CNS1505701
Security and Privacy-Aware Cyber-Physical Systems

Miroslav Pajic

miroslav.pajic@duke.edu

Cyber-Physical Systems Lab (CPSL)

Department of Electrical and Computer Engineering

Department of Computer Science

Pratt School of Engineering

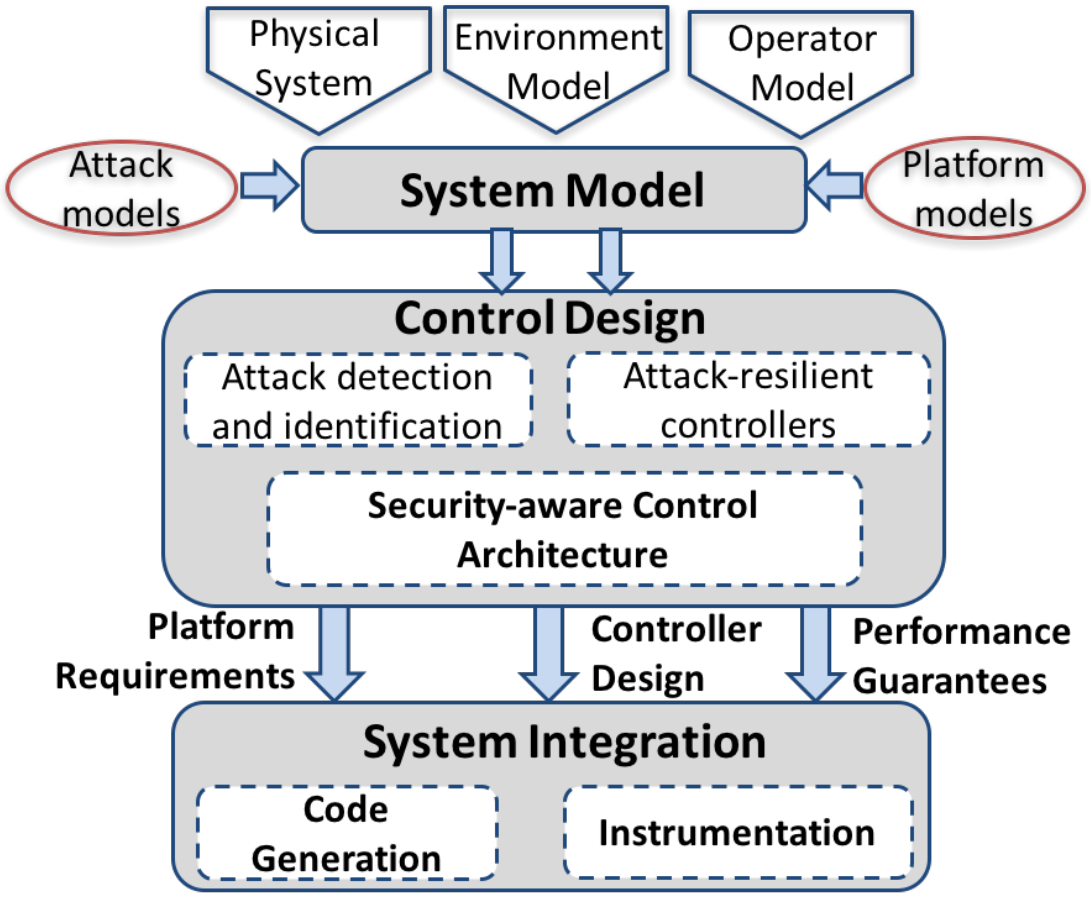
Duke University

Duke UNIVERSITY | PRATT SCHOOL of ENGINEERING

DUKE ROBOTICS

Platform-Aware Design Framework for Attack-Resilient CPS

Duke
PRATT SCHOOL OF
Engineering



– Control-level techniques
  - Attack detection and identification using redundant sensing and model of the system's dynamics
  - Attack-resilient control architectures

– Code-level techniques
  - Ensure that the control code is correctly implemented and integrated
  - Preventing malicious code injection into the controller

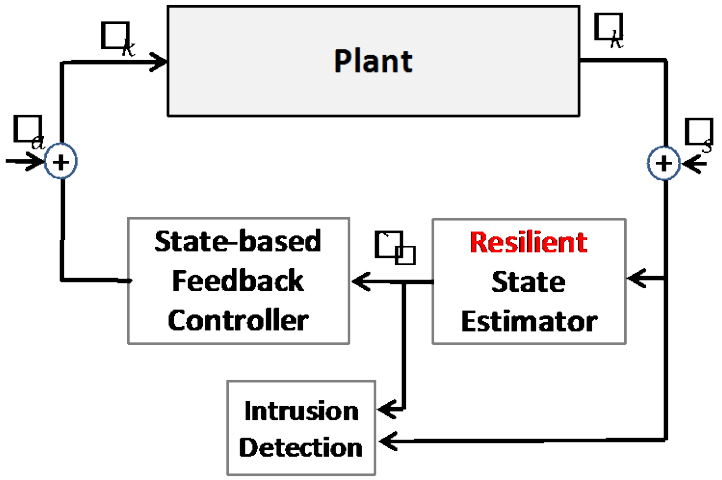
Goal: Ensure that the system maintains a degree of control even when the system is under ***cyber*** and/or ***physical*** attack

Integrity Requirements for Resilient Cyber-Physical Systems

Duke
PRATT SCHOOL OF
Engineering

Challenges:

- Existing security-aware control techniques impose very restrictive systems assumptions
  - No noise in the system
  - No DoS attacks
  - Only a subset of sensors can be compromised
- Very conservative requirements on data-integrity

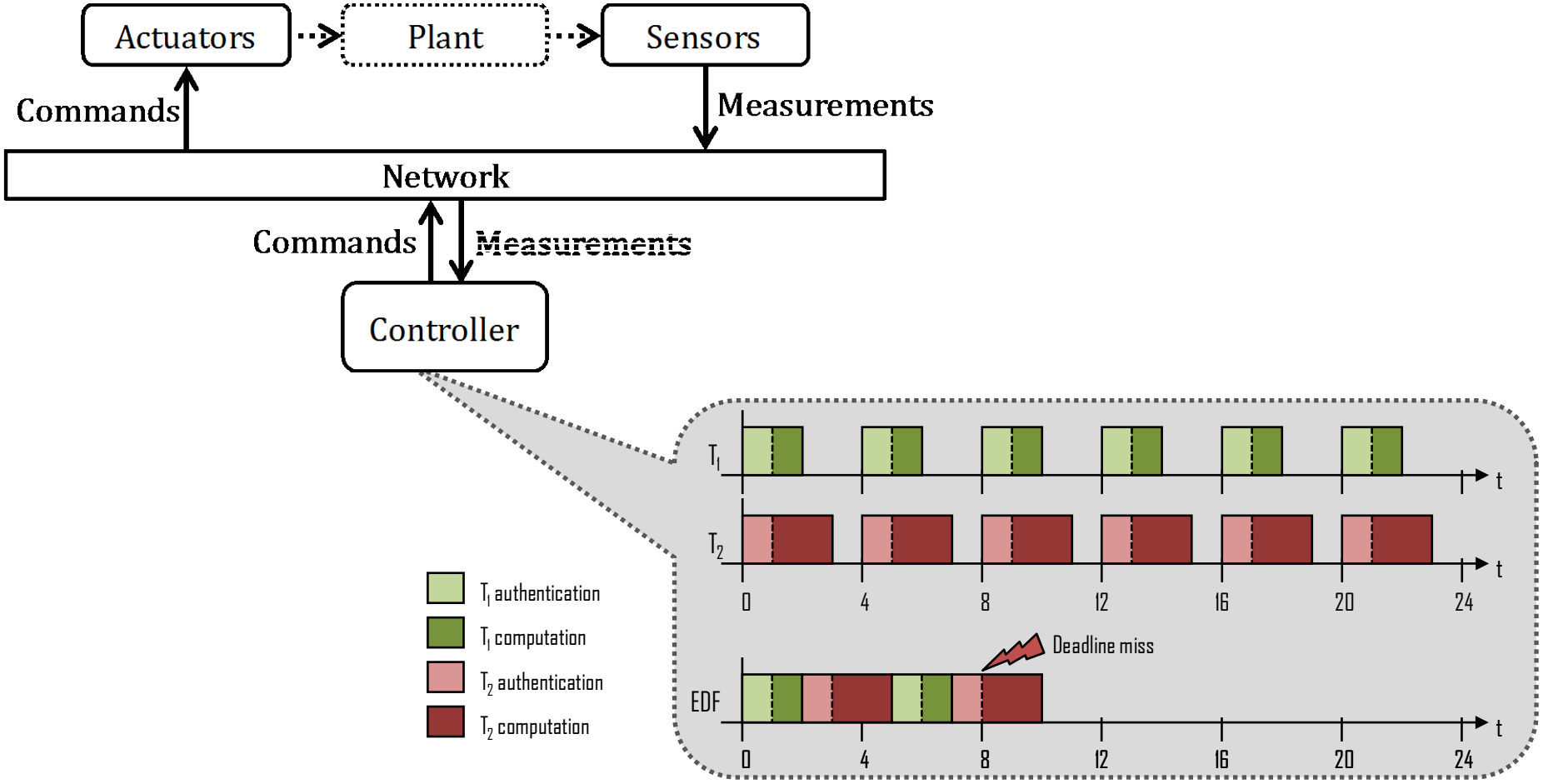


Solutions:

- Attack-resilient state estimation in the presence of noise [CDC'15,CSM'17,TCNS'16]
  - Formal robustness guarantees even for the computationally efficient convex-optimization based estimator
- Control-aware *intermittent* integrity enforcement – e.g., using Message Authentication Codes (MAC) [CDC'17,RTSS'17,EMSOFT'17/ACM TECS'17]
  - Case studies: design of resilient automotive features over
    - CAN bus, V2V/I – resilient & safe trajectory following with < 20% packets with MAC

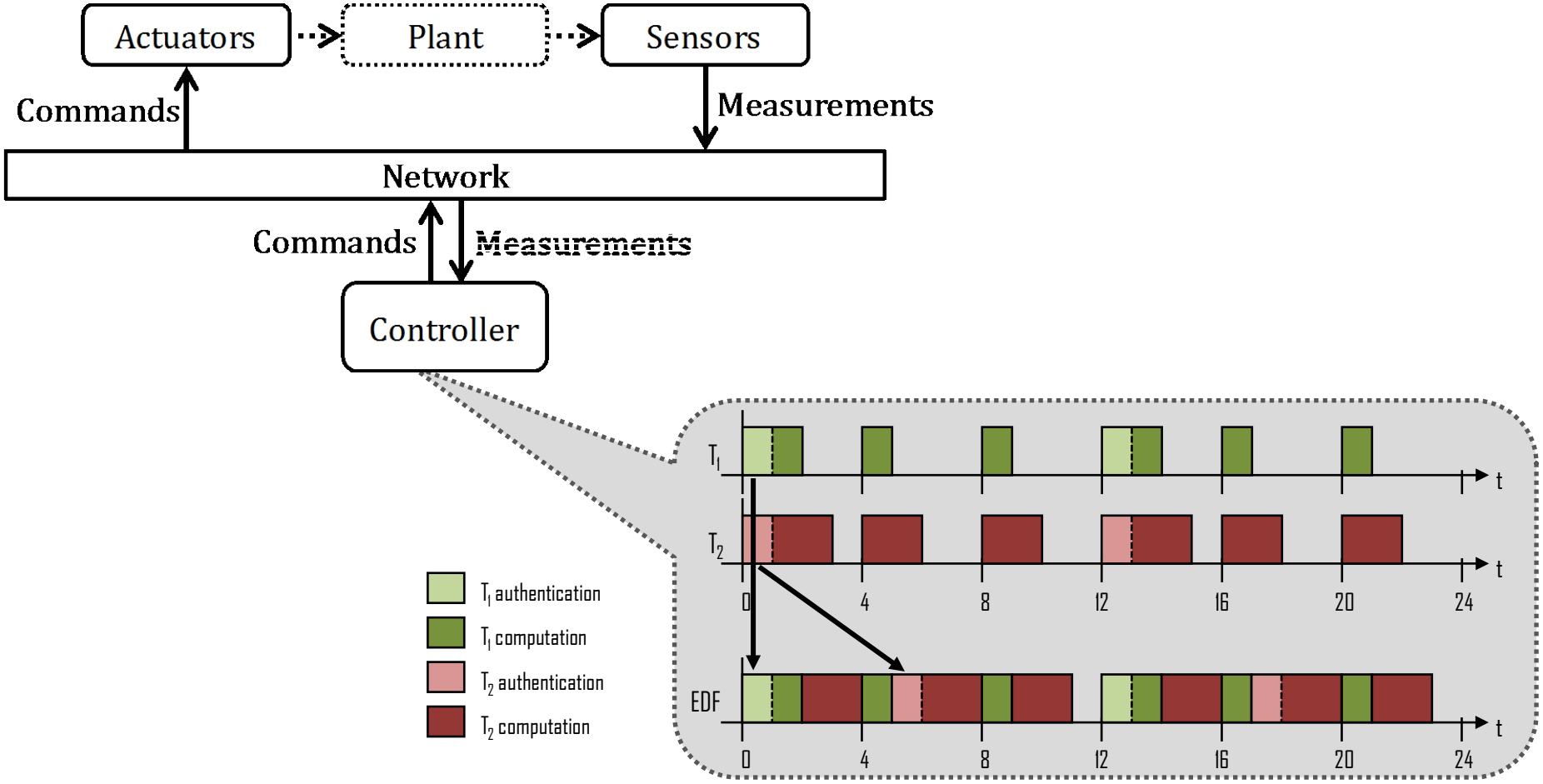
Standard Architecture Under Consideration
Can we afford security-related overhead?

Duke
PRATT SCHOOL OF
Engineering



Standard Architecture Under Consideration
Idea– Exploit physics to relax security overhead

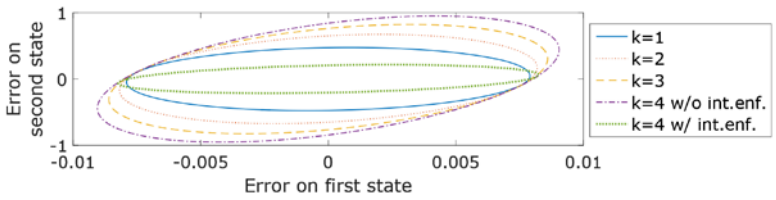
Duke
PRATT SCHOOL OF
Engineering



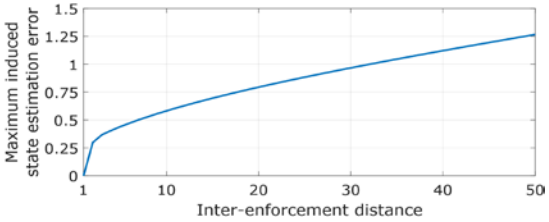
Security-Aware Scheduling in CPS
Co-design reduces security-related overhead

Duke
PRATT SCHOOL OF
Engineering

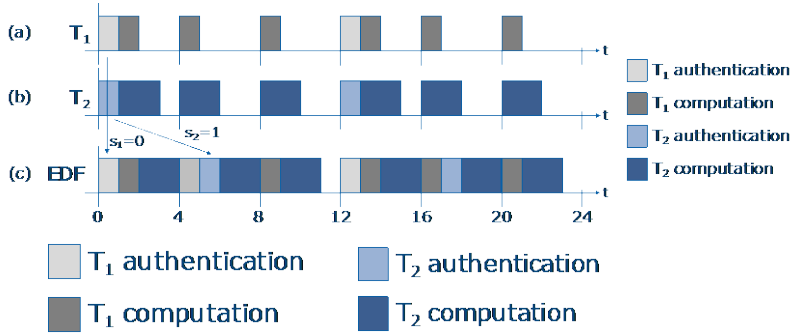
Reachable regions for a trajectory tracking system

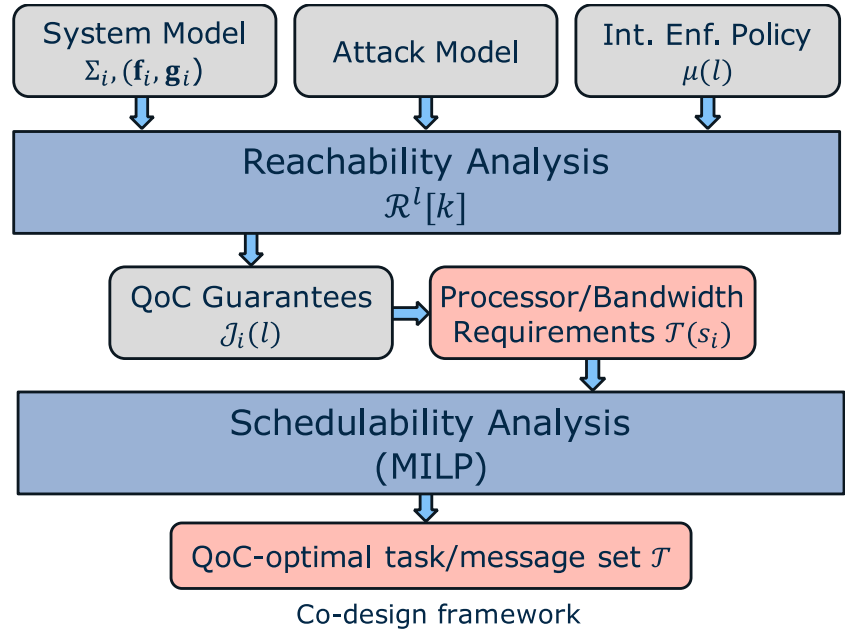


QoC degradation curve for a vehicle trajectory system

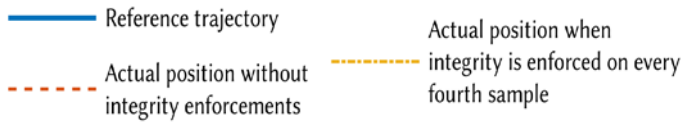


Real-time requirements

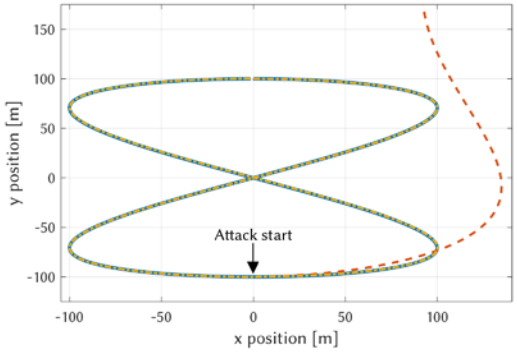




Co-design framework



Trajectory tracking with <15% of authenticated messages



- V. Lesi, I. Jovanov, and M. Pajic, "Security-Aware Scheduling of Embedded Control Tasks", **Best Paper Award at EMSOFT 2017**.
- V. Lesi, I. Jovanov, and M. Pajic, "Network Scheduling for Secure Cyber-Physical Systems", RTSS 2017.

Thank You