한국군사과학기술학회지 제13권 제5호, pp. 793~800, 2010년 10월

학술논문 전자 · 통신 부문

의사거리 측정치를 이용하는 기만신호 검출 기법의 성능 비교

Performance Comparison of Anti-Spoofing Methods using Pseudorange Measurements

조 성 룡* 신 미 영* 이 상 정* 박 찬 식**
SungLyong Cho MiYoung Shin SangJeong Lee Chansik Park

Abstract

GPS spoofing is an intentional interference which uses the mimic GPS signals to fake the receivers. The generic GPS receiver is hard to recognize the spoofing signal because the spoofer generates the fake signals as close as possible to the GPS signal. So the spoofer can do critical damage to public operations. This paper introduces a basic concept of spoofing and analyzes the effect of the spoofing signal to the GPS receiver. Also for stand-alone GPS receivers, two anti-spoofing methods are implemented : RAIM based method and the SQM based method. To evaluate the performance of anti-spoofing method, the software based spoofing signal generator and GPS signal generator are implemented. The performance of the anti-spoofing methods obtained using the output of the software based GPS receiver shows that SQM based method is more effective when multiple spoofing signals exist.

Keywords : GPS(전지구 측위 시스템), Spoofing Signal(기만신호), Anti-Spoofing Method(기만대응기법), RAIM(Receiver Autonomous Integrity Monitoring), SQM(Signal Quality Monitoring)

1. 서 론

GPS(Global Positioning System)는 군사적 목적으로 미국방성에 의해서 구축되었지만, 민간용 신호의 개방으로 현재는 민간도 사용 가능한 전파 항법시스템으로 항공, 해양, 육상에서의 항법뿐 아니라 시각동기, 전력 망, 군용시스템 등 수 많은 분야에서 사용되고 있다[1]. 그러나 잡음보다 낮은 세기의 GPS 위성신호는 의도적 혹은 비의도적인 간섭에 취약한 특성을 가지므로 이에 대한 대비가 필요하다. 비의도적인 간섭은 도심의 빌딩, 숲 등에 의한 다중경로가 대표적이며 수신기의 성능 저하를 유발한다[2]. 반면 의도적인 간섭은 정상적인 GPS 사용을 고의적으로 방해하기 위하여 사용하며 재밍(Jamming)과 기만(Spoofing)이 대표적이다[3]. 재밍은 GPS 위성신호와 동일한 주파수 대역에 센 신호를 방사하여 GPS 수신기에서 정상적인 위성신호의 획득을 방해하거나 신호 추적 손실을 유

† 2010년 7월 1일 접수~2010년 9월 10일 게재승인
* 충남대학교(Chungnam National University)
** 충북대학교(Chungbuk National University)
책임저자 : 박찬식(chansp@cbnu.ac.kr)

발시킨다. 기만은 GPS 위성신호와 동일한 구조의 신호를 이용하여 기만대상 수신기의 항법 오차 증가를 목적으로 한다. 기만대상 수신기는 기만신호 생성기에 의하여 생성된 신호를 획득, 추적함으로써 잘못된 위치를 추정하게 된다. 기만은 사용자가 인식하지 못하기 때문에 재밍보다 더 치명적인 결과를 초래한다. 현재 대부분의 GPS 시뮬레이터는 RF와 안테나의 추가로 쉽게 기만신호 생성기로 사용할 수 있으므로 이에 대한 대비가 시급하다. P(Y) 코드를 사용하는 군용 수신기에서는 암호로 기만에 대응 할 수 있지만, C/A 코드를 사용하는 민간용 수신기에서는 별도의 기만신호 대응기법이 필요하다.

2001년 Volpe 보고서[4]에서 GPS의 취약성을 지적한 후 기만에 대한 연구가 본격적으로 시작되었으며 Warner 등[5]은 시뮬레이터에서 생성된 기만신호를 검출하는 방법으로 수신된 위성신호세기 감시, 위성 번호 감시, 시각 감시 등의 방법을 제시하였다. Hein 등[6]은 기만에 대응하기 위하여 항법메시지와 확산코드의 인증(authentication)과 암호(encryption)를 사용할 것을 제안하였다. Montgomery 등[7]은 배열 안테나를 이용하여 신호의 입사각을 측정하여 기만을 감지하는 기법을 시연하였다. 이 방법들 중 암호화와 배열안테나를 사용하는 방법은 특별히 설계된 신호 또는 수신기에서만 적용이 가능하며 일반 상용수신기에서 적용하기에는 어려움이 있다. 본 논문에서는 사용자가 하드웨어 변경 없이 소프트웨어 알고리즘 추가만으로 적용가능한 기만신호 대응 기법을 대상으로 구현 방법과 성능을 비교 분석하였다. 하드웨어의 추가 없이 소프트웨어 플랫폼에서 구현 가능한 기만신호 대응 기법은 기본적으로 무결성 감지기법이 있다. 즉 기만신호가 수신기에 미치는 영향이 위성신호의 이상과 같으므로 기존의 LAAS(Local Area Augmentation System)의 기준국에서 적용되는 측정치 무결성 감지 기법[8]이나 수신기 내부에서 처리되는 RAIM(Receiver Autonomous Integrity Monitoring) 기법[3]을 활용할 수 있다. 기만신호를 생성하는 방법은 다양하지만 본 논문에서는 TOA(Time of Arrival)에 영향을 주는 기만신호에 대하여 생성하였다. 기만신호 대응 수신기의 의사거리 측정치만으로 기만신호 대응이 가능한 RAIM 기법의 일종인 패리티 공간기법[3,11]과 LAAS 기준국에서 사용되는 SQM(Signal Quality Monitoring) 기법의 일종인 코드-반송파 발산검사기법을 선정하여 그 구현 방법과 성능을 비교 분석하였다.

논문의 구성은 다음과 같다. 먼저 2장에서 기만신호의 특성과 대응기법을 소개하고, RAIM 기반의 패리티 기법과 측정치 무결성 기반의 코드-반송파 발산 검사 기법의 구현 방법과 특징을 나타내었다. 3장에서는 성능평가를 위하여 구현된 기만신호 생성기와 기만신호 대응 수신기의 설계를 나타내고, 4장에서 이를 이용한 성능평가 결과를 나타내고, 마지막 5장에서 결론을 나타낸다.

2. 기만신호 특성 및 대응기법

GPS 기만신호는 GPS 신호와 동일한 구조를 가지며, 기만대상 수신기가 정확한 PVT(Position, Velocity, Time) 정보를 구하지 못하도록 거짓된 위성 위치, 시각 정보를 항법메시지에 포함하고, 잘못된 TOA를 구하도록 오차가 포함된 C/A코드 신호를 갖는다. 즉 기만신호 생성기는 기만대상 수신기가 수신 가능하도록 GPS 위성신호와 동일한 주파수, 코드, 항법메시지, 도플러, 신호전력 등을 기만대상 수신기의 위치를 고려하여 신호를 생성하여 방송해야 한다.

GPS 민간용 C/A 코드신호는 ICD-GPS-200[9]에 신호구조가 공개되어 있고, 코드가 암호화되어 있지 않으므로 쉽게 기만신호 생성기를 만들 수 있다. 기만신호 생성기는 기만대상 수신기에 위치한 중계기에서 받은 위성 정보를 이용하여 쉽게 기만할 수 있다[5]. 두 번째 방법으로는 기만신호 생성기의 GPS 수신기로부터 수신된 신호에서 원하는 부분만 변경하여 다시 송신하는 기법[5]이 있으며, 세 번째로는 스스로 모든 신호를 생성하는 방법으로 의사위성과 GPS 시뮬레이터가 여기에 해당된다.

가시위성 정보로부터 기만신호를 생성하는 기만환경은 Fig. 1과 같다[10]. 기만신호 생성기는 기만 대상 수신기의 현재 수신 상황을 파악하기 위하여 GPS 수신기를 포함하여 운용된다. 기만신호 세기는 기만신호 생성기와 기만대상 수신기 간의 거리 및 주변 환경에 따라 변화가 심하고, 수신기에서는 수신된 신호 세기를 비교하여 기만신호임을 판단할 수 있으므로[5], 기만신호 생성기는 기만 범위를 정하여 기만신호 생성기와 기만대상 수신기 사이의 거리로부터 신호 세기를 조정하여 생성한다. 따라서, DGPS(Differential GPS) 기준국과 같이 사용자의 위치가 고정된 환경이나, 공항, 선박장, 공사장과 같이 사용자의 이동 패턴이 일

정한 지역에서 기만신호 생성기가 효과적으로 동작할 수 있다. 그러나 신호의 세기를 잘 조절한 경우에도 수신기의 움직임이 있는 경우 기만신호의 도플러가 위성신호의 도플러 보다 많이 변화하므로 수신기에서 이를 이용하여 기만신호임을 판단할 수 있다[5].

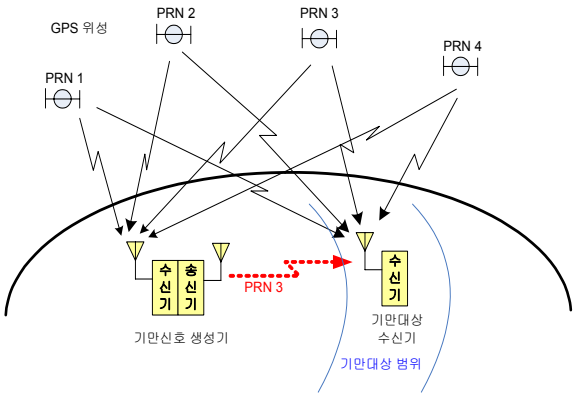

Fig. 1. 기만 환경

기만신호 생성기는 현재 보이지 않는 위성신호를 생성하여 전송할 수 있지만, 수신기에서 위성 궤도력이 있는 경우 쉽게 기만신호임을 판단할 수 있으므로 이를 고려하여 가시위성에 대해서 기만신호를 생성한다. 궤도력을 해석하여 조만간 나타날 위성신호를 생성하여 실제 신호보다 조금 먼저 전송하는 방법 또는 순간적으로 센 신호를 송출하여 실제 위성신호를 놓치게 한 후 수신기에서 기만신호 생성기 신호를 추적하도록 하는 방법들이 알려져 있다[4]. 모든 위성신호를 모두 놓치게 한 다음 기만신호 생성기 신호만을 수신기가 추적하도록 하면 수신기를 원하는 오차로 기만할 수 있지만, 수신기 내부에서도 갑작스런 신호 단절로 측정치를 의심하게 할 수 있으므로 터널 출구 등에서와 같이 자연적인 환경에서 효과적으로 적용할 수 있다.

본 논문에서는 항법해 이외에 의사거리 측정치를 제공하는 수신기는 많이 보급되어 있으므로 의사거리 측정치를 이용하여 기만신호를 감지하는 기법을 구현한다. 기만대상 수신기 입장에서 기만신호는 위성신호의 이상과 동일한 방법으로 처리할 수 있으므로, 기존의 무결성 감시기법을 쉽게 적용할 수 있다. LAAS 기준국에서 수행되는 무결성 감시기법은 SQM, DQM (Data Quality Monitoring), MQM(Measurement Quality Monitoring)으로 구성되지만 SQM에서 사용되는 코드-반송파 발산검사 기법은 의사거리 측정치만으로 구현 가능하므로 본 논문에서는 이 방법을 고려하였다. 또 다른 방법으로 고려하는 RAIM 기반의 측정치 무결성 검사 기법은 최소자승법, 패리티공간 기법, 의사거리 비교법으로 나눌 수 있으며, 이들 방법은 수학적으로 동치이며 구현 방법의 차이만 있음이 알려져 있다[3]. 패리티 공간기법은 의사거리 측정 오차를 패리티 공간으로 투영하여 고장을 검출하는 방법으로 이중 고장이 있는 경우에도 검출할 수 있는 확장된 방법도 소개되고[11], 구현의 편의성으로 많이 사용되고 있으므로 본 논문에서도 이 방법을 고려하였다.

가. 패리티 공간 기법[3]

기만진단을 위하여 선형화된 식 (1)을 사용한다.

$$y = Hx + \varepsilon \tag{1}$$

여기서 y는 측정된 의사거리와 추정한 의사거리의 차, x는 위치와 수신기 시계오차, H는 관측행렬, ε는 측정 잡음이다. 식 (1)의 관측행렬에 대하여 식 (2)와 같이 패리티 변환행렬을 정의할 수 있다. 패리티 변환행렬은 식 (3)의 성질을 갖는다.

$$PH = 0 \tag{2}$$

$$PP^T = I, \quad P^T P = I - H(H^T H)^{-1} H^T \tag{3}$$

식 (1), (2)로부터 패리티 벡터는 식 (4)와 같이 상태변수에 관계없이 오차만으로 표현할 수 있다.

$$p = Py = P\varepsilon \tag{4}$$

패리티 공간에서 판별값은 식 (5)와 같이 표현된다.

$$TS_D = p^T (PP^T)^{-1} p = p^T p \tag{5}$$

기만여부는 식 (5)의 판별값과 임계값을 비교하여 판단한다. 임계값은 식 (6)과 같이 계산할 수 있다. 패리티 벡터가 가우시안 정규분포를 갖는다고 가정하면 임계값은 경고발생확률(P_A), 의사거리 측정 잡음의 분산(σ), 가시위성 개수(n)의 함수로 나타난다.

$$T_D = \sigma \sqrt{2}\, erfc^{-1}\left(\frac{P_A}{n-4}\right) \tag{6}$$

여기서 $erfc(z)=\frac{2}{\pi}\int_{z}^{\infty}e^{-\lambda^2}\delta\lambda$는 상보오차함수이다.

패리티 벡터(p)는 크기와 방향 성분을 동시에 갖는다. 판별값은 패리티 벡터의 크기를 나타내며 패리티 변환행렬의 열들이 각각의 가시위성 특성을 나타내므로 열벡터와 패리티 벡터의 방향 일치 여부를 찾아냄으로써 기만신호를 식별할 수 있다. 식 (4)에서 보는 바와 같이 서로 다른 행은 직교하므로 Fig. 2와 같이 2차원 직교좌표 평면의 패리티 공간으로 나타낼 수 있다. Fig. 2에서 원의 반경은 임계값으로 패리티 벡터의 판별값이 원의 안쪽에 위치하면 정상이고(P_1, P_2, P_n), 원의 바깥에 위치하면 기만신호(P_3)가 존재한다고 판단하고, 패리티 벡터와 일치하는 방향의 패리티 변환행렬의 열벡터에 해당하는 신호를 기만신호로 식별한다. 수신기에서는 기만신호로 판별된 신호를 제외한 나머지 위성의 측정치를 이용하여 항법해를 계산한다.

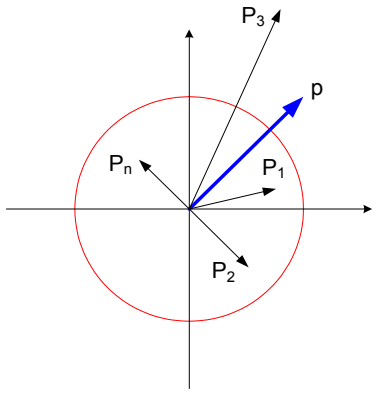

Fig. 2. 패러티 공간 기법을 이용한 기만신호 식별

나. 코드-반송파 발산검사

코드-반송파 발산검사는 기만대상 수신기와 기만신호 생성기 사이의 도플러 효과로 인하여 반송파 위상 측정치를 기만하기 어려운 특성을 이용하여 코드 측정치와 반송파 위상 측정치를 비교하여 기만을 판단하고 식별 한다[12]. 즉 코드-반송파 발산검사는 기만신호가 코드에만 인가된 경우 코드와 반송파 위상 측정치의 변화를 검사하는 방법으로, 수신기 내부의 신호처리부에서 구한 코드 측정치와 반송파 위상 측정치를 이용한다. 코드와 반송파 위상 측정치는 미지정수만큼의 차이와 분해능 차이를 가지며, 이온층 지연의 효과가 반대로 나타난다[3]. 짧은 측정 시간 동안에는 이온층 지연의 변화가 크지 않으므로 코드와 반송파 위상 측정치의 차이는 일정하게 유지된다.

코드-반송파 발산검사는 코드 측정치의 변화량과 반송파 위상 측정치의 변화량의 차를 판별값으로 사용하고, 이를 임계값과 비교하여 기만신호를 검출한다. 코드 측정치 및 반송파 위상 측정치의 의사거리 변화량(Pseudorange Rate)은 각각 식 (7), (8)과 같다[5].

$$PR_{code,k}=\frac{r(t_i)_k-r(t_j)_k}{t_i-t_j} \tag{7}$$

$$PR_{phase,k}=\int_{t_i}^{t_j}\Phi(t)_k dt/(t_i-t_j) \tag{8}$$

여기서 k는 위성을, t는 관측시간을 나타내며, $PR_{code,k}$은 코드 측정치, $PR_{phase,k}$는 반송파 위상 측정치를 나타낸다. 모든 가시위성에 대하여 식 (9)의 판별값(TS_k)과 임계값을 비교하여 기만 여부 판단 및 식별한다.

$$TS_k=|PR_{code,k}-PR_{phase,k}| \tag{9}$$

임계값은 수신기 성능에 따라 차이를 고려하여 일반적인 수신환경에서의 GPS 위성신호 측정치를 바탕으로 통계적으로 설정한다. 본 논문에서는 소프트웨어로 생성한 GPS 위성 신호의 측정치를 바탕으로 각 채널 당 측정치의 표준편차가 1 보다 작은 경우에는 3, 1 보다 큰 경우에는 실험적으로 구해진 평균값으로 설정하였다.

패리티 공간 기법과 코드-반송파 발산검사 기법은 하드웨어 추가 없이 수신기에서 제공되는 측정치만을 이용하여 소프트웨어 알고리즘의 추가만으로 쉽게 구현할 수 있다. 특히 패리티 공간 기법은 코드 측정치만을 이용하므로 FLL(Frequency Locked Loop)을 사용하는 저가의 수신기에서 구현이 가능하다. 반면, 코드-반송파 발산검사 기법은 반송파 위상 측정을 위한 PLL(Phase Locked Loop) 루프가 추가로 필요하므로 수신기의 신호 추적부가 복잡해진다. 계산량 면에서는 패리티 공간 기법은 역행렬 및 행렬 덧셈과 곱셈이 필요한 반면 코드-반송파 발산검사는 덧셈과 곱셈 만 필요하다. 특히 행렬 곱셈이나 역행렬 계산은 위성수의 증가에 따라 연산량이 지수적으로 증가 하는 반면 코드-반송파 발산검사는 위성의 추가에 대하여 연산량이 일정하게 증가하는 장점이 있다.

3. 기만신호 생성기 및 기만신호 대응 수신기 설계

가. 기만신호 생성기 설계

기만신호 생성기는 기만대상 위성과 기만대상 수신기간의 TOA 정보를 예측하고, 기만대상 위성과 동일한 신호를 생성한다. 또한, 기만대상 수신기에서 기만신호가 획득 및 추적되기 위한 기만신호 세기를 결정하고, 기만을 위한 오차가 포함된 항법데이터 또는 TOA 정보를 생성한다. 기만신호 생성기의 송신 신호 전력은 기만대상 수신기로부터의 거리에 따른 전파전력 손실 식 (10)을 고려하여 결정한다[3].

$$(L_p)_{dB} = 20\log_{10}\left(\frac{4\pi d}{\lambda}\right)\ [dB] \tag{10}$$

여기서 L_p는 전파전력 손실, d는 기만신호 생성기와 기만대상 수신기 사이의 거리, λ는 송신신호의 파장으로 GPS L1에서는 19.05cm 이다.

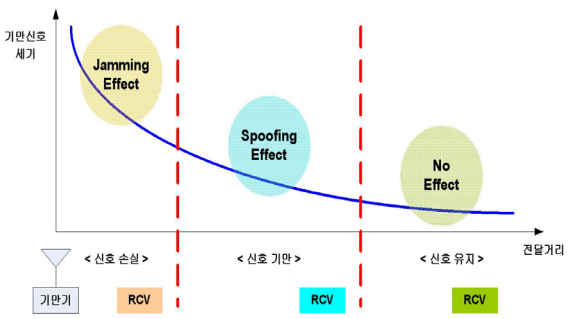

Fig. 3. 전파전력 손실에 따른 기만신호 영향

전파전력 손실에 따른 기만신호가 기만대상 수신기에 미치는 영향은 Fig. 3과 같다. 기만신호 생성기에서 가까운 곳은 신호세기가 강해 기만신호가 재밍으로 동작하며, 너무 먼 거리에 위치하면 수신기에 어떤 영향도 미치지 못한다. 따라서 기만신호 생성기는 기만대상 수신기의 위치를 파악하여 전력의 세기를 조절해야 한다.

기만신호의 생성 방법은 크게 항법데이터에 오차를 인가하거나 TOA에 오차를 인가하는 기법으로 나눌 수 있다[13]. 항법데이터에 오차를 인가하는 기법은 기만대상 수신기에서 의사거리 계산에 사용되는 항법데이터에 오차를 인가하는 것으로 위성 궤도나 시계오차 혹은 이온층 보상 계수가 그 대상이 된다. TOA에 오차를 인가하는 기법은 GPS 위성과 기만대상 수신기 사이의 C/A 코드 위상에 TOA 오차를 인가시켜 의사거리 측정치에 오차가 발생하도록 한다. 항법 데이터에 오차를 인가하는 기법은 항법 데이터를 송신하는데 시간이 걸리고, 이전에 수신된 항법 데이터와의 비교를 통하여 기만 검출이 가능하므로 본 논문에서는 항법 메시지는 변경하지 않고 C/A 코드 위상에 TOA 오차를 인가하는 기만신호 생성기를 구현하였다.

C/A 코드 위상에 TOA 오차를 인가하기 위해서, 신호세기의 조작 등을 통하여 수신기가 GPS 위성신호 대신 기만신호 생성기에서 생성된 신호를 획득하도록 초기 단계에서는 기만신호가 GPS 위성과 동일한 C/A 코드 위상을 갖도록 생성하고, 이후 C/A 코드 위상을 원하는 형태로 변경하여 기만대상 수신기를 기만한다[5]. 기만신호 생성기가 포함된 소프트웨어 기반의 신호생성기는 Fig. 4와 같다[13].

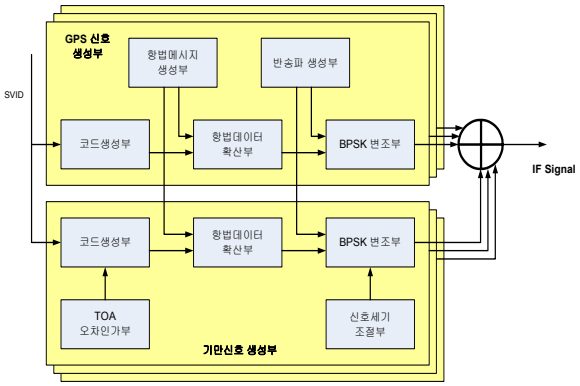

Fig. 4. 기만신호 생성기가 포함된 신호생성기 구조

기만신호 생성부는 기존의 다채널 GPS 위성신호 생성기에 기만신호 생성부 채널을 추가하였다. 기만신호 생성부는 TOA 오차를 인가와 신호 세기를 조절하기 위한 기능이 추가되어 사용자가 원하는 TOA 오차와 기만대상 수신기와의 거리에 따른 신호 세기 조절할 수 있다. GPS 위성신호 생성기는 가시위성에 대해서 신호를 생성하고 기만신호 생성부에서는 동일한 조건에서 가시위성 중 기만대상 위성에 TOA 오차인가로 사용자가 설정한 시나리오를 구현할 수 있다. 기만신호는 채널 추가가 가능하기 때문에 다수의 기만신호 생성이 가능하며 최종적으로 GPS 신호와 기만신호가 하나의 IF 신호로 생성된다.

나. 기만대응 수신기 설계

기만대응 수신기는 기존 소프트웨어 기반 GPS 수신기[14]에 기만신호 대응 알고리즘부를 추가하여 구현 하였으며, 구조는 Fig. 5와 같다.

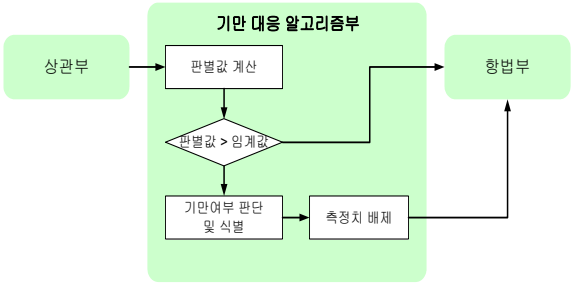

Fig. 5. 기만대응 수신기 구조

기만대응 알고리즘은 판별값 계산부, 기만여부 판단 및 식별부, 측정치 배제부로 구성된다. 판별값 계산부에서는 기만신호와 GPS 위성신호 특성을 비교하여 기만 판단 여부 및 식별에 사용될 판별값을 계산한다. 패리티 공간기법을 사용하는 경우 식 (6), 코드-반송파 발산검사를 사용하는 경우 식 (9)를 사용하여 판별값을 계산한다. 기만여부 판단 및 식별 부에서는 계산된 판별값과 정해진 임계값 비교를 통하여 기만여부를 판단하고 해당 기만신호를 배제한다. 항법부에서는 기만신호가 배제된 측정치를 최소자승법을 이용하여 항법해를 계산한다.

4. 시뮬레이션 및 성능 분석

기만대응 기법들의 성능을 비교하기 위한 소프트웨어 기반의 시뮬레이션 환경은 Fig. 6과 같이 3절에서 설계된 신호 생성기와 기만대응 수신기로 구성하였다. 구현된 신호 생성기의 타당성은 상용 NordNav 수신기[15]를 이용하여 확인하였다[13].

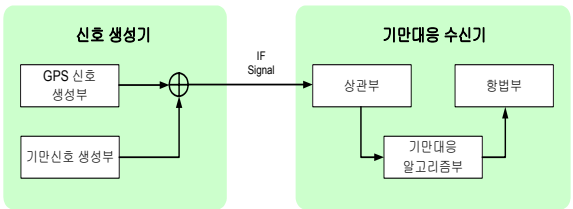

Fig. 6. 시뮬레이션 환경 설정

기만신호 대응기법 성능 분석을 위한 기만대상 수신기의 위치는 위도 36도, 경도 127도, 고도 100m이고, 가시위성의 배치 및 기만신호 시나리오는 Fig. 7과 같다.

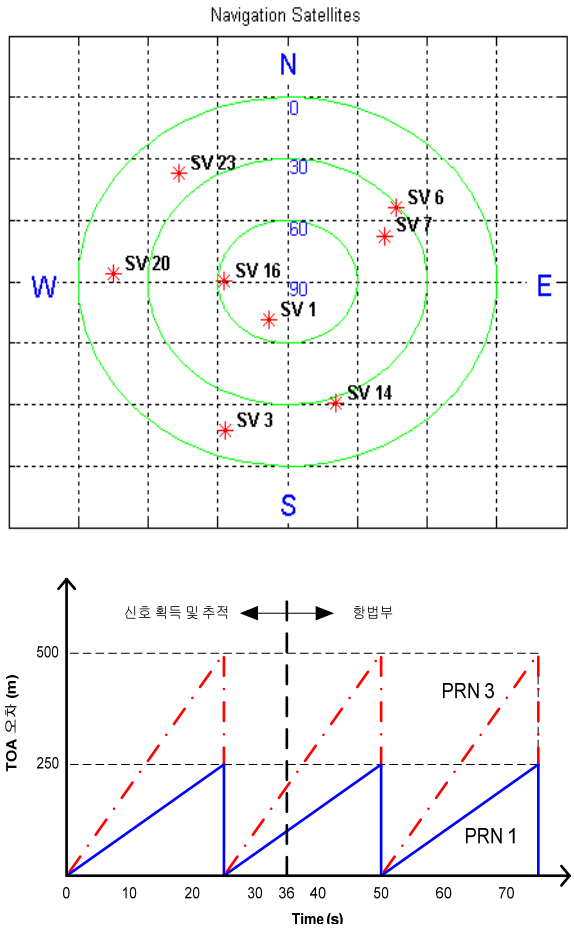

Fig. 7. 가시위성의 배치 및 기만신호 시나리오

항법 성능은 시뮬레이션 시간 70초 중 수신기가 신호 획득 및 추적 기능을 수행하는 초기 36초를 제외한 나머지 시간(34회)에 대하여 단일 기만과 이중 기만에 대해서 나누어 분석하였다. 단일 기만 시나리오는 Fig. 7과 같이 기만대상 수신기의 획득 및 추적이 가능한 도플러 주파수에서 기만대상 위성신호와 비슷한 신호전력으로 PRN 1번 위성에 대해서 TOA 오차가 초당 10m씩 증가하며, 25초 마다 오차를 초기화하는 기만신호를 이용하였다. 단일 기만신호 식별 및 항법 성능은 Table 1과 같다.

Table 1. 단일 기만신호 식별 및 항법 성능

	기만식별		수평오차 (CEP)	수직오차 (RMS)
	판단/ 기만	오식별/ 기만		
GPS	0/0	0/0	1.45m	2.32m
GPS+Spoofing	0/33	0/0	8.83m	19.18m
패리티공간	31/33	0/31	1.58m	2.59m
코드-반송파 발산검사	33/33	0/33	1.39m	2.46m

기만신호가 없는 경우에 비하여 기만신호가 있는 경우 약 8배 정도 수평, 수직 오차가 증가하였으며, 패리티 공간기법은 기만되지 않은 50초의 경우를 제외한33회 중 31회 기만신호를 검출한 반면 코드-반송파 발산검사는 33회 모두 기만신호를 검출하고 제거함으로써 항법 성능을 향상시킴을 확인하였다. 패리티 공간기법은 오차의 크기가 작은 부분에서 기만신호를 판단하지 못하는 경우에 대해서 임계값(Threshold)과 판별값(TS)을 비교하면 Fig. 8과 같다.

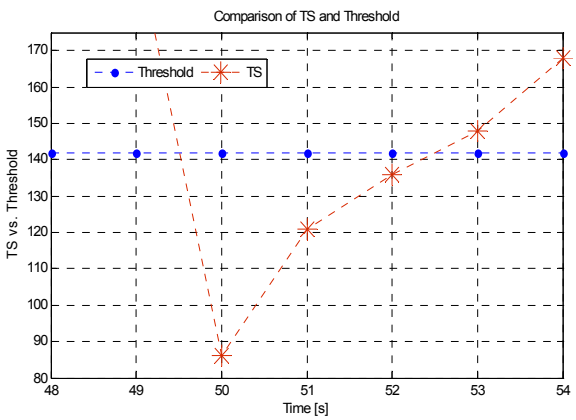

Fig. 8. 패리티 기법의 임계값과 판별값 비교

그림에서 51초와 52초에는 TOA 오차가 각각 10m, 20m로 인가 되었지만, 패리티 기법으로는 위성 고장 발생률로 임계값을 설정하기 때문에 TOA 오차가 적어 기만신호를 판단할 수 없었다. 50초인 경우는 기만에 의한 TOA 오차가 인가되지 않은 환경에 대해서 기만신호가 존재하지 않음을 판단하였다. 일반적인 패리티 기법은 1개의 기만신호를 대상으로 유도된 방법이므로 기만신호가 1개 이상인 경우 적용이 어렵다. 본 논문에서는 다중 기만에 대해서는 다중 기만에 효율적인 패리티 공간 재구성 기법[11]을 추가로 구현하여 성능을 분석하였다. 이중 기만신호 시나리오는 Fig. 7과 같이 단일 기만 시나리오에 PRN 3번 위성에 대해서 TOA 오차가 초당 20m씩 증가하며 25초마다 초기화하는 기만신호를 추가하여 성능을 분석하였다. 모의시험결과 패리티 공간기법은 항법 성능이 악화되고, 패리티 공간 재구성 기법과 코드-반송파 발산검사는 이중 기만신호를 검출하고 제거할 수 있어 항법 성능이 향상되었다. 패리티 공간기법은 TOA 오차가 적은 51초를 제외한 33회 중 32회 기만신호를 검출하였으나, 잘못된 식별로 정상 GPS 위성신호가 제거되고 기만신호는 계속 유지되어 항법 성능이 기만신호 검출 기법을 적용하지 않은 경우보다 더 나빠진 것을 확인할 수 있다. 반면 패리티 공간 재구성 기법은 51 초의 경우를 제외하고는 모두 기만신호를 판단하고 제거할 수 있었다. 코드-반송파 발산검사는 위성 별로 따로 기만신호 검출을 진행하므로 이중 기만인 경우에도 성능이 악화되지 않고 100% 제거하였다. 이중 기만신호 식별 및 항법 성능은 Table 2와 같다.

Table 2. 이중 기만신호 식별 및 항법 성능

	기만식별		수평오차 (CEP)	수직오차 (RMS)
	판단/ 기만	오식별/ 기만		
GPS	0/0	0/0	1.45m	2.32m
GPS+Spoofing	0/33	0/0	11.29m	74.3m
패리티 공간기법	32/33	32/32	35.01m	97.18m
패리티공간 재구성기법	32/33	0/32	2.73m	4.58m
코드-반송파 발산검사	33/33	0/33	2.14m	4.21m

각각의 알고리즘을 PC(Intel(R) Core(TM) 2 Quad CPU @ 2.4GHz, 2.4GHz)에서 Matlab 프로그램 수행에 소요 시간을 측정한 결과 코드-반송파 발산검사는 0.8764초인 반면에 패리티 공간기법 및 패리티 공간 재구성 기법은 각각 1.0792초, 1.3748초로 각각 약 1.2배, 1.5배의 차이를 보였다.

5. 결 론

본 논문에서는 GPS 기만신호에 대한 개념 및 특성을 분석하고, 기만대응 기법을 살펴보았다. 특히 의사거리 측정치에 기만신호가 포함되는 경우, 기존의 상용수신기로 쉽게 구현할 수 있는 RAIM 기법인 패리티 공간기법과 LAAS 기준국에서 SQM으로 사용되는 코드-반송파 발산검사를 이용하여 효과적으로 검출하고 제거할 수 있음을 시뮬레이션을 통하여 확인하였다. 소프트웨어 기반으로 설계된 위성신호 생성기, 기만신호 생성기 및 기만대응 수신기를 이용하여 수행한 성능 평가에서 단일 기만과 이중 기만 모두에 대해서 위성 별로 기만 여부 판단 및 식별이 가능한 코드-반송파 발산검사 기법이 패리티 공간기법이나 패리티 공간 재구성 기법에 비하여 나은 성능을 나타내고, 적은 계산량으로 구현할 수 있음을 확인하였다.

후 기

본 논문은 2009년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음.

Reference

[1] 김병두, 김봉수, 최완식, “GNSS 표준화 동향 및 주요 표준화 기관”, 대한측량협회학회지 측량지, 통권 제77호, pp. 81～87, 2004.

[2] 이은성, 천세범, 이영재, 강태삼, 지규인, “자세결정시의 GPS 반송파 다중경로 오차 추정”, 한국항공우주학회지, 제33권, 제3호, pp. 65～70, 2005.

[3] Parkinson, B. W., Spilker, J. J. Jr., Global Positioning System : Theory and Applications, Vols. 1 and 2, American Institute of Aeronautics and Astronautics, Inc., Washington, DC, USA, pp. 143～164, 1996.

[4] Volpe, John A., Vulnerability Assessment of the Transportation Infrastructure Relying On the Global Positioning System : Final Report, Department of Transportation, USA, pp. 73～54, 2001.

[5] J. Warner and R. Johnston, “A Simple Demonstration That the Global Positioning System(GPS) Is Vulnerable to Spoofing”, Journal of Security Administration, in Press, pp. 5～8, 2003.

[6] G. W. Hein and F. Kneissl, “Authenticating GNSS Proofs Against Spoofs : Part 1”, Inside GNSS, Vol. 2, No. 5, pp. 58～63, 2007.

[7] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, “A Multi-Antenna Defense : Receiver-Autonomous GPS Spoofing Detection”, Inside GNSS, Vol. 4, No. 2, pp. 40～46, 2009.

[8] 박찬식, 이상정 외 8명, GPS 신호감지, 이상판단 및 방송기법 연구 : 연구 보고서, 충남대학교, 대전, pp. 121～176, 2005.

[9] “NAVSTAR GPS Space Segment/Navigation User Interface”, Rev C., ICD-GPS-200, 10 Otober 1993.

[10] 신미영, 조성룡, 임순, 정호철, 이진우, 이상정, “GPS 수신기에 대한 기만신호 영향 분석”, 제14차 GNSS Workshop, (주)GNSS 기술협의회, 제주도, p. 32, 2007.

[11] 유창선, 안이기, 이상정, “패러티 공간을 이용한 2개 GPS 파라미터 고장진단”, 한국항공우주학회지, 제31권, 제6호, pp. 52～60, 2003.

[12] Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, John Fagan, “Countermeasures for GPS Signal Spoofing”, ION GNSS 2005, ION, pp. 1285～1290. 2005.

[13] 임순, 신미영, 조성룡, 박찬식, 이상정, “소프트웨어 기반 GPS 기만신호 생성기 설계,” ICS’08 정보 및 제어 심포지엄, 대한전기학회 정보 및 제어부문회, 서울, pp. 63～64, 2008.

[14] 조득재, 다중 비트 처리 기법 기반의 소프트웨어 GPS 수신기 설계 : 공학박사 학위 논문, 충남대학교, 대전, pp. 53～128, 2005.

[15] NordNav User Manual, NordNav Technologies, www.nordnav.com