한국군사과학기술학회지 제13권 제2호, pp. 296~303, 2010년 4월

학술논문 센서 · 신호처리 부문

GPS 신호기만의 특성 및 수신기에 미치는 영향 분석

Analysis of GPS Spoofing Characteristics and Effects on GPS Receiver

신 미 영* 조 성 룡* 김 준 오** 송 기 원** 이 상 정*
Mi-Young Shin Sung-Lyong Cho Jun-Oh Kim Ki-Won Song Sang-Jeong Lee

Abstract

The term “spoofing” refers to the transmission of counterfeit signals to provide undetectable falsification of GPS service. A spoofing can be accomplished using information from open literature which defines the signal format and the data structure. Spoofing is intended either to produce erroneous navigation solutions or saturate the processor of the victim receiver. The GPS receiver has no way to get rid of the effect of a spoofing because GPS receivers for civil service do not have an anti-spoofing scheme. This paper analyzes the spoofing characteristics, spoofing methods and environment conditions. And the spoofing effects on GPS receiver are analyzed in detail using the designed software-based spoofer and the Nordnav receiver.

Keywords : GPS(Global Positioning System), Interference(방해요소), Spoofing(신호기만), Spoofer(기만기), Anti-spoofing (기만대응), Spoofing signal(기만 신호), C/A code spoofing(코드기만)

1. 서 론

GPS(Global Positioning System)는 사용자에게 정확한 PVT(Position, Velocity, Time) 정보를 전달하기 위한 목적으로 운용중인 전파항법시스템이다. GPS 시스템의 기능을 방해하기 위한 고의적인 방해요소(Interference)로 재밍(Jamming), 블러킹(Blocking), 신호기만(Spoofing), 미코닝(Meaconing) 등이 있다[1,2]. GPS 신호는 지구의 표면에서 약 1×10^{-16}[watts]의 낮은 전력세기를 갖기 때문에 GPS 수신기 안테나를 결렬시키거나 금속물체를 이용하여 안테나를 커버함으로써 쉽게 GPS 신호를 블러킹 할 수 있다. 뿐만 아니라 GPS 신호와 같은 주파수 대역의 큰 신호전력을 송신하는 재머를 이용하여 쉽게 재밍할 수 있다. 블러킹이나 재밍의 목적은 타깃 수신기의 획득 및 추적기능을 방해하여 수신기가 PVT 정보를 서비스 받지 못하도록 하는 것이다. GPS 수신기는 신호 획득 및 추적을 못하므로 블러킹이나 재밍으로 인한 방해여부를 쉽게 인지할 수 있다. 이에 반해 신호기만과 미코닝은 타깃 수신기가 거짓된 정보를 실제 GPS 신호라고 판단하고 신뢰하여 사용하도록 하므로 사용환경에 따라 더 치명적인 영향을 미칠 수 있다. GPS 기만기는 공개된 GPS 신호 구조를 이용하여 오차가 인가된 거짓 GPS 신호를 생성하여 타깃 수신기에 송신함으로써 수신기를 기만할 수 있다. 미코닝은 수신기가 TOA(Time of Arrival) 정보를 사용하여 위

† 2010년 2월 3일 접수~2010년 3월 19일 게재승인
* 충남대학교(Chungnam National University)
** 국방과학연구소(ADD)
책임저자 : 이상정(eesjl@cnu.ac.kr)

치를 계산한다는 점을 이용하여 수신한 GPS 신호를 시간지연한 후 다시 수신기에 재송신함으로써 오차가 인가된 PVT 정보를 서비스 한다. 신호기만과 미코닝은 사용자가 정확한 PVT 정보를 서비스 받지 못하도록 거짓된 정보를 전달하는 것을 목적으로 한다. 수신기 입장에서는 신호기만 및 미코닝 여부를 판단하기 위한 알고리즘을 추가하기 이전에는 방해여부를 인지할 수 없으므로 어플리케이션 환경에 따라 치명적인 실수를 유도할 수 있다. 이를 방지하기 위해서 GPS 군용 신호인 P 코드는 Y 코드로 암호화되어 있으나 GPS 민간용 신호에 대해서는 기만 신호 방지기법이 구현되어 있지 않다.

현재의 GPS 군용 신호인 P 코드나 현대화 GPS 군용 신호인 M 코드 수신기를 우리 군의 모든 무기 체계에 적용하기 보다는 가격과 성능 및 기술 확보 등의 측면뿐 아니라 다양한 전술 능력의 확보를 위해서도 민간용 GPS 수신기를 적용하는 것이 합리적인 방안이라고 볼 수 있다. 따라서 GPS 수신기 내에서의 기만 신호 방지기법의 개발은 필수적인 요소이다. 특히, 정확성 및 신뢰성이 요구되는 공항 지역 및 해안 지역의 경우 사용자 수신기의 이동경로 및 패턴이 일정하므로 신호기만의 위험성이 높으며, 만일의 사태를 위하여 GPS 수신기 자체적으로 기만 신호에 대한 대처 방안 및 기만 신호 방지기법이 필요하다. 그러나 아직까지는 민간분야 뿐만 아니라 항공분야, 군용분야에서 사용하고 있는 민간용 GPS 수신기에도 기만여부를 판단하고 대응하기 위한 알고리즘이 구성되어 있지 않다. 신호기만의 위험성 및 기만 대응의 필요성에 대한 인식이 확산되는 상황에서, 기만 대응 연구에 앞서 기만 신호의 특성 및 기만 신호가 GPS 수신기에 미치는 영향에 대한 연구가 선행되어야 할 것이다. 본 논문에서는 기만 신호의 특성을 분석하고, 기만 신호가 GPS 수신기에 미치는 영향을 분석하기 위하여, 구현한 소프트웨어 기반의 기만기와 상용 GPS 수신기를 사용하여 각 세부블록에 미치는 영향을 분석하였다.

2. 기만 신호의 특성

가. 기만 신호의 정의

GPS 기만 신호는 GPS 신호와 동일한 구조를 갖으나, 수신기가 정확한 PVT 정보를 서비스 받지 못하도록 거짓된 항법 데이터(위성 위치, 시각, 보정 관련 데이터의 기만) 또는 의사거리 정보를 포함한다. 신호의 기만은 수신기가 GPS 신호가 아닌 거짓된 정보를 갖고 있는 기만 신호를 획득하여 항법 시 오차를 유도함으로써 어플리케이션 환경에서 오류가 발생하도록 하기위한 목적으로 거짓 정보를 송신하는 것을 말한다.

현재 어플리케이션 환경에서 사용하고 있는 대부분의 GPS 수신기는 신호기만에 대하여 대응기능을 전혀 갖추지 않은 상태이므로, 굳이 복잡하고 정밀한 기만 방법을 사용하지 않더라도 항법 데이터 기만과 같이 간단하고 단순한 방법에도 쉽게 기만될 수 있다. 기만 검출 기능을 갖고 있는 수신기라면 기만된 위성신호를 이용하여 계산한 의사거리를 제외한 나머지 위성신호를 이용하여 계산한 의사거리를 이용하여 항법해를 도출함으로써 신호기만에 쉽게 대응할 수 있다. 따라서 GPS 기만기 입장에서는 타깃 수신기에서 실제 GPS 신호와 비슷한 특성을 보이도록 기만 신호를 생성하는 것이 관건이고, 수신기 입장에서는 각 위성채널마다 기만여부를 검출할 수 있는 기능을 추가하여 기만에 대응하는 것이 관건이다.

나. 신호기만 조건

GPS 기만 신호는 GPS 신호와 동일한 구조 및 형태가 요구되고, 사용자의 수신 안테나에 GPS 신호와 비슷한 신호전력 레벨로 수신되어야 하며, 실제 GPS 위성으로부터 수신기까지의 신호 전달 시간을 고려한 측정치 정보를 포함하여야 한다. GPS의 민간용 신호는 ICD-GPS-200C[3]에 신호구조가 공개되어 있고, 코드가 암호화되어 있지 않으므로 동일한 구조와 형태로 신호를 모사할 수 있다. 수신 전력은 기만기와 타깃 수신기 간의 거리와 주변 환경에 따라 민감하게 변하므로 타깃 수신기 근처에 기만기와 네트웍으로 연결된 별도의 수신기를 위치시켜 조정할 수 있다. 하지만 이 방법은 구조가 복잡하고, 여러 제약조건으로 인해 구성하기 까다로운 단점이 있다. 매 순간의 수신기의 위치정보를 갖고 있지 않은 상황에서는 신호전력의 정밀한 조정이 어렵기 때문에 일반적으로 기만 신호는 타깃 수신기를 정하기보다는 Fig. 1과 같이 타깃 범위를 정하고 그 범위 안에 위치한 수신기를 기만하기 위한 목적으로 사용할 수 있다. 따라서 기준국과 같이 사용자의 위치가 고정된 환경이나 공항, 선박장, 공사장과 같이 사용자의 이동 패턴이 일정한 지역이

신호기만의 주요 타깃이 될 수 있다. Fig. 1과 같이 기만 환경을 구축하면 타깃 수신기의 대략적인 위치와 기만기의 위치 정보를 알 수 있고, 두 수신기는 동일한 가시위성을 갖기 때문에 타깃 위성의 위치 정보도 알 수 있다. 세 지점의 위치 정보를 이용하여 기만기는 타깃 위성으로부터 타깃 수신기까지의 TOA 정보를 예측하고, 이를 고려한 기만 신호를 생성할 수 있다.

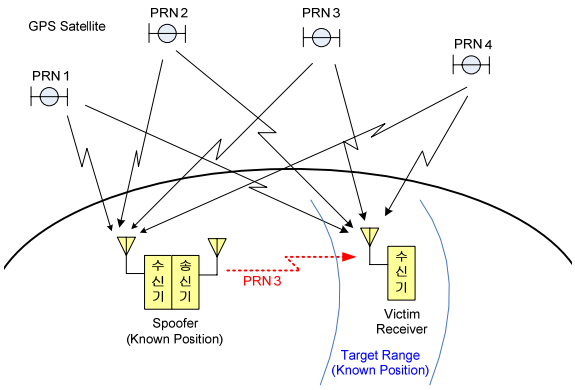


Fig. 1. 기만환경

1) 기만 신호의 생성 시 고려사항

타깃 위성의 위치와 타깃 수신기의 위치를 기만한 기만 신호의 의사거리는 식 (1)과 같다[4].

$$PR_{Spoofer-i} = \sqrt{(x_{Spoofed\ Rec.}-x_i)^2+(y_{Spoofed\ Rec.}-y_i)^2+(z_{Spoofed\ Rec.}-z_i)^2} + \sqrt{(x_{Rec.}-x_{Spoofer})^2+(y_{Rec.}-y_{Spoofer})^2+(z_{Rec.}-z_{Spoofer})^2} + cb_{Spoofer}+cb_{Rec.} \quad (1)$$

여기서 $(x_{Spoofed\ Rec.},\ y_{Spoofed\ Rec.},\ z_{Spoofed\ Rec.})$는 타깃 수신기의 기만된 위치, $(x_i,\ y_i,\ z_i)$는 i번째 타깃 위성의 기만된 위치, $(x_{Rec.},\ y_{Rec.},\ z_{Rec.})$는 타깃 수신기의 실제 위치, $(x_{Spoofer},\ y_{Spoofer},\ z_{Spoofer})$는 기만기의 실제 위치, $b_{Spoofer}$는 기만기의 내부 클럭 오차, $b_{Rec.}$는 타깃 수신기의 내부 클럭 오차, c는 빛의 속도이다. 이 때, 첫 번째 항은 기만기로 인해 기만된 위성과 타깃 수신기간의 거리를 나타내고, 두 번째 항은 기만기와 타깃 수신기간의 거리를 나타낸다. 따라서 기만기는 두 항의 관계를 고려하여 측정치를 생성하여야 한다.

2) 기만 신호의 송신 시 고려사항

기만기는 일반적으로 GPS 수신기와 같이 지면에 위치한다. 대부분의 GPS 수신기는 낮은 앙각으로 수신되는 GPS 신호를 사용하지 않기 위하여 막음각(Mask Angle)을 설정하므로 기만기의 위치는 타깃 수신기보다 비교적 높은 고도에 위치하여야 한다. 또한 기만기의 송신 신호전력은 거리에 따라 식 (2)와 같이 전파 전력 손실을 가지므로 이에 대한 영향을 반영하여 타깃 수신기로부터의 기만기의 위치와 송신전력을 결정하여야 한다. 여기서 L_p는 전파 전력 손실이며, d는 기만기로부터의 거리이고, λ_j는 송신신호의 파장이다.

$$(L_p)_{dB} = 20\log_{10}\left(\frac{4\pi d}{\lambda_j}\right)[\mathrm{dB}] \quad (2)$$

3) 기만기의 위치 선정 시 고려사항

기만 신호를 송신하는 기만기의 위치가 결정되고 나면, 기만기를 중심으로 Fig. 2와 같이 기만기와 수신기간의 거리에 따라 수신기에 미치는 영향을 구분할 수 있다. 이 영향은 기만기의 송신전력과 기만기와 타깃 수신기의 거리에 따른 전력 손실과 밀접한 관계가 있다. 만약 타깃 수신기가 r_{jam} 범위 내에 위치하면 높은 기만 신호 전력은 타깃 수신기에 재밍과 같은 영향을 미쳐 획득 및 추적 손실을 유도한다. 타깃 수신기가 r_{spoof} 범위 내에 위치하면 기만 신호는 타깃 수신기를 기만하여 항법오차를 유도한다. 그러나 타깃 수신기가 r_{spoof} 범위를 벗어나면 미약한 기만 신호 전력으로 인해 기만기는 타깃 수신기에 어떤 영향도 미치지 못한다. 따라서 기만기의 위치는 이와 같은 영향을 고려하여 선정하여야 한다. 이 때, r_{jam}은 수신기의 재밍여유 이상의 레벨로 신호가 수신되는 범위이며, r_{spoof}는 수신기의 신호획득 임계값 이상의 레벨로 신호가 수신되는 범위이다.

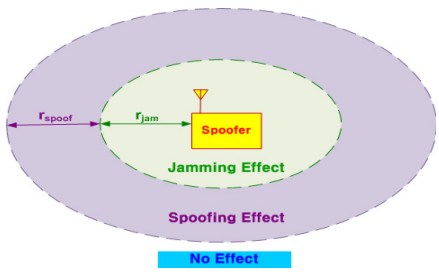


Fig. 2. 기만기와 수신기간 거리에 따른 영향

다. 기만 방법론

기만기는 타깃 위성과 타깃 수신기 간의 TOA를 예측하고, 타깃 수신기에 위성과 동일한 신호를 전송하여 실제 위성신호로 오판하도록 한 다음, 타깃 수신기가 기만 신호를 획득하고 추적하면 TOA 조정, 도플러 변경, 신호 크기 변경 등을 가하여 타깃 수신기의 항법 오차를 증가시킬 수 있다.

1) 기만 방법에 따른 시나리오

GPS 신호를 기만하여 수신기의 항법 오차를 증가시키기 위한 구조는 크게 항법 데이터를 기만하는 방법과 측정치의 시간지연을 통해 의사거리를 기만하는 방법이 있다.

항법 데이터 기만은 타깃 위성의 위치 정보 및 클럭 정보와 관련된 데이터를 기만하는 구조이다. 수신기는 위성과 수신기의 위치를 이용하여 식 (3)과 같이 위성과 수신기간 의사거리를 계산한다.

$$PR_i = \sqrt{(x_{Rec.} - x_i)^2 + (y_{Rec.} - y_i)^2 + (z_{Rec.} - z_i)^2} + cb_{Rec.} \quad (3)$$

그리고 4개 이상의 위성과 수신기간 의사거리를 이용하여 삼각측량법으로 수신기 위치를 결정한다. 그러므로 항법 데이터의 위성의 위치정보를 기만하면 의사거리 오차가 발생하고, 이는 항법 오차에 영향을 미친다. 의사거리 오차에 영향을 미치는 기만의 타깃이 되는 항법 데이터는 Subframe 1의 위성 클럭 오차 보정 파라미터 (a_{f2}, a_{f1}, a_{f0}), Subframe 2, 3의 Ephemeris 관련 파라미터 (M_0, C_{rs}, C_{uc}, C_{us}, C_{ic}, C_{is}, C_{rc}), Subframe 4의 이온층 지연 오차 보정 파라미터 (α_0, α_1, α_2, α_3, β_0, β_1, β_2, β_3) 등이 있다.

의사거리 기만은 기만기에서 코드 위상 지연을 통해 수신기의 의사거리 측정치 PR_i에 직접 오차를 인가하는 방법으로 적용 시나리오에 따라 구분할 수 있다. 우선 가시위성이 아닌 위성이 타깃인 경우 제약조건 없이 스텝 함수, 펄스변환 함수, 램프 함수 형태로 오차를 인가할 수 있다. 반면 가시위성이 타깃인 경우 이미 수신기 자체적으로 획득 및 추적하고 있는 위성 신호를 대신하여 기만 신호가 획득되어야 하므로(Range Gate Capture 기술[1]) 몇 가지 제약조건이 필요하다. 첫째는 기만 신호의 수신전력 조건이다. 안테나 수신 전력은 $P_{antenna} = P_A + P_S + P_N$와 같으며, 여기서 P_A는 GPS 신호 전력, P_S는 기만 신호 전력, P_N는 잡음 전력이다. 기만 신호는 $P_A \ll P_S$와 같이 타깃 수신기가 기만여부를 판별해내지 못할 정도의 크기 내에서 위성신호에 비하여 높은 신호전력으로 수신되어야 한다. 만약 타깃 수신기에서 기만 신호와 타깃 위성신호의 코드 위상이 일치했다면, 수신기는 신호전력이 높은 신호를 추적할 것이기 때문이다. 둘째는 타깃 수신기 및 타깃 범위에 대한 정확한 위치정보를 갖고, 대략적인 TOA를 예측해야 한다. 기만 신호와 타깃 위성신호의 코드 위상을 일치시키기 위해서는 기만 신호의 코드위상을 특정 범위 안에서 적당히 흔들어 타깃 위성신호와 코드 위상을 일치시키는 방법밖에 없으며, 이때 램프 함수 형태의 오차를 이용할 수 있다. 기만기가 타깃 수신기로부터 코드 위상 오프셋, 주파수 변화, 위상 변화, 진폭과 같은 별도의 정보를 제공받지 않는 한 타깃 수신기가 기만 신호를 획득했는지 여부를 확인할 방법은 없으므로, 기만기는 특정 지연범위에서 지연량을 램프 함수 형태로 반복적으로 변동하여 타깃 수신기가 획득/추적하고 있는 코드 위상의 탐색 및 지연 오차 인가를 동시에 수행한다.

2) 기만 타깃에 따른 시나리오

기만의 대상을 어떤 것으로 하느냐에 따라 시나리오를 분류할 수 있다. 첫째로 한 개의 기만기가 한 개의 타깃 위성을 기만하는 것이 목적이라면, 기만기의 구조는 타깃 수신기가 수신하고 있는 가시위성에 대한 정보를 알고 있는 상태에서 타깃 위성의 한 채널에 대한 기만을 수행하면 된다. 이 때 타깃 수신기가 자체적으로 RAIM과 같은 무결성 알고리즘을 수행한다면 기만여부는 쉽게 검출될 것이다. 둘째로 한 개의 기만기가 다수의 타깃 위성을 기만하는 것이 목적이라면, 타깃 수신기가 수신하고 있는 가시위성에 대한 정보를 알고 있는 상태에서 타깃 위성의 다 채널에 대한 기만을 수행해야 한다. 만약 정교한 기만을 요구한다면 기만기의 구조는 처리구조가 복잡하고 정밀성이 떨어진다. 타깃 수신기가 GPS 신호를 수신하는 것과 똑같은 형태를 모사하기 위하여 정교한 기만을 하는 것은 까다로운 작업이므로 일반적으로 기만기가 하나의 타깃 위성을 대상으로 하는 이유가 이 때문이다. 정교한 기만을 요구하지 않는다면 간단하게 GPS 시뮬레이터만을 이용해서도 다수의 타깃 위성을 대상으로 하는 기만기를 구성할 수 있다. 다수의 타깃 위성을 대상으로 하는 기만기는 아무리 정교하게 신호를 모사한다고 하더라도 송신방향이 같다는 한계가 있고, 타깃 수신기 입장에서 보면 다수의 가시위성의 입

사방향이 동일하므로 이 특성을 이용하여 대응할 수 있다. 마지막으로 한 개의 타깃 위성을 기만하는 것을 목적으로 하는 기만기를 다수로 구성한다면, 기만기는 한 개의 기만기가 한 개의 타깃 위성을 기만하는 구조를 그대로 사용하여 정교한 기만이 가능하고, 타깃 수신기가 대응하기에도 어려운 구성이 된다.

3) 기만 환경에 따른 시나리오

기만 환경에 따른 시나리오는 기만 전의 재밍 인가 여부에 따라 분류할 수 있다. 타깃 수신기가 추적하고 있는 위성 신호를 대신하여 기만 신호가 획득되는 환경을 구성하기 위하여 기만기는 타깃 수신기 및 타깃 범위에 대한 정확한 위치정보를 갖고, TOA를 예측해야 한다. 하지만 기만기가 신호전송 과정에서 발생하는 도플러의 영향을 정확하게 계산하는 것은 어렵기 때문에 타깃 수신기에서 기만 신호와 추적 중인 타깃 위성신호의 코드 위상이 일치되도록 조정하는 것은 쉽지 않다. 만약 기만기가 기만 신호를 송출하기 전에 간섭을 인가하여 타깃 수신기가 획득 손실 및 재획득 과정을 거친다면 타깃 수신기가 재탐색 과정에서 기만 신호를 획득하도록 유도할 수 있다. 상용화된 수신기의 대부분의 경우에 재획득(Re-acquisition) 기능을 갖고 있으며, 재획득 시 획득 손실 전의 위성 궤도 정보와 대략적인 시간 정보 및 이전의 항법 정보를 이용하여 탐색범위를 최소화한 상태에서 재탐색을 시도한다. 따라서 기만기 입장에서는 타깃 위성을 기만하기 위하여 요구되는 기만 신호의 코드 위상 정확도를 낮출 수 있는 반면, 타깃 수신기의 상태에 따라 간섭을 인가하고 기만하는 추가적인 구성이 필요하다.

3. 기만이 GPS 수신기에 미치는 영향 분석

가. 수신기 단에 미치는 영향 분석

1) 실험환경

GPS 신호기만이 수신기에 미치는 영향을 분석하기 위하여 소프트웨어 기반의 기만 신호 발생기를 구현하고, Navsys 사의 GPS Signal Simulation Toolbox(Ver. 2.0)에서 제공하는 소프트웨어 기반 GPS 수신기를 사용하였다. 구현한 신호 발생기로 타깃 위성 신호와 램프 함수 형태의 오차를 인가한 기만 신호를 생성하고, 수신기의 상관부, 획득 및 추적부, 항법부에 미치는 영향을 분석하였다. 기만기가 타깃 위성에 대한 신호 전력과 TOA를 안다는 가정하에 PRN 15의 위성 신호에 같은 채널에 대하여 Fig. 3과 같이 램프 함수 형태의 오차가 인가된 기만 신호를 추가하였다. PRN 15의 위성 신호의 C/N_0는 43dB-Hz이고, PRN 15를 타깃으로 한 기만 신호의 C/N_0는 45dB-Hz로 설정하였으며, 오차는 신호를 획득한지 3초 이후부터 1chip/s로 증가하도록 설정하였다.

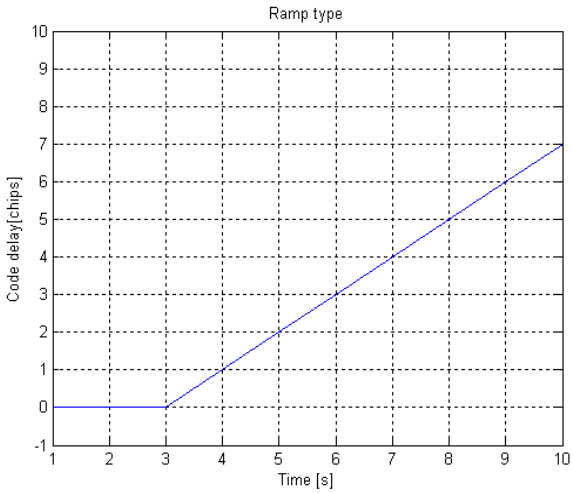


Fig. 3. 램프 함수 형태의 오차 인가

2) 영향분석

램프 함수 형태의 기만 신호 인가 시의 상관함수 형태는 Fig. 4와 같다. 3칩 이내에서 다른 칩 지연을 갖는 기만 신호가 인가된 경우에 시간에 따른 상관함수의 변이를 보기 위하여 GPS 소프트웨어 수신기의 추적부에서 2초에서 7초까지의 구간을 1초 단위로 확인하고, 시간에 따른 추이를 명암으로 표현하였다. Fig. 4를 통해 2초, 3초에서는 GPS 신호와 기만 신호가 같이 인가되어 상관함수의 최고치가 4배 정도로 나타나며, 4초에서는 기만 신호에 램프 함수 형태의 오차가 인가되어 상관왜곡이 발생하고, 5초 이후부터는 기만 신호를 추적하여 상관함수가 +1chip/s로 이동하고, 최고치도 기만 신호 크기로 유지되는 것을 확인하였다. Fig. 5는 램프 함수 형태의 기만 신호 인가 시의 C/N_0이다. 3초 전에는 43dB-Hz의 GPS 신호와 45dB-Hz의 기만 신호가 같이 인가되어 50dB-Hz의 신호전력을 보이며, 3초부터 5초 사이에는 기만 신호에 램프 함수 형태의 오차가 인가되고, 기만 신호를 추적하며, 신호 전력이 45dB-Hz까지 감소된 후, 5초 이후부터는 기만

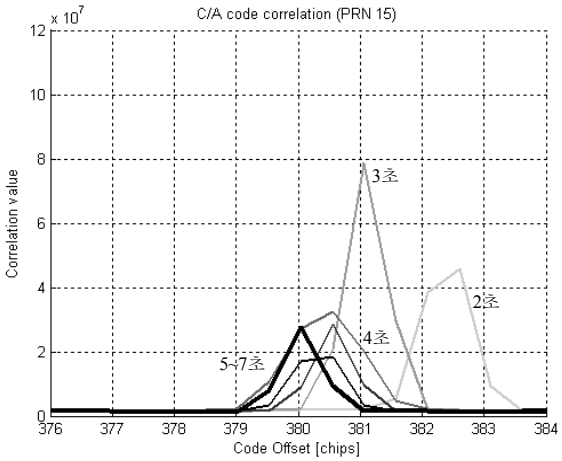


Fig. 4. 상관함수

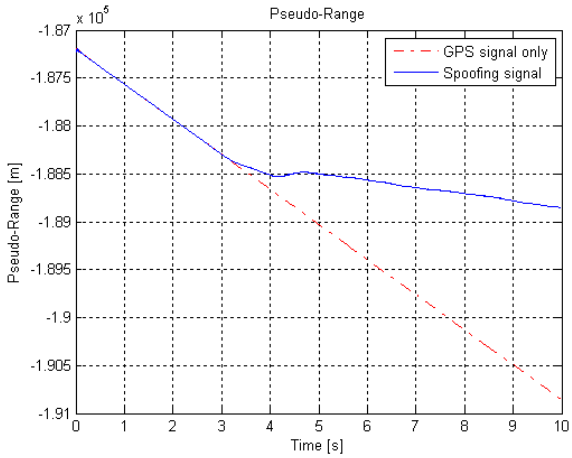


Fig. 7. 의사거리

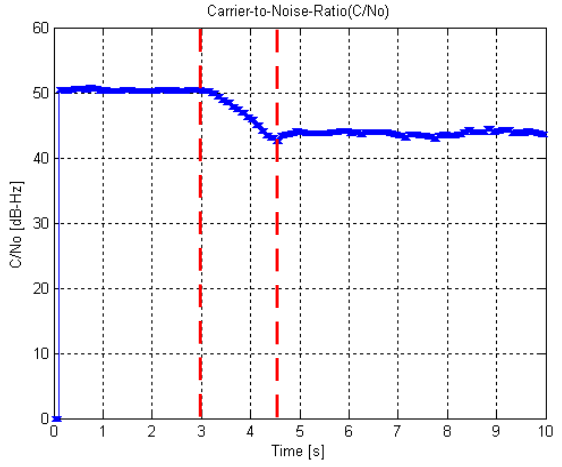


Fig. 5. C/N_0

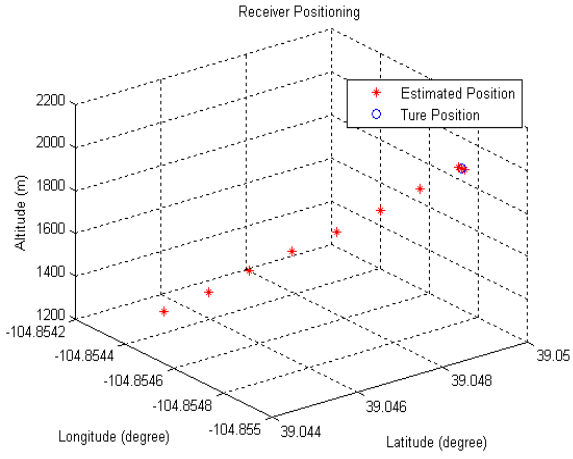


Fig. 8. 항법 결과

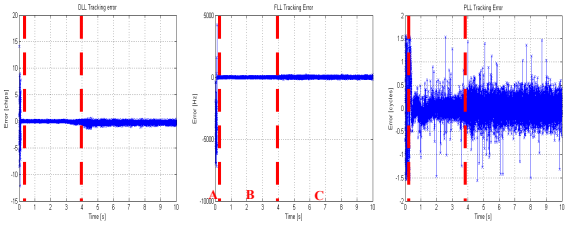


Fig. 6. 추적루프 오차

신호 전력만을 출력하는 것을 확인하였다. Fig. 6은 램프 함수 형태의 기만 신호 인가 시의 DLL 추적루프 오차, FLL 추적루프 오차, PLL 추적루프 오차이다. A구간은 신호 획득 전이고, B구간은 GPS 신호와 기만 신호를 같이 추적중인 상태이며, C구간은 기만 신호에 램프 함수 형태의 오차가 인가되어 기만 신호를 추적중인 상태이다. 추적루프 오차는 신호전력에 반비례하므로 B구간보다 C구간의 추적루프 오차가 크다. Fig. 7은 램프 함수 형태의 기만 신호 인가 시의 의사거리 측정치이다. 3초 전에서는 GPS 신호의 의사거리 측정치와 같으나, 3초 이후부터는 기만 신호에 램프 함수 형태의 오차가 인가되고, 기만 신호를 추적하여, 7초 동안 약 2,000m의 오차가 발생한 것을 확인하였다. 램프 함수 형태의 기만 신호에 의해 기만이 된 수신기의 항법 성능은 Fig. 8과 같다. 이 때, 수평면 오차는 110.237m(CEP)이며, 수직면 오차는 385.823m (RMS)로 증가한 것을 확인하였다. 실험을 통해 기만

신호가 GPS 수신기의 상관부, 획득 및 추적부, 항법부에 미치는 영향과 원인을 분석하였다. 우선 한 채널에 GPS 신호와 기만 신호가 동시에 인가되며 C/N_0 및 상관함수의 크기 변화를 가져오고, 3칩 이내에서 다른 칩 지연을 갖는 기만 신호가 인가되면 상관함수의 왜곡이 발생한다. 같은 칩 지연을 갖는 GPS 신호와 기만 신호를 추적하다가 기만 신호의 오차가 커짐으로 인하여 기만 신호만을 추적하는 과정에서 추적루프 오차가 커지며, 기만 신호에 인가된 오차의 영향으로 의사거리 오차 및 항법 오차가 증가한다. 따라서 기만 신호에 의해 GPS 수신기에 영향을 미치는 파라미터 중에서 C/N_0, 상관함수의 크기, 의사거리 측정치는 기만대응을 위한 목적으로 사용할 수 있다.

나. 거리에 따른 영향 분석

1) 실험환경

수신기의 위치에 따라 기만 신호가 미치는 영향을 분석하기 위하여 Fig. 9와 같이 시나리오를 구성하고, 수신기와 기만기의 거리에 따른 신호전력의 변화를 고려하여 실험 환경을 구성하였다. GPS 수신기는 NordNav사의 R30 모델을 사용하였다. 수신기의 초기 위치는 위도 36.364도, 경도 127.345도, 고도 93.798m로 설정하였고, 기만기 방향으로 50m/s의 속도로 총 80초 동안 이동하도록 시나리오를 구성하였다. 이 때 GPS 신호의 수신전력은 -126dBm으로 설정하였다. 기만기의 위치는 위도 36.416도, 경도 127.345도, 고도 1093.798m로 설정하였다. PRN 1 위성 채널을 기만하며, 인가한 기만 신호의 오차는 60초 이후부터 30m/s로 코드 지연 오차가 증가하고, 25초마다 리셋되는 램프 함수 형태이다.

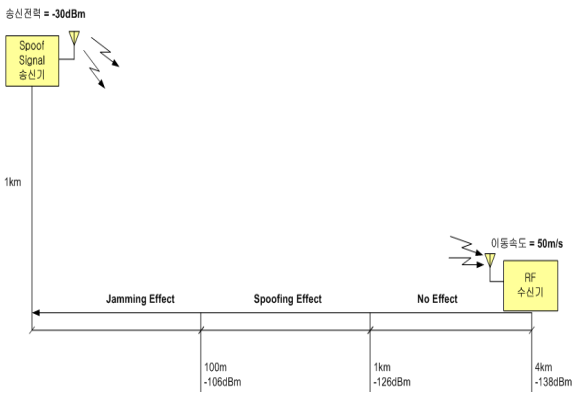


Fig. 9. 기만 시나리오

2) 영향 분석

시나리오를 통해 기만기로부터 수신기까지의 거리가 1km 이상 떨어져 있을 경우에는 기만 신호의 세기가 GPS 신호 전력보다 작아 큰 영향을 주지 않지만, 100m에서 1km 사이의 범위에서는 인가된 기만 신호의 세기가 GPS 신호 전력보다 약 2dB 이상 크므로 인가한 오차 형태로 기만이 발생하고, 100m 이내에 위치하면 기만 신호의 전력(C/N_0)이 60dB 이상으로 커져 다른 채널에 재밍으로 작용하여 신호 획득 손실을 일으킬 것으로 예상된다.

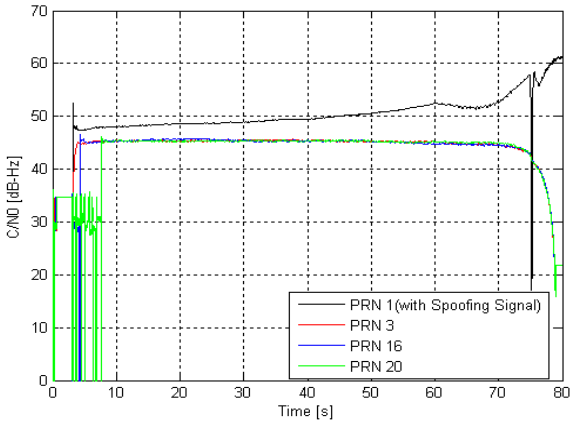


Fig. 10. 기만 신호가 인가되었을 경우의 C/N_0

성능 분석을 위하여 Nordnav 수신기를 이용하여 C/N_0, 의사거리, 측위 정확도를 확인하였다. C/N_0의 결과는 Fig. 10과 같다. PRN 1은 초기에 기만 신호와 GPS 신호가 같이 인가되므로 다른 채널에 비하여 C/N_0가 크다. 또한 수신기가 기만기를 향하여 50m/s로 이동하므로 기만기와 거리가 가까워짐에 따라 75초 이전까지 C/N_0가 증가하는 것을 확인할 수 있다. 기만기로부터 수신기까지의 거리가 250m 정도가 되면 기만 신호가 재밍으로 작용하여 다른 채널의 C/N_0가 급격히 하강하다가 기만기로부터 수신기까지의 거리가 100m 정도가 되면 PRN 1을 제외한 다른 채널의 위성 신호는 신호 획득 손실이 발생한다. 기만 신호가 인가된 PRN 1도 순간적으로 신호 획득 손실이 발생하나 수 초 이내에 신호 재획득이 이루어진 것을 확인할 수 있다. Fig. 11에서 GPS 위성 신호만 인가했을 때의 PRN 1의 의사거리와 GPS 위성 신호와 기만 신호를 인가했을 때의 PRN 1의 의사거리를 보였다. 수신기가 기만 신호를 추적하므로 램프 함수 형태의 기만오차

에 의하여 의사거리 오차가 발생하는 것을 확인할 수 있다. 기만기로부터 수신기까지의 거리가 1km 정도가 되면 기만 신호의 전력이 PRN 1의 신호전력보다 약 2dB 정도 크며, 이때부터 램프 함수 형태의 오차가 인가되어 의사거리 오차가 발생한다. 75초 이후에서 간혹 의사거리가 튀는 것은 이 때 당시에 신호 획득 손실 및 재획득이 이루어졌기 때문이다. 신호기만의 영향으로 측위 오차가 발생한 것을 보이기 위하여 Fig. 12에서 기만 신호를 인가하지 않은 경우의 측위 성능과 기만 신호를 인가한 경우의 측위 성능을 보였다. 그림을 통해 기만 신호를 인가한 경우 잘못된 위치정보를 추정해 나가는 것을 볼 수 있다.

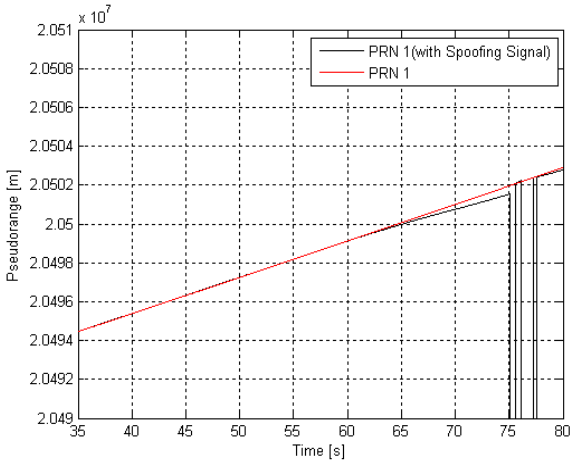
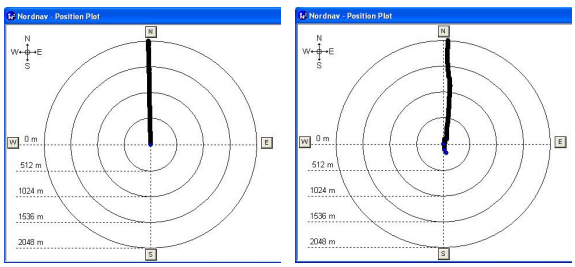


Fig. 11. 기만 신호 인가시의 의사거리



(a) 기만 신호 미인가 (b) 기만 신호 인가

Fig. 12. 항법 결과

위 그림과 같이 기만기와 수신기간 거리에 따라 시나리오와 같이 크게 세 구역에서 오차 미반영 지역(No Effect), 기만 지역(Spoofing Effect), 재밍 지역(Jamming Effect)이 구분되어 나타나는 것을 확인하였다.

4. 결 론

본 논문에서는 기만 신호의 특성을 분석하고, 기만 방법 및 환경 조건을 요약하였으며, 이를 바탕으로 소프트웨어 기반의 기만기를 구현하였다. 기만 신호가 GPS 수신기에 미치는 영향을 분석하기 위하여 구현한 기만기와 상용 GPS 수신기를 사용하여 기만 신호가 수신기의 상관부, 획득 및 추적부, 항법부에 미치는 영향과 원인을 분석하였다. 실험을 통해 기만 신호가 GPS 신호를 대신하여 획득되는 과정(Match-Capture-Pull off[11])에서 C/N_0가 변화하고, 상관함수의 크기 변화 및 왜곡이 발생하며, 추적루프 오차가 커지는 것을 확인하였다. 이와 같은 현상은 결국 의사거리 오차 및 항법 오차의 증가를 가져온다. 그리고 기만기와 수신기의 거리에 따른 기만 신호의 영향을 분석하기 위하여 시나리오를 구성하고, 결과를 분석하였다. 실험을 통해 기만기와 수신기와의 거리가 가까워짐에 따라 수신 전력도 증가하므로 기만기가 재밍으로서도 작용하는 것을 확인하였다.

본 연구결과에서 분석한 기만 신호의 특성, 제한사항, 동작절차, 적용범위, 수신기에 미치는 영향에 대한 정보는 기만 신호 탐지 및 대응전략을 연구하는데 필요한 기본 연구 자료로서 활용을 기대한다.

References

[1] John A. Volpe National Transportation Systems Center, “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System”, Final Report, Department of Transportation, August 29, 2001.

[2] Jon S. Warner, Roger G. Johnston, “GPS Spoofing Countermeasures”, Homeland Security Journal, December 12, 2003.

[3] Interface Control Document GPS-ICD-200 with IRN-200C-001 and IRN-200C-002, U.S. Dept. Air Force, 1997.

[4] Logan Scott, “Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems”, ION GPS/GNSS 2003, Portland, OR, September 9～12, 2003.