Analysis and Control of Networked Embedded Systems

DEWS
CENTER OF EXCELLENCE

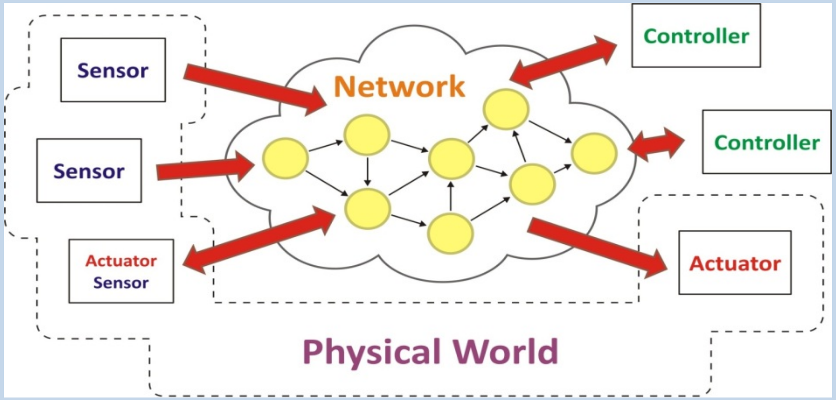
Basilica di Santa Maria di Collemaggio, 1287, L'Aquila

Maria Domenica Di Benedetto

University of L'Aquila

Networked control systems

- Networked Control Systems (NCS) are spatially distributed systems where the communication among plants, sensors, actuators and controllers occurs in a shared communication network
- Many aspects of NCS have been investigated, in particular stability and stabilizability problems



Outline

- **Part I: Symbolic Control Design of Nonlinear Networked Control Systems**
  - Mathematical model of nonlinear NCS
  - Symbolic models for NCS
  - Symbolic control design of NCS
  - Efficient control design algorithms

- **Part II: Modeling, Analysis and Co-Design of Wireless Multi-hop Control Networks (MCN)**
  - Mathematical model of linear MCN implementing time-triggered communication protocols
  - Co-design for asymptotic stability and optimal control
  - Fault tolerant control via FDI methods

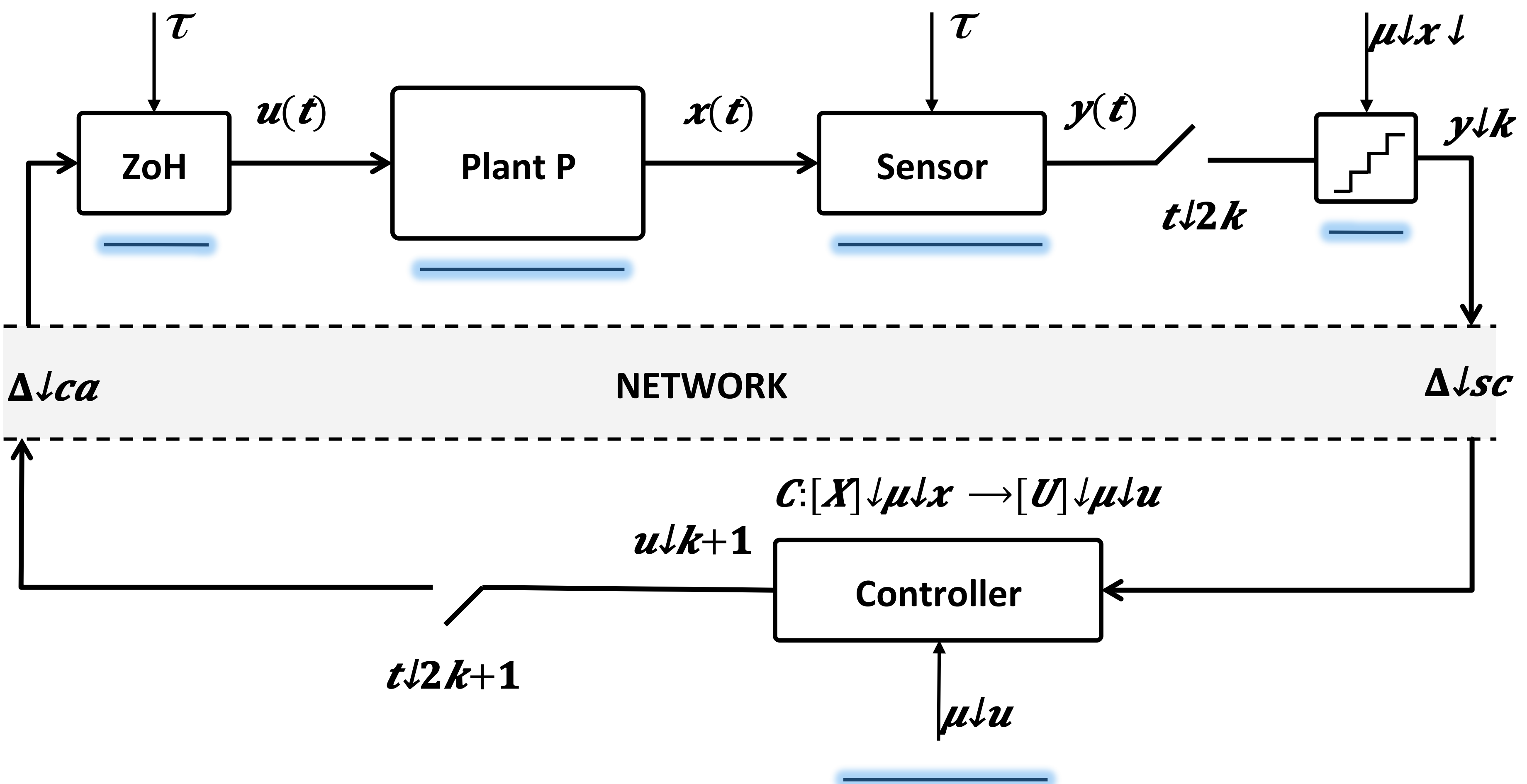
Part I: Symbolic Control Design of Nonlinear Networked Control Systems

Networked control systems: Our model

$u(s\tau+t)=u(s\tau),$
$t\in[0,\tau[, s\in\mathbb{N}_0$

$\{\dot{x}=f(x(t),u(t))\; x\in X\subseteq\mathbb{R}^n, x(0)\in X_0\subseteq X, u\in U\subseteq\mathbb{R}^m$

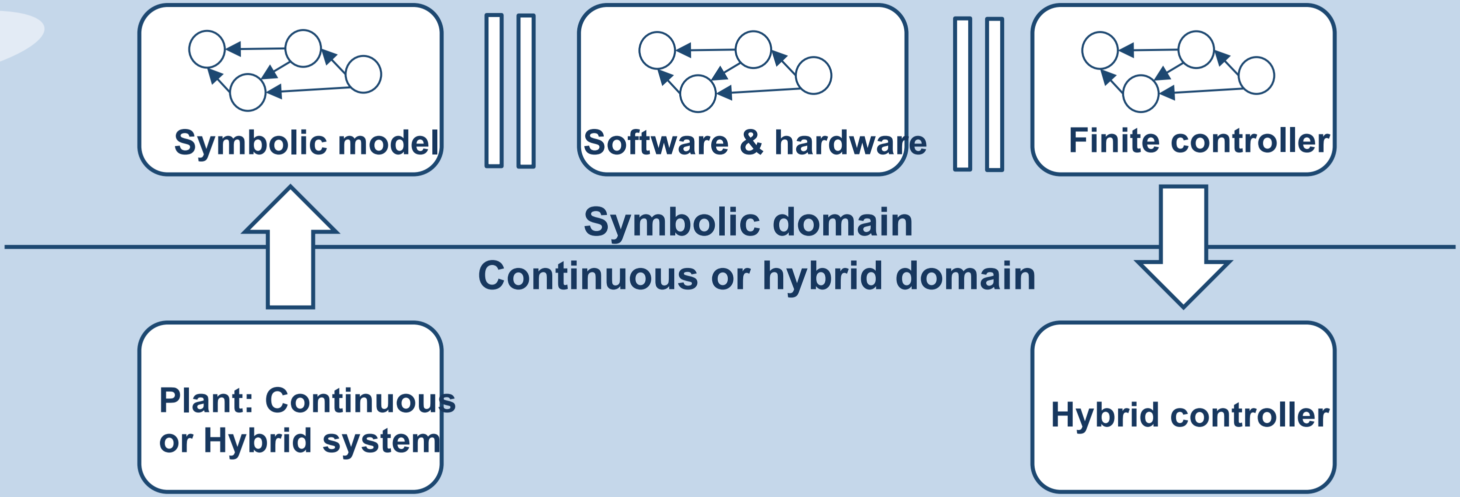
$y(s\tau+t)=y(s\tau)=x(s\tau),$
$t\in[0,\tau[, s\in\mathbb{N}_0$



Correct-by-design controller synthesis

Correct-by-design embedded control software:

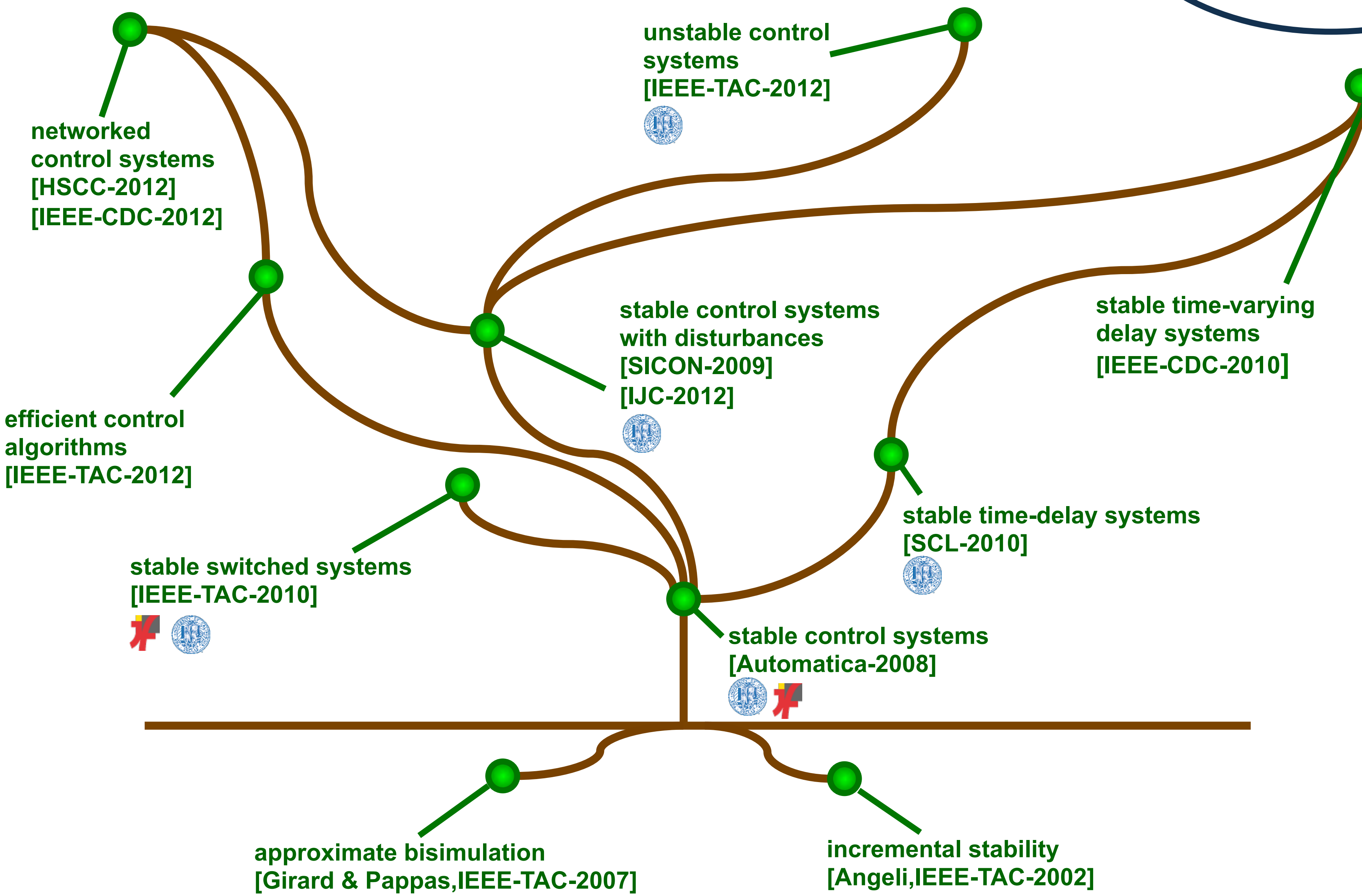
1. Construct a finite model T*(Σ) of the plant system Σ
2. Design a finite controller C that solves the specification S for T*(Σ)
3. Design a controller C' for Σ on the basis of C



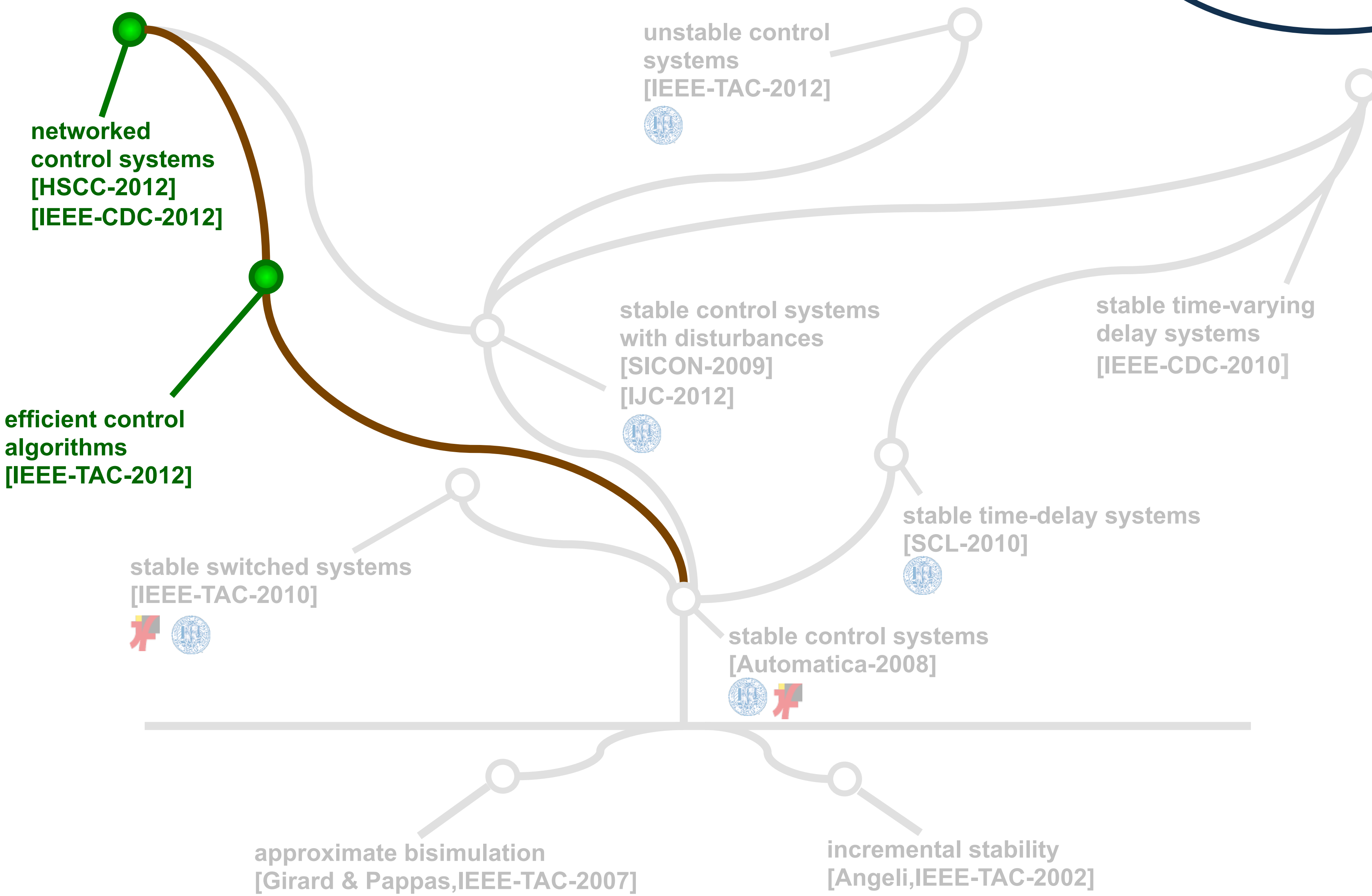
<u>**Advantages:**</u>

- **Integration of software and hardware constraints in the control design of purely continuous processes**
- **Use of computer science techniques to address complex specifications**

Correct-by-design controller synthesis



Correct-by-design controller synthesis for NCS



Dealing with heterogeneity

A Labelled Transition System (LTS) is a tuple

$$T = (Q, L, \longrightarrow, O, H)$$

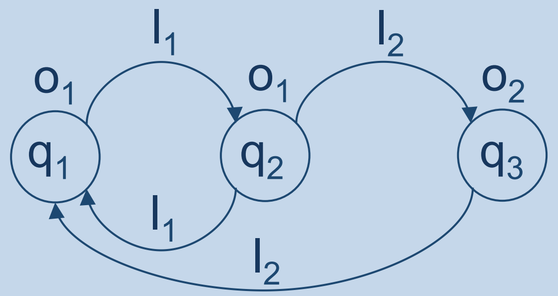
where:

- Q is the set of states
- L is the set of labels
- $\longrightarrow \subseteq Q \times L \times Q$ is the transition relation
- O is the set of outputs
- $H: Q \rightarrow O$ is the output function

We denote $(q,l,p) \in \longrightarrow$ by $q \xrightarrow{l} p$

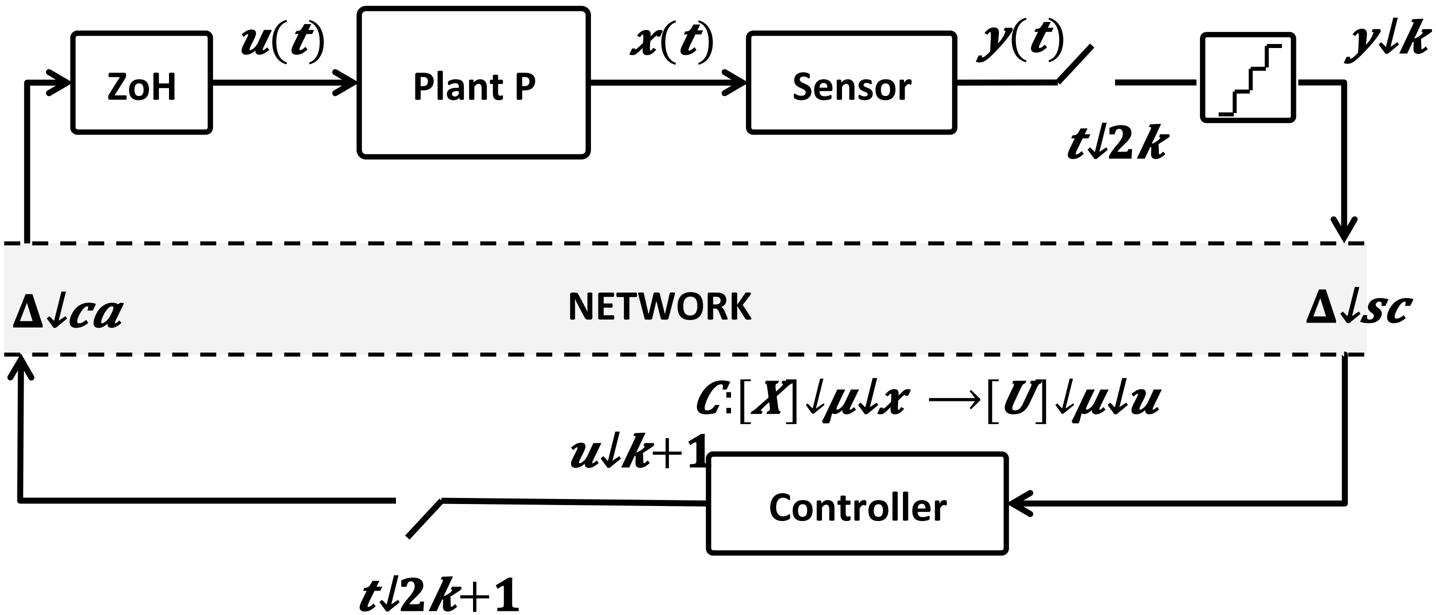
T is said to be:

- symbolic/finite when Q and L are finite
- countable when Q and L are countable
- metric when O is a metric space



Dealing with heterogeneity

Nonlinear Networked control system as an LTS



t	0	τ	2τ	3τ	4τ	5τ	6τ	7τ	8τ	9τ	…
u	0	0	0	u_1	u_1	u_1	u_1	u_1	u_1	u_2	…
x	x(0)	x(τ)	x(2τ)	x(3τ)	x(4τ)	x(5τ)	x(6τ)	x(7τ)	x(8τ)	x(9τ)	…
	$N_1 = 4$				$N_2 = 6$						…

Dealing with heterogeneity

Nonlinear Networked control systems as LTSs

$$(x(0),x(\tau),x(2\tau),x(3\tau)) \xrightarrow{u_1} (x(4\tau),x(5\tau),x(6\tau),x(7\tau),x(8\tau),x(9\tau))$$

t	0	τ	2τ	3τ	4τ	5τ	6τ	7τ	8τ	9τ	…
u	0	0	0	u_1	u_1	u_1	u_1	u_1	u_1	u_2	…
x	x(0)	x(τ)	x(2τ)	x(3τ)	x(4τ)	x(5τ)	x(6τ)	x(7τ)	x(8τ)	x(9τ)	…
	$N_1 = 4$				$N_2 = 6$						…

Dealing with heterogeneity

Nonlinear Networked control systems as LTSs

$(x(0),x(\tau),x(2\tau),x(3\tau)) \xrightarrow{u_1} (x(4\tau),x(5\tau),x(6\tau),x(7\tau),x(8\tau),x(9\tau))$ $(N_2 = 6)$

$(x(0),x(\tau),x(2\tau),x(3\tau)) \xrightarrow{u_1} (x(4\tau),x(5\tau),x(6\tau),x(7\tau))$ $(N_2 = 4)$

$(x(0),x(\tau),x(2\tau),x(3\tau)) \xrightarrow{u_1} (x(4\tau),x(5\tau),x(6\tau),x(7\tau),x(8\tau))$ $(N_2 = 5)$

Denote by $T(\Sigma)$ the LTS associated with a NCS Σ

t	0	τ	2τ	3τ	4τ	5τ	6τ	7τ	8τ	9τ	…
u	0	0	0	u_1	u_1	u_1	u_1	u_1	u_1	u_2	…
x	$x(0)$	$x(\tau)$	$x(2\tau)$	$x(3\tau)$	$x(4\tau)$	$x(5\tau)$	$x(6\tau)$	$x(7\tau)$	$x(8\tau)$	$x(9\tau)$	…
	$N_1 = 4$				$N_2 = 6$						…

Quantifying accuracy

[Pola, Tabuada, SICON-09]

Alternating approximate bisimulation

Given LTSs $T_i = (Q_i, A_i \times B_i, \longrightarrow_i, O_i, H_i)$ ($i = 1,2$) with $O_1 = O_2$, and a precision $\varepsilon > 0$, consider a relation

$$R \subseteq Q_1 \times Q_2$$

R is an <u>alternating approximate simulation relation</u> of T_1 by T_2 if for all $(q_1, q_2) \in R$

- $d(H_1(q_1), H_2(q_2)) \leq \varepsilon$
- $\forall a_1 \, \exists a_2 \, \forall b_2 \, \exists b_1$ such that
  $q_1 \xrightarrow{(a_1,b_1)}_1 p_1$ and $q_2 \xrightarrow{(a_2,b_2)}_1 p_1$ and $(p_1, p_2) \in R$

R is an <u>alternating approximate bisimulation relation</u> between T_1 and T_2 if

- R is an alternating approximate simulation relation of T_1 by T_2
- R^{-1} is an alternating approximate simulation relation of T_2 by T_1

T_1 is <u>ε-alternating simulated</u> by T_2, denoted $T_1 \preccurlyeq_\varepsilon T_2$, if $\pi|_{Q_1}(R) = Q_1$

T_1 and T_2 are <u>ε-alternating bisimilar</u>, denoted $T_1 \cong_\varepsilon T_2$, if $\pi|_{Q_1}(R) = Q_1$ and $\pi|_{Q_2}(R) =$

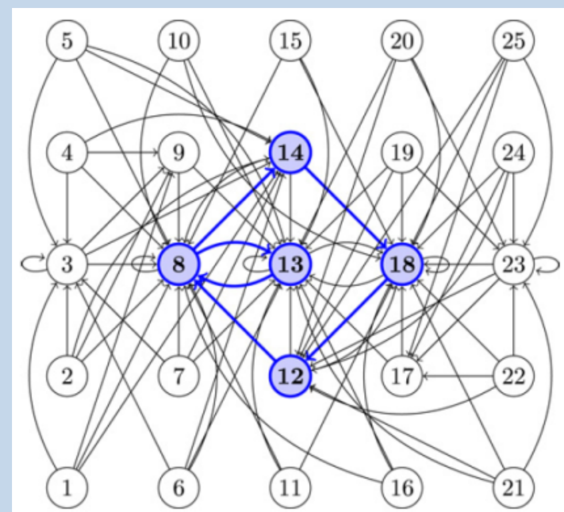
Symbolic models

Theorem [HSCC-2012] For any δ-GAS nonlinear NCS Σ with compact state and input spaces,

$$\forall \varepsilon > 0 \;\; \exists \text{ symbolic transition system } T^*(\Sigma):$$

$$T^*(\Sigma) \cong_{\varepsilon} \Sigma$$

$\approx_{\varepsilon}$

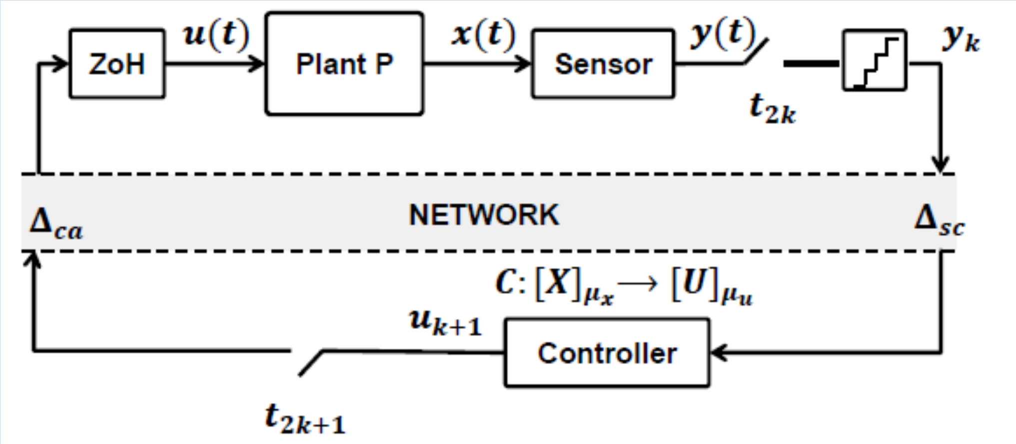


Symbolic control design

<u>Problem formulation:</u>

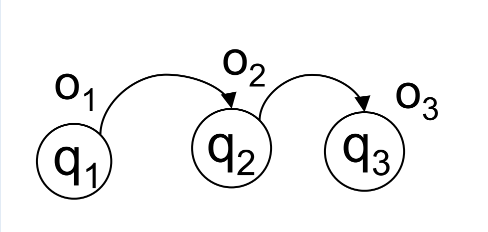
Given a NCS $\boldsymbol{\Sigma}$, a specification LTS S and a desired precision $\varepsilon > 0$, find a symbolic controller C such that:

- $T(\boldsymbol{\Sigma}) \,\|_{\mu}\, C \preccurlyeq_{\varepsilon} S$
- $T(\boldsymbol{\Sigma}) \,\|_{\mu}\, C$ is non-blocking



Networked Control System Σ

$\preccurlyeq_{\varepsilon}$



Specification LTS S

Symbolic control design

Solution: $C = Nb\,(\,T^*(\Sigma)\,||_{\mu x}\,S\,)$

Drawback:

High computational complexity!

Efficient on-the-fly (off-line) algorithms that integrate the synthesis of C with the construction of $T^*(\Sigma)$ proposed in:

[Pola, Borri, Di Benedetto, IEEE-TAC-2012]

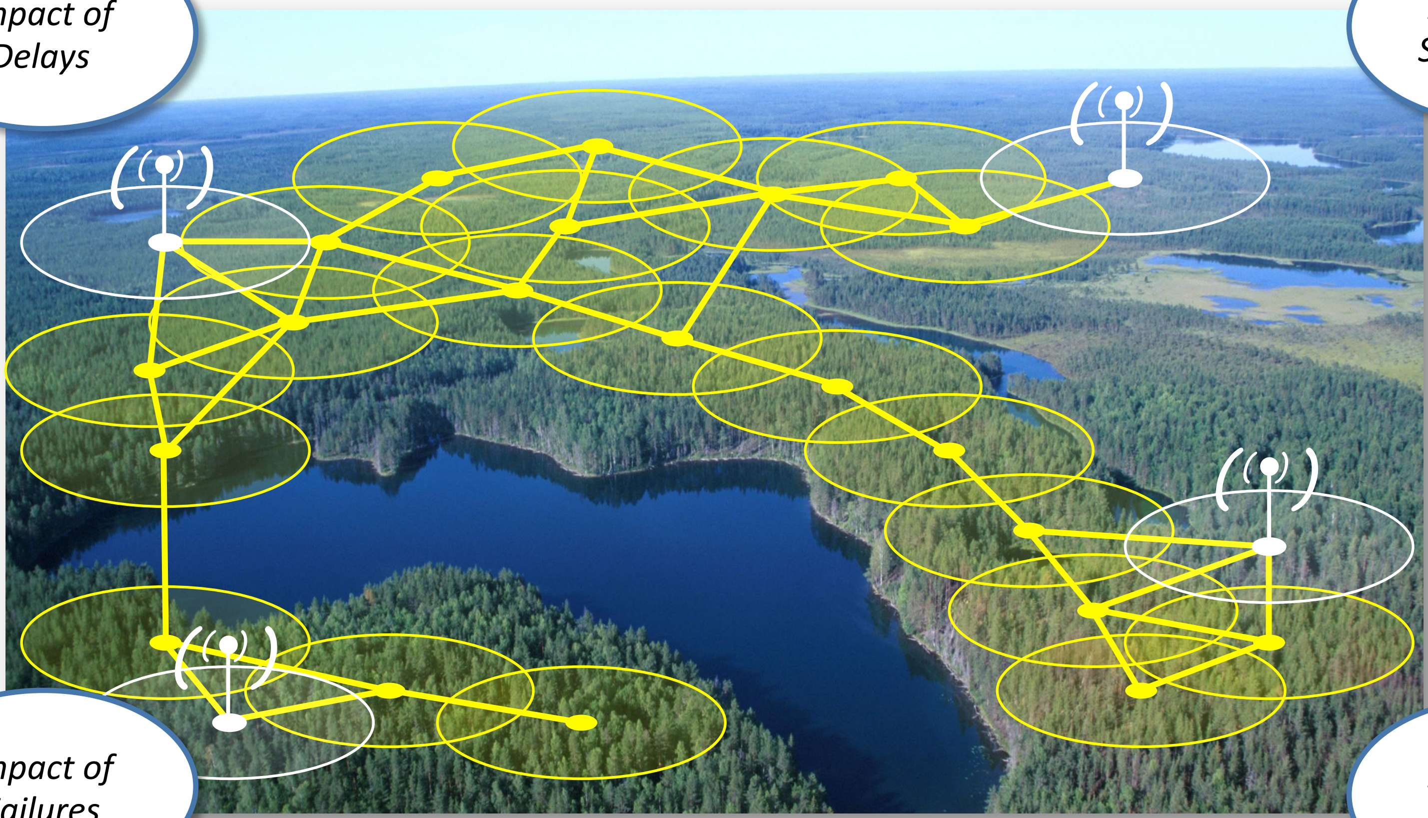
[Borri, Pola, Di Benedetto, IEEE-CDC-2012]

One academic example	Space complexity	Time complexity
Traditional approaches	2,759,580 data	5,442 sec
On-the-fly approach	48 data	13 sec

Part II: Modeling, Analysis and co-Design of Wireless Networked Control Systems

Impact of Delays

Impact of Scheduling

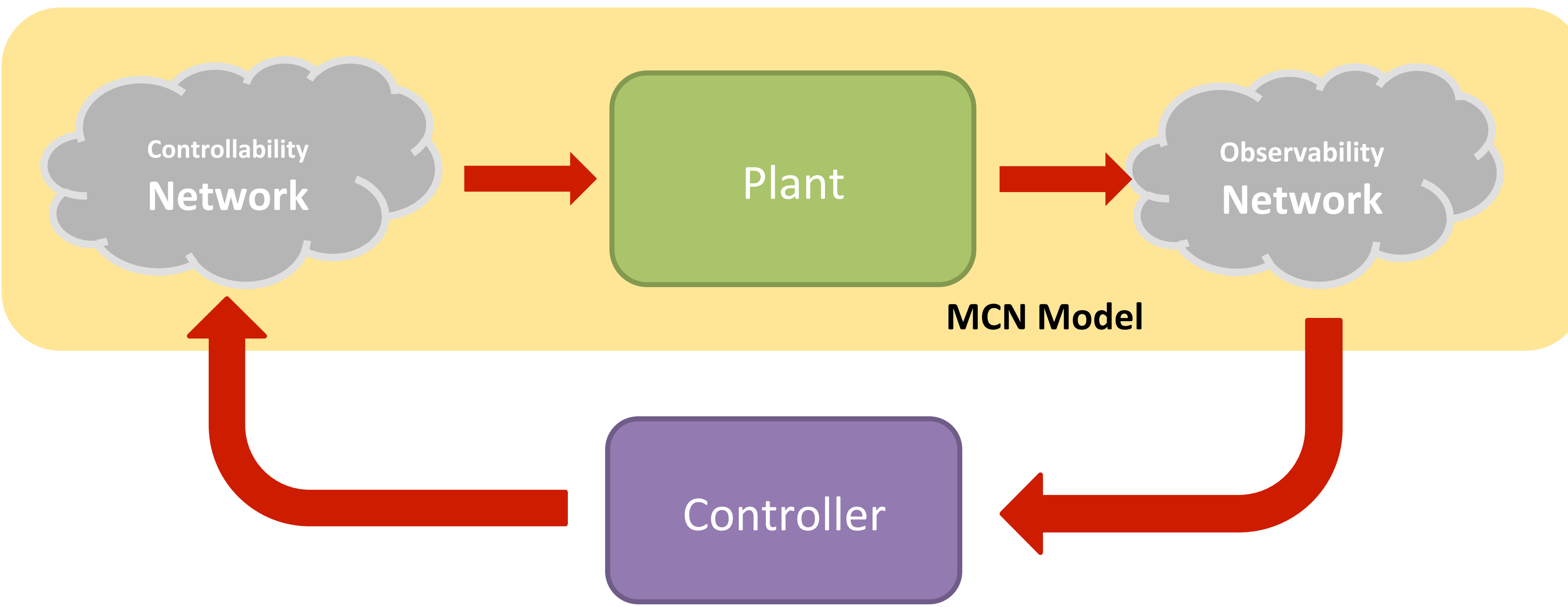


Impact of Failures

Impact of Routing

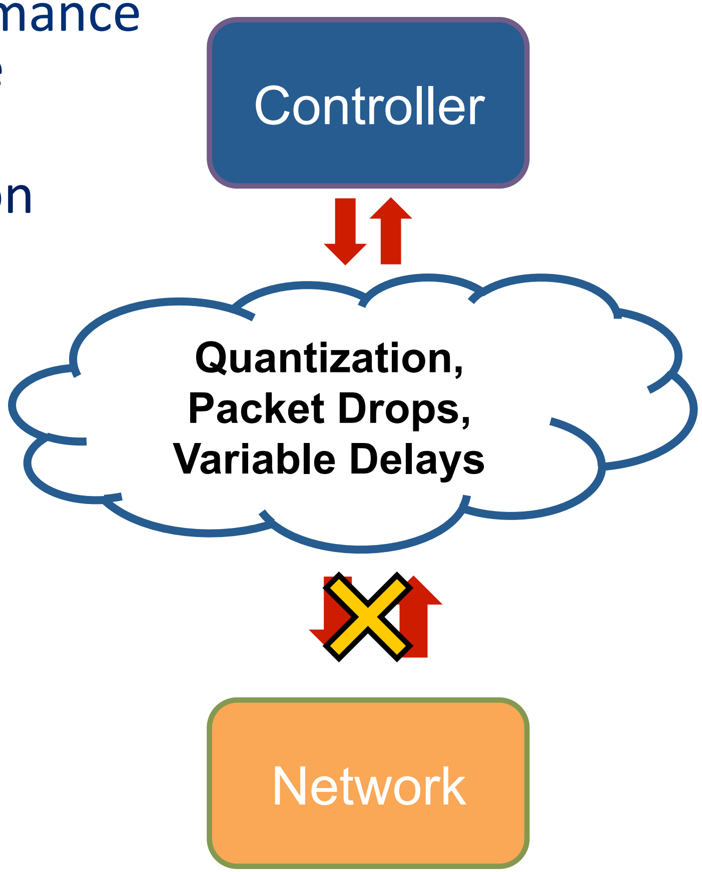
Multi-hop control network model

- Control signals sent to the plant via a controllability network
- Measured data sent to the controller via an observability network



A different level of abstraction

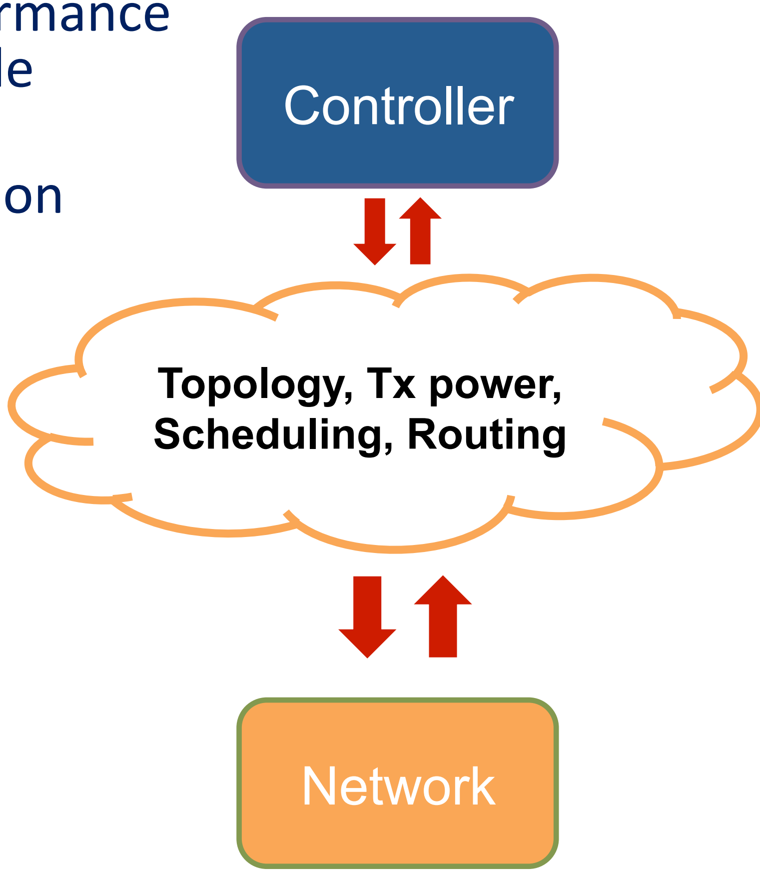
- Network perceived through aggregate performance variables: quantization, packet drops, variable delays and their effect on control system
- Lose information at a lower level of abstraction



A different level of abstraction

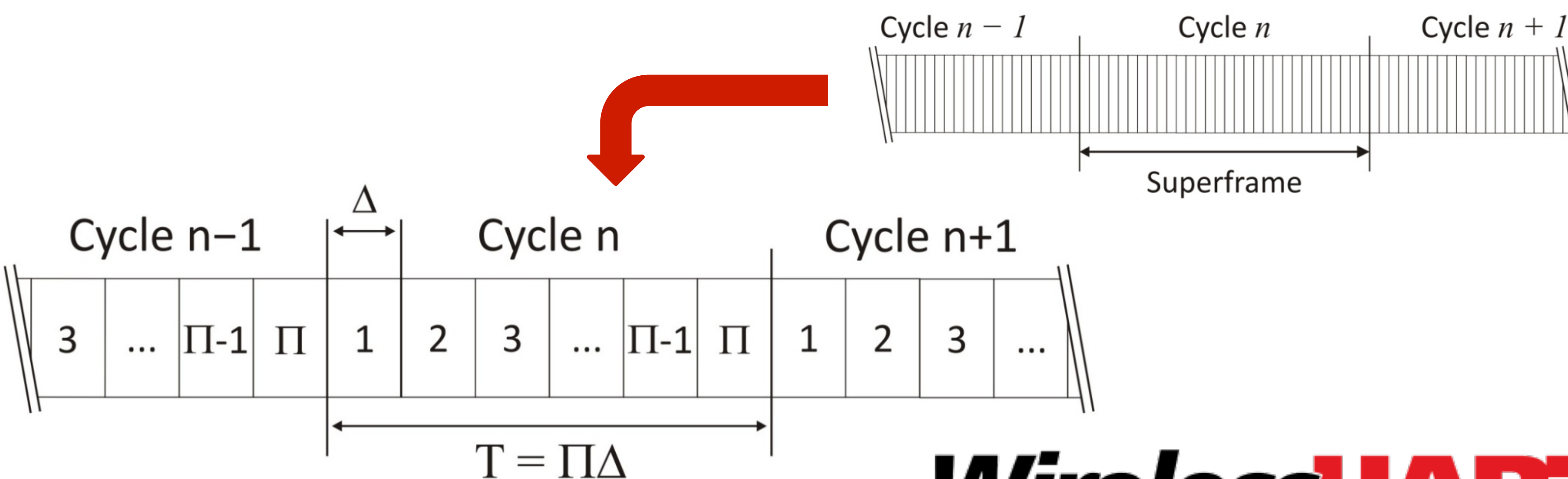
- Network perceived through aggregate performance variables: quantization, packet drops, variable delays and their effect on control system
- Lose information at a lower level of abstraction

- Relate network non-idealities to network parameters: topology, transmission power, scheduling, routing:
  - Mathematical model of linear MCN implementing time-triggered communication protocols
  - Co-design for asymptotic stability and optimal control
  - Node failure and malicious intrusion detection, fault tolerant control



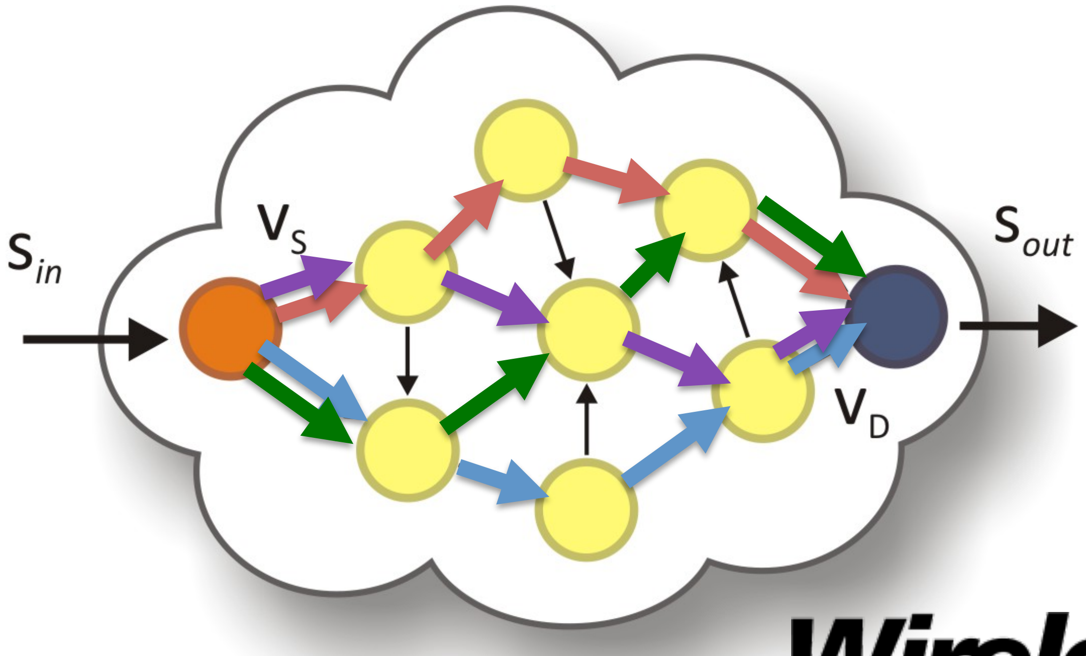
WirelessHART MAC layer (scheduling)

- Time is divided in periodic frames, each divided in Π time slots, each of duration Δ
- To avoid interference, a periodic scheduling allows each node to transmit data only in a subset of time slots



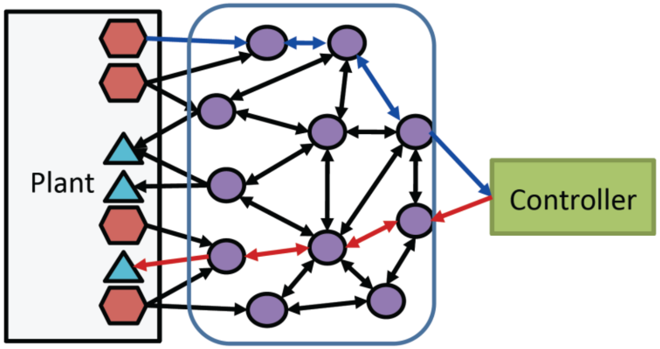
WirelessHART network layer (multi-path routing)

- To each pair of nodes source-destination (v_S, v_D) is associated an acyclic graph that defines the set of allowed routing paths
- Redundancy in the routing paths



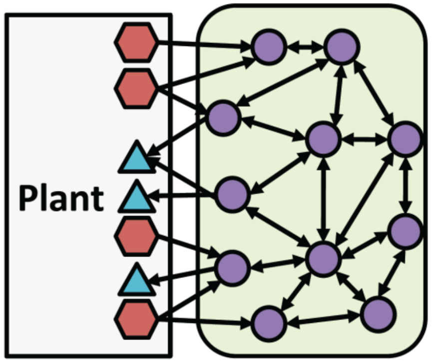
WirelessHART

Multi-hop control networks



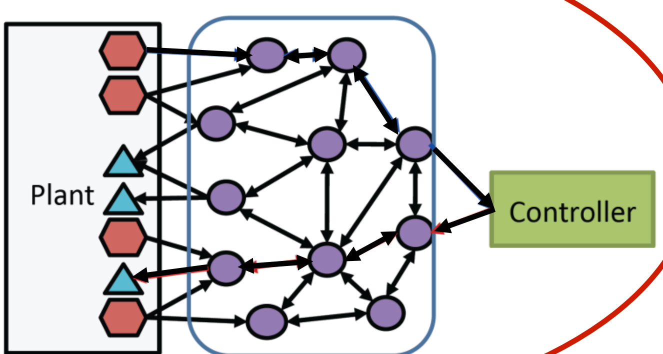
Centralized Controller, Relay Network:
no data processing (acyclic graph)

[Alur, D'Innocenzo, Johansson, Pappas, Weiss, IEEE-TAC-11]



Controller Network:
linear data processing (cyclic weighted graph)

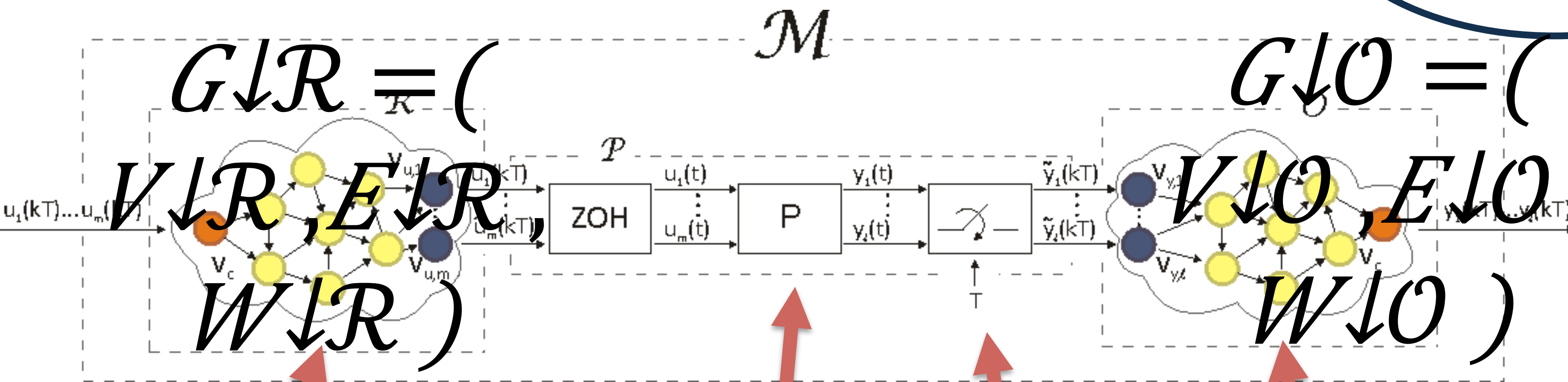
[Pajic, Sundaram, Pappas, Mangharam, IEEE-TAC-11]



Centralized Controller, Relay Network:
linear data processing (acyclic weighted graph)

[D'Innocenzo, Di Benedetto, Serra, IEEE-TAC, provisionally accepted, 2012]

Multi-hop control networks model



$G_R = (V_R, E_R, W_R)$ $\quad$ $\mathcal{P}=(A,B,C)$ $\quad$ $G_O = (V_O, E_O, W_O)$

$W_{R_i}: E_R \to \mathbb{R}^+$, $i=1,\cdots,m$ $\quad$ $T=\Pi\Delta$ $\quad$ $W_{O_i}: E_O \to \mathbb{R}^+$, $i=1,\cdots,l$

$\eta_{R_i}: \{1,\dots,\Pi\} \to 2^{E_R}$ $\quad$ $\eta_{O_i}: \{1,\dots,\Pi\} \to 2^{E_O}$

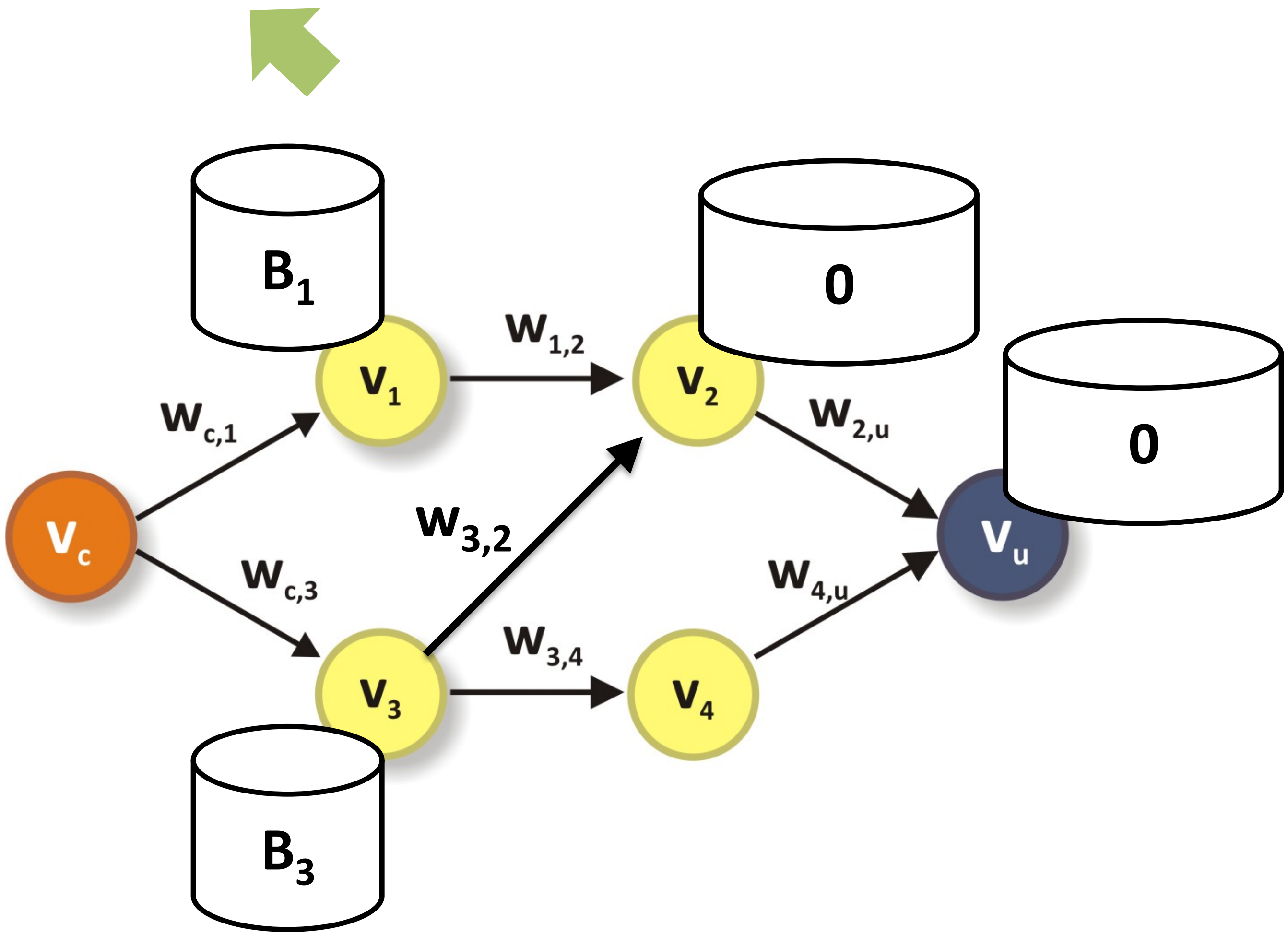
Syntax:

- Linear plant and discrete-time linear controller
- Weight function W determines data processing through the network - reminiscent of network coding
- Communication scheduling η assigns transmission of nodes

Data flow dynamics at time scale of slots

η

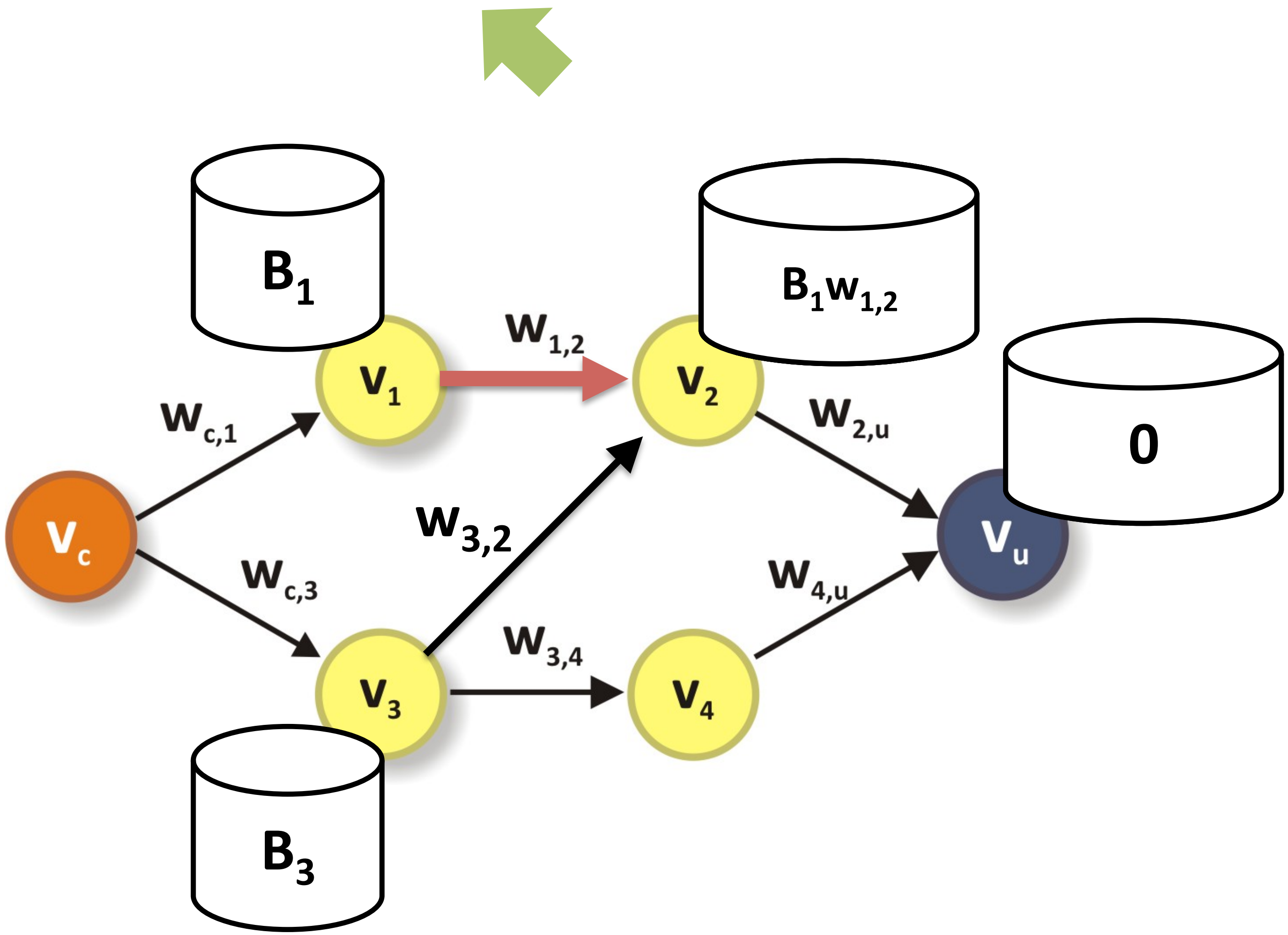
...	v_1, v_2	v_3, v_2	v_2, v_u	...



Data flow dynamics at time scale of slots

η

...	v_1, v_2	v_3, v_2	v_2, v_u	...

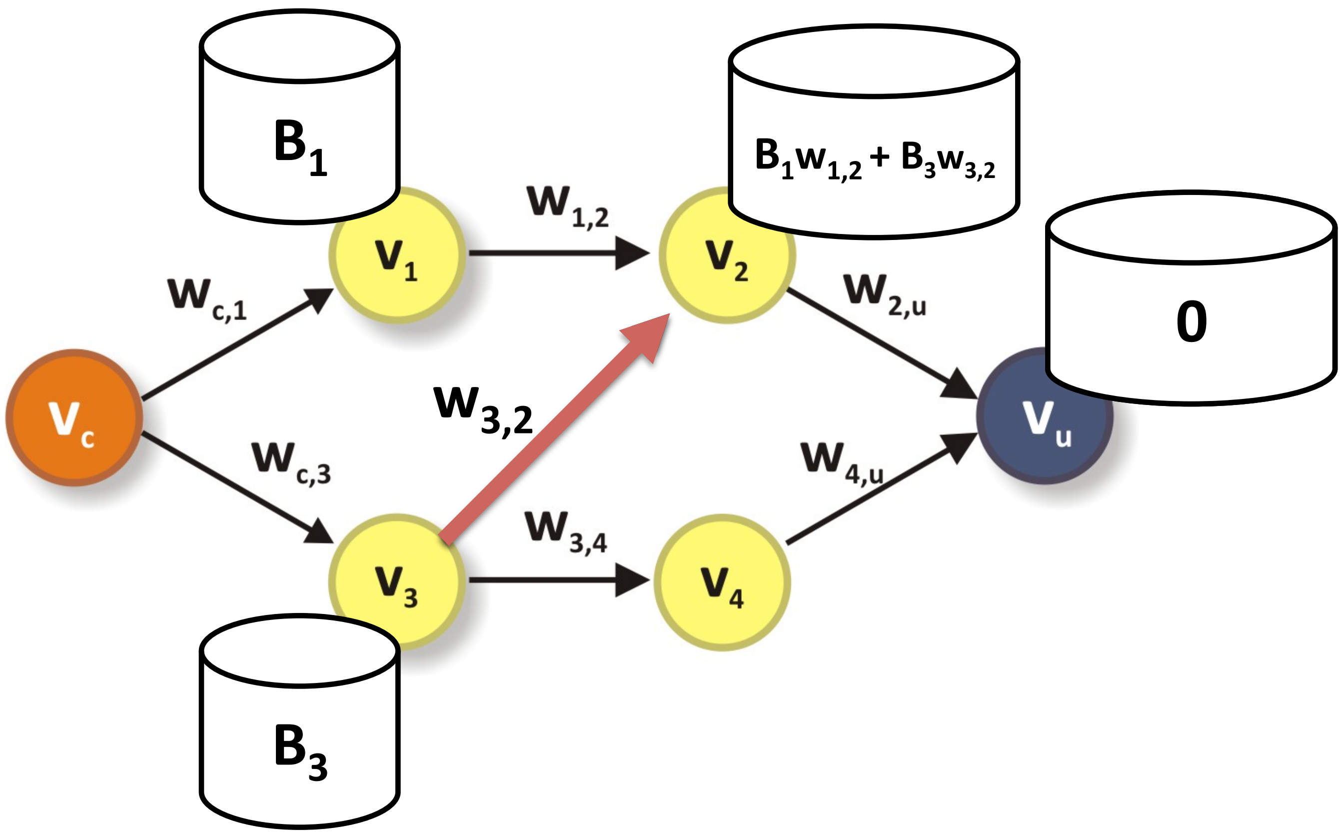


Data flow dynamics at time scale of slots

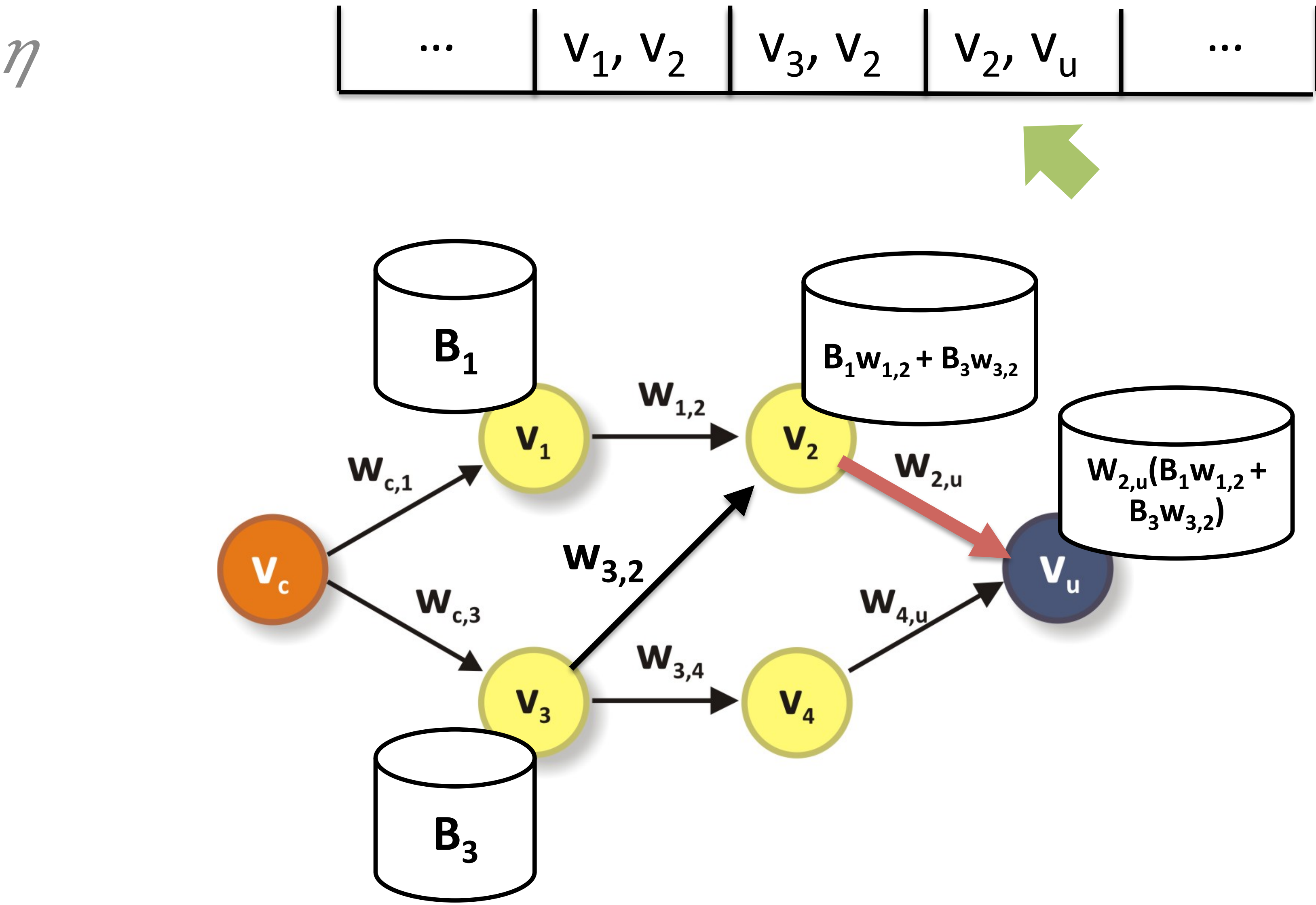
CENTER OF EXCELLENCE

η

...	v_1, v_2	v_3, v_2	v_2, v_u	...



Data flow dynamics at time scale of slots



Asymptotic stabilizability of a MCN

- Model the semantics of MCN by cascade of discrete time MIMO LTI systems, with sampling time equal to the frame duration
- $\mathcal{R}(z)$ depends on network topology $G\downarrow\mathcal{R}$, weight function $W\downarrow\mathcal{R}$ and scheduling $\eta\downarrow\mathcal{R}$

Theorem: A MCN is controllable if and only if:

1. (A,B) is controllable
2. At least one scheduled path connects controller and actuator (condition on network topology and on scheduling function $\eta\downarrow\mathcal{R}$)
3. No zero-pole cancelations (algebraic conditions on weight function $W\downarrow\mathcal{R}$)

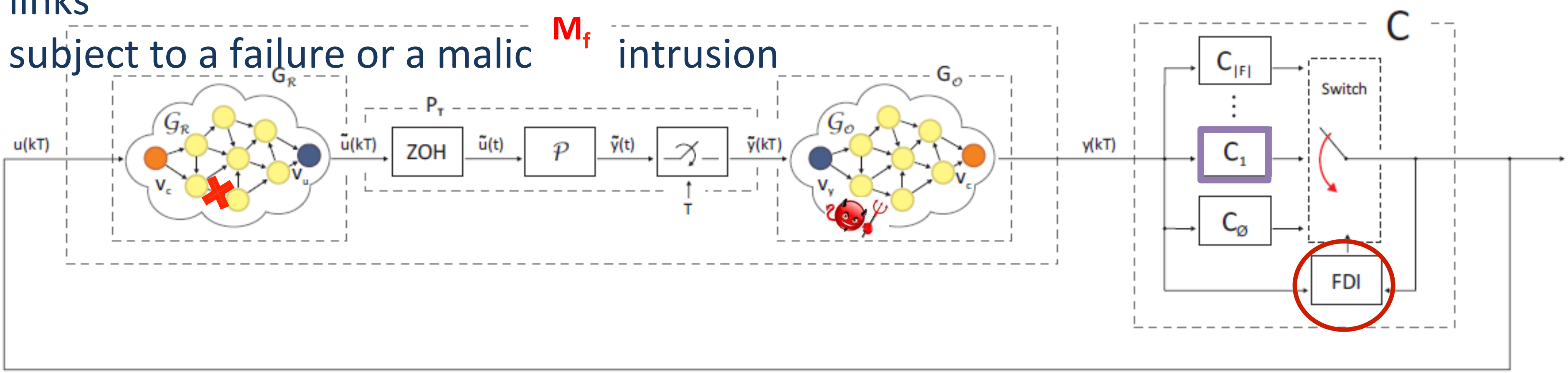
[Smarra, D'Innocenzo, Di Benedetto, NecSys'12]

Transient response to unit-step: optimal L_2-norm co-design

[Smarra, D'Innocenzo, Di Benedetto, IEEE-CDC-12]

Fault tolerant stabilizability of a MCN

Let $\mathcal{F}=2^{\mathcal{E}_{\mathcal{R}} \cup \mathcal{E}_{\mathcal{O}}}$ be the set of all configurations of links
subject to a failure or a malic intrusion



Assumptions:

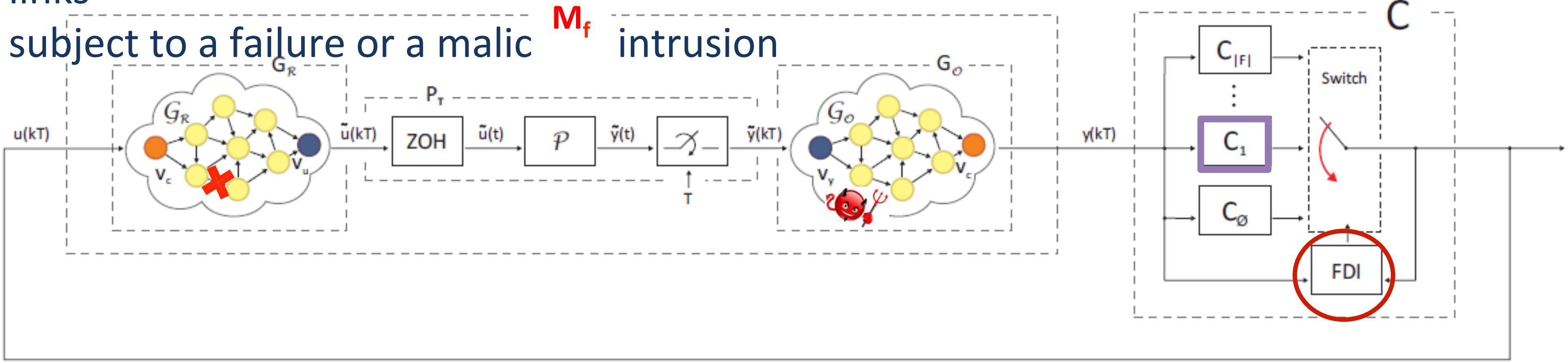
- No fault detection algorithms in the network protocol: only use input to and output from the MCN
- Failures are slow with respect to plant time constants

Problem 1: Guarantee existence of a stabilizing controller for the MCN dynamics M_f associated to any $f \in \mathcal{F}$

[Di Benedetto, D'Innocenzo, Serra, IFAC World Congress, 2011]

Fault tolerant stabilizability of a MCN

Let $F=2^{E_{\mathcal{R}} \cup E_{\mathcal{O}}}$ be the set of all configurations of links
subject to a failure or a malic M_f intrusion



Assumptions:

- No fault detection algorithms in the network protocol: only use input to and output from the MCN
- Failures are slow with respect to plant time constants

Problem 2: Design a dynamical system (FDI) able to detect and isolate any $f \in F$

[D'Innocenzo, Di Benedetto, Serra, IEEE-CDC-ECC-11]

Conclusions

Part I

- Mathematical model of general class of nonlinear NCS
- Symbolic models for NCS
- Symbolic controllers for NCS
- Efficient control algorithms

Part II

- Mathematical framework for co-design of control networks implementing time-triggered protocols
- Relate properties of multi-hop control networks and network configuration (topology, scheduling and routing)
- Fault tolerant control:
  - Permanent failures and malicious attacks via FDI
  - Transient failures (packet losses): work in progress

HYCON2-EECI Graduate School on Control 2013

DEWS
CENTER OF EXCELLENCE

”Symbolic control design of Cyber-Physical systems”

29/04/2013 – 03/05/2013
Istanbul (Turkey)

www.eeci-institute.eu

Appendix A (1/1)

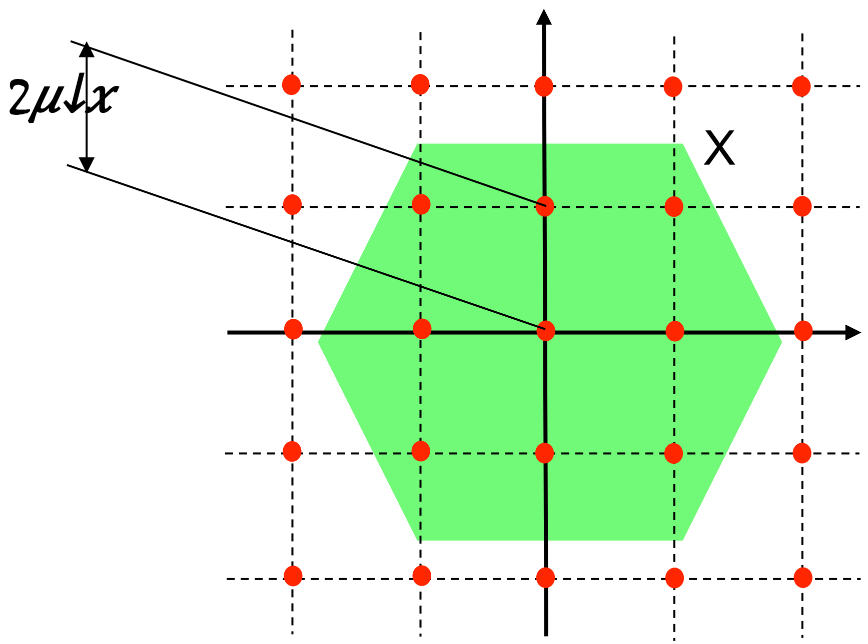
Given a NCS Σ define the LTS

$T(\Sigma)=(Q_\tau, Q_{0,\tau}, L_\tau, \longrightarrow_\tau, O_\tau, H_\tau)$ where:

- $Q_\tau \subseteq Q_0 \cup Q_e$ where $Q_e := \bigcup_{N=N_{min}}^{N_{max}} Q^N$ and for any $q=(x_1, x_2, \ldots, x_N) \in Q^N$, $x_{i+1} = \boldsymbol{x}(\tau, x_i, u^-)$, $i \in [1; N-2]$, and $x_N = \boldsymbol{x}(\tau, x_{N-1}, u^+)$ for some control inputs u^-, u^+
- $Q_{0,\tau} = Q_0$
- $L_\tau = [U]_{\mu_U}$
- $q^1 \xrightarrow{u}_{\tau} q^2$ where, for some N_1, N_2 $\in [N_{min}; N_{max}]$
  $x_{i+1}^1 = \boldsymbol{x}(\tau, x_i^1, u_1^-)$, $i \in [1; N_1 - 2]$
  $x_N^1 = \boldsymbol{x}(\tau, x_{N_1 - 1}^1, u_1^+)$
  $x_{i+1}^2 = \boldsymbol{x}(\tau, x_i^2, u_2^-)$, $i \in [1; N_2 - 2]$
  $x_N^2 = \boldsymbol{x}(\tau, x_{N_2 - 1}^2, u_2^+)$
  $u_2^- = u_1^+$
  $u_2^+ = u$
  $x_1^2 = \boldsymbol{x}(\tau, x_{N_1}^1, u_2^-)$
- $O_\tau = X_\tau$
- H_τ is the identity function

Appendix B (1/4)

T(Σ) collects all the information of the NCS Σ available at the sensor, but it is not a symbolic model. We therefore propose a symbolic model by quantizing the state space X of the plant P



Given x ∈ X let $[x]_{\mu_X} \in [X]_{\mu_X}$ be such that $\| x - [x]_{\mu_X} \| \leq \mu_X$

Appendix B (2/4)

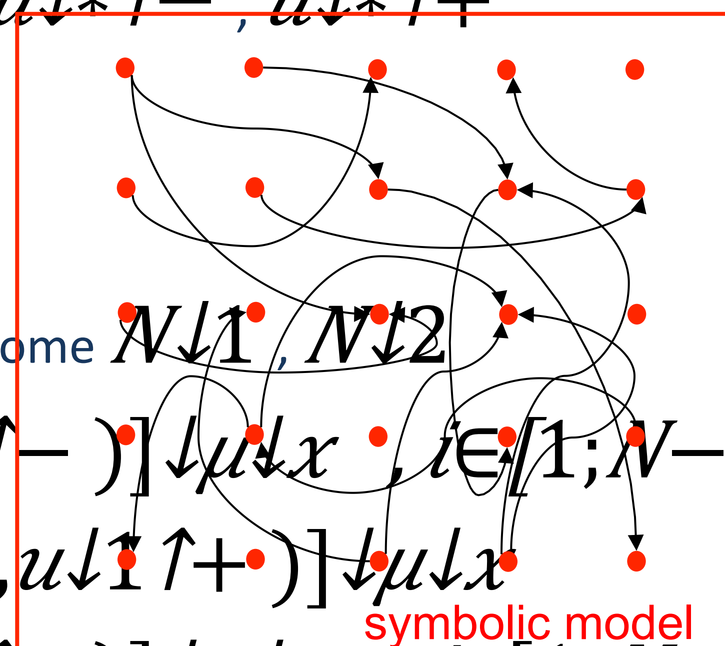
Define the system $T^*(\Sigma) = (Q_*, Q_{0,*}, L_*, \longrightarrow_*, O_*, H_*)$ where:

- $Q_* \subseteq [Q_0 \cup Q_e]_{\mu_x}$ s.t. for any $q^* = (x_1^*, x_2^*, \ldots, x_N^*) \in Q_*$, $x_{i+1}^* = [\mathbf{x}(\tau, x_i^*, u_*^-)]_{\mu_x}$, $i \in [1; N-2]$, and $x_N^* = [\mathbf{x}(\tau, x_{N-1}^*, u_*^+)]_{\mu_x}$ for some u_*^-, u_*^+
- $Q_{0,*} = [X_0]_{\mu_x}$
- $L_* = [U]_{\mu_u}$
- $q^1 \longrightarrow_*^{u_*} q^2$ where, for some N_1, N_2

  $x_{i+1}^1 = [\mathbf{x}(\tau, x_i^1, u_1^-)]_{\mu_x}$, $i \in [1; N-2]$

  $x_N^1 = [\mathbf{x}(\tau, x_{N_1-1}^1, u_1^+)]_{\mu_x}$

  $x_{i+1}^2 = [\mathbf{x}(\tau, x_i^2, u_2^-)]_{\mu_x}$, $i \in [1; N-2]$



Appendix B (3/4)

Def [Angeli, IEEE-TAC-2002]

Given a nonlinear control system $x = f(x,u)$, a smooth function

$$V: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_0^+$$

is said to be a δ-GAS Lyapunov function for P if there exist $\lambda \in \mathbb{R}^+$ and K_∞ functions α_1, α_2 such that, for any $x_1, x_2 \in \mathbb{R}^n$ and any $u \in U$

1) $\alpha_1(\| x_1 - x_2 \|) \leq V(x_1,x_2) \leq \alpha_2(\| x_1 - x_2 \|)$;

2) $\frac{\partial V}{\partial x_1} f(x_1,u) + \frac{\partial V}{\partial x_2} f(x_2,u) \leq -\lambda V(x_1,x_2)$.

Theorem [Angeli, IEEE-TAC-2002]

A nonlinear control system $x = f(x,u)$ is δ-GAS if it admits a δ-GAS Lyapunov function

Appendix B (4/4)

Theorem 1 [HSCC-2012]

Consider the NCS Σ and suppose that the plant nonlinear control system P enjoys the following properties:

1. There exists a δ-GAS Lyapunov function for Σ, hence there exists $\lambda \in \mathbb{R}^+$ s.t. for any $x_1, x_2 \in X$, and any $u \in U$

$$\frac{\partial V}{\partial x_1} f(x_1, u) + \frac{\partial V}{\partial x_2} f(x_2, u) \leq -\lambda V(x_1, x_2).$$

2. There exists a K_∞ function γ such that $V(x, x') \leq V(x, x'') + \gamma(\|x' - x''\|)$

   for every $x, x', x'' \in X$.

Then for any desired precision $\varepsilon > 0$, any sampling time $\tau > 0$, and any state quantization $\mu_x > 0$ such that

Appendix C (1/1)

How to capture interaction between the symbolic model and the symbolic controller?

Approximate parallel composition

Def [Tabuada, IEEE-TAC-2008]

Given $T_1 = (Q_1, L_1, \longrightarrow_1, O_1, H_1)$ and $T_2 = (Q_2, L_2, \longrightarrow_2, O_2, H_2)$, with $O_1 = O_2$, and a precision $\theta > 0$, the approximate composition of T_1 and T_2 is the system

$$T_1 \,||_\theta\, T_2 = (Q, L, \longrightarrow, O, H)$$

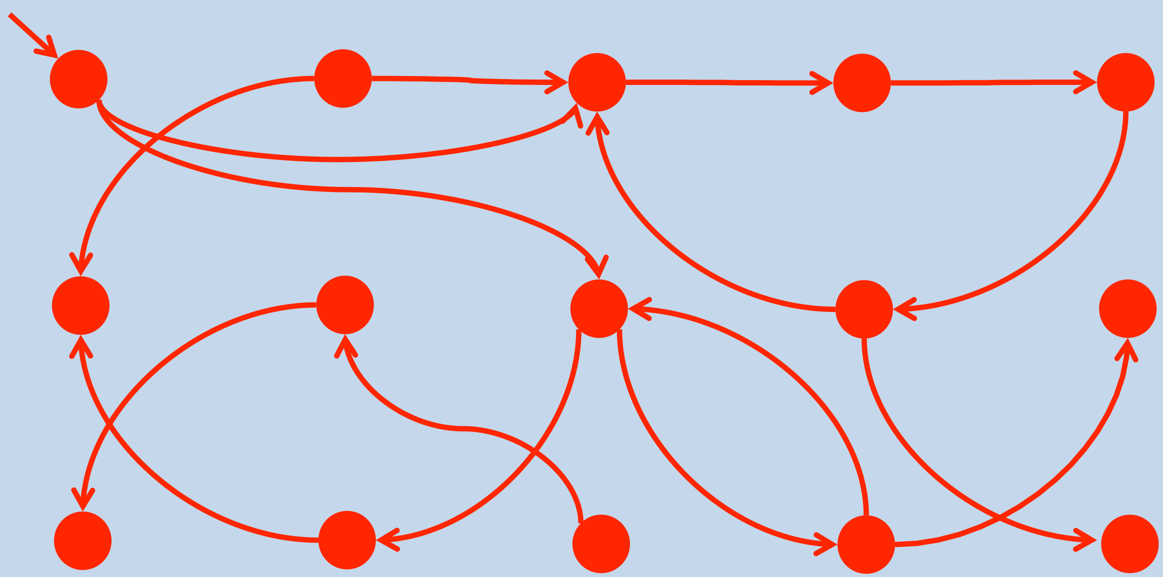
where:

- $Q = \{(q_1, q_2) \in Q_1 \times Q_2 : d(H_1(q_1), H_2(q_2)) \leq \theta\}$
- $L = L_1 \times L_2$
- $(q_1, q_2) \xrightarrow{(l_1, l_2)} (q'_1, q'_2)$, if $q_1 \xrightarrow{l_1}_1 q'_1$ and $q_2 \xrightarrow{l_2}_2 q'_2$
- $O = O_1$
- $H(q_1, q_2) = H_1(q_1)$

Appendix D (1/5)

Synthesis through a three-step process:

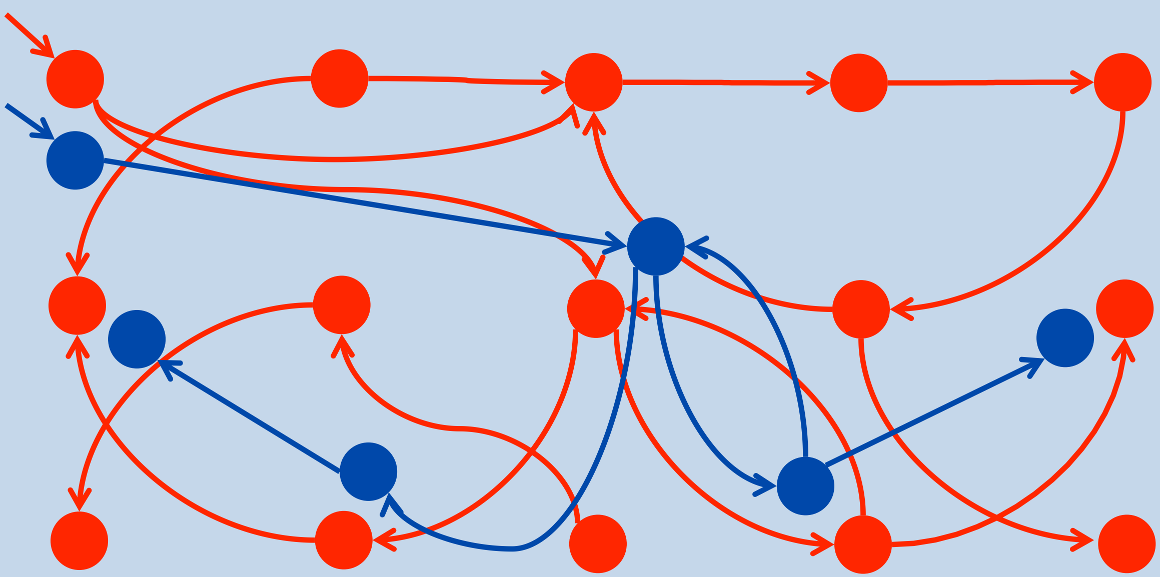
1. Compute the symbolic model $T^*(\Sigma)$ of Σ
2. Compute the approximate parallel composition $C^* = T^*(\Sigma) \,||_{\mu x}\, S$
3. Compute the maximal robust non-blocking part $Nb(C^*)$ of C^*



Appendix D (2/5)

Synthesis through a three-step process:

1. Compute the symbolic model $T^*(\Sigma)$ of Σ
2. Compute the approximate parallel composition $C^* = T^*(\Sigma) \,||_{\mu x}\, S$
3. Compute the maximal robust non-blocking part Nb(C*) of C*



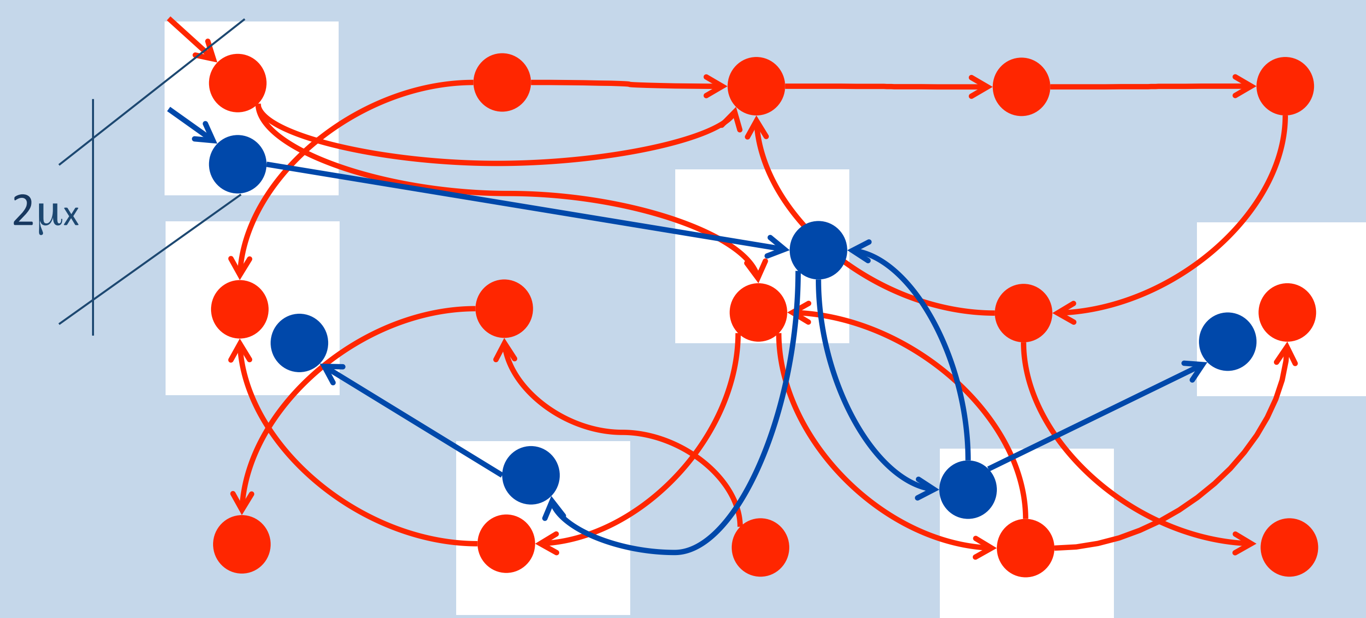
Appendix D (3/5)

Synthesis through a three-step process:

1. Compute the symbolic model $T^*(\Sigma)$ of Σ

2. Compute the approximate parallel composition $C^* = T^*(\Sigma) \,||_{\mu x}\, S$

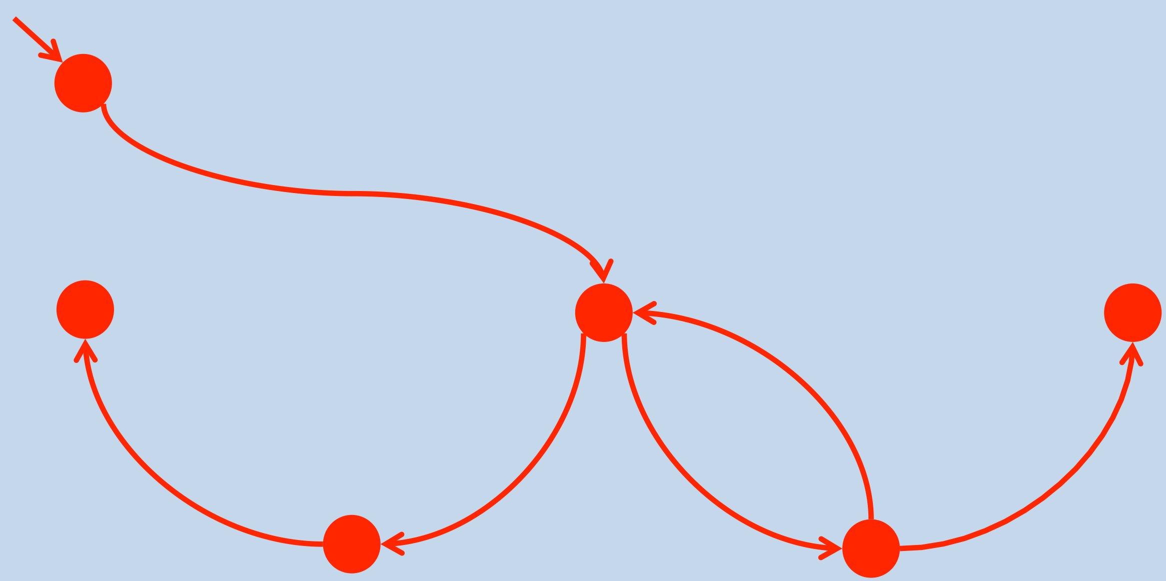
3. Compute the maximal robust non-blocking part $Nb(C^*)$ of C^*



Appendix D (4/5)

Synthesis through a three-step process:

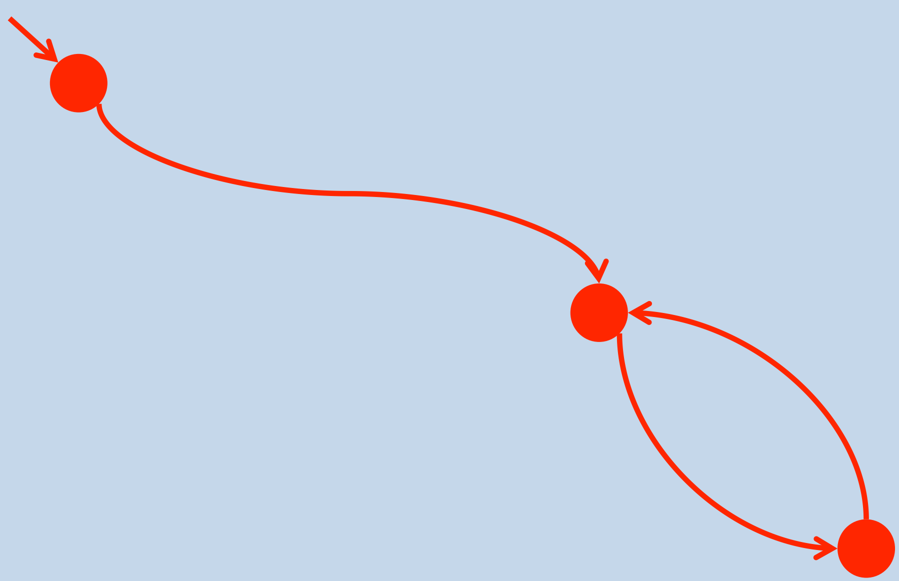
1. Compute the symbolic model $T^*(\Sigma)$ of Σ
2. Compute the approximate parallel composition $C^* = T^*(\Sigma) \,||_{\mu x}\, S$
3. Compute the maximal part $Nb(C^*)$ of C^*



Appendix D (5/5)

Synthesis through a three-step process:

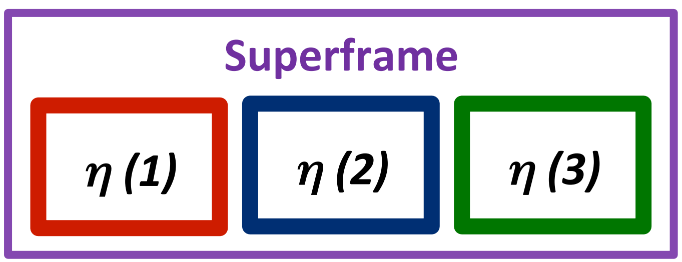
1. Compute the symbolic model $T^*(\Sigma)$ of Σ
2. Compute the approximate parallel composition $C^* = T^*(\Sigma) \,||_{\mu x}\, S$
3. Compute the maximal [illegible] part $Nb(C^*)$ of C^*

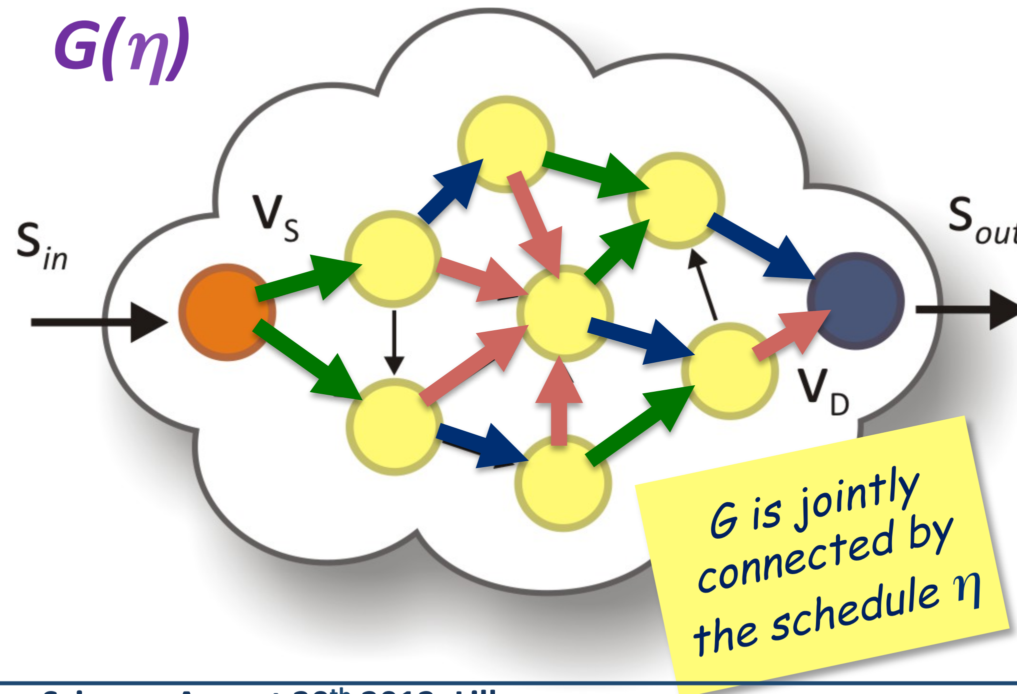


Appendix E – Joint connectivity

Definition: Given a multi-hop network *G* and the associated scheduling η, we define *G*(η) the subgraph of *G* induced by the set of all edges scheduled by η during the whole frame.

Definition: We say that *G* is jointly connected by the scheduling η if and only if there exists a path from the source node v_S to the destination node v_D in *G*(η).





Appendix F (1/2) – Conditions on $W{\downarrow}\mathcal{R}$

Consider a discrete-time MIMO LTI system described by the l x m transfer function matrix H(z).

$$\Theta \doteq \{(J,K): J \subseteq m, K \subseteq l, |J| = |K| \geq 1\}$$

Set of all combinations of rows and columns of a l x m matrix such that the number of rows is equal to the number of columns.

$$\left\{ \left| H_{J,K}(z) \right| : (J,K) \in \Theta \right\}$$

Set of all minors of H(z).

$$\psi_{J,K}^{H}(z) = \delta_H(z) \left| H_{J,K}(z) \right|$$

For $(J,K)\in\Theta$, are the zero polynomials of H(z), where dH(z) is the characteristic polynomial of H.

$$\psi^{H}(z) = \gcd\left(\psi_{J,K}^{H}(z), \forall (J,K) \in \Theta \right)$$

Least zero polynomial, namely the greatest common divisor of all zero polynomials of H(z).

Theorem [Tarokh, ACC-1986]: A MIMO LTI system with transfer function matrix H(z) is controllable and observable if and only if the scalar transfer function $\psi{\uparrow}H(z)/\delta{\downarrow}H(z)$ has no pole-zero cancelations.

Appendix F (2/2) – Conditions on $W\downarrow\mathcal{R}$

Lemma: The zero polynomials of a MCN M are given by the following expression:

$$\psi_{J,K}^{M}(z)=\delta_M(z)\cdot\left|O_{J,J}(z)\right|\cdot\left|P_{J,K}(z)\right|\cdot\left|R_{K,K}(z)\right|$$

where $\delta_M(z)=\delta_O(z)\,\delta_P(z)\,\delta_R(z),\ \forall\,(J,K)\in\Theta.$

Theorem: A MCN M is controllable and observable if and only if the following hold:

(5a) for all $i\in m$ and for all j$\in l$, the pairs $(G\downarrow R, \eta\downarrow R\downarrow i)$ and $(G\downarrow O, \eta\downarrow O\downarrow i)$ are jointly connected;

(5b) for each root p of $\delta\downarrow P(z)$, $\exists\,(J,K)\in\Theta\ s.t.\ \psi_{J,J}^{O}(\overline{p})\neq 0\wedge\psi_{J,K}^{P}(\overline{p})\neq 0\wedge\psi_{K,K}^{R}(\overline{p})\neq 0;$

(5c) $m=l$ and $\psi\downarrow l,m\uparrow(0)\neq 0$

Corollary : A MCN M is controllable and observable if Conditions (5a),(5c) hold and:

(6b) for each root p of $\delta\downarrow P(z)$, the numerators of $R\downarrow i(z)$ and of $O\downarrow i(z)$ do not have roots in p for all $i\in m$ and for all j$\in l$.