소프트웨어 기반 GPS 기만 신호 생성기 설계

임순*, 신미영*, 조성룡*, 박찬식**, 이상정*
*충남대학교 대학원 전자전파정보통신공학과, **충북대학교 전기정보통신공학부

Design of Software-based GPS Spoofing Signal Generator

Soon Lim*, Mi Young Shin*, Sung Lyong Cho*, Chansik Park**, Sang Jeong Lee*
*Division of Electronics, Radio Sciences & Engineering, and Information Communications Engineering, Chungnam National University
**School of Electrical and Computer Engineering, Chungbuk National University

Abstract - GPS의 활용 분야는 군용 항법 시스템에서 항공, 선박 등의 개인 항법 시스템으로 확장되었다. GPS가 넓은 범위에서 응용됨에 따라 Jamming과 같은 고의적인 간섭 신호의 제거에 대하여 많은 연구가 진행되었다. 그러나 기만 신호의 특성이나 기만 기법에 대한 연구는 미비하다.

본 논문에서는 기만 신호의 구조와 기만 개념을 연구하였으며 기만신호의 생성 기법으로 항법 메시지를 이용한 기법과 GPS PRN 코드를 이용하여 TOA(Time of Arrival)에 오차를 인가하는 기법을 정리하고 이중 TOA에 오차를 인가하는 방식을 GPS 소프트웨어 플랫폼에 구현하여 기만신호를 생성하였다. 또한 기만 신호 대응 기법의 개발 및 성능 분석을 위하여 소프트웨어 GPS 수신기를 이용하여 생성한 기만 신호가 GPS 수신기에 미치는 영향을 분석하였다.

1. 서 론

기만 신호 대응 기법은 INS를 이용한 통합 항법 시스템, 신호의 암호화를 통한 인증 알고리즘, 필터를 이용한 알고리즘이 있으며 이외에도 다양한 알고리즘이 존재한다. 하지만 기만 신호가 GPS 수신기에 미치는 영향에 대한 자료는 많지 않다. 기만 신호의 구조와 기만 기법의 연구를 통해 기존의 대응 기법 알고리즘보다 효율적인 알고리즘의 개발이 가능하다. 암호화를 통해 기만 신호 대응 기법을 제공하는 예로 P(Y) 신호가 있다. P 코드는 기만의 여지가 충분하지만 Y 코드로 암호화한 P(Y) 코드는 기만하는 입장에서 코드를 알 수 없으므로 기만이 불가능하다. 하지만 민간에서 사용할 수 있는 C/A 코드에는 암호화를 제공하지 않는다. 현재 C/A 코드를 이용하는 민간용 신호의 활용 범위가 넓으므로 기만 신호의 대응 기법이 필요하다. 본 논문은 추후에 연구할 기만 신호의 대응 기법 개발을 위해 기만 신호 생성기를 구현하고 시뮬레이션을 통해 기만 신호가 GPS 수신기에 미치는 영향을 확인하였다.

2. 본 론

2.1 GPS 기만 신호의 개념

대상 수신기가 잘못된 신호임을 인지하지 못하게 하여 대상 수신기에게 거짓 정보를 제공하는 신호를 기만 신호라고 한다. GPS 기만 신호는 대상 GPS 수신기에 인가되어 대상 수신기가 위성 신호 대신 기만 신호를 획득하고 추적하게 하여 항법 성능에 영향을 미친다.

GPS L1 신호는 암호화한 P 코드(P(Y) 코드)를 이용한 신호와 C/A 코드를 이용한 신호로 나눈다. P 코드는 10.23MHz에 1주일의 주기를 가지는 PRN 코드로 C/A 코드에 비해 주기와 길이가 길고 Y 코드를 이용한 암호화로 군용으로만 사용하고 있다[3]. C/A 코드는 1.023MHz에 1ms 주기의 코드로 P(Y) 코드와 달리 암호화를 제공하지 않으며 코드의 주기도 짧다. 그러므로 C/A 코드는 P 코드에 비해 좋은 기만 대상이다. GPS L1 C/A 신호는 수식(1)과 같이 표현한다[5].

$$S_{L1} = A_{L1}x(t)D(t)\sin(f_1 t) \tag{1}$$

A_{L1}는 신호의 전력, $x(t)$는 C/A 코드, $D(t)$는 항법데이터이다. GPS 기만 신호는 수식(2)과 같이 표현한다.[5]

$$S_{L1}' = A_{L1}'x(t-\tau)D'(t)\sin((f_1+\Delta f')t+\Phi') \tag{2}$$

A_{L1}'는 기만 신호의 전력, $x(t-\tau)$는 기만 신호의 C/A 코드, $D'(t)$는 기만 신호의 항법데이터이다. 기만 신호의 C/A 코드에는 τ만큼의 전송 지연을 인가했다. $D'(t)$는 기만 신호 생성기가 생성한 항법 데이터이다.

GPS 기만 신호는 GPS 위성 신호보다 전력 레벨이 높아야 한다. 그래야 대상 수신기의 추적부가 위성 신호 대신 기만 신호를 추적할 것이다. 그러나 기만 신호의 전력 레벨은 GPS 위성 신호의 최대 전력 레벨을 넘어가면 안된다. 기만 신호가 GPS 신호처럼 인가되려면 -153dBW를 넘어가지 않는 신호를 생성해야 한다[3].

기만 신호는 앞에서 언급한 신호 전력 레벨 외에 몇 가지의 조건을 더 요구한다. 우선 기만 신호 생성기는 자신의 위치를 정확히 알고 있어야 한다. 그리고 대상 수신기의 위치도 알고 있어야 한다. 이 두 좌표를 정확히 안다면 GPS 위성 신호의 전파 지연과 도플러 주파수를 계산할 수 있다. 만약 기만 신호 생성기가 도플러 주파수와 전파 지연을 정확하게 알고 있는 상태에서 기만 신호를 생성한다면 대상 수신기가 위성 신호 대신 전력 레벨이 높은 기만 신호를 추적할 것이다. 하지만 대상 수신기가 운동 중이면 전송 지연과 도플러 주파수는 정확하게 알 수 없다. 대상 수신기의 이동 속도에 따라 전송 지연과 도플러 주파수가 변하기 때문이다.

2.2 기만 기법

2.2.1 항법 메시지를 이용한 기만 기법

항법 메시지를 이용한 기만 기법은 기만 신호 생성기가 오차를 포함하는 항법 메시지를 생성하여 대상 수신기에 인가한다. 항법 데이터에는 시간, 위성의 궤도 정보, 전리층 지연 모델링 파라미터, 위성의 클럭 바이어스 보정 파라미터, 그리고 Almanac 정보가 있다.

위성 궤도 정보 중 기만이 가능한 파라미터로 위성의 클럭 바이어스 보정 파리미터, 위성의 궤도 정보가 있다. 위성 클럭 바이어스 보정 파라미터에는 항법 데이터의 서브프레임 1번에 a_{f2}, a_{f1}, a_{f0}가 있으며 수식(3)과 같이 클럭 바이어스 보정값 Δt_{SV}를 구한다[3].

$$\Delta t_{SV} = a_{f0} + a_{f1}(t-t_{oc}) + a_{f2}(t-t_{oc})^2 + \Delta t_r \tag{3}$$

a_{f0}는 클럭 바이어스(s), a_{f1}는 클럭 드리프트(s/s), a_{f2}는 주파수 드리프트(s/s^2)를 나타내는 파라미터이다. 의사거리의 수식(4)와 같이 계산한다.

$$\rho = r + c(t_u - \Delta t_{SV}) \tag{4}$$

만약 대상 수신기가 기만 신호 생성기가 제공하는 클럭 바이어스 보정 파라미터를 이용한다면 의사거리에 오차가 생기며 항법 성능에 영향을 미친다.

위성 궤도 정보 파라미터는 서브프레임 2, 3번에 있다. 궤도 정보 파라미터에는 Δn, M_0, Ω_e, e_s, i_0, $\sqrt{a_s}$, t_{oe}, w, $\dot{\Omega}$, $idot$가 있으며 궤도 보정 파라미터에는 C_{rs}, C_{rc}, C_{is}, C_{ic}, C_{us}, C_{uc}가 있다. 대상 수신기가 기만 신호가 제공하는 위성 궤도 파라미터를 이용해 위성 좌표를 구하면 위성과 수신기 사이의 거리 계산에 오차가 발생하며 항법 성능에 영향을 미친다.

2.2.2 TOA(Time of Arrival)에 오차를 인가하는 기만 기법

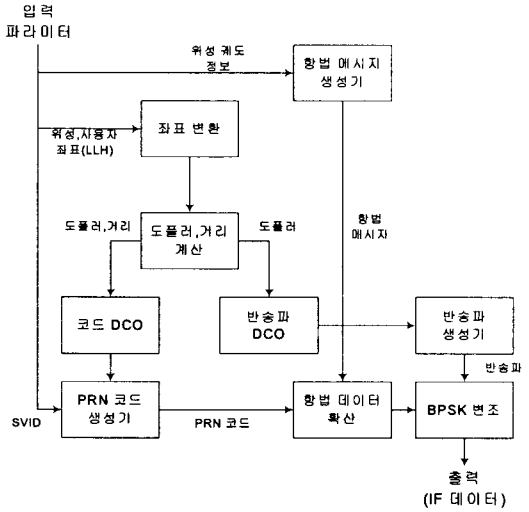
TOA(Time of Arrival))에 오차를 인가하는 방식은 GPS 위성 신호의 PRN 코드를 이용하는 기법이다. 위성 신호의 전송 지연은 PRN 코드로 구할 수 있다. 만약 기만 신호 생성기가 전송 지연을 인가한 PRN 코드를 생성하여 대응 수신기가 획득하고 추적하게 한다면 전송 지연이 의사거리에 반영되고 항법 성능에 영향을 준다.

TOA에 오차를 인가하는 방식은 Ramp 함수와 지수 함수의 형태로 증가하게 구성할 수 있다. 또한 Step 함수를 이용하여 TOA에 오차를 바이어스와 같이 인가할 수 있다.

3 소프트웨어 기반의 GPS 기만 신호 생성기의 설계 및 영향 분석

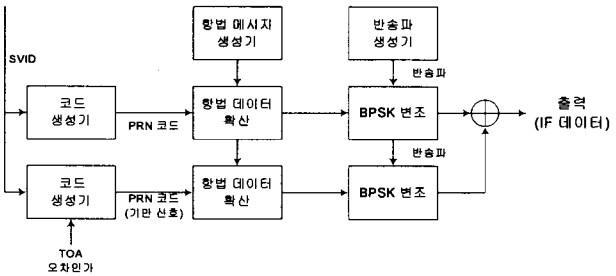
3.1 소프트웨어 GPS 기만 신호 생성기의 설계

소프트웨어 기반의 기만 신호 생성기는 Yuma Almanac 파일을 입력으로 받아 위성의 궤도 정보를 읽고 기만 신호를 생성할 위성 번호, 신호 생성 시간, 수신기 좌표, IF 대역, 그리고 샘플링 주파수를 사용자 임의로 입력받는다. 출력 데이터는 수신기의 디지털 부에 입력될 IF 데이터이다. 출력 데이터의 처리는 소프트웨어 GPS 수신기의 디지털 처리부를 이용하였다. 그림 2는 소프트웨어 GPS 신호 발생기의 블록 다이어그램이다.



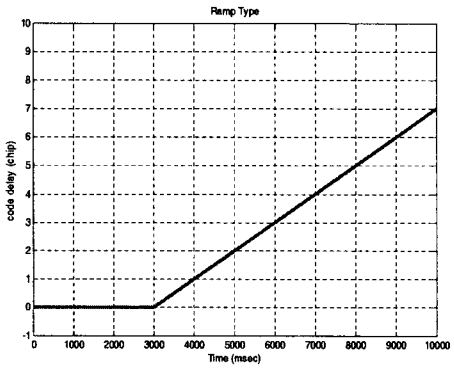
<그림 1> 소프트웨어 GPS 신호 발생기 블록다이어그램

그림 3는 GPS 위성 신호와 기만 신호를 생성하는 블록 다이어그램이다. 하나의 GPS 위성에 대하여 GPS 위성 신호와 기만 신호를 생성하여 IF 데이터로 출력하였다.



<그림 2> 기만 신호 생성 블록다이어그램

그림 3은 TOA에 인가할 오차이다. 기만 시작 시간이 3초라면 3초 이후에 TOA에 인가할 오차가 그림 3처럼 증가한다.



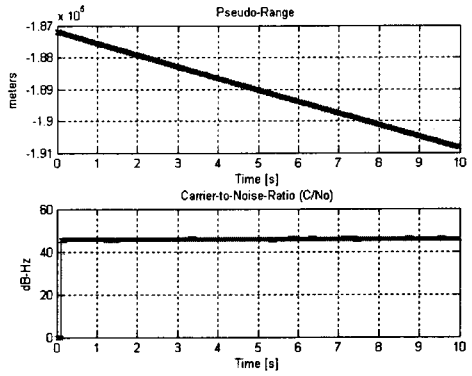
<그림 3> 램프 함수 형태의 오차 인가

3.2 소프트웨어 GPS 수신기를 이용한 영향 분석

본 논문에서는 기만 신호 생성기와 대상 수신기의 가시 위성이 같고 전파 지연, 도플러 주파수를 정확히 알고 있으며 대상 수신기가 고정 위치에 있는 이상적인 상황을 가정하였다.

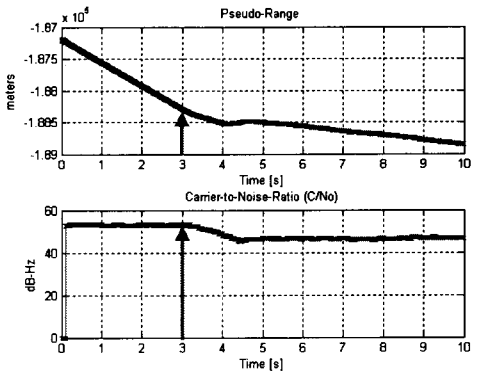
GPS 기만 신호 생성기를 이용하여 이상적인 GPS 기만 신호와 위성 신호를 생성하였다. 위성 신호의 전력은 43dB-Hz로 설정하고 기만 신호의 전력은 45dB-Hz로 설정했다. 기만 기법은 TOA에 오차를 Ramp 함수의 형태로 1chip/s씩 인가하는 기법을 사용했다. 기만의 시작은 3초 이후로 시작하도록 설정하였다.

아래의 그림 4에서 GPS 위성 15번의 의사거리와 C/N_0를 출력하였다.



<그림 4> 수신기의 획득 및 추적부 결과(GPS 신호)

그림 5는 기만 신호와 GPS 신호를 같이 인가하였을 때의 결과이다. 10초 동안 의사거리에 약 2000m의 오차가 발생하였다. 오차는 1초에 1chip을 증가하므로 3초부터 10초까지 7초 동안 Ramp 함수 형태로 증가하면 $293.255 \times 7 \approx 2000$m이다. 1chip은 293.255m이다. C/N_0는 3초 이후에 감소하다가 약 45dB-Hz에 수렴하는 것을 확인하였다.



<그림 7> 수신기의 획득 및 추적부 결과 (GPS 신호 + 기만 신호)

4. 결과 및 고찰

본 논문에서는 기만신호의 기본 개념을 조사하고 기만 신호가 GPS 수신기에 어떠한 영향을 미치는지에 대하여 분석하였다. 소프트웨어 기반의 기만 신호 생성기를 통하여 기본 개념을 토대로 IF 데이터를 생성하였으며 이를 소프트웨어 기반의 GPS 수신기를 이용하여 기만 신호의 영향이 측정치 오차로 나타남을 확인하였다.

추후 계획으로는 연구한 기만 신호의 영향을 토대로 수신기에 적용할 기만 신호 대응 기법 알고리즘을 개발하고 시뮬레이션을 통하여 대응 기법의 성능을 검증할 것이다.

[참 고 문 헌]

[1] 신미영, 조성룡, 임순, 정호철, 이진우, 이상정 "GPS 수신기에 대한 기만 신호 영향 분석," 제 14회 GNSS Workshop, 2007.11.

[2] Logan Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation System," ION GPS/GNSS 2003, 2003.

[3] John A., "Vulnerability Assessment of the Transportation Infrastructure Relying On the Global Positioning System," Final Report, U.S. Department of Transportation, 2001

[4] K.Deergha Rao, M.N.S.Swamy, E.I.Plotkin, "Anti-Spoofing Filter for Accurate GPS Navigation," ION GPS 2000, 2000.

[5] Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, John Fagan, "Countermeasures for GPS signal spoofing," The University of Oklahoma.

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

[7] Elliott D.Kaplan, Christopher J. Hegarty, Understanding GPS, second edition, Artech House, 2006.