DAFTAR PUSTAKA

[1] I. Pokrajac, N. Kozić, A. Čančarević, and R. Brusin, “Jamming of GNSS Signals,” *Scientific and Technical Review*, vol. 68, no. 3, pp. 17–21, 2018.

[2] J. Gaspar, R. Ferreira, P. Sebastiao, and N. Souto, “Capture of UAVs Through GPS Spoofing,” in *6th Global Wireless Summit (GWS)*, pp. 21–26, 2018, doi: 10.1109/GWS.2018.8686727.

[3] G. Blass, A. Hennigar, and S. Mao, “Implementation of a Software-Defined Radio Based Global Positioning System Repeater,” in *2015 ASEE Southeast Section Conf.*, p. 10, 2015.

[4] A. H. Aboud, R. Ramadan, and T. Alsharabati, “Software Defined Radio Implementing GPS Parallel Frequency Space Search Acquisition Algorithm in Real Time Environment,” in *2015 Int. Conf. Inf. Commun. Technol. Res. (ICTRC)*, pp. 234–237, 2015, doi: 10.1109/ICTRC.2015.7156465.

[5] B. A. Chapman, *2017 Tech Notes*, no. Jan., pp. 20–33, 2017.

[6] J. Magiera and R. Katulski, “Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing,” *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–57, 2015, doi: 10.1016/S1665-6423(15)30004-3.

[7] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, “Effect of Spoofing on Unmanned Aerial Vehicle Using Counterfeited GPS Signal,” *J. Positioning, Navig. Timing*, vol. 4, no. 2, pp. 57–65, 2015, doi: 10.11003/jpnt.2015.4.2.057.

[8] E. Grayver, *Implementing Software Defined Radio*, New York: Springer, 2013.

[9] J. Bhatti and T. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[10] M. N. Akhlaq and M. R. Usman, "A review of GNSS spoofing countermeasures," *Journal of Navigation*, vol. 74, no. 6, pp. 1251–1275, Nov. 2021.

[11] C. Yang, H. Zhang, and S. Han, "Detection of spoofing signals based on RAIM and INS integration," in *Proc. IEEE International Conf. on Information and Automation (ICIA)*, Yinchuan, China, Aug. 2019, pp. 1118–1123.

[12] T. E. Humphreys, "Detection strategy for cryptographic GNSS antispoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, Apr. 2013.

[13] X. Zhang, F. Dovis, and C. Gioia, "GNSS spoofing detection using DNN under low and high C/N0 conditions," in *Proc. European Navigation Conference (ENC)*, Warsaw, Poland, Apr. 2020, pp. 1–10.

[14] J. Gross, S. Rathinam, and M. T. Wolf, "GNSS spoofing detection using 3D signal propagation modeling," *Sensors*, vol. 19, no. 20, pp. 1–19, 2019.

[15] A. Broumandan, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver autonomous integrity monitoring (RAIM)," *Navigation*, vol. 60, no. 4, pp. 267–277, 2013.

[16] D. Psiaki and T. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[17] L. Heng, D. B. Work, and G. Gao, "GPS spoofing attack and defense in smart grid time synchronization," in *Proc. IEEE Int. Conf. on Smart Grid Communications (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 217–222.

[18] D. Shepard, J. Bhatti, T. Humphreys, and A. Fansler, “Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks,” Int. J. of Critical Infrastructure Protection, vol. 5, no. 3–4, pp. 146–153, 2012.

[19] M. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” Int. J. of Navigation and Observation, vol. 2012, pp. 1–16, 2012.

[20] X. Zhang, F. Dovis, and C. Gioia, “Low-cost and low-complexity GNSS spoofing detection based on a rule-based model,” in Proc. European Navigation Conf. (ENC), 2020, pp. 1–6.

[21] Hegarty, E. Powers, and B. Fonville, “Accounting for the effects of group delay and signal dynamics in GPS receiver design,” Proc. PLANS, pp. 167–174, 2000

[22] F. Wang, W. Li, J. Liu, and X. Zhang, “IoT-based real-time GNSS spoofing detection using low-cost receivers,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6676–6688, 2021.

[23] B. Zhu, Y. Zhang, and K. Liu, “A web-based GNSS monitoring system for spoofing and jamming detection,” Sensors, vol. 20, no. 15, p. 4266, Jul. 2020.

[24] S. Daneshmand, A. Broumandan, and G. Lachapelle, “GNSS spoofing detection using statistical analysis of raw measurements,” in Proc. ION GNSS+, 2012, pp. 1232–1239.

[25] J. Nielsen, A. Broumandan, and G. Lachapelle, “Spoofing detection and mitigation with a moving antenna array,” GPS Solutions, vol. 24, no. 2, pp. 1–14, 2020.

[26] T. E. Humphreys, “Detection strategy for cryptographic GNSS antispoofing,” IEEE Trans. Aerospace Electron. Syst., vol. 49, no. 2, pp. 1073–1090, 2013.

[27] u-blox, “NEO-6M GPS Modules Data Sheet,” u-blox AG, 2015. [Online]. Available: https://www.u-blox.com.

[28] Espressif Systems, “ESP32 Technical Reference Manual,” Version 4.4, 2020. [Online]. Available: https://www.espressif.com.

[29] X. Zhang, F. Dovis, and C. Gioia, “Low-cost and low-complexity GNSS spoofing detection based on a rule-based model,” in *Proc. European Navigation Conf. (ENC)*, Warsaw, Poland, 2020, pp. 1–6.\

[30] B. Zhu, Y. Zhang, and K. Liu, “A web-based GNSS monitoring system for spoofing and jamming detection,” *Sensors*, vol. 20, no. 15, p. 4266, Jul. 2020.

[31] M. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS vulnerability to spoofing threats and a review of antispoofing techniques,” *Int. J. of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[32] IEEE P1937.1, “Standard for GNSS Spoofing and Jamming Detection and Mitigation,” IEEE Standards Association, 2021.

[33] Kementerian Komunikasi dan Informatika RI, “Permenkominfo No. 27 Tahun 2015 tentang Persyaratan Teknis Alat dan/atau Perangkat Telekomunikasi,” Jakarta, Indonesia.

[34] C. M. Bell, “Calculate distance, bearing and more between Latitude/Longitude points,” *Movable Type Scripts*, [Online]. Available: https://www.movable-type.co.uk/scripts/latlong.html. [Accessed: Jul. 23, 2025].

[35] ITU-T Recommendation Y.1541, "Network performance objectives for IP-based services," International Telecommunication Union, 2006.

[36] G. Ash, A. Morton, Y. El Mghazli, M. Dolly, P. Tarapore, and C. Dvorak, "Y.1541-QOSM: Model for Networks Using Y.1541 Quality-of-Service Classes," RFC 5976, Internet Engineering Task Force (IETF), 2010. Available: datatracker.ietf.org.