Performance Analysis of DOA-Based Spoofing Detection Techniques in Non-Terrestrial Networks

Minkyu Oh
Department of Artificial Intelligence
Convergence Network, Ajou University
Suwon, South Korea
Email : mkoh@ajou.ac.kr

Bang Chul Jung
Department of Electrical and
Computer Engineering, Ajou University
Suwon, South Korea
Email : bcjung@ajou.ac.kr

Abstract— Positioning techniques based on non-terrestrial networks (NTNs), such as the global navigation satellite system (GNSS) and low earth orbit (LEO) satellites, have become essential components in a variety of applications. However, GNSS signals are known for their properties, making them vulnerable to malicious spoofing attacks [1,2]. To address this important security vulnerability, an algorithm is proposed that leverages direction of arrival (DOA) estimation in multi-antenna arrays [3-6]. In this paper, we mathematically approximate the performance of spoofing detection techniques based on DOA estimation proposed in [6]. The proposed technique leverages the spatial diversity of received signals for authentication. The core algorithm is designed to work robustly even in challenging environments where real satellite signals and fake spoofing signals coexist. The discrimination mechanism relies on identifying significant disparities between their estimated DOA. While the efficacy and robustness of this technique have been validated through comprehensive simulations, demonstrating excellent empirical performance, a rigorous theoretical analysis of its performance bounds remains an unaddressed area.

This work aims to provide a more accurate mathematical performance analysis. We note that previous analyses based on the Cramér-Rao lower bound (CRLB) were primarily confined to single-signal scenarios, exhibiting deviations from simulation results under low SNR conditions. To address these limitations, we derive detection and false-alarm probabilities using Q-function approximation based on the variance of DOA estimates and verify our analytical model for simulation results.

Keywords—Low earth orbit (LEO) satellite, non-terrestrial networks (NTN), global navigation satellite system (GNSS), spoofing detection, DOA estimation

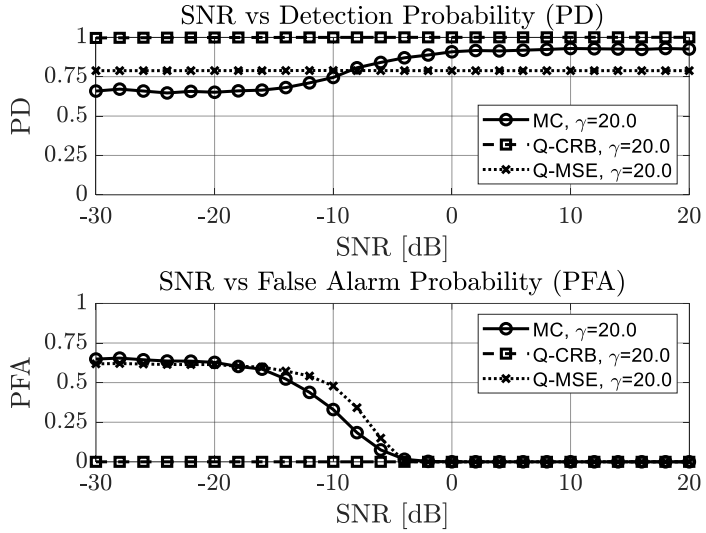

Figure 1. Performance analysis and comparison of simulation results using the Q function

[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] H.-S. Cha, G. Lee, A. Ghosh, M. Baker, S. Kelley, and J. Hofmann, "5G NR positioning enhancements in 3GPP release-18," *IEEE Commun. Stand. Mag.*, vol. 9, no. 1, pp. 22-27, Mar. 2025.

[3] Young-Seok Lee, Jeong Seon Yeom, and Bang Chul 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. Tan, N. Xie, L. Huang, and H. Li, "Enhancing GNSS signal authentication through multi-antenna systems," *IEEE Trans. Wireless Commun.,* vol. 24, no. 5, pp. 4361-4374, May 2025.

[5] X. Peng, C. Huang, X. Zhu, Z. Chen, and X. Yuan, "GLRT-based spacetime detection algorithms via joint DoA and Doppler shift method for GNSS spoofing interference," *IEEE Internet Things J.*, vol. 11, no. 23, pp. 37452-37462, Dec. 2024.

[6] M. Oh, Y.-S. Lee, C.-O. Kang, and B. C. Jung, "Robust GNSS spoofing detection based on prior information of satellite trajectories," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2024.