Introduction

In today's world, air traffic control and management depends much on Automatic Dependent Surveillance-Broadcast (ADS-B) to be able to broadcast aircraft positions, identification and velocity. Although it is widely used, it is still vulnerable to spoofing attacks there is lack of authentication and encryption in its messages. The main aim of this report is to make sure the already implement spoofer within the Drone-sim environment is adapted to be more realistic and also use gradual spoofing technique. This improved approach will steadily change the drone's reported ADS-B coordinates over time, rather than introducing abrupt "teleportation" jumps.
This kind of spoofing is motivated by the need to create a stealthier and more realistic attack as indicated multiple ADS-B security studies. For instance in [1] where the ease with which attackers can forge ADS-B data. By adding smaller stepwise offset, our goal is to extend the simplistic approach which is easily detected due to large and random changes to an advanced and stealthy spoof that cannot be easily identified through anomaly checks.

Background

ADS-B is a surveillance system that uses the 1090 MHz frequency spectrum to automatically broadcast the position, velocity, and identity of each aircraft. By receiving these signals, ground stations (and other aircraft) can get a real-time picture of air traffic. However, because regular ADS-B broadcasts lack encryption and authentication, spoofing—the fabrication of position/identification data—poses a serious risk. Fake ADS-B broadcasts can pose serious safety risks by deceiving nearby aircraft or ground controllers into misjudging locations, according to numerous studies [2].

Existing Implementation

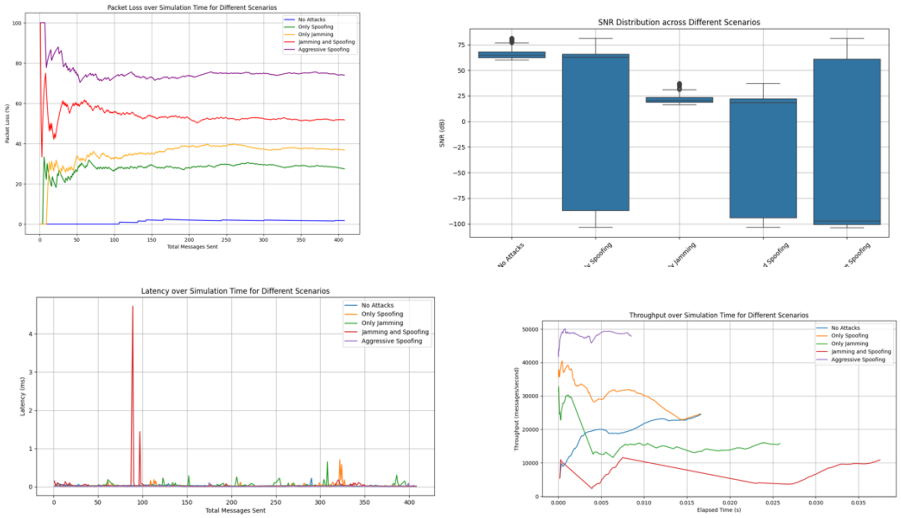
The existing spoofer in the original repo has some random offsets of latitude, longitudes and altitude, this is able to create some measure of data falsification but has sudden jumps which are easy to detect [1]. In real world scenarios an attacker is most likely to infer incremental changes to remain under the radar of anomaly-detection algorithms. As a result the original approach is considered unrealistic and forms the basics of the gradual spoofing enhancement

Channel Enhancements and Realism and Implementation of Gradual Spoofer

We modified the channel modules with free-space path loss, thermal noise computations, and time-based delays to better represent real-world ADS-B conditions and support our gradual spoofing strategy. In addition to environmental effects like receiver noise figures and probability-based message corruption, these modifications mimic the real physics of signal propagation . This makes our incremental spoof more plausible and difficult to identify since spoof ADS-B messages now experience more real attenuation and delay as they travel over the channel. A tighter match with the realistic conditions outlined in ADS-B security literature is ensured by the combination of modeling signal degradation and modest spoof offsets.
The gradual spoofer maintains constant offsets for latitude, longitude, and altitude, which results in a gradually drift in the drone's reported coordinates rather than abrupt jumps. It gradually increases these offsets whenever it decides to fake a message. Since the frequency of the offsets is decided by a chance factor and the amount of this drift is regulated by modest "step" values, not all messages are spoofs. In line with real research on ADS-B spoofing techniques, which indicates that minor alterations entail greater stealth risks than big, sudden ones, this progressive change makes the drone's trajectory more believable and harder to spot.

Results

In the no-attack baseline, throughput is steady, latency is low, SNR is high, and packet loss is negligible. Only spoofing causes significant packet loss and alters SNR while maintaining a relatively high throughput. Higher packet loss and delay are the results of more severe jamming-induced SNR drop. Combining jamming with spoofing causes the most disturbance, leading to a discernible drop in throughput and frequent spikes in packet loss. These results show that whereas jamming has a more negative effect on communication quality, spoofing mainly increases message volume and gradually alters reported statistics.



References

[1] M. TajDini, V. Sokolov, and P. Skladannyi, "Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio," in *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odesa, Ukraine: IEEE, Nov. 2021, pp. 1–5. doi: 10.1109/UkrMiCo52950.2021.9716665.

[2] H. A. Khan, H. Khan, S. Ghafoor, and M. A. Khan, "A Survey on Security of Automatic Dependent Surveillance -Broadcast (ADS-B) Protocol: Challenges, Potential Solutions and Future Directions," *IEEE Commun. Surv. Tutor.*, pp. 1–1, 2024, doi: 10.1109/COMST.2024.3513213.