2024 15th International Conference on Information and Communication Technology Convergence (ICTC) | 979-8-3503-6463-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICTC62082.2024.10827561

# Robust GNSS Spoofing Detection Based on Prior Information of Satellite Trajectories

Minkyu Oh, Young-Seok Lee, Chang-Ok Kang†, and Bang Chul Jung
Department of Electronics Engineering, Chungnam National University, Daejeon, South Korea
† Duksan Navcours, Co. Ltd., Daejeon, South Korea
Email: minkyuoh@o.cnu.ac.kr, yslee@o.cnu.ac.kr, cokang@oneduksan.com, bcjung@cnu.ac.kr

***Abstract*—GNSS spoofing attacks aim to control the tracking loop of a target receiver and may cause significant damage to GNSS users and corresponding properties. In this paper, we propose a novel spoofing detection technique for the global navigation satellite system (GNSS), which leverages trajectory information of satellites and array antenna-based direction of arrival (DoA) estimation. In particular, in the proposed GNSS spoofing detection technique, the target receiver compares satellite trajectory information with the array antenna-based DoA estimation result to extract the feature of the GNSS spoofing attack and determine whether it is currently under attack. Simulation results show that the proposed technique has robust spoofing detection performance compared with conventional techniques, even under multiple spoofers' attacks.**

***Index Terms*—Global navigation satellite system (GNSS), anti-spoofing, spoofing detection, direction of arrival (DoA).**

## I. Introduction

Applications where localization capability is one of the key performance indicators, such as aviation or satellite communications, autonomous driving, and integrated sensing and communication (ISAC), have recently been receiving much attention [1]. Hence, the importance of global navigation satellite systems (GNSS) has also increased significantly as it can provide precise and robust localization performance. However, because GNSS signal structures and protocols are already known, they are vulnerable to intentional interference attacks such as jamming and spoofing.

In particular, GNSS spoofing attacks aim to control the tracking loop of a target receiver by transmitting counterfeit signals with the same structure as the satellite signal [2]. Among them, sophisticated GNSS spoofing attack scenarios are more challenging to detect since the spoofer initially transmits spoofing signals with similar power to the authentic signal and gradually increases the power to deceive the target receiver [3]. In these sophisticated GNSS spoofing scenarios, direction-finding algorithms using array antennas have been primarily exploited for GNSS spoofing detection [3], [4]. However, most GNSS spoofing detection studies considering sophisticated spoofing scenarios assume that a single spoofer mimics multiple pseudo-random noise (PRN) signals and that the target receiver constantly receives many PRN satellite signals. In practical GNSS environments, existing spoofing detection methods may not work if multiple spoofers exist or if a sufficient number of satellite PRNs are not observed at a specific time and location.

In this paper, we propose a novel GNSS spoofing detection strategy that jointly utilizes satellite trajectory information corresponding to the receiver's location and time and array antenna-based direction of arrival (DoA) estimation. As geostationary earth orbit (GEO) satellites are used as GNSS, they move along with the Earth's rotation, so satellite trajectory information at a specific time and location can be easily obtained through the ephemeris [5]. Specifically, the proposed technique estimates DoA on each PRN signal and calculates the difference from the reference DoA according to satellite trajectory information. For post-despreading GNSS signals, the correlation between authentic and spoofing signals can be a crucial feature interfering with DoA estimation at the receiver. Through extensive simulations, we verify that the proposed GNSS spoofing detection technique can have robust spoofing detection performance even in the presence of multiple spoofers.

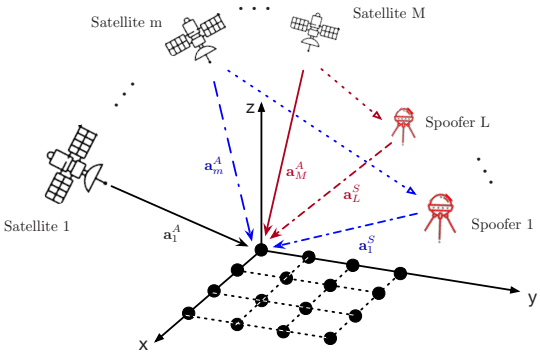


Fig. 1. System model where a target receiver with a UPA and multiple spoofers exist.

## II. System Model & GNSS Spoofing Scenario

This paper considers a single GNSS receiver equipped with an $N$-element uniform planar array antenna (UPA), as shown in Fig. 1. We assume a general environment where, at a specific time, the receiver receives $M$ satellite signals and $Q$ spoofers are imitating $L(\leq M)$ authentic signals. For each PRN signal, there may be no spoofing signal or multiple spoofers may attack it. Here, we also assume a sophisticated GNSS spoofing scenario where the spoofers synchronize time and Doppler frequency through the location information of the target receiver and its own GNSS receiver and transmit spoofing signals at a power level similar to the authentic signal [3].

Therefore, after carrier frequency compensation and despreading, the received signal for the $m(\in \{1, \cdots, M\})$-th PRN satellite at a specific time $t$ can be represented as

$$\mathbf{y}(t) = \mathbf{a}_m^A(\gamma_m, t)x_m^A(t) + \sum_{q=1}^{Q} \beta_q \mathbf{a}_q^S(\gamma_q, t)x_q^S(t) + \mathbf{n}_m(t), \quad (1)$$

where the superscripts $A$ and $S$ denote for authentic and spoofing signal, respectively, and $\mathbf{a}(\gamma, t)(\in \mathbb{C}^N)$ represents

the steering vector for the directional information $\gamma = \{\phi, \theta\}$ at time $t$. Here, $\phi(\in [0, 2\pi])$ and $\theta(\in [0, \pi/2])$ denote the azimuth and elevation angle, respectively. In addition, $x$ refers to the signal with spreading gain. And, $\beta_q(\in \{0, 1\})$ represents an indicator bit as to whether a particular $q(\in \{1, \cdots, Q\})$-th spoofer has imitated the $m$-th PRN satellite signal.

## III. Satellite Trajectory-based GNSS Spoofing Detection Technique

Without loss of generality, we explain the proposed spoofing detection technique for $m$-th PRN satellite. This paper assumes that satellite trajectory information at a specific time and location of the receiver can be easily obtained through the ephemeris [5]. Through this trajectory information, we can also obtain the $m$-th reference directional information $\bar{\gamma}_m(= \{\bar{\phi}_m, \bar{\theta}_m\})$. Note that this reference direction information represents the approximate direction of the satellite and is not the exact direction information of the satellite. The receiver collects received signal samples as in (1) and performs DoA estimation for a single signal source. Then, the difference between the estimated DoA and reference DoA for $m$-th PRN satellite can be calculated as

$$\Delta\phi_m = \mathrm{mod}(|\bar{\phi}_m - \hat{\phi}_m|, 2\pi), \quad \Delta\theta_m = |\bar{\theta}_m - \hat{\theta}_m|, \qquad (2)$$

where mod, $\hat{\phi}$, and $\hat{\theta}$ denote modulo operator, estimated azimuth angle, and estimated elevation angle, respectively.

If both the azimuth and elevation angles for a PRN satellite differ within a certain threshold, the satellite signal for that PRN satellite has been correctly found. It is worth noting that if the satellite DoA is correctly found, the effect of a spoofing attack can be mitigated by beamforming in the direction of the satellite. On the other hand, if the estimated DoA differs from the reference DoA by more than a threshold in either the azimuth or elevation angle, it means that spoofing signals are affecting the DoA estimation. Therefore, the receiver declares preliminary attack alarms for these PRN satellites. Considering the false alarm performance, we set the design parameter $\zeta(\leq M)$, which can count the attacked PRN satellites. A spoofing attack alarm is alerted when $\zeta$ or more preliminary alarms among $M$ satellites are checked.

## IV. Simulation Results

To validate the proposed technique, we set the center frequency to 1575.42 MHz, considering the GPS L1 C/A band, and assumed that the receiver was equipped with a UPA consisting of 16 elements spaced at half-wavelength intervals and receiving four satellite PRN signals. We adopted the multiple signal classification (MUSIC) algorithm for DoA estimation and used 10 samples for covariance calculation. The thresholds for the differences in DoA are established at $18^\circ$ for azimuth and $5^\circ$ for elevation. These values are based on twice the average DoA between the closest satellites, as determined from GNSS trajectory data collected at 30-minute intervals on Aug. 3, 2024. We also considered a spoofing scenario in which four spoofers exist at random angles, and each spoofer transmits a spoofing signal corresponding to a single satellite.

Fig. 2 shows the proposed technique's detection and false alarm probability according to the received signal-to-noise ratio (SNR). In this paper, we compared the performance of our proposed techniques with the multi-PRN diversity-based GNSS spoofing detection algorithm [3]. The conventional multi-PRN-based technique can operate when a single spoofer

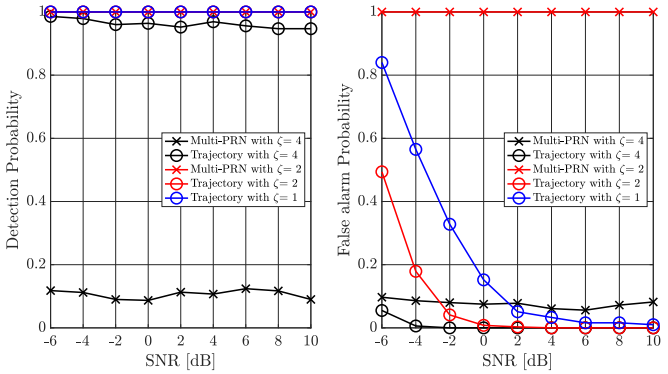


Fig. 2. Detection and false alarm probabilities of the proposed technique for different $\zeta$ thresholds.

mimics all PRN satellites. This shows that the detection probability is high only when the threshold $\zeta$ for the number of PRN satellites determined to have a spoofing signal is low. However, since the false alarm probability in this case is also high, the conventional technique does not work in environments where multiple spoofers exist. On the other hand, we confirmed that our proposed technique has high detection and low false alarm probabilities for all operating SNR regions compared to the existing technique. The proposed technique has also been verified to generate almost no false alarms in the high SNR range, where DoA estimation is accurate. In other words, the proposed technique can achieve robust GNSS spoofing detection performance even when multiple spoofers exist.

## V. Conclusion

In this paper, we proposed a robust GNSS spoofing detection algorithm based on the trajectory information of satellites. Through extensive simulations, we verified that the proposed technique using trajectory information data exhibits robust spoofing detection performance even in sophisticated GNSS spoofing scenarios with multiple spoofers. We identified a trade-off between the proposed technique's detection probability and false alarm probability.


## Acknowledgment

This work was partly supported by the Defense Acquisition Program Administration's weapon system parts localization support project "Embedded GNSS and Inertial (EGI) device for Light Armed Helicopter (LAH)" (Development Control Number: C220020) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00396992).


## References


[1] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, "Localization and navigation in autonomous driving: Threats and countermeasures," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 38–45, Aug. 2019.

[2] Z. Kassas, J. Khalife, A. Abdallah, and C. Lee, "I am not afraid of the GPS jammer: Resilient navigation via signals of opportunity in GPS-denied environments," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 7, pp. 4–19, Jul. 2022.

[3] Y. -S. Lee, J. S. Yeom, and B. C. Jung, "A novel antenna-based GNSS spoofing detection and mitigation technique," in *Proc. 2023 IEEE 20th Consum. Commun. Netw. Conf.*, pp. 489-492, Jan. 2023.

[4] H. Wang, H. Li, M. Zhong, and M. Lu, "A space-time-ambiguity decomposition method for DOA estimation enhancing anti-spoofing via rotating dual antennas," *IEEE Aerosp. Electron. Syst. Mag.*, 2024 (Early access).

[5] "About the crustal dynamic data information system (CDDIS) GNSS data and products archive," [Online] Available: https://cddis.nasa.gov.