FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Monitoring, Diagnosis, Control, and System/Security Codesign for CPS

Waseem Abbas, Amin Ghafouri, Gabor Karsai, Xenofon Koutsoukos, Aron Laszka, David Lindecker, Istvan Madari, Janos Sztipanovits

Berkeley University of California
Massachusetts Institute of Technology
NSF
Michigan
Vanderbilt University

Overview

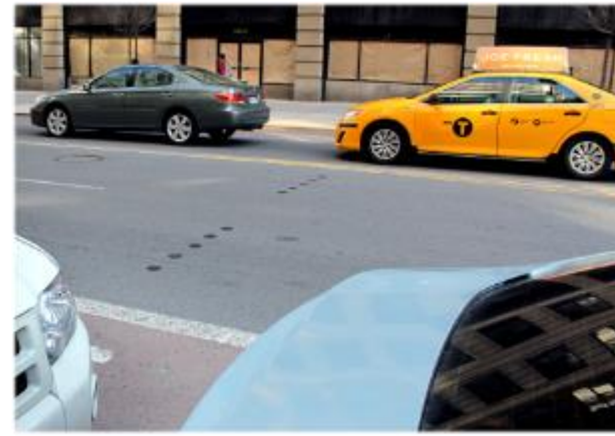
* Resilient Monitoring
  * Attack-resilient observation selection
  * Mobile guards
  * Placement and scheduling of intrusion detection in CPS
  * Optimal monitoring to mitigate attacks
* Diagnosis
  * Sensor placement for fault detection and localization
  * Network monitoring: DDS detection and mitigation
* Control
  * Resilient supervisory control for autonomous traffic intersections
  * Attack-resilient traffic control
* System/security codesign
  * Information Flow Policies in Cyber-Physical Systems
  * Platform-supported Resilience for CPS

Resilient Monitoring for CPS

Attacks against CPS Monitoring

A. Laszka

* To dynamically control any system, we must have accurate information about its evolving state
* An attacker may compromise sensors in order to maliciously alter control decisions
* For example, recent studies have found vulnerabilities in many traffic sensors
  * an attacker may cause disastrous traffic congestions by compromising these sensors



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Sensor Placement

A. Laszka

- We assume a denial-of-service type attacker, who impairs some of our sensors after they have been deployed
- **Resilient placement problem**: placing sensors so that even if some of them are impaired, we can still perform state estimation and prediction with minimal uncertainty
- Results:
  - computational complexity (NP-hardness)
  - approximation algorithms
  - optimal algorithms for special cases
- Traffic simulation results on the Vanderbilt campus area show that resilient placement can reduce uncertainty by 67%

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Guarding Networks through Mobile Heterogeneous Guards

W. Abbas

* Mobile guards (such as UAVs) are being increasingly used for the surveillance and monitoring of critical infrastructure networks such as gas and oil pipelines.

* Advantages include increased efficiency, deployment in remote areas, cost-effectiveness, immediate response etc.

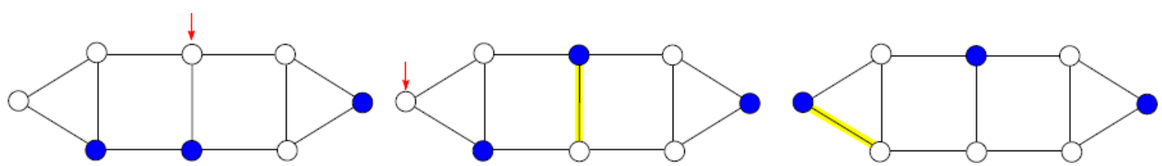
* Challenges: Using the capabilities of mobile guards and considering the network structure
    * How many guards should be deployed?
    * At what critical points within the networks?
    * What could be the movement strategies of guards?

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Guarding Networks through Mobile Heterogeneous Guards

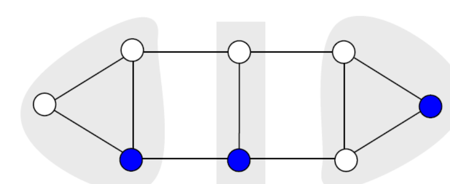
W. Abbas

- Mobile guards' deployment within a network for the detection and response against intruders can be related to the ***eternal security*** type problems in graphs.
- **Eternal security:** At all times, all nodes are being guarded by at least one guard even after a guard moves from one node to the other in response to an intrusion activity.



- **Major issues**: How many guards? Where to deploy? Which guard should respond?
- Finding optimal number of guards to achieve eternal security is *NP-hard*.
- We propose a an efficient algorithm to achieve eternal security through mobile guards having different detection and response ranges.
- **Basic idea:**

Partition a graph into appropriate clusters → Assign appropriate guard to each cluster → Nodes in each cluster are eternally secured by its guard

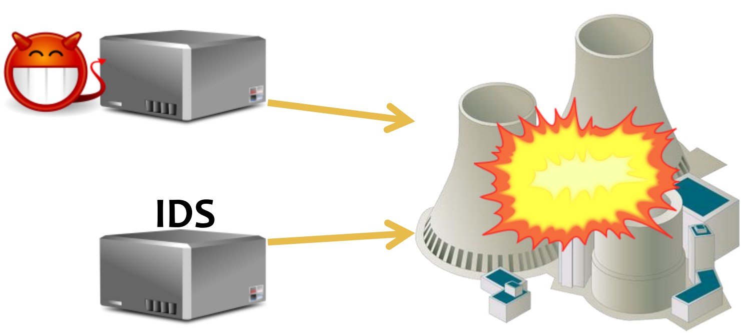


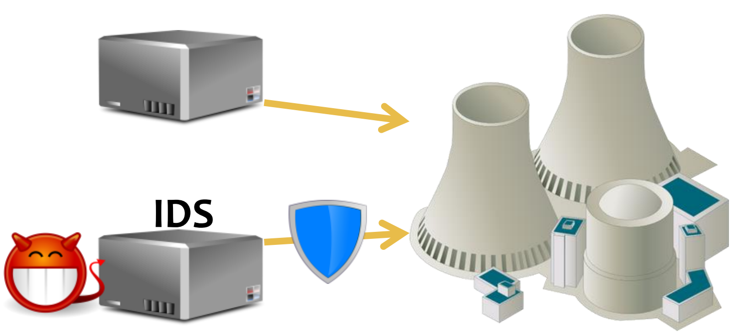
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Intrusion Detection Systems (IDS) for CPS

W. Abbas, A. Laszka

* IDS alarms about the attack before it can cause major damage
* Deploying IDS can increase the resilience of CPS
* Challenges:
  * CPS may have resource bounded (e.g., limited energy supply, computational capabilities) devices
  * IDS may not be deployed at every node, or may not be active at all times
* Thus, **placement and scheduling** problems need to be solved





Example: IDS for Water Distribution Networks

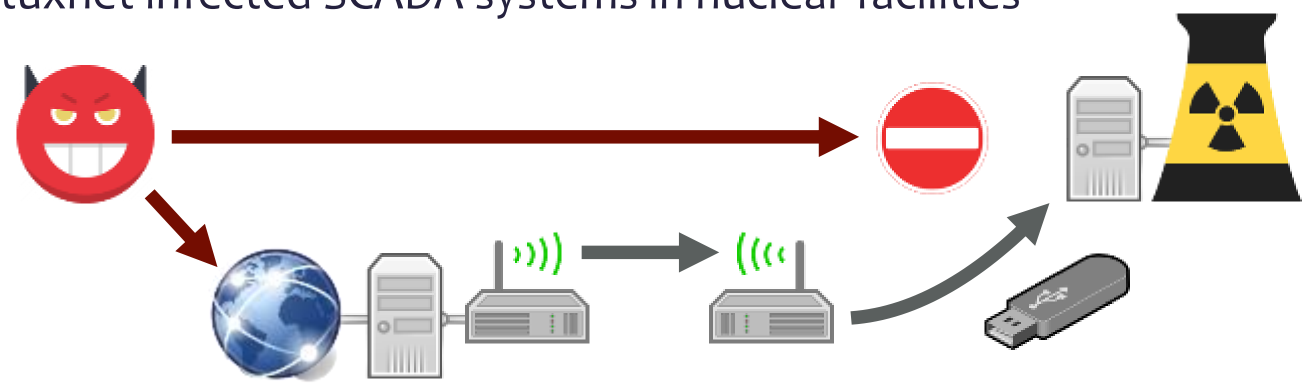
W. Abbas, A. Laszka

- Leaks may occur in the pipes, which can be detected by sensors deployed at various points
- An attacker might compromise sensors to generate false alarms or to suppress valid alarms
- We assume resource-bounded sensing devices, and formulate the scheduling problem for optimal detection of attacks with respect to the minimization of losses
- Results:
  - Computational complexity (NP hard)
  - Heuristics
  - Special cases

Computer Worms and CPS

A. Laszka

* Highly sensitive cyber-physical systems (e.g., control systems for nuclear facilities) are usually supposed to be secured by the "air gap"
* However, computer worms that propagate over removable drives and local networks may infect even these systems
  * e.g., Stuxnet infected SCADA systems in nuclear facilities



* In order to stop a worm before it can cause substantial damage to our system, we have to be able to detect it in time

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Optimal Monitoring to Mitigate Attacks

A. Laszka

* Worm propagation is modeled as a non-deterministic diffusion process
* Defender can monitor a limited number of nodes for the presence of a worm (e.g., auditing log files to detect suspicious activity)
* Attacker can select some starting points for the worm
* Defender wins if the worm is detected some time before it reaches the target system (or if it never reaches the target system)
* Results:
  * non-strategic attacker: optimal deployment is NP-hard, but approximable
  * strategic attacker: optimal deployment is inapproximable, but we have good heuristics

Resilient Diagnosis for CPS

Sensor placement for fault detection and localization in water distribution systems

W. Abbas

Objective

For a given flow network (water distribution network), the goal is to distribute the minimum number of sensors that can

1) Detect a link failure AND
2) Identify a link failure (uniquely identify a link failure)

Approach:
Sensor network design for the detection and identification of faults

Evaluation:
Simulation of real networks

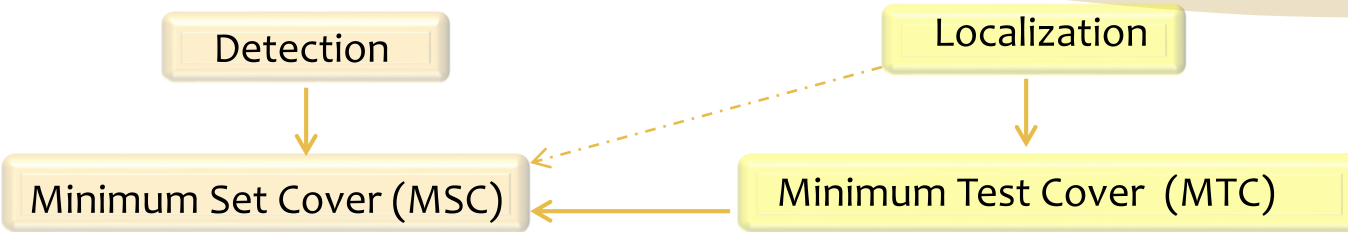
Methods:

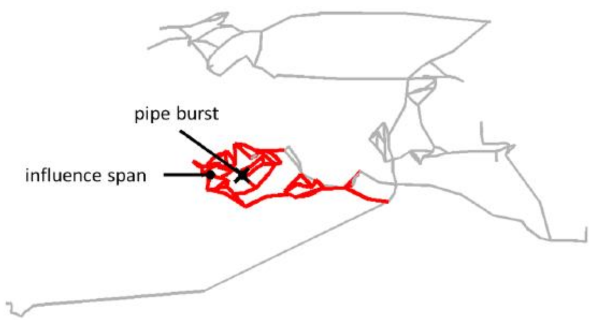
- System models (network flow model, fault model, sensor model, and influence model).
- Formulation of detection & localization as coverage problems.
- Submodular function optimization

Resilient monitoring:
Resilience to sensors failures, Performance evaluations

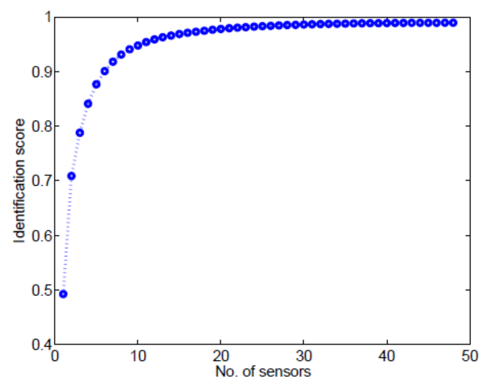
Sensor placement for fault detection and localization in water distribution systems

W. Abbas

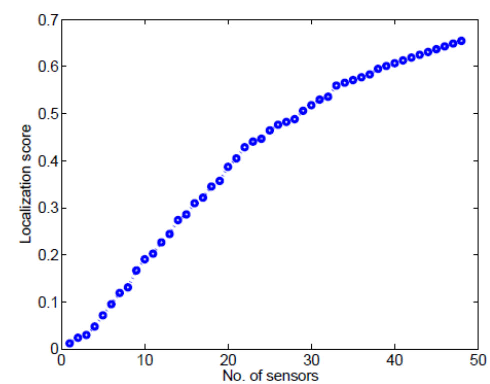




A water distribution network with 168 pipes and 129 nodes.



Identification score: Percentage of pair-wise link failures detected.

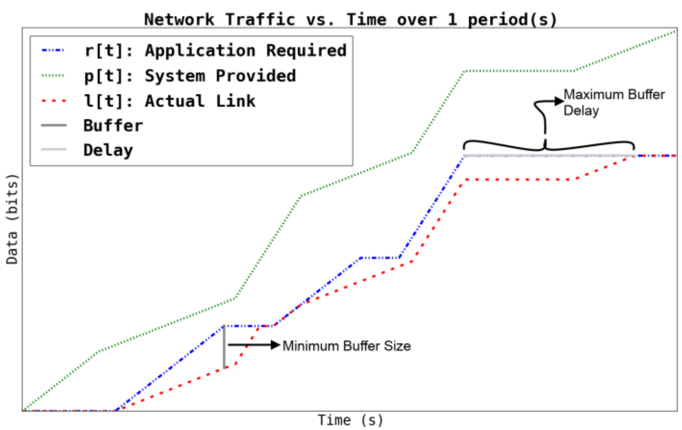


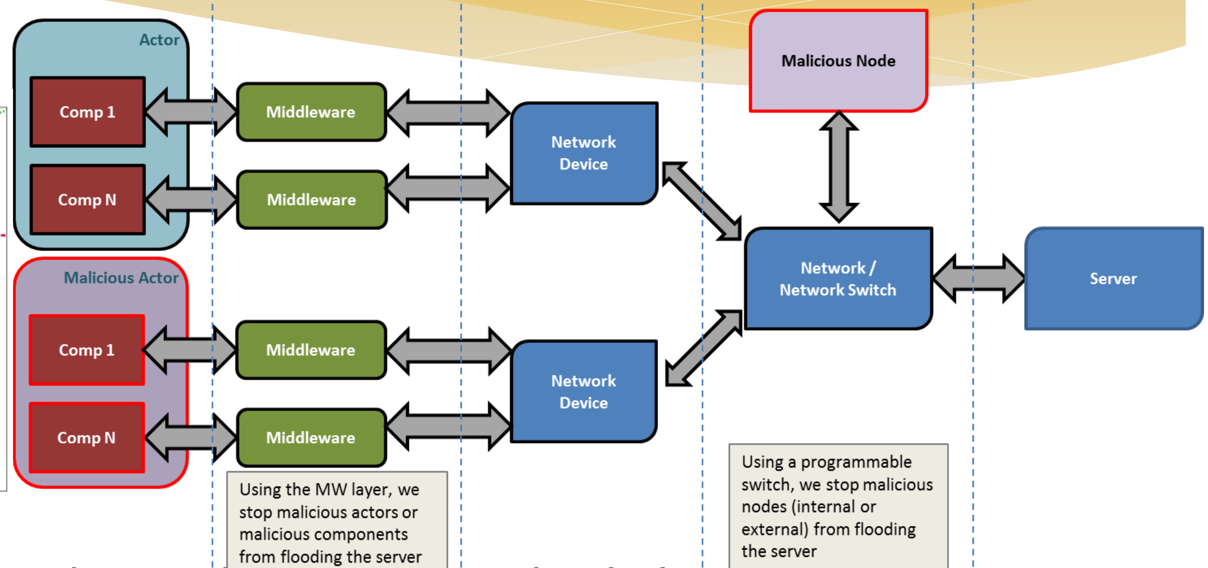
Localization score: Percentage of localization sets that can uniquely identify fault events.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

DDoS Detection & Prevention

W. Emfinger





* Using network modeling/analysis techniques based on Network Calculus
  * Precisely model application network behavior, with some bounds on deviation
* Assume infrastructure is controlled and verified; only applications may be compromised
* Middleware detects that application traffic production deviates from model
* Use out-of-band communication between server and clients
  * Server sees multiple clients simultaneously producing more data than normal
  * Informs client-side middleware to throttle clients and prevent denial of service

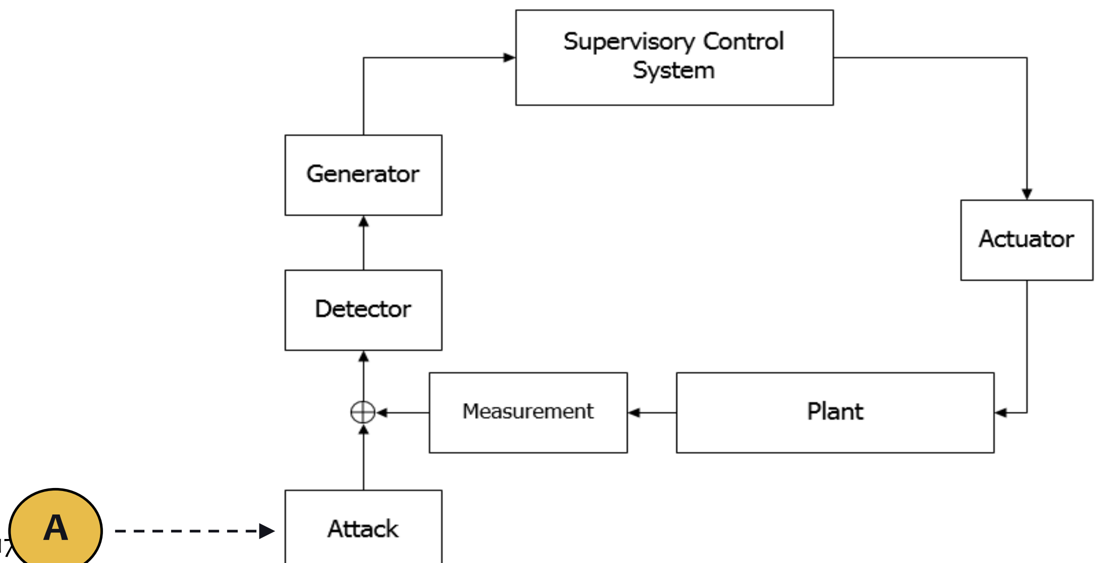
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attack-Resilient Control

Resilient Supervisory Control for Autonomous Intersection

A. Ghafouri

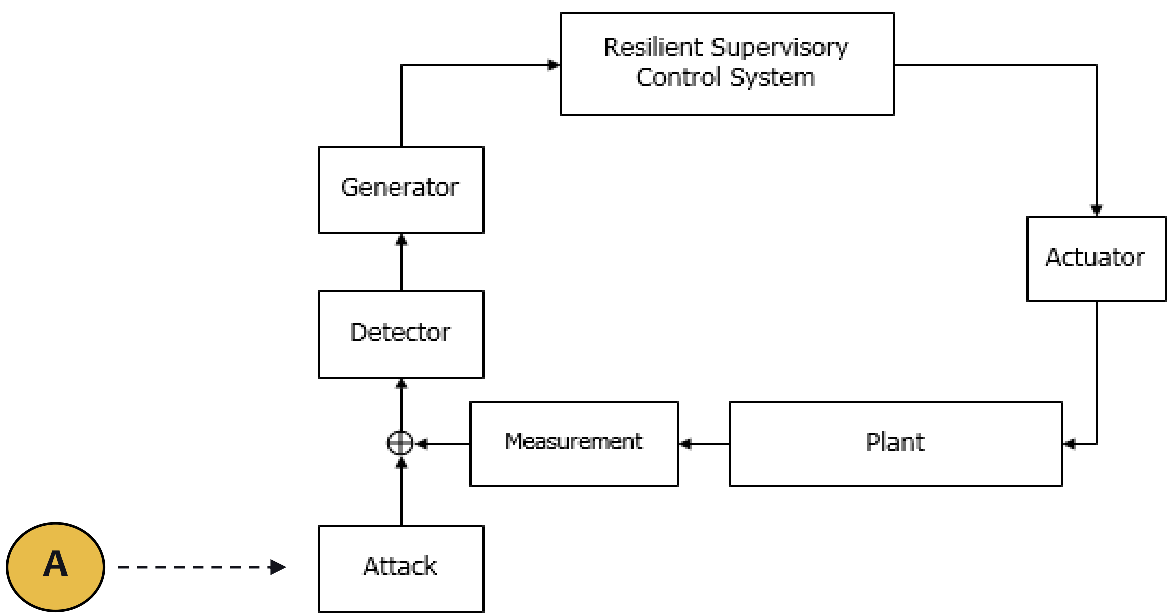
- Modeling sensor attacks for an autonomous intersection that is governed by the supervisory control system
- Characterization of *stealthy attacks* that compromise the safety of the system
- Developing an algorithm for finding all the successful attacks (i.e., stealthy attacks that lead to collision)
- Proving the vulnerability of the supervisory control system to stealthy attacks



Resilient Supervisory Control for Autonomous Intersection

A. Ghafouri

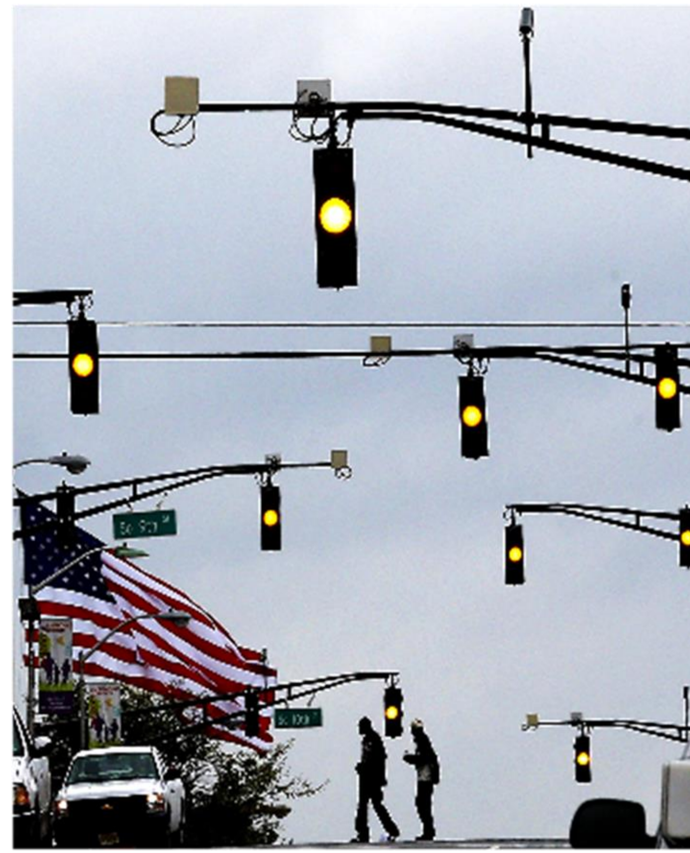
* Design of the **Resilient Supervisory Control System** (RSCS) ***(in progress)***
  * The RSCS is robust to stealthy deception attacks, i.e., safety will not be compromised even in the presence of stealthy attacks.
* Simulation and performance analysis of the RSCS using SUMO ***(in progress)***
  * Trade-off between resiliency and performance of the system is expected.



Attack-Resilient Traffic Control

A. Laszka

* Recent studies have shown that many traffic control devices (e.g., traffic lights) are vulnerable to cyber-attacks
* Attackers cannot cause accidents due to hardware-based failsafes , but they may cause disastrous traffic congestions
* **Resilient traffic control**: configuring traffic lights so that even if some of them are maliciously reconfigured, the level of traffic congestion remains minimal
* We study a game between a defender, who configures traffic lights, and an attacker, who compromises and reconfigures some of them



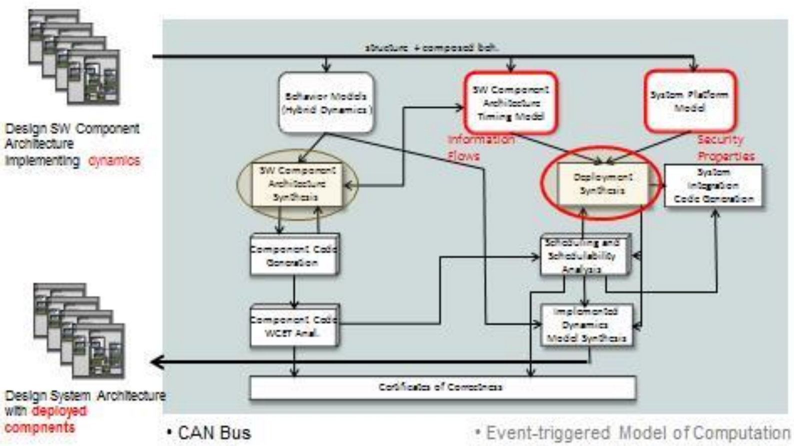
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

System-security Co-design

System-Level Co-design for CPS Security

D. Lindecker, I. Madari, J. Sztipanovits

System-level Synthesis Steps Information Architecture



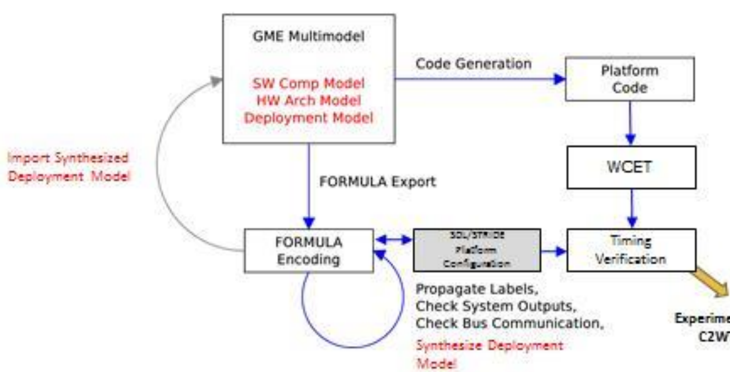
- CAN Bus
- TT bus

- Event-triggered Model of Computation
- Time-triggered Model of Computation

Challenges

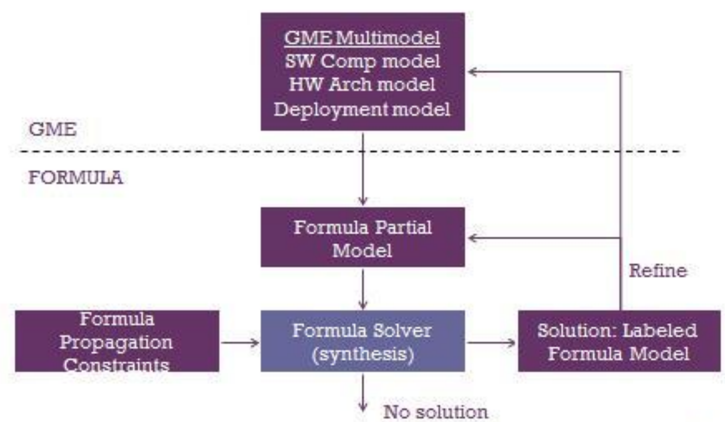
- Modeling language suite
  (behavior, information flows, SW components, architecture, timing, platform, deployment) - reuse previous work
- Security Requirement Modeling
  (need to be composable with other modeling aspects)
- Common Semantic Domain and Formal Framework
  (functional, performance and security models need to be anchored to a semantic domain suitable for synthesis)
- Synthesis Framework and Co-design flow
  (mapping system-level synthesis problem on the formal framework and tools)
- Integrated Tool Suite and Validation
  (target domain rich enough for testing the co-design tool suite)

Workflow for Designing Secure Distributed Embedded Systems



FORCE
FOUNDATIONS OF RESI
CYBER-PHYSICAL SYS

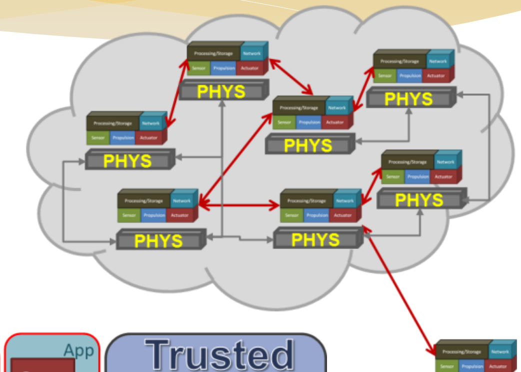
Label Propagation and Synthesis

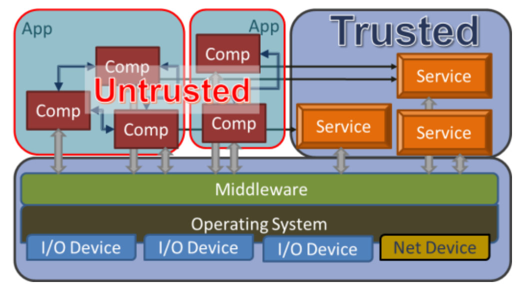


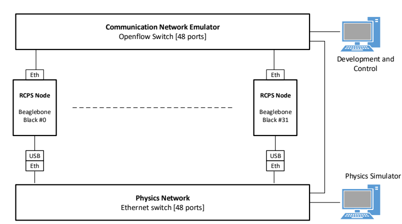
Platform-supported Resilience for CPS

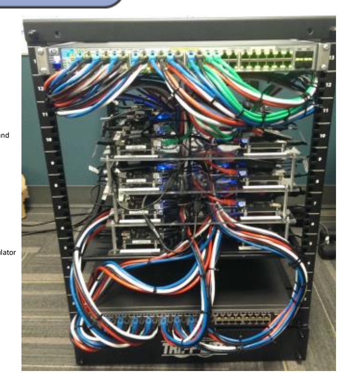
W. Emfinger. G. Karsai, P. Kumar

- Resilience is a system-level property, permeating the entire CPS architecture
- Model: Trusted (and protected) platform + Untrusted apps
- Challenges:
  - How to model the resilient architecture? What makes it resilient?
  - How to build a resilient software application platform for CPS?
  - How to analyze in a scalable manner to obtain assurances for resilience?
- Resilient CPS Platform
  - Component-based application model: component model with interaction semantics
  - Application deployment model: trusted and managed deployment
  - Resource monitoring and constrained information flows on the platform level
  - Hardened platform interfaces and services
- CPS Experimentation:
  - Embedded controllers + Emulated network + Physics sim









FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS