PX4 autopilot hijacking strategy*

Jiwoo Suh, Jaehoon Kim, Weonji Choi, Dohyun Kim, Sangmin Woo, Hyunmin Ju, and Yongdae Kim

KAIST, Daejeon, South Korea
{suhjw0323, jaehoon.kim99, wec69, dohyunjk, wsm723, hyunmin.ju, yongdaek}@kaist.ac.kr

1 Introduction

Drones have become increasingly prevalent due to their affordability, lightweight design, and ease of deployment. However, this accessibility has also turned them into tools for destruction. As a result, the demand for effective countermeasures has surged. Various techniques have been proposed to address these threats, including corrupting IMU sensor data through electromagnetic interference (EMI) signals [3] and manipulating gyroscope and accelerometer values using acoustic resonance [4]. More direct approaches, such as deploying nets to physically capture drones mid-flight, have also been explored [5,6].

While these methods demonstrate innovation in combating the growing drone threat, they often overlook an essential factor: safety during the interception process. A poorly executed attempt to neutralize or hijack a drone can pose significant risks. A study published in TOPS (2019) by Noh proposed a novel approach to safely hijack drones by exploiting a fundamental vulnerability in GPS signals: their lack of encryption.

Noh's research took a black-box approach, focusing primarily on stationary commercial drones with limited insight into their internal systems. In contrast, I adopted a white-box approach, targeting one of the most widely used open-source flight controllers, PX4 Autopilot. This strategy allowed me to delve deeper into the system's architecture, enabling the development of a more generalized hijacking strategy with significantly improved controllability—even for moving drones. While my work on the SITL (Software-in-the-Loop) phase has been successfully completed, the next step involves testing this strategy in real-world environments to fully evaluate its effectiveness, which I have reserved for future work.

2 PX4 autopilot vulnerability and attack strategy

Analysis of the PX4 autopilot revealed a critical design vulnerability tied to its EKF algorithm. The EKF continuously monitors its variance to ensure reliable state estimation. When this variance exceeds a predefined threshold, the algorithm performs a hard reset, defaulting its estimates to the incoming GPS signal. An attacker could exploit this behavior by intentionally manipulating GPS signals to trigger frequent resets.

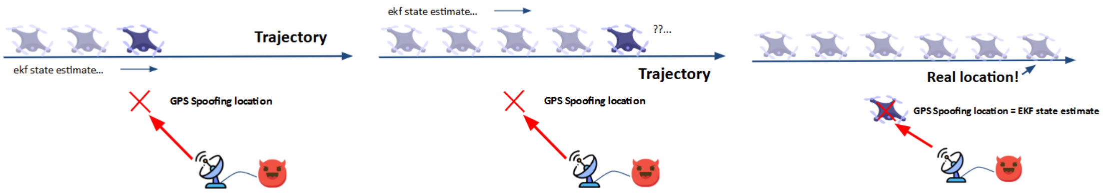
To exploit the vulnerabilities identified in the system, I analyzed the behavior of the PX4-Autopilot following an EKF reset. The analysis revealed that each time an EKF reset occurs, the flight controller attempts to steer the drone back to its original trajectory as quickly as possible.

As shown in Fig. 1-(a), the drone initially adheres to its planned trajectory despite the GPS spoofing. This resistance is due to the EKF algorithm, which cross-verifies GPS data with

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-51, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

IMU sensor readings, delaying the acceptance of the spoofed position. In Fig. 1-(b), the drone continues to follow its trajectory correctly, but the EKF error gradually increases over time, eventually reaching a critical threshold. Finally, in Fig. 1-(c), the EKF reset is triggered when the error exceeds this threshold, causing the drone to adjust its path toward the spoofed GPS position, significantly deviating from its intended trajectory.

Fig. 2 provides a detailed view of the positional adjustments following the EKF reset. The figure illustrates how the drone veers upward along the horizontal plane, as this is the most direct route to return to its original trajectory. These observations provide valuable insight into how the PX4 autopilot reacts under GPS spoofing, revealing exploitable behaviors that could inform more advanced strategies.



(a) Spoofing start. (b) Error accumulation. (c) EKF reset.

Figure 1: Drone trajectory response under GPS spoofing.

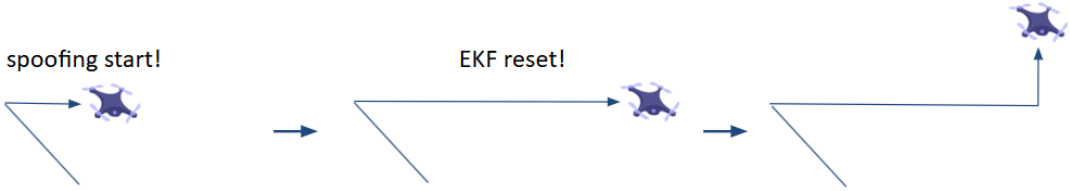


Figure 2: Real position of the drone during the spoofing process.

3 Evaluation

Using the strategies discussed in this study, I have confirmed that hijacking a PX4-autopilot using only GPS signals is not only feasible but also controllable. By carefully sequencing spoofing signals, the attacker can manipulate the drone's trajectory in a variety of ways, depending on their objective. Importantly, this method requires minimal prior knowledge of the drone's original trajectory. Once the spoofing process begins, the drone becomes indefinitely locked to the manipulated path.

References

[1] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, *Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing*, ACM Trans. on Privacy and Security (TOPS), vol. 22, no. 2, pp. 1–26, 2019.

[2] Y. Son, J. Noh, J. Choi, and Y. Kim, *GyrosFinger: Fingerprinting Drones for Location Tracking based on the Outputs of MEMS Gyroscopes*, ACM Trans. on Privacy and Security (TOPS), vol. 21, no. 2, pp. 1–25, 2018.

[3] J.-H. Jang, M. Cho, J. Kim, D. Kim, and Y. Kim, *Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels*, NDSS, 2023.

[4] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, *Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors*, Proc. 24th USENIX Security Symposium, pp. 881–896, 2015.