Against Coordinated Cyber and Physical Attacks: Unified Theories and Technologies

Xiaofeng Wang[1], Naira Hovakimyan[2], Lui Sha[3] and Petros G. Voulgaris[4]

[1]College of Engineering and Computing, University of South Carolina

[2]Department of Mechanical Science and Engineering, [3]Department of Computer Science, [4]Department of Aerospace, University of Illinois at Urbana-Champaign

Award Number: ECCS-1739732, ECCS-1739886

MOTIVATION

Challenge: Signal processing, robust fault-tolerant control (RFTC) theory and the software assurance technologies are developed under different assumptions and models.

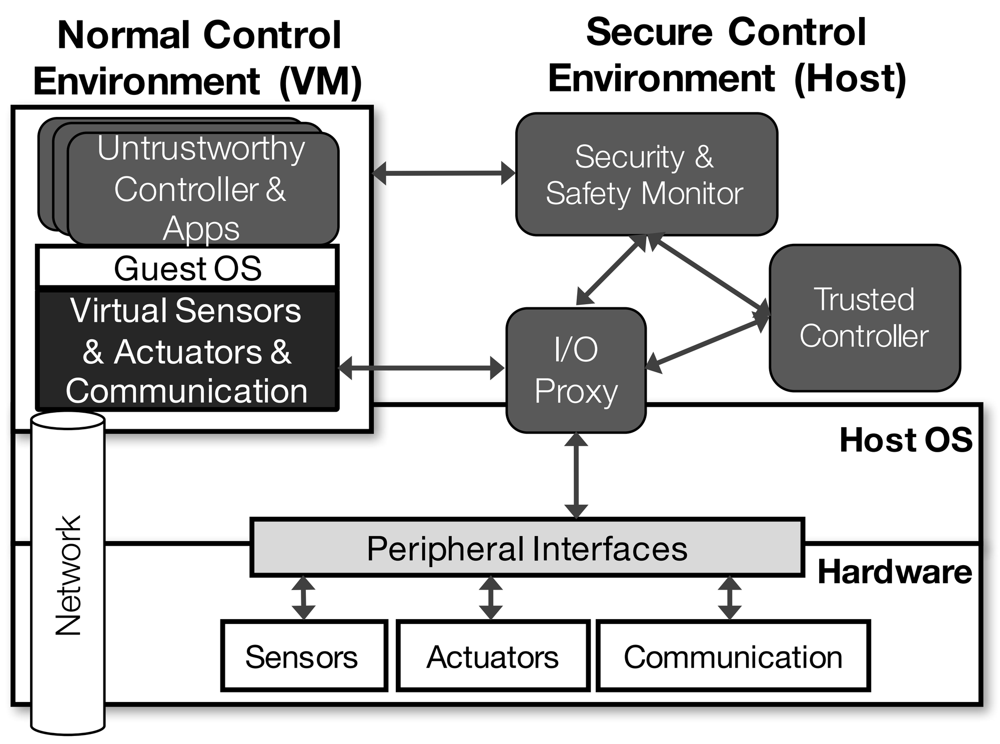
- The software assurance technologies are usually model-based that require the profile of the physical dynamics and the observation of the system state.
- Though the existing RFTC techniques can efficiently compensate for the physical damage, it is critical to guarantee that the control software and the sensor data are not compromised.

Goal: *Unified models with coherent set of assumptions, supported by integrated technologies that can defend against CCPA, are the focus of this research.*

ATTACK-RESILIENT SIMPLEX (ARSIMPLEX) ARCHITECTURE

ARSimplex software architecture:

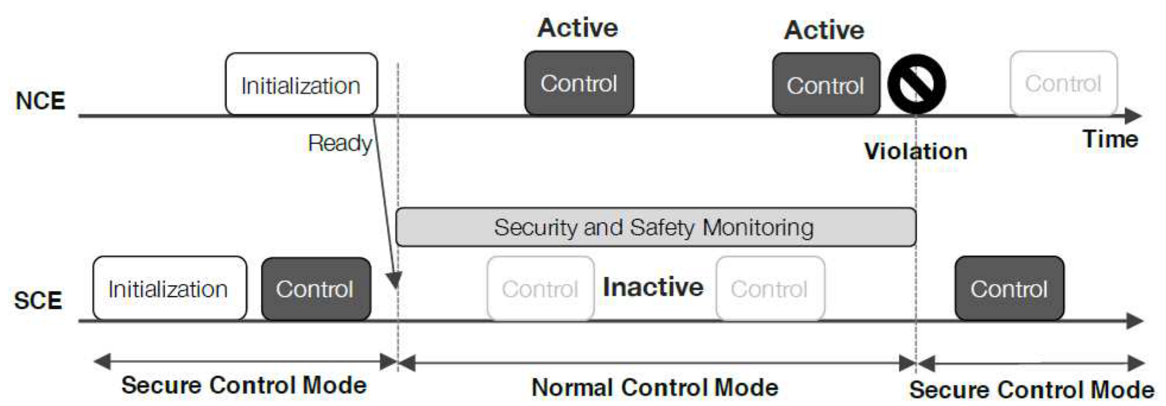
- ***Normal Control Environment (NCE):*** It runs software components for any normal function.
- ***Secure Control Environment (SCE):*** It runs a minimal set of software components that are critically required to control the physical system.



ARSimplex Architecture [1].

Features:

- A Simplex design, *i.e.*, using simplicity to control complexity.
- Creates a Trusted Computing Base (TCB) that promptly acts upon security and safety violations by closely monitoring the behavior of untrustworthy components.
- This architecture can be achieved by taking advantage of modern embedded processors that feature virtualization technology.



Switching between NCE and SCE

Control Modes:

- *High-Performance Controller (HPC) mode in the NCE*. The HPC is designed with the purpose of optimizing system performance. It can adopt a complex software structure and therefore may not be fully certified.
- *Robust High-Assurance Controller (RHAC) mode in the SCE*. The RHAC is a feedback controller that ensures safe and stable operation of the system with limited levels of performance and reduced functionalities.
- *Open-Loop Emergency Controller (OLEC) mode in the SCE*. The OLEC guarantees safety in emergency situations (e.g., not enough feedback is available for HPC or RHAC).

SAMPLED-DATA DRIVEN DETECTION and ADAPTATION for RESILIENCE AGAINST STEALTHY ZERO-DYNAMICS ATTACKS

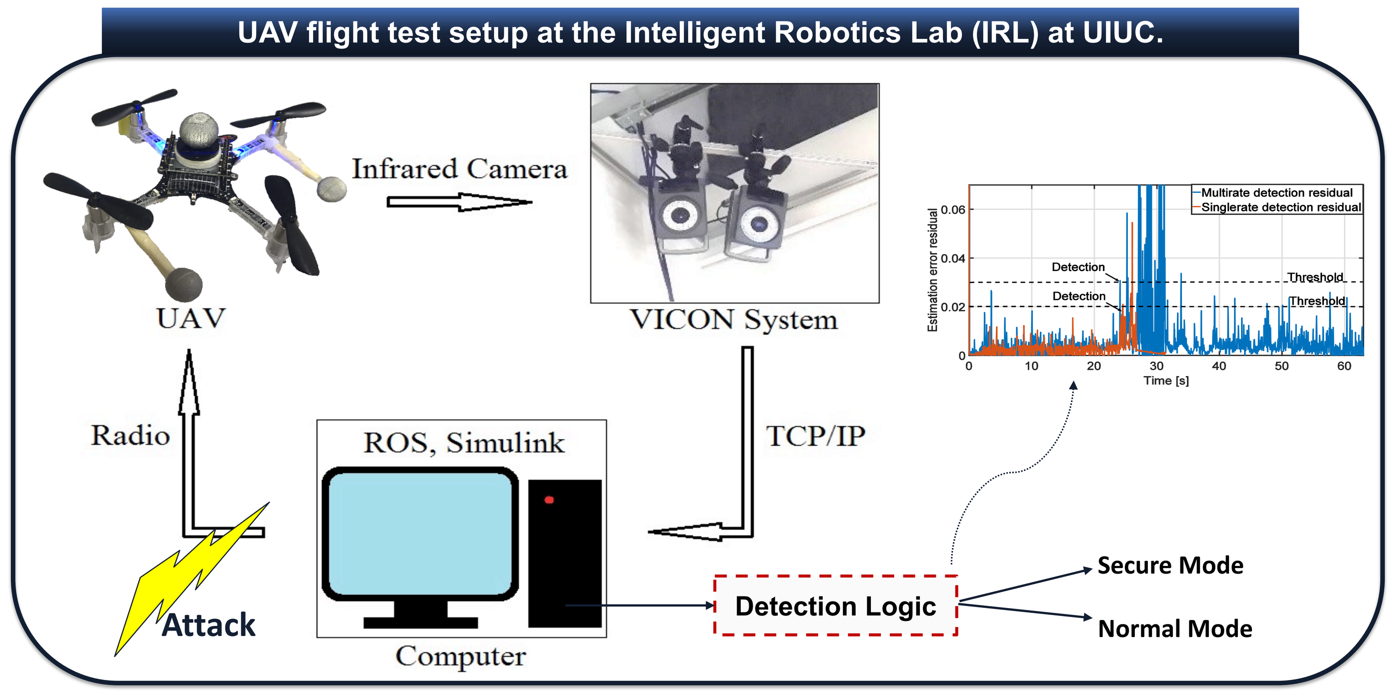
Challenge: Digital implementation of controllers in CPSs generates vulnerability to *stealthy zero-dynamics attacks*, which are hardest to detect from a control theory perspective.
Mutirate adaptive control as the RHAC: By multirate sampling, certain unstable zeros of a discrete-time system can be removed. This research aims to extend the L1 adaptive control theory to multirate sampled-data framework for the purpose of:

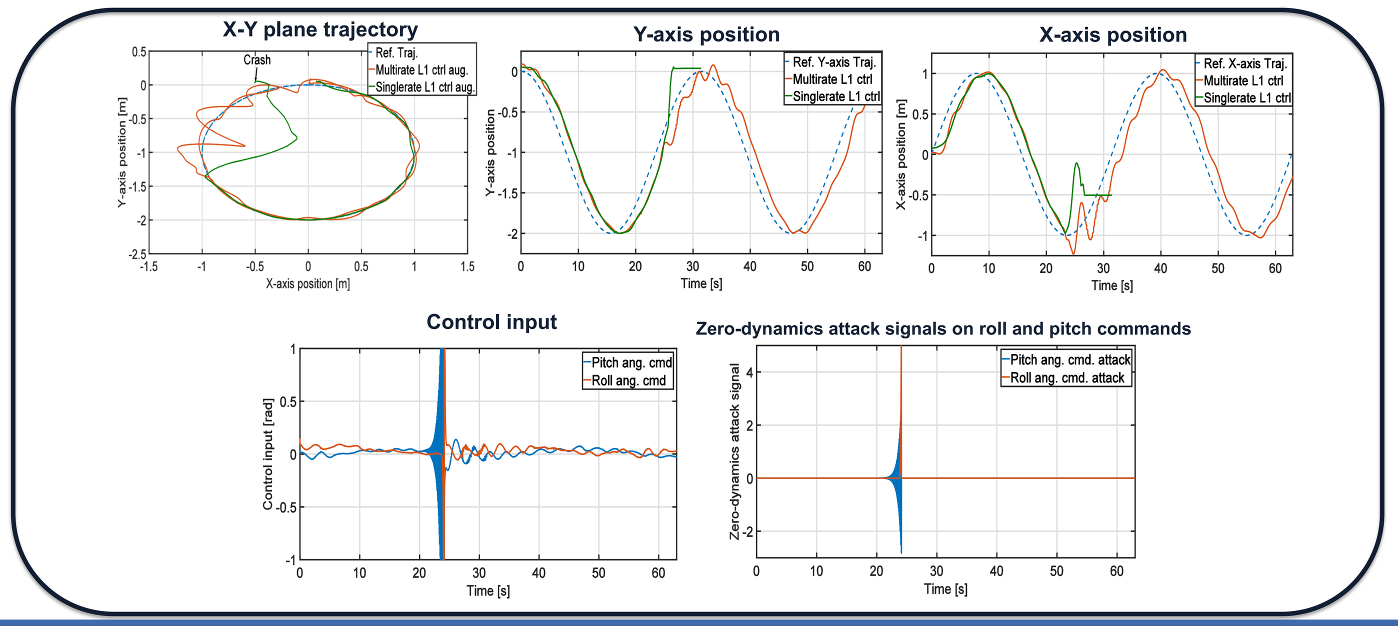
- Compensation for uncertainties and adaptation to failures.
- Detection of cyber and physical failures/attacks such as stealthy sensor/actuator attacks by the fast estimation loop.

Testbed:

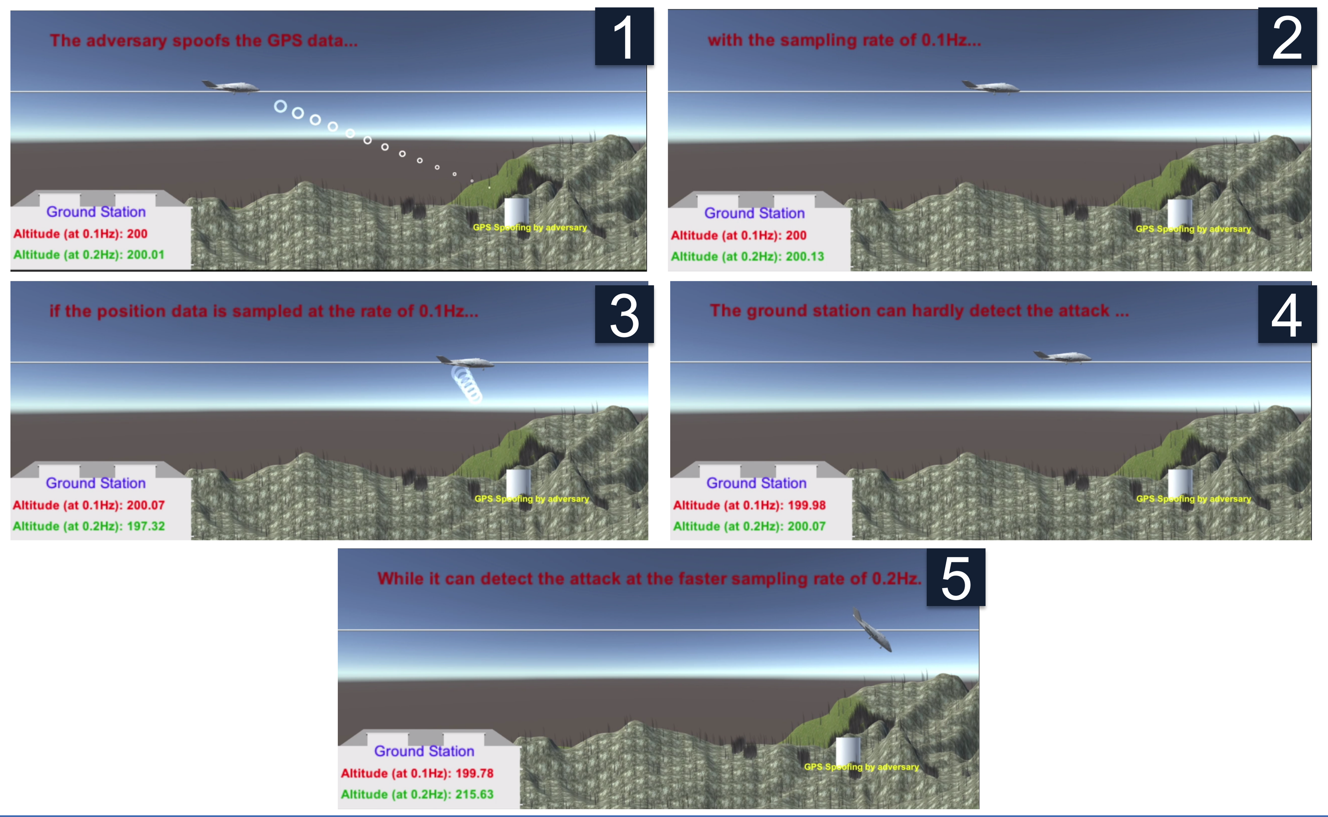
- We focus on UAV platforms (fixed-wing and quadrotor drones) to illustrate the challenges and to validate the theoretical security solutions.
- Various software and physical fault/attack scenarios (ex. sensor/actuator attacks, malware execution, ...) are considered.

UAV flight test setup at the Intelligent Robotics Lab (IRL) at UIUC.





A dual rate L1 adaptive controller is augmented to a multirate sampled-data (MSRD) baseline controller for attack detection and mitigation. A residual calculated based on the output prediction error in the dual rate L1 control structure can quickly detect a zero dynamics attack.

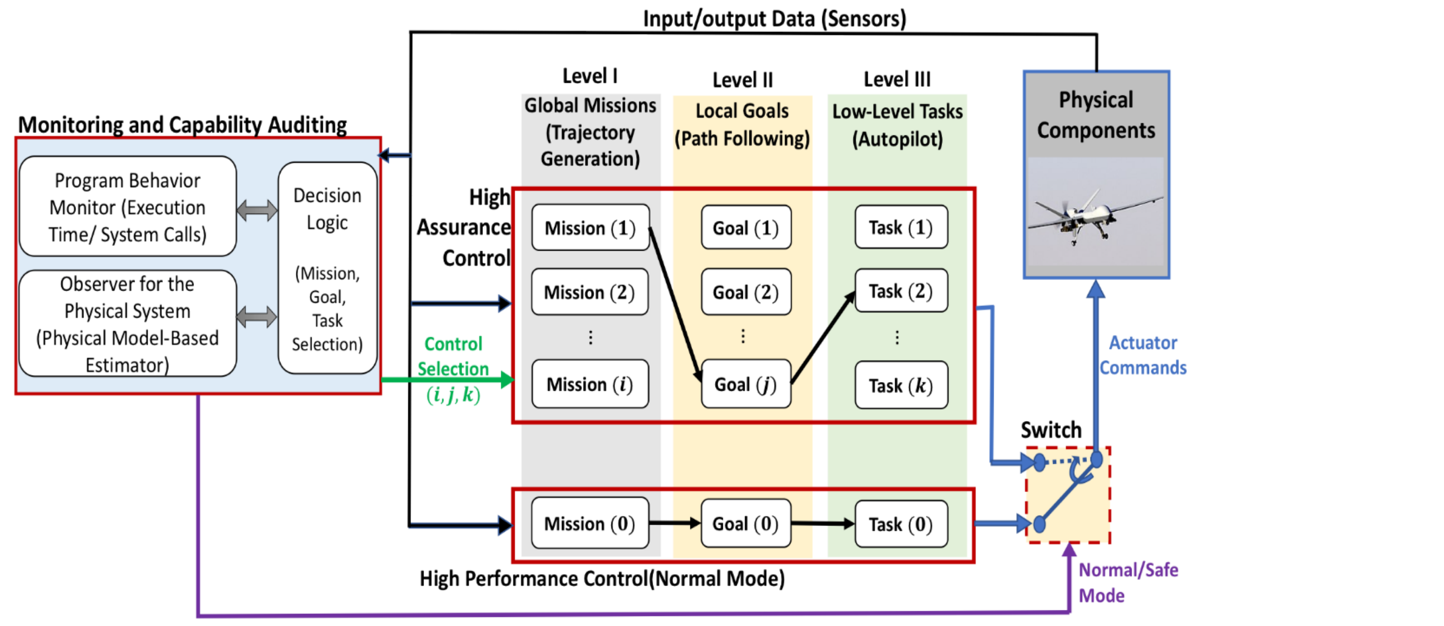


Zero-dynamics attack on altitude measurement (via GPS spoofing) is simulated to show the advantage of multirate sampling scheme in detecting stealthy attacks.

CCPA-RESILIENT AUTOPILOT DESIGN for AUTONOMOUS DRONES

Multi-Level Control Design for Autonomous drones: To address zero-day emergencies due to CCPA, a multilevel control strategy [6] can be used for adaptation of high level missions, local goals, and low-level control tasks to uncertainties

- The multi-loop structure is used for navigation and control of autonomous drones
- Decoupling between the outer loop and the inner loop for reliable implementation and to satisfy input/state constraints.
- The control strategy can be integrated with Simplex fault-tolerant architecture

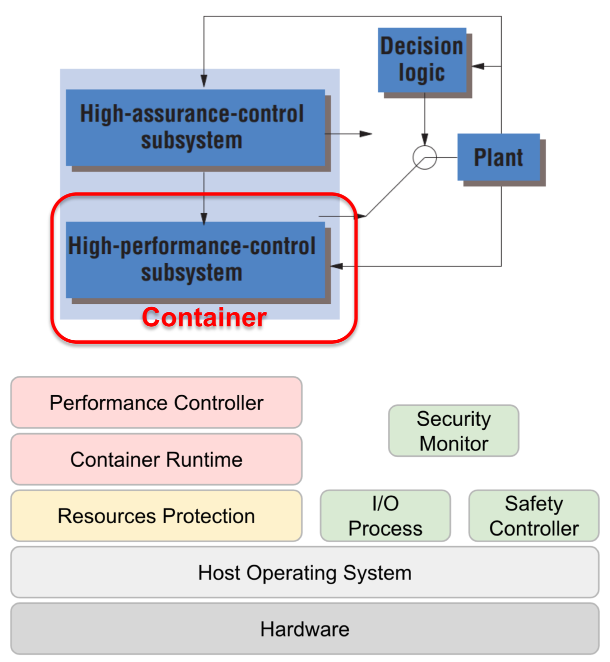


Simplex structure can be integrated with the proposed multi-level multirate approach for navigation and control of autonomous CPSs.

CONTIANER-BASED DoS ATTACK-RESILIENT CONTROL FRAMEWORK FOR REAL-TIME UAV SYSTEMS

A novel Denial-of-Service (DoS) attack-resilient control framework for real-time UAV system is developed using containers.

- **Simplex architecture:**
  - Safety controller running on host environment
  - Performance controller running inside container
- **Three level of resources protection:**
  - *CPU:* Linux Cgroup[1] limits cpu core and utilization
  - *Memory:* Linux Cgroup limits memory size, Memguard[2] limits memory bus bandwidth
  - *Communication:* Simulated sensors and actuators, security monitoring



- **Implementation:**
  - Hardware: Raspberry Pi 3B, Navio 2 sensor board Prototype drone
  - Software: Linux 4.4, Docker container[3], PX4 autopilot[4]

[1]Linux control groups, [online] Available: http://man7.org/linux/man-pages/man7/cgroups.7.html.
[2]Yun, Heechul, et al. "Memguard: *Memory bandwidth reservation system for efficient performance isolation in multi-core platforms." Real-Time and Embedded Technology and Applications Symposium (RTAS),* 2013 IEEE 19th. IEEE, 2013.
[3]Docker container, [online] Available: https://www.docker.com/resources/what-container.
[4]PX4 autopilot, [online] Available: https://dev.px4.io/en/.

REFERENCES

[1] M.-K. Yoon, B. Liu, N. Hovakimyan, and L. Sha, "VirtualDrone: Virtual sensing, actuation, and communication for attack resilient unmanned aerial systems," in *Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems*, 2017.
[3] H. Jafarnejadsani, H. Lee, N. Hovakimyan, and P. G. Voulgaris, "Multirate Adaptive Control for MIMO Systems with Application to Cyber-Physical Security", 57th IEEE Conference on Decision and Control, Miami, IL, December 2018 (accepted).
[2] H. Jafarnejadsani, H. Lee, N. Hovakimyan, and P. G. Voulgaris, "Dual-rate L1 Adaptive Controller for Cyber-Physical Sampled-Data Systems", *IEEE Conference on Decision and Control*, 2017.
[4] X. Wang, N. Hovakimyan, and L. Sha, "RSimplex: A Robust Control Architecture against Cyber and Physical Failures", to appear in *ACM Transactions on Cyber-Physical Systems*.
[5] X. Wang and L. Yang, "Sporadic Model Predictive Control Using Lebesgue Approximation", *American Control Conference*, May 2017.
[6] H. Jafarnejadsani, N. Wan, N. Hovakimyan, and P. G. Voulgaris, "A Multi-Level Sampled-Data Approach for Resilient Navigation and Control of Autonomous Systems," International Journal of Robust and Nonlinear Control, 2018 (submitted).

UNIVERSITY OF SOUTH CAROLINA

ILLINOIS — UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN