AIAA SciTech Forum
January 3-7, 2022, San Diego, CA & Virtual
AIAA SCITECH 2022 Forum

10.2514/6.2022-0969

Towards Intelligent Security for Unmanned Aerial Vehicles: A Taxonomy of Attacks, Faults, and Detection Mechanisms

Lijing Zhai[1], Aris Kanellopoulos[1], Filippos Fotiadis[1], and Kyriakos G. Vamvoudakis [2]
The Daniel Guggenheim School of Aerospace Engineering, Georgia Institute of Technology, 270 Ferst Dr, Atlanta, GA 30313

Jérôme Hugues[3]
Carnegie Mellon University/Software Engineering Institute, 4500 Fifth Avenue Pittsburgh, PA 15213-2612

In this extended paper we provide two mappings using a fault taxonomy as a pivot: first, we map attacks or faults scenarios to a class of well-known error types. Then, we categorize detection mechanisms by their ability to detect error types. By combining those two tables, a designer can confidently select a detection mechanism for identified attack or fault scenarios.

I. Introduction

UNMANNED Aerial Vehicles (UAV) are becoming increasingly integrated in various facets of civilian life [1]. UAVs have also become more susceptible to both stochastic faults – stemming from faults occurring on the different components comprising the system – and to malicious attacks who compromise either the physical components (sensors, actuators, airframe, etc.) or the software coordinating their operation. Different research communities have been investigating the causes and effects of faults that occur in UAVs employing a plethora of tools, often incompatible with each other. Our objective is to identify the core properties and elements of these approaches in order to decompose them based on those. This will enable designers of UAV systems to take into account all the different results on faults and the associated detection techniques via an integrated algorithmic approach.

The issue of faults and attacks on UAVs has been studied in the literature, both in terms of detection and mitigation. Regarding detection, in [2], the authors provide experimental results for applying a model-based residual generation algorithm and a data-driven anomaly detection algorithm for a small UAV. The work of [3] combine a neuro-fuzzy inference system and an online data-training mechanism in order to detect navigation sensor faults on UAVs, and verify their results through experiments. In a similar manner, neural networks are trained using an extended Kalman filter in [4], and are employed for the detection of either sensor or actuator UAV faults. But the problem of detection and mitigation of UAV faults and attacks can also be specialized to certain UAV types. For example, in [5], the authors propose a method capable of both diagnosing and mitigating control surface failures for the aeroonde UAV. The authors of [6] propose a robust fault detection and diagnosis scheme to estimate actuator faults for a quadrotor UAV with the influence of external disturbances by decoupling an adaptive augmented state Kalman filter into three parallel sub-filters.

A system designer needs a vocabulary to capture those scenarios and then detection mechanisms to report and eventually mitigate them. This is the goal of attack or error taxonomies. The authors in [7] discuss an attack taxonomy on Supervisory Control and Data Acquisition (SCADA) systems. In [8], the authors consider an attack taxonomy on general cyber-physical systems and attacks against them that cross the digital-physical boundary. The work of [9] propose an abstract fault taxonomy to formally express the previous scenarios. A taxonomy of threats, vulnerabilities, and attacks for smart cars are examined from a CPS perspective [10]. The authors of [11] introduce taxonomy of attacks of agent-based smart grids with the introduction of the structure of space-time and information flow direction, security feature, and cyber-physical causality. In this paper, we claim that these taxonomies are insufficient to assist engineers in designing mitigation strategies. Indeed, they have to select a fault or attack detection mechanism sufficient for a collection of scenarios.

Contributions: We propose a decision process made of two elements: first, a mapping from fault or attack scenarios to abstract error types. Second, a survey of detection mechanisms based on the abstract error types they help detecting. By combining both elements, designers can select with confidence a detection mechanism that protects the system.

[1]Graduate Student, The Daniel Guggenheim School of Aerospace Engineering, Georgia Institute of Technology.
[2]Assistant Professor, The Daniel Guggenheim School of Aerospace Engineering, Georgia Institute of Technology.
[3]Senior Researcher, Carnegie Mellon University/Software Engineering Institute.

Outline: In the following, we provide a sketch of this approach that will be the core of an extended version. First, we present a survey of faults and attacks on UAVs in plain text. Subsequently, we employ the taxonomy from [9] to categorize the attacks based on their properties. We, then, present intrusion detection mechanisms that operate based on different principles. We connect them to the same taxonomy as to the types of properties they can manage. Finally, we discuss how these two classifications can be used in tandem to construct a map between potential attack scenarios and the available intrusion detection mechanisms. In this paper, we showcase the use of the process via an example situation. The final version of the paper will contain a more detailed discussion on all the different attack scenarios.

II. Attack Taxonomy

In this section, we discuss the emergence of faults and attacks on UAVs and we characterize them with respect to properties found in the taxonomy introduced in [9]. To classify the attacks on UAVs, we present a list of component compromises, focusing on those that reside at the intersection of the physical and the digital realms. The following list is far from comprehensive but it is adequate in representing the major qualities that describe the effects of those attacks to the system. We present the list considering attacks and faults on sensing, actuating and communication components, as well as more complex attacks targeting multiple elements so as to cause system-wide errors.

A. Attacks in UAVs

Sensor attacks and faults: Those types of errors are caused by discrepancies between the actual value of a variable of interest in the environment and the value that is received by the UAV.

- *Physical jamming/Outage:* Those attacks require the adversary to be able to compromise the information flow in the physical realm, e.g., in the medium underlying a wireless sensor network. An agent aiming to launch such attacks should have the necessary equipment that will allow them to either inject a physical signal to a wireless transmission, or have direct physical access to the sensing devices and components [12].
- *Replay attacks:* In order for a malicious agent to launch such an attack, initially they need to obtain access to the data transmitted by the sensor. Given this access, they are able to record the information transmitted over a window of time where the system operates normally. Then, the attacker leverages this recording by injecting it back into the information flow of the sensing components, and thus deceives the operators and the rest of the UAV components into believing that the system maintains its nominal operation [13].
- *Failure/Data drops:* Those errors can be of either stochastic or malicious nature. Although the mechanisms behind the causes of data drops may vary, the core effect of those errors is the loss of packages of information that is either gathered by the sensors or transmitted to the rest of the system components [14].
- *Spoofing (man-in-the-middle attacks):* An attacker is able to launch a spoofing attack to a sensor system by deceiving the sensing component as to the nature of a transmitted signal. By "convincing" the sensors that an attacker developed signal is produced by the environment, the attacker will be able to manipulate the decision-making mechanisms of the UAV [15].
- *Quantization errors:* Those errors appear due to the analog-to-digital conversion of the measured signals. UAV control algorithms rely on discrete values quantizised from the continuous physical domain. The quantization process that assigns one of the possible discrete values to the measured continuous signal causes a discrepancy between the true and transmitted value [16].

Actuator attacks and faults: Those attacks are caused by discrepancies between the desired actuating signal to the physical plant and the one that eventually drives the system.

- *Jamming:* Those attacks operate on the software that produces the input signals of the UAV. An attacker that launches a jamming attack is able to disrupt the flow of information between the computational components of the UAV and the actuators [17].
- *Malicious data injection:* Via access to the software that transmits the control signals to the UAV, an attacker is able to inject their own driving signals to the system [18].
- *Physical malfunction/Catastrophic malfunction:* Those types of attacks or faults operate solely on the physical domain of the UAV. The mechanisms behind a catastrophic malfunction are dependent on the specific UAV.

Communication attacks and faults: Those errors target the network that connects the various computational, sensing and actuating components of a UAV.

- *Jamming/DoS:* Denial of Service (DoS) attacks are launched by an attacker who is able to completely disrupt the transmission of data between the system components [19].
- *Spoofing:* Deceiving signals can also be injected on the links between different components of the UAV. For example, this way, an attacker will gain access to the information processed by the system's actuator, and thus induce a specific behavior to the UAV [20].
- *Low SNR:* In environments with low Signal-to-Noise Ratio (SNR), the communication between components of a UAV that are connected via a wireless medium can be compromised due to the existence of irrelevant signals being transmitted through the same medium as background noise [21].
- *Low SINR:* An attacker can induce a low Signal-to-Inference and Noise Ratio (SINR) in order to further compromise the transmission of information between system components [22].
- *Delays:* Depending on the specific scenario, the communication links might display delays in information transmission. This, in turn, can cause discrepancies between the required signal at the physical components and the transmitted ones by the computational components.

B. Taxonomy of UAV attacks

Given the aforementioned list of attacks on UAV, as well as instances of those on UAV platforms, we now identify their properties in terms of the taxonomy criteria developed in [9]. The taxonomy provides a set of guide-words to describe errors based on their class: value, timing, quantity, etc. Due to space limitations, we present and analyze a subset of those classes as they apply to UAV faults and attacks as they are shown in Table 1.

Faults	*Value*			*Timing*		*Presence*		*Quantity*			*Subtlety*		*Replication*		*Recoverability*		*Permanence*		*Consistency*	
	H	*L*	*U*	*E*	*L*	*C*	*O*	*SI*	*S*	*Sv*	*U*	*D*	*S*	*A*	*O*	*W*	*T*	*P*	*S*	*J*
Sensor																				
Physical Jamming/Outage			X		X		X		X								X			
Replay attacks	X	X		X					X								X		X	
Data drops			X	X			X	X									X			
Spoofing	X	X				X			X								X			
Quantization errors	X	X								X								X		
Actuators																				
Jamming			X				X		X								X			
Stealthy attacks	X	X				X			X								X			
Malicious data injection	X	X				X			X								X			
Physical malfunction	X	X				X	X		X								X			
Catastrophic malfunction	X	X					X			X								X		
Communication																				
Jamming/DoS			X				X		X								X			
Spoofing	X	X				X			X								X			
Low SNR	X	X				X				X								X		
Low SINR	X	X				X				X								X		
Delays			X				X			X								X		

Table 1 Classification of attacks and faults on UAVs based on the EMV2 error taxonomy.

III. Taxonomy of Detection Mechanisms

A. Intrusion detection mechanisms

The problem of securing UAVs, and UAV in general, has been extensively investigated in recent years, leading to the development of various detection and mitigation techniques [23–27]. In this work, we will present the algorithms that we have developed in our previous works, and integrate them in the taxonomy of Section II. This will enable us to determine which detection mechanism is most appropriate in shielding the system against specific types of attacks. Furthermore, by developing a mapping between the properties of the attack taxonomy and the detection mechanisms, it

will be possible to add newly developed algorithms to this process in a modular way.

Statistics-based intrusion detection: Statistics-based intrusion detection is based on the distribution difference between normal behavior and abnormal behavior due to malicious attacks. A typical statistics-based intrusion detection in UAV domain is watermarking-based detection scheme against replay attacks [28]. Replay attacks are really common in UAV since an adversary does not need to know the physics of the system. The attack strategy of replay adversaries is to record a sequence of sensor measurement for a period of time, and later to modify the current sensor measurement to the recorded signals. Since the modified output data follow the same distribution as the previous data, replay attacks remain undetectable. The key idea of the watermarking-based detection scheme is to add an authentication watermarking signal which follows a Gaussian distribution into the optimal control signal. Based on the Neyman-Pearson Lemma, an alarm signal is computed at every instant of time. If the alarm signal is greater than a predetermined threshold then it shows the system is under replay attacks.

Sample-based intrusion detection: In this approach, an uncertain continuous-time system is monitored for actuator attacks or faults intermittently [29]. In particular, it is assumed that the uncertainty that affects the system is bounded by norm. In addition, although the system's trajectories evolve in continuous-time, it is assumed that the state is measured only at some arbitrary time instants. Given these assumptions, it is evaluated whether the system is under an attack/fault based on whether the samples of the measured state are compatible with the assumptions imposed on the model uncertainty. This is equivalent to a reachability condition, which is verified by checking, either directly or indirectly, the feasibility of an optimization problem.

Bellman-based intrusion detection: In this approach, the health of the system is evaluated according to its performance, quantified by an optimal control value function [30]. The detection mechanism monitors the cost accumulated by the system (or the reward gathered) over a predefined time window and computes discrepancies with the ideal cost that the non-compromised system would have [31]. The evaluation of the ideal cost can be model-free.

B. Integration of detection mechanisms to taxonomy

In this section, we show how detection mechanisms can relate to fault taxonomy:

Statistics-based intrusion detection:

- **Value:** The compromised value in the sensor output can be either higher or lower than the real one.
- **Timing:** The detection mechanism calculates the alarm signal at every instant of time and thus it is a real time detection mechanism.
- **Presence:** The attacker records the output data and later replaces the current measurement with the recorded one.
- **Quantity:** The detection scheme operates on a sequence of signals.
- **Subtlety:** The detection scheme only detects cyber adversary (i.e., attacks are able to eavesdrop information from system without acquiring system dynamics to inject adversarial output signals), but fails in terms of cyber-physical adversary (i.e., attackers have the ability to infer the system model and thus mislead the controller).
- **Recoverability:** The detection scheme only detects replay attacks but does not have mitigation techniques. Replay attacks may drive the system state beyond the safety zone and thus unrecoverable.
- **Permanence:** The detection system is able to uncover both permanent and transient attacks.
- **Consistency:** This detection mechanism only works for replay attacks which have to follow certain statistical distribution.

Sample-based intrusion detection:

- **Value:** The compromising value in the actuator can be either higher or lower than the ideal one.
- **Timing:** The detection mechanism uses two samples of the state, and checks whether the latter sampled state is reachable from the former sampled state in the time interval in-between. Hence, for an attack to be detected, it has to take place in the time interval in-between these two measurements.
- **Presence:** If an unexpected measurement of the state is delivered, in the sense that it is not be justified by the assumptions on the uncertainty, a fault/attack is declared.
- **Quantity:** The detection mechanism can detect attacks/faults happening for any amount of time, as long as these attacks/faults are detectable.

- **Subtlety:** An attack/fault may affect the system, but the resulting measurements of the state may still be compatible with the assumptions imposed on the system uncertainty. In this case, the attack/fault is undetectable.
- **Recoverability:** The detection scheme does not inherently contain an attack/fault mitigation technique.
- **Permanence:** The detection system is able to uncover both permanent and transient attacks.
- **Consistency:** There are no assumptions imposed on whether the attack/fault follows a particular distribution.

Bellman-based intrusion detection:

- **Value:** The compromising value in the actuator/sensor can be either higher or lower that the ideal one.
- **Timing:** The detection is based on a time window that extends to the past, thus the detection mechanism may arrive at a decision after the attack has finished.
- **Quantity:** The detection is able to detect compromised signals over a nontrivial time window. Thus it operates on sequences and services, but not single items.
- **Detectable:** The system works for faults that are detectable based on derived bounds. Anything outside this signal set, is stealthy and cannot be distinguished from noise.
- **Recoverability:** Current system implementation's mitigation ability rests on a binary decision on the existence of healthy subsystems.
- **Permanence:** The detection system is able to uncover both permanent and transient attacks.
- **Consistency:** There are no *a-priori* assumptions on attack statistics. In the general case, the system is able to detect jittery compromising signals.

These conclusions are summarized in Table 2. We present an example of the procedure via the use of the two tables in order to help the designer select the detection mechanism. Initially, we assume that the designer knows the system to be vulnerable to sensor replay attacks based on the environment on which it operates. By using the information of Table 1, we can see that replay attacks induce measurement values both higher and lower than the correct ones. Furthermore, since replay attacks replace the current measurements with recorded ones, they follow a certain type of distribution. The designer now has to cross-reference those properties with the ones given to the detection mechanisms in Table 2. It can be seen that most properties can be captured by all three detection mechanisms, but the statistics-based detection scheme is also able to handle attacks with errors following a certain distribution in the taxonomy. Thus, the designer would select to include this mechanism during the deployment of the UAV.

Detection mechanisms	*Value*			*Timing*		*Presence*		*Quantity*			*Subtlety*		*Replication*		*Recoverability*		*Permanence*		*Consistency*	
	H	L	U	E	L	C	O	Sl	S	Sv	U	D	S	A	O	W	T	P	S	J
Detection mechanisms																				
Sample-based	X	X		X	X	X		X	X	X		X					X	X		X
Bellman-based	X	X			X				X	X		X					X	X		X
Statistics-based	X	X								X		X					X	X	X	

Table 2 Classification of intrusion detection mechanisms based on the EMV2 error taxonomy.

C. Properties of Three Proposed Detection Mechanisms

Properties of detection mechanisms are investigated. A list of information requirements, assumptions and operational properties are proposed and compiled as Table 3. As an example of our classification approach, we use the three detection mechanisms developed by our group.

IV. Make Detection Mechanism Decision

Flowchart 1 presents the basic components of our proposed decision-making algorithm. Our objective is for a CPS designer or operator to have a well-structured tool that enables them to augment the system with intrusion detection mechanisms that are appropriate and relevant both to the system itself and to the potential environmental threats.

Our method aims to allow for a wide variety of intrusion detections developed by different research communities. Thus, the starting point of the analysis is the physical system itself, composed of sensing, actuating, communication, and computation components. The first step that the analyst has to take is to decide on the appropriate modeling of the system. Although all the intrusion detection mechanisms used in our examples are based on a state-space dynamical

Detection Mechanics	Sample-based	Bellman-based	Statistics-based
System			
Dynamics type	Linear	Linear	Linear
Model knowledge	Completely known	Not needed / VF needed	Completely known
Time evolution	Continuous	Continuous	Discrete
Controller Type	Arbitrary		
Controller knowledge	Full trajectory needed	Known feedback gain (LQR)	Output feedback control
Disturbance	Allowed	Allowed	Allowed
Disturbance type	Deterministic	Deterministic	Stochastic
Disturbance knowledge	Norm bound	Norm bound	Gaussian distribution
Noise	No	No	Allowed
Noise type	-	-	Stochastic
Noise knowledge	-	-	Gaussian distribution
Measurements			
Data needed	Full state vector	Full state vector	Output and input data
Intermittent data allowed	Yes	No	No
Reactive measures	Not developed	Switching among redundant	Not developed
Undetectable attacks	Possible	Possible	Only detect replay attacks
Time to detection	Time till first sample after attack	After learning	Time when replay attacks happen

Table 3 Sample properties of the three proposed detection mechanisms.

system representation of the CPS – albeit in both continuous and discrete time domains – different models, such as transfer functions or Markov Decision Processes can also be integrated.

Subsequently, the ability of the designer to know the parameters of the CPS comes into question. Depending on the availability of such values, e.g., the availability of the system matrices in a state space model, or the coefficients of a transfer function, the designer can employ either model-based or model-free intrusion detection mechanisms. It should be noted that completely model-free intrusion detection is a research topic that is currently under investigation, while in most cases there is a different type of information needed. Specifically, in our optimality-based intrusion detection, there is no need for the security analyst to have knowledge of the system's matrices, but a preprocessing phase during which a reinforcement learning algorithm is utilized to derive optimal value functions of the system.

Given this information regarding the system as a mathematical object, the analyst should have a list of potential intrusion detection mechanisms that are appropriate for the specific instance. This in turn, via the use of Table 2, corresponds to knowledge of the types and specifications of faults and attacks that each one of the potential detection mechanisms can address.

In order to correctly identify the appropriate mechanisms that are needed for the CPS, the environment and the specific scenarios that will arise need to be considered. As such, a comprehensive list of potential attacks and faults must be developed. Towards this, the different components of the system are analyzed. Once the physical scenarios are identified, the analyst is able to leverage Table 1 to extract the abstract properties of such attacks.

V. Taxonomy Applications to UAV Design

In order to elucidate the proposed decision-making process, we present an example on a UAV system. Specifically, we consider a scenario in which the vehicle partakes in a mission where the probability of it being subject to acoustic manipulation of its IMU is high. Acoustic injections were first demonstrated in accelerometers in [32], where the authors showed the ways via which manipulation of the output measurements of such a device can be spoofed with adequate precision. The simulated results for an instance of such an attack are shown in Figures 2 and 3, from which a designer can identify the properties of the attack that correspond to Table 1.

Given this scenario, an analyst would refer to the table containing the properties of the attack and choose the abstract "attack class" of the acoustic injection. Given the nature of the attack, the appropriate choice would be the spoofing sensor attack in this case. Subsequently, based on the properties given by the attack taxonomy table, the analyst would be able to identify the key characteristics of the attack. Cross-referencing the properties of the attack with the span of detectable characteristics of the different intrusion detection mechanisms will determine the subset of the mechanisms that will be successful in environments with those types of attacks.

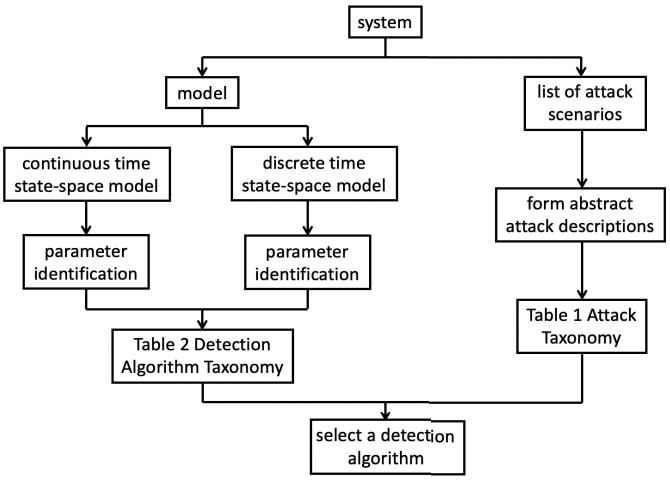

Fig. 1 Decision-making flow chart.

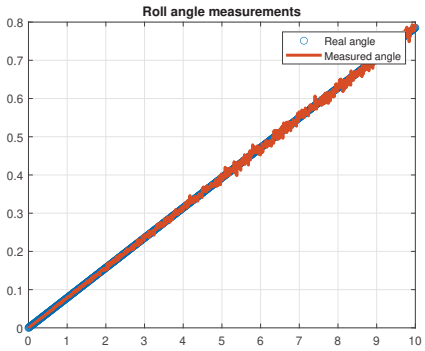

Fig. 2 Roll angle measurement of an accelerometer under acoustic attack.

VI. Conclusion

In this work, we constructe a taxonomy of attacks and faults that can have a deteriorating effect on the performance of UAV. In addition, after introducing three different detection mechanisms, we characterize the class of attacks/faults these work well against. As a result, we have effectively created a tool that can assist a UAV operator in selecting the appropriate detection mechanisms for their system. Future work will focus on implementing the proposed taxonomy on a specific UAV platform, where the exact sources of the attacks/faults can be explicitly identified on a low architectural level.

Acknowledgments

This material is based upon work funded and supported in part by ARO under grant No. W911NF-19 – 1 – 0270, by ONR Minerva under grant No. N00014 – 18 – 1 – 2160, and by NSF under grant Nos. CAREER CPS-1851588, S&AS 1849198, SATC-1801611, by the Onassis Foundation-Scholarship ID: F ZQ 064 – 1/2020 – 2021, and by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT. [DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. DM21-0985

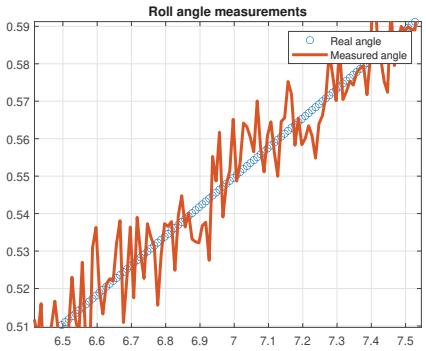

Fig. 3 Roll angle output under acoustic attacks. The properties associated with spoofing attacks according to Table 1 are seen here.

References

[1] Valavanis, K. P., and Vachtsevanos, G. J., *Handbook of unmanned aerial vehicles*, Vol. 1, Springer, 2015.

[2] Freeman, P., Pandita, R., Srivastava, N., and Balas, G. J., "Model-based and data-driven fault detection performance for a small UAV," *IEEE/ASME Transactions on mechatronics*, Vol. 18, No. 4, 2013, pp. 1300–1309.

[3] Sun, R., Cheng, Q., Wang, G., and Ochieng, W. Y., "A novel online data-driven algorithm for detecting UAV navigation sensor faults," *Sensors*, Vol. 17, No. 10, 2017, p. 2243.

[4] Abbaspour, A., Aboutalebi, P., Yen, K. K., and Sargolzaei, A., "Neural adaptive observer-based sensor and actuator fault detection in nonlinear systems: Application in UAV," *ISA transactions*, Vol. 67, 2017, pp. 317–329.

[5] Bateman, F., Noura, H., and Ouladsine, M., "Fault diagnosis and fault-tolerant control strategy for the aerosonde UAV," *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 47, No. 3, 2011, pp. 2119–2137.

[6] Zhong, Y., Zhang, Y., Zhang, W., Zuo, J., and Zhan, H., "Robust actuator fault detection and diagnosis for a quadrotor UAV with external disturbances," *IEEE Access*, Vol. 6, 2018, pp. 48169–48180.

[7] Zhu, B., Joseph, A., and Sastry, S., "A taxonomy of cyber attacks on SCADA systems," *2011 International conference on internet of things and 4th international conference on cyber, physical and social computing*, IEEE, 2011, pp. 380–388.

[8] Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., and Sztipanovits, J., "Taxonomy for description of cross-domain attacks on CPS," *Proceedings of the 2nd ACM international conference on High confidence networked systems*, 2013, pp. 135–142.

[9] Procter, S., and Feiler, P., "The AADL Error Library: An Operationalized Taxonomy of System Errors," *ACM SIGAda Ada Letters*, Vol. 39, No. 1, 2020, pp. 63–70. https://doi.org/10.1145/3379106.3379113, URL https://dl.acm.org/doi/10.1145/3379106.3379113.

[10] Humayed, A., and Luo, B., "Cyber-physical security for smart cars: taxonomy of vulnerabilities, threats, and attacks," *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems*, 2015, pp. 252–253.

[11] Hu, J., Pota, H. R., and Guo, S., "Taxonomy of attacks for agent-based smart grids," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 7, 2013, pp. 1886–1895.

[12] Ängskog, P., Näsman, P., and Mattsson, L.-G., "Resilience to intentional electromagnetic interference is required for connected autonomous vehicles," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 61, No. 5, 2018, pp. 1552–1559.

[13] Krishna, C. L., and Murphy, R. R., "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, IEEE, 2017, pp. 194–199.

[14] Cetinkaya, A., Ishii, H., and Hayakawa, T., "An overview on denial-of-service attacks in control systems: Attack models and security analyses," *Entropy*, Vol. 21, No. 2, 2019, p. 210.

[15] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., and Song, D., "Robust physical-world attacks on deep learning visual classification," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 1625–1634.

[16] Kavanagh, R. C., and Murphy, J. M., "The effects of quantization noise and sensor nonideality on digital differentiator-based rate measurement," *IEEE Transactions on Instrumentation and Measurement*, Vol. 47, No. 6, 1998, pp. 1457–1463.

[17] Hussain, Y., Burrow, S., Henson, L., and Keogh, P., "A review of techniques to mitigate jamming in electromechanical actuators for safety critical applications," *International Journal of Prognostics and Health Management*, Vol. 9, No. 9, 2018, pp. 1–11.

[18] Fawzi, H., Tabuada, P., and Diggavi, S., "Security for control systems under sensor and actuator attacks," *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, IEEE, 2012, pp. 3412–3417.

[19] Zhong, C., Yao, J., and Xu, J., "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Communications Letters*, Vol. 23, No. 2, 2018, pp. 286–289.

[20] Psiaki, M. L., and Humphreys, T. E., "GNSS spoofing and detection," *Proceedings of the IEEE*, Vol. 104, No. 6, 2016, pp. 1258–1270.

[21] Li, J., Liu, M., Tang, N., and Shang, B., "Non Data-Aided SNR Estimation for UAV OFDM Systems," *Algorithms*, Vol. 13, No. 1, 2020, p. 22.

[22] Li, Y., Quevedo, D. E., Dey, S., and Shi, L., "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Transactions on Control of Network Systems*, Vol. 4, No. 3, 2016, pp. 632–642.

[23] Abbaspour, A., Yen, K. K., Noei, S., and Sargolzaei, A., "Detection of fault data injection attack on uav using adaptive neural network," *Procedia computer science*, Vol. 95, 2016, pp. 193–200.

[24] Sedjelmaci, H., Senouci, S. M., and Ansari, N., "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 48, No. 9, 2017, pp. 1594–1606.

[25] Panice, G., Luongo, S., Gigante, G., Pascarella, D., Di Benedetto, C., Vozella, A., and Pescapè, A., "A SVM-based detection approach for GPS spoofing attacks to UAV," *2017 23rd International Conference on Automation and Computing (ICAC)*, IEEE, 2017, pp. 1–11.

[26] Zhu, H., Cummings, M. L., Elfar, M., Wang, Z., and Pajic, M., "Operator strategy model development in uav hacking detection," *IEEE Transactions on Human-Machine Systems*, Vol. 49, No. 6, 2019, pp. 540–549.

[27] Gu, Y., Yu, X., Guo, K., Qiao, J., and Guo, L., "Detection, estimation, and compensation of false data injection attack for UAVs," *Information Sciences*, Vol. 546, 2021, pp. 723–741.

[28] Zhai, L., and Vamvoudakis, K. G., "A data-based private learning framework for enhanced security against replay attacks in cyber-physical systems," *International Journal of Robust and Nonlinear Control*, Vol. 31, No. 6, 2021, pp. 1817–1833.

[29] Fotiadis, F., and Vamvoudakis, K. G., "Detection of actuator faults for continuous-time systems with intermittent state feedback," *Systems & Control Letters*, Vol. 152, 2021, p. 104938.

[30] Lewis, F. L., Vrabie, D., and Syrmos, V. L., *Optimal control*, John Wiley & Sons, 2012.

[31] Kanellopoulos, A., and Vamvoudakis, K. G., "A moving target defense control framework for cyber-physical systems," *IEEE Transactions on Automatic Control*, Vol. 65, No. 3, 2019, pp. 1029–1043.

[32] Trippel, T., Weisse, O., Xu, W., Honeyman, P., and Fu, K., "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," *2017 IEEE European symposium on security and privacy (EuroS&P)*, IEEE, 2017, pp. 3–18.