JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

항행 및 항법

J. Adv. Navig. Technol. 20(5): 394-400, Oct. 2016

암호화 신호원을 이용한 위성항법 기만 검출기법 모의

Simulation of GNSS Spoofing Detection Method Using Encrypted Ranging Signal

소 형 민
국방과학연구소

Hyoungmin So
Agency for Defense Development, Daejeon 34186, Korea

[요 약]

GPS P(Y) 코드와 같은 암호화 항법 신호원은 재생이 불가능하므로 기만에 강건하다. 하지만 암호화 신호원을 이용하기 위해서는 위성항법시스템 운용국가로부터 허가를 얻어야 하고 이용에 있어서도 상당한 제약이 따른다. 본 논문에서는 고이득 지향성 안테나를 이용하는 지상 기준국과 일반 위성항법 사용자를 모의하였다. 지상 기준국은 특정 항법위성에 대한 고이득 신호로부터 해당 위성이 방송하는 암호화 신호 코드를 복조하였다. 복조된 암호화 신호코드는 사용자 수신기 모의 데이터의 이상여부를 판단하고, 기만여부를 판단할 수 있었다. 본 논문은 이와 같은 방식을 적용하는 기만검출 기법을 제안하고 GPS 시뮬레이터를 이용한 모의분석 결과를 다룬다.

[Abstract]

It is well known that the encrypted ranging signal, such as GPS P(Y) code, is immune to spoofing attack. However, in order for users to use the signal, there needs permission from the operator. And also there are many restrictions for use because of security issues. In this paper, a ground reference station equipped with high-gain directional antenna and a user receiver were simulated. In the reference station, the encrypted code can be demodulated from the high-gain signal. And then the code can be used to detect spoofing attack in the user receiver. This paper proposes the spoofing detection method using the encrypted signal and deals with simulation results.

Key word : GPS spoofing, Anti-spoofing, GPS P(Y) code, Directional antenna, Encrypted signal.

http://dx.doi.org/10.12673/jant.2016.20.5.394

Received 21 September 2016 **Revised** 28 September 2016
Accepted (Publication) 19 October 2014 (30 October 2016)

***Corresponding Author; Hyoungmin So**

Tel: +82-42-821-4463
E-mail: hyoungmin.so@gmail.com

Ⅰ. 서 론

GPS (global positioning system)로 대표되는 위성항법 시스템은 인위적인 교란인 재밍(jamming)과 기만(spoofing) 공격에 취약한 것으로 알려져 있다 [1]. 재밍은 위성항법 수신 신호보다 강한 세기의 방해 전파를 방송하여 위성항법 사용자가 항법 위성 신호를 수신할 수 없도록 하는 교란 방식이다. 반면, 기만 공격은 항법위성 신호와 유사한 신호세기, 코드지연, 도플러 주파수, 항법메시지 등을 갖는 신호를 방송하여 사용자에게 혼란을 주는 방식이다. 재밍 공격은 사용자의 항법 가용성을 제한시켜 위성항법을 사용할 수 없게 만들지만, 기만 공격은 사용자가 교란 여부를 알지 못한채 잘못된 신호를 수신하고 항법을 수행한다는 점에서 잠재된 위험성이 매우 크다 [2]. 2011년 미국의 드론이 이란에 의해 탈취된 사건을 계기로 위성항법 기만에 대한 관심과 관련 연구가 증가하고 있다 [3]. 미국 University of Texas의 Todd Humphreys 교수는 무인 헬기를 대상으로 GPS 기만 실험을 수행하여 기만 공격을 통해 GPS 사용자를 잘못된 위치로 유도할 수 있음을 확인한 바 있다 [4].

이와 같은 기만 공격에 대응하는 항기만 기술에 관한 연구도 활발히 진행되고 있다. 미국의 Volpe 교통 센터에서 미국 교통성에 제출한 보고서에서는 기만 대응 기법을 성능에 따라 6가지로 분류하였다 [5]. 분류된 기법들 중 가장 우수한 기만 대응 기술은 암호화 인증 (cryptography authentication) 방식으로 암호화된 신호원을 이용하여 원천적으로 기만 공격을 배제하는 방식이다. 현재 가용한 암호화 항법위성 신호원으로는 GPS P(Y)코드가 있다. 하지만 해당 신호원을 이용하기 위해서는 암호화 신호원을 해독하기 위한 SAASM (selective availability anti-spoofing module) 장치가 탑재된 수신기를 이용하여야 한다 [6]. 미국은 자국의 무기체계와 우방국의 일부 무기체계에만 제한적으로 SAASM의 판매를 허용하고 있어, 우리나라와 같이 독자 위성항법시스템이 없는 경우 GPS P(Y)코드의 사용은 상당히 제한적이다. SAASM을 구매한 이후에도 주기적인 암호 장입 절차, 수신기 운용 환경 제약, 고비용 및 형상 제약 등의 한계를 갖게 된다.

최근의 기만 대응 기술 연구 결과 중, SAASM 장치 없이 GPS P(Y)코드를 이용하여 사용자 수신기의 기만 여부를 검출하는 기법이 제안된 바 있다 [7],[8]. 해당 연구에서는 두 개의 수신기를 사용하여 각각을 기준국과 사용자 수신기로 가정하고, 각 수신기에서 수집된 RF (radio frequency) 데이터 내에 동일한 GPS P(Y)코드 신호가 존재하는 지를 상호 비교하는 방식의 기만 검출 기법을 제안하였다. 실제 GPS P(Y)코드를 알지 못하더라도 두 개 수신기 가 수집한 RF 데이터를 상호 비교하여 상관이득을 확인할 수 있으므로, 암호화 신호인증 수준의 기만 대응 성능을 기대할 수 있다. 하지만 RF 데이터간의 상관 처리를 위한 고성능 프로세서가 필요하고, 데이터를 전송하기 위한 별도의 양방향 데이터 링크 및 RF 데이터 전송에 따른 높은 대역폭이 요구되는 단점이 있다. 또한 두 개의 수신기에서 채집된 GPS 신호의 채널간 간섭을 배제하기 위해서는 두 개 수신기 간의 상당한 이격 거리를 두어야 하는 운용상의 제약도 있다 [8].

본 논문에서는 두 개 수신기를 이용하는 기만 검출 기법의 제약을 완화하기 위한 방안을 제안하고 시뮬레이션을 통해 제안된 방식의 구현 가능성을 확인하고자 한다. 제안하는 방식은 기준국에 고이득 지향성 안테나를 적용하여 개별 항법 위성의 신호원을 획득한다. 일반적인 GPS 안테나로는 잡음 수준 이하에서 신호를 수신하게 되지만 접시 안테나를 적용하여 고이득을 얻게 되면 직접적으로 기저대역 신호를 해독할 수 있게 된다 [9]. 본 논문에서는 GPS 시뮬레이터를 이용하여 개별 위성의 고이득 신호 수신 데이터를 모의하고, 해당 신호원으로부터 GPS P코드를 복조하였다. 복조된 GPS P코드를 이용하여 사용자 수신기의 GPS 수집데이터의 상관이득을 확인하여, 제안된 기법의 가용성을 확인하고자 한다.

논문의 구성은 다음과 같다. 2장에서는 기존의 두 개 수신기를 이용하여 GPS P(Y)코드의 교차상관을 수행하는 기만 검출 기법을 간단히 정리한다. 3장에서는 본 논문에서 제안하는 기만 검출 기법의 개요를 설명한다. 4장에서는 제안된 기법을 모의 검증하기 위한 시뮬레이션 결과를 제시하고 5장에서 결론을 맺는다.

Ⅱ. 두 개 수신기를 이용하는 GPS P(Y)코드 교차 상관 기만 검출 기법 개요

본 장에서는 두 개 수신기를 이용한 GPS P(Y)코드 교차 상관 방식의 기만 검출 기법에 관하여 간략히 설명한다. 보다 자세한 알고리즘에 대해서는 미국 Stanford 대학 및 University of Texas 대학의 참고논문에서 확인할 수 있다 [7],[8]. 해당 논문들에서는 이러한 방식을 Codeless correlation 기반의 기만 검출 기법이라 하고, P(Y)코드 자체의 시퀀스를 모른채 두 개 수신기에서 채집된 RF 데이터 내에 동일한 P(Y)코드가 있는지를 확인하는 알고리즘을 제시하였다. 해당 기법에 적용되는 수신기를 각각 *a, b*라고 했을 때, 각 수신기에서 수신되는 GPS 신호모델을 수식 (1)과 같이 정의할 수 있다.

$$\begin{aligned} y_{ai} &= A_{ca}C_f(t_{ai})\cos\left[\omega_{IF}t_{ai}+\phi_a(t_{ai})\right] \\ &\quad + A_{pa}P_{Yf}(t_{ai})\sin\left[\omega_{IF}t_{ai}+\phi_a(t_{ai})\right]+n_{ai} \\ y_{bi} &= A_{cb}C_f(t_{bi})\cos\left[\omega_{IF}t_{bi}+\phi_b(t_{bi})\right] \\ &\quad + A_{pb}P_{Yf}(t_{bi})\sin\left[\omega_{IF}t_{bi}+\phi_b(t_{bi})\right]+n_{bi}. \end{aligned} \tag{1}$$

여기서 y_{ai}, y_{bi}는 수신기 *a, b*에서 수신된 GPS 신호의 i번째 샘플이다. 수신기 *a*를 기준으로 수식 (1)의 각 변수를 설명하면, A_{ca}, A_{pa}는 각각 GPS C/A코드와 GPS P(Y) 코드의 수신 신호 세기이고, $C_f(t_{ai}), P_{Yf}(t_{ai})$는 각각 i번째 샘플의 GPS C/A

(coarse/acquisition) 코드 및 P(Y)코드, $\omega_{IF}, \phi_a(t_{ai})$는 반송파 중간주파수와 위상, n_{ai}는 측정잡음을 나타낸다.

수식 (1)은 GPS 위성이 C/A코드와 P(Y)코드를 90°의 위상차이를 갖는 반송파에 변조하여 동시에 방송하고 있음을 보여준다. 상용 GPS 수신기는 공개된 GPS C/A코드를 재생하여, 수신된 신호의 GPS C/A코드와 동기를 맞추어 각 위성으로부터의 거리측정치를 획득할 수 있게 된다. 반면 P(Y)코드에 대해서는 허가된 사용자 외에는 해당 코드를 재생할 수 없기 때문에 상용 수신기는 P(Y)코드를 이용한 의사거리 측정치 및 항법메시지를 획득할 수 없게 된다. 동일한 원리로, 기만 공격을 수행하는 경우에도 P(Y)코드를 알 수 없기 때문에 P(Y)코드에 대한 기만 공격은 원천적으로 불가능하다.

Codeless correlation 기반의 기만 검출기법에서는 개별 수신기에서 P(Y)코드를 해독할 수 없으나, 두 개의 수신기 *a, b*에서 수신된 RF 신호에 동일한 P(Y)코드가 있다는 점을 이용한다. P(Y)코드로 항법을 수행할 수는 없으나 기만 여부를 판단하는 기준 신호로 이용하는 방식이다. 수신기 *a*를 안전한 장소에 설치되는 기준 수신기(인증시스템)로 가정하고, 수신기 *b*를 사용자 수신기로 가정하면, 수신기 *a*와 *b*에 동일한 P(Y)코드가 동기되어 존재하는 지를 확인하여 사용자 수신기 *b*의 기만여부를 판단할 수 있다.

Codeless correlation 기반의 기만 검출 기법은 P(Y)코드의 암호화 특성을 이용하기 때문에 기만 검출 성능은 가장 우수한 수준을 보여준다. 하지만 직접적으로 P(Y)코드를 이용할 수 없고, 두 개 수신기에서 채집된 RF/IF (radio frequency/intermediate frequency) 신호를 서로 상관하는 과정에서 구현상의 한계들을 갖고 있다. 그림 1에 해당 기법의 구현 개념도를 보였다. 우선적으로는 RF/IF 데이터를 상관처리하기 위해서는 고성능의 프로세서가 필요하기 때문에, 기만 검출 과정은 사용자 수신기가 아닌 지상의 기준용 수신기 또는 인증시스템에서 처리되어야 한다. 따라서 사용자는 인증시스템에 고용량의 RF/IF 데이터를 전송하여야 하고, 인증시스템은 기만여부를 사용자에게 전송하는 양방향 데이터링크가 확보되어야 한다. 성능 측면에서는 RF/IF를 상관하는 과정에서 상관이득 손실이 발생한다. 또한 두 개 수신기가 너무 가까이 위치하는 경우 채널간 간섭으로 인해 해당 알고리즘을 사용할 수 없게 되어, 지상 인증시스템 운용상의 제약도 발생한다.

Ⅲ. 고이득 지향성 안테나를 이용하는 Codeless correlation 기반의 기만 검출 기법

3-1 알고리즘 개요

본 논문에서는 이상의 기존 codeless correlation 기반의 기만 검출 기법이 갖는 한계를 극복하기 위하여 고이득 지향성 안테나를 이용하는 방식의 기만 검출 기법을 제안한다.

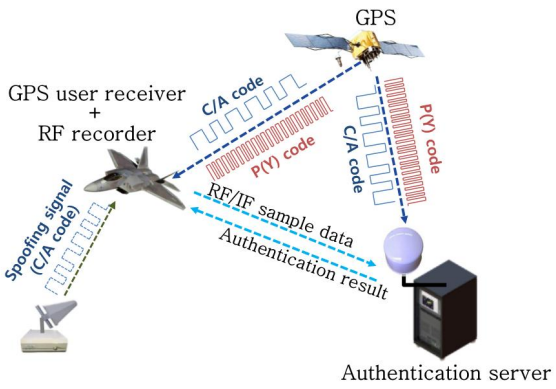

그림 1. Codeless correlation 기반의 기만 검출 기법 구현 개념도

Fig. 1. Conceptual view of the implementation of spoofing detection method based on codeless correlation.

GPS 신호는 지상에서 −130 dBm의 세기로 수신되어 잡음 보다 낮은 신호 세기를 갖기 때문에 확산대역코드를 역확산하는 방식으로 동기 검출을 수행한다. 하지만 개별 위성을 지향하여 고효율의 수신 이득을 확보하는 지향성 안테나 또는 위상배열 안테나를 이용하면 −130 dBm에서 30~50 dB 가량 증폭된 신호를 수신할 수 있다. 잡음 수준 이상의 세기로 수신된 신호에서 GPS C/A코드의 동기 정보를 이용하여 P(Y)코드의 시퀀스를 추출 할 수 있다. 추출된 코드 시퀀스를 사용자에게 방송하면 임의의 다수 사용자는 RF/IF 데이터가 아닌 P(Y)코드 시퀀스 자체를 기준 신호로 이용하여 기만 여부를 검증할 수 있다.

수식 (2)는 수식 (1)의 수신기 *a*에 고이득 지향성 안테나를 적용하는 경우의 수신 신호 모델을 정의하였다.

$$y'_{ai} = A'_{ca} C_f(t_{ai}) \cos\left[\omega_{IF} t_{ai} + \phi_a(t_{ai})\right] + A'_{pa} P_{Yf}(t_{ai}) \sin\left[\omega_{IF} t_{ai} + \phi_a(t_{ai})\right] + n_{ai}. \quad (2)$$

수식 (2)의 수신 신호세기 A'_{ca}, A'_{pa}는 수식 (1)의 A_{ca}, A_{pa}와 달리 잡음수준 n_{ai}보다 큰 값을 갖게 되어 기저대역의 코드 시퀀스 $C_f(t_{ai}), P_{Yf}(t_{ai})$를 직접 관측할 수 있다.

수식 (2)의 수신 신호로부터 P(Y)코드 시퀀스를 추출하는 과정은 다음과 같다. 우선 C/A코드에 대한 신호 획득 및 추적을 통하여 반송파 도플러와 위상정보를 획득한다. 추정된 반송파 도플러와 위상 $\hat{\omega}_{IF}, \hat{\phi}_a(t_{ai})$을 이용하여 수식 (2)에서 P(Y) 코드 성분을 분리하기 위한 믹싱과정은 수식 (3)과 같다. 이후 저역통과필터를 적용하면 수식 (4)와 같이 P(Y)코드 시퀀스를 추정할 수 있다.

$$\begin{aligned} y'_{ai} &= y_{ai} \cdot 2\sin\left[\widehat{\omega_{IF}} t_{ai} + \hat{\phi}_a(t_{ai})\right] \\ &= A'_{pa} P_{Yf}(t_{ai}) \left\{ \begin{array}{l} \cos\left[\left(\omega_{IF} - \widehat{\omega_{IF}}\right) t_{ai} + \left(\phi_a - \hat{\phi}_a\right)(t_{ai})\right] \\ -\cos\left[\left(\omega_{IF} + \widehat{\omega_{IF}}\right) t_{ai} + \left(\phi_a + \hat{\phi}_a\right)(t_{ai})\right] \end{array} \right\} + n'_{ai}. \end{aligned} \quad (3)$$

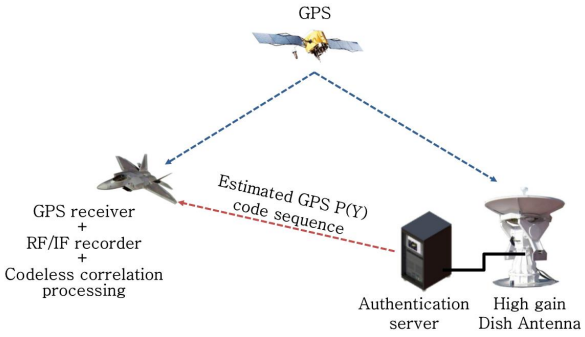

그림 2. 고이득 지향성 안테나를 적용하는 Codeless correlation 기반의 기만 검출 기법 구현 개념도
Fig. 2. Conceptual view of the implementation of spoofing detection method based on codeless correlation using directional high-gain antenna.

$$\widehat{P_{Yf}}(t_{ai}) \cong LPF\left[y_{ai}^{'}\right]. \quad (4)$$

수식 (4)에서 얻어진 P(Y)코드 추정결과는 기존의 codeless correlation에서 사용되는 RF/IF 데이터가 아니라 기저대역의 P(Y)코드 시퀀스를 직접 획득한 것이기 때문에 수 ms 수준의 코드 시퀀스만을 이용하여 기만 검출에 필요한 기준 데이터를 사용자에게 제공할 수 있다. 또한 상관 과정에 소요되는 과정도 단순화되어 사용자 수신기에서 처리과정을 수행할 수 있기 때문에 단방향 통신 링크만을 이용해서 기만검출 시스템을 구성할 수 있다. 기존의 사용자-인증시스템 양방향 통신 방식은 서비스할 수 있는 사용자의 수도 제한되고 소요되는 데이터 통신량도 높아지는 반면 제안하는 방식은 이러한 문제들을 해결할 수 있다. 또한 인증시스템과 사용자간의 거리에 대한 제한 조건도 본 방식에서는 해결할 수 있는 장점이 있다. 그림 2는 제안된 기법의 구현 개념도를 나타낸다.

3-2 구현 방안

이상에서 제안한 기만검출 기법은 개별 위성에 대하여 고이득 안테나를 이용해서 기만여부 판단의 기준이 되는 P(Y)코드 시퀀스를 획득하는 것이다. 이러한 기법을 구현하는데 있어서의 한계는 한 번에 다수의 위성에 대해 고이득 신호를 획득하기 어렵다는 점이다. 따라서 Dish 안테나를 이용하는 경우 순차적으로 개별 위성에 대한 P(Y)코드를 추출하는 방안을 고려할 수 있다. 배열 안테나를 이용하는 경우에는 수집된 RF 데이터로부터 후처리 방식으로 개별 위성에 대한 빔포밍 결과를 사용할 수 있다.

본 논문에서 제안하는 또 다른 방법은 단일 위성에 대하여 기만 여부를 확인하고 RAIM (receiver autonomous integrity monitoring)과 유사한 방식을 적용하여 전체 위성 군에 대한 기만 여부를 판단하는 방법이다 [9]. 일반적인 RAIM은 다수의 가시 위성에 대한 측정치와 항법해에 대하여 일관성을 벗어나는 측정치에 대하여 오류를 판단하는 방식을 이용한다 [10]. 이러한 접근은 위성항법 수신기가 기만을 당하는 경우 기만을 당한 의사거리 측정치와 그렇지 않은 의사거리 측정치 간의 일관성을 검증하는 방식에도 적용될 수 있다. 즉, 수식 (2)~(4)의 방법으로 하나의 위성에 대한 기만 여부를 판단하면, 해당 위성을 기준으로 다른 위성들과의 일관성을 검증하여 기만여부를 판단할 수 있다. 단일 기준신호와 RAIM을 이용하여 기만검출을 수행하는 알고리즘에 대한 구체적인 설명은 참고논문에서 확인할 수 있다 [9].

Ⅳ. 기만 검출 기법 시뮬레이션

4-1 시뮬레이션 구성

그림 2와 같이 제안된 기만 검출 기법을 구현하기 위해서는 GPS 신호 대역을 수신할 수 있는 Dish 안테나 또는 빔포밍 배열 안테나와 개별 위성을 추적할 수 있는 제어 장치가 필요하다. 본 논문에서는 이러한 장치가 구비되지 못한 상태에서 제안된 알고리즘의 가용성을 확인하기 위해 GPS 시뮬레이터를 이용하여 고이득 지향성 안테나로부터 수신된 신호를 모의하고 소프트웨어 수신기를 이용하여 GPS P(Y)코드를 추출하는 시뮬레이션을 수행하였다. 그림 3은 시뮬레이션 전체 구성도를 나타낸다.

그림 4는 GPS 시뮬레이터에서 PRN 18번 신호의 세기를 높이고 다른 위성에 대한 신호 세기를 낮추어 40 dB 이상의 이득을 갖는 신호를 생성하고 그 RF 출력을 스펙트럼 분석한 결과이다. 실제의 GPS 신호는 지상에서 −130 dBm으로 수신되어 C/A코드 및 P(Y)코드는 모두 잡음 수준 이하에 존재한다. 하지만 그림 4와 같이 특정 위성에 대한 고이득 신호 수신 결과는 각 코드의 스펙트럼을 직접 확인할 수 있다. 그림 4는 시뮬레이터

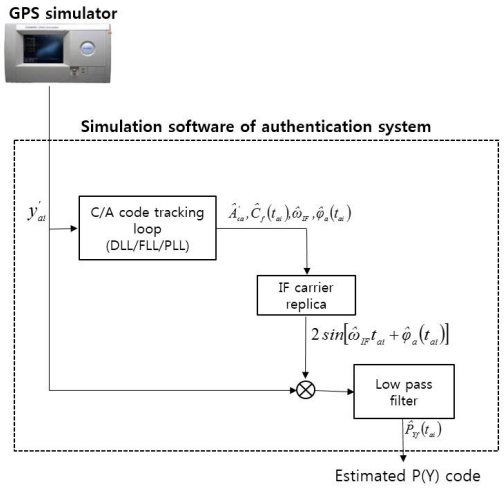

그림 3. GPS 시뮬레이터를 이용한 인증시스템 모의
Fig. 3. GPS spoofing detection simulation using GPS simulator.

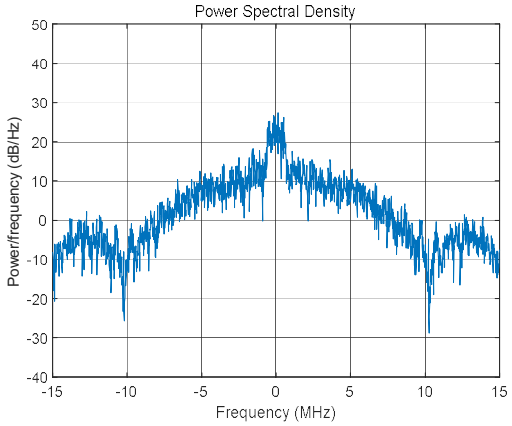

그림 4. GPS 시뮬레이터로 생성된 특정 위성의 고이득 RF 신호의 스펙트럼 분석 결과

Fig. 4. Power spectral density of the simulated high-gain GPS signal for a certain satellite generated by a GPS simulator.

를 이용하여 생성되었으나 고이득 dish 안테나를 이용하면 이와 동일한 수준의 GPS 위성 신호를 수신할 수 있다 [11].

4-2 시뮬레이션 결과

GPS C/A코드와 P(Y)코드를 추출하기 위해서는 직교 위상으로 방송되는 반송파를 분리할 수 있어야 한다. 그림 3에 도시한 바와 같이 소프트웨어 수신기를 이용하여 C/A코드에 대한 반송파 위상 추적 정보를 추출하고, 이로부터 P(Y)코드 신호에 대한 반송파 신호를 재생할 수 있다. 본 시뮬레이션에서는 GPS 시뮬레이터가 P(Y)코드 대신 P코드를 방송하고 있으므로, 추정 대상은 P코드가 된다. 그림 5는 GPS C/A코드 추적 정보를 이용하여 입력된 RF/IF 신호 y'_{ai}를 in-phase와 quadrature-phase로 구분한 샘플데이터를 도시한 결과이다. 그림에서 보인 바와 같이 단지 반송파를 제거해주는 것만으로도 기저대역 신호인 코드의 시퀀스를 직접 확인할 수 있다. In-phase 신호는 GPS C/A코드 반송파와 동기된 반송파 replica를 적용하였으므로 C/A코드 정보를 의미하고, quadratue-phase 신호는 90° 위상 천이된 반송파를 적용하였으므로 P코드 신호를 나타낸다.

그림 5의 반송파가 제거된 IF 샘플데이터를 저역통과 필터를 적용하고 +1과 −1로 부호를 설정하여 실제 코드 시퀀스를 추출할 수 있다. 그림 6은 GPS C/A코드에 대하여 IF 샘플데이터로부터 추정한 시퀀스와 GPS PRN 18번 코드의 시퀀스를 비교한 그림으로, 성공적으로 GPS C/A코드를 추출하였음을 확인할 수 있다. 그림 7은 그림 6의 IF 샘플데이터를 부호화 하여 코드를 추출한 결과이다.

그림 6의 추정 결과 성능을 검증하기 위하여 C/A 코드에 대해서는 GPS PRN 18번의 실제 C/A코드 시퀀스와 추정된 결과를 비교하고, P 코드에 대해서는 수집된 RF 데이터와 상관을

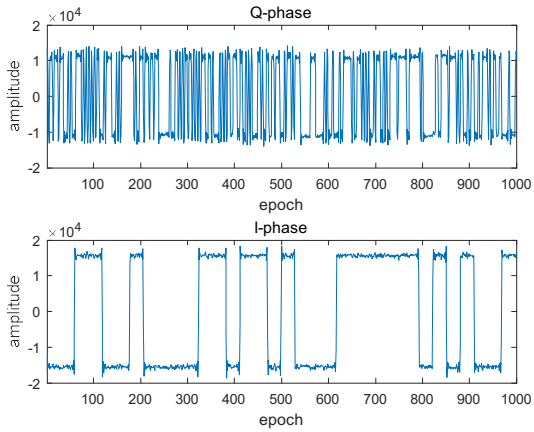

그림 5. GPS 시뮬레이터 신호의 quadrature-phase 신호 (위) 및 in-phase 신호 (아래) IF 샘플데이터

Fig. 5. Quadrature-phase (top) and in-phase (bottom) IF sample data of simulated GPS signal.

수행하여 상관이득이 발생하는지를 확인하였다.

그림 7은 추정된 C/A코드와 실제 코드를 비교한 그림으로 고이득 신호로부터 기저대역 신호를 성공적으로 복조하였음을 확인할 수 있다. 실제 코드와 추정된 코드의 부호가 서로 반대인 것은 항법메시지의 비트 반전에 의한 것으로 상관이득을 얻는 데는 영향을 미치지 않는다. 그림 8은 그림 6과 같이 추정된 P 코드를 이용하여 GPS 시뮬레이터의 IF 샘플데이터와 상관을 수행한 결과이다. 그림에서 보인바와 같이 성공적으로 상관이득을 얻을 수 있으므로, 고이득 신호로부터 P 코드가 성공적으로 추출되었음을 확인할 수 있다. 실제 GPS 위성은 P 코드와 이를 암호화하기 위한 W코드 변조가 적용된 P(Y)코드를 방송한다. W코드는 P코드와 동기되어 약 480 kHz의 비트율을 갖기 때문에 P코드의 부호가 반전되는 효과만을 일으킨다. 따라서

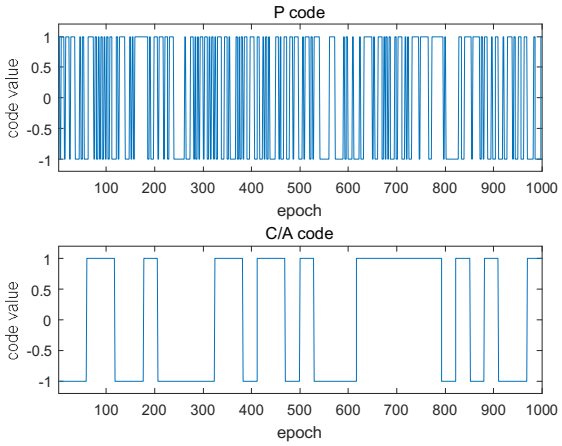

그림 6. GPS 시뮬레이터 신호로부터 추정된 P코드 (위) 및 C/A코드 (아래)

Fig. 6. Estimated GPS P code (top) and C/A code (bottom) from simulated GPS signal.

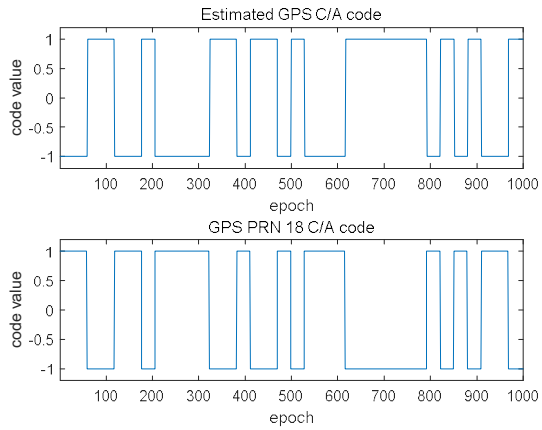

그림 7. GPS 시뮬레이터 신호로부터 추정된 GPS C/A코드 (위) 및 실제 GPS PRN 18번의 C/A코드 (아래)
Fig. 7. Estimated GPS C/A code (top) and true GPS C/A code of PRN 18 (bottom).

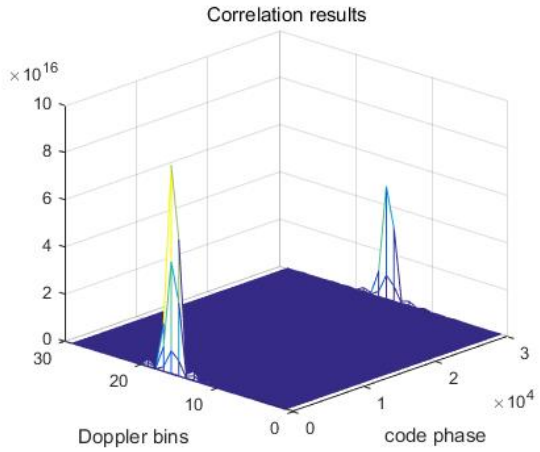

그림 8. GPS 시뮬레이터 신호 IF 데이터와 추정된 P 코드를 이용한 상관 결과
Fig. 8. Correlation results between IF sample data of GPS simulator and estimated P code.

본 논문에서 제안한 추출 방식은 P코드뿐만 아니라 P(Y)코드에도 동일하게 적용가능하다.

Ⅴ. 결 론

본 논문에서는 암호화 신호를 이용하는 기만 검출 기법을 제안하고 제안된 기법의 구현 가능성을 확인하기 위하여 GPS 시뮬레이터를 이용한 모의 결과를 제시하였다.

기존의 연구에서 제안된 두 개 수신기를 이용한 codeless correlation 방식의 기만 검출 기법은 GPS P(Y)코드에 대한 해독 정보가 없는 경우에도 P(Y)코드 신호를 기만 검출에 사용하는 방안을 제시하였다. 두 개 수신기에서 수집된 RF 데이터 내에 존재하는 P(Y)코드 신호를 상호 비교하여 상관이득이 존재하는 지를 검증하는 방식이다. 기존 방식은 RF 데이터를 이용하여 상관을 수행하기 때문에 처리를 위한 고성능 프로세서가 필요하고, 양방향 통신 및 고용량 데이터 전송이 요구된다. 또한 채널간의 간섭을 배제하기 위하여 지상의 인증시스템 설치에 대한 제약이 발생한다.

본 논문에서 제안하는 방법은 기만 검증의 기준이 되는 GPS P(Y)코드 신호를 고이득 지향성 안테나를 이용하여 채집하는 방법이다. 충분한 이득으로 채집된 RF 데이터에서 P(Y)코드를 추출하고 이를 사용자에게 방송하면, 사용자 수신기는 RF 데이터가 아닌 기저대역 코드신호를 그대로 입력 데이터와 상관할 수 있게 된다. 이러한 접근 방식의 장점은 데이터 처리량이 감소하여 사용자 수신기에서 상관 절차를 수행할 수 있게 되어 양방향 통신이 아닌 단방향 통신이 가능해 진다는 점이다. 또한 전송하는 데이터양도 RF 데이터 대신 기저대역 코드 시퀀스로 대체되어 전송량을 줄일 수 있는 장점이 있다. 채널간의 간섭에 의해 발생하는 지상 인증시스템의 설치 장소 제약 또한 극복할 수 있다.

제안된 방법의 가용성을 확인하기 위하여 GPS 시뮬레이터를 이용해서 고이득으로 채집된 GPS RF데이터를 모의하고, 소프트웨어 수신기에 제안된 알고리즘을 구현하였다. 시뮬레이션 결과 고이득 신호원으로부터 성공적으로 GPS C/A코드 및 P코드를 추출할 수 있었다. 향후 고이득 Dish 안테나를 이용하여 제안된 알고리즘을 실제 GPS 신호에 대하여 적용할 계획이다. 또한 GPS 기만 상태를 모의하여 실제 기만 환경에서 제안된 기법의 성능을 확인해 볼 예정이다.

참고 문헌

[1] E. D. Kaplan, *Understanding GPS : Principles and Applications,* 2nd ed. Norwood, MA: Artech House, 2005.

[2] F. Dovis, *GNSS Interference Threats and Countermeasures,* Norwood, MA: Artech House, 2015.

[3] S. Peterson, and P. Faramarzi, “Exclusive: Iran hijacked US drone, says Iranian engineer,” Csmonitor.com, Retrieved 15 December 2011.

[4] T. E. Humphreys, “Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing,” [Internet]. Available: http://homeland.house.gov/sites/homeland.house.gov /files/Testimony-Humphreys.pdf, July 2012.

[5] Anon. “Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System Technology Report,” John A. Volpe National Transportation Systems Center, 2001.

[6] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, *Global Positioning System Theory and Practice*, 5th ed.

New York, NY: Springer, 2001.

[7] S. Lo, D. E. Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, Sept/Oct 2009.

[8] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proceedings of the 24th ITM of The Institute of Navigation 2011,* Portland: OR, Sept. 2011.

[9] H. So, J. Jang, K. Lee, K. Song and J. Park, "GNSS spoofing detection scheme based on the combined use of a single authentic ranging signal and RAIM," in *Proceedings of 2015 International Association of Institutes of Navigation World Congress*, Prague: Czech, Oct. 2015.

[10] R. G. Brown, "A baseline GPS RAIM scheme and a note on the equivalence of three RAIM methods," *Navigation,* Vol. 39, No. 3, pp. 301-316, 1992.

[11] G. X. Gao, A. Chen, S. Lo, D. D. Lorenzon, T. Walter and P. Enge, "Compass-M1 broadcast codes in E2, E5b, and E6 frequency bands," *IEEE Journal of Selected Topics in Signal Processing*, Vol. 3, No. 4, Aug. 2009.

소 형 민 (Hyoungmin So)

2001년 2월 : 고려대학교 기계공학과 (공학사)
2003년 9월 : 서울대학교 기계항공공학부 (공학석사)
2009년 9월 : 서울대학교 기계항공공학부 (공학박사)
2011년 1월 ~ 현재 : 국방과학연구소 선임연구원
※관심분야 : 위성항법시스템, 광역보강시스템, 위성항법수신기