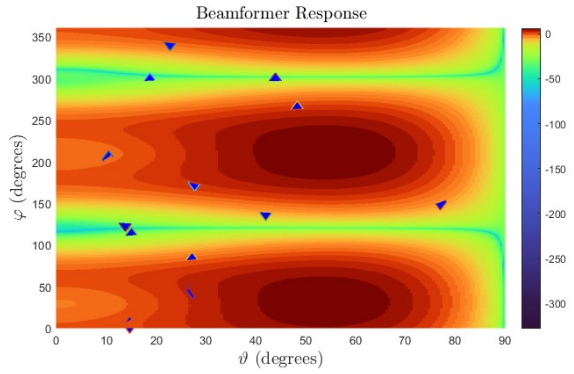

Fig. 6. Response of the beamformer without $\mathbf{T}$.

Fig. 5 reports a prominent attenuation denoted by the yellow and blue regions. It is also observed that such attenuation affects some satellites as well which are denoted by the blue triangles. A more detailed analysis can be performed by observing the azimuth and elevation profile shown in Fig. 6. Applying the Toeplitz matrix $\mathbf{T}$ with $\alpha = 1$, as shown in Fig. 7 and 8, results to a much lesser suppression of the satellite signals, except for the actual spoofing signal and the satellites with DOAs close to the spoofing signals. Note that the null in the direction of the spoofing signals is significantly widened by $\mathbf{T}$ with $\alpha = 1$ introducing robustness to DOA estimation errors by the CBF.

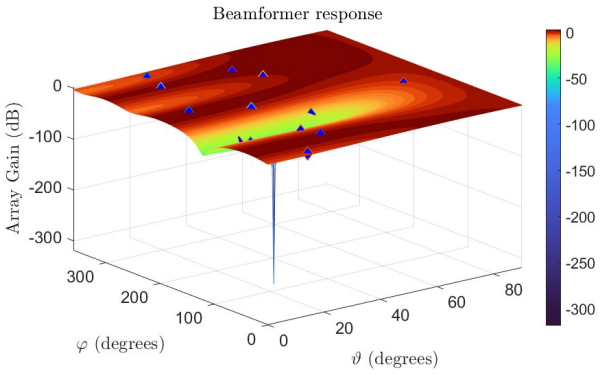

Fig. 7. Response of the beamformer with $\mathbf{T}$ in 3D.

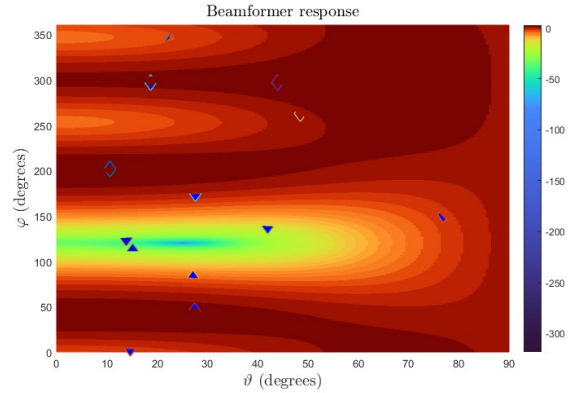

Fig. 8. Response of the beamformer with $\mathbf{T}$.

V. Conclusion

This work presented a pre-correlation spoofing mitigation approach based on a loose integration of an antenna array. The anti-spoofing subsystem detects spoofing attacks by DOA estimation of the spoofing signals and performs subsequent mitigation of the spoofing by adaptive spatial filtering. The CBF was introduced as a suitable DOA estimation algorithm. Simulation results show that for a SSR higher than 3 dB and $K > 200$ reasonable small RMSE for the azimuth and elevation angle of the spoofing signals can be achieved. The proposed beamformer achieves nulling the spoofing signals based on the DOA estimates provided by the CBF while trying to amplify as much as possible the GPS satellite signals. The proposed approach shows good performance in a realistic scenario and the beamformer manages to robustly mitigate a meaconing attack while providing GPS satellite signals with sufficient array gain to a state-of-the-art GNSS receiver.

This study, in addition to not adopting other specific anti-spoofing countermeasures, is different from most of the techniques that can be found in the literature. Most of the literature is based on post-correlation DOA estimation and requires knowledge of the spreading sequences of each satellite [6]. The only approach found in the literature that could also be applied in pre-correlation was presented in [9]. However, this proposed approach does not estimate the DOAs of the spoofing signals and its beamformer is based on post-correlation signal processing and knowledge of the DOAs of the received satellite signals.

References

[1] D. Egea-Roca, M. Arizabaleta-Diez, T. Pany, F. Antreich, J. A. López-Salcedo, M. Paonni, and G. Seco-Granados, "GNSS User Technology: State-of-the-Art and Future Trends," *IEEE Access*, vol. 10, pp. 39 939–39 968, 2022.

[2] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*.

[3] J. R. Merwe, X. Zubizarreta, I. Lukcin, A. Rugamer, and W. F. Fraunhofer, "Classification of spoofing attack types," in *European Navigation Conference (ENC), Proceedings*, 2018, pp. 91–99.

[4] D. L. da Silva, R. Machado, O. L. Coutinho, and F. Antreich, "A Soft-Kill Reinforcement Learning Counter Unmanned Aerial System (C-UAS) With Accelerated Training," *IEEE Access*, vol. 11, pp. 31 496–31 507, 2023.

[5] A. Iliopoulos, C. Enneking, O. G. Crespillo, T. Jost, M. Appel, and F. Antreich, "Robust GNSS Ranging in the Presence of Repeater Signals," in *Proceedings of ION GNSS+ 2017*, Portland, OR , U.S.A., September 2017.

[6] M. Appel, A. Iliopoulos, F. Fohlmeister, E. P. Marcos, M. Cuntz, A. Konovaltsev, F. Antreich, and M. Meurer, "Experimental validation of gnss repeater detection based on antenna arrays for maritime applications," *CEAS Space Journal*, pp. 7–19, 2018.

[7] D. Goward, "Ukraine attacks changed russian gps jamming," *GPSWorld*, 2022. [Online]. Available: https://www.gpsworld.com/ukraine-attacks-changed-russian-gps-jamming/

[8] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, "Direction-of-arrival assisted sequential spoofing detection and mitigation," in *2016 International Technical Meeting (ION ITM), Monterey, Proceedings*, 2016, pp. 25–28.

[9] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandan, and G. Lachapelle, "A gnss structural interference mitigation technique using antenna array processing," in *IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, Coruna, 2014, pp. 109–112.

[10] H. L. V. Trees, *Optimum Array Processing. Detection, Estimation and Modulation Theory, Part IV*. Wiley Interscience, 2002.