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

N
ti

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

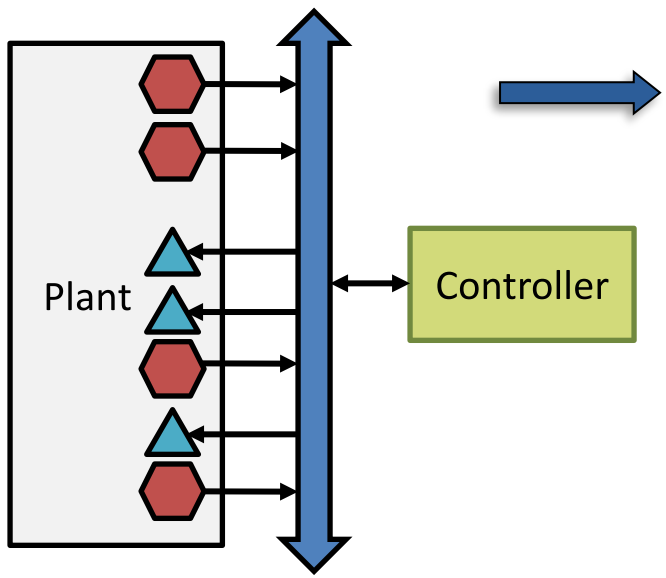
RENOVABITUR UT AQUILAE JUVENTUS TUA
IUS LITTERAE SCIENTIAE

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

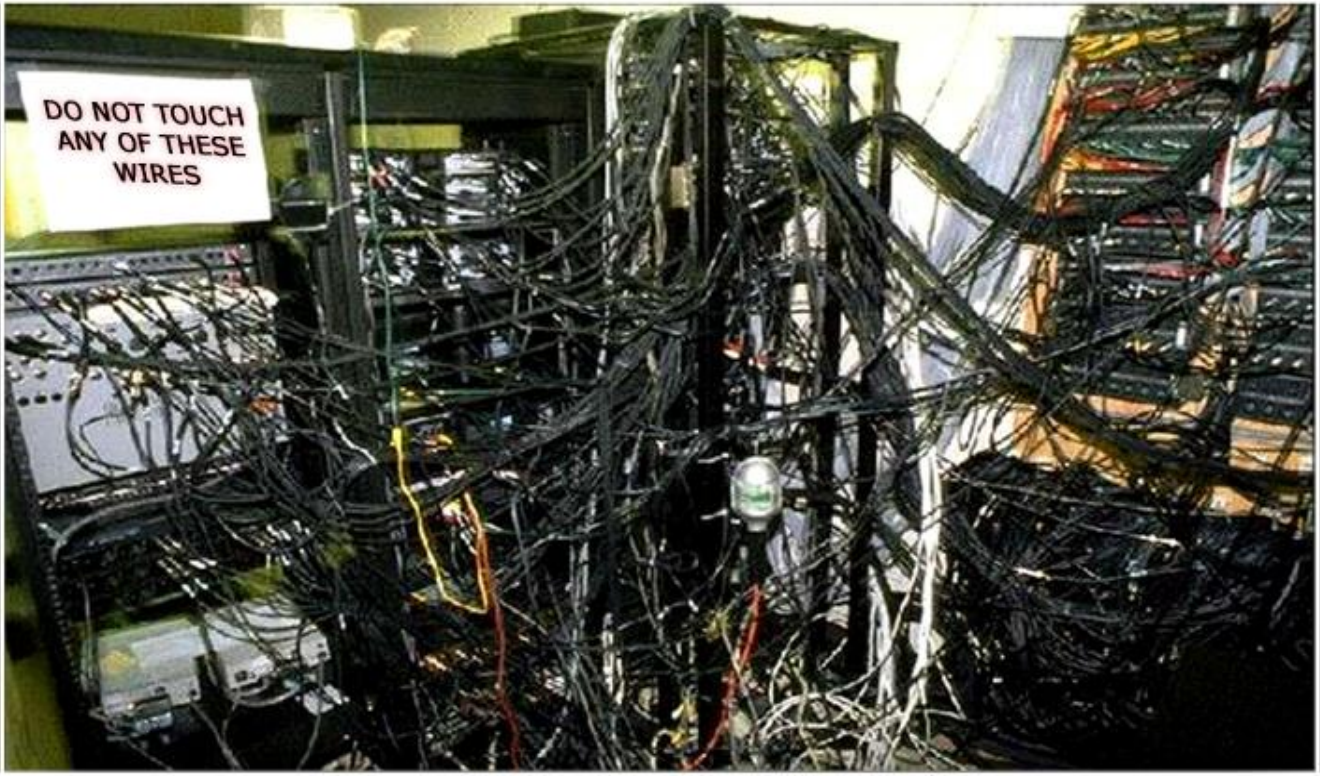
Wired Control Architecture



- CAN (TTCAN)
- UART
- FlexRay
- TT Ethernet
- …

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

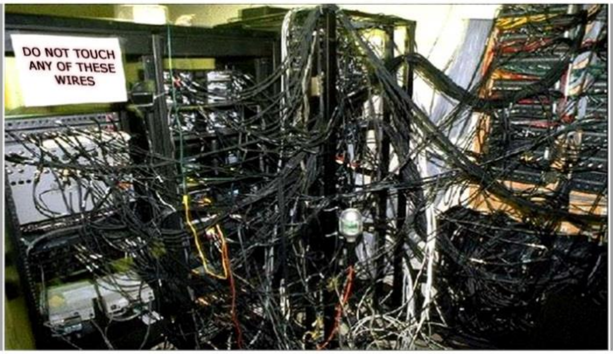
State-of-the-art: Wired Control Systems



Courtesy of **Honeywell**

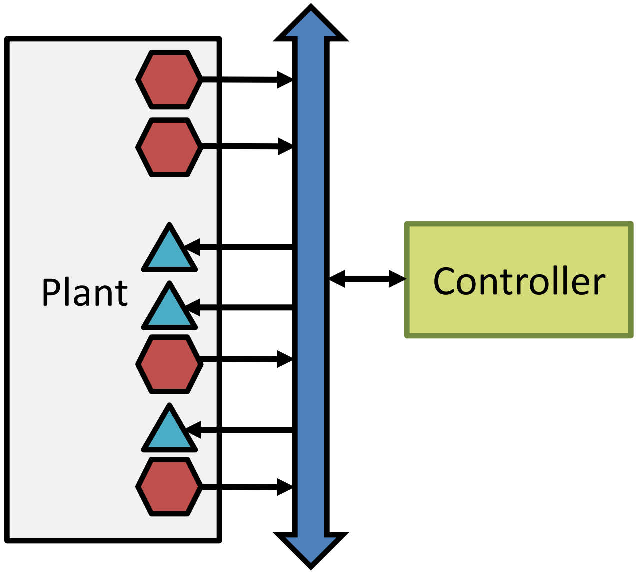
Challenges with Wired Control Systems

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

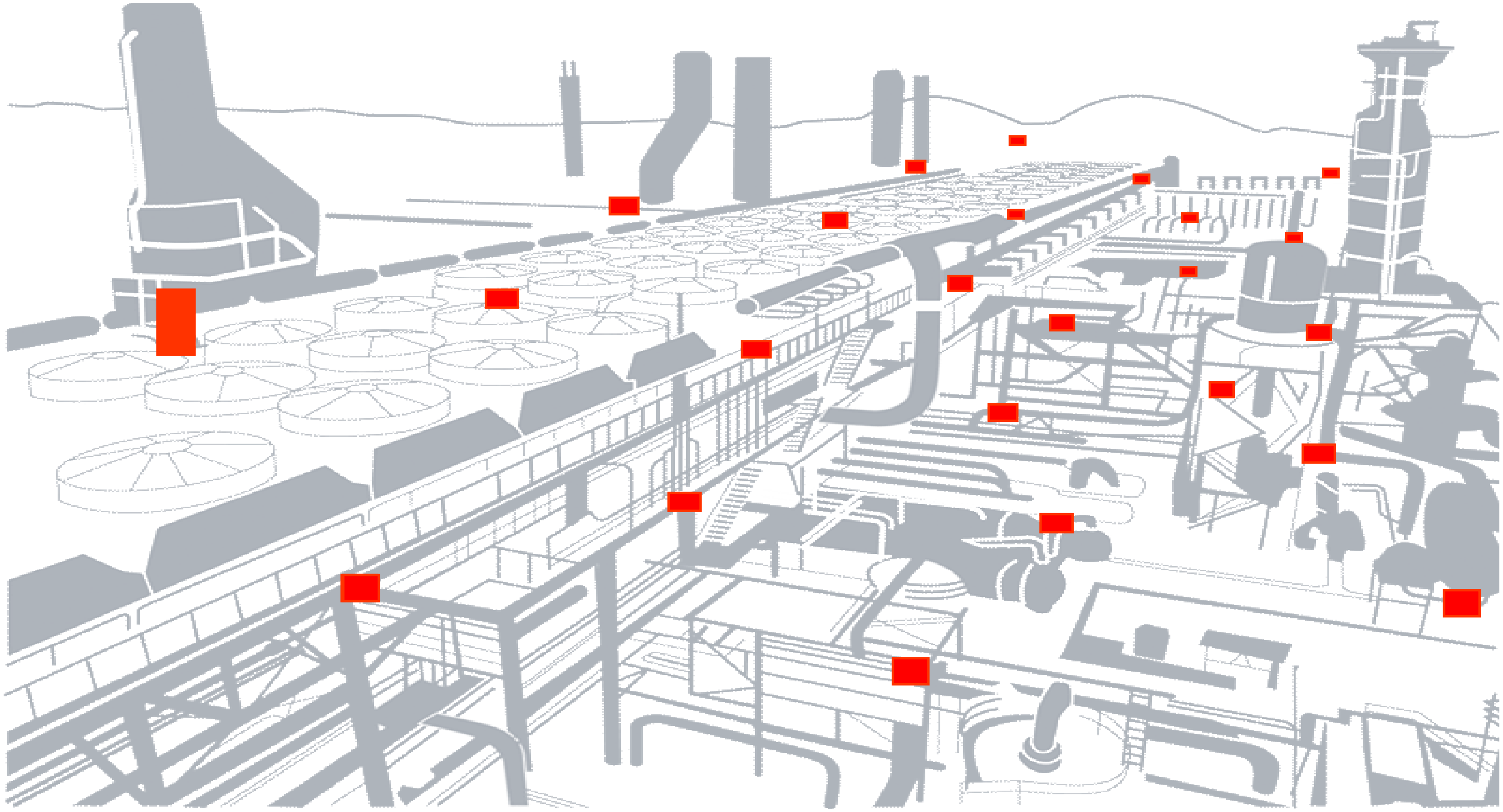


- Lack of flexibility
  - Wires constrain sensor/actuator mobility
  - Limited reconfiguration options

- Restricted control architectures
  - Centralized control paradigm

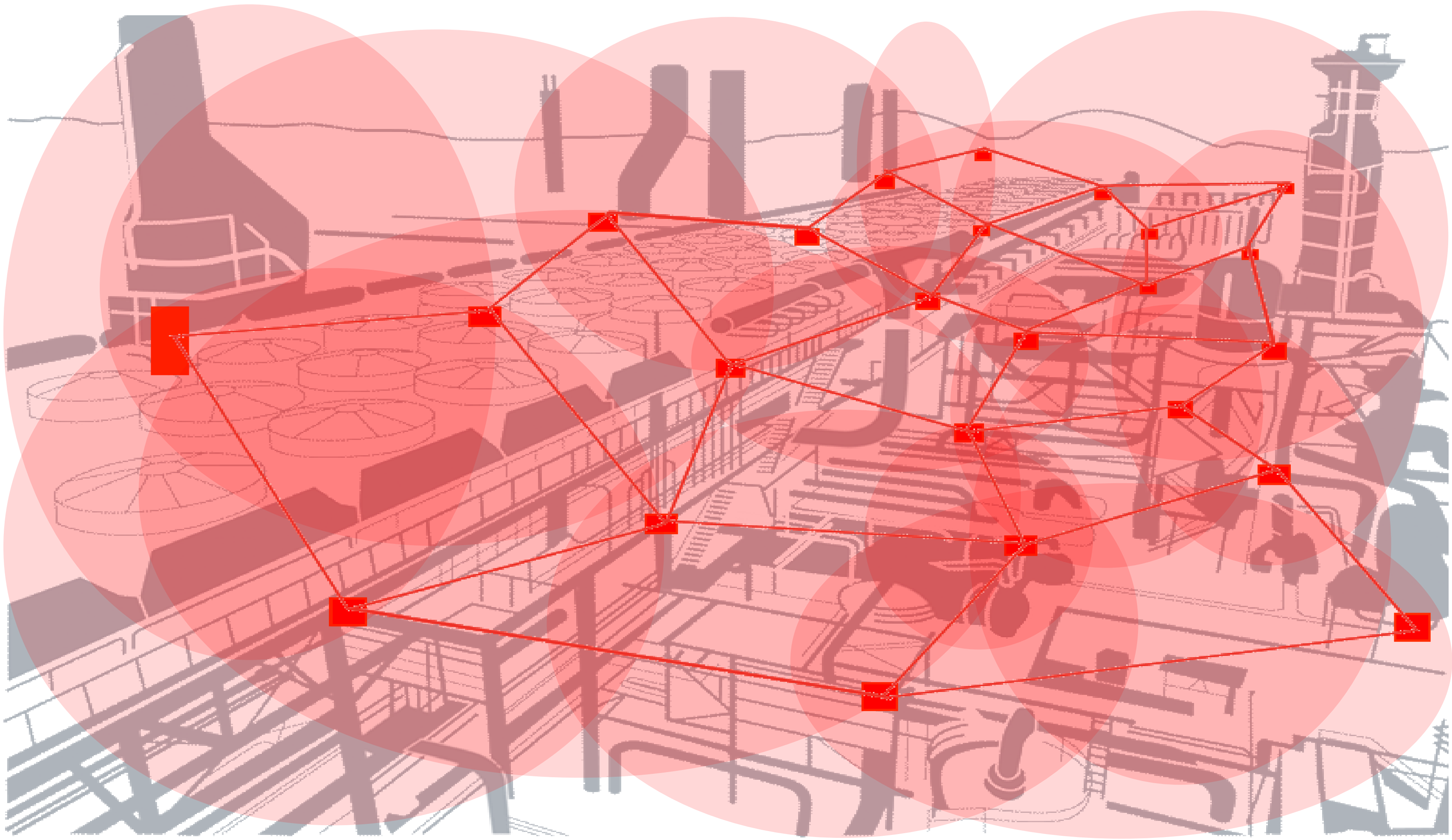


The promise: Wireless Control Systems



Courtesy of Honeywell

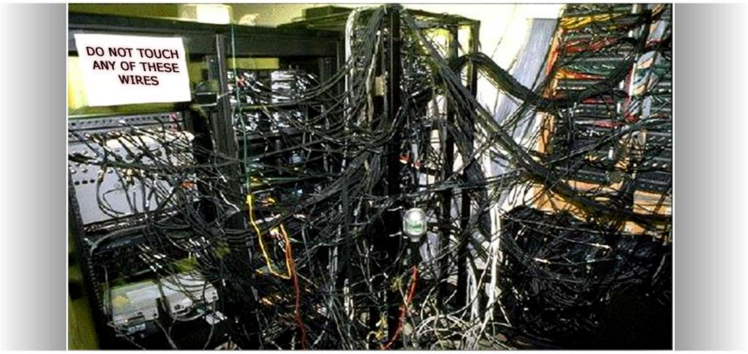
The promise: Wireless Control Systems



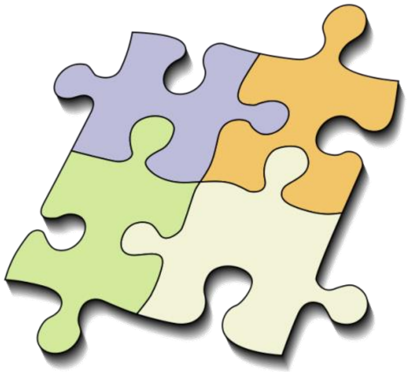
Courtesy of Honeywell

Opportunities with Wireless Control Systems

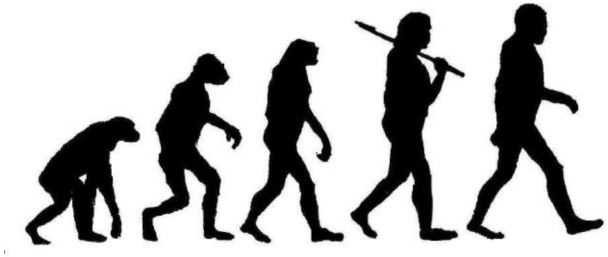
- Lower costs, easier installation
  - Suitable for emerging markets



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



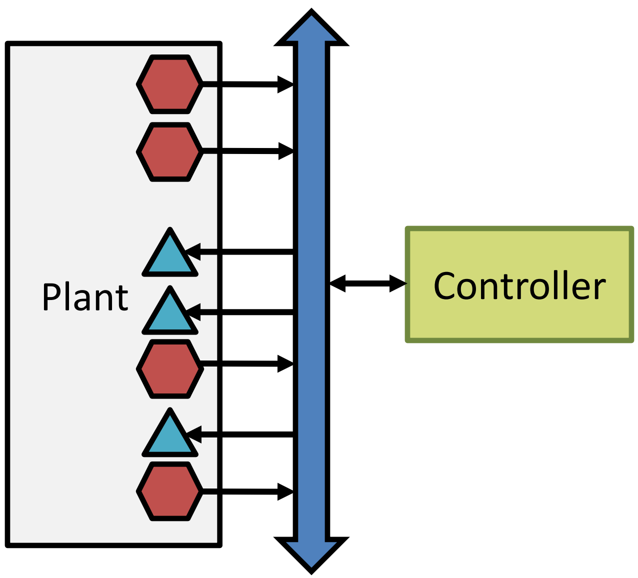
- Compositionality
  - Enables system evolution through logical expansion/contraction of plants and controllers with composable control systems.



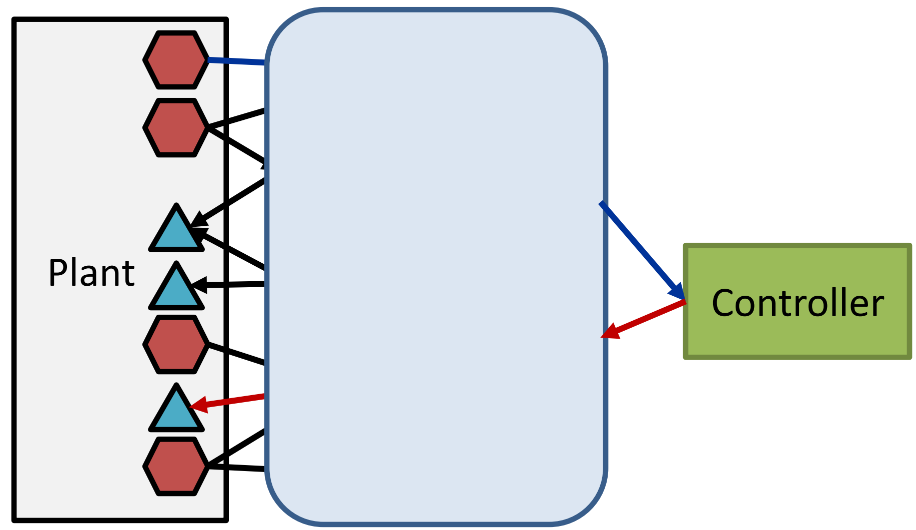
- Runtime adaptation
  - Control stability and performance are maintained in the presence of node, link and topological changes.

Wireless is transformative for industrial control

- Paradigm shift towards wireless control architectures



Wired Control System

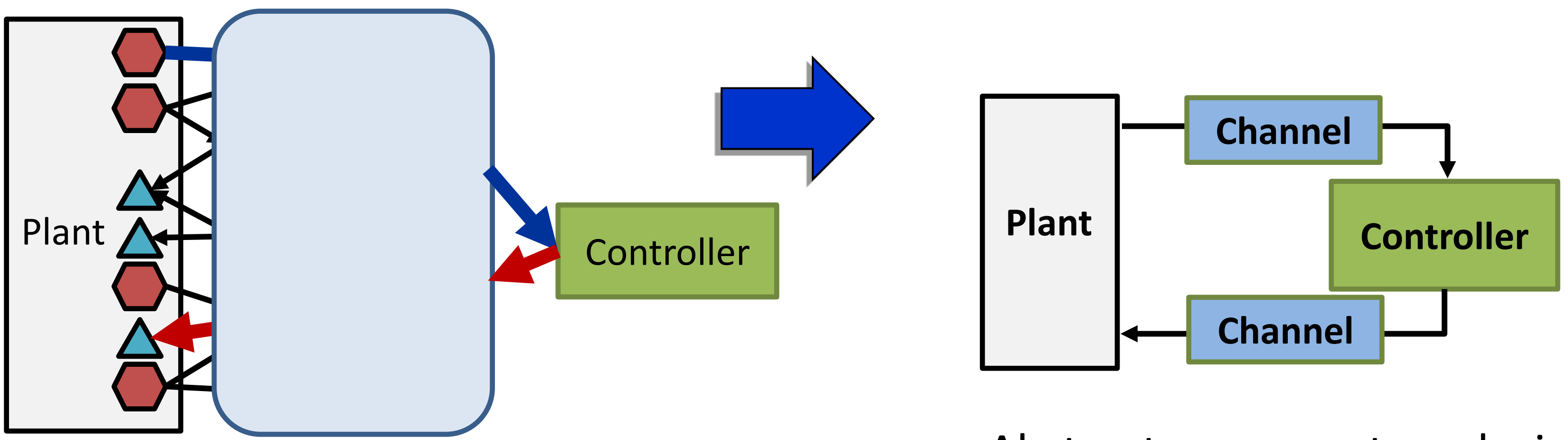


Wireless Control System

- ***Single-hop*** and ***multi-hop*** communication networks

Control over wireless communication networks

- Standard Wireless Control Systems employ packet routing to deliver information to centralized controllers
  - Control performance depends on the network's QoS

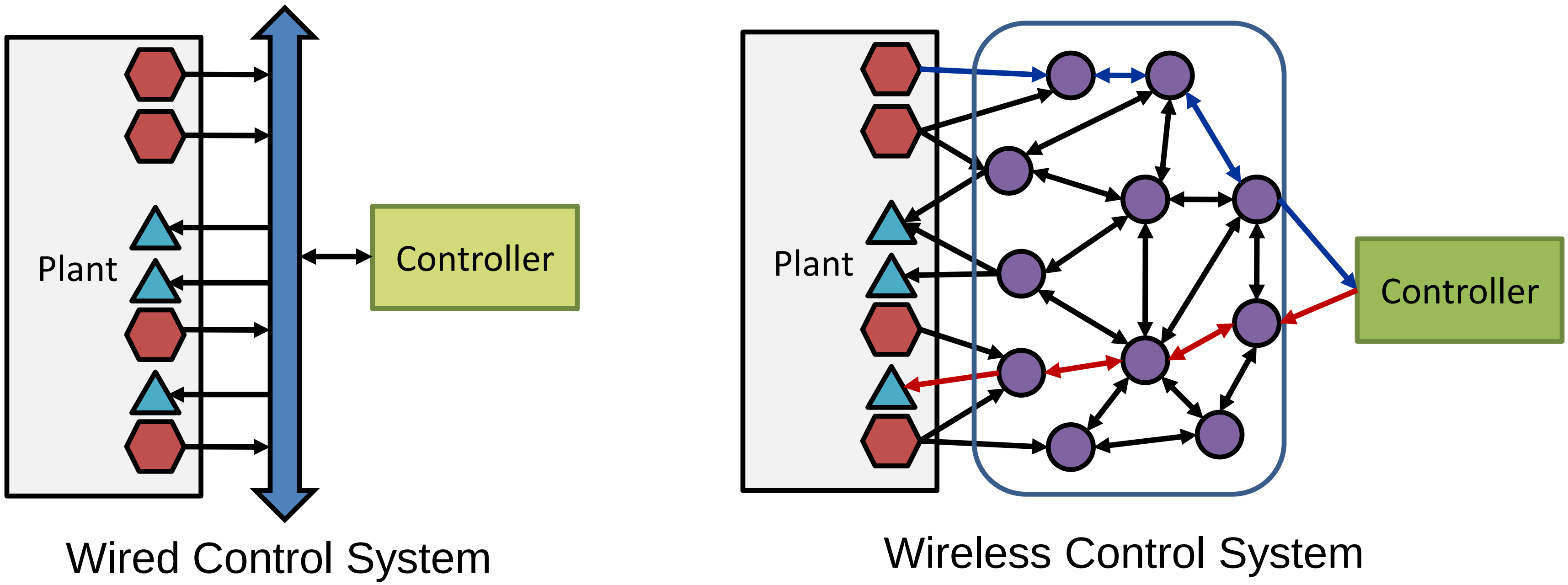


Abstracts away system design

- General challenges include network-induced delay, single-packet vs. multi-packet transmission systems, dropping of communication packets
- Single-hop vs multi-hop networks

Wireless is transformative for industrial control

- Paradigm shift towards multi-hop control architectures

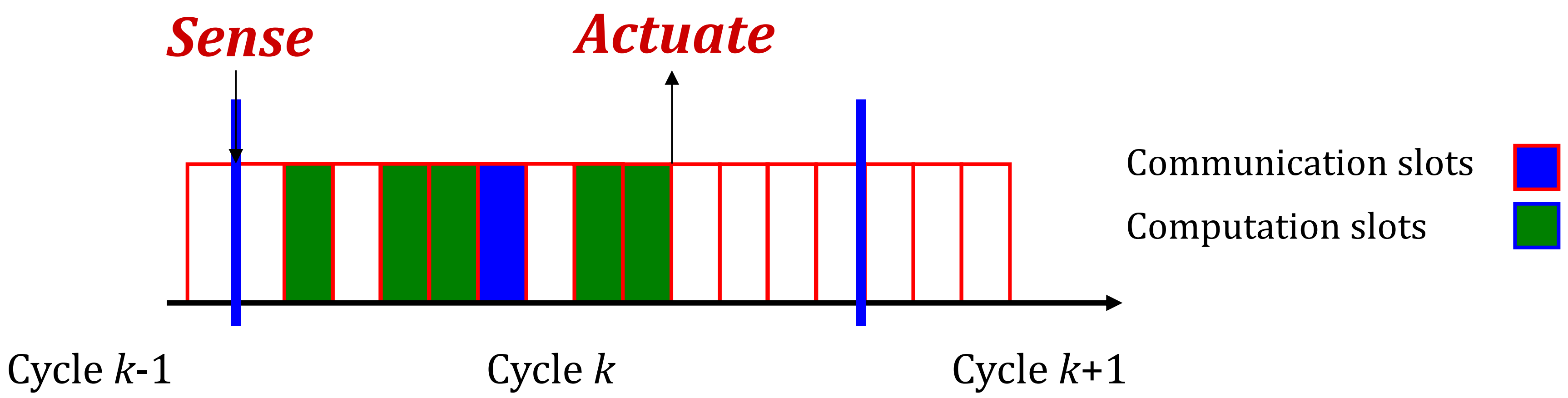


HART COMMUNICATION PROTOCOL

WirelessHART

Time-Triggered Protocols

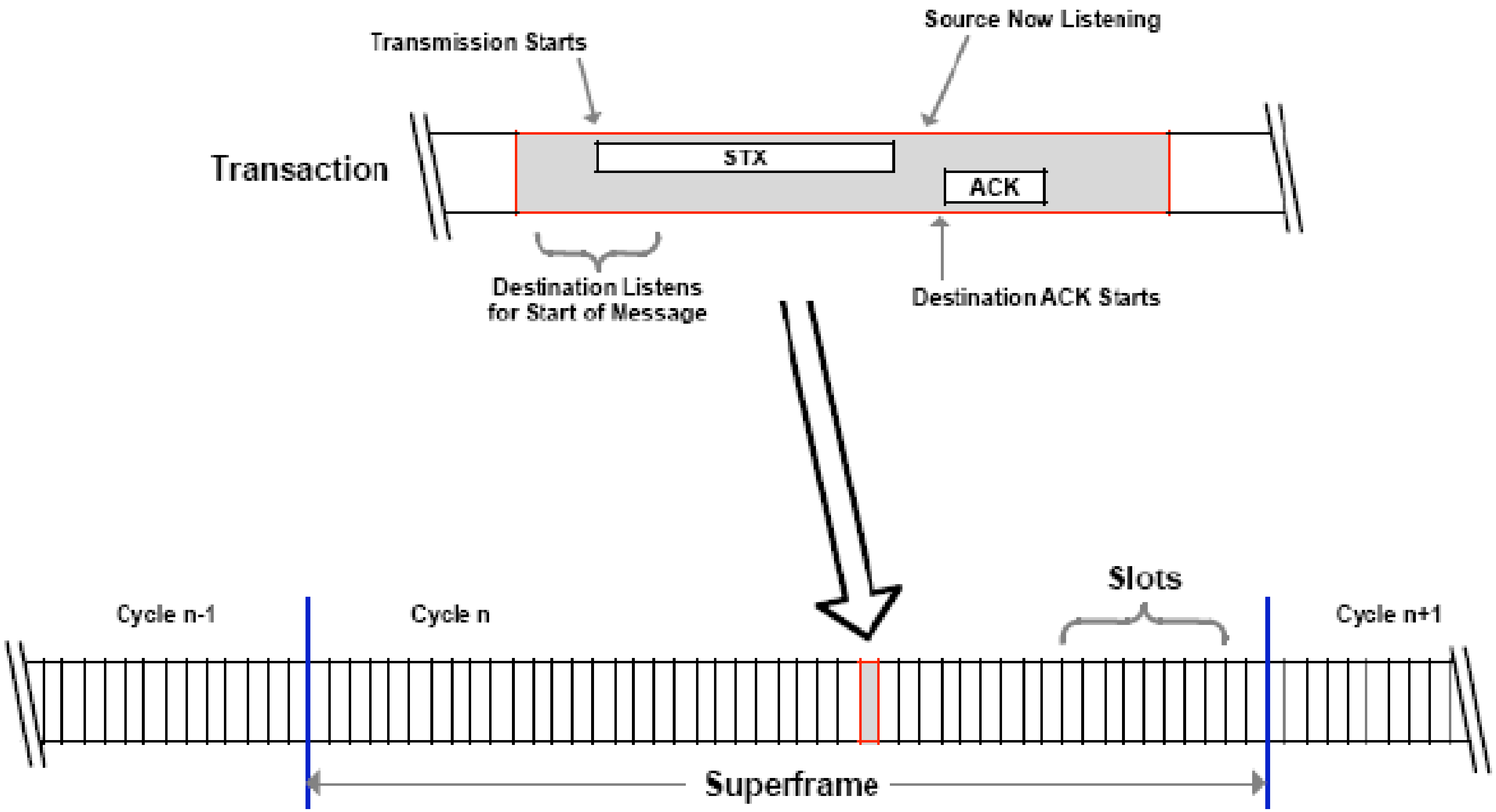
- Widely used for time-critical industrial control applications
- Instead of mapping control computation and communication to periodic-tasks, we allocate them to precise time-slots



- Wireless time-triggered standards (ISA100, WirelessHART)

WirelessHART

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



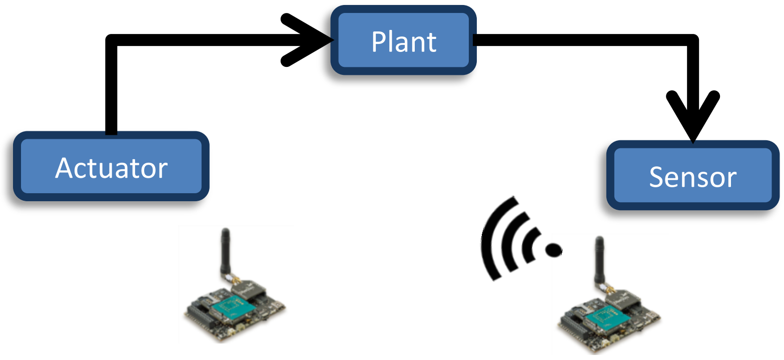
WirelessHART®

Wireless Control Systems: Technical Challenges

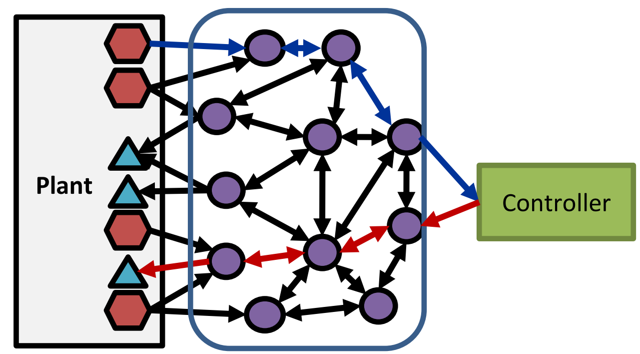
- Modeling
  - Holistic modeling of control, communication, computation
  - Interfaces between control and time-triggered communication
- Analysis
  - Impact of TDMA-based wireless on control performance
  - Compositional scheduling of multiple control loops
- Synthesis
  - Control-scheduling co-design
  - 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

Outline

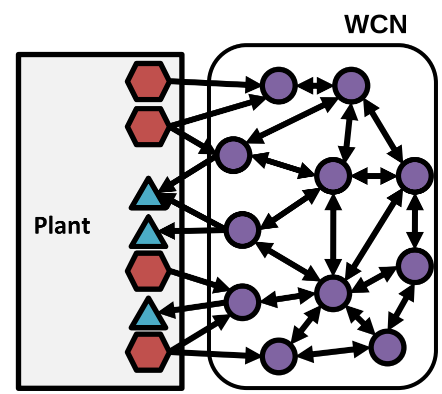
- Optimal Power Management in Wireless Control Systems
  - Power-aware control over single-link networks



- Control with multi-hop wireless networks
  - Routing-based control over time-triggered networks

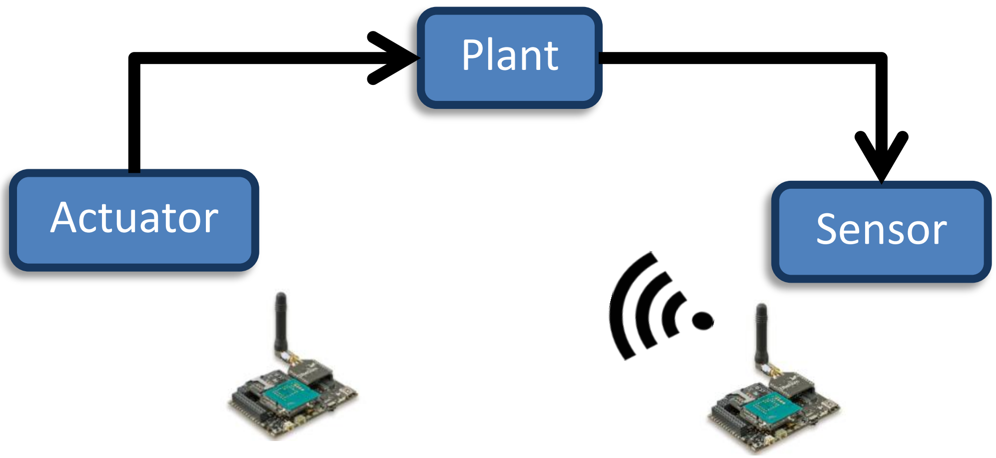


- Wireless Control Networks
  - A simple decentralized approach for *in-network* control



Optimal Power Management in Wireless Control Systems

- Optimal Power Management in Wireless Control Systems*

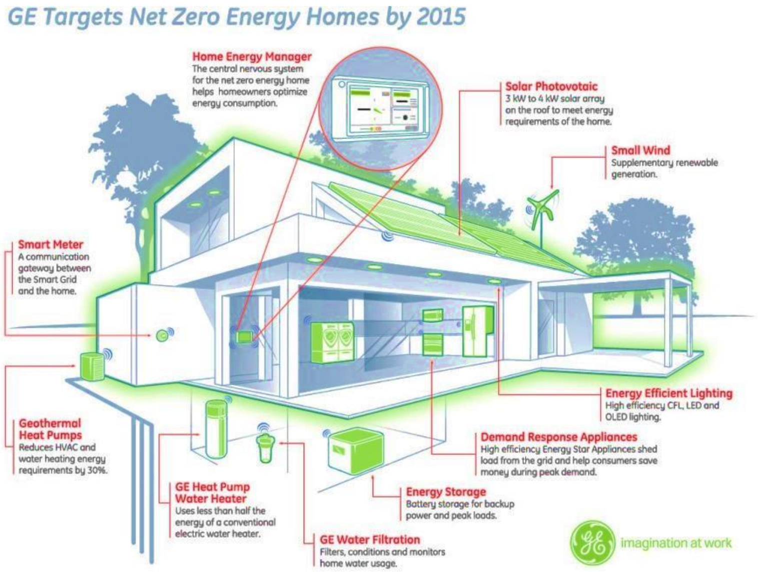


  - Control over a single wireless link
  - Separation & optimal plant control
  - Optimal and suboptimal communication policies

*K. Gatsis, M. Pajic, A. Ribeiro, and G.J. Pappas. *Power-aware communication for wireless sensor-actuator systems*, IEEE Conference on Decision and Control, submitted.
K. Gatsis, A. Ribeiro, G.J. Pappas, *Optimal power management in wireless control systems*, American Control Conference, 2013.
K. Gatsis, A. Ribeiro, G.J. Pappas, *Optimal power management in wireless control systems. IEEE Transactions on Automatic Control*, submitted

Motivation: Managing Power Resources

- Control systems with power-constrained wireless sensors, e.g. HVAC, building/industry automation
- Power regulation: ⬆ sensor lifetime
- Impact & trade-offs with closed-loop control task



Challenges of Power Management in Wireless Control

- Common mathematical framework for control/wireless communications
  - unpredictable wireless conditions
  - online power adaptation (PHY layer)

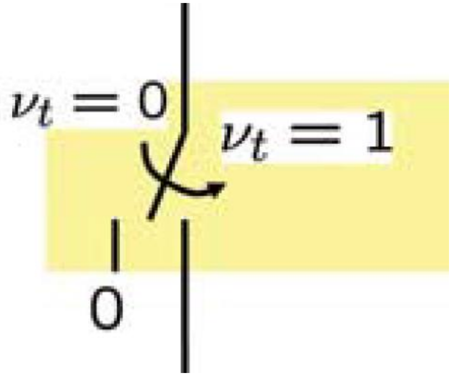
    } Communications
  - timely & reliable information delivery
  - controller design

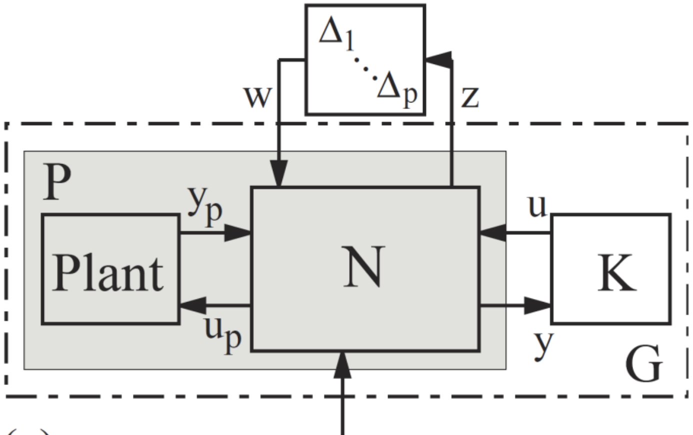
    } Control
- Methodology for (co-) design power & plant control mechanisms
- Advantages & new insights – in contrast to "control-only" or "communication-only" perspectives

Literature: Control under Communication Constraints

- **Communication as a constraint/disturbance**

- Estimation and Control under packet drops [Hespanha et al 2007], [Sinopoli et al 2004], [Schenato et al 2007], [Gupta et al 2007], [Imer et al 2006]
- Communication as model uncertainty (robust control techniques) [Elia 2005], [Braslavsky et al 2007]
  - ➢ Communication not part of the design





(c)

Literature: Communication & Control

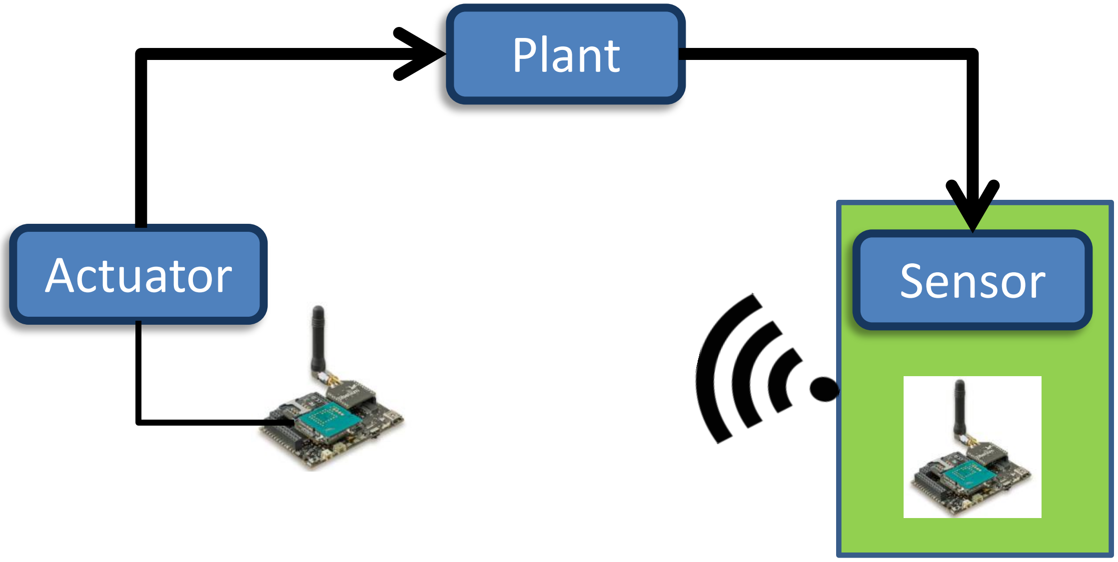
- **Communication with data-rate constraints: coding & control design**

- [Tatikonda, Mitter 2004], [Nair et al 2007], including power [Quevedo et al 2010]
  - ➢ Communication design: encoding & bit-rate for stability

- **Event-based paradigm: sensor (actuator) decides whether to transmit (actuate) or not**

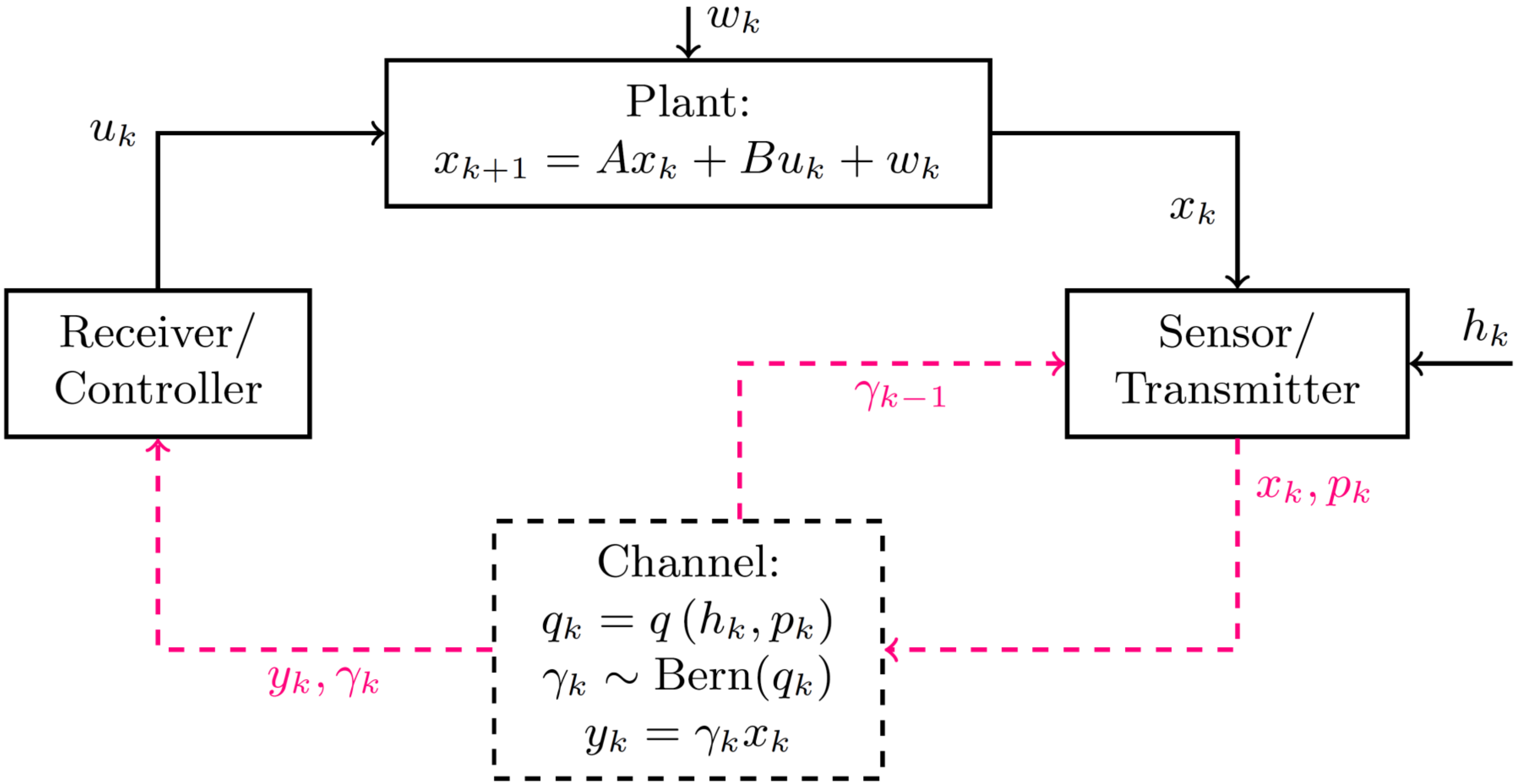
- Estimation [Xu, Hespanha 2004], [Cogill et al 2007], [Mesquita et al 2012], [Li, Lemmon 2011]
- Control [Tabuada 2007], [Anta, Tabuada 2010], [Rabi, Johansson 2009], [Molin, Hirche 2009], [Donkers et al 2011]
  - ➢ Communication cost: average number of transmissions

Power-aware Control over Wireless



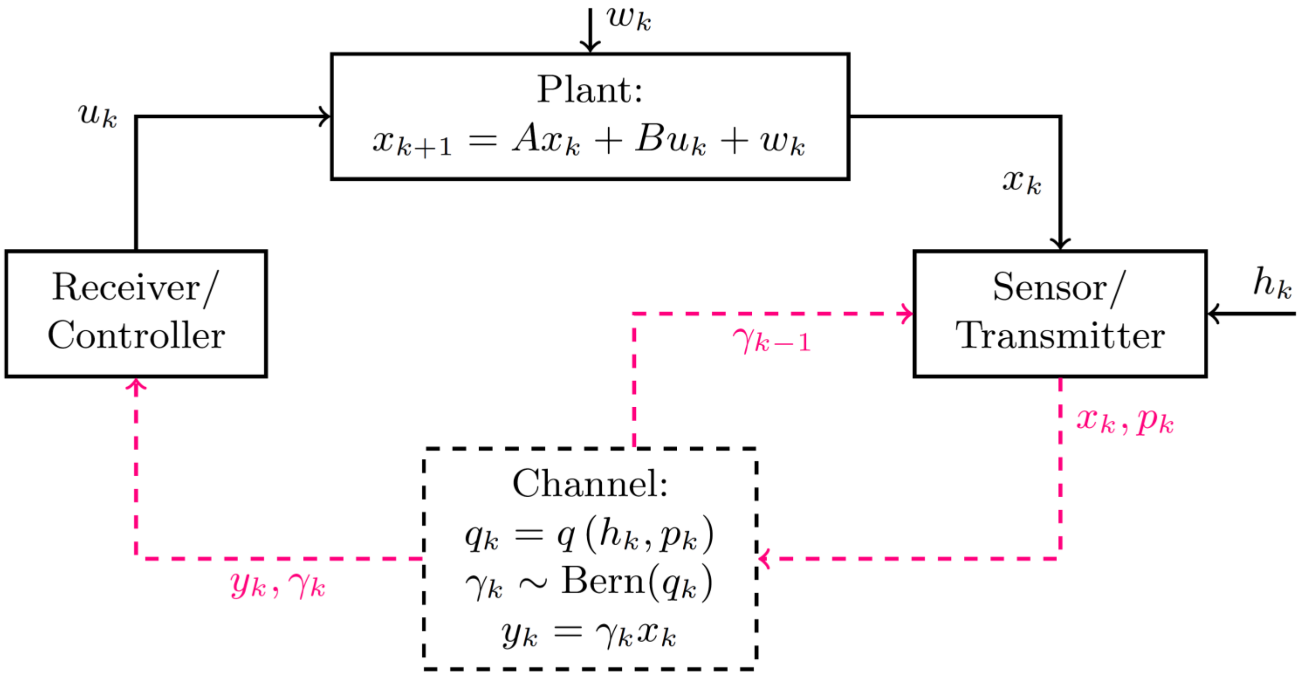
- Single loop with power-constrained sensor/transmitter & power-free receiver/actuator
- Goal: design power control & plant control mechanisms
- On-line by adapting to both wireless channel conditions and plant state
  - Less power when plant ‘close’ to stability
  - Good channel - cheap to transmit vs. bad channel - costly

Wireless Control Architecture



- Channel state information h_k available at transmitter
- Power adaptation p_k to both channel h_k & plant x_k
- Packet drops capture both effects of random wireless channel & protection by power

Wireless Control Architecture & Co-design



Decision variables

$\pi := \{p_0, p_1, \ldots\}$

$\theta := \{u_0, u_1, \ldots\}$

- Performance: Joint average linear quadratic and power costs

$$\text{minimize} \quad J(\pi, \theta) := \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathbb{E}^{\pi,\theta} \left[x_k^T Q x_k + u_k^T R u_k + \lambda p_k \right]$$

Wireless Communication Model

Decoding depends on power and channel

- Received signal-to-noise ratio

$$SNR_k = \frac{h_k\, p_k}{N_0}$$

- $p_k \in [0, p_{\max}]$

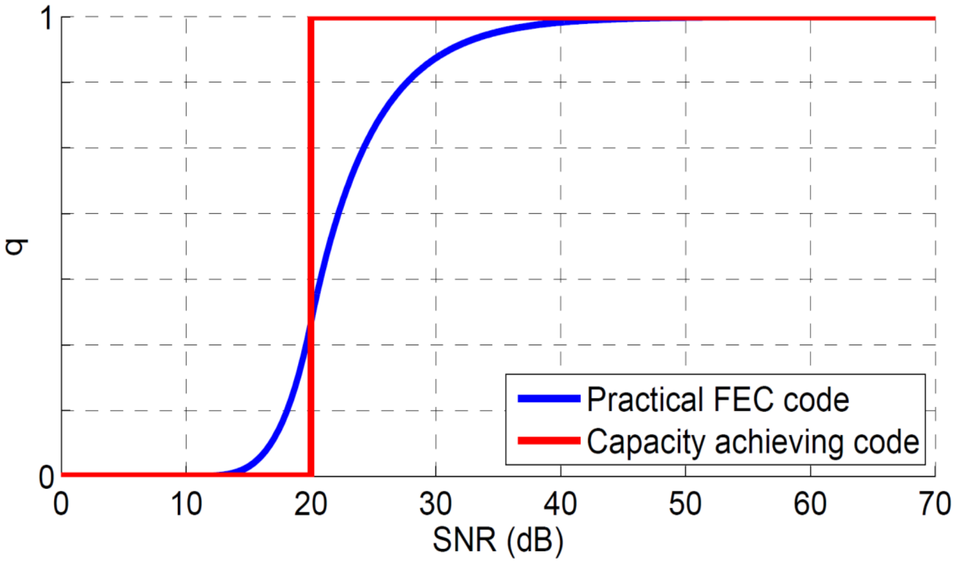
- h_k block fading, i.i.d.

- N_0 : AWGN power level

- Probability of successful decoding

$$q_k = q(SNR_k)$$

- determined experimentally
- depends on error-correcting code



- Combine in $q_k = q(h_k, p_k)$

Novelties of our Wireless Control Architecture

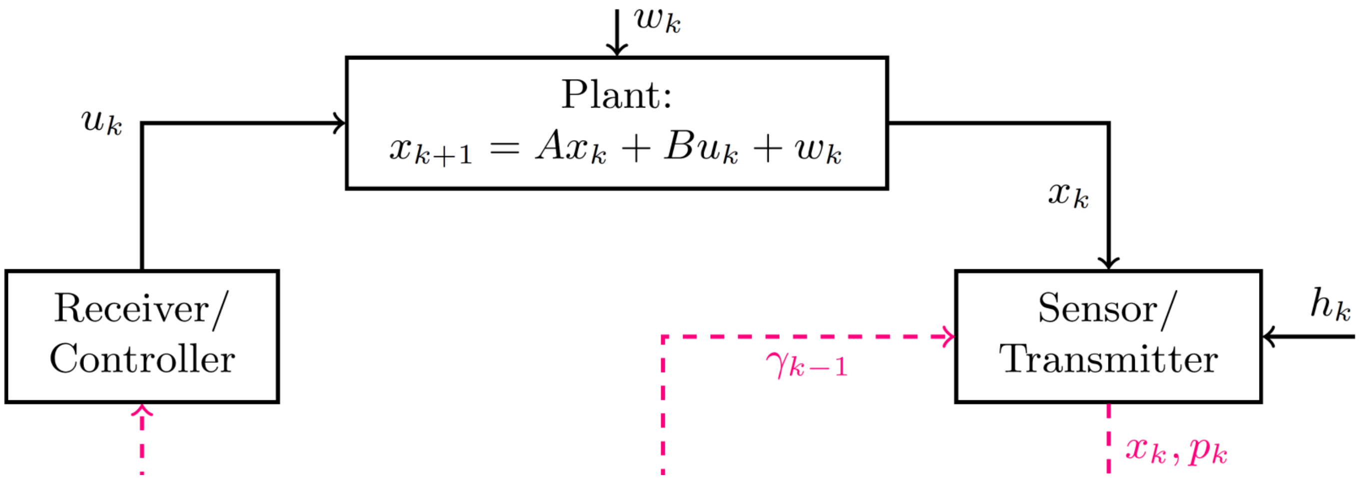
- Generalizes standard Bernoulli packet drops
  - Wireless effects are explicitly captured
  - Bernoulli successes are actively controlled by power
- Generalizes event-triggered transmissions
  - Decision depends also on wireless conditions
  - Communication cost is power consumption vs. transmission rate
- Packet-based communication: unlike data-rate constraints & coding

Joint Optimal Communication & Control

$$\text{minimize} \quad J(\pi, \theta) := \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathbb{E}^{\pi,\theta}\left[x_k^T Q x_k + u_k^T R u_k + \lambda p_k\right]$$

- Information structure couples decisions:

Control action u_k affects power decision p_{k+1} through x_{k+1}



Restricted Information Structure

- Controller keeps estimate*

$$\hat{x}_k = \begin{cases} x_k & \text{if } \gamma_k = 1, \\ A\hat{x}_{k-1} + Bu_{k-1} & \text{if } \gamma_k = 0 \end{cases}$$

- Innovation terms at sensor/transmitter (known by ACK):

$$\varepsilon_k := x_k - \underbrace{(A\hat{x}_{k-1} + Bu_{k-1})}_{\text{controller's best estimate}}$$

- Restrict available information: innovation and channel

$$\{x_0, h_0, \gamma_0, \ldots, \gamma_{k-1}, x_k, h_k\} \rightarrow \{\varepsilon_0, h_0, \ldots, \varepsilon_k, h_k\}$$

- Control input does not affect transmitter - no effect on quality of future plant state estimation

* Optimal if information from lost packets is removed

Separation & Optimal Plant Control

- Adapt power to innovation and channel

$$\Pi = \left\{ \begin{array}{l} p_k = p(\varepsilon_k, h_k), \\ \text{such that } \|\varepsilon\| \geq L \Rightarrow p(\varepsilon, h) = p_{max} \end{array} \right.$$

Theorem: For any communication policy $\pi \in \Pi$

$$\min_{\theta} J(\pi, \theta) = Tr(PW) + \underbrace{\lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathbb{E}^{\pi} \left[e_k^T \tilde{P} e_k + \lambda p_k \right]}_{J_{\text{COMM}}(\pi)}$$

where P is the algebraic Riccati equation solution, $\tilde{P} := A^T P A + Q - P$, and the optimal control is the standard LQR

$$\theta^* : u_k = K \hat{x}_k$$

Conditions for Optimal Control Theorem

- Assumptions: (A,B) controllable, (A, $Q^{1/2}$) observable, and

for every channel h *

$$q(h, p_{\max}) > 1 - \frac{1}{\lambda_{max}(A)^2}$$

- relates to stability of the jump estimation errors when transmitter uses full power

$$e_k = \begin{cases} 0 & \text{if } \gamma_k = 1, \\ A e_{k-1} + w_{k-1} & \text{if } \gamma_k = 0 \end{cases}$$

- guarantees that for any $\pi \in \Pi$

there exists a finite uniform bound $\mathbb{E}^{\pi} e_k^T e_k \leq M$

* Can be relaxed – in expectation over h

Proof of Optimal Control Theorem

- Finite horizon N - standard LQR Bellman equation & solution

$$V_k := \min_{u_k} \mathbb{E}^\pi \left[x_k^T Q x_k + u_k^T R u_k + V_{k+1} | G_k \right], \quad V_N := 0$$

$$V_k = \mathbb{E}^\pi \left[x_k^T P_{N-k} x_k | G_k \right] + \sum_{j=k}^{N-1} Tr(P_{N-j-1} W) + \sum_{j=k}^{N-1} \mathbb{E}^\pi \left[e_j^T \tilde{P}_{N-j} e_j | G_k \right]$$

since plant input has no effect on future plant estimates, and $u_k = -K_{N-k}\hat{x}_k$

with standard Riccati recursion

$$K_{k+1} := (R + B^T P_k B)^{-1} B^T P_k A,$$
$$\tilde{P}_{k+1} := A^T P_k B K_{k+1},$$
$$P_{k+1} := A^T P_k A + Q - \tilde{P}_{k+1}, \; P_0 := 0$$

Converge by controllability/ observability assumptions

- Limit of finite horizon optimal cost

$$\inf_{\theta \in \Theta} J_{\text{LQR}}^N(\pi, \theta) = \mathbb{E}^\pi V_0 = x_0^T P_0 x_0 + \underbrace{\sum_{k=0}^{N-1} Tr(P_{N-k-1} W)}_{\text{average converges to } Tr(PW)} + \underbrace{\mathbb{E}^\pi \sum_{k=0}^{N-1} e_k^T \tilde{P}_{N-k} e_k}_{\text{average converges: } e_k \text{ bounded}}$$

Optimal Communication Policy

- Optimal communication: estimation vs. power

$$J^*_{\text{COMM}} = \min_{\pi \in \Pi} \lim_{N \to \infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathbb{E}^{\pi} \left[e_k^T \tilde{P} e_k + \lambda p_k \right]$$

- Reduces to a Markov Decision Process: state (ε, h), action p
- **Existence** of solution to Bellman equation is shown

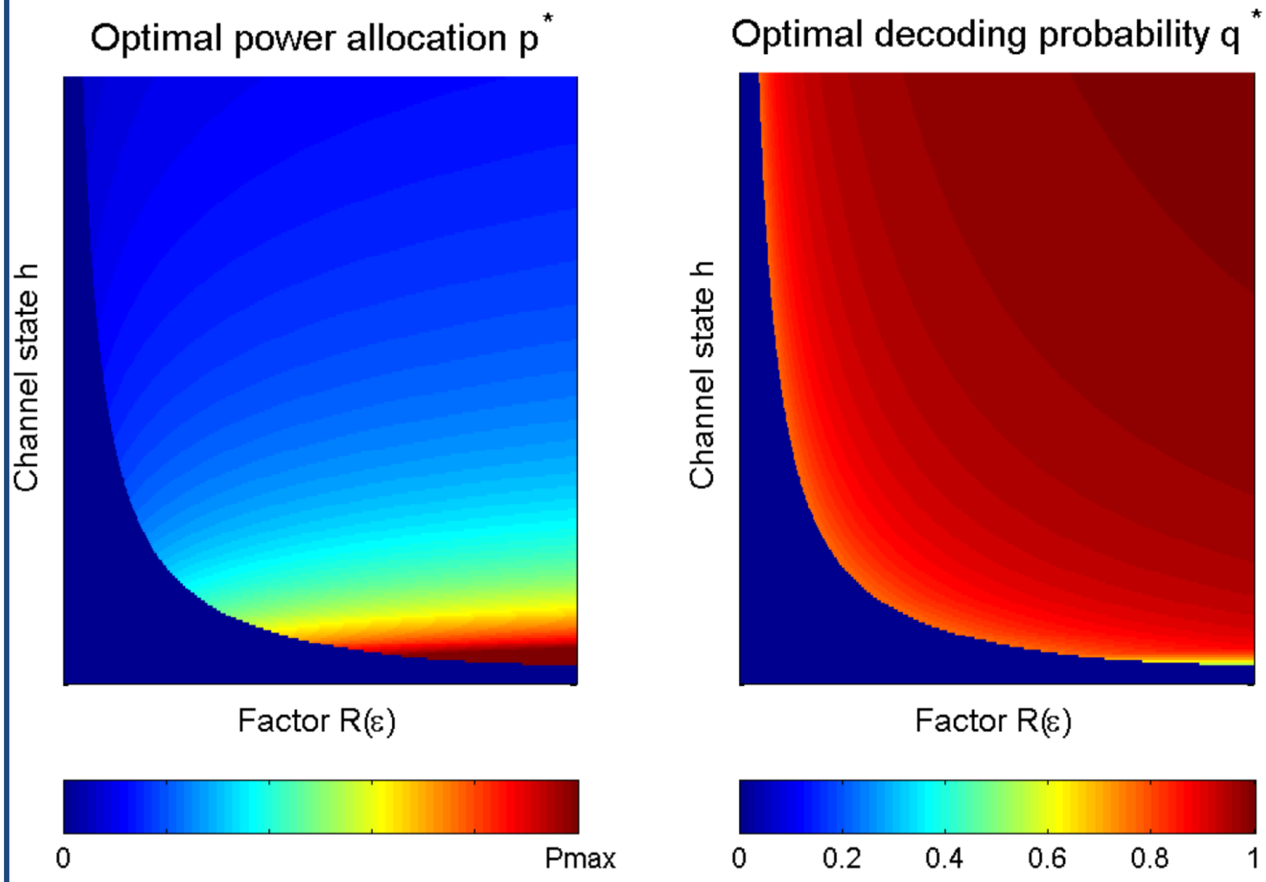
$$V(\varepsilon, h) + J^*_{\text{COMM}}$$
$$= \min_{p \in [0, p_{\max}]} (1 - q(h,p))\varepsilon^T \tilde{P} \varepsilon + \lambda p + \mathbb{E}\left[V(\varepsilon^+, h^+) | \varepsilon, h, p \right]$$

- **Not computationally tractable** due to continuous state space

Characterization of Optimal Communication Policy

- Optimal power allocation in terms of an unknown penalty on innovation

$$p^*(\varepsilon, h) := \underset{p \in [0, p_{\max}]}{\operatorname{argmin}} \quad (1 - q(h,p))\, R(\varepsilon) + \lambda p$$



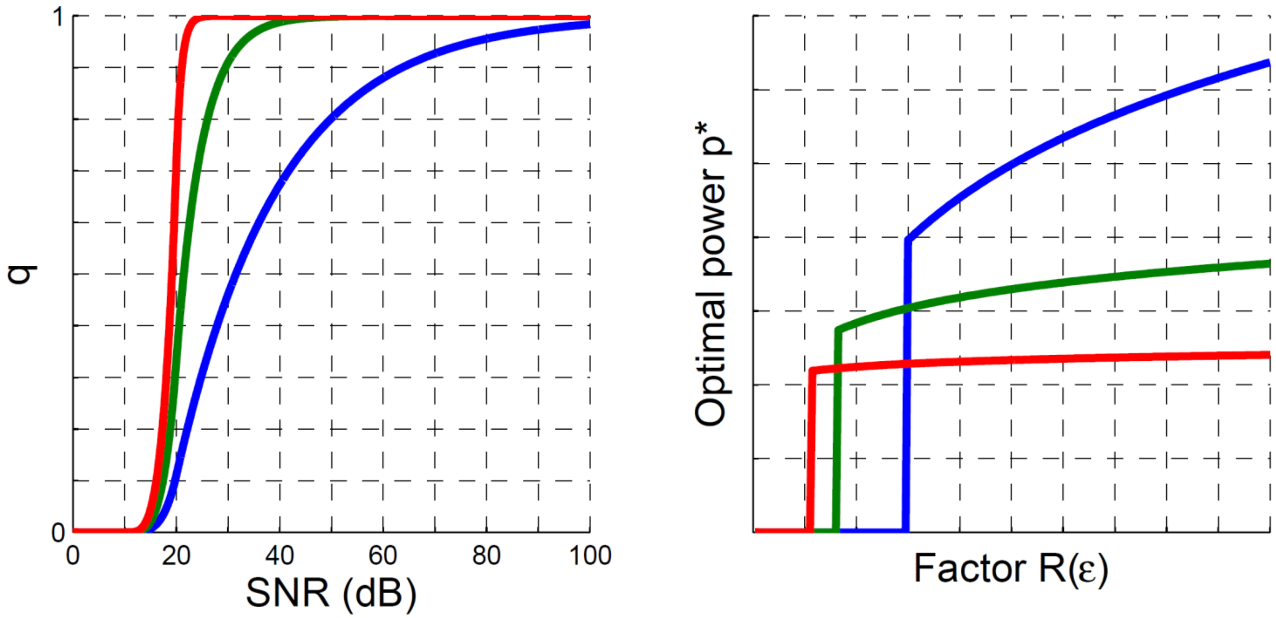
- Zero power when error small or channel fading low
- Area depends on weight λ
- Outside zero-power region adapt power to both plant and channel
- *"Soft"* event-triggering

Characterization of Optimal Communication Policy

Dependence on error-correcting code

- Effect of different error-correcting codes

$$p^*(\varepsilon, h) := \underset{p \in [0, p_{\max}]}{\operatorname{argmin}} \; (1 - q(h, p))\, R(\varepsilon) + \lambda p$$

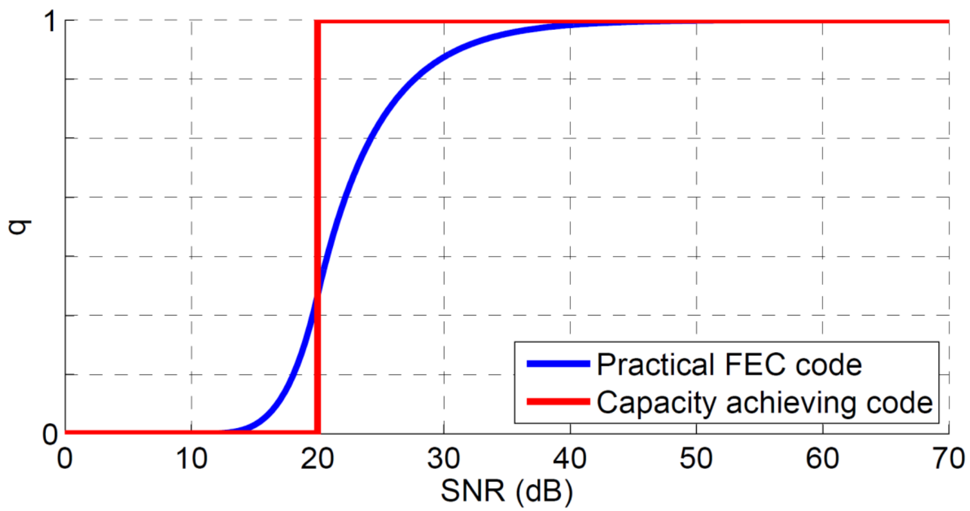


- Fixed channel h
- Zero-power region depends on shape of function *q(h,p)*
- *"Soft"* event-triggering: power adapts to plant when transmitting

Theoretical Limit for Capacity Achieving Codes

- Model capacity achieving codes by indicator

$$q(h, p) = \mathbb{I}\,(p\,h \geq p_0)$$



- Optimal (not tractable)

$$p^{CA}(\varepsilon, h) := \begin{cases} 0 & \text{if } \; h\,R(\varepsilon) \leq \lambda\,p_0 \\ p_0 / h & \text{otherwise} \end{cases}$$

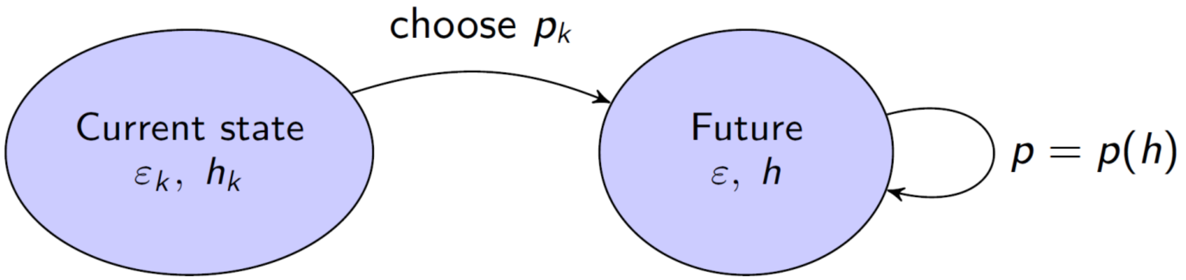
- Packet success $q_k = 0 \text{ or } 1$

➢ *Recover standard event-triggered transmit-or-not policies, trigger depends on channel and estimation error!*

Suboptimal Communication Policies

Rollout policy (model predictive):

"optimize current power as if future policy is some reference"



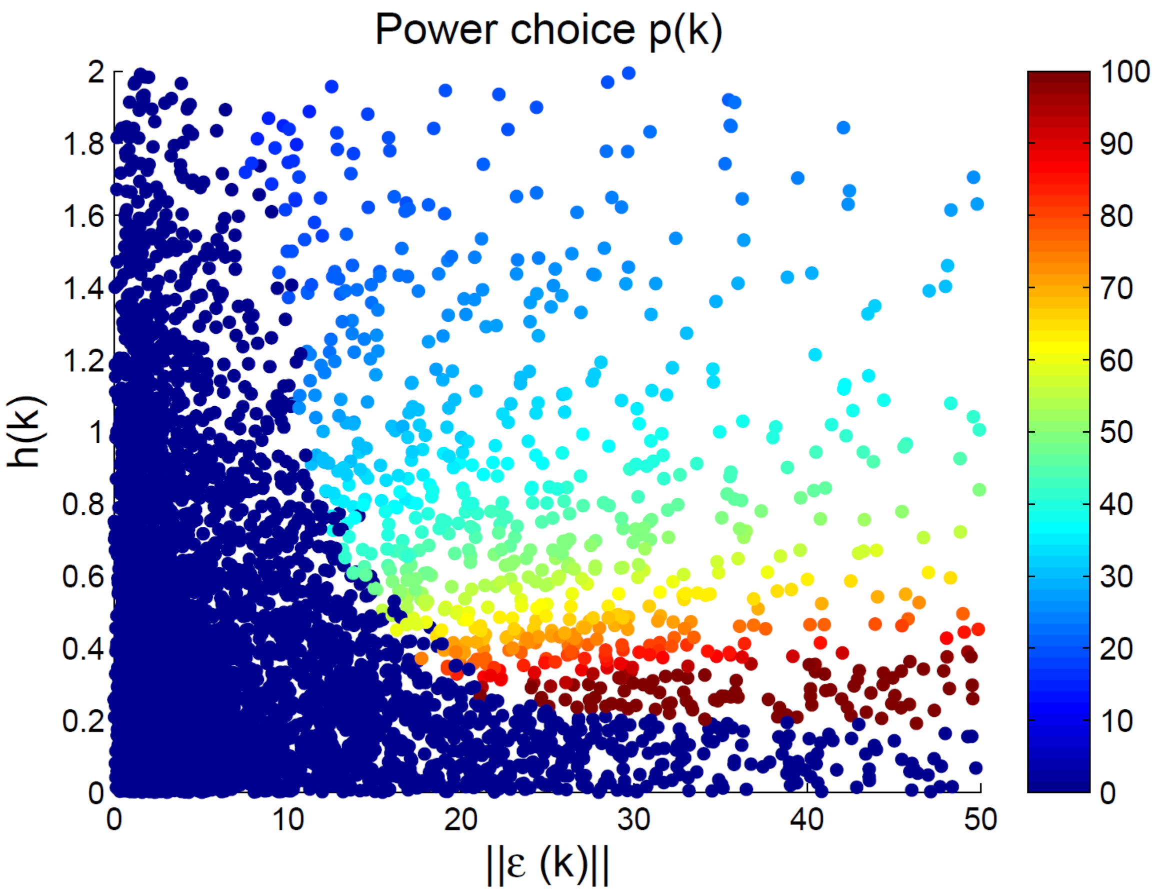
- Reference policy adapting only to channel *p(h)*
- Bernoulli packet success $\bar{q} := \mathbb{E}_h q(h, p(h))$
- Quadratic cost-to-go $H = (1-\bar{q})(A^T H A + \tilde{P})$

$$p^{\text{roll}}(\varepsilon, h) = \underset{p\in[0,p_{\max}]}{\text{argmin}}\ (1 - q(h,p))\frac{\varepsilon^T H \varepsilon}{1-\bar{q}} + \lambda p$$

Approximates optimal $R(\varepsilon)$

Simulation of Suboptimal Policies – General Codes

$$A = \begin{bmatrix} 2 & 0 \\ 1 & 0.8 \end{bmatrix}, \; B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

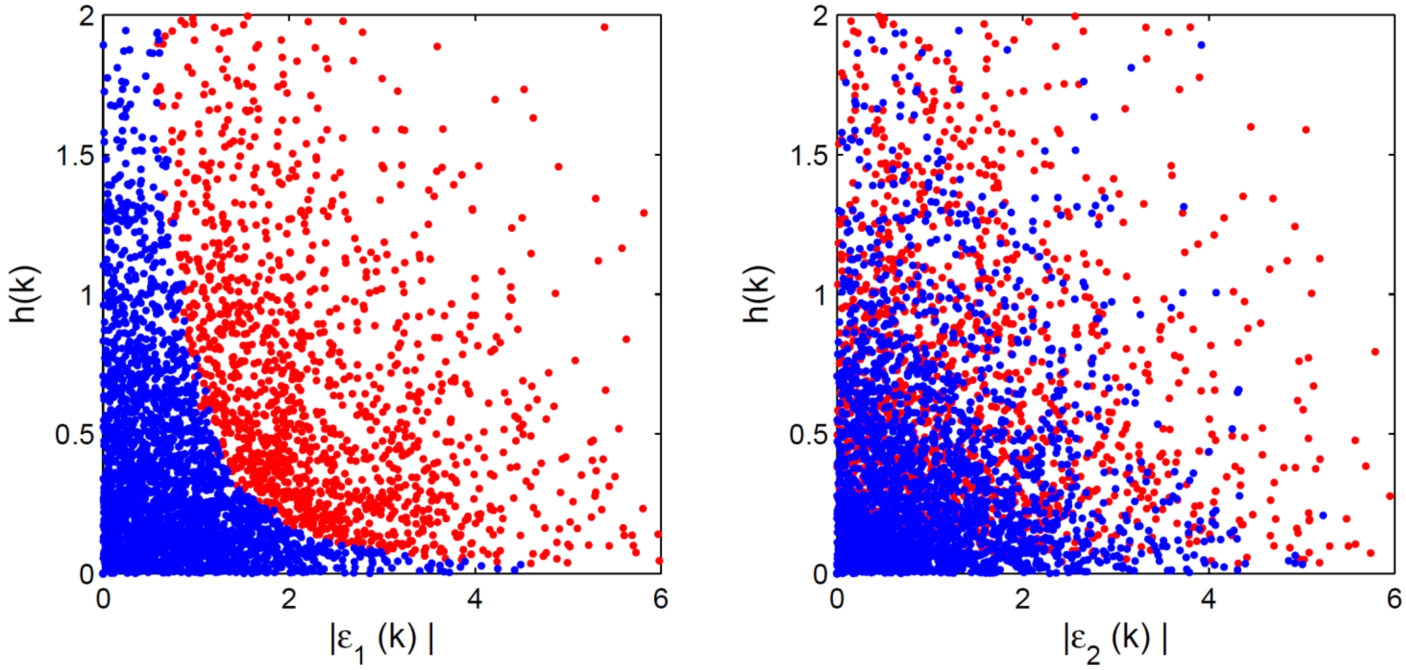


- Quadratic penalty on error
- Characteristics similar to the optimal policy

Simulation of Suboptimal Policies – Capacity Achieving

$$A = \begin{bmatrix} 2 & 0 \\ 1 & 0.8 \end{bmatrix}, \; B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

Blue: don't transmit,
Red: transmit



- Policies become event-triggered
- Rollout policy adapts to plant structure

Summary of Results

- Richer communication model:
  - captures uncertainties of wireless & power adaptation
- Communication/control separation can be established (suboptimal but otherwise joint cost hard to analyze)
- Optimal communication is ‘soft’ event-triggered
  - zero power if error small or channel adverse
  - power adaptation to both plant and channel states otherwise
- Communication policies can be designed by ADP techniques

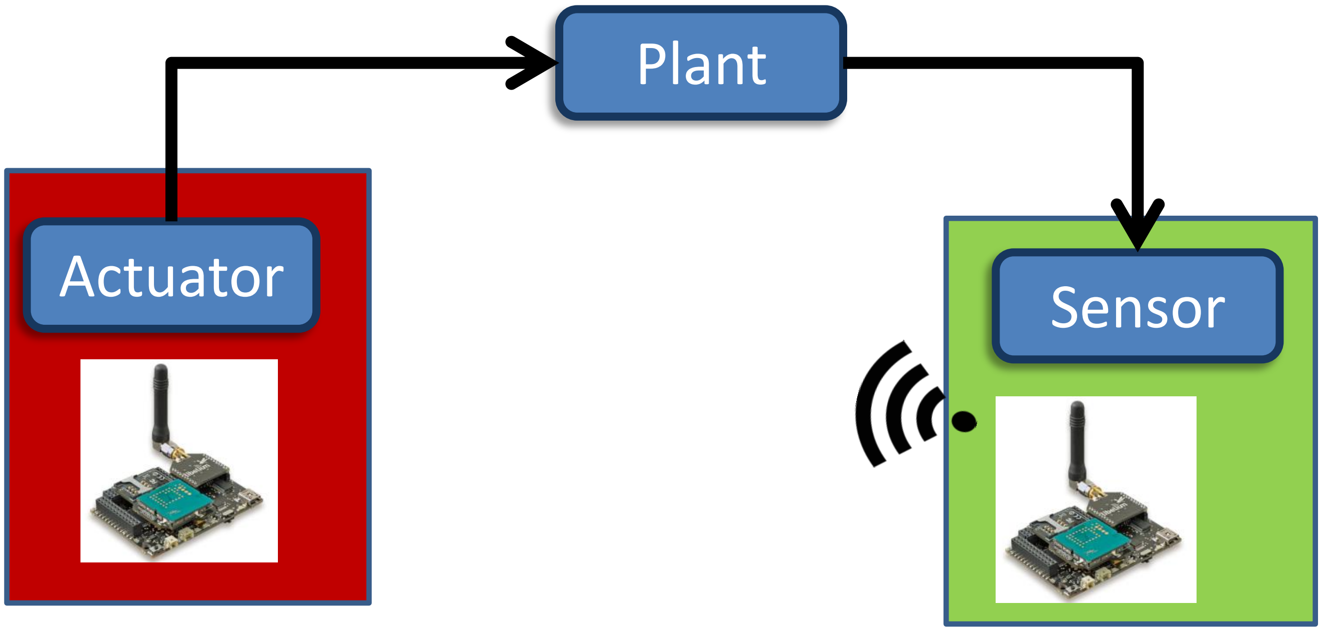
A New Paradigm for Control / Wireless Networking

- **Model, analysis, communication/control co-design of complex wireless sensor & actuator networks**

- Multiple or distributed plants
- Shared wireless channels (interference)
- Optimal **control-aware resource allocation**, e.g. power, scheduling
- Economic **resource-aware controller synthesis**

Limitation: Not Power-aware at Receiver

- Architecture limitation:
  - wireless receiver/controller *always listens*
  - comparable power consumption at both ends
  - common in any event-based scheme over wireless



Power-aware Wireless Receiver Design

Event-based → Low Transmission Rate → Receiver Under-utilized

- Ideally: Turn off receiver *between transmissions…*
  - ➢ inconsistent with event-triggering
- Our approach: coordination protocol
  - ➢ Devices turn off and agree on next wake-up time (self-triggered* step)
  - ➢ Upon wake-up sensor decides whether to transmit or not (event-triggered step)
  - ➢ How to '*predict*' when next event will occur?
  - ➢ Consider power costs at both ends, current channel & plant states

*[Anta, Tabuada 2010]

Simplified Problem Setup

- **Markov fading** channel (**finite states**, irreducible, aperiodic)
  - possibility of *predicting* good channels
- Capacity achieving code
- ***Constant* power penalty *p_a* for awake receiver**, p_k for transmitter as before

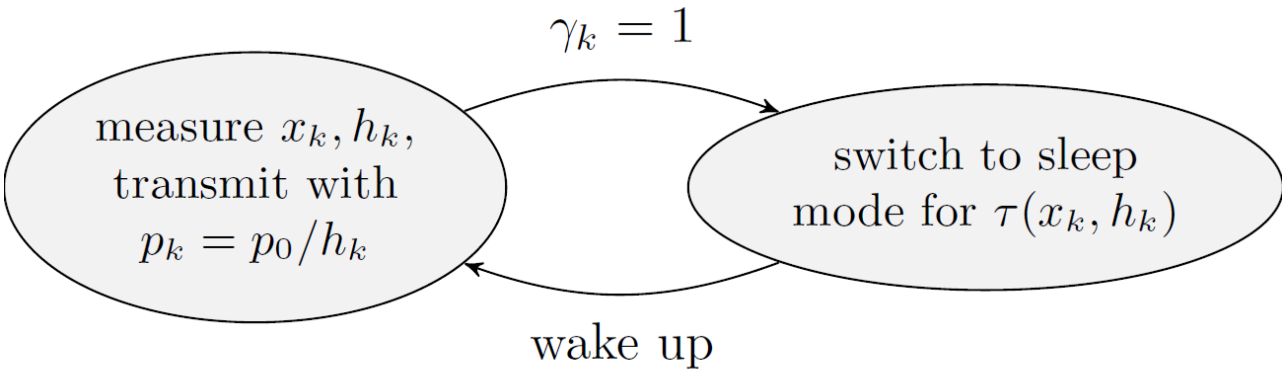
$$p'_k := \begin{cases} p_a + p_k & \text{if awake at } k, \\ 0 & \text{if in sleep mode at } k \end{cases}$$

- Fixed LQR controller $u_k = K\hat{x}_k$
- Trade-off estimation error vs. power at both ends

$$J := \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathbb{E}\left[e_k^T P e_k + \lambda p'_k\right]$$

Optimal Self-triggered Protocol

- Self-triggered protocol:

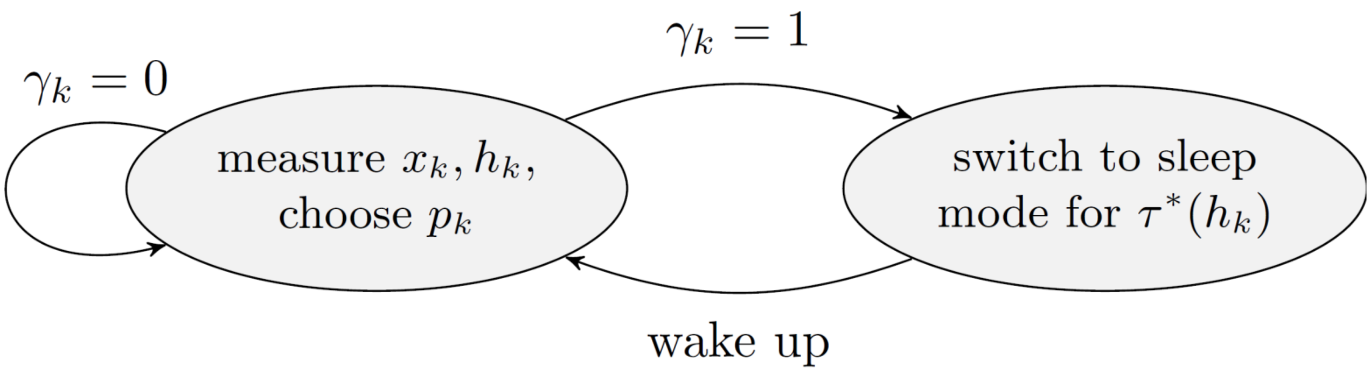


- ➢ Cost independent of plant state : estimation error is reset on every transmission
- ➢ Sleep-time need only depend on channel state : predict when channel suitable and estimation error not too large
- ➢ Optimal computed by analogy to a MDP (tractable for finite channel states)

Proposed Protocol

Improvement to optimal self-triggered

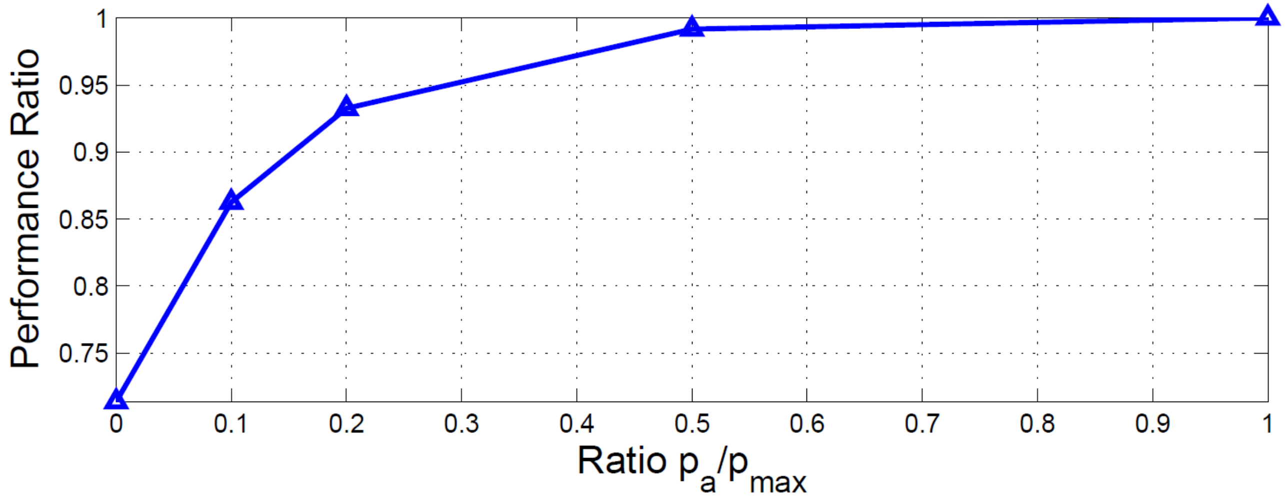
- Proposed protocol – model predictive



- Upon wake-up decide whether to transmit & sleep according to optimal self-triggered, or skip current step
- Current decision based on modeling future behavior & cost
- Guaranteed to perform not worse than optimal self-triggered
- Injects event-triggered steps between sleep

Protocol Performance Comparison

- Ratio of proposed protocol / optimal self-triggered as receiver's constant power increases



➢ If power for receiver to stay awake dominates power for transmitter to communicate, self-triggered performs best

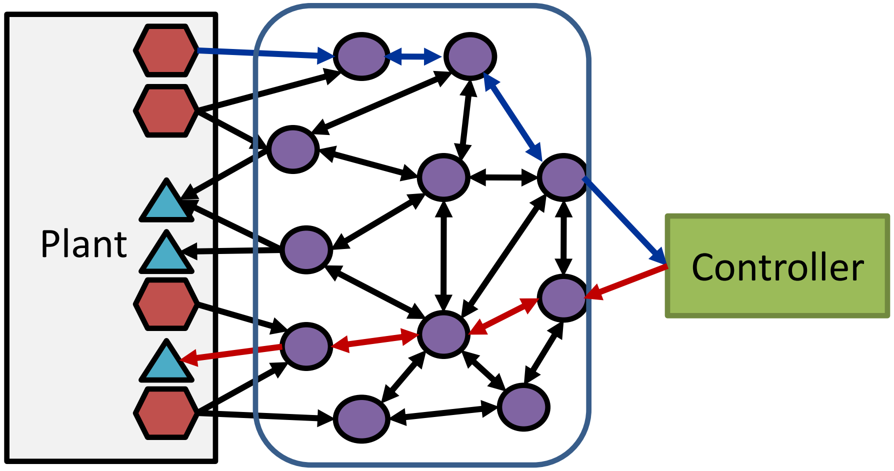
Summary & Future Work

- New Paradigm for Control/ Wireless Networking
  - Model capturing explicitly wireless fading channel effects and power allocation & interaction with control task
  - Novel Physical Layer design: Characterization of optimal power adaptation to channel & plant conditions
  - Receiver power considerations via a coordination protocol

- Future work
  - Medium Access Control for multiple closed-loops over a shared wireless channel
  - Control-aware Resource Allocation, e.g. scheduling, power, in wireless networked control systems

Control with multi-hop networks

- Control with multi-hop wireless networks*

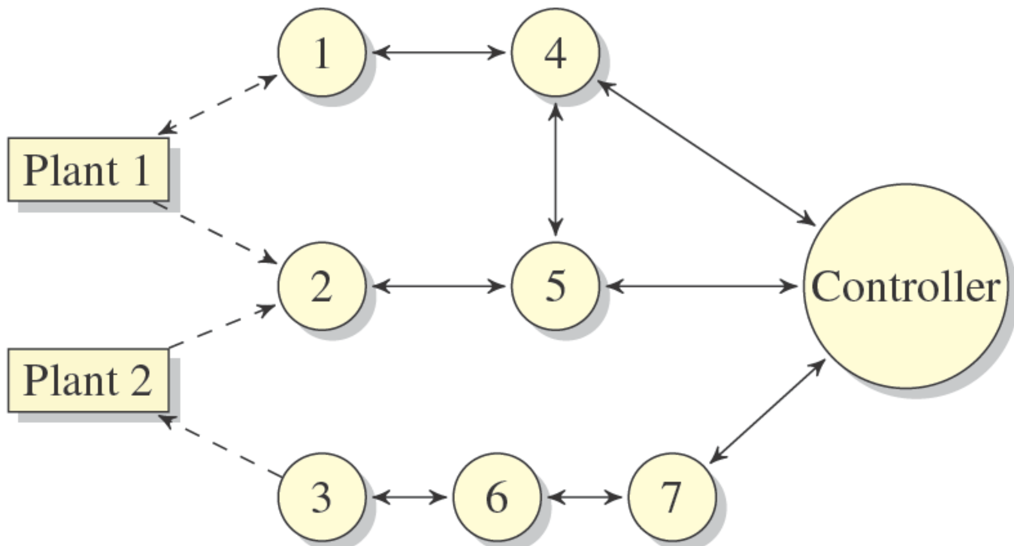


  - **Formal modeling**
  - Analysis & synthesis
  - Compositional analysis
  - Industrial case study

*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, October 2011

Control with multi-hop networks: Modeling

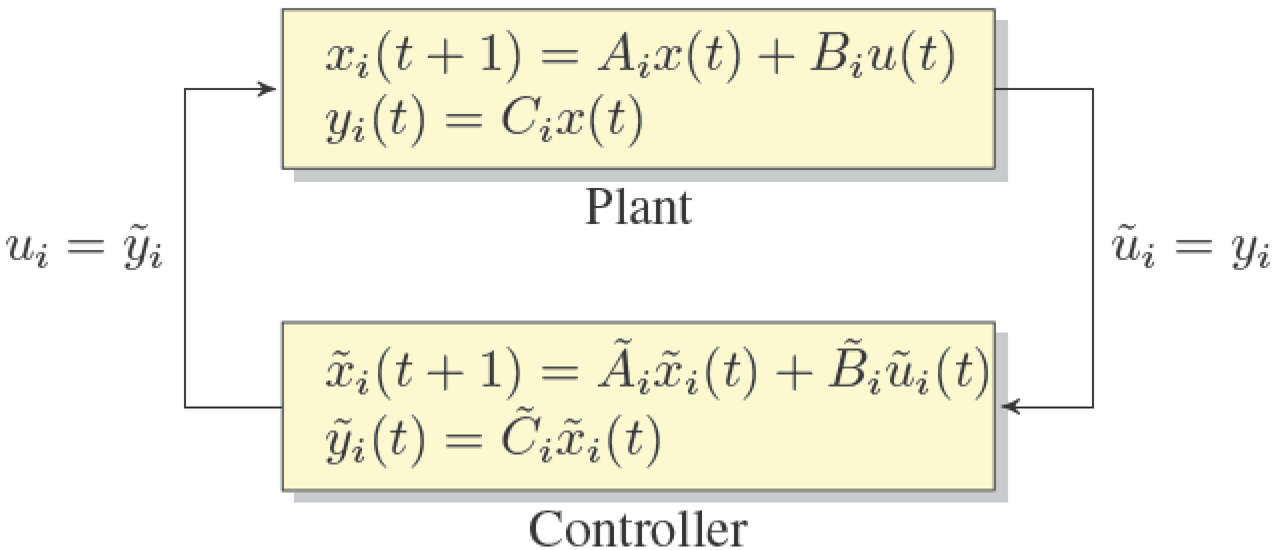
- A multi-hop wireless networked system



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

Control with multi-hop networks: Modeling

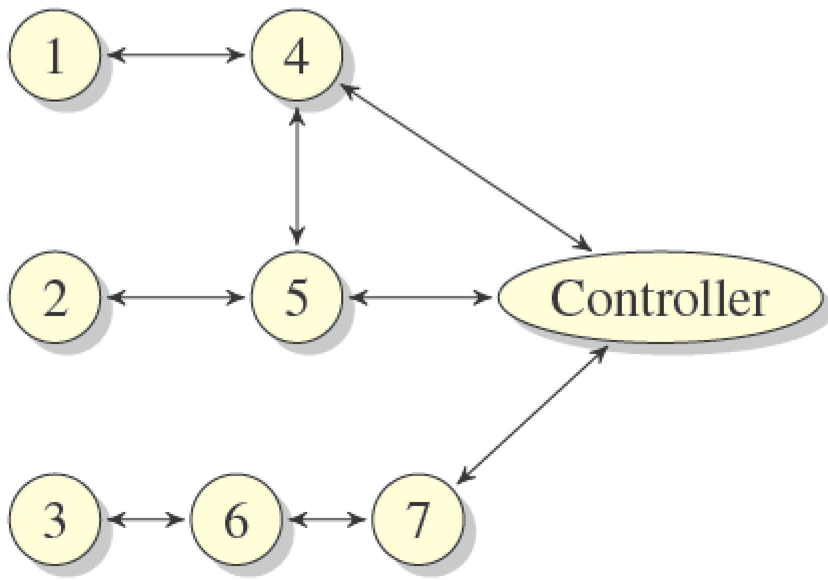
- Plants/controllers are discrete-time linear systems



- Controllers are designed to achieve suitable performance

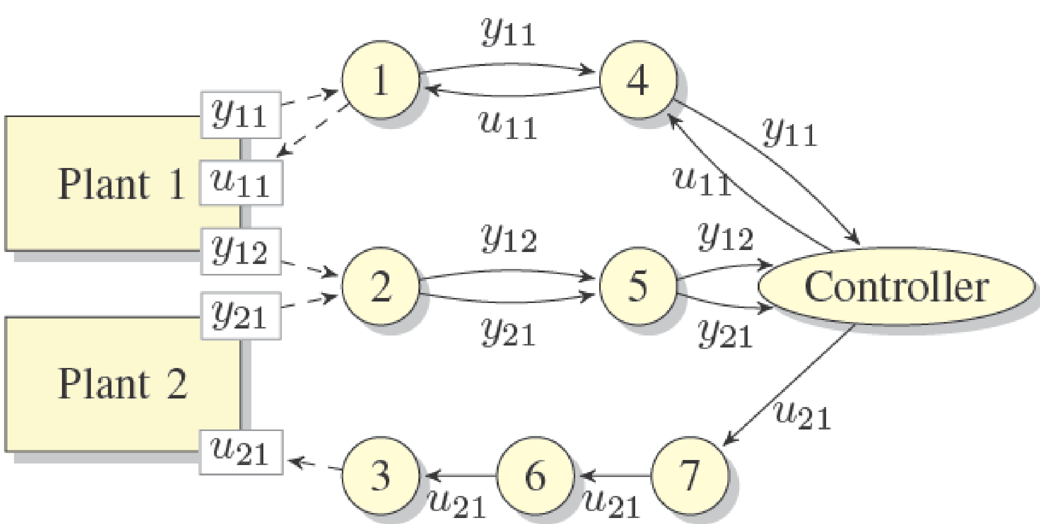
Control with multi-hop networks: Modeling

- 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

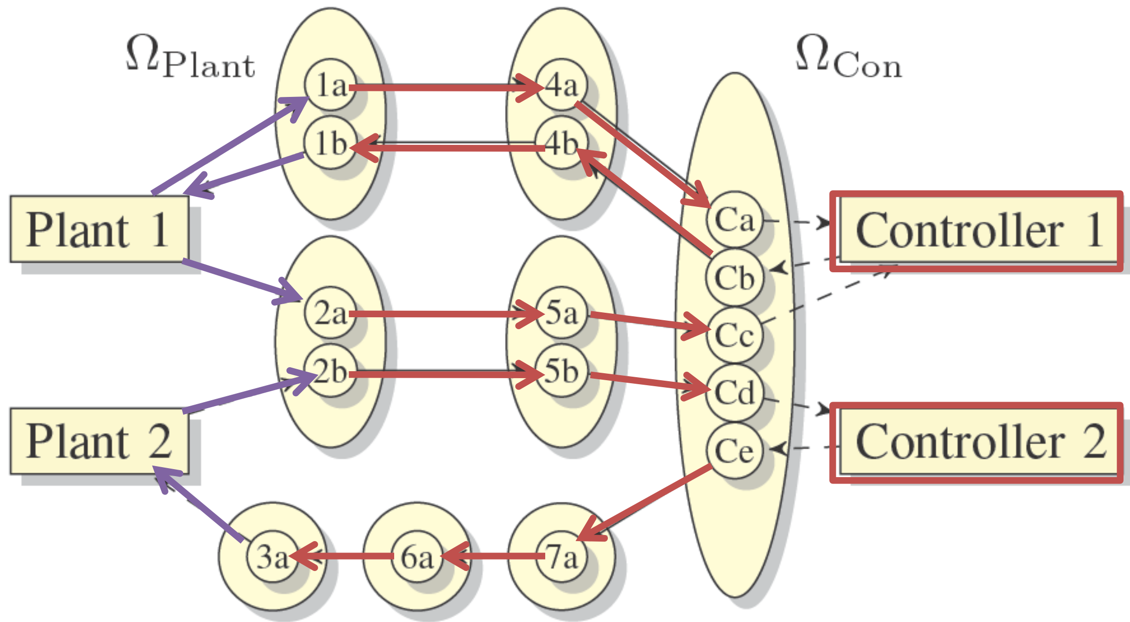


Control with multi-hop networks: Modeling

- 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 ∪ O → 2V*\{Ø} associates to each pair sensor-controller or controller-actuator a set of allowed routing paths

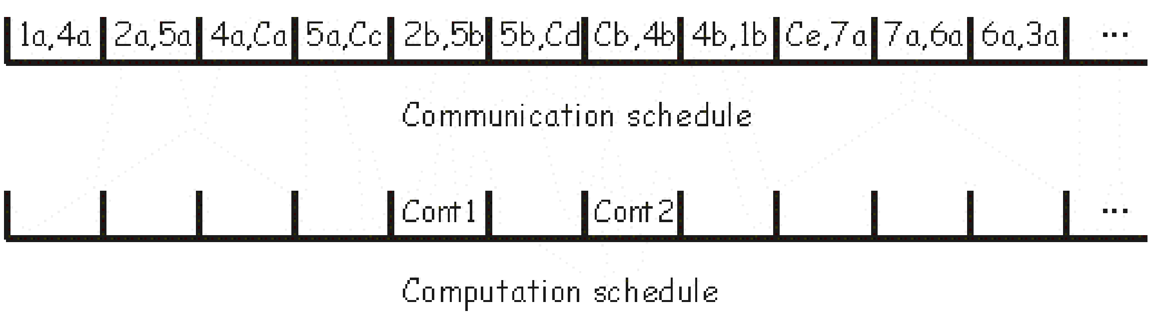


Communication and computation schedule

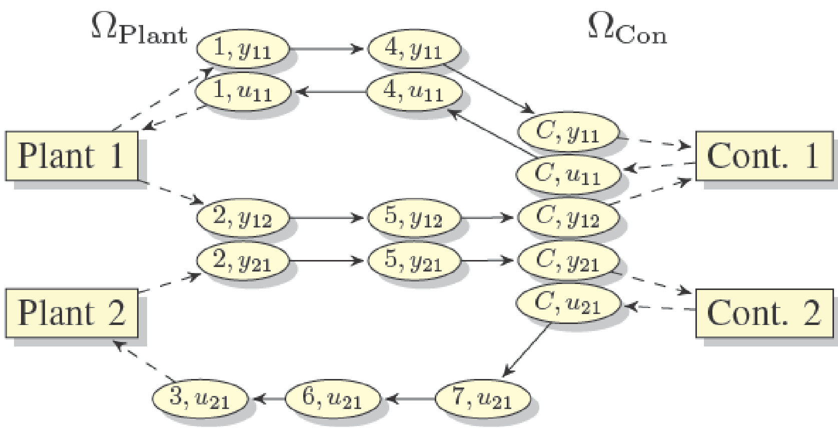


Communication schedules: $\eta : \mathbb{N} \rightarrow 2^{E \times (\mathbb{I} \cup \mathbb{O})}$

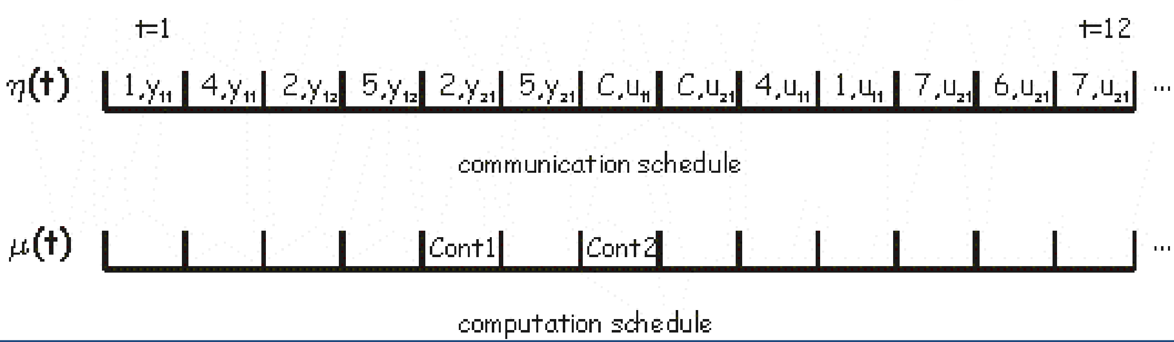
Computation schedules: $\mu_i : \mathbb{N} \rightarrow \{\text{Idle, Active}\}$



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

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

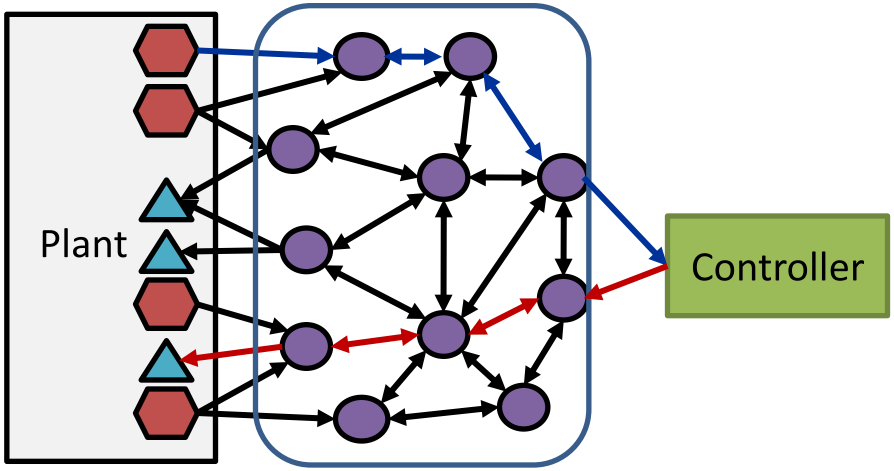
where the schedule (discrete switching signal) is either:

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

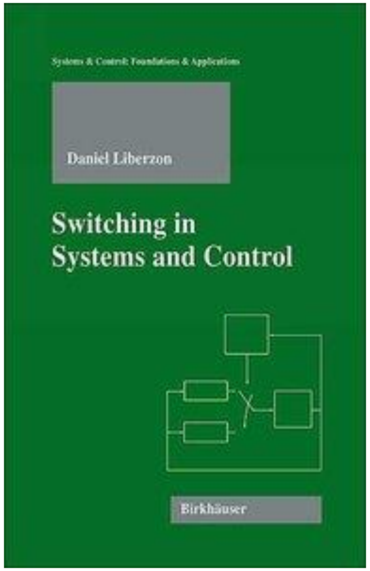
- Control with multi-hop wireless networks



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

Analysis of multi-hop control networks

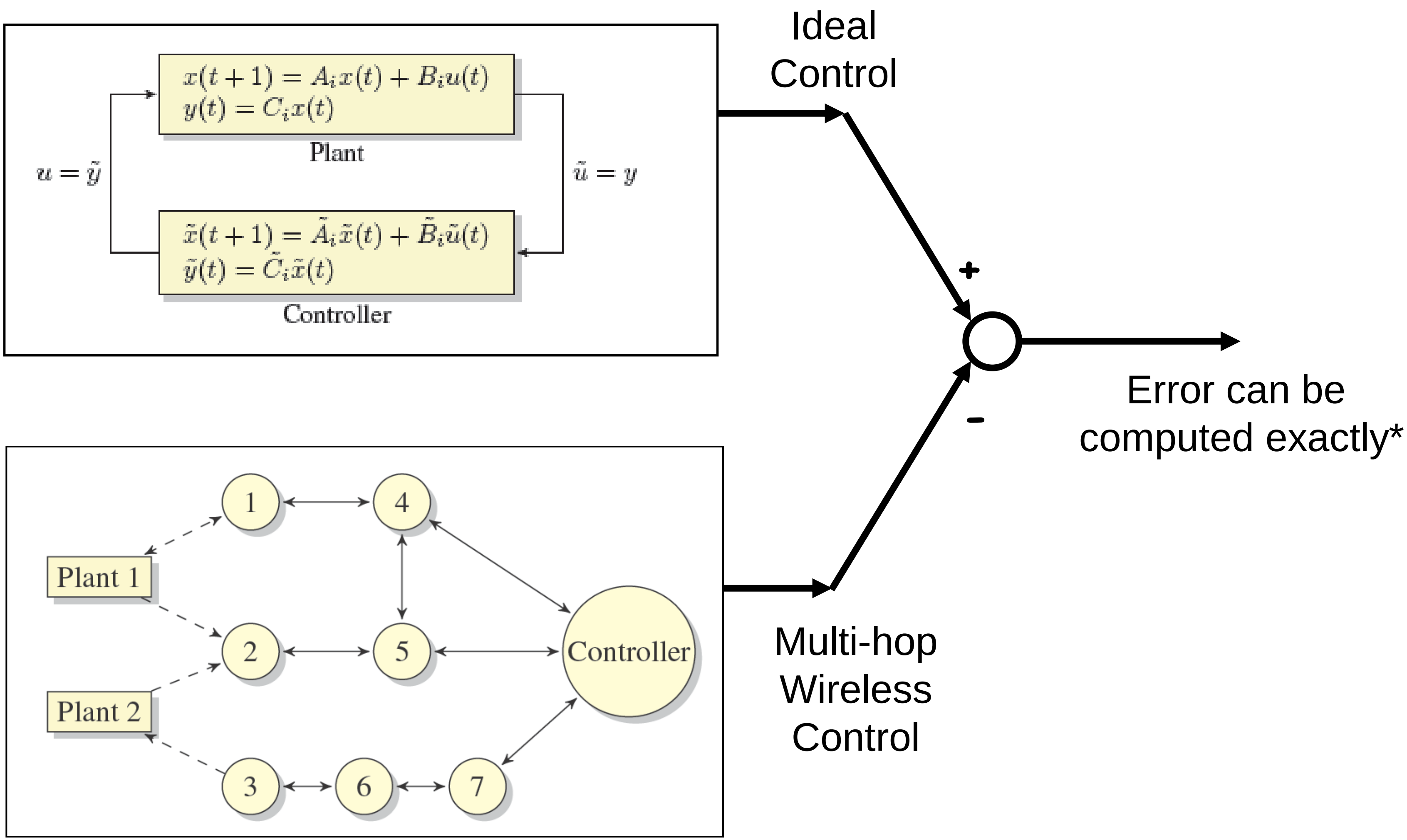
- Periodic deterministic schedule (static routing, no TX errors):
  - Theory of periodic time varying linear systems applies
  - Schedule is a fixed string in the alphabet of edges/controllers
  - Nghiem, Pappas, Girard,Alur – EMSOFT 2006, ACM TECS 2012



- 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

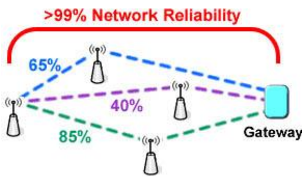
- Stochastic analysis (stochastic packet loss, failures):
  - Theory of discrete time Markov jump linear systems applies
  - Schedule is a Markov Chain over edges/controllers
  - Alur, D'Innocenzo, K.H. Johannsson, Pappas, Weiss, IEEE CDC 2009, IEEE TAC 2011

Periodic deterministic schedules



*T. Nghiem, G. Pappas, A. Girard, R. Alur, *Time triggered implementations of dynamic controllers*, ACM Transactions on Embedded Computing Systems, 2012, In press

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

$$P_{stable}\ {}^{3}\ a$$

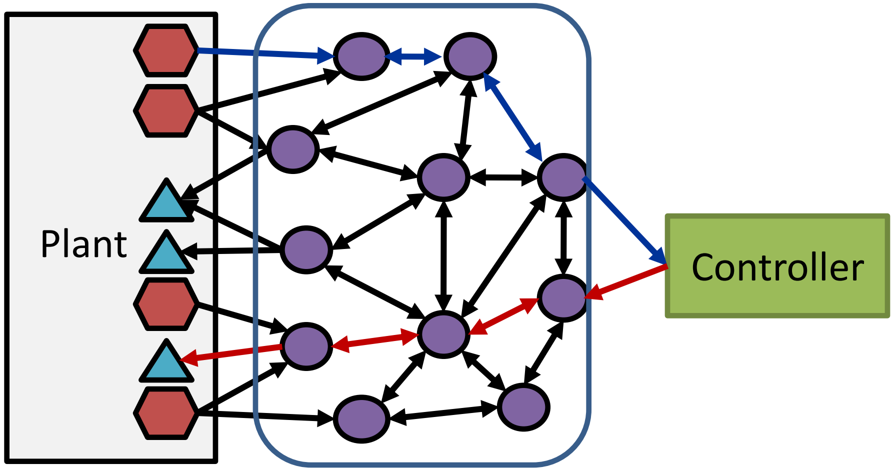
where P_{stable} - probability that the multi-hop control is stable.

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

Works for small networks/control loops

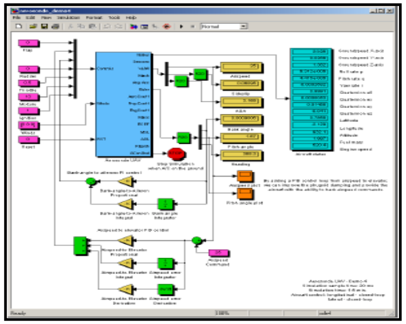
Control with multi-hop networks

- Control with multi-hop wireless networks



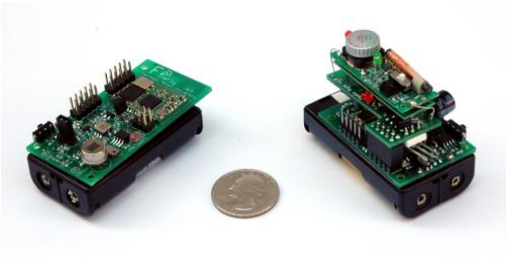
  - Formal modeling
  - Analysis & synthesis
  - **Compositional analysis**
  - Industrial case study

Interfaces for compositional control



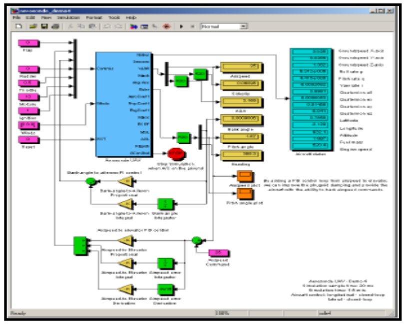
<u>Control Design</u>
Sampling frequency
Delays, jitter

<u>Problems</u>
Impact of scheduling on control
Composing schedules



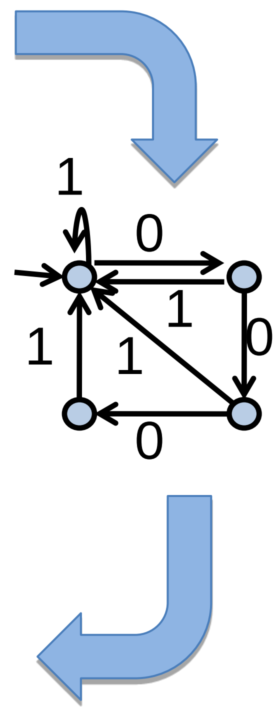
<u>Scheduling</u>
WCET
RM, EDF

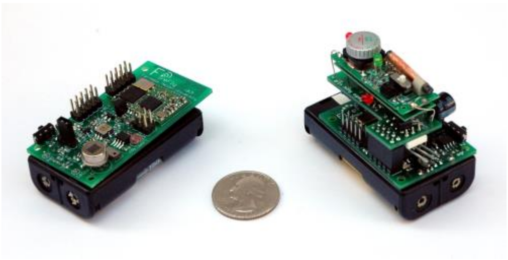
Interfaces for compositional control*



<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 TTA

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

LQR over TTA architectures*

- Consider control plant with resource constraints on actuator

$$\dot{x} = Ax + \left(\sum_{i=1}^{N} \beta_i(t) B_i \right) u(t) + w.$$

- Time-dependent switching signal allows only one actuator active at any time

$$\beta(t) \in \{0,1\}^N \text{ such that } \sum_{i=1}^{N} \beta_i(t) \leq 1$$

- Many related approaches by Hristu/Brockett ‘95, Lincoln and Bernhandnsson 2000, Zhang, Hu, Abate 2010 etc.
- Generally discrete-time, computationally intensive search for switching signal.

*J. Le Ny, E. Feron, and G. J. Pappas, *Resource constrained LQR control under fast sampling*, HSCC 2011

LQR over TTA architectures

- Minimize steady state LQR cost over control input and switching signal

$$J_T(\beta, u) = \frac{1}{T} E\left\{ \int_0^T x^T Q x + \left(\sum_i \beta_i(t) u^T R_i u \right) dt + x^T(T) Q_f x(T) \right\}$$

$$J(\beta, u) = \lim \sup_{T \to \infty} J_T(\beta, u)$$

- Subject to constraints

$$\dot{x} = Ax + \left(\sum_{i=1}^{N} \beta_i(t) B_i \right) u(t) + w.$$

$$\beta(t) \in \{0, 1\}^N \text{ such that } \textstyle\sum_{i=1}^{N} \beta_i(t) \leq 1$$

Key technical ideas

- Given switching signal and T, LQR controller is optimal. Hence

$$J(\beta) = \lim_{T\to\infty} \sup J_T(\beta) = \lim_{T\to\infty} \sup \frac{1}{T}\int_0^T \mathrm{Tr}[P_\beta(t;T)W]\, dt$$

- Optimize above cost over steady-state average utilizations per input

$$b_i \quad \longleftrightarrow \quad \lim_{T\to\infty} \sup \frac{1}{T}\int_0^T \beta_i(t)dt$$

- We are keeping average utilization but we are ignoring order

Performance bounds over average utilization

- Compute performance bound using semi-definite programming

$$\min_{X \succ 0, \{b_i\}_{1 \leq i \leq N}} \quad \mathrm{Tr}[X^{-1} W]$$

$$\text{s.t.} \quad XA^T + AX - \left(\sum_{i=1}^{N} b_i B_i R_i^{-1} B_i^T \right) + XQX \preceq 0$$

$$\sum_{i=1}^{N} b_i \leq 1, \quad 0 \leq b_i, i = 1, \ldots, N.$$

- Optimize above cost over steady-state average utilizations per input

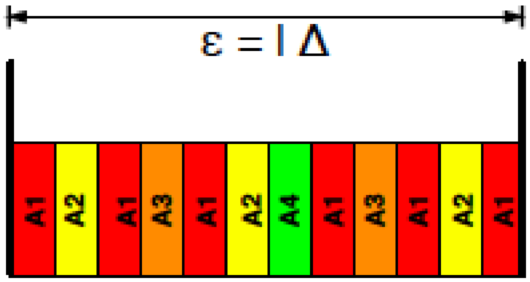
- Theorem (HSCC 2011): In the limit of arbitrarily fast switching , these policies are asymptotically optimal.

Time-triggered approximations to LQR

- For simple system with three inputs, SDP provides optimal utilization rates

$$b_1 \approx 0.54, b_2 \approx 0.44, b_3 \approx 0.02$$

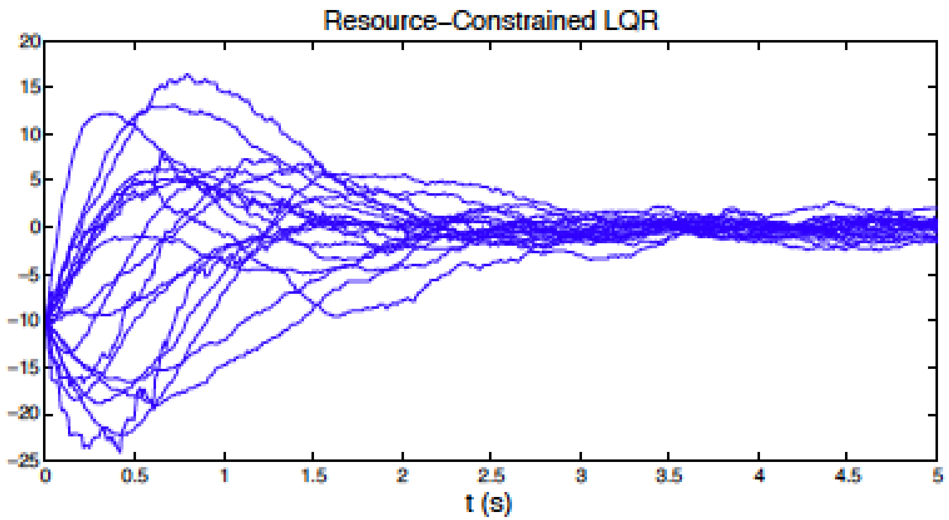
- Approximate optimal utilization rates

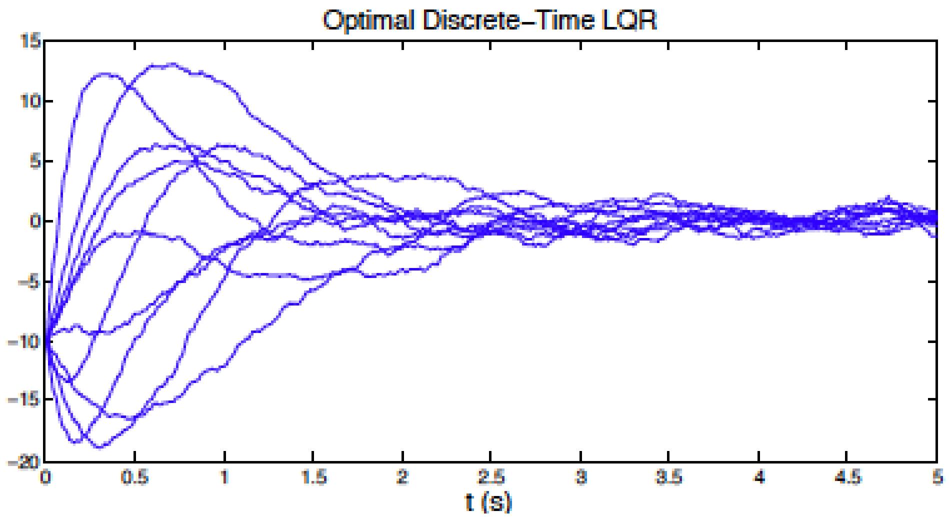


$$b_i \approx \frac{l_i}{l}, \quad i = 1, \ldots, N, \sum_{i=1}^{N} l_i \leq l$$

- In a schedule of 100 slots, 54 slots go to input 1, 44 to input 2, etc
- Tradeoff between length of schedule and approximation of utilization

Sample system realizations (10ms slots)





Control specifications as automata

- Stability Control Specifications

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

→ Automata specifying schedules that guarantee performance

- Periodic Control Specifications on TT

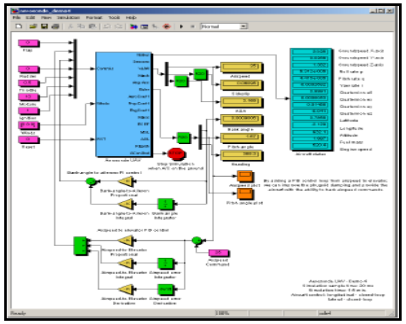
Sample every 100 seconds

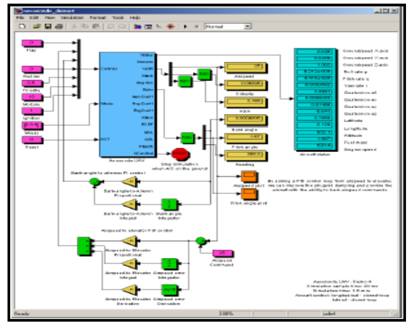
If not sampled in the last 200 seconds, sample every 10 seconds for the next minute

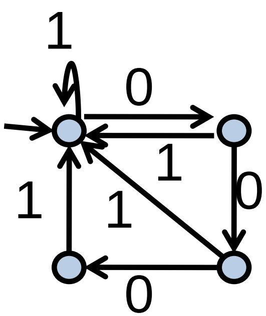
Specifications of maximal time delays between events

→ Automata that specify valid periodic schedules

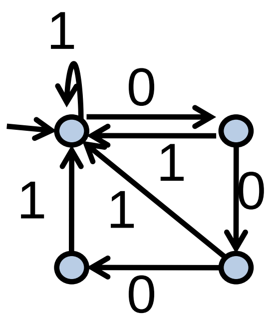
Automata are compositional



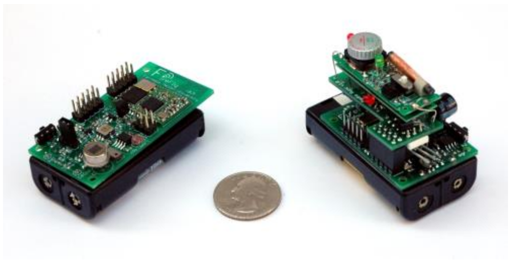




∩



= ?

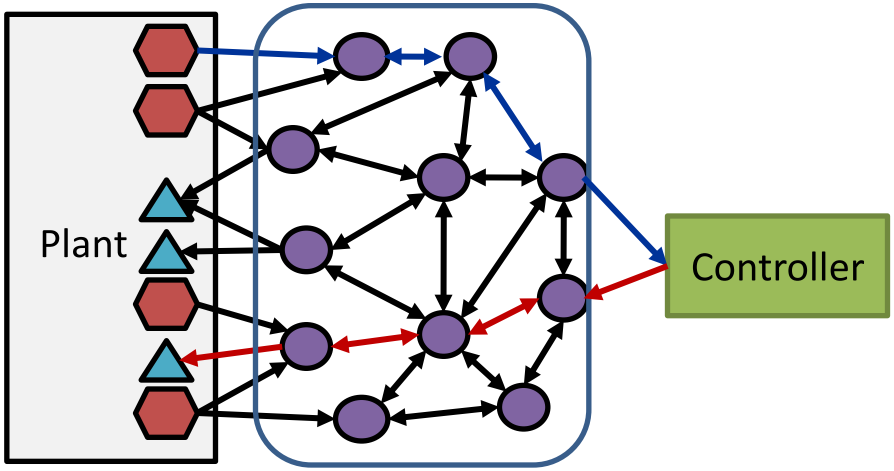


Price of composability

- The more robust the controller, the larger the automaton that can be tolerated with acceptable performance loss.
- The larger the automaton that can tolerated, the more composable our limited resources will be.
- Tradeoff between control performance and composability

Control with multi-hop networks

- Control with multi-hop wireless networks

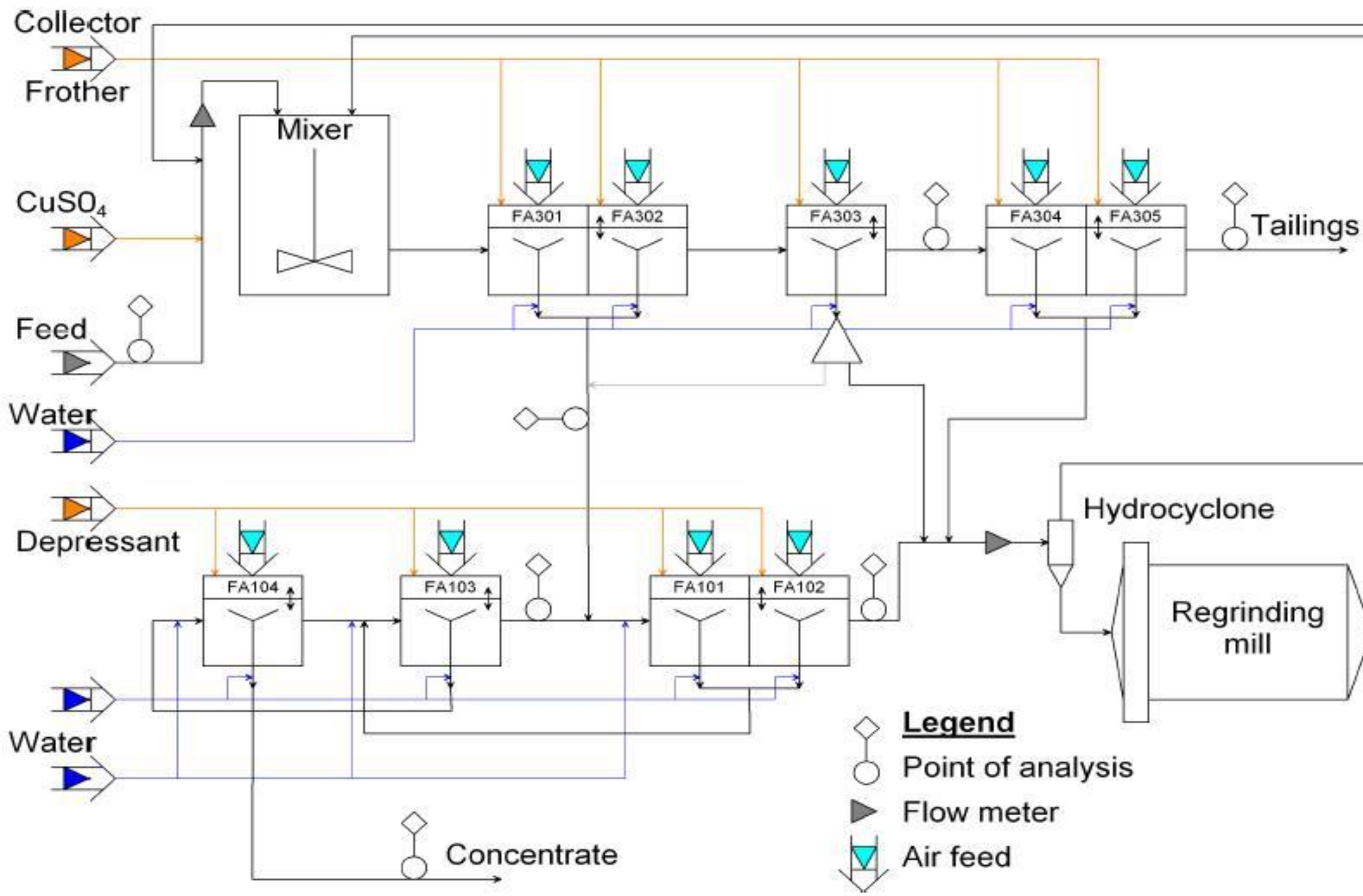


  - Formal modeling
  - Analysis & synthesis
  - Compositional analysis
  - **Industrial case study**

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.

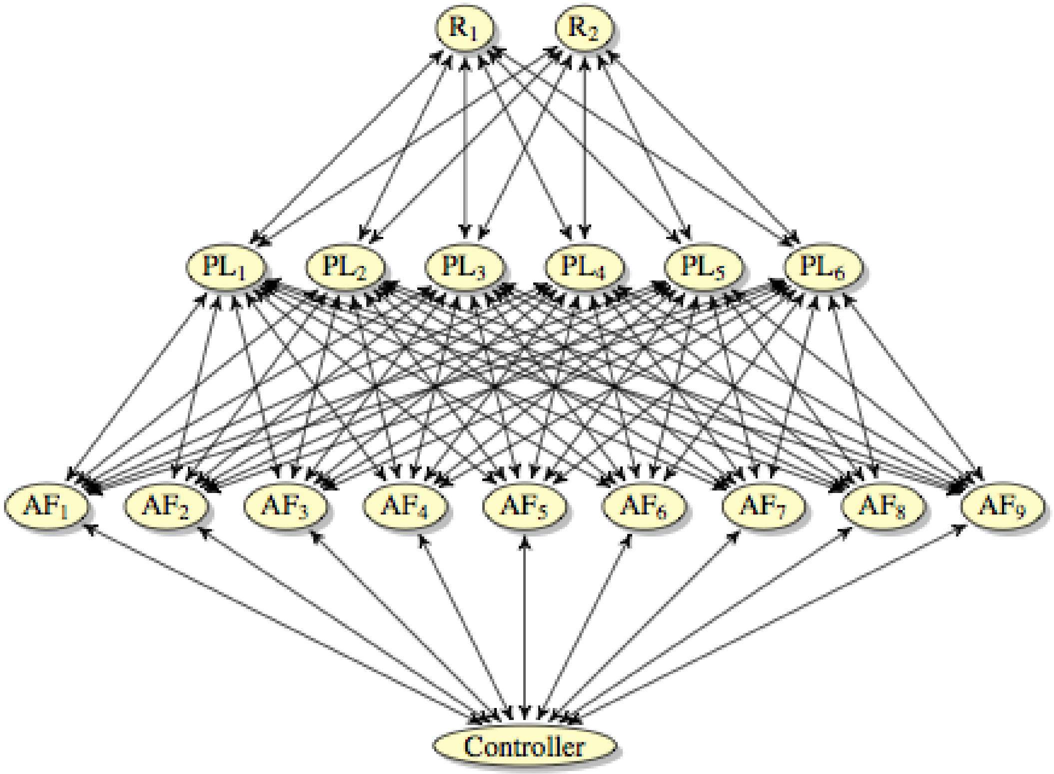
Process Time Scales: Zn Flotation

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

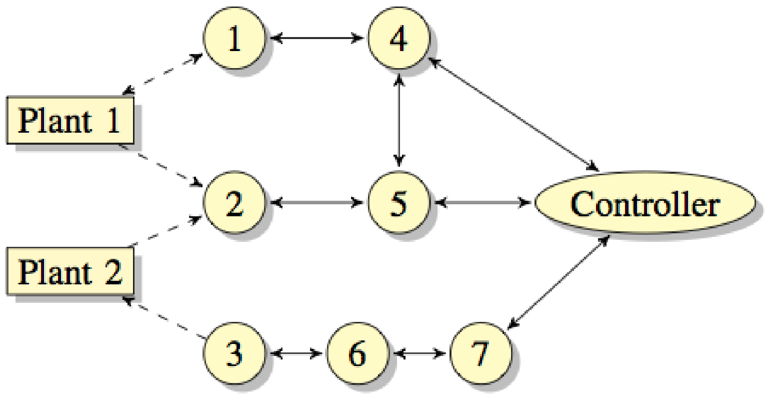
Req. For Plant 2:
e2to5, e5toC, …,e6to3 must be a subsequence of the schedule

```
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;
```

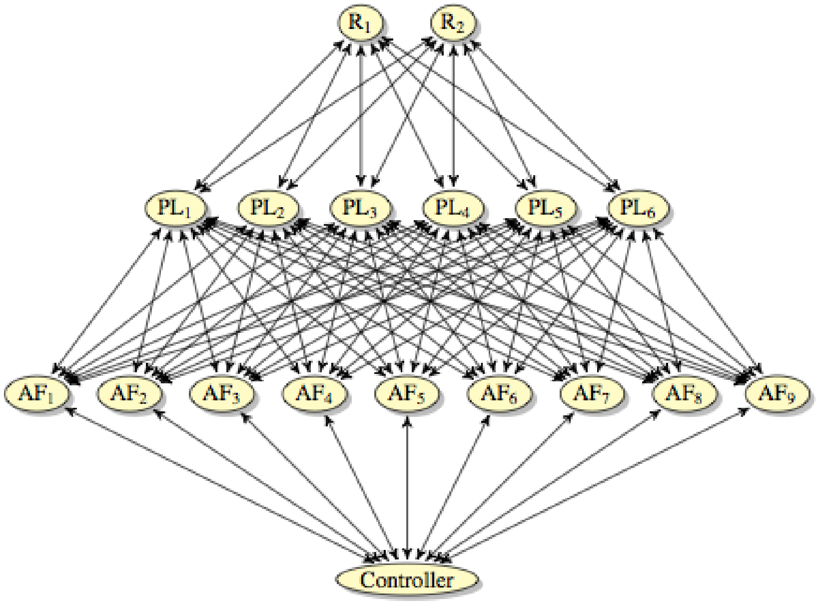
Req. For Plant 1:
more involved because it has two inputs

```
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

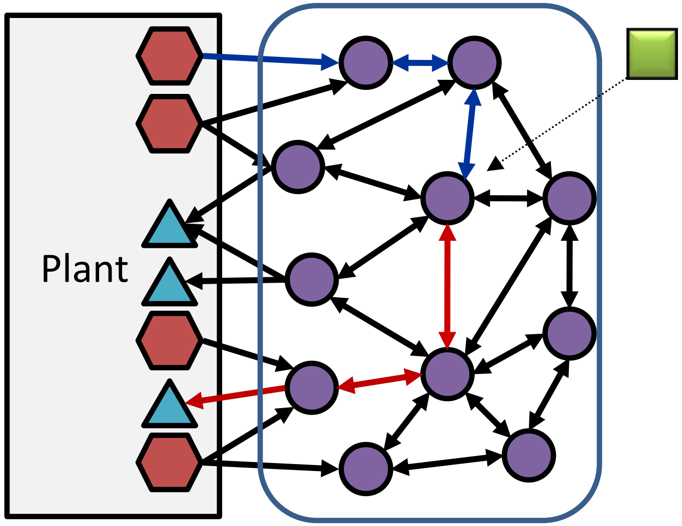
SMV code with 18 modules
272 lines
BDD nodes allocated: 26797

~2 minutes

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

Future challenges

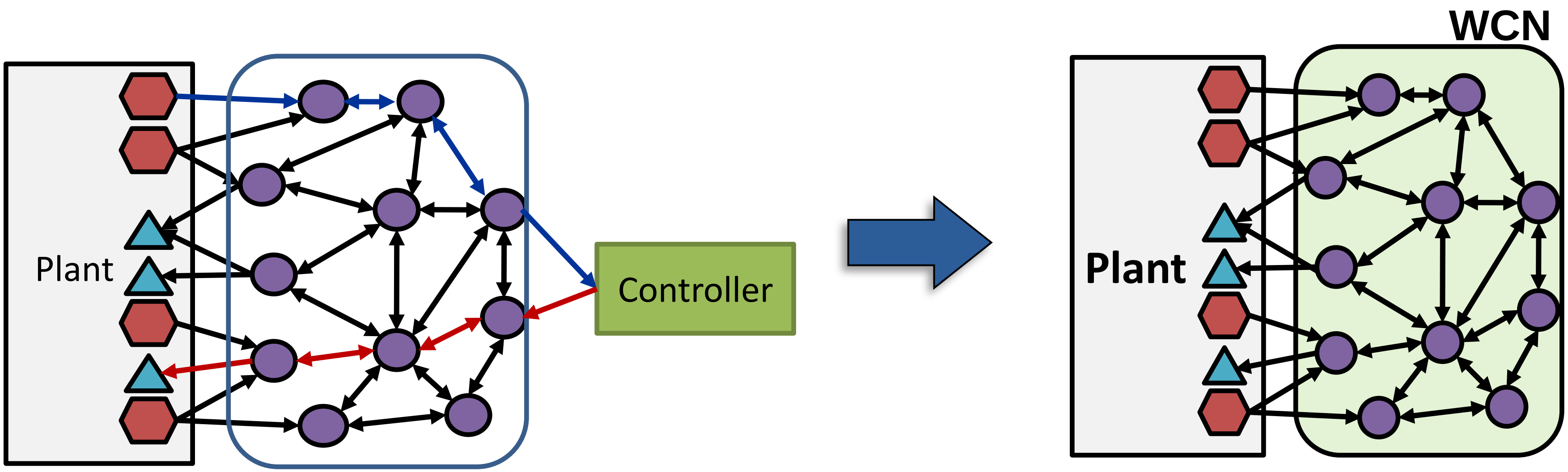
- Time-triggered architectures not optimal for event-based systems
  - Hybrid TDMA/CSMA or LTTA architectures
  - Event-based sensing and control
- Time-synchronization for large networks
  - Model TDMA clock drift using timed automata
  - Scheduling by composing timed-automata
- Wireless models are 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 2012]

The Wireless Control Network (WCN)

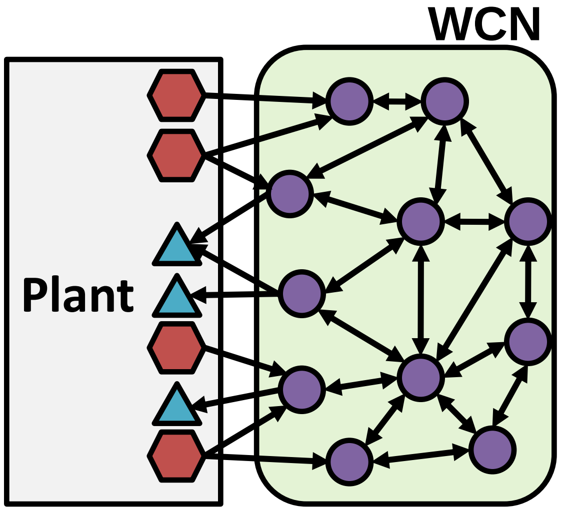
- In multi-hop control, nodes route information to controller



- 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*



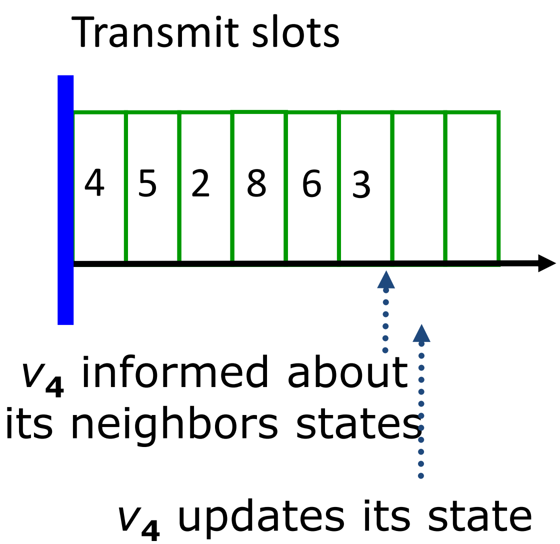
  - **Modeling**
  - Controller synthesis
  - Robustness & security

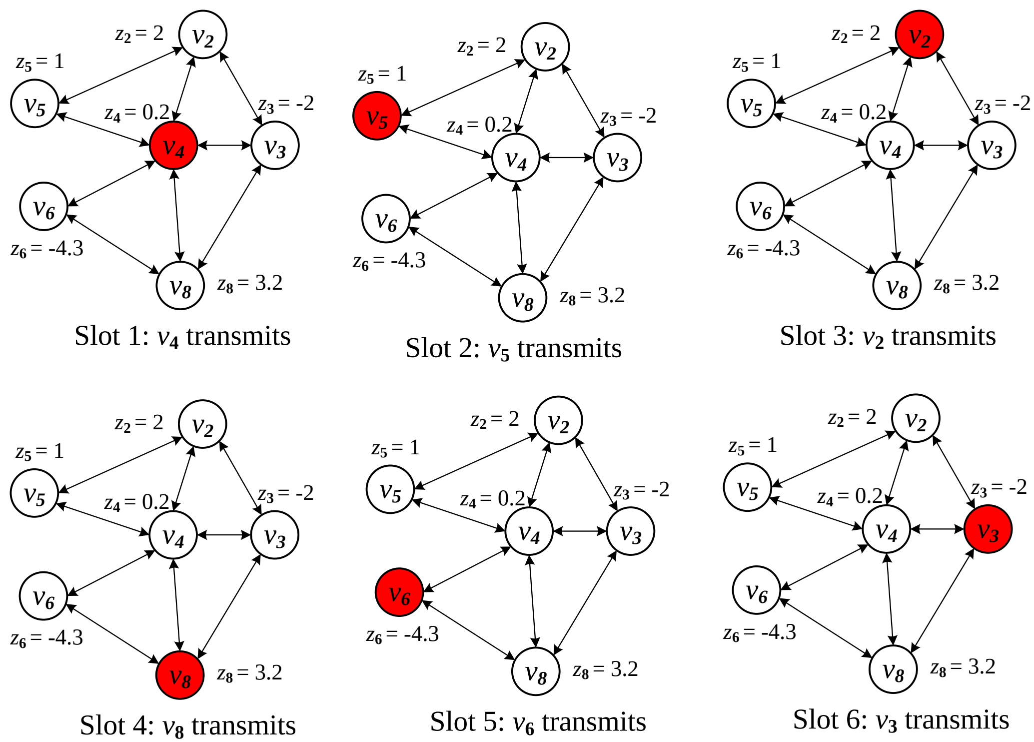
*M. Pajic, S. Sundaram, G. Pappas, R. Mangharam, *Wireless Control Network: A New Approach for Control over Network*, IEEE Transactions on Automatic Control, 2011.
M. Pajic, R. Mangharam, G.J. Pappas, S. Sundaram, Topological Conditions for In-Network Stabilization of Dynamical Systems, IEEE Journal on Selected Areas of Communication, 2013
M. Pajic, S. Sundaram, J. Le Ny, G.J. Pappas , R. Mangharam, Closing the Loop: A Simple Decentralized Method for Control over Wireless Networks, IPSN'12

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

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

- Node state update procedure:

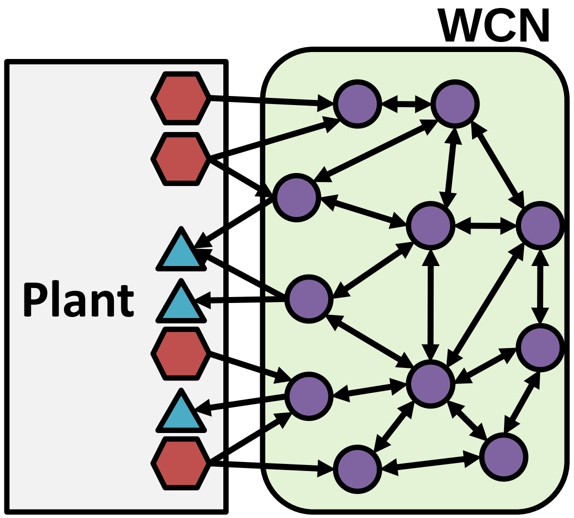
$$z_i[k+1] = w_{ii} z_i[k] + \sum_{v_j \in \mathcal{N}_{v_i}} w_{ij} z_j[k] + \sum_{s_j \in \mathcal{N}_{v_i}} h_{ij} y_j[k]$$

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

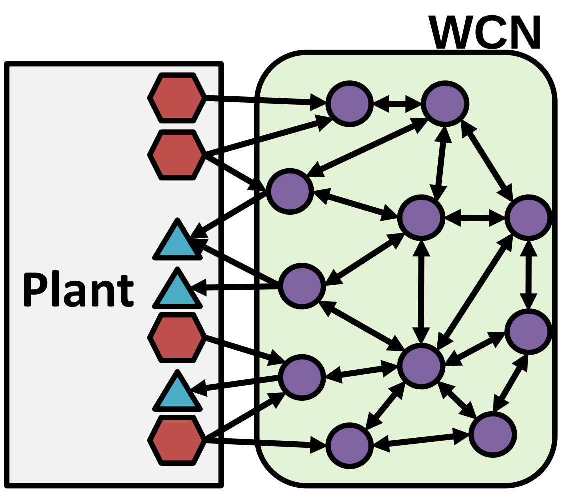


WCN modeling

- 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

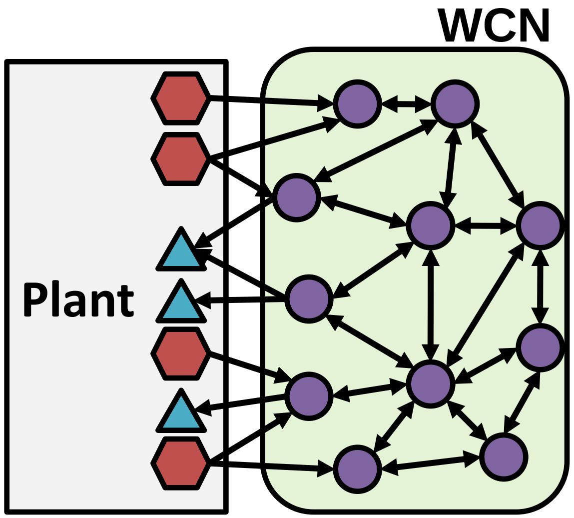
- Overall system state:

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

- Closed-loop system:

$$\hat{\mathbf{x}}[k+1] = \underbrace{\begin{bmatrix} \mathbf{A} & \mathbf{BG} \\ \mathbf{HC} & \mathbf{W} \end{bmatrix}}_{\hat{\mathbf{A}}} \underbrace{\begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix}}_{\hat{\mathbf{x}}[k]} + \underbrace{\begin{bmatrix} \mathbf{B}_w \\ \mathbf{0} \end{bmatrix}}_{\hat{\mathbf{B}}} \mathbf{u}_w$$

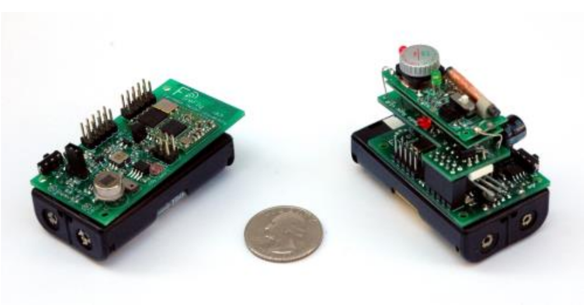
- Matrices W, G, H are structured
- Sparsity constraints imposed by topology!



WCN Advantages: Simple & Powerful

Penn
UNIVERSITY of PENNSYLVANIA

- 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

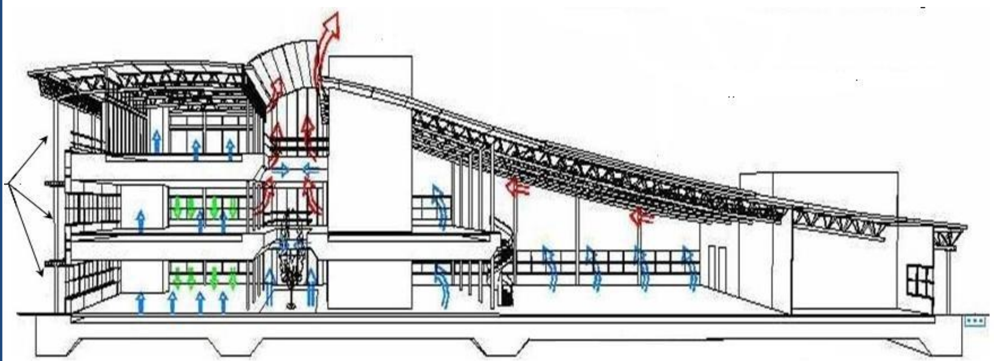


WCN Advantages: Scheduling

- 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



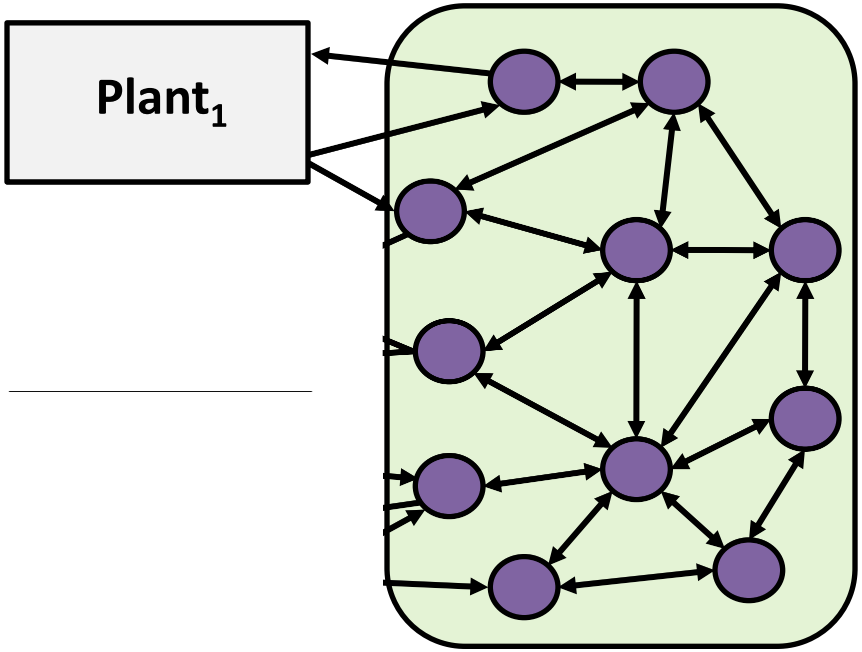
WCN Advantages: Compositionality

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

- WCN configurations can be combined

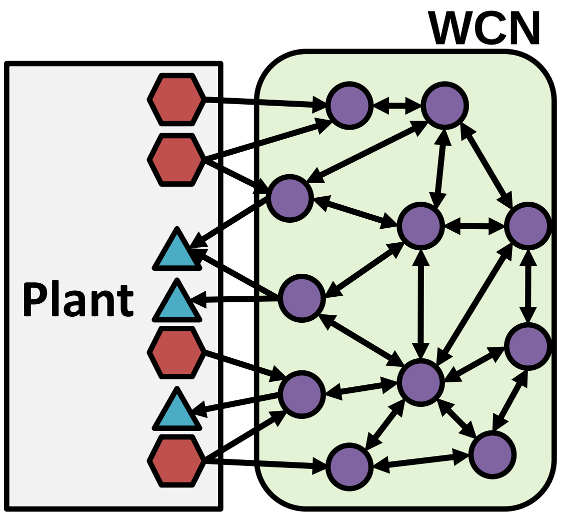
Stable configuration

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



Wireless control network

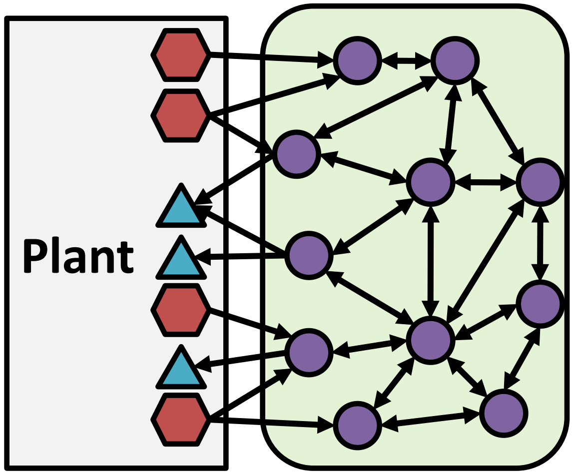
- Wireless control network



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

WCN controller synthesis

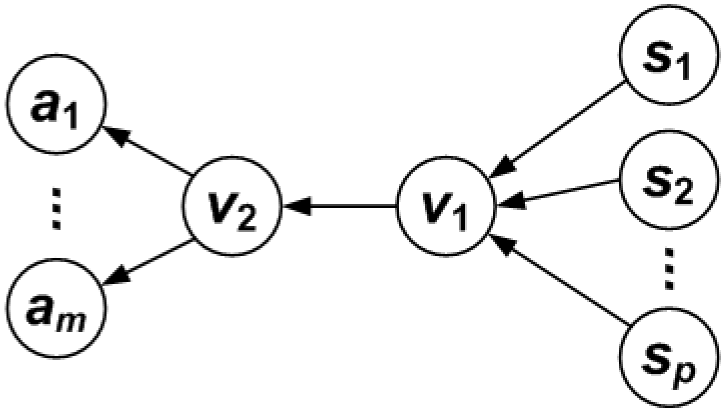
- Use WCN to stabilize the closed-loop system
  - Synthesis of optimal WCN configurations



- 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

Topological conditions for stabilization vs. information transmissions

- The objective of the network is systems stabilization!
- Example:



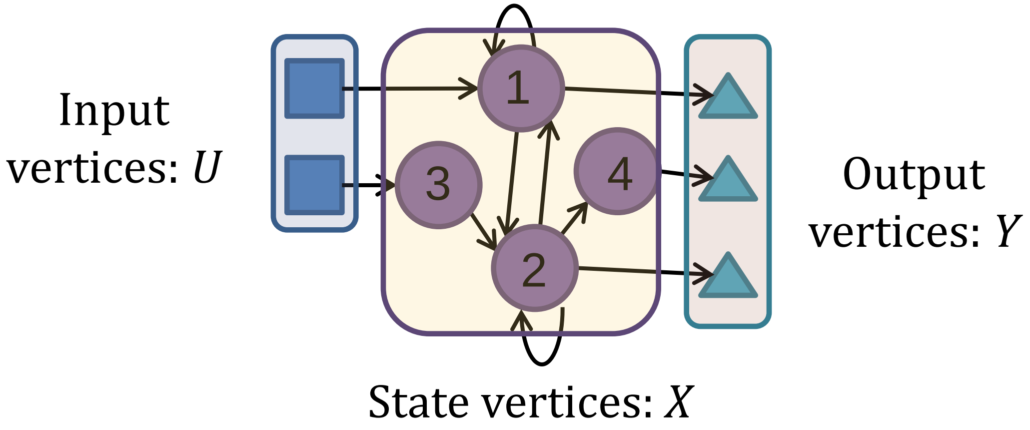
- This network is not capable of delivering all of the source information to all of the sinks at each time-step
- That is not necessarily a cause for concern when the main objective is to stabilize the system.

WCN topological conditions

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

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

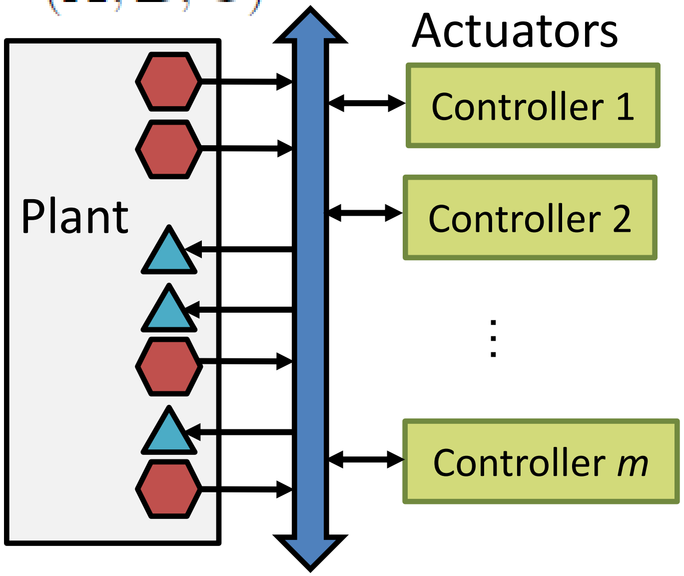
- Associated graph H



- Properties of graph are generic properties of structured system

A small detour into decentralized control…

$\Sigma = (\mathbf{A}, \mathbf{B}, \mathbf{C})$



Decentralized control system

From feedback patterns $J_1, J_2, \ldots, J_m$

$$\mathbf{K}_f = \{\mathbf{K} \in \mathbb{R}^{m \times p} | k_{ij} = 0 \text{ if } j \notin J_i\}$$

Fixed Modes [Wang & Davison, 1973; Siljak, 1981]

$$\Lambda_f = \bigcap_{\mathbf{K} \in \mathbf{K}_f} \Lambda(\mathbf{A} + \mathbf{BKC})$$

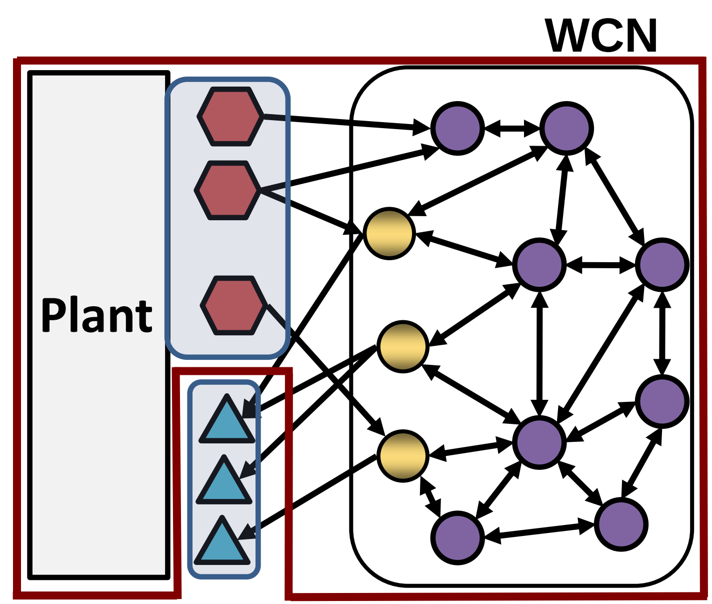
Indicate whether the system can be stabilized

New closed-loop system model

The plant ↔ network model

$$\hat{\mathbf{x}}[k+1] = \begin{bmatrix} \mathbf{x}[k+1] \\ \mathbf{z}[k+1] \end{bmatrix} = \underbrace{\begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{HC} & \mathbf{W} \end{bmatrix}}_{\tilde{\mathbf{A}}} \begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix} + \underbrace{\begin{bmatrix} \mathbf{B} \\ \mathbf{0} \end{bmatrix}}_{\tilde{\mathbf{B}}} \mathbf{u}[k]$$

$$\hat{\mathbf{y}}[k] = \underbrace{\begin{bmatrix} \mathbf{0} & \mathbf{E}_{\mathcal{V}_A} \end{bmatrix}}_{\tilde{\mathbf{C}}} \begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix},$$



New plant: Plant & WCN

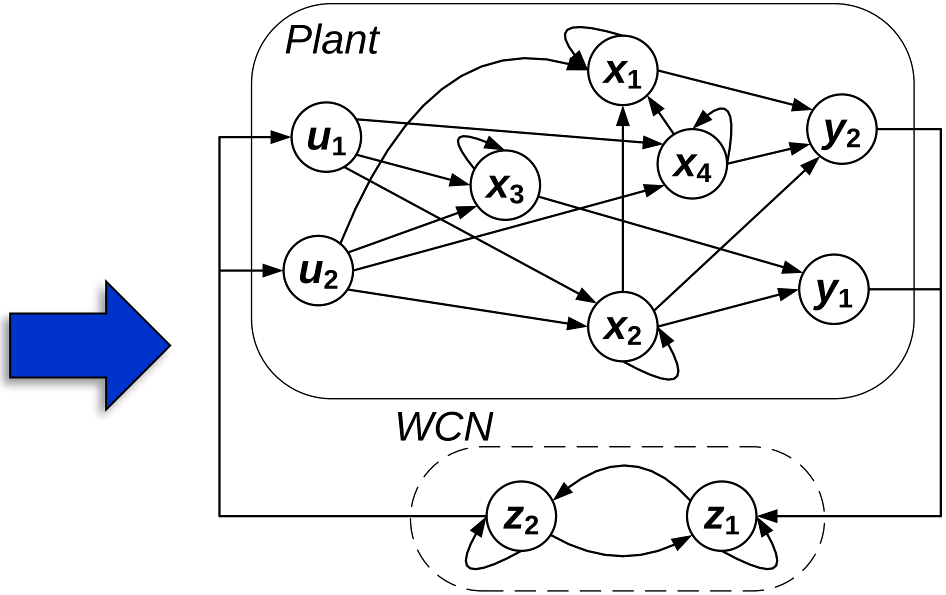
Controlled by controllers at the actuators

WCN topological conditions

- Use structured system theory and decentralized control on the 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

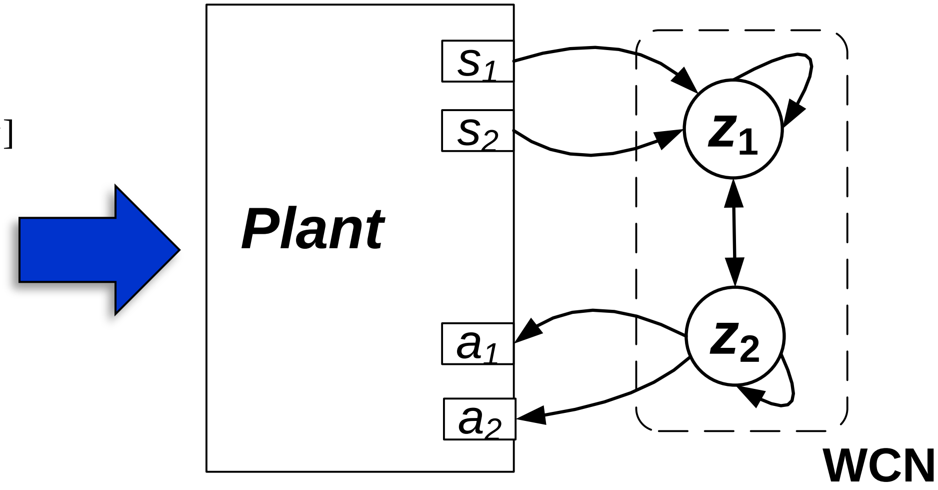
then there exists a stabilizing configuration for WCN

WCN topological conditions

- Use structured system theory on WCN and network

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

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



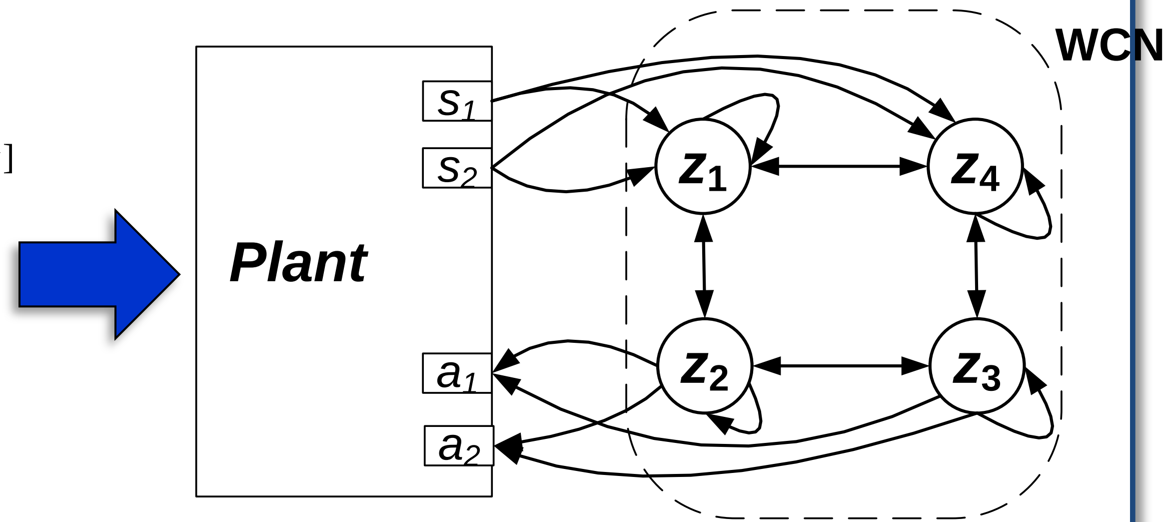
- We **cannot** stabilize with with 2 nodes!

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,

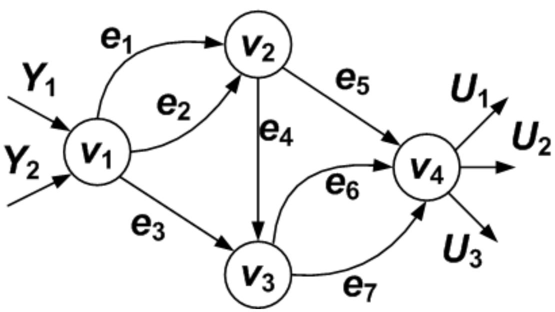
then it can be stabilized with a strongly connected network, where each sensor and actuator is connected to the network.

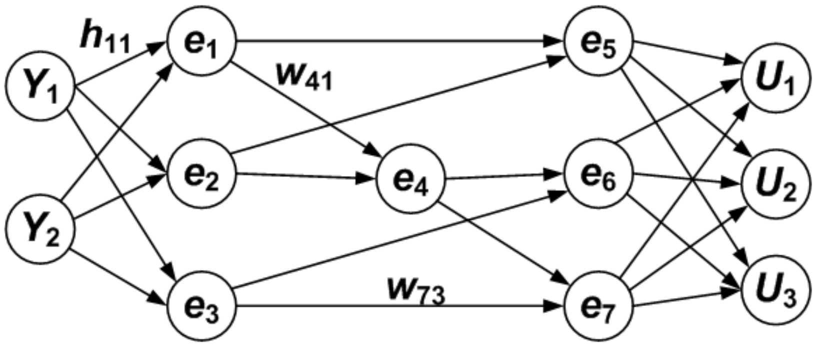
Generic condition!

Topological conditions for point-to-point networks

- **Problem:** network synthesis for stabilization when ***network coding over point-to-point communication links*** is used

- Example: Point to point communication in a simple network





Direct labeled line graph

- Algebraic approach to network coding (Koetter, Medard, 2005)
  - each link in the initial graph is mapped to a unique vertex in the line graph

- The labeled line graph directly corresponds to the WCN model!

Topological conditions for point-to-point networks

- Consequently, the same reasoning can be used for point-to-point networks

Sufficient condition when point-to-point networks with linear network coding are used for communication:

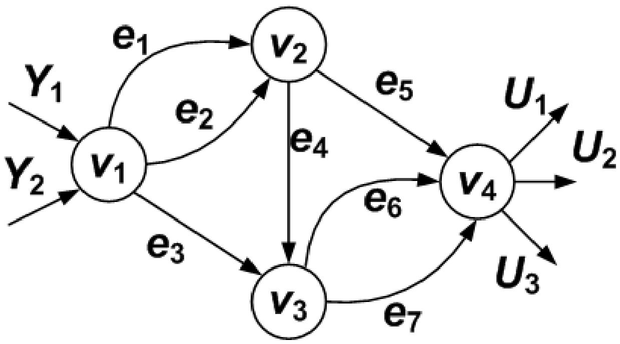
Let *d* denote the largest geometric multiplicity of any unstable e-value of a detectable and stabilizable plant. If ***edge connectivity*** of the network **between sensors and actuators** is at least *d* then the system can be stabilized using dynamic compensators at actuators.

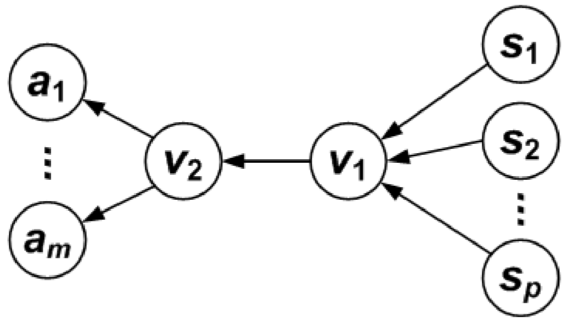
The equivalent generic condition also holds!

Topological conditions for point-to-point networks

- Problem: network synthesis for stabilization, in the case where ***network coding over point-to-point communication links*** is used

- Examples: Point-to-point communication in simple networks



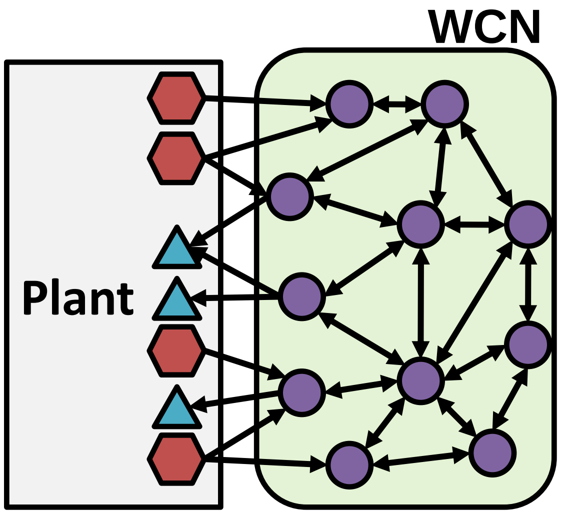


Stabilizable for d≤3

Stabilizable for d≤1

WCN controller synthesis

- Use WCN to stabilize the closed-loop system



- For a specific WCN network topology
  - How to stabilize the closed-loop system

Stabilizing the Closed-Loop System

- Problem: Find numerical matrices **W, H, G** satisfying structural constraints such that

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

- Solution: Formulate Lyapunov function and try to solve using Linear Matrix Inequalities (LMIs)
  - Find positive definite matrix P such that

$$\mathbf{P} - \hat{\mathbf{A}}^T \mathbf{P} \hat{\mathbf{A}} > 0$$

Stabilizing the Closed-Loop System

- Schur complement:

$$\begin{matrix} \mathbf{Q} - \mathbf{R}^{\mathrm{T}}\mathbf{S}^{-1}\mathbf{R} > 0 \\ \mathbf{S} > 0 \end{matrix} \Leftrightarrow \begin{bmatrix} \mathbf{Q} & \mathbf{R}^{\mathrm{T}} \\ \mathbf{R} & \mathbf{S} \end{bmatrix} > 0$$

- Standard application to stability:

$$\mathbf{P} - \hat{\mathbf{A}}^T\mathbf{P}\hat{\mathbf{A}} > 0 \Leftrightarrow \mathbf{P} - \hat{\mathbf{A}}^T\mathbf{P}\mathbf{P}^{-1}\mathbf{P}\hat{\mathbf{A}} > 0$$

$$\Leftrightarrow \begin{bmatrix} \mathbf{P} & \hat{\mathbf{A}}^T\mathbf{P} \\ \mathbf{P}\hat{\mathbf{A}} & \mathbf{P} \end{bmatrix} > 0$$

  - Bilinear matrix inequality (free variables in $\hat{\mathbf{A}}$ multiply free variables in **P**)
  - Not a problem when **W**, **H** and **G** are unstructured -> a change of variables produces an LMI

Stabilizing the Closed-Loop System

- Change of variables no longer works when $\hat{\mathbf{A}}$ is structured

- Alternative approach [*de Oliveira et. al*, CDC'00]:

$$\mathbf{P}-\hat{\mathbf{A}}^T\mathbf{P}\hat{\mathbf{A}}>0 \Leftrightarrow \begin{bmatrix} \mathbf{P} & \hat{\mathbf{A}}^T \\ \hat{\mathbf{A}} & \mathbf{P}^{-1} \end{bmatrix} > 0$$

linear in $\hat{\mathbf{A}}$

$$\Leftrightarrow \begin{bmatrix} \mathbf{P} & \hat{\mathbf{A}}^T \\ \hat{\mathbf{A}} & \mathbf{Q} \end{bmatrix} > 0, \quad \boxed{\mathbf{QP}=\mathbf{I}}$$

nonconvex constraint

- Problem is still nonconvex,
  - This form appears frequently in design of static output feedback controllers

Stabilizing the Closed-Loop System

- Various methods developed to deal with constraint **QP = I**

- Use approach by [*El Ghaoui et al., TAC, 1997*]:

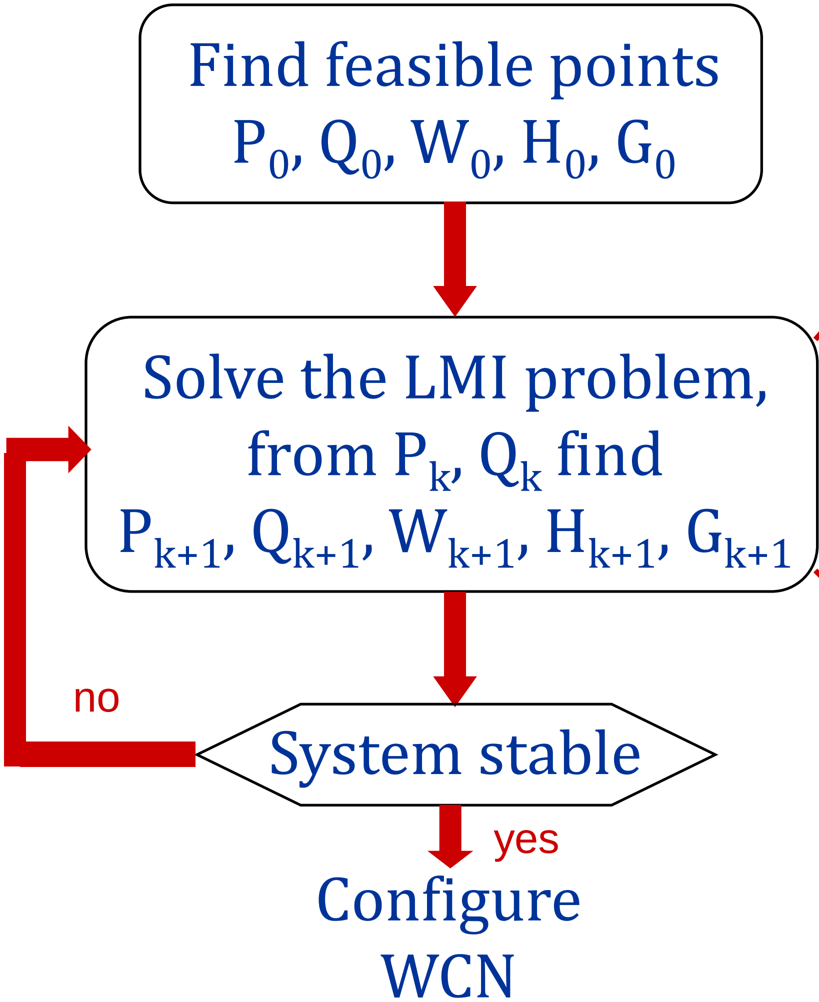
  — Positive definite *nxn* matrices **P** and **Q** satisfy **QP = I** if and only if they are optimal solutions to the problem

$$\min tr(\mathbf{QP})$$
$$s.t. \begin{bmatrix} \mathbf{P} & \mathbf{I} \\ \mathbf{I} & \mathbf{Q} \end{bmatrix} \geq 0$$

  and the minimum cost is *n*.

- Still nonlinear -> linearize around a feasible point $\mathbf{P}_0$, $\mathbf{Q}_0$

Convex relaxation for controller synthesis



Function Linearization

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

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

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

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

Synthesis of optimal WCNs

Goal: A WCN configuration that minimizes the impact of disturbances!

Disturbance impact $\hat{\mathbf{y}} = \hat{\mathbf{C}}\hat{\mathbf{x}}[k]$ $\hat{\mathbf{x}}[k] = \begin{bmatrix} \mathbf{x}[k] \\ \mathbf{z}[k] \end{bmatrix}$

- Model as a new system: $\hat{\mathbf{C}} = \begin{bmatrix} \mathbf{I} & \mathbf{0} \end{bmatrix}$

$$\hat{\mathbf{x}}[k+1] = \hat{\mathbf{A}}\hat{\mathbf{x}}[k] + \hat{\mathbf{B}}\mathbf{u}_w[k]$$

$$\hat{\mathbf{y}}[k] = \hat{\mathbf{C}}\hat{\mathbf{x}}[k].$$

closed-loop: WCN & plant!

where the goal is to minimize $\hat{\mathbf{y}}$

Synthesis of optimal WCNs

How to capture size of discrete time signals?

$$\|\mathbf{v}\|_{\ell_2} \triangleq \left(\sum_{k=0}^{\infty} \|\mathbf{v}[k]\|^2\right)^{1/2} \qquad \|\mathbf{v}\|_{\ell_\infty} \triangleq \sup_{k\geq 0} \|\mathbf{v}[k]\|$$

System gains for the discrete-time system

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

- ***Energy-to-Peak Gain:*** $\gamma_{ep} = \sup_{\|\mathbf{u}_w\|_{\ell_2}\leq 1} \|\hat{\mathbf{y}}\|_{\ell_\infty}$
- ***Energy-to-Energy Gain:*** $\gamma_{ee} = \sup_{\|\mathbf{u}_w\|_{\ell_2}\leq 1} \|\hat{\mathbf{y}}\|_{\ell_2}$

Synthesis of optimal WCNs

System gains for the discrete-time system

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

- *Energy-to-Peak Gain:* $\gamma_{ep} = \sup_{\|\mathbf{u}_w\|_{\ell_2} \leq 1} \|\hat{\mathbf{y}}\|_{\ell_\infty}$
- *Energy-to-Energy Gain:* $\gamma_{ee} = \sup_{\|\mathbf{u}_w\|_{\ell_2} \leq 1} \|\hat{\mathbf{y}}\|_{\ell_2}$

- **Theorem:**

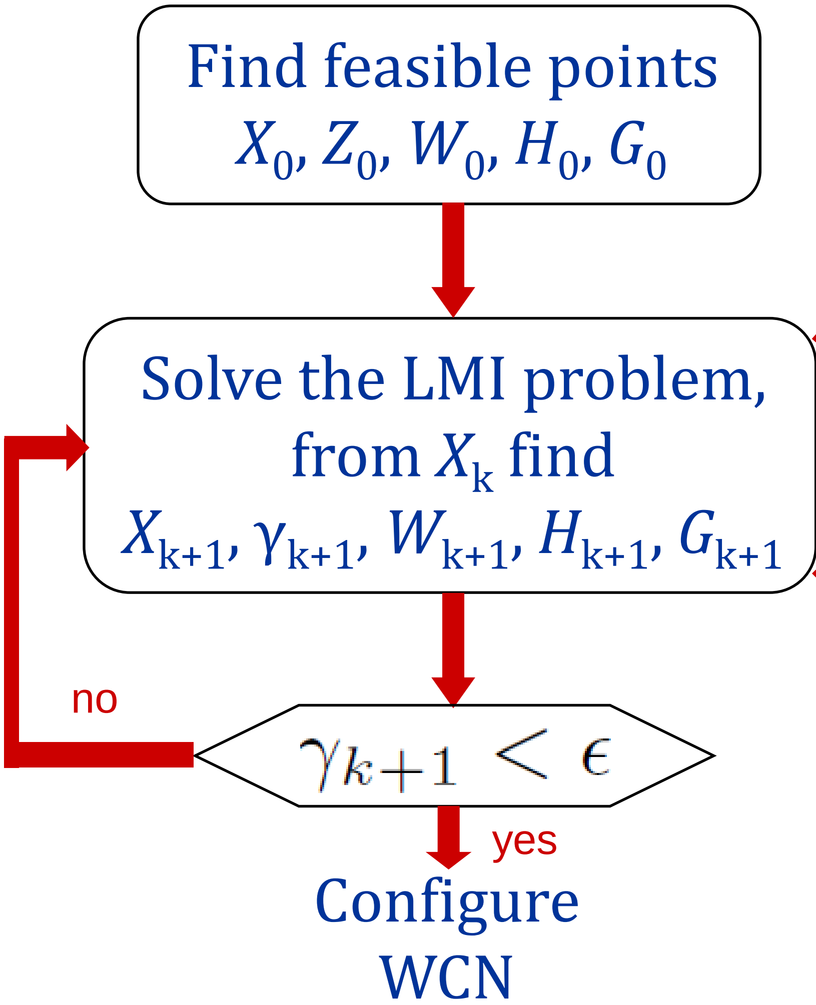
a) $\gamma_{ep} < \gamma \Leftrightarrow \quad \mathcal{X} \succ 0, \Upsilon \succeq 0$

$$\Upsilon \prec \gamma \mathbf{I} \qquad \mathcal{R}(\mathcal{X}, \mathcal{Z}, \Upsilon, \mathcal{X}^{-1}) = \begin{bmatrix} \mathcal{X} & \mathcal{Z} & \hat{\mathbf{A}} & \hat{\mathbf{B}} \\ \mathcal{Z}^T & \Upsilon & \hat{\mathbf{C}} & \mathbf{0} \\ \hat{\mathbf{A}}^T & \hat{\mathbf{C}}^T & \mathcal{X}^{-1} & \mathbf{0} \\ \hat{\mathbf{B}}^T & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \succ 0$$

non-convex!

Linearization: $LIN(\mathcal{X}^{-1}, \mathcal{X}_k) = \mathcal{X}_k^{-1} - \mathcal{X}_k^{-1}(\mathcal{X} - \mathcal{X}_k)\mathcal{X}_k^{-1}$

Convex relaxation for controller synthesis



Function Linearization

$$\mathcal{X}_{k+1} = \arg \min_{\mathcal{X},\mathcal{Z},\Upsilon,\mathbf{W},\mathbf{H},\mathbf{G},\gamma_{k+1}} \gamma_{k+1}$$

$$\mathcal{R}(\mathcal{X}, \mathcal{Z}, \Upsilon, LIN(\mathcal{X}^{-1}, \mathcal{X}_k)) \succ 0,$$

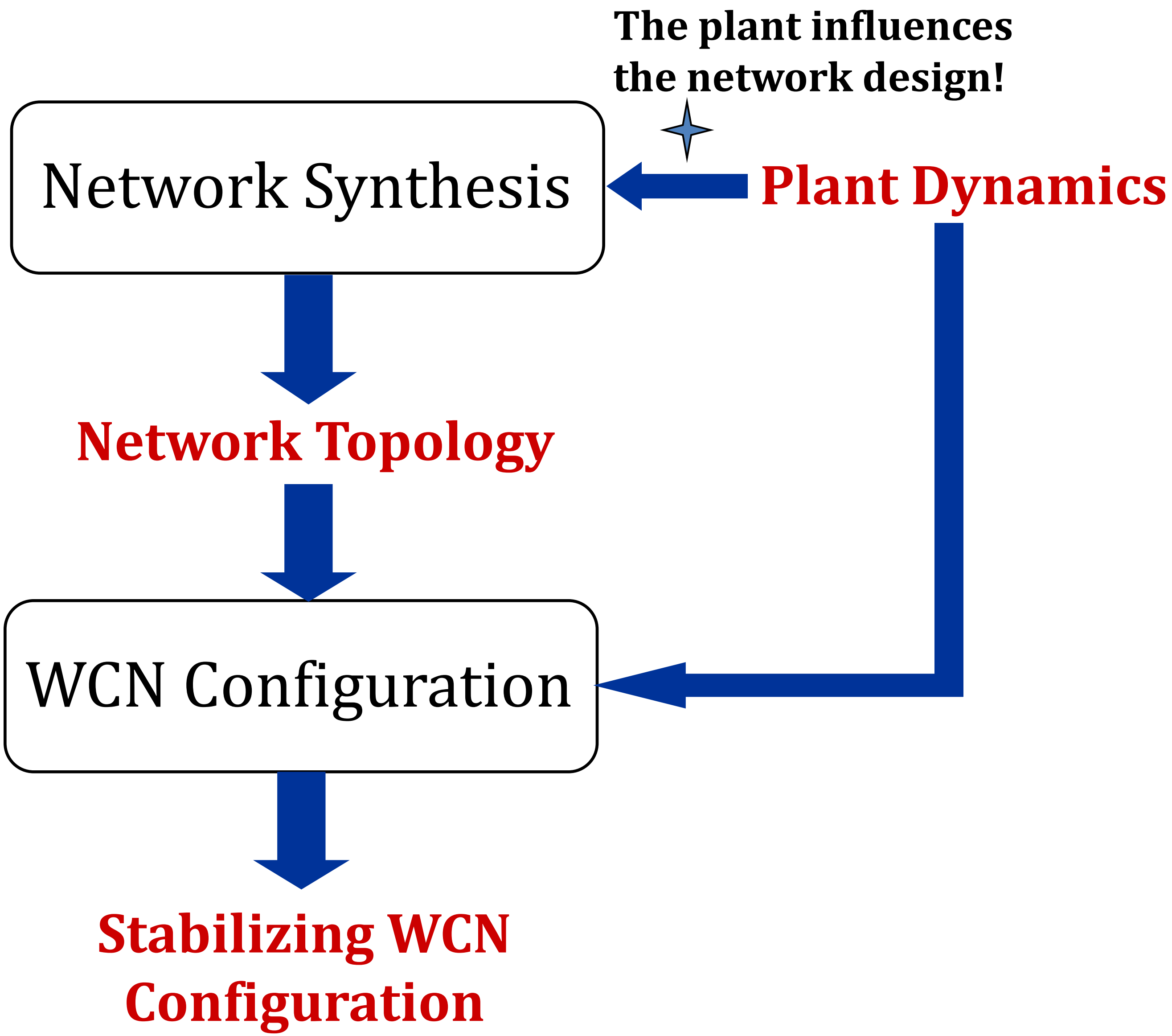
$$\Upsilon \prec \gamma_{k+1}\mathbf{I},$$

$$(\mathbf{W}, \mathbf{H}, \mathbf{G}) \in \Psi, \ \ \mathcal{X} \succ 0, \Upsilon \succeq 0$$

For γ_{ee}, $\mathcal{Z} = \mathbf{0}$

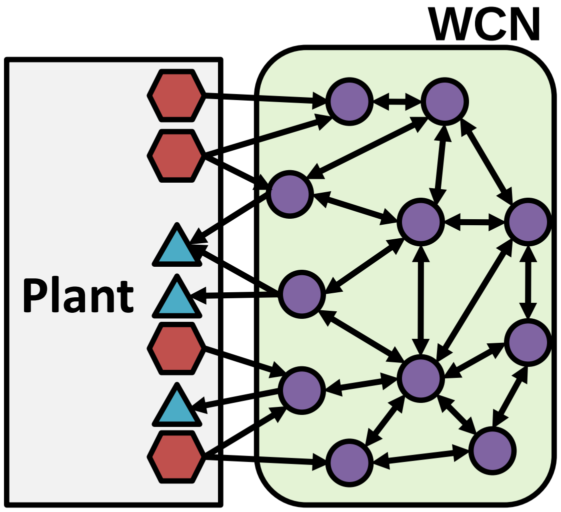
$$\mathcal{R}(\mathcal{X}, \mathcal{Z}, \Upsilon, \mathcal{X}^{-1}) = \begin{bmatrix} \mathcal{X} & \mathcal{Z} & \hat{\mathbf{A}} & \hat{\mathbf{B}} \\ \mathcal{Z}^T & \Upsilon & \hat{\mathbf{C}} & \mathbf{0} \\ \hat{\mathbf{A}}^T & \hat{\mathbf{C}}^T & \mathcal{X}^{-1} & \mathbf{0} \\ \hat{\mathbf{B}}^T & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{bmatrix} \succ 0$$

WCN Synthesis



Wireless control network

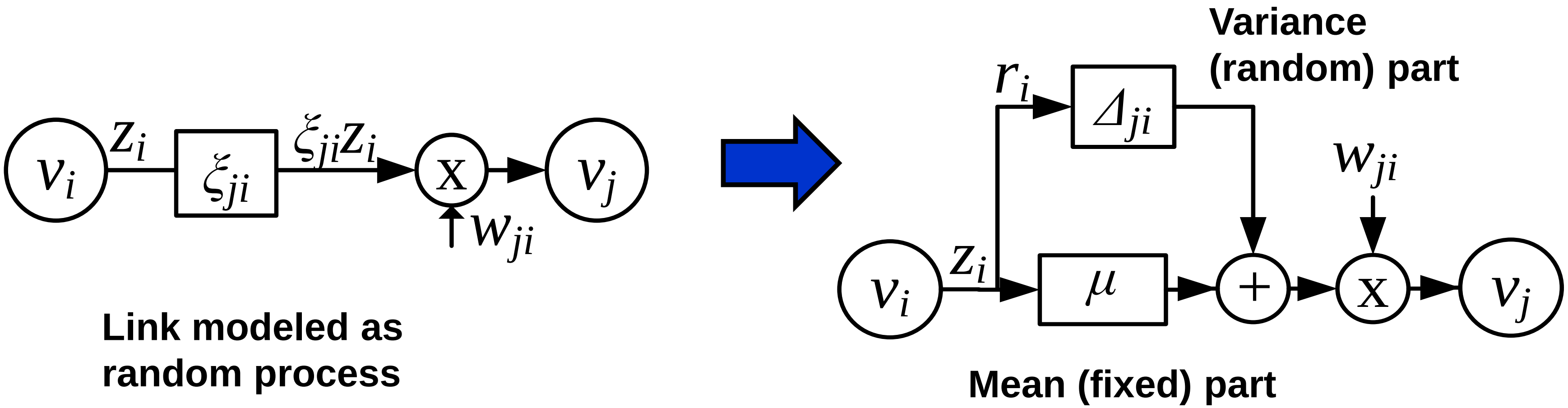
- Wireless control network



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

WCN robustness to link failures

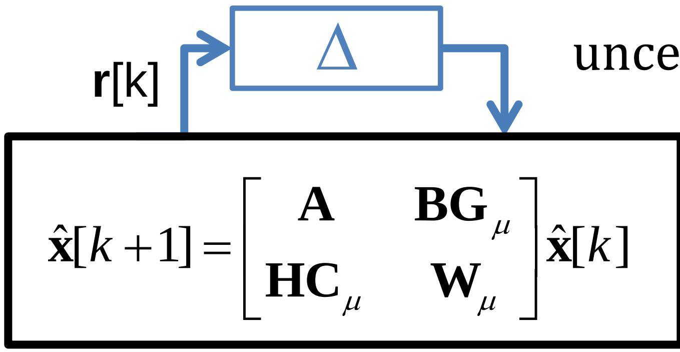
- What happens if links in the network fail?
  - Bernoulli distribution: fails with some probability
- Many links in network: how to model concisely?
  - Use robust control [Elia, Sys & Control Letters, ‘05]



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

random variable — mean (constant) — zero-mean random variable

System Model with Link Failures



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

- Closed loop system with uncertainties:

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

Mean (fixed) part **Random part**

$$\mathrm{r}[k] = \hat{\mathrm{J}}^{\mathrm{or}} \hat{\mathrm{x}}[k]$$

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

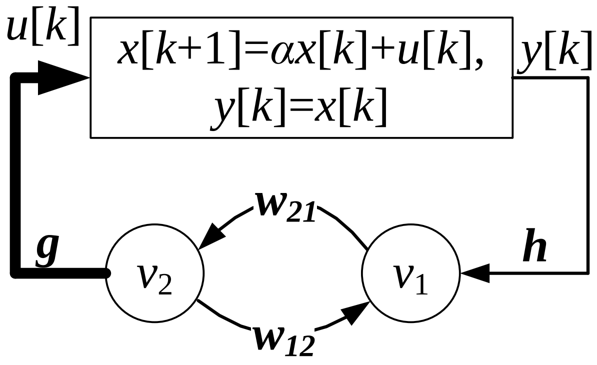
$$\mathbf{X} \succ \hat{\mathbf{A}}_{\mu}\mathbf{X}\hat{\mathbf{A}}_{\mu}^{T} + \mathbf{J}\mathrm{diag}\{\alpha\}(\mathbf{J})^{T}$$

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

- Robustness requires
  - One additional constraint added for each link (Bernoulli failures)
  - More constraints for more general failure models
  - Significant improvements with observer style updates

Robustness to Link Failures

- Example



For α=2, maximal message drop probability which guarantees MSS

$$p_{max} \leq 1.18\%$$

How can we improve robustness of the WCN to link failures?

Problem: How to improve robustness to link failures?

- Idea: Include observer style updates
  - different weights depending of the success of the transmission

$$z_j[k+1] = (w_{jj} - \sum_{i \in \mathcal{N}_{v_j}} \xi_{ji} q_{ji}) z_j[k] + \sum_{i \in \mathcal{N}_{v_j}} \xi_{ji} w_{ji} z_i[k]$$

Observer Style Updates – for reliable communication links

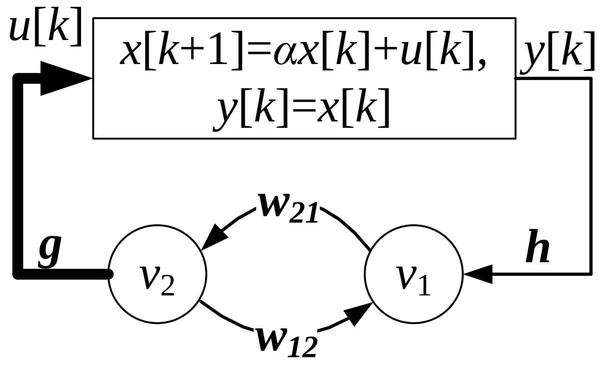
$$z_j[k+1] = w_{jj} z_j[k] + \sum_{i \in \mathcal{N}_{v_j}} \boxed{(w_{ji} z_i[k] - q_{ji} z_j[k])}$$

Standard observer

A similar **design-time** iterative algorithm can be used to extract robust WCN configurations!

Robustness to Link Failures - Evaluation

- Example

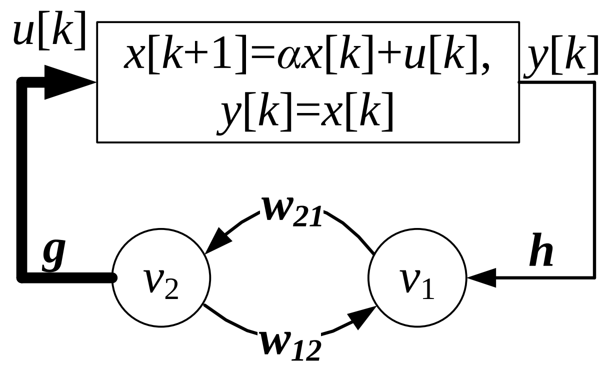


- Maximal message drop probability which guarantees MSS, α=2

	WCN (scalar state)	WCN ($\mathbb{R}^2$ state)	$oWCN$ (scalar state)	$oWCN$ ($\mathbb{R}^2$ state)
$N=2$	$p_m = 1.18\%$	$p_m = 1.30\%$	$p_m = 10.46\%$	$p_m = 17.82\%$
$N=3$	$p_m = 1.32\%$	$p_m = 1.46\%$	$p_m = 11.24\%$	$p_m = 17.88\%$
$N=4$	$p_m = 1.41\%$	$p_m = 1.54\%$	$p_m = 11.46\%$	$p_m = 17.88\%$
		$oWCN$ ($\mathbb{R}^3$ state)	$oWCN$ ($\mathbb{R}^4$ state)	$oWCN$ ($\mathbb{R}^5$ state)
$N=2$		$p_m = 20.40\%$	$p_m = 20.48\%$	$p_m = 20.64\%$

Robustness to Link Failures - Evaluation

- Example

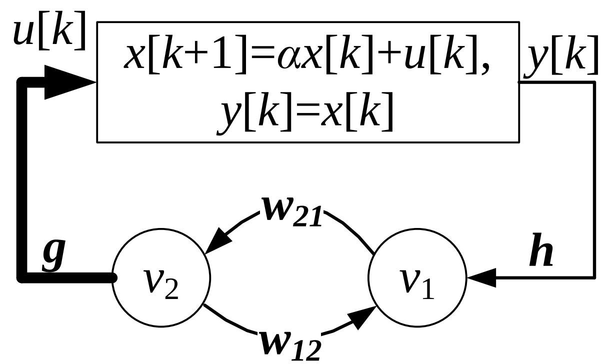


- Maximal message drop probability which guarantees MSS, α=2

	WCN (scalar state)	WCN ($\mathbb{R}^2$ state)	$oWCN$ (scalar state)	$oWCN$ ($\mathbb{R}^2$ state)
$N = 2$	$p_m = 1.18\%$	$p_m = 1.30\%$	$p_m = 10.46\%$	$p_m = 17.82\%$
$N = 3$	$p_m = 1.32\%$	$p_m = 1.46\%$	$p_m = 11.24\%$	$p_m = 17.88\%$
$N = 4$	$p_m = 1.41\%$	$p_m = 1.54\%$	$p_m = 11.46\%$	$p_m = 17.88\%$
		$oWCN$ ($\mathbb{R}^3$ state)	$oWCN$ ($\mathbb{R}^4$ state)	$oWCN$ ($\mathbb{R}^5$ state)
$N = 2$		$p_m = 20.40\%$	$p_m = 20.48\%$	$p_m = 20.64\%$

Robustness to Link Failures - Evaluation

- Example

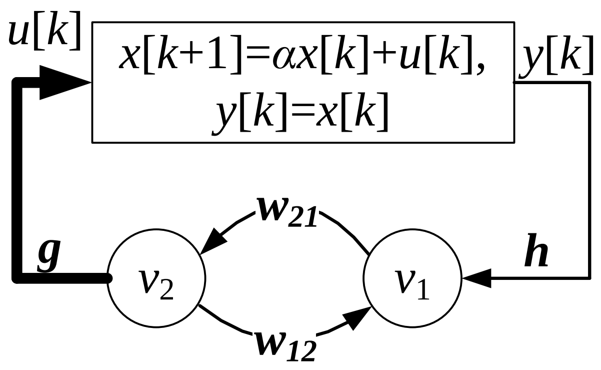


- Maximal message drop probability which guarantees MSS, α=2

	WCN (scalar state)	WCN ($\mathbb{R}^2$ state)	$oWCN$ (scalar state)	$oWCN$ ($\mathbb{R}^2$ state)
$N=2$	$p_m = 1.18\%$	$p_m = 1.30\%$	$p_m = 10.46\%$	$p_m = 17.82\%$
$N=3$	$p_m = 1.32\%$	$p_m = 1.46\%$	$p_m = 11.24\%$	$p_m = 17.88\%$
$N=4$	$p_m = 1.41\%$	$p_m = 1.54\%$	$p_m = 11.46\%$	$p_m = 17.88\%$
		$oWCN$ ($\mathbb{R}^3$ state)	$oWCN$ ($\mathbb{R}^4$ state)	$oWCN$ ($\mathbb{R}^5$ state)
$N=2$		$p_m = 20.40\%$	$p_m = 20.48\%$	$p_m = 20.64\%$

Robustness to Link Failures

- Example – WCN with observer style updates



For α=2, maximal message drop probability which guarantees MSS

$$p_{max} \approx 21\% < 25\%$$

Approaching theoretical limit for robustness with centralized controllers!

Monitoring for faulty and malicious behavior

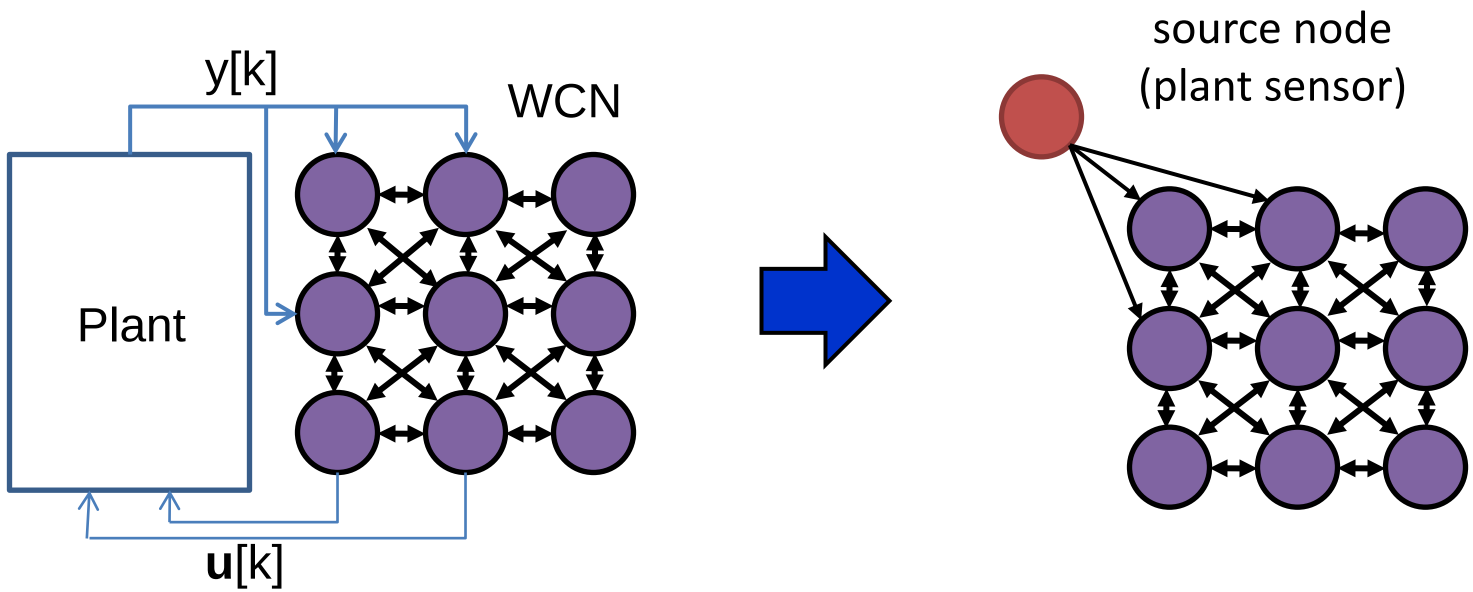
- What if certain nodes in the WCN become faulty or malicious?

- 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

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

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

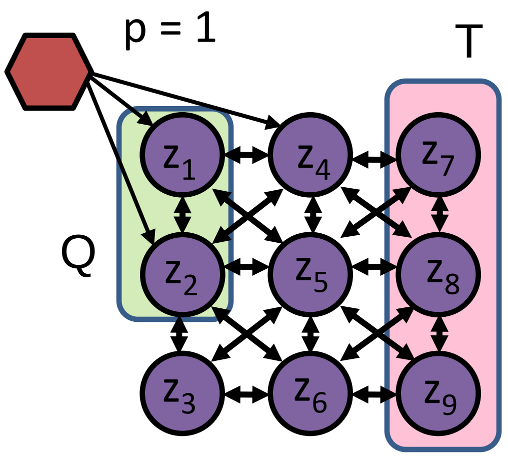
is invertible for **any known set** Q of **2b** nodes

⟺ (generically)

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

IDS Example

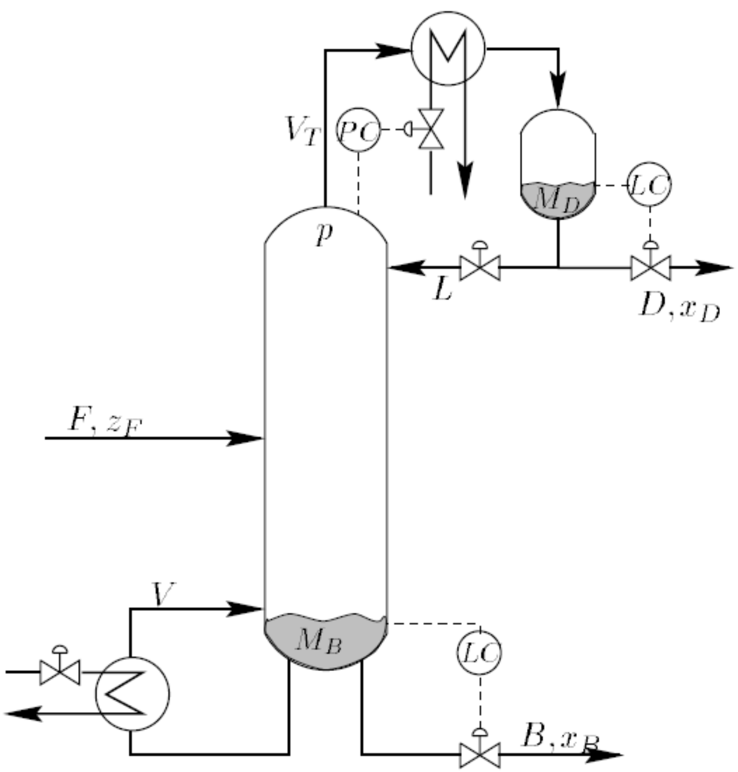
- Suppose we want to identify b = 1 faulty/malicious node and recover the plant outputs in this setting:

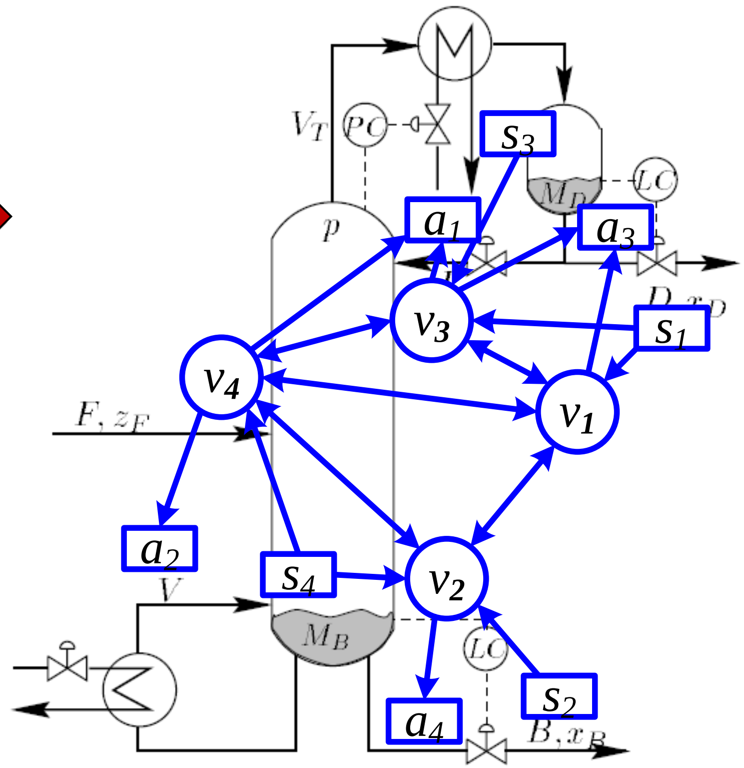


- Consider set Q = $\{v_1, v_2\}$
  - p+2b vertex disjoint paths from sensor and Q to T
- Can verify that this holds for any set Q of 2b nodes
- Sufficient condition: Network is p+2b connected

WCN demo: Distillation column process control

- Distillation column control
  - Plant **continuous-time** model contains 8 states, 4 inputs, 4 outputs
- Distillation column structure





System configuration

WCN demo: Distillation column process control

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

- WCN contains 4 nodes

Stable configuration (obtained after plant discretization):

node→node

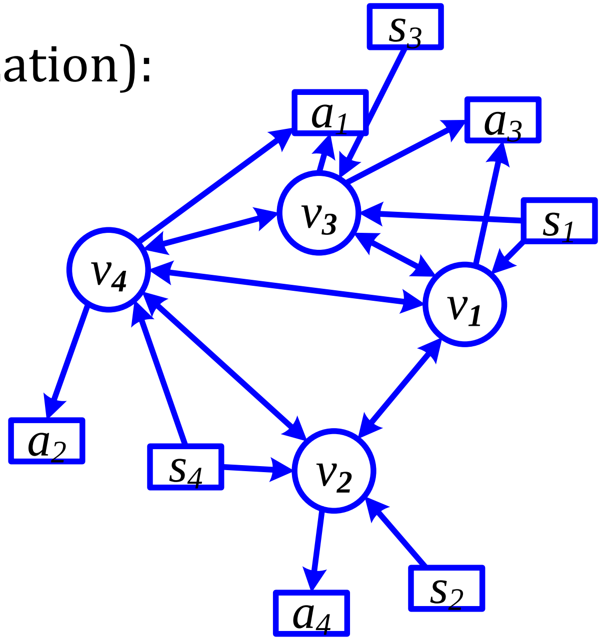
$$\mathbf{W} = \begin{bmatrix} -0.470 & 0.339 & -0.260 & -0.390 \\ -1.117 & -0.145 & 0 & -0.269 \\ 0.0514 & 0 & -0.703 & 0.600 \\ 0.854 & 0.277 & -0.086 & -0.112 \end{bmatrix}$$

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

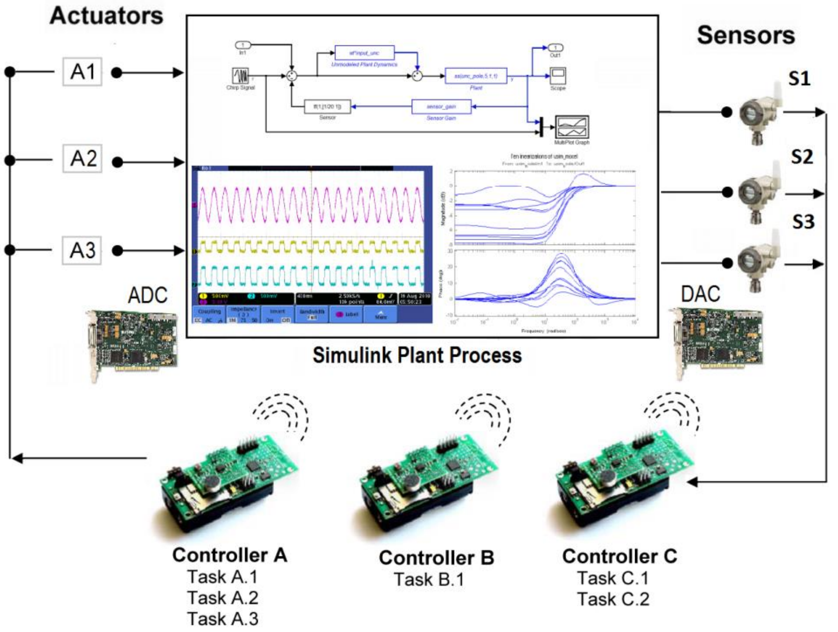
$$\mathbf{G} = \begin{bmatrix} 0 & 0 & -0.226 & -0.459 \\ 0 & 0 & 0 & 0.102 \\ 0.120 & 0 & 1.072 & 0 \\ 0 & 2.549 & 0 & 0 \end{bmatrix}$$



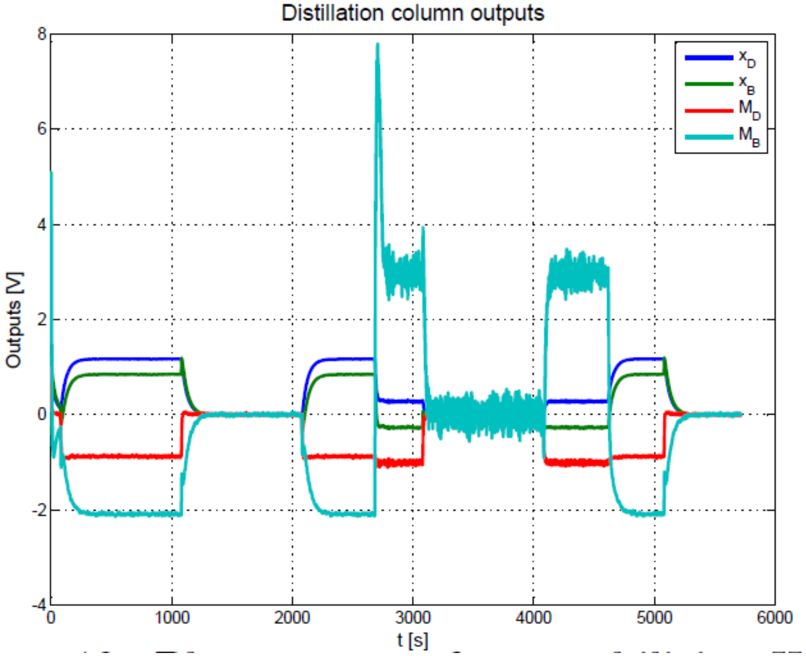
Network topology

WCN demo: Distillation column process control

Process-in-the-loop test-bed



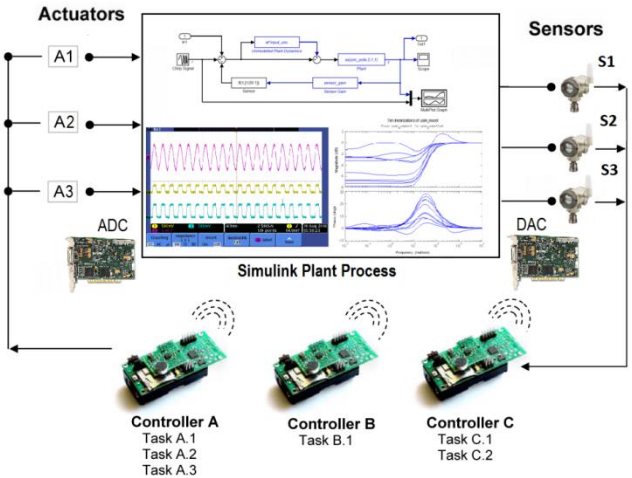
Scenario I: v_1 turned OFF/ON



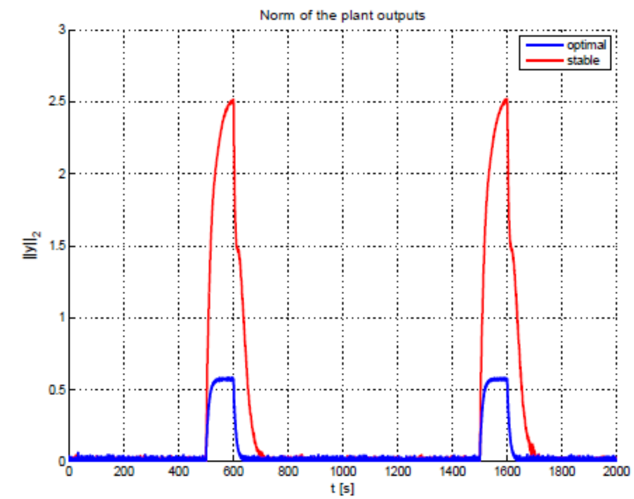
WCN demo: Distillation column process control

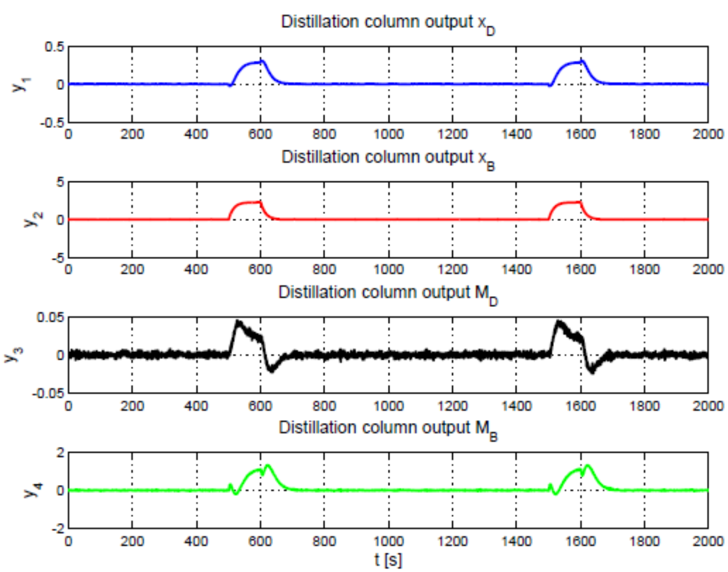
Penn
UNIVERSITY of PENNSYLVANIA

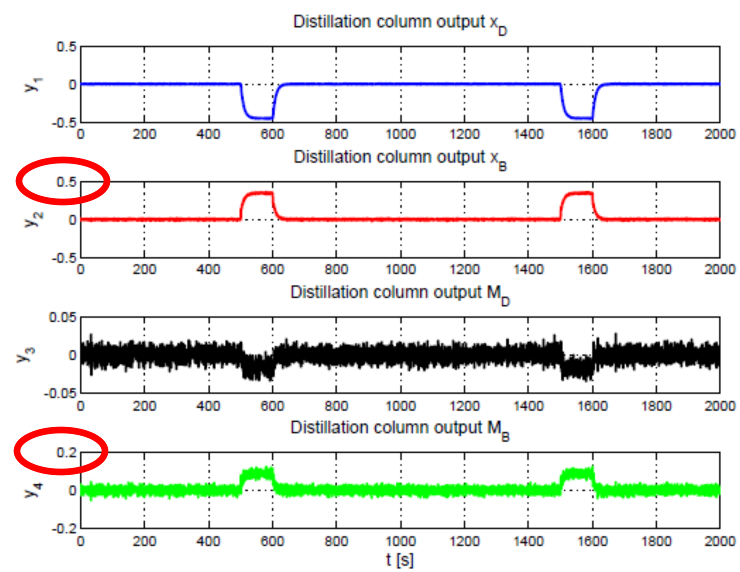
Process-in-the-loop test-bed



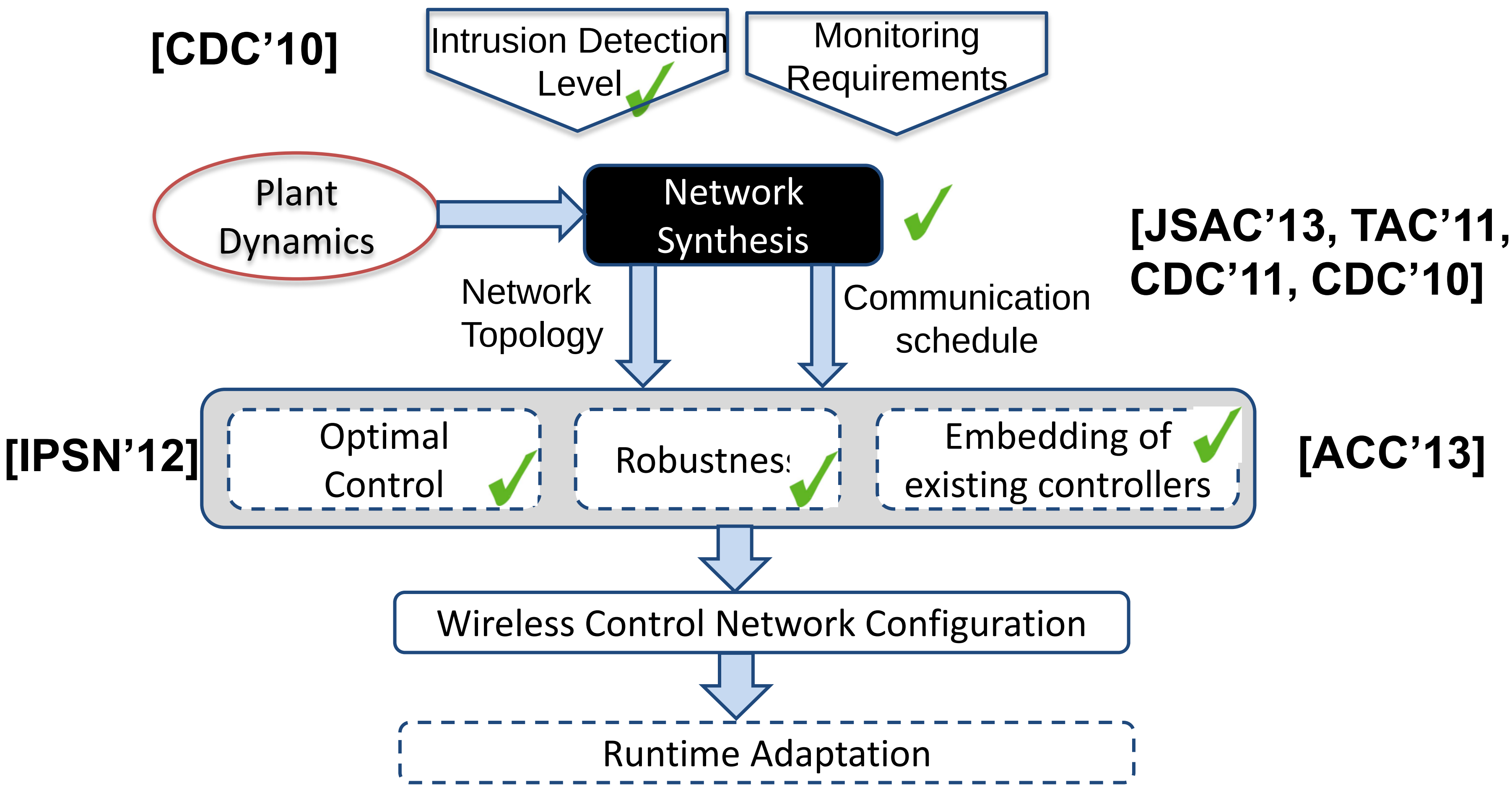
Scenario II: Optimal control







WCN Research Efforts



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

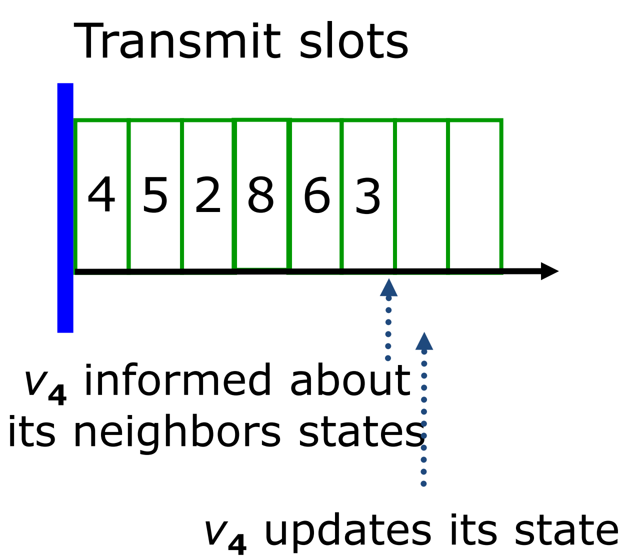
Honeywell

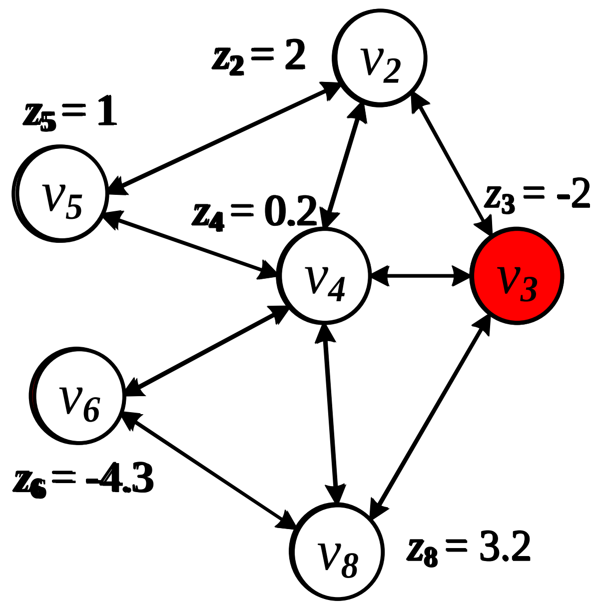
University of Waterloo

RENOVABITUR UT AQUILAE JUVENTUS TUA
JUS LITTERAE SCIENTIAE

Distributed control over time-triggered network

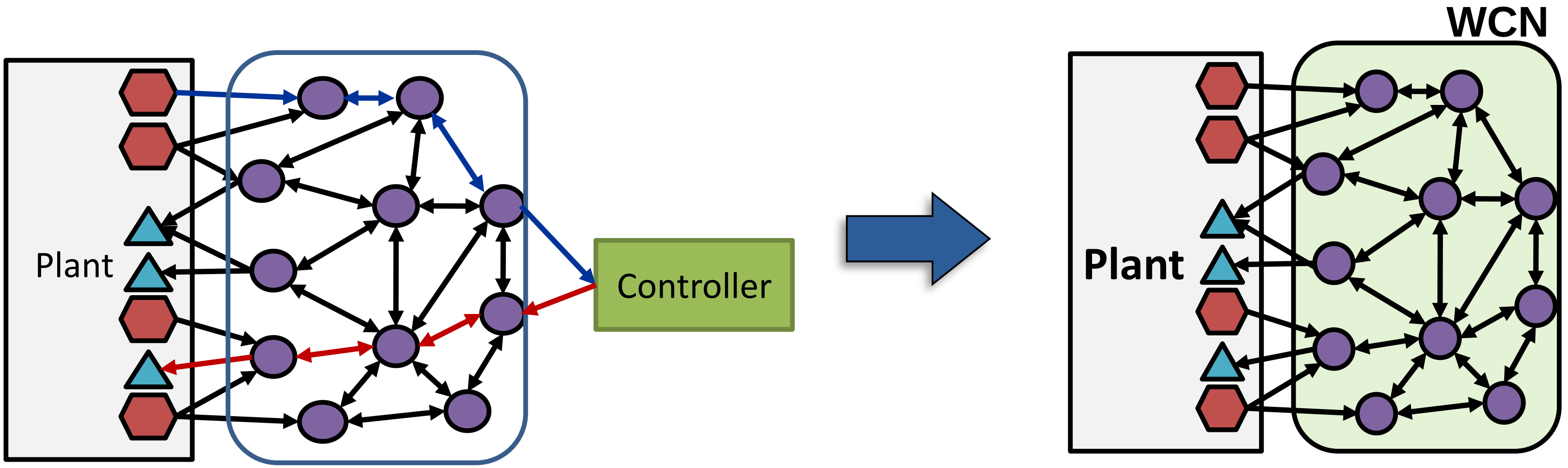
- Each node maintains its (possible vector) state
  - Transmits state exactly once in each step (per frame)
  - Updates own state using linear iterative strategy
- Example:





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