Preliminary Study on Cyberattack Impacts on Drone Flight Control

Donghan Yoo [a], Taewoo Tak [a], Taejin Kim[b], Seungyong Han[c*]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea*
[b]*Idaho National Laboratory, 1955 Fremont Ave, Idaho Falls, ID, United States*
[c]*Jeonbuk National University, 567 Baekje-daero, Deokjin-gu, Jeonju-si, Jeonbuk-do, Republic of Korea*
[*]*Corresponding author: hansy@jbnu.ac.kr*

***Keywords :** drone, cyberattack, drone flight control, anti-drone system

1. Introduction

The threat of illegal drones has been increased against critical national infrastructure, such as nuclear facilities and airports. For example, Nuclear Safety and Security Commission (NSSC) reported 13 cases of illegal drone activity near nuclear power plants between 2015 and 2019 [1]. In response, researches on anti-drone technologies have actively conducted to address this issue.

Anti-drone systems perform functions, like detection, identification, analysis, and neutralization of illegal drones. Ground-based neutralization equipment physically disables or destroys illegal drones, but the anti-drone systems take preemptive action without destroying them. It offers the advantages of having more response time and facilitating analysis of the attacker's information.

While the neutralization of illegal drones has been the focus of extensive research, it is also crucial to ensure protection against potential cyberattacks targeting these systems. Therefore, this paper investigates various types of cyberattack that could be launched against drone systems and analyzes their potential impact.

2. Identification of cyberattacks on drone systems

Vikas Sihag et al. systematically categorized the types of cyberattacks on drone systems [2]. In this section, the architecture of drone systems and cyberattacks targeting them are introduced based on this paper [2] and supplemented from several additional studies [3-6]. Furthermore, the cyberattacks on drone systems are classified from the perspective of their impacts on drone flight control.

2.1 Architecture of drone systems and cyberattacks targeting them

A drone system is basically composed of the drone itself, a ground control station (GCS), and a communication link and it also acquires location information from GPS and obtains aircraft traffic control information from ADS-B stations in Fig. 1 [2].

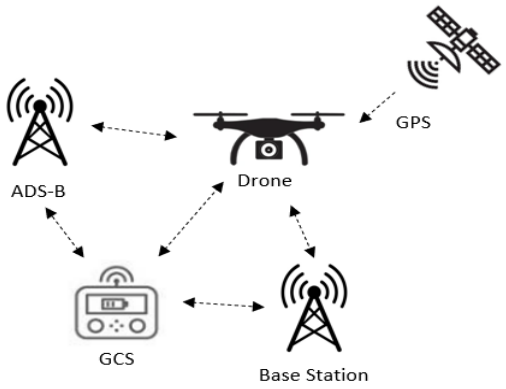

Fig. 1. Architecture of drone system [2]

Drone systems can be exposed to cyberattacks at various components, including the drone, communication network, base stations, ground control stations, and the supply chain. The types of cyberattacks for drone systems are presented in Table I [2-6].

Table I: Cyberattacks on drone system [2-6]

Impact	Cyberattacks on drone systems
Privacy	- Traffic Analysis and Network Stalking - Interception - Data Capturing and Forensics - Location Tracing
Integrity	- Data/Information Leakage - Access Control List Modifications - Man-In-Middle Attacks - Message Forgery
Confidentiality	- Identify Spoofing and Key exploitations - Unauthorized Access and Controls - Replay Attacks - Command Injection - False Data Injection - Eavesdropping
Availability	- Physical Attacks - DoS Attacks/DDoS Attacks - IMU Spoofing - GPS Spoofing - Channel Jamming - Routing Attacks
Trust	- Use of Fake Drones

2.2 Cyberattacks affecting drone flight control

The cyberattacks mentioned in Section 2.1 are classified into indirect and direct impacts on drone flight control.

The indirect impacts are categorized into "access compromise" caused by unauthorized access and manipulation, and "information leakage", which involves the exposure of sensitive drone-related data.

The direct impacts are classified into "direct flight control threats", which immediately affect drone control, and "service denial", which involves the disruption of communication.

Based on the above classification, the cyberattacks were categorized and listed in the Table II.

Table II: Classification of cyberattacks on drone control

Group	Cyberattacks on drone control
Access & Control Compromise	- Access Control List Modifications - Man-In-Middle Attacks - Message Forgery - Identify Spoofing and Key exploitations - Unauthorized Access and Controls - Use of Fake Drones
Information Leakage	- Data/Information Leakage - Traffic Analysis and Network Stalking - Interception - Data Capturing and Forensics - Location Tracing - Eavesdropping
Direct Flight Control Threats	- Replay Attacks - Command Injection - False Data Injection - IMU Spoofing - GPS Spoofing - Routing Attacks - Physical Attacks
Service Denial	- DoS Attacks/DDoS Attacks - Channel Jamming

3. Analysis of their potential impacts on drone flight control

The most common type of drone is the quadrotor, which consists of four individual rotors [7]. In this section, the control architecture of drones is introduced based on the quadrotor vehicle. Furthermore, the impact of various types of cyberattacks on the drone's control structure is analyzed.

3.1 Hierarchical control structure of drone systems

According to Mahony et al. (2012) [7], a hierarchical control approach is typically employed for drone control in Fig. 1, consisting of three levels:

1) High-level: position controller,
2) Mid-level: attitude controller, and
3) Low-level: motor controller.

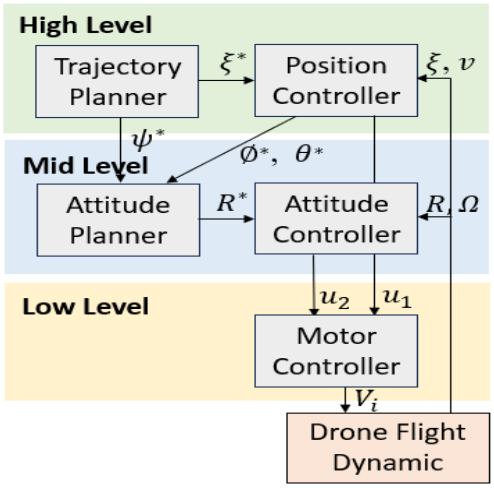

Fig. 2. Hierarchical control structure for drone control [7]

The trajectory planner provides desired position, denoted by ξ^*, and desired yaw angle, denoted by ψ^*, to the position controller and to the attitude planner respectively. The attitude planner generates the desired attitude, denoted by R^*, based on ψ^* from the trajectory planner and the desired roll and pitch from the positional controller, denoted by $\emptyset^*$ and θ^* respectively, and sends it to the attitude controller.

The position controller computes the desired thrust, denoted by u_1 based on the current position and the current linear velocity, denoted by ξ and v respectively, and sends it to the motor controller. The desired thrust can be obtained by projecting the position error and its derivatives and can be expressed as follows [7]:

$$u_1 = m\vec{b}_3^T(\ddot{\xi}^* + K_d(\dot{\xi}^* - \dot{\xi}) + K_p(\xi^* - \xi) + g\vec{a}_3)$$

- $\vec{a}_3$: $\vec{z}$ axis of an inertial frame of the airframe
- $\vec{b}_3$: $\vec{z}$ axis of a body fixed frame of the airframe
- K_p,K_d: Proportional and derivative gain matrices
- g: Gravity compensation vector

The attitude controller computes the desired torques, denoted by u_2 based on $R^*$from the attitude planner, and sends it to the motor controller. The desired torques can be obtained by calculating the error in rotations and can be expressed as follows [7]:

$$\tau = -K_R \cdot e_R - K_\Omega \cdot e_\Omega$$

- e_R: Error in rotations
- e_Ω: Error in angular velocity
- K_R,K_Ω: Positive definite gain matrices

The motor controller computes the applied motor voltage, denoted by V_i, based on u_1 from the positional controller and u_2 from the attitude controller. Since a motor voltage is simply proportional to a motor speed, most of quadrotor vehicles use a voltage control of the motors by high-frequency pulse width modulation (PWM). The motor voltage can be obtained by calculating the difference between the desired motor speed and the actual motor speed, denoted by ω_i^* and ω_i respectively, and compensating feed-forward term for steady-state PWM and can be expressed as follows [7]:

$$V_i = k(\omega_i^* - \omega_i) + V_{ff}(\omega_i^*)$$

- V_i: The applied motor voltage
- V_{ff}: The feed-forward term

The hierarchical control levels nested feedback loops allow for effective decoupling of translational and rotational dynamics, enabling stable and responsive drone flight control. In this section, a brief conceptual explanation about quadrotor control is provided along with simplified equations. For more detailed information, see reference [7].

3.2 Analysis of cyberattack impacts on drone flight control

The indirect impacts described in Section 2.2 are excluded in order to analyze cyberattacks that directly affect drone flight control. Among various direct impacts, “Direct Flight Control Threats” and “Service Denial” are intensively analyzed for their impacts on the hierarchical control levels of drone flight control. Exceptionally, “Physical Attacks” carried out using net guns, high-energy lasers, or other physical countermeasures are excluded, as they impact the drone physically rather than affecting its control system.

The results of the analysis are described as shown below and presented in Table III:

1) Replay Attack
- Attack: Replayed old sensor/command data
- Propagation Path: Position/Attitude Controller misinterprets as current state/command
- Impact: Repeating faulty or meaningless path

2) Command Attack
- Attack: Fake throttle/Yaw/Pitch/Roll command
- Propagation Path: Position/Attitude Controller receives fake commands
- Impact: Fly to wrong location or unintended move

3) False Data Attack
- Attack: Fake sensor data
- Propagation Path: Position/Attitude Controller receives fake commands
- Impact: Fly to wrong location or unintended move

4) IMU Spoofing Attack
- Attack: Tampered IMU sensor
- Propagation Path: Attitude controller receives tampered inputs
- Impact: Oscillation/Instability

5) Spoofing Attack
- Attack: Spoofed GPS signal
- Propagation Path: Position controller receives wrong GPS signals
- Impact: Incorrect path

6) Routing Attack
- Attack: Malicious routing table manipulation
- Propagation Path: Position/Attitude Controller receives delayed or wrong inputs
- Impact: Control or navigation disruption, Loss of control

7) DoS/DDoS Attacks
- Attack: Communication/CPU resource overload
- Propagation Path: Position and Attitude Controllers unable to process commands/sensor data
- Impact: Control loop failure

8) Channel Jamming
- Attack: Communication interference
- Propagation Path: Position/Attitude Controller receives no or delayed inputs
- Impact: Control or navigation disruption, Loss of control

Table III: Cyberattack impact on drone flight control

Type	Main Impact	Control Levels
Replay Attacks	- Replays of previously valid commands or data	- Mid - High
Command Injection	- Insertion of malicious commands - Altering control flow	- Mid - High
False Data Injection	- Tampering with sensor data to mislead control logic	- Mid - High
IMU Spoofing	- Manipulation of inertial measurement unit outputs	- Mid
GPS Spoofing	- Falsification of positional data	- High

Routing Attacks	- Modification or disruption of message routing	- Mid - High
DoS/ DDoS Attacks	- Overloading of system resources - Blocking communication	- Mid - High
Channel Jamming	- Interference with RF communication channels	- Mid - High

4. Conclusions

In this paper, we analyzed the types of cyberattacks against drone systems their impacts on the hierarchical control levels of drone flight control. The position and attitude controllers at high and mid levels are directly influenced by delayed and falsified inputs caused by cyberattacks, making them directly vulnerable cyberattacks, but there is no direct impact on the motor controller at low level. That is, by applying the position and attitude control algorithms that are resilient to cyberattacks, we strengthen cyber defense at the controller level. This study will be utilized to design a resilient control algorithm for drone flight system under cyberattacks against cyberattacks for drone flight control.

ACKNOWLEDGEMENTS

This work was supported by the Korea AeroSpace Administration (KASA) grant funded by the Korea government (No. RS-2021-NR056672)

REFERENCES

[1] Kim, J., Nuclear power plants 'vulnerable to drone attacks'. The Korea Times,https://www.koreatimes.co.kr/business/tech-science/20191006/nuclear-power-plants-vulnerable-to-drone-attacks, 2019.
[2] Sihag, Vikas, et al., Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones, Drones, vol 7, no. 7, 2023.
[3] Ashish Mahalle, et al., Cyber attacks on UAV networks: A comprehensive survey, Review of Computer Engineering Research, Conscientia Beam, vol. 11, no. 1, pp. 45-57, 2024.
[4] Anthony C. Tang, A Review on Cybersecurity Vulnerabilities for Urban Air Mobility, in AIAA SciTech Forum, 2021.
[5] F. Pasqualetti, et al., Attack detection and identification in cyber-physical systems, IEEE Transactions on Automatic Control, vol. 58, no. 11, pp.2715–2729, Nov. 2013.
[6] Shepard, D.P., et al., Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. GPS World, 2012.
[7] Mahony, R., Kumar, V., & Corke, P., Multirotor aerial vehicles: Modeling, estimation, and control, IEEE Robotics & Automation Magazine, vol. 19, no. 3, pp.20–32, 2012.