2015년도 대한전기학회 하계학술대회 논문집 2015. 7. 15 - 17

4 채널 GPS Fake 신호 발생기 구현

권금철*, 양철관*, **심덕선***
중앙대학교*

Implementation of 4-Channel Fake GPS Signal Generator

Keum-Cheol Kwon*, Cheol-Kwan Yang*, Duk-Sun Shim*
Chung-Ang University*

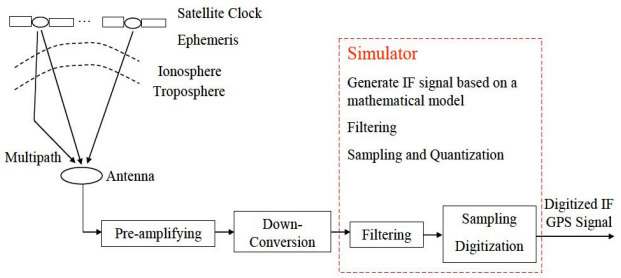
Abstract - As a basic research for the detection of GPS spoofing signal we study to generate a GPS fake signal which can mislead GPS receivers, and show that the fake signal is generated and transmitted through a pseudolite and the GPS receivers produce a wrong position as designated in the fake signal.

1. 서 론

군사목적으로 개발된 위성항법시스템인 GPS는 민간용으로 개방된 이후 여러 분야에서 활용이 증가되고 있다. GPS 신호는 지상에서의 세기가 -160dBW로 매우 낮아 여러 가지 전파 간섭의 영향을 받기 쉽다. 기만은 GPS 위성 신호와 같은 구조의 위조 신호를 이용하여 수신기로 하여금 오동작을 유도하는 방식이다. 현재 일반 상용GPS 수신기에는 기만신호에 대하여 대응하는 기능이 포함되어 있지 않아 이에 대한 감지 및 대응 기법에 대한 연구가 필요한 상황이다. 본 연구는 GPS 기만 신호 탐지를 위한 기초 연구로, 상용의 GPS 하드웨어 수신기에서 위조 신호에서 정한 임의의 사용자 위치 및 속도를 표시하도록 GPS 위조 신호를 생성하는 연구를 수행하였다.

2. 본 론

소프트웨어 GNSS IF 신호 생성기는 신호를 생성하는 데에 있어서 GNSS 위성 신호 종류와 중간 주파수(IF), 샘플링 주파수, 전치부(front-end) 필터 대역폭, 양자화 비트 등을 쉽게 변경할 수 있어 GNSS 관련 다양한 알고리즘 개발 및 성능 평가에 이용할 수 있다. 소프트웨어 GNSS IF 신호 생성기는 GNSS RF 신호가 안테나로 입사하여 하드웨어 전치부 처리를 통해서 IF 신호가 생성되는 과정으로 모사한다. 따라서 생성한 IF 신호는 GNSS RF 신호의 구조적인 특성뿐만 아니라 필터의 대역폭과 양자화 비트 등과 같이 하드웨어 RF 전치부에 의한 영향도 포함한다. 그림 1은 GNSS 신호 전송과 수신기에서의 신호처리 과정을 보여주고 있다.



<그림 1> GNSS 신호 전송과 RF 전치부에서의 신호처리 과정

2.1 GPS IF 신호 모델

GNSS IF 신호 발생기의 기본적인 블록으로부터 합성 신호가 생성되면, 합성 신호는 대역통과 필터와 A/D 컨버터를 통해 최종의 디지털 IF GNSS 신호가 생성된다. CDMA(Code Division Multiple Access) 방식을 사용하는 기본 GNSS 위성신호 모델은 다음과 같이 표현될 수 있다. 안테나에서 수신한 GNSS 신호는 아래식과 같이 위성시계오차, 이온층 및 대류층 지연 오차가 포함되어 있으며 신호 전송 시간과 도플러 주파수의 영향이 포함되어 있다. 다음 식은 오차 성분들을 포함한 GPS L1 C/A 신호의 표현식을 나타낸다.

$$S_{GNSSANTRF}(t) = \sqrt{2P_{GNSS}} * D_{GNSS-DATA}(t - t_p - t_{iono} - t_{tropo} - t_{clk}) * CACode(t - t_p - t_{iono} - t_{tropo} - t_{clk}) * C_{GNSS\blacksquare CARRIER}(w_{RF} + w_{doppler})(t - t_p - t_{iono} - t_{tropo} - t_{clk})$$

여기서 각 기호는 다음과 같다.

- w_{RF} : GNSS 신호의 RF 주파수
- $w_{doppler}$: GNSS 신호의 Doppler 주파수
- t_p : 신호 전송지연
- t_{iono} : 이온층 지연
- t_{tropo} : 대류층 지연
- t_{clk} : 위성 시간 오차

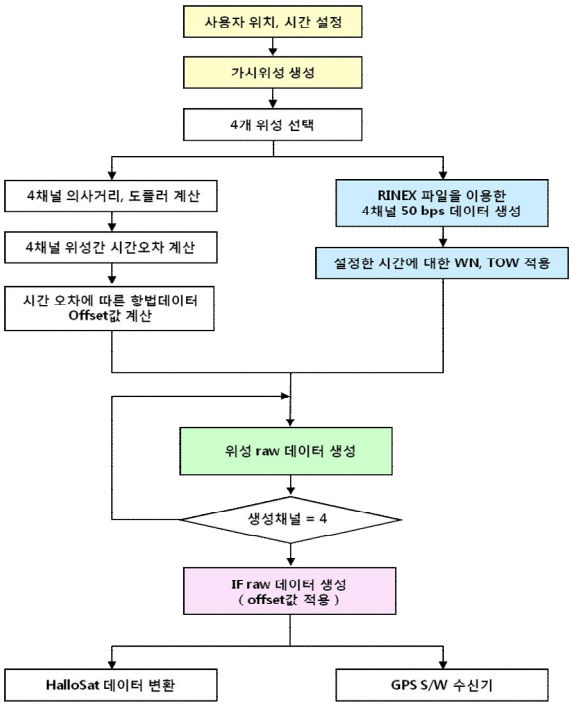
사용자 위치 계산을 위해서는 사용자 위치에서 위성들 간의 거리가 측정되어야 하는데 이 거리를 의사거리라고 한다. 시뮬레이터는 사용자 위치에서 설정된 4개의 위성에 대하여 위성의 궤도정보로부터 위성위치를 계산하여 사용자 위치에서의 거리를 계산한 다음 이를 이용하여 각 위성과 사용자 간의 의사거리와 도플러 주파수를 계산하여 GPS 신호 생성시 위성간의 전송시간 오차값으로 적용하여 위성 신호를 생성한다.

2.2 Matlab을 이용한 4채널 Fake 위성 신호 생성기 구현

4채널 GPS 신호 생성기는 그림2와 같이 구현된다. 사용자 위치와 시간을 설정하면 그 시간의 사용자 위치에서 보이는 가시위성에 대한 정보를 생성하고 이중에서 4개 위성을 선택하게 된다. 선택한 4개 위성에 대하여 RINEX 파일의 ephemeris 데이터를 이용하여 50bps의 위성 데이터를 생성하고 설정한 시간에 맞게 Week number와 TOW값을 계산하여 적용한다. 그리고 4개 위성에 대한 위성 위치와 위성간의 시간 오차와 도플러 주파수를 계산한다. 계산된 도플러 주파수를 반영하여 각 채널에 대한 위성 raw 데이터를 생성한다. 이렇게 생성된 4개의 위성 raw 데이터는 위성간 시간오차를 이용하여 계산된 offset값을 적용하여 더하는 과정을 거쳐 IF raw 데이터를 생성하게 된다. 이렇게 생성한 IF raw 데이터는 소프트웨어 수신기에 바로 적용이 가능한 형태로 만들어지고 HalloSat으로 송신하기 위하여 추가적인 변환과정을 거치게 된다.

- 사용자 위치, 시간 설정 : 사용자 위치 정보는 경위도 좌표값을 사용하며 위도, 경도는 degree 단위로 고도는 meter값으로 적용하고 프로그램 내부에서는 radian값으로 변환후 ECEF 좌표값으로 변환되어 사용된다.

- 가시위성 생성, 4개 위성 선택 : 특정 시간, 위치에서 보이는 위성을 모두 찾은 다음에 그중에서 4개의 위성을 선택한다. 그리고 선택한 위성에 대해서 각 위성의 위치가 ECEF 좌표값으로 구해진다.



<그림 2> GNSS 신호 전송과 RF 전치부에서의 신호처리 과정

- 4채널 의사거리, 도플러 계산 : 사용자의 ECEF 좌표값과 각 위성의 ECEF 좌표값을 이용하여 사용자와 위성간의 거리를 계산할 수 있고 시간에 따른 위성의 위치 변화값을 계산하여 도플러 주파수를 계산한다.

- 시간오차에 대한 항법데이터 offset값 계산 : 초기 위성의 배치상황에서 사용자와 위성간 신호 도달시간을 계산할 수 있다. 4개의 위성신호의 도달 시간 차이를 생성하는 IF 데이터에 맞게 샘플의 offset으로 계산한다.

- RINEX 파일을 이용한 50bps 데이터 생성 : 가시위성 생성에 사용한 RINEX 파일을 이용하여 선택한 4개 위성에 대해서 50bps 데이터를 생성한다.

- 설정한 시간에 대한 WN, TOW 적용 : subframe별로 변환된 파일의 시간정보는 RINEX 파일의 시간정보를 반영하고 있기 때문에 사용자가 설정한 시간에 대하여 week number와 TOW값을 계산하여 설정된 시간 정보값을 적용한다.

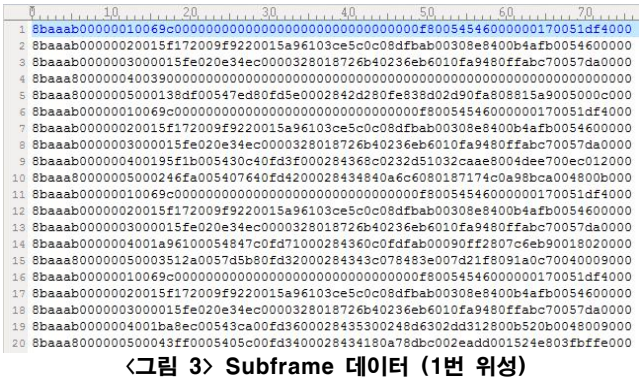
- 위성 raw 데이터 생성 : 계산된 도플러 주파수를 반영한 반송파(carrier wave) 신호를 생성하여 만들어 놓은 위성의 50bps 항법데이터와 C/A 코드를 적용하여 위성의 raw 데이터를 생성한다.

- IF raw 데이터 생성 : 생성된 4개 위성의 raw 데이터를 초기 위성의 시간오차로부터 계산된 offset값을 적용하여 더한 결과로 IF raw 데이터가 생성된다.

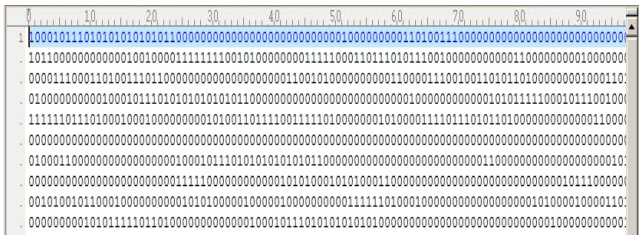
2.3 Fake GPS 신호 발생 및 수신 실험

본 연구에서 IF 신호 및 위성정보를 생성하기 위한 실험환경은 Inter Core(TM) i7-2600K CPU @3.40GHz, 16GB ram, windows7 64비트 컴퓨터에서 MATLAB 2013을 이용하여 생성하였다. Fake GPS 신호 발생기는 아래와 같은 장소, 시간에 맞는 신호를 발생하여 의사위성을 통해 송신하고 서울에서 수신한 상용 수신기가 아래 지정된 장소와 시간을 나타내는지 확인하는 실험을 수행하였다.

- 사용자 위치 설정(제주도 일출봉) : LLH = [33.458199, 126.941917 300];
- 시간 설정 : 2008년 1월 3일 8시 0분 0초 ~ 2008년 1월 3일 8시 2분 0초
- RINEX 파일 : brdc0010_2.09n

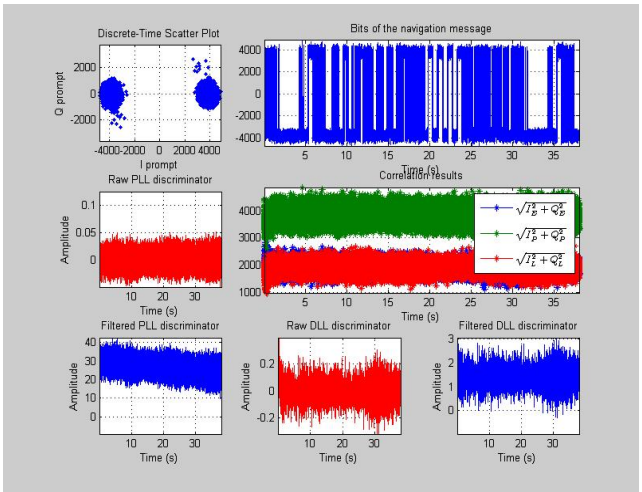


<그림 3> Subframe 데이터 (1번 위성)



<그림 4> IF 데이터 생성에 사용하는 50bps 데이터 파일

그림 3은 RINEX 파일로부터 생성한 1번 위성의 subframe 데이터를 보여주고 있다. Subframe 번호가 1~5번으로 반복되면서 각 해당 subframe에 값이 들어 있는 것을 확인할 수 있다. 그림 4는 IF 데이터 생성에 사용하는 50bps 데이터이며 그림 3의 subframe 데이터를 변환하여 사용한다. 그림5는 fake 신호에 대한 수신기 tracking 결과이다. 서울에서 수신한 신호의 측위계산 결과 fake 신호에서 지정된 제주도 성산 일출봉 위치가 잘 계산됨을 확인하였다.



<그림 5> GPS 소프트웨어 수신기의 Fake 신호추적 결과

3. 결 론

본 연구에서는 4채널 GPS fake 신호를 구현하는 연구를 수행하였다. Matlab을 사용하여 신호를 발생시키고 의사위성을 통하여 방사하였으며 GPS 수신기를 통하여 신호획득, 추적을 통하여 측위를 수행한 결과 fake 신호에서 제공한 거짓 위치가 잘 계산됨을 확인할 수 있었다.

[감사의 글]

본 논문은 중소기업청에서 지원하는 2014년도 산학연 공동기술개발 사업(No.C0212929)의 연구 지원으로 수행되었습니다.

[참 고 문 헌]

[1] James Bao-Yen Tusi, "Fundamentals of Global Positioning System Receivers: A Software Approach, John Wiley & Sons, 2005.