Demo Abstract: Platform for Security-Aware Design of Human-on-the-Loop Cyber-Physical Systems

Mahmoud Elfar Haibei Zhu Adithya Raghunathan Yi Y. Tay Jeffrey Wubbenhorst
Missy L. Cummings Miroslav Pajic
Duke University
{mahmoud.elfar, haibei.zhu, ra102, yt61, jsw51}@duke.edu
{mary.cummings, miroslav.pajic}@duke.edu

1 INTRODUCTION

Cyber-Physical Systems (CPS) are commonly supervisory control systems where a human-on-the-loop (HOL) supervises one or more autonomous systems, and the embedded autonomy allows the operators to intermittently attend to the system while they attend to other tasks. Thus, it is imperative that the design of any security-aware CPS considers the human factor – i.e., the impact of the interaction between humans and the system on security guarantees. Yet, there has been very little work on design of Human-CPS that promotes human situational awareness for enhanced system performance, particularly in terms of cyber-physical security and real-time defense against attacks. One of the main obstacles in rapidly advancing this line of research is almost a complete lack of available testbeds for evaluating security-aware interactions between humans and CPS.

We developed RESCHU-SA, an extendable virtual platform that facilitates studying the impact that HOL has on the security of CPS with varying levels of autonomy. RESCHU-SA allows users to analyze how the human power of inductive reasoning and ability to provide context, particularly during an attack, affects the overall CPS security guarantees. The proposed platform is an extension of the Research Environment for Supervisory Control of Heterogeneous Unmanned Vehicles (RESCHU) simulation environment [2], previously used in various applications, including studies focused single- and multi-operator supervision of Unmanned Aerial Vehicles (UAVs) missions (e.g. [1]), as well as interface usability metrics [3].

2 DEMONSTRATION

We illustrate the developed platform on multi-UAV missions supervised by a single operator, where some of the UAVs may be compromised. As depicted in Fig. 1, the RESCHU-SA operator interface consists of a map area capturing information about UAVs (e.g., their flight plans, targets, threat zones and the expected-time-to-arrival), a camera-feed display from the selected UAV, and a communication panel. Through the graphical user interface (GUI), the operator can supervise a fleet of UAVs on a timed mission where several target locations should be visited by the UAVs with a set of visual tasks to be completed by the operator using the UAV camera feed.

According to predefined attack scenarios, some UAVs are attacked by injecting malicious GPS data into the planner of the corresponding UAVs, as well as the information reported to the user. Due to the stealthy nature of such attacks, the reported location of an UAV under attack slowly changes over time, limiting the operator's ability to detect such attacks from the displayed UAV's trajectory. To analyze

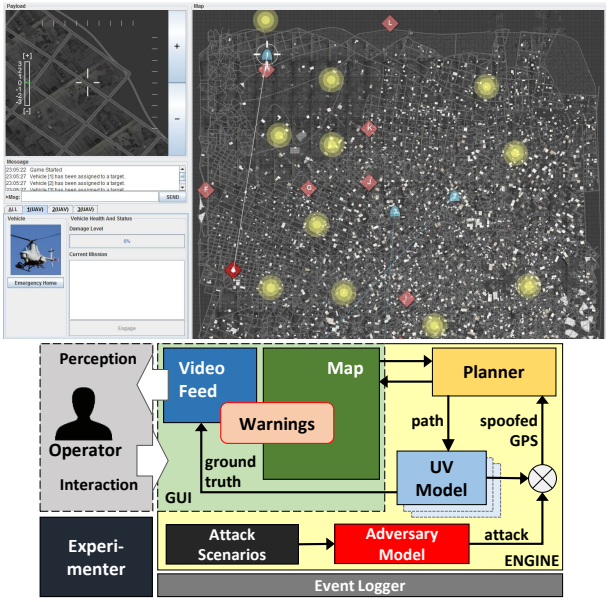

Figure 1: RESCHU-SA operator interface (top) and the platform architecture (bottom).

the operator's situational awareness, we use the UAV's live video feed that always reflects the ground truth; thus, an operator might be able to contribute to detecting such attacks if she can identify discrepancies between the video feed and the reported location.

Due to the modular platform design, the attack models and UAV dynamics can be simply extended, and new behaviors can be easily incorporated by the system designer. The current attack model allows for configuring adversary behavior, including aggressive vs. stealthy attacks, timing, target regions, and warnings raised by intrusion detection systems. Similarly, we use randomized maps containing regions with various feature richness to enable studying how feature density influences the operator's ability to identify an UAV's location from the video feed. Unlike the conventional camera feed that shows sporadic static images of predefined areas on the map, RESCHU-SA emulates continuous video feeds and supports a number of features that can increase the video fidelity, including noise overlay, vehicle vibrations and communication delays.

REFERENCES

[1] M. L. Cummings, L. F. Bertucelli, J. Macbeth, and A. Surana. 2014. Task versus vehicle-based control paradigms in multiple unmanned vehicle supervision by a single operator. *IEEE Trans. on Human-Machine Systems* 44, 3 (2014), 353–361.
[2] Carl E Nehme. 2009. *Modeling human supervisory control in heterogeneous unmanned vehicle systems*. Technical Report. DTIC Document.
[3] J. R. Peters, A. Surana, and L. Bertuccelli. 2015. Eye-Tracking Metrics for Task-Based Supervisory Control. *arXiv preprint arXiv:1506.01976* (2015).

This work was supported in part by the NSF CNS-1505701 grant and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy. This material is also based on research sponsored by the ONR under agreement number N00014-17-1-2012.
ICCPS, Pittsburgh, PA USA
2017. 978-x-xxxx-xxxx-x/YY/MM…$15.00
DOI: 10.1145/nnnnnnn.nnnnnnn