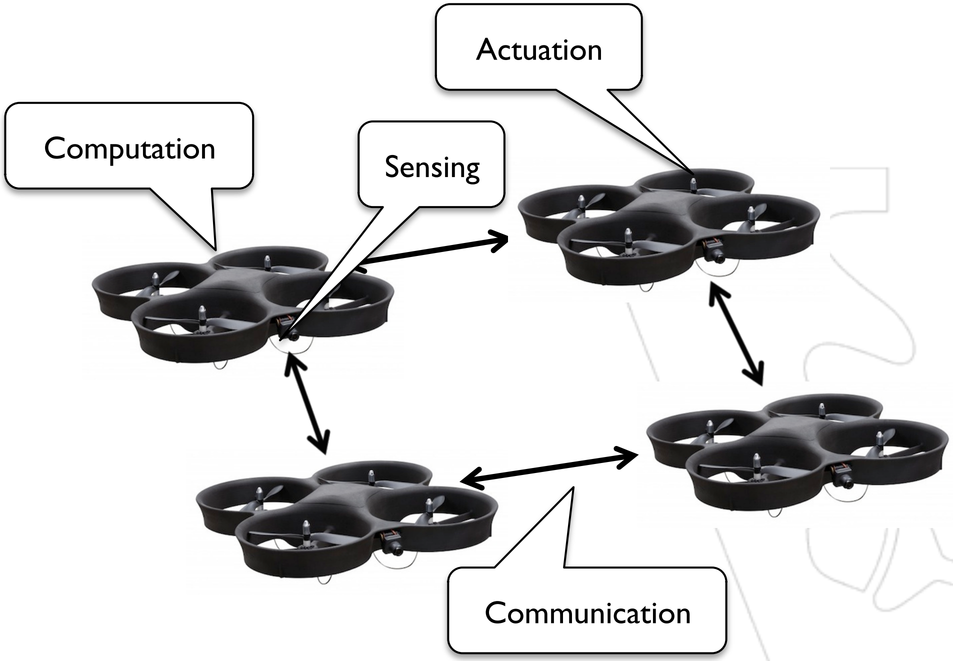
Toward Resilient Monitoring and Control of Distributed Cyber-Physical Systems

Xenofon Koutsoukos

Heath LeBlanc, Mark Yampolskiy, Aron Laszca, Waseem Abbas, Himansu Neema, Eugene Vorobeychic, Gabor Karsai, Janos Sztipanovits

HCSS Conference
Annapolis, MD, May 8, 2014

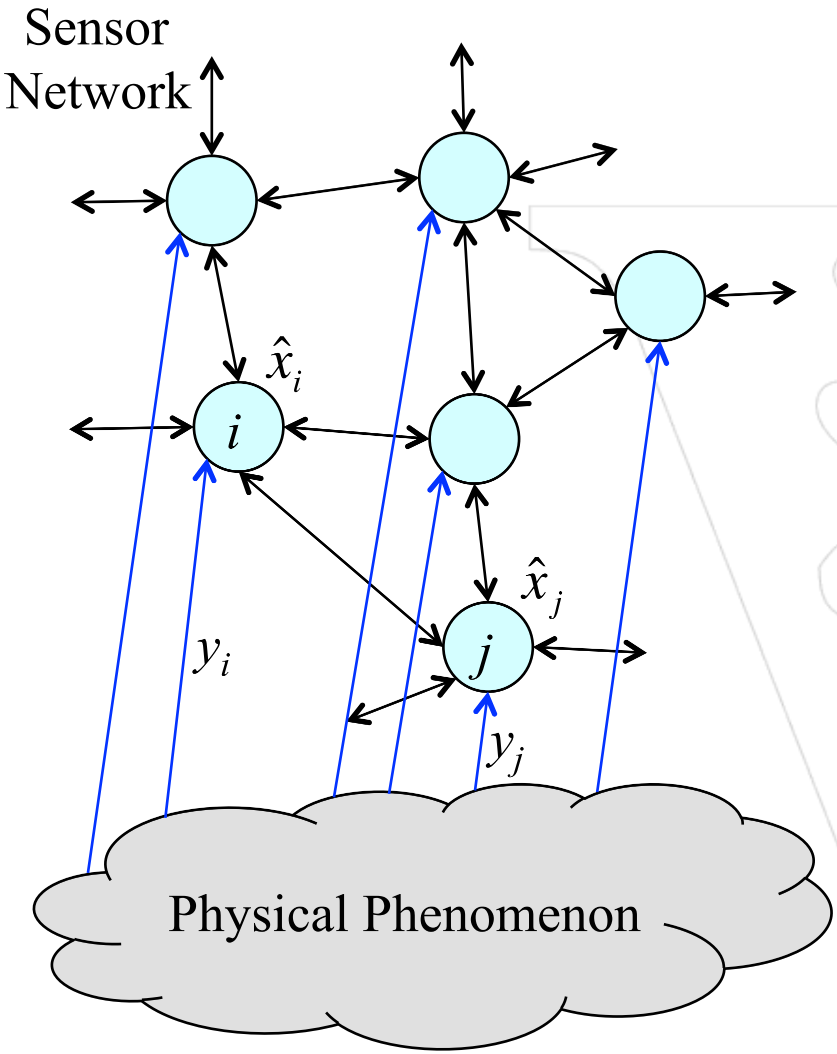
Distributed Control of Multi-Agent Systems



Group Objective: Flocking

- Basic models of flocking behavior are controlled by three simple rules:
  - Separation - avoid crowding neighbors
  - Alignment - steer towards average heading of neighbors
  - Cohesion - steer towards average position of neighbors

Distributed Parameter Estimation



- All sensors measure independently some physical phenomenon with some error due to noise

$$y_i = \theta + v_i, v_i \sim N(0, \sigma_i^2), i = 1, 2, \ldots, n$$

- The sensors improve their estimate by averaging the measurements
- Minimum variance estimate

$$\hat{\theta}_{MV} = \frac{\frac{1}{n}\sum_{i=1}^{n} \frac{1}{\sigma_i^2} y_i}{\frac{1}{n}\sum_{j=1}^{n} \frac{1}{\sigma_j^2}}$$

- It can be asymptotically computed in a distributed fashion using two average consensus algorithms in parallel

Consensus in Networked Multi-agent Systems

- Synchronous linear iterative consensus

$$x_i(t+1) = w_{ii}(t)x_i(t) + \sum_{j \in N_i^{in}(t)} w_{ij}(t)x_j(t)$$

- Conditions
  - There exists $0 < \alpha < 1$ such that

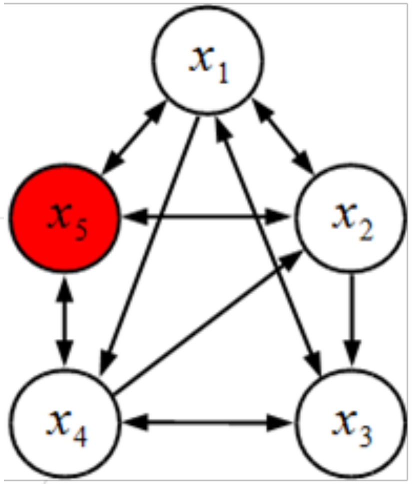
$$w_{ii}(t) \geq \alpha, \forall i,t$$

$$w_{ij}(t) = 0 \text{ if } j \notin N_i^{in}(t), \forall i,j,t$$

$$w_{ij}(t) \geq \alpha \text{ if } j \in N_i^{in}(t), \forall i,j,t$$

$$\sum_{j=1}^{n} w_{ij}(t) = 1, \forall i,t$$

- Consensus is reached if there exists a rooted out-branching periodically over time (in the union of digraphs)



- Resilient consensus in the presence of adversaries
- Applications
  - Vehicle rendezvous, formation control, parameter estimation, least squares data regression, sensor calibration, time synchronization, node counting, Kalman filtering, …

Overview

- Resilient Consensus Protocols in the Presence of Adversaries
  - Adversary models
  - Robust Network Topologies
- Resilient Consensus Protocols with Trusted Nodes
  - Connected Dominating Set
  - Trusted Nodes and Network Robustness
- Distributed Simulation Testbed
  - C2 Wind Tunnel (C2WT)
  - Industrial Control Systems
- Conclusions

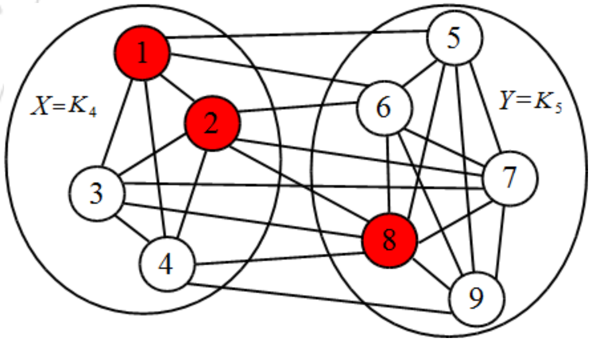
Overview

- Resilient Consensus Protocols in the Presence of Adversaries
    - Adversary models
    - Robust Network Topologies
- Resilient Consensus Protocols with Trusted Nodes
    - Connected Dominating Set
    - Trusted Nodes and Network Robustness
- Distributed Simulation Testbed
    - C2 Wind Tunnel (C2WT)
    - Industrial Control Systems
- Conclusions

Adversary Models

- Crash Adversary
- Malicious Adversary
  - Must convey the same information to all neighbors
    - Local broadcast model
- Byzantine Adversary
  - Can convey different information to different neighbors
- All adversaries are omniscient
  - Topology of the network
  - States and algorithms of the other nodes
  - Other adversaries (can collude)

- F-Total Model
  - At most F adversaries in the entire network
- F-Local Model
  - At most F adversaries in the neighborhood of any normal node
- f-Fraction Local Model
  - At most a fraction f of adversaries in the neighborhood of any normal node



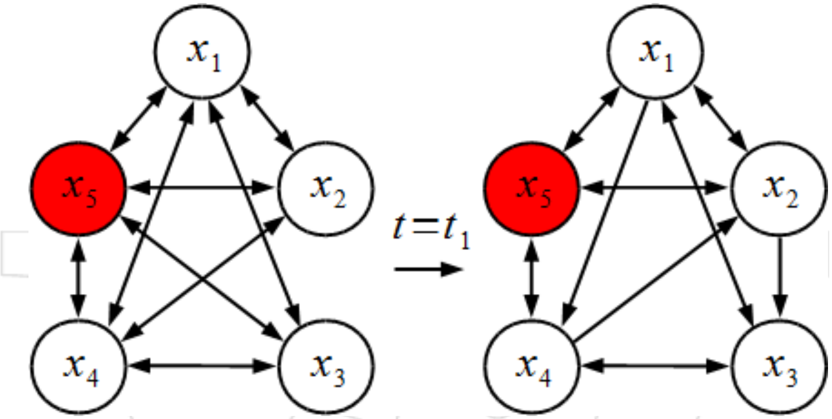
3-total, 3=local, (3/5)-fraction local

Adversarial Resilient Consensus Protocol (ARC-P)

- Weighted consensus protocol with selective reduce
  - Parameter F (or f)
    - $F_i(t) = F$ if the parameter is F
    - $F_i(t) = \lfloor f d_i(t) \rfloor$ if the parameter is f
  - Nonnegative, piecewise continuous, bounded weights
    - $0 < \alpha \leq w_{(j,i)}(t) \leq \beta$ if j is a neighbor at time t
    - $w_{(j,i)}(t) = 0$ otherwise
  - Compare values of neighbors with own value $x_i(t)$
    - Remove (up to) $F_i(t)$ values strictly larger than $x_i(t)$
    - Remove (up to) $F_i(t)$ values strictly smaller than $x_i(t)$
  - Let $\mathcal{R}_i(t)$ denote the set of nodes whose values are removed
  - Update as

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

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

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

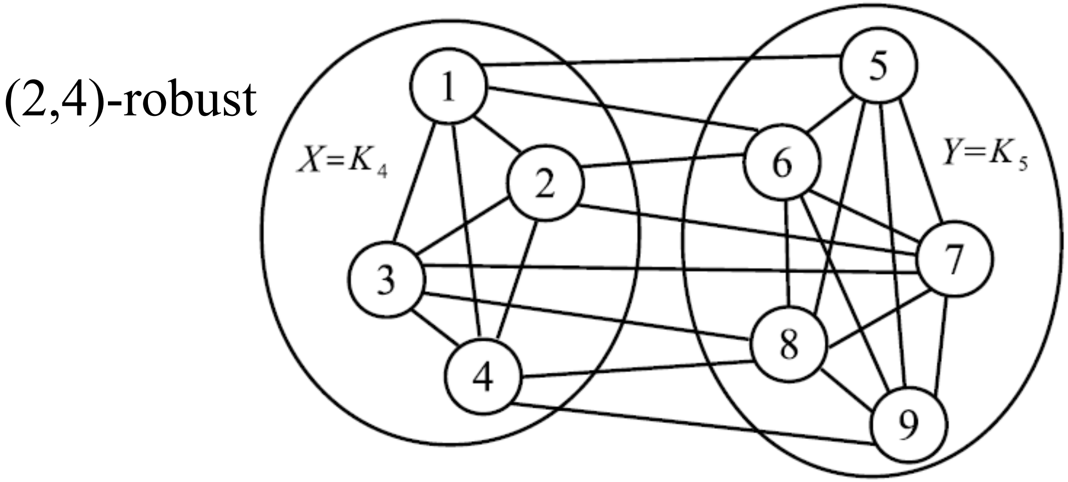
- Safety Condition

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

- 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 Network Topologies



- We need a new graph theoretic property to capture local redundancy
- Specify a minimum number of nodes that are sufficiently influenced from outside their set
- (r,s)-robustness: For every pair of nonempty disjoint sets, there are at least s nodes with at least r in-neighbors outside their respective sets

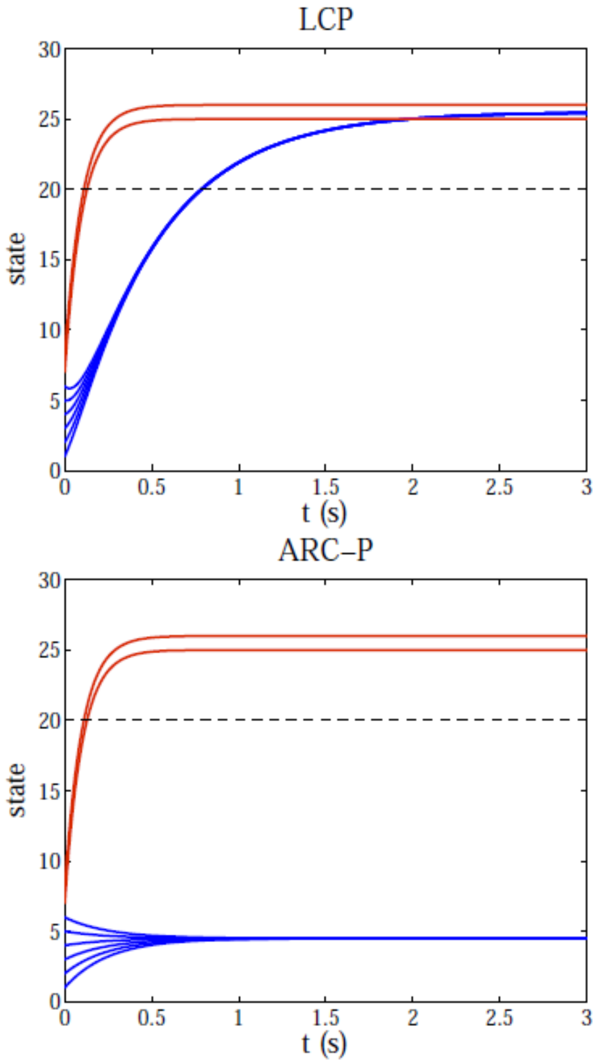
Robust Networks

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 $p > f$

- 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

[LeBlanc et al., IEEE JSAC, April 2013]

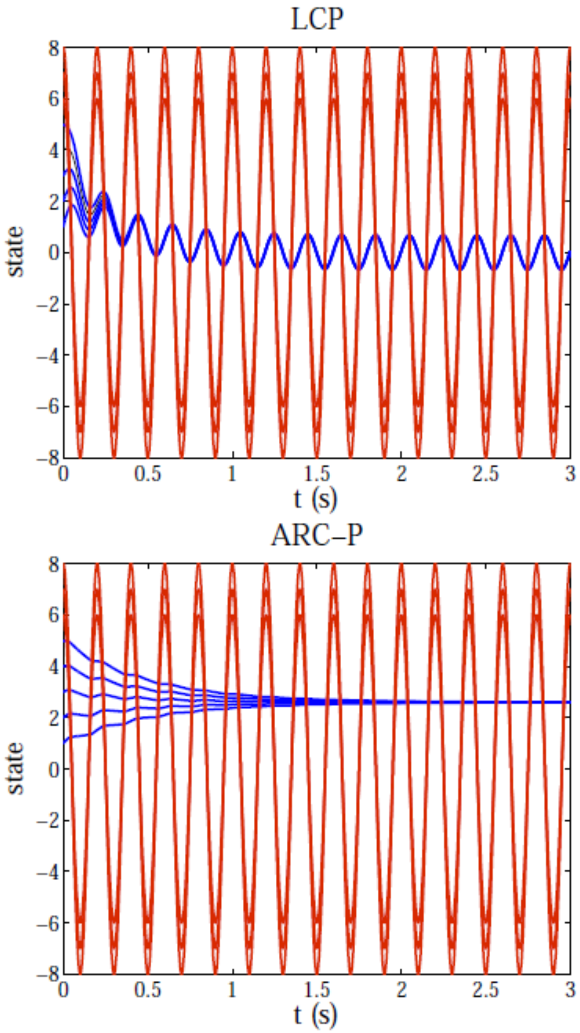
Simulation Results



LCP

ARC–P

Unsafe Region: 8-agent network, 2 adversaries



LCP

ARC–P

Oscillations: 8-agent network, 3 adversaries

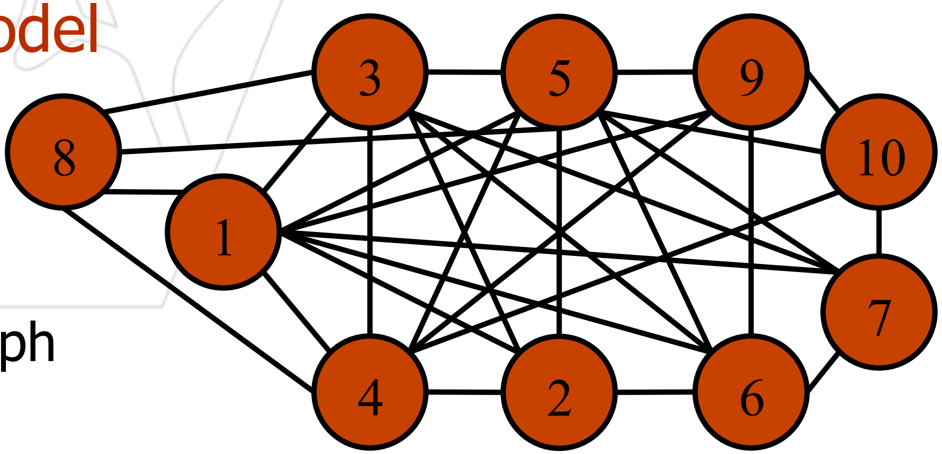
Construction of Robust Networks

- Let $D=(V, E)$ be a nontrivial (r,s)-robust digraph . Then, $D'=(V \cup \{v_{\text{new}}\}, E \cup E_{new})$, where v_{new} is a new node added to D and E_{new} is the directed edge set related to v_{new}, is (r,s)-robust if

$$d^{\text{in}}_{v_{\text{new}}} \geq r + s - 1$$

Preferential-attachment model

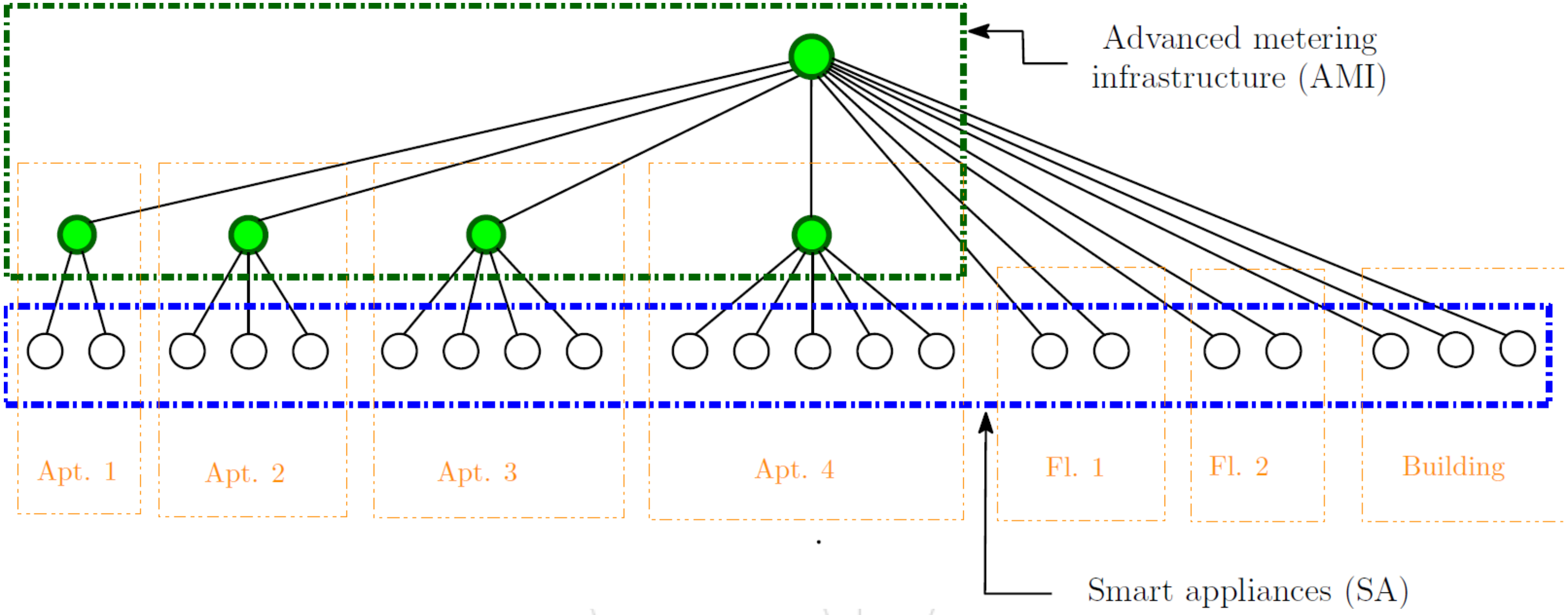
- Initial graph: K_5
- K_5 is (3,2)-robust
- Num edges / round: 4
- End with (3,2)-robust graph



Overview

- Resilient Consensus Protocols in the Presence of Adversaries
  - Adversary models
  - Robust Network Topologies
- Resilient Consensus Protocols with Trusted Nodes
  - Connected Dominating Set
  - Trusted Nodes and Network Robustness
- Distributed Simulation Testbed
  - C2 Wind Tunnel (C2WT)
  - Industrial Control Systems
- Conclusions

Trusted Nodes

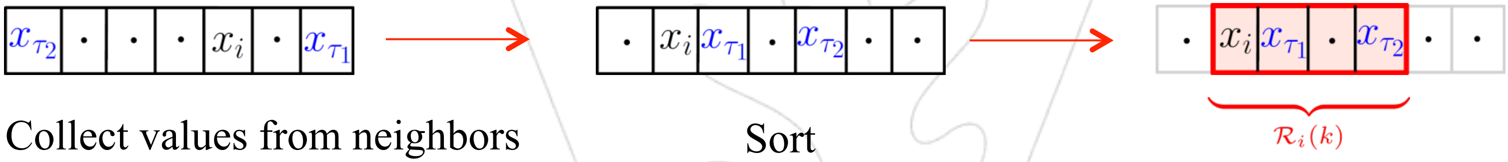


- Assume that some nodes are trusted
    - AMI is generally more secure than SA
- Can we exploit the notion of trusted nodes for relaxing the redundancy conditions?

Resilient Consensus Protocol with Trusted Nodes (RCP-T)

$$x_i(k+1) = \sum_{j \in \mathcal{R}_i(k)} w_{ij}\, x_j(k)$$

- If node i is connected to at least one trusted node

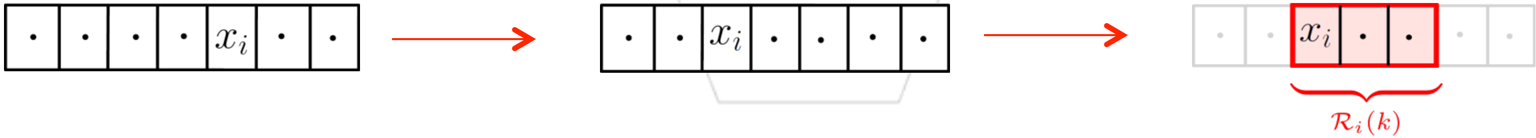


Collect values from neighbors

Sort

(x_{τ_1}, x_{τ_2} are trustworthy nodes' values)

- If node i is not connected to any trusted node



Collect values from neighbors

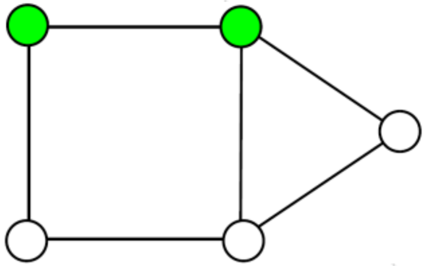
Sort

Remove F largest and F smallest values (Here, F=2)

Connected Dominating Set

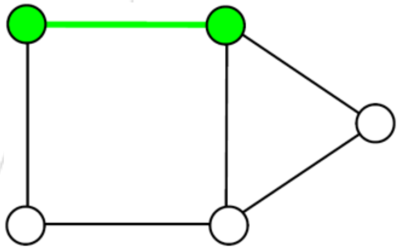
Dominating Set

$$D \subseteq V, \quad \text{s.t.} \quad \bigcup_{v_i \in D} \mathcal{N}[v_i] = V$$



Connected Dominating Set

Nodes in the dominating set induce a connected subgraph



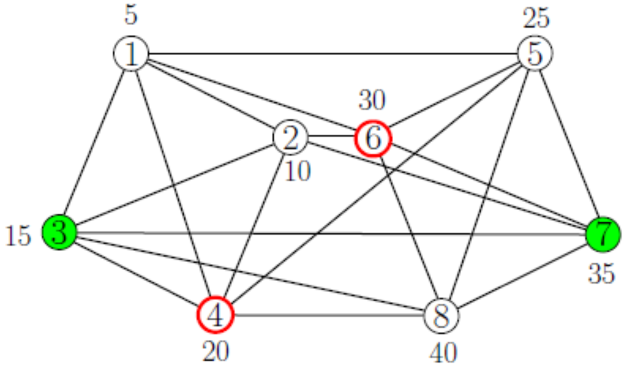
- Under RCP-T, consensus is always achieved in the presence of *arbitrary number of adversaries* if and only if there exists a set of trusted nodes that form a **connected dominating set**

[Abbas et al., ISRCS 2014, Submitted]

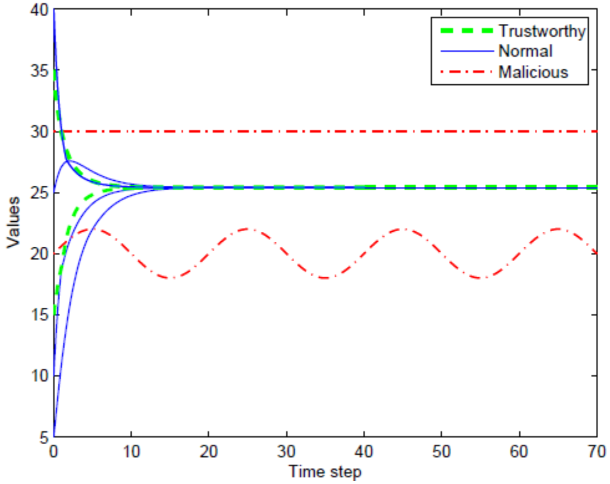
(2,2)-Robust Graph

$$\text{Attacked nodes} = \{4, 6\}$$

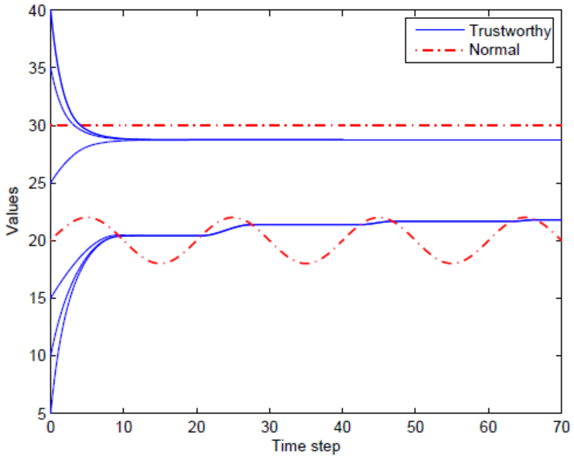
$$\text{Trusted nodes} = \{3, 7\}$$



RCP-T

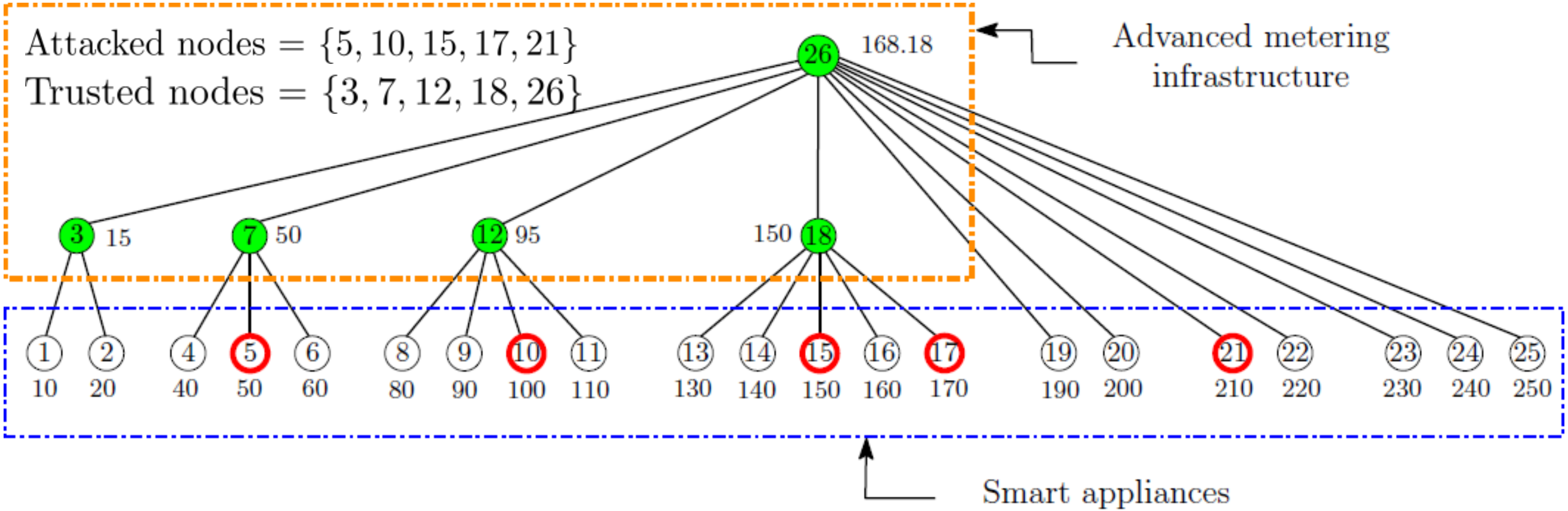


ARC-P



- **RCP-T** achieves consensus in the presence of two adversaries
- **ARC-P** algorithm can handle a single adversary but not two

Tree Networks



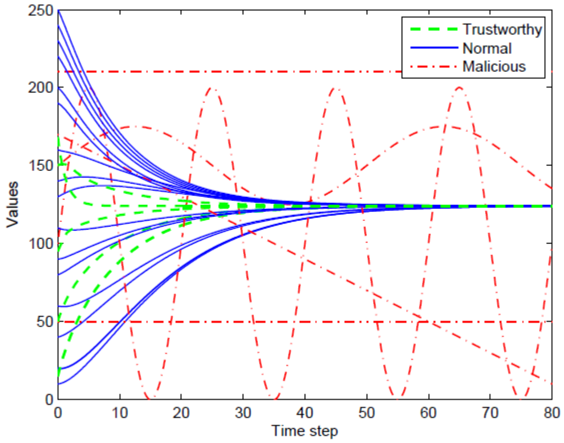
Attacked nodes $= \{5, 10, 15, 17, 21\}$

Trusted nodes $= \{3, 7, 12, 18, 26\}$

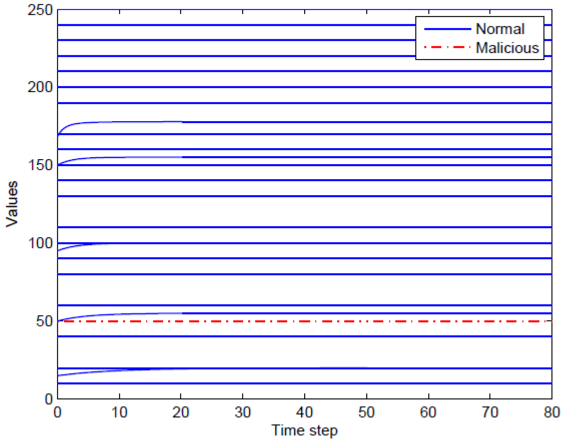
Advanced metering infrastructure

Smart appliances

RCP-T



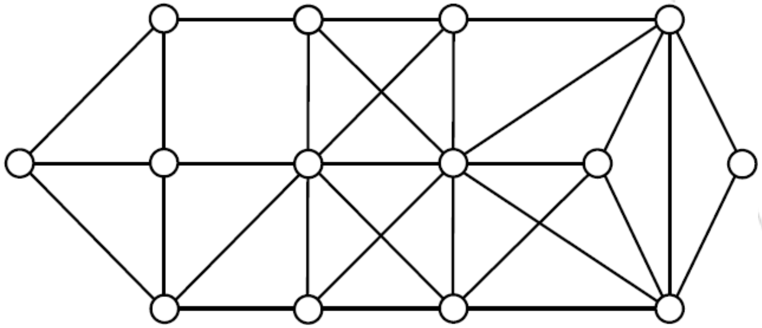
ARC-P



- **RCP-T** achieves consensus even with five adversaries
- **ARC-P** algorithm is not resilient even to a single adversary

Trusted Nodes and Network Robustness

- The **connected domination number** d is the number of vertices in the minimum connected dominating set
- If the number of trusted nodes is at least d, the network can be made resilient against any number of adversaries
- Can we improve resilience if the number of trusted nodes < d?



(2,2)-robust ⟷ Resilient against a single attack (with no trusted nodes)

$d = 4$ ⟷ Resilient against any no. of attacks (with 4 trusted nodes)

With any three trusted nodes, the network is not resilient against two adversarial attacks.

Overview

- Resilient Consensus Protocols in the Presence of Adversaries
  - Adversary models
  - Robust Network Topologies
- Resilient Consensus Protocols with Trusted Nodes
  - Connected Dominating Set
  - Trusted Nodes and Network Robustness
- Distributed Simulation Testbed
  - C2 Wind Tunnel (C2WT)
  - Industrial Control Systems
- Conclusions

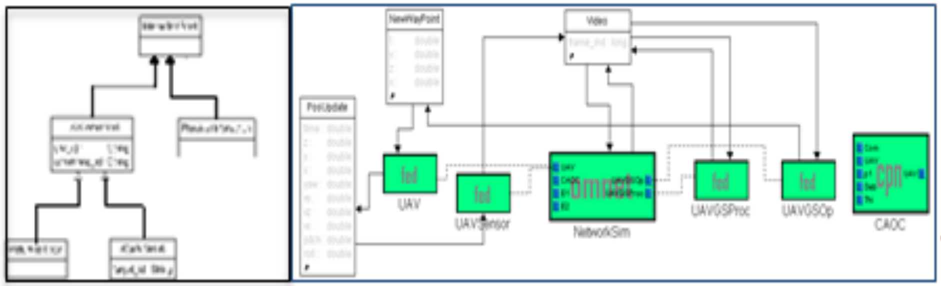
Command and Control Wind Tunnel (C2WT)

Simulation models

Domain-specific models (abstract simulation models)

- CPN
- Simulink
- Delta3D Terrain
- DEVS-Java
- OMNeT++

-Data models (interaction & data models)
-Integration models (data-flow, timing, parameters)
-Compute Infrastructure models
-Deployment models
-Experiment models
-Configuration models



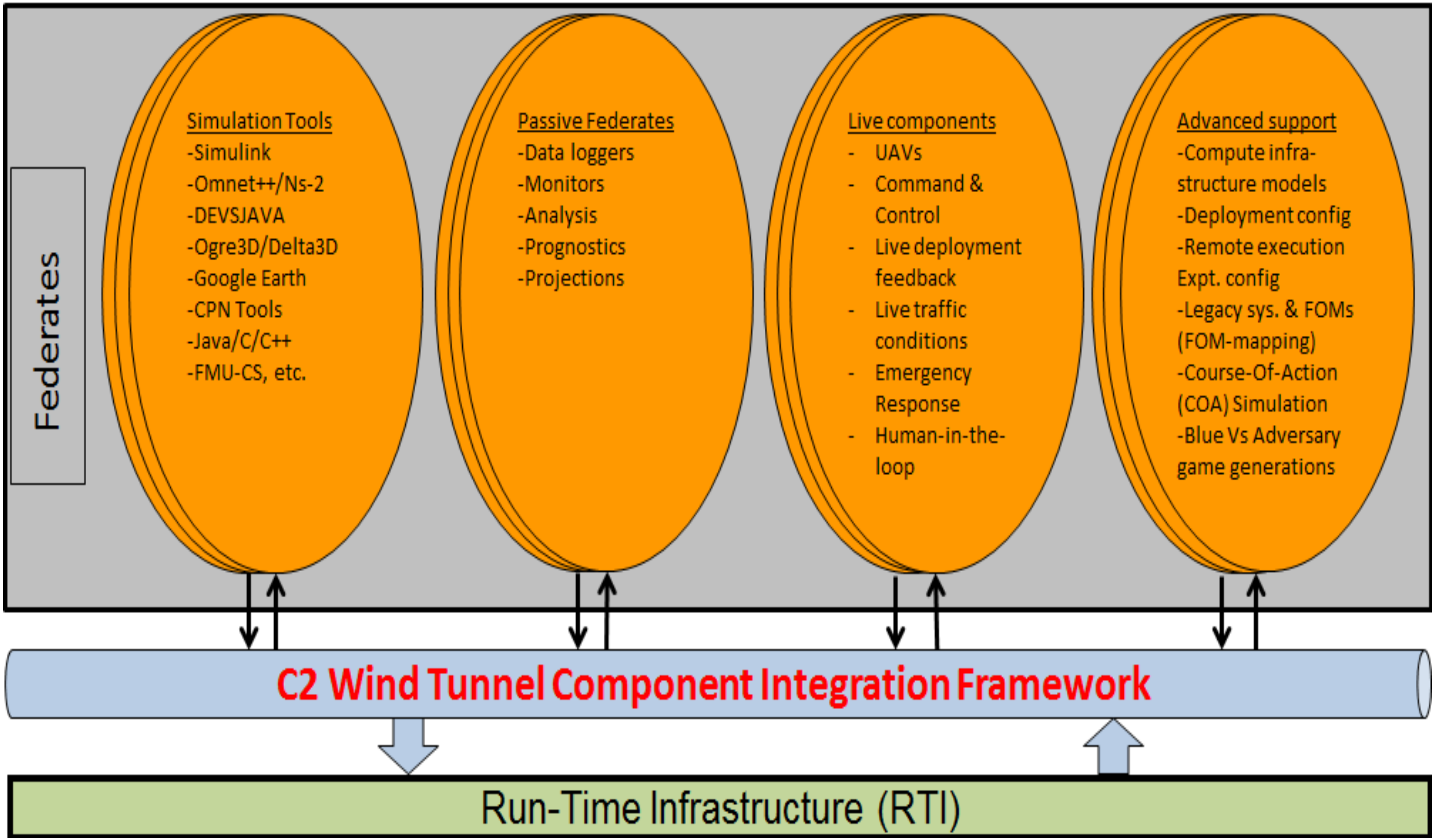
Model transformation

Domain specific federates

OMNeT++ federate	CPN federate	Devs Java federate	Simulink federate	Physics federate	Sensor simulation federate

High-Level Architecture (HLA) Run-Time Infrastructure (RTI): Portico (*open source*)

C2WT Capabilities



Federates

Simulation Tools
- -Simulink
- -Omnet++/Ns-2
- -DEVSJAVA
- -Ogre3D/Delta3D
- -Google Earth
- -CPN Tools
- -Java/C/C++
- -FMU-CS, etc.

Passive Federates
- -Data loggers
- -Monitors
- -Analysis
- -Prognostics
- -Projections

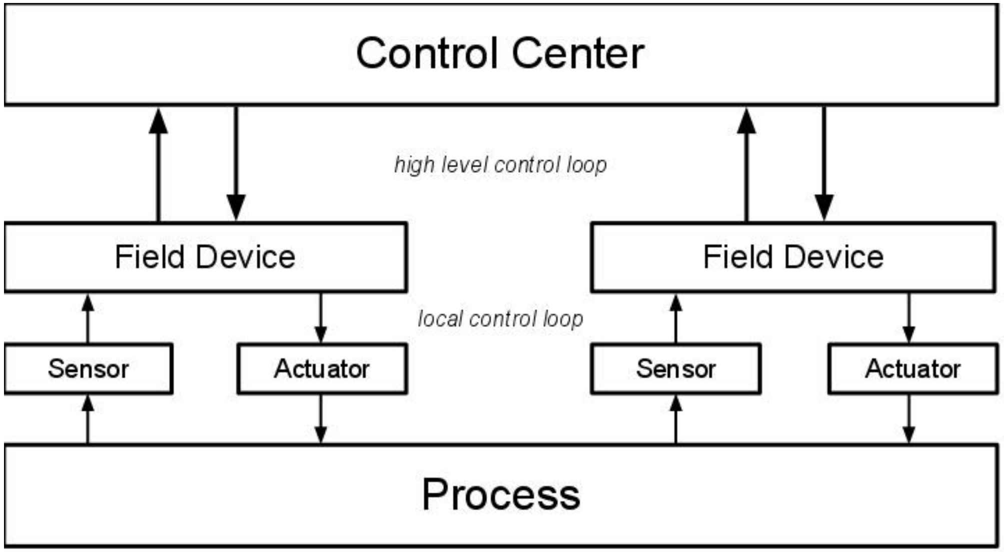
Live components
- UAVs
- Command & Control
- Live deployment feedback
- Live traffic conditions
- Emergency Response
- Human-in-the-loop

Advanced support
- -Compute infra-structure models
- -Deployment config
- -Remote execution Expt. config
- -Legacy sys. & FOMs (FOM-mapping)
- -Course-Of-Action (COA) Simulation
- -Blue Vs Adversary game generations

C2 Wind Tunnel Component Integration Framework

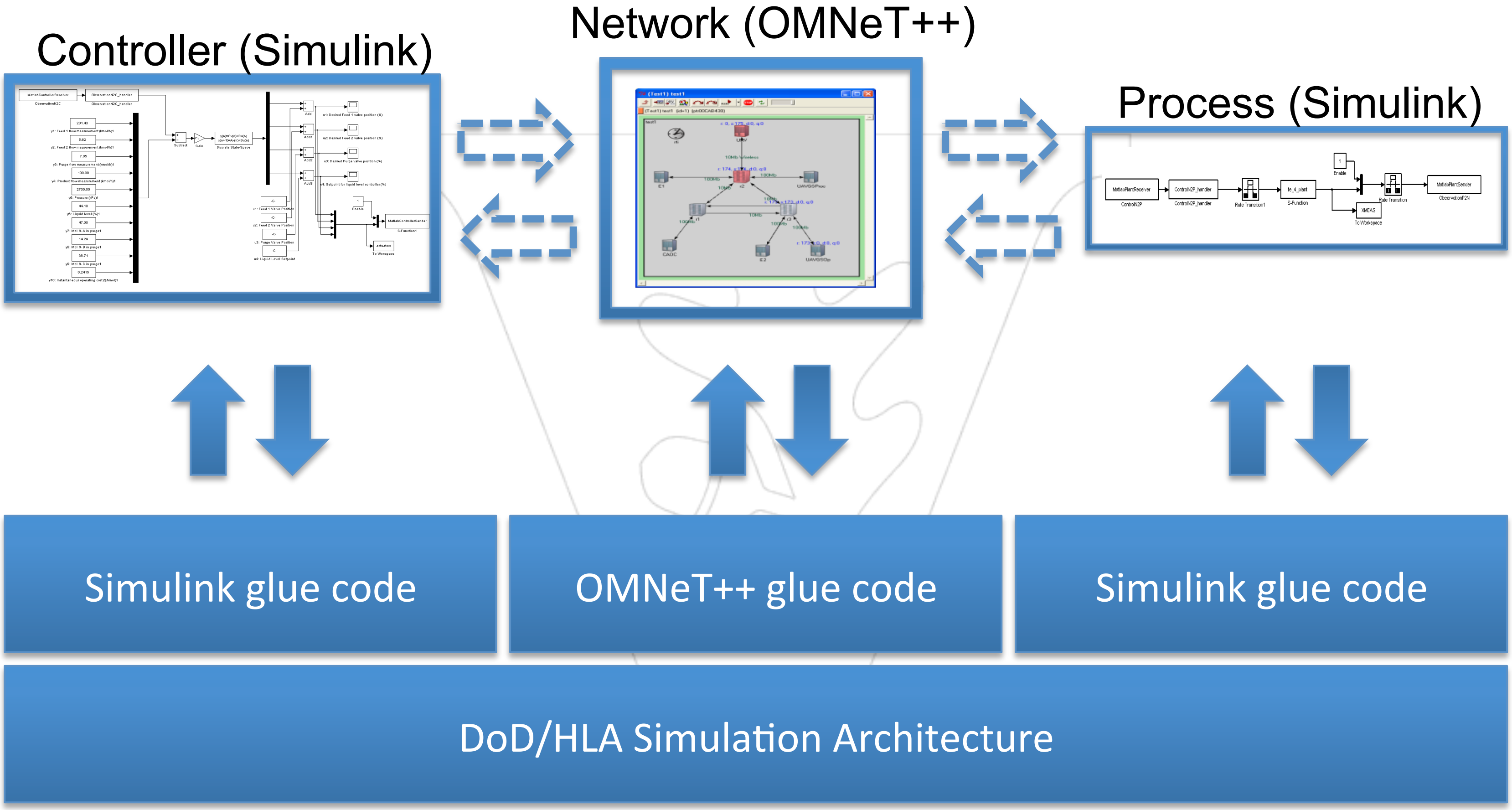
Run-Time Infrastructure (RTI)

Industrial Control Systems (ICS)



- Control center communicates with field devices interacting with the process
- Two levels of control loops:
    - High-level feedback loop over network
    - Low-level feedback loop local to physical process

ICS Simulations using C2WT



Controller (Simulink)

Network (OMNeT++)

Process (Simulink)

Simulink glue code

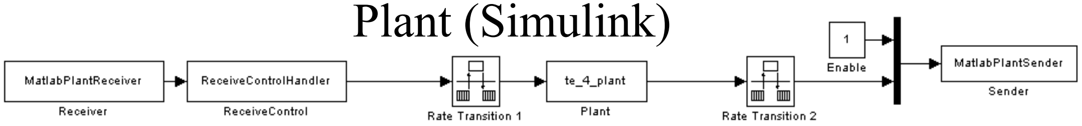
OMNeT++ glue code

Simulink glue code

DoD/HLA Simulation Architecture

Simulation of DDOS Attack

Plant (Simulink)



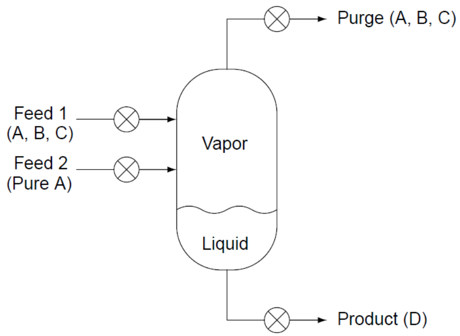
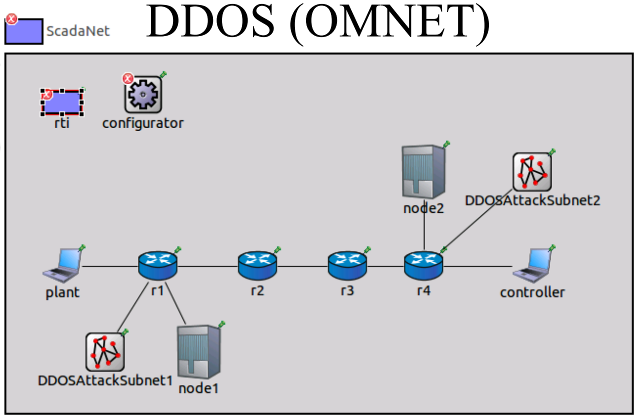
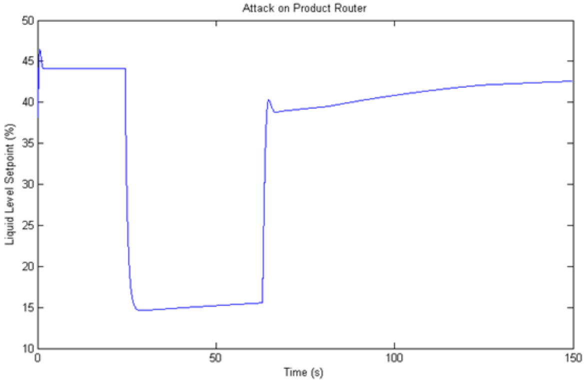


Figure: Chemical Plant (A + C → D)

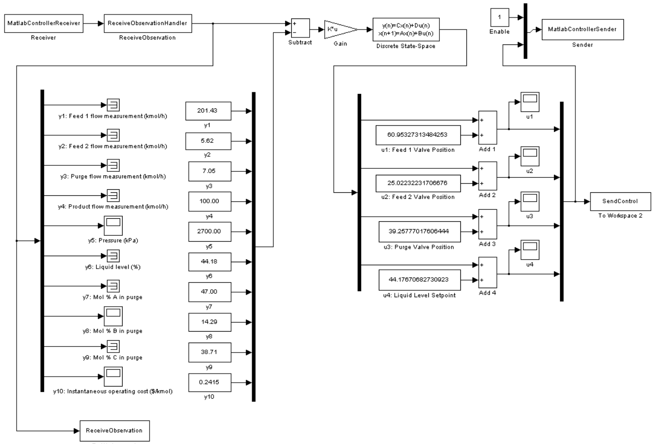
Tennessee Eastman Reactor

DDOS (OMNET)





Cyber attack destabilizes the liquid level in the reactor



Controller (Simulink)

Conclusions

- Resilient Consensus Protocols in the Presence of Adversaries
  - Exploit local information redundancy to ensure asymptotic consensus
  - Characterize robust network topologies
- Resilient Consensus Protocols with Trusted Nodes
  - Trusted nodes form a connected dominating set
- Simulation of CPS using the C2 Wind Tunnel (C2WT)
  - Industrial Control Systems