Persistent Stochastic Non-Interference

Citation for published version:
Hillston, J, Piazza, C & Rossi, S 2018, Persistent Stochastic Non-Interference. in Proceedings Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics . vol. 276, Beijing, China, pp. 53-68, 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics , Beijing, China, 3/09/18. DOI: 10.4204/EPTCS.276.6

Digital Object Identifier (DOI):
10.4204/EPTCS.276.6

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Proceedings Combined 25th International Workshop on Expressiveness in Concurrency and 15th Workshop on Structural Operational Semantics

Persistent Stochastic Non-Interference

Jane Hillston
University of Edinburgh, UK
Jane.Hillston@ed.ac.uk

Carla Piazza
Università di Udine, Italy
carla.piazza@uniud.it

Sabina Rossi
Università Ca' Foscari Venezia, Italy
sabina.rossi@unive.it

In this paper we present an information flow security property for stochastic, cooperating, processes expressed as terms of the Performance Evaluation Process Algebra (PEPA). We introduce the notion of *Persistent Stochastic Non-Interference (PSNI)* based on the idea that every state reachable by a process satisfies a basic *Stochastic Non-Interference (SNI)* property. The structural operational semantics of PEPA allows us to give two characterizations of *PSNI*: the first involves a single bisimulation-like equivalence check, while the second is formulated in terms of unwinding conditions. The observation equivalence at the base of our definition relies on the notion of lumpability and ensures that, for a secure process P, the steady state probability of observing the system being in a specific state P' is independent from its possible high level interactions.

1 Introduction

Non-Interference is an information flow security property which aims at protecting sensitive data from undesired accesses. In particular, it consists in protecting the confidentiality of information by guaranteeing that high level, sensitive, information never flows to low level, unauthorized, users. It is well known that access control policies or cryptographic protocols are, in general, not sufficient to forbid unwanted flows which may arise from the so called covert channels or from some weakness in the cryptographic algorithms.

The notion of Non-Interference for deterministic systems has been introduced in [17] and it has been extended to non-deterministic systems. Non-Interference has been then studied in different settings such as programming languages [16, 30, 31], trace models [22, 25], cryptographic protocols [1, 6, 13], process calculi [7, 8, 12, 19, 29], probabilistic models [2, 10], timed models [14, 18], and stochastic models [2].

In this paper we study a notion of Non-Interference for stochastic, cooperating, processes expressed as terms of the Performance Evaluation Process Algebra (PEPA) [20]. We introduce the notion of *Persistent Stochastic Non-Interference (PSNI)* based on the idea that every state reachable by a process satisfies a basic *Stochastic Non-Interference (SNI)* property. By imposing that security persists during process execution, the system is guaranteed to be dynamically secure in the sense that every potential transition leads the process to a secure state. Property *SNI* is inspired by the *Bisimulation-based Non-Deducibility on Compositions (BNDC)* property defined in [11] for non-deterministic CCS processes. In our setting, the definition has the following form: a process P is secure if a low level observer cannot distinguish the behavior of P in isolation from the behavior of P cooperating with any possible high level process H. The notion of observation that we consider is based on the concept of lumpability for the underlying Markov chain [21, 23, 24]. Formally, property *SNI* is defined as: for any high level process H which may enable only high level activities,

$$P \setminus \mathscr{H} \approx_l (P \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$$

where $P \setminus \mathscr{H}$ represents the low level view of P in isolation, while $(P \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$ denotes the low level view of P interacting with the high process H. The observation equivalence $\approx_l$ is the *lumpable bisimilarity* defined in [21] which is a characterization of a lumpable relation over the terms of the process

J.A. Pérez and S. Tini (Eds.): Combined Workshop on Expressiveness in
Concurrency and Structural Operational Semantics (EXPRESS/SOS 2018).
EPTCS 276, 2018, pp. 53–68, doi:10.4204/EPTCS.276.6

algebra PEPA preserving contextuality and inducing a lumping in the underlying Markov processes. Notice that this basic security property, that we call *Stochastic Non-Interference (SNI)* is not persistent in the sense that it is not preserved during system execution. Thus, it might happen that a system satisfying *SNI* reaches a state which is not secure. To overcome this problem we introduce the notion of *Persistent Stochastic Non-Interference (PSNI)* which requires that every state reachable by the system is secure, i.e., P is secure if and only if

$$\forall P' \text{ reachable from } P,\ \ P' \text{ satisfies } SNI\,.$$

Notice that this property contains two universal quantifications: one over all the reachable states and another one, inside the definition of *SNI*, over all the possible high level processes which may interact with the considered system. The main contributions of this paper are:

- we provide a characterization of *PSNI* in terms of a single bisimulation-based check thus avoiding the universal quantification over all the high level contexts;
- based on the structural operational semantics of PEPA, we provide a characterization of *PSNI* expressed in terms of unwinding conditions;
- we prove that *PSNI* is compositional with respect to low prefix, cooperation over low actions and hiding;
- we prove that if P is secure then the equivalence class $[P]$ with respect to lumpable bisimilarity $\approx_l$ is closed under *PSNI*;
- we show through an example that if P is secure then, from the low level point of view, the steady state probability of observing the system being in a specific state P' is independent from the possible high level interactions of P.

Structure of the paper. The paper is organized as follows: in Section 2 we introduce the process algebra PEPA, its structural operational semantics, and the observation equivalence named *lumpable bisimilarity*. The notion of *Persistent Stochastic Non-Interference (PSNI)* and its characterizations are presented in Section 3. In Section 4 we prove some compositionality result and other properties of *PSNI*. Comparisons with other SOS-based persistent security properties are discussed in Section 5. Finally, Section 6 concludes the paper.

2 The Calculus

PEPA (Performance Evaluation Process Algebra) [20] is an algebraic calculus enhanced with stochastic timing information which may be used to calculate performance measures as well as prove functional system properties.

The basic elements of PEPA are *components* and *activities*. Each activity is represented by a pair (α, r) where α is a label, or *action type*, and r is its *activity rate*, that is the parameter of a negative exponential distribution determining its duration. We assume that there is a countable set, $\mathscr{A}$, of possible action types, including a distinguished type, τ, which can be regarded as the *unknown* type. Activity rates may be any positive real number, or the distinguished symbol $\top$ which should be read as *unspecified*.

The syntax for PEPA terms is defined by the grammar:

$$\begin{array}{rcl} P & ::= & P \underset{L}{\bowtie} P \mid P/L \mid S \\ S & ::= & (\alpha, r).S \mid S + S \mid A \end{array}$$

where S denotes a *sequential component*, while P denotes a *model component* which executes in parallel. We assume that there is a countable set of *constants*, A. We write $\mathscr{C}$ for the set of all possible components.

$$\frac{}{(\alpha,r).P \xrightarrow{(\alpha,r)} P} \qquad \frac{P \xrightarrow{(\alpha,r)} P'}{P+Q \xrightarrow{(\alpha,r)} P'} \qquad \frac{Q \xrightarrow{(\alpha,r)} Q'}{P+Q \xrightarrow{(\alpha,r)} Q'}$$

$$\frac{P \xrightarrow{(\alpha,r)} P'}{P/L \xrightarrow{(\alpha,r)} P'/L}\ (\alpha \notin L) \qquad \frac{P \xrightarrow{(\alpha,r)} P'}{P/L \xrightarrow{(\tau,r)} P'/L}\ (\alpha \in L)$$

$$\frac{P \xrightarrow{(\alpha,r)} P'}{A \xrightarrow{(\alpha,r)} P'}\ (A \overset{def}{=} P) \qquad \frac{P \xrightarrow{(\alpha,r)} P'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,r)} P' \underset{L}{\bowtie} Q}\ (\alpha \notin L) \qquad \frac{Q \xrightarrow{(\alpha,r)} Q'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,r)} P \underset{L}{\bowtie} Q'}\ (\alpha \notin L)$$

$$\frac{P \xrightarrow{(\alpha,r_1)} P' \quad Q \xrightarrow{(\alpha,r_2)} Q'}{P \underset{L}{\bowtie} Q \xrightarrow{(\alpha,R)} P' \underset{L}{\bowtie} Q'} \qquad R = \frac{r_1}{r_\alpha(P)} \frac{r_2}{r_\alpha(Q)} \min(r_\alpha(P), r_\alpha(Q)) \quad (\alpha \in L)$$

Table 1: Operational semantics for PEPA components

2.1 Structural Operational Semantics

PEPA is given a structural operational semantics, as shown in Table 1. The component $(\alpha,r).P$ carries out the activity (α,r) of type α at rate r and subsequently behaves as P. When $a = (\alpha,r)$, the component $(\alpha,r).P$ may be written as $a.P$. The component $P+Q$ represents a system which may behave either as P or as Q. $P+Q$ enables all the current activities of both P and Q. The first activity to complete distinguishes one of the components, P or Q. The other component of the choice is discarded. The component P/L behaves as P except that any activity of type within the set L are *hidden*, i.e., they are relabeled with the unobservable type τ. The meaning of a constant A is given by a defining equation such as $A \overset{def}{=} P$ which gives the constant A the behavior of the component P. The cooperation combinator $\underset{L}{\bowtie}$ is in fact an indexed family of combinators, one for each possible set of action types, $L \subseteq \mathscr{A} \setminus \{\tau\}$. The *cooperation set* L defines the action types on which the components must synchronize or *cooperate* (the unknown action type, τ, may not appear in any cooperation set). It is assumed that each component proceeds independently with any activities whose types do not occur in the cooperation set L (*individual activities*). However, activities with action types in the set L require the simultaneous involvement of both components (*shared activities*). These shared activities will only be enabled in $P \underset{L}{\bowtie} Q$ when they are enabled in both P and Q. The shared activity will have the same action type as the two contributing activities and a rate reflecting the rate of the slower participant [20]. If an activity has an unspecified rate in a component, the component is passive with respect to that action type. In this case the rate of the shared activity will be completely determined by the other component. For a given P and action type α, this is the *apparent rate* [21] of α in P, denoted $r_\alpha(P)$, that is the sum of the rates of the α activities enabled in P.

The semantics of each term in PEPA is given via a labeled *multi-transition system* where the multiplicities of arcs are significant. In the transition system, a state or *derivative* corresponds to each syntactic term of the language and an arc represents the activity which causes one derivative to evolve into another. The set of reachable states of a model P is termed the *derivative set* of P, denoted by $ds(P)$, and constitutes the set of nodes of the *derivation graph* of P ($\mathscr{D}(P)$) obtained by applying the semantic rules exhaustively. We denote by $\mathscr{A}(P)$ the set of all the *current action types* of P, i.e., the set of action types which the component P may next engage in. We denote by $\mathscr{A}ct(P)$ the multiset of all the *current activities* of P. Finally we denote by $\vec{\mathscr{A}}(P)$ the union of all $\mathscr{A}(P')$ with $P' \in ds(P)$, i.e., the set of all action types syntactically occurring in P. For any component P, the *exit rate* from P will be the sum of the activity rates of all the activities enabled in P, i.e., $q(P) = \sum_{a \in \mathscr{A}ct(P)} r_a$, with r_a being the rate of activity a. If P enables more than one activity, $|\mathscr{A}ct(P)| > 1$, then the dynamic behavior of the model is determined by a race condition. This has the effect of replacing the nondeterministic branching of the pure process algebra with probabilistic branching. The probability that a particular activity completes is given by the ratio of the activity rate to the exit rate from P.

2.2 Underlying Stochastic Process

In [20] it is proved that for any finite PEPA model $P \overset{def}{=} P_0$ with $ds(P) = \{P_0, \ldots, P_n\}$, if we define the stochastic process $X(t)$, such that $X(t) = P_i$ indicates that the system behaves as component P_i at time t, then $X(t)$ is a continuous time Markov chain.

The *transition rate* between two components P_i and P_j, denoted $q(P_i, P_j)$, is the rate at which the system changes from behaving as component P_i to behaving as P_j. It is the sum of the activity rates labeling arcs which connect the node corresponding to P_i to the node corresponding to P_j in $\mathscr{D}(P)$, i.e.,

$$q(P_i, P_j) = \textstyle\sum_{a \in \mathscr{A}ct(P_i|P_j)} r_a$$

where $P_i \neq P_j$ and $\mathscr{A}ct(P_i|P_j) = \{| a \in \mathscr{A}ct(P_i)| \ P_i \xrightarrow{a} P_j |\}$. Clearly if P_j is not a one-step derivative of P_i, $q(P_i, P_j) = 0$. The $q(P_i, P_j)$ (also denoted q_{ij}), are the off-diagonal elements of the infinitesimal generator matrix of the Markov process, $\mathbf{Q}$. Diagonal elements are formed as the negative sum of the non-diagonal elements of each row. We use the following notation: $q(P_i) = \sum_{j \neq i} q(P_i, P_j)$ and $q_{ii} = -q(P_i)$. For any finite and irreducible PEPA model P, the steady-state distribution $\Pi(\cdot)$ exists and it may be found by solving the normalization equation and the global balance equations: $\sum_{P_i \in ds(P)} \Pi(P_i) = 1$ and $\Pi\mathbf{Q} = \mathbf{0}$. The *conditional transition rate* from P_i to P_j via an action type α is denoted $q(P_i, P_j, \alpha)$. This is the sum of the activity rates labeling arcs connecting the corresponding nodes in the derivation graph which are also labeled by the action type α. It is the rate at which a system behaving as component P_i evolves to behaving as component P_j as the result of completing a type α activity. The *total conditional transition rate* from P to $S \subseteq ds(P)$, denoted $q[P, S, \alpha]$, is defined as

$$q[P, S, \alpha] = \sum_{P' \in S} q(P, P', \alpha)$$

where $q(P, P', \alpha) = \sum_{P \xrightarrow{(\alpha, r_\alpha)} P'} r_\alpha$.

2.3 Observation Equivalence

In a process algebra, actions, rather than states, play the role of capturing the observable behavior of a system model. This leads to a formally defined notion of equivalence in which components are regarded as equal if, under observation, they appear to perform exactly the same actions. In this section we recall a bisimulation-like relation, named *lumpable bisimilarity*, for PEPA models [21].

Two PEPA components are *lumpably bisimilar* if there is an equivalence relation between them such that, for any action type α different from τ, the total conditional transition rates from those components to any equivalence class, via activities of this type, are the same.

Definition 1. (Lumpable bisimulation) *An equivalence relation over PEPA components, $\mathscr{R} \subseteq \mathscr{C} \times \mathscr{C}$, is a* lumpable bisimulation *if whenever $(P, Q) \in \mathscr{R}$ then for all $\alpha \in \mathscr{A}$ and for all $S \in \mathscr{C}/\mathscr{R}$ such that*

- *either $\alpha \neq \tau$,*
- *or $\alpha = \tau$ and $P, Q \notin S$,*

it holds

$$q[P, S, \alpha] = q[Q, S, \alpha] .$$

It is clear that the identity relation is a lumpable bisimulation. We are interested in the relation which is the largest lumpable bisimulation, formed by the union of all lumpable bisimulations.

Definition 2. (Lumpable bisimilarity) *Two PEPA components P and Q are* lumpably bisimilar*, written $P \approx_l Q$, if $(P, Q) \in \mathscr{R}$ for some lumpable bisimulation $\mathscr{R}$, i.e.,*

$$\approx_l = \bigcup \{\mathscr{R} \mid \mathscr{R} \textit{ is a lumpable bisimulation}\}.$$

$\approx_l$ is called lumpable bisimilarity *and it is the largest symmetric lumpable bisimulation over PEPA components.*

In [21] we proved that lumpable bisimilarity is a congruence for the so-called evaluation contexts, i.e., if $P_1 \approx_l P_2$ then

- $a.P_1 \approx_l a.P_2$;
- $P_1 \underset{L}{\bowtie} Q \approx_l P_2 \underset{L}{\bowtie} Q$ for all $L \subseteq \mathscr{A}$.
- $P_1/L \approx_l P_2/L$.

Notice that the notion of strong equivalence defined in [20] is stricter than that of lumpable bisimilarity because the latter allows arbitrary activities with type τ among components belonging to the same equivalence class.

In [3] a notion of weak bisimulation for CTMCs is introduced. This is based on the idea that the time-abstract behavior of equivalent states is weakly bisimilar and that the relative speed of these states to move to a different equivalence class is equal. To capture this intuition, the authors propose a definition of weak-bisimulation which resembles our notion of lumpable bisimulation if we ignore action types and labels. This bisimulation is defined in the context of both discrete and continuous time Markov chains without any notion of compositionality, and hence of contextuality. Compositionality is considered in [2, 5, 9], where definitions of weak bisimilarities for stochastic process algebra based on the classical concept of weak action are proposed. Our approach shares with these bisimilarities the idea of ignoring the rates for non-synchronizing (labeled τ) transitions between a state and the others belonging to the same equivalence class. The main difference between our definition and those presented in [2, 5, 9] is that we explicitly studied the relationships between our lumpable bisimilarity at the process algebra level and the induced lumping of the underlying Markov chains. This led to a coinductive characterization of a notion of contextual lumpability as described in [21].

3 Persistent Stochastic Non-Interference

The security property named *Persistent Stochastic Non-Interference (PSNI)* tries to capture every possible information flow from a *classified (high)* level of confidentiality to an *untrusted (low)* one. A strong requirement of this definition is that no information flow should be possible even in the presence of malicious processes that run at the classified level. The main motivation is to protect a system also from internal attacks, which could be performed by the so-called *Trojan Horse* programs, i.e., programs that appear honest but hide some malicious code inside them.

More precisely, the notion of *PSNI* consists of checking all the states reachable by the system against all high level potential interactions.

In order to formally define our security property, we partition the set $\mathscr{A} \setminus \{\tau\}$ of visible action types, into two sets, $\mathscr{H}$ and $\mathscr{L}$ of high and low level action types. A high level PEPA component H is a PEPA term such that for all $H' \in ds(H)$, $\mathscr{A}(H') \subseteq \mathscr{H}$, i.e., every derivative of H may next engage in only high level actions. We denote by $\mathscr{C}_H$ the set of all high level PEPA components.

A system P satisfies *PSNI* if for every state P' reachable from P and for every high level process H a low level user cannot distinguish P' from $P' \underset{\mathscr{H}}{\bowtie} H$. In other words, a system P satisfies *PSNI* if what a low level user sees of the system is not modified when it cooperates with any high level process H.

In order to formally define the *PSNI* property, we denote by $P \setminus \mathscr{H}$ the PEPA component $(P \underset{\mathscr{H}}{\bowtie} \bar{H})$ where $\bar{H}$ is any high level process that does not cooperate with P, i.e., for all $P' \in ds(P)$, $\mathscr{A}(P') \cap \mathscr{A}(\bar{H}) = \emptyset$. Intuitively $P \setminus \mathscr{H}$ denotes the component P prevented from performing high level actions. Notice that the definition is well formed in the sense that if $\bar{H}_1$ and $\bar{H}_2$ are two high level processes that do not cooperate with P, then the derivation graphs of $(P \underset{\mathscr{H}}{\bowtie} \bar{H}_1)$ and $(P \underset{\mathscr{H}}{\bowtie} \bar{H}_2)$ are isomorphic.

Properties *SNI* and *PSNI* are formally defined as follows.

Definition 3. (Stochastic Non-Interference) *Let P be a PEPA component.*

$$P \in \mathit{SNI} \text{ iff } \forall H \in \mathscr{C}_H,$$

$$P \setminus \mathscr{H} \approx_l (P \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}.$$

Definition 4. (Persistent Stochastic Non-Interference) *Let P be a PEPA component.*

$$P \in \mathit{PSNI} \text{ iff } \forall P' \in ds(P), \forall H \in \mathscr{C}_H,$$

$$P' \in \mathit{SNI}, \text{ i.e., } P' \setminus \mathscr{H} \approx_l (P' \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}.$$

We introduce a novel bisimulation-based equivalence relation over PEPA components, named $\approx_l^{hc}$, that allows us to give a first characterization of *PSNI* with no quantification over all the high level components H. In particular, we show that $P \in \mathit{PSNI}$ if and only if $P \setminus \mathscr{H}$ and P are not distinguishable with respect to $\approx_l^{hc}$. Intuitively, two processes are $\approx_l^{hc}$-equivalent if they can simulate each other in any possible high context, i.e., in every context $C[\_]$ of the form $(\_ \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$ where $H \in \mathscr{C}_H$. Observe that for any high context $C[\_]$ and PEPA model P, all the states reachable from $C[P]$ have the form $C'[P']$ with $C'[\_]$ being a high context too and $P' \in ds(P)$.

We now introduce the concept of *lumpable bisimulation on high contexts*: the idea is that, given two PEPA models P and Q, when a high level context $C[\_]$ filled with P executes a certain activity moving P to P' then the same context filled with Q is able to simulate this step moving Q to Q' so that P' and Q' are again lumpable bisimilar on high contexts, and vice-versa. This must be true for every possible high context $C[\_]$. It is important to note that the quantification over all possible high contexts is re-iterated for P' and Q'. For a PEPA model P, $\alpha \in \mathscr{A}$, $S \subseteq ds(P)$ and a high context $C[\_]$ we define:

$$q_C(P, P', \alpha) = \sum_{C[P] \xrightarrow{(\alpha, r_\alpha)} C'[P']} r_\alpha$$

and

$$q_C[P,S,\alpha] = \sum_{P' \in S} q_C(P,P',\alpha)\,.$$

The notion of *lumpable bisimulation on high contexts* is defined as follows:

Definition 5. (Lumpable bisimilarity on high contexts) *An equivalence relation over PEPA components, $\mathscr{R} \subseteq \mathscr{C} \times \mathscr{C}$, is a* lumpable bisimulation on high contexts *if whenever $(P,Q) \in \mathscr{R}$ then for all high context $C[\_]$, for all $\alpha \in \mathscr{A}$ and for all $S \in \mathscr{C}/\mathscr{R}$ such that*

- *either $\alpha \neq \tau$,*
- *or $\alpha = \tau$ and $P,Q \notin S$,*

it holds

$$q_C[P,S,\alpha] = q_C[Q,S,\alpha]\,.$$

Two PEPA components P and Q are lumpably bisimilar on high contexts, *written $P \approx_l^{hc} Q$, if $(P,Q) \in \mathscr{R}$ for some lumpable bisimulation on high contexts $\mathscr{R}$, i.e.,*

$$\approx_l^{hc} = \bigcup \{\mathscr{R} \mid \mathscr{R} \textit{ is a lumpable bisimulation on high contexts}\}.$$

$\approx_l^{hc}$ *is called* lumpable bisimilarity on high contexts *and it is the largest symmetric lumpable bisimulation on high contexts over PEPA components. It is easy to prove that $\approx_l^{hc}$ is an equivalence relation.*

The next theorem gives a characterization of *PSNI* in terms of $\approx_l^{hc}$.

Theorem 1. *Let P be a PEPA component. Then*

$$P \in PSNI \textit{ iff } P \setminus \mathscr{H} \approx_l^{hc} P\,.$$

Proof. We first show that $P \setminus \mathscr{H} \approx_l^{hc} P$ implies $P \in PSNI$. In order to do it we prove that

$$\mathscr{R} = \{(P_1 \setminus \mathscr{H}, (P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}) \,|\, H \in \mathscr{C}_H \text{ and } P_1 \setminus \mathscr{H} \approx_l^{hc} P_2\}$$

is a lumpable bisimulation. This is sufficient to say that $P \in PSNI$.

First observe that, if $P \setminus \mathscr{H} \approx_l^{hc} P$ then for all $P' \in ds(P)$ there exists $P'' \setminus \mathscr{H} \in ds(P \setminus \mathscr{H})$ such that $P'' \setminus \mathscr{H} \approx_l^{hc} P'$ and, by definition of $\mathscr{R}$, for all $H \in \mathscr{C}_H$, $(P'' \setminus \mathscr{H}, (P' \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}) \in \mathscr{R}$. Since $\mathscr{R}$ is a lumpable bisimulation, we have that for all $H \in \mathscr{C}_H$, $P'' \setminus \mathscr{H} \approx_l (P' \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$. In particular, there exists $\bar{H} \in \mathscr{C}_H$ such that $(P' \underset{\mathscr{H}}{\bowtie} \bar{H})/\mathscr{H}$ coincides with $P' \setminus \mathscr{H}$. Since $\approx_l$ is an equivalence relation, by symmetry and transitivity, we have that for every $P' \in ds(P)$ and for every $H \in \mathscr{C}_H$, $P'' \setminus \mathscr{H} \approx_l P' \setminus \mathscr{H} \approx_l (P' \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$, i.e., $P \in PSNI$. The fact that $\mathscr{R}$ is a lumpable bisimulation follows from:

- if $P_1 \setminus \mathscr{H} \approx_l^{hc} P_2$ then for all $\alpha \in \mathscr{A}$ with $\alpha \neq \tau$ and for all $S \in \mathscr{C}/\approx_l^{hc}$ and for all high context $C[\_]$, we have $q_C[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S, \alpha]$. Since a high context can only perform high level activities, we have that for all high level context $C[\_]$, it holds that $q[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_1 \setminus \mathscr{H}, S, \alpha]$ and then $q[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S, \alpha]$, i.e., we have that for all $(P_1 \setminus \mathscr{H}, (P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}) \in \mathscr{R}$ and for all $S' \in \mathscr{C}/\mathscr{R}$ it holds $q[P_1 \setminus \mathscr{H}, S', \alpha] = q[(P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}, S', \alpha]$.
- if $P_1 \setminus \mathscr{H} \approx_l^{hc} P_2$ then for $\alpha = \tau$ and for all $S \in \mathscr{C}/\approx_l^{hc}$ with $P_1 \setminus \mathscr{H}, P_2 \notin S$ and for all high context $C[\_]$, we have $q_C[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S, \alpha]$. Since a high context can only perform high level activities, we have that for all high level context $C[\_]$, it holds that $q[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_1 \setminus \mathscr{H}, S, \alpha]$. Hence for all $(P_1 \setminus \mathscr{H}, (P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}) \in \mathscr{R}$ and for all $S' \in \mathscr{C}/\mathscr{R}$ with $P_1 \setminus \mathscr{H}, (P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}) \notin S'$ it holds $q[P_1 \setminus \mathscr{H}, S', \alpha] = q[(P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}, S', \alpha]$.

We now show that if $P \in \mathit{PSNI}$ then $P \setminus \mathscr{H} \approx_l^{hc} P$. To this end it is sufficient to prove that

$$\mathscr{R} = \{(P_1 \setminus \mathscr{H}, P_2) \,|\, P_1 \setminus \mathscr{H} \approx_l P_2 \setminus \mathscr{H} \text{ and } P_2 \in \mathit{PSNI}\}$$

is a lumpable bisimulation on high contexts. Indeed, let $C[\_]$ be a high context and $\alpha \in \mathscr{A}$.

- Assume $\alpha \neq \tau$. From $P_1 \setminus \mathscr{H} \approx_l P_2 \setminus \mathscr{H}$, we have that for all $S \in \mathscr{C}/\approx_l$, $q[P_1 \setminus \mathscr{H}, S, \alpha] = q[P_2 \setminus \mathscr{H}, S, \alpha]$. Since a high context can only perform high level activities, we have that for all high context $C[\_]$ it holds $q[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_1 \setminus \mathscr{H}, S, \alpha]$. Moreover, since $\alpha \neq \tau$, $q[P_2 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S', \alpha]$ where $S' = \{P \,|\, P \setminus \mathscr{H} \in S\}$, i.e., for all high context $C[\_]$ and $S \in \mathscr{C}/\mathscr{R}$ it holds $q_C[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S, \alpha]$.
- Consider now $\alpha = \tau$. From $P_1 \setminus \mathscr{H} \approx_l P_2 \setminus \mathscr{H}$, we have that for all $S \in \mathscr{C}/\approx_l$ such that $P_1 \setminus \mathscr{H}$, $P_2 \setminus \mathscr{H} \notin S$, $q[P_1 \setminus \mathscr{H}, S, \alpha] = q[P_2 \setminus \mathscr{H}, S, \alpha]$. Since a high context can only perform high level activities and both $P_1 \setminus \mathscr{H}$ and $P_2 \setminus \mathscr{H}$ do not perform high activities, we have that $q[P_i \setminus \mathscr{H}, S, \alpha] = q_C[P_i \setminus \mathscr{H}, S, \alpha]$ for all high level context $C[\_]$ and for $i \in \{1,2\}$. From the fact that $P_2 \in \mathit{PSNI}$, we have $P_2 \setminus \mathscr{H} \approx_l (P_2 \underset{\mathscr{H}}{\bowtie} H)/\mathscr{H}$ for all $H \in \mathscr{C}_H$, and then $q[P_2 \setminus \mathscr{H}, S, \alpha] = q_C[P_2 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S', \alpha]$ for all high context $C[\_]$, $S \in \mathscr{C}/\approx_l^{hc}$ and $S' \in \mathscr{C}/\mathscr{R}$ such that $P_2 \setminus \mathscr{H} \notin S$ and $P_2 \notin S'$, i.e., $q_C[P_1 \setminus \mathscr{H}, S, \alpha] = q_C[P_2, S, \alpha]$ for all high context $C[\_]$ and $S \in \mathscr{C}/\mathscr{R}$ such that $P_1 \setminus \mathscr{H}, P_2 \notin S$.

□

Finally, we show how it is possible to give a characterization of *PSNI* avoiding both the universal quantification over all the possible high level components and the universal quantification over all the possible reachable states.

Before we have shown how the idea of "being secure in every state" can be directly moved inside the lumpable bisimulation on high contexts notion ($\approx_l^{hc}$). However this bisimulation notion implicitly contains a quantification over all possible high contexts. We now prove that $\approx_l^{hc}$ can be expressed in a rather simpler way by exploiting local information only. This can be done by defining a novel equivalence relation which focuses only on observable actions that do not belong to $\mathscr{H}$. More in detail, we define an observation equivalence where actions from $\mathscr{H}$ *may* be ignored.

We first introduce the notion of *lumpable bisimilarity up to $\mathscr{H}$*.

Definition 6. (Lumpable bisimilarity up to $\mathscr{H}$) *An equivalence relation over PEPA components, $\mathscr{R} \subseteq \mathscr{C} \times \mathscr{C}$, is a* lumpable bisimulation up to $\mathscr{H}$ *if whenever $(P,Q) \in \mathscr{R}$ then for all $\alpha \in \mathscr{A}$ and for all $S \in \mathscr{C}/\mathscr{R}$*

- *if $\alpha \notin \mathscr{H} \cup \{\tau\}$ then*
$$q[P,S,\alpha] = q[Q,S,\alpha],$$
- *if $\alpha \in \mathscr{H} \cup \{\tau\}$ and $P,Q \notin S$, then*
$$q[P,S,\alpha] = q[Q,S,\alpha].$$

Two PEPA components P and Q are lumpably bisimilar up to $\mathscr{H}$, *written $P \approx_l^{\mathscr{H}} Q$, if $(P,Q) \in \mathscr{R}$ for some lumpable bisimulation up to $\mathscr{H}$, i.e.,*

$$\approx_l^{\mathscr{H}} = \bigcup \{\mathscr{R} \mid \mathscr{R} \textit{ is a lumpable bisimulation up to } \mathscr{H}\}.$$

$\approx_l^{\mathscr{H}}$ *is called* lumpable bisimilarity up to $\mathscr{H}$ *and it is the largest symmetric lumpable bisimulation up to $\mathscr{H}$ over PEPA components.*

The next theorem shows that the binary relations $\approx_l^{hc}$ and $\approx_l^{\mathscr{H}}$ are equivalent.

Theorem 2. *Let P and Q be two PEPA components. Then*

$$P \approx_l^{hc} Q \text{ if and only if } P \approx_l^{\mathscr{H}} Q\,.$$

Proof. We first show that $P \approx_l^{hc} Q$ implies $P \approx_l^{\mathscr{H}} Q$. In order to do it we prove that

$$\mathscr{R} = \{(P,Q) \,|\, P \approx_l^{hc} Q\}$$

is a lumpable bisimulation up to $\mathscr{H}$. This follows from the following cases. First observe that, by definition of $\mathscr{R}$, $S \in \mathscr{C}/\approx_l^{hc}$ if and only if $S \in \mathscr{C}/\mathscr{R}$.

- Let $\alpha \notin \mathscr{H} \cup \{\tau\}$. From the fact that $P \approx_l^{hc} Q$ it holds that for all $S \in \mathscr{C}/\approx_l^{hc}$ and for all high context $C[\_]$, $q_C[P,S,\alpha] = q_C[Q,S,\alpha]$. Since $\alpha \notin \mathscr{H} \cup \{\tau\}$, we have that $q[P,S,\alpha] = q[Q,S,\alpha]$.
- Let $\alpha \in \mathscr{H} \cup \{\tau\}$. From the fact that $P \approx_l^{hc} Q$ it holds that for all $S \in \mathscr{C}/\approx_l^{hc}$ such that $P,Q \notin S$ and for all high context $C[\_]$, $q_C[P,S,\tau] = q_C[Q,S,\tau]$. If $C[\_]$ does not synchronize with P, we have that $q[P,S,\tau] = q[Q,S,\tau]$. On the other hand, consider a context $C[\_]$ with only one current action type $h \in \mathscr{H}$. Then, from $q_C[P,S,\tau] = q_C[Q,S,\tau]$ and $q[P,S,\tau] = q[Q,S,\tau]$, it follows that if P cooperates over h then also Q cooperates over h and $q[P,S,h] = q[Q,S,h]$.

We now show that if $P \approx_l^{\mathscr{H}} Q$ then $P \approx_l^{hc} Q$. To this end it is sufficient to prove that

$$\mathscr{R} = \{(P,Q) \,|\, P \approx_l^{\mathscr{H}} Q\}$$

is a lumpable bisimulation on high contexts. This follows from the following cases. First observe that, by definition of $\mathscr{R}$, $S \in \mathscr{C}/\approx_l^{hc}$ if and only if $S \in \mathscr{C}/\mathscr{R}$.

- Let $\alpha \notin \mathscr{H} \cup \{\tau\}$. From the fact that $P \approx_l^{\mathscr{H}} Q$ it holds that for all $S \in \mathscr{C}/\approx_l^{\mathscr{H}}$, $q[P,S,\alpha] = q[Q,S,\alpha]$. Since a high context can only perform high level activities, we have that $q[P,S,\alpha] = q_C[P,S,\alpha]$ and $q[Q,S,\alpha] = q_C[Q,S,\alpha]$ for all high context $C[\_]$. Hence, $q_C[P,S,\alpha] = q_C[Q,S,\alpha]$.
- Let $\alpha = \tau$. From the fact that $P \approx_l^{\mathscr{H}} Q$ it holds that for all $S \in \mathscr{C}/\approx_l^{\mathscr{H}}$ such that $P,Q \notin S$, $q[P,S,\alpha] = q[Q,S,\alpha]$. Hence for all high level context that do not synchronize with P and Q we have that $q[P,S,\alpha] = q_C[P,S,\alpha]$ and $q[Q,S,\alpha] = q_C[Q,S,\alpha]$, i.e., $q_C[P,S,\alpha] = q_C[Q,S,\alpha]$.
- Let $h \in \mathscr{H}$. From the fact that $P \approx_l^{\mathscr{H}} Q$ it holds that for all $S \in \mathscr{C}/\approx_l^{\mathscr{H}}$ such that $P,Q \notin S$, $q[P,S,h] = q[Q,S,h]$. From this and the fact that $q[P,S,\tau] = q[Q,S,\tau]$ it follows that for all high level context $C[\_]$ with only one current action type $h \in \mathscr{H}$, $q_C[P,S,\tau] = q_C[Q,S,\tau]$. By induction on the number of current action types of a high level context $C[\_]$, we obtain that for $\alpha = \tau$, for all $S \in \mathscr{C}/\mathscr{R}$ with $P,Q \notin S$ it holds $q_C[P,S,\alpha] = q_C[Q,S,\alpha]$.

□

Theorem 2 allows us to identify a local property of processes (with no quantification on the states and on the high contexts) which is a necessary and sufficient condition for *PSNI*. This is stated by the following corollary:

Corollary 1. *Let P be a PEPA component. Then*

$$P \in \mathit{PSNI} \text{ iff } P \setminus \mathscr{H} \approx_l^{\mathscr{H}} P\,.$$

Finally we provide a characterization of *PSNI* in terms of *unwinding conditions*. In practice, whenever a state P' of a *PSNI* PEPA model P may execute a high level activity leading it to a state P'', then P' and P'' are indistinguishable for a low level observer.

Theorem 3. *Let P be a PEPA component.*

$$P \in PSNI \textit{ iff } \forall P' \in ds(P),$$

$$P' \xrightarrow{(h,r)} P'' \textit{ implies } P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$$

Proof. We first prove that if $P \in PSNI$ then for all $P' \in ds(P)$, $P' \xrightarrow{(h,r)} P''$ implies $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$. Indeed, by Definition 4, $P' \in PSNI$ and therefore, by Corollary 1, $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P'$. By Definition 6 of $\approx_l^{\mathscr{H}}$, for all $S \in \mathscr{C}/\approx_l^{\mathscr{H}}$ such that $P' \setminus \mathscr{H}, P' \notin S$, both $q[P' \setminus \mathscr{H}, S, \tau] = q[P', S, \tau]$ and $q[P' \setminus \mathscr{H}, S, h] = q[P', S, h]$. Since $P' \setminus \mathscr{H}$ does not perform any high level action, $q[P' \setminus \mathscr{H}, S, h] = 0$ while, since $P' \xrightarrow{(h,r)} P''$, $q[P', S, \hat{h}] \neq 0$. Therefore, from $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P'$, either h is not a current action type of P' or $P' \setminus \mathscr{H}, P' \in S$, i.e., $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P''$. Since also $P'' \in PSNI$, from $P'' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P''$ it follows that $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P'' \setminus \mathscr{H}$. Finally, since both $P' \setminus \mathscr{H}$ and $P'' \setminus \mathscr{H}$ do not perform any high level activity, $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P'' \setminus \mathscr{H}$ is equivalent to $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$.

We now prove that if for all $P' \in ds(P)$, $P' \xrightarrow{(h,r)} P''$ implies $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$ then $P \in PSNI$. Indeed observe that for all $\alpha \notin \mathscr{H} \cup \tau$, and for all $S \in \mathscr{C}/\approx_l^{\mathscr{H}}$, $q[P' \setminus \mathscr{H}, S, \alpha] = q[P', S, \alpha]$. Moreover, if $P' \setminus \mathscr{H}, P' \notin S$ then $q[P' \setminus \mathscr{H}, S, \tau] = q[P', S, \tau]$. This is sufficient to prove that $P' \setminus \mathscr{H} \approx_l^{\mathscr{H}} P'$, i.e., by Corollary 1, $P \in PSNI$. □

4 Properties of Persistent Stochastic Non-Interference

In this section we prove some interesting propertis of *PSNI*. First we prove that *PSNI* is compositional with respect to low prefix, cooperation over low actions and hiding.

Proposition 1. *Let P and Q be two PEPA components. If $P, Q \in PSNI$, then*

- $(\alpha, r).P \in PSNI$ *for all* $\alpha \in \mathscr{L} \cup \{\tau\}$
- $P/L \in PSNI$ *for all* $L \subseteq \mathscr{A}$
- $P \underset{L}{\bowtie} Q \in PSNI$ *for all* $L \subseteq \mathscr{L}$

Proof. Assume that $P, Q \in PSNI$.

- If $P \in PSNI$ then for all $P' \in ds(P)$, $P' \xrightarrow{(h,r)} P''$ implies $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$. This property is clearly maintained for the PEPA component $(\alpha, r).P$ when $\alpha \in \mathscr{L} \cup \{\tau\}$.
- If $P \in PSNI$ then for all $P' \in ds(P)$, $P' \xrightarrow{(h,r)} P''$ implies $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$. Let $L \subseteq \mathscr{A}$ and $P'/L \in ds(P)$. Assume that $P'/L \xrightarrow{(h,r)} P''/L$. From the fact that $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$ we have that $(P' \underset{\mathscr{H}}{\bowtie} \bar{H}) \approx_l (P'' \underset{\mathscr{H}}{\bowtie} \bar{H})$ for any high level PEPA component $\bar{H}$ that does not cooperate with P. From the fact that lumpable bisimilarity is a congruence for the evaluation contexts, we have that for all $L \subseteq \mathscr{A}$, $(P' \underset{\mathscr{H}}{\bowtie} \bar{H})/L \approx_l (P'' \underset{\mathscr{H}}{\bowtie} \bar{H})/L$. We can assume that $\vec{\mathscr{A}}(\bar{H}) \cap L = \emptyset$ and hence, since also $\vec{\mathscr{A}}(\bar{H}) \cap \vec{\mathscr{A}}(\bar{P}) = \emptyset$, $(P'/L \underset{\mathscr{H}}{\bowtie} \bar{H})/L \approx_l (P''/L \underset{\mathscr{H}}{\bowtie} \bar{H})/L$, i.e., $(P'/L) \setminus \mathscr{H} \approx_l (P''/L) \setminus \mathscr{H}$.

- If $P, Q \in PSNI$ then for all $P' \in ds(P)$, $P' \xrightarrow{(h,r)} P''$ implies $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$ and for all $Q' \in ds(Q)$, $Q' \xrightarrow{(h,r)} Q''$ implies $Q' \setminus \mathscr{H} \approx_l Q'' \setminus \mathscr{H}$. Let $L \subseteq \mathscr{L}$ and $P' \underset{L}{\bowtie} Q' \in ds(P \underset{L}{\bowtie} Q)$. Assume that $P' \underset{L}{\bowtie} Q' \xrightarrow{(h,r)} P'' \underset{L}{\bowtie} Q''$. In this case, either $P' \xrightarrow{(h,r)} P''$ or $Q' \xrightarrow{(h,r)} Q''$. Assume that $P' \xrightarrow{(h,r)} P''$ and then $P' \underset{L}{\bowtie} Q' \xrightarrow{(h,r)} P'' \underset{L}{\bowtie} Q'$. From the hypothesis that $P \in PSNI$ we have that $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$, i.e., $(P' \underset{\mathscr{H}}{\bowtie} \bar{H}) \approx_l (P'' \underset{\mathscr{H}}{\bowtie} \bar{H})$ for any high level PEPA component $\bar{H}$ that does not cooperate with P and Q. From the fact that $\approx_l$ is a congruence with respect to the cooperation operator we have $(P' \underset{\mathscr{H}}{\bowtie} \bar{H}) \underset{L}{\bowtie} (Q' \underset{\mathscr{H}}{\bowtie} \bar{H}) \approx_l (P'' \underset{\mathscr{H}}{\bowtie} \bar{H}) \underset{L}{\bowtie} (Q' \underset{\mathscr{H}}{\bowtie} \bar{H})$, moreover sice $\mathscr{H} \cap L = \emptyset$ we obtain $(P' \underset{L}{\bowtie} Q') \underset{\mathscr{H}}{\bowtie} \bar{H} \approx_l (P'' \underset{L}{\bowtie} Q') \underset{\mathscr{H}}{\bowtie} \bar{H}$, i.e., $(P' \underset{L}{\bowtie} Q') \setminus \mathscr{H} \approx_l (P'' \underset{L}{\bowtie} Q') \setminus \mathscr{H}$. In the case that $Q' \xrightarrow{(h,r)} Q''$ the proof is analogous.

□

Notice that the fact that *PSNI* is not preserved by the choice operatior is a consequence of the fact that lumpable bisimilarity is not a congruence for this operator.

We now prove that if $P \in PSNI$ then the equivalence class $[P]$ with respect to lumpable bisimilarity $\approx_l$ is closed under *PSNI*.

Proposition 2. *Let P and Q be two PEPA components. If $P \in PSNI$ and $P \approx_l Q$ then also $Q \in PSNI$.*

Proof. Let $P \in PSNI$ such that $P \approx_l Q$. Let $Q' \in ds(Q)$ such that $Q' \xrightarrow{(h,r)} Q''$. From the hypothesis that $P \approx_l Q$, there exist $P', P'' \in ds(P)$ such that $P' \approx_l Q'$ and $P'' \approx_l Q''$. Hence there exists r' such that $P' \xrightarrow{(h,r')} P''$ and $P' \setminus \mathscr{H} \approx_l P'' \setminus \mathscr{H}$. From the fact that $\approx_l$ is a congruence with respect to the cooperation operator we have $Q' \setminus \mathscr{H} \approx_l Q'' \setminus \mathscr{H}$ and then also $Q \in PSNI$. □

5 Comparison with other SOS-based persistent security properties

The security property presented in this paper is *persistent* in the sense that if a model P is secure then all the states reachable by P during its execution are also secure. Persistence is not a common feature of Non-Interference properties. For example, many properties based on trace models, like *generalized Non-Inference* and *separability* [25], and the *non local bisimulation based noninterference* properties for the Markovian process calculus defined in [2] are not persistent. Persistence is used in program verification techniques based on type-systems to provide sufficient conditions to Non-Interference properties, like, e.g., in [1, 19, 30, 31]. In this setting persistence provides sufficient static conditions which are invariant with respect to execution and imply the desired dynamic property.

In [15], a persistent property named *P_BNDC* has been proposed for non-deterministic CCS processes. The aim of this definition is to capture a robust notion of security for processes which may move in the middle of a computation. In this context persistence ensures that a secure process always migrates to a secure state. Notice that if the system satisfies a non-persistent property then it might migrate when it is executing in an insecure state and then, from the point of view of the new host, the incoming process is insecure and, consequently, it should not be executed. As our Persistent Stochastic Non-Interference property *PSNI*, property *P_BNDC* is provided with two sound and complete characterizations: one in terms of a behavioural equivalence between processes up to high level contexts and another one in terms of unwinding conditions. Let us compare the expressivity of *P_BNDC* and *PSNI* by considering their SOS-based characterization in terms of unwinding conditions. The formal unwinding characterization of *P_BNDC* for CCS processes is the following:

Definition 7. *Let P be a CCS process and H denote the set of all high level actions.*

$$P \in P\_BNDC \text{ iff } \forall P' \text{ reachable from } P\ ,$$

$$P' \xrightarrow{h} P'' \text{ implies } P' \overset{\hat{\tau}}{\Longrightarrow} P''' \text{ and } P'' \setminus H \approx P''' \setminus H$$

where $\overset{\hat{\tau}}{\Longrightarrow}$ *represents a possibly empty sequence of* τ *transitions and* $\approx$ *denotes Milner's weak bisimulation relation [27].*

Both PEPA and CCS are provided with a structural operational semantics that allows us to compare the definitions of *PSNI* (for PEPA processes) and *P_BNDC* (for CCS processes) just by considering the processes label transition systems eventually removing information concerning the activity rates. Consider for instance the simple process depicted in Figure 1. If we discard the activity rates we can interpret the graph as the labeled transition system of a CCS process P. According to Definition 7 we have that P satisfies *P_BNDC*. On the contrary, when we consider the activity rates we have the model of a PEPA process P which, according to Theorem 3, does not satisfies *PSNI*. Indeed we cannot find a lumpable bisimulation such that $P \setminus \mathscr{H} \approx_l P' \setminus \mathscr{H}$.

The unwinding definition of *PSNI* resembles the definition of *Strong BNDC (SBNC)* which has been introduced in [4] as a sufficient condition for verifying *P_BNDC*.

Recently, in [2] Non-Interference properties for processes expressed as terms of a Markovian process calculus are introduced. The calculus presented in the paper allows the authors to model three kinds of actions: exponentially timed actions, immediate actions and passive actions. As a consequence, the proposed process algebra encompasses nondeterminism, probability, priority and stochastic time. The behavioral observation defined by the authors extends the classical bisimulation relation of Milner [27]. The property named Bisimulation-based Strong Stochastic Local Non-Interference (*BSSLNI*) is defined in the style of our unwinding conditions but it is based on an observation equivalence named $\approx_{EMB}$ which abstracts from internal τ actions with zero duration. In particular, the relation $\approx_{EMB}$ is based on the idea that if a given class of processes is not reachable directly after executing a certain action, then one has to explore the possibility of reaching that class indirectly via a finite-length path π of internal actions with zero duration but with a specific probability of execution $prob(\pi)$. As observed by the authors, in general the performance indices of a system satisfying *BSSLNI* are not independent from the presence or the absence of high level interactions.

On the contrary, the observation equivalence at the base of our definition relies on the notion of lumpability and ensures that, for a secure process P, the steady state probability of observing the system being in a specific state P' is independent from its possible high level interactions. In order to show it consider the simple three state system depicted in Figure 2. In this case, following Theorem 3, we can prove that $P_1 \in PSNI$. Indeed, it is easy to prove that $P_1 \setminus \mathscr{H} \approx_l P_2 \setminus \mathscr{H}$ when $\approx_l$ is the lumpable bisimilarity. In particular, the probability for a low level user to observe, in steady state, the system being in state P_3 is independent from whether or not P_1 has performed the high level activity (h, λ). To prove

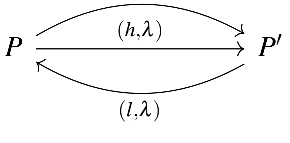


Figure 1: A simple two state model.

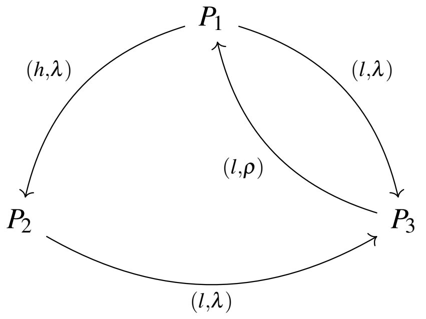


Figure 2: A simple three state model.

this, suppose that P_1 synchronizes over h. Then, for a low level observer, the system behaves as $P_1/\mathscr{H}$ depicted in Figure 3 (a). We can compute the steady state distribution of $P_1/\mathscr{H}$ by solving the global balance equations together with the normalization condition, obtaining:

$$\begin{array}{rcl} \pi_1 * 2\lambda & = & \pi_3 * \rho \\ \pi_2 * \lambda & = & \pi_1 * \lambda \\ \pi_3 * \rho & = & \pi_1 * \lambda + \pi_2 * \lambda \\ \pi_1 + \pi_2 + \pi_3 & = & 1 \end{array}$$

whose solution is

$$\pi_1 = \frac{\rho}{2(\lambda+\rho)} \qquad \pi_2 = \frac{\rho}{2(\lambda+\rho)} \qquad \pi_3 = \frac{\lambda}{\lambda+\rho}$$

where π_1, π_2 and π_3 denote the steady state probabilities of states $P_1/\mathscr{H}$, $P_2/\mathscr{H}$ and $P_3/\mathscr{H}$, respectively.

Consider now the case in which P_1 does not synchronize over h. Then the low level view of the system is represented by $P_1 \setminus \mathscr{H}$ depicted in Figure 3 (b). Again we can compute the steady state distribution of $P_1 \setminus \mathscr{H}$ by solving the global balance equations together with the normalization condition, obtaining:

$$\begin{array}{rcl} \pi_1 * \lambda & = & \pi_3 * \rho \\ \pi_3 * \rho & = & \pi_1 * \lambda \\ \pi_1 + \pi_3 & = & 1 \end{array}$$

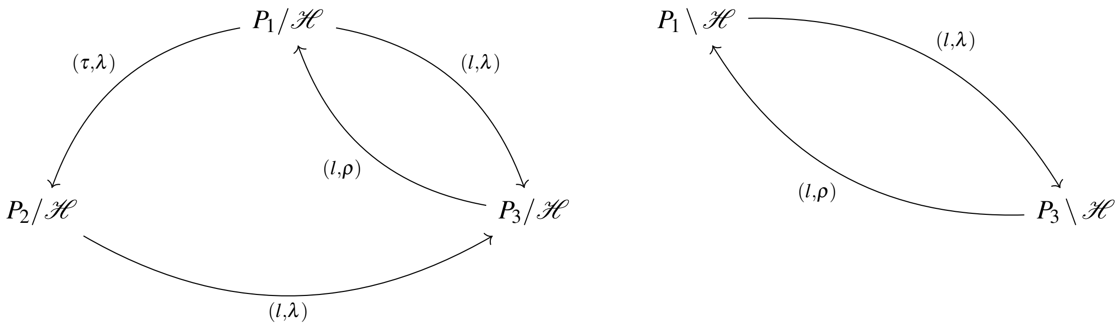
whose solution is

$$\pi_1 = \frac{\rho}{\lambda+\rho} \qquad \pi_3 = \frac{\lambda}{\lambda+\rho}$$

where π_1 and π_3 are the steady state probabilities of states $P_1 \setminus \mathscr{H}$ and $P_3 \setminus \mathscr{H}$, respectively. This proves that, from the low level point of view, the steady state probability of P_3 is independent from the fact that P has cooperated with a high level context or not.

6 Conclusion

In this paper we presented a *persistent* information flow security property for stochastic processes expressed as terms of the PEPA process algebra. Our property, named *Persistent Stochastic Non-Interference* (*PSNI*) is based on a structural operational semantics and a bisimulation based observation equivalence for the PEPA terms. We provide two characterizations for *PSNI*: one in terms of a bisimulation-like equivalence relation and another one in terms of unwinding conditions.



(a) $P_1/\mathscr{H}$

(b) $P_1 \setminus \mathscr{H}$

Figure 3: The models of $P_1/\mathscr{H}$ and $P_1 \setminus \mathscr{H}$.

The first characterization allows us to perform the verification of *PSNI* for finite state processes in polynomial time with respect to the number of states of the system [28].

The second characterization is based on unwinding conditions. This kind of conditions for possibilistic security properties have been already explored in the literature, like, e.g., in [29, 26, 22]. Such unwinding conditions have been proposed for traces-based models and represent only sufficient conditions for their respective security properties. Differently, our unwinding conditions provide both necessary and sufficient conditions for *PSNI*.

Finally, in this paper we also deal with compositionality issues. Indeed, the development of large and complex systems strongly depends on the ability of dividing the task of the system into subtasks that are solved by system subcomponents. Thus, it is useful to define properties which are compositional in the sense that if the properties are satisfied by the system subcomponents then the system as a whole will satisfy the desired property by construction. We show that *PSNI* is compositional with respect to low prefix, cooperation over low actions and hiding.

Acknowledgments: The work described in this paper has been partially supported by the Università Ca' Foscari Venezia - DAIS within the IRIDE program. It has been also partially supported by the PRID project ENCASE financed by Università degli Studi di Udine and by GNCS-INdAM project Metodi Formali per la Verifica e la Sintesi di Sistemi Discreti e Ibridi.

References

[1] M. Abadi, B. Blanchet & C. Fournet (2018): *The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication*. *Journal of the ACM* 65(1), pp. 1:1–1:41, doi:10.1145/3127586.

[2] A. Aldini & M. Bernardo (2009): *A General Framework for Nondeterministic, Probabilistic, and Stochastic Noninterference*. In: *Foundations and Applications of Security Analysis, Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, (ARSPA-WITS)*, pp. 18–33, doi:10.1007/978-3-642-03459-6_2.

[3] C. Baier, J.-P. Katoen, H. Hermanns & V. Wolf (2005): *Comparative branching-time semantics for Markov chains*. Information and Computation 200(2), pp. 149–214, doi:`10.1016/j.ic.2005.03.001`.

[4] A. Bossi, R. Focardi, C. Piazza & S. Rossi (2004): *Verifying Persistent Security Properties*. Computer Languages, Systems and Structures 30(3-4), pp. 231–258, doi:`10.1016/j.cl.2004.02.005`.

[5] H. Boudali, P. Crouzen & M. Stoelinga (2007): *A compositional semantics for dynamic fault trees in terms of interactive Markov chains*. In: Proc. of (ATVA'07, Springer-Verlag, pp. 441–456. Available at `https://doi.org/10.1007/978-3-540-75596-8_31`.

[6] M. Bugliesi & S. Rossi (2005): *Non-interference proof techniques for the analysis of cryptographic protocols*. Journal of Computer Security 13(1), pp. 87–113, doi:`10.3233/JCS-2005-13104`. Available at `http://content.iospress.com/articles/journal-of-computer-security/jcs227`.

[7] S. Crafa & S. Rossi (2006): *P-congruences as non-interference for the pi-calculus*. In: Proceedings of the 2006 ACM workshop on Formal methods in security engineering, (FMSE'06), pp. 13–22, doi:`10.1145/1180337.1180339`.

[8] S. Crafa & S. Rossi (2007): *Controlling information release in the pi-calculus*. Information and Computation 205(8), pp. 1235–1273, doi:`10.1016/j.ic.2007.01.001`.

[9] Y. Deng & M. Hennessy (2013): *On the semantics of Markov automata*. Inf. Comput. 222, pp. 139–168, doi:`10.1016/j.ic.2012.10.010`.

[10] A. Di Pierro, C. Hankin & H.Wiklicky (2002): *Approximate Non-Interference*. In: Proc. of the IEEE Computer Security Foundations Workshop (CSFW'02), IEEE Computer Society Press, pp. 3–17, doi:`10.1109/CSFW.2002.1021803`.

[11] R. Focardi & R. Gorrieri (1994/1995): *A Classification of Security Properties for Process Algebras*. Journal of Computer Security 3(1), pp. 5–33, doi:`10.3233/JCS-1994/1995-3103`.

[12] R. Focardi & R. Gorrieri (2000): *Classification of Security Properties (Part I: Information Flow)*. In R. Focardi & R. Gorrieri, editors: Proc. of Foundations of Security Analysis and Design (FOSAD'00), LNCS 2171, Springer-Verlag, pp. 331–396, doi:`10.1007/3-540-45608-2_6`.

[13] R. Focardi, R. Gorrieri & F. Martinelli (2000): *Non Interference for the Analysis of Cryptographic Protocols*. In U. Montanari, J. D. P. Rolim & E. Welzl, editors: Proc. of Int. Colloquium on Automata, Languages and Programming (ICALP'00), LNCS 1853, Springer-Verlag, pp. 744–755, doi:`10.1007/3-540-45022-X_31`.

[14] R. Focardi, R. Gorrieri & F. Martinelli (2003): *Real-Time Information Flow Analysis*. IEEE Journal on Selected Areas in Communications 21(1), doi:`10.1109/JSAC.2002.806122`.

[15] R. Focardi & S. Rossi (2006): *Information flow security in dynamic contexts*. Journal of Computer Security 14(1), pp. 65–110, doi:`10.3233/JCS-2006-14103`. Available at `http://content.iospress.com/articles/journal-of-computer-security/jcs255`.

[16] R. Focardi, S. Rossi & A. Sabelfeld (2005): *Bridging Language-Based and Process Calculi Security*. In: Foundations of Software Science and Computational Structures, 8th International Conference, (FOSSACS'05), pp. 299–315, doi:`10.1007/978-3-540-31982-5_19`.

[17] J. A. Goguen & J. Meseguer (1982): *Security Policy and Security Models*. In: Proc. of the Symposium on Security and Privacy, IEEE Computer Society Press, pp. 11–20, doi:`10.1109/SP.1982.10014`.

[18] R. Gorrieri, E. Locatelli & F. Martinelli (2003): *A Simple Language for Real-Time Cryptographic Protocol Analysis*. In P. Degano, editor: Proc. of European Symposium on Programming (ESOP'03), LNCS 2618, Springer-Verlag, pp. 114–128, doi:`10.1007/3-540-36575-3_9`.

[19] M. Hennessy & J. Riely (2002): *Information Flow vs. Resource Access in the Asynchronous Pi-calculus*. ACM Transactions on Programming Languages and Systems (TOPLAS) 24(5), pp. 566–591, doi:`10.1145/570886.570890`.

[20] J. Hillston (1996): *A Compositional Approach to Performance Modelling*. Cambridge Press, doi:`10.1017/CBO9780511569951`.

[21] J. Hillston, A. Marin, C. Piazza & S. Rossi (2013): *Contextual Lumpability*. In: *Proc. of Valuetools 2013*, ACM Press, pp. 194–203, doi:10.4108/icst.valuetools.2013.254408.

[22] H. Mantel (2000): *Unwinding Possibilistic Security Properties*. In: *Proc. of the European Symposium on Research in Computer Security (ESoRiCS'00)*, *LNCS* 2895, Springer-Verlag, pp. 238–254, doi:10.1007/10722599_15.

[23] A. Marin & S. Rossi (2014): *On the Relations between Lumpability and Reversibility*. In: *Proc. of MASCOTS 2014*, pp. 427–432, doi:10.1109/MASCOTS.2014.59.

[24] A. Marin & S. Rossi (2017): *On the relations between Markov chain lumpability and reversibility*. *Acta Informatica* 54(5), pp. 447–485, doi:10.1007/s00236-016-0266-1.

[25] J. McLean (1994): *A General Theory of Composition for Trace Sets Closed under Selective Interleaving Functions*. In: *Proc. of the IEEE Symposium on Security and Privacy (SSP'94)*, IEEE Computer Society Press, pp. 79–93, doi:10.1109/RISP.1994.296590.

[26] J. K. Millen (1994): *Unwinding Forward Correctability*. In: *Proc. of the IEEE Computer Security Foundations Workshop (CSFW'94)*, IEEE Computer Society Press, pp. 2–10, doi:10.1109/CSFW.1994.315952.

[27] R. Milner (1989): *Communication and Concurrency*. Prentice-Hall. Available at https://dblp.org/rec/bib/books/daglib/0067019.

[28] C. Piazza, E. Pivato & S. Rossi (2004): *CoPS - Checker of Persistent Security*. In: *Tools and Algorithms for the Construction and Analysis of Systems, 10th International Conference (TACAS'04)*, pp. 144–152, doi:10.1007/978-3-540-24730-2_11.

[29] P. Y. A. Ryan & S. Schneider (2001): *Process Algebra and Non-Interference*. *Journal of Computer Security* 9(1/2), pp. 75–103, doi:10.3233/JCS-2001-91-204. Available at http://content.iospress.com/articles/journal-of-computer-security/jcs142.

[30] A. Sabelfeld & A. C. Myers (2003): *Language-Based Information-Flow Security*. *IEEE Journal on Selected Areas in Communication* 21(1), pp. 5–19, doi:10.1109/JSAC.2002.806121.

[31] G. Smith & D. M. Volpano (1998): *Secure Information Flow in a Multi-threaded Imperative Language*. In: *Proc. of POPL'98*, ACM Press, pp. 355–364, doi:10.1145/268946.268975.