Wireless Control Networks
Modeling, Synthesis, Robustness, Security

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

George J. Pappas
Joseph Moore Professor
School of Engineering and Applied Science
University of Pennsylvania
pappasg@seas.upenn.edu

Penn
UNIVERSITY of PENNSYLVANIA

Many thanks

Penn
University of Pennsylvania

NSF

MuSyC

KTH
VETENSKAP OCH KONST

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

ABB

Honeywell

University of Waterloo

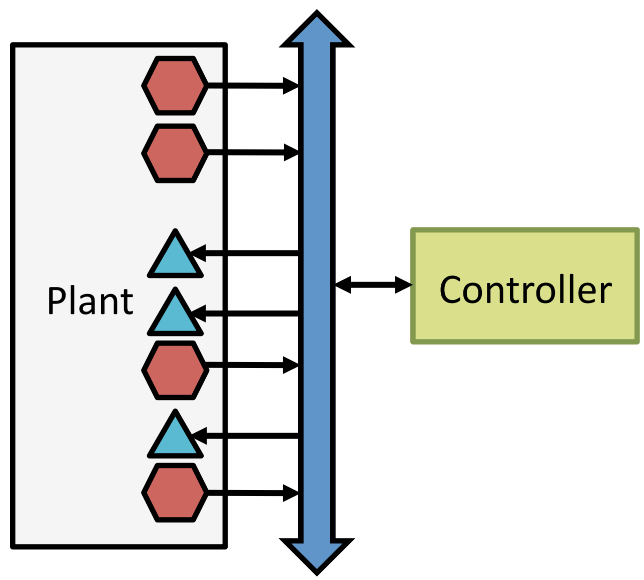
RENOVABITUR UT AQUILAE JUVENTUS TUA
JUS LITTERAE SCIENTIAE

Industrial Control Systems: $120Billion/Year market

Industrial Control Systems: Architectures

- Sensors ( ) and Actuators ( ) are installed on a plant
- Communicate with controller ( ) over a wired network

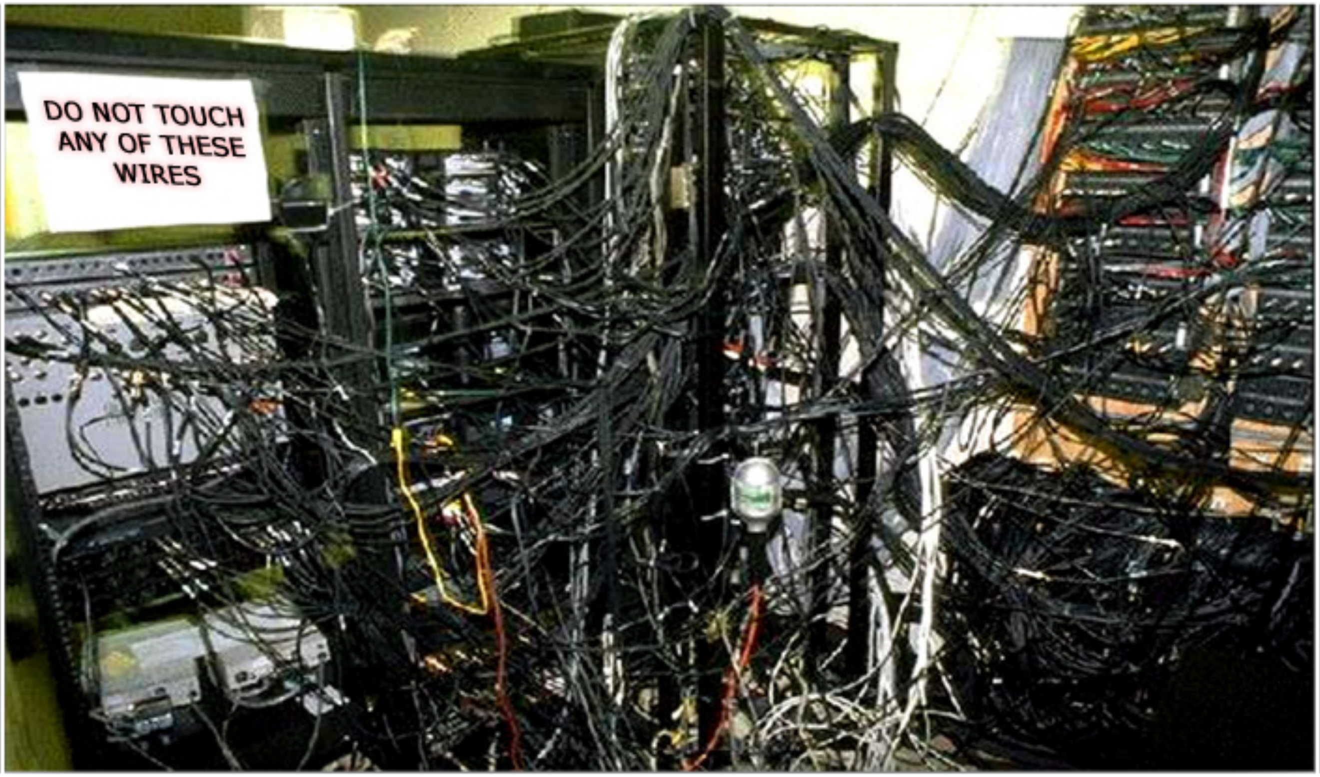
Wired Control Architecture



- Control is typically PID loops running on PLC
- Communication protocols are increasingly time-triggered

State-of-the-art: Wired Control Systems

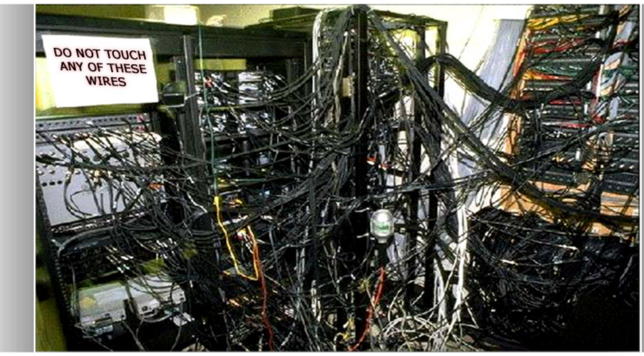
Penn
UNIVERSITY of PENNSYLVANIA



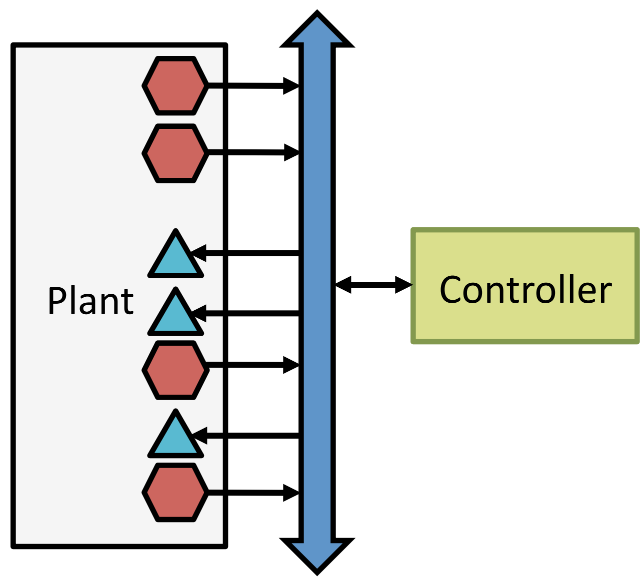
Courtesy of Honeywell

Challenges with Wired Control Systems

- Wires are expensive
  - Wires as well as installation costs
  - Wire/connector wear and tear

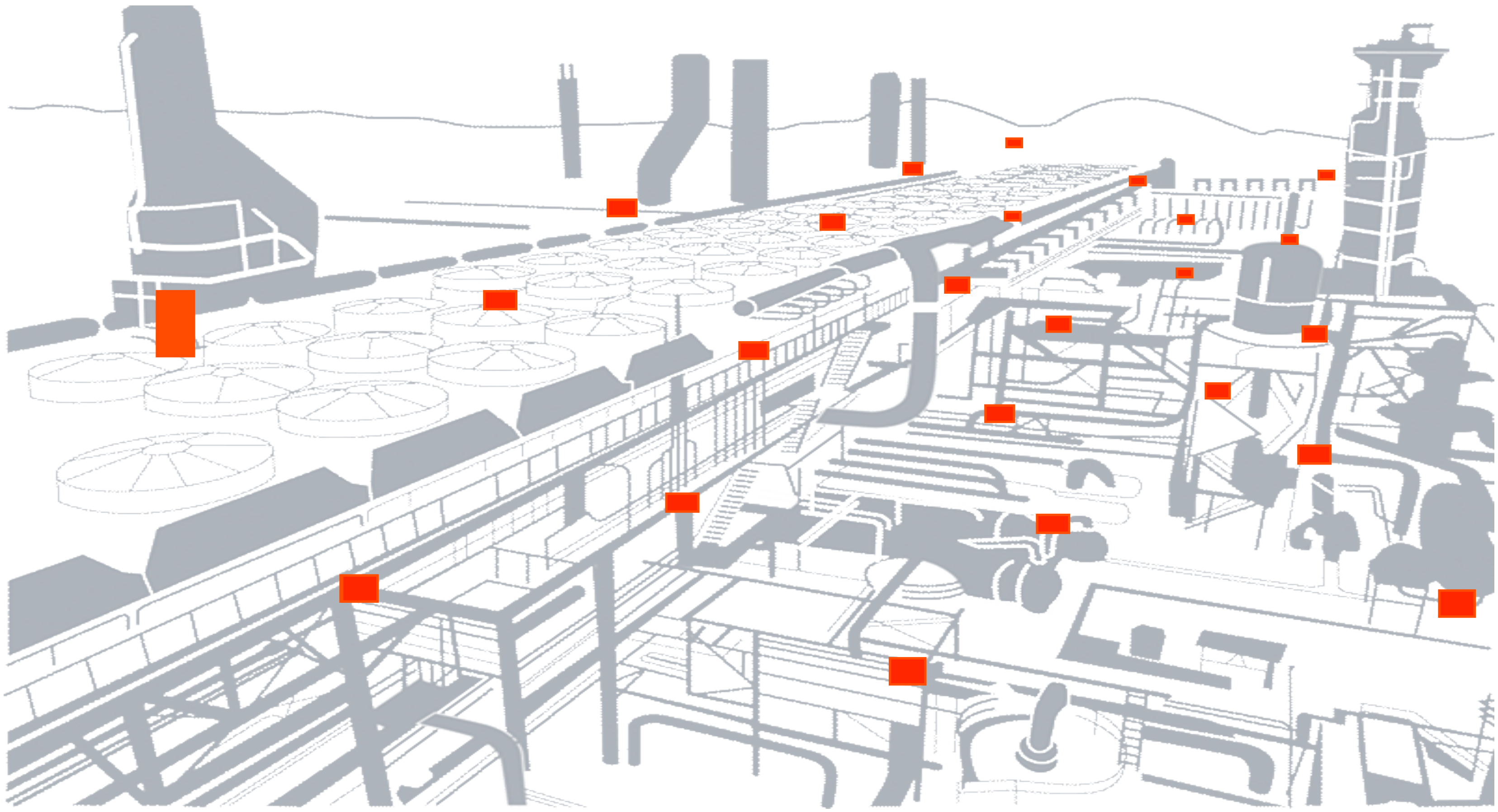


- Lack of flexibility
  - Wires constrain sensor/actuator mobility
  - Limited reconfiguration options
- Restricted control architectures
  - Centralized control paradigm



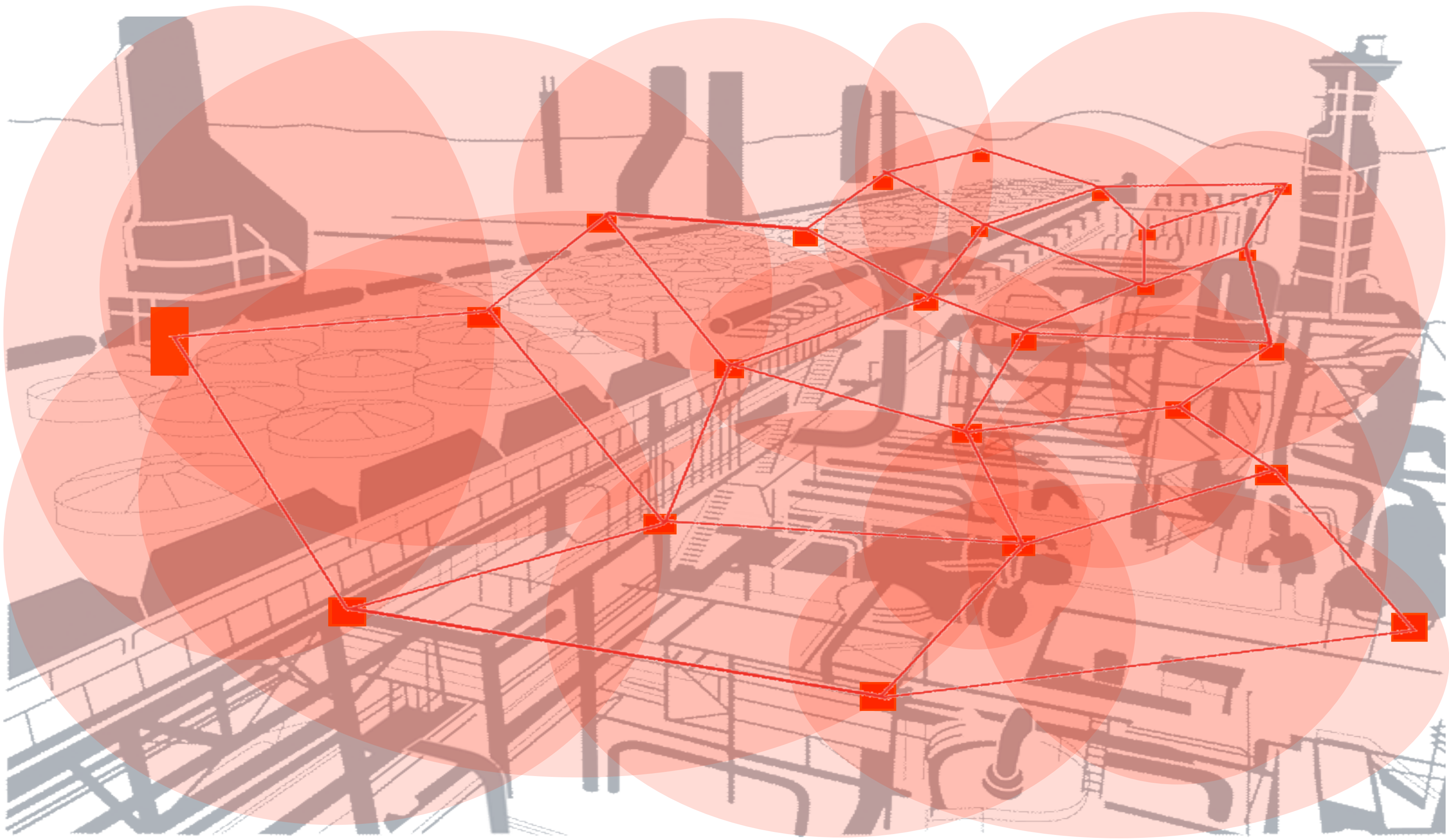
The promise: Wireless Control Systems

Penn UNIVERSITY of PENNSYLVANIA



Courtesy of **Honeywell**

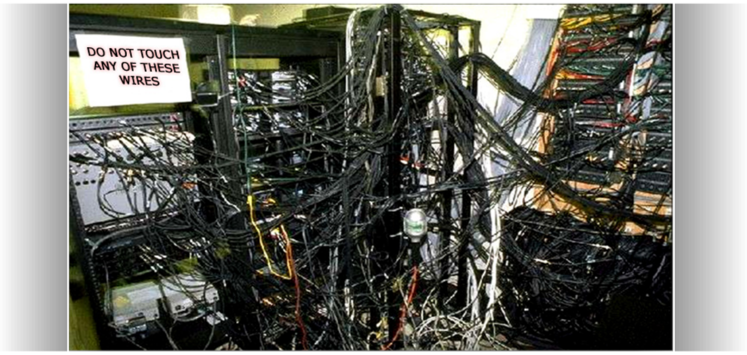
The promise: Wireless Control Systems



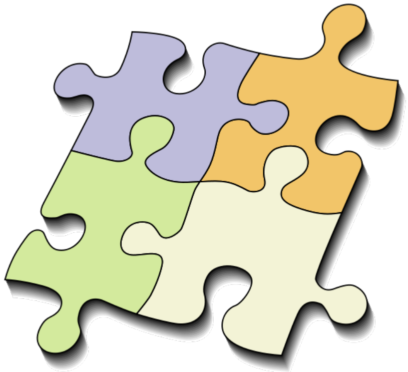
Courtesy of Honeywell

Opportunities with Wireless Control Systems

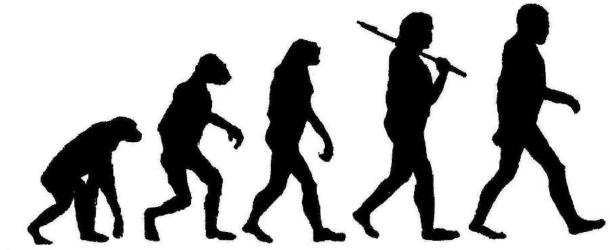
- Lower costs, easier installation
  - Suitable for emerging markets



- Broadens scope of sensing and control
  - Easier to sense/monitor/actuate
  - New application domains



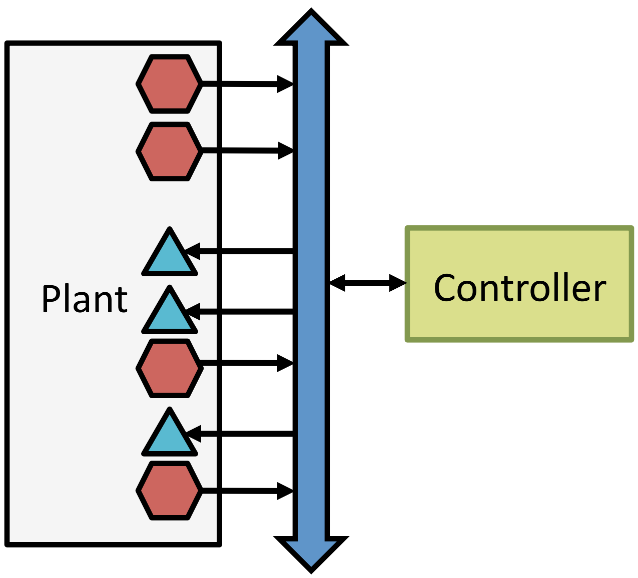
- Compositionality
  - Enables system evolution through logical expansion/contraction of plants and controllers with composable control systems.



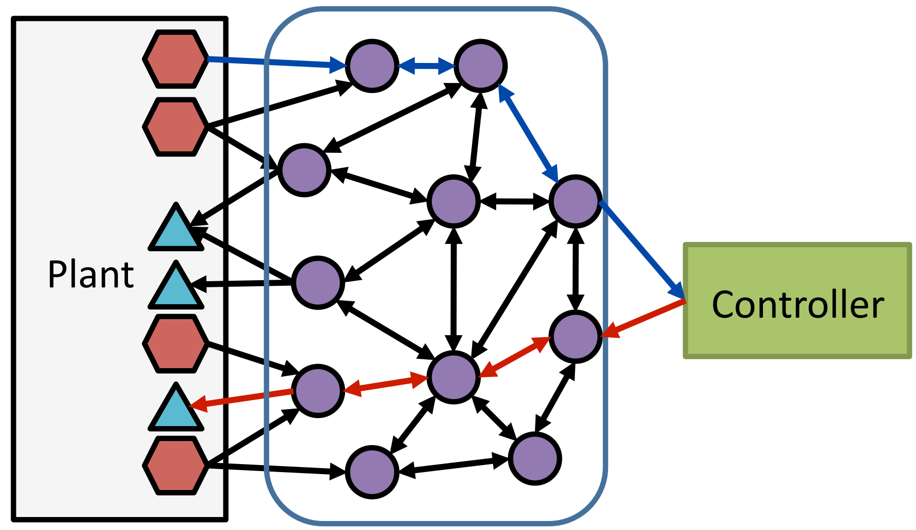
- Runtime adaptation
  - Control stability and performance are maintained in the presence of node, link and topological changes.

Wireless is transformative for industrial control

- Paradigm shift towards multi-hop control architectures



Wired Control System

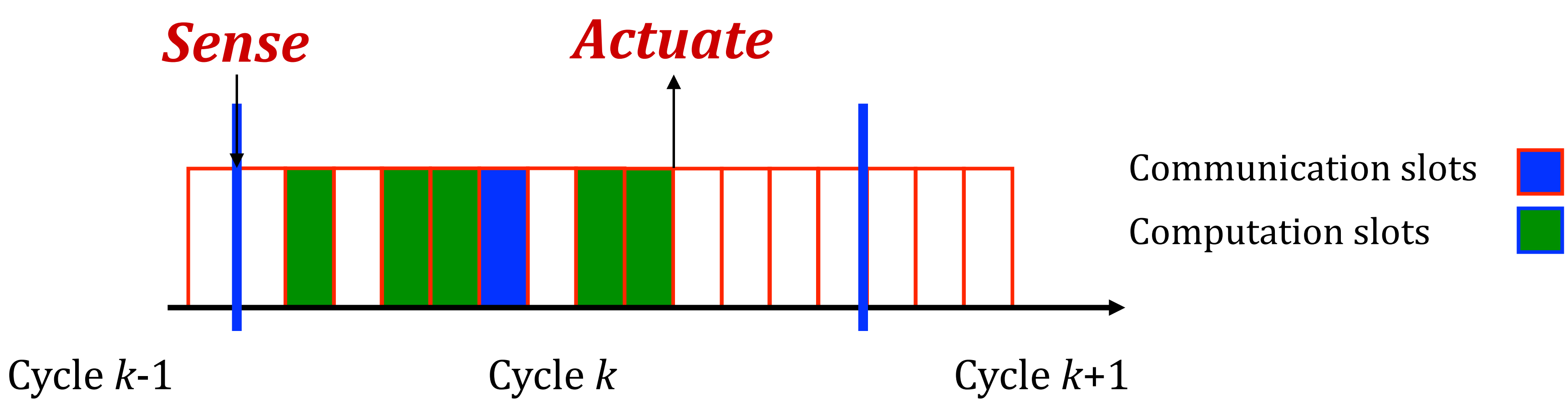


Wireless Control System

Time-Triggered Protocols

Penn
UNIVERSITY of PENNSYLVANIA

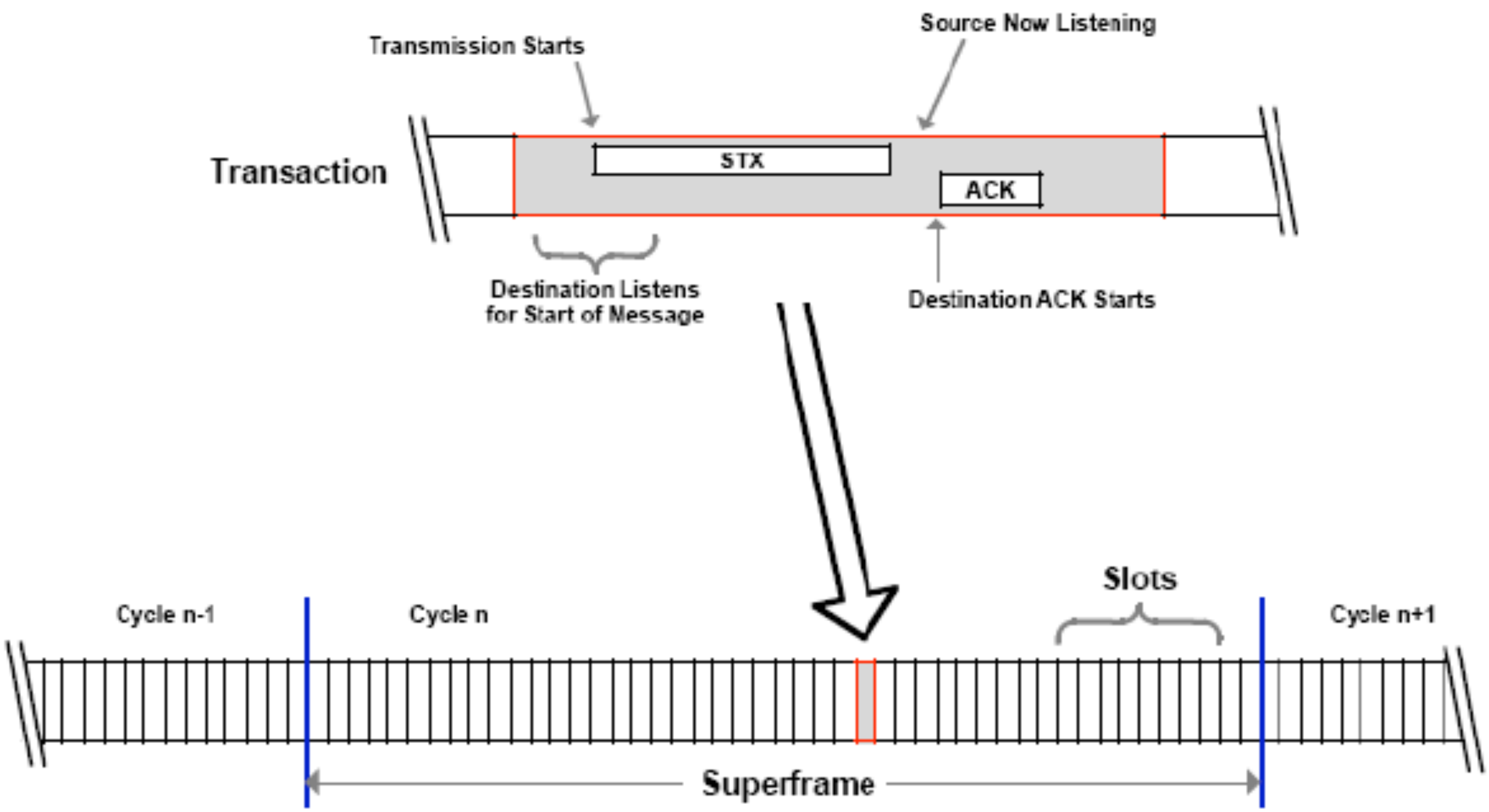
- Widely used for time-critical industrial control applications
- Instead of mapping control computation and communication to periodic-tasks, we allocate them to precise time-slots



- Wireless time-triggered standards (ISA100, WirelessHART)

WirelessHART

- TTA Architecture (TDMA – FDMA), 10ms slots



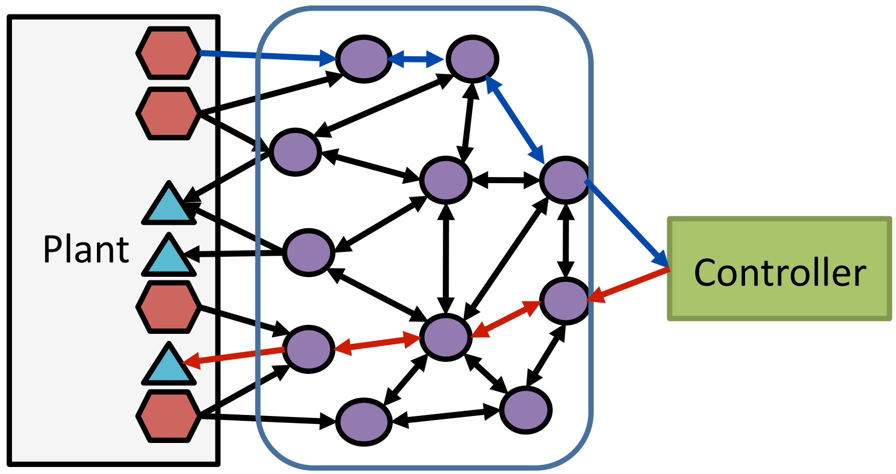
Wireless Control Systems: Technical Challenges

- Modeling
  - Holistic modeling of control, communication, computation
  - Interfaces between control and time-triggered communication
- Analysis
  - Impact of TDMA-based wireless on control performance
  - Compositional scheduling of multiple control loops
- Synthesis
  - Control-scheduling co-design
  - Controller design incorporating TDMA-based properties
  - Network topology design based on physical plant properties
- Robustness
  - Robustness analysis with respect to packet loses, node failures
  - Robustness with respect to faulty or malicious nodes

Control with multi-hop networks

Penn
University *of* Pennsylvania

- Control with multi-hop wireless networks*

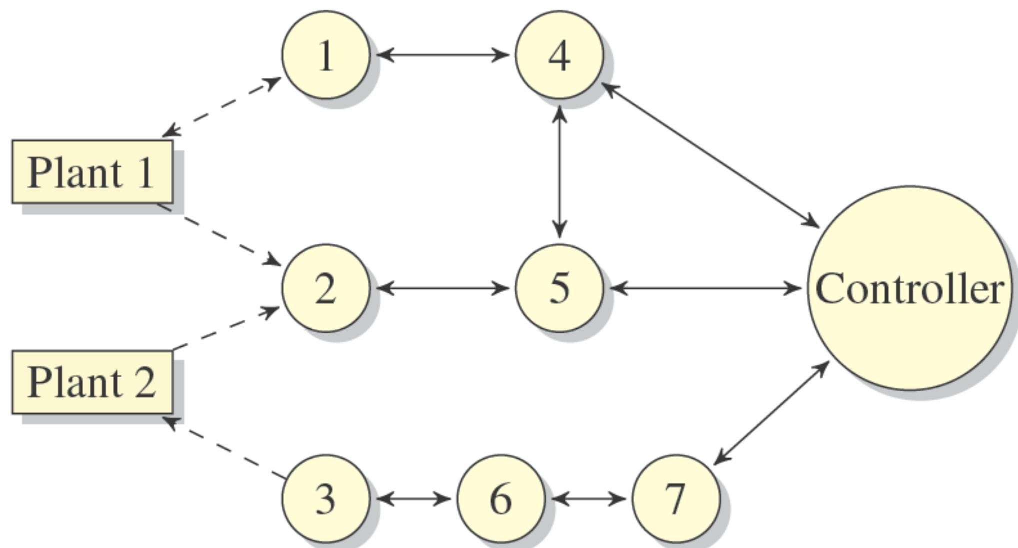


  - **Formal modeling**
  - Analysis & synthesis
  - Compositional analysis
  - Industrial case study

*R. Alur, A. D'Innocenzo, K.H. Johansson, G. Pappas, G. Weiss *Compositional modeling and analysis of multi-hop networks*, IEEE Transactions on Automatic Control, to appear

Control with multi-hop networks: Modeling

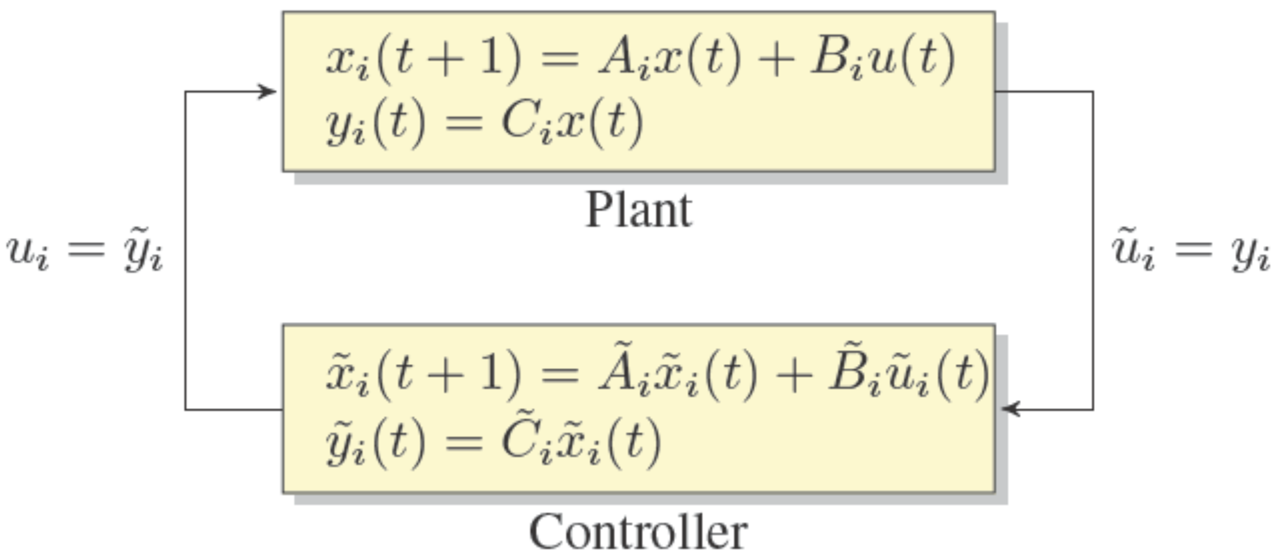
- A multi-hop wireless networked system



- Assumptions:
  – Plants/controllers are discrete-time linear systems
  – Multi-hop network runs time-triggered protocol

Control with multi-hop networks: Modeling

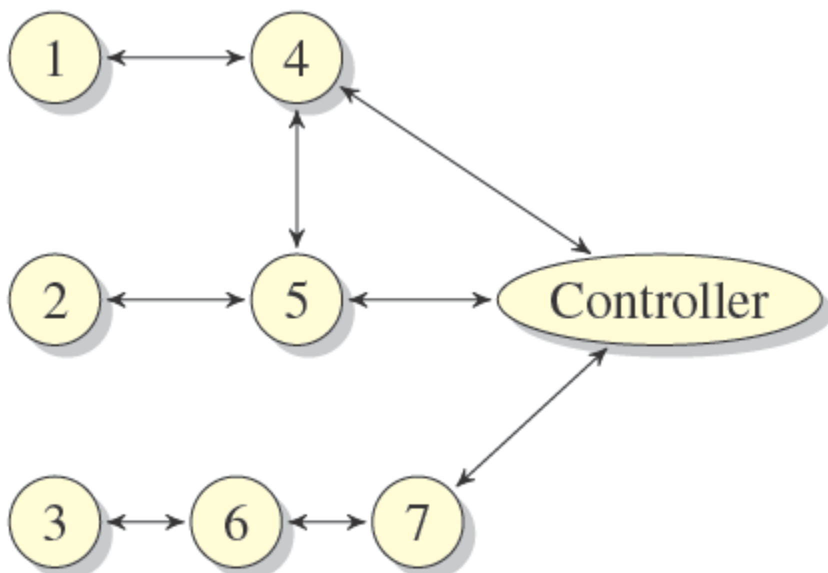
- Plants/controllers are discrete-time linear systems



- Controllers are designed to achieve suitable performance

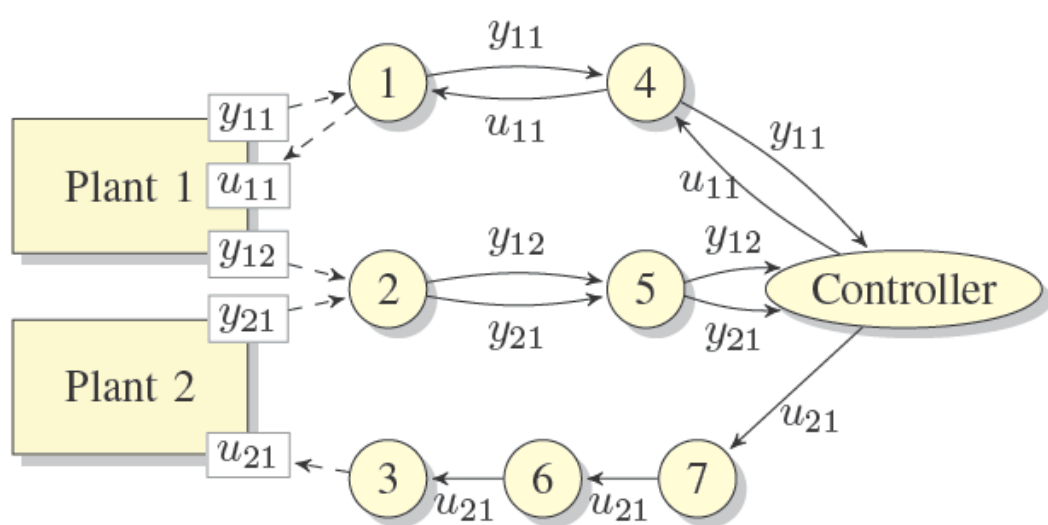
Control with multi-hop networks: Modeling

- Plants/controllers are discrete-time linear systems
- Graph G = (V,E) where V is the set of nodes and E is the radio connectivity graph

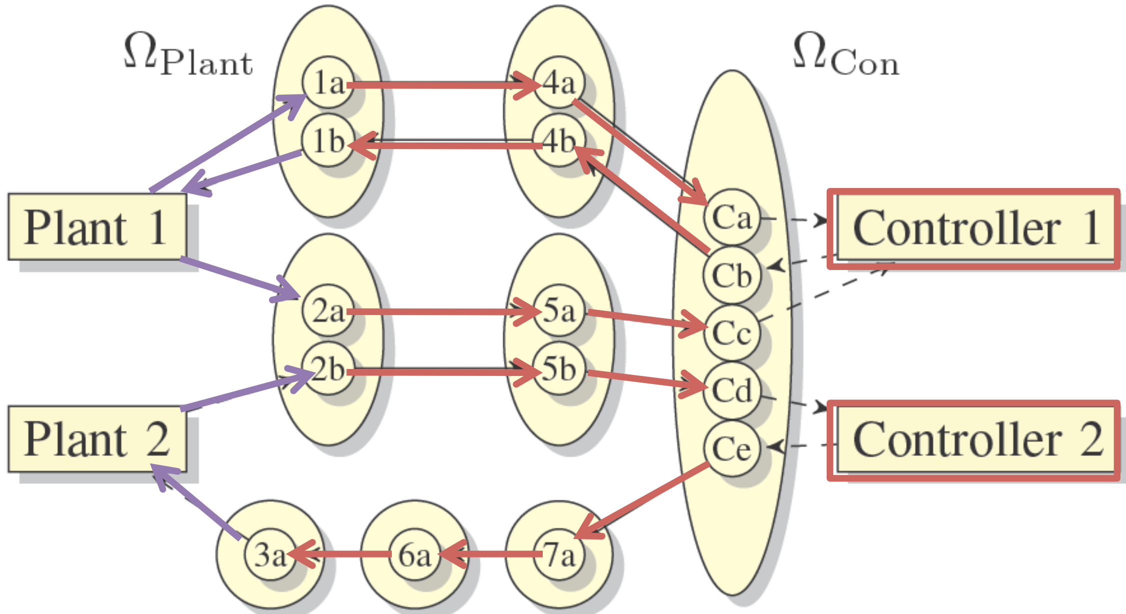


Control with multi-hop networks: Modeling

- Plants/controllers are discrete-time linear systems
- Graph G = (V,E) where V is the set of nodes and E is the radio connectivity graph
- Routing $R : I \cup O \rightarrow 2V^{*}\setminus\{\emptyset\}$ associates to each pair sensor-controller or controller-actuator a set of allowed routing paths

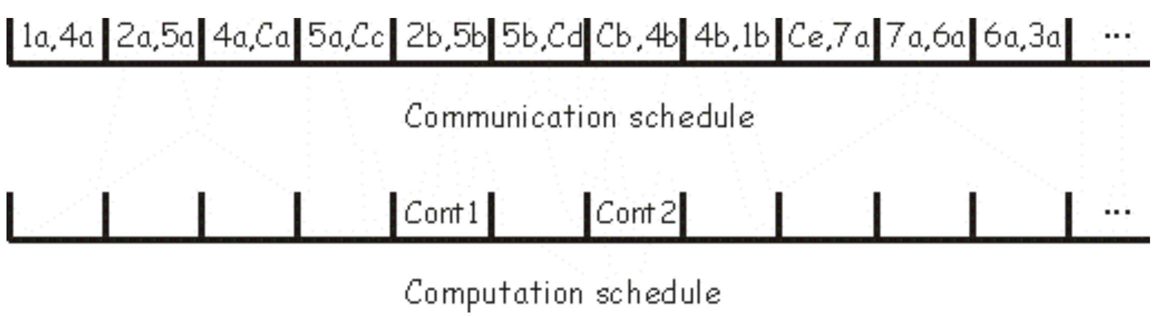


Communication and computation schedule

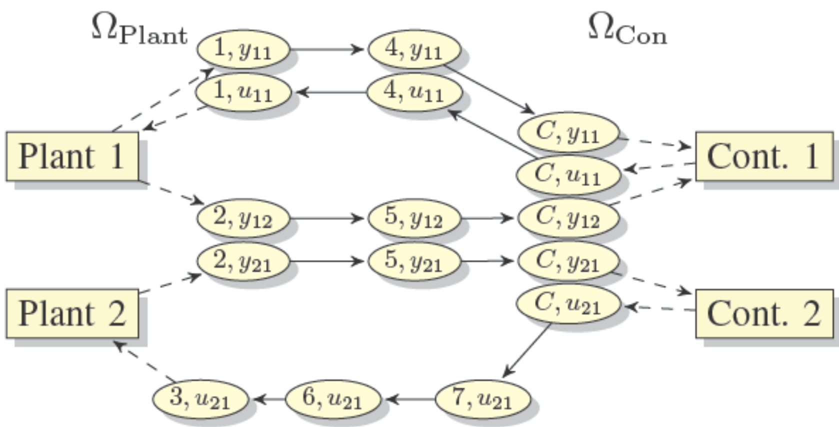


Communication schedules: $\eta: \mathbb{N} \rightarrow 2^{E\times(\mathbb{I}\cup\mathbb{O})}$

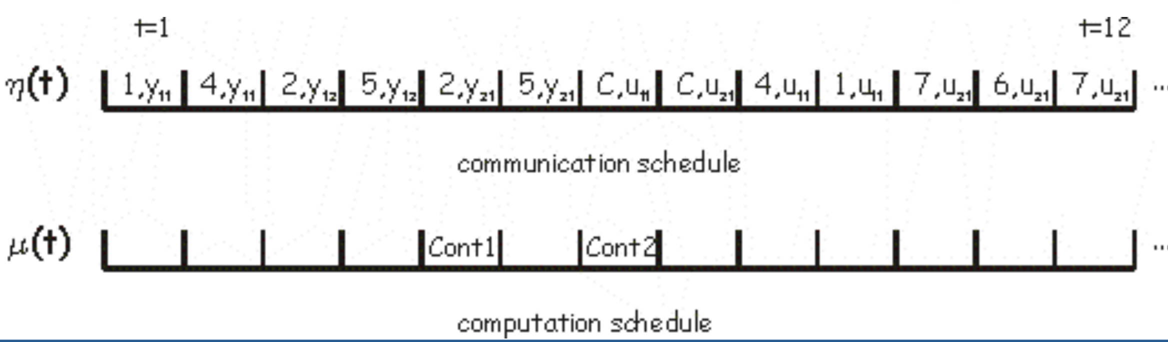
Computation schedules: $\mu_i: \mathbb{N} \rightarrow \{\text{Idle, Active}\}$



Evolution in each time step



$$T[\eta(t), \mu(t)] = \begin{pmatrix} A_{\text{Plant}} & B_{\text{Plant}} \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix} & 0 \\ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} C_{\text{Plant}} & \text{Adjacency matrix of } \eta(t) & \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} C^{\mu(t)}_{\text{Controller}} \\ 0 & B^{\mu(t)}_{\text{Controller}} \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} & A^{\mu(t)}_{\text{Controller}} \end{pmatrix}$$



Integrated modeling

Given communication and computation schedules, the closed loop multi-hop control system is a switched linear system

$$x(t+1) = T[\eta(t), \mu(t)]x(t)$$

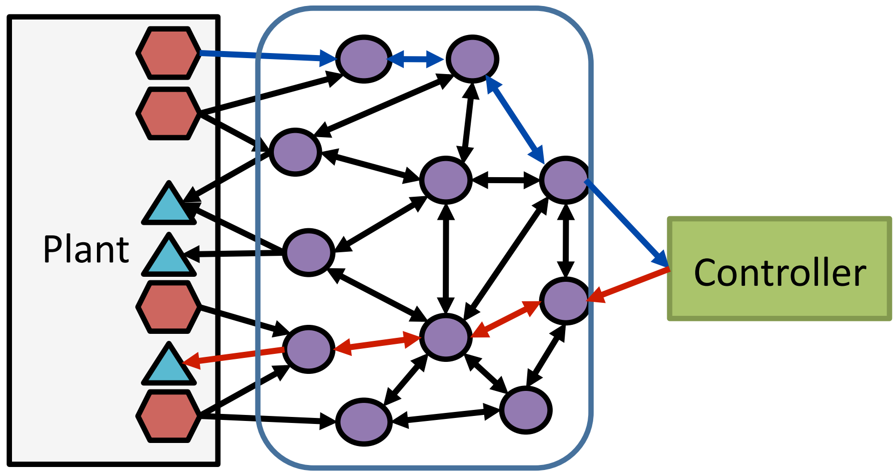
where the schedule (discrete switching signal) is either:

1. Deterministic and periodic
2. Nondeterministic and periodic
3. Stochastic due to packet loss, failures

Modeling the multi-hop control network as a hybrid system!

Control with multi-hop networks

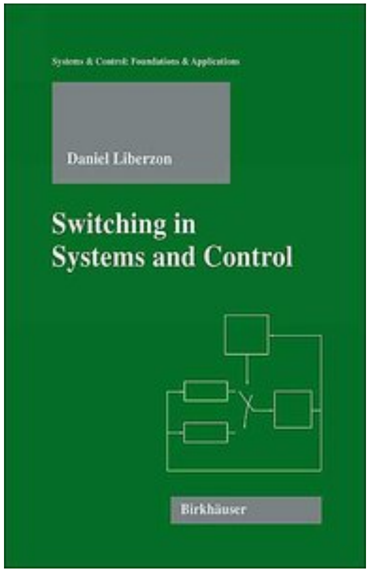
- Control with multi-hop wireless networks



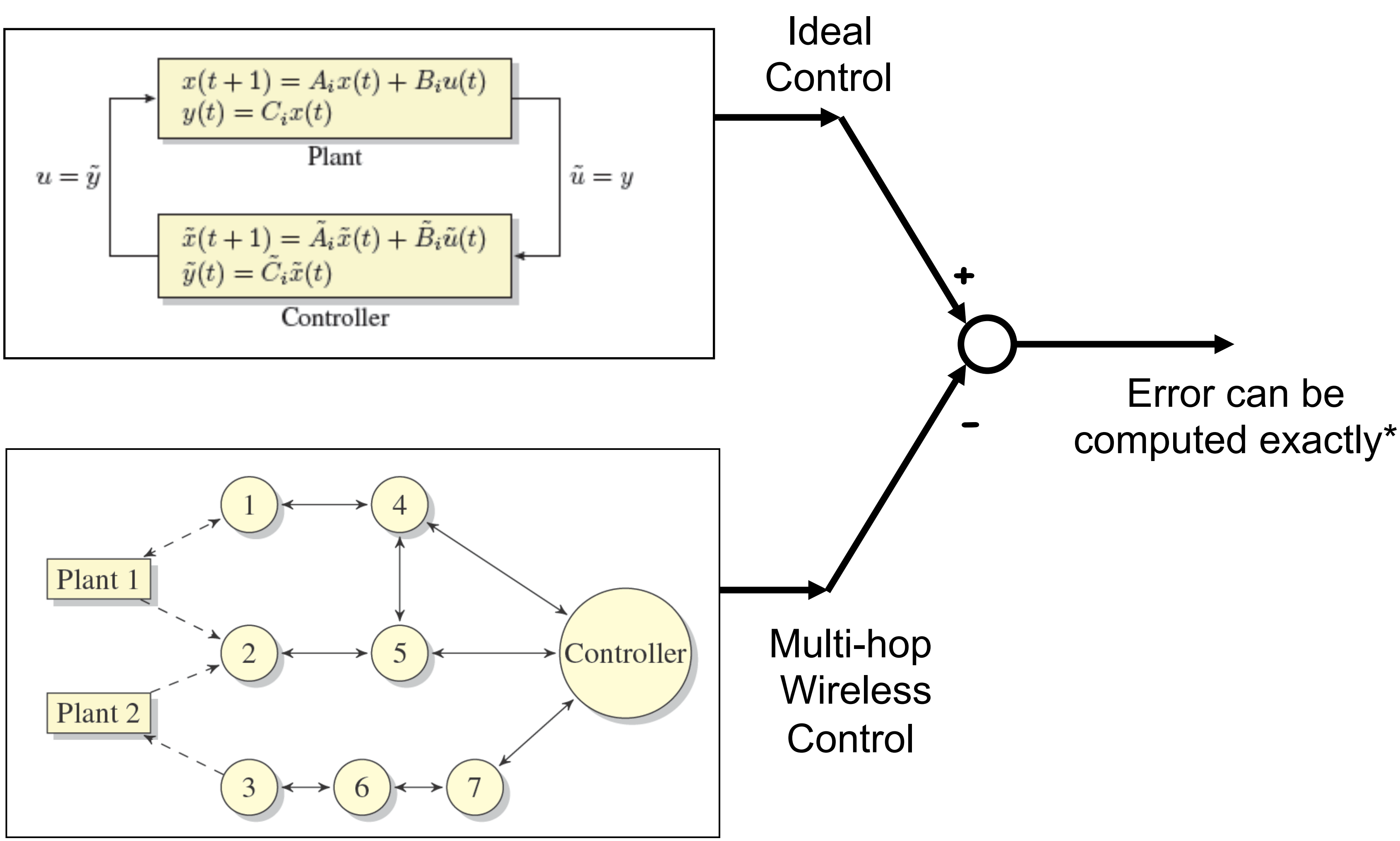
  - Formal modeling
  - **Analysis & synthesis**
  - Compositional analysis
  - Industrial case study

Analysis of multi-hop control networks

- Periodic deterministic schedule (static routing, no TX errors):
  - Theory of periodic time varying linear systems applies
  - Schedule is a fixed string in the alphabet of edges/controllers
  - Nghiem, Pappas, Girard,Alur – EMSOFT 2006, ACM TECS 2010
- Periodic non-deterministic schedule (dynamic routing):
  - Theory of switched/hybrid linear system can be applied
  - Schedule is an automaton over edges/controllers
  - Alur, Weiss – HSCC 2007
- Stochastic analysis (stochastic packet loss, failures):
  - Theory of discrete time Markov jump linear systems applies
  - Schedule is a Markov Chain over edges/controllers
  - Alur, D'Innocenzo, K.H. Johannsson, Pappas, Weiss, IEEE CDC 2009

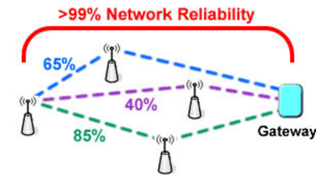


Periodic deterministic schedules



*T. Nghiem, G. Pappas, A. Girard, R. Alur, *Time triggered implementations of dynamic controllers*, ACM Transactions on Embedded Computing Systems, to appear

Modeling communication failures



We consider 3 types of failure models:

Long communication disruptions (w.r.t the speed of the control system) → Permanent link failures

Typical packet transmission errors (errors with short time span) → Independent Bernoulli Failures

A general failure model where errors have random time span → A Markov model

Permanent link failures

Permanent failures are modeled by a function $F : E \rightarrow [0,1]$

$F(v_1, v_2)$ models the probability that the link (v_1,v_2) fails.

Decision problem: Given a permanent failure model, determine if

$$P_{stable} \geq \alpha$$

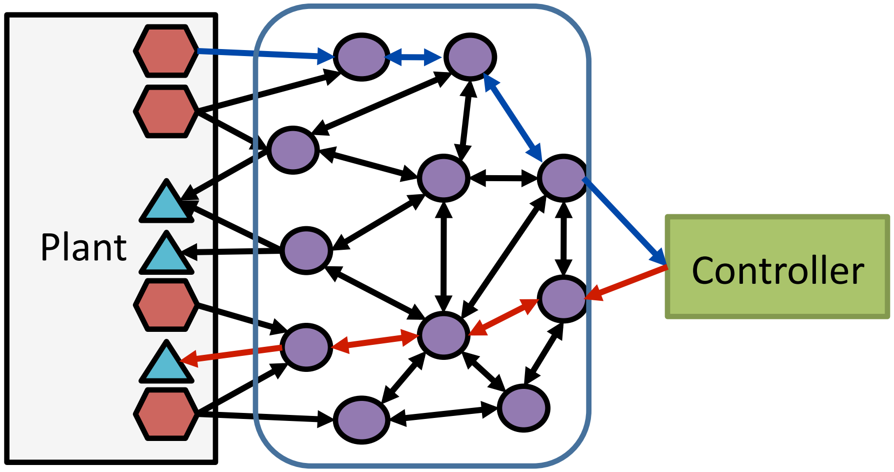
where P_{stable} - probability that the multi-hop control is stable.

Permanent failure decision problem is NP-hard (CDC 2009)

Works for small networks/control loops

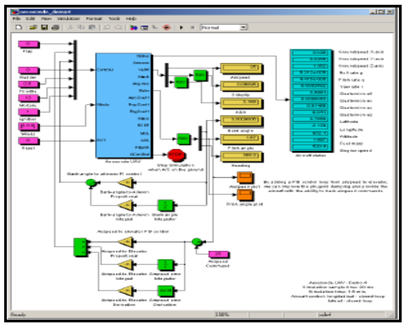
Control with multi-hop networks

- Control with multi-hop wireless networks



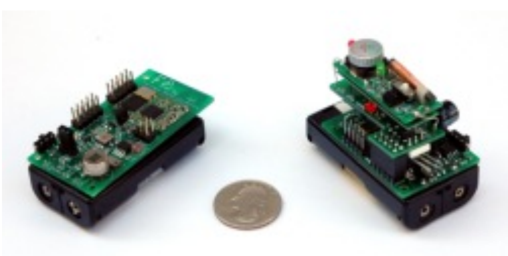
  - Formal modeling
  - Analysis & synthesis
  - **Compositional analysis**
  - Industrial case study

Interfaces for compositional control



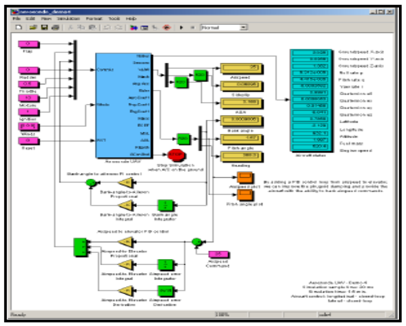
Control Design
Sampling frequency
Delays, jitter

Problems
Impact of scheduling on control
Composing schedules

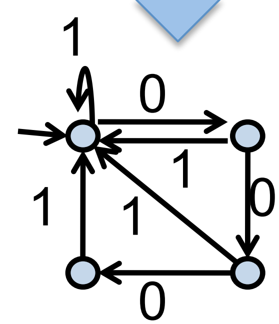


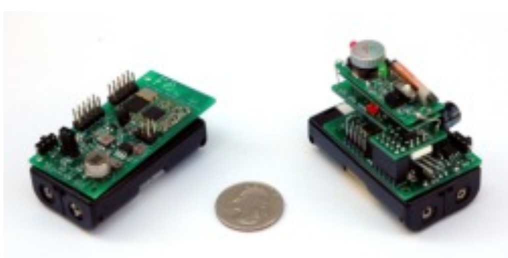
Scheduling
WCET
RM, EDF

Interfaces for compositional control*



<u>Control Design</u>
Control loop must get at least one slot in a superframe of 4 slots





<u>Scheduling</u>
Non-deterministic schedules for time-triggered platforms

*R. Alur and G. Weiss, *Automata-based interfaces for control and scheduling*, HSCC 2007

Control specifications as automata

- Stability Control Specifications

$$x(t+1) = T[\eta(t), \mu(t)]x(t)$$

→ Automata specifying schedules that guarantee stability

- Periodic Control Specifications on TT

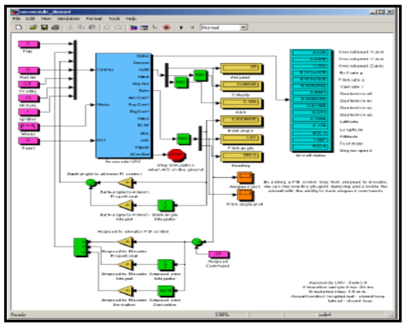
Sample every 100 seconds

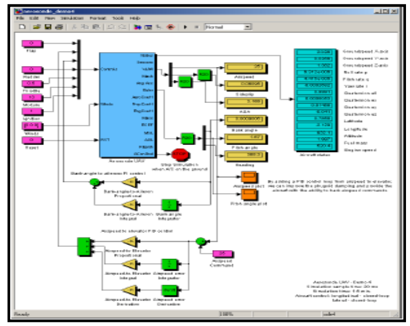
If not sampled in the last 200 seconds, sample every 10 seconds for the next minute

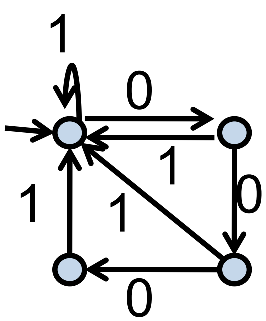
Specifications of maximal time delays between events

→ Automata that specify valid periodic schedules

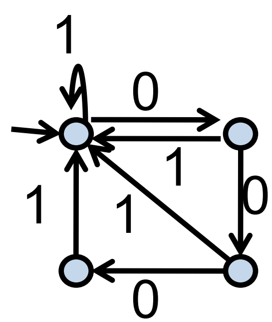
Automata are compositional



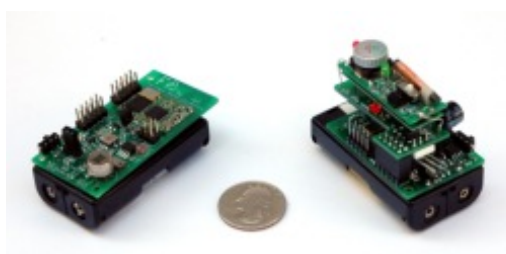




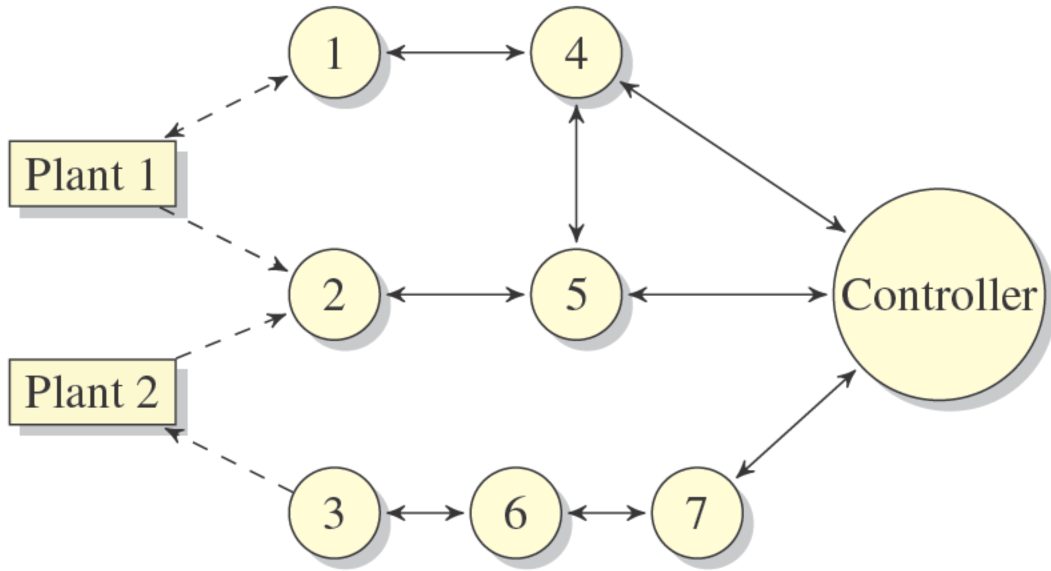
∩



= ?



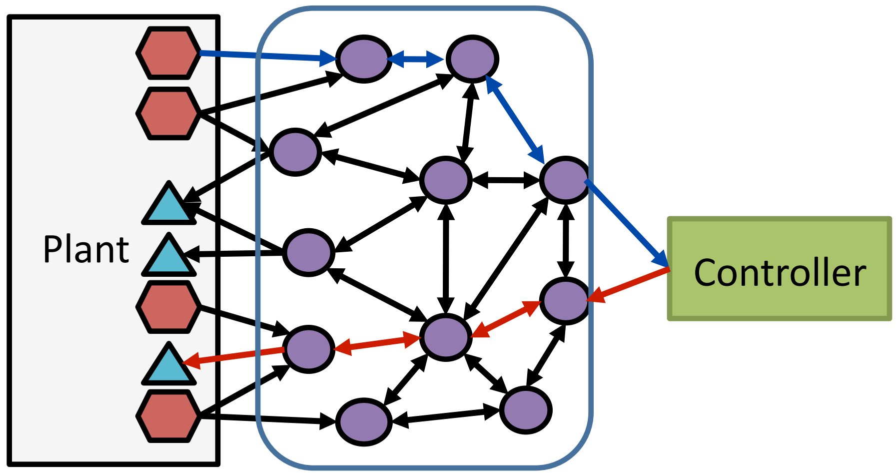
Compositional analysis for multi-hop networks



$$
\begin{aligned}
A_1 &= \text{SwitchedSystem}_1[\text{controlLoops}, \text{netTopology}, \text{routing}];\\
\text{lang}_1 &= \text{ExpStabLang}[A_1, 5, 1];\\
\\
A_2 &= \text{SwitchedSystem}_2[\text{controlLoops}, \text{netTopology}, \text{routing}];\\
\text{lang}_2 &= \text{ExpStabLang}[A_2, 5, 1];\\
\\
\text{inter} &= \text{LangIntersection}[\text{lang}_1, \text{lang}_2];\\
\text{schedule} &= \text{ExtractShortestPeriodicSchedule}[\text{inter}];
\end{aligned}
$$

Control with multi-hop networks

- Control with multi-hop wireless networks



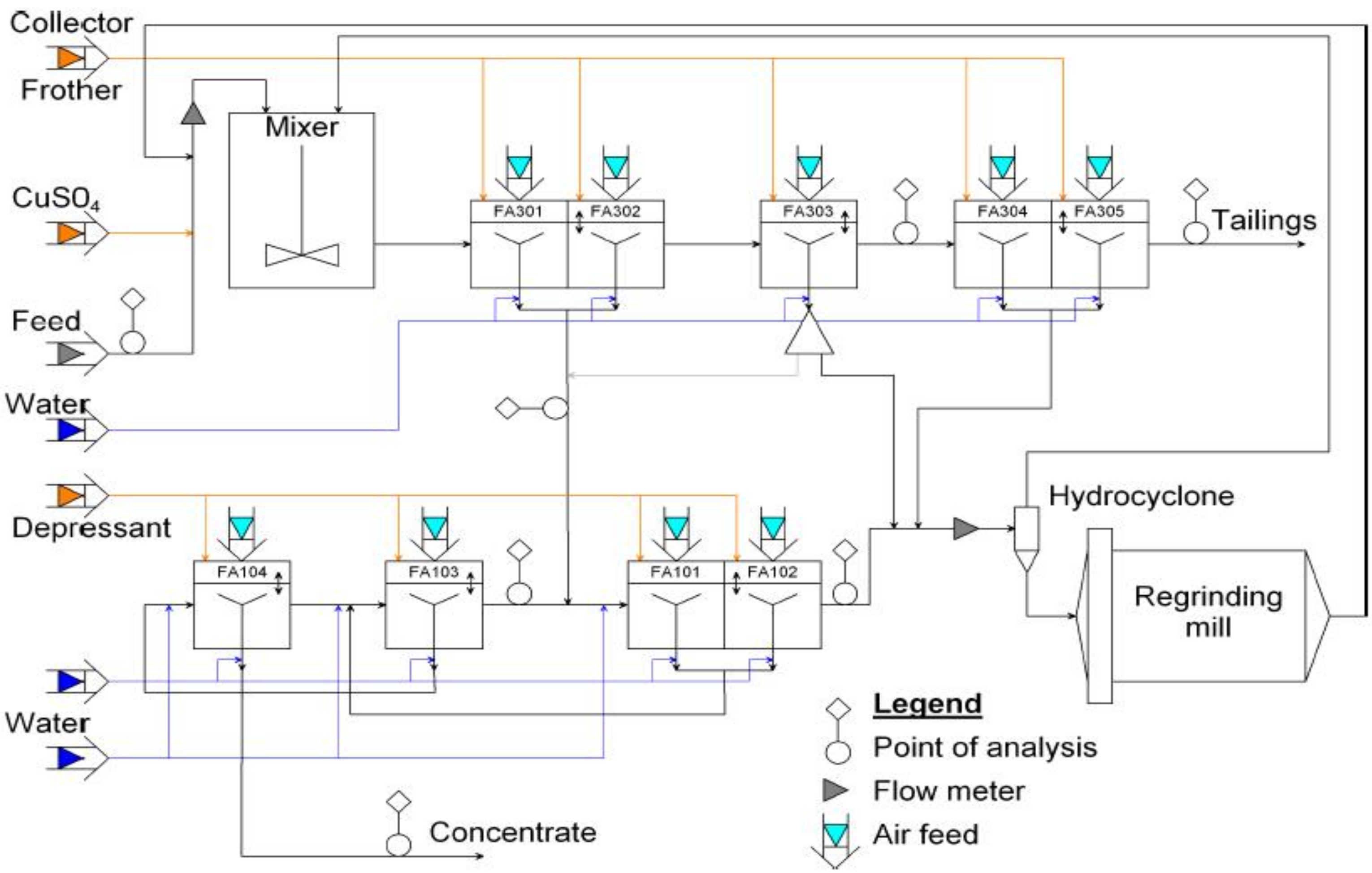
  - Formal modeling
  - Analysis & synthesis
  - Compositional analysis
  - **Industrial case study**

Mining Industry Case Study

Boliden mine in Garpenberg, Sweden

- Mining phases:
  - Drilling and blasting
  - Ore transportation
  - Ore concentration

Floatation bank control problem



H. Lindvall, "Flotation modelling at the Garpenberg concentrator using Modelica/Dymola,", 2007.

Process Time Scales: Zn Flotation

Loop category	# of loops in category	Loop name	Sampling interval (T_s)
Air flow	9	FA301_FC1	2
		FA302_FC1	2
		FA303_FC1	2
		FA304_FC1	2
		FA305_FC1	2
		FA101_FC1	2
		FA102_FC1	2
		FA103_FC1	2
		FA104_FC1	2
Level	6	FA302_LC1	2
		FA303_LC1	1
		FA305_LC1	8
		FA102_LC1	8
		FA103_LC1	8
		FA104_LC1	8

Loop category	# of loops in category	Loop name	Sampling interval (T_s)
Reagents	2	BL031_FC1	2
		FA300_FC2	1

- Each controlled variable represents a control loop
- Only the main control loops:
  - air flow, pulp level and reagent
- Each loop abstracted by a time constraint (the sampling interval)
  - specifies the maximum delay between sensing and actuation
- The sampling interval used as a constraint for defining the set of “good” schedules

Wireless network topology

Using SMV to compose schedules

```
MODULE loop2(bus)
VAR
    cnt:0..6;
ASSIGN
    init(cnt):=0;
    next(cnt):=case
bus=e2to5 & cnt=0 : 1;
bus=e5toc & cnt=1 : 2;
bus=bus & cnt=2 : 3;
bus=ecto7 & cnt=3 : 4;
bus=e7to6 & cnt=4 : 5;
bus=e6to3 & cnt=5 : 6;
1:cnt;
    esac;
DEFINE
    done := cnt=6;
```

progress counters

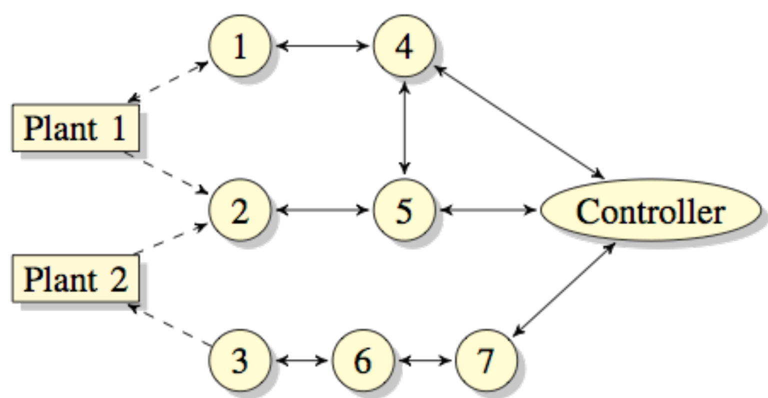
Req. For Plant 2: e2to5, e5toC, …,e6to3 must be a subsequence of the schedule

```
MODULE loop1(bus)
VAR
    in1:0..2;
    in2:0..2;
    out1:0..3;
ASSIGN
    init(in1):=0;
    init(in2):=0;
    init(out1):=0;
    next(in1):=case
bus=e1to4 & in1=0 : 1;
bus=e4toc & in1=1 : 2;
1:in1;
    esac;
    next(in2):=case
bus=e2to5 & in2=0 : 1;
bus=e5toc & in2=1 : 2;
1:in2;
    esac;
    next(out1):=case
bus=bus & allin & out1= 0 :1;
bus=ecto4 & allin & out1= 1 : 2;
bus=e4to1 & allin & out1= 2 : 3;
1 : out1;
    esac;
DEFINE
    allin := in1=2 & in2=2;
    done := out1=3;
```

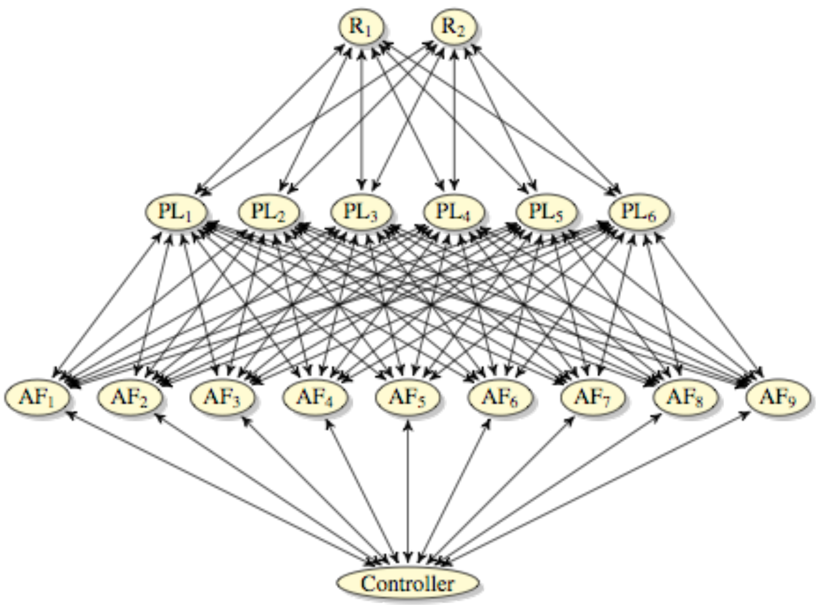
Req. For Plant 1: more involved because it has two inputs

```
MODULE main
VAR
    bus:{e1to4, e2to5, e4to1, e4toc, e5toc, e6to3, e7to6, ecto4, ecto7, idle};
    l1:loop1(bus);
    l2:loop2(bus);
SPEC
    AG !(l1.done & l2.done);
```

We are looking for a schedule that satisfies both requirements which comes as a counter-example to the claim that there is no such schedule



Case study results



17 single-input-single-output loops
Timing constraints
At most one message in a time slot

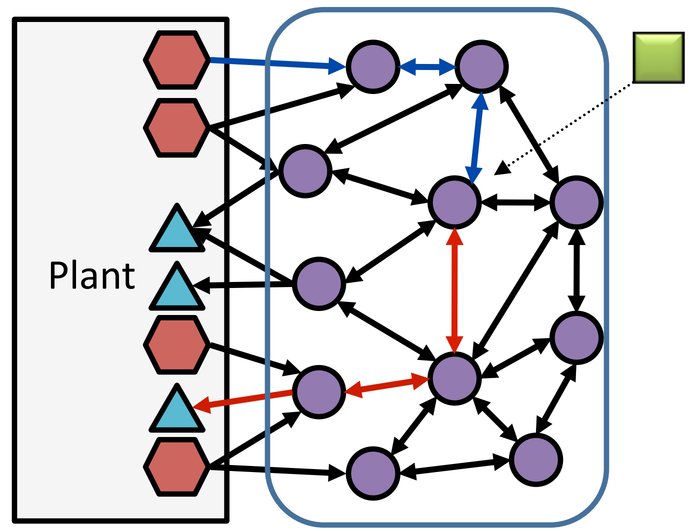
SMV code with 18 modules
272 lines
BDD nodes allocated: 26797

~2 minutes

Shortest schedule that satisfy the constraints posed by all 17 loops
37 time slots

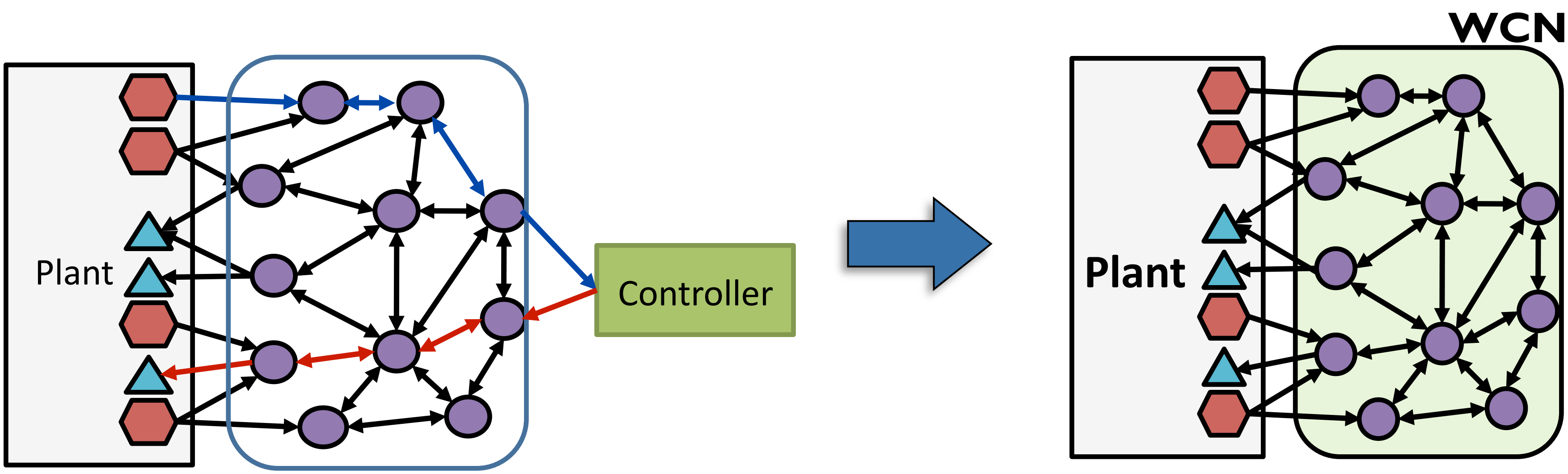
Future challenges

- Time-triggered architectures not optimal for event-based systems
  - Hybrid TDMA/CSMA or LTTA architectures
  - Event-based sensing and control
- Time-synchronization for large networks
  - Model TDMA clock drift using timed automata
  - Scheduling by composing timed-automata
- Wireless models are not precise
  - On-line adaptation of packet drop probability
  - Robust/adaptive control
- Control over virtual network computation
  - Runtime control reconfiguration in presence of node failures
  - Embedded virtual machines for control (Pajic, Mangharam)



The Wireless Control Network (WCN)

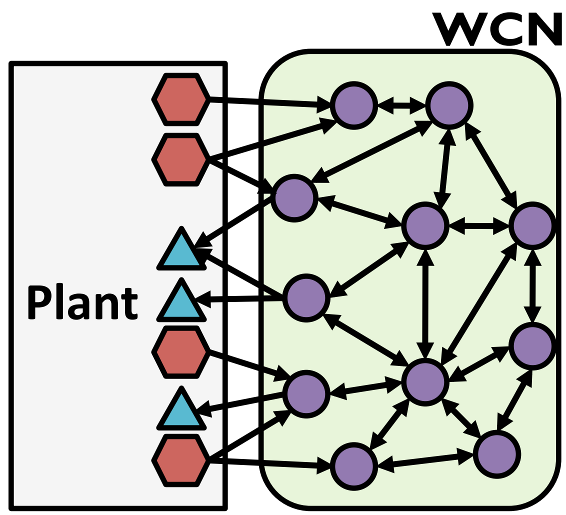
- In multi-hop control, nodes route information to controller



- Can we leverage computation of the network?
- Can we distribute the controller to nodes of the network?
- Reminiscent of network coding

Wireless control network

- Wireless control network*

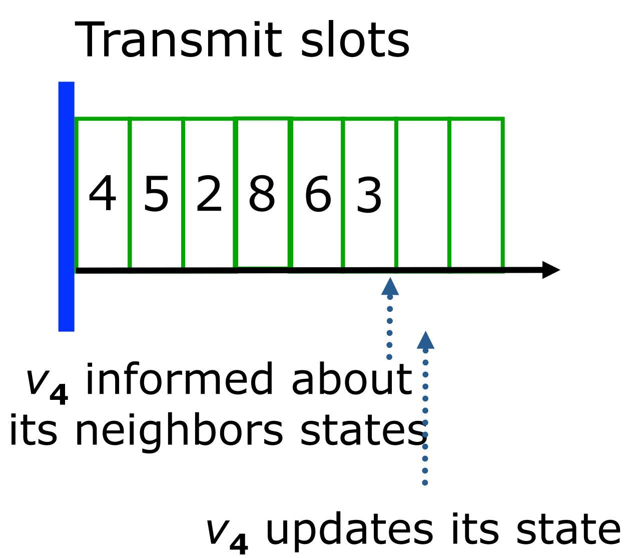


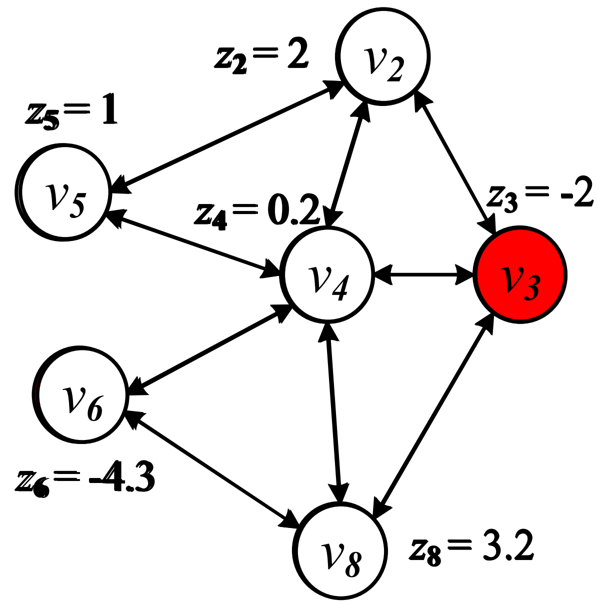
  - **Modeling**
  - Controller synthesis
  - Robustness & security

*M. Pajic, S. Sundharam, G. Pappas, R. Mangharam, *Wireless control network: a new paradigm for network control*, IEEE Transactions on Automatic Control, to appear

Distributed control over time-triggered network

- Each node maintains its (possible vector) state
  - Transmits state exactly once in each step (per frame)
  - Updates own state using linear iterative strategy
- Example:





WCN modeling

- Discrete-time plant

$$\mathbf{x}[k+1] = \mathbf{A}\mathbf{x}[k] + \mathbf{B}\mathbf{u}[k]$$
$$\mathbf{y}[k] = \mathbf{C}\mathbf{x}[k]$$

- Node state update procedure:

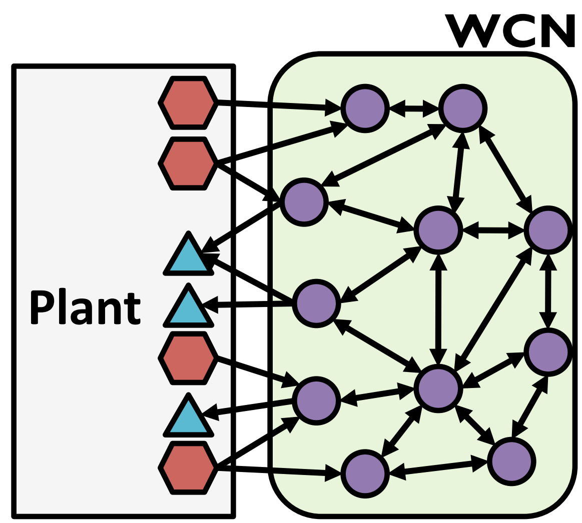
$$z_i[k+1] = w_{ii} z_i[k] + \sum_{v_j \in \mathcal{N}_{v_i}} w_{ij} z_j[k] + \sum_{s_j \in \mathcal{N}_{v_i}} h_{ij} y_j[k]$$

From neighbors **From sensors**

- Actuator update procedure:

$$u_i[k] = \sum_{j \in \mathcal{N}_{a_i}} g_{ij} z_j[k]$$

From actuator's neighbors

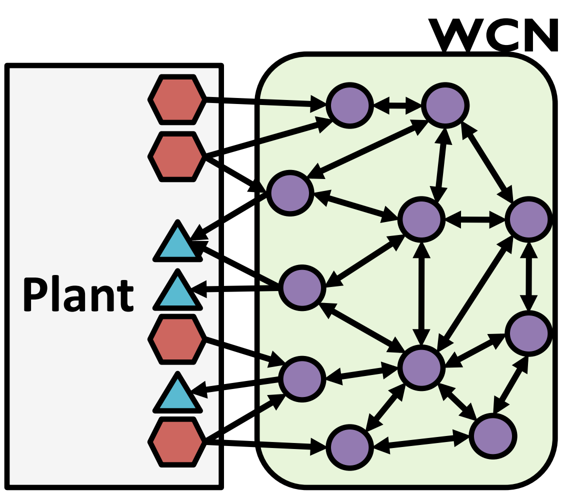


WCN modeling

- Network acts as a linear dynamical compensator

$$\mathbf{z}[k+1] = \underbrace{\begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1N} \\ w_{21} & w_{22} & \cdots & w_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ w_{N1} & w_{N2} & \cdots & w_{NN} \end{bmatrix}}_{\mathbf{W}} \mathbf{z}[k] + \underbrace{\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1p} \\ h_{21} & h_{22} & \cdots & h_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N1} & h_{N2} & \cdots & h_{Np} \end{bmatrix}}_{\mathbf{H}} \mathbf{y}[k]$$

$$\mathbf{u}[k] = \underbrace{\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1N} \\ g_{21} & g_{22} & \cdots & g_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ g_{m1} & g_{m2} & \cdots & g_{mN} \end{bmatrix}}_{\mathbf{G}} \mathbf{z}[k]$$



Structural constraints: Only elements corresponding to existing links (link weights) are allowed to be non-zero

WCN modeling: Closing the loop

- Overall system state:

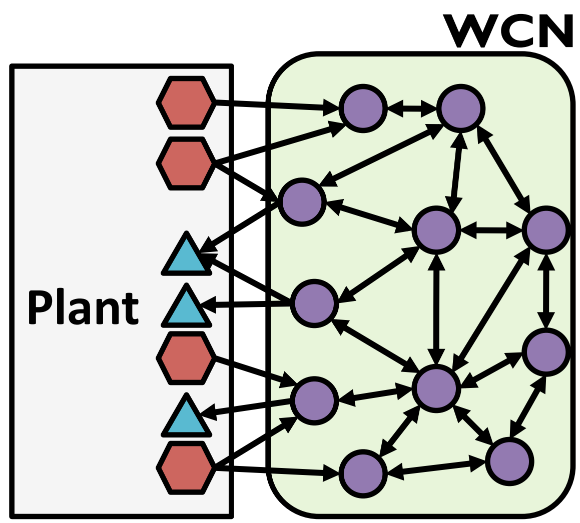
$$\hat{\mathbf{x}}[k] = \begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix} \begin{matrix} \leftarrow \text{plant} \\ \leftarrow \text{network} \end{matrix}$$

- Closed-loop system:

$$\hat{\mathbf{x}}[k+1] = \begin{bmatrix} \mathbf{x}[k+1] \\ \mathbf{z}[k+1] \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{A} & \mathbf{BG} \\ \mathbf{HC} & \mathbf{W} \end{bmatrix}}_{\hat{\mathbf{A}}} \begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix} = \hat{\mathbf{A}}\hat{\mathbf{x}}[k]$$

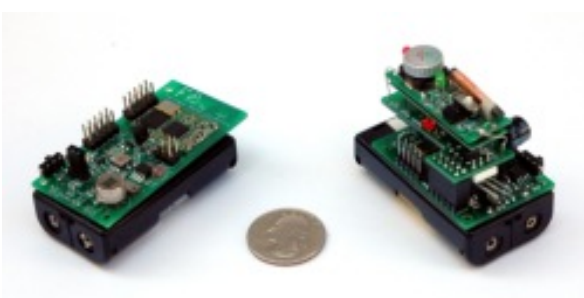
- Matrices W, G, H are structured

- Sparsity constraints imposed by topology



WCN Advantages: Simple & Powerful

- Low overheard
  - Each node only calculates linear combination of its states and state of its neighbors
  - Suitable even for resource constrained nodes
  - Easily incorporated into existing wireless networks (e.g., systems based on the ISA100.11a or wirelessHART)
  - Backup mechanism in ‘traditional’ networked control systems; used for graceful degradation

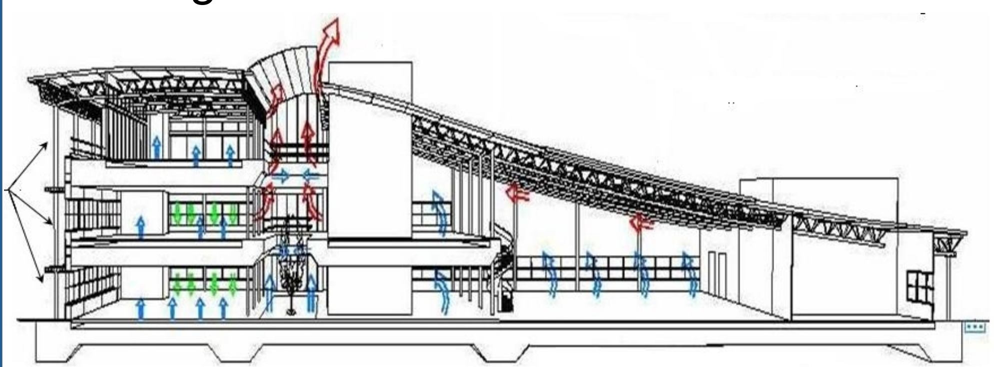


WCN Advantages: Scheduling

- Simple scheduling
  - Each node needs to transmit only once per frame
  - Static (conflict-free) schedule
- No routing!
- Multiple sensing/actuation points
  - Geographically distributed sensors/actuators

Process control

Building automation



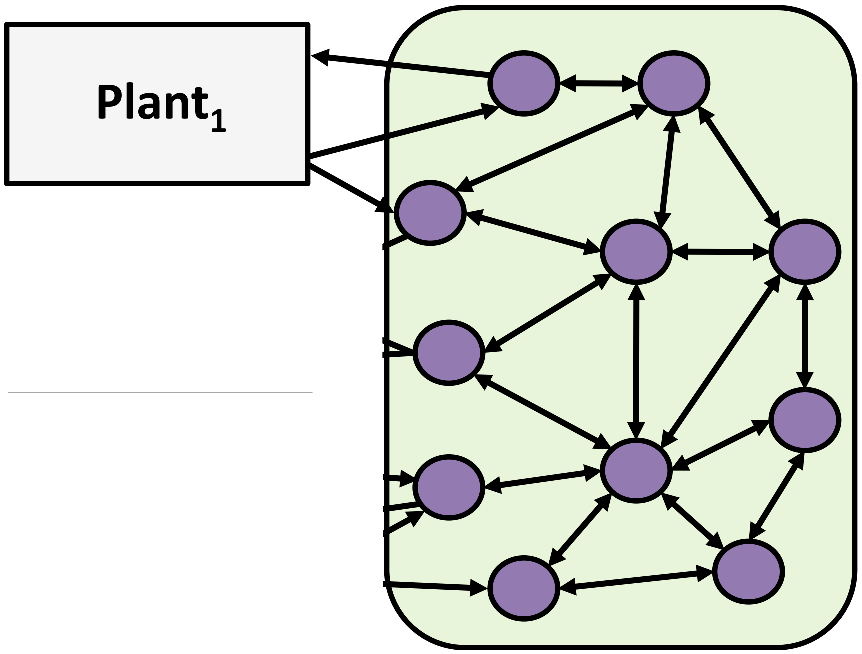
WCN Advantages: Compositionality

- Adding new control loops is easy!
  - Does not require any communication schedule recalculation

- Stable configurations can be combined

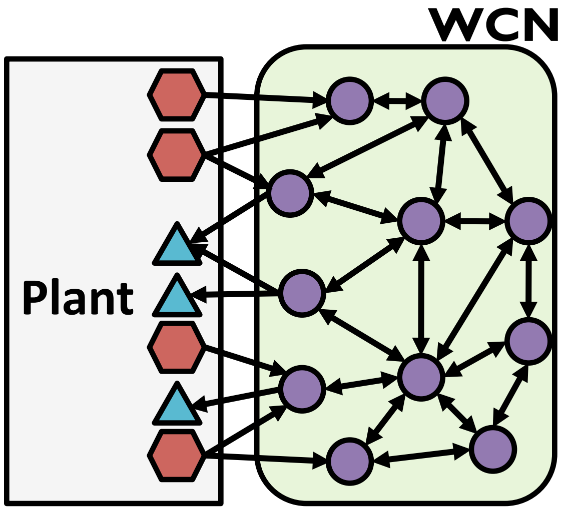
Stable configuration

$$(\mathbf{W}_1, \mathbf{H}_1, \mathbf{G}_1) \in \Psi$$



Wireless control network

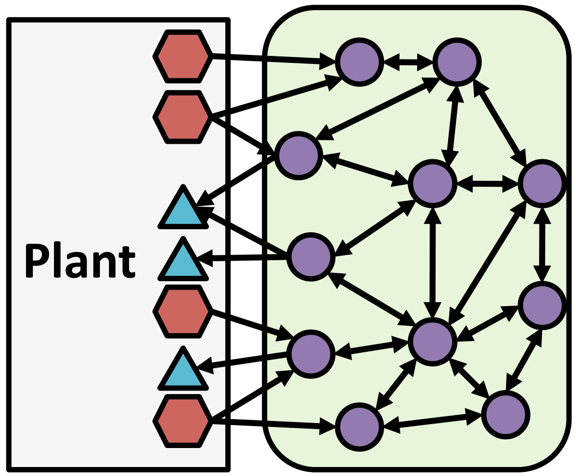
- Wireless control network



  - Modeling
  - **Controller synthesis**
  - Robustness & security

WCN controller synthesis

- Use WCN to stabilize the closed-loop system



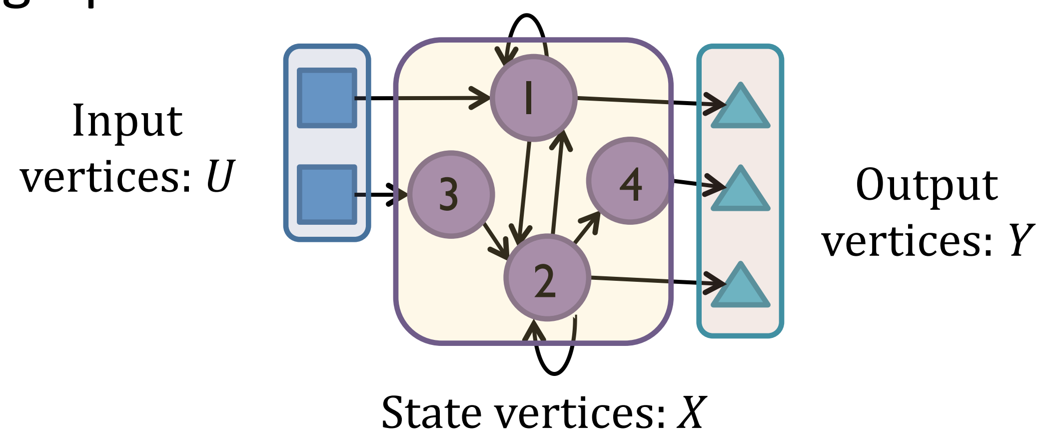
- Does the plant influence the WCN network topology?
  - How many nodes? How to interconnect them?
- Given network topology, design distributed controller
  - Extracting a stabilizing closed loop configuration

WCN topological conditions

- Structured system theory: Systems represented as graphs
- Linear system

$$x[k+1] = \begin{bmatrix} \lambda_1 & \lambda_2 & 0 & 0 \\ \lambda_3 & \lambda_4 & \lambda_5 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & \lambda_6 & 0 & 0 \end{bmatrix} x[k] + \begin{bmatrix} \lambda_7 & 0 \\ 0 & 0 \\ 0 & \lambda_8 \\ 0 & 0 \end{bmatrix} u[k], \qquad y[k] = \begin{bmatrix} \lambda_9 & 0 & 0 & 0 \\ 0 & \lambda_{10} & 0 & 0 \\ 0 & 0 & 0 & \lambda_{11} \end{bmatrix} x[k]$$

- Associated graph H



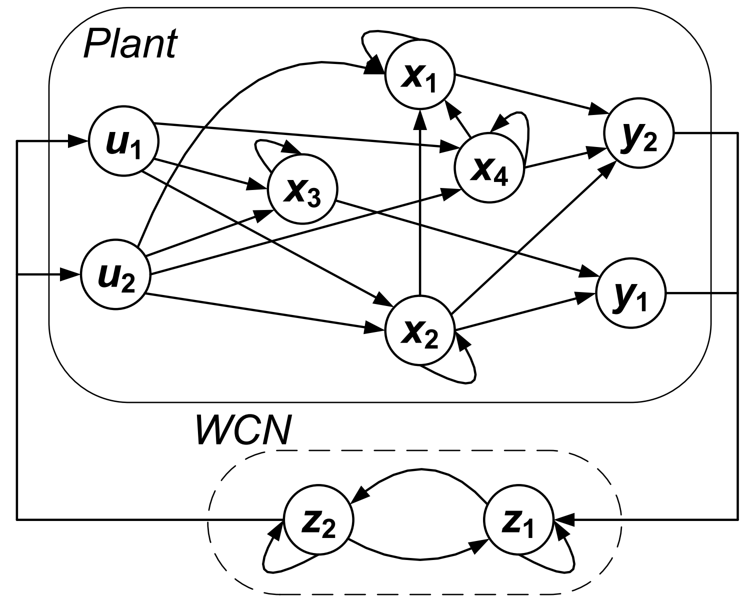
- Properties of graph are generic properties of structured system

WCN topological conditions

- Use structured system theory on WCN and network

$$x[k+1] = \begin{bmatrix} 2 & 0 & 1 & -3 \\ 0 & 2 & 10 & -4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} x[k] + \begin{bmatrix} 0 & 1 \\ 1 & 1.6 \\ -0.5 & 4 \\ 2 & 5 \end{bmatrix} u[k]$$

$$y[k] = \begin{bmatrix} 1 & 0.3 & 2 & 0 \\ 0 & 0.1 & 0 & 1 \end{bmatrix} x[k]$$



- Can we stabilize the plant with 2 nodes?

Topological Conditions for WCN

- Consider a numerically specified system
- Example: A system with integrators

$$A = \begin{bmatrix} 2 & 0 & 1 & -3 \\ 0 & 2 & 10 & -4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$$

Eigenvalues are 2,2,2,3

Λ=2 has geometric multiplicity d=2 (≥ 1)

Network condition: Let d denote the largest geometric multiplicity of any unstable eigenvalue of the plant. If

1) connectivity of the network is at least *d*, and

2) each actuator has at least *d* nodes in neighborhood

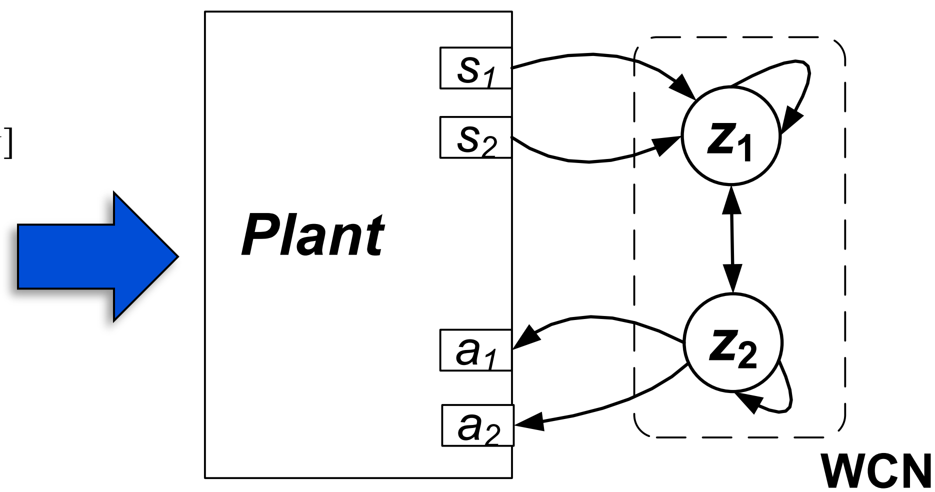
then there exists a stabilizing configuration for WCN

WCN topological conditions

- Use structured system theory on WCN and network

$$x[k+1] = \begin{bmatrix} 2 & 0 & 1 & -3 \\ 0 & 2 & 10 & -4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix} x[k] + \begin{bmatrix} 0 & 1 \\ 1 & 1.6 \\ -0.5 & 4 \\ 2 & 5 \end{bmatrix} u[k]$$

$$y[k] = \begin{bmatrix} 1 & 0.3 & 2 & 0 \\ 0 & 0.1 & 0 & 1 \end{bmatrix} x[k]$$



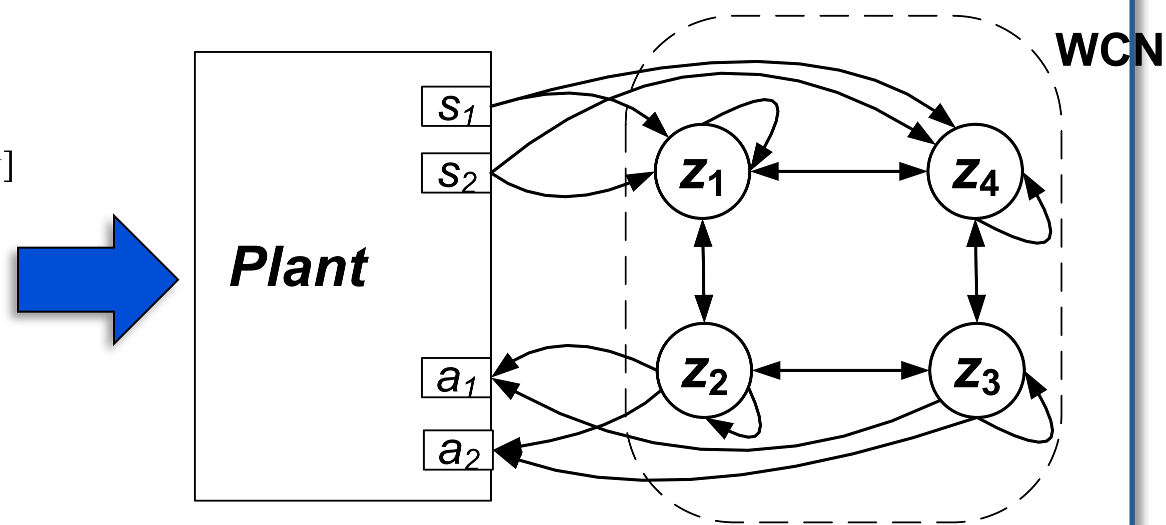
- We **cannot** stabilize with with 2 nodes!

WCN topological conditions

- Use structured system theory on WCN and network

$$x[k+1]=\begin{bmatrix}2 & 0 & 1 & -3\\ 0 & 2 & 10 & -4\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 3\end{bmatrix}x[k]+\begin{bmatrix}0 & 1\\ 1 & 1.6\\ -0.5 & 4\\ 2 & 5\end{bmatrix}u[k]$$

$$y[k]=\begin{bmatrix}1 & 0.3 & 2 & 0\\ 0 & 0.1 & 0 & 1\end{bmatrix}x[k]$$



- We **cannot** stabilize with with 2 nodes!
- But we can stabilize plant with 4 nodes

WCN topological conditions

- Is fully connected network sufficient?

Sufficient condition: If

1) Geometric multiplicity is 1 for all unstable eigenvalues,

2) System is controllable and and observable,

then it can be stabilized with a strongly connected network, where each sensor and actuator is connected to the network.

Stabilizing the closed-loop system

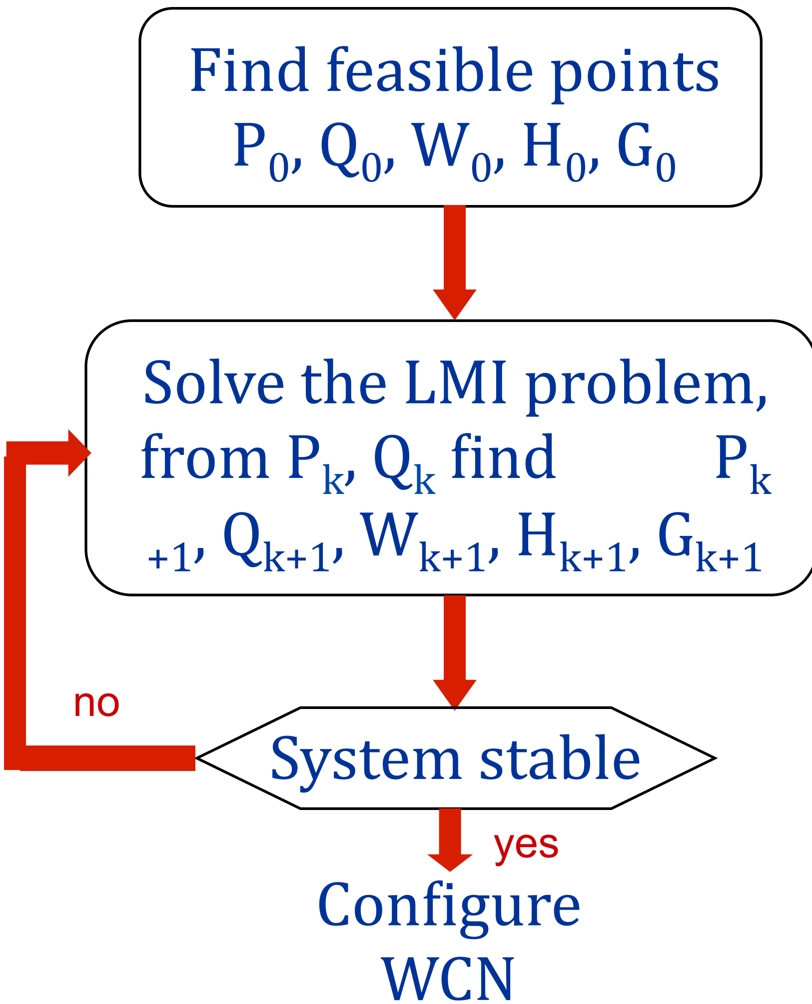
- Controller synthesis problem: Find numerical matrices W, H, G satisfying structural constraints such that

$$\hat{\mathbf{A}} = \begin{bmatrix} \mathbf{A} & \mathbf{BG} \\ \mathbf{HC} & \mathbf{W} \end{bmatrix} \quad \text{is stable}$$

- Topological conditions ensure existence of W, H, G matrices
- Standard approach: Find P>0 such that $\mathbf{P} - \hat{\mathbf{A}}^T \mathbf{P} \hat{\mathbf{A}} > 0$
  - Bilinear matrix inequality (free variables in multiply free variables in P)
  - Not a problem when W, H and G are unstructured => change of variables produces standard LMI

Convex relaxation for controller synthesis

Penn University of Pennsylvania



Function Linearization

$$\min tr(\mathbf{P}_k\mathbf{Q}_{k+1} + \mathbf{Q}_k\mathbf{P}_{k+1})$$

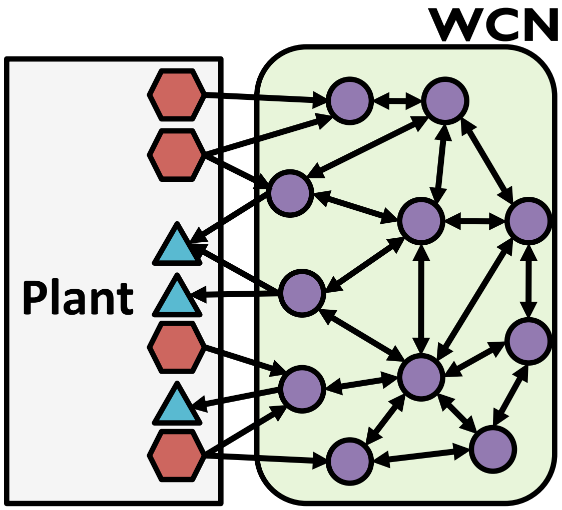
$$\begin{bmatrix} \mathbf{P}_{k+1} & \hat{\mathbf{A}}_{k+1}^T \\ \hat{\mathbf{A}}_{k+1} & \mathbf{Q}_{k+1} \end{bmatrix} > 0, \quad \begin{bmatrix} \mathbf{P}_{k+1} & \mathbf{I} \\ \mathbf{I} & \mathbf{Q}_{k+1} \end{bmatrix} \geq 0,$$

$$\hat{\mathbf{A}}_{k+1} = \begin{bmatrix} \mathbf{A} & \mathbf{BG}_{k+1} \\ \mathbf{H}_{k+1}\mathbf{C} & \mathbf{W}_{k+1} \end{bmatrix},$$

$$(\mathbf{W}_{k+1}, \mathbf{H}_{k+1}, \mathbf{G}_{k+1}) \in \Psi, \quad \mathbf{P}_{k+1} > 0, \quad \mathbf{Q}_{k+1} > 0$$

Wireless control network

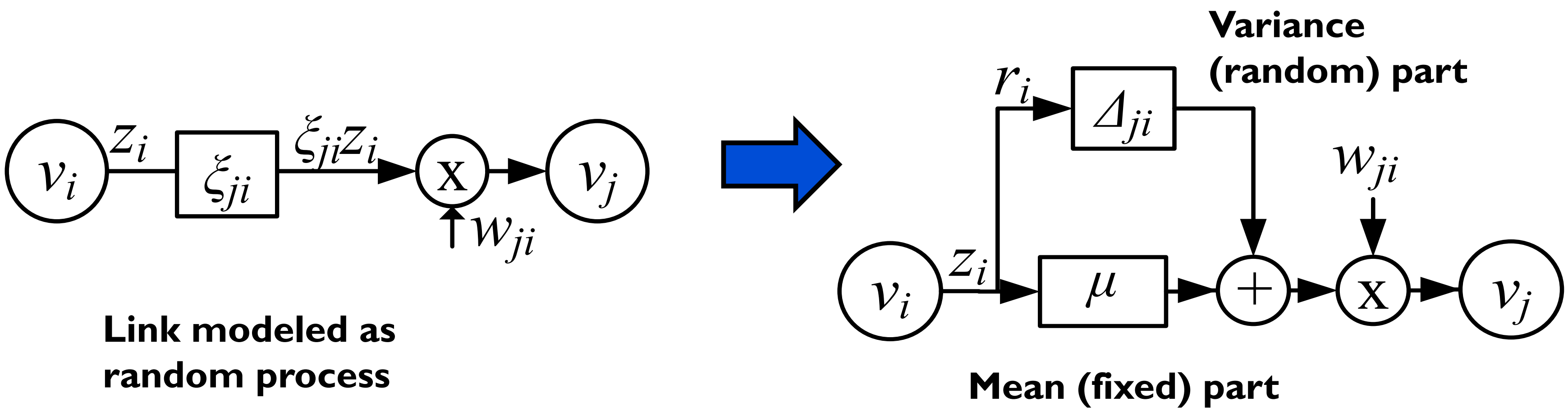
- Wireless control network



  - Modeling
  - Controller synthesis
  - **Robustness & security**

WCN robustness to link failures

- What happens if links in the network fail?
  - Bernoulli distribution: fails with some probability
- Many links in network: how to model concisely?
  - Use robust control [Elia, Sys & Control Letters, '05]



  - Received value: $\xi_{ji}[k]zi[k] = (\mu + \Delta_{ji}[k])zi[k]$

random variable

mean (constant)

zero-mean random variable

WCN robustness to link failures

- Closed loop system with random Bernoulli failures

$$\hat{\mathbf{x}}[k+1] = \begin{bmatrix} \mathbf{A} & \mathbf{B}\mathbf{G}_{\mu} \\ \mathbf{H}_{\mu}\mathbf{C} & \mathbf{W}_{\mu} \end{bmatrix} \hat{\mathbf{x}}[k] + \mathbf{J}\Delta[k]\mathbf{r}[k]$$

System is mean square stable if and only if there exists X, $\alpha_1, \alpha_2, \ldots, \alpha_N$ such that

$$\mathbf{X} \succ \hat{\mathbf{A}}_{\mu}\mathbf{X}\hat{\mathbf{A}}_{\mu}^{T} + \mathbf{J}\mathrm{diag}\{\alpha\}(\mathbf{J})^{T}$$

$$\alpha_i \geq \sigma_i^2 (\hat{\mathbf{J}}^{or})_i \mathbf{X} (\hat{\mathbf{J}}^{or})_i^T, \ \forall i \in \{1, \ldots, N_l\}$$

- Robustness requires
  - One additional constraint added for each link (Bernoulli failures)
  - More constraints for more general failure models

Monitoring for faulty and malicious behavior

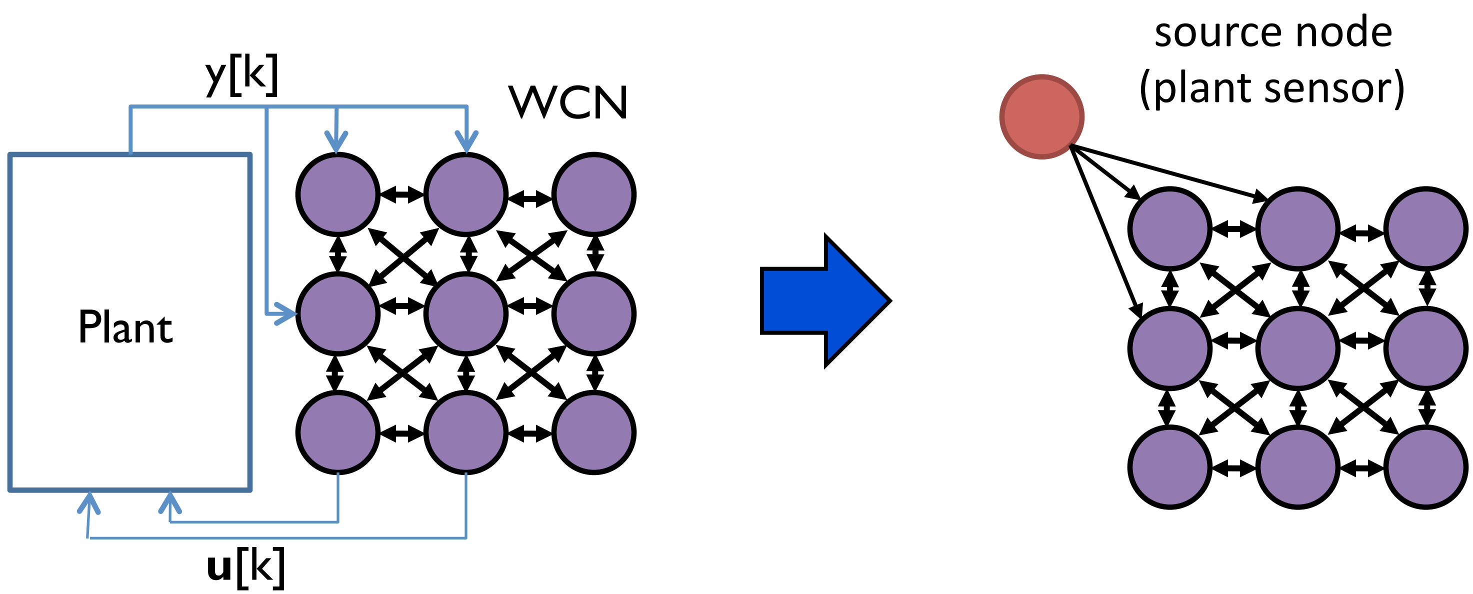
- What if certain nodes in the WCN become faulty or malicious?

- Security of control networks in industrial control systems is a major issue [NIST Technical Report, 2008]
  - Data Historian: Maintain and analyze logs of plant and network behavior
  - Intrusion Detection System: Detect and identify any abnormal activities

- Is it possible to design an Intrusion Detection System to determine if any nodes are not following WCN protocol?
- Can IDS scheme avoid listening all nodes? Under what conditions? Which nodes?

IDS for wireless control network

- Consider graph of wireless control network with plant sensors



- Denote transmissions of any set T of monitored nodes by

$$\mathbf{t}[k] = \mathbf{T}\mathbf{z}[k]$$

  - T is a matrix with a single 1 in each row, indicating which nodes z[k] are being monitored

Modeling with malicious nodes

- WCN model with set S of faulty/malicious nodes:

$$\mathbf{z}[k+1] = \mathbf{W}\mathbf{z}[k] + \mathbf{H}\mathbf{y}[k] + \mathbf{B}_S\mathbf{f}_S[k]$$
$$\mathbf{t}[k] = \mathbf{T}\mathbf{z}[k]$$

- Objective: Recover y[k], f_s[k] and S (initial state z[0] known)
  - Almost equivalent to invertibility of system
- Problem: Don't know the set of faulty nodes S
  - Assumption: At most b faulty/malicious nodes
- Approach: Must ensure that output sequence cannot be generated by a different y[k] and possibly different set of b malicious nodes

Conditions for IDS Design

IDS can recover **y**[k] and identify up to *b* faulty nodes in the network by monitoring transmissions of set T

⟺

Can recover inputs and set S in system

$$\mathbf{z}[k+1] = \mathbf{W}\mathbf{z}[k] + \begin{bmatrix} \mathbf{H} & \mathbf{B}_S \end{bmatrix} \begin{bmatrix} \mathbf{y}[k] \\ \mathbf{f}_S[k] \end{bmatrix}$$

$$\mathbf{t}[k] = \mathbf{T}\mathbf{z}[k]$$

for **any unknown set** S of **b** nodes

⇕

Linear system

$$\mathbf{z}[k+1] = \mathbf{W}\mathbf{z}[k] + \begin{bmatrix} \mathbf{H} & \mathbf{B}_Q \end{bmatrix} \begin{bmatrix} \mathbf{y}[k] \\ \mathbf{f}_Q[k] \end{bmatrix}$$

$$\mathbf{t}[k] = \mathbf{T}\mathbf{z}[k]$$

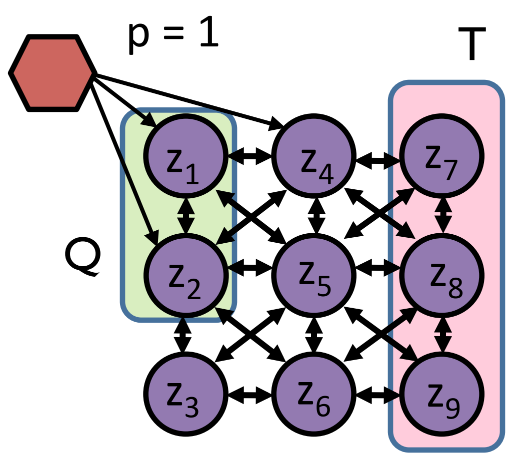
is invertible for
any known set Q of **2b** nodes

(generically) ⟺

There are p+2b node-disjoint paths from sensors and any set Q of 2b nodes to monitoring set T

IDS Example

- Suppose we want to identify b = 1 faulty/malicious node and recover the plant outputs in this setting:



- Consider set Q = $\{v_1, v_2\}$
  - p+2b vertex disjoint paths from sensor and Q to T
- Can verify that this holds for any set Q of 2b nodes
- Sufficient condition: Network is p+2b connected

WCN demo: Distillation column process control

- Distillation column control
  - Plant model contains 8 states, 4 inputs, 4 outputs
- WCN contains 4 nodes

Stable configuration:

node→node

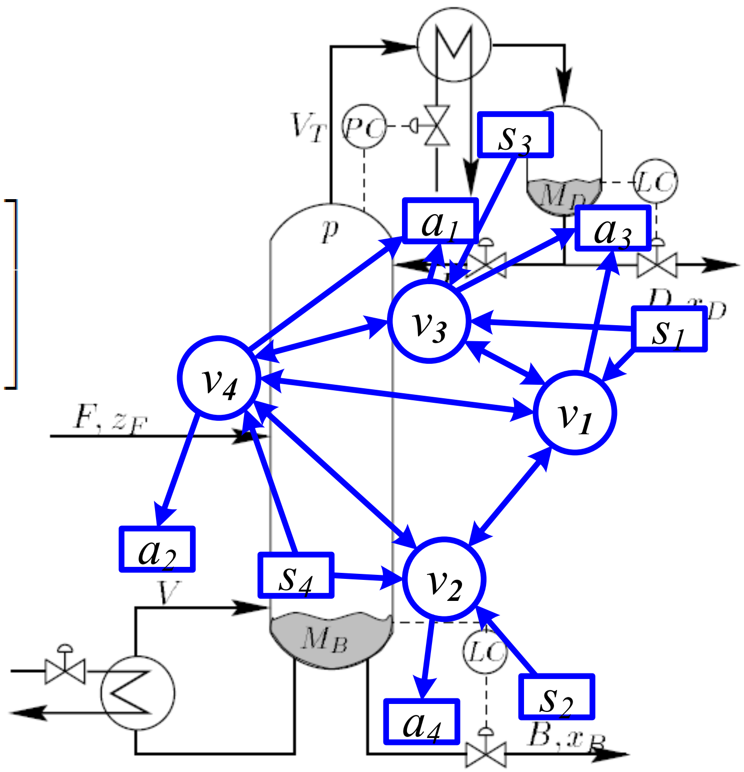
$$\mathbf{W} = \begin{bmatrix} -0.470 & 0.339 & -0.260 & -0.390 \\ -1.117 & -0.145 & 0 & -0.269 \\ 0.0514 & 0 & -0.703 & 0.600 \\ 0.854 & 0.277 & -0.086 & -0.112 \end{bmatrix}$$

sensor→node

$$\mathbf{H} = \begin{bmatrix} 1.260 & 0 & 0 & 0 \\ 0 & 0.104 & 0 & 0.075 \\ 0 & 0 & 0.421 & 0 \\ 0 & 0 & 0 & -0.034 \end{bmatrix}$$

node→actuator

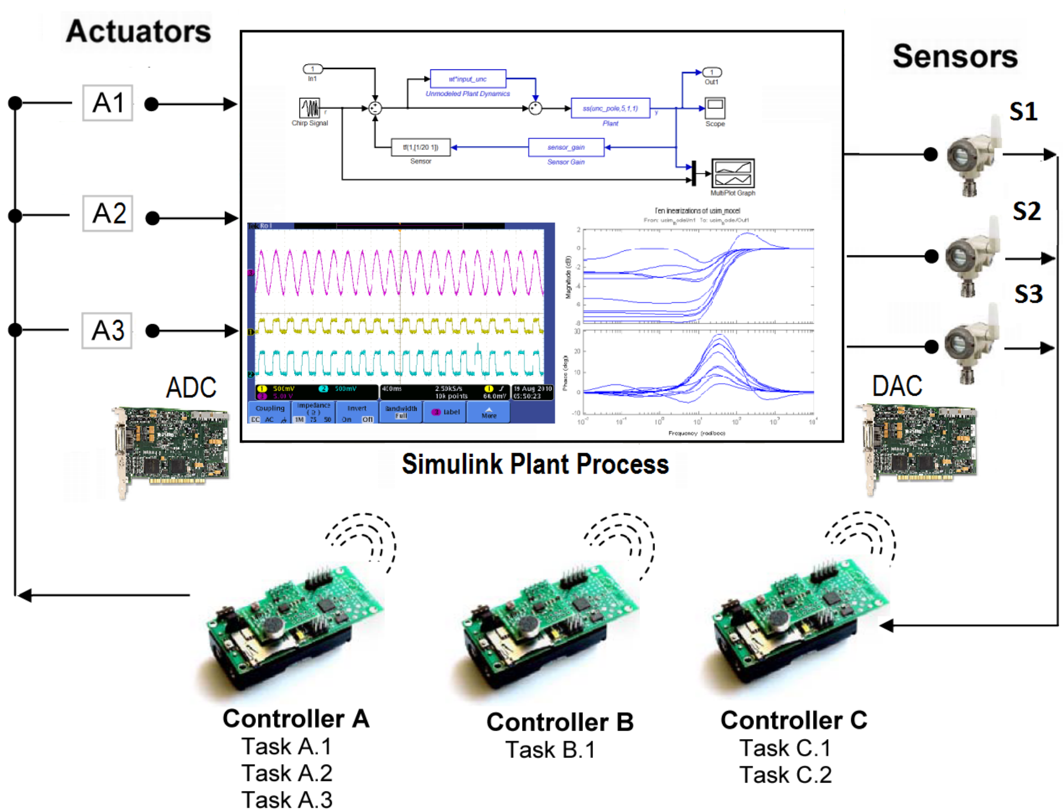
$$\mathbf{G} = \begin{bmatrix} 0 & 0 & -0.226 & -0.459 \\ 0 & 0 & 0 & 0.102 \\ 0.120 & 0 & 1.072 & 0 \\ 0 & 2.549 & 0 & 0 \end{bmatrix}$$



System configuration
Network topology

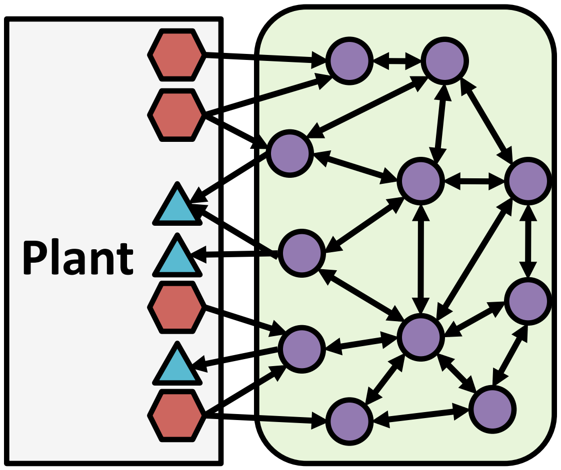
WCN demo: Distillation column process control

- IPSN 2011 Demo
- Process-in-the-loop test-bed



Future WCN challenges

- Mapping legacy PID control to WCN architecture
  - Realization theory with sparsity constraints
- Self organizing nodes for plant stabilization
  - Runtime control adaptation



- Topology control for control performance
  - Beyond stability
- Tradeoffs between control performance
  - Runtime reconfiguration in presence of node failures or attacks

Many thanks for your attention!

Penn
UNIVERSITY of PENNSYLVANIA

NSF

MuSyC

KTH
VETENSKAP
OCH KONST

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

ABB

Honeywell

University of Waterloo

RENOVABITUR UT AQUILAE JUVENTUS TUA
JUS LITTERAE SCIENTIAE