SPOOFING REPORT

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Abstract  The Gradual Spoofer gradually modifies a drone’s position information over time, making the changes gradual enough to resemble natural drift, enabling it to elude detection. Unlike sudden spoofing, it imparts gradual distortions and can change the drone’s identity, making it harder to track. Configurable parameters support realistic attack simulations, such as standalone spoofing and spoofing-jamming scenarios. It aids in evaluating the robustness of Unmanned Aerial Vehicle(UAVs) to stealthy threats, thus facilitating the emergence of progressive detection and defensive and suppression for UAS security. **Keywords--**Gradual Spoofing, Drift Rate, Probability, Fake Drone ID, Message Manipulation.  Introduction  Gradual spoofing attack is a great and stealthy cyber threat against **Cyber-Physical Systems (CPS)**, especially **Unmanned Aerial Vehicles (UAV)**. Unlike sudden spoofing which leads to sharp and detectable changes in the least-squares estimate, gradual spoofing changes the position estimates over time and reduces the signals efficiency to detect and cope with it. UAVs must provide systems such as **Automatic Dependent Surveillance–Broadcast (ADS-B)**, which transmits real-time position data to **GCS (ground control stations)**, as a matter of higher priority. But slow and methodical spoofing can alter these data much more, which could change the trajectory inadvertently, or fake flight paths, leading to compromising missions or unsafe flying. Effect of Cumulative GPS **Spoofing** on the **Destination’s PDR**, **Latency**, and **MRA Accuracy** in a **Simulation of an Attack.** It further aims to assist in detection and mitigation measures for increasing UAV resilience through thorough characterization. **Gradual spoofing** - which refers to a gradual divergence of a UAV's position, velocity or time estimate, compared to the true values - is a major concern for the security and reliability of UAVs in civilian and military applications alike.  Characateristics of Spoofing   1. **Spoofer class:** Gradual spoofing with parameters:  probability of spoofing, fake drone identities, drift rates.   2. **Spoofed Drones:** An Unmanned Aerial Vehicle (UAV) where the positional state (latitude, longitude, altitude) is modified in small increments with realistic deviations.  3. **Original Message:** Real-time UAV telemetry data with positional data sent to the GCS (Ground Control Station).  4. **Spoofed Message:** Fake position data with drift and optional transponder data to spoof detection. |  |  | | 1. **Fake Drone ID:** This is a generated identifier which is used to pose as an alternative UAV in the spoofing operation.  5. **Drift Mechanism:** Shifts the positional values on the bleachers from the original values by some starting drift rate gradually. By doing so it will remove the wake created initially in flat mode and so avoid detection for a long period of time.   Implementation  The **gradual spoofer** was integrated into the system via the Spoofer class (defined in **spoofer.py**), designed to simulate a subtle spoofing attack by gradually manipulating the positional data (latitude, longitude, altitude) of UAVs over time. The focus of the implementation is on **incremental data distortion**, with key aspects including:  ****Gradual Spoofing:****   1. The introduction of a drift\_rate parameter, which determines the speed at which spoofed data deviates from the original values. 2. A spoofed\_drones dictionary is used to track and progressively alter the positional data of targeted drones. 3. Small, incremental adjustments are made to latitude, longitude, and altitude to ensure the attack remains realistic and undetectable.   ****Spoofing Logic**:**   1. The decision to spoof a message is based on a probabilistic approach utilizing the spoof\_probability parameter. 2. When a message is spoofed, incremental drift is applied to the positional data, and future drift values are adjusted accordingly.  |  |  |  | | --- | --- | --- | | **SPOOFING TYPE** | **EFFECT** | **IMPLEMENTATION** | | Gradual Spoofing | Subtle, incremental distortion of positional data | Drift rate (drift\_rate) applied to latitude, longitude, and altitude. |   Table 1: Gradual Spoofing Implementation and Effects |
| Results and Observations   1. **Latency Plot (latency\_plot.png)**: Illustrates how different spoofing methods affect the communication delays experienced by drones.   **2. Packet Loss (packet\_loss.png)**: Highlights the amount of data lost during transmission under the influence of spoofing attacks.  **3. SNR Box Plot (snr\_box\_plot.png)**: Shows how spoofing attacks cause fluctuations in the signal-to-noise ratio of the system.  **4. Throughput Plot (throughput\_plot.png)**: Depicts the effect of spoofing on the efficiency of data transmission in drone systems.  latency(after)packet_loss(after)snr_distribution(after)throughput(after) ****Latency Plot (latency\_plot.png)**:** Gradual spoofing leads to substantial communication delays, especially when coupled with jamming. This emphasizes the need for improved detection mechanisms to address latency issues in UAV systems.****2. Packet Loss (packet\_loss.png)**:** Gradual spoofing, particularly in its aggressive form, significantly contributes to packet loss, undermining the reliability of drone communications. This highlights the importance of implementing error correction and redundancy protocols.****3. SNR Box Plot (snr\_box\_plot.png)**:** While both jamming and gradual spoofing degrade SNR, jamming has a more pronounced effect. This emphasizes the need for adaptive signal processing techniques to sustain communication quality under adverse conditions.****4. Throughput Plot (throughput\_plot.png)**:** While gradual spoofing reduces throughput, jamming has a far greater impact. This underscores the need for optimized communication protocols to ensure reliable data transmission under attack conditions. Conclusion  This research highlights the significant impact of **gradual spoofing attacks** on drone communication and navigation. The effects vary based on the type and intensity of the spoofing employed. **Incremental spoofing** causes subtle and progressive distortions to positional data, making detection |  | |  | more challenging, whereas **aggressive spoofing** leads to abrupt changes, resulting in severe navigation errors. Additionally, spoofing degrades communication performance by lowering the Signal-to-Noise Ratio (SNR), increasing packet loss, and subsequently affecting latency and throughput. These findings emphasize the necessity for robust countermeasures, including **anomaly detection systems**, **machine learning-based spoofing detection**, **multi-sensor fusion techniques**, and **secure communication protocols** to strengthen UAV resilience. Future work should focus on developing real-time detection and mitigation methods to improve drone security and operational effectiveness in hostile environments.  References   1. M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1066-1087, 2015.   [2] K. Zeng, G. Gao, and T. Zhang, "GPS Spoofing and Countermeasures for UAVs: A Survey," IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no. 4, pp. 2718-2734, 2020.  [3] Y. Liu, P. Ning, and M. K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 808-819, 2011.  [4] J. Zhang, T. Zhang, and Y. Liu, "Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2192-2218, 2017.  [5] M. Li, S. Zhu, and Z. Han, "Spoofing and Anti-Spoofing Technologies for UAVs: A Comprehensive Review," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9575-9592, 2021. | |