CYSE 587 (Spring 2025)

Cyber Security System Engineering

Lab1: ADS-B Signal Spoofing and Jamming

Team Securetight

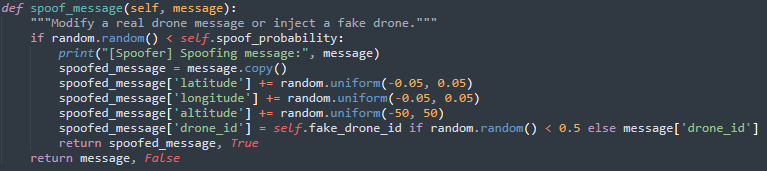
1. Tasks to perform

ADS-B spoofing involves broadcasting fake aircraft location signals to deceive aviation systems. Attackers can create nonexistent aircraft or deceive real aircraft positions, potentially causing dangerous confusion in air traffic management and increasing collision risks.

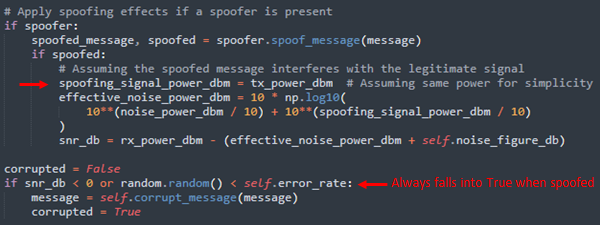
The task is to enhance the channel to be more realistic, implement gradual spoofing attack, and perform various jamming attacks in the given simulation source code.

1. Implementing Gradual Spoofing Attack

A gradual spoofing attack involves slowly and incrementally modifying aircraft position data over time, making the false data harder to detect compared to sudden position changes. The attacker gradually shifts reported coordinates to make the deception appear more natural and bypass anomaly detection. The given implementation performs the spoofing of position in a random way.



But before making some modifications to the function, we need to first change the way ADS-B channel works in the simulation. In *transmit* function in *ADSBChannel*, it assumes that spoofing signal power is same as that of normal transmission power(*tx\_power\_dbm*).



This is a bad approach in terms of “realistic” simulation because spoofers in real-world typically use lower power to avoid detection, i.e., having equal power would make the attack too obvious. Also, setting spoofing signal power same as transmission power causes signal-to-noise ratio(*snr\_db*) to fall into negative value, causing every spoofing messages to be classified as corrupted message. This should be avoided. So we decided to carefully calculate spoofing\_signal\_power\_dbm in such way that it does not overwhelm legitimate signal but strong enough to be injected.