Work-in-progress (WIP): Development of a Laboratory Platform for UAV Cybersecurity Education

Introduction

With the advent of the era of the Internet of Things (IoT), unmanned aerial vehicles (UAVs), also known as unmanned aerial systems (UAS) or drones, have been used to enable a wide variety of beneficial applications [1–3]. According to the navigant research [4], it is expected that the global UAS market would reach 16.2 billion USD by 2024, with rapid growth in all technology categories. Due to their small size, good functionality, and high flexibility, UAVs have been applied to a variety of fields, including manufacturing, agriculture, geography, urban management, police, and military, which facilitates the development of UAVs in both industry and academia.

While the reconnaissance of UAVs produced a huge amount of economic and social benefits, such popularity exposes many vulnerabilities that may impede the development of UAVs and pose risks for many safety-crucial and security-critical applications. One of the most critical vulnerabilities is UAV cybersecurity [5]. The characteristics of drone communications through wireless networks introduce the surface for malicious attacks in multiple aspects, including availability, privacy, and integrity [6–8]. Nowadays, there is a rising number of cyber-attack attempts on UAVs which raises the concern of the entire UAS community [9–11]. Therefore, it is necessary to study, analyze, and then mitigate cybersecurity threats for UAVs to avoid any possible adversary crashing or malfunction of drones, which remains a task for both UAVs training and cybersecurity education [12, 13]. However, the education resources for UAV cybersecurity are limited, especially for hands-on practices, which are indispensable for students to conduct such study. This limitation is mainly due to the regulations and state laws of UAV operations specifying the qualification to fly drones and certain prohibited areas [14, 15]. Most students do not have the required certificate to fly a drone, and not all institutions have nearby authorized UAV flying zones, which make it difficult to carry out related educational activities.

Considering the above facts, we are motivated to develop a platform with a list of laboratory activities that are consistent with the UAV cybersecurity curriculum materials, which aims at overcoming these non-technical challenges and enabling hands-on exercises. Besides, this platform is going to have the capacity of extension and serve as the base for instructors and researchers to customize or develop additional modules. To be specific, software simulation (e.g., SITL, software in the loop, known as SITL) will be mainly used in our developments, but hardware-in-the-loop (HIL, or called HITL) simulation will also be supported for the evaluation of the UAV system's robustness with the existence of cybersecurity threats. We propose to utilize a firmware for UAV system development, Pixhawk [16] with related open-source software packages, such as ROS-Gazebo [17] and OMNet++ [18], as the basic simulation framework for UAV cybersecurity events with visualization. On top of the framework, a set of hands-on exercise modules can be developed to cover common threats in UAV and additional modules for newly identified threats, in which a manner offense and defense tasks can be further developed. In the remainder of this paper, the framework architecture that we propose to develop will be introduced, the verification method of our platform, and a brief summary will be made.

Framework Architecture

In this section, the proposed framework for the UAV cybersecurity laboratory platform will be introduced, which includes the UAV simulator, the network simulator, and their integration towards the development of our laboratory platform and hands-on exercises.

UAV Simulator with Pixhawk firmware

One of the key components in our laboratory platform is the simulation of UAV behaviors. Recently, many UAV simulation tools, such as FlightGear, UE4Sim, JMavSim, Gazebo, and Air-Sim, have been developed to support the simulation of different UAV models with different functionality and capacity of extension. We propose to use ROS based Gazebo as the basic UAV simulator, where Gazebo performs the 3D simulation for various drone models such as the quadcopter, multi-copter, and fixed-wing under different environments with high fidelity and efficiency, while ROS serves as the interface for drones with the ability to extend with other software packages for the platform development. Moreover, the ROS-Gazebo simulator can be used with PX4, one of the most popular professional autopilot software in the worldwide drone community, so that both SITL and HITL simulations can be performed. In HITL simulation, Pixhawk serves as the reference hardware platform for PX4 to provide the simulation which is closest to the actual flight without actually flying.

Besides the modules mentioned above, Ground Control Station (GCS) is used as another important component within the UAV simulator, whose main function is to prepare the plans and path for UAVs, send control signals to UAVs, and communicate with UAVs for data exchange. There are several GCS software such as QGroundControl, UGCS, and MAVProxy, which have different capabilities of communication protocol support and autopilot support. Besides, some of them have been used to implement attacks and exploit vulnerabilities of UAV communication protocol [19], which would be useful for the development of our laboratory exercise.

To be more specific, the UAV simulator that we propose to develop mainly consists of two modes of simulation discussed above, SITL and HITL. Figure 1 illustrates how modules integrate and communicate to enable simulation in both cases, where the black lines stand for the necessary communication made in SITL while the blue ones are for HITL. Moreover, both serial and MAVLink communication is used, where MAVLink is a typical communication protocol for drones enabled by MAVROS packages in the context of ROS. In SITL simulation, the PX4 module communicates with the Gazebo simulator to receive sensor data and send data (e.g., values of UAV motor and actuator), which is done via MAVLink communication in the inner simulated environment. PX4 also communicates with the GCS and ROS to send telemetry data from the inner simulated world and receive commands, which is also done via MAVLink. Different from SITL that executes more of the code for the implemented flight control system, HITL runs PX4 on the actual flight controller hardware, where Pixhawk is used in our development. To be specific, Gazebo is connected to Pixhawk via USB or UART for an actual flight control input. Moreover, Gazebo acts as a gateway to bridge MAVLink data between PX4 and GCS/ROS. By leveraging HITL set-up mentioned above, a more realistic UAV simulation environment is provided in which manner UAV system's robustness under cybersecurity attacks can be better evaluated.

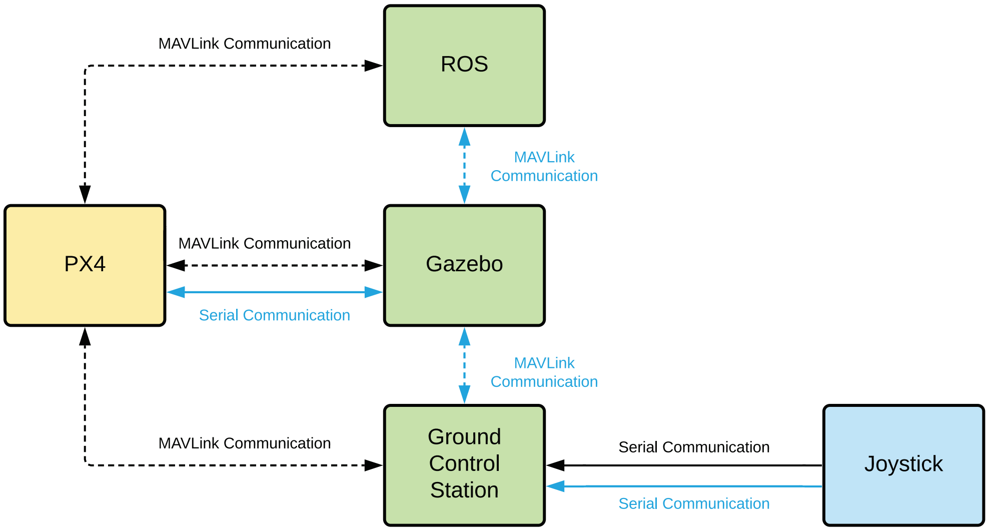

Figure 1: SITL and HITL Mechanism of ROS-Gazebo Simulator with PX4/Pixhawk

Network Simulator

While the UAV simulator mainly performs the simulation for UAV behaviors in different scenarios, the network simulator is utilized for the simulation for most cybersecurity events. Recently, several network simulation frameworks have been developed and widely used by the research community, such as NS-2, NS-3, OMNet, and OMNet++, which are capable of highly representing the behaviors and status of the wireless networks with different features and scalability. Recently many attempts are made to leverage network simulators for the study of wireless communication behaviors among robots, with or without the integration of ROS. In our development of the UAV cybersecurity laboratory platform, we also propose to integrate both frameworks for a better illustration of UAV behaviors with the existence of cybersecurity threats so that students can have a clearer view of how those threats impact UAV and how they can develop countermeasures to mitigate them. In this section, we will introduce the network simulation framework with the necessary libraries that we propose to use.

To be specific, we propose to use the OMNet++ simulation environment with the INET framework and the satellite simulator (OS3) module to simulate the normal drone communication events and cyberattack scenarios. INET is an OMNeT++ based library that provides various protocols, agents, and other models of communication networks [20]. INET has an advantage when extending the simulation modules of our laboratory platform, as it is capable of validating new protocols or exploring new simulation scenarios. Our proposed platform considers communication not only between UAV and GCS, UAV and other UAVs but also between UAV and satellite where the modeling of accurate satellite mobility and GPS is needed. To enable the simulation of satellite-based communication, our platform adopts the OS3 module, which is also based on OMNet++[21]. OS3 is able to automatically import actual satellite tracks and weather information to simulate complex scenarios at a certain point in time series. Moreover, it is extendable for more complicated and thorough analysis tasks and supports the calculation of typical measures such as SNR, BER, and packet loss, which makes it possible for the researchers and teaching faculty to customize or further develop simulation modules related to drone navigation systems.

Towards the laboratory platform and hands-on exercise modules

The integration of UAV simulator and network simulator is another key component in our development towards the laboratory platform as it bridges two types of behaviors, i.e., drone behavior and communication network behavior, and enables the simulation in a joint manner. Recently, there have been several studies towards the integration of robotics simulation framework, and discrete network event simulation framework [22–24]. The main idea is to utilize ROS as the drone interface with supported mechanisms like publish/subscribe where is also followed by MAVLink, or implemented module to integrate network simulator with drone simulator. To be specific, in our case, the UAV simulation environment in ROS is also configured in OMNet++, which makes it possible to capture any changes in the environment. Each UAV is represented as a node in OMNet++ and communicates wirelessly by using the INET library. However, there is another challenge due to the different simulation mechanisms between Gazebo and OMNet++. The Gazebo is a time-based simulator, and OMNet++ is an event-driven simulator which means the synchronization of both simulators needs to be carefully and accurately handled. One alternative is to implement a module setting ROS clock as the time reference and scheduling a corresponding OMNet++ message so as to force the OMNet++ simulator to generate an event based on timestamps in ROS [22].

Most recently, a more sophisticated open-source integration interface of ROS-Network simulators has been proposed for simulating high-fidelity Perception-Action-Communication or Perception-Action loops of multi-robot systems [24], which also has advantages to be leveraged towards our UAV cybersecurity laboratory platform. The general mechanism is presented in Figure 2. The basic mechanism is similar to the previous one, but two more coordination modules are developed for the communication channel abstracting and information forwarding process. To be more specific, the Gazebo coordination module gathers the channel information and passes it to the OMNet++ coordination module and simulator, while the OMNet++ coordination module captures the data traffic generated by ROS nodes handling communication within the network. Furthermore, both modules maintain the synchronicity between ROS nodes and simulators. Thus, both the UAVs and communication network status can be simulated under normal scenarios. In order to simulate other cybersecurity events and visualize the behaviors of UAV on Gazebo, we also propose to develop several ROS-Gazebo compatible plugins that is similar to tum_simulator[25] and can be used to control drone motion and deliver navigation information and modules to feed the simulated parameters to the OMNet++ coordination module and then forward them to developed plugins. In this way, the functionality similar to AVENS Simulator[26] can be achieved, and the effect of cyber threats on UAVs can be visualized in a synchronized manner.

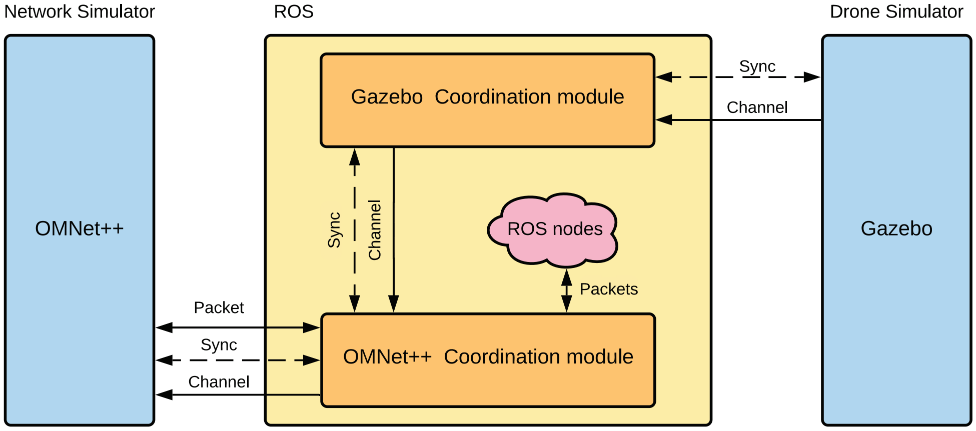

Figure 2: Reproduce of ROS-network integration interface under our context

After the basic joint simulator is set up, more modules can be integrated, and more advanced features can be further developed. Inspired by [27], we consider a more detailed design of attack hosts, including the fixed attack host and the wireless one. Moreover, we consider the basic/advanced simulation options with different levels of details. The basic simulation mode treats UAV as a block box, and the advanced mode provides options to users for in-depth configuration of the UAV from attitude and heading reference system (AHRS) to data logging. The basic mode provides a set of default configurations to users, which will enable fast initialization of pre-configured lab modules and also benefit the users at the beginning stage of UAV cybersecurity study to avoid complex setup.

Based on the framework of our platform, different types of cybersecurity threats to UAVs can be implemented. We will mainly design six categories of exercise modules and add additional modules according to newly identified threats. These modules will be mapped to the proposed course materials. In each category of exercise, the scenario-based design is adopted [28], wherein a UAV cybersecurity setting will be created with corresponding actors, goals, actions, and events. In this manner, offense and defense tasks can be further developed. Besides, our laboratory platform also provides threat impact score, likelihood score, and difficulty levels for exercise modules which will serve as the guidance for users to select exercise modules according to their technical skill levels and learning needs. Finally, the command-line-based and GUI versions of our laboratory platform will also be offered, where GUI enables users to select configurations and adjust different parameters according to the requirements of the lab exercises. The overview of our UAV cybersecurity laboratory platform is present in Figure 3.

Verification Method

To guarantee the effectiveness of exercise modules to be developed, our UAV cybersecurity laboratory platform will be evaluated in the indoor and outdoor UAV cybersecurity testing facilities at Embry-Riddle Aeronautical University. Most of the flying tasks under the regulation of FAA and the State laws will be conducted. Each module will be adjusted and tuned based on the feedback of the tests. During the life-cycle of our platform, periodical tests will be conducted

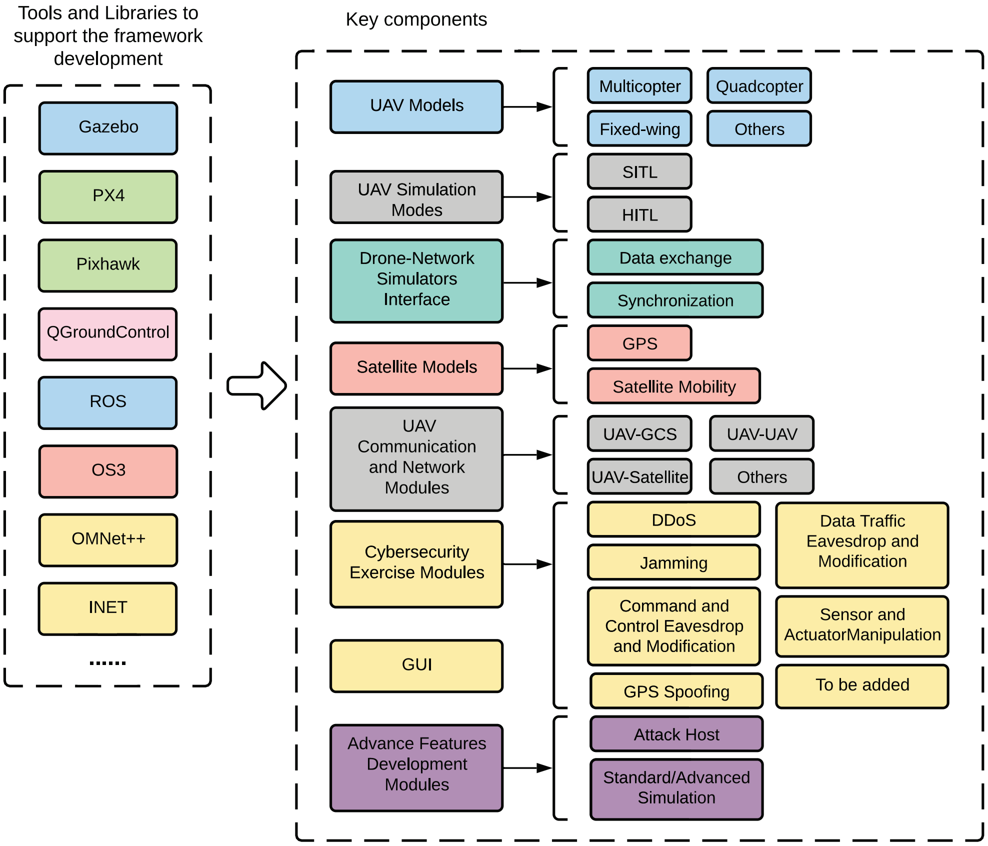
Tools and Libraries to support the framework development
Gazebo
PX4
Pixhawk
QGroundControl
ROS
OS3
OMNet++
INET
......
Key components
UAV Models
Multicopter
Quadcopter
Fixed-wing
Others
UAV Simulation Modes
SITL
HITL
Drone-Network Simulators Interface
Data exchange
Synchronization
Satellite Models
GPS
Satellite Mobility
UAV Communication and Network Modules
UAV-GCS
UAV-UAV
UAV-Satellite
Others
Cybersecurity Exercise Modules
DDoS
Jamming
Command and Control Eavesdrop and Modification
GPS Spoofing
Data Traffic Eavesdrop and Modification
Sensor and ActuatorManipulation
To be added
GUI
Advance Features Development Modules
Attack Host
Standard/Advanced Simulation

Figure 3: Overview of our UAV Cybersecurity Laboratory Platform Framework

to match the update of hardware, software, and network environment, with which updated configurations of corresponding exercise modules will be distributed to users at the project repository with detailed documents. Therefore, our platform can be transferred to institutions without UAV cybersecurity facilities and help students carry out hands-on practice close to actual scenarios.

Summary

In this paper, we propose to develop an educational UAV cybersecurity laboratory platform with a hands-on exercise module to solve the teaching resource limitation and enable related educational activities. In general, our platform will support both SITL and HITL for different drone models with the joint simulation of drones and networks to evaluate the effect of cybersecurity events. Based on the implemented platform, the UAV cybersecurity curriculum materials will be leveraged to design hands-on exercises for UAV training and cybersecurity education. To verify the effectiveness of our implementation, the implemented modules will be evaluated with testing facilities and adjusted according to the feedback of the tests.

Acknowledgement

This work was supported in part by the National Science Foundation under Grant No. 1956193. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] Y. Sun, H. Song, A. J. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[2] X. Yue, Y. Liu, J. Wang, H. Song, and H. Cao, "Software defined radio and wireless acoustic networking for amateur drone surveillance," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 90–97, 2018.

[3] J. Wang, Y. Liu, and H. Song, "Counter-unmanned aircraft system(s) (c-uas): State of the art, challenges, and future trends," *IEEE Aerospace and Electronic Systems Magazine*, 2021.

[4] "Drones and robotics for utility transmission and distribution: Unmanned aerial vehicle and robotics solutions for utility td inspection and maintenance: Global market analysis and forecasts," https://blog.aee.net/drones-robotics-for-utility-transmission-distribution-offer-improved-safety-and-cost-effectiveness, accessed: December 14, 2020.

[5] H. Song, G. Fink, and S. Jeschke, *Security and privacy in cyber-physical systems.* Wiley Online Library.

[6] M. Albalawi and H. Song, "Data security and privacy issues in swarms of drones," in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, 2019, pp. 1–11.

[7] B. Jiang, J. Yang, and H. Song, "Protecting privacy from aerial photography: State of the art, opportunities, and challenges," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 799–804.

[8] B. Jiang, J. Yang, H. Xu, H. Song, and G. Zheng, "Multimedia data throughput maximization in internet-of-things system based on optimization of cache-enabled uav," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3525–3532, 2019.

[9] J. Wang, Y. Liu, S. Niu, and H. Song, "Beamforming-constrained swarm uas networking routing," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[10] ——, "Extensive throughput enhancement for 5g enabled uav swarm networking," *IEEE Journal on Miniaturization for Air and Space Systems*, pp. 1–1, 2021.

[11] X. Liu, H. Song, and A. Liu, "Intelligent uavs trajectory optimization from space-time for data collection in social networks," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2020.

[12] C. Xu, B. Chen, Y. Liu, F. He, and H. Song, "Rf fingerprint measurement for detecting multiple amateur drones based on stft and feature reduction," in *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2020, pp. 4G1–1–4G1–7.

[13] J. Eason, C. Xu, and H. Song, "Software define radio in realizing the intruding uas group behavior prediction," in *2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC)*, 2020, pp. 1–5.

[14] "Fact Sheet Small Unmanned Aircraft Regulations (Part 107)," https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=22615, accessed: June 14, 2020.

[15] "FAA - Rules of the Sky," https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_101/, accessed: June 14, 2020.

[16] "Pixhawk," https://pixhawk.org/, accessed: May 20, 2020.

[17] "ROS-Gazebo," http://gazebosim.org/tutorials?tut=ros_overview, accessed: May 23, 2020.

[18] "OMNet++," https://omnetpp.org/, accessed: May 21, 2020.

[19] J. A. Marty, "Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft," AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH GRADUATE SCHOOL OF ENGINEERING AND MANAGEMENT, Tech. Rep., 2013.

[20] "INET," https://inet.omnetpp.org/, accessed: May 21, 2020.

[21] "OS3," https://omnetpp.org/download-items/OS3.html, accessed: June 2, 2020.

[22] B. Vieira, R. Severino, A. Koubâa, and E. Tovar, "Towards a realistic simulation framework for vehicular platooning applications," in *2019 IEEE 22nd International Symposium on Real-Time Distributed Computing (ISORC)*. IEEE, 2019, pp. 93–94.

[23] S. Behera, B. Panigrahi, H. K. Rath, and A. Pal, "Wireless characteristics study for indoor multi-robot communication system," in *Proceedings of the 1st Workshop on Complex Networked Systems for Smart Infrastructure*, 2018, pp. 1–6.

[24] M. Calvo-Fullana, D. Mox, A. Pyattaev, J. Fink, V. Kumar, and A. Ribeiro, "Ros-netsim: A framework for the integration of robotic and network simulators," *arXiv preprint arXiv:2101.10113*, 2021.

[25] "tum_simulator," https://github.com/dougvk/tum_simulator, accessed: December 23, 2020.

[26] E. A. Marconato, M. Rodrigues, R. d. M. Pires, D. F. Pigatto, A. R. Pinto, K. R. Branco *et al.*, "Avens-a novel flying ad hoc network simulator with automatic code generation for unmanned aircraft system," in *Proceedings of the 50th Hawaii international conference on system sciences*, 2017.

[27] A. Y. Javaid, "Cyber security threat analysis and attack simulation for unmanned aerial vehicle network," Ph.D. dissertation, University of Toledo, 2015.

[28] J. M. Carroll, *Making use: scenario-based design of human-computer interactions*. MIT press, 2000.