# Framework for Analyzing Abnormal Behavior of Real Drones through Simulation Parallelization

Ahn Sung Kyu
SysCore Laboratory
Seoul, Republic of Korea
yiimfn@gmail.com

Jung Hyelim
SysCore Laboratory
Seoul, Republic of Korea
hyello13@gmail.com

Ki-Woong Park*
Dept. of Information Security
Sejong University
Seoul, Republic of Korea
woongbak@sejong.ac.kr

**Abstract**

The use of unmanned vehicles has substantially increased in the military, security, logistics, and facility management fields. Among unmanned vehicles, drones are being increasingly commercialized. With the increasing use of drones, the likelihood of failure and abnormal behaviors increases owing to security threats targeting drones. To analyze an abnormal behavior, the triggering command can be injected to the drone, but the vehicle may be lost and the analysis is time consuming. Thus, we propose a framework to identify abnormal drone behavior through parallelization of drone simulation. The user can easily determine which command elicits an abnormal behavior in the drone. Hence, the framework may contribute to prevent abnormal behaviors in drone management while accelerating the analysis of such behaviors.

**Keywords**: IoT Security, Embedded Security, Drone, Unmmaned veihicles Security

## 1 Introduction

An unmanned vehicle may be defined as a vehicle directly controlled by a user or capable of performing a specific task automatically based on information collected from sensors. A drone is a type of unmanned aerial vehicle used for various purposes in fields such as military, security, logistics, agriculture, facility management, and media. As the usage scope of drones expands, various countries and institutions are planning infrastructure and devising relevant policies [1, 2]]. Software and hardware for drones are developing together with the drone market. However, with market expansion, abnormal behaviors owing to security threats to drones or malfunctioning firmware and sensors are becoming increasingly common. Examples of attacks targeting drones include intercepting control signals, stealing control by imitating signals to seize control, and jamming attacks that interfere with the drone signals [3]. Abnormal behaviors related to operation include overheating of batteries, failure of motors, and mechanical damage of blades. In addition to responding to abnormal behaviors, the causes of abnormal behaviors after attacks or breakdowns should be identified and analyzed. Thus, a method to analyze abnormal behaviors that may occur during drone operation and determine the cause of these behaviors must be devised. Analyzing the cause of an abnormal behavior using a real drone is time consuming because repetitive commands must be performed to reproduce physical damage to the drone.

Alternatively, abnormal behavior analysis using drone simulations has recently been adopted. A representative drone simulation environment includes software-in-the-loop (SIL ) simulation, software-based simulation, and hardware-in-the-loop (HIL) simulation involving both hardware and software components. Using this simulation environment eliminates the risk of damage to a real drone during abnormal behavior analysis. Further, the time for repetitive command executions can be greatly shortened by

The 6th International Symposium on Mobile Internet Security (MobiSec'22), December 15-17, 2022, 2021, Jeju Island, Republic of Korea
Article No. 1, pp. 1-7

*Corresponding Author

performing a high-speed simulation. However, even if simulation-based drone anomaly analysis is used, the drone commands should be manually provided to induce every abnormal behavior per simulation for subsequent analysis. In addition, it is difficult to execute various flight simulations simultaneously.

We propose a method to parallelize a simulation environment through containers for analysis of abnormal drone behaviors and operation data in real time, obtaining the corresponding drone flight scenario. Thus, command and environmental data can be retrieved when an abnormal behavior occurs during real drone operation, and the abnormal behavior can be easily analyzed. In addition, the time consumed for analyzing and verifying abnormal behaviors can be substantially shortened.

The remainder of this paper is structured as follows. Section 2 presents related work on drone analysis. Section 3 details the proposed framework for abnormal behavior analysis of drones based on parallel simulations. Section 4 presents the conclusions of this study.

## 2 Related Work

This section summarizes studies on abnormal behavior analysis of drones. First, an anomaly detection method that can be applied to robot systems, including drones, is presented. Then, existing research on simulation tools is analyzed.

### 2.1 Drone Anomaly Detection

Three main methods for detecting anomalies are employed in robotic systems including unmanned vehicles and drones: knowledge-, model-, and data-based anomaly detection [4]. The knowledge-based method determines abnormal behavior patterns by summarizing empirical data acquired from experts and determining the anomalies based on the extracted patterns. Although the abnormal behavior patterns are reliable, patterns for previously unknown cases are difficult to extract. In the model-based method, anomalies are detected by deriving the difference between the estimated value and measured value through a physical model of the target system. To improve the anomaly detection performance, deep knowledge of the system mechanism is required. For the data-based method, normal behavior is distinguished from abnormal behavior through learning of the system model based on collected data. In this method, the system can handle abnormal behavior patterns whose rules are not known in advance. This method has been used in various recent studies.

We propose a model-based framework for abnormal behavior analysis of drones. The knowledge required for model-based anomaly detection is obtained by comparing operation data generated through simulations with those acquired from real drones.

### 2.2 Abnormal Behavior Based on Drone Flight Simulation

MAYDAY[5] proposed a framework for identifying the causes of abnormal behaviors in real drones. To analyze the causes of abnormal behaviors, operation data were collected in real time during drone operation. Then, the drone control and program levels were analyzed. However, the gathered information is often insufficient to accurately identify the cause of abnormal behaviors in a drone. Hence, we use a drone simulation environment involving SIL and HIL simulations with an operation interface similar to that of a real drone and build a framework to collect and analyze massive data generated from simulated drones. Therefore, abnormal behaviors of a drone can be tracked. In addition to collecting diverse data generated from the drone and analyzing the collected data to detect abnormal behaviors, we enhance the verification system for the safety and stability of drone operation by determining the causes of abnormal behaviors.

In [6], a system configuration for building a virtual drone simulator was introduced. The requirements for building the simulator were discussed. The simulator was built, and its efficiency was verified. Furthermore, based on original model data used from real drones, an optimized mesh for real-time rendering was extracted. Textures, normal maps, and optical properties were provided for texture expression of the model data for realistic rendering. Through this simulator, SIL-based verification was added such that the dynamic characteristics of the virtual drone were reflected during motion. In addition, the error was corrected by comparing the posture and position of the simulated and actual drones through an optimization search algorithm based on the dynamic model. An optimized simulation environment based on a real drone was obtained for accurate simulation. However, this environment hindered real-time data collection and identification of the cause of abnormal behaviors in drone simulation by emphasizing the visualization-oriented simulation environment.

ETRI[7] developed an Octopus simulator based on Microsoft AirSim [8] released in 2018. Octopus creates a drone class that passes control inputs and sensor information to the Unreal Engine tool and calculates the drone dynamics through the PhysX physics engine. Only one simulation can be performed in existing drone simulators at a time owing to the high-quality 3D rendering in one computing system. Nevertheless, Octopus is equipped with a multi-drone simulation function by leveraging server–client distributed computing. The server collects and manages the entire simulation state in a distributed simulation, and the client performs the simulation tasks. Accordingly, a multi-drone simulation environment was implemented in [6]. However, as this system drives multiple drones in one simulation environment, the drones in the simulation can interfere with each other.

AnDrone [9]was used for virtualization through a Linux container architecture. The system multiplexed access from virtual drones to a full range of real drones via device containers including cameras and other sensors. In addition, an AnDrone prototype was implemented using the Raspberry Pi 3 board. The real-time Linux flight controller container supported existing drone flight software and geofencing flight control for virtual drones.

Inspired by the development in [10] , we propose a fuzzy learning algorithm based on a Markov chain for vehicle speed prediction. To update the Markov chain for speed prediction, real-time state transitions are observed using the latest available vehicle information. The algorithm performs state prediction by finding a certain area in a fuzzy method using the state transition table of the Markov chain.

# 3 Proposed Framework for Analysis of Abnormal Drone Behavior

## 3.1 Design

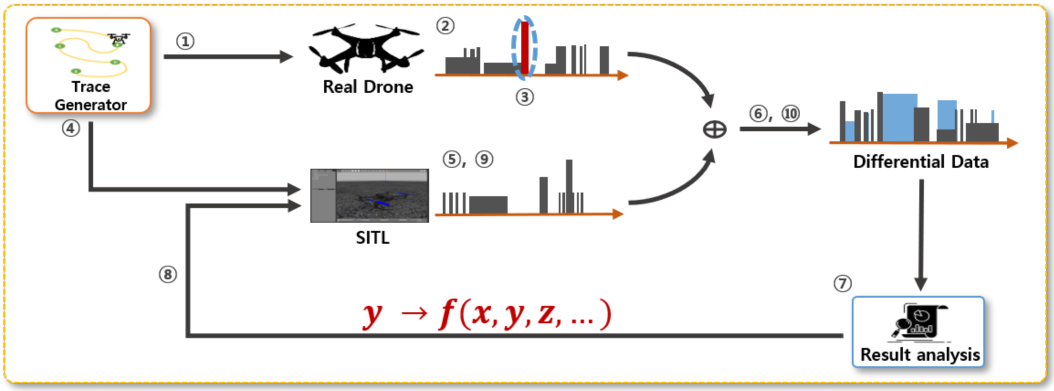

Figure 1: Framework diagram for identifying and analyzing drone abnormal behaviors.

We aim to compare the operation data of drones acquired from SIL and HIL simulations in an environment based on internal operation data generated during real drone operation to ultimately identify the cause of abnormal behaviors. [Figure 1] shows a diagram of the proposed framework in terms of data flow. First, mission data are allocated to a real drone and operation begins. The drone operation data are collected in real time. If an abnormal behavior occurs during operation, the timing of the abnormal behavior and operation data are divided into analysis targets. The first simulation-based drone operation proceeds with the same mission data assigned to the real drone. The data generated in this simulation-based drone operation environment are collected in real time. The data collected from the real and simulation environments are compared to obtain a delta measurement (i.e., differential data). The flight data given by the delta measurement indicate the similarity between the flight data from the real and simulated environments under the occurrence of an abnormal behavior. The mission data assigned to the simulated drone are modified in real time through similarity analysis. The adjusted mission data are allocated to another simulated drone for operation in a new simulation environment. Flight data from the drone in the new simulation environment are collected in real time. The delta measurement with respect to the real flight data is calculated in real time. The steps to determine the cause of the abnormal behavior in the drone are repeated. The maximum data similarity is obtained between the simulated and real drones when an abnormal behavior occurs.

To perform the abovementioned processes, the proposed framework consists of a simulation interface that drives the environments for SIL and HIL simulations, a data collection interface that collects operation data generated from simulations in real time, and a data storage system that categorizes and archives data. Furthermore, it consists of a module for creating the drone flight scenario and comparing the actual and simulation operation data based on stored data. This module also generates commands in real time and delivers them to the simulation environment. Hence, data generated from multiple simulations can be simultaneously stored, while delta measurement calculations can be performed using real operation data, and the similarities can be drawn to identify and analyze the causes of abnormal drone behaviors.

### 3.2 Simulation Interface

For the proposed drone simulation interface, SIL and HIL simulation environments are used, as shown in [Figure 2] . SIL simulations can be run in parallel based on the container environment, as illustrated in [Figure 3]. Drone operations in the simulation interface can be performed through high-speed parallel processing, and simulation operation data can be compared with real data through time synchronization.

### 3.3 Data Processing Gateway

Massive simulation operation data are generated from SIL and HIL simulations in real time when using high-speed parallel processing. For efficient data collection, we configure a high-speed data processing gateway, as illustrated in [Figure 3]. This environment collects data generated from SIL and HIL simulations and delivers it to the storage system.

### 3.4 Drone system operation data archiving system

A storage system is required for analysis and processing data generated by drones. We need to store unstructured data generated by drones. In addition, the requirements for real-time distributed/high-speed processing of massive drone data are described as follows:

- A message queue is required to collect data generated by drones.

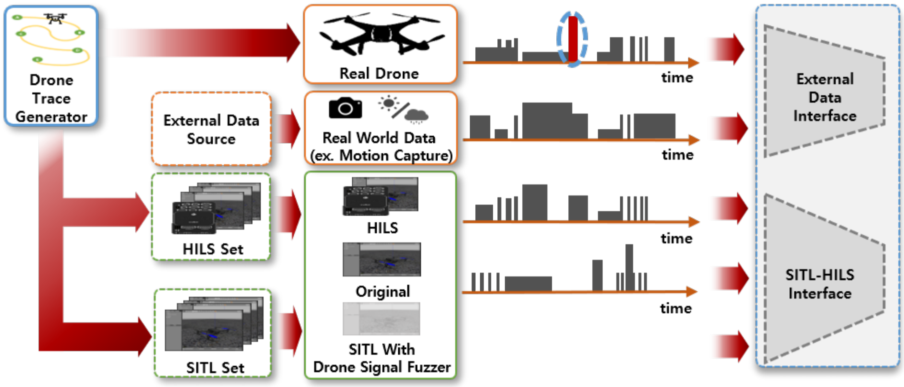

Figure 2: Drone simulation operation data processing.

- Distributed processing structure and management are required to collect unstructured data in addition to data generated by drones.
- Fast data processing is required to analyze abnormal behavior of drones.

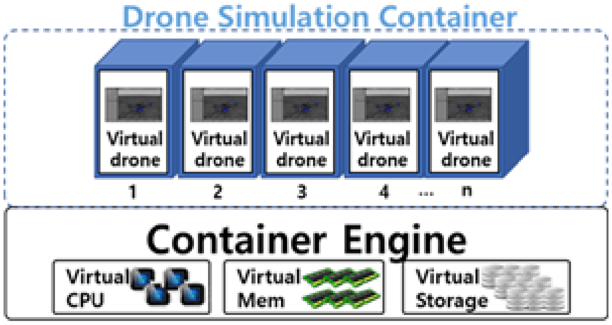

Figure 3: Parallelization of Drone Simulation.

The proposed module for distributed data processing classifies and stores a large amount of data generated during drone simulations in a container environment at high speed via in-memory processing. Simultaneously, the abnormal behavior of drones can be detected, and operation data can be quickly transferred to the module for analysis of the delta measurement. Simulation data are analyzed and processed at high speeds, as illustrated in [Figure 4]. The results of data processing allow to rapidly identify and analyze the causes of abnormal drone behaviors by running multiple simulations of the container environment with real-time varying flight mission parameters.

## 3.5 Module for Analysis of Delta Measurement

When analysis is performed using the proposed framework, the cause of an abnormal behavior can be identified by analyzing the input value of the drone simulation that leads to the highest similarity between the simulation and real operation data. Hence, it is possible to derive the cause of abnormal behavior in the real drone from the simulations. To this end, continuously changing drone commands should be delivered in the simulation environment, and we establish a module for analysis of the delta measurement. The module operates based on a Markov chain, analyzes the stored simulation operation data,

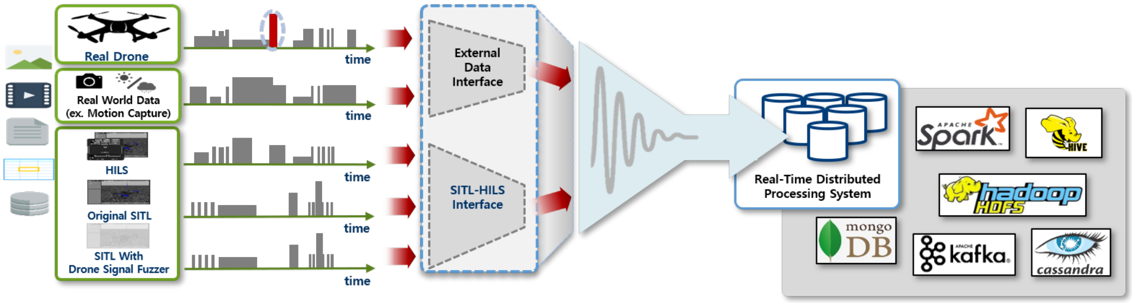

Figure 4: High-capacity drone data distribution/high-speed processing architecture.

and generates drone system control commands in real time. More simulation operation data from the simulation interface are obtained from increasing usage of the module, aiming to increase the similarity with the real data as shown in [Figure 5].

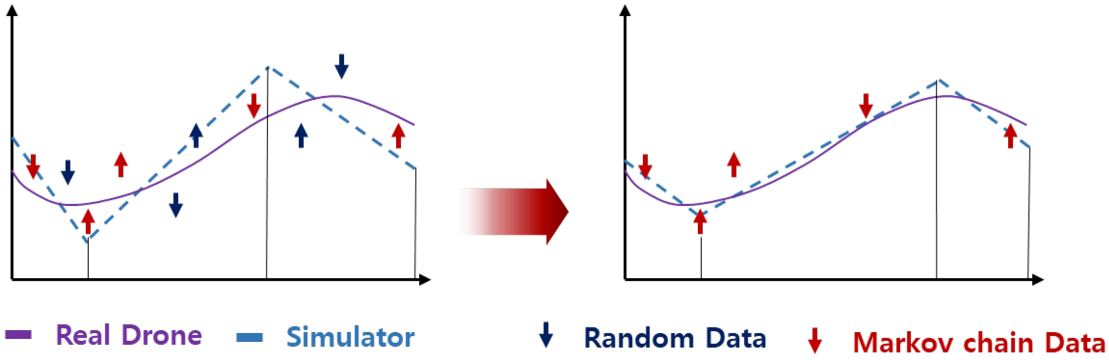

Figure 5: Creation of flight scenario based on Markov chain.

### 3.6 Abnormal Behavior Analysis

After completing the framework operation, the storage system can be accessed if the maximum matching rate between the actual and simulation operation data is obtained. The analysis module generates the command data and their related unstructured data. Then, the cause of an abnormal drone behavior can be identified and analyzed using the command data and complementary unstructured data during the period of abnormal behavior experienced by the real drone.

## 4 Conclusion

With the development of drone technology, their usage scope and types are expanding. Extensive drone usage increases the likelihood of abnormal behaviors owing to accidents or security threats. Solutions to prevent damage by analyzing the causes of abnormal behaviors are increasingly required. However, real-time data are difficult to obtain from a real drone, and even if an abnormal behavior occurs, its analysis is expensive. To solve this problem, we propose a framework for identifying and analyzing the causes of abnormal behavior in drones through parallelization of simulations. The proposed framework processes the drone simulation environment in parallel through a container, and delta measurements are used to determine the similarity between simulation and real drone operation data. The delta measurements allow to retrieve the drone commands and environmental data related to the occurrence of an abnormal behavior in the real drone. By synthesizing these data, the cause of the abnormal drone behavior can be unveiled. In future work, we plan to expand the proposed framework to generate and examine diverse simulation scenarios.

## Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) , South Korea(Project No. 001657941G0003072, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents, 50%), a National Research Foundation of Korea (NRF), South Korea grant funded by the Korean government (Project No. NRF-2020R1A2C4002737, 40%), and the ICT R&D Program of MSIT/IITP, South Korea (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, South Korea, 10%)

## References

[1] P. Kopardekar, J. Rios, T. Prevot, M. Johnson, Jaewoo J., and John E Robinson. Unmanned aircraft system traffic management (utm) concept of operations. In *AIAA Aviation and Aeronautics Forum (Aviation 2016)*, number ARC-E-DAA-TN32838, 2016.

[2] Haye Kesteloo. Amazon, boeing, ge and google to develop private unmanned traffic management (utm) system. *dronedj*.

[3] Li Wang, Yu Chen, Pu Wang, and Zheng Yan. Security threats and countermeasures of unmanned aerial vehicle communications. *IEEE Communications Standards Magazine*, 5(4):41–47, 2021.

[4] Eliahu Khalastchi and Meir Kalech. On fault detection and diagnosis in robotic systems. *ACM Computing Surveys (CSUR)*, 51(1):1–24, 2018.

[5] T.G Kim, C.H Kim, Altay Ozen, Fan Fei, Zhan Tu, Xiangyu Zhang, Xinyan Deng, Dave Jing Tian, and D.Y Xu. From control model to program: Investigating robotic aerial vehicle accidents with {MAYDAY}, 2020.

[6] Lee T.H. The Construction Method for Virtual Drone System. *THE JOURNAL OF KOREAN INSTITUTE OF NEXT GENERATION COMPUTING*, 13:124–131, 2017.

[7] S.J Lee, J.G Yang, and B.S Lee. Drone simulation technologies. *Electronics and Telecommunications Trends*, 35(4):81–90, 2020.

[8] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor. Airsim: High-fidelity visual and physical simulation for autonomous vehicles. In *Field and service robotics*, pages 621–635. Springer, 2018.

[9] Alexander Van't Hof and Jason Nieh. Androne: Virtual drone computing in the cloud. In *Proceedings of the Fourteenth EuroSys Conference 2019*, pages 1–16, 2019.

[10] Qingyu Zhang, Dimitar Filev, Steven Szwabowski, and Reza Langari. A real-time fuzzy learning algorithm for markov chain and its application on prediction of vehicle speed. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1–6. IEEE, 2019.