Towards Developing a Feasible End-to-End IEMI Attack Platform for Robotic Vehicles

Steven Thompson
Department of Computer Science & Engineering
Washington University in St. Louis
St. Louis, MO
steven.t@wustl.edu

I. Background and Motivation

A. Robotic Vehicle Security

Robotic Vehicles (RVs): Robotic vehicles like autonomous cars, delivery robots, and drones, are becoming increasingly integrated in human society. These systems depend on the cohesive integration of sensors, perception, planning, and control to operate safely in dynamic environments. Sensor suites for these vehicles typically include LiDAR and radar for ranging, cameras for scene understanding, GNSS and IMUs for localization, and numerous other sensors for health and state estimation. Since these vehicles act on sensed information to make real-time and safety-critical decisions, any disturbance of the physical sensing system can directly lead to hazardous outcomes such as collisions, loss of control, or mission failure [1].

Therefore, attacks against robotic vehicles differ from typical cyber attacks. With these systems, an adversary does not need to compromise software or computer networks to cause harm. Instead, an attacker can manipulate the physical sensing layer either by spoofing or jamming signals or by injecting voltages or currents via conducted or radiated EMI [1], [2]. Furthermore, because many sensing systems were optimized for cost and performance rather than adversarial robustness [2], attackers with access only to modest resources can sometimes produce substantial effects by targeting known weak points [3].

Intentional Electromagnetic Interference (IEMI): In an IEMI attack, an adversary radiates electromagnetic energy to induce currents and voltages inside vehicle electronics with goals ranging from temporary disruption of perception systems to destroying hardware. EMI attacks directly target sensing hardware and communication channels, which are common across many platforms. These attacks also tend to be stealthier than light, laser, or acoustic signal attacks, further making them an attractive mechanism to disrupt vehicle function [4].

These practical constraints shape the real-world feasibility of IEMI against robotic vehicles. Effective coupling depends on attacker antenna gain and accuracy, distance between the attacker and target, PCB design, and relative motion between attacker and vehicle [1], [2]. However, defenses such as shielded enclosures, cable routing and bonding, board-level filtering and decoupling, sensor fusion and redundancy, and on-sensor diagnostics raise the bar for successful exploitation by increasing required attack strength, tightening timing tolerances for synchronized spoofing, or enabling rapid detection [1], [2], [5]. Many reported lab demonstrations assume idealized aiming, short ranges, or specially configured test setups [6], [7]. Therefore, bridging the gap between lab to realistic operation requires models that include mobility and aiming error, mission-level impact, and coupling measurements for targeted components.

B. IEMI Attack Countermeasures

Robotic vehicles are exposed to an array of IEMI threats that exploit sensor physics rather than software bugs, and although many mitigation techniques have been proposed, no single defense is universally applicable. Practical protection requires context-aware tradeoffs among size, weight, cost, thermal buildup, sensing performance, and operational complexity [1], [2], [5].

Physical Countermeasures: Physical hardening appears to be the most direct way to reduce coupling of attacker signals to analog sensor paths. When applied correctly, shielding and board-level filtering can substantially attenuate injected signals [8]. Careful design of PCB layout can further reduce entry points for coupling [5], and dummy circuits can further mitigate the effects of malicious EMI signals [9]. However, these mitigations can reduce legitimate sensor functionality, complicate thermal and mechanical design, and can ultimately increase the system's mass, volume, and cost [1]. Moreover, gaps within the shielding are still exploitable by well-crafted directional attacks. [10]. Additionally, hardware redundancy and sensor diversity reduces single-point failures but increase weight, power draw, and system complexity. These mitigations push the problem into the sensor-fusion domain with the assumption that coordinated, multimodal attacks are not possible. However, as discussed by the authors of [1], the dominant sensor mechanism can still be exploited.

Digital Countermeasures: Digital defenses aim to detect or mitigate injected signals without changes to hardware. Statistical contamination metrics, anomaly detection, and sensor-level plausibility checks can identify attack signals and trigger fail-safe modes [8], [11], [12]. Software and compiler-directed approaches can add resilient processing that reduces attack impact without hardware modification [13]. However, attackers who learn detection metrics can craft waveforms that mimic legitimate signals. Additionally, detection thresholds that are tuned to avoid false positives in noisy operational environments may be ineffective against sophisiticated injections [1].

Assessing the real-world feasibility of systems using one or many of these countermeasures is crucial. Robotic vehicles are safety-critical machines and must be robust against any conceivable attack. Therefore, a high-fidelity attack simulation platform should integrate known countermeasures into its systems.

C. Assessing Feasibility of IEMI Attacks

Profiling an Adversary: The real-world feasibility of mission-critical attacks depends on attacker resources, aiming capability, environmental factors, and target configuration [3], [10]. These conditions limit generalization to field settings because many published experiments require precise accuracy, have only been demonstrated at short ranges, or do not consider end-to-end effects on the target cyber-physical system [6], [7], [14], [15]. To make feasibility claims actionable, researchers should adopt explicit attacker models that capture transmitter power, antenna gain, aiming accuracy, and mitigations taken by the target. Attack success metrics should include measurement perturbation magnitude and mission level probabilities of failure.

Developing High-Fidelity Attack Simulation and Validation: Some prior works [2], [6], [12] have seen success in simulating attacks on robotic vehicles. The authors of [2] developed RVProber to assign prerequisite conditions that make a variety of physical robotic vehicle attacks possible. To determine prerequisite parameters, RVProber uses a SITL simulator to model robotic vehicles under attack by injecting scheduling jitters and mutating attack parameters based on compromised sensor values. However, modeling attacks like this does not account for the complex electrical characteristics of sensors, integration with communication channels, countermeasures, or, as discussed in the previous section, attacker capabilities.

In [6], the authors attempt to demonstrate the feasibility of their proposed paralyzing drone attack using PX4 SITL simulation and analyzing how the attack propagates through a simulated drone's control logic. The simulation uses a fluctuating IMU data stream to mimic their attack. Using this attack method, the authors found that the simulated drone did not attempt to filter the compromised IMU values. Thus, the measurements were directly sent to the drone's attitude control algorithm. This result, however, is likely infeasible in the real-world because state estimation or countermeasures like sensor fusion algorithms are likely to prevent the corrupted IMU data from propagating through the control logic and crashing the drone.

The authors of [12] sought to develop an acoustic signal injection testbed using PX4 SITL and HITL, finding that sampling jitter, which originates from hardware imperfections, is a critical consideration for accurate attack modeling. The authors also attempted to capture drone movement in the SITL simulator by emulating resonant MEMs sensors under stationary and dynamic cases. Overall, this attack testbed, while more comprehensive than previously proposed ones, is still narrowly focused on MEMs accelerometers and gyroscopes. These sensors, while critical for localization, only make up a fraction of the sensors onboard drones. While sensors related to a drone's perception system, like LiDAR and cameras, may be unaffected by acoustic signal injection attacks, these sensors are vulnerable to IEMI attacks. Thus the effects of these attacks are crucial to capture in a comprehensive simulation platform.

From the above analysis, one can conclude that bridging the gap between controlled demonstrations and field reality requires an approach which combines high-fidelity simulation with hardware-in-the-loop (HITL) validation. To account for directionality, a practical IEMI attack simulator for robotic vehicles should combine radio wave propagation models with antenna pattern models. Moreover, detailed sensor models that capture sensor-specific behaviors along with EM coupling models are necessary to analyze how the EMI signals translate into currents and voltages on the target system's circuits and propagate through the system's perception and control stacks. Additionally, an attacker waveform library informed by documented attacks will let researchers exercise realitic threat scenarios and explore important parameter spaces such as power, frequency, attack accuracy, and relative motion between the attacker and target. This library should further be integrated with vehicle dynamics to analyze completely analyze the end-to-end outcome of a given attack.

References

[1] S. Xiao *et al.*, "SoK: Understanding the Fundamentals and Implications of Sensor Out-of-band Vulnerabilities." Aug. 2025. doi: 10.14722/ndss.2026.230450.

[2] H. Kim *et al.*, "A Systematic Study of Physical Sensor Attack Hardness," in *2024 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2024, pp. 2328–2347. doi: 10.1109/SP54263.2024.00143.

[3] 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.

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

[5] A. Z. Mohammed *et al.*, "The IEMI Effect: On the Efficacy of PCB-Level Countermeasures in Adversarial Environments," in *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&amp;P)*, Vienna, Austria: IEEE, Jul. 2024, pp. 361–380. doi: 10.1109/EuroSP60621.2024.00027.

[6] 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.

[7] Y. Son *et al.*, "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors."

[8] D. F. Kune *et al.*, "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," in *2013 IEEE Symposium on Security and Privacy*, May 2013, pp. 145–159. doi: 10.1109/SP.2013.20.

[9] 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.

[10] 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 Electromag-

netic 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.

[11] Y. Zhang and K. Rasmussen, "Detection of Electromagnetic Interference Attacks on Sensor Systems," in *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA: IEEE, May 2020, pp. 203–216. doi: 10.1109/SP40000.2020.00001.

[12] J. Jeong, D. Kim, J. Jang, J. Noh, C. Song, and Y. Kim, "Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof," in *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2023. doi: 10.14722/ndss.2023.24112.

[13] J. Choi, H. Joe, C. Jung, and J. Choi, "Defending Against EMI Attacks on Just-In-Time Checkpoint for Resilient Intermittent Systems," in *2024 57th IEEE/ACM International Symposium on Microarchitecture (MICRO)*, Nov. 2024, pp. 121–135. doi: 10.1109/MICRO61859.2024.00019.

[14] L. C. Lavau, M. Suhrke, and P. Knott, "Securing Temperature Measurements: An Assessment of Sensors' Vulnerability to IEMI," in *2023 International Symposium on Electromagnetic Compatibility – EMC Europe*, Sep. 2023, pp. 1–6. doi: 10.1109/EMCEurope57790.2023.10274337.

[15] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles," in *2020 IEEE Security and Privacy Workshops (SPW)*, May 2020, pp. 98–103. doi: 10.1109/SPW50608.2020.00032.