A Survey on Non-Interference with Petri Nets

Nadia Busi and Roberto Gorrieri

Dipartimento di Scienze dell'Informazione, Università di Bologna
Mura A. Zamboni, 7, 40127 Bologna, Italy

Abstract. Several notions of non-interference have been proposed in the literature to study the problem of confidentiality in nondeterministic and concurrent systems. Here we rephrase some of them – notably *SNNI* and *BNDC* – over the model of safe Place/Transition Petri Nets. The common feature of these non-interference properties is that they are all defined as extensional properties based on some notion of behavioural equivalence on systems. Here we also address the problem of defining non-interference by looking at the structure of the net systems under investigation. We define *structural* non-interference properties based on the absence of particular places in the net. We characterize structural properties that are slight refinement of well-known properties such as *SNNI* and *SBNDC*. We then argue that, in order to capture all the intuitive interferences at the structural level, it is necessary to consider the net originated by the region construction, yielding the property *RBNI* we advocate.

1 Introduction

Non-interference has been defined in the literature as an extensional property based on some observational semantics: the high part of a system is non-interfering with the low part if whatever is done at the high level produces no visible effect on the low part of the system. The original notion of non-interference in [8] was defined, using trace semantics, for system programs that are deterministic. Generalized notions of non-interference were then designed to include (nondeterministic) labeled transition systems and finer notions of observational semantics such as bisimulation (see, e.g., [12, 6, 11, 13, 7]). Relevant properties in this class are the trace-based properties *SNNI* and *NDC*, as well as the bisimulation-based properties *BSNNI*, *BNDC* and *SBNDC* proposed by Focardi and Gorrieri some years ago [6, 7] on a CCS-like process algebra. In particular, *SNNI* states that a system R is secure if the two systems $R \setminus H$ (all the high level actions are prevented) and R/H (all the high level actions are permitted but are unobservable) are trace equivalent. *BNDC* intuitively states that a system R is secure if it is bisimilar to R in parallel with any high level process Π w.r.t. the low actions the two systems can perform. And *SBNDC* tells that a system R is secure if, whenever a high action h is performed, the two instances of the system before and after performing h are bisimilar from a low level point of view.

The first part of the paper is devoted to show that these non-interference properties, originally proposed on the Security Process Algebra, can be naturally defined also on Petri Nets; in particular – to keep the presentation as simple as possible – we use 1-safe Place/Transition Petri Nets [10]. The advantage of this proposal is the import in the Petri Net theory of security notions that makes possible the study of security problems. Technically, what we do is to introduce two operations on nets, namely parallel composition (with synchronization in TCSP-like style) and restriction, and suitable notions of observational equivalences on the low part of the system (low trace equivalence and low bisimulation); then, five security properties are defined and compared in a rather direct way. In particular, the two properties based on low trace semantics, namely *SNNI* and *NDC*, are equivalent. On the contrary, in the bisimulation case, *BSNNI* is weaker than *BNDC*, which turns out to be equivalent to *SBNDC*.

In this approach, the security property is based on the dynamics of systems; they are all defined by means of one (or more) equivalence check(s); hence, non-interference checking is as difficult as equivalence checking, a well-studied hard problem in concurrency theory.

In the second part of the paper, instead, we address the problem of defining statically non-interference by looking at the structure of the net systems under investigation:

– in order to better understand the causality and conflict among different system activites, hence grounding more firmly the intuition about what is an interference, and
– in order to find more efficiently checkable non-interference properties that are sufficient conditions for those that have already received some support in the literature.

We define structural non-interference properties based on the absence of particular places in the net. We identify two special classes of places: *causal places*, i.e., places for which there are an incoming high transition and an outgoing low transition; and, *conflict places*, i.e. places for which there are both low and high outgoing transitions. Intuitively, causal places represent potential source of interference (*hilo* flow for *high input – low output*), because the occurrence of the high transition is a prerequisite for the execution of the low transition. Similarly, conflict places represent potential source of interference (*holo* flow for *high output – low output*), because the occurrence of a low event tells us that a certain high transition will not occur.

The first result of the paper is that when causal places are absent, we get a non-interference property which is slightly finer than *SNNI*. More precisely, if N has no causal places, then N satisfies *SNNI*. We present an example that shows that this structural notion is actually finer than *SNNI*.

The second result is that when also conflict places are absent, we get a property, called *Place-Based Non-Interference* (*PBNI* for short), which is slightly finer than *SBNDC*. More precisely, if the net N has no causal and no conflict places, then N satisfies *SBNDC*. A relevant counterexample shows that the inclusion is strict. This counterexample also hints that *PBNI* may still miss some potentially dangerous interferences.

In order to capture all the intuitive interferences at the structural level, we argue that it is necessary to consider nets that are *saturated* w.r.t. the region construction [4, 1]. Intuitively, given the marking graph $MG(N)$ of a net N, another net N' is obtained by adding to N all the possible (useful) places such that $MG(N')$ is isomorphic to $MG(N)$. The final property we propose is called *Region-Based Non-Interference* (*RBNI* for short) that we advocate as the most intuitive non-interference notion in this setting.

The paper is organised as follows. In Section 2 we recall the basic definitions about transition systems and Petri Nets. In Section 3 we recast the behavioural approach to non-interference properties, originally defined in a process algebraic setting, on Petri Nets. The original structural property *PBNI* is introduced in Section 4, while *RBNI* is presented in Section 5. Finally, some conclusive remarks are drawn.

2 Basic definitions

Here we recall the basic definition about transition systems and safe Place/Transition Petri Nets we will use in the following.

2.1 Transition systems

Definition 1. *A transition system is a triple $TS = (St, E, \rightarrow)$ where*

- *St is the set of states*
- *E is the set of events*
- *$\rightarrow \subseteq St \times E \times St$ is the transition relation.*

In the following we use $s \stackrel{e}{\rightarrow} s'$ to denote $(s, e, s') \in \rightarrow$.

A rooted *transition system is a pair (TS, s_0) where $TS = (St, E, \rightarrow)$ is a transition system and $s_0 \in St$ is the* initial state.

Definition 2. *Let $TS_1 = (St_1, E_1, \rightarrow_1, s_1)$ and $TS_2 = (St_2, E_2, \rightarrow_2, s_2)$ be two rooted transition systems. An* isomorphism *is a bijection $f : St_1 \rightarrow St_2$ such that*

- *$s \stackrel{e}{\rightarrow} s'$ iff $f(s) \stackrel{e}{\rightarrow} f(s')$*
- *$s_2 = f(s_1)$.*

If there exists an isomorphism between TS_1 and TS_2 then we say that TS_1 and TS_2 are isomorphic.

2.2 Petri nets

Definition 3. *Given a finite set S, a* multiset over S *is a function $m : S \rightarrow \omega$. The set of all multisets over S is denoted by $\mathcal{M}(S)$ The* multiplicity *of an element s in m is the natural number $m(s)$. We write $m \subseteq m'$ if $m(s) \leq m'(s)$ for all $s \in S$. The operator $\oplus$ denotes* multiset union*: $(m \oplus m')(s) = m(s) + m'(s)$ for all $s \in S$. The operator $\setminus$ denotes* multiset difference*: $(m \setminus m')(s) = max\{m(s) - m'(s), 0\}$. We say that $s \in m$ if $m(s) > 0$. If $X \subseteq S$, with abuse of notation we use X to denote the multiset $X(s) = 1$ if $s \in X$ and $X(s) = 0$ otherwise.*

Definition 4. *A net is a tuple $N = (S, T, F)$, where*

- *S and T are the (finite) sets of* places *and* transitions, *such that $S \cap T = \emptyset$*
- *$F \subseteq (S \times T) \cup (T \times S)$ is the flow relation*

A multiset over the set S of places is called *marking*. Given a marking m and a place s, we say that the place s contains $m(s)$ tokens.

Let $x \in S \cup T$. The *preset* of x is the set ${}^\bullet x = \{y \mid F(y, x)\}$. The *postset* of x is the set $x^\bullet = \{y \mid F(x, y)\}$. The preset and postset functions are generalized in the obvious way to set of elements: if $X \subseteq S \cup T$ then ${}^\bullet X = \bigoplus_{x \in X} {}^\bullet x$ and $X^\bullet = \bigoplus_{x \in X} x^\bullet$. A transition t is enabled at marking m if ${}^\bullet t \subseteq m$. The firing (execution) of a transition t enabled at m produces the marking $m' = (m \backslash {}^\bullet t) \oplus t^\bullet$. This is usually written as $m[t\rangle m'$.

A *net system* is a pair (N, m_0), where N is a net and m_0 is a marking of N, called *initial marking*. With abuse of notation, we use (S, T, F, m_0) to denote the net system $((S, T, F), m_0)$.

The set of *markings reachable from* m, denoted by $[m\rangle$, is defined as the least set of markings such that

- $m \in [m\rangle$
- if $m' \in [m\rangle$ and there exists a transition t such that $m'[t\rangle m''$ then $m'' \in [m\rangle$.

The set of *firing sequences* is defined inductively as follows:

- m_0 is a firing sequence;
- if $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n$ is a firing sequence and $m_n[t_{n+1}\rangle m_{n+1}$ then $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n[t_{n+1}\rangle m_{n+1}$ is a firing sequence.

Given a firing sequence $m_0[t_1\rangle m_1 \ldots [t_n\rangle m_n$, we call $t_1 \ldots t_n$ a *transition sequence*. The set of transition sequences of a net N is denoted by $TS(N)$. We use σ to range over $TS(N)$. Let $\sigma = t_1 \ldots t_n$; we use $m[\sigma\rangle m_n$ as an abbreviation for $m[t_1\rangle m_1 \ldots [t_n\rangle m_n$.

The *marking graph* of a net N is

$$MG(N) = ([m_0\rangle, T, \{(m, t, m') \mid m \in [m_0\rangle \wedge t \in T \wedge m[t\rangle m'\})$$

A net is *pure* if ${}^\bullet t \cap t^\bullet = \emptyset$ for all transitions $t \in T$. A net is *simple* if the following condition holds for all $x, y \in S \cup T$: if ${}^\bullet x = {}^\bullet y$ and $x^\bullet = y^\bullet$ then $x = y$.

A net system is *safe* if each place contains at most one token in any marking reachable from the initial marking, i.e., $m(s) \leq 1$ for all $s \in S$ and for all $m \in [m_0\rangle$. A net system is *reduced* if each transition can occur at least one time: for all $t \in T$ there exists $m \in [m_0\rangle$ such that $m[t\rangle$.

In the following we consider safe net systems. To lighten the definitions, in Sections 4 and 5 we we consider safe net systems that are pure, simple and reduced.

3 A Behavioural Approach to Non-interference

In this section we want to recast some basic properties, proposed by Focardi and Gorrieri some years ago [6, 7], in our setting. Our aim is to analyse systems that can perform two kinds of actions: high level actions, representing the interaction of the system with high level users, and low level actions, representing the interaction with low level users. We want to verify if the interplay between the high user and the high part of the system can affect the view of the system as observed by a low user. We assume that the low user knows the structure of the system, and we check if, in spite of this, he is not able to infer the behavior of the high user by observing the low view of the execution of the system.

Hence, we consider nets whose set of transitions is partitioned into two subsets: the set H of high level transitions and the set L of low level transitions. To emphasize this partition we use the following notation. Let L and H be two disjoint sets: with (S, L, H, F, m_0) we denote the net system $(S, L \cup H, F, m_0)$.

The non-interference properties we are going to introduce are based on some notion of *low* observability of a system, i.e., what can be observed of a system from the point of view of low users. The low view of a transition sequence is nothing but the subsequence where high level transitions are discarded.

Definition 5. *Let $N = (S, L, H, F, m_0)$ be a net system. The* low view *of a transition sequence of N is defined as follows:*

$$\Lambda_N(\varepsilon) = \varepsilon$$

$$\Lambda_N(\sigma t) = \begin{cases} \Lambda_N(\sigma)t & \text{if } t \in L \\ \Lambda_N(\sigma) & \text{otherwise} \end{cases}$$

The definition of Λ_N is extended in the obvious way to sets of transitions sequences: $\Lambda_N(\Sigma) = \{\Lambda_N(\sigma) \mid \sigma \in \Sigma\}$ for $\Sigma \subseteq (L \cup H)^*$.

Definition 6. *Let N_1 and N_2 be two net systems. We say that N_1 is* low-view trace equivalent *to N_2, denoted by $N_1 \overset{\Lambda}{\approx}_{tr} N_2$, iff $\Lambda_{N_1}(TS(N_1)) = \Lambda_{N_2}(TS(N_2))$.*

We define the operations of parallel composition (in TCSP-like style) and restriction on nets, that will be useful for defining some non-interference properties.

Definition 7. *Let $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ be two net systems such that $S_1 \cap S_2 = \emptyset$ and $(L_1 \cup L_2) \cap (H_1 \cup H_2) = \emptyset$. The parallel composition of N_1 and N_2 is the net system*

$$N_1 \mid N_2 = (S_1 \cup S_2, L_1 \cup L_2, H_1 \cup H_2, F_1 \cup F_2, m_{0,1} \oplus m_{0,2})$$

Definition 8. *Let $N = (S, L, H, F, m_0)$ be a safe net system and let U be a set of transitions. The restriction on U is defined as $N \backslash U = (S, L', H', F', m_0)$, where*

$$L' = L \setminus U$$
$$H' = H \setminus U$$
$$F' = F \setminus (S \times U \cup U \times S)$$

Strong Nondeterministic Non-Interference (*SNNI* for short) is a trace-based property, that intuitively says that a system is secure if what the low-level part can see does not depend on what the high-level part can do.

Definition 9. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is SNNI iff $N \overset{\Lambda}{\approx}_{tr} N \backslash H$.*

The intuition is that, from the low point of view, the system where the high level transitions are prevented should offer the same traces as the system where the high level transitions can be freely performed. In essence, a low-level user cannot infer, by observing the low view of the system, that some high-level activity has occurred.

As a matter of fact, this non-interference property captures the information flows from high to low, while admits flows from low to high. For instance, the net N' of Figure 1 is *SNNI* while the net N'' is not *SNNI*.

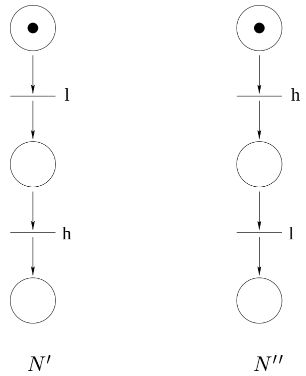

Fig. 1. The net system N' is *SNNI* while N'' is not *SNNI*.

An alternative notion of non-interference, called *Nondeducibility on Composition* (*NDC* for short), says that the low view of a system N in isolation is not to be altered when considering each potential interaction of N with the high users of the external environment.

Definition 10. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is a high-level net if $L = \emptyset$.*

Definition 11. *Let $N = (S, L, H, F, m_0)$ be a net system. N is NDC iff for all high-level nets $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$: $N \backslash H \overset{\Lambda}{\approx}_{tr} (N \mid K) \backslash (H \setminus H_K)$.*

The left-hand term represents the low view of the system N in isolation, while the right-hand term expresses the low view of N interacting with the high environment K (note that the activities resulting from such interactions are invisible by the definition of low bisimulation). *NDC* is a very intutive property: whatever high level system K is interacting with N, the low effect is unobservable. However, it is difficult to check this property because of the universal quantification over high systems. Luckily enough, we will then prove that *SNNI* and *NDC* are actually the same non-interference property.

Theorem 1. *Let $N = (S, L, H, F, m_0)$ be a net system. N is SNNI if and only if N is NDC.*

The two properties above are based on (low) trace semantics. It is well-known [7] that bisimulation semantics is more appropriate than trace semantics because it captures also some indirect information flows due to, e.g., deadlocks. For this reason, we now consider non-interference properties based on bisimulation. To this aim, we first need to introduce a notion of low–view bisimulation.

Definition 12. *Let $N_1 = (S_1, L_1, H_1, F_1, m_{0,1})$ and $N_2 = (S_2, L_2, H_2, F_2, m_{0,2})$ be two net systems. A* low–view bisimulation *from N_1 to N_2 is a relation on $\mathcal{M}(S_1) \times \mathcal{M}(S_2)$ such that if $(m_1, m_2) \in R$ then for all $t \in \bigcup_{i=1,2} L_i \cup H_i$:*

- *if $m_1[t\rangle m_1'$ then there exist σ, m_2' such that $m_2[\sigma\rangle m_2'$, $\Lambda_{N_1}(t) = \Lambda_{N_2}(\sigma)$ and $(m_1', m_2') \in R$*
- *if $m_2[t\rangle m_2'$ then there exist σ, m_1' such that $m_1[\sigma\rangle m_1'$, $\Lambda_{N_2}(t) = \Lambda_{N_1}(\sigma)$ and $(m_1', m_2') \in R$*

If $N_1 = N_2$ we say that R is a low–view bisimulation on N_1.

We say that N_1 is low–view bisimilar *to N_2, denoted by $N_1 \overset{\Lambda}{\approx}_{bis} N_2$, if there exists a low–view bisimulation R from N_1 to N_2 such that $(m_{0,1}, m_{0,2}) \in R$.*

The first obvious variation on the theme is to define the bisimulation based version of *SNNI*, yielding *BSNNI*.

Definition 13. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is BSNNI iff $N \overset{\Lambda}{\approx}_{bis} N \backslash H$.*

Obviously, *BSNNI* $\subseteq$ *SNNI*. The converse is not true: the net N in Figure 2 is *SNNI* but not *BSNNI*. Note that *SNNI* misses to capture the indirect information flow present in this net: if the low transition l is performed (and hence low observed), the low user can infer that the high transition h has not been performed, hence deducing one piece of high knowledge.

Similarly, *BNDC* can be defined from *NDC*, yielding a rather appealing security property, which is finer than *BSNNI*.

Definition 14. *Let $N = (S, L, H, F, m_0)$ be a net system. N is BNDC iff for all high-level nets $K = (S_K, \emptyset, H_K, F_K, m_{0,K})$: $N \backslash H \overset{\Lambda}{\approx}_{bis} (N \mid K) \backslash (H \setminus H_K)$.*

Theorem 2. *Let $N = (S, L, H, F, m_0)$ be a net system. If N is BNDC then N is BSNNI.*

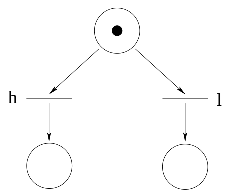

Fig. 2. A net system that is *SNNI* but not *BSNNI*.

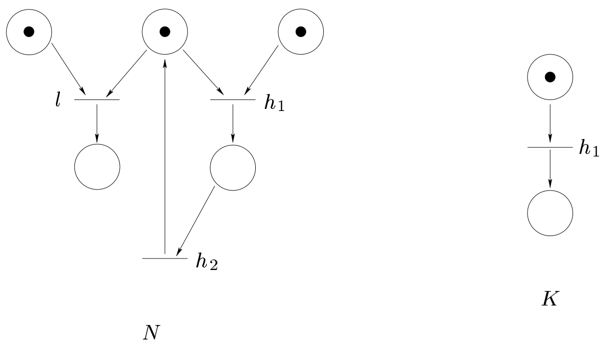

Fig. 3. A net system that is *BSNNI* but not *BNDC*.

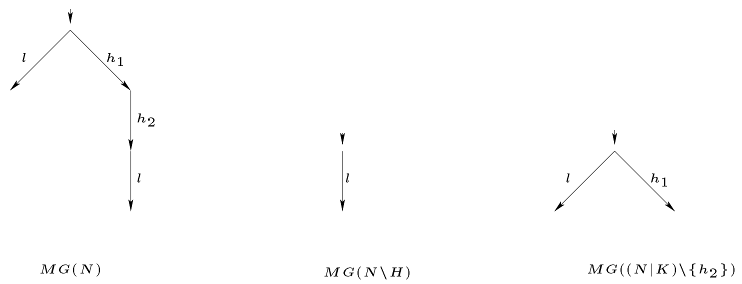

Fig. 4. The marking graphs of the net systems N, $N\backslash H$ and $(N \mid K)\backslash\{h_2\}$.

Unfortunately, the converse is not true: Figure 3 reports a net that is *BSNNI* but not *BNDC*; the reason why can be easily grasped by looking at their respective marking graphs in Figure 4.

BNDC is quite appealing but, because of the universal quantification on all poossible high level systems, it is difficult to check. The next property, called *Strong Bisimulation Non Deducibility on Composition* (*SBNDC* for short), is actually an alternative characterization of *BNDC* which is easily checkable.

Definition 15. *Let $N = (S, L, H, F, m_0)$ be a net system. N is SBNDC iff for all markings $m \in [m_0\rangle$ and for all $h \in H$ the following holds:*
if $m[h\rangle m'$ then there exists a low–view bisimulation R on $N \backslash H$ such that $(m, m') \in R$.

Theorem 3. *Let $N = (S, L, H, F, m_0)$ be a net system. N is BNDC if and only if N is SBNDC.*

The theorem above holds because we are in an unlabeled setting: transitions are not labeled. In [6, 7] it is proved that – for the security Process Algebra – *SBNDC* is strictly finer than *BNDC*.

4 Place-Based Non-Interference in Petri Nets

In this section we define a non-interference property based on the absence of some kinds of places in a net system. Consider a net system $N = (S, L, H, F, m_0)$.

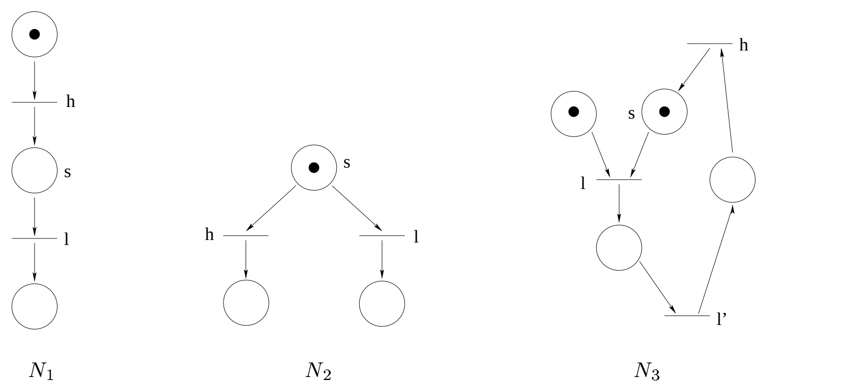

Fig. 5. Examples of net systems containing conflict and (potentially) causal places.

Consider a low level transition l of the net: if l can fire, then we know that the places in the preset of l are marked before the firing of l; as the nets under investigation are pure nets, we also know that such places become unmarked after the firing of l. If there exists a high level action h that produces a token in a place s in the preset of l (see the system N_1 in Figure 5), then the low level user can infer that h has occurred if he can observe the occurrence of the low level action l. We note that there exists a causal dependency between the transitions h and l, because the firing of h produces a token is consumed by l. Consider now the situation illustrated in the system N_2 of Figure 5: in this case, place s is in the preset of both l and h, i.e., l and h are competing for the use of the resource represented by the token in s. Aware of the existence of such a place, a low user knows that no high-level action h has been performed, if he observes the low-level action l. Place s represents a conflict between transitions l and h, because the firing of l prevents h from firing.

Our idea is to consider a net system secure if it does not contain places of the kinds illustrated above.

In order to avoid the definition of a security notion that is too strong, and that prevents systems with no flow of information to be considered secure, we need to refine the concept of causal place. Let s be a place such that $s \in h^\bullet \cap {}^\bullet l$. If s is empty in the initial state of the system, then the low user can infer that h has occurred from the occurrence of l. On the other hand, if s is marked in the initial state, then the first occurrence of l can happen even if h has not fired; thus, the low level user can infer that h has occurred by observing two occurrences of l. Hence, in this last case, such a place s is a source of a flow of information only if transition l can be fired at least two times. For example, consider the net system N_3 reported in Figure 5. Place s is a potentially causal place, but the system has to be considered secure, as the only (maximal) transition sequence is $ll'h$.

Definition 16. *Let $N = (S, L, H, F, m_0)$ be a net system. Let s be a place of N such that $s^\bullet \cap L \neq \emptyset$.*

The place $s \in S$ is a potentially causal place *if ${}^\bullet s \cap H \neq \emptyset$. A potentially causal place s is a* causal place *if the following condition holds: if $m_0(s) > 0$ then there exists a transition sequence $t_1 \ldots t_n$ and $i < n$ s.t. $t_i, t_n \in s^\bullet \cap L$.*

The place $s \in S$ is a conflict place *if $s^\bullet \cap H \neq \emptyset$.*

Definition 17. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is PBNI (*Place Based Non-Interference*) if, for all $s \in S$, s is neither a causal place nor a conflict place.*

Now we show that the absence of causal places implies *SNNI*. We need the following preliminary lemma.

Lemma 1. *Let $N = (S, L, H, F, m_0)$ be a net system without causal places. if $m_0[\sigma\rangle m_1$ then there exists m_2 s.t. $m_0[\Lambda_N \sigma\rangle m_2$ and $m_2(s) \geq m_1(s)$ for all $s \in {}^\bullet L$.*

Theorem 4. *Let $N = (S, L, H, F, m_0)$ be a net system. If N has no causal places then N is SNNI.*

The converse is not true. For example, consider the net system N_4 in Figure 6: place s is a causal place, but N_4 is *SNNI* (but not *SBNDC*). However, as we will

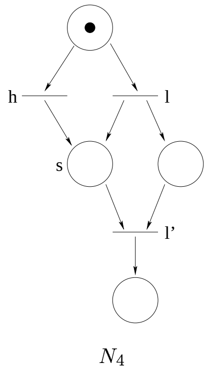

Fig. 6. A net system containing a causal place, whose marking graph is *SNNI*.

see in Section 5, in absence of any form of conflicts in the system, *SNNI* implies the absence of causal places.

As *SBNDC* can reveal the presence of conflicts between high-level transitions and low-level transitions, the absence of causal places in a system is not sufficient to guarantee *SBNDC*. Consider for example the system N_2 in Figure 5, and its marking graph $MG(N_2)$ reported in Figure 8. The system N_2 has no causal places, but N_2 is not *SBNDC*. In fact, $m_1 \xrightarrow{h} m_2$ and the markings m_1 and m_2 have different low-level behaviours, because m_1 can perform l whereas m_2 cannot perform any action.

If we take into account also conflict places, we obtain that the absence of both causal and conflict places is a sufficient condition for *SBNDC*.

Theorem 5. *Let $N = (S, L, H, F, m_0)$ be a net system. If N is PBNI then N is SBNDC.*

On the other hand, the absence of causal and conflict places is not a necessary condition for *SBNDC*. Consider the system N_5 reported in Figure 7: the system contains a conflict place, s, hence N_5 is not *PBNI*. However, N_5, whose marking graph is reported in Figure 8, is *SBNDC*: in fact, the only high-level transition is $m_3 \xrightarrow{h} m_4$, and m_3 and m_4 are behaviourally equivalent because both markings have no low outgoing moves.

In our opinion, the system N_5 is not secure, because the occurrence of the low-level transition l permits to a low-level user to deduce that no high-level action has been (and will be) performed. We note that the same kind of information flow is exhibited by the system N_2 of Figure 5, which, on the contrary, is not *SBNDC*.

Hence, *SBNDC* fails to capture some kinds of interference, concerned with the presence of a conflict between a low-level transition and a high-level one. Indeed, also the absence of conflict places, hence *PBNI*, is not sufficient to ensure the absence of the kind of interference discussed above. Consider for the example

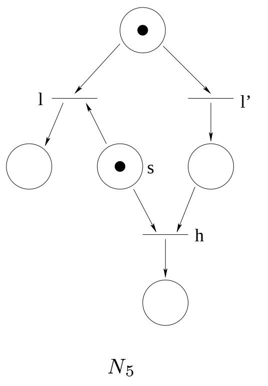

Fig. 7. Two examples of net systems that illustrate the inadequacy of *SBNDC* and *PBNI*.

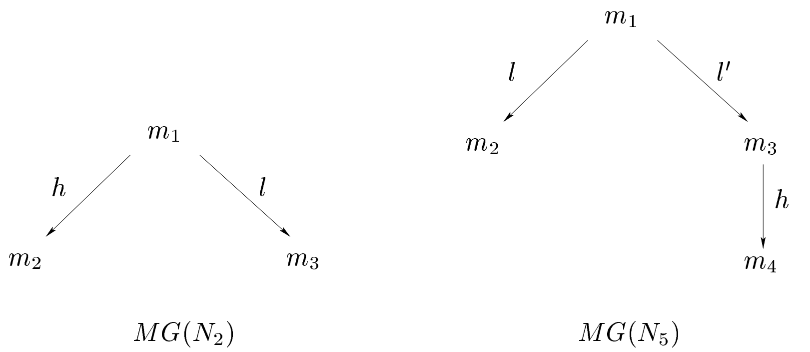

Fig. 8. The marking graphs of the systems N_2 (Figure 5) and N_5 (Figure 7).

the system N_5^- of Figure 7, obtained by removing the conflict place s from N_5. The two systems N_5 and N_5^- have the same behaviour, as their marking graphs are isomorphic, but N_5^- is *PBNI*. The example above suggests us to look for conflict places not only in the system under investigation, but in all the systems exhibiting the same marking graph.

5 Region-Based Non-Interference in Petri Nets

In this section we enhance *PBNI* to capture the kind of interference we envisaged in system N_5^-. We learned from the previous section that in order to capture some kinds of information flows – arising from conflicts among high and low transitions – it is necessary to look for the presence of conflict places in all the systems whose marking graph is isomorphic to the marking graph of the analyzed system. To construct all such places, we exploit the notion of region, introduced in [4] and investigated, e.g., in [1, 2] for the synthesis of Petri nets. [1] A region is a set of states in the marking graph of a net, corresponding to a real or a potential place of the net. After recalling some basic notions and results on regions (see, e.g., [2]), the non-interference notion based on regions is introduced.

5.1 Theory of regions

Given the marking graph G of a safe net system N, a region of G is basically a set of markings corresponding to the states where a real or potential place of N is marked. In other words, a region r groups together all the states of the graph in which a place r contains a token. Let r be a region of $MG(N)$. Consider a place s that is necessary for a transition t to happen, i.e., $s \in {}^\bullet t$. Let $m \in r$ and assume that $m[t\rangle$; then, s is marked in m; as we consider pure nets, s is no longer marked after the firing of t. Thus, we have a transition $m \xrightarrow{t} m'$ in the marking graph, and $m'(s) = 0$; hence, $m' \notin r$. So, for each state in r, if a t-labelled transition exits from it then that transition enters a state that is not in r. Moreover, if a state m is outside r, then t cannot happen in m, because the place s in the preset of t is empty; so we do not have t- labelled transitions exiting from s. To summarize, if $s \in {}^\bullet t$, then each t-labelled transition of the graph starts inside r and ends outside r. Analogously, if a transition t produces a token in s, i.e., $s \in t^\bullet$, then each t-labelled transition in the graph has source outside r and target inside r.

Suppose now that place s is unrelated to transition t, i.e., $s \notin {}^\bullet t \cup t^\bullet$. If t fires in a state where s is marked, then place s is marked also after the firing of t; that is, if a t-labelled transition starts inside r, then it also ends inside r. Analogously, if t happens in a state where s is empty, then s remains empty also after the firing of t, i.e., t-labelled transitions that start outside r also end outside r.

[1] The restriction to safe Place/Transition nets is essential to keep the presentation of the region construction as simple as possible.

From the above discussion we deduce that t-labelled transitions have a uniform behaviour w.r.t. r: either all of them cross r exiting, or all of them cross r entering, or none of them cross r.

We recall here the notion of region and some relevant results that will be used later.

Definition 18. *Let $TS = (St, E, \rightarrow)$ be a transition system, a set $r \subseteq St$ is said to be a* region *if and only if $\forall s_1 \xrightarrow{e} s_1', s_2 \xrightarrow{e} s_2'$ the following conditions hold:*

- *if $s_1 \in r$ and $s_1' \notin r$ then $s_2 \in r$ and $s_2' \notin r$;*
- *if $s_1 \notin r$ and $s_1' \in r$ then $s_2 \notin r$ and $s_2' \in r$.*

It is easy to see that both St and $\emptyset$ are regions, and they are called the *trivial* regions. The set of *non-trivial* regions of a transition system TS will be denoted with $Reg(TS)$.

The complementary set of a region is itself a region:

Proposition 1. *Let $TS = (St, E, \rightarrow)$ be a transition system. If r is a region of TS, then also $St \setminus r$ is a region of TS.*

As t-labelled arcs have a uniform behaviour w.r.t. a region, we can define the analogous of preset and postset for events and regions

Definition 19. *Let $TS = (St, E, \rightarrow)$ be a transition system and $e \in E$. The preregionset and the postregionset of e are the sets of regions defined as follows:*

$$
\begin{aligned}
{}^\circ e &= \{r \in Reg(TS) \mid \forall (s, e, s') \in \rightarrow : s \in r \wedge s' \notin r\} \\
e^\circ &= \{r \in Reg(TS) \mid \forall (s, e, s') \in \rightarrow : s \notin r \wedge s' \in r\}
\end{aligned}
$$

Given a region r of TS, ${}^\circ r = \{e \in E \mid r \in e^\circ\}$ and $r^\circ = \{e \in E \mid r \in {}^\circ e\}$.

The following proposition explains the relation between the places of a net system and the regions of its marking graph.

Definition 20. *Let $N = (S, T, F, m_0)$ be a net system and let $s \in S$. With r_s we denote the set of states of $MG(N)$ where s is marked: $r_s = \{m \in [m_0\rangle \mid m(s) = 1\}$.*

Proposition 2. *Let $N = (S, T, F, m_0)$ be a net system and let $s \in S$. The set r_s is a region of $MG(N)$.*

Proposition 3. *Let $N = (S, T, F, m_0)$ be a net system and let $s \in S$. We have that ${}^\bullet s = {}^\circ r_s$ and $s^\bullet = r_s^\circ$.*

On the other hand, a region not always corresponds to a place of the net, but may represent a potential place. The addition of such a potential place to the net system has no influence on its behaviour.

Definition 21. *Let $N = (S, T, F, m_0)$ be a net system and let r be a region of $MG(N)$ s.t. the following holds: $\forall s \in S : {}^\circ r \neq {}^\bullet s$ or $r^\circ \neq s^\bullet$. Let s_r be a place s.t. $s_r \notin S$. We net system $N^{+r} = (S', T, F', m_0')$ is defined as follows:*

$$\begin{aligned} S' &= S \cup \{s_r\} \\ F' &= F \cup \{(s_r, t) \mid r \in {}^\circ t\} \cup \{(t, s_r) \mid r \in t^\circ\} \\ m_0' &= \begin{cases} m_0 \oplus \{s_r\} & \textit{if } m_0 \in r \\ m_0 & \textit{otherwise} \end{cases} \end{aligned}$$

Proposition 4. *Let N be a net system and r be a region of $MG(N)$. Then $MG(N)$ is isomorphic to $MG(N^{+r})$.*

Given a net sytem N, we can construct the *saturated* version of (the marking graph of) N, obtained by using all the nontrivial regions of $MG(N)$ as places. Note that the set $Reg(MG(N))$ is finite, as the set of nontrivial regions of a transition system is a subset of the powerset of the set of states of the transition system, and the set of states of the marking graph of a safe Petri net is finite.

Definition 22. *Let $TS = (St, E, \rightarrow, s_0)$ be the marking graph of a net system. The net system $Sat(G) = (S, T, F, m_0)$ is defined as follows:*

$$\begin{aligned} S &= Reg(G) \\ T &= E \\ F &= \{(r, e) \mid r \in {}^\circ e\} \cup \{(e, r) \mid r \in e^\circ\} \\ m_0(r) &= \begin{cases} 1 & \textit{if } s_0 \in r \\ 0 & \textit{otherwise} \end{cases} \end{aligned}$$

Proposition 5. *Let N be a net system. Then $MG(N)$ is isomorphic to $MG(Sat(MG(N)))$.*

5.2 Region-Based Non-Interference

We introduce a non-interference property based on the absence of some kinds of regions in the marking graph of a net system.

Definition 23. *Let $N = (S, L, H, F, m_0)$ be a net system. Let r be a region in $Reg(MG(N))$ such that $r^\circ \cap L \neq \emptyset$.*

The region $r \in Reg(MG(N))$ is a potentially causal region *if ${}^\circ r \cap H \neq \emptyset$. A potentially causal region r is a* causal region *if the following condition holds: if $m_0 \in r$ then there exists a transition sequence $t_1 \dots t_n$ and $i < n$ s.t. $t_i, t_n \in r^\circ \cap L$.*

The region r is a conflict region *if $r^\circ \cap H \neq \emptyset$.*

Definition 24. *Let $N = (S, L, H, F, m_0)$ be a net system. We say that N is RBNI (*Region-Based Non-Interference*) if, for all regions $r \in Reg(MG(N))$, r is neither a causal region nor a conflict region.*

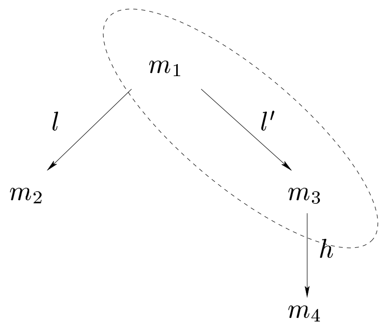

Fig. 9. A conflict region of net N_5^- (Figure 7).

Consider the net system N_5^- in Figure 7. We have that the region $r = \{m_1, m_3\}$ illustrated in Figure 9 is a conflict region, as $l, h \in r^\circ$. Hence, N_5^- is *PBNI* but it is not *RBNI*.

Proposition 6. *Let $N = (S, L, H, F, m_0)$ be a net system. If N is RBNI then N is also PBNI.*

Instead of looking for causal (resp. conflict) regions in the marking graph of a net system N, we can equivalently check for presence of causal (resp. conflict) places in the saturated version of N.

Proposition 7. *Let $N = (S, L, H, F, m_0)$ be a net system. The system N is RBNI if and only if the system $Sat(MG(N))$ is PBNI.*

In Section 4 we argued that the absence of causal regions is not a necessary condition for *SNNI*, because of the existence of places that contain both causal and conflict relations. Now we show that if no conflict is present, i.e., there exist no conflict region in the marking graph of the system, then *SNNI* is equivalent to the absence of causal places.

Theorem 6. *Let $N = (S, H \cup L, F, m_0)$ be a net system such that $MG(N)$ has no conflict regions. Then N has no causal places if and only if N is SNNI.*

A consequence of the above result is that, in absence of conflicts, *PBNI* is equivalent to *RBNI*.

Corollary 1. *Let $N = (S, L, H, F, m_0)$ be a net system such that $MG(N)$ has no conflict regions. Then N is PBNI if and only if N is RBNI.*

6 Conclusions

A survey is presented on five behavioural non-interference properties, as well as on two new structural ones, *PBNI* and *RBNI*, that we propose to firm more strongly the intuition about the nature of interferences and to obtain more efficiently checkable property. With the help of many examples, we have shown that *RBNI* seems to capture all the intuitive interferences that are possible due to causality and conflict. Moreover, *PBNI* is a sufficient condition for *SNNI* and *SBNDC*, hence offering a very efficient way to check these observational non-interference properties.

The two properties *PBNI* and *RBNI* are structural because no notion of observational equivalence is considered in their definition; however, to be precise, the definition of *RBNI* requires an exploration of the state space (marking graph), hence it is in some sense a *behavioural* property.

The current investigation was conducted for safe Place/transition Petri nets. The choice of such a restrictive class is due to the fact the we wanted to introduce our security properties, in particular *RBNI* with the minimal technical overhead. The results presented here scales smoothly to elementary net systems [5] as well as safe nets with self-loops.

The current investigation was conducted in an unlabeled setting: transitions in the Petri nets are unlabeled. A natural extension of this approach is to consider labeled systems, also equipped with the unobservable action ε. Labels can be used to represent an abstraction of the system where different transitions are considered as equivalent (from the observational point of view). Therefore, we can model situations where the low user is not able to recognize precisely the low transition in execution but only its equivalence class w.r.t. observation. Similarly, label ε is used to model transitions that the low user cannot observe and which is not interested to. Such an extension would also permit to export our approach to process algebras, because it is well-known (see e.g., [3]) how to map (some) process algebras to safe Petri nets.

References

1. E. Badouel and Ph. Darondeau. Theory of regions. *Lectures on Petri Nets I: Basic Models*, Springer LNCS 1491:529:586, 1998.
2. J. Desel and W. Reisig. The synthesis problem of Petri nets. *Acta Informatica*, 33:296–315, 1996.
3. P. Degano, R. De Nicola, U. Montanari, "A Distributed Operational Semantics for CCS based on C/E Systems", *Acta Informatica* 26, 59-91, 1988.
4. A. Ehrenfeucht and G. Rozenberg. Partial (set) 2-structures; I and II. *Acta Informatica*, 27:315–368, 1990.
5. J.Engelfriet and G. Rozenberg. Elementary Net Systems *Lectures on Petri Nets I: Basic Models*, Springer LNCS 1491, 1998.
6. R. Focardi, R. Gorrieri, *"A Classification of Security Properties"*, Journal of Computer Security 3(1):5-33, 1995
7. R. Focardi, R. Gorrieri, *"Classification of Security Properties (Part I: Information Flow)"*, Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R. Gorrieri, Eds.), Springer LNCS 2171:331-396, 2001
8. J.A. Goguen, J. Meseguer, *"Security Policy and Security Models"*, Proc. of Symposium on Security and Privacy, IEEE CS Press, pp. 11-20, 1982

9. C. A. Petri, *Kommunikation mit Automaten*, PhD Thesis, Institut für Instrumentelle Mathematik, Bonn, Germany, 1962.
10. W. Reisig, "Petri Nets: An Introduction", EATCS Monographs in Computer Science, Springer, 1985.
11. A.W. Roscoe, *"CSP and Determinism in Security Modelling"*, Proc. of IEEE Symposium on Security and Privacy, IEEE CS Press, pp. 114-127, 1995
12. P.Y.A. Ryan, *"Mathematical Models of Computer Security"*, Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R. Gorrieri, Eds.), Springer LNCS 2171:1-62, 2001
13. P.Y.A. Ryan, S. Schneider, *"Process Algebra and Noninterference"*, Proc. of 12th Computer Security Foundations Workshop, IEEE CS Press, pp. 214-227, 1999