GPS L1 기만신호 검출 알고리즘 성능 분석

김태희*, 김재훈*, 이상욱*

Analysis of Performance of Spoofing Detection Algorithm in GPS L1 Signal

Taehee Kim*, Jaehoon Kim*, Sanguk Lee* *Regular Members*

요 약

본 논문에서는 GPS L1 신호에 대한 기만의 종류 및 이를 검출하기 위한 방법에 대한 연구를 수행하고 GPS L1 신호에 대한 기만신호 검출 및 판단 알고리즘을 구현한 후 시뮬레이션을 통하여 성능을 분석하였다. 수신기의 동작 여부에 따라 기만과 재밍신호가 차이가 있으며 기만신호는 재밍신호와 달리 GPS 신호와 유사한 신호로 수신기를 공격하므로 기만 대상 수신기에서는 정상동작하는 것처럼 판단하게 되며 따라서 수신기에서 기만공격을 판단하기란 매우 어렵다. 기만신호 검출 및 판단 알고리즘의 성능을 검증하기 위하여 소프트웨어 기반의 기만신호/정상 GPS 신호생성기와 소프트웨어 기반의 수신기를 구현하였다. 본 논문에서 기만신호의 코드지연 및 도플러 주파수 변이에 따른 수신기의 DLL/PLL의 출력 오차를 확인하였다. 또한 수신기의 출력값인 의사거리, 신호세기, 항법해를 이용하여 기만신호 검출 및 판단 알고리즘을 구현하였으며 기만신호를 효율적으로 검출 및 판단할 수 있었다.

Key Words : GNSS, Spoofing, Detection, GPS, L1 C/A

ABSTRACT

In this paper, we investigate the type and detection methode of spoofing attack, and then analyze the performance of spoofing detection algorithm in GPS L1 signal through the simulation. Generally spoofer is different from the jammer, because the receiver can be operated and not. In case of spoofing the GPS receiver is hard to recognize the spoofing attack and can be operated normally without stopping because the spoofing signal is the mimic GPS signal. To evaluate the performance of spoofing detection algorithm, both the software based spoofing and GPS signal generator and the software based GPS receiver are implemented. In paper, we can check that spoofing signal can affect to the DLL and PLL tracking loop because code delay and doppler frequency of spoofing. The spoofing detection algorithm has been implemented using the pseudorange, signal strength and navigation solution of GPS receiver and proposed algorithm can effectively detect the spoofing signal

I. 서 론

최초의 위성항법 시스템인 GPS는 미국방성에서 미국의 군사적 목적으로 구축되었지만 민간신호인 C/A 코드를 개방한 현재 해양/육상/항공 교통 뿐만 아니라 시각동기가 필요한 이동통신, 금융, 증권 망과 같은 수많은 민간 분야에서 활용하고 있다. 그러나 GPS 시스템은 미국국방성의 소유라 전쟁 또는 미국의 이해관계에 따라 신호를 제어할 수 있기 때문에 현재 GPS에 의존되어 활용되는 모든 분야에 심각한 타격이 전해질 것이다. 이에 따라 각 지역에서 독자적인 위성항법 시스템 구축 필요성을 인지하고 최근 유럽의 Galileo 프로젝트가 진행되고 있고 중국에서는 BeiDou 위성을 통한 항법시스템을 구축하고 있다. 중국의 BeiDou 위성항법 시스템의 경우 2020년까지 전체 시스템의 구성을 완료할 예정이며 현재까지 14개의 위성이 발사되어 시험을 진행하고 있는 상태이다. 미국의 GPS 시스템 또한 세계 각국에서 이러한 위성항법 시스템을 구축하는 것에 자극을 받아 민간 서비스 제공을 확대하기 위하여 L2C 신호와 L5신호를 제공할 수 있는 위성인 GPS Block IIR(M)과 GPS Block IIF를 2018년 및 2021년까지 발사 완료할 계획을 수립하고 있다.[1]

※ 본 연구는 미래창조과학부가 지원한 2013년 정보통신·방송(ICT)연구개발사업의 연구결과로 수행되었음.
*ETRI 위성항법연구실 (thkim72@etri.re.kr)
접수일자 : 2013년 5월 3월, 수정완료일자 : 2013년 6월 21일, 확정게재일자 : 2013년 6월 26일

이렇듯 위성항법 시스템은 군사적, 상업적 목적 이외에 민간 서비스 분야에 깊숙이 자리 잡고 있다. 따라서 악의적 의도로 항법시스템의 장애를 야기하여 사회적 혼란을 발생하려는 무리 또한 나타나고 있다. 항법시스템의 장애 형태로 재밍, 기만, 재방송 기만 등이 있다.

재밍 신호의 경우 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 사용이 어려운 단점이 있으나 간단하게 재밍신호가 도달하는 광범위한 지역의 항법단말기 동작을 방해할 수 있는 장점이 있다.[2] 기만신호의 경우 재밍신호와 달리 항법 단말기에서 파악하기 어려우며 정상적으로 동작하는 것으로 인지하며 동작하기 때문에 재밍신호 형태보다 위험한 공격방법이다. 기만 신호 관련하여 일반적으로 GPS L1 C/A 코드에 대해 이루어진다. 이는 해당 코드에 인증 및 인코딩과 같은 기능이 포함되지 않아 해당 서비스를 제공 받는 사용자를 손쉽게 기만할 수 있기 때문이다. 현재까지 우리나라의 산업 전반에 구축되어진 위성항법 시스템은 GPS C/A 신호처리 수신 시스템이다.

따라서 이러한 기만신호 공격에 대한 대책이 필요하며 이를 위하여 기만공격에 대한 검출 기능에 대해 본 논문에서 살펴볼 것이다.

Ⅱ. 기만신호 형태

기만공격을 수행하기 위하여 측정치의 변이를 주거나 항법메시지의 궤도 혹은 시간 성분의 값을 의도적으로 변경하여 수신기가 잘못된 항법해를 생성하도록 하는 것이다. 기만신호의 형태는 기만신호를 발생하는 방법에 크게 3가지로 나누어 볼 수 있다.[3]

첫 번째로 단순히 현재 GPS위성과 시각 동기 없이 GNSS 신호생성 시뮬레이터를 이용하여 RF 신호를 불특정 다수의 수신기에게 신호를 전송하게 된다. 따라서 해당 기만신호와 근접한 수신기에서는 신호세기가 강하여 재밍으로 판단하는 반면 코드지연이 1칩 이내에 위치한 수신기에서는 기만신호의 영향을 받을 수 있다. 이러한 기만의 형태는 기만신호 대상 수신기에서 새로운 신호획득을 수행할 경우 기만신호에 따라서 비정상적인 위치를 산출하지만, 새로운 신호획득이 아니라면 현재 추적된 수신 채널에 영향을 미칠 확률은 현저히 떨어지게 된다.

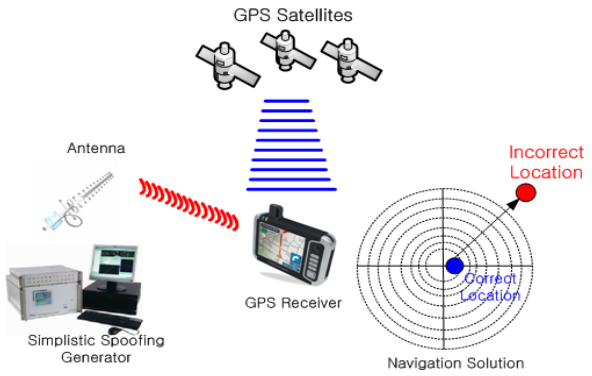

그림 1. 초급기만의 개념도

두 번째 기만의 형태는 현재 GPS 위성에서 전송하는 신호와 동기를 맞춰 기만신호를 생성하는 것이다. 이와 같은 기만 신호생성기는 현재 GPS신호와 동기를 유지하기 위한 GPS 수신기 및 GPS와 동기되어 기만 대상 수신기를 기만하기 위한 기만신호생성기로 구성된다. 이러한 기만신호 생성기는 기만대상 수신기에서 수신하는 동일한 GPS 신호를 수신처리하기 때문에 항법데이터 및 측정데이터 정보를 이용하여 기만대상 수신기로 GPS 신호와 동일한 형태의 기만신호를 송출할 수 있다. 따라서 이러한 기만을 수행하기 위하여 기만대상 수신기의 위치에 대한 정보를 정확히 알고 있어야 어려움이 있다. 기만대상 수신기에서는 해당 기만신호를 수신할 경우 현재 수신하고 있는 정상적인 GPS 신호 대신 기만신호를 처리하여 잘 못된 위치를 산출하게 된다. 이렇듯 현재 GPS 신호와 동기를 유지하기 때문에 기만 대상목표를 기만 공격을 수행하는 자자의 의도대로 기만대상 수신기를 기만할 수 있게 된다. [3,4]

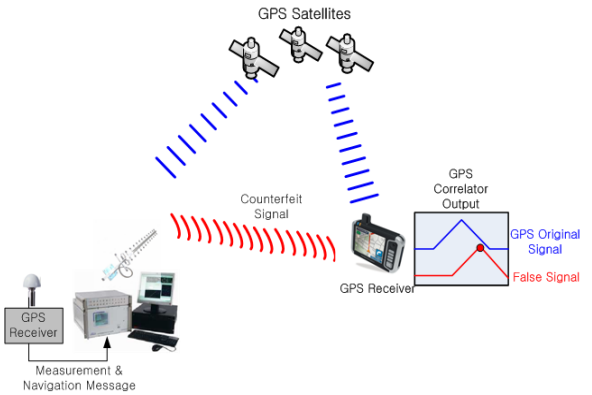

그림 2. 중급기만의 개념도

마지막 기만발생의 형태는 다중 안테나를 이용하여 다수의 기만대상 수신기로 기만신호를 송출할 수 있는 형태이다. 즉 기만대상이 하나의 수신기가 아니라 다수개로 각각의 기만대상 수신기에서 GPS위성신호와 동일한 형태의 기만신호를 각각 생성하여 전송할 수 있다. 이러한 기만방법은 좀 더 진화된 방법의 기만형태로 기만대상 수신기가 기만공격을 수행하는 위치를 알 수 없도록 하는 방법이다. 그러나 기만

을 수행하기 위해 복잡한 구조를 가지고 있다.

Ⅲ. 기만신호 검출 방법

GPS 신호 기만에 대한 검출을 위하여 절대적 위성신호 세기에 대한 감시, 신호세기의 변화 감시, 다른 주파수와 상대적 신호세기 감시, 의사거리 변화율 및 도플러 변화 등의 방법으로 감시한다.[4]

1. 절대적 위성신호 세기에 대한 감시

GPS의 수신 신호 전력은 L1 채널의 P(Y) 코드에 대해서는 -155.5dBw, C/A 코드에 대해서는 -153dBw, L2 채널의 모든 신호에 대해서는 -158dBw를 초과하지 않을 것으로 예상된다. 이들 신호전력 값은 안테나 형태 및 자세, 다중경로 같은 환경 효과가 수신 신호 전력을 극적으로 변화시킬 수 있기 때문 모든 수신기에 대해서 신호 전력의 상한값으로 정해지지 않는다. 그럼에도 불구하고, 기만기는 적어도 3dB 이상은 신호전력을 증가시켜야 하기 때문에 상식적인 최대 전력값이 기만 신호 전력의 한계로 정해질 수 있다.

2. 신호세기의 변화 감시

특정 지점으로부터 RF 신호 방사는 수식은 (1)과 같다

$$P \times r^2 = constant \tag{1}$$

수식에서 P는 수신 전력, r은 위성과 수신기간 거리를 나타낸다. GPS 위성은 지구로부터 2만km 떨어져있기 때문에 지구 표면 근처의 어떠한 위치 변화에 대해서도 신호 전력이 급격하게 변하지 않는다. 하지만 다중경로 안테나 자세등과 같은 환경에 따라서 수신 전력이 변화하므로, 이 방법은 고정 된 지점에서 측정할 경우만 적용가능 하다. 위성 앙각이 수신 신호 전력에 영향을 주므로 이 방법은 위성 앙각이 상수로 유지되는 시간 구간 동안에만 사용하는 것도 가능하다. 대부분의 GPS 수신기에서 사용가능한 신호 대 잡음비는 수식(1)에서 P값 대체용으로 사용한다.

3. 다른 주파수와 상대적 신호세기 감시

L1 주파수의 최저 수신 RF 신호 전력을 P(Y) 코드의 경우 -163.0dBw, C/A 코드의 경우 -160dBw로 제시하고 있다. L2 주파수의 최저 신호 전력 세기는 -166dBw이다. 현대화된 GPS 위성은 L2에 2개의 신호, L5에 한 개의 신호 가지며 이들 신호는 상대적으로 고정 전력 비율을 가지고 있다. 상대적인 전력 비율을 확인하면서, 모든 주파수, 모든 신호 항목(L1/L2 및 L5)과 부합되지 않은 기만 신호와 같은 형태는 쉽게 검출이 가능하다. 이 방법의 이득은 안테나 자세에 의해 영향을 받지 않는다는 것이다.

4. 의사거리 변화율 감시

코드 및 반송파 위상의 의사거리 측정치 변화율은 아래와 같이 정의한다.

$$RR_{code} = (r_i - r_j)/(t_i - t_j) \tag{2}$$

$$RR_{phase} = \int_{t_i}^{t_j} \Phi(t)dt/(t_i - t_j) \tag{3}$$

수식 에서 i,j는 측정 인덱스, r은 코드 의사거리 측정치, Φ는 부분 반송파 위상 측정치, t는 측정치 시점을 나타낸다.

코드/반송파 위상검사는 기만대상 수신기와 기만신호 생성기 사이의 도플러 효과로 인하여 반송파 위상측정치를 기만하기 어려운 특성을 이용하여 코드 측정치와 반송파 위상 측정치를 비교하여 기만을 판단한다. [5]

기만기가 고정된 수신기의 위상 측정치를 기만하는 것이 쉬울 지라도, 이동중인 수신기의 위상 측정치를 기만기에서 제어하기란 쉽지 않다. 만일 수신기를 기만하기 위해서 기만기가 위상거리가 코드거리에 일치하기를 원한다면, 코드 거리가 알맞게 기만되어야만 하고, 위상 거리가 코드 거리와 일치하여 기만되어야 한다. 반송파 위상 거리가 코드 거리에 따라서 위조되었을 때, 아마도 위상 거리 변화율은 위상 거리 기만은 어려울 것이다. 따라서 코드와 위상 거리 변화율를 비교함으로써 비정상적 상태가 검출 가능하고 이를 이용한 검출 기법이 개발될 수 있다. 단순 기만의 경우 GPS 위성 각각에 대한 거리 변화율은 지상기반 송신기에서 전송된 기만 신호에서 측정된 거리 변화율과 비교할 수조차 없다.

5. 도플러 변화 감시

GPS 수신기는 항법해 및 위성 위치를 계산할 수 있다. 따라서 각 GPS 위성에 대한 수신기의 상대적인 속도 유도가 가능하다. 도플러 이동(D)은 수식(4)와 같이 정의 할 수 있다.

$$D = f' - f_0 = -f_0/(1 + c/v) \tag{4}$$

수식(4)에서 는 f_0는 기존의 도플러 주파수 이며 f'는 위성의 움직이는 속도에 의한 변이된 도플러 주파수 이다. 단일 송신기를 사용하는 기만기에서 실제 모든 위성에 대해 기만하기 위한 모든 도플러 이동을 구현하는 것은 불가능하다. 왜냐하면 도플러 이동은 반송파 주파수를 변경하기 때문이다. 서로 다른 PRN 코드를 갖는 CDMA 신호들이 반송파로 변조되기 전에 합해지는 반면 기만기에서 도플러 변이를 이용한 검출을 피하기 위하여 기만 신호는 서로 다른 반송파에

변조되어야만 한다. 따라서 기만기는 각각의 기만시킬 위성마다 개별적으로 송신기를 가져야만 한다. 도플러 이동은 또한 의사거리 변화율을 활용하여 비교될 수도 있다. 왜냐하면 위상거리 변화율 등과 내적관계를 갖기 때문이다.

Ⅳ. 기만신호 검출 알고리즘 구현

본 논문에서는 기만신호 검출 알고리즘을 구현하기 위하여 의사거리변화율 및 항법해 변화, 신호세기 변화를 이용하였다.

일반적으로 수신기에서는 안테나로부터 입력되는 RF 신호를 수신하여 RF Front End 모듈에서신호처리가 가능한 샘플링된 신호로 변환한다. 신호획득부에서는 이렇게 샘플링된 신호로부터 코드 시작점과 신호의 도플러 정보를 획득하며 이를 위하여 신호를 주파수 영역에서 자기상관을 하여 각 샘플마다 상관값을 얻어내고 그 크기를 비교하여 위성번호와, 코드위상, 도플러 주파수를 결정하게 된다. 신호획득이 완료되면 수신기는 신호획득 정보를 이용하여 연속적인 위성신호를 추적한다. 신호추적은 각 채널을 In-phase와 Quad-phase의 반송파 상관 신호와, 각각 Early, Prompt, Late 3개의 코드 상관 신호를 구성하여 총 6개의 상관기를 기본적으로 포함하며, 추적 루프는 코드 추적을 위한 DLL (Delay Lock Loop)과 반송파 추적을 위한 FLL(Frequency Lock Loop)과 PLL(Phase Lock Loop)을 구현한다. 코드추적루프 및 반송파추적루프를 통해 신호처리가 안정화가 이루어지면 상관기로부터 생성된 상관값을 이용하여 비트동기를 생성하는 비트동기, 비트동기 후 프레임동기를 생성하는 프레임동기, 프레임동기 후 상관기로부터 측정된 값을 이용하여 항법해를 생성하기 위해 측정데이터 생성을 수행하게 된다. 측정데이터는 주로 위성과 수신기간 의사거리로 정의하고 이를 생성하기 위하여 프레임동기 후 위성으로부터 수신한 시각정보를 이용하여 위성과 수신기의 절대적 초기시간을 결정한다. 이후 측정주기 마다 수신기 시간을 측정주기 시간간격을 더하여 갱신한 수신기 시간과 각 측정주기마다 카운트값 및 코드위상을 이용하여 위성 시간의 차를 이용하여 의사거리를 생성한다.[6]

이렇게 위성과 수신기간 의사거리가 측정이 되면 해당 측정값을 이용하여 기만 신호 검출 및 판단을 다음 그림 3과 같이 수행한다.

본 논문에서 제시한 알고리즘에서는 기만주의, 기만검출, 기만판단 세 단계로 기만판단을 수행하였다. 기만판단을 위하여 수신기에서 의사거리 측정값이 생성이 되면 현재 시간 이전에 측정된 의사거리 간 변화율을 계산한다. 만약 의사거리 변화율이 임계값보다 클 경우 기만주의 단계를 발령한다.

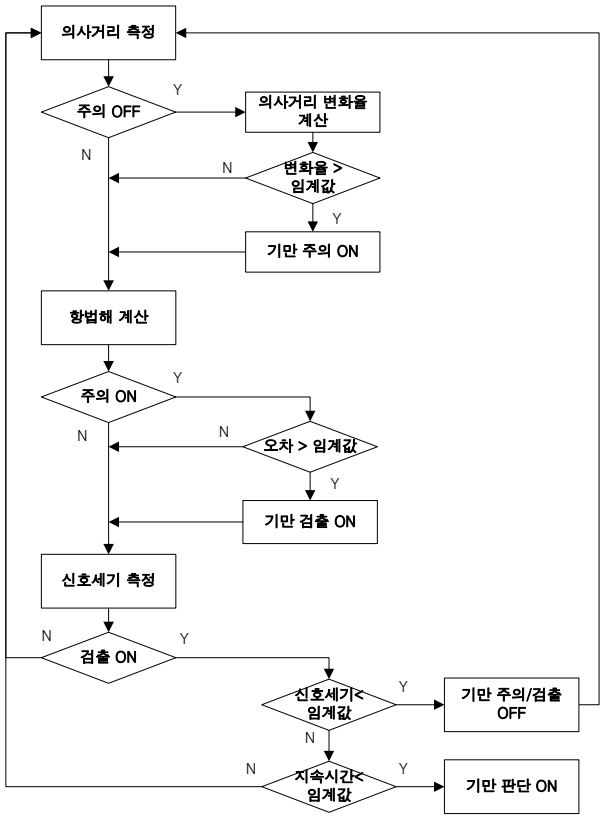

그림 3. 기만 판단 알고리즘

의사거리 변화율의 임계값은 일정 시간동안 의사거리 변화율을 누적한 평균값을 기준 값으로 설정하고 기준값에서 벗어나는 오차의 크기로 결정하였다. 실제 환경에서 위성과 수신기간 의사거리 변화는 급격하게 발생하지 않는다. 따라서 이러한 의사거리 변화가 짧은 시간 동안 급격한 변화가 발생하면 기만의 의심단계인 기만주의 단계를 생성하게 된다. 기만주의 단계에서는 의사거리 변화율이 임계값보다 큰 채널 즉 기만 공격의 목표가 된 위성의 PRN 번호를 확인할 수 있다. 기만주의 단계 이후 기만검출 여부를 판단하기 위하여 의사거리 변화율에 대한 비교 후 항법해에 대한 영향을 확인한다. 항법해는 측정된 의사거리를 이용하여 생성하기 때문에 비정상적인 의사거리 변화가 발생할 경우 항법해 오차가 크게 발생한다. 따라서 항법해의 오차가 임계값 이상으로 클 경우에 기만검출단계를 발령하고 임계값 이하로 오차가 발생할 경우에 기만주의단계를 유지하게 된다. 본 논문에서 이동통신 기지국과 같이 고정 지점의 수신기에서 항법해를 산출하기 때문에 항법해 오차 관련 임계값은 수신기의 평균 오차 성능으로 설정 할 수 있다. 그러나 이동하고 있는 수신기의 절대적 위치 정보를 알 수 없기 때문에 항법해의 오차를 인지하기는 어렵다. 마지막으로 신호세기를 측정하여 기만검출 단계가 발령된 경우 신호세기를 임계값과 비교한다. 일반적으로 기만신호는 정상신호를 공격하기 위하여 3dB ~ 5dB정도의 신호세기가 크다 따라서 해당 기만신호가 검출된 채널의 신호세기가 임계값보다 큰지 확인하고 얼마나 지속되는지 확인한다. 만약 신호세기가 임계값보다 큰 상

태로 지속적으로 수신되면 최종 기만판단 단계를 발령하게 된다. 기만판단 단계는 현재 수신된 신호 중 기만 공격이 확실히 발생하고 공격 대상 위성의 PRN을 결정하는 단계이다.

V. 성능평가

1. 시뮬레이션 환경

기만신호의 검출 및 판단 알고리즘의 기능 검증을 위하여 다음 그림 4와 같이 시뮬레이션 환경을 구축하였다.

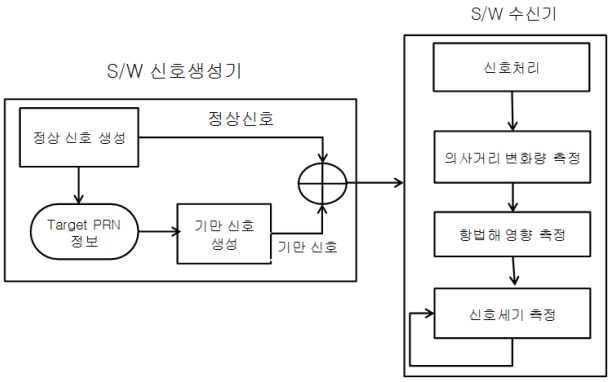

그림 4. 시뮬레이션 환경

소프트웨어 신호생성기를 이용하여 정상신호를 생성하고 일정시간 후 기만공격 대상의 PRN 신호의 코드 및 도플러 성분을 변화하여 기만신호를 생성하였다. 두 신호가 결합된 샘플 신호를 소프트웨어 수신기를 이용하여 신호획득 및 신호추적을 수행하였다. 신호추적과정에서 산출되는 의사거리, 항법해, 신호세기를 이용하여 기만 검출 및 판단을 수행하였다.

기만신호 발생을 위한 파라메터는 표 1과 같다. 기만신호의 영향을 파악하기 위하여 신호획득 및 추적 단계에서 정상적인 PRN 1의 의사거리에 1칩의 지연을 추가하고 도플러 주파수를 50Hz 이동하여 기만신호를 생성하였다. 두 파라메터는 기만신호가 발생되는 동안 동일한 값으로 유지하였다.

표 1. 기만신호 파라메터

Item	Value
Spoofing PRN	1
Spoofing chip delay	1chip
Spoofing Carrier delay	50Hz
Spoofing input time	45sec
Spoofing PRN C/No	50dB

정상신호를 생성하기 위한 파라메터는 표 2와 같다. 모두 6개의 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	75sec
Quantization Bit	8bit
Normal PRN	1, 3, 6, 7, 14, 16
Normal PRN C/No	45dB

2. 시뮬레이션 결과

기만신호 판단 알고리즘 검증을 분석을 위하여 신호추적 결과인 코드추적루프(DLL) 및 위상추적루프(PLL)의 필터 출력값을 우선 비교하였다.

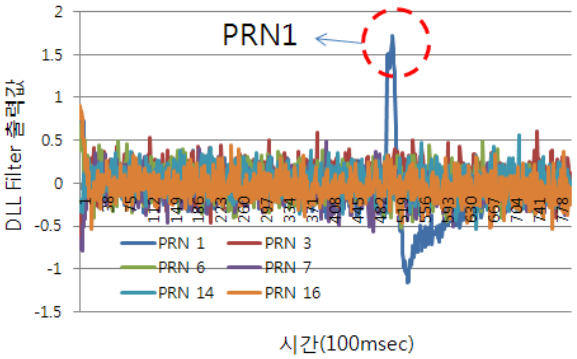

그림 5. 기만신호 인가에 따른 DLL 출력값비교

그림 5는 정상적으로 신호추적하는 과정에서 기만신호의 코드지연을 1칩으로 설정하여 인가했을 때 DLL 출력값의 영향을 보여준다. 6개의 위성중 기만신호가 인가된 PRN 1의 DLL 출력값만 기만신호가 인가된 시점에서 비정상적으로 흔들리다 다시 수렴하는 다시 수렴하는 형태를 보이고 있다. DLL 값이 출렁이는 것은 현재 정상신호 처리에서 코드가 1칩 이동된 기만신호 처리로 변환되는 현상이며 수렴과정에서 DLL 출력값의 변이가 줄어든 것은 기만신호의 세기가 정상신호의 세기보다 크기 때문이다.

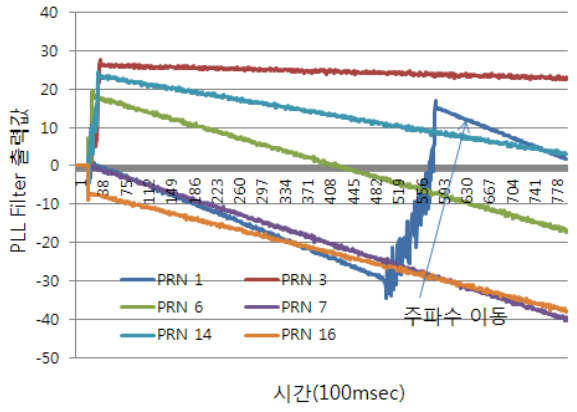

그림 6. 기만신호 인가에 따른 PLL 출력값비교

그림 6은 정상적으로 신호추적하는 과정에서 기만신호의 주파수 변이를 50Hz로 설정하여 인가했을 때 PLL 출력값의 영향을 보여준다. 그림에서 보면 주파수 추적은 FLL 이후에 PLL을 이용한다. 따라서 초기에 PLL의 출력주파수가 0에서 FLL로 결정된 주파수로 이동하게 된다. PLL의 출력값이 시간에 따라 일정한 기울기를 가지며 주파수를 추적하게 된다. 그러나 기만신호가 인가된 시점에서 PRN 1의 PLL 출력값은 50Hz 이동된 주파수로 변이한 뒤 기만신호의 주파수를 추적하는 것을 확인할 수 있다.

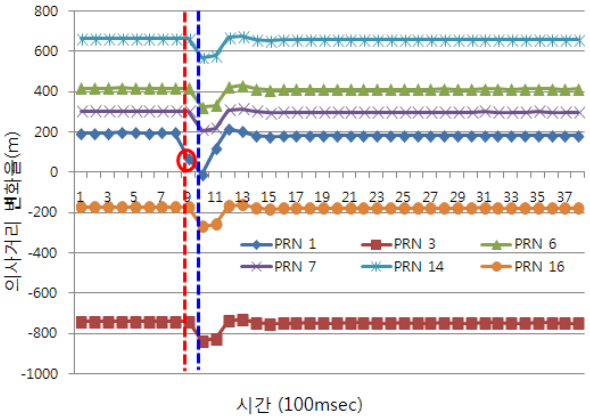

그림 7. 신호추적 단계에서 기만신호 인가에 따른 항법해 영향

그림 7은 기만신호 검출 및 판단을 수행하기 위하여 신호추적 결과로 산출되는 의사거리 변화율을 이용하여 기만신호의 검출 여부를 판단한다. 빨간 점선으로 된 시점에서 보면 PRN 1의 의사거리 변화율이 급격하게 변하는 반면 다른 위성의 의사거리 변화율에는 변화가 없는 것을 확인할 수 있다. 그러나 다음에 측정된 의사거리 변화율을 보면 모든 PRN이 급격히 변화하고 있다. 이는 빨간 점선으로 된 시점에서 기만신호의 영향으로 PRN 1의 의사거리가 비정상적인 값으로 측정하고 해당 의사거리를 이용하여 항법해를 산출하게 된다. 따라서 항법해 산출시 발생되는 시각오차 성분값이 수신기 시간에 영향을 줘 다음 의사거리 측정에 모든 PRN의 의사거리 변화가 비정상적으로 생성되는 것이다. 또한 기만공격을 받은 후 정상적인 PRN의 의사거리 변화율은 다시 정상적인 의사거리 변화율을 유지하는 반면 PRN 1의 의사거리 변화율이 정상적인 상태와 다르게 생성된다. 이는 수식(5)를 이용하여 설명할 수 있다.

$$f_{out} = f_{code} + \frac{f_{dopp} \times f_{code}}{f_{L1}} \qquad (5)$$

수식 (5)에서 f_{code}는 코드주파수, f_{L1}은 RF 주파수로 GPS L1인 경우 각각 1.023MHz 과 1575.42MHz의 상수값을 가지며 f_{dopp}는 수신기에서 측정한 위성과 수신기간 도플러 주파수이다. 따라서 기만공격으로 인한 도플러 주파수의 변이는 PRN1의 코드출력 주파수(f_{out})에 영향을 줘 비정상적인 코드추적을 수행하고 이에 따라 의사거리가 비정상적으로 생성되게 된다.

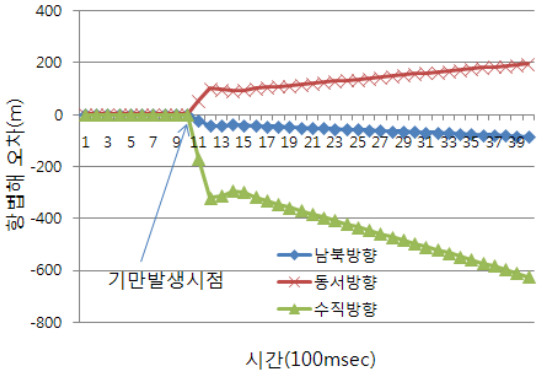

그림 8. 기만신호 인가에 따른 항법해 오차 영향

그림 8은 기만신호의 영향으로 인한 항법해 오차에 관한 것이다. 그림에서 보면 기만신호가 인가된 시점부터 항법해의 오차가 급격히 증가되며 시간에 따라 오차가 증가하는 것을 확인할 수 있다. 이는 초기 기만신호의 코드 지연 오차 성분으로 인한 의사거리 영향으로 항법해오차가 급격하게 발생되며, 시간에 따라 기만신호의 도플러 성분의 주파수 오차로 인하여 PRN 1 채널이 잘못된 코드추적을 수행하기 때문에 발생되는 현상이다. 만약 코드 지연오차 만을 갖는 기만공격이 가해지면 기만으로 항법해 오차가 발생된 후 일정한 오차값을 유지하는 것을 확인하였다.

그림 9는 기만신호의 영향으로 위성별 신호세기를 나타낸 것이다. 정상적인 상태에서는 모든 PRN이 동일한 신호세기를 나타내는 반면 기만신호를 인가한 시점에서 PRN1의 신호세기가 5dB 커진 것을 확인할 수 있다. 이는 기만신호 생성을 정상신호보다 5dB 높게 생성한 결과가 반영된 것이며 기만신호세기가 일정하게 유지되는 시간이 임계값보다 클 경우 최종 기만을 판단할 것이다. 지속시간이 유지를 확인하는 것은 일시적 현상에 기만을 판단하여 사용자가 혼란을 야기하는 것보다 지속적으로 유지되는 현상을 확인한 후 최종 기만을 판단하기 위함이다.

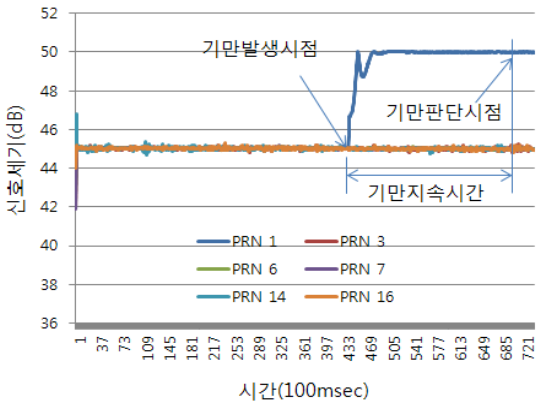

그림 9. 기만신호 인가에 따른 신호세기 영향

Ⅵ. 결 론

본 논문에서는 GPS L1 신호에 대한 기만의 종류 및 이를 검출하기 위한 방법에 대한 연구를 수행하고 GPS L1 신호에 대한 기만신호 검출 및 판단 알고리즘을 구현한 후 시뮬레이션을 통하여 성능을 분석하였다. 기만신호는 발생 방법에 따라 측정치 변이를 가지거나 항법메시지의 궤도 및 시간 정보를 변경시키며 기만신호 발생 형태에 따라 3가지 형태를 가진다. 본 논문에서 기만신호 검출 및 판단 알고리즘의 성능을 검증하기 위하여 소프트웨어 기반의 기만신호/정상 GPS 신호생성기와 소프트웨어 기반의 수신기를 구현하였다. 시뮬레이션 결과로 기만신호의 코드지연 및 도플러 주파수 변이에 따른 수신기의 DLL/PLL의 출력 오차를 확인하였으며 수신기에서 제공하는 의사거리 변화율의 비교를 통하여 의심되는 기만 신호채널을 확인할 수 있었다. 또한 기만 주의 단계이후 항법해 오차를 분석하여 기만검출을 확인하고, 신호세기의 크기 및 지속시간으로 최종 기만신호를 판단할 수가 있었다.

참 고 문 헌

[1] "Pacific PNT : GNSS, SBAS Updates" GPS world, April.24.2013

[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] Jon S. Warner, Roger G. Johnston, "GPS Spoofing Countermeasures, Los Alamos research, December 2003

[5] 조성룡,신미영,이상정,"의사거리 측정치를 이용한 기만신호 검출 기법의 성능 비교", 한국군사과학기술학회지 제 13권 제 5호, pp 793-800, 2010

[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(Tae Hee 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

이 상 욱(San Guk Lee) **정회원**

- 1991년 2월 : 연세대학교 천문학과 석사졸업
- 1994년 2월 : University of Auburn 항공우주공학과 박사졸업
- 1993년1월~현재 : 한국전자통신연구원 책임연구원

<관심분야> : 위성시스템. 위성항법, 탐색구조

김 재 훈(Jae Hoon Kim)

- 2001년 2월 : 충북대학교 컴퓨터공학 박사 졸업
- 1983년1월~현재 : 한국전자통신연구원 책임연구원
- 1992년~1994년 : KOREASAT 프로젝트 개발

<관심분야> : 위성시스템. 위성항법, 탐색구조