Introduction and Background

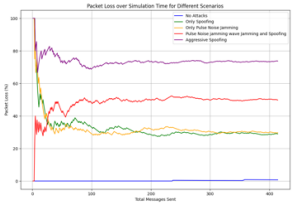
Automatic Dependent Surveillance–Broadcast (ADS-B) aids in broadcasting aircraft locations, velocity, and identification in contemporary air traffic management. But when adversaries use jamming assaults, ADS-B signals remain unencrypted and vulnerable to denial-of-service strikes. Real-world jammers can mislead a UAV or ground station by changing frequencies, sending pulses, or focusing energy on certain directions. They rarely just block communications at random. The current Drone-Sim code only employed one jamming probability, however references such as [1] demonstrate that more sophisticated jamming techniques, such as continuous wave, sweeping, pulsed, or directed, are riskier and require more accurate simulation.

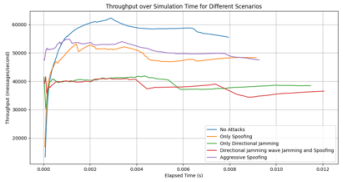
Implementation

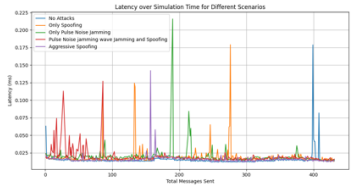
In our implementations we enhanced the basic jamming approach by adding four distinct modes. Continuous wave (CW) jamming keeps a steady noise floor that steadily reduces SNR. Sweeping or frequency-hopping jammers shift interference across bands in timed intervals, causing periodic outages. Pulsed noise sends short bursts of high-intensity interference, creating abrupt spikes in packet loss. Directional jamming focuses on a narrow beam or range angle, only affecting a drone if it's inside that cone. There are 4 different scripts or modules for each type of jammer. The various jammer types are imported in the main simulation anytime we want to run for a specific jammer type. For the case of the directional jammer an additional target position was added when the jammer object is initialized in the *n_scent_stat.py.*

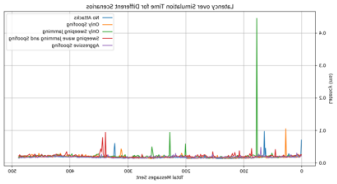
Results

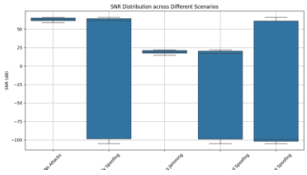
For the continuous wave jammer, packet loss begins moderately and remains stable, demonstrating a constant drop in SNR. For the sweeping jammer, interference patterns are cyclical: packet loss and latency peak whenever the jammer's active window occurs but dip during "off" periods. For the pulsed noise jammer, the percentage of packet loss starts very high at nearly 100% and eventually drops to around 35% after fewer than 100 messages, while some runs sustain roughly 50% packet loss and exhibit high peak latency of about 0.225 ms. The lowest throughput within 0.002 s was measured under the pulsed noise scenario combined with spoofing. One observation we made is that while results differ slightly across simulations, the main trends—like pulsed jamming's sharp spikes—remain consistent. Only a small sample of the resulting graphs are shown here; the rest are available in the GitHub repository.

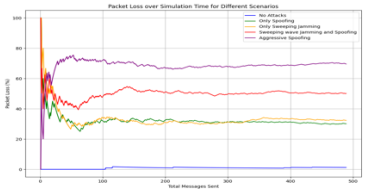












References

[1] M. Leonardi, E. Piracci, and G. Galati, “ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions,” in *2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*, Rome, Italy: IEEE, Sep. 2014, pp. 41–46. doi: 10.1109/TIWDC-ESAV.2014.6945445.