On the Decidability of Non Interference over Unbounded Petri Nets

Eike Best
Universität Oldenburg, 26111 Oldenburg, Germany
eike.best@informatik.uni-oldenburg.de

Philippe Darondeau
Inria Rennes - Bretagne Atlantique, Rennes, France
Philippe.Darondeau@inria.fr

Roberto Gorrieri
Dipartimento di Scienze dell'Informazione, Università di Bologna, Bologna, Italy
gorrieri@cs.unibo.it

Non-interference, in transitive or intransitive form, is defined here over unbounded (Place/Transition) Petri nets. The definitions are adaptations of similar, well-accepted definitions introduced earlier in the framework of labelled transition systems [4, 5, 8]. The interpretation of intransitive non-interference which we propose for Petri nets is as follows. A Petri net represents the composition of a controlled and a controller systems, possibly sharing places and transitions. Low transitions represent local actions of the controlled system, high transitions represent local decisions of the controller, and downgrading transitions represent synchronized actions of both components. Intransitive non-interference means the impossibility for the controlled system to follow any local strategy that would force or dodge synchronized actions depending upon the decisions taken by the controller after the last synchronized action. The fact that both language equivalence and bisimulation equivalence are undecidable for unbounded labelled Petri nets might be seen as an indication that non-interference properties based on these equivalences cannot be decided. We prove the opposite, providing results of decidability of non-interference over a representative class of infinite state systems.

1 Introduction

Non-interference has been defined in the literature as an extensional property based on some observational semantics: the high part H (i.e., the secret part) of a system does not interfere with the low part L (i.e., the public part) if whatever is done in H produces *no visible effect* on L. The original notion of non-interference in [6] was defined, using language equivalence, for deterministic automata with outputs. Generalized notions of non-interference were then designed to include (nondeterministic) labelled transition systems and finer notions of observational semantics such as bisimulation (see, e.g., [19,4,20,5,13,21]). Recently, the problem of defining suitable non-interference properties has been attacked also in the classical model of elementary Petri nets, a special class of Petri nets where places can contain at most one token [1,2]. When it is necessary to declassify information (e.g., when a secret plan has to be made public for realization), the two-level approach (secret/public – H/L) is usually extended with one intermediate level of downgrading (D), so that the high actions that have been performed prior to a declassifying action are made public by this declassifying action. This security policy is known under the name of *intransitive* noninterference [18] (*INI* for short) because the information flow relation is considered not transitive: even if information flows from H to D and from D to L are allowed, direct flows from H to L are forbidden. In [8] intransitive non-interference has been defined for elementary net systems.

Submitted to:
Secco 2010

The technical goal of this paper is to show the decidability of intransitive non-interference in the extended framework of unbounded (Place/Transition) Petri nets, and this for both definitions based alternatively on language equivalence or on weak bisimulation equivalence. As both equivalences are undecidable for unbounded labelled Petri nets [9] [11], the decidability of intransitive non-interference is not a trivial result. This is however not the first result of this type for infinite-state systems. It was actually shown in [3] that Strong Low Bisimulation and Strong Security which is based on the latter equivalence can be decided for *Parallel While Programs* defined over expressions from decidable first order theories. Decidability is also established in [3] for Strong Dynamic Security that takes both downgrading and upgrading into account. In that work, decidability comes for a large part from the property of Strong Low Bisimulation to envisage implicitly through its recursive definition all possible modifications of the dynamic store by a concurrent context (without any effective definition). In our work, decidability comes also for a large part from the fact that our basic security properties are *NDC* (*NonDeducibility on Composition*) and its bisimulation version *BNDC* [4, 5], hence we envisage implicitly arbitrary concurrent contexts defined by Petri nets with high-level transitions. Now, the results presented in [3] concern language based security whereas our results concern discrete event systems security. As a matter of fact, both settings do not compare: on the one hand, owing to the impossibility of testing places for zero, unbounded Place/Transition nets have less computing power than Parallel Write Programs, but on the other hand they have *labeled* transition semantics whereas Parallel Write Programs have *unlabeled* transition semantics.

Let us now explain the meaning of non-interference in the context of systems and control. In the Ramadge and Wonham approach to supervisory control for safety properties of discrete event systems [16, 17], one considers closed loop systems made of a plant (the system under control) and a controller that may share actions but have disjoint sets of local states. Synchronization on shared actions allows the controller to observe the plant and to disable selected actions of the plant. Actions of the plant may be invisible to the controller, but all actions of the controller are shared with the plant and synchronized. Moreover controllers are deterministic, hence the current state of the controller may be inferred from the past behaviour of the plant. In the present paper, the closed system made of the plant and the controller is modelled by an unbounded Petri net with three levels of transitions L, D and H. A place may count e.g. an unbounded number of clients or goods. Transitions in L represent actions of the plant alone. Transitions in D represent synchronized actions of the plant and the controller. Transitions in H represent actions of the controller alone. Here the controller can check and modify proactively the global state to orient runs towards reaching some set of states or to maximize some profit. Intransitive non-interference means the impossibility for the controlled system, seen as the adversary of the controller, to win by forcing or dodging synchronized actions that depend upon the decisions taken by the controller after the last synchronized action. An example is given in Section 4.

We are mainly interested in intransitive non-interference. Nevertheless, in a large part of the paper, we shall focus on classical non-interference, in order to establish first the technical results in a simpler framework. In Section 2 we recall the basics of labeled transition systems and Petri nets. Section 3 presents the definitions of classical non-interference notions for PT-nets, and proves that both language equivalence and weak bisimulation equivalence based notions of classical non-interference are decidable. Section 4 presents the definition of intransitive non-interference for PT-nets, introduces examples showing the practical significance of this notion in the context of discrete event systems, and provides decidability results extending the results of Section 3. Section 5 reports some conclusive remarks. A short appendix recalls some results on Petri nets and semi-linear sets used in our proofs.

2 Background

2.1 Transition systems and bisimulations

Definition 2.1 (LTS)**.** *A* labeled transition system *over a set of* labels Σ *is a tuple* $\mathscr{T} = (Q, T, q_0)$ *where* Q *is a set of* states, $q_0 \in Q$ *is the initial state, and* $T \subseteq Q \times \Sigma \times Q$ *is a set of* labeled transitions. *An LTS is said to be* deterministic *if* $(q, \sigma, q') \in T$ *and* $(q, \sigma, q'') \in T$ *entail* $q' = q''$.

Definition 2.2 (LTS under partial observation)**.** *A partially observed LTS is an LTS* $\mathscr{T} = (Q, T, q_0)$ *over a set of labels* Σ *which is partitioned into* observable *labels* $\sigma \in \Sigma_o$ *(for convenience, we assume that* $\varepsilon \notin \Sigma_o$*) and* unobservable *labels* $\tau \in \Sigma_{uo}$. *In a partially observed LTS,* $q \rightarrow^* q'$ *denotes the least binary relation on states such that* $q \rightarrow^* q$ *for all* $q \in Q$, $q \rightarrow^* q'$ *for all* $(q, \tau, q') \in T$ *with* $\tau \in \Sigma_{uo}$, *and* $q \rightarrow^* q'$ *whenever* $q \rightarrow^* q''$ *and* $q'' \rightarrow^* q'$ *for some* q''.

Definition 2.3 (Language equivalence)**.** *The* language *of a partially observed LTS is the set of all finite words* $\sigma_1\sigma_2\ldots\sigma_n$ *(including* ε *which corresponds to* $n = 0$*) such that* $q_0 \rightarrow^* q_1 \xrightarrow{\sigma_1} q'_1 \rightarrow^* q_2 \xrightarrow{\sigma_2} q'_2 \ldots \rightarrow^* q_n \xrightarrow{\sigma_n} q'_n$ *for some adequate sequence of states* q_i *and* q'_i. *Two partially observed LTS's* $\mathscr{T}$ *and* $\mathscr{T}'$ *are* language equivalent *(in notation,* $\mathscr{T} \sim \mathscr{T}'$*) if they have the same language.*

Definition 2.4 (Weak simulation)**.** *Given a set of labels* $\Sigma = \Sigma_o \cup \Sigma_{uo}$ *and two partially observed LTS's* $\mathscr{T}$ *and* $\mathscr{T}'$ *over* Σ, $\mathscr{T}$ *is* weakly simulated *by* $\mathscr{T}'$ *(or* $\mathscr{T}'$ *weakly simulates* $\mathscr{T}$*) if there exists a binary relation* $R \subseteq Q \times Q'$, *called a* weak simulation, *such that* $(q_0, q'_0) \in R$ *and the following requirements are satisfied for all* $(q_1, q'_1) \in R$, *and for all* $\sigma \in \Sigma_o$ *and* $\tau \in \Sigma_{uo}$*:*

- *if* $q_1 \xrightarrow{\sigma} q_2$ *then* $(\exists q'_2) : (q_2, q'_2) \in R$ *and* $q'_1 \rightarrow^* q''_1 \xrightarrow{\sigma} q''_2 \rightarrow^* q'_2$,
- *if* $(q_1, \tau, q_2) \in T$ *then* $(\exists q'_2) : (q_2, q'_2) \in R$ *and* $q'_1 \rightarrow^* q'_2$.

If $\mathscr{T}$ is simulated by $\mathscr{T}'$, then the language of $\mathscr{T}$ is included in the language of $\mathscr{T}'$.

Definition 2.5 (Weak bisimilarity)**.** *Given a set of labels* $\Sigma = \Sigma_o \cup \Sigma_{uo}$, *two partially observed LTS's* $\mathscr{T} = (Q, T, q_0)$ *and* $\mathscr{T}' = (Q', T', q'_0)$ *over* Σ *are* weakly bisimilar *(in notation,* $\mathscr{T} \approx \mathscr{T}'$*) if and only if there exists some binary relation* $R \subseteq Q \times Q'$, *called a* weak bisimulation, *such that* $(q_0, q'_0) \in R$ *and both* R *and* R^{-1} *are weak simulations.*

If $\mathscr{T}$ and $\mathscr{T}'$ are weakly bisimilar, then they are language equivalent.

2.2 Place/Transition Petri nets

In order to keep the presentation concise, we omit here the basic definition of Petri nets which may be found in an appendix together with some classical decidability results.

Definition 2.6 (PT-net system)**.** *A* PT-net system $\mathscr{N} = (P, T, F, M_0)$ *is a PT-net with an* initial marking M_0. *The* reachability set $RS(\mathscr{N})$ *of* $\mathscr{N}$ *is the set of all markings that may be reached from* M_0 *by sequences of transitions of the net. The* reachability graph $RG(\mathscr{N})$ *of* $\mathscr{N}$ *is the LTS with the set of states* $[M_0\rangle$ *and the initial state* M_0, *where* $[M_0\rangle = RS(\mathscr{N})$ *and there is a transition from* M *to* M' *labeled with* t *iff* $M[t\rangle M'$. *Given* $\mathscr{N} = (P, T, F, M_0)$, *the* underlying net *is* $\mathscr{U}(\mathscr{N}) = (P, T, F)$. *For convenience, we write* $\mathscr{N} = (\mathscr{U}(\mathscr{N}), M_0)$.

Definition 2.7 (Composition of net systems)**.** *Given two PT-net systems* $\mathscr{N}_1 = (P_1, T_1, F_1, M_{1,0})$ *and* $\mathscr{N}_2 = (P_2, T_2, F_2, M_{2,0})$ *such that* $P_1 \cap P_2 = \emptyset$, *their composition* $\mathscr{N}_1 \,|\, \mathscr{N}_2$ *is the PT-net system* (P, T, F, M_0) *where* P *is the union of* P_1 *and* P_2, T *is the union of* T_1 *and* T_2, *and* F *and* M_0 *are the unions of the maps* F_i *and* $M_{i,0}$ *respectively, for* $i = 1, 2$. *Also let* $\mathscr{U}(\mathscr{N}_1) \,|\, \mathscr{U}(\mathscr{N}_2) = \mathscr{U}(\mathscr{N}_1 \,|\, \mathscr{N}_2)$.

Note that synchronisation occurs over those transitions that are shared by the two nets, that is, for a transition t that occurs both in T_1 and T_2, we have that, e.g., $F(p,t) = F_1(p,t)$ if $p \in P_1$, $F(p,t) = F_2(p,t)$ otherwise.

Definition 2.8 (Restriction of a net system)**.** *Given a PT-net system $\mathcal{N} = (P,T,F,M_0)$ and a subset of transitions $T' \subseteq T$, let $\mathcal{N} \setminus T' = (P, T \setminus T', F', M_0)$ where F' is the induced restriction of F on $T \setminus T'$. Also let $\mathscr{U}(\mathcal{N}) \setminus T' = (P, T \setminus T', F')$.*

Definition 2.9 (Labeled net system)**.** *A* labeled net system $(\mathcal{N}, \lambda)$ *is a PT-net system $\mathcal{N} = (P,T,F,M_0)$ with a* transition labelling map $\lambda : T \to \Sigma_o \cup \{\varepsilon\}$ *(the subscript o in Σ_o means an alphabet of observations). The* labeled reachability graph *of $(\mathcal{N}, \lambda)$ is the partially observed LTS over $\Sigma = \Sigma_o \cup \{\varepsilon\}$ which derives from $RG(\mathcal{N})$ by replacing each transition $M[t\rangle M'$ with a corresponding transition $(M, \lambda(t), M')$.*

Definition 2.10 (Weak simulation)**.** *Given two labeled net systems $(\mathcal{N}, \lambda)$ and $(\mathcal{N}', \lambda')$ over the same set of labels Σ_o, $(\mathcal{N}, \lambda)$ is weakly simulated by $(\mathcal{N}', \lambda')$ if the labeled reachability graph of $\mathcal{N}$ is weakly simulated by the labeled reachability graph of $\mathcal{N}'$.*

Definition 2.11 (Equivalences of labeled net systems)**.** *Two labeled net systems $(\mathcal{N}, \lambda)$ and $(\mathcal{N}', \lambda')$ over the same set of labels Σ_o are:*

- language equivalent *(in notation, $(\mathcal{N}, \lambda) \sim (\mathcal{N}', \lambda')$ or for short $\mathcal{N} \sim \mathcal{N}'$ when the labelling maps are clear from the context) if their labeled reachability graphs are language equivalent;*
- weakly bisimilar *(in notation, $(\mathcal{N}, \lambda) \approx (\mathcal{N}', \lambda')$ or for short $\mathcal{N} \approx \mathcal{N}'$ when the labelling maps are clear from the context) if their labeled reachability graphs are weakly bisimilar.*

A weak bisimulation between the labeled reachability graphs of two labeled net systems is called a weak bisimulation between them.

A particular case is with *partially observed net systems*, i.e. when $\Sigma_o = T_o \subseteq T$, $\lambda(t) = t$ for $t \in T_o$, and $\lambda(t) = \varepsilon$ for $t \in T \setminus T_o$. For partially observed net systems, $(\mathcal{N}, \lambda) \sim (\mathcal{N}', \lambda')$ if and only if the reachability graphs of $\mathcal{N}$ and $\mathcal{N}'$, considered as partially observed LTS's with $\Sigma_{uo} = T \setminus T_o$, are language equivalent in the sense of Definition 2.3. In the same conditions, $(\mathcal{N}, \lambda) \approx (\mathcal{N}', \lambda')$ if and only if $RG(\mathcal{N}) \approx RG(\mathcal{N}')$ in the sense of Definition 2.5.

Proposition 2.12. *If λ is the identity, $(\mathcal{N}, \lambda) \approx (\mathcal{N}', \lambda)$ iff $(\mathcal{N}, \lambda) \sim (\mathcal{N}', \lambda)$*

3 Classical non-interference in PT-nets

In this section, we focus on 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 of the system with low-level users. The system has the property of non-interference if the interplay between its low-level part and high-level part cannot affect the low level user's view of the system, even assuming that the low-level user knows the structure of the system. As already said in the introduction, the goal of this section is to provide the technical basis that we need for showing subsequently the decidability of intransitive non-interference for PT-nets, which we feel has more direct interest for applications in the context of discrete event systems. We must therefore postpone the presentation of motivating examples.

Definition 3.1 (Two-level net system)**.** *A two-level PT-net system is a PT-net system $\mathcal{N} = (P,T,F,M_0)$ whose set of transitions T is partitioned into* low level *transitions $l \in L$ and* high level *transitions $h \in H$, such that $T = L \cup H$ and $L \cap H = \emptyset$. A net system $\mathcal{N}$ is a* high-level net system *if all transitions in T are high-level transitions. It is a* low-level net system *if all transitions in T are low-level transitions.*

Henceforth, *two-level net systems are considered as partially observed net systems* where the transitions in L are observable while the transitions in H are unobservable ($\Sigma_o = L$ and $\Sigma_{uo} = H$). This interpretation applies to all instances of the relations $\mathscr{N} \sim \mathscr{N}'$ or $\mathscr{N} \approx \mathscr{N}'$ between two-level net systems. We denote by $\mathscr{L}(\mathscr{N})$ the language of a two-level net system $\mathscr{N}$, that is to say, the set of images $\lambda(t_1 t_2 \ldots t_n)$ of sequences of transitions $M_0[t_1 t_2 \ldots t_n\rangle M$ under the labelling map $\lambda(t) = t$ for $t \in L$ and $\lambda(t) = \varepsilon$ for $t \in H$.

Definition 3.2 (NDC-BNDC)**.** *A* two-level *net system $\mathscr{N}$ has the property NDC (Non-Deducibility on Compositions), resp. BNDC (Bisimulation-Based Non-Deducibility on Compositions), if for any high-level net system $\mathscr{N}'$ with a set of transitions H' not intersecting L, the two-level net systems $\mathscr{N} \setminus H$ and $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$ are language equivalent, resp. weakly bisimilar.*

The definitions of NDC and BNDC are very strong, and their verification is indeed quite demanding: infinitely many equivalence checks are required, one for each choice of a high-level net system $\mathscr{N}'$. Moreover, each equivalence check may be a problem, as both language equivalence and bisimulation equivalence are undecidable over unbounded labeled PT-nets and likewise over unbounded partially observed PT-nets [9, 11]. We shall discuss about the strength of these notions in section 4. For the moment, what we need is an alternative characterization of these properties, more amenable for an algorithmic treatment in view of showing decidability.

3.1 Deciding on NDC

In this section, we show that $\mathscr{N}$ enjoys NDC if and only if $\mathscr{N}$ and $\mathscr{N} \setminus H$ are language equivalent.

Proposition 3.3. *For any high-level net system $\mathscr{N}'$ with set of transitions H' not intersecting L, $\mathscr{N} \setminus H$ is weakly simulated by $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$ which in turn is weakly simulated by $\mathscr{N}$ (where all net systems under consideration have the same set of observable transitions $\Sigma_o = L$).*

Proof. Any transition from L has similar place neighbourhoods in $\mathscr{N} \setminus H$, $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$ and $\mathscr{N}$, and the transitions from L and H' have disjoint place neighbourhoods in $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$. □

Proposition 3.4. *$\mathscr{N}$ has the property NDC iff $\mathscr{N} \sim \mathscr{N} \setminus H$. Moreover, this property can be decided.*

Proof. By definition, $\mathscr{N}$ has the property NDC iff, for any high-level net system $\mathscr{N}'$ with a set of transitions H' not intersecting L, the two-level net systems $\mathscr{N} \setminus H$ and $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$ are language equivalent. Now, the chain of inclusion relations $\mathscr{L}(\mathscr{N} \setminus H) \subseteq \mathscr{L}((\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')) \subseteq \mathscr{L}(\mathscr{N})$ holds for Proposition 3.3. Both bounds are reached for some net system $\mathscr{N}'$; indeed, the lower bound is reached when $\mathscr{N}'$ has no place and $H' = \emptyset$, and the upper bound is reached when $\mathscr{N}'$ has no place and $H' = H$. Suppose $\mathscr{N}$ has the property NDC, then $\mathscr{L}(\mathscr{N} \setminus H) = \mathscr{L}((\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')) = \mathscr{L}(\mathscr{N})$ for $\mathscr{N}'$ realizing the upper bound. Conversely, suppose that $\mathscr{L}(\mathscr{N} \setminus H) = \mathscr{L}(\mathscr{N})$, then necessarily $\mathscr{L}(\mathscr{N} \setminus H) = \mathscr{L}((\mathscr{N} | \mathscr{N}') \setminus (H \setminus H'))$. Hence, the first claim in the proposition has been established. As all transitions are observable in the net system $\mathscr{N} \setminus H$, the language $\mathscr{L}(\mathscr{N} \setminus H)$ is a free Petri net language. By E. Pelz's theorem and corollary (Theorem 6.4 in the appendix), one can decide whether $\mathscr{L}(\mathscr{N}) \subseteq \mathscr{L}(\mathscr{N} \setminus H)$, and hence whether the two languages are equal. □

Example 3.5. *The net system $\mathscr{N}_1$ of Figure 1(a) is insecure, as $\mathscr{N}_1$ can perform the low transition l at some stage, while $\mathscr{N}_1 \setminus H$ cannot. On the contrary, the net system $\mathscr{N}_2$ in Figure 1(b) enjoys NDC.*

Figure 1: Two simple two-level net systems

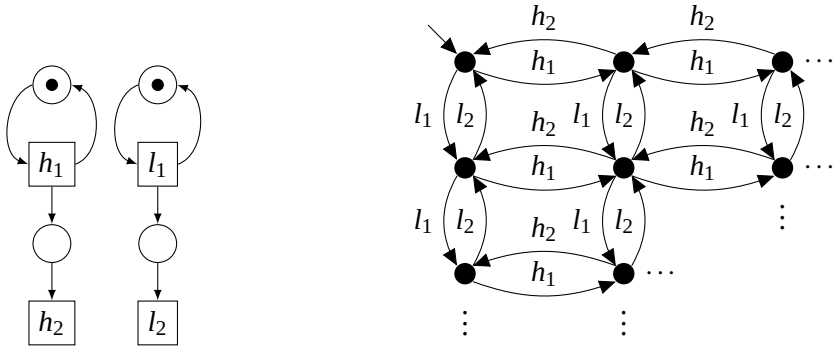

Figure 2: An infinite-state net system (l.h.s.) and its labeled reachability graph (r.h.s.)

Example 3.6. *Consider the disconnected net system $\mathcal{N}$ in Figure 2 (l.h.s.). Intuitively, we expect that this system is secure because the high part of the net (the left part) and the low part of the net (the right part) are disconnected and so it appears that no interference is possible. In view of Definition 3.2, it seems however difficult to verify this property by direct inspection of the infinite labeled reachability graph of $\mathcal{N}$ shown in Figure 2 (r.h.s.). With the help of Proposition 3.4, this verification becomes straightforward: the transition system that generates the language $\mathscr{L}(\mathcal{N} \setminus H)$, which corresponds with the left column of the picture, and the deterministic transition system that generates the language $\mathscr{L}(\mathcal{N})$ (obtained by replacing all labels h_i by ε and then applying the usual subset construction) are indeed identical.*

3.2 Reducing BNDC to SBNDC

For BNDC, things are a bit more complex, although we have the following property.

Lemma 3.7. *If $\mathcal{N}$ has the property BNDC, then $\mathcal{N} \approx \mathcal{N} \setminus H$.*

Proof. Let $\mathcal{N}'$ be the high-level net system with no place and with the set of transitions $H' = H$, then the reachability graphs of $\mathcal{N}$ and $(\mathcal{N} \,|\, \mathcal{N}') \setminus (H \setminus H')$ are isomorphic, hence they are weakly bisimilar, that is $\mathcal{N} \approx (\mathcal{N} \,|\, \mathcal{N}') \setminus (H \setminus H')$. If $\mathcal{N}$ has the property BNDC, then $\mathcal{N} \setminus H \approx (\mathcal{N} \,|\, \mathcal{N}') \setminus (H \setminus H')$, and the lemma follows since $\approx$ is an equivalence. □

Example 3.8. *Consider the net system $\mathcal{N}$ in Figure 3. $\mathcal{N}$ is NDC because $\mathcal{N} \sim \mathcal{N} \setminus H$. However, $\mathcal{N}$ is not BNDC because $\mathcal{N} \not\approx \mathcal{N} \setminus H$. Indeed, this net is insecure: a low-level user who is unable to perform transition l can deduce from this failure that the high-level transition h has been performed.*

In the rest of the section, we show that $\mathcal{N}$ enjoys BNDC if and only if it enjoys the property SBNDC defined below.

Definition 3.9 (SBNDC)**.** *A two-level net system $\mathcal{N}$ has the property SBNDC (Bisimulation-Based Strong Non-Deducibility on Compositions) if, for any reachable marking M_1 of $\mathcal{N} = (N, M_0)$ and for any high-level transition $h \in H$, $M_1[h\rangle M_2$ entails that $(N \setminus H, M_1)$ and $(N \setminus H, M_2)$ are weakly bisimilar.*

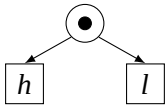

Figure 3: A simple two-level net system

Note that, in view of Proposition 2.12, the relation between M_1 and M_2 required in Definition 3.9 may be equivalently expressed as $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_2)$.

Definition 3.10. *Let $R \subseteq RS(\mathscr{N} \setminus H) \times RS(\mathscr{N})$ be the binary relation on markings which is generated from the axiom $M_0 R M_0$ by the following two inference rules where $h \in H$ and $l \in L$:*

- *$M_1 R M_2$ and $M_1 = M_1'$ and $M_2[h\rangle M_2'$ entail $M_1' R M_2'$*
- *$M_1 R M_2$ and $M_1[l\rangle M_1'$ and $M_2[l\rangle M_2'$ entail $M_1' R M_2'$*

Paraphrasing the definition, MRM' if and only if there exist $w \in L^*$ and $w' \in (L \cup H)^*$ such that $M_0[w\rangle M$, $M_0[w'\rangle M'$, and w is the projection of w' on L^*. In the specific case where $\mathscr{N}$ is BNDC, R is a weak bisimulation between $\mathscr{N} \setminus H$ and $\mathscr{N}$, and it is indeed the *least* weak bisimulation between them.

Lemma 3.11. *Let $\mathscr{N} = (N, M_0)$ be a net system with the BNDC property and let M_1 and M_2 be reachable markings of $\mathscr{N} \setminus H$ and $\mathscr{N}$, respectively. If $M_1 R M_2$, then $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$.*

Proof. As $M_1 R M_2$, there exist $w \in L^*$ and $w' \in (L \cup H)^*$ such that $M_0[w\rangle M_1$, $M_0[w'\rangle M_2$, and w is the projection of w' on L^*. Let $k = |w'| - |w|$ be the difference of length between w' and w. Consider the high-level net system $\mathscr{K} = (K, M_k)$ where K is a net with a unique place p_k, the set of transitions H, and flow relations $F(p_k, h) = 1$ and $F(h, p_k) = 0$ for every transition h, and where $M_k(p_k) = k$. Let M_0' and M_2' be the markings of $N' = \mathscr{U}(\mathscr{N} | \mathscr{K})$, extending M_0 and M_2, respectively, such that $M_0'(p_k) = k$ and $M_2'(p_k) = 0$. By construction, $M_0'[w'\rangle M_2'$ in $\mathscr{N} | \mathscr{K}$. As $\mathscr{N}$ has the property BNDC and $\mathscr{K}$ is a high-level net system, $\mathscr{N} \setminus H \approx (\mathscr{N} | \mathscr{K}) \setminus (H \setminus H) = \mathscr{N} | \mathscr{K}$. As all transitions of $\mathscr{N} \setminus H$ are observable and w is the observable projection of w', M_1 and M_2' are two weakly bisimilar markings of $\mathscr{N} \setminus H$ and $\mathscr{N} | \mathscr{K}$, hence $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N | K, M_2')$. As $M_2'(p_k) = 0$, no transition in H can occur in any sequence fired from M_2' in $N|K$, and therefore $\mathscr{L}(N|K, M_2') = \mathscr{L}(N \setminus H, M_2)$. Altogether, $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$. □

Proposition 3.12. *$\mathscr{N} = (N, M_0)$ has the property BNDC* iff *for all reachable markings M_1 and M_2 of $N \setminus H$ and N, respectively, $M_1 R M_2$ entails $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$.*

Proof. The direct implication has already been established. To show the converse implication, consider any high-level net system $\mathscr{N}'$ with set of transitions H' not intersecting L. Let B be the relation between the reachable markings of $\mathscr{N} \setminus H$ and $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$ defined as follows. Let $(M_2 | M_2')$ denote the marking of $(\mathscr{N} | \mathscr{N}')$ that projects on the markings M_2 and M_2' of $\mathscr{N}$ and $\mathscr{N}'$, respectively. Then, let $M_1 B (M_2 | M_2')$ iff $M_1 R M_2$. Assume that $M_1 R M_2$ entails $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$. We will show that B is a weak bisimulation between $\mathscr{N} \setminus H$ and $(\mathscr{N} | \mathscr{N}') \setminus (H \setminus H')$, entailing that $\mathscr{N}$ has the property BNDC. As $M_1 R M_2$ for $M_1 = M_0$ and $M_2 = M_0$, the relation B holds between the initial states of the two net systems. Now consider any occurrence $M_1 B (M_2 | M_2')$ of the relation B, hence $M_1 R M_2$ (by construction of B).

- Let $M_1[l\rangle \widetilde{M_1}$ for $l \in L$. As $M_1 R M_2$ entails $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$, necessarily, $M_2[l\rangle \widetilde{M_2}$ for some marking $\widetilde{M_2}$, and then by definition of R, $\widetilde{M_1} R \widetilde{M_2}$. Thus, $(M_2 | M_2')[l\rangle (\widetilde{M_2} | M_2')$ with $\widetilde{M_1} B (\widetilde{M_2} | M_2')$.

- Let $(M_2|M_2')[l\rangle(\widetilde{M_2}|M_2')$ for $l \in L$. As $M_1 R M_2$ entails $\mathscr{L}(N \setminus H, M_1) = \mathscr{L}(N \setminus H, M_2)$, necessarily $M_1[l\rangle\widetilde{M_1}$ for some marking $\widetilde{M_1}$ such that $\widetilde{M_1} R \widetilde{M_2}$, hence $M_1 B(\widetilde{M_2}|M_2')$ by definition of B.
- Let $(M_2|M_2')[h\rangle(\widetilde{M_2}|M_2'')$ for $h \in H$, then certainly $M_2[h\rangle\widetilde{M_2}$ in $\mathscr{N}$. Suppose $M_1[h\rangle M_2$, then we have also $M_1 R \widetilde{M_2}$ by definition of R, hence $M_1 B(\widetilde{M_2}|M_2'')$ by definition of B.

Summing up, B is a weak bisimulation and $\mathscr{N}$ has the property BNDC. □

Proposition 3.13. *$\mathscr{N}$ has the property SBNDC iff for any reachable marking M_1 of $\mathscr{N} = (N, M_0)$ and for any high-level transition $h \in H$, $M_1[h\rangle M_2$ entails that $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_2)$.*

Proof. As for $\mathscr{N} \setminus H$ the labelling is the identity $\lambda(l) = l$, the thesis follows by Proposition 2.12. □

Theorem 3.14. *$\mathscr{N}$ has the property BNDC* iff *it has the property SBNDC.*

Proof. Suppose that $\mathscr{N}$ has the property BNDC. Then , by Lemma 3.7, $\mathscr{N} \approx \mathscr{N} \setminus H$, hence $\mathscr{L}(\mathscr{N}) = \mathscr{L}(\mathscr{N} \setminus H)$. Let $M_0[s\rangle M_1$ in $\mathscr{N}$, then necessarily, $M_0[s'\rangle M_1'$ in $\mathscr{N} \setminus H$ for s' defined as the observable projection of s. Thus $M_1' R M_1$ by definition of R. As $M_1[h\rangle M_2$, we have also $M_1' R M_2$. By Proposition 3.12, $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_1') = \mathscr{L}(\mathscr{N} \setminus H, M_2)$, hence $\mathscr{N}$ has the property SBNDC.

Now assume that $\mathscr{N}$ has the property SBNDC. By Proposition 3.12, in order to prove that $\mathscr{N}$ has the property BNDC, it suffices to show that $M_1 R M_2$ entails $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_2)$ for all reachable markings M_1 and M_2 of $\mathscr{N} \setminus H$ and $\mathscr{N}$, respectively. Let M_1 and M_2 be two such markings and assume that $M_1 R M_2$. In view of Definition 3.10, this relation has been derived from the axiom MRM using the two inference rules (where we have exchanged the M_i and the M_i' from Definition 3.10):

- $M_1' R M_2'$ and $M_1' = M_1$ and $M_2'[h\rangle M_2$ entail $M_1 R M_2$
- $M_1' R M_2'$ and $M_1'[l\rangle M_1$ and $M_2'[l\rangle M_2$ entail $M_1 R M_2$

If $M_1 = M_2$, then there is nothing to prove. In the converse case, one can assume by induction on the derivation of $M_1 R M_2$ that $\mathscr{L}(\mathscr{N} \setminus H, M_1') = \mathscr{L}(\mathscr{N} \setminus H, M_2')$. The desired conclusion follows then from Definition 3.9 for the first rule, and from the definition of R and the injective labelling of nets for the second rule. □

Despite the fact that SBNDC requires infinitely many equivalence checks, one for each reachable marking enabling a high-level transition, it (and hence also BNDC) can be decided, as will be seen in the next section.

3.3 Deciding SBNDC

In this section, we reduce SBNDC to the conjunction, for all high-level transitions h and for all low-level transitions l, of a predicate $P(h,l)$ meaning that the enabling or disabling of l in the net after a sequence of low transitions $s \in L^*$ gives no indication on whether h has been fired immediately before s.

Definition 3.15. *Given a two-level net system $\mathscr{N}$ and two transitions $h \in H$ and $l \in L$, we say that $P(h,l)$ holds* iff *for any words $s \in L^*$ and $w \in (L \cup H)^*$, if $M_0[w\rangle M_1$, $M_1[h\rangle M_2$, $M_1[s\rangle M_3$, and $M_2[s\rangle M_4$, then $M_3[l\rangle$ iff $M_4[l\rangle$.*

Figure 4 shows a situation where $P(h,l)$ is *not* satisfied, because l is enabled at M_4 but not at M_3. This corresponds roughly to *causal information flow* [2] from h to l. The other situation in which $P(h,l)$ is not satisfied is the symmetric one, when l is enabled at M_3 but disabled at M_4; this roughly corresponds to *conflict information flow* [2] from h to l.

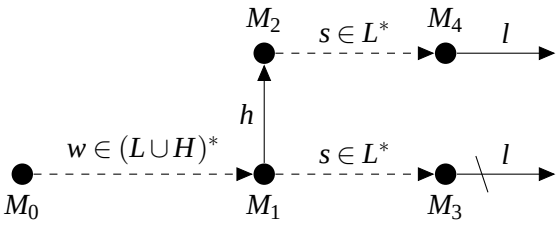

Figure 4: Illustration of Property $P(h,l)$

Proposition 3.16. *$\mathscr{N}$ has the property SBNDC* iff *$P(h,l)$ holds for any high-level action $h \in H$ and for any low-level action $l \in L$.*

Proof. This is a direct consequence of Proposition 3.13. Indeed, $M_1[h\rangle M_2$ and $P(h,l)$ for all l entail $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_2)$, and conversely, $\mathscr{L}(\mathscr{N} \setminus H, M_1) = \mathscr{L}(\mathscr{N} \setminus H, M_2)$ for all transitions $M_1[h\rangle M_2$ entail $P(h,l)$ for all l. □

We will now show that $P(h,l)$ is a decidable property, entailing that one can decide whether a given net system $\mathscr{N}$ has the property SBNDC (because in a finite net, there are finitely many pairs (h,l)).

Proposition 3.17. *$P(h,l)$ is a decidable property.*

Proof. Let a net $\mathscr{N}$ with initial marking M_0 and two fixed transitions $h \in H$ and $l \in L$ be given. Let $\mathscr{N}_1$ be an exact copy of $\mathscr{N}$, with place set P_1, except that it also contains another 'local' copy l'_1 of transition l. Let $\mathscr{N}_2$ be another exact copy of $\mathscr{N}$, with place set P_2 (disjoint from P_1), except that it also contains a local copy l'_2 of transition l and a local copy h' of transition h. Let $\mathscr{N}'$ be defined as $\mathscr{N}_1|\mathscr{N}_2$ plus two further places x and y and the following extension of F':

(a) x is connected to all transitions in H by a side-condition loop.

(b) $F'(x,h') = 1$, $F'(h',y) = 1$, $F'(y,l'_1) = 1$ and $F'(y,l'_2) = 1$.

Finally, let x be initially marked with 1 token and y with 0 tokens. The idea is that $\mathscr{N}'$ contains two components, one simulating the path from M_0 to M_3 in Figure 4, and another one simulating the path from M_0 to M_4, if such paths exist.

It is claimed that $P(h,l)$ holds true in $\mathscr{N}$ if and only if in the net $\mathscr{N}'$ so constructed, it is *not* possible to reach a marking M' such that

$$(M'[l'_1\rangle \wedge \neg M'[l'_2\rangle) \vee (\neg M'[l'_1\rangle \wedge M'[l'_2\rangle). \tag{1}$$

To see ($\Rightarrow$), suppose that $M'_0[v\rangle M'$ where M'_0 is the initial marking of $\mathscr{N}'$ defined above, and where M' satisfies (1). By (b) and because M' enables either l'_1 or l'_2, h' occurs exactly once in v, and neither l'_1 nor l'_2 occur in v. Hence v can be split as $M'_0[v_1h'v_2\rangle M'$ such that v_1 and v_2 contain only transitions of $H \cup L$. By (a), v_2 contains only transitions from L. Because h' does not change the tokens on place set P_1, v_1v_2 is an execution sequence of $\mathscr{N}_1$, whence $M_0[v_1v_2\rangle$ in $\mathscr{N}$. Because h' acts on P_2 exactly as h does, v_1hv_2 is an execution sequence of $\mathscr{N}_2$, whence $M_0[v_1hv_2\rangle$ in $\mathscr{N}$. Because l'_1 and l'_2 act on P_1 and P_2, respectively, as does l, $M'_0[v_1h'v_2l'_1\rangle$ in $\mathscr{N}'$ iff $M_0[v_1v_2l\rangle$ in $\mathscr{N}$ and $M'_0[v_1h'v_2l'_2\rangle$ in $\mathscr{N}'$ iff $M_0[v_1hv_2l\rangle$ in $\mathscr{N}$. Because M' satisfies (1), this means that $P(h,l)$ is false in $\mathscr{N}$. More precisely, referring to Definition 3.15, putting $w = v_1$ and $s = v_2$ yields $M_0[ws\rangle M_3$ and $M_0[whs\rangle M_4$ with $\neg(M_3[l\rangle \Leftrightarrow M_4[l\rangle)$ in $\mathscr{N}$.

This argument can easily be reversed in order to prove ($\Leftarrow$).

The proof is finished because by Corollary 6.8, it is decidable whether or not a marking satisfying (1) is reachable in $\mathcal{N}'$. □

Corollary 3.18. *SBNDC is decidable for finite PT-nets.*

Corollary 3.19. *BNDC is decidable for finite PT-nets.*

Figures 5 and 6 show an example for the construction in the preceding proof. In Figure 5, which depicts the net $\mathcal{N}$ with $H = \{h\}$ and $L = \{k, l\}$ on its left-hand side, we have

$$M_0[k\rangle M_3 \text{ with } \neg M_3[l\rangle \text{ and } M_0[hk\rangle M_4 \text{ with } M_4[l\rangle,$$

that is, $P(h,l)$ is violated in $\mathcal{N}$. In Figure 6, which depicts the net $\mathcal{N}'$ resulting from the construction in the proof, we have

$$M_0'[h'k\rangle M' \text{ with } \neg M'[l_1'\rangle \text{ and } M'[l_2'\rangle,$$

that is, we find a reachable marking M' satisfying (1).

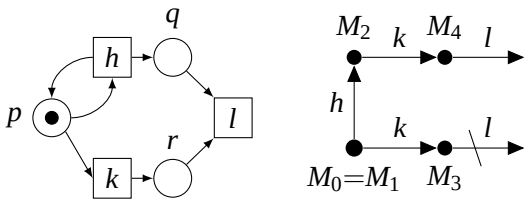

Figure 5: A system $\mathcal{N}$ violating $P(h,l)$

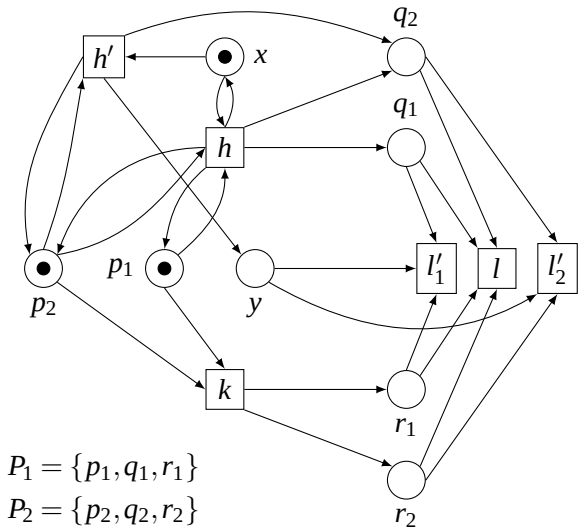

Figure 6: A system $\mathcal{N}'$ satisfying (1) for some M'

4 Intransitive non-interference

We enter now a less technical part of the paper, where we try to show how the decision results established in Section 3 may be applied to check quality of control in the framework of discrete event systems. As it would be difficult to present applications to real systems, we shall consider toy examples which we hope will at least make the intuitions clear.

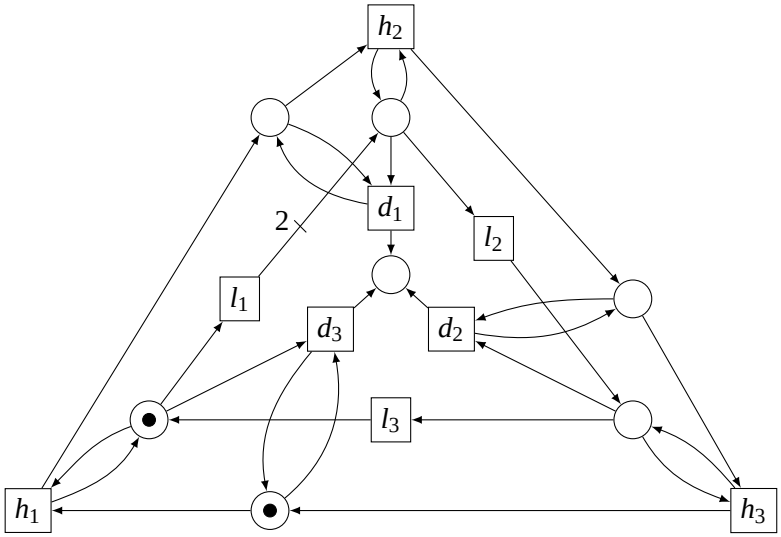

Figure 7: A three-level net system

Our first example is the net system shown in Figure 7. This net is composed of two directed rings interconnected by bidirectional arcs plus a sink place (in the center) fed by three transitions connected to both rings. Each arc from a place p to a transition t means a flow $F(p,t) = 1$. Each arc from a transition t to a place p means a flow $F(t,p) = 1$, except for the arc from l_1 labeled with 2, meaning that $F(l_1,p) = 2$ for the target place p. The internal ring formed with the low-level transitions l_1, l_2, l_3 represents a flock of prey that travel clockwise from place to place, and split each time they go through l_1. The external ring formed with the high-level transitions h_1, h_2, h_3 represents an observer that also travels clockwise and watches the prey but moves only if some prey has been detected in the location currently observed. The three (downgrading) transitions d_1, d_2, d_3 represent the actions of a predator that receives delayed notification of the presence of prey from the observer, and therefore anticipates their possible moves by one position. The objective of the observer and predator is of course to catch prey. The transitions l_1, l_2, l_3 are scheduled by a guardian that pursues the opposite objective. Whenever a prey is caught, this has direct effect on the set of the possible schedules in $\{l_1, l_2, l_3\}^*$, hence there exist interferences between d_1, d_2, d_3 and l_1, l_2, l_3. If the set of possible schedules in $\{l_1, l_2, l_3\}^*$ was directly affected by the transitions in h_1, h_2, h_3, the guardian could glean information on the position of the observer and therefore drive the prey to safe locations. This is actually not the case, because the high-level transitions do not affect the contents of the places connected to the low-level transitions. The fact that each d_i transition reveals that the last transition of the observer was the corresponding h_i makes no problem since the prey has already been caught. This is the essence of downgrading transitions and intransitive non-interference in PT-nets, whose definitions follow.

Definition 4.1 (Three-level net system)**.** *A* three-level *PT-net system is a PT-net system* $\mathcal{N} = (P, T, F, M_0)$

whose set T of transitions is partitioned into low level *transitions $l \in L$,* downgrading *transitions $d \in D$, and* high level *transitions $h \in H$, such that $T = L \cup D \cup H$ and the sets L, D and H do not intersect.*

The low-level transitions are supposed to be observed by the low user, while the high-level transitions cannot be observed and should hopefully be kept *secret*, i.e. they should not be revealed to the low user by the observation of the firing sequences in which they occur. The downgrading transitions may be observed by the low user, but when such a transition occurs, the requirement that all high-level transitions that possibly occurred before should be kept secret is cancelled. This is a strong form of declassification, but we do not know at present about the decidability of INI or BINI for more flexible forms of declassification, where each transition $d \in D$ would declassify a corresponding subset H_d of H (Lemma 4.3, which is crucial to our proofs, does not apply in such a case).

Definition 4.2 (INI-BINI)**.** *A three-level net system (N, M_0) has the property INI (Intransitive Non-Interference), resp. BINI (Bisimulation-Based Intransitive Non-Interference) iff the two-level net system $(N \setminus D, M)$ has the property NDC, resp. BNDC, for $M = M_0$ and for any marking M such that $M_0[\upsilon d\rangle M$ in N for some sequence $\upsilon \in T^*$ and for some downgrading transition $d \in D$.*

The intuition under Definition 4.2 is as follows. The *secret* to be covered is that some high-level transition h has occurred *after the last downgrading transition d*, if any such transition was ever fired in $\mathcal{N}$. Whenever some downgrading transition d is fired, the current secret is deemed obsolete (the high-level transitions that may have occurred before may be revealed by the downgrading transition itself or by subsequent low-level transitions), and a new secret (namely, that some high-level transition may have occurred after the new downgrading transition) is decreed. Thus, INI (resp. BINI) is just a clocked version of NDC (resp. BNDC), where the ticks of the clock are the downgrading transitions. INI/BINI are weakenings of NDC/BNDC but they are still very strong security properties. We feel that such strong properties are really needed in the general context of games, including discrete event systems control as a particular case, where *any* piece of information leaked about the strategy of a player to reach its objective can be used by the adversary to the opposite goal.

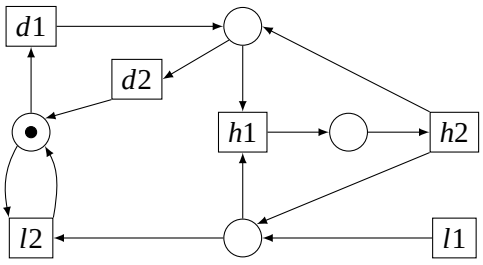

Figure 8: Another three-level net system

In order to illustrate better non-interference in unbounded PT-nets, we would like to present a second example in which the high-level transitions do modify the (contents of the) input places of the low-level transitions. Consider the net system shown in Figure 8. The low-level transition $l1$ is always enabled and it represents the arrival of goods in a shop. The low-level transition $l2$ represents a sale operation and it can only be performed when the shop is open, which is indicated by the presence of one token in the leftmost place. The downgrading transitions $d1$ (closing the shop) and $d2$ (opening the shop) are operated by a guard whose friend takes one article from the shop after closing time (high-level transition $h1$) and brings it back before opening (high-level transition $h2$). It is easily seen that the two high-level transitions form a T-invariant and that $l2$ cannot be fired between $h1$ and $h2$ because the shop is closed during this

period. However, in principle, the guard's friend might grab the key of the shop ($h1$) immediately after each release (by $h2$), and this would impact the low view of the system since the transition $l2$ could then stay blocked forever (blocking may be perceived in weak-bisimulation based semantics). Our definition of BINI does not take this pathologic behaviour into account. Intuitively, Definition 4.2 means that high-level transitions are transparent to the low-level user (that is to say, to the controlled system) unless they cause a starvation of the downgrading transitions (that is to say, of the controller). Therefore, the net system of Figure 8 is secure w.r.t. BINI.

In the rest of the section, we show that both properties INI and BINI can be decided for unbounded PT-nets. $\mathscr{N} = (N, M_0)$ denotes always a three-level net system where $N = (P, T, F)$ and T is partitioned into low-level transitions $l \in L$, high-level transitions $h \in H$, and downgrading transitions $d \in D$.

Lemma 4.3. *(N, M_0) has the property INI iff $(N \setminus D, M) \sim (N \setminus (H \cup D), M)$ for $M = M_0$ and for any marking M such that $M_0[\upsilon d\rangle M$ (in N) with $\upsilon \in T^*$ and $d \in D$.*

Proof. This is a direct application of Proposition 3.4. □

Proposition 4.4. *One can decide whether (N, M_0) has the property INI.*

Proof. First, it can be checked whether $(N \setminus D, M_0) \sim (N \setminus (H \cup D), M_0)$, because all transitions of the net system $(N \setminus (H \cup D), M_0)$ are observable. As a matter of fact, $\mathscr{L}((N \setminus (H \cup D), M_0))$ is always included in $\mathscr{L}((N \setminus D, M_0))$, and by E. Pelz's theorem and corollary (Theorem 6.4 in the appendix), the reverse inclusion can be decided since $\mathscr{L}((N \setminus (H \cup D), M_0))$ is a free PT-net language.

Now fix some downgrading transition $d \in D$. Let $\mathscr{N}_d$ be the net system (with underlying net N_d) constructed as follows.

- N_d has all places of N plus two places p_d and p'_d (the complement of p_d). The initial marking M_{0d} of $\mathscr{N}_d$ extends M_0 by setting one token in p_d and leaving p'_d empty.
- N_d has all transitions t of N with flow relations extended by $F(p_d, t) = 1$ and $F(t, p_d) = 1$.
- N_d has a new transition d' with the same flow relations as d except that $F(d', p_d) = 0$ and $F(d', p'_d) = 1$ (whereas $F(d, p_d) = 1$ and $F(d, p'_d) = 0$).
- N_d has a fresh copy t' of each transition $t \in L \cup H$, with the same flow relations as t except that $F(p'_d, t') = 1$ and $F(t', p'_d) = 1$ (whereas $F(p_d, t) = 1$ and $F(t, p_d) = 1$).
- all transitions of N_d, including H and D, are low-level transitions except for $H' = \{t' \mid t \in H\}$.

We claim that $(N \setminus D, M) \sim (N \setminus H \cup D, M)$ for any M such that $M_0[\upsilon d\rangle M$ in N for the fixed $d \in D$ and for some $\upsilon \in T^*$ iff $\mathscr{N}_d \sim \mathscr{N}_d \setminus H'$ (the proof of this claim, easy but a bit lengthy, is given in the annex, see Claim 6.9). As all transitions of $\mathscr{N}_d \setminus H'$ are observable, the language of this net system is a free PT-net language. It follows by E. Pelz's theorem and corollary (Theorem 6.4 in the appendix) that one can decide on the inclusion relation $\mathscr{L}(\mathscr{N}_d) \subseteq \mathscr{L}(\mathscr{N}_d \setminus H')$. As there are finitely many downgrading transitions $d \in D$, by the above claim, one can decide whether a PT-net system has the property INI. □

Lemma 4.5. *(N, M_0) has the property BINI iff for any reachable marking M_1 of $\mathscr{N}$ and for any high-level transition $h \in H$, $M_1[h\rangle M_2$ entails $\mathscr{L}(N \setminus (H \cup D), M_1) = \mathscr{L}(N \setminus (H \cup D), M_2)$.*

Proof. By Proposition 3.13 and Theorem 3.14, (N, M_0) has the property BINI iff the following entailment relation is satisfied for $M = M_0$ and for any marking M such that $M_0[\upsilon d\rangle M$ (in N) for some $\upsilon \in T^*$ and $d \in D$:
if $M[w\rangle M_1$ in $N \setminus D$ for some $w \in (H \cup L)^*$

and $M_1[h\rangle M_2$ in $N \setminus D$ for some $h \in H$,
then $\mathscr{L}(N \setminus (H \cup D), M_1) = \mathscr{L}(N \setminus (H \cup D), M_2)$.
Grouping the case $M = M_0$ with the other cases, one obtains the lemma. □

Definition 4.6. *Given a three-level net system $\mathscr{N}$ and two transitions $h \in H$ and $l \in L$, we say that $Q(h,l)$ holds* iff *for any words $\chi \in T^*$ and $s \in L^*$, if $M_0[\chi\rangle M_1$, $M_1[h\rangle M_2$, $M_1[s\rangle M_3$, and $M_2[s\rangle M_4$, then $M_3[l\rangle$* iff *$M_4[l\rangle$.*

Proposition 4.7. *One can decide whether (N, M_0) has the property BINI.*

Proof. By Lemma 4.5, $\mathscr{N}$ has the property BINI iff $Q(h,l)$ holds for every high-level action h and for every low-level action l. As $Q(h,l)$ is the same as $P(h,l)$, up to replacing H with $H \cup D$, $Q(h,l)$ is decidable. Therefore, the BINI property can be decided for PT-net systems. □

As nets are labeled injectively on transitions, $\mathscr{L}(N \setminus (H \cup D), M_1) = \mathscr{L}(N \setminus (H \cup D), M_2)$ iff $M_1 \approx M_2$ w.r.t. $\Sigma_o = L$. Therefore, BINI coincides exactly with the property BNID specified by Definition 5.7 in [8].

5 Conclusion and future work

The examples we have discussed seem to suggest that there is a clear, structural reason why an interference is present in a net system: either a high-level transition is causing a low-level transition (e.g., Example 3.5) or a high-level transition and a low-level one are competing for the same token in a place (e.g., Example 3.8). As a matter of fact, in [2] one of the authors showed that precisely this is the case when restricting net systems to elementary net systems (which are essentially PT-nets where each place can contain at most one token). More precisely, a (contact-free) elementary net system $\mathscr{N}$ is BNDC if and only if it is never the case that a low transition consumes a token that *must* have been produced by a high transition nor that a high transition and a low-transition compete for the very same token in a place.

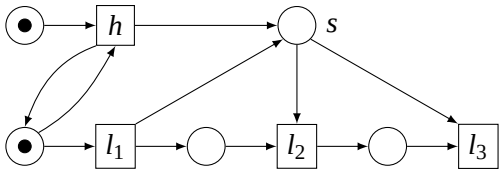

Figure 9: A non BNDC net

Unfortunately, generalizing this characterization in the setting of general PT-nets seems problematic. Consider the net system $\mathscr{N}$ shown in Figure 9. Let M_0 be the initial marking indicated in the figure. Set $M_0[h\rangle M_1$ and set also $M_0[l_1 l_2\rangle M_2$ and $M_1[l_1 l_2\rangle M_3$. Clearly, transition l_3 is enabled at M_2 but disabled at M_3, hence $\mathscr{N}$ is not BNDC. However, in the firing sequence $M_0[h l_1 l_2 l_3\rangle$, the token consumed from place s by the low-level transition l_3 *may* have been produced by the high-level transition h but it *may* also have been produced alternatively by the low-level transition l_1.

As regards continuations of this work, it would be useful to look at flexible versions of downgrading, where each downgrading action bears upon a specific subset of high-level actions. A wider perspective would be to investigate non-interference in the framework of games of partial information, see e.g. [15] for a survey on Games for Security.

Acknowledgment

The authors would like to thank the reviewers for their comments.

References

[1] N. Busi and R. Gorrieri. A Survey on Non-Interference with Petri Nets. *Advanced Course on Petri Nets 2003*, Springer LNCS 3098:328-344, 2004.

[2] N. Busi and R. Gorrieri. Structural Non-Interference in Elementary and Trace Nets. *Mathematical Structures in Computer Science*, 19(6):1065-1090, 2009.

[3] M. Dam. Decidability and Proof Systems for Language-based Noninterference Relations, in Proc. *POPL'2006* 67-78, 2006.

[4] R. Focardi, R. Gorrieri. A Classification of Security Properties. *Journal of Computer Security* 3(1) pp.5-33, 1995.

[5] 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.

[6] J.A. Goguen, J. Meseguer. Security Policy and Security Models. Proc. of Symposium on Security and Privacy (SSP'82), IEEE CS Press, pp. 11-20, 1982.

[7] S. Ginsburg, E.H. Spanier. Bounded Algol-like languages. *Trans. Amer. Math. Soc.* 113:333-368, 1964

[8] R.Gorrieri, M. Vernali. On Intransitive Non-interference in Some Models of Concurrency. submitted, 2009.

[9] M.H.T. Hack. "Petri Net Languages", Technical Report 159, MIT, 1976.

[10] M.H.T. Hack. Decidability questions for Petri nets. PhD thesis, MIT, 1976. *available at* http://dspace.mit.edu/handle/1721.1/27441

[11] P. Jančar. Undecidability of bisimilarity for Petri nets and some related problems. *Theoretical Computer Science* 148(2):281-301, 1995.

[12] E.W. Mayr. An Algorithm for the General Petri Net Reachability Problem. *SIAM J. Comput.* 13(3): 441-460, 1984.

[13] D. McCullough. Noninterference and the Composability of Security Properties. In Proceedings 1988 IEEE Symposium on Security and Privacy, pages 178-186, IEEE Computer Society Press, April 1988.

[14] E. Pelz. Closure Properties of Deterministic Petri Nets. Proc. of STACS'87, Springer LNCS 247:671-681, 1987.

[15] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, D. Shandilya and Q. Wu. A Survey of Game Theory as Applied to Network Security. Proc. HICSS'10, IEEE Computer Society, 1-10, 2010.

[16] P.J. Ramadge and W.M. Wonham. Supervisory Control of a Class of Discrete Event Systems. *SIAM J. Control and Optimization* 25: 206-230, 1987.

[17] P.J. Ramadge and W.M. Wonham. The Control of Discrete Event Systems. *Proc. IEEE, Special Issue on Dynamics of Discrete Event Systems* 77: 81-98, 1989.

[18] J. Rushby. Noninterference, Transitivity, and Channel-control Security Policies. Technical Report CSL-92-02, SRI International, 1992.

[19] 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.

[20] P.Y.A. Ryan, S. Schneider. Process Algebra and Noninterference, Proc. of 12th Computer Security Foundations Workshop, IEEE CS Press, pp. 214-227, 1999.

[21] J.T. Wittbold, D.M. Johnson. Information Flow in Nondeterministic Systems, In Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pages 144-161, IEEE Computer Society Press 1990.

6 Annex

Definition 6.1 (PT-nets)**.** *A* PT-net *is a bi-partite graph $N = (P,T,F)$, where P and T are* finite *disjoint sets of vertices, called* places *and* transitions*, respectively, and $F : (P \times T) \cup (T \times P) \to \mathbb{N}$ is a set of directed edges with non-negative integer weights. A* marking *of N is a map $M : P \to \mathbb{N}$. A transition $t \in T$ is* enabled at *a marking M (notation:$M[t\rangle$) if $M(p) \geq F(p,t)$ for all places $p \in P$. It t is enabled at M, then it can* be fired*, leading to the new marking M' (notation: $M[t\rangle M'$) defined by $M'(p) = M(p) + F(t,p) - F(p,t)$ for all $p \in P$. These definitions are extended inductively to transition sequences $s \in T^*$: for the empty sequence ε, $M[\varepsilon\rangle$ and $M[\varepsilon\rangle M$ are always true; for a non-empty sequence st with $t \in T$, $M[st\rangle$ (or $M[st\rangle M'$) iff $M[s\rangle M''$ and $M''[t\rangle$ (or $M''[t\rangle M'$, respectively) for some M''. A marking M' is* reachable *from a marking M if $M[s\rangle M'$ for some $s \in T^*$. The set of markings reachable from M is denoted by $[M\rangle$.*

Theorem 6.2 (Mayr [12])**.** *Given a PT-net N and two markings M and M', one can decide whether M' is reachable from M.*

Definition 6.3 (Free language of a net system)**.** *The* free language *of a Petri net system $\mathscr{N}$ is the language of the LTS $RG(\mathscr{N})$, where all transitions are considered observable, i.e., $\Sigma_o = T$. In this case, we write $\mathscr{L}(\mathscr{N})$ to denote the free language.*

Theorem 6.4 (Pelz [14])**.** *The complement in Σ_o^* of the free language of a net system may be generated by a labeled net $(\mathscr{N},\lambda)$ with a finite set of final partial markings, characterized by a formula $\mathscr{F}$ built from the logical connectives $\wedge$ and $\vee$ and atomic formulas $M(p) = i$ (with $p \in P$ and $i \in \mathbb{N}$). In other words, a sequence $s \in \Sigma_o^*$ belongs to this complement if and only if $s = \lambda(t_1 t_2 \ldots t_n)$ for some sequence of transitions $M_0[t_1 t_2 \ldots t_n\rangle M$ of $\mathscr{N}$ such that M satisfies $\mathscr{F}$.*

Corollary 6.5 (Pelz)**.** *The problem whether the language of a labeled net system $\mathscr{N}_1$ is included in the free language of a net system $\mathscr{N}_2$ is decidable.*

Proof. The language of $\mathscr{N}_1$ is included in the free language of $\mathscr{N}_2$ if and only if no marking satisfying $\mathscr{F}$ can be reached in $\mathscr{N}_1 \,|\, \mathscr{N}_2'$ where $\mathscr{N}_2'$ is the complementary net of $\mathscr{N}_2$ and $\mathscr{F}$ is the logical formula defining the final partial markings of $\mathscr{N}_2'$. The latter reachability property can be decided in view of the Proposition 6.7 recalled below in this appendix. □

In order to make the statement of Proposition 6.7 understandable, let us recall first the basics of semi-linear sets and their decidable properties. Given a number $n \in \mathbb{N}$, we consider the commutative monoid $(\mathbb{N}^n, +)$ where $+$ denotes the componentwise addition of n-vectors and the null n-vector is the neutral element. Typically, n is the number of places of a Petri net and then $\mathbb{N}^n$ is the realm of all possible markings of this net (markings are seen as vectors in which each entry defines the number of tokens in the corresponding place for some fixed enumeration of the places of the net).

A subset $E \subseteq \mathbb{N}^n$ is called *linear* if it is of the form

$$E = \{a + k_1 \cdot b_1 + \ldots + k_m \cdot b_m \mid k_1, \ldots, k_m \in \mathbb{N}\}$$

for some specific vectors $a \in \mathbb{N}^n$ and $b_1, \ldots, b_m \in \mathbb{N}^n$. For example, let an unmarked net with n places and a transition t be given. Then the set of markings enabling t is linear, since any such marking M can be expressed as the following sum:

$$M \;=\; M_t + k_1 \cdot b_1 + \ldots + k_n \cdot b_n$$

where M_t is the (unique!) minimal marking enabling t and the $b_1,\ldots,b_n$ are the unit vectors corresponding to the places of the net. The natural numbers $k_1,\ldots,k_n$ simply describe excess tokens which may be present in M but are not needed for enabling t.

A subset $E \subseteq \mathbb{N}^n$ is called *semi-linear* if it is a finite union of linear sets. For example, if t_1 and t_2 are two transitions, then the set of markings enabling t_1 or t_2 (or both) is semi-linear, since it is the union of the set of markings enabling t_1 and the set of markings enabling t_2.

Theorem 6.6 (Ginsburg and Spanier [7])**.** *The semi-linear subsets of* $\mathbb{N}^n$ *form an effective boolean algebra.*

Thus, if E, E_1 and E_2 are semi-linear subsets of $\mathbb{N}^n$, then so are $\mathbb{N}^n \setminus E$, $E_1 \cap E_2$ and $E_1 \cup E_2$. The effectiveness part of Ginsburg and Spanier's theorem concerns the possible description of semi-linear sets as linear expressions, and it states that the expressions of a composed set (such as $E_1 \cap E_2$) can be computed effectively from the linear expressions of the constituent set(s) (such as E_1 and E_2).

Proposition 6.7. *Given a PT-net system* $\mathcal{N} = (P,T,F,M_0)$ *and a semi-linear subset of markings* $E \subseteq \mathbb{N}^n$*, where* $n = |P|$*, one can decide whether (some marking in)* E *can be reached from* M_0*.*

The above proposition follows from Lemma 4.3 in [10] where the semi-linear reachability problem is reduced to the reachability problem, and from Theorem 6.2.

In this paper, we use Proposition 6.7 and Theorem 6.6 in the special form as follows.

Corollary 6.8. *Let* $\mathcal{N}$ *be a PT-net system with initial marking* M_0 *and let* t_1 *and* t_2 *be two transitions. The question whether there is some marking* $M \in [M_0\rangle$ *with*

$$(M[t_1\rangle \wedge \neg M[t_2\rangle) \vee (\neg M[t_1\rangle \wedge M[t_2\rangle) \tag{2}$$

is decidable.

Proof. The set of all markings M satisfying (2) is semi-linear. This follows from Theorem 6.6, together with the fact that the set of markings enabling a single transition is linear. The claim now follows directly from Proposition 6.7. □

We finally give a detailed proof of the claim made in the proof of Proposition 4.4.

Claim 6.9. *With the notations used in the proof of Proposition 4.4* $(N \setminus D, M) \sim (N \setminus H \cup D, M)$ *for any* M *such that* $M_0[\upsilon d\rangle M$ *in* N *for some* $\upsilon \in T^*$ **iff** $\mathcal{N}_d \sim \mathcal{N}_d \setminus H'$*.*

Proof. We need examining closely the relationship between the firing sequences of N and N_d. Let $M_0[\upsilon d\rangle M$ be a firing sequence of N and let $M[t_1\ldots t_n\rangle$ be a firing sequence of $N \setminus D$. Then $M_{0d}[\upsilon d\rangle M_d$ in $\mathcal{N}_d$ where $M_d(p_d) = 1$, $M_d(p'_d) = 0$, and $M_d(p) = M(p)$ for every place p of N. Clearly, $M_d[t_1\ldots t_n\rangle$ is a firing sequence of $N_d \setminus D$. In a similar way, $M_{0d}[\upsilon d'\rangle M'_d$ in $\mathcal{N}_d$ where $M'_d(p_d) = 0$, $M'_d(p'_d) = 1$, and $M'_d(p) = M(p)$ for every place p of N. Also clearly, $M'_d[t'_1\ldots t'_n\rangle$ is a firing sequence of $N_d \setminus D$. Conversely, consider now a firing sequence $M_{0d}[u\rangle$ in $\mathcal{N}_d$. If d' does not occur in u, then $M_0[u\rangle$ in N. If $u = \upsilon d' w$, then necessarily, $M_0[\upsilon d\rangle M$ for some M in N, and $w = t'_1\ldots t'_n$ for some sequence $t_1\ldots t_n \in (L \cup H)^*$ such that $M[t_1\ldots t_n\rangle$ in N and hence also in $N \setminus d$.

Suppose that $(N \setminus D, M) \sim (N \setminus H \cup D, M)$ for any M such that $M_0[\upsilon d\rangle M$ in N for the fixed $d \in D$ and for some $\upsilon \in T^*$. By construction, any sequence of transitions of $\mathcal{N}_d$ not including d' is also a sequence of transitions of $\mathcal{N}_d \setminus H'$. Now any sequence of transitions of $\mathcal{N}_d$ including d' is of the form $M_{0d}[\upsilon d' t'_1\ldots t'_n\rangle$, where no transition from H' occurs in υ and $t'_1\ldots t'_n$ is the primed version of some sequence $t_1\ldots t_n \in (L \cup H)^*$. Then, $M_0[\upsilon d\rangle M$ and $M[t_1\ldots t_n\rangle$ for some M in N. For all t_j let $\lambda(t_j) = \varepsilon$

if $t_j \in H$ and $\lambda(t_j) = t_j$ otherwise. As $(N \setminus D, M) \sim (N \setminus H \cup D, M)$, one has also $M[\lambda(t_1)\dots\lambda(t_n)\rangle$. Therefore, if we let $\lambda'(t'_j) = \varepsilon$ if $t'_j \in H'$ and $\lambda'(t'_j) = t'_j$ otherwise, then $M'_d[\lambda'(t'_1)\dots\lambda'(t'_n)\rangle$ in $N_d \setminus D$ where M'_d is the marking of $\mathscr{N}_d$ defined with $M'_d(p_d) = 0$, $M'_d(p'_d) = 1$, and $M'_d(p) = M(p)$ for every place p of N. As no transition from H' occurs in $\upsilon d'\lambda'(t'_1)\dots\lambda'(t'_n)$, this sequence is a firing sequence of $\mathscr{N}_d \setminus H'$. Thus, $\mathscr{N}_d \sim \mathscr{N}_d \setminus H'$.

In order to establish the converse implication, suppose now that $\mathscr{N}_d \sim \mathscr{N}_d \setminus H'$. Consider any two firing sequences $M_0[\upsilon d\rangle M$ and $M[t_1\dots t_n\rangle$ of N with $t_1\dots t_n \in (L \cup H)^*$. By construction of $\mathscr{N}_d$, $M_{0d}[\upsilon d' t'_1\dots t'_n\rangle$. As no transition from H' occurs in υ, by the above assumption, $M_{0d}[\upsilon d'\lambda'(t'_1)\dots\lambda'(t'_n)\rangle$ in $\mathscr{N}_d \setminus H'$ where $\lambda'(t'_j) = \varepsilon$ if $t'_j \in H'$ and $\lambda'(t'_j) = t'_j$ otherwise. Thus, if we set $\lambda(t_j) = \varepsilon$ if $t_j \in H$ and $\lambda(t_j) = t_j$ otherwise, then $M_{0d}[\upsilon d\lambda(t_1)\dots\lambda(t_n)\rangle$ by construction of $\mathscr{N}_d$. . As a consequence, $M[\lambda(t_1)\dots\lambda(t_n)\rangle$ in N and hence also in $N \setminus H \cup d$, concluding the proof of the claim. □