SYSTEM SCIENCE OF SECURITY AND RESILIENCE FOR CYBER-PHYSICAL SYSTEMS (SURE)

XENOFON KOUTSOUKOS

VANDERBILT UNIVERSITY

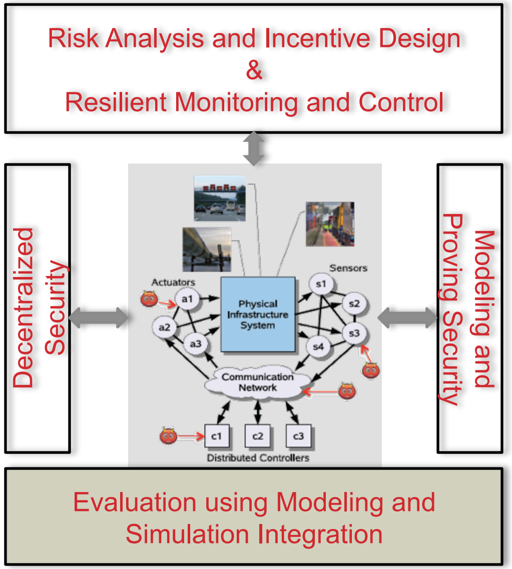
PROJECT KICKOFF MEETING – 2014 OCTOBER 27

VANDERBILT UNIVERSITY Berkeley UNIVERSITY OF CALIFORNIA Massachusetts Institute of Technology INFORMATION & COMPUTER SCIENCES UNIVERSITY of HAWAI'I at MĀNOA

SURE

SYSTEM SCIENCE OF SECURITY AND RESILIENCE OF CPS

SURE

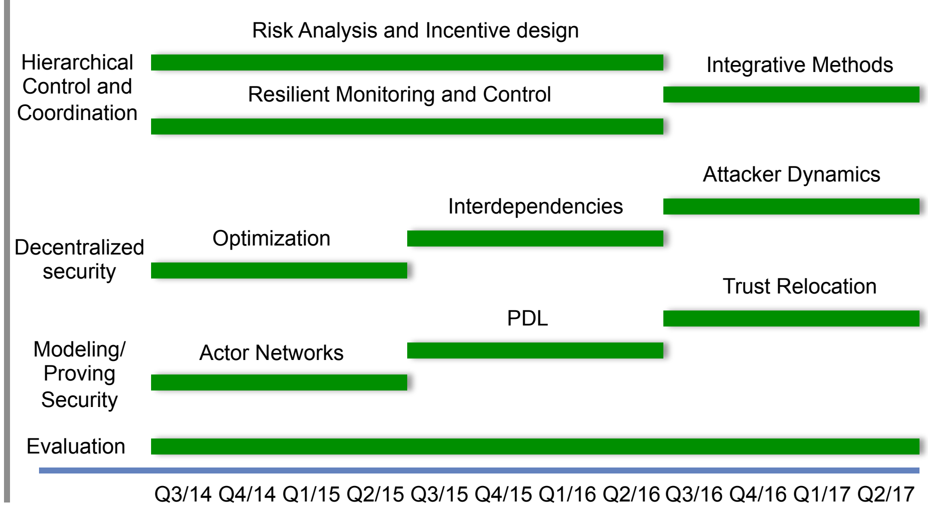


Key Ideas

1. Hierarchical Control and Coordination
   1. Risk analysis and incentive design that aim at developing regulations and strategies at the management level
   2. Resilient monitoring and control of the networked control system infrastructure
2. Science of decentralized security which aims to develop a framework that will enable reasoning about the security of all the integrated constituent CPS components
3. Reliable and practical reasoning about secure computation and communication in networks which aims to contribute a formal framework for reasoning about security in CPS
4. Evaluation and experimentation using modeling and simulation integration of cyber and physical platforms that directly interface with human decision makers.
5. Education and outreach

Impact

- Equip CPS designers and operators with foundations and theory-based comprehensive tools improve resilience against faults and intrusions
- Enable designers to take security decisions and allocate resources in a decentralized manner
- Enable experimentation, evaluation, and training using a modeling and simulation integration platform



Berkeley UNIVERSITY OF CALIFORNIA

Massachusetts Institute of Technology

INFORMATION & COMPUTER SCIENCES UNIVERSITY of HAWAI'I at MĀNOA

VANDERBILT UNIVERSITY

OVERVIEW

- **Team**
- **Resilience of Cyber-Physical Systems**
- **Research Problems**
- **Project Thrusts**
  - Risk Analysis and Incentive Design
  - Resilient Monitoring and Control
  - Decentralized Security
  - Formal Reasoning about Security
  - Evaluation using Modeling and Simulation Integration

TEAM

- Saurabh Amin (MIT)
- Katie Dey (Vanderbilt) – Outreach
- Anthony Joseph (UC Berkeley)
- Gabor Karsai (Vanderbilt)
- Xenofon Koutsoukos (Vanderbilt) – PI
- Dusko Pavlovic (U. of Hawaii)
- Larry Rohrbough (UC Berkeley)
- S. Shankar Sastry (UC Berkeley
- Janos Sztipanovits (Vanderbilt)
- Claire Tomlin (Vanderbilt)
- Peter Volgyesi (Vanderbilt) - Technology Integration and Evaluation
- Yevgeniy Vorobeychik (Vanderbilt)

- Team with interdisciplinary activities in multiple areas:
  - CPS, critical infrastructure, embedded software, mobile/distributed computing
  - Security and resilience, incentive design, game theory fault diagnosis, control theory, model-integrated computing, multi-agent systems, secure machine learning
- Successful collaborative projects
  - NSF Foundations of Hybrid and Embedded Systems ITR (2003- 2010)
  - Command and Control Wind Tunnel PRET (2006 - 2009)
  - High-Confidence Design of Networked Embedded Control Systems MURI (2006 – 2011)
  - NSF STC TRUST (2005 – 2014)
  - NSF CPS Frontier FORCES (2013 – 2018)

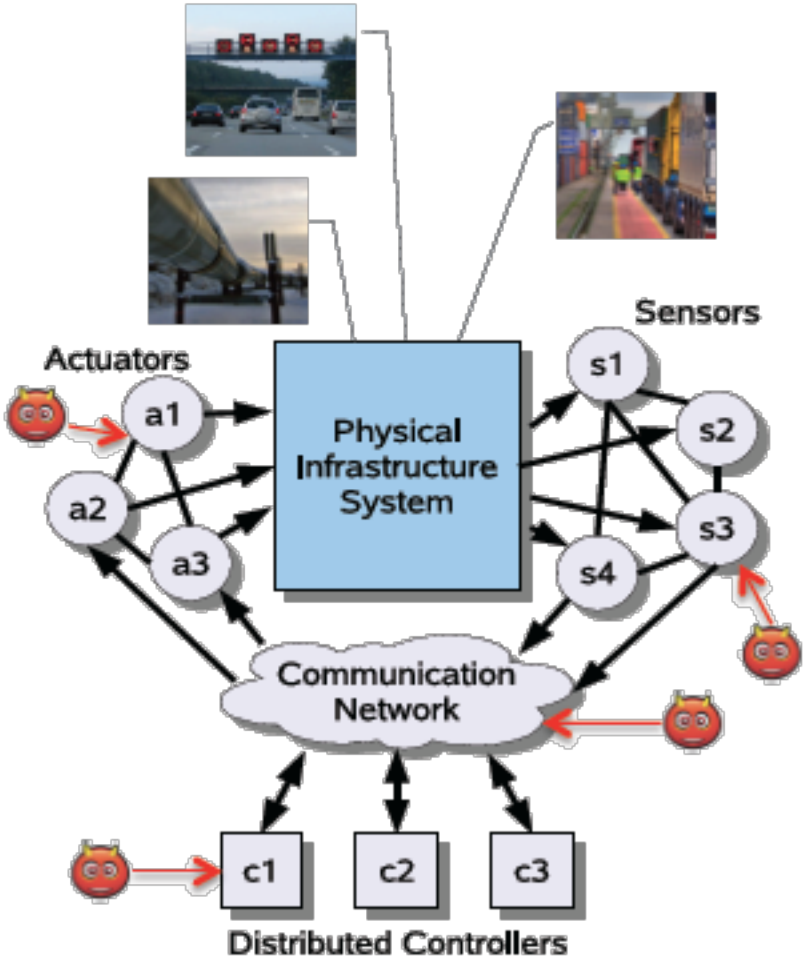
RESILIENCE OF CPS

Attributes of Resilience

- Functional correctness (by design)
- Robustness to *reliability* failures (faults)
- Survivability against *security* failures (attacks)

Challenges to Resilience

- Spatio-temporal dynamics
- Many strategic interactions with network interdependencies
- Inherent uncertainties (public & private)
- Tightly coupled control and economic incentives



PRIOR RELATED RESULTS

SURE

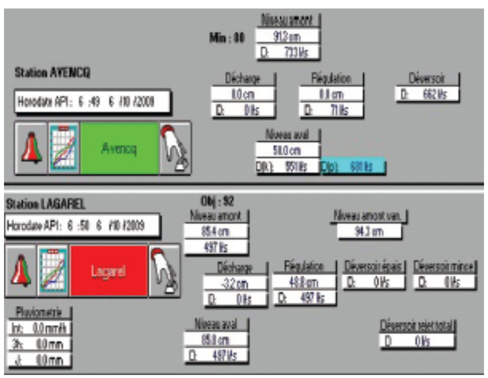
1. S. Amin, X. Litrico, S. S. Sastry, A. M. Bayen. **Analysis of deception attacks on network controlled water distribution systems.** *IEEE Trans. on Control Systems Technology*, 2011.
2. H. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram. **Resilient Asymptotic Consensus in Robust Networks**, *IEEE Journal on Selected Areas on Communication*, 2013.
3. S. Amin, G.A. Schwartz, and H. Tembine, **Incentives and Security in Electricity Distribution Networks**. *GameSec* 2012.
4. Y. Vorobeychik and J. Letchford. **Securing interdependent assets**. Journal of Autonomous Agents and Multiagent Systems, 2014.
5. M. Barreno, B. Nelson, A. Joseph, and J. Tygar**, The Security of Machine Learning**, Machine Learning Journal, 2010
6. W. Pieters, T. Dimkov, and D. Pavlovic. **Security policy alignment: A formal approach**. *IEEE Systems Journal, 2013*.
7. J. Sztipanovits, G. Biswas, G. Karsai, H. Neema, C. Tomlin, K. Goldberg, S. Sastry, P. Varaiya, A. Levis, L. Wagenhals. **Multi-model simulation: The C2 Wind Tunnel**. *Workshop on Synthetic Environments for Assessment*, 2009.

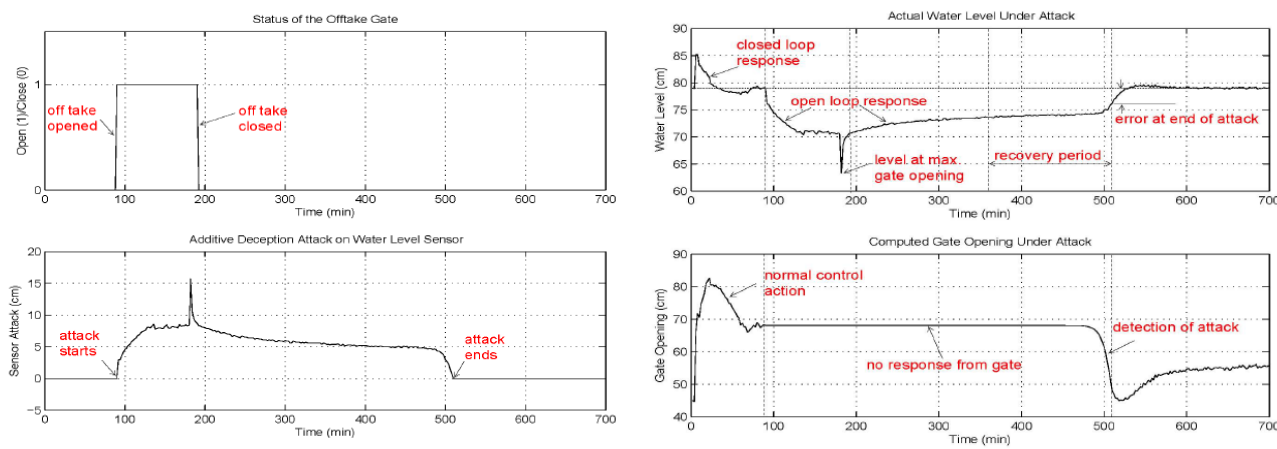
SCADA SYSTEMS FOR WATER DISTRIBUTION

Avencq cross-regulator

- **Regulatory control of canal pools**
  - Manipulate gate opening
  - Control upstream water level
  - Reject disturbances (offtake withdrawals)
- **SCADA components**
  - Level & velocity sensors
  - PLCs & gate actuators
  - Wireless communication

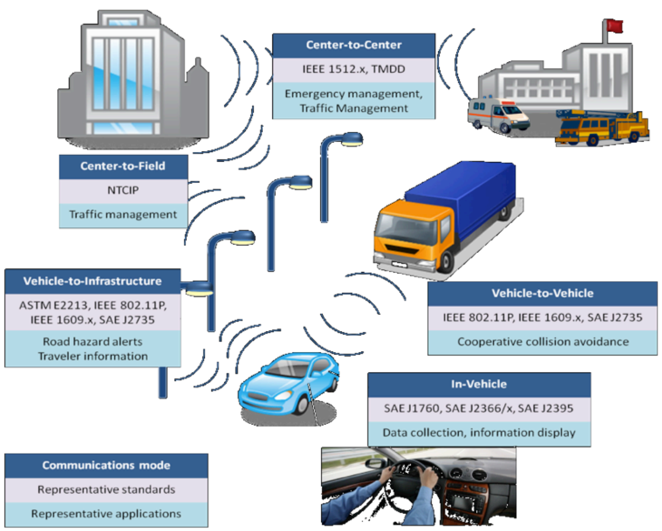
SCADA Interface

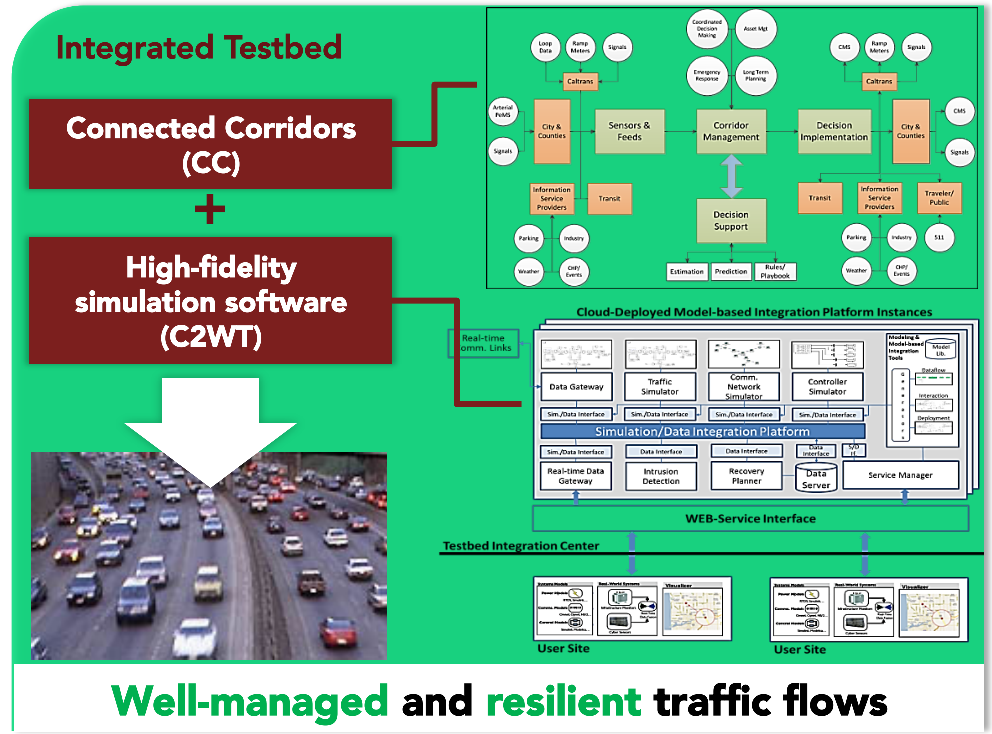




Successful attack: Field operation test (Oct. 12, 009)

TRAFFIC CONTROL SYSTEMS





ACHIEVING RESILIENCE: REDUNDANCY AND DIVERSITY

A System Function *can be* allocated to various (combinations of) providers: Applications / Processes / Components

Processes / Components *can be* allocated to various (combinations of) platform Nodes

When a Node / Link / Process / Component fails (compromised), functionality can be restored by an

- alternative allocation of *functions* to *providers*, or
- alternative allocation of *providers* to *platform* nodes

RESEARCH PROBLEMS

Risk Analysis and Incentive Design

1. How the collection of agents in CPS can deal with strategic adversaries?
2. How strategic agents contribute to CPS efficiency and safety, while protecting their conflicting individual objectives?

Resilient Monitoring and Control

1. What are the control architectures that can improve resilience against intrusions and faults?
2. What types of dynamics can provide inherent robustness against impacts of faults and cyber attacks?
3. What are the physics-based invariants that can be used as "ground truth" in intrusion detection?

Decentralized Security

1. How can we design systems that are resilient event when there is significant decentralization of resources and decisions?

Formal Reasoning about Security in CPS

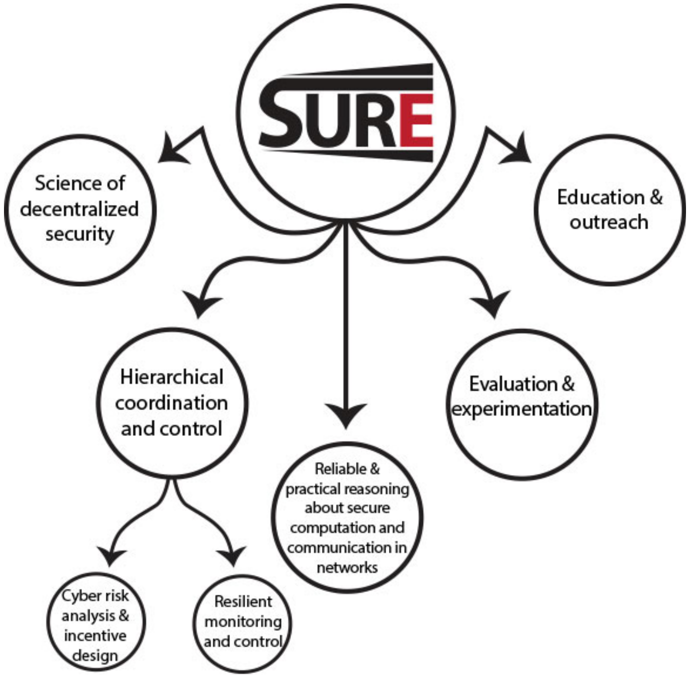
1. How do formally and practically reason about secure computation and communication?

Integrative Research and Evaluation

1. How to integrate and evaluate cyber & physical platforms and resilient monitoring & control architectures?
2. How to interface and support human decision makers?

PROJECT THRUSTS

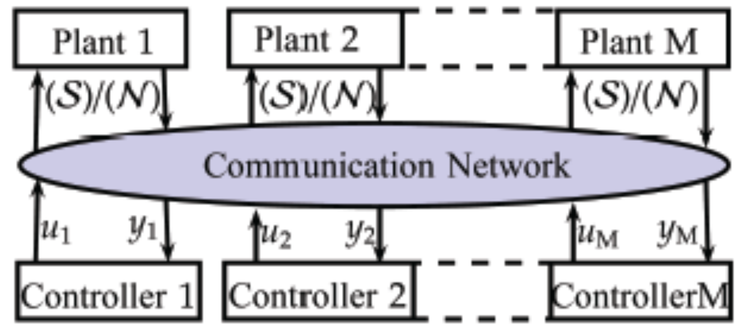
1. **Hierarchical Coordination and Control**
    1. **Risk analysis and incentive design** that aim at developing regulations and strategies at the management level
    2. **Resilient monitoring and control** of the networked control system infrastructure
2. **Science of decentralized security** which aims to develop a framework that will enable reasoning about the security of all the integrated constituent CPS components
3. **Reliable and practical reasoning about secure computation and communication** in networks which aims to contribute a formal framework for reasoning about security in CPS
4. **Evaluation and experimentation** using modeling and simulation integration of cyber and physical platforms that directly interface with human decision makers.
5. **Education and outreach**



RISK ANALYSIS AND INCENTIVE DESIGN

1. *Game Theory*: How to model and solve large-scale network games that a) model both security (malicious attacks) and reliability (random faults) failures, b) account for the presence of dynamics and information incompleteness?
2. *Theory of incentives*: How to design and solve stochastic control and incentive-theoretic schemes, coupled with the outcome of the network games (mentioned above)?

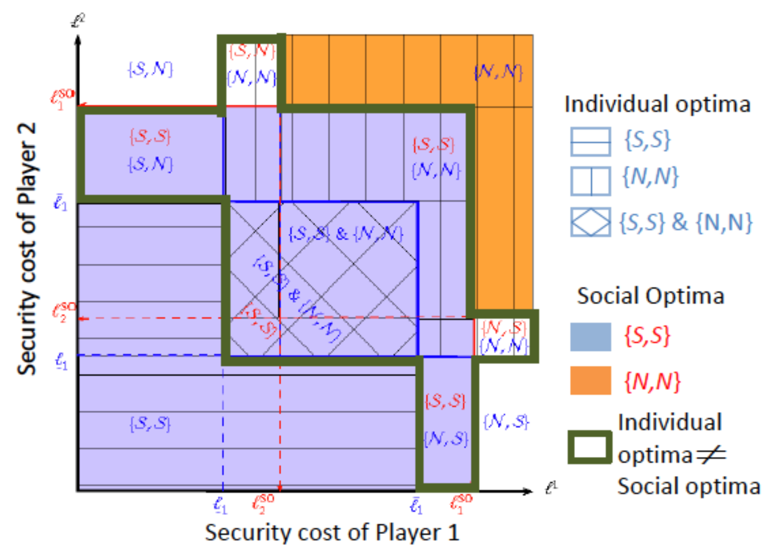
Two-stage game of M plant-controller systems



A problem of incentives: Due to the presence of network-induced interdependencies, the individual optimal (Nash) security allocations are suboptimal

Goal: Develop mechanisms to reduce CPS incentive sub-optimality

Theorem [Increasing incentive case]

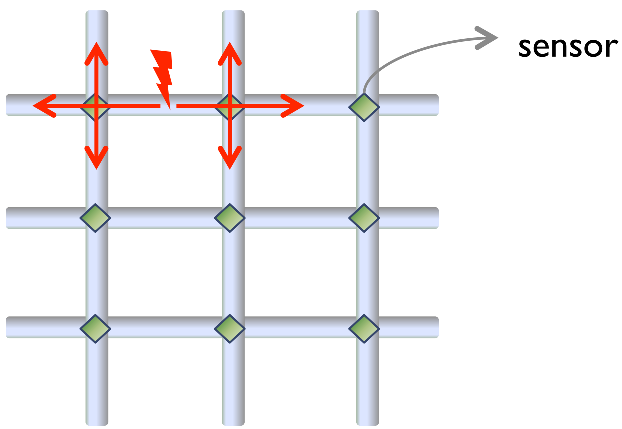


[Amin and Sastry]

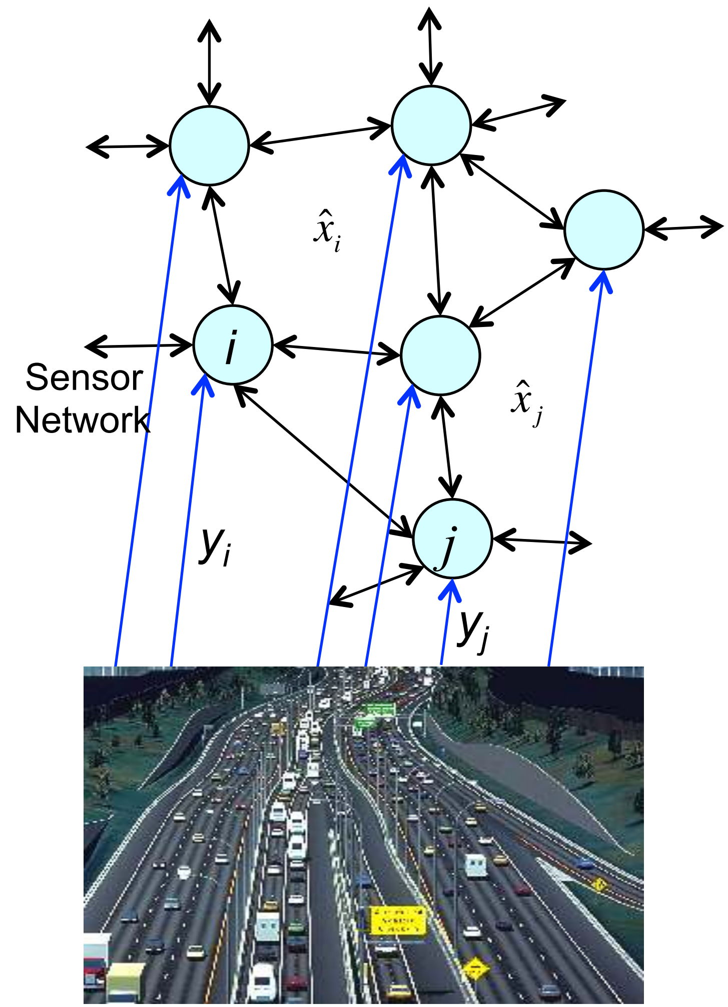
VANDERBILT UNIVERSITY

RESILIENT MONITORING

1. How to to detect faults and attacks, which may degrade system performance, cause instability, and affect system operation and mission?
2. How to design resilient monitoring protocols that are robust to both random faults and adversarial attacks?
3. How to place and select sensors to improve resilience?



Resilient Fault Diagnosis for Flow Networks



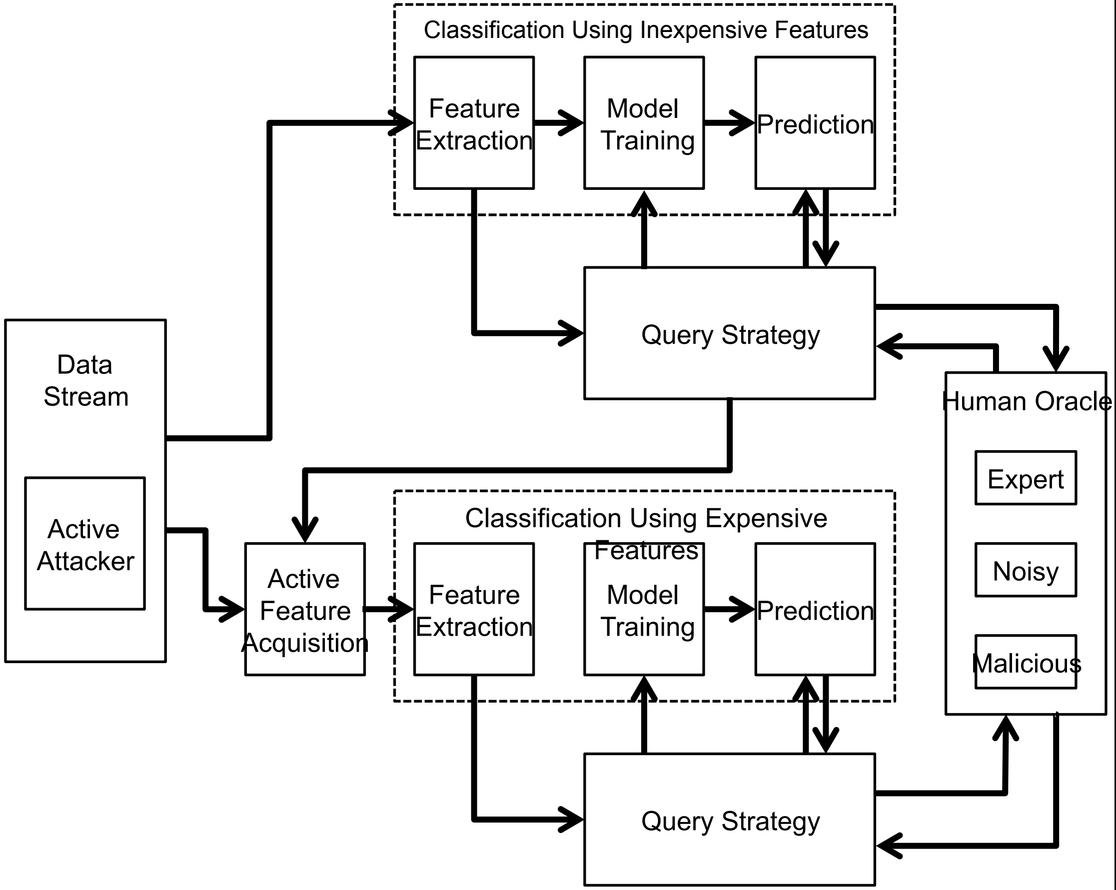
Resilient Distributed Consensus

[Amin and Koutsoukos]

ADVERSARIAL MACHINE LEARNING

- How to acquire labeled (ground truth) data for evaluation?
- How to achieve very high accuracy (low false positive and low false negative rates) and transparency?
- How to reduce human and machine workloads while retaining very high accuracy?
- How to explore these problems in a scientifically repeatable and valid environment?

SALT: Secure Active Learning Testbed



[Joseph]

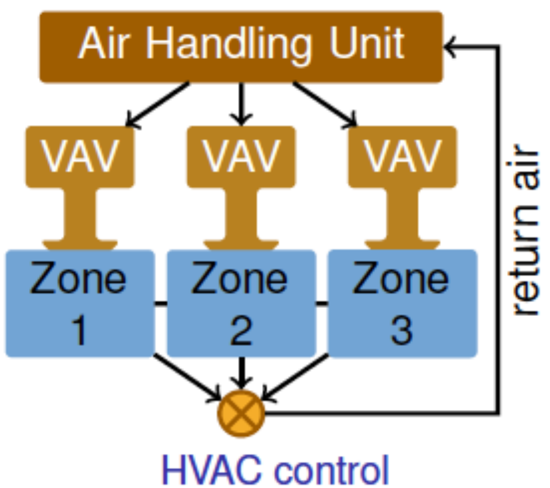
RESILIENT CONTROL

Resilient network (supervisory) and local (regulatory) control: How to design practical control algorithms, which improve the survivability of CPS against network-level attacks and/or faults?

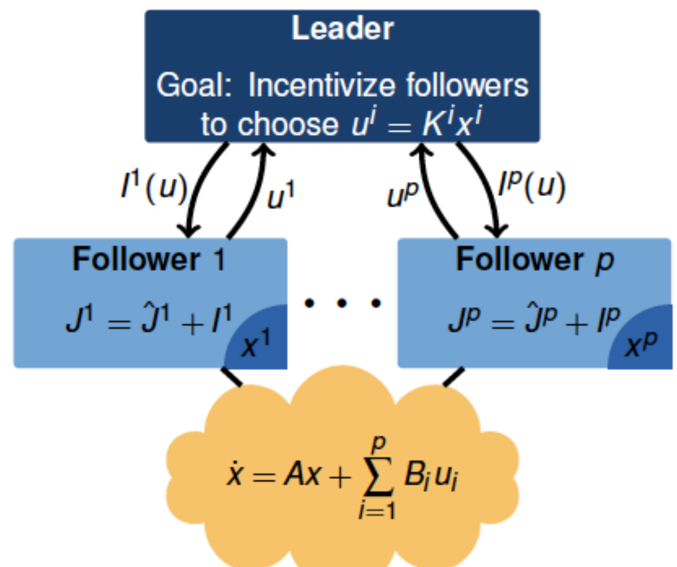
Manager's objective: Min social discomfort + inefficiencies

Zone's objective: Min individual discomfort + energy bill

Goal: Incentivize security via monitoring and control



Resilient Control of Building Energy Systems



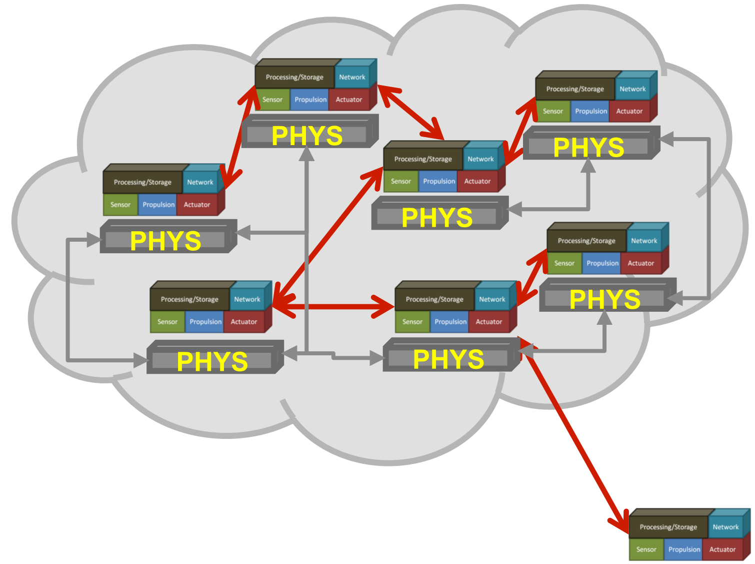
Stackelberg games for resilient control design

[Amin, Sastry, and Tomlin]

SENSOR/CONTROL NETWORK PLATFORM

Challenge: How to design and analyze system architectures that deliver required service in the face of compromised components?

Concept: Apply principles and techniques from run-time fault management to managing cyber effects



Resilience to faults:

- Detect anomaly
  - Locally or globally
- Isolate fault source
  - App, process, node, link, …
- Recover
  - Restart, replace, reconfigure

Platform provides:

- Overall architecture
- Reusable services for detection, diagnosis, mitigation

Application specific:

- Specific logic for detection, isolation, mitigation

Resilience to cyber *effects*:

- Detect anomaly
  - Locally or globally
- Isolate source of anomaly
  - App, process, node, link
- Recover
  - Restore, replace, reconfigure

Platform provides:

- Overall architecture
- Reusable services for detection, diagnosis, mitigation

Application specific:

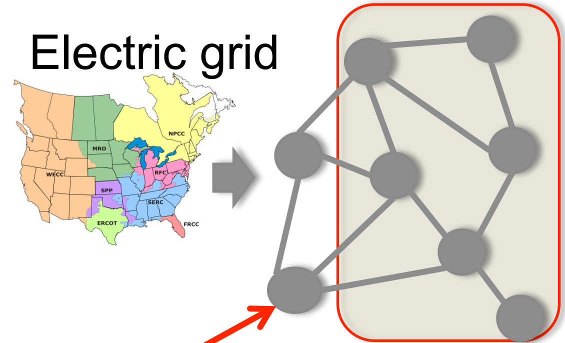
- ???

[Karsai]

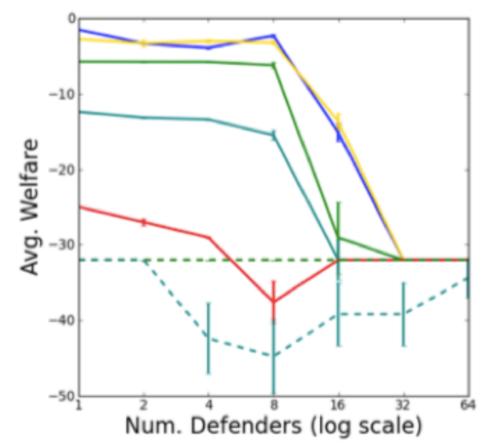
DECENTRALIZED SECURITY

How can we design systems that are resilient even when there is significant decentralization of resources and decisions?

- Defenders “jointly” own CPS (e.g., electric power grid; train system; transportation)
- Attacker chooses where to attack to cause the most damage (e.g., maximum disruption)
- Attacker responds to defensive measures (resilient control strategies; intrusion detection/prevention measures)



How do defenders who are primarily concerned about the portion of CPS they own choose their security measures?
Depends on the level of decentralization and the degree of system interdependence



[Vorobeychik]

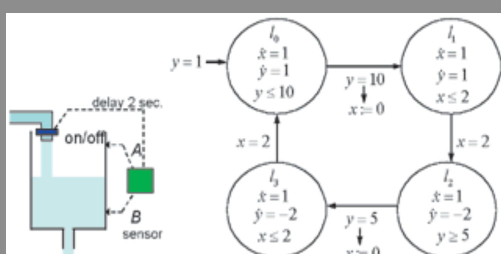
MODELING AND PROVING SECURITY IN NETWORKS

SURE

PROBLEM

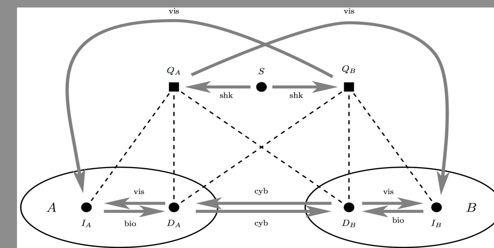
- *High assurance for Cyber Physical Systems*
- *Network computation with physical interface*

BACKGROUND

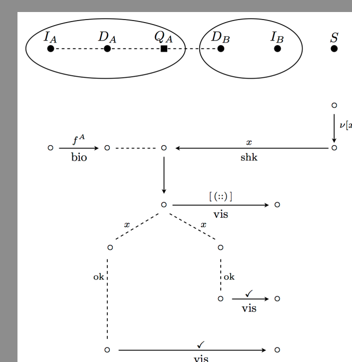


- *Hybrid systems, Petri nets*
- *Protocol Derivation Logic, Strand spaces*

APPROACH



- ***Actor networks**: fibered state machines*
- ***Network computation**: partially ordered multisets (pomsets)*



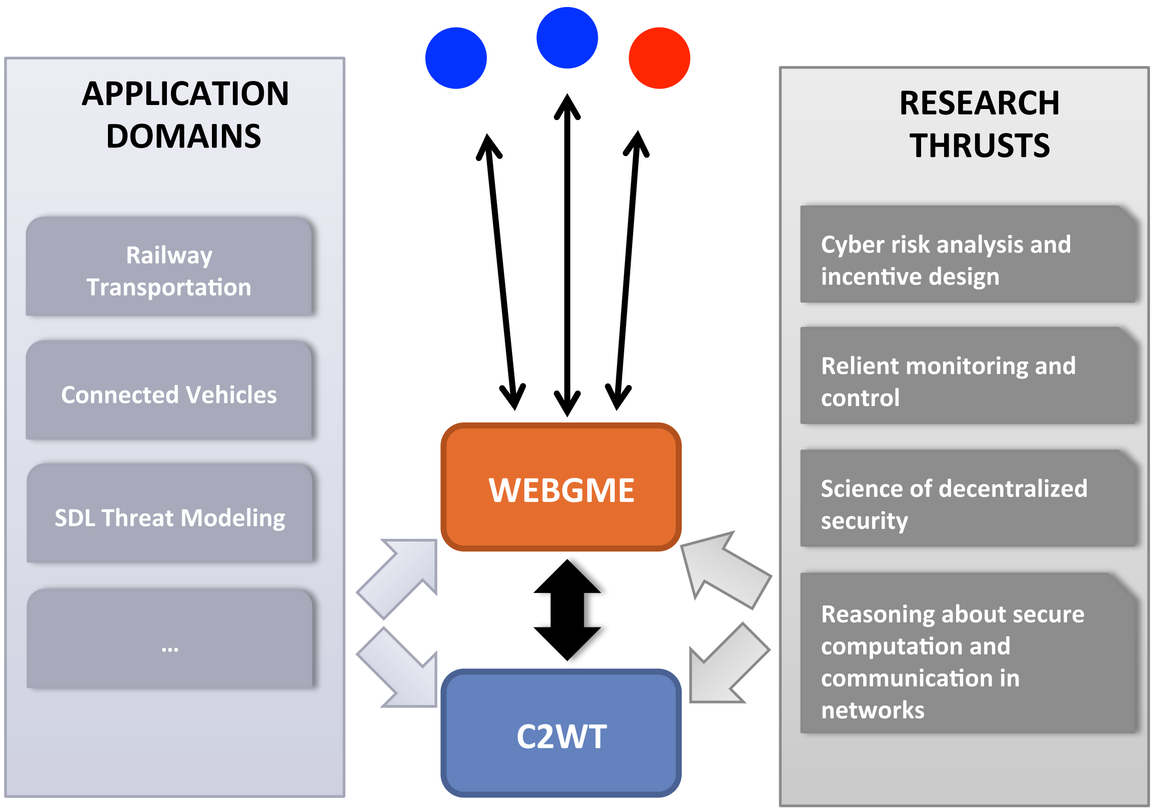
- ***<u>Procedure</u> Derivation Logic***
- ***Authentication templates** extended to capture physical and social channels*

[Pavlovic]

VANDERBILT UNIVERSITY

EVALUATION USING MODELING AND SIMULATION INTEGRATION

- **Validation of basic research**
  - Scenario-based experimentation
- **Collaboration**
  - SURE research thrusts
  - Integration: Tools and languages
- **Motivation**
  - Red team vs Blue team scenarios and challenges
- **Outreach**
  - Accessible tools and technologies on the web
- **Model libraries and repositories**



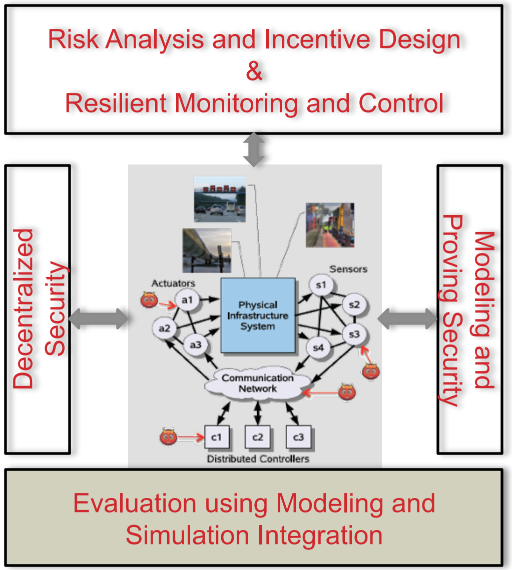
[Volgyesi and Sztipanovits]

EDUCATION AND OUTREACH

- **Classes**
  - S. Amin, 1.208 Resilient Infrastructure Networks, MIT, Fall 2014
  - X. Koutsoukos, CS 396 Security of CPS, Vanderbilt, Spring 2015.
- **Online Modules**
- **Workshops/Conferences**
  - How to Engineer Resilient Cyber-Physical Infrastructures, IEEE CDC 2014 [Amin]
  - Big Data Analytics for Societal Scale CPS: Energy Systems, IEEE CDC 2014 [Sastry]
  - Secure and Resilient Infrastructure CPS (HiCoNS) track, ICCPS 2015 [Koutsoukos]
- **Evaluation and Experimentation Testbed**
- **SOS-VO**

SYSTEM SCIENCE OF SECURITY AND RESILIENCE OF CPS

SURE

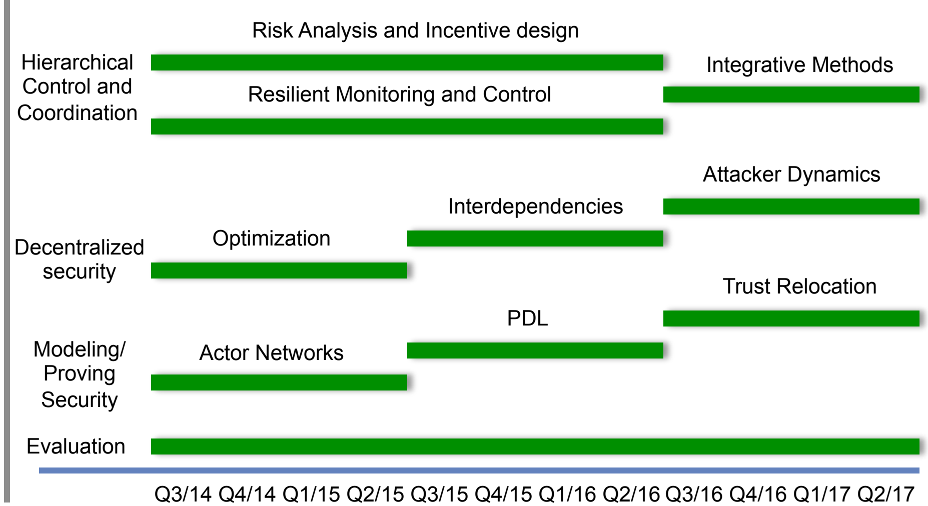


Key Ideas

1. Hierarchical Control and Coordination
   1. Risk analysis and incentive design that aim at developing regulations and strategies at the management level
   2. Resilient monitoring and control of the networked control system infrastructure
2. Science of decentralized security which aims to develop a framework that will enable reasoning about the security of all the integrated constituent CPS components
3. Reliable and practical reasoning about secure computation and communication in networks which aims to contribute a formal framework for reasoning about security in CPS
4. Evaluation and experimentation using modeling and simulation integration of cyber and physical platforms that directly interface with human decision makers.
5. Education and outreach

Impact

- Equip CPS designers and operators with foundations and theory-based comprehensive tools improve resilience against faults and intrusions
- Enable designers to take security decisions and allocate resources in a decentralized manner
- Enable experimentation, evaluation, and training using a modeling and simulation integration platform



Berkeley UNIVERSITY OF CALIFORNIA

Massachusetts Institute of Technology

INFORMATION & COMPUTER SCIENCES UNIVERSITY of HAWAI'I at MĀNOA

VANDERBILT UNIVERSITY

AGENDA

SURE

0830 – 0900 *Security Check-In | Breakfast*

0900 – 0905 **Introductions and Opening Remarks**
William Martin (NSA) and William McKeever (AFRL)

0905 – 0930 **Project Overview**
Xenofon Koutsoukos (Vanderbilt University) – Lead PI

0930 – 1015 **The Science of Decentralized Security in Cyber-Physical Systems**
Yevgeniy Vorobeychik (Vanderbilt University)

1015 – 1030 *Break*

1030 – 1115 **Covert Flows and Authentication in Cyber, Physical, and Social Systems**
Dusko Pavlovic (U of Hawaii)

1115 – 1200 **Resource Aware Large-scale Malware Classification**
Anthony Joseph (UC Berkeley)

1200 – 1300 *Lunch*

1300 – 1330 **Secure Control and Optimization for Cyber-Physical Systems**
Larry Rohrbough (UC Berkeley)

1330 – 1400 **Resilient Monitoring and Control of Flow Networks**
Xenofon Koutsoukos (Vanderbilt University)

1400 – 1430 **Incentive Mechanisms for CPS Security**
Saurabh Amin (MIT) – presented by Xenofon Koutsoukos

1430 – 1440 *Break*

1440 – 1500 **Resilience and Security in Component-Based Software Architectures for CPS**
Gabor Karsai (Vanderbilt University)

1500 – 1520 **Model-Based Simulation for Evaluation of CPS Security and Resilience**
Peter Volgyesi (Vanderbilt University)

1520 – 1530 *Break*

1530 – 1630 **Science of Security for Cyber-Physical Systems: Status and Open Discussion**
Shankar Sastry (UC Berkeley) and Janos Sztipanovtis (Vanderbilt University)

1630 – 1700 *Government Caucus and Feedback*