만

고급기만은 중급기만의 보다 향상된 형태의 기만이다. 고급기만은 다중 안테나를 이용하여 다수의 기만대상 수신기로 기만신호를 송출할 수 있는 형태이다. 즉 고급기만은 기만대상이 하나의 수신기가 아니라 다수개로 각각의 기만대상 수신기에서 GPS위성신호와 동일한 형태의 기만신호를 각각 생성하여 전송할 수 있다.

현재 기만신호에 대한 연구는 기만신호 검출 위주로 이루어지고 있으며 기만신호 대응방법에는 현재 해당 PRN을 제거하는 기초적인 방법들이 사용되고 있는 상황이다.

Ⅲ. 소프트웨어 기반의 기만신호 생성기

1. GPS 기만 신호 특성

GPS L1 신호는 상용으로 사용되고 있는 C/A 코드와 암호화한 군용 P코드로 나누어진다. C/A 코드는 1.023MHz의 1ms 주기를 갖는 반면 P코드는 10.23MHz의 1주일의 코드주기를 갖는다. 일반적으로 암호화 및 코드주기가 긴 P코드 대신 일반 사용자가 사용하고 있는 C/A 코드에 대해 기만을 수행하게 된다. GPS L1 C/A 코드는 다음과 같이 나타낸다.

$$S_{L1} = A\,C(t)D(t)\cos\left(w_{L1}(t) + \phi_0\right) \quad (1)$$

S_{L1}은 시간 t에서 정상적으로 입력되는 GPS 신호를 나타내며, S_{L1}의 A는 GPS 신호의 전력, $C(t)$는 코드위치, $D(t)$는 데이터 비트, $\cos\left(w_{L1}(t) + \phi_0\right)$는 주파수 성분을 나타낸다.

일반적으로 기만신호는 정상신호보다 신호세기가 크며 코드의 시간지연이 발생하며 도플러의 변이 값이 존재하게 된다. 따라서 기만신호의 특성은 수식 2와 같이 나타낼 수 있다.[5]

$$S_{L1}' = A'C(t-\tau)D(t)\cos\left((w_{L1} + \triangle w)(t) + \phi_0\right) \quad (2)$$

S_{L1}'은 시간 t에서 입력되는 기만신호를 나타내며, S_{L1}'의 A'는 기만신호의 전력으로 A보다 큰 값을 갖는다. $C(t-\tau)$는 기만신호의 코드위치로 정상신호에서 τ 만큼의

시간지연이 발생한다. $\cos((w_{L1}+\triangle w)(t)+\phi_0)$는 기만신호의 주파수 성분으로 $\triangle w$ 만큼의 도플러 변이가 발생한다.

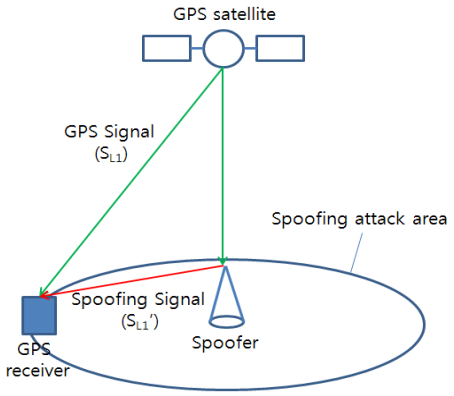

그림 1. 기만신호 개념도

따라서 GPS 수신기로 입력되는 신호 S_{L1}''는 GPS 정상신호 S_{L1}와 기만신호 S_{L1}'를 모두 수신하여 처리하게 된다.

$$S_{L1}'' = S_{L1} + S_{L1}' \tag{3}$$

수신기에서 S_{L1} 신호를 정상적으로 신호추적하는 과정에서 기만신호가 입력이 되면 수신기는 S_{L1}''신호를 처리하게 된다. 그런데 S_{L1}'의 기만신호가 정상적인 신호 S_{L1} 보다 신호세기가 크기 때문에 수신기는 S_{L1} 신호처리에서 S_{L1}'신호처리로 변환하게 된다. 그림 2에서 보면 (a)는 정상신호만 처리한 상관함수가 되며, (b)는 기만신호가 입력되었을 때 상관함수를 나타낸다.

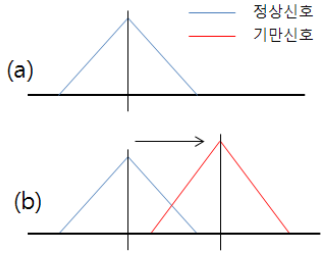

그림 2. 기만신호 상관함수

그림2의 (b)에서 보듯이 정상적인 상관함수 위치에서 기만신호의 상관함수 위치로 이동하게 되므로 의사거리 측정값의 변화가 발생하며 또한 상관함수의 크기가 커짐으로 C/No값 또한 변화가 발생하게 된다.

2. GPS 기만 신호 생성기

GPS 기만신호 생성기의 구조는 그림 3과 같다.

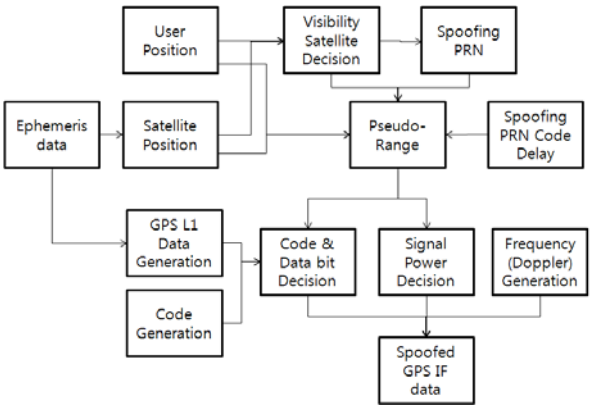

그림 3. 기만신호생성기 블록 다이어그램

GPS 기만신호생성기는 정상적인 GPS 신호를 생성하는 기능에 기만신호 생성을 추가한 형태이다. 또한 다양한 기만 형태 중 중급기만에서 코드시간지연 및 도플러변이에 따른 기만신호를 생성할 있도록 하였다. GPS 기만신호생성기는 GPS 신호를 생성하기 위하여 RINEX 데이터로부터 궤도데이터를 읽어오고 해당 시뮬레이션 시간에 맞춰 항법데이터를 생성하게 된다. 또한 시뮬레이션 시간의 궤도데이터를 이용하여 위성의 위치를 계산하고 입력된 수신기위치에서 가시위성을 판단하게 된다. 이렇게 판단된 가시위성에서 기만할 위성 PRN을 선택한다. 기만신호를 생성할 위성의 시간지연을 입력하면 의사거리 계산부에서 정상신호의 의사거리 및 기만신호의 의사거리를 계산하게 된다. IF 신호생성을 위하여 PRN 별로 계산된 의사거리에 따른 코드위치, 데이터 비트위치를 결정하고 도플러에 따른 반송파를 생성하여 결합하게 된다. 결합된 IF 신호는 수신기에서 처리 가능한 신호로 변환하기 위하여 ADC를 수행하게 된다.[6] 연속적인 신호생성을 위하여 코드 및 반송파 DCO를 이용하여 IF 데이터를 생성하며 DCO의 증가값은 시간에 따른 위성별 도플러를 반영하여 업데이트 한다. 기만신호생성기에서는 PRN 별로 별도의 채널을 유지하며 주기적 가시위성 판단을 수행하여 채널의 추가 및 삭제가 가능하다.

기만신호생성의 예를 보면 가시위성이 PRN 1~10이면 이중 기만할 PRN(예 PRN 1)을 선택하게 된다. 그러면 PRN 1~10의 정상적 GPS 신호와 기만된 PRN 1의 신호를 동시에 생성하게 된다. 따라서 총 11개의 신호를 합성하여 하나의 IF 신호를 생성하게 된다.

Ⅳ. 성능평가

1. 시뮬레이션 환경

기만신호의 영향분석을 위해 개발된 기만신호생성기에서 생성한 IF 신호를 개발된 소프트웨어 수신기를 이용하여 수신처리하였다. 시뮬레이션을 위한 구성은 아래 그림과 같다.[4]

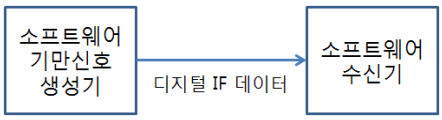

그림 4. 시뮬레이션 구성도

기만신호 발생을 위한 파라메터는 표 1과 같다. 기만신호의 영향을 파악하기 위하여 신호획득 및 추적 단계에서 정상적인 PRN 1의 의사거리에 0.5, 1, 1.5칩의 지연을 추가 기만신호를 생성하였다.

표 1. 기만신호 파라메터

Item	Value
Spoofing PRN	1
Spoofing chip delay	0.5chip, 1chip, 1.5chip
Spoofing input time	0sec, 40sec
Spoofing PRN C/No	50dB

정상신호를 생성하기 위한 파라메터는 표 2와 같다. 모두 5개의 위성신호를 생성하고 양자화 비트를 8비트로 IF 신호의 특성을 설정하였다.

표 2. 시뮬레이션 파라메터

Item	Value
Sampling Rate	5.714Mhz
IF Frequency	1.132Mhz
Total simulation time	60sec
Quantization Bit	2bit
Normal PRN	1, 3, 6, 7,16
Normal PRN C/No	45dB

2. 시뮬레이션 결과

기만신호의 영향을 분석하기 위하여 신호추적 결과인 코드추적루프(DLL) 및 위상추적루프(PLL)의 필터 출력값을 비교 분석하였고 기만신호에 따른 항법해 및 시간 바이어스에 대해 살펴보았다.

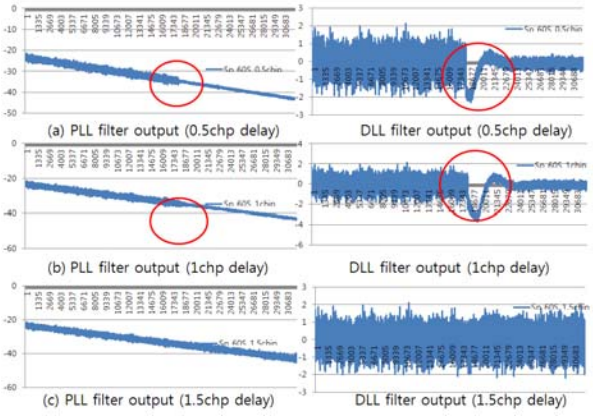

그림 5. 기만신호 인가에 따른 DLL 및 PLL 출력값 비교

그림 5는 정상적으로 신호추적하는 과정에서 기만신호의 지연을 0.5, 1, 1.5칩으로 설정하여 인가했을 때 DLL 및 PLL의 출력값의 영향을 보여준다. 정상적 신호처리 과정에서는 DLL 값의 변화가 일정하나 0.5, 1칩의 코드지연을 갖는 기만신호가 인가된 시점부터 출렁거리며 다시 수렴하는 형태를 보이고 있다. DLL 값이 출렁이는 것은 현재 정상신호를 처리에서 기만신호 처리로 변환되는 현상이며 수렴과정에서 DLL 출력값의 변이가 줄어든 것은 기만신호의 세기가 정상신호의 세기보다 크기 때문이다. PLL의 출력값은 단순히 변이값의 범위만 줄어들었는데 이는 도플러를 정상 PRN의 도플러와 동일하게 설정하였기 때문에 시간에 따른 PLL의 변화 경향은 동일하나 기만신호 세기의 영향으로 변이값의 범위가 줄어들었다. 기만신호의 지연이 1칩 이상일 경우에는 정상신호에 영향을 주지 않는 것으로 판단된다.

그림 6은 기만신호에 따른 I/Q 상관값을 비교한 것이다. 그림 6의 (a)는 정상적 I/Q 값의 분포를 나타내고 (b)는 기만신호의 영향을 받은 I/Q 값의 분포를 나타내고 있다. 기만신의 칩지연이 0.5, 1칩일 때 I/Q의 분포가 (a)에서 (b)로 이동한 것을 확인할 수 있다. 이는 기만신호의 신호세기 특성이 크기 때문에 정상적인 신호보다 I값이 커지게 되기 때문이다.

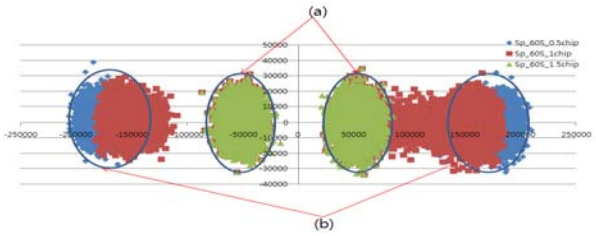

그림 6. 기만신호 인가에 따른 I/Q 상관값 비교

그림 7은 기만신호에 따른 항법해 영향을 나타낸 것이다. 그림에서 보면 기만신호가 1칩 이내의 지연을 가져 정상신호에 영향을 줄 경우 코드 지연 0.5 칩과 1칩에 따른 항법해의 변화가 그림 7의 (a)와 (b)로 이동하며 (c)의 경우에는 정상신호에 영향이 없는 기만신호의 코드지연이기 때문에 정상신호의 항법해 분포를 갖게 된다.

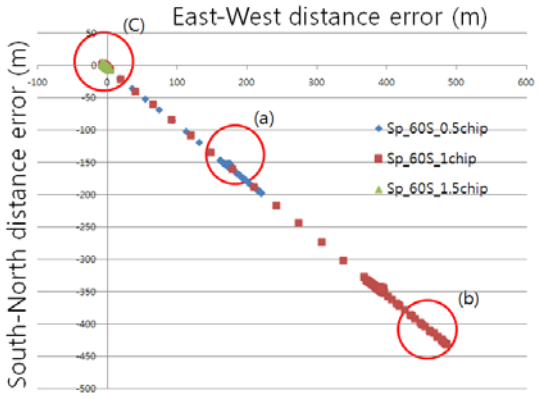

그림 7. 신호추적 단계에서 기만신호 인가에 따른 항법해 영향

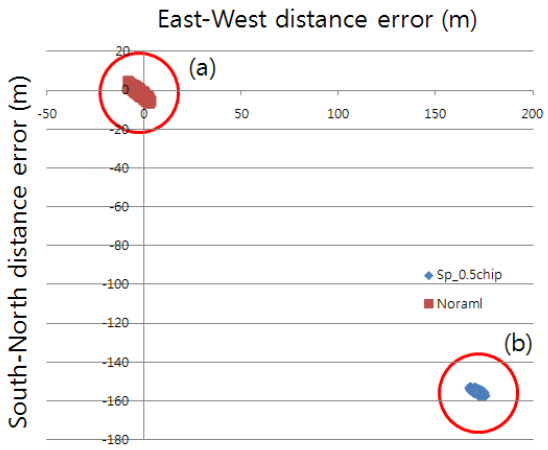

그림 8. 신호획득 단계에서 기만신호 인가에 따른 항법해 영향

그림 8은 신호획득 과정에서 기만신호가 입력될 경우의 항법해의 영향을 나타내고 있다. 그림 8의 (a)는 정상신호의 항법해를 나타내고 (b)는 기만신호를 획득하여 항법해를 나타낸 경우이다. 그림에서 보듯이 초기 기만신호를 획득하여 신호처리를 수행할 경우 수신기는 기만신호의 영향으로 잘못된 항법해를 생성하고 있다.

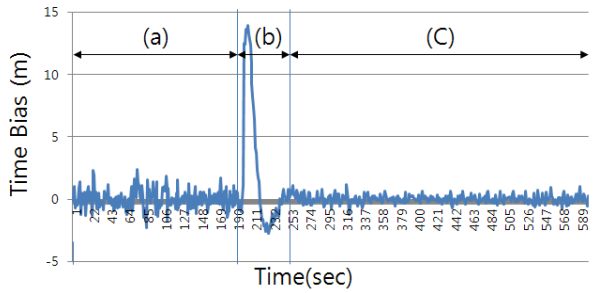

그림 9. 기만신호에 따른 시간 바이어스 영향

그림 9는 항법해 생성에 따른 수신기의 시간 바이어스를 나타낸다. 그림에서 보면 3가지 구간으로 나누어지는데 (a)는 정상적인 신호처리를 통한 시간 바이어스이고 (b)는 기만신호 인가 시점에 따른 시간 바이어스, (c)는 기만신호의 영향에 따른 시간바이어스이다. 기만신호가 인가된 시점(b)에서 시간 바이어스가 크게 출렁거리다 안정화 되고 있다. 이는 정상적인 의사거리에서 기만신호의 코드 지연에 따른 의사거리 반영 때문에 발생하는 것이다.

V. 결론

본 논문에서는 기만신호의 영향을 분석하기 위하여 기만신호의 코드지연에 따른 코드 및 반송파 추적에 대한 결과를 분석하였다. 기만신호의 특성 및 방어 방법에 대한 조사를 통하여 현재 GPS 신호와 동기를 유지할 수 있는 중급기만을 고려하여 기만신호생성기를 이용하여 시뮬레이션을 수행하였다. 기만신호생성기에서 생성한 정상신호 및 기만신호가 합성된 신호를 소프트웨어 수신기를 통하여 신호처리를 수행하였다. 본 논문에서는 코드추적루프(DLL) 및 위상추적루프(PLL)의 출력값을 비교분석하여 기만신호의 영향을 파악하였으며 또한 기만신호 인가 시 잘못된 의사거리에 따른 항법해의 영향을 분석하였다. 결과적으로 기만신호의 영향은 신호추적 단계에서는 1칩 이내의 코드지연을 갖는 기만신호의 영향을 받으며 신호획득에서는 코드 지연에 상관없이 영향을 받는 것을 확인하였다.

참 고 문 헌

[1] S. J. Harding, Study into the impact on capability of U.K. commercial and domestic services resulting from the loss of GPS signals, Qinetiq, 2001

[2] 임성혁, 임준혁"GPS L1 C/A 신호추적루프에서의 기만에 의한 영향", 한국항행학회, 제15권, 2011.02

[3] B. M. Ledvina at al., "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," in the Proc. of National Technical Meeting - ION NTM 2010, 25-27 January 2010, San Diego, CA.

[4] M. Nicola, L. Musumeci, M. Pini, M. Fantino. P. Mulassano, "Design of a GNSS Spoofing Device Based on a GPS/Galileo Software Receiver for the Development of Robust Countermeasures", ENC GNSS 2010, Braunschweig, Germany, 19-21 October 2010

[5] 임순, 신미영, 조성룡,"소프트웨어 기반 GPS 기만신호 생성기 설계", ICS'08 63-64

[6] Tae-Hee Kim, Jae-Eun Lee, Sanguk Lee, Jae-Hoon Kim, "Algorithm of the IF Signal Generation in the Software-Based IF GNSS Signal Simulator", GPS/GNSS 2008, Tokyo

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 (Cheon Sig 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

이 상 욱 (Sanguk Lee) **정회원**

・1991년 2월 : 연세대학교 천문학과 석사졸업
・1994년 2월 : University of Auburn 항공우주공학과 박사졸업
・1993년1월～현재 : 한국전자통신연구원 책임연구원
<관심분야> : 위성시스템. 위성항법, 탐색구조