JPNT 10(3), 169-177 (2021)
https://doi.org/10.11003/JPNT.2021.10.3.169

JPNT Journal of Positioning, Navigation, and Timing

A Novel GNSS Spoofing Detection Technique with Array Antenna-Based Multi-PRN Diversity

Young-Seok Lee, Jeong Seon Yeom, Jae Hee Noh, Sang Jeong Lee, Bang Chul Jung†

Department of Electronics Engineering, Chungnam National University, Daejeon 34140, Korea

ABSTRACT

In this paper, we propose a novel global navigation satellite system (GNSS) spoofing detection technique through an array antenna-based direction of arrival (DoA) estimation of satellite and spoofer. Specifically, we consider a sophisticated GNSS spoofing attack scenario where the spoofer can accurately mimic the multiple pseudo-random number (PRN) signals since the spoofer has its own GNSS receiver and knows the location of the target receiver in advance. The target GNSS receiver precisely estimates the DoA of all PRN signals using compressed sensing-based orthogonal matching pursuit (OMP) even with a small number of samples, and it performs spoofing detection from the DoA estimation results of all PRN signals. In addition, considering the initial situation of a sophisticated spoofing attack scenario, we designed the algorithm to have high spoofing detection performance regardless of the relative spoofing signal power. Therefore, we do not consider the assumption in which the power of the spoofing signal is about 3 dB greater than that of the authentic signal. Then, we introduce design parameters to get high true detection probability and low false alarm probability in tandem by considering the condition for the presence of signal sources and the proximity of the DoA between authentic signals. Through computer simulations, we compare the DoA estimation performance between the conventional signal direction estimation method and the OMP algorithm in few samples. Finally, we show in the sophisticated spoofing attack scenario that the proposed spoofing detection technique using OMP-based estimated DoA of all PRN signals outperforms the conventional spoofing detection scheme in terms of true detection and false alarm probability.

Keywords: GNSS anti-spoofing, GNSS spoofing detection, array processing, compressed sensing

1. INTRODUCTION

최근 군수 및 민간 산업분야에서 무인항공기, 임무 수행용 원격로봇 그리고 군집 드론 (drone swarm) 등의 사용으로 인해 위성항법시스템(global navigation satellite system: GNSS)의 활용이 급격히 증가하고 있으며 특히, 자율주행자동차와 같은 사용자의 위치 정보가 중요한 민간 응용 분야의 경우에 기존보다 더 정확하고 신뢰성 있는 사용자 위치 정보가 요구된다. 그러나, GNSS 수신기는 실내 또는 도심에서의 사용에 제약이 있고 고의적 간섭 공격인 재밍(jamming) 공격과 기만(spoofing) 공격에 취약하다는 단점이 있다 (Humphreys et al. 2008). 특히, 기만 공격의 경우 기만신호는 재밍 신호와는 달리 실제 위성신호와 동일한 구조를 가지면서 비슷한 전력으로 수신되기 때문에 GNSS 수신기가 기만 공격 자체를 인지하기 어렵다. GNSS 수신기가 기만신호를 실제 위성신호로 착각하여 부정확한 위치, 속도, 시간 정보를 수신할 경우 수신기의 항법 정확도가 크게 감소하게 되고 이는 상황에 따라 큰 재산 및 인명 피해가 발생할 수 있다. 이에 따라 국내외에서는 항기만(anti-spoofing) 기술 개발의 필요성이 크게 대두되고 있으며 관련 연구가 활발히 진행중에 있다 (Broumandan et al. 2016).

GNSS 수신기의 항기만 기술은 단일 안테나와 배열 안테나 기반 기술 그리고 상관 전/후 기술로 구분할 수 있다. 단일 안테나 기반의 항기만 기술은 신호 전력 모니터링 기법 (Wesson et al.

Received Aug 14, 2021 **Revised** Aug 22, 2021 **Accepted** Aug 23, 2021
†**Corresponding Author**
E-mail: bcjung@cnu.ac.kr
Tel: +82-42-821-6580 Fax: +82-42-823-5436
Young-Seok Lee https://orcid.org/0000-0002-8552-1731
Jeong Seon Yeom https://orcid.org/0000-0003-0480-034X
Jae Hee Noh https://orcid.org/0000-0002-6314-738X
Sang Jeong Lee https://orcid.org/0000-0002-9400-5157
Bang Chul Jung https://orcid.org/0000-0002-4485-9592

2013)과 수신기의 이동성으로 인해 발생하는 도플러 주파수 차이를 비교하여 기만 공격에 대응하는 연구가 진행되었다 (Nielsen et al. 2010, Ziółkowski & Kelner 2020). 그러나, 기만기가 자체 GNSS 수신기를 내장하고 있고 타겟 수신기의 위치 정보를 실시간으로 획득하여 실제 위성신호의 신호 전력, 도플러 주파수 및 코드 칩 지연 정보와 같은 주요 신호 파라미터를 보다 정밀하게 모사하는 정교한 기만 공격 환경에서 이러한 단일 안테나 기반의 항기만 기술로는 기만 신호를 탐지할 수 없다. 또한, Huang et al. (2016)에서는 관성 측정 장비(inertial measurement units: IMU) 센서나 비전(vision) 센서와 같은 부가적인 장비를 도입하여 기만 공격에 대응하는 기술이 제안되었고, Guo et al. (2019)에서는 다중 상관기(multi-correlator)를 이용하여 정교한 기만 공격을 탐지하는 기법을 제안하였다. 그러나, 이러한 기술들은 GNSS 수신기에 추가적인 비용이 발생할 뿐만 아니라 무게나 크기 등이 증가하여 실제 운용하는데 제약이 발생할 수 있다.

배열 안테나 기반의 항기만 기법은 신호의 공간적 특성을 활용할 수 있어 정교한 기만 공격 시나리오에서도 우수한 기만 탐지 및 감쇄 성능을 갖는다. Zhang et al. (2019)에서는 global positioning system (GPS) PRN 신호 코드의 자기 상관(autocorrelation) 함수 특성인 순환정상성 (cyclostationarity)을 활용하였다. 구체적으로, 해당 기법은 임의의 PRN 신호와 한 주기 뒤 신호에 대해 상관한 순환 상관 함수(cyclic correlation function: CAF)를 연산한 후 CAF의 최대 고유값 (eigenvalue) 분포를 통한 상관 전 기만 탐지 기법이 제안되었다. 그러나, 이러한 기법은 기만신호 전력이 위성신호의 전력보다 3 dB 이상 더 클 때만 동작이 가능하며, 상관 전 기법은 잡음 수준보다 낮은 전력 레벨의 위성 PRN 신호를 다루기 때문에 배열 안테나의 공간적 특성을 이용하는데 한계가 있다. 배열 안테나를 통해 신호 입사 방향(direction of arrival: DoA)을 추정하여 공간적 특성을 활용한 기만 탐지 기법들도 제안되었다. Hu et al. (2018) 과 Zhang et al. (2019)에서는 배열 안테나를 활용하여 신호의 DoA를 추정해 기만신호를 분류하는 기술을 제안하였다. 일반적으로 기만신호의 DoA를 정밀하게 추정하기 위한 기술에는 다중 신호 분류 알고리즘(multiple signal classification: MUSIC)과 파라미터 기반의 DoA 추정 기법인 estimation of signal parameter using rotational invariance techniques (ESPRIT)이 사용되었다 (Meurer et al. 2012, Bao et al. 2017). 그러나, MUSIC 알고리즘이나 ESPRIT 기법을 적용하여 기만신호를 추정할 때 일반적으로 기만신호의 전력이 상대적으로 실제 위성신호보다 3 dB 정도 크다고 가정하였으며, 수신되는 모든 신호의 방향을 정밀하게 추정하기 위해서는 다수의 샘플을 통한 공분산 행렬을 연산해야 한다. 하지만, 공분산 연산은 상관 후 신호에 대해 실시간으로 기만 공격을 대응하는데 다소 무리가 있으며 연산을 위한 다수의 신호 샘플을 저장하기 위한 메모리나 버퍼가 추가로 필요할 수 있다.

따라서, 적은 수의 신호 샘플만을 이용하여 수신 신호의 DoA를 정밀하게 추정할 수 있는 방법인 다중경로 감쇄 기술(multi-path mitigation technology: MMT)을 적용한 항기만 알고리즘이 제안되었다 (Magiera 2019). 각 PRN 신호의 다중 경로 신호를 기만신호로 모델링하여 각 PRN 별 모든 안테나 원소에 대한 조향벡터(steering vector) 파라미터를 추정하고 조향벡터들 간의 거리 차이로부터 기만 신호를 탐지한다. 하지만 파라미터 추정에 있어서 2차원 최대 우도 추정 (maximum likelihood estimation) 기법이 사용되기 때문에 매우 높은 복잡도를 갖으며 조향벡터들 간의 거리 차이에 대한 임계치가 특정 지역에서만 유효하다는 단점이 있다. 압축 센싱 기반 DoA 추정 기법 또한 적은 수의 샘플만을 이용하여 기만신호를 탐지하는 기술로 제안되었다 (Yang et al. 2019). 그러나, 해당 기법은 DoA 추정을 위한 최적화 과정에서 높은 복잡도와 연산량을 갖게 되며 이는 매우 느린 연산 속도로 인해 실시간으로 정교한 기만 공격에 대응하기에 무리가 있다.

본 논문에서는 고정된 위치에서 다수의 PRN을 모사하는 단일 기만기와 배열 안테나를 갖는 GNSS 수신기가 존재할 때 각 PRN 별 상관 후 신호에 대한 DoA 추정을 통해 수행되는 기만 탐지 알고리즘을 제안한다. 본 논문에서는 정교한 기만 공격 시나리오를 고려하며 이때, 기만신호 전력이 위성신호 전력보다 비슷하거나 심지어 더 작을 때에도 우수한 탐지 성능을 보이도록 알고리즘을 설계하였다. 구체적으로, 다수의 PRN으로부터 1 ms 동안 수신되는 단일 샘플 신호에 대해 압축 센싱 기반의 휴리스틱 알고리즘인 직교 매칭 퍼슛(orthogonal matching pursuit: OMP) 기법을 적용한다 (Shen et al. 2016). 이후, 추정된 DoA를 모두 이용하여 각 PRN에서 추정된 DoA 사이 차를 연산하고 이를 기반으로 다수의 PRN 위성에 대해 한 방향으로만 입사되는 신호를 검출하여 기만신호를 탐지한다. 또한, 본 논문에서는 다중 샘플 신호에 대해서 동시 직교 매칭 퍼슛 (simultaneous OMP: SOMP) 기법을 통해 확장 적용하였으며 종래의 MUSIC 기법 간의 DoA 추정 성능을 비교하였다. 이후, 각 PRN 신호에 대해 신호원 개수를 추정할 수 있는 임계 조건과 위성간 DoA가 유사한 상황을 고려한 기만 탐지 조건을 추가하여 높은 기만 탐지 확률을 보이면서 낮은 거짓 경보 확률을 갖는 것을 MATLAB 모의 실험을 통해 검증하였다.

본 논문은 다음과 같이 구성된다. 2장에서는 본 논문에서 고려하고 있는 기만 시나리오와 기만신호와 다수의 위성 PRN 신호를 수신하는 배열안테나 GNSS 수신기의 시스템 모델을 제시하고, 3장에서는 제안하는 압축 센싱 기반 위성 및 기만신호 방향 추정 기법과 추정된 DoA를 이용한 기만탐지 알고리즘을 설명한다. 4장에서는 모의 실험을 통해 제안하는 기법의 기만 신호 DoA 추정 성능 및 기만 탐지 성능을 확인하고, 5장에서 결론을 도출하였다.

2. 시스템 모델

본 논문에서는 Fig. 1과 같이 N개의 균일한 선형 배열(uniform linear array: ULA) 안테나를 갖는 고정형 GNSS 수신기가 M개의 PRN 신호를 수신 및 추적하고 있고, 자체 GNSS 수신기와 단일 안테나를 갖는 단일 기만기가 L ($L \leq M$)개의 PRN을 모사하고 있는 환경을 고려한다. 또한, 기만기는 타겟 GNSS 수신기의 위치 정보를 사전에 알고 있으며 해당 위치 정보와 자체 GNSS 수신 신호를 이용하여 Fig. 2와 같이 실제 위성신호와 도플러 주파수 및 코드 칩 지연 등의 주요 파라미터를 정밀하게 모사할 수 있다고 가정하였다. 구체적으로 t=1부터 t=3까지 기만기는 타겟 GNSS 수신기가 기만 공격을 인지하지 못하도록 실제 위성신호보다 낮은 전력 수준으로 시간 지연 동기를 맞추고 t=4부

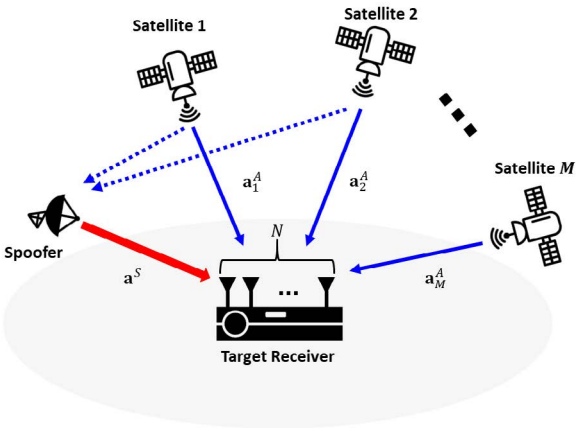

Fig. 1. System model where a target receiver with array antennas and a spoofer imitating multi-PRN signals exist.

터 점차 전력을 키워 타겟 GNSS 수신기의 추적 루프를 제어한다 (Ioannides et al. 2016, Psiaki & Humphreys 2016). 따라서, 본 논문에서는 위와 같은 기만 공격 시나리오를 고려하여 GNSS 수신기가 초기에 대응할 수 있도록 위성신호 대비 기만신호의 전력 크기는 더 작거나 비슷하다고 가정하였고 기만 탐지가 최대한 빨리 동작할 수 있도록 적은 수의 샘플에 대해 기만 탐지를 수행한다. 또한, 본 논문에서 기만기에 의해 모사된 PRN 신호는 실제 위성신호와 도플러 주파수는 완벽하게 동기를 맞추었고 코드 칩 지연은 0.5 chip 이내의 오차를 갖는다고 가정하였다 (Psiaki & Humphreys 2016, Magiera 2019, Noh et al. 2021).

이때, t째 시간에 타겟 GNSS 수신기의 배열 안테나로 수신되는 신호 $\mathbf{r}(t)(\in\mathbf{C}^N)$는 식 (1)과 같이 표현할 수 있다.

$$\mathbf{r}(t)=\sum_{m=1}^{M}\mathbf{a}_m^A s_m^A(t)+\mathbf{a}^S\sum_{l=1}^{L}s_l^S(t)+\mathbf{n}(t) \tag{1}$$

여기서, 위 첨자 A와 S는 각각 위성과 기만신호를 의미한다. $\mathbf{a}(\in\mathbf{C}^N)=[a_1,a_2,\cdots,a_N]^T$는 신호 조향벡터를 의미하고 각 벡터의 $i\in\{1,2,\cdots,N\}$ 째 성분은 식 (2)와 같다.

$$a_i=e^{-j\frac{2\pi}{\lambda}(i-1)d\sin\theta} \tag{2}$$

이때, λ,d,θ는 각각 신호의 파장, 안테나 이격거리, 신호의 입사각을 의미하며 본 논문에서는 $d=\lambda/2$로 가정하였다. $\mathbf{n}\in\mathbf{C}^N$은 수신기에서 발생하는 부가 열잡음 벡터를 의미하며 본 논문에서 모든 열잡음은 $\mathcal{CN}(0,\sigma_n^2\cdot\mathbf{I}_N)$의 분포를 갖는다고 가정한다. 또한, m째 PRN에서의 위성 신호 모델 $s_m^A(t)$와 l째 PRN에서의 기만 신호 모델 $s_l^S(t)$는 식 (3-4)와 같이 표현할 수 있다.

$$s_m^A(t)=\sqrt{P_m^A}D_m^A(t-\tau_m^A)C_m^A(t-\tau_m^A)e^{j2\pi(f+f_m^A)t} \tag{3}$$

$$s_l^S(t)=\sqrt{P_l^S}D_l^S(t-\tau_l^S)C_l^S(t-\tau_l^S)e^{j2\pi(f+f_l^S)t} \tag{4}$$

여기서, P_m^A와 P_l^S는 각각 m째 실제 위성 PRN 신호의 수신 전력과 l째 기만 PRN 신호의 수신 전력을 의미하며 D_m^A와 D_l^S는 각각 위성과 기만신호의 항법 비트 정보, C_m^A와 C_l^S는 위성과 기만신호의

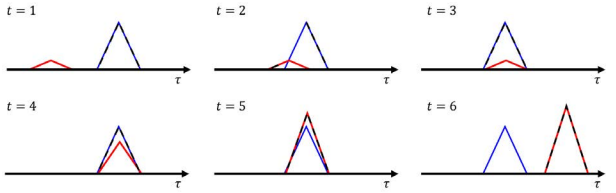

Fig. 2. Sophisticated spoofing attack scenario.

PRN 코드를 의미한다. f는 신호의 반송파 주파수를 나타내며 f_m^A와 f_l^S는 각각 위성과 기만신호의 도플러 주파수를 의미하고 τ_m^A와 τ_l^S는 위성과 기만 PRN 신호의 코드 지연을 의미한다.

본 논문에서는 모든 항법 비트 정보 D를 1로 가정하였고 타겟 GNSS 수신기는 사전에 M개의 실제 위성 PRN 신호를 추적하고 있다고 가정하였다. 또한, 본 논문에서는 각 신호원 방향을 정밀하게 추정하기 위해 상관기(correlator) 이후 역확산(despreading)된 각 PRN 별 신호에 대해 DoA 추정 알고리즘을 적용한다. 따라서, 1 ms 동안 N_s개의 상관 전 샘플에 대해 반송파 주파수를 보상한 역확산 신호 $\mathbf{y}\in\mathbf{C}^N$는 각 PRN에 대해 식 (5)와 같이 두 가지 가설(hypothesis)로 표현될 수 있다.

$$\mathbf{y}=\begin{cases}x^A\mathbf{a}^A+\tilde{\mathbf{n}}, & \mathcal{H}_0\\ x^A\mathbf{a}^A+x^S\mathbf{a}^S+\tilde{\mathbf{n}}, & \mathcal{H}_1\end{cases} \tag{5}$$

여기서, $\mathcal{H}_0$ 가설은 기만신호가 존재하지 않는 PRN에 대한 역확산 신호 모델로 실제 위성 PRN 신호와 잡음만이 존재하는 신호 모델을 의미하며 이때, 다중경로 신호나 기타 간섭은 무시할 만하거나 없다고 가정하였다. $\mathcal{H}_1$ 가설은 기만신호가 존재하는 PRN에 대한 역확산 신호 모델을 의미하며 $\mathcal{H}_0$의 신호모델에서 기만신호가 포함된 신호 모델을 나타낸다. 이때, x^A와 x^S는 각각 위성과 기만 PRN 신호 $s^A(t)$와 $s^S(t)$에 대한 역확산 신호를 의미하며 $\tilde{\mathbf{n}}\in C^N$는 역확산 코드가 곱해진 잡음 벡터를 의미하고 동일한 $\mathcal{CN}(0,\sigma_n^2\cdot\mathbf{I}_N)$의 분포를 갖는다.

3. 제안하는 압축 센싱 기반 DOA 추정을 통한 기만 탐지 기법

3.1 압축 센싱 기반 위성 및 기만신호 DoA 추정 기법

본 장에서는 각 위성 PRN에서 타겟 GNSS 수신기로 입사되는 신호에 대해 신호원 유무와 방향을 탐지하기 위한 DoA 추정 알고리즘을 설계한다. 본 논문에서는 정교한 기만 시나리오를 고려하여 적은 샘플로도 DoA를 정밀하게 추정하여 기만신호를 탐지하기 위해 압축 센싱 기반의 DoA 추정 알고리즘을 적용한다. 각 PRN 신호 채널에서 타겟 GNSS 수신기에 가시선(line-of-sight)으로 입사되는 신호의 개수는 $\mathcal{H}_0$ 가설을 고려할 때 하나이고, $\mathcal{H}_1$ 가설을 고려할 때 두 개이므로 각 PRN 신호 채널에서 존재할 수 있는 신호원의 수는 최대 두 개이다. 따라서, 수신기에 도달할 수 있는 입사각을 전체 P개로 분할할 때, 식 (5)는 식 (6)과 같이 표현할 수 있다.

$$\mathbf{y} = \mathbf{A}\mathbf{x} + \tilde{\mathbf{n}} = [\mathbf{a}_1\ \mathbf{a}_2\ \cdots \mathbf{a}_P]\begin{bmatrix}0\\ \vdots\\ x\\ \vdots\\ 0\end{bmatrix} + \tilde{\mathbf{n}} \quad (6)$$

여기서, $\mathbf{A}\in\mathbb{C}^{N\times P}$는 P개의 신호 방향에 대한 배열안테나의 조향벡터를 포함하는 센싱 행렬을 의미하며 각 열은 $p\in\{1,2,\cdots,P\}$째 방향에 대한 조향벡터를 의미한다. 또한, $\mathbf{x}\in\mathbb{C}^P$는 입사 방향에 대한 수신 신호 벡터이며 신호 벡터 $\mathbf{x}$는 $\mathcal{H}_0$에 대해서 하나의 원소만 0이 아닌 값을 가지고, $\mathcal{H}_1$에 대해서 두 개의 원소만 0이 아닌 값을 갖는 희소 벡터이다.

본 논문에서는 희소 벡터의 $L1$-norm을 최소화하는 복잡도가 높고 연산 속도가 매우 느린 기존의 최적화 과정을 수행하는 압축 센싱 기반 방향 추정 알고리즘이 아닌 효율적으로 신호 방향을 추정할 수 있는 압축 센싱 기반의 휴리스틱 알고리즘인 OMP 기법을 통해 DoA를 추정한다. OMP 알고리즘은 k째 반복에서 이전 반복 단일 샘플 신호 $\mathbf{y}_{(k-1)}$에 $\mathbf{A}$의 각 열인 조향벡터를 내적하고 이 때 내적값 중 최대값을 가지는 방향 p_k를 신호 방향 후보 집합 $\mathbf{\Lambda}_{(k)}$에 포함한다. 이후, $\mathbf{\Lambda}_{(k)}$에 포함된 후보 방향에 대한 조향벡터를 통해 투영 행렬 $\mathbf{P}_k\in\mathbb{C}^{N\times N}$을 생성하여 이전 반복 신호 $\mathbf{y}_{(k-1)}$에 널사영(null projection)하여 현재 추정한 방향 성분을 제거하고 잔차를 업데이트한다. 이러한 과정은 최대 반복수 K 번 동안 수행되어 신호 $\mathbf{y}$에 존재하는 방향 성분을 반복 추정하는 휴리스틱 알고리즘이며 algorithm 1과 같이 정리될 수 있다. 이때, 신호원 유무는 임계치 $3\sigma_n$을 두어 신호원의 개수를 추정할 수 있도록 설계하였으며 이는 $\mathcal{H}_0$의 PRN 신호 채널에서 위성 방향 이외의 DoA 추정 결과가 이후 기만 탐지에 영향을 주지 않게 하기 위함이다. 즉, 특정 PRN신호 채널에서 출력 $\mathbf{\Lambda}_{(k)}$의 원소는 추정된 방향 인덱스를 의미하고 $|\mathbf{\Lambda}_{(k)}|$의 값은 추정된 신호원 개수가 된다. 만약 $|\mathbf{\Lambda}_{(k)}|$=2 일 때 해당 PRN 신호 채널에 존재하는 신호원이 두 개인 $\mathcal{H}_1$ 가설을 의미하며, $|\mathbf{\Lambda}_{(k)}|$=1 일 때 신호에 존재하는 신호원이 위성 뿐인 $\mathcal{H}_0$ 상태를 의미한다.

Algorithm 1 OMP algorithm for Spoofing Detection

Input: $\mathbf{y}\in\mathbb{C}^{N\times 1}$, $\mathbf{A}\in\mathbb{C}^{N\times P}$
Output: $\Lambda_{(K)}$.
Initialization:
  $\mathbf{y}_{(0)} = \mathbf{y}$,
  $\Lambda_{(0)} = \varnothing$,
  $k = 1$.
for $k = 1, \cdots, K$ **do**
  if $\max_{p\in\mathcal{P}} \left(|<\mathbf{a}_p, \mathbf{y}_{(k-1)}>|\right) > 3\sigma_n$ **then**
    $p_k = \arg\max_{p\in\mathcal{P}} \left(|<\mathbf{a}_p, \mathbf{y}_{(k-1)}>|\right)$
    Update $\Lambda_{(k)} \leftarrow \Lambda_{(k-1)} \cup \{p_k\}$
    $\mathbf{P}_k = \mathbf{A}\left(\Lambda_{(k)}\right)\left(\mathbf{A}\left(\Lambda_{(k)}\right)^H\mathbf{A}\left(\Lambda_{(k)}\right)\right)^{-1}\mathbf{A}\left(\Lambda_{(k)}\right)^H$
    $\mathbf{y}_{(k)} = \left(\mathbf{I}_N - \mathbf{P}_k\right)\mathbf{y}_{(k-1)}$
  end if
  $k = k + 1$
end for

단일 샘플이 아닌 I개의 샘플을 고려할 때 OMP 알고리즘은 SOMP 알고리즘으로 확장하여 적용할 수 있다. I개의 샘플에 대해 P개 방향에 대한 수신 신호 모델 식 (6)은 식 (7)과 같이 표현할 수 있다.

$$\mathbf{Y} = \mathbf{A}\mathbf{X} + \mathbf{N} = [\mathbf{a}_1\ \mathbf{a}_2\ \cdots \mathbf{a}_P]\begin{bmatrix}0 & \cdots & 0 & \cdots & 0\\ \vdots & \cdots & \vdots & \cdots & \vdots\\ x_1 & \cdots & x_i & \cdots & x_I\\ \vdots & \cdots & \cdots & \cdots & \vdots\\ 0 & \cdots & 0 & \cdots & 0\end{bmatrix} + \mathbf{N} \quad (7)$$

여기서, $\mathbf{Y}\in\mathbb{C}^{N\times I}$는 각 샘플에 대한 수신 신호 행렬을 의미하며 $\mathbf{X}\in C^{P\times I}$의 각 원소는 각 샘플 별 전체 방향에 대한 신호 성분을 의미한다. 따라서, 위성 및 기만기의 위치가 크게 변하지 않는 시간 동안의 샘플을 고려할 때 $\mathbf{X}$는 결합 희소성(joint sparsity)을 갖게 된다. $\mathbf{N}\in C^{N\times I}$은 각 시간 샘플 동안 수신기에서 발생하는 부가 열잡음을 의미한다. SOMP 알고리즘은 k 째 반복에서 A의 각 열과 각 시간 샘플에서의 수신신호간 모든 내적값의 합이 최대가 되는 방향 p_k를 신호 방향 후보 집합 $\mathbf{\Lambda}_{(k)}$에 포함한다. 신호원 유무 및 신호의 DoA 추정을 위한 SOMP 동작은 algorithm 2와 같이 정리되며 SOMP 알고리즘의 경우 수신신호의 결합 희소성에 대한 시간 (샘플) 다이버시티 효과로 인해 단일 샘플을 이용하는 OMP 알고리즘보다 정밀한 DoA 추정이 가능하고 I=1일 때 SOMP 알고리즘은 OMP 알고리즘과 동일하다.

Algorithm 2 SOMP algorithm for Spoofing Detection

Input: $\mathbf{Y}\in\mathbb{C}^{N\times I}$, $\mathbf{A}\in\mathbb{C}^{N\times P}$
Output: $\Lambda_{(K)}$.
Initialization:
  $\mathbf{Y}_{(0)} = \mathbf{Y}$,
  $\Lambda_{(0)} = \varnothing$,
  $k = 1$.
for $k = 1, \cdots, K$ **do**
  if $\max_{p\in\mathcal{P}} \left(\sum_{i=1}^{I}|<\mathbf{a}_p, \mathbf{y}_{(k-1),i}>|\right) > 3I\sigma_n$ **then**
    $p_k = \arg\max_{p\in\mathcal{P}} \left(\sum_{i=1}^{I}|<\mathbf{a}_p, \mathbf{y}_{(k-1),i}>|\right)$
    Update $\Lambda_{(k)} \leftarrow \Lambda_{(k-1)} \cup \{p_k\}$
    $\mathbf{P}_k = \mathbf{A}\left(\Lambda_{(k)}\right)\left(\mathbf{A}\left(\Lambda_{(k)}\right)^H\mathbf{A}\left(\Lambda_{(k)}\right)\right)^{-1}\mathbf{A}\left(\Lambda_{(k)}\right)^H$
    $\mathbf{Y}_{(k)} = \left(\mathbf{I}_N - \mathbf{P}_k\right)\mathbf{Y}_{(k-1)}$
  end if
  $k = k + 1$
end for

3.2 추정된 DoA를 통한 다중 PRN 기반 기만 탐지 기법

본 논문에서는 고정된 위치에서 단일 기만기가 다수의 PRN을 모사한다고 가정하였으므로 모든 PRN 신호 채널에 대해 정밀한 DoA 추정이 이루어졌다면 유사한 DoA를 갖는 신호의 개수는 기만기가 모사하는 PRN 수만큼 존재하게 된다. 따라서, GNSS 수신기는 모든 PRN 신호 채널에서 추정한 DoA 간의 차이를 계산하고 그 차이가 매우 작은 방향이 단일 방향이면서 다수의 PRN으로부터 관측될 때 해당 각도로부터 기만신호가 수신되었다고 탐지할 수 있다. 구체적으로, 모든 PRN 신호 채널에서 $\binom{M+L}{2}$ 개의 신호 방향 차이 정보를 계산할 수 있고 이를 이용하여 다음과 같은 DoA 간 차이 벡터 $\mathbf{\Phi}\in\mathbb{R}^{M+L\mathrm{C}_2}$를 고려한다.

$$\mathbf{\Phi} = \left[\Delta\phi_{12}, \Delta\phi_{13}, \cdots \Delta\phi_{(M+L-1)(M+L)}\right]^T \quad (8)$$

$\lvert\phi_i-\phi_j\rvert$		PRN1		PRN2		PRN3		PRN4	
		ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8
PRN1	ϕ_1	0	40	21	70	40	41	39	22
	ϕ_2		0	39	6	23	5	69	3
PRN2	ϕ_3			0	19	25	65	110	47
	ϕ_4				0	59	3	91	5
PRN3	ϕ_5					0	19	26	48
	ϕ_6						0	55	3
PRN4	ϕ_7							0	89
	ϕ_8								0

(a)

$\lvert\phi_i-\phi_j\rvert$		PRN1		PRN2		PRN3		PRN4	
		ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6	ϕ_7	ϕ_8
PRN1	ϕ_1	0	40	5	70	40	41	39	22
	ϕ_2		0	39	6	23	5	69	3
PRN2	ϕ_3			0	19	25	65	110	47
	ϕ_4				0	59	3	91	5
PRN3	ϕ_5					0	19	26	48
	ϕ_6						0	55	3
PRN4	ϕ_7							0	89
	ϕ_8								0

(b)

Fig. 3. (a) Example 1 of spoofing detection considering the difference between DoAs, (b) Example 2 of spoofing detection considering the difference between DoAs.

이때, 각 원소 $\Delta\phi_{ij}$ ($i\in\{1, 2,\cdots, M+L-1\}$, $j\in\{2,\cdots, M+L\}$, $i\neq j$)는 각각 i와 j째 추정한 DoA 간의 차를 의미한다 (*i.e.*, $\Delta\phi_{ij}=|\phi_i-\phi_j|$). 따라서, 식 (8)의 원소 중 특정 단일 방향에 대해 각도차가 작은 원소가 $\binom{L}{2}$개 만큼 존재할 때 기만 공격을 탐지할 수 있고 기만기의 방향도 알 수 있다. 그러나, 실제 환경에서 기만기가 몇 개의 PRN 신호를 모사하는지 타겟 GNSS 수신기는 알 수 없으며 수신기의 배열 안테나 종류와 개수에 따른 DoA 각도 분해능이 다르고, 위성의 방향이 기만기 근처에 존재하거나 위성간 방향이 유사할 경우 OMP 알고리즘을 통한 정확한 DoA 추정이 어려울 수 있다.

먼저, 본 논문에서는 이러한 수신기 배열 안테나의 각도 분해능을 고려하여 두 신호의 DoA가 유사한지 판단하기 위한 임계치 η를 수신기 배열 인자(array factor)를 통해 설정한다. N 소자 ULA를 고려할 때, 특정 수신 각도 $\tilde{\phi}$에 대해 공간 주파수는 $\tilde{\theta}=\frac{d}{\lambda}\sin\tilde{\phi}\in\left[-\frac{1}{2},\frac{1}{2}\right]$이고 임의의 θ에서의 배열 인자는 식 (9)와 같이 계산 된다.

$$\mathrm{AF}(\theta)=\left|\mathbf{a}^H(\tilde{\theta})\mathbf{a}(\theta)\right|^2=\sum_{i\in\mathcal{I}(N)}e^{-j2\pi(\tilde{\theta}-\theta)(i-1)}=\frac{\sin\pi N(\tilde{\theta}-\theta)}{\sin\pi(\tilde{\theta}-\theta)} \quad (9)$$

식 (9)는 Dirichlet sinc function으로 알려져 있으며 두 신호가 반 전력 빔 너비(half power beam width) 이내에 존재할 경우 배열 안테나를 통해 두 신호를 구분할 수 없게 되며 본 논문에서는 반 전력 빔 너비 이내 각도 차를 보일 때 두 신호가 유사한 방향에서 입사된다고 가정하였다. 따라서, ULA에 대한 두 신호간 유사 각도 차 임계치 η는 식 (10)과 같이 정의된다.

$$\eta=\frac{1}{2}\sin^{-1}\frac{2}{N} \quad (10)$$

반면에, 실제 환경에서 특정 위성들 간 각도차가 유사한 경우가 생길 수 있다. 이는 기만신호가 존재하지 않을 때 이러한 위성들로 인해 거짓 경보를 야기할 수 있다. 따라서, 이러한 문제를 해결하기 위해 수신기는 기만 탐지에 있어 유사한 각도 차를 갖는 식 (8)의 원소 수에 대한 마진을 두어야 한다. 또한, 기만신호가 존재할 때에도 기만기가 몇 개의 PRN을 모사하는지 정확히 알 수 없으므로 위성 간의 유사한 방향으로 인해 기만기 방향을 제대로 추정하지 못할 수 있으며 이 경우에 이러한 아웃라이어(outlier)를 기만 방향에서 제외시킬 수 있는 방안이 필요하다.

일반적으로 수신기는 자신의 위치 정보를 추정하기 위해 최소 4개의 PRN 신호를 수신하여 위치 추정에 필요한 방정식을 세울 수 있다 (Magiera 2019). 그러므로, 본 논문에서는 4개 이상의 PRN에서 유사한 각도로 수신되는 신호가 존재할 때 기만신호가 존재한다고 탐지하고 η 보다 낮은 각도 차를 갖는PRN 신호 방향 중 특정 PRN에서의 방향 ϕ_i가 3개 이상 존재할 때만 기만 후보 방향에 포함한다. 예를 들어, Fig. 3a는 본 논문에서 제안하는 다중 PRN에서의 DoA 각도차를 이용한 기만 탐지 기법의 M=L=4 일 때의 예시로 η=7일 때 PRN 1의 ϕ_2는 PRN 2의 ϕ_4, PRN 3의 ϕ_6, 그리고 PRN 4의 ϕ_8과 임계치 이내의 DoA 차이를 가지므로 PRN 1의 ϕ_2는 기만 후보 방향이 된다. 마찬가지로 PRN 1, 2, 3, 4에서 {ϕ_2, ϕ_4, ϕ_6, ϕ_8}이 서로 간의 DoA 차가 η보다 작으면서 3개 이상 발생하므로 기만 후보 방향이 된다. 반면에, Fig. 3b는 동일하게 M=L=4이지만 두 개의 위성이 서로 근접한 방향에서 수신될 때의 기만 탐지 예시이다. 이 경우 각 PRN에서 η보다 낮은 각도차를 갖는 DoA는 {ϕ_1, ϕ_2, ϕ_3, ϕ_4, ϕ_6, ϕ_8}이지만 {ϕ_1, ϕ_3}은 오직 한 번만 발생하므로 기만 후보 방향에 제외될 수 있어 거짓 경보 및 잘못된 기만 방향 추정이 발생하지 않는다. 본 논문에서는 찾은 기만 후보 방향의 DoA 평균값을 기만신호 방향으로 추정하며 이는 기만기가 다수의 위성 PRN을 모사할수록 다중 PRN 다이버시티 효과로 인해 더욱 정밀한 기만신호 DoA를 추정할 수 있게 된다.

4. 모의 실험 결과

본 장에서는 제안하는 압축 센싱 기반 신호의 DoA 추정 및 다중 PRN 기반의 기만 탐지 기법의 성능을 MATLAB 모의 실험을 통해 분석한다.

먼저, GNSS 기만 시나리오의 모의 실험 환경은 Table 1과 같다. 또한, 각 위성과 기만신호의 방향 정보는 Table 2와 같이 설정하였다. 본 논문에서는 DoA 추정에 있어 [-90˚,90˚]의 도래각(azimuth angle) 범위를 고려하였으며 각도 해상도를 1˚로 설정하여 P=181개의 센싱 행렬 $\mathbf{A}$를 설계하였다.

Fig. 4a는 단일 샘플에 대한 본 논문에서의 DoA 추정 알고리즘인 압축센싱 기반 OMP 알고리즘의 DoA 추정 결과이며 Fig. 4b는 MUSIC 알고리즘의 DoA 추정 결과를 나타낸다. MUSIC 알고리즘의 경우 단일 샘플에서 정확한 공분산 연산이 수행되지 않아 잡음과의 상관이 커지므로 모든 신호에서 DoA 추정이 정확하게 수행되지 않으나 OMP 알고리즘의 경우 신호 전력이 잡음 대비 충분히 클 때 상대적으로 모든 신호원에 대해 높은 정확도로 신

Table 1. Simulation environment.

Parameter	Value
Sampling frequency	2 MHz
Received power of authentic signal	-158 dBW
Noise variance	-140 dBW
Doppler frequency difference	0 Hz
Code chip delay difference	0.5 chip
Spoofing to authentic power ratio	0 dB
The number of authentic PRNs	9
The number of spoofing PRNs	4
The number of antennas	7

Table 2. The azimuth angles of authentic and spoofing signal.

PRN number	Azimuth angle (°)	PRN number	Azimuth angle (°)
PRN 2	-20	PRN 8	54
PRN 14	-5	PRN 18	60
PRN 20	-30	PRN 22	-90
PRN 24	40	PRN 25	80
PRN 26	-70	Spoofer	20

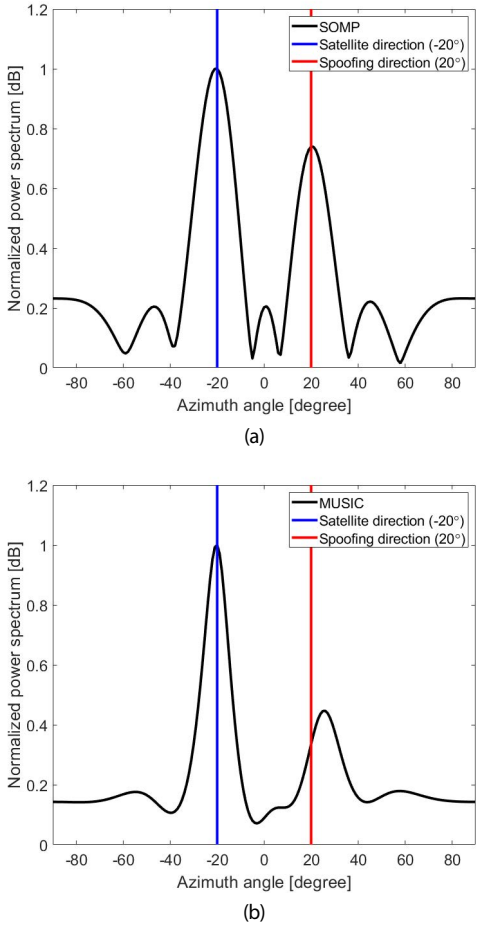

Fig. 4. (a) Power spectrum with SOMP algorithm according to azimuth angle in a single sample, (b) Power spectrum with MUSIC algorithm according to azimuth angle in a single sample.

호원의 DoA를 추정할 수 있다.

Fig. 5는 SOMP 알고리즘과 MUSIC 알고리즘으로 추정한 모든 신호들의 DoA에 본 논문에서 제안하는 다중 PRN 기반 기만

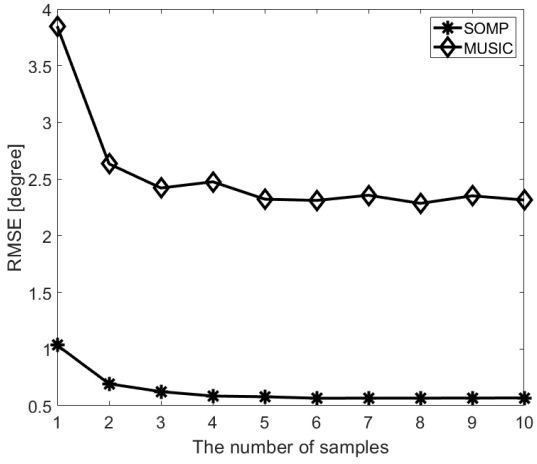

Fig. 5. DoA RMSE performance of SOMP and MUSIC algorithms in a few number of samples.

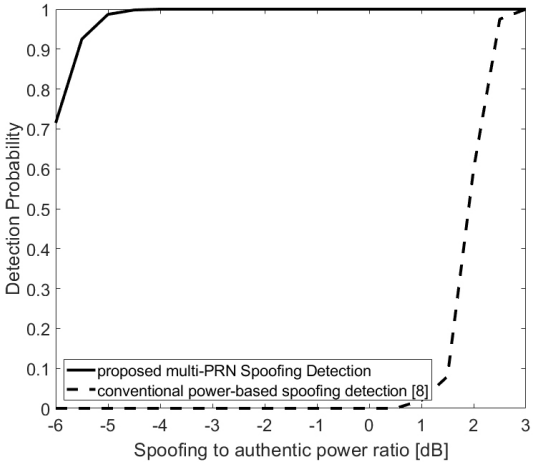

Fig. 6. Spoofing detection probability of conventional power-based spoofing detection method and the proposed direction-based spoofing detection method according to spoofing to authentic power ratio.

탐지 기법을 각각 적용하여 추정한 기만신호의 DoA root mean squared error (RMSE) 성능을 샘플 수에 따라 확인한 결과이다. MUSIC 알고리즘은 샘플 수가 증가함에 따라 수신 신호의 공분산 행렬이 정확해지기 때문에 성능향상을 보인다. 그러나, 여전히 적은 샘플 수에 대해서 압축센싱 기반의 SOMP 알고리즘이 MUSIC 알고리즘 기반 DoA 추정보다 좋은 성능을 보이는 것을 확인할 수 있다. 이러한 이유는 앞서 Fig. 4b와 같이 공분산 기반의 기법이 최대 전력 신호원을 제외한 나머지 신호원에 대해 DoA를 정밀하게 추정하기 위해서 더 많은 샘플이 필요하기 때문이며 본 모의 실험 환경과 같이 기만 신호의 전력이 위성 신호 전력과 비슷하거나 심지어 더 낮은 경우 추정된 기만 DoA에 오차가 발생하게 된다.

Fig. 6은 제안하는 기법과 상관 전 수신 신호로부터 기만 신호를 탐지하는 전력 기반 기만 탐지 기법 (Zhang et al. 2019)과의 성능 비교 결과이다. 이때 본 논문에서의 기만 탐지 및 거짓 경보 확률은 각각 기만신호가 존재할 때와 존재하지 않을 때의 전체

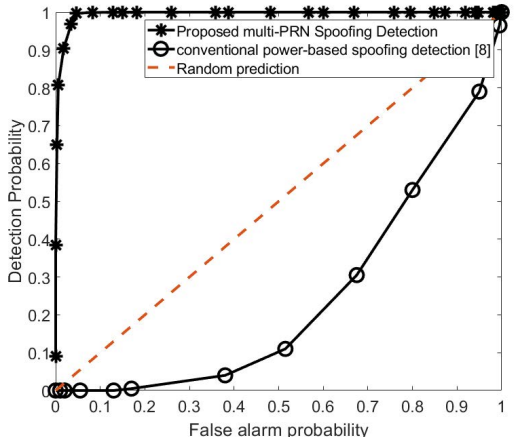

Fig. 7. Receiver operating characteristic curves of conventional power-based spoofing detection method and proposed direction-based spoofing detection method.

모의 실험 반복 횟수 대비 기만신호가 탐지된 횟수의 비율을 의미하며 본 실험에서는 1,000번의 몬테카를로(Monte-Carlo) 실험을 통한 기만 탐지 확률을 산출하였다. 전력 기반의 비교 기만 탐지 기법은 최대 고유값의 분포를 통해 기만신호를 탐지하므로 기만신호의 전력이 위성신호 전력보다 더 클 때만 높은 탐지 성능을 보인다. 반면 본 논문에서 제안하는 다중 PRN 기반의 기만 탐지 기법은 신호원의 방향 추정으로부터 수행되기 때문에 기만신호와 위성 신호의 상대적인 전력비와는 상관없이 높은 확률로 기만신호를 탐지할 수 있다. 그렇기 때문에 Fig. 2와 같은 기만 공격 시나리오에서 초기 대응이 가능함을 알 수 있다.

Fig. 7은 본 논문에서 고려하고 있는 정교한 기만 시나리오에서 제안하는 기만 탐지 알고리즘과 기존의 전력 기반 기만 탐지 기법의 수신기 동작 특성 커브(receiver operating characteristic curve: ROC curve)를 나타낸다. 마찬가지로, 전력 기반 기법의 경우 기만 대 위성 신호 전력 비가 비슷하거나 더 작은 정교한 기만 시나리오에서 기만 탐지가 제대로 이루어지지 않고, 실제 위성의 PRN 수가 기만기가 모사하는 PRN 보다 더 많기 때문에 각 위성 신호의 성분이 최대 고유값에 영향을 끼쳐 높은 거짓 경보 확률을 가진다. 반면에, 제안하는 기법의 경우 DoA 추정에 있어 신호원 유무 확인을 위한 임계 조건 및 근접한 위성 방향에 대한 거짓 경보 방지 조건을 통해 높은 탐지 성능을 보이면서 거짓 경보 확률 또한 낮은 것을 확인할 수 있다.

5. 결론

본 논문에서는 다수의 PRN을 모사하는 단일 기만기가 존재하는 GNSS 환경에서 타겟 GNSS 수신기가 배열 안테나와 다중 PRN 신호를 이용하여 기만 신호를 탐지하는 기법을 제안하였다. 기만 탐지는 압축 센싱의 OMP 알고리즘으로부터 모든 신호의 DoA를 추정하며 동일 DoA로 추정된 다수의 신호를 기만 신호로 판단하여 기만 탐지를 수행한다. 또한, 제안하는 기법은 신호원 유무를 확인할 수 있는 임계와 위성간 방향이 근접할 경우에 대한 방안을 통해 거짓 경보에 강인하게 설계되었으며 기존 전력 기반의 기만 탐지 기법과 비교하여 기만신호의 전력이 위성신호의 전력과 비슷하거나 심지어 더 작은 환경에서도 우수한 기만 탐지 성능을 보이면서 낮은 거짓 경보 확률을 갖는 것을 시뮬레이션을 통해 검증하였다.

따라서, 제안하는 기술은 정교한 기만 공격 시나리오에 대해 위성신호를 추적중인 GNSS 수신기가 실시간으로 DoA를 추정하여 초기에 기만 탐지가 이루어 질 수 있으며 또한, 본 연구 결과를 통해 군수 및 민간 분야의 위성항법시스템 활용 분야에서 보다 더 정교한 의도적 간섭 공격 대응 기술 연구에 중요한 토대가 될 것으로 예상된다.

ACKNOWLEDGMENTS

본 연구는 덕산넵코어스㈜의 지원에 의해 수행되었습니다.

AUTHOR CONTRIBUTIONS

Conceptualization, S.J.L. and B.C.J.; investigation, Y.-S.L., J.S.Y., J.H.N., S.J.L. and B.C.J.; methodology, Y.-S.L. J.S.Y. and J.H.N.; project administration, S.J.L. and B.C.J.; software, Y.-S.L. and J.H.N.; supervision, B.C.J.; validation, J.S.Y.; writing-original draft, Y.-S.L.; writing-review and editing, J.S.Y., J.H.N., S.J.L. and B.C.J.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Bao, L., Wu, R., Wang, W., & Lu, D. 2017, Spoofing mitigation in Global Positioning System based on C/A code self-coherence with array signal processing, Journal of Communications Technology and Electronics, 62, 66-73. https://doi.org/10.1134/S1064226917010090

Broumandan, A., Jafarnia-Jahromi, A., Daneshmand, S., & Lachapelle, G. 2016, Overview of spatial processing approaches for GNSS structural interference detection and mitigation, Proc. IEEE, 104, 1246–1257. https://doi.org/10.1109/JPROC.2016.2529600

Guo, Y., Miao, L., & Zhang, X. 2019, Spoofing detection and mitigation in a multi-correlator GPS receiver based on the maximum likelihood principle, MDPI Sensors, 19, 37. https://doi.org/10.3390/s19010037

Hu, Y., Bian, S., Li, B., & Zhou, L. 2018, A novel array-based spoofing and jamming suppression method for GNSS receiver, IEEE Sensors Journal, 18, 2952-2958.

https://doi.org/10.1109/JSEN.2018.2797309
Huang, J., Presti, L. L., Motella, B., & Pini, M. 2016, GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky, ICT Express, 2, 37-40. https://doi.org/10.1016/j.icte.2016.02.006
Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, Jr., P. M. 2008, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, Prod. 21st Int. Techn. Meet. Satellite Division ION GNSS, Savannah, GA, Sep 2008, pp.2314-2325. https://doi.org/10.15781/T26T0HC7Q
Ioannides, R. T., Pany, T., & Gibbons, G. 2016, Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques, Proc. IEEE, 104, 1174–1194. https://doi.org/10.1109/JPROC.2016.2535898
Magiera, J. 2019, A multi-antenna scheme for early detection and mitigation of intermediate GNSS spoofing, Sensors, 19, 2411. https://doi.org/10.3390/s19102411
Meurer, M., Konovaltsev, A., Cuntz, M., & Hättich, C. 2012, Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM, Prod. 25th Int. Techn. Meet. Satellite Division ION GNSS, Nashville, TN, Sep 2012, pp.3007-3016.
Nielsen, J., Broumandan, A., & Lachapelle, G. 2010, Spoofing detection and mitigation with a moving handheld receiver, GPS world, 21, 27-33.
Noh, J. H., Gong, B. H., Lee, Y. S., Jung, B. C., Lee, S. J., et al. 2021, Performance analysis of GNSS spoofing mitigation techniques based on array antennas in various spoofing scenarios, In Proc. of the 2021 ITM ION GNSS, Jan 25-28, 2021, pp.282-294. https://doi.org/10.33012/2021.17833
Psiaki, M. L. & Humphreys, T. E. 2016, GNSS spoofing and detec-tion, Proc. IEEE, 104, 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658
Shen, Q., Liu, W., Cui, W., & Wu, S. 2016, Underdetermined DOA estimation under the compressive sensing framework: A review, IEEE Access, 4, 8865-8878. https://doi.org/10.1109/ACCESS.2016.2628869
Wesson, K. D., Evans, B. L., & Humphreys, T. E. 2013, A combined symmetric difference and power monitoring GNSS anti-spoofing technique, In 2013 IEEE Global Conference on Signal and Information Processing, Austin, TX, Dec 2013, pp.217-220. https://doi.org/10.1109/GlobalSIP.2013.6736854
Yang, Q., Zhang, Y., Tang, C., & Lian, J. 2019, A combined antijamming and antispoofing algorithm for GPS arrays, International Journal of Antennas and Propagation, 2019, Article ID 8012569. https://doi.org/10.1155/2019/8012569
Zhang, J., Cui, X., Xu, H., & Lu, M. 2019, A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing, Sensors, 19, 3870. https://doi.org/10.3390/s19183870
Ziółkowski, C. & Kelner, J. M. 2020, Doppler-based navigation for mobile protection system of strategic maritime facilities in GNSS jamming and spoofing conditions, IET Radar, Sonar & Navigation, 14, 643-651. https://doi.org/10.1049/iet-rsn.2019.0413

Young-Seok Lee received the B.S. degree in Electronics Engineering from the Chungnam National University, Daejeon, South Korea in 2020. He is currently an M.S. student for communications and signal processing in Electronics Engineering at Chungnam National University, Daejeon, South Korea. His research interests include wireless sensor networks (WSNs), multiple-input multiple-output (MIMO), Internet of Things (IoT) sensor networks and array processing.

Jeong Seon Yeom received his B.S. degree in electronics engineering and M.S. degree in electronics, radio sciences, and engineering and information communications engineering from Chungnam National University, Daejeon, Rep. of Korea in 2017 and 2019, respectively. He is currently a Ph.D student studying communications and signal processing in electronics engineering at Chungnam National University, Daejeon, Rep. of Korea. His research interests include non-orthogonal multiple access, multiple-input multiple-output, and interference mitigation in wireless communication systems.

Jae Hee Noh is a Ph.D candidate with the Department of Electronics Engineering at Chungnam National University in Korea. She received B.S and M.S degrees from Chungnam National University, Department of Electronic Engineering in 2017 and 2019, respectively. Her research interests include GNSS receiver, anti-spoofing techniques and message authentication.

Sang Jeong Lee is a professor with the Department of Electronics Engineering, Chungnam National University, Korea. He received his B.S., M.S., and Ph.D. degrees from Seoul National University, Korea, in 1979, 1981, and 1987, respectively. His research interests include GNSS receiver design and robust control.

Bang Chul Jung received the B.S. degree in Electronics Engineering from Ajou University, Suwon, Korea, in 2002 and the M.S. and Ph.D degrees in Electrical & Computer Engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in 2004 and 2008, respectively. He was a senior researcher/ research professor with KAIST Institute for Information Technology Convergence, Daejeon, Korea, from January 2009 to February 2010. From Mar. 2010 to Aug. 2015, he was a faculty of Gyeongsang National University, Tongyeong, Korea. He is currently a Professor of the Dept. of EE, Chungnam National University, Daejeon, Korea. Prof. Jung has served as an Associate Editor of IEEE Vehicular Technology Magazine since May 2020. He has also served as Associate Editor of IEICE Transactions on Fundamentals of Electronics, Communications, and Computer Sciences since 2018. Dr. Jung was the recipient of the 5th IEEE Communication Society AsiaPacific Outstanding Young Researcher Award in 2011, the KICS Haedong Young Scholar Award in 2015, and the 29th KOFST Science and Technology Best Paper Award in 2019. His research interests include 6G wireless communications, wireless IoT communications, statistical signal processing, information theory, wireless localization, interference management, radar signal processing, spectrum sharing, multiple antennas, multiple access techniques, radio resource management, machine learning, and GNSS receiver signal processing.