A General Framework for Nondeterministic, Probabilistic, and Stochastic Noninterference

Alessandro Aldini

University of Urbino “Carlo Bo”, Italy

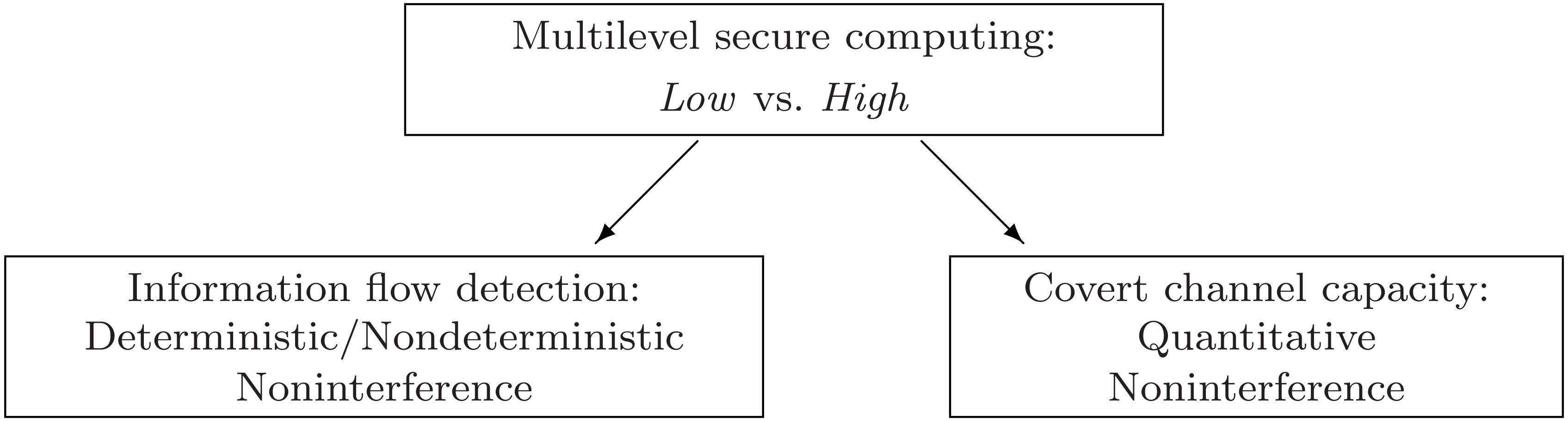
aldini@sti.uniurb.it

joint work with Marco Bernardo

Outline

- Noninterference and fine-grain models
- Noninterference properties and covert channels
- Formal framework
- Future work

Noninterference and fine-grain models



Multilevel secure computing:
Low vs. *High*

Information flow detection:
Deterministic/Nondeterministic
Noninterference

Covert channel capacity:
Quantitative
Noninterference

- exact analysis
- 0/1 result

Nondeducibility (Sutherland), Causality (Roscoe)
Nondeducibility on Strategies (Wittbold&Johnson)
Generalized Noninterference, Restrictiveness (McCullough, McLean)
Nondeducibility on Compositions (Focardi&Gorrieri)

- approximate analysis
- Probabilistic noninterference: $[0;1]$ result

  Gray, Dipierro et al., Aldini et al., Smith, Sabelfeld and Sands, . . .
- Stochastic noninterference

  Aldini and Bernardo

Unifying framework

- Stochastically timed process algebra encompassing: nondeterminism, probability, priority, and (stochastic) time
- Weak nondeterministic/probabilistic/extended-Markovian bisimulation
- Modeling expressiveness and wide-developed theory for numerical analysis

Noninterference properties: an example

Bisimulation-Based Strong Noninterference **BSNI**:

1. BS**N**NI: P is secure iff $P/Name_H \approx_{\mathrm{B}} P\backslash Name_H$

2. BS**P**NI: P is secure iff $P/Name_H \approx_{\mathrm{PB}} P\backslash Name_H$

3. BS**S**NI: P is secure iff $P/Name_H \approx_{\mathrm{EMB}} P\backslash Name_H$

1. is sensitive to functional covert channels
2. adds quantitative covert channels based on probability distributions associated with event execution
3. adds quantitative covert channels based on the timing of events, described through exponentially distributed random variables

I

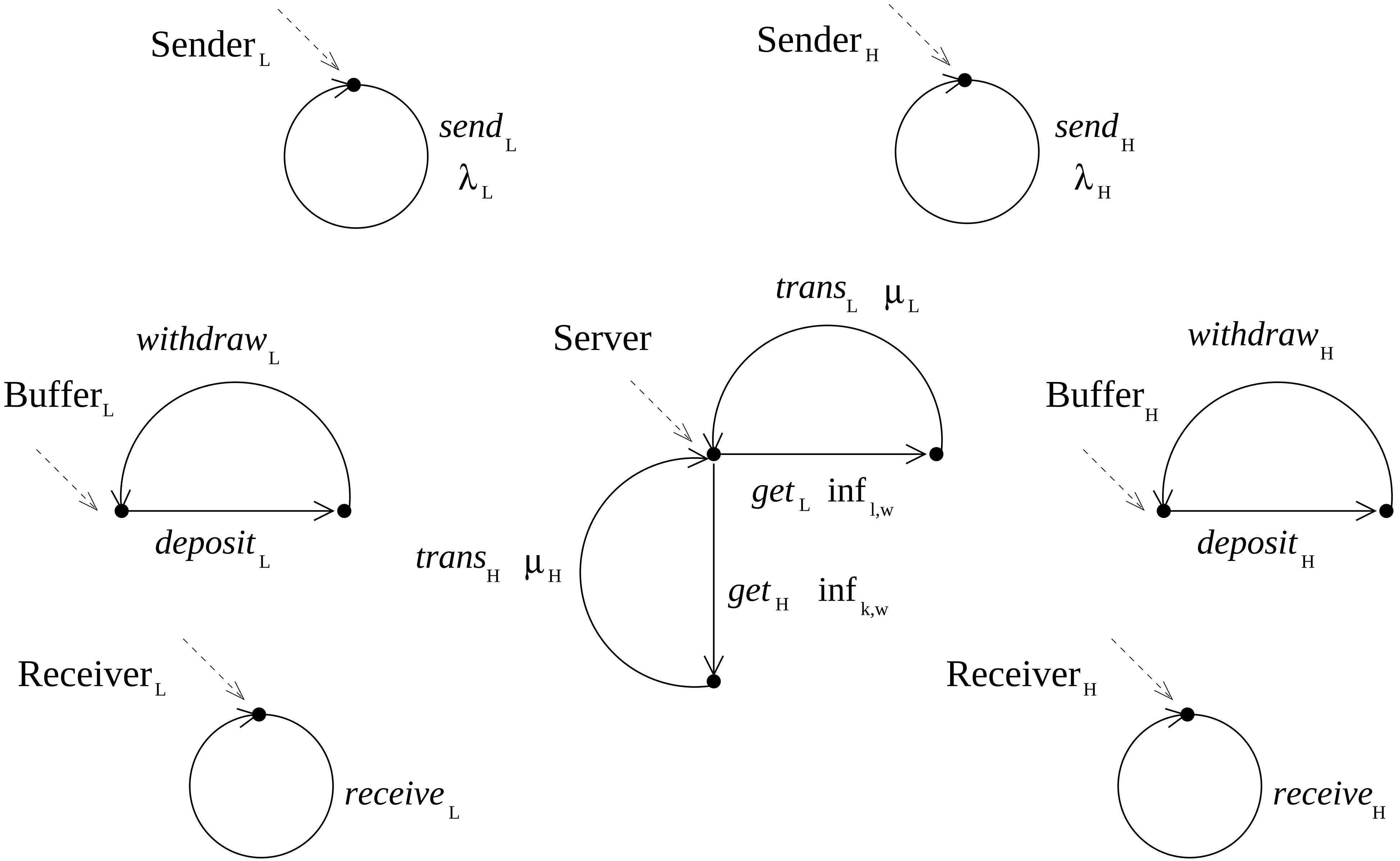
Noninterference properties: an example

Bisimulation-Based Strong Local Noninterference **BSLNI**:

P is secure iff $\forall P' \in Der(P)$ and $\forall P''$ such that $P' \xrightarrow{a,\tilde{\lambda}} P''$, with $a \in Name_H$, $P' \backslash Name_H \approx_\eta P'' \backslash Name_H$.

- $\eta \in \{\mathrm{B}, \mathrm{PB}, \mathrm{EMB}\}$.
- It is very restrictive.
- It ensures that the low-level user cannot distinguish which, if any, high-level event has occurred at some point in the past.

Example: multilevel security routing system



Example: multilevel security routing system

BS**N**NI based analysis

- Semantics: labeled transition system.
- Noninterference check: positive.
- Conclusion: the availability to serve low messages is never compromised independently of the behavior of the high sender.

Example: multilevel security routing system

BS**P**NI based analysis

- Semantics: labeled probabilistic transition system.
- Noninterference check: positive.
- Conclusion: the high activities are not able to alter the probabilistic choices that can be observed at the low level.

Example: multilevel security routing system

BS**S**NI based analysis

- Semantics: labeled continuous-time Markov chain.
- Noninterference check: negative.
- Diagnostic information: modal logic formulas.

- the high sender is immediately revealed by the low receiver, because it describes a working process competing for the resource time with the other durational processes
- whenever the high sender is blocked because the related buffer is not available to accept further requests, then it does not compete for the resource time anymore, thus revealing to the low receiver that the high buffer is full
- the time spent by the server to deliver high messages describes an observable busy-waiting phase

Methodological approach

Performance-oriented perspective:

the feedback reveals that the low productivity of the system, in terms of number of low messages delivered per unit of time to the low receiver, changes depending on the presence/absence of high interactions.

Use the diagnostic information to:

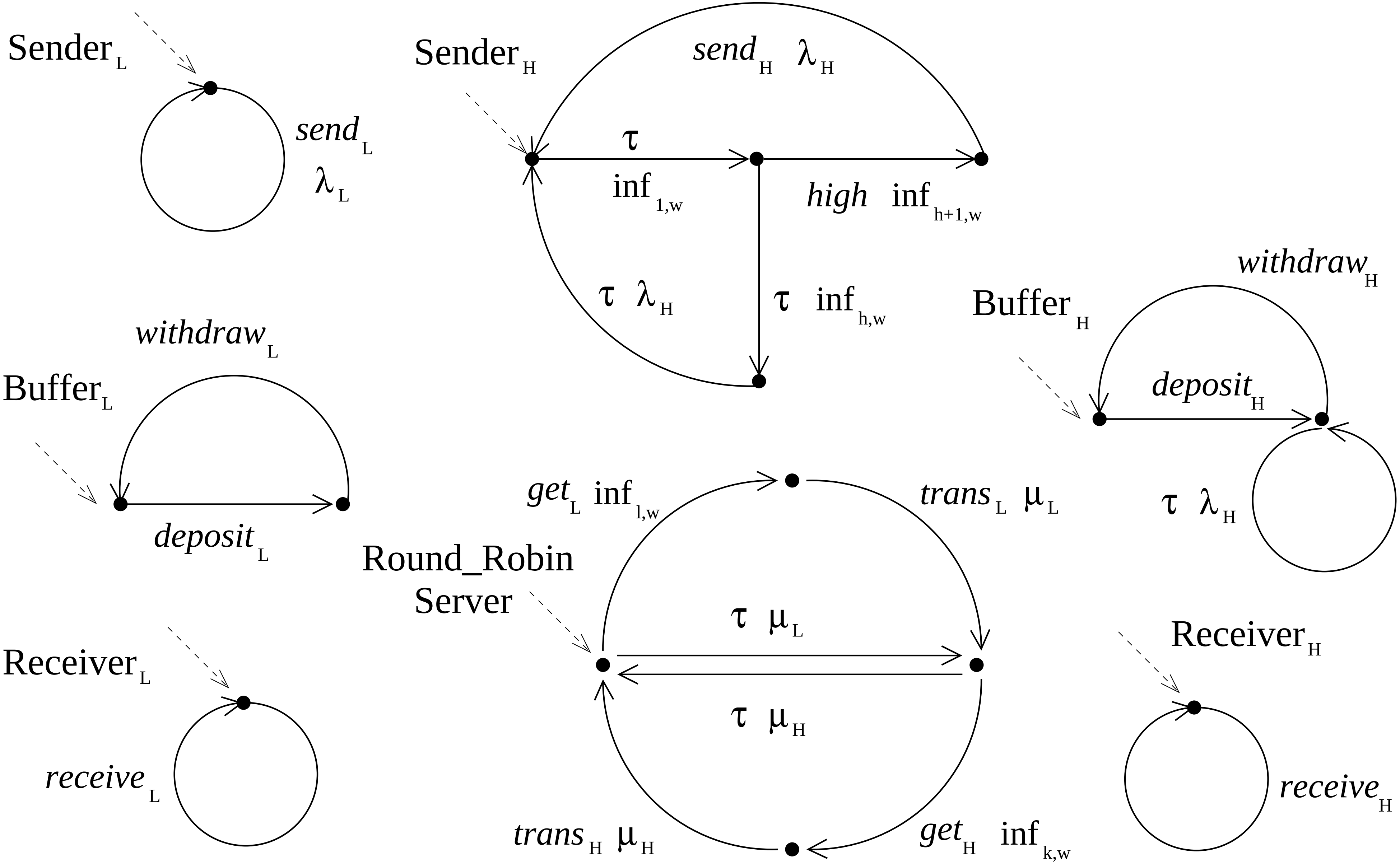
- pinpoint the information flow and solve it through adequate securing strategies
- measure the performance metric revealing the information flow (e.g.: reward-based steady-state numerical analysis reveals the information leakage on the long run)

Methodological Approach

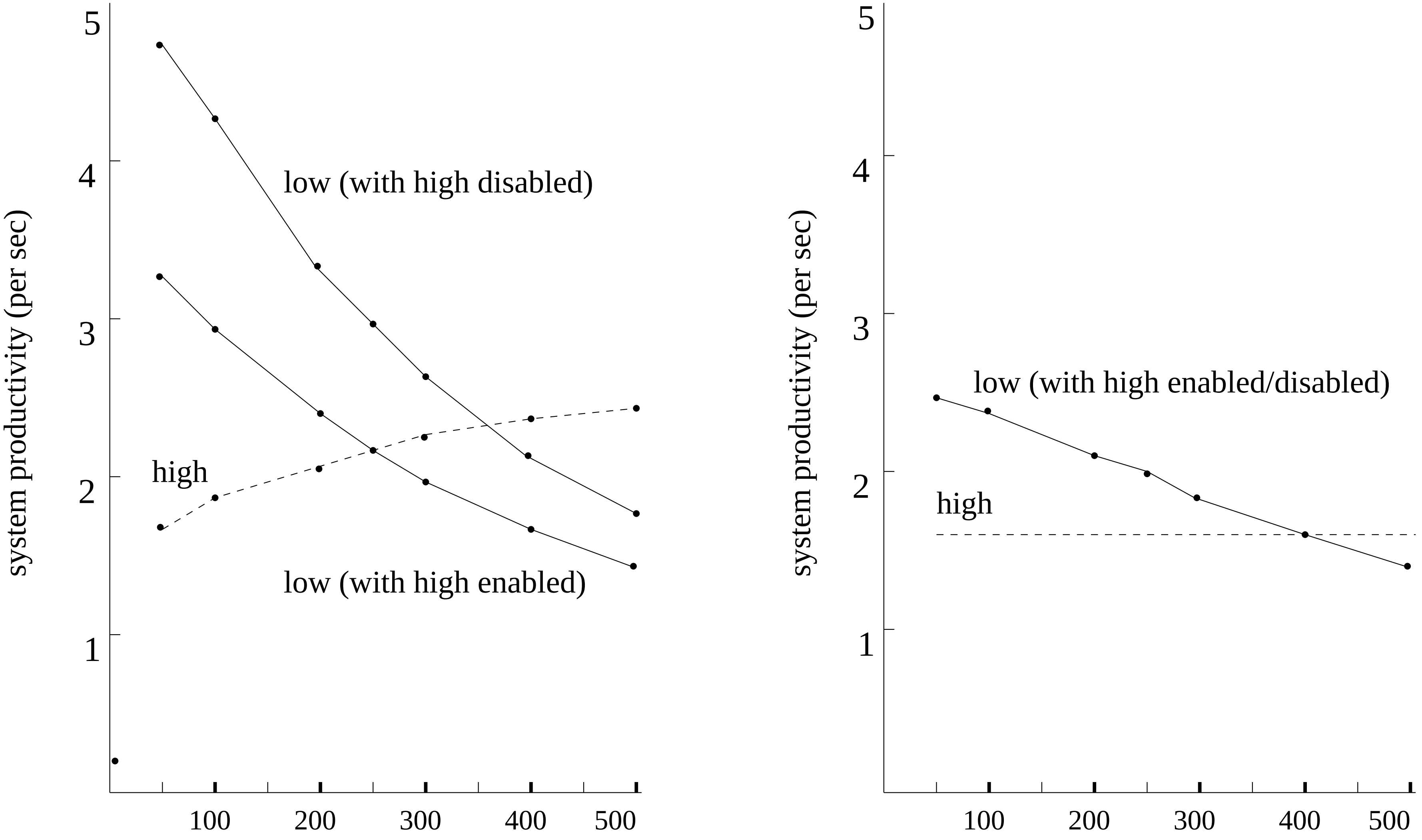
Problem: trading the results of these operations.

1. Tolerance thresholds: negligible difference with respect to a family of performance metrics of interest establish the tolerance to unwanted information flows
2. Approximate analysis: relaxed notion of behavioral equivalences are used to estimate the difference between the system views to compare and to relate them whenever they are similar but do not behave exactly the same

Example: multilevel security routing system



Example: performance evaluation



(a) low sending frequency (msec)

(b) low sending frequency (msec)

Markovian process calculus

Features:

- durational actions – three kinds:
  - exponentially timed: $<a, \lambda>$ with $\lambda \in \mathbb{R}_{>0}$
  - prioritized weighted immediate: $<a, \infty_{l,w}>$, where $l \in \mathbb{N}_{>0}$ is the priority level and $w \in \mathbb{R}_{>0}$ is the weight
  - constrained weighted passive: $<a, *_{w}^{l'}>$, where $l' \in \mathbb{N}$ is the priority constraint and $w \in \mathbb{R}_{>0}$ is the weight
- multiway communication based on a mixture of the generative and reactive models

Markovian process calculus

The set of process terms is generated by the following syntax:

$$P ::= \underline{0} \mid {<}a, \tilde{\lambda}{>}.P \mid P + P \mid A \mid P/L \mid P \parallel_S P$$

The semantics for a closed and guarded process term P is given by the labeled multitransition system $[\![P]\!]$.

Bisimulation semantics

Markovian bisimulation equivalence relates two process terms whenever they are able to mimic each other's functional and performance behavior stepwise.

Basic concept: **exit rate** – the rate at which a process term can execute actions of a certain name that lead to a certain set of terms and is given by the sum of the rates of those actions due to the race policy.

- Exit rates of process terms are compared by taking into account the three kinds of actions
- Pre-emption due to actions of the form $<\tau, \infty_{l,w}>$ is taken into account
- Abstraction of immediate τ-actions

Bisimulation semantics

An equivalence relation $\mathcal{B} \subseteq \mathcal{P} \times \mathcal{P}$ is a weak extended Markovian bisimulation iff, whenever $(P_1, P_2) \in \mathcal{B}$, then for all action names $a \in \mathit{Name}$ and levels $l \in \mathbb{Z}$ such that $\mathit{no\text{-}pre}(l, P_1)$ and $\mathit{no\text{-}pre}(l, P_2)$:

$$\begin{array}{rcll} \mathit{rate}_{\mathrm{w}}(P_1, a, l, C) & = & \mathit{rate}_{\mathrm{w}}(P_2, a, l, C) & \text{for all observable } C \in \mathcal{P}/\mathcal{B} \\ \mathit{rate}_{\mathrm{w}}(P_1, a, l, \mathcal{P}_{\mathrm{fu}}) & = & \mathit{rate}_{\mathrm{w}}(P_2, a, l, \mathcal{P}_{\mathrm{fu}}) & \end{array}$$

Weak extended Markovian bisimilarity, denoted by $\approx_{\mathrm{EMB}}$, is the union of all the weak extended Markovian bisimulations.

Bisimulation semantics: examples

$$<a,\lambda>.<\tau,\infty_{l,w}>.<b,\mu>.\underline{0} \;\approx_{\mathrm{EMB}}\; <a,\lambda>.<b,\mu>.\underline{0}$$

$$<a,\lambda>.(<\tau,\infty_{l,w_1}>.<b,\mu>.\underline{0} + <\tau,\infty_{l,w_2}>.<c,\gamma>.\underline{0})$$

$$\approx_{\mathrm{EMB}}$$

$$<a,\lambda\cdot\tfrac{w_1}{w_1+w_2}>.<b,\mu>.\underline{0} + <a,\lambda\cdot\tfrac{w_2}{w_1+w_2}>.<c,\gamma>.\underline{0}$$

$$\approx_{\mathrm{EMB}}$$

$$<a,\lambda>.A$$

$$A \triangleq <\tau,\infty_{l,w_1}>.<b,\mu>.\underline{0} + <\tau,\infty_{l,w_2}>.<c,\gamma>.\underline{0} + <\tau,\infty_{l,w_3}>.A$$

$$<\tau,\infty_{l,w}>.<a,\lambda>.\underline{0} \;\not\approx_{\mathrm{EMB}}\; <a,\lambda>.\underline{0}$$

Noninterference properties comparison

(Conservative Extension)

- $BSSNI \subset BSPNI \subset BSNNI$
- $BSSLNI \subset BSPLNI \subset BSNLNI$

(Inclusion Relations)

- $BSNLNI \subset BSNNI$ and $BSPLNI \subset BSPNI$
- $BSSLNI \not\subset BSSNI$ and $BSSNI \not\subset BSSLNI$

Example:
$<\!h, \lambda\!>.<\!l, \mu\!>.\underline{0} + <\!l, \mu\!>.\underline{0}$

Future work

- define approximate behavioral equivalences in the stochastic setting

- investigate properties stronger than strong noninterference that do not imply the explicit analysis of every possible high process, as it happens in Nondeducibility on Compositions:

  $(P \parallel_{Name_H} H) \approx_{\mathrm{EMB}} P \backslash Name_H$ for every high process term H