

GPS L1 C/A 기만 신호 검출 기법 설계

Design of GPS L1 C/A Spoofing Signal Detection Algorithm

임순* · 임덕원 · 허문범 · 남기욱

¹한국항공우주연구원 교통항법연구센터 위성항법팀

Soon Lim* · Deok-Won Lim · Moon-Beom Heo · Gi-Wook Nam

Satellite Navigation Team, CNS/ATM and Satellite Navigation Research Center, Korea Aerospace Research Institute, Daejeon 305-806, Korea

[요 약]

본 논문에서는 GPS 전파 간섭 신호의 한 종류인 기만 신호를 검출하는 기법을 제안한다. 본 논문에서 기만의 대상이 되는 신호에는 민간에 구조가 공개된 GPS L1 C/A 신호로 선정하였으며 GPS L1 C/A 기만 신호의 영향을 분석하고 이를 통해서 기만 신호 검출 기법을 제안한다. 제안하는 기만 신호 검출 기법은 상관함수가 왜곡된 정도로 기만 신호의 인가를 판단한다. 기만 신호의 판단 기준은 수신기 열잡음의 통계적 특성으로부터 정량적인 수치로 계산된 임계값을 이용하였다. 제안하는 기법을 검증하기 위한 시뮬레이션은 MATLAB을 기반으로 구성하였으며 기만 신호에 의한 상관함수 왜곡 및 코드 위상 오차를 확인하였다. 그리고 본 논문에서 제안하는 기만 신호 검출 기법을 적용하여 기만 신호의 검출 시뮬레이션을 수행하여 제안하는 기법에 의한 기만 신호 검출 성능을 확인하였다.

[Abstract]

In this paper, an effect on a GPS receiver by spoofing signal is analyzed and a GPS spoofing signal detection algorithm for GPS L1 C/A spoofing signal is proposed. A proposed detection algorithm monitors the correlation function distortion by the spoofing signal. If detected distortion is over a detection threshold, we can determine that the spoofing signal is received. The detection threshold is calculated from the statistical characteristics of a thermal noise. For verifying the suggested algorithm, a MATLAB-based simulation platform is implemented. This platform has functionalities to track GPS signal and measure the correlation values. By using this platform, the correlation function distortion by spoofing signal is observed. Also a performance of the algorithm proposed in this paper is applied and confirm the detection of a spoofing signal.

Key word : GPS spoofing, Spoofing detection, Correlation function distortion

<http://dx.doi.org/10.12673/jkoni.2014.18.1.7>



This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 21 October 2013; Revised 13 February 2014

Accepted 10 February 2014

*Corresponding Author; Soon Lim

Tel: +82-042-870-3971

E-mail: dlatns78@kari.re.kr

I. 서 론

GPS는 군용으로 개발되어 주요 산업분야 또는 개인용 내비게이션에까지 넓은 범위에서 활용되고 있다. GPS L1 신호는 신호의 주요 정보가 민간에 공개되어있어 손쉽게 신호를 수신하여 PVT(Position, Velocity, Time) 정보를 획득할 수 있다. 하지만 재밍, 신호 기만 등과 같은 간섭 신호에 의해 정상적인 항법이 방해받을 수 있다. 이 중에서도 기만 신호는 재밍과 달리 일반적인 위성 신호를 모사한 신호이므로 수신기에서 기만 여부를 판단하기 어렵다. 기만 신호는 GPS L1 신호와 같은 민간 공개 신호를 모사하고 여기에 거리 오차를 인가하거나 잘못된 항법 데이터를 제공하여 대상 수신기가 오차를 가지는 측위 결과를 얻게 한다. 실례로 2011년 12월 이란에서 미국의 무인 정찰기가 실종되는 사건이 발생했는데 기만 신호에 의한 무인기가 나포된 것이라 보도된 바 있다[1]. 또한 2012년 6월에 미국 텍사스 대학의 연구원들은 GPS 수신기가 탑재된 무인기에 기만 신호를 송신하여 무인기 통제를 시연함으로써 기만 신호의 위험성을 증명하였다[1]. 현재 미 FAA(Federal Aviation Administration)는 2015년 9월까지 민간 공역에 무인기의 진입 허가를 준비 중이므로[1] 만약 GPS 기만 신호에 대한 대비가 없다면 기만 신호에 의한 무인기 나포, 또는 무인기 항법 통제를 이용한 사고 발생으로 재산 및 인명 피해를 유발할 수 있다. 무인기뿐만 아니라 일반 여객기에도 영향을 미칠 수 있어 기만 신호에 대한 대책이 시급한 상황이다[1].

기존의 기만 신호 검출 기법 중 Parity 검출 기법, 수신된 신호의 통계적 특성을 이용한 기법은 연산량이 크다는 단점을 가지고 있다[2][3]. 본 논문에서는 기만 신호의 특성과 영향을 분석하고 이를 토대로 보다 효율적으로 기만 신호를 검출하기 위한 기법을 제안한다. 본 논문에서 제안하는 기법은 기만 신호에 의한 상관값 왜곡을 판단하는 방법을 사용하였으며 MATLAB 기반의 시뮬레이션을 통하여 기만 신호를 인가하였을 때에 대한 기만 신호 검출 성능을 검증하였다.

II. 기만 신호의 구조 및 기만 원리

2-1 기만 신호의 구조

기만 신호는 기만 대상이 되는 신호의 구조를 모사하는 신호로 GPS L1 C/A 신호와 같은 민간 신호를 대상으로 한다. 식 (1)은 임의의 시간 t 에 수신기에 인가된 GPS L1 C/A IF(Intermediate Frequency) 대역 신호이다[4].

$$s_d(t) = A_d C(t - \tau_d) D(t - \tau_d) \times \cos\{2\pi(f_{IF} + f_D(t)) + \phi_d(0)\} + n_d(t) \tag{1}$$

$$= A_d C(t - \tau_d) D(t - \tau_d) \times \cos\{\omega_{IF}(t) + \phi_d(0)\} + n_d(t)$$

$$= A_d C(t - \tau_d) D(t - \tau_d) \cos\{\phi_d(t)\} + n_d(t)$$

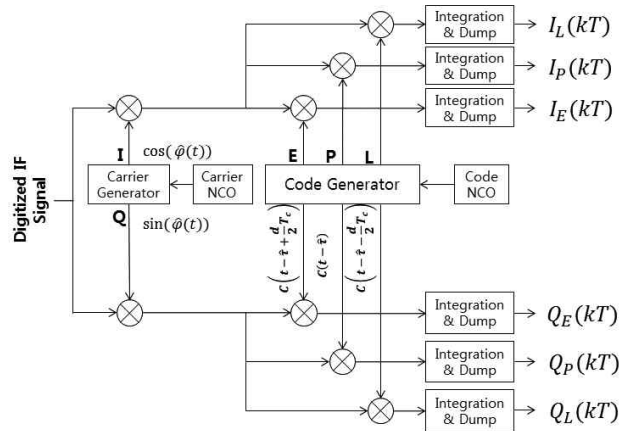


그림 1. 코드 추적 루프 구조
Fig 1. Code tracking loop structure

식 (1)에서 A_d 는 신호 전력 크기, $C(t)$ 는 C/A 코드, $D(t)$ 는 항법 데이터, f_{IF} 는 IF 대역으로 변환된 반송파, f_D 는 Doppler 주파수, $\phi_d(t)$ 는 반송파 초기 위상, $n_d(t)$ 는 수신기의 열잡음이다[4]. 식 (1)의 IF 신호는 그림 1의 상관기에 입력되고 상관기는 Inphase, Quadrature phase 두 채널에 대하여 상관값을 생성하는데 이 상관값은 식 (2), (3)과 같다[4].

$$I_{(Y)}(kT) = B \text{sinc}\left(\frac{\delta\omega_{IF}(kT)T}{2}\right) R\left(\frac{\delta\tau_d(kT)}{T_c} + \gamma_{(Y)}d\right) \times \cos\left(\frac{\delta\omega_{IF}(kT)T}{2} + \delta\phi_d(kT)\right) + n_I(kT) \tag{2}$$

$$Q_{(Y)}(kT) = B \text{sinc}\left(\frac{\delta\omega_{IF}(kT)T}{2}\right) R\left(\frac{\delta\tau_d(kT)}{T_c} + \gamma_{(Y)}d\right) \times \sin\left(\frac{\delta\omega_{IF}(kT)T}{2} + \delta\phi_d(kT)\right) + n_Q(kT) \tag{3}$$

식 (2), (3)에서 B 는 상관값의 크기, $\text{sinc}(x) = \sin(x)/x$, T 는 적분 주기, $R(x)$ 는 C/A 코드의 정규화된 자기상관 함수, d 는 Early, Late tap의 칩 간격이다. $n_I(kT)$ 와 $n_Q(kT)$ 는 각각 I, Q 채널에 대한 열잡음이다. $\delta\omega_{IF}(kT)$ 는 IF 대역으로 변환된 반송파 주파수 오차, $\delta\phi_{IF}(kT)$ 는 반송파 위상오차, $\delta\tau_d(kT)$ 는 C/A 코드 위상 오차이며 각각 식 (4) ~ (6)과 같이 정의하였다[4].

$$\delta\omega_{IF}(kT) = \sum_t^{T/T_s} [\hat{\omega}_{IF}(lT_s) - \omega_{IF}(lT_s)] \tag{4}$$

$$\delta\phi_d(kT) = \sum_t^{T/T_s} [\hat{\phi}(lT_s) - \phi_d(lT_s)] \tag{5}$$

$$\delta\tau_d(kT) = \sum_t^{T/T_s} [\hat{\tau}(lT_s) - \tau_d(lT_s)] \tag{6}$$

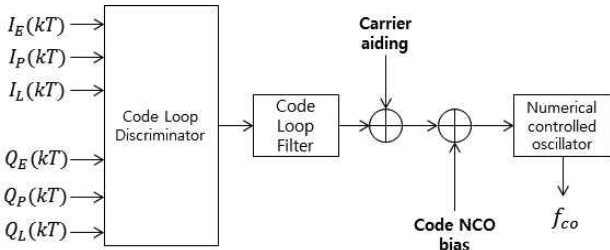


그림 2. 코드 추적 루프 구조
Fig 2. Code tracking loop structure

식 (2), (3)의 $\gamma_{(Y)}$ 는 위상 조절 계수이며 칩 간격 d 가 1 칩으로 가정하면 Early, Late, Prompt tap의 위상 조절 계수 $\gamma_{(Y)}$ 의 값은 식 (7)과 같다. 여기서 $Y \in \{E, P, L\}$ 이다[4].

$$\gamma_{(Y)} = \begin{cases} 0.5, & Y = E(\text{Early Tap}) \\ 0, & Y = P(\text{Prompt Tap}) \\ -0.5, & Y = L(\text{Late Tap}) \end{cases} \quad (7)$$

식 (2), (3)의 I, Q 채널의 상관값은 그림 2의 Discriminator로 입력된다. Discriminator는 입력된 I, Q 채널의 상관값으로부터 Early, Prompt, Late tap의 상관값 x_E, x_P, x_L 을 구한다. Early, Prompt, Late tap의 상관값은 식 (8)과 같이 계산된다[5].

$$\begin{aligned} x_E &= \sqrt{I_E^2 + Q_E^2} \\ x_P &= \sqrt{I_P^2 + Q_P^2} \\ x_L &= \sqrt{I_L^2 + Q_L^2} \end{aligned} \quad (8)$$

Discriminator는 식 (8)의 Early, Prompt, Late 상관값으로부터 수신된 C/A 코드와 수신기에서 생성한 Replica 코드의 위상차를 구한다. 본 논문에서 코드 위상차를 구하는 Discriminator 함수는 식 (9)를 이용하였다[5].

$$\frac{1}{2} \frac{x_E - x_L}{x_E + x_L} \quad (9)$$

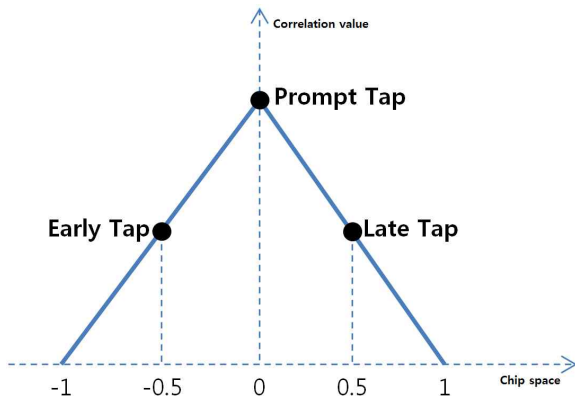


그림 3. C/A 코드의 상관함수
Fig 3. Correlation function of C/A code

식 (9)의 Discriminator 함수를 이용하여 GPS C/A 신호를 추적하면 GPS 상관기의 Early, Prompt, Late 상관값은 그림 3과 같이 분포한다. 그림 3에서 파란 선은 이상적인 형태의 C/A 코드의 자기 상관함수이다[5]. 기만 신호는 실제 위성 신호를 모사하여 그 구조가 동일한 신호이다. 식 (10)은 기만 신호를 수식으로 나타낸 것이다[2][4].

$$\begin{aligned} s_{spoof}(t) &= A_{spoof} C(t - \tau_{spoof}(t)) D(t - \tau_{spoof}(t)) \\ &\times \cos\{\phi_{spoof}(t)\} + n_{spoof}(t) \\ &= (1 + \alpha) A_d C(t - \tau_d - \Delta\tau(t)) D(t - \tau_d - \Delta\tau(t)) \\ &\times \cos\{\phi_{spoof}(t)\} + n_{spoof}(t) \end{aligned} \quad (10)$$

기만 신호는 실제 위성 신호보다 큰 전력을 가지며 수신기를 기만하기 위한 C/A 코드 위상 오차를 가진다. 식 (10)에서 α 는 실제 위성 신호와 기만 신호의 전력 차이이며 τ_{spoof} 는 코드 위상 오차이다. α 는 0보다 큰 값을 가진다. 기만 대상 수신기가 받는 신호는 위성 신호와 기만 신호의 합으로 표현되며 식 (11)과 같이 표현할 수 있다[2].

$$s_t(t) = s_d(t) + s_{spoof}(t) \quad (11)$$

2-2 기만 원리

기만 신호는 수신기가 기만 신호를 획득 및 추적하게 해야 하므로 실제 위성 신호보다 큰 신호 전력을 가진다. 따라서 식 (10)의 α 는 0보다 큰 값을 가지게 된다. 그림 4는 기만 신호의 기만 원리를 3단계로 보여준다[2].

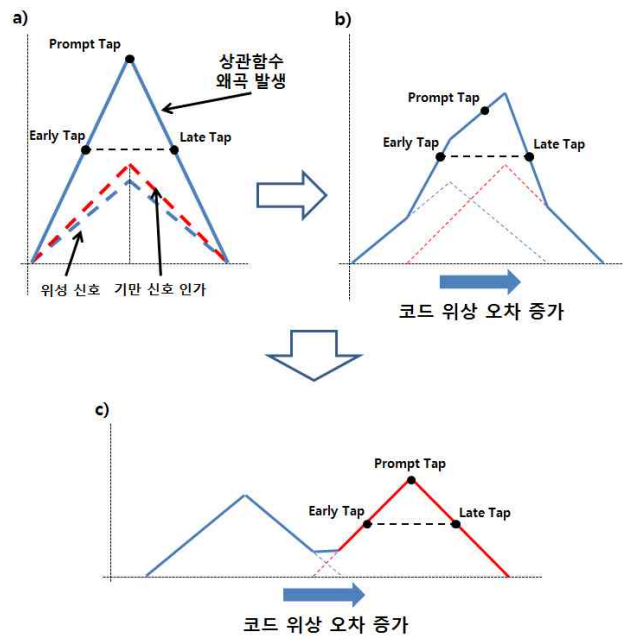


그림 4. 기만 신호의 기만 원리
Fig 4. Principle of Spoofing signal

파란 점선은 위성신호의 상관함수, 붉은 점선은 기만 신호의 상관함수이다. 그림 4의 b)는 기만 신호가 코드 위상 오차를 증가시키는 모습이다. 식 (10)에서 $\tau_{spoof}(t)$ 는 $\tau_d - \Delta\tau(t)$ 로 나타낼 수 있으며 $\Delta\tau(t)$ 는 기만 신호가 인가하는 코드 위상 오차이다. $\Delta\tau(t)$ 가 증가함에 따라 GPS 수신기는 그림 4의 c)와 같이 신호 전력이 더 큰 기만 신호를 추적하게 된다[2].

III. 기만 신호 검출 기법

3-1 상관함수 왜곡 검출

본 논문에서 제안하는 기만 신호 검출 기법은 그림 4에서와 같이 기만 신호에 의해 발생하는 상관함수 왜곡을 감지하여 기만 신호의 수신 여부를 판단한다. 그림 3의 이상적인 자기 상관함수에 열잡음이 없는 환경을 가정하면 식 (8)의 Early, Prompt, Late Tap의 상관값은 식 (12)의 관계를 만족한다[3].

$$x_E = x_L = \frac{x_P}{2} \tag{12}$$

본 논문의 기만 신호 검출 기법은 상관값의 변화량을 이용한다. 그림 4의 b)에서 Early, Late Tap의 상관값 변화에 비해 Prompt Tap의 값이 더 큰 폭으로 감소함을 보였다. 상관함수 왜곡 검출은 Early, Late Tap과 Prompt Tap의 차이를 이용하여 기만 신호에 의하여 상관함수가 왜곡되었다고 판단한다.

3-2 기만 신호 검출식

기만 신호 검출식은 식 (13), (14)와 같이 나타낸다. 식 (13)의 검출식은 식 (12)의 Early, Prompt tap의 상관값 관계식을 이용하여 하였으며 식 (14)는 Late, Prompt tap의 상관값 관계식을 이용하여 도출하였다.

$$\left| \frac{x_P}{2} - x_E \right| > V_{t.Spoof} \tag{13}$$

$$\left| \frac{x_P}{2} - x_L \right| > V_{t.Spoof} \tag{14}$$

식 (13), (14)에서 $V_{t.Spoof}$ 는 수신기의 열잡음의 통계적 특성으로부터 계산된 기만 신호 검출 임계값이다. 만약 수신기의 열잡음이 없는 이상적인 상관함수를 가정하면 식 (13)의 $|x_P/2 - x_E|$ 와 $|x_P/2 - x_L|$ 의 결과는 0이 된다. 여기에 기만 신호의 인가에 의한 상관함수 왜곡이 발생하면 $|x_P/2 - x_E|$ 와 $|x_P/2 - x_L|$ 의 결과는 0보다 큰 값이 된다. 본 논문에서 제안하는 기만 신호 검출 방식은 식 (13), (14)의 조건을 만족하는 경우 기만신호에 의한 상관함수 왜곡을 판단한다. 식 (13)의 상관값에 대한 검출식을 2차원 평면에 나타내면 그림 5와 같다.

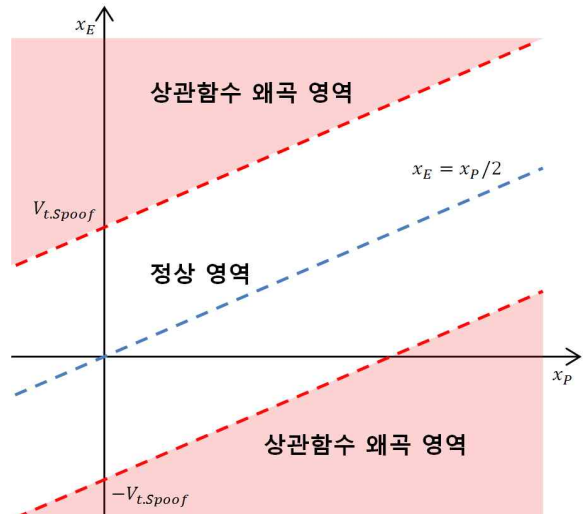


그림 5. 기만 신호 검출 영역(Early & Prompt Tap)
Fig 5. Region of spoofing detection(Early & Prompt Tap)

그림 5에서 붉은 점선은 $V_{t.Spoof}$ 를 표현한 것으로 두 점선 사이의 영역은 정상 영역, 그 외의 부분은 상관함수 왜곡 영역이다. 파란 점선은 $x_E = x_P/2$ 를 나타낸다.

본 논문에서는 기만 신호 검출 임계값을 구하기 위해 기만 신호 오검출 확률을 계산하였다. 식 (8)에서 구한 상관값 x_E, x_P, x_L 을 각각 Early, Prompt, Late Tap의 확률변수에 대한 값이라 하면 이 상관값들은 Rician 확률분포로 가진다[3]. Early, Prompt, Late Tap의 상관값에 대한 확률밀도함수를 Rician 확률밀도함수로 표현하면 식 (15), (16), (17)과 같다[5].

$$p_s(x_E) = \begin{cases} \frac{x_E}{\sigma_E^2} e^{-\left(\frac{x_E^2 + A_E^2}{2\sigma_E^2}\right)} I_0\left(\frac{x_E A_E}{\sigma_E^2}\right), & x_E \geq 0 \\ 0, & x_E < 0 \end{cases} \tag{15}$$

$$p_s(x_P) = \begin{cases} \frac{x_P}{\sigma_P^2} e^{-\left(\frac{x_P^2 + A_P^2}{2\sigma_P^2}\right)} I_0\left(\frac{x_P A_P}{\sigma_P^2}\right), & x_P \geq 0 \\ 0, & x_P < 0 \end{cases} \tag{16}$$

$$p_s(x_L) = \begin{cases} \frac{x_L}{\sigma_L^2} e^{-\left(\frac{x_L^2 + A_L^2}{2\sigma_L^2}\right)} I_0\left(\frac{x_L A_L}{\sigma_L^2}\right), & x_L \geq 0 \\ 0, & x_L < 0 \end{cases} \tag{17}$$

식 (15), (16), (17)에서 $A_E, A_L = B/2, A_P = B$ 이며, $\sigma_E^2, \sigma_P^2, \sigma_L^2$ 는 잡음의 분산이다. 식 (15), (16), (17)은 Rician K factor 값에 따라 간략화가 가능하다. 상관값 중 Prompt tap의 상관값에 대한 Rician K factor는 식 (18)과 같다[6].

$$K = \frac{A_P^2}{2\sigma_P^2} = C/N \tag{18}$$

식 (18)에서 Rician K factor는 C/N 과 같으며 이를 이용하여 C/N_0 를 구하면 식 (19)와 같이 구할 수 있다[5].

표 1. 기만 신호 검출 임계값

Table 1. Spoofing signal detection threshold

P_{FA}	$V_{t.Spoof}$
1%	2.88
0.1%	3.68
0.01%	4.35
0.001%	4.94
0.0001%	5.46

$$C/N_0 = C/N \cdot \frac{1}{T} = \frac{A_P^2}{2\sigma_P^2} \cdot \frac{1}{T} \quad (19)$$

Rician 확률밀도함수는 Rician K factor(또는 $C/N \gg 1$ 이면 Gaussian 분포로 간략화 할 수 있다[6]. 식 (19)에서 T 가 1ms라고 하면 Prompt Tap의 C/N_0 가 43dB-Hz 이상인 경우 Gaussian 분포로 간략화가 가능하다. 따라서 식 (15), (16), (17)을 Gaussian 확률 밀도함수로 간략화 하면 식(20), (21), (22)와 같다[6].

$$p_s(x_E) = \frac{1}{\sqrt{2\pi\sigma_E^2}} e^{-\frac{(x_E + m_E)^2}{2\sigma_E^2}} \quad (20)$$

$$p_s(x_P) = \frac{1}{\sqrt{2\pi\sigma_P^2}} e^{-\frac{(x_P + m_P)^2}{2\sigma_P^2}} \quad (21)$$

$$p_s(x_L) = \frac{1}{\sqrt{2\pi\sigma_L^2}} e^{-\frac{(x_L + m_L)^2}{2\sigma_L^2}} \quad (22)$$

여기서 m_E, m_P, m_L 과 $\sigma_E^2, \sigma_P^2, \sigma_L^2$ 는 Early, Prompt, Late Tap의 상관값의 평균과 잡음의 분산이며 본 논문에서 잡음의 분산은 1로 가정하였고 각각의 상관값의 평균은 $m_E = m_L = m_P/2$ 를 만족한다[7]. 여기서 검출식 (13), (14)를 $x_{d,E}, x_{d,L}$ 에 대한 식으로 변환하면 식 (23), (24)와 같다.

$$x_{d,E} = x_E - \frac{x_P}{2} \quad (23)$$

$$x_{d,L} = x_L - \frac{x_P}{2} \quad (24)$$

$x_{d,E}, x_{d,L}$ 는 검출식 (13), (14)에 대한 확률변수의 값이다. 본 논문에서는 검출식 (13), (14)의 검출식의 결과가 양의 값인 경우만을 가정하였다. 식 (23)과 (24)로부터 $x_{d,E}, x_{d,L}$ 의 평균인 $m_{d,E}, m_{d,L}$ 은 0이며 분산 $\sigma_{d,E}^2, \sigma_{d,L}^2$ 은 1.25를 만족한다[7].

본 논문에서는 식 (13), (14)를 만족해야 상관함수 왜곡을 판단하므로 기만 신호 오검출 확률의 확률 밀도 함수는 식 (25)와 같이 결합 Gaussian 확률밀도함수로 나타낸다.[7].

표 2. 시뮬레이션 환경 설정

Table 2. Simulation parameter setup

시뮬레이션 parameter	설정 값
총 시뮬레이션 시간	10s
위성 신호 세기	43dB-Hz
위성 번호	1
기만 신호 C/N_0	44.77dB-Hz
기만 신호 코드 위상 오차	0.1chip/s
기만 신호 인가 시간	1s
오검출 확률	0.0001%

$$f(x_{d,E}x_{d,L}) = \frac{1}{2\pi\sigma_{d,E}\sigma_{d,L}\sqrt{1-\rho^2}} \times \exp\left[\frac{-1}{2(1-\rho^2)}\left(\frac{(x_{d,E}-m_{d,E})^2}{\sigma_{d,E}^2} - \frac{2\rho(x_{d,E}-m_{d,E})(x_{d,L}-m_{d,L})}{\sigma_{d,E}\sigma_{d,L}} + \frac{(x_{d,L}-m_{d,L})^2}{\sigma_{d,L}^2}\right)\right] \quad (25)$$

(where $\rho = \frac{\sigma_{d,E} \cdot \sigma_{d,L}}{\sigma_{d,E}\sigma_{d,L}}$)

앞에서 가정한 $x_{d,E}, x_{d,L}$ 의 평균과 분산으로부터 상관 계수 ρ 를 계산하면 대략 0.2이다. 계산한 상관계수를 이용하여 식 (25)를 풀면 식 (26)과 같다[7].

$$f(x_{d,E}x_{d,L}) = \frac{1}{2\pi \times 1.25 \times \sqrt{1-0.2^2}} \times \exp\left[\frac{-1}{2(1-0.2^2)}\left(\frac{x_{d,E}^2}{1.25} - \frac{0.4x_{d,E}x_{d,L}}{1.25} + \frac{x_{d,L}^2}{1.25}\right)\right] \quad (26)$$

식 (26)으로부터 기만 신호 오검출 확률을 구하기 위한 식은 식 (27)과 같다. 식 (27)에서 v 는 $V_{t.Spoof}$ 를 나타낸다[7].

$$F(x_{d,E}x_{d,L}) = \int_v^\infty \int_v^\infty f(x_{d,E}x_{d,L}) dx_{d,E} dx_{d,L} \quad (27)$$

식 (27)로부터 기만 신호 오검출 확률에 따른 기만 신호 임계값은 표 1과 같다.

IV. 시뮬레이션 및 결과

4-1 MATLAB 기반 시뮬레이션 플랫폼

기만 신호의 영향 및 상관함수 왜곡 검출 기법의 성능을 평가하기 위한 시뮬레이션 플랫폼은 MATLAB을 기반으로 구성하였다[8]. 시뮬레이션은 GPS L1 C/A 신호 단일 채널을 생성하고 이 신호에 대한 기만 신호를 생성하였다. 시뮬레이션 플랫폼은 신호 생성 및 추적부로 구성되며 기만 신호의 인가 여부에 대하여 수행하였다. 수행한 시뮬레이션의 환경은 표 2와 같다. 총 시뮬레이션 시간은 10초, 위성 신호의 세기는 43dB-Hz, 위성의 PRN 번호는 1번을 선택하였다.

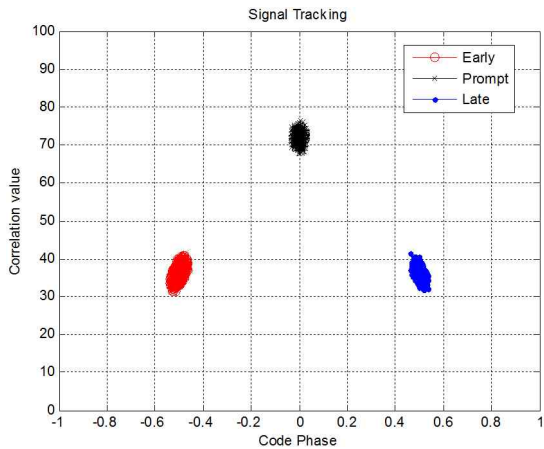


그림 6. 상관값의 코드 위상 변화
Fig 6. Code phase change of correlation value

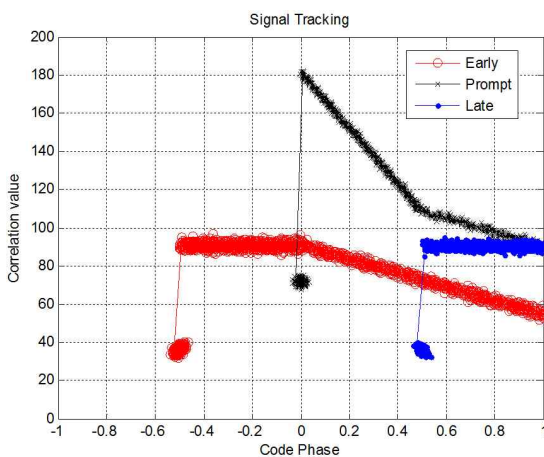


그림 7. 기만 신호에 의한 상관값의 코드 위상 변화
Fig 7. Code phase change of correlation value (with spoofing signal)

기만 신호는 생성한 위성신호와 동일한 PRN 번호인 1번으로 생성하였으며 신호의 세기는 위성신호의 1.5배인 44.77dB-Hz로 설정하였다. 기만 신호는 시뮬레이션이 시작하고 1초 이후에 인가하도록 하였으며 기만 신호가 인가하는 코드 위상 오차는 0.1chip/s로 설정하였다. 기만 신호 오검출 확률은 0.0001%로 설정하였으므로 기만 신호 검출 임계값은 약 5.46이다.

4-2 시뮬레이션 결과

기만 신호가 없는 경우 Early, Prompt, Late 상관값은 그림 6과 같다. 그림 7에서 기만 신호가 인가된 직후 코드 위상에 의한 상관 함수의 왜곡을 확인하였다. 그림 8, 9는 본 논문에서 제시하는 기만 신호 검출 기법을 적용하고 기만 신호를 검출한 시점에서의 상관값을 붉은 X로 표시한 그림이다. 그림 8은 Early Tap과 Prompt Tap, 그림 9는 Late Tap과 Prompt Tap을 나타낸다. 그림 8, 9에서 붉은 X로 표시된 상관값이 Early, Late Tap의 상관값 모두 기만 신호 검출 임계값을 초과한 경우이다.

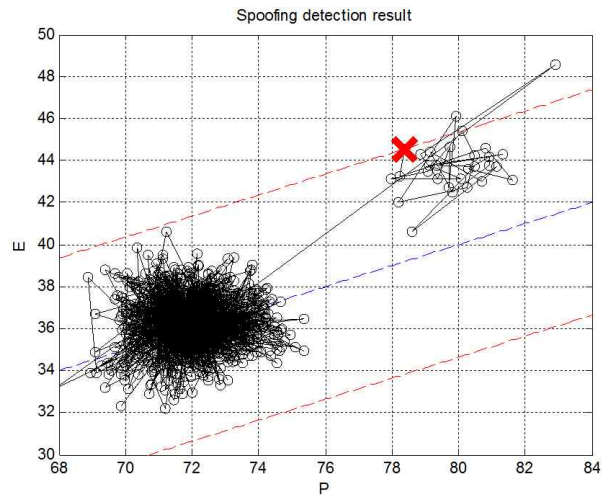


그림 8. 기만 신호 검출 결과(Early tap)
Fig 8. Spoofing detection result(Early tap)

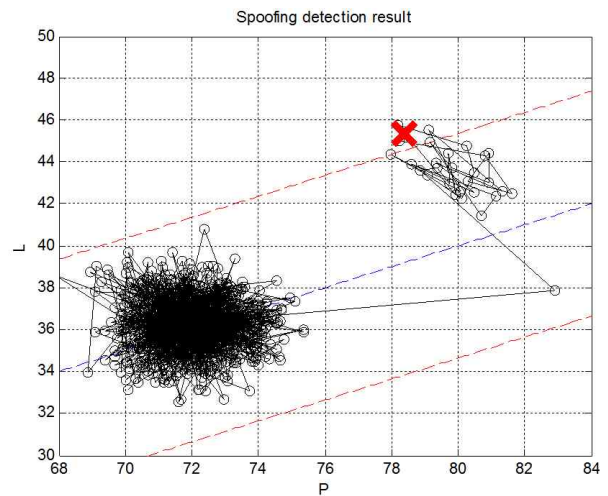


그림 9. 기만 신호 검출 결과 (Late tap)
Fig 9. Spoofing detection result(Late tap)

V. 결 론

본 논문에서는 기만 신호의 인가로 인한 상관함수 왜곡을 감지하고 이 왜곡을 통해 기만 신호의 인가를 판단하는 알고리즘을 제안하였다. 그리고 MATLAB을 통한 알고리즘의 검증을 수행하였다. 본 논문에서 소개하는 기만 신호 검출 기법은 이상적인 상태에서 수신기의 열잡음만을 가정한 환경에서 GPS L1 C/A 신호를 생성하고 이에 대한 기만 신호의 영향 분석 및 검출을 완료하였다.

추후의 연구 과제로 이상적인 환경이 아닌 실제 환경에 가까운 시뮬레이션 환경을 구축하여 제안하는 알고리즘의 성능을 평가할 예정이다. 또한 단순히 기만 신호의 인가를 검출하는 것에서 그치지 않고 기만 신호의 영향을 감쇄하는 검출 및 대응 기법에 대한 연구를 수행할 예정이다.

감사의 글

본 연구는 기초기술연구회의 “재난예방 및 국민안전제고를 위한 위성기반 위치추적기술 연구” 과제의 일환으로 수행되었으며 지원에 감사드립니다.

참고문헌

- [1] Inside GNSS, UAVs Vulnerable to Civil GPS Spoofing [Internet]. Available: <http://insidegnss.com/node/3131>
- [2] H. Wen et al, “Countermeasures for GPS signal spoofing,” *Proceedings of ION GNSS 2005*, pp.1285-1290, Sep, 2005.
- [3] A. Jafarnia-Jahromi et al, “Detection and Mitigation of Spoofing Attacks on a Vector-Based Tracking GPS Receiver,” *Proceedings of ION ITM 2012*, pp.790-800, Jan, 2012.
- [4] D. Lim et al, “A Model-Based Multipath Estimation Technique for GPS Receiver,” *Journal of Institute of Control, Robotics and Systems*, vol.18, no.4, pp.391-399, 2012.
- [5] E. D. Kaplan et al, *Understanding GPS*, second edition, Artech House, 2006.
- [6] G. D. Durgin, *Space-Time Wireless Channels*, Prentice Hall, 2002.
- [7] R. E. Ziemer et al, *Principles of Communications, 6th Edition*, John Wiley & Sons, 2009.
- [8] S. Lim et al, “Design of Software-based GPS Spoofing Signal Generator,” *Proceedings of ICS08*, pp.63-64, Apr, 2008.



임 순 (Soon Lim)

2007년 2월 : 충남대학교 전기정보통신공학부 (공학사)
 2009년 2월 : 충남대학교 전자전파정보통신공학과 대학원 (공학석사)
 2009년 11월 ~ 2013년 1월 : 한국천문연구원 (연구보조원)
 2013년 1월 ~ 현재 : 한국항공우주연구원 (연구원)
 ※ 관심분야 : GNSS, Software simulator, Anti-spoofing



임 덕 원 (Kil-Dong Hong)

2004년 2월 : 충남대학교 전자공학과(공학사)
 2011년 2월 : 충남대학교 전자공학과(공학박사)
 2011년 3월 ~ 현재 : 한국항공우주연구원 선임연구원
 ※ 관심분야 : GNSS 수신기 설계, Anti-jamming



허 문 범 (Moon Beom Heo)

1992년 2월 : 경희대학교 기계공학과(공학사)
 1997년 12월 : Illinois Institute of Technology 항공기계공학과(공학석사)
 2004년 12월 : Illinois Institute of Technology 항공기계공학과(공학박사)
 2005년 10월 ~ 현재 : 항공우주연구원 선임연구원
 ※ 관심분야 : GNSS, 위성항법, 항행시스템 등



남 기 옥 (Ki-Wook Nam)

1983년 2월 : 한국항공대학교 항공운항학과(공학사)
 1988년 2월 : 한국항공대학교 항공운항학과(공학석사)
 1996년 6월 : Cranfield Univ. 항공공학과(공학박사)
 1988년 7월 ~ 1989년 7월 : 한국과학기술연구원 연구원
 1989년 8월 ~ 1992년 7월 : 한국항공우주연구원 선임연구원
 1996년 12월 ~ 현재 : 한국항공우주연구원 책임연구원
 ※ 관심분야 : GNSS, 위성항법, 항행시스템 등