Requirements Derivation of Testbed of UAV Anomaly Detection

Ki-Wan Kang
SysCore Lab.
Sejong University
Seoul, South Korea
kkwan0226@gmail.com

SungKyung Kim
SysCore Lab.
Sejong University
Seoul, South Korea
Jotun9935@gmail.com

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

Abstract— **UAV(Unmanned Aerial Vehicle) uses a variety of components, including cameras, sensors and weapons, depending on the purpose. However, when the UAV is hijacked by an attacker, the UAV security problem should be dealt with importantly because various damages such as casualty, facility damage and personal information leakage can occur. Various algorithms have been developed and various studies have been conducted for successful detection of abnormal behavior of UAV. However, there are difficulties in experimenting with algorithms and anomaly detection methods due to the UAV characteristics. Therefore, in this paper, we derive test bed requirements for experiments of algorithms and studies for detection of abnormal symptoms of UAV.**

Keywords—UAV; Anomaly Detection; Testbed Design; Requirements Derivation

I. Introduction

The UAV industry is a convergence of high technology such as aviation, ICT (Information&Communication Technology), software, and sensors. Unlike the past, which was mainly used in the military industry, the UAV industry is used in various industries such as hobby, imaging, land survey, transportation, and agriculture [1].

UAV is expected to be widely used in various industries and has high growth potential and economic impact. However, it can be used as a means of personal information infringement, crimes, and assassinations for specific people in the process of UAV loss and facility damage, and information acquisition. It can also create national security-related threats, such as the destruction of key national facilities. [2].

As such various security threats occur, it is necessary to identify whether a security threat has occurred in the UAV when an abnormal behavior of the UAV occurs, and to analyze the abnormal behavior. Therefore, in this paper, the requirements of the test bed to collect and analyze various data of UAVs are derived.

The paper is organized as follows. Section 2 analyzes studies related to existing UAV testbeds. Section 3 suggests the need for testbed to accommodate various UAV anomaly detection researches. Section 4 derives section the testbed requirements to accommodate various uav anomaly detection researches. Finally, the conclusion of this paper is concluded in Section 5.

II. Related Works

In this paper, we classified three methods (redundancy-based detection, learning based detection, behavior rule-based detection) of detecting abnormal behavior of UAV.

Redundancy-based anomaly detection is a method of cross-checking output in real time by duplicating key system components. Fan Fei et al. proposed the detection of abnormal behavior by additionally equipped with a flight controller, which is a major component of UAV [3]. An additional flight controller was installed to read and inspect sensor data from existing driverless vehicle controllers to detect abnormal behavior. However, there is a disadvantage of low economical cost due to additional cost of replication.

Learning-based anomaly detection is a method of defining normal behaviors through learning and checking for violations. Alirea Abbaspour et al. developed the NNAS (Neural Network Adaptive Structure) algorithm that utilized the existing NN (Neural Network) detection algorithm [6]. However, there is a difficulty in obtaining training data for detecting abnormality of UAV.

Behavior rule-based anomaly detection is a method of defining anomalies in a program and detecting anomalies by observing state transitions. Robert Mitchell et al. proposed anomaly detection based on rules that regulate the normal operation of a sensor or actuator in a UAV [9]. When an actions changes, it defines the anomaly through the probability that can occur for the next action. However, when there is continuous data, there is a limitation that it is difficult to clearly define the normal operation.

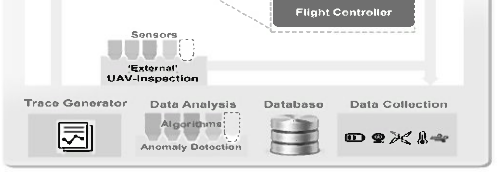

Fig. 1. Overview of UAV Anomaly Detection Testbed Platform

*: Corresponding author

TABLE I. Sensor Data Used for UAV Anomaly Detection Researches

Methods	Related Research	Sensors							
		Gyro	*Accel*	*Magn*	*Pos*	*Velocity*	*Thrust*	*Ctr-sign*	*Actu*
Redundancy Based Detection	[3]	√	√	√	√		√		√
	[4]	√	√	√	√	√	√		√
	[5]	√	√	√	√				√
Learning Based Detection	[6]	√	√	√					
	[7]								√
Behavior Rule Based Detection	[8]		√		√	√			
	[9]	√	√	√	√		√	√	
	[10]	√	√	√	√	√	√		

III. Necessity of UAV Anomaly Detection Testbed

UAV has various risks and threats, so if an abnormality is detected in the UAV, the UAV should be equipped with a security system that can identify the source of the security threat and respond to the abnormality on its own. However, UAV has the characteristics of Cyber-Physics system that combines both software and physical elements, so it is difficult to consider software and physical factors in order to derive the cause of abnormal behavior. Therefore, in order to detect abnormal symptoms of the UAV, a process of complex observation of factors influencing the state change of the UAV including sensor data is required.

This section suggests the three necessity for UAV anomaly detection testbed. First, various studies exist for the detection of anomalies in UAV, but cannot detect various anomalies through one algorithm. However, it is possible to detect anomalies that are superior to one algorithm by using various algorithms together. Second, UAV is used by attaching various sensors and weapons according to the situation. Due to the high extensibility of this UAV, various abnormal behaviors can occur. Therefore, various data generated during UAV operation should be collected to be used for abnormal detection. Third, UAV has the characteristics of Cyber-Physics system that combines both software and physical factors, so it is difficult to consider software and physical factors in order to derive the cause of abnormal behavior. However, if the UAV abnormality can be reproduced, it may be easier to analyze the UAV abnormal behavior.

IV. Derivation of Testbed Requirements for Detection of Abnormal of UAV

This section derives testbed requirements for UAV anomaly detection analysis.

A. Data Collection

UAV is used by attaching various sensors and weapons according to the situation. Sensors required for operation and weapons for attack can be attached, but pluggable modules can be attached for abnormal detection. The existing UAV anomaly detection studies mainly analyze the sensing data generated inside the UAV. However, abnormal behavior may occur due to additional sensors and weapons attached. Therefore, it is necessary to collect not only internal sensor data of UAV but also data that cannot be collected internally such as battery temperature through pluggable data collection module.

B. Data Archive

Table.1 shows that the data used in the existing UAV anomaly detection studies are different. In addition, due to the extensibility of the UAV, a wide variety of data are generated. Therefore, this paper requires a database that can utilize various data generated when operating UAV. In addition, the database needs to be designed to ensure extensibility and flexibility by considering the analyst's needs and the characteristics of the data.

C. Trace Generator

There is a limitation in applying the method used in the existing software fuzzing because it is directly affected by the hardware sensing result. Therefore, in this paper, based on the software fuzzing technology, randomly generated state values that are difficult to occur during the normal operation of the UAV are injected into the UAV, and the abnormal state of the UAV is detected by continuously storing and monitoring the state change of the UAV.

In addition, since it is a UAV that analyzes and operates various factors, it is difficult to reproduce abnormal behavior. However, through the Trace Generator, the same abnormal behavior can be reproduced by making various factors the same.

D. Data Analysis and Visualization

In order to analyze the various data collected to detect abnormal behavior of the UAV, it is necessary to support analysis and visualization tools according to the analyst's needs.

V. Conclusion

In this paper, we present the necessity and requirements of the testbed that can collect and analyze various data generated in the operation of unmanned mobile vehicle to identify the abnormal behavior of UAV. Through the researches related to the excellent scalability of UAV and the existing UAV anomaly detection, we could confirm the diversity of data that can be used for the detection of the UAV abnormal behavior. Flexible testbeds are essential to take advantage of the diverse data generated by unmanned vehicle operations. To this end, in this paper, four items (data collection, data storage, data injection, data analysis and visualization) were derived as requirements of testbed for identifying abnormal behavior of UAV. Subsequent studies will conduct a study of designing the testbed based on the requirements derived.

Acknowledgment

This work was supported by the Institute for Information & Communications Technology Promotion (IITP) of the Korea government (MSIT) (Grant no. 2019-0-00426)

References

[1] Taegin Chang, "Reglatory Environment and Structural Change of UAV Industry", Journal of Aerospace System Engineering, Vol. 9, No 3, pp. 17-25, 2015.

[2] Kyung-Hwan Lee, Gab-Sang Ryu, "Research for Improving Vulnerability of Unmanned Aerial Vehicles", Smart Media Journal, Vol.7, No.3, pp. 64-71, 2018.

[3] Fan Fei, Zhan Tu, Ruikun Yu, Taegyu Kim, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng, "Cross-Layer Retrofitting of UAVs Against Cyber-Physical Attacks", IEEE International Conference on Robotics and Automation(ICRA), 2018.

[4] Choi, Hongjun, et al. "Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach", ACM SIGSAC Conference on Computer and Communications Security, pp. 801-816, 2018.

[5] G. Heredia, A. Ollero, M. Bejar, and R. Mahtani, "Sensor and Actuator Fault Detection in Small Autonomous Helicopters", Mechatronics Vol.18, No.2, pp. 90-99, 2008.

[6] Alireza Abbaspour, Kang K Yen, Shirin Noei, and Arman Sargolzaei, "Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network", Procedia computer science 95, pp. 193–200, 2016.

[7] Qikun Shen, Bin Jiang, Peng Shi, and Cheng-Chew Lim, "Novel Neural Networks-based Fault Tolerant Control Scheme with Fault Alarm", IEEE transactions on cybernetics, Vol.44, No.11, pp. 2190–2201, 2014.

[8] Robert Mitchell and Ray Chen, "Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications" IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol.44, No.5, pp. 593–604, 2014.

[9] Stanley Bak, Karthik Manamcheri, Sayan Mitra, and Marco Caccamo, "Sandboxing Controllers for Cyber-Physical Systems", IEEE/ACM Second International Conference on Cyber-Physical Systems, pp. 3–12, 2011.

[10] Balachandran, S, and Atkins, E, "Markov Decision Process Framework for Flight Safety Assessment and Management" Journal of Guidance, Control, and Dynamics, Vol.40, No.4, pp. 817-830, 2016.