A unifying view of Loosely Time-Triggered Architectures

Albert Benveniste (Inria-Rennes) , **Paul Caspi** (Verimag)
Anne Bouillard (ENS)
Alberto Sangiovanni-Vincentelli
Stavros Tripakis, and Claudio Pinello

EMSOFT 2010 — revisited 2012

Motivation

Moving from Federated to Integrated Architectures:

- aeronautics: IMA
- automobile: AUTOSAR

Motivation

Moving from Federated to Integrated Architectures:

- aeronautics: IMA
- automobile: AUTOSAR

Model-based design processes:

- Platform-based Design [A. Sangiovanni-Vincentelli]
- COC tool at PSA; and more

Motivation

Moving from Federated to Integrated Architectures:

- aeronautics: IMA
- automobile: AUTOSAR

Model-based design processes:

- Platform-based Design [A. Sangiovanni-Vincentelli]
- COC tool at PSA; and more

Models of Computation and Communication (MoCC)

- for the functions (synchronous, Kahn Networks,. . .) with corresponding formalisms
- for the architectures

Motivation

TTA (Time-Triggered Architecture) [Kopetz]
A comprehensive MoCC-based architecture:

- strong synchrony
- global discrete notion of time
- time-based fault-tolerance
- time-based scheduling (TDMA)
- time-based interfaces

Motivation

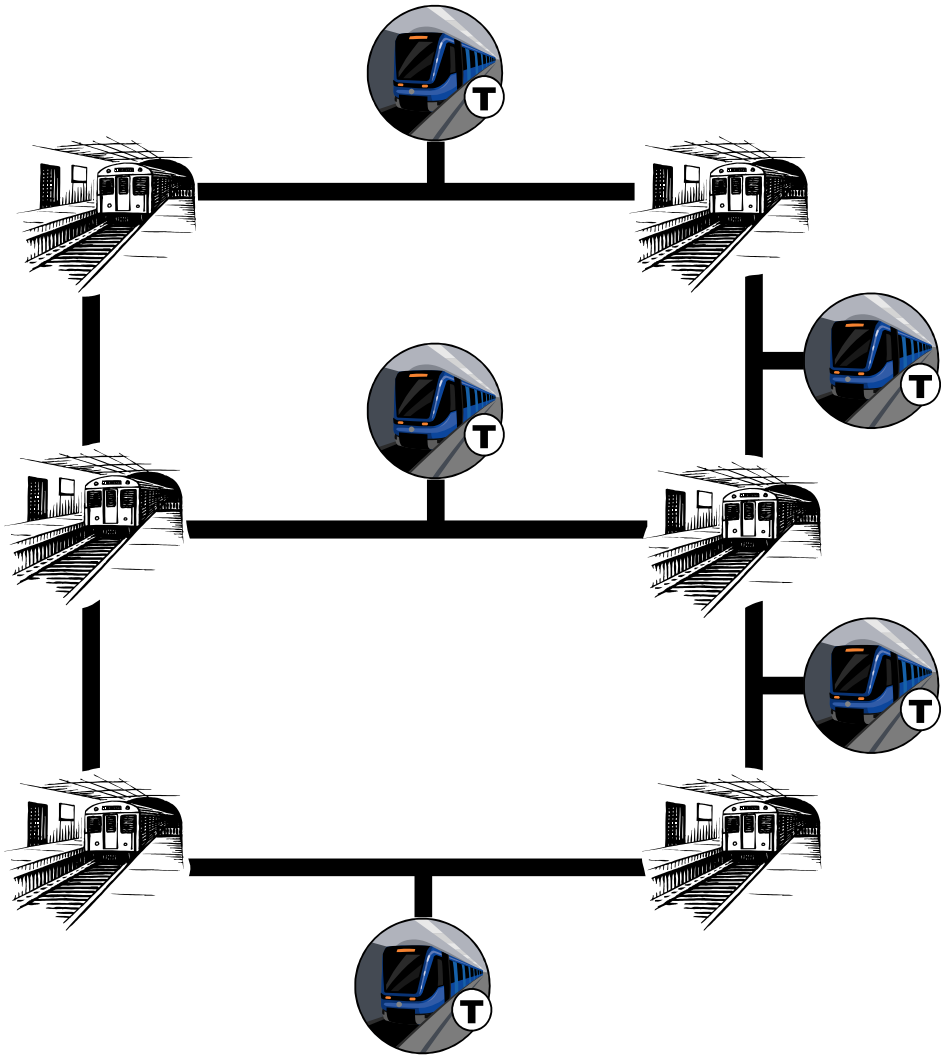
TTA (Time-Triggered Architecture) [Kopetz]
A comprehensive MoCC-based architecture:

- strong synchrony
- global discrete notion of time
- time-based fault-tolerance
- time-based scheduling (TDMA)
- time-based interfaces

Resistances to TTA:

- cost of synchronization
- rigidity of TDMA
- cost of re-design (adaptations & upgrades)

Motivation



Computers on trains for speed control

Computers on tracks for collision avoidance and to avoid losing a train (ghost train!!)

MBPC

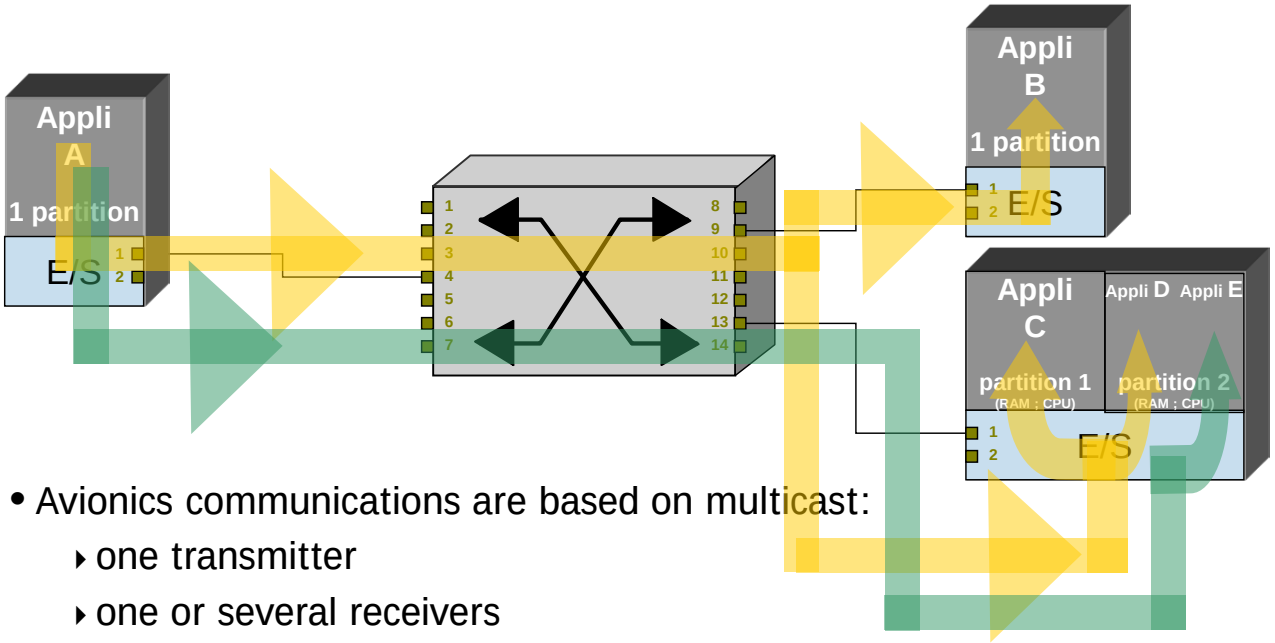
Wired communications for fixed computers

For computers on trains: use wheels or wireless

Communication by Sampling (LTTA)

Motivation

AFDX technology – Addressing : MAC,IP,UDP



- Avionics communications are based on multicast:
  - one transmitter
  - one or several receivers
- Asynchrony of individual clocks
- NO reconfiguration capability in the AFDX network

Alt = 10 000 ft	UDP SRC / UDP DEST	IP SRC / IP DEST	MAC SRC / MAC DEST

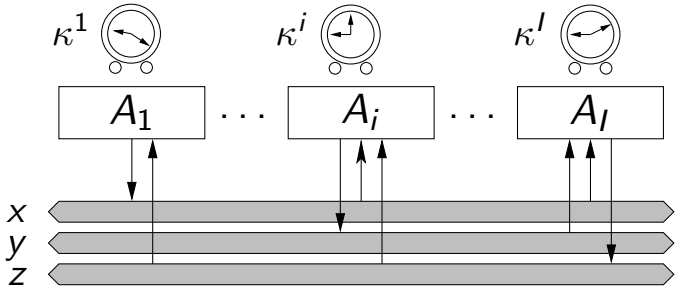
ARTIST2 - Integrated Modular Avionics A380 Page 1

Motivation

$\Longrightarrow$ **Relax TTA to LTTA**

(Loosely Time-Triggered Architecture)

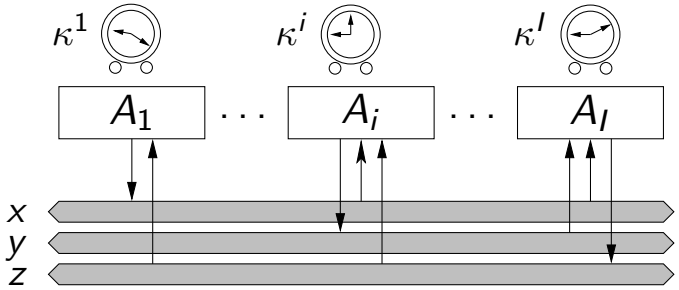
Loosely Time-Triggered Architecture



Communication by Sampling (CbS)

1. Communication medium $\sim$ set of shared memories, 1 per variable
2. Each computer periodically samples its external world
   And so does the communication medium itself

Loosely Time-Triggered Architecture



Communication by Sampling (CbS)

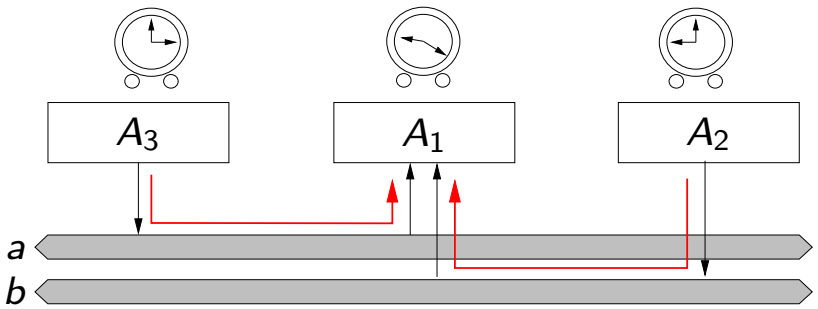
1. Communication medium $\sim$ set of shared memories, 1 per variable
2. Each computer periodically samples its external world
   And so does the communication medium itself

Advantages:

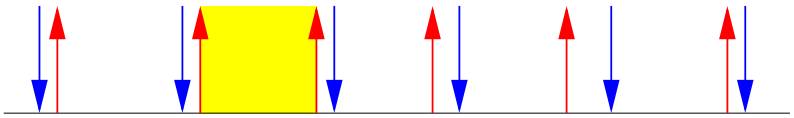
- communication medium off-the-shelf;
- autonomy, no deadlock, no livelock;

Results, however, in losses and duplications.

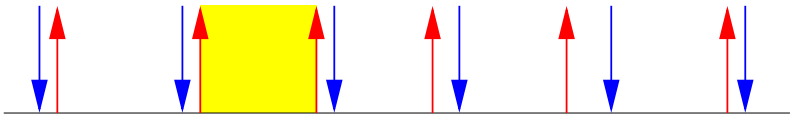
Loosely Time-Triggered Architecture



Problems when writing/sensing with non synchronized clocks:

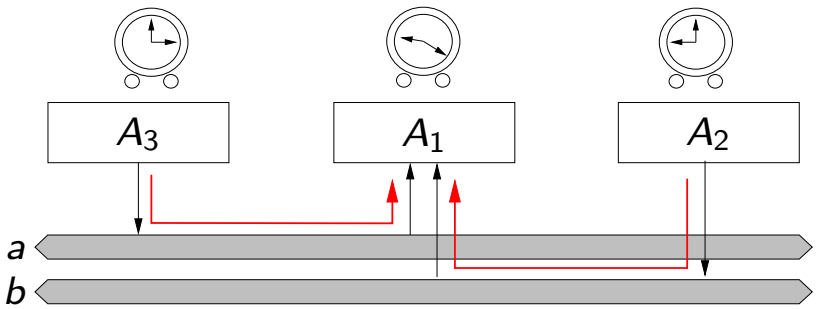


duplications

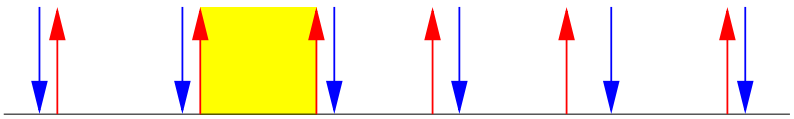


losses

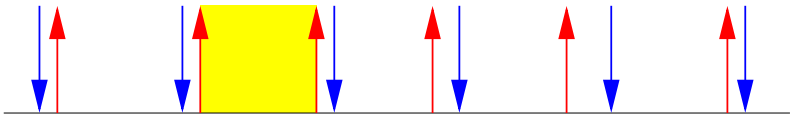
Loosely Time-Triggered Architecture



Problems when writing/sensing with non synchronized clocks:

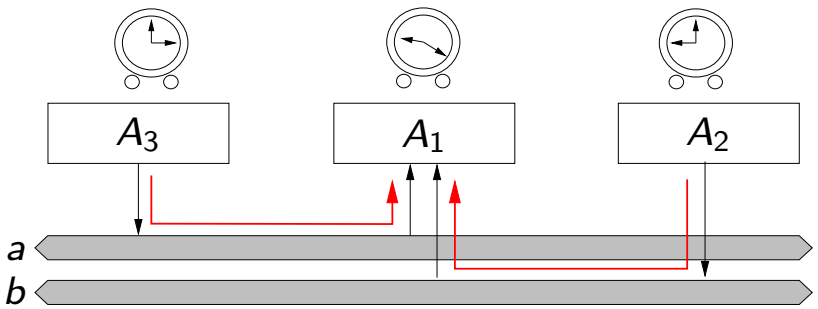


no harm so far for continuous feedback control

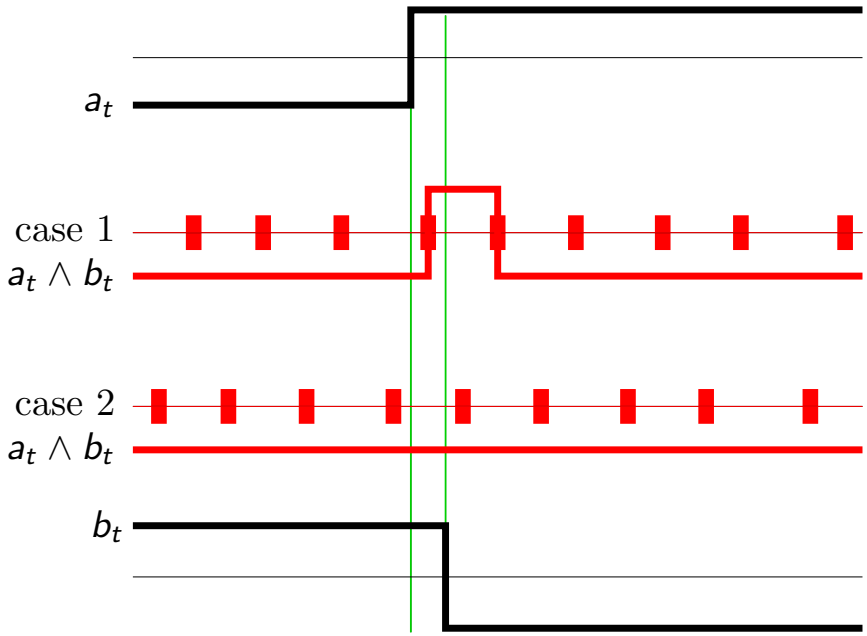


RT-Builder [Geensys→DS]
JitterBug/TrueTime [Arzen]

Loosely Time-Triggered Architecture

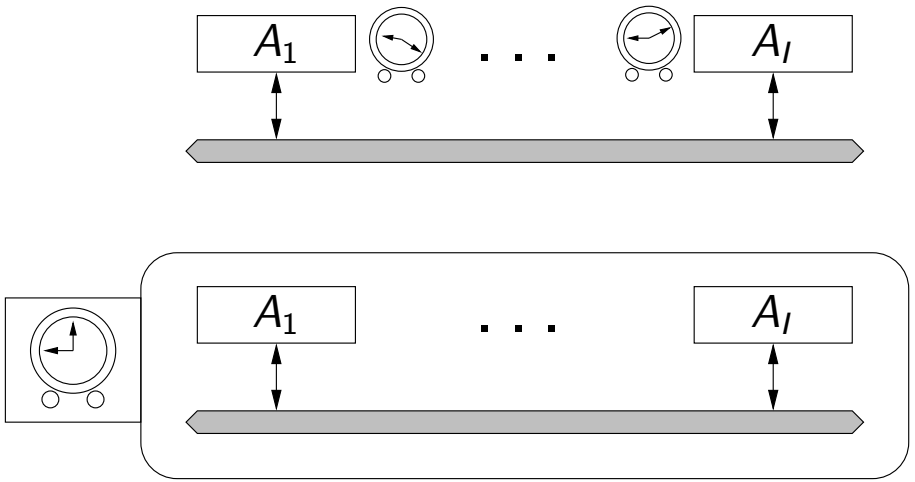


Problems when writing/sensing multiple discrete signals:



Cases 1 and 2 correspond to two different outcomes for the local clock of A_1.

Preservation of the semantics: setting the problem



ensuring flow equivalence between LTTA Design (top) and Synchronous Design (bottom).

Flow equivalence ensured by a special *LTTA protocol*.

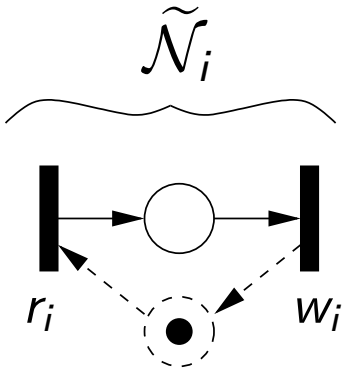
Two approaches:

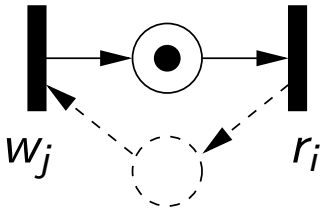
- building on *back-pressure* and *elastic circuits*
- building on *time*

Back-Pressure LTTA

top: Node as a Net
reads and writes alternate

bottom: Link as a Net
1-buffer on each link



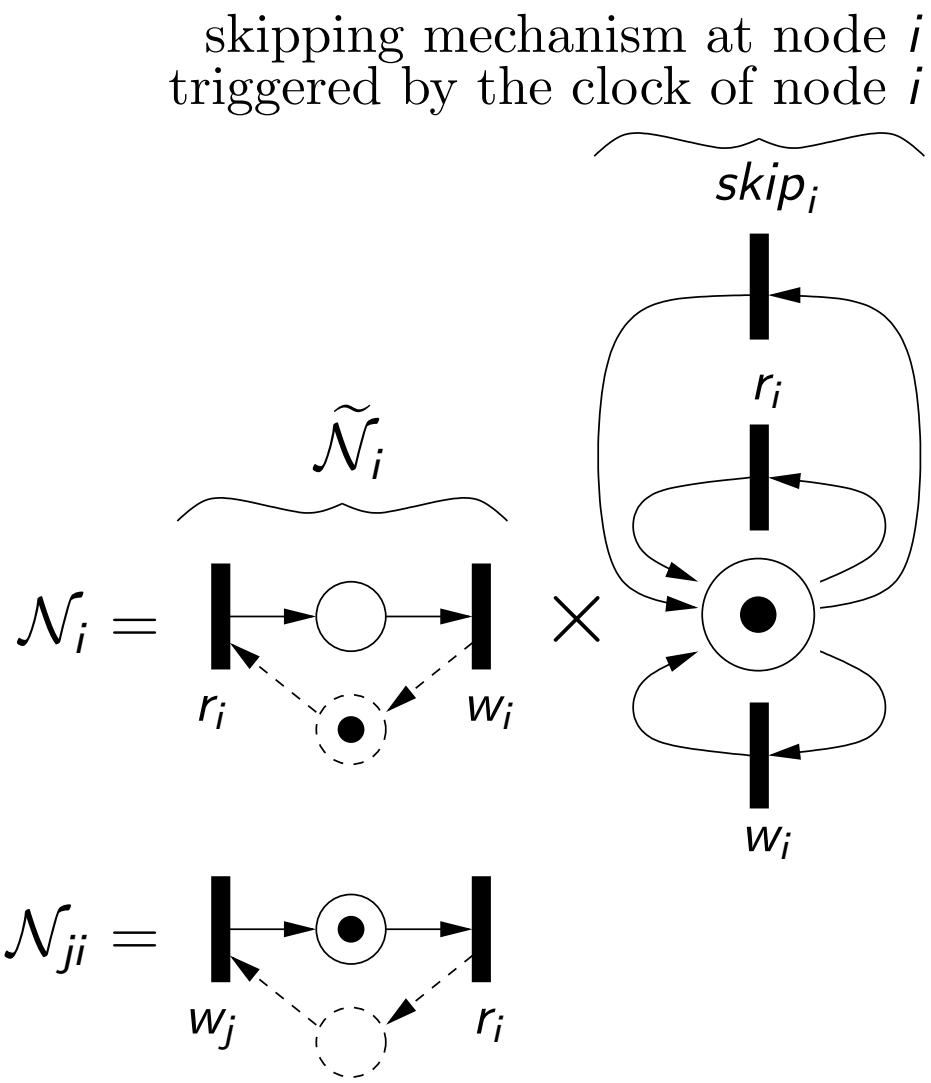
$\mathcal{N}_{ji} =$ 

$\mathcal{N}_{ji}$: directed link $j \to i$
dashed: back-pressure

$$\left(\prod_i \widetilde{\mathcal{N}}_i\right) \times \left(\prod_{j \to i} \mathcal{N}_{ji}\right)$$

elastic circuit (BP-EC)

Back-Pressure LTTA



$\mathcal{N}_{ji}$: directed link $j \to i$
dashed: back-pressure

$$\left(\prod_i \widetilde{\mathcal{N}}_i\right) \times \left(\prod_{j \to i} \mathcal{N}_{ji}\right)$$

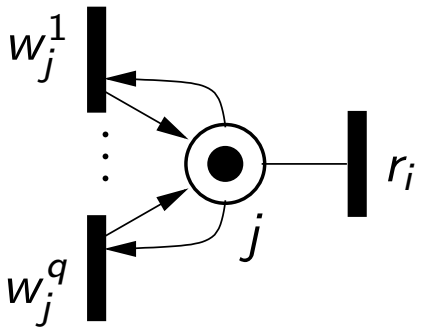
elastic circuit (BP-EC)

$$\left(\prod_i \mathcal{N}_i\right) \times \left(\prod_{j \to i} \mathcal{N}_{ji}\right)$$

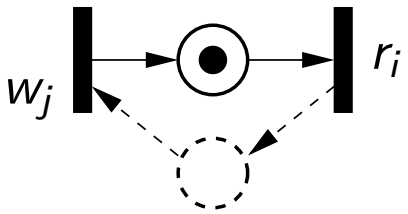
BP-LTTA

Time-based LTTA: difficulty

$\mathcal{M}_{ji} =$



$\mathcal{N}_{ji} =$



Time-based, pure CbS link (top), is compared to BP-link (bottom)

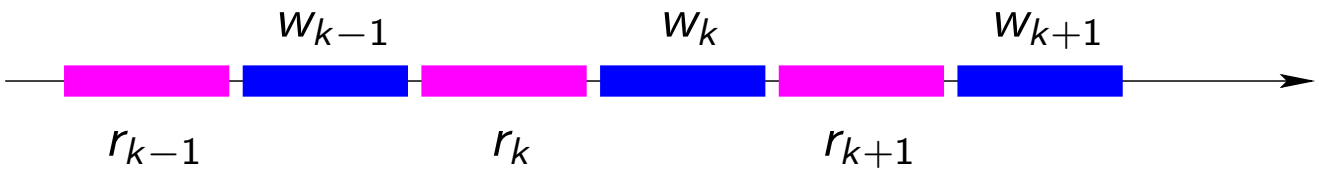
Observe the read arc and lack of synchronization that results

To recover synchronization:

- slow-down by synchronizing on *local* physical time
- accelerate using a token-based *publication* mechanism

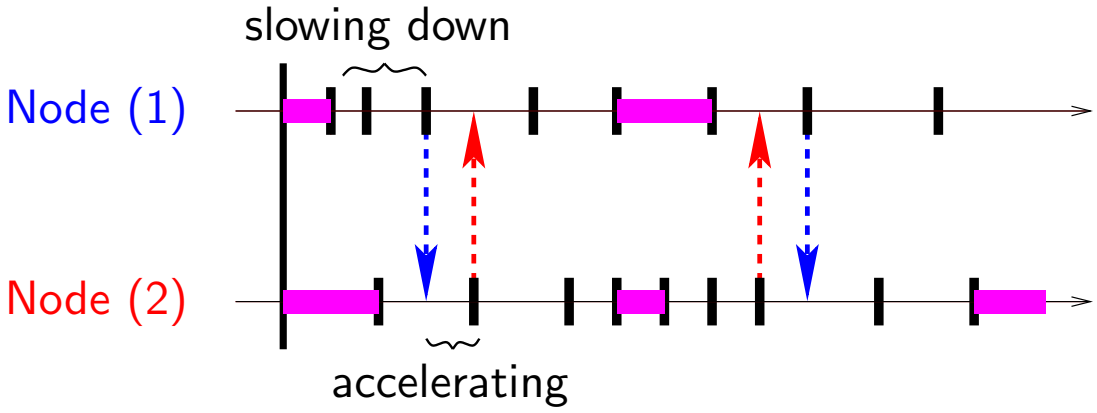
Time-based LTTA: general principle

Aim: ensure a clean alternation of writing and reading phases throughout the entire architecture.

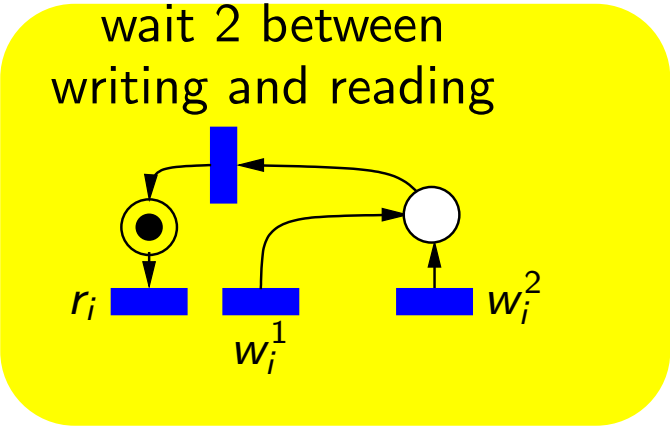


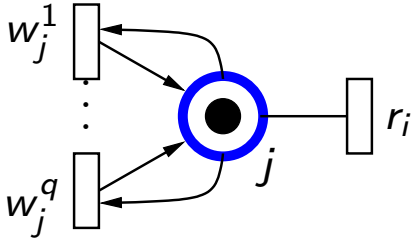
To recover synchronization:

- slow-down by synchronizing on *local* physical time
- accelerate using a token-based *publication* mechanism



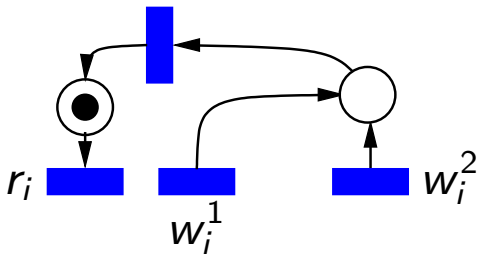
Time-based LTTA: distributed protocol (2 nodes)

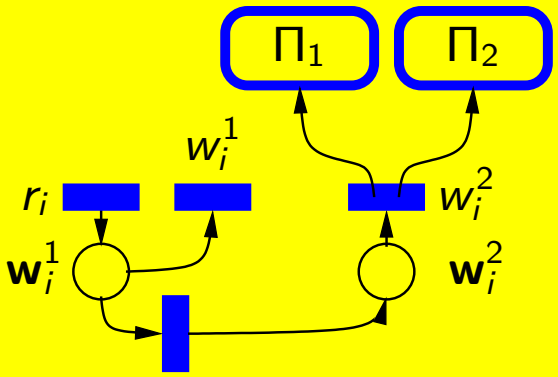




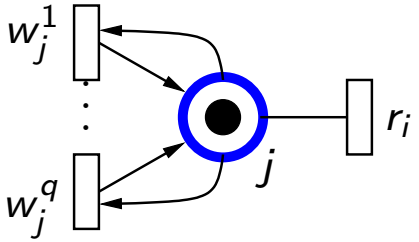
Time-based LTTA: distributed protocol (2 nodes)

wait 2 between
writing and reading



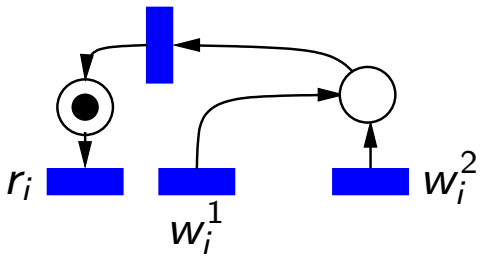


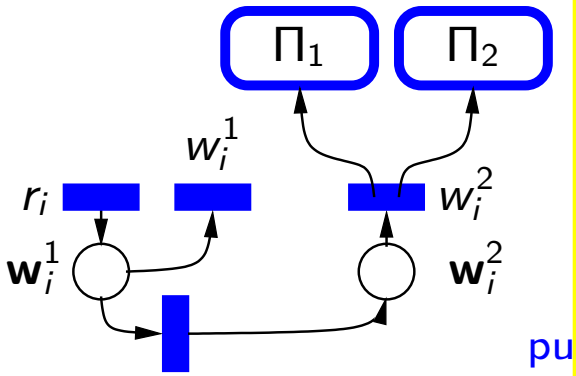
wait before writing
and publishing



Time-based LTTA: distributed protocol (2 nodes)

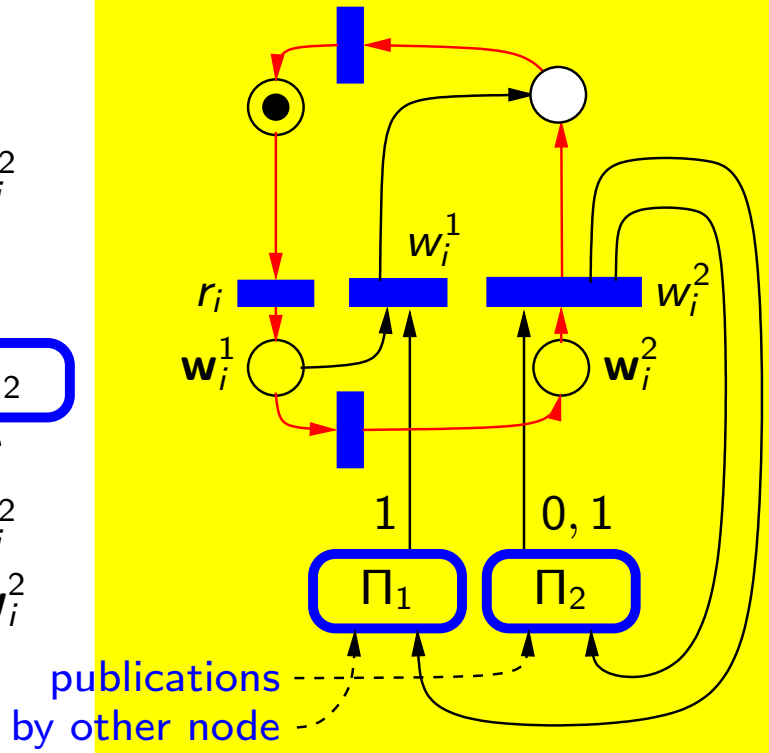
wait 2 between writing and reading



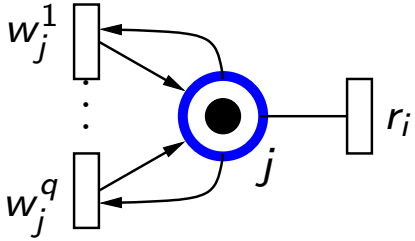


wait before writing and publishing

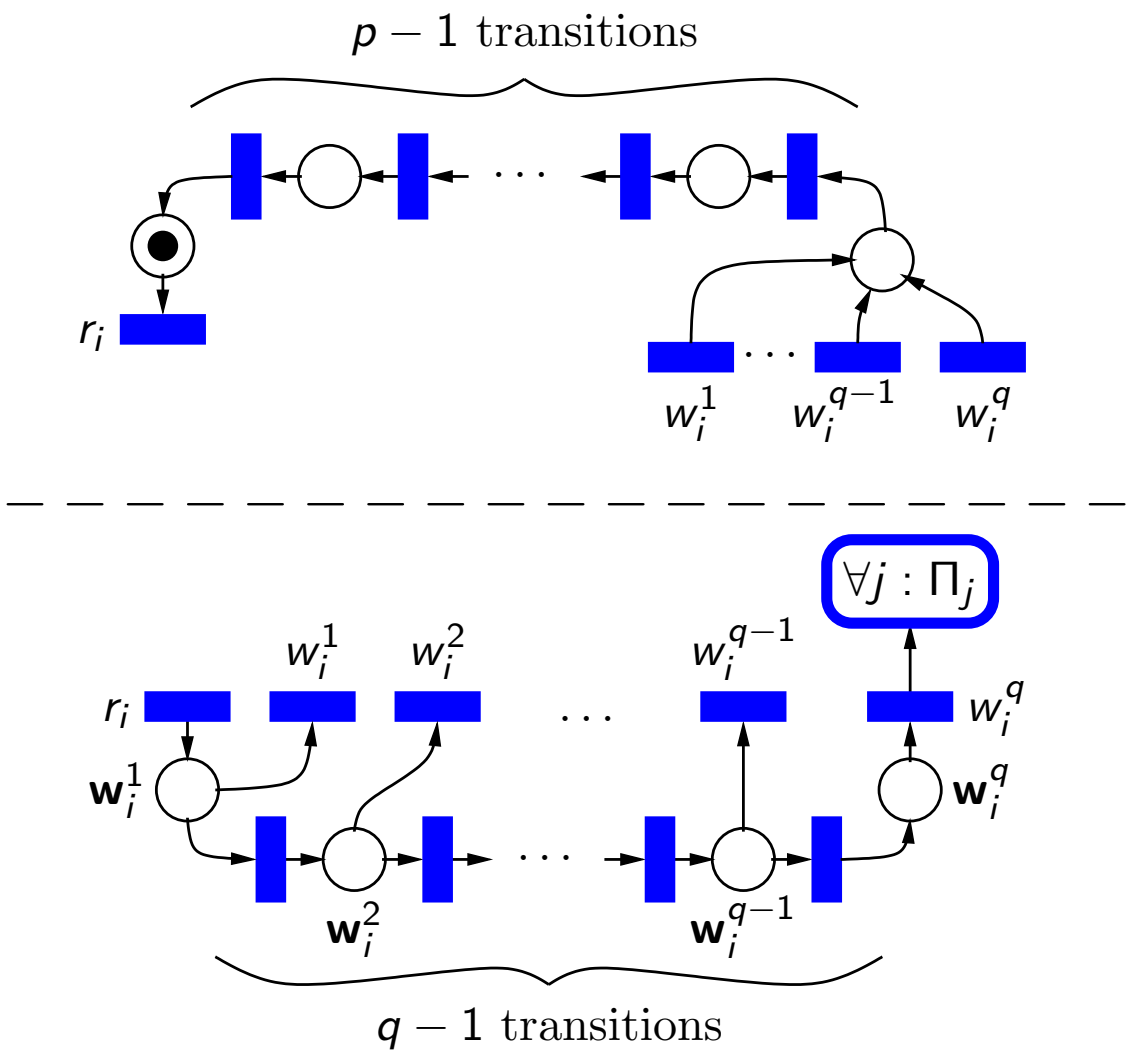
synchronize writings



on publications

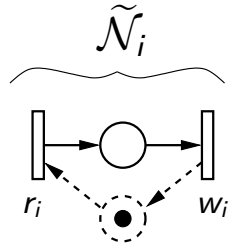


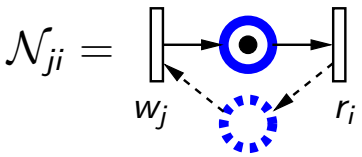
Time-based LTTA: distributed protocol (general)



Back-pressure LTTA performance

- Inter-tick time of local clocks: $T_{\min} \leq \kappa^i_{k+1} - \kappa^i_k \leq T_{\max}$
- Communication delays: $\tau \leq \tau_{\max}$.



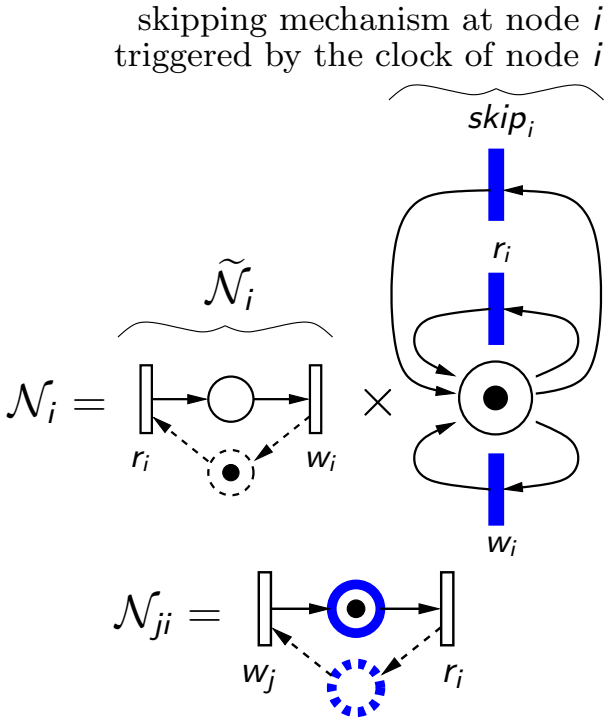


Back-Pressure LTTA

Elastic circuit: $\lambda_{\widetilde{\mathcal{N}}} = \frac{1}{2(\bar{T}_{max} + \bar{\tau}_{\max})}$

Back-pressure LTTA performance

- Inter-tick time of local clocks: $T_{\min} \leq \kappa^i_{k+1} - \kappa^i_k \leq T_{\max}$
- Communication delays: $\tau \leq \tau_{\max}$.



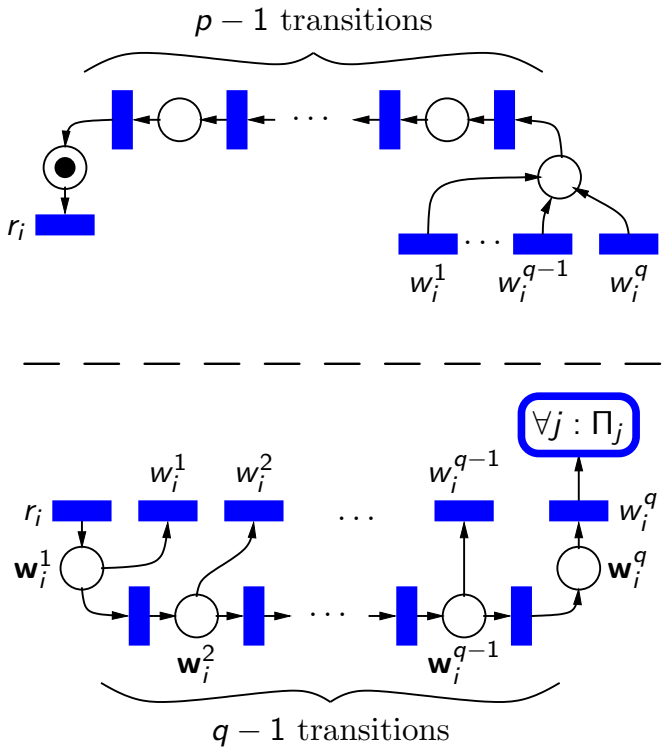
Back-Pressure LTTA

Elastic circuit: $\lambda_{\widetilde{\mathcal{N}}} = \frac{1}{2(\bar{T}_{max}+\bar{\tau}_{\max})}$

With skipping mechanism: $T_{max} = \bar{T}_{\max}$ and $\tau_{\max} = \tau_{\max} + T_{\max}$

$$\lambda_{\mathcal{N}} = \frac{1}{4\,\bar{T}_{max} + 2\bar{\tau}_{\max}}$$

Time-based LTTA performance

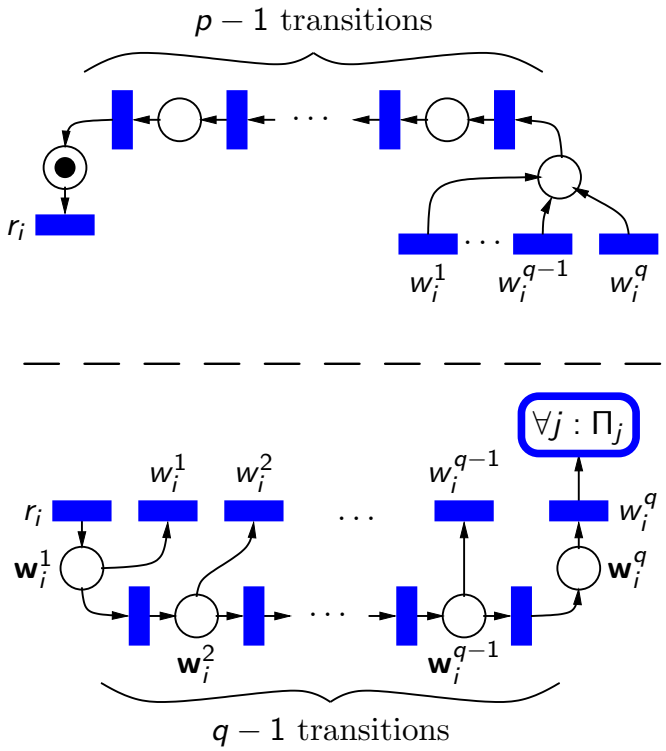


Tuning p and q

Rd The k-th firing of transition r_i occurs only after after all places Π_j have been written $k-1$ times.

Wr The kth firing of one of the (conflicting) transitions $w_i^1 \ldots w_i^q$ occurs only after transitions $r_j, j = 1 \ldots n$ have all been fired k times.

Time-based LTTA performance



Theorem

These conditions on p, q ensure $\hat{\mathcal{L}}_{\mathcal{M}} = \mathcal{L}_{\widetilde{\mathcal{N}}}$:

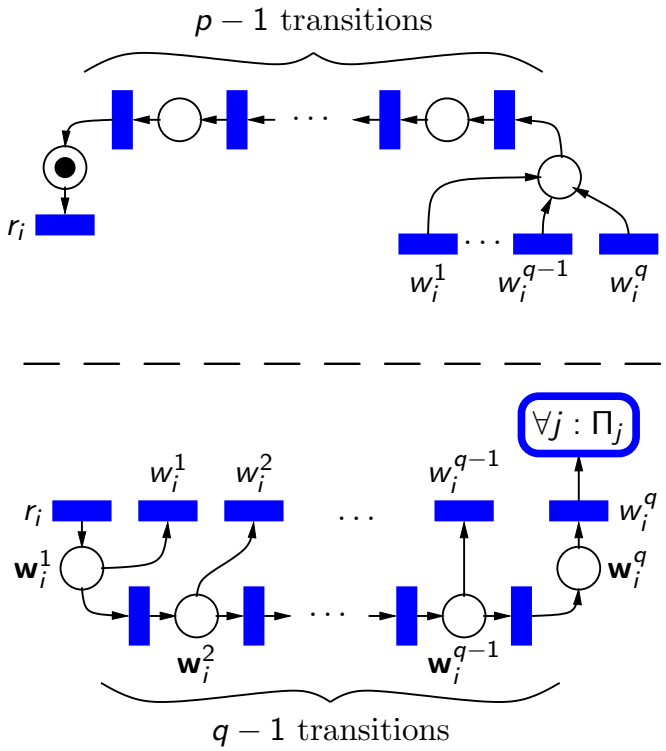
$$\begin{aligned} p &\geq \frac{\tau_{\max}}{T_{\min}} + \frac{T_{\max}}{T_{\min}} \\ q &\geq \frac{\tau_{\max}}{T_{\min}} + \frac{T_{\max}}{T_{\min}} + p\left(\frac{T_{\max}}{T_{\min}} - 1\right) \end{aligned}$$

Theorem

Worst case throughput ($p_\star$ and $q_\star$ optimal) :

$$\lambda_{\mathcal{M}} = \frac{1}{(p_\star + q_\star)T_{\max}}$$

Time-based LTTA performance



Theorem

These conditions on p, q ensure $\hat{\mathcal{L}}_{\mathcal{M}} = \mathcal{L}_{\widetilde{\mathcal{N}}}$:

$$\begin{aligned} p &\geq \frac{\tau_{\max}}{T_{\min}} + \frac{T_{\max}}{T_{\min}} \\ q &\geq \frac{\tau_{\max}}{T_{\min}} + \frac{T_{\max}}{T_{\min}} + p\left(\frac{T_{\max}}{T_{\min}} - 1\right) \end{aligned}$$

Theorem

Worst case throughput ($p_\star$ and $q_\star$ optimal) :

$$\lambda_{\mathcal{M}} = \frac{1}{(p_\star + q_\star)\, T_{\max}}$$

t:	date of the first $(k-1)$th writing
last $k-1$th writing:	$t_w \leq \min(t + qT_{\max}, t + \tau_{\max} + T_{\max})$
first kth reading:	$t_r \geq t + pT_{\min}$
	$pT_{\min} \geq \tau_{\max} + T_{\max}$
	$\min(qT_{\max}, \tau_{\max} + T_{\max}) + pT_{\max} \leq \tau_{\max} + (p+1)T_{\max}$

Comparison regarding throughput

- BP-LTTA: lower bound for throughput is

$$1/\lambda_{\mathcal{N}} = 4\,T_{\max} + 2\tau_{\max}$$

- Time-LTTA when delay and jitter small relative to nominal period
  The lower bound for the throughput is

$$1/\lambda_{\mathcal{M}} \approx 4\,T_{\max}$$

- Time-LTTA for distant communications, i.e.,

$$\frac{T_{\max}}{T_{\min}} \approx 1 \text{ and } \frac{\tau_{\max}}{T_{\min}} \gg 1$$

  The lower bound for the throughput is

$$1/\lambda_{\mathcal{M}} \approx 2\left(\frac{T_{\max}}{T_{\min}}\right)^2 \tau_{\max} \approx 1/\lambda_{\mathcal{N}}$$

Conclusion

- Relaxing TTA to LTTA while preserving MoCC
- Back-Pressure LTTA & Time-Based LTTA
- Similar performances w.r.t. throughput
- BP-LTTA more flexible & TB-LTTA more robust

- Blending the two (see paper)

- Services must be studied:
  - fault tolerance
  - scheduling
  - interfacing