FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Cooperative Control in Tree Topology Networks

Xenofon Koutsoukos

Work with : Mark Yampolskiy and Yevgeniy Vorobeychik

Berkeley UNIVERSITY OF CALIFORNIA

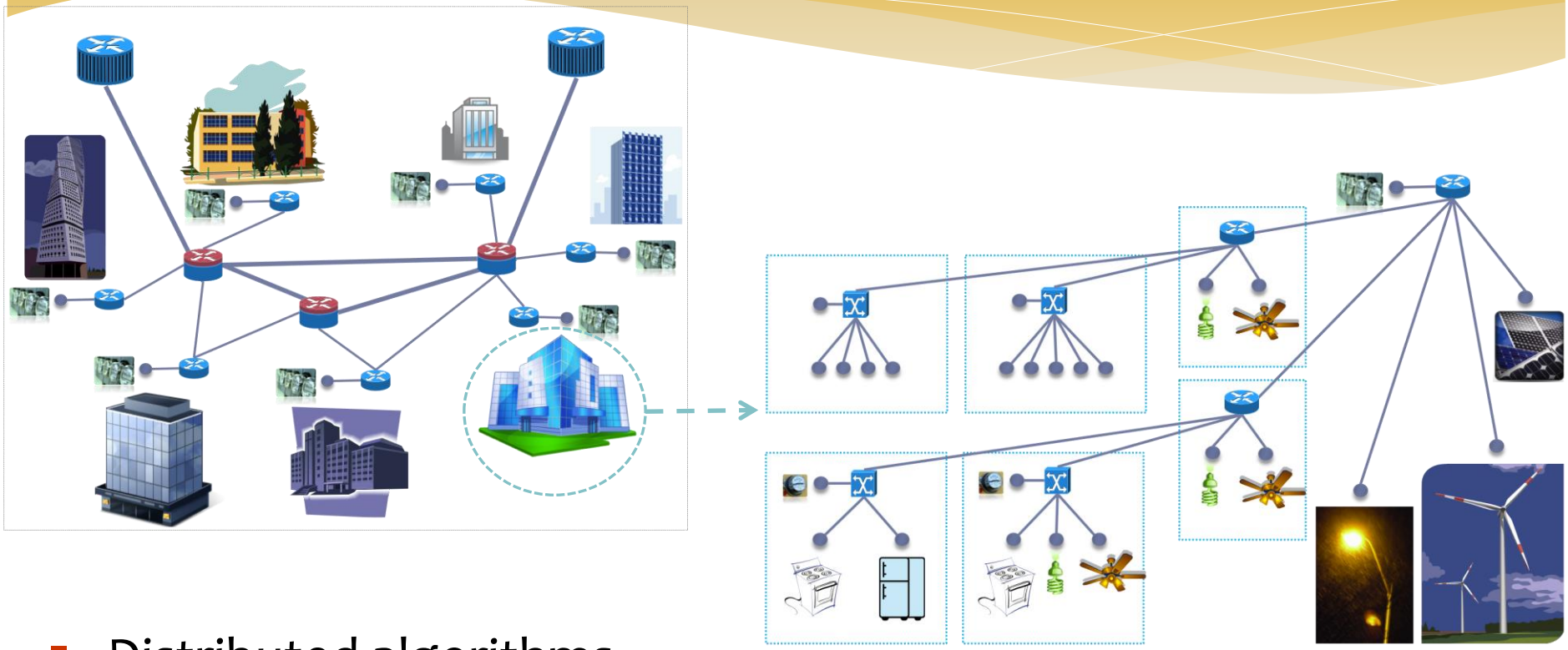
Massachusetts Institute of Technology

NSF

MICHIGAN

VANDERBILT UNIVERSITY

Objective: Design of Resilient Consensus Protocols



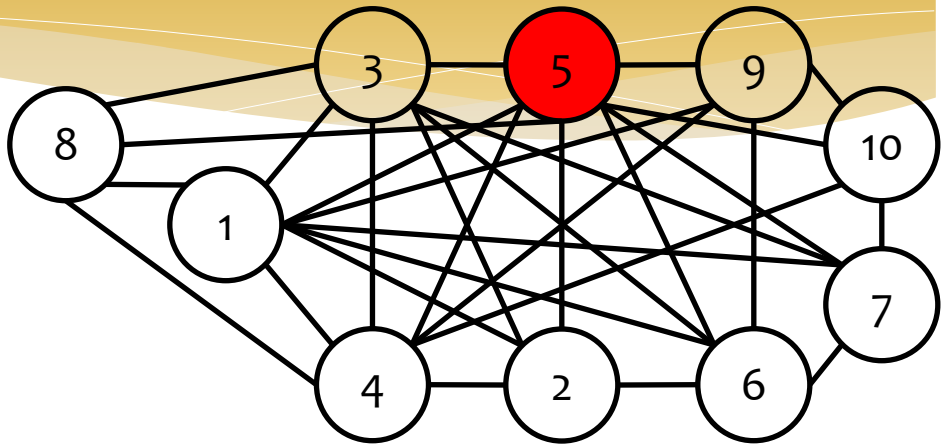
- Distributed algorithms
  - Parameter and state estimation
  - Fault detection and diagnosis
  - Coordination and cooperative control

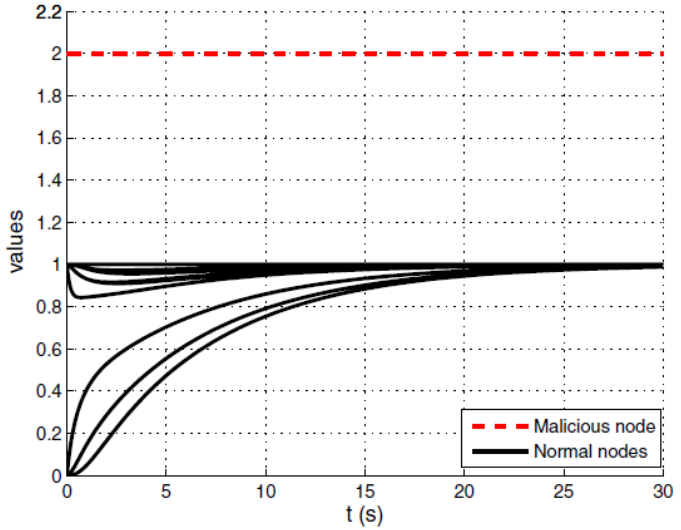
Resilient Consensus Protocols

- Adversary model
  - Crash
  - Malicious
  - Byzantine
- Adversary scope
  - F-total
  - F-local
  - f-fraction local
- Resilient protocols

$$x_i(t+1) = w_{(i,i)}(t)x_i(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)} w_{(j,i)}(t)x_{(j,i)}(t)$$

- Characterization of network resilience based on local information





(b) ARC-P.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilient Asymptotic Consensus

* Hybrid system dynamics

$$x_i(t+1) = f_{i,\sigma(t)}(t, x_i(t), \{x_{(j,i)}(t)\}),\ \ i \in \mathcal{N}, j \in \mathcal{N}_i^{\text{in}}, t \in \mathbb{Z}_{\geq 0}, \mathcal{D}_{\sigma(t)} \in \Gamma_n$$

* Agreement Condition

$$\lim_{t\to\infty} \Psi(t) = 0 \quad \text{where } \Psi(t) = M_{\mathcal{N}}(t) - m_{\mathcal{N}}(t)$$

* Safety Condition

$$x_i(t) \in \mathcal{I}_t = [m_{\mathcal{N}}(t), M_{\mathcal{N}}(t)], \quad \forall t \in \mathbb{Z}_{\geq 0}, \forall i \in \mathcal{N}$$

* Weighted Mean-Subsequence-Reduced (W-MSR) Algorithm

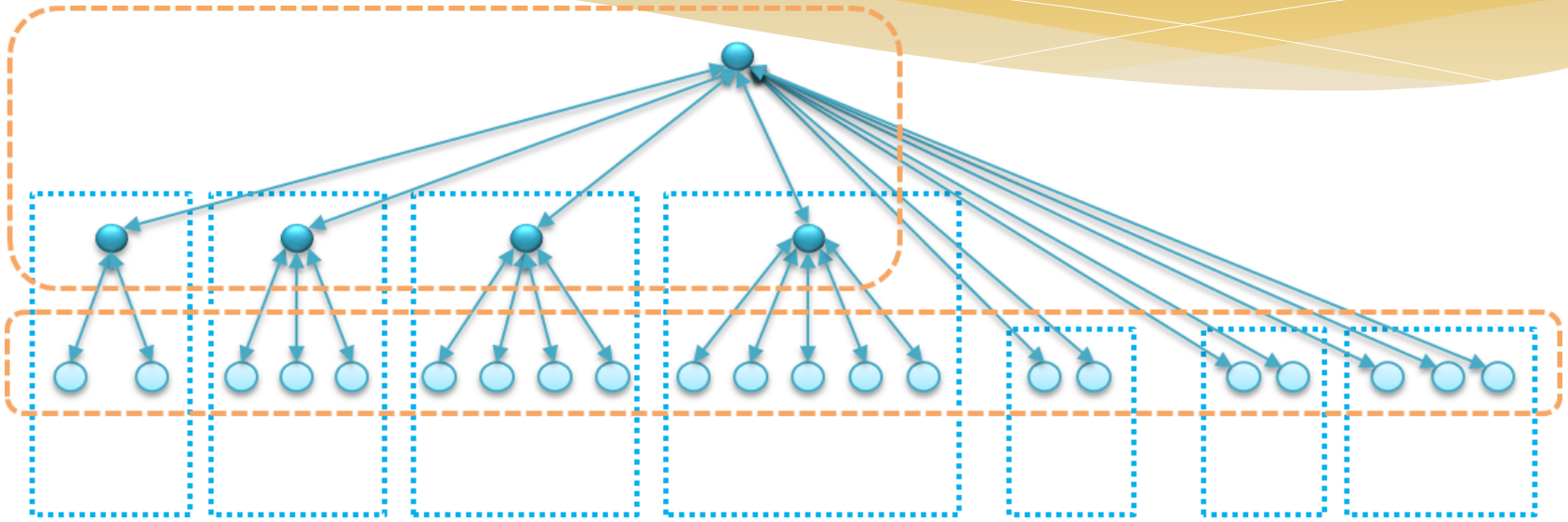
$$x_i(t+1) = w_{(i,i)}(t)x_i(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)} w_{(j,i)}(t)x_{(j,i)}(t)$$

Robust Networks

Threat	Scope	Necessary	Sufficient
Crash & Malicious	F-Total	$(F+1,F+1)$-robust	$(F+1,F+1)$-robust
Crash & Malicious	F-Local	$(F+1,F+1)$-robust	$(2F+1)$-robust
Crash & Malicious	f-Fraction local	f-fraction robust	p-fraction robust, where $2f < p \leq 1$
Byzantine	F-Total & F-Local	Normal Network is $(F+1)$-robust	Normal Network is $(F+1)$-robust
Byzantine	f-Fraction local	Normal Network is f-robust	Normal Network is p-robust where $p > f$

* [LeBlanc et al., *IEEE JSAC*, April 2013]
* Normal network is the network induced by the normal nodes
* Necessary Conditions for F-Total and F-Local are necessary for any successful DTRAC algorithm

Resilient Consensus in Tree Networks

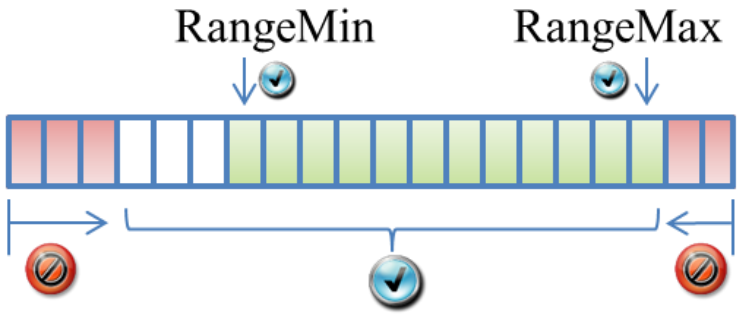


- Previous protocols require high-degree of redundancy
- Assumption
  - Adversaries can compromise only leaf nodes

Resilient Consensus for Tree Topology Network

* Trust parent node
* Trusted value range
  * Between own and parent node value
* Remove F outliers if they are not in trusted value range
* Update state based on remaining values

* Trusted value range



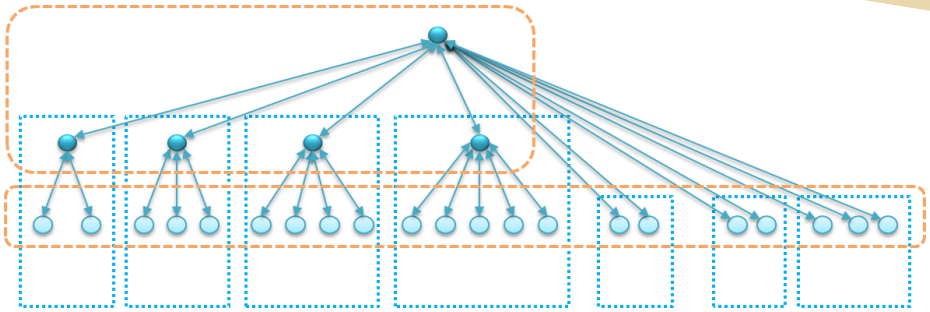
RangeMin = min (ownVal, parentVal)
RangeMax = max (ownVal, parentVal)

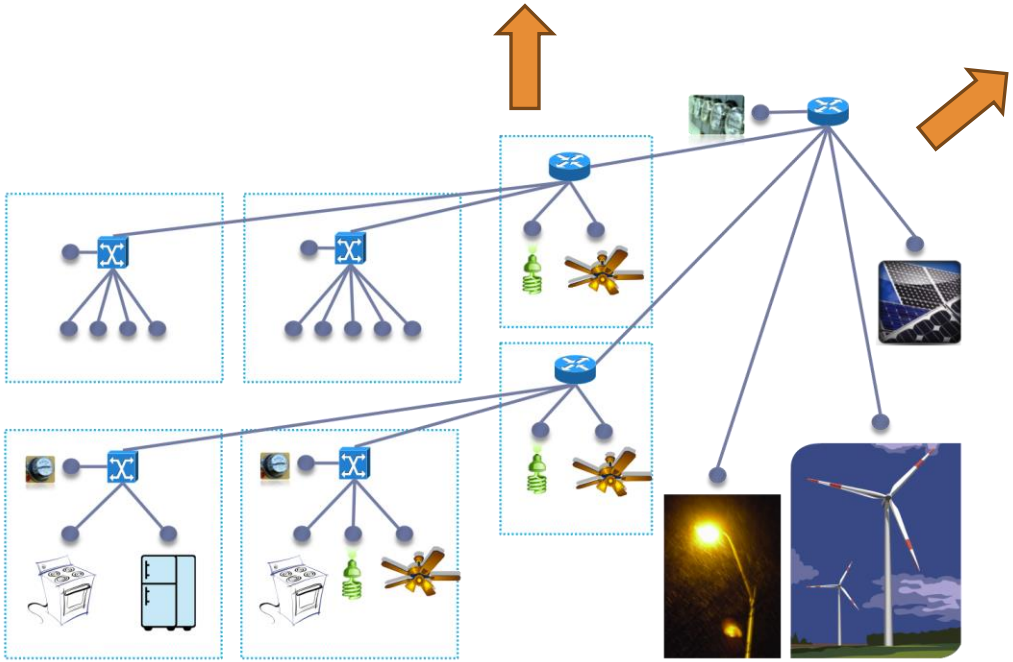
$$x_i(t+1) = w_{(i,i)}(t)x_i(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}(t) \setminus \mathcal{R}_i(t)} w_{(j,i)}(t)x_{(j,i)}(t)$$

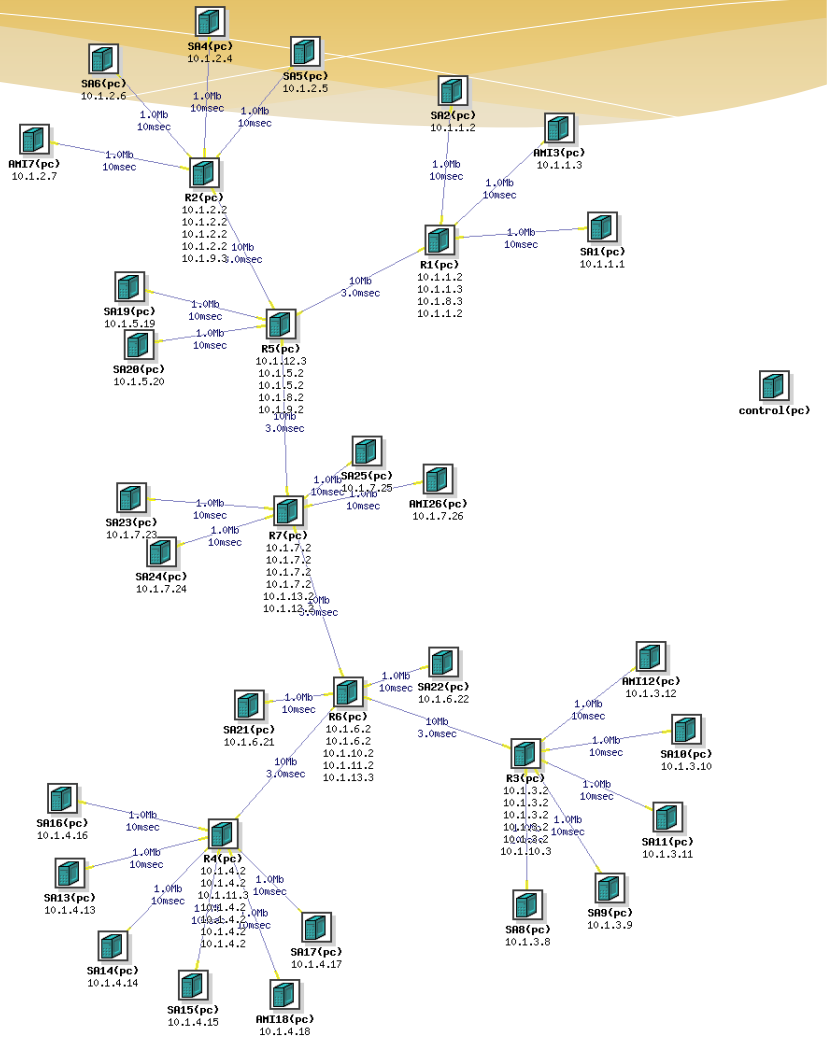
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

[Yampolskiy et al., *HiCoNS,* 2014]

Emulation in DeterLab

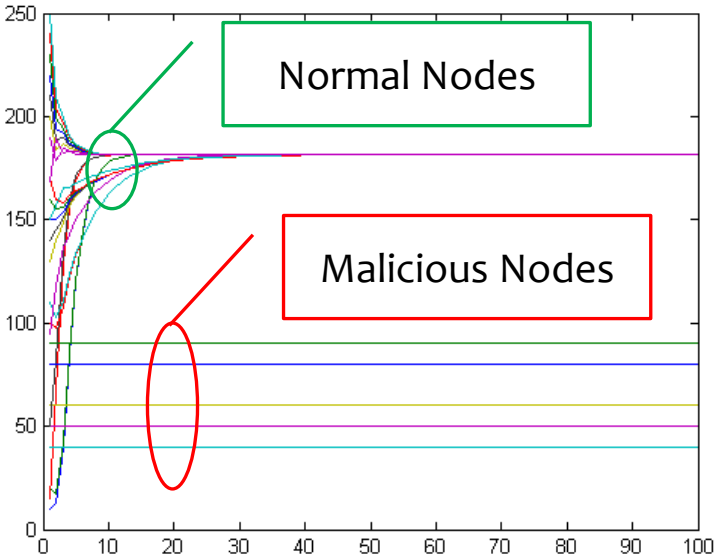




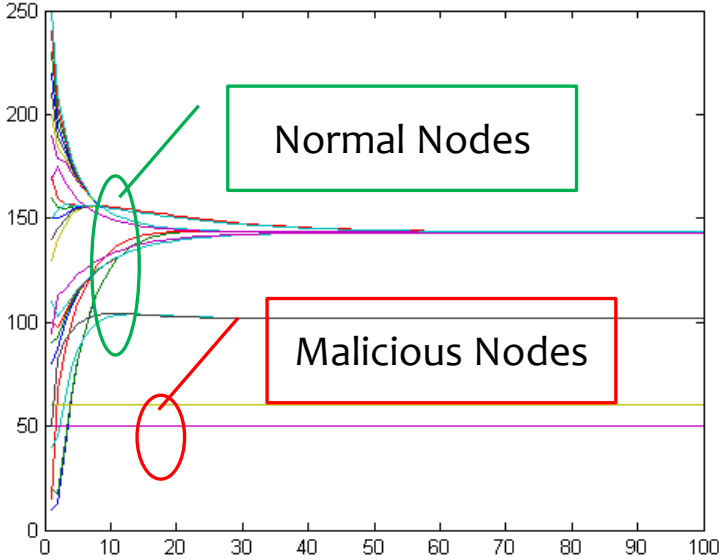


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Simulation Results



* Adversary model
  * Malicious nodes
  * F-total = 5
  * F-local = 3

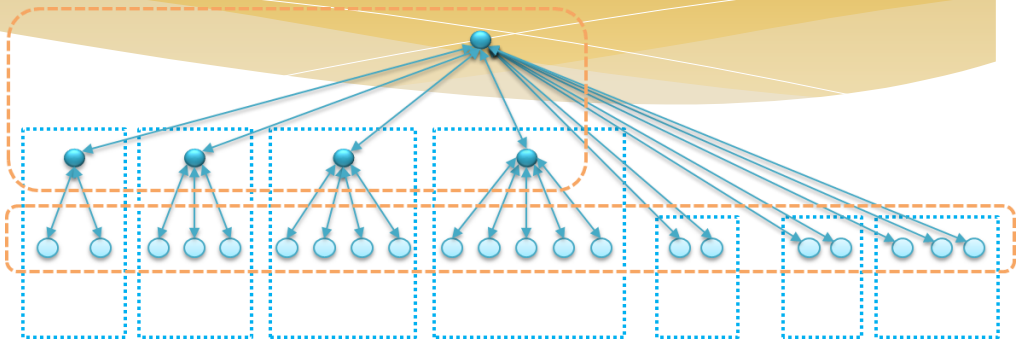


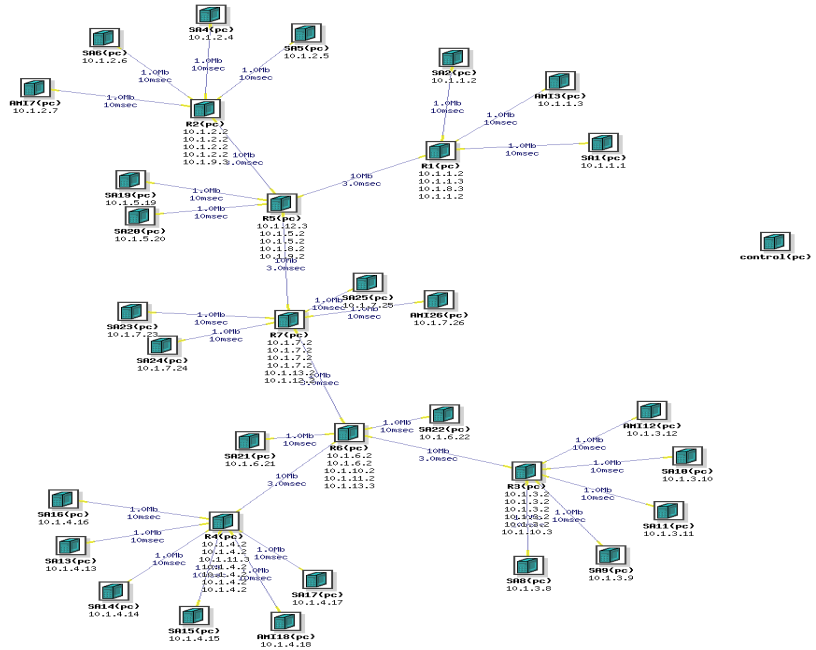
* Adversary model
  * Malicious nodes
  * F-total = 2
  * F-local = 1

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Current Work

- EI-aware resilient control design
- Distributed algorithms
  - Resilient state estimation
  - Resilient fault detection and diagnosis
- Adversaries
  - DDOS attacks
  - Multi-layer attacks
  - Synchronization attacks





FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS