Non-Interference Notions Based on Reveals and Excludes Relations for Petri Nets

Luca Bernardinello, Görkem Kılınç, and Lucia Pomello

Dipartimento di informatica, sistemistica e comunicazione
Università degli Studi di Milano-Bicocca, Italy

Abstract. In distributed systems, it is often important that a user is not able to infer if a given action has been performed by another component, while still being able to interact with that component. This kind of problems has been studied with the help of a notion of "interference" in formal models of concurrent systems (e.g. CCS, Petri nets). Here, we propose several new notions of interference for ordinary Petri nets, study some of their properties, and compare them with notions already proposed in the literature. Our new notions rely on the unfolding of Petri nets, and on an adaptation of the "reveals" relation for ordinary Petri nets, previously defined on occurrence nets, and on a new relation, called "excludes", here introduced for detecting negative information flow.

Keywords: information flow, non-interference, reveals, excludes, Petri nets, unfolding.

1 Introduction

In distributed systems, information flows among components. The flow can be used to rule the behavior of the system, to guarantee the correct synchronization of tasks, to implement a communication protocol, and so on.

In some cases, a flow of information from one component to another is actually a *leakage*: that piece of information should not have passed from here to there. Such unwanted flows can endanger the working of the system.

In this paper, we study formal notions of unwanted information flow, based on a general notion of *non-interference*, within the theory of Petri nets, and compare our approach with existing approaches.

Non-interference was first defined for deterministic programs [1]. Later, several adaptations were proposed for more abstract settings, like transition systems, usually related to observational semantics [2–6].

Broadly speaking, these approaches assume that the actions performed in a system belong to two types, conventionally called *high* (hidden) and *low* (observable). A system is then said to be free from interference if a user, by interacting only via low actions, cannot deduce information about which high actions have been performed.

This approach was formalized in terms of 1-safe Petri nets in [7], relying on known observational equivalences, including bisimulation. Similarly to Busi and Gorrieri [7], in this paper we analyze systems that can perform high and low level actions and we check if an observer, who knows the structure of the system, can deduce information about the high actions by observing low actions. We rely on a progress assumption which was ignored in non-interference notions in the literature.

We propose new notions of non-interference for ordinary Petri nets. They deal with positive information flow as well as negative information flow, regarding both past and future occurrences and are based on unfoldings and on reveals and excludes relations which are formally defined in Section 3. *Reveals* was originally defined as a relation between events of an occurrence net in [8] and applied in fault diagnosis. Here, we adapt this relation to transitions of Petri nets. Intuitively, a transition t_1 reveals another transition t_2 if, by observing the occurrence of t_1, it is possible to deduce the occurrence of t_2. *Excludes* is a new relation between transitions of a Petri net, which is introduced in order to detect negative information flow. A transition t_1 excludes another transition t_2 if, by observing the occurrence of t_1, it is possible to deduce that t_2 has not yet occurred and will not occur in the future, i.e., they never appear together in the same run.

The first notion of non-interference we introduce is called *Reveals based Non-Interference (RNI)* and it states that a net is secure if no low transition reveals any high transition. This new notion is introduced in Section 4.1. We also propose more restrictive notions called *k-Extended-Reveals based Non-Interference (k-ERNI)* and *n-Repeated-Reveals based Non-Interference (n-ReRNI)*, they are based on observation of multiple occurrences of low transitions. These two parametric non-interference notions are introduced and discussed in Section 4.2 and Section 4.3. In Section 4.4, *Positive/Negative Non-Interference (PNNI)* is introduced on the basis of both the reveals and excludes relations between low and high transitions capturing both positive and negative information flow. The new notions are discussed and compared with each other while they are introduced. In Section 5, we compare, on the basis of examples, the new introduced notions with the ones already introduced in the literature and mentioned at the beginning of Section 4. Finally, Section 6 concludes the paper and discusses some possible developments.

2 Basic Definitions

In this section we collect preliminary definitions and set the notation which will be used in the rest of the paper.

Let $R \subseteq I \times I$ be a binary relation, the transitive closure of R is denoted by R^+; the reflexive and transitive closure of R is denoted by R^*.

A *net* is a triple $N = (B, E, F)$, where B and E are disjoint sets, and $F \subseteq (B \times E) \cup (E \times B)$ is called the *flow relation*. The pre-set of an element $x \in B \cup E$

is the set ${}^\bullet x = \{y \in B \cup E \mid (y,x) \in F\}$. The post-set of x is the set $x^\bullet = \{y \in B \cup E \mid (x,y) \in F\}$.

An (ordinary) Petri net $N = (P, T, F, m_0)$ is defined by a net (P, T, F), and an initial marking $m_0 : P \to \mathbb{N}$. The elements of P are called *places*, the elements of T are called *transitions*. A net is finite if the sets of places and of transitions are finite.

A *marking* is a map $m : P \to \mathbb{N}$. A marking m is safe if $m(p) \in \{0, 1\}$ for all $p \in P$. Markings represent global states of a net.

A transition t is *enabled* at a marking m if, for each $p \in {}^\bullet t$, $m(p) > 0$. We write $m[t\rangle$ when t is enabled at m. A transition enabled at a marking can *fire*, producing a new marking. Let t be enabled at m; then, the firing of t in m produces the new marking m', defined as follows:

$$m'(p) = \begin{cases} m(p) - 1 & \text{for all } p \in {}^\bullet t \setminus t^\bullet \\ m(p) + 1 & \text{for all } p \in t^\bullet \setminus {}^\bullet t \\ m(p) & \text{in all other cases} \end{cases}$$

We will write $m[t\rangle m'$ to mean that t is enabled at m, and that firing t in m produces m'.

A marking q is *reachable* from a marking m if there exist transitions $t_1 \dots t_{k+1}$ and intermediate markings $m_1 \dots m_k$ such that

$$m[t_1\rangle m_1[t_2\rangle m_2 \dots m_k[t_{k+1}\rangle q$$

The set of markings reachable from m will be denoted by $[m\rangle$. If all the markings reachable from m_0 are safe, then $N = (P, T, F, m_0)$ is said to be 1-safe (or, shortly, safe).

Let $N = (B, E, F)$ be a net, and $x, y \in B \cup E$. If there exist $e_1, e_2 \in E$, such that $e_1 \neq e_2$, $e_1 F^* x$, $e_2 F^* y$, and there is $b \in {}^\bullet e_1 \cap {}^\bullet e_2$, then we write $x \# y$.

A net $N = (B, E, F)$ is an *occurrence net* if the following restrictions hold:

1. $\forall x \in B \cup E : \neg(x F^+ x)$
2. $\forall x \in B \cup E : \neg(x \# x)$
3. $\forall e \in E : \{x \in B \cup E \mid x F^* e\}$ is finite
4. $\forall b \in B : |{}^\bullet b| \leq 1$

The set of minimal elements of an occurrence net N with respect to F^* will be denoted by ${}^\circ N$. The elements of B are called *conditions* and the elements of E are called *events*. If $x \# y$ in an occurrence net, then we say that x and y are in conflict. Let $e \in E$ be an event in an occurrence net; then the *past* of e is the set of events preceding e in the partial order given by F^*: $\uparrow e = \{t \in E \mid t F^* e\}$. An occurrence net represents the alternative histories of a process; therefore its underlying graph is acyclic, and paths branching from a condition, corresponding to a choice between alternative behaviors, never converge.

A *run* of an occurrence net $N = (B, E, F)$ is a set R of events which is closed with respect to the past, and free of conflicts: (1) for each $e \in R$, $\uparrow e \subseteq R$; (2)

for each $e_1, e_2 \in R$, $\neg(e_1 \# e_2)$. A run is maximal if it is maximal with respect to set inclusion.

Let $N_i = (P_i, T_i, F_i)$ be a net for $i = 1, 2$. A map $\pi : P_1 \cup T_1 \to P_2 \cup T_2$ is a morphism from N_1 to N_2 if:

1. $\pi(P_1) \subseteq P_2$; $\pi(T_1) \subseteq T_2$
2. $\forall t \in T_1$ the restriction of π to ${}^\bullet t$ is a bijection from ${}^\bullet t$ to ${}^\bullet \pi(t)$
3. $\forall t \in T_1$ the restriction of π to $t^\bullet$ is a bijection from $t^\bullet$ to $\pi(t)^\bullet$

In the rest of the paper, we will consider finite Petri nets, i.e., Petri nets whose underlying net is finite, except for occurrence nets. Of course, Petri nets may have infinite behavior. Moreover, we assume that all transitions of a Petri net have non-empty preset, i.e., all have input places.

A *branching process* of a Petri net $N = (P, T, F, m_0)$ is a pair (O, π), where $O = (B, E, G)$ is an occurrence net, and π is a morphism from O to N such that:

1. $\forall p \in P\ m_0(p) = |\pi^{-1}(p) \cap {}^\circ O|$
2. $\forall x, y \in E$, if ${}^\bullet x = {}^\bullet y$ and $\pi(x) = \pi(y)$, then $x = y$

A branching process $\Pi_1 = (O_1, \pi_1)$ is a prefix of $\Pi_2 = (O_2, \pi_2)$ if there is an injective morphism f from O_1 to O_2 which is a bijection when restricted to ${}^\circ O_1$, and such that $\pi_1 = \pi_2 f$.

Any finite Petri net N has a unique branching process which is maximal with respect to the prefix relation. This maximal process, called the *unfolding* of N, will be denoted by $\mathrm{Unf}(N) = ((B, E, F), \lambda)$, where λ is the morphism from (B, E, F) to N [9]. In Fig. 1, a Petri net with its infinite unfolding is illustrated.

The following definition will be used in the rest of the paper to denote the set of events of an unfolding corresponding to a specific transition of a given Petri net.

Definition 1. *Let $N = (P, T, F, m_0)$ be a Petri net, $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ be its unfolding and $t \in T$, the set of events corresponding to t is denoted $E_t = \{e \in E \mid \lambda(e) = t\}$.*

The following definitions concern the *reveals* relation, originally introduced in [8] and applied to diagnostics problems. This notion has been further studied in [10] and [11].

Definition 2. *Let $O = (B, E, F)$ be an occurrence net, $\Omega \subseteq 2^E$ be the set of its maximal runs, and e_1, e_2 be two of its events. Event e_1 reveals e_2, denoted $e_1 \rhd e_2$, iff $\forall \sigma \in \Omega$, $e_1 \in \sigma \implies e_2 \in \sigma$*

Definition 3. *[10]Let $O = (B, E, F)$ be an occurrence net, $\Omega \subseteq 2^E$ be the set of its maximal runs, and A, B two sets of events. A extended-reveals B, $A \twoheadrightarrow B$, iff $\forall \omega \in \Omega, A \subseteq \omega \implies B \cap \omega \neq \emptyset$.*

In other words, a set of events, A, extended-reveals another set of events, B, written $A \twoheadrightarrow B$, iff every maximal run that contains A also hits B. The reveals relation can be expressed as extended-reveals relation between singletons: $a \rhd b$ can be written as $\{a\} \twoheadrightarrow \{b\}$.

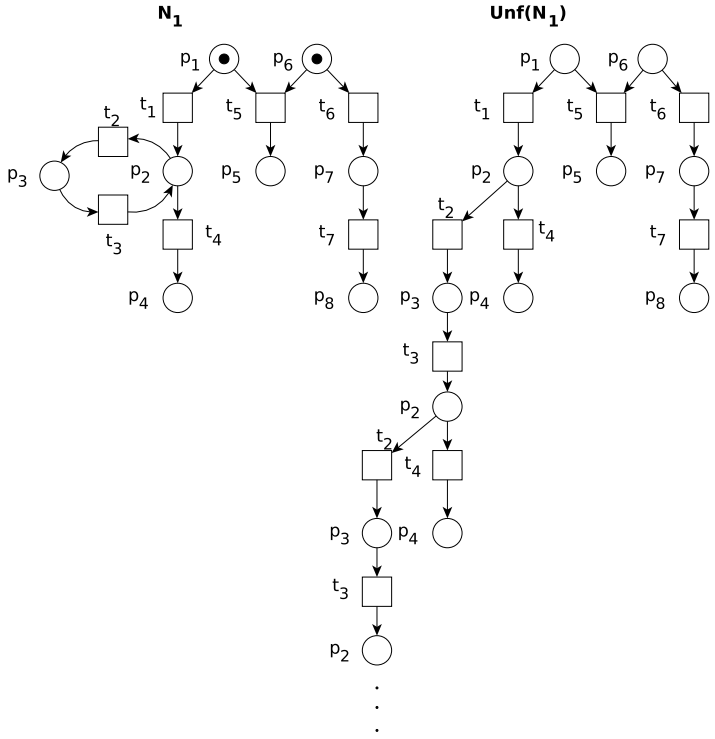

Fig. 1. A Petri net and its unfolding

Example 1. To give a simple example on the original reveals and extended-reveals notions, we examine the occurrence net in Fig. 2. In this net, $e_2 \rhd e_4$ and $e_4 \rhd e_2$. In general reveals relation is not symmetrical. As an example, $e_6 \rhd e_4$ but $e_4 \not\rhd e_6$ since after e_4, e_7 can occur instead of e_6.

In the same occurrence net, the occurrence of e_1 does not necessarily mean that e_5 will occur, but e_1 together with e_2 extended-reveals e_5, denoted as $\{e_1, e_2\} \twoheadrightarrow \{e_5\}$. The occurrence of e_4 reveals neither e_6 nor e_7. However, it reveals that either e_6 or e_7 will occur, denoted as $\{e_4\} \twoheadrightarrow \{e_6, e_7\}$.

3 Excludes and Reveals Relations on Petri Nets

In this section, we first introduce a new relation between transitions, called *excludes*, which will be used to detect negative information flow. Later, we define a *reveals* and an *extended-reveals* relation on the set of transitions of a Petri net, relying on the corresponding relations on occurrence nets as recalled in Section 2. Moreover, we introduce a new parametric relation, called *repeated-reveals*, again on the set of transitions of a Petri net. Reveals, extended-reveals and repeated-

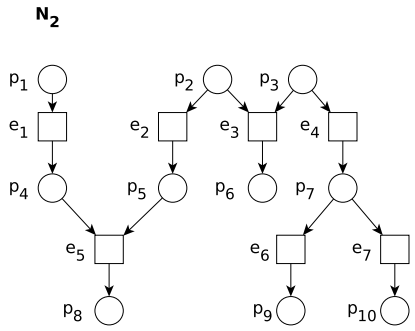

Fig. 2. An occurrence net.

reveals relations will be used to detect positive information flow, however they can also be applied in other areas, e.g. fault diagnosis as explored in [8] by using original reveals relation on occurrence nets. In the following three definitions we assume progress in the behavior of the nets, which means that a constantly enabled transition occurs if it is not disabled by another transition. This means that we consider only maximal runs in the unfolding.

Definition 4. *Let* $N = (P, T, F, m_0)$ *be a Petri net and* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ *be its unfolding,* Ω *be the set of all its maximal runs. Let* $t_1, t_2 \in T$ *be two transitions, we say* t_1 excludes t_2*, denoted* $t_1 \underline{ex}\, t_2$*, iff* $\forall \omega \in \Omega \;\; E_{t_1} \cap \omega \neq \emptyset \implies E_{t_2} \cap \omega = \emptyset$*, i.e., they never appear in the same run.*

It is easy to see that excludes is a symmetric relation and it is not transitive as well as obviously not reflexive.

In the case of Petri nets whose underlying net is an acyclic graph, if two transitions are in conflict, i.e., they are both enabled and the firing of one disables the other one, then one excludes the other. However, in general, transitions which are in conflict can still appear in the same maximal run and therefore they could be in not-excludes relation.

Example 2. The transitions t_2 and t_4 of N_1 in Fig. 1 are in conflict whereas $\neg(t_2 \,\underline{\mathrm{ex}}\, t_4)$. In the unfolding in the same figure, it is possible to see a maximal run including occurrences of both.

$t_5 \,\underline{\mathrm{ex}}\, t_4$ although they are not in conflict.

$t_7 \,\underline{\mathrm{ex}}\, t_5$, $t_5 \,\underline{\mathrm{ex}}\, t_1$ but $\neg(t_7 \,\underline{\mathrm{ex}}\, t_1)$, indeed the relation is not transitive.

Definition 5. *Let* $N = (P, T, F, m_0)$ *be a Petri net, and* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$*, be the unfolding of* N*. Let* Ω *be the set of all maximal runs of* N*. Let* $t_1, t_2 \in T$ *be two transitions, we say that* t_1 reveals t_2*, denoted* $t_1 \rhd_{tr} t_2$*, iff* $\forall\, \omega \in \Omega \;\; E_{t_1} \cap \omega \neq \emptyset \implies E_{t_2} \cap \omega \neq \emptyset$*.*

We say transition t_1 reveals transition t_2 if and only if each maximal run which contains an occurrence of t_1 also contains at least one occurrence of t_2. This

means that for each observation of t_1, t_2 has been already observed or will be observed.

Remark 1. The reveals relation on transitions is *reflexive* and *transitive*, i.e., let $N = (P, T, F, m_0)$ be a Petri net, $t_1, t_2, t_3 \in T$, then $t_1 \rhd_{tr} t_1$, and $(t_1 \rhd_{tr} t_2 \ \wedge \ t_2 \rhd_{tr} t_3) \implies t_1 \rhd_{tr} t_3$.

Example 3. In the net N_1, in Fig. 1, t_3 reveals both t_2 and t_1. It is easy to notice that to be able to fire t_3 we must first fire t_1 and t_2. In fact, in the unfolding, $\mathrm{Unf}(N_1)$, given in Fig. 1, for each occurrence of t_3 there is at least one occurrence of t_2 and similarly, for each occurrence of t_3 there is at least one occurrence of t_1. However, t_1 does not reveal t_2 or t_3, since there is a run in which t_1 occurs and neither t_2 nor t_3 occurs. If an observer, who knows the structure of N_1, can only observe t_1 he cannot have information about t_2 or t_3, however if he is able to observe t_3, he can deduce that t_2 and t_1 must have occurred.

Transition t_1 also reveals transition t_6 because when t_1 fires, t_5 cannot fire anymore and, since the net progresses, t_6 must fire. Since we do not assume strong fairness, $t_1 \not\rhd_{tr} t_4$, after the occurrence of t_1, t_2 and t_3 can loop forever. Reveals relation is not only about past occurrences but also about future occurrences. Observing t_1 does not tell us when t_6 fires. It might have fired already or it will fire in the future. $t_1 \rhd_{tr} t_6$ tells us that when t_1 occurs, an occurrence of t_6 is inevitable.

Remark 2. Reveals relation is neither symmetric nor antisymmetric. For example, in Fig. 1, $t_2 \rhd_{tr} t_3$ and $t_3 \rhd_{tr} t_2$, however $t_2 \rhd_{tr} t_1$ and $t_1 \not\rhd_{tr} t_2$.

In some cases, one transition alone does not give much information about the behavior of the net whereas a set of transitions together can give some information about the behavior of the net. This relation is defined as in the following.

Definition 6. *Let $N = (P, T, F, m_0)$ be a Petri net,* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ *be its unfolding and Ω be the set of all maximal runs. Let $W, Z \subseteq T$ and W* extended-reveals *Z, denoted $W \twoheadrightarrow_{tr} Z$, iff $\forall\, \omega \in \Omega$*

$$\bigwedge_{t \in W} (\omega \cap E_t \neq \emptyset) \implies \bigvee_{t \in Z} (\omega \cap E_t \neq \emptyset)$$

We say that a set of transitions W extended-reveals another set of transitions Z, if and only if each maximal run, which contains at least an occurrence of each transition in W, also contains at least an occurrence of a transition in Z.

The reveals relation on transitions, $t_1 \rhd_{tr} t_2$, corresponds to the extended-reveals relation between singletons, $\{t_1\} \twoheadrightarrow_{tr} \{t_2\}$.

Example 4. In the net shown in Fig. 3, t_2 alone does not reveal t_5, whereas t_2 and t_3 together tell us that t_5 will fire, denoted as $\{t_2, t_3\} \twoheadrightarrow_{tr} \{t_5\}$. In the same net, the occurrence of t_5 tells us that either t_8 or t_9 will fire, denoted as $\{t_5\} \twoheadrightarrow_{tr} \{t_8, t_9\}$. Similarly, $\{t_7, t_8\} \twoheadrightarrow_{tr} \{t_{10}\}$, i.e., there is no maximal run which includes occurrences of t_7, t_8 and not t_{10}.

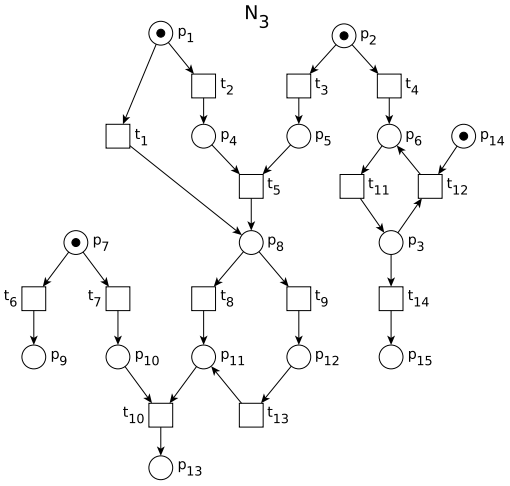

Fig. 3.

In some cases, repeated occurrences of the same transition can give more information about the behavior of a net than only one occurrence of that transition. A relation based on this fact is defined in the following.

Definition 7. *Let $N = (P, T, F, m_0)$ be a Petri net,* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ *be its unfolding and R be the set of all runs. Let $t_1, t_2 \in T$ be two transitions of N, and n be a positive integer. Let $R^n_{t_i} = \{\omega \in R : |\omega \cap E_{t_i}| = n\}$ and $\Omega^n_{t_i}$ denotes the set of maximal runs in $R^n_{t_i}$ with respect to set inclusion (i.e., $\Omega^n_{t_i} \subseteq R^n_{t_i}$ such that if $u, v \in \Omega^n_{t_i} \wedge u \subseteq v$ then $u = v$).*

*If $\Omega^n_{t_1} \neq \emptyset$ then t_1 n-*repeated reveals *t_2, denoted $t_1\ Re^n_{\rhd_{tr}}\ t_2$, iff $\forall \omega \in \Omega^n_{t_1}\ E_{t_2} \cap \omega \neq \emptyset$.*

If $\Omega^n_{t_1} = \emptyset$ then $t_1\ Re^n_{\rhd_{tr}}\ t_2$ is not defined.

Notation. $t_1\ Re^n_{\not\rhd_{tr}}\ t_2$ will denote that there is at least one run in $\Omega^n_{t_1}$ such that t_1 appears n times and t_2 does not appear. $\neg(t_1\ Re^n_{\rhd_{tr}}\ t_2)$ will denote that either $t_1\ Re^n_{\rhd_{tr}}\ t_2$ is not defined, or $t_1\ Re^n_{\not\rhd_{tr}}\ t_2$.

Example 5. Let us consider N_3 in Fig. 3. Transition t_{11} does not reveal t_{12}, however if the occurrence of t_{11} is observed twice then it is evident that t_{12} occurred, therefore t_{11} 2-Repeated reveals t_{12}, denoted $t_{11}\ Re^2_{\rhd_{tr}}\ t_{12}$, whereas $t_{11}\ Re^1_{\not\rhd_{tr}}\ t_{12}$ since after the first occurrence of t_{11}, t_{14} can fire instead of t_{12}.

Note that $t_{11}\ Re^3_{\rhd_{tr}}\ t_{12}$ and $t_{11}\ Re^3_{\not\rhd_{tr}}\ t_{12}$ are both not defined since t_{11} can fire at most twice, therefore in this case $\neg(t_{11}\ Re^3_{\rhd_{tr}}\ t_{12})$.

Proposition 1. *Let $N = (P, T, F, m_0)$ be a Petri net,* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ *its unfolding and R be the set of all runs. Let $t_1, t_2 \in T$ be two transitions of N,*

$$t_1\ Re^1_{\rhd_{tr}}\ t_2 \implies t_1\ \rhd_{tr}\ t_2$$

Proof. Let $R^1_{t_1} = \{\omega \in R : \ |\omega \cap E_{t_1}| = 1\}$ and $\Omega^1_{t_1}$ be the set of maximal runs in $R^1_{t_1}$. If $t_1 \ Re^1_{\rhd_{tr}} \ t_2$, then $\Omega^1_{t_1} \neq \emptyset$ and $\forall \omega \in \Omega^1_{t_1} \ \omega \cap E_{t_2} \neq \emptyset$. Let σ be an arbitrary maximal run of $\mathrm{Unf}(N)$. Suppose that $\sigma \cap E_{t_1} \neq \emptyset$ then we can always take a run $\omega \in \Omega^1_{t_1}$ such that $\omega \subseteq \sigma$. Then we know that σ contains at least one occurrence of t_2 and so $t_1 \rhd_{tr} t_2$. □

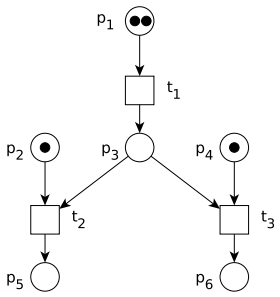

Fig. 4.

However, the implication of the previous proposition does not hold in the other direction. In fact, consider the net in Fig. 4, $t_1 \rhd_{tr} t_2$, $t_1 \rhd_{tr} t_3$, $t_1 \ Re^1_{\not\rhd_{tr}} \ t_2$ and $t_1 \ Re^1_{\not\rhd_{tr}} \ t_3$. The main difference is that we consider only maximal runs for reveals relation. For this net there is only one maximal run which contains t_1 (twice), t_2 and t_3. However, there is a run in $\Omega^1_{t_1}$ in which t_1 appears and t_2 does not appear, as well as a run in which t_1 appears and t_3 does not appear. All runs in $\Omega^2_{t_1}$, i.e., including t_1 twice, contain both t_2 and t_3, i.e., $t_1 \ Re^2_{\rhd_{tr}} \ t_2$ and $t_1 \ Re^2_{\rhd_{tr}} \ t_3$.

Proposition 2. *Let $N = (P, T, F, m_0)$ be a Petri net,* $\mathrm{Unf}(N) = ((B, E, F), \lambda)$ *be its unfolding and R be the set of all runs. Let $t_1, t_2 \in T$ be two transitions, if $t_1 \ Re^n_{\rhd_{tr}} \ t_2$ and $\Omega^{n+1}_{t_1} \neq \emptyset$ then $t_1 \ Re^{n+1}_{\rhd_{tr}} \ t_2$.*

Proof. Let $R^n_{t_1} = \{\omega \in R : \ |\omega \cap E_{t_1}| = n\}$ and $\Omega^n_{t_1}$ be the set of maximal runs in $R^n_{t_1}$. If $t_1 \ Re^n_{\rhd_{tr}} \ t_2$, then $\Omega^n_{t_1} \neq \emptyset$ and $\forall \omega \in \Omega^n_{t_1} \ \omega \cap E_{t_2} \neq \emptyset$. Let $\sigma \in \Omega^{n+1}_{t_1}$, we can always choose a run $\omega \in \Omega^n_{t_1}$ such that $\omega \subseteq \sigma$. Then we know that $\sigma \cap E_{t_2} \neq \emptyset$, so $t_1 \ Re^{n+1}_{\rhd_{tr}} \ t_2$. □

4 Non-interference

In this section, before introducing the new notions, we briefly recall the most used non-interference notions in the literature and discuss our motivation for introducing new non-interference notions based on reveals and excludes relations.

The notions recalled in the following are based on some notion of low observability of a system. It is what can be observed of a system from the point of view of low users.

There are mainly two kinds of information flows that non-interference notions deal with. These are *positive information flow* and *negative information flow*. A positive information flow arises when the occurrence of a high level transition can be deduced from the low level behavior of the system, whereas a negative information flow is concerned with the non-occurrences of a high transition.

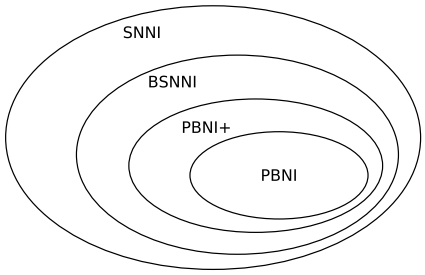

Fig. 5. Relation between some existing interference notions in the literature. *SNNI*≡*NDC*, *BSNNI* ⊆*SNNI*, *SBNDC* ≡ *BNDC* ≡ *PBNI+* ⊆ *BSNNI*, *PBNI*⊆*PBNI+* (see [7])

In the following, we will use acronyms to denote the set of nets satisfying the corresponding security notion.

The less restrictive notion, introduced in [6, 3] and also studied on 1-safe Petri nets in [7], is *Strong Nondeterministic Non-Interference (SNNI)*. It is a trace-based property (trace as sequence of event occurrences), that intuitively says that a system is secure if what the low part can see does not depend on what the high level part does. If a net system N is *SNNI* secure, then it should offer, from the low point of view, the same traces as the system where the high level transitions are prevented. In *SNNI* secure systems, information can flow from low to high but not from high to low. A different characterization of the same notion, called *Non-Deducibility on Composition (NDC)*, is given in [7].

While *SNNI* is based on trace equivalence, the more restrictive notions *Bisimulation based Strong Nondeterministic Non-Interference (BSNNI)* and *Bisimulation based Non-Deducible on Composition (BNDC)* are based on bisimulation.

Strong Bisimulation based Non-Deducible on Composition (SBNDC) is an alternative characterization of *BNDC* [6, 3]. In fact, Busi and Gorrieri in [7] show that *BNDC* is equivalent to *SBNDC*, and it is stronger than *BSNNI*.

Another non-interference notion called *Place Based Non-Interference (PBNI)* was introduced in [7]. It is based on the absence of some kinds of specific places in the net, namely causal and conflict places. A causal place is a place between a low transition and a high transition such that the low transition consumes the token from the place which was produced by the high transition. A conflict place is a place such that at least one low transition and one high transition consume a token from it. A net is considered to be *PBNI* secure in the absence of such

places. In [7], it is shown that if a net is *PBNI* secure then it is also *SBNDC* secure.

In [12], a similar notion, called *Positive Place Based Non-Interference (PBNI+)*, is proposed by introducing the notions of active causal and active conflict places. *PBNI+* is weaker than *PBNI* and it coincides with *SBNDC*.

The overall relationship between these mentioned notions is illustrated in Fig. 5. In the rest of the paper, we will refer only to the notions which are illustrated in the figure since the others are equivalent to those.

With respect to the above mentioned different kinds of information flow, *SNNI*, *BSNNI* and *PBNI+* deal with positive information flow, whereas *PBNI* deals also with negative information flow.

All these notions seem to aim mainly at deducing past occurrences of high transitions, for example they all consider system N_6 in Fig. 7 secure, whereas, by considering progress, after the occurrence of l, a low user deduces h is inevitable and therefore N_6 is not secure with respect to the ability of deducing information about the future behavior.

Differently from the previous notions, the ones we are going to propose do not only capture information flow about past occurrences of high transitions, but also information flow about inevitable or impossible future occurrences of high transitions.

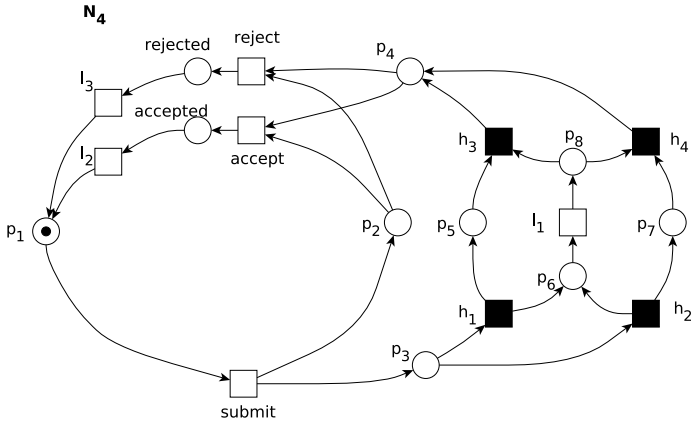

Fig. 6. A net modeling paper submission and evaluation.

In some cases, the mere ability to deduce that some high transition has occurred is not a security threat, provided the low user cannot know which one occurred.

Let us illustrate this issue with the help of an example. The net in Fig. 6 represents a system in which a user can repeatedly submit a paper to a committee, each time receiving a judgment (accept or reject). The black squares represent

high transitions. The review process can follow either of two paths, and we do not want the user to know which one was chosen. When the user receives an answer, he knows that some high transition occurred, however he cannot infer which one.

For this reason, the new notions we are going to introduce in the following will consider such a system secure, whereas it is not secure with respect to *SNNI*, and the other above recalled notions.

In the sequel, the set of high transitions will be denoted by H and the set of low transitions will be denoted by L.

4.1 Non-Interference Based on Reveals

Reveals-based Non-Interference accepts a net as secure if no low transition reveals any high transition.

Definition 8. *Let $N = (P, T, F, m_0)$ be a Petri net, $T = H \cup L$, $H \cap L = \emptyset$, $L, H \neq \emptyset$. N is secure with respect to* Reveals-based Non-Interference (RNI) *iff* $\forall l \in L\ \forall h \in H\colon l \not\rhd_{tr} h$.

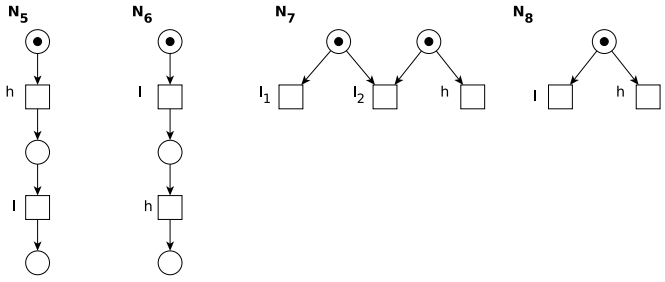

Fig. 7.

Example 6. N_4 in Fig. 6 is *RNI* secure. N_5 and N_6 in Fig. 7 are not secure with respect to *RNI*, since in both nets a low transition reveals a high transition, i.e., $l \rhd_{tr} h$. An observer who knows the structure of the net can deduce that h has already fired in N_5 by observing l. For N_6, again by observing l, he can deduce that h will fire. N_7 in Fig. 7 is also not secure in this context because the observation of l_1 tells the observer that h has already fired or will fire since l_2 cannot fire anymore.

With *RNI*, we are able to capture positive information flow. Moreover, we not only capture past occurrences of high transitions but also future occurrences, and this is because of the progress assumption.

Although it is useful to capture positive information flow, *RNI* is not able to capture the negative information flow. N_8 in Fig. 7 is considered to be secure with respect to *RNI* since it cannot capture the flow between h and l. However, an observer could deduce that h has not fired and will not fire in the future by observing the occurrence of l. In Section 4.4 we will introduce a notion which deals with this kind of information flow.

4.2 Non-Interference Based on Extended-Reveals

As explained in Section 3, in some cases, a transition does not tell much about the behavior of the net, whereas a set of transitions together gives some more information. Extended-reveals deals with this relation between transitions of a Petri net. We propose to use this relation in order to define a new non-interference notion in which the occurrences of a set of low transition together give information about some high transitions.

Definition 9. *Let* $N = (P, T, F, m_0)$ *be a Petri net,* $T = H \cup L$, $H \cap L = \emptyset$, $L, H \neq \emptyset$, $|L| \geq k \geq 1$. N *is secure with respect to* k-Extended-Reveals based Non-Interference (k-ERNI) *iff* $\forall\{l_1, ..., l_k\} \subseteq L \ \forall h \in H$, $\{l_1, ..., l_k\} \not\rightarrowtriangle_{tr} \{h\}$.

N *is* ERNI *secure if it satisfies the above condition for* $k = |L|$.

Intuitively, we say that a net is *k-ERNI* secure, if an attacker is not able to deduce information about the hidden part of the net by observing occurrences of k low level transitions. If a net is *k-ERNI* secure then it is secure with respect to all *n-ERNI* where $1 \leq n \leq k$.

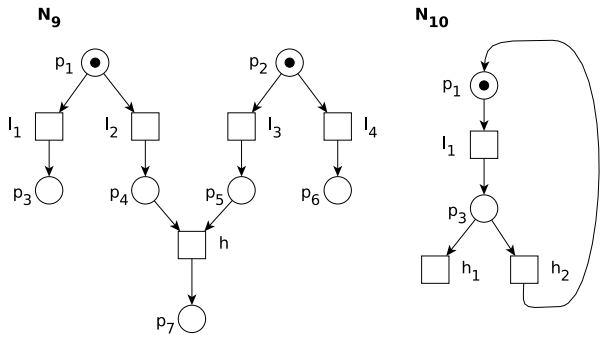

Fig. 8.

Example 7. N_9 in Fig. 8 is not secure with respect to *2-ERNI*. When l_2 and l_3 occur, a low level observer can deduce that h will occur, i.e., $\{l_2, l_3\} \rightarrowtriangle_{tr} \{h\}$. In this net, the occurrence of only one low transition does not give sufficient

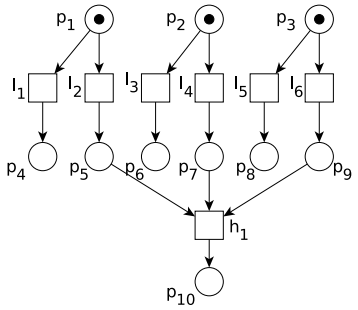

Fig. 9.

information about any high transitions, whereas the occurrence of two low level transitions together does. In the net in Fig. 9, no low transition alone reveals a high transition as well as no pair of low level transitions reveals a high transition. However, $\{l_2, l_4, l_6\} \twoheadrightarrow_{tr} \{h_1\}$, i.e., a low user, observing that all these three transitions occurred, can deduce that h_1 will inevitably occur. Thus, this net is 2-*ERNI* secure whereas it is not 3-*ERNI* secure.

Obviously, 1-*ERNI* coincides with *RNI*, where no low transition alone reveals a high transition. Moreover, k-*ERNI* $\subseteq$ *RNI*, for $k \geq 1$. N_9 is *RNI* secure since none of the low transitions reveals a high transition alone.

4.3 Non-Interference Based on Repeated-Reveals

Another case can be the one in which an attacker is not able to deduce information by observing low transitions and this is because only repeated occurrence of a low transition gives information about the hidden part of the net. Thus, we assume that the attacker can count the occurrences of low transitions and so he can deduce information about the high transitions.

Definition 10. *Let* $N = (P, T, F, m_0)$ *be a Petri net,* $T = H \cup L$, $H \cap L = \emptyset$, $L, H \neq \emptyset$. *Let* $\mathrm{Unf}(N)$ *be the unfolding of* N, *where* $\mathrm{Unf}(N) = ((B, E, F, c_0), \lambda)$, $\lambda : B \cup E \to P \cup T$. *Let* $n > 0$.

N *is secure with respect to* n-Repeated-Reveals based Non-Interference (n-ReRNI) *iff* $\forall l \in L \ \ \forall h \in H \ \ \forall m \leq n \ \ \neg(l \ Re^{m}_{\triangleright_{tr}} \ h)$.

N *is* ReRNI, *iff it is* n-ReRNI *for all* $n > 0$.

Proposition 3. n-ReRNI $\implies$ $(n-1)$-ReRNI

The proof follows from the definition.

Example 8. N_{10} in Fig. 8 is not 2-*ReRNI* secure. Although the first occurrence of l_1 does not reveal a high transition, by observing its second occurrence an observer can deduce that h_2 occurred. However, the net is *RNI* secure as well

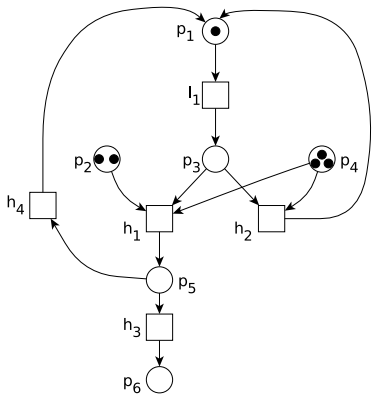

Fig. 10.

as *ERNI* secure. In the net in Fig. 10, an observer cannot infer about the high transitions by observing l_1 occurring only once. Also the second occurrence of l_1 does not tell the observer which high transition occurred or will occur. However, the observer can deduce that h_2 has already occurred or will occur inevitably if he observes three occurrences of l_1. Therefore, this net is 2-*ReRNI* secure but it is not 3-*ReRNI* secure. Note that if the transition h_3 was absent then every maximal run would include at least one occurrence of h_2 and then, even without observing l_1, the occurrence of h_2 would be inevitable.

The following proposition is directly derived from Prop. 1.

Proposition 4. *If a net is* RNI *secure then it is* 1-ReRNI *secure.*

However, the previous implication does not hold in the opposite direction. Consider the net in Fig. 4 and let t_1 be a low transition, t_2 and t_3 be high transitions. This net is 1-*ReRNI* secure since the first occurrence of t_1 does not reveal information about t_2 and t_3, as discussed in Example 5. However the net is not *RNI* secure since $t_1 \rhd_{tr} t_2$ and $t_1 \rhd_{tr} t_3$. Note that this net is not secure with respect to 2-*ReRNI* since the second occurrence of t_1 reveals both t_2 and t_3, i.e. $t_1\ Re^2_{\rhd_{tr}}\ t_2$ and $t_1\ Re^2_{\rhd_{tr}}\ t_3$.

Although k-*ERNI* and n-*ReRNI* are not comparable since they are parametric notions which are based on observing different things (for k-*ERNI* it is observation of occurrences of different low transitions together whereas for n-*ReRNI* it is observation of multiple occurrences of the same low transition) there are nets which are secure with respect to both and which are secure with respect to only one of them.

Both k-*ERNI* and n-*ReRNI* catch positive information flow about the past or future occurrences of high transitions, whereas they allow negative information flow. In the following we will introduce a notion considering both positive and negative information flow.

4.4 Positive/Negative Non-Interference Based on Reveals and Excludes

Until now we explored positive information flow on Petri nets. In order to catch negative information flow which is related to non-occurrence of high transitions, we need to consider the excludes relation between low and high transitions, as introduced in Def. 4.

Definition 11. *Let $N = (P, T, F, m_0)$ be a Petri net, $T = H \cup L$, $H \cap L = \emptyset$, $L, H \neq \emptyset$. N is secure with respect to* Positive/Negative Non-Interference (PNNI) *iff $\forall l \in L\ \forall h \in H$, $l \not\rhd_{tr} h$ and $\neg(l \underline{ex}\ h)$.*

If in a Petri net N, no low transition reveals a high transition and no low transition excludes a high transition, N is considered to be *PNNI* secure. *PNNI* is stronger than *RNI*, i.e., *PNNI* $\subseteq$ *RNI*, and this follows directly from the definitions. In order to be *PNNI* secure, a net has to be *RNI* secure (no low transition reveals a high transition) and to satisfy an additional requirement (no low transition excludes a high transition).

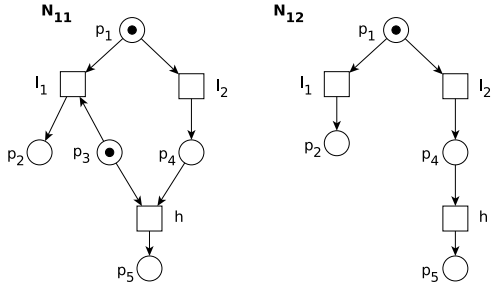

Fig. 11.

Example 9. Both N_{11} and N_{12} in Fig. 11 are not *PNNI* secure since a low transition l_1 excludes a high transition h. Thus, by observing occurrence of l_1, an observer can deduce that h did not occur and will not occur.

N_{13} in Fig. 12 is not secure with respect to *PNNI* because of the negative information flow, i.e., l_2 excludes h_1 as well as it excludes h_2. An observer can deduce that none of the high transitions occurred and they will not occur in the future by observing l_2 or l_3. This net is *RNI*, *ERNI* and *ReRNI* secure.

In the same figure, N_{14} is a *PNNI* secure Petri net. No low transition reveals a high transition as well as no low transition excludes a high transition. However an observer is able to deduce that h_1 will occur inevitably by observing the occurrences of both l_2 and l_3, i.e., $\{l_2, l_3\} \rightarrowtriangle_{tr} \{h_1\}$. In other words, this net is not 2-*ERNI* while it is *RNI* and *ReRNI* secure.

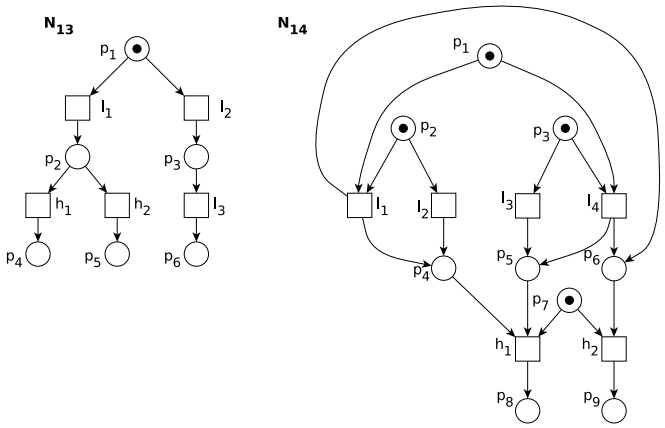

Fig. 12.

As seen in the previous example, *PNNI* is strictly stronger than *RNI*.

PNNI and *k-ERNI* are intersecting for any k, $PNNI \cap k\text{-}ERNI \neq \emptyset$, $PNNI \setminus k\text{-}ERNI \neq \emptyset$, $k\text{-}ERNI \setminus PNNI \neq \emptyset$. None of them is stronger than the other one. The net N_{15} in Fig. 13 is both *ERNI* and *PNNI* secure, whereas N_{16} in Fig. 13 is not *PNNI* secure, however it is *ERNI* secure. N_{14} of Fig. 12 is *PNNI* secure, whereas it is not secure with respect to 2-*ERNI* as it is discussed in example 9.

PNNI and *n-ReRNI* are also intersecting for any n. A net which is both *PNNI* and *ReRNI* secure is the one in Fig. 6. The net in Fig. 10 is not secure with respect to 3-*ReRNI* whereas it is *PNNI* secure. If we add to the net another low transition l_2 which consumes a token from p_5, the net becomes not secure with respect to *PNNI* as well as with respect to *RNI*, since l_2 reveals h_1.

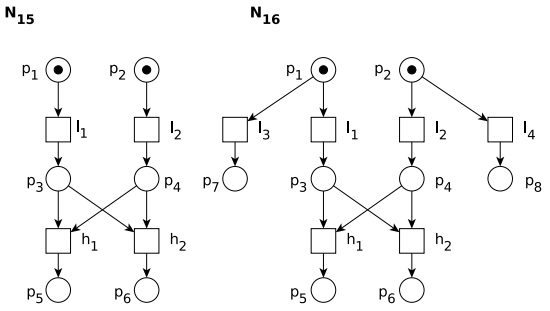

Fig. 13.

5 Comparison of Non-interference Notions

We have introduced new notions of non-interference for Petri nets. These notions are based on the reveals and the excludes relations and on the progress assumption.

One major difference between these notions with the existing ones, recalled in Section 4, is that the new notions explicitly consider the information flow both about the past and the future occurrences of high transitions. For example, if a low user can tell that the occurrence of a high transition is inevitable in the future, such a system is considered to be not secure according to the notions we have here introduced, whereas it is considered secure by the old notions such as *SNNI*, *BSNNI*, *PBNI+* and *PBNI*. Similarly, for the negative information flow, we consider both past and future non-occurrences of high transitions.

Another important difference is shown by N_4 in Fig. 6. This net is not secure according to *SNNI* even if a low user cannot infer which high transitions actually occurred. On the other hand, it is secure with respect to all non-interference notions based on reveals and excludes, since these require the capability of differentiating among the high transitions.

Moreover, the notions recalled in Section 4 are defined for 1-safe Petri nets, whereas *RNI*, *k-ERNI*, *n-ReRNI* and *PNNI* are defined for general Petri nets.

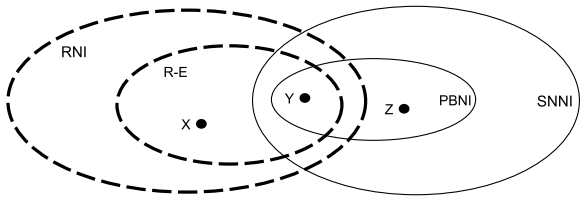

Fig. 14.

Figure 14 illustrates the relation between our notions and the other notions we have discussed so far. For the sake of simplicity, we only consider the weakest (*SNNI*) and the strongest (*PBNI*) notions from the ones recalled in Section 4. with the weakest of the new notions, i.e., *RNI*, and with the intersection set, denoted *R-E* in Fig. 14, of the new notions *RNI*, *k-ERNI*, *n-ReRNI* and *PNNI*.

We will examine three examples to discuss the differences of these classes.

A net which is secure with respect to all notions based on reveals and excludes and which is not secure with respect to *SNNI* is denoted by *X* in Fig. 14 and it is the one in Fig. 6. We consider this net secure since an observer cannot differentiate among the high transitions even if he can know some high actions have been performed (or will be performed). However, this net is not secure with respect to *SNNI*.

The net denoted by Y in Fig. 14 is secure with respect to all non-interference notions based on reveals and excludes as well as with respect to *PBNI*. This net can be N_{15} in Fig. 13. This net is secure since no low transition reveals a high transition (alone or together with another transition) as well as no low transition excludes a high transition. Thus there is neither positive nor negative information flow. It is also secure with respect to *PBNI* due to the fact that there is no active causal or active conflict place.

Two nets which are secure with respect to *PBNI* but not secure with respect to any of the non-interference notions based on reveals and excludes, denoted by Z in Fig. 14, are for example N_6 in Fig. 7 and N_{12} in Fig. 11.

6 Conclusion

In this paper, we have proposed several new notions of non-interference for Petri nets, and compared them with notions already proposed in the literature. In this approach, the transitions of a system net are partitioned into two disjoint sets: the low and the high transitions. A system net is considered *secure*, or *free from interference*, if, from the observation of the occurrence of a low transition, or a set of low transitions, it is not possible to infer information on the occurrence of a high transition. Our new non-interference notions rely on net unfolding and on two relations among transitions. The first one is an adaptation to Petri nets of the *reveals* relation, previously defined on occurrence nets and not yet considered in this context; in particular we have introduced a class of parametrized reveals relations for Petri nets. The second relation is called *excludes* and it has been introduced here with the aim of capturing negative information flow.

The notion of *RNI* states that a net is secure if no low transition reveals any high transition. We have shown that this notion captures some situations which were not captured by the existing notions. We also propose more restrictive notions: *k-ERNI* based on observing occurrences of multiple low transitions and *n-ReRNI* based on the ability of the low user to count the occurrences of a low transition.

By adding the *excludes* relation to the picture, we allow one to infer negative information, namely the fact that a high transition has not occurred and will not occur. This is the basis of *PNNI*. The paper includes a comparison between the notions introduced here and those found in the literature on the subject.

The notions proposed in this paper, and further variants of them, should now be tested on more realistic cases. Our aim is to build a collection of different non-interference properties, so that a system designer, or a system analyzer, can choose those more appropriate to a specific case. A generalization could be a non-interference notion based on a parametric reveals relation between multisets of transitions.

We are currently starting to explore algorithms to check non-interference. In particular, along a similar line to that followed in [13], we are evaluating the use of finite prefixes of the unfoldings of nets.

We are also interested in further investigating the excludes relation and the possibility to apply it in different contexts.

Acknowledgements

This work was partially supported by MIUR and by MIUR - PRIN 2010/2011 grant 'Automi e Linguaggi Formali: Aspetti Matematici e Applicativi', code H41J12000190001.

References

1. Goguen, J.A., Meseguer, J.: Security policies and security models. In: IEEE Symposium on Security and Privacy. (1982) 11–20
2. Ryan, P.Y.A.: Mathematical models of computer security. [14] 1–62
3. Focardi, R., Gorrieri, R.: A taxonomy of security properties for process algebras. Journal of Computer Security **3** (1995) 5–34
4. Roscoe, A.W.: Csp and determinism in security modelling. In: IEEE Symposium on Security and Privacy, IEEE Computer Society (1995) 114–127
5. Ryan, P.Y.A., Schneider, S.A.: Process algebra and non-interference. In: CSFW, IEEE Computer Society (1999) 214–227
6. Focardi, R., Gorrieri, R.: Classification of security properties (part i: Information flow). [14] 331–396
7. Busi, N., Gorrieri, R.: A survey on non-interference with Petri nets. In Desel, J., Reisig, W., Rozenberg, G., eds.: Lectures on Concurrency and Petri Nets. Volume 3098 of Lecture Notes in Computer Science., Springer (2003) 328–344
8. Haar, S.: Unfold and cover: Qualitative diagnosability for Petri nets. In: Proc. 46th IEEE Conference on Decision and Control. (2007)
9. Engelfriet, J.: Branching processes of Petri nets. Acta Inf. **28** (1991) 575–591
10. Balaguer, S., Chatain, T., Haar, S.: Building tight occurrence nets from reveals relations. In Caillaud, B., Carmona, J., Hiraishi, K., eds.: 11th International Conference on Application of Concurrency to System Design, ACSD 2011, Newcastle Upon Tyne, UK, 20-24 June, 2011, IEEE (2011) 44–53
11. Balaguer, S., Chatain, T., Haar, S.: Building occurrence nets from reveals relations. Fundam. Inform. **123** (2013) 245–272
12. Busi, N., Gorrieri, R.: Positive non-interference in elementary and trace nets. In Cortadella, J., Reisig, W., eds.: Applications and Theory of Petri Nets 2004, 25th International Conference, ICATPN 2004, Bologna, Italy, June 21-25, 2004, Proceedings. Volume 3099 of Lecture Notes in Computer Science., Springer (2004) 1–16
13. Baldan, P., Carraro, A.: Non-interference by unfolding. In Ciardo, G., Kindler, E., eds.: Application and Theory of Petri Nets and Concurrency - 35th International Conference, PETRI NETS 2014, Tunis, Tunisia, June 23-27, 2014. Proceedings. Volume 8489 of Lecture Notes in Computer Science., Springer (2014) 190–209
14. Focardi, R., Gorrieri, R., eds.: Foundations of Security Analysis and Design, Tutorial Lectures [revised versions of lectures given during the IFIP WG 1.7 International School on Foundations of Security Analysis and Design, FOSAD 2000, Bertinoro, Italy, September 2000]. In Focardi, R., Gorrieri, R., eds.: FOSAD. Volume 2171 of Lecture Notes in Computer Science., Springer (2001)