**JAMMING REPORT**

**ABSTRACT**

As Cyber-physical systems (CPS) like drones become increasingly reliant on wireless communication, they face heightened vulnerability to jamming attacks that disrupt critical operations. This study examines the impact of four jamming techniques—Continuous Wave (CW) Jamming, Sweeping Jamming, Pulsed Noise Jamming, and Directional Jamming—on drone navigation and communication. By simulating these attacks on the ADS-B (Mode S Extended Squitter transponder - 1090ES) channel, this research evaluates their effectiveness and consequences. The findings highlight key vulnerabilities and emphasize the need for robust countermeasures to enhance UAV resilience in adversarial environments.

INTRODUCTION

**Unmanned Aerial Vehicles (UAVs)** rely on Automatic **Dependent Surveillance–Broadcast (ADS-B)** for real-time communication and navigation. However, jamming attacks pose a significant threat by disrupting these signals, leading to connection loss, operational failure, or course deviation. This research explores the impact of four distinct jamming techniques—**Continuous Wave, Sweeping, Pulsed Noise, and Directional Jamming**—within a simulated drone environment. By assessing their effects, this study highlights critical security vulnerabilities and underscores the need for advanced mitigation strategies to enhance UAV resilience in both civilian and defense applications.

**JAMMING CATEGORIES**

**1.Continuous Wave** **Jamming**

This jamming technique introduces a continuous noise signal that intensifies progressively over time. As the interference grows, drone communication becomes increasingly unstable, leading to signal degradation and potential loss of connectivity

**2. Sweeping Jamming**

This technique simulates a frequency-hopping jammer by generating periodic oscillations in signal interference. The fluctuating disruption leads to temporary communication losses, making drone tracking inconsistent and unreliable

**3. Pulsed Noise Jamming**

This method injects random bursts of interference into the communication channel, causing periodic disruptions. The unpredictable signal loss impacts real-time drone navigation, leading to momentary lapses in control and data transmission

**4.Directional Jamming**

This technique focuses jamming signals within a defined geographic zone, selectively disrupting drones operating in the affected area while leaving those outside its range unaffected

**IMPLEMENTATION**

Jamming mechanisms were integrated into the Drone-Sim project by modifying the Jammer class and associated simulation scripts, enabling realistic interference scenarios. The Jammer class, defined in jammer.py, simulates multiple types of jamming attacks, each executed through dedicated functions. These methods define how different jamming techniques impact UAV communication and navigation:

**Jammer.py** – Establishes jamming probability, noise intensity, and signal attenuation.

**Jammer\_continous\_wave.py** – Simulates Continuous Wave (CW) Jamming, where jamming strength gradually increases over time using frame / 100, leading to progressive signal degradation.

**Jammer\_sweeping.py** – Implements Sweeping Jamming, introducing periodic signal interference by applying a sinusoidal wave function sin(frame / 5), affecting jamming probability in cycles.

**Jammer\_Pulsed\_noises.py** – Models Pulsed Noise Jamming, creating short bursts of interference using sin(frame / 10), resulting in intermittent jamming that unpredictably disrupts connections.

**Jammer\_directional.py** – Executes Directional Jamming, selectively targeting drones within a specific geographic boundary. Interference is applied if distance <= radius, ensuring localized disruption.

## **RESULTS AND OBSERVATIONS**

1. **Latency Analysis**

**I.Continuous Jamming:** Leads to a steady increase latency, indicating prolonged interference in communication

**II.Frequency-Sweeping Jamming**: Causes noticeable fluctuations in latency, reflecting periodic disruptions in the signal.

**III.Intermittent Pulse Jamming**: Results in sporadic latency spikes, affecting real-time control mechanisms.

**IV.Directional Jamming**: Induces localized latency increases, affecting only specific regions within the transmission range.

**V.Progressive Jamming**: Demonstrates a continuous yet controlled rise in latency, aligned with increasing interference strength.

**2.Packet Loss Assessment**

**I.Continuous Jamming:** Leads to a progressive increase in packet loss with growing interference intensity.

**II.Sweeping Jamming:** Results in periodic packet loss, impacting communication reliability.

**III.Intermittent Pulse Jamming:** Causes irregular packet loss, leading to uncertainty in data transmission.

**IV.Directional Jamming**: Creates significant packet loss within affected zones but leaves other regions unaffected.

**V.Progressive Jamming:** Demonstrates a rising trend in packet loss as jamming effects accumulate over time.

**3. Signal-to-Noise Ratio (SNR) Analysis**

**I.Continuous Jamming:** Causes a sustained drop in SNR, signifying persistent interference.

**II.Sweeping Jamming**: Produces oscillating SNR levels, corresponding to periodic disturbances.

**III.Intermittent Pulse Jamming**: Results in fluctuating SNR with brief recovery periods.

**IV.Directional Jamming**: Reduces SNR selectively in affected zones while leaving other areas stable.

**V.Progressive Jamming**: Leads to a gradual decline in SNR, correlating with the increasing impact of interference.

**4. Throughput Evaluation**

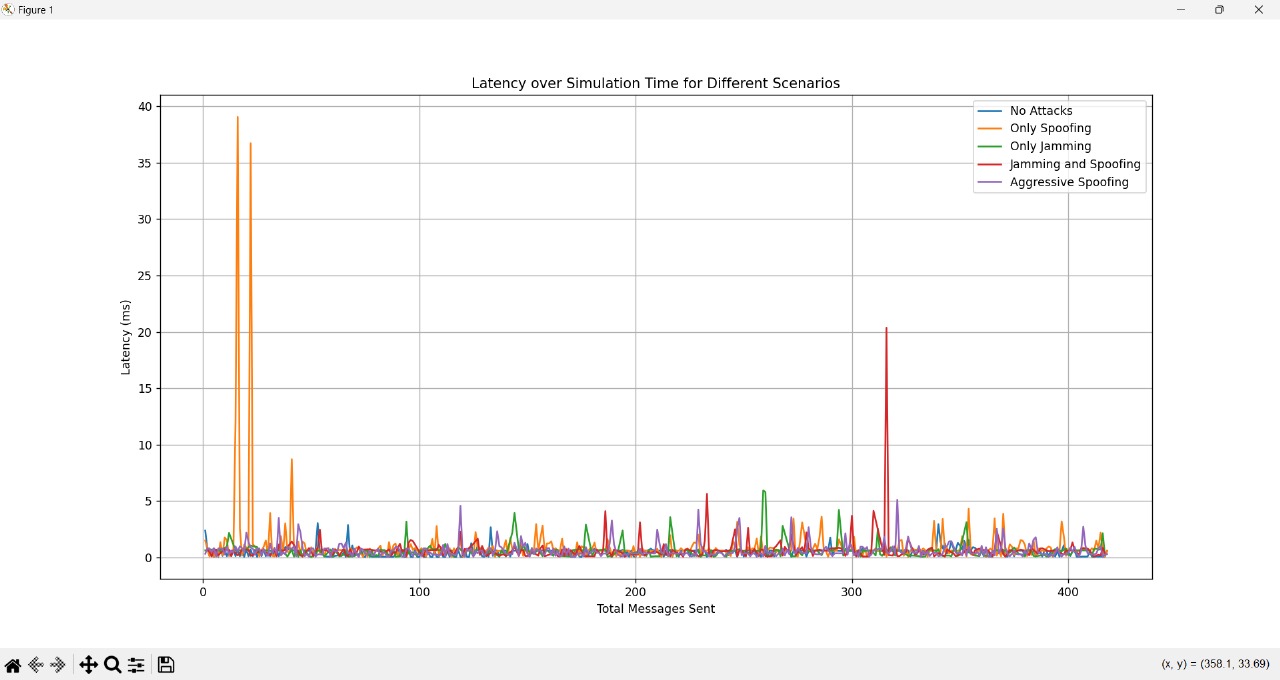
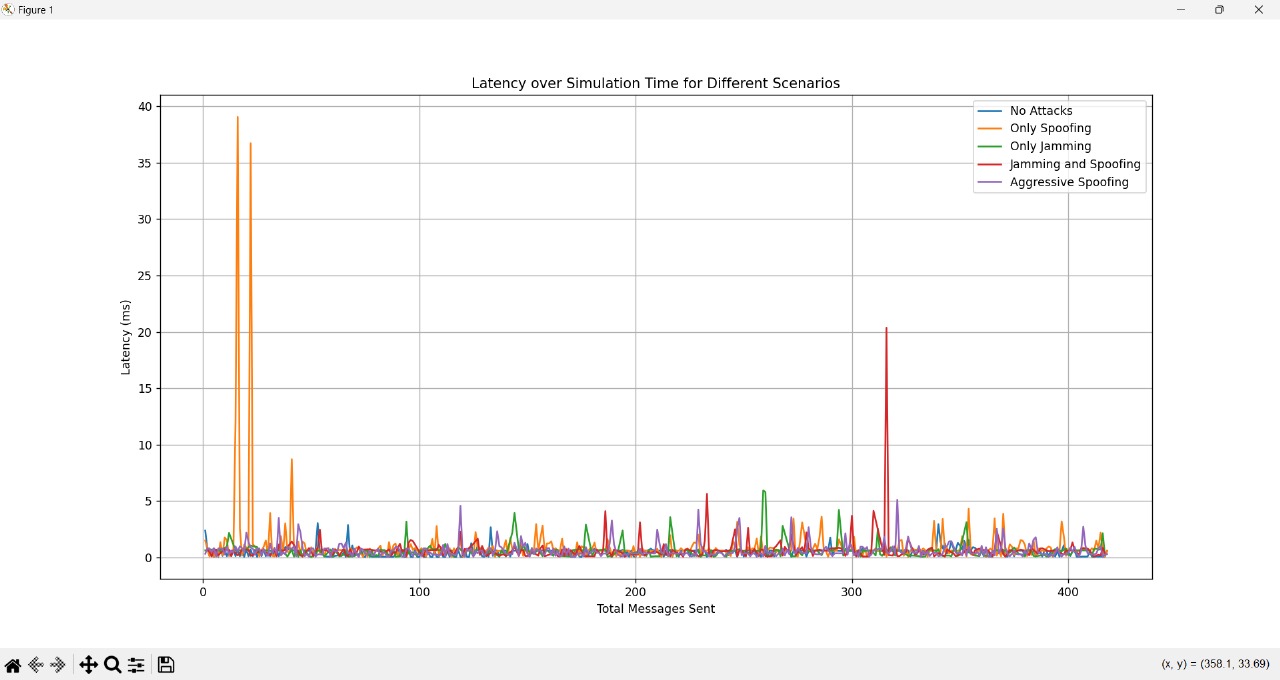
**I.Continuous Jamming**: Gradually diminishes throughput over time, limiting data transfer efficiency.

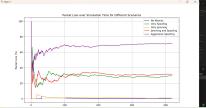
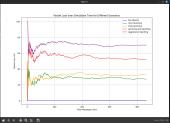
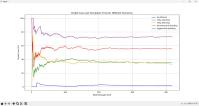
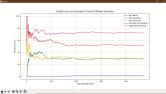
**II.Sweeping Jamming:** Causes variations in throughput, reflecting intermittent connectivity loss

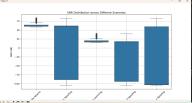
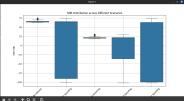
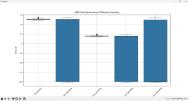
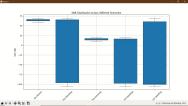
**III.Intermittent Pulse Jamming**: Induces short-lived drops in throughput, affecting stability.

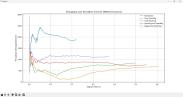
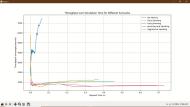
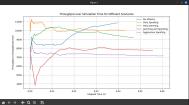
**IV.Directional Jamming:** Restricts throughput within targeted areas, leaving unaffected regions intact.

**V.Progressive Jamming:** Exhibits a steady throughput decline as interference escalates.









##### **CONCLUSION**

This study underscores the significant impact of jamming attacks on drone communication and navigation, with each technique exhibiting distinct interference patterns. Persistent jamming leads to a steady decline in system performance, while frequency-sweeping interference induces periodic disruptions. Intermittent pulsed interference creates sporadic connectivity failures, whereas targeted jamming affects only specific regions within the operational area. These vulnerabilities highlight the necessity for robust countermeasures, including adaptive frequency techniques, future research should prioritize real-time detection and dynamic mitigation strategies to strengthen drone security and operational reliability in contested environments.

##### **References**

[1] T. Multerer et al., "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," 2017 European Radar Conference (EURAD), Nuremberg, Germany, 2017, pp. 299-302

[2] H. Alamleh and N. Roy, "Manipulating GPS Signals to Determine the Launch Location of Drones in Rescue Mode," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422539.

1. Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities

and challenges," IEEE Communications Magazine, vol. 54, no. 5, pp. 36-42, 2016.

[4] J. Wang, Y. Chen, and T. Jiang, "Jamming-Resistant UAV Communication Networks Based on Deep Reinforcement Learning," IEEE Transactions on Wireless Communications, vol. 20, no. 5, pp. 3455-3469, 2021