RF Attack Tables

Attack Type	Target Component	Wavelength	Distance	Required Power	Reference
Spoofing	Pressure sensor	655 - 800 MHz	0.2 m	Have not found exact value yet	[1]
Denial of Service	SPI or I2C channel between control unit and IMU	The exact value depends on board. Tested ranges are from 18 - 354 MHz	Real tests conducted @ 0.44 m and 2.4 m	The exact value depends on board. Arduino: ~30 dBm @ 2.4m Pixhawk4: 47x more power than Arduino DJI: 98x more power than Arduino	[2]
Spoofing	CCD Camera	Sweeping range from 20-100 MHz @ 0.1 MHz increments. Most cameras were vulnerable between 50-90 MHz	0 - 60 cm	Have not found exact value yet	[3]
Spoofing	LiDAR time-of-flight circuit	Sweeping range from 400-1000 MHz. Sensors found vulnerable @ 949.8 MHz, 960.9 MHz, and 977.4 MHz	2 m , 4 m, 6 m	maximum gain of 25 dB in real-world experiments	[4]

Attack Type	Target Component	Wavelength	Distance	Required Power	Reference
Spoofing	Power conversion system (AC-DC converter, DC-DC converter, current sensor, battery charger)	Frequency sweep from 50 MHz to 3 GHz @ 19 dBm power. DC-DC converters most vulnerable between 1-1.3 GHz AC-DC converters most vulnerable between 1.4-1.6 GHz Current sensors most vulnerable between 0.3-0.5 GHz Battery chargers most vulnerable between 0.7-0.9 GHz and 1.2-1.4 GHz	A battery charger was tested at range between 1-5 m. The authors note that the attack can be successful up to 2 m distance.	19 dBm	[5]

Bibliography

[1] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, Virtual Event Hong Kong: ACM, May 2021, pp. 901–915. doi: 10.1145/3433210.3453097.

[2] J. Jang, M. Cho, J. Kim, D. Kim, and Y. Kim, "Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels," in *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2023. doi: 10.14722/ndss.2023.24616.

[3] "GhostShot: Manipulating the Image of CCD Cameras with Electromagnetic Interference."

[4] S. H. V. Bhupathiraju, J. Sheldon, L. A. Bauer, V. Bindschaedler, T. Sugawara, and S. Rampazzi, "EMI-LiDAR: Uncovering Vulnerabilities of LiDAR Sensors in Autonomous Driving Setting

Using Electromagnetic Interference," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, in WiSec '23. New York, NY, USA: Association for Computing Machinery, Jun. 2023, pp. 329–340. doi: 10.1145/3558482.3590192.

[5] M. Szakály, S. Köhler, M. Strohmeier, and I. Martinovic, "Assault and Battery: Evaluating the Security of Power Conversion Systems Against Electromagnetic Injection Attacks," in *2024 Annual Computer Security Applications Conference (ACSAC)*, Dec. 2024, pp. 224–239. doi: 10.1109/ACSAC63791.2024.00033.