Inference of Local Properties in Petri Nets Composed through an Interface

Carlo Ferigato[1] and Elisabetta Mangioni[2]

[1] Joint Research Centre of the European Commission
via Enrico Fermi, 1, I-21027 Ispra, Italia
carlo.ferigato@jrc.ec.europa.eu
[2] DISCo - Università degli Studi di Milano-Bicocca
viale Sarca, 336, I-20126 Milano, Italia
mangioni@disco.unimib.it

Abstract. We study a notion of *visibility* of the local states of an Elementary Petri net obtained by composition through an interface. The components are three EN systems: the *defender*, providing a service to the environment, the *attacker*, a client of the service, and the *interface*, that models the protocol of interaction between the other two nets. Intuitively, the definition of *visibility* is meant to capture the idea that an *attacker* tries to infer the validity of a local state of the *defender* even if he can observe only the interface and itself. Our analysis is based on the notion of invariant properties and bisimilarity in Petri nets. We suggest also a measure of the degree of visibility of local states of the *defender* as seen by the *attacker*.

Keywords: Elementary Net System, composition, invariant

1 Introduction

The object of our study is open since the beginning of *Computer Science* [6]: we aim at a structural characterization of the hidden internal states of a system that become *visible* after its interaction with a defined subsystem. We assume to have a *high-level* system that wants to keep secret its internal local states from a *low-level* system interacting with the *high-level* component through an *interface*.

Basically, we explore the consequences of a proposal originally made in [3] for defining *non-interference* properties as *structural* properties by using the local validity of conditions as observable properties.

The general context of our study is known today in the literature as *non-interference*. The notions of *opacity* and *interference* between subsystems have been originally defined formally for *process algebras* [4]. In the context of Petri Nets, Busi and Gorrieri [3] applied these notions to Elementary Net Systems and Best, Darondeau and Gorrieri [2] extended recently the results to unbounded P/T Systems.

In these latter works, non-interference is basically defined as language equivalence. The equivalent languages are, respectively, the one generated by the restriction of the system to the *low-level* component alone, and the language generated by the composition of the *low-level* component with any *high-level* component.

The definition of non interference in terms of languages forces at considering *events* as basic observable entities, but this is partly in contradiction with the traditional view of events in nets as entities observable only indirectly, via the modifications of their pre- and post-conditions.

Since we consider as basic observables the local properties of systems represented by conditions, we call the property we describe *visibility*. In terms of *visibility*, two interacting systems can be seen as *defender* and *attacker*. The defender offers a service to the environment and wants to keep secret part of its local states. The attacker uses the service of the defender and tries to get information about its internal local states.

We will represent systems with Elementary Net (EN) systems, a basic model of Petri Nets. The service is modeled by a third EN system called *interface*. The interaction among these systems is given by the composition of the defender and the attacker through the interface. By using standard techniques related to S-invariants and bisimilarity in Petri Nets, we prove a theorem that allows us to recognize the places of the interface visible to, at least, one attacker. Moreover, we discuss the general cases of attackers bisimilar and non bisimilar to the interface. In the conclusions, we propose a measure of the *degree of visibility* of conditions as seen from the attacker.

2 Basic definitions

This section recalls basic definitions about net theory ([10]).

Definition 1. *An Elementary Net (EN) system is a quadruple $N = (B, E, F, m_0)$, where B and E are distinct finite sets of conditions and events, $F \subseteq (B \times E) \cup (E \times B)$ is the flow relation, $m_0 \subseteq B$ is the initial case and*

1. $dom(F) \cup ran(F) = B \cup E$.
2. $\forall e \in E, p, q \in B : (p, e), (e, q) \in F \Rightarrow p \neq q$

The preset of an element $x \in B \cup E$ is defined by ${}^\bullet x = \{y \in B \cup E | (y, x) \in F\}$; the postset of x is given by $x^\bullet = \{y \in B \cup E | (x, y) \in F\}$.

The structure of a net can be represented by a matrix M called the incidence matrix. In this matrix there is a row for each condition, a column for each event and the element (k, j) is set to 1 if there is an arc from the event e_j to the condition b_k, -1 if there is an arc from b_k to e_j, 0 otherwise.

The behaviour of EN systems is defined through the firing rule which specifies when an event can occur, and how event occurrences modify the holding of conditions. Let N be an EN system, $e \in E$ and $m \subseteq B$. The event e is *enabled* at m, denoted $m\,[e\rangle$, if ${}^\bullet e \subseteq m$ and $e^\bullet \cap m = \emptyset$; the occurrence of e at m leads

from m to m', denoted $m\,[e\rangle\,m'$, iff $m' = (m \setminus {}^\bullet e) \cup e^\bullet$. Let ϵ denote the empty word in E^*. It is possible to extend the firing rule to sequences of events in the following way:

$$m\,[\epsilon\rangle\,m$$

$$\forall e \in E, \forall w \in E^*, m\,[ew\rangle\,m' = m\,[e\rangle\,m'[w\rangle m''$$

and w is called *firing sequence*.

A subset $m \subseteq B$ is a *reachable marking* of N if there exists a $w \in E^*$ such that $m_0\,[w\rangle\,m$. The *set of all reachable markings* of N is denoted by $[m_0\rangle$.

An EN system is 1-live if every event can fire in, at least, one reachable marking.

Some properties of a net can be studied through the incidence matrix and its invariants. An S-invariant associates weights to conditions so that the weighted sum of tokens is the same in all reachable markings.

Definition 2. *Let N be a net and let M be its incidence matrix. A vector $\mathbf{I} : B \to \mathbb{N}$ is an S-invariant iff it is a solution of: $\mathbf{I}^T \circ M = \mathbf{0}$.*

Similarly, a T-invariant is defined as a vector $\mathbf{J} : E \to \mathbb{N}$ iff it is a solution of: $M \circ \mathbf{J} = \mathbf{0}$.

An S-invariant is *monomarked* iff its coefficients are in $\{0, 1\}$ and exactly one condition corresponding to a 1 in the invariant belongs to the initial marking m_0.

In the following, when we write N_i we will refer to an EN system: $N_i = (B_i, E_i, F_i, m_0^i)$.

Relations between EN systems can be expressed by N-morphisms ([7]), corresponding to a form of partial simulation. $\widehat{N}$-morphisms are a special case of N-morphisms and will be used in defining the operation of composition.

Definition 3. *A $\widehat{N}$-morphism from N_1 to N_2 is a pair (β, η), such that:*

1. *$\beta \subseteq B_1 \times B_2$, and $\beta^{-1} : B_2 \to B_1$ is a total and injective function;*
2. *$\eta : E_1 \to^* E_2$ is a partial and surjective function;*
3. *if $\eta(e_1)$ is undefined, then $\beta({}^\bullet e_1{}^\bullet) = \emptyset$;*
4. *if $\eta(e_1) = e_2$, then $\beta({}^\bullet e_1) = {}^\bullet e_2$ and $\beta(e_1{}^\bullet) = e_2{}^\bullet$;*
5. *$\forall (b_1, b_2) \in \beta : [b_1 \in m_0^1 \Leftrightarrow b_2 \in m_0^2]$.*

$\widehat{N}$-morphisms reflect S-invariants ([1]), but do not preserve them.

We recall an operation of composition (defined in [8]) that composes two EN systems, N_1 and N_2, with respect to a third EN system N_I called interface because it expose the protocol of interaction between the two systems. The composition is driven by a pair of $\widehat{N}$-morphisms, (β_1, η_1) and (β_2, η_2), respectively from N_1 to N_I, and from N_2 to N_I. In this way, N_1 and N_2 can be seen as composed each one by a local component and a component isomorphic to N_I.

Definition 4. *Let $D_i = \{b \in B_i | \beta_i(b) \neq \emptyset\}$, and $G_i = dom(\eta_i)$.*

We define $N_1\langle N_I\rangle N_2 = N = (B, E, F, m_0)$ as follows:

1. $B = (B_1 \setminus D_1) \cup (B_2 \setminus D_2) \cup B_I$;
2. $E = (E_1 \setminus G_1) \cup (E_2 \setminus G_2) \cup E_{sync}$,
   where $E_{sync} = \{\langle e_1, e_2\rangle | e_1 \in G_1, e_2 \in G_2, \eta_1(e_1) = \eta_2(e_2)\}$;
3. F *is defined by the following clauses:*
   (a) $\forall b \in (B_i \setminus D_i), \forall e \in (E_i \setminus G_i), i = 1, 2$ *we have* $(b, e) \in F \Leftrightarrow (b, e) \in F_i$ *and* $(e, b) \in F \Leftrightarrow (e, b) \in F_i$;
   (b) $\forall b \in (B_i \setminus D_i), \forall e \in G_i, \forall e_j \in E_{3-i}$ *and* $e_s = \langle e, e_j\rangle$ *if* $i = 1$ *or* $e_s = \langle e_j, e\rangle$ *if* $i = 2$, *we have* $(b, e_s) \in F \Leftrightarrow e_s \in E, (b, e) \in F_i$ *and* $(e_s, b) \in F \Leftrightarrow e_s \in E, (e, b) \in F_i$;
   (c) $\forall b \in B_I, \forall e = \langle e_1, e_2\rangle \in E_{sync}$ *we have* $(b, e) \in F \Leftrightarrow (\beta_1^{-1}(b), e_1) \in F_1, (\beta_2^{-1}(b), e_2) \in F_2$ *and* $(e, b) \in F \Leftrightarrow (e_1, \beta_1^{-1}(b)) \in F_1, (e_2, \beta_2^{-1}(b)) \in F_2$;
4. $m_0 = (m_0^1 \setminus D_1) \cup (m_0^2 \setminus D_2) \cup m_0^I$.

From this construction it follows immediately that $N = N_1\langle N_I\rangle N_2$ *as above is an EN system.*

The pair (γ_i, δ_i), *with* $\gamma_i \subseteq B \times B_i$ *and* $\delta_i : E \to E_i$ *defined as:*

- $\gamma_i = \{(b, b) | b \in B_i \setminus D_i\} \cup \{(b, \beta_i^{-1}(b)) | b \in B_I\}$,
- $\forall e \in E_i \setminus G_i : \delta_i(e) = e, \delta_{3-i}(e) =$ *undefined,*
- $\forall \langle e_1, e_2\rangle \in E_{sync} : \delta_i(\langle e_1, e_2\rangle) = e_i$.

is an $\widehat{N}$*-morphism from* $N = N_1\langle N_I\rangle N_2$ *to* $N_i, i = 1, 2$.

Informally, the composition creates a new EN system with the original conditions, events and arcs local to the components plus the conditions of the interface and the Cartesian product of the events to be synchronized. Synchronized events are connected to the local conditions, if there is an arc in the components between these objects, and to the conditions of the interface, if there is an arc in both the components between these events and the inverse-image of the conditions of the interface.

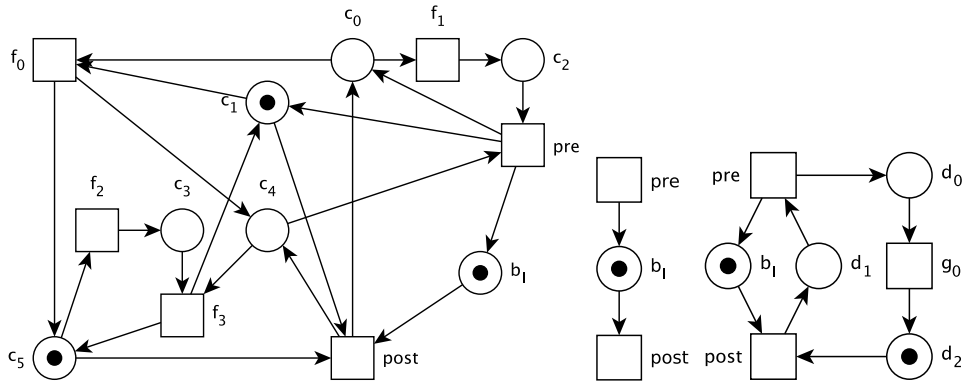
In Fig. 1 it is shown an example of the two EN systems to be composed and the interface; in Fig. 2 there is the resulting net. The $\widehat{N}$-morphisms are defined by identical labels on conditions and events.

Composition through $\widehat{N}$-morphisms assure that, if a component N_1 is bisimilar to the interface, then the composed net is bisimilar to the other component, N_2 [1].

Bisimulation relations have been introduced as an equivalence notion with respect to event observation [5]. We define the observability of events of a system by using a labelling function which associates the same label to different events, when viewed as equal by an observer, and the label τ to unobservable events.

Definition 5. *Let* $N = (B, E, F, m_0)$ *be an Elementary Net System,* $l : E \to L \cup \{\tau\}$ *be a labelling function where* L *is the alphabet of observable actions and* $\tau \notin L$ *the unobservable action. Let* ϵ *denote the empty word in both* E^* *and* L^*. *The function* l *is extended to a homomorphism* $l : E^* \to L^*$ *in the following way:*

$$l(\epsilon) = \epsilon$$



(a) N_1 (b) N_I (c) N_2

Fig. 1: The EN systems N_1 and N_2 being composed through the interface N_I

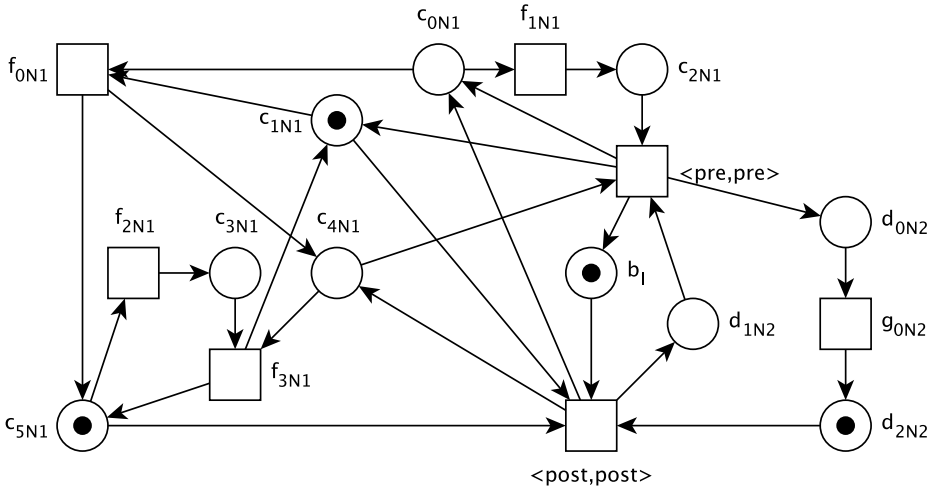


Fig. 2: The resulting EN system $N_1\langle N_I\rangle N_2$

$$\forall e \in E, \forall w \in E^*, l(ew) = \begin{cases} l(e)l(w) & \text{if } l(e) \neq \tau \\ l(w) & \text{if } l(e) = \tau \end{cases}$$

The pair (N, l) *is called* Labelled *Elementary Net System.*

Let $m, m' \in [m_0\rangle$ *and* $a \in L \cup \{\epsilon\}$ *then:*

- a *is enabled at* m*, denoted* $m\,(a\rangle$*, iff* $\exists w \in E^* : l(w) = a$ *and* $m\,[w\rangle$*;*
- *if* a *is enabled at* m*, then the occurrence of* a *can lead from* m *to* m'*, denoted* $m\,(a\rangle\,m'$*, iff* $\exists w \in E^* : l(w) = a$ *and* $m\,[w\rangle\,m'$*.*

We define weak bisimulation as a relation between reachable markings of Labelled Elementary Net Systems [9].

Definition 6. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be an Elementary Net System for* $i = 1, 2$*, with the labelling function* $l_i : E_i \to L \cup \{\tau\}$*. Then* (N_1, l_1) *and* (N_2, l_2) *are* weakly bisimilar*, denoted* $(N_1, l_1) \approx (N_2, l_2)$*, iff* $\exists r \subseteq \left[m_0^1\right\rangle \times \left[m_0^2\right\rangle$ *such that:*

- $(m_0^1, m_0^2) \in r$*;*
- $\forall (m_1, m_2) \in r, \forall a \in L \cup \{\epsilon\}$ *it holds*

$$\forall m_1' : m_1\,(a\rangle\,m_1' \Rightarrow \exists m_2' : m_2\,(a\rangle\,m_2' \wedge (m_1', m_2') \in r$$

and (vice versa)

$$\forall m_2' : m_2\,(a\rangle\,m_2' \Rightarrow \exists m_1' : m_1\,(a\rangle\,m_1' \wedge (m_1', m_2') \in r$$

Such a relation r *is called* weak bisimulation*.*

As example, consider the systems N_2 and N_I of Fig. 1. The observable actions are the ones on E_I. As labelling function for N_2 take l_2 that maps each event on the correspondent one in E_I but for g_0 that is mapped on τ. As labelling function for N_I take the identity function. Now we can write $\{b_I, d_2\}\,(post\rangle\,\{d_1\}$ because we have $\{g_0, post\} \in E_2^*$ such that $l_2(\{g_0, post\}) = post$ and $\{b_I, d_2\}\,[\{g_0, post\}\rangle\,\{d_1\}$.

For simplicity, in the remaining part of the paper we will use the term *bisimulation* instead of *weak bisimulation.*

3 Visibility

Let us consider two EN systems, the defender N_D and the attacker N_A, together with their composition on the interface N_I: $N_D\langle N_I\rangle N_A$ as defined above.

In the following definitions, we will use invariants and markings either as vectors or as characteristic functions: if $\mathbf{v}$ is a vector $x \in \mathbf{v} \Leftrightarrow \mathbf{v}(x) \neq 0$. Since the whole system can be seen as composition of subsystems, we can restrict every vector to the components belonging to a given subsystem. We will use the symbol $\downarrow$ for such a restriction. If $\mathbf{v}$ is a vector related to N, we can divide it in parts associated to the defender, the interface and the attacker: $\mathbf{v}_{\downarrow D}$, $\mathbf{v}_{\downarrow I}$, $\mathbf{v}_{\downarrow I \cup A}$ and $\mathbf{v}_{\downarrow A}$.

We can now define the observability that the attacker has on the markings of the whole system.

Definition 7. *The* attacker-view *of a marking m of the system N is the restriction of the marking on the conditions of N_A and N_I.*

$$\forall m \in [m_0\rangle\,, m_{\downarrow_{I\cup A}} = m \cap (B_A \cup B_I)$$

In general, the attacker is able to distinguish only subsets of markings of the composed system.

Definition 8. *We say that two distinct markings $m, m' \in [m_0\rangle$ are* attacker-view equivalent *if $m_{\downarrow_{I\cup A}} = m'_{\downarrow_{I\cup A}}$.*

A marking $m \in [m_0\rangle$ is distinguishable *by the attacker if $\neg\,\exists\, m' \in [m_0\rangle : m_{\downarrow_{I\cup A}} = m'_{\downarrow_{I\cup A}}$.*

The attacker has a complete distinguishability *of the markings of the whole system if:*

$$\forall m, m' \in [m_0\rangle\,, m_{\downarrow_{I\cup A}} = m'_{\downarrow_{I\cup A}} \Rightarrow m = m'$$

The interesting cases are the ones in which there is no complete distinguishability. We define as follows the conditions visible or invisible to the attacker.

Definition 9. *Condition $p \in B_D \setminus B_I$ is* invisible from a marking $m_A \in \left[m_0^A\right\rangle$ *for an attacker N_A, in isolation, iff*

$$\exists\, m, m' \in [m_0\rangle : m(p) = 0 \wedge m'(p) = 1 \wedge m_{\downarrow_{I\cup A}} = m'_{\downarrow_{I\cup A}} = m_A$$

Condition $p \in B_D \setminus B_I$ is invisible *for N_A iff p is invisible for every $m_A \in \left[m_0^A\right\rangle$. If a condition is not invisible then we will say that is visible.*

We will call $S_D \subseteq B_D \setminus B_I$ the set of invisible conditions computed as in the procedure reported below for *an* attacker N_A, such that N_A is composed with N_D through the interface N_I.

We will call $S_D^* \subseteq B_D \setminus B_I$ the set of invisible conditions for *all* attacking net systems N_A, such that N_A is composed with N_D through the interface N_I.

3.1 Invisible and visible conditions: results

To determine which conditions are in S_D we have to follow this procedure:

- partition the reachable markings of the composed system according to the markings of the attacker;
- for each marking of the attacker, compute the invisible conditions and
- compute the intersection of the sets of invisible conditions above.

Since the computation of all the markings of a Petri Net is exponential, to find the set of invisible conditions is an exponential computation too.

Let us explain this procedure by means of the example of Fig. 1. We use the markings of the composed system, showed in Table 1, and of the attacker, Table 2, to compute S_D. Starting by the markings of the attacker N_2, let us partition the markings of the composed system in sets of undistinguishable markings as

	b_I	c_{0N1}	c_{1N1}	c_{2N1}	c_{3N1}	c_{4N1}	c_{5N1}	d_{0N2}	d_{1N2}	d_{2N2}
S_0	1	0	1	0	0	0	1	0	0	1
S_1	0	1	0	0	0	1	0	0	1	0
S_2	1	0	1	0	1	0	0	0	0	1
S_3	0	0	0	1	0	1	0	0	1	0
S_4	1	1	1	0	0	0	0	1	0	0
S_5	1	1	1	0	0	0	0	0	0	1
S_6	1	0	1	1	0	0	0	1	0	0
S_7	1	0	0	0	0	1	1	1	0	0
S_8	1	0	1	1	0	0	0	0	0	1
S_9	1	0	0	0	0	1	1	0	0	1
S_{10}	1	0	0	0	1	1	0	1	0	0
S_{11}	1	0	0	0	1	1	0	0	0	1
S_{12}	1	0	1	0	0	0	1	1	0	0
S_{13}	1	0	1	0	1	0	0	1	0	0

Table 1: Reachable states of system $N_1\langle N_I\rangle N_2$ of Fig. 2

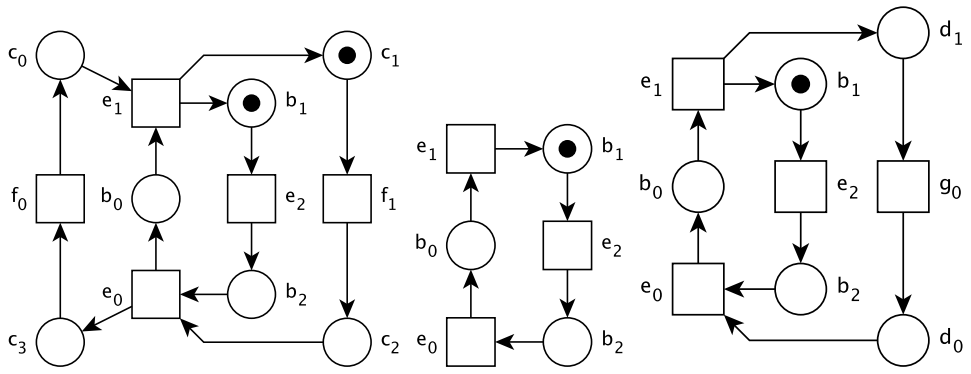
	b_I	d_0	d_1	d_2	possible markings of the composed system	conditions invisible
S_{0A}	1	0	0	1	S_0, S_2, S_5, S_8, S_9, S_{11}	$\{c_{0N1}, c_{1N1}, c_{2N1}, c_{3N1}, c_{4N1}, c_{5N1}\}$
S_{1A}	0	0	1	0	S_1, S_3	$\{c_{0N1}, c_{2N1}\}$
S_{2A}	1	1	0	0	S_4, S_6, S_7, S_{10}, S_{12}, S_{13}	$\{c_{0N1}, c_{1N1}, c_{2N1}, c_{3N1}, c_{4N1}, c_{5N1}\}$

Table 2: Reachable states of system N_2 of Fig. 1c

in Table 2. In the same table are as well listed the conditions invisible from each marking of the attacker; the conditions invisible for N_2 are $\{c_{0N1}, c_{2N1}\}$ given by the intersection of all of the computed S_D sets.

In order to compute S_D^*, we should construct every possible attacker compatible with the interface N_I in respect to the composition operation. This is obviously impossible and we cannot compute the set of conditions invisible to every attacker. Nevertheless, we conjecture that the conditions invisible to the interface (or to an attacker isomorphic to the interface) allow to infer a limit to the set S_D^*. The cases in which the attacker is bisimilar to the interface are discussed below.

Note that we are not interested in *controlling* the behaviour of the defender by imposing a specific marking of the attacker. This situation, at the extreme consequences, could be seen as a deadlock situation imposed by an attacker that blocks completely the interface. Consequently, we are not interested in, for example, a visible condition that is constant in every marking of the composed system since this would be a situation of (local) deadlock related to an attacker taking explicit control of the the defender by but not to the concept of visibility.



(a) N_D (b) N_I (c) N_A

Fig. 3: Two EN systems to be composed through the interface N_I

Let us now prove the central result. We define a necessary constraint for a defined attacker N_A such that a condition of the defender is not in S_D. This situation happens when a condition of the defender is in a monomarked invariant with a condition of the interface. In this case, it is possible to construct an attacker (isomorphic to the interface itself) with a marking in which that condition is visible.

Theorem 1. *Let N_D, N_I be bisimilar EN systems, and $(\beta_D, \eta_D) : N_D \to N_I$ an $\widehat{N}$-morphism. If N_I is 1-live and $b \in B_D \setminus \beta_D^{-1}(B_I), i \in \beta_D^{-1}(B_I)$ satisfies*

$b, i \in I_D$ *with* I_D *monomarked S-invariant of* N_D*, then* b *is visible for each attacker bisimilar to the interface.*

Proof. Consider an attacker isomorphic to the interface, $N_A = N_I$. Given that we consider each attacker bisimilar to the interface, if we prove that this result hold for the interface, it holds for all these attackers too.

Since S-invariants are reflected, I_D is an invariant of the composed net (that in this case is isomorphic to N_D). So, if we can reach a marking in which $i = 1$ then we are sure that $b = 0$ and then b is visible. If $m_0(i) = 1$ this is the marking we are looking for. Suppose $m_0(i) = 0$. Since N_I is an EN system, $\beta_D(i)$ is not isolated. If ${}^\bullet\beta_D(i) = \emptyset$, then $\beta_D(i)$ should have at least a post-event. In this case this post-event is dead while N_I is 1-live by hypothesis. So, the preset of $\beta_D(i)$ is not empty. Given that N_I is 1-live, an event in the preset of $\beta_D(i)$ will fire at some reachable case. Let us call $u \in E_I^*$ a sequence of events such that $m_0^I [u\rangle m_1^I$ and $m_1^I(\beta_D(i)) = 1$. From the assumption that $N_D \approx N_I$ with the labelling function $h : E_D \to E_I \cup \{\tau\}$ we can deduce that $\exists w \in E_D^* : h(w) = u, m_0^D [w\rangle m_1^D, m_1^D(i) = 1$. □

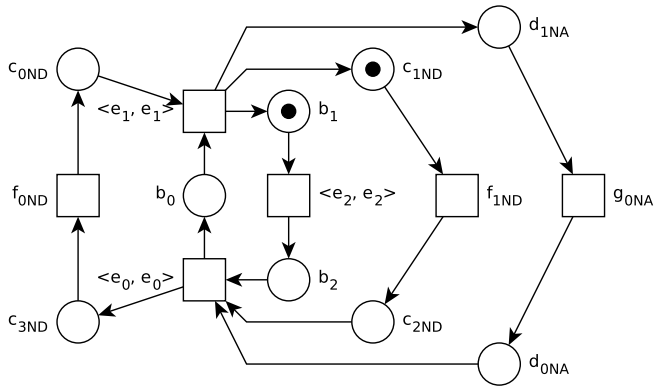


Fig. 4: The composition of the EN systems of Fig. 3

Note that taking into account an attacker not bisimilar to the interface is not of interest because this attacker can introduce some restrictions of behaviour, hence hiding some visible part of the defender. We can see an example of this case in Fig. 3 where the $\widehat{N}$-morphisms are implicitly defined by the identical labels of conditions and events.

If we modify the initial marking m_0 by adding a token in condition d_1 of net N_A, the attacker becomes bisimilar to the interface. In this case, conditions c_1, c_2, c_3 and c_4 of N_D are visible. If we consider the net system as it is, c_1 and c_2 are not visible, as we can see in Fig. 4 and Tables 3 and 4.

Asking a defender bisimilar to the interface is reasonable, because the interface is the protocol of interaction exposed by the defender, so we expect that

	b_0	b_1	b_2	c_{0ND}	c_{1ND}	c_{2ND}	c_{3ND}	d_{0NA}	d_{1NA}
S_0	0	1	0	0	1	0	0	0	0
S_1	0	0	1	0	1	0	0	0	0
S_2	0	1	0	0	0	1	0	0	0
S_3	0	0	1	0	0	1	0	0	0

Table 3: Reachable states of system $N_D\langle N_I\rangle N_A$ of Fig. 4

	b_0	b_1	b_2	d_0	d_1	possible markings of the composed system	invisible conditions
S_{0A}	0	1	0	0	0	S_0, S_2	$\{c_{1ND}, c_{2ND}\}$
S_{1A}	0	0	1	0	0	S_1, S_3	$\{c_{1ND}, c_{2ND}\}$

Table 4: Reachable states of system N_A of Fig. 3c

the system respect his own contract. Also the constraint on the liveness of the interface is reasonable. The only constraint that is not so easy to respect is the one on the S-invariant, because compute all the invariants of an Elementary Net is exponential. Nevertheless, a lot of tools compute the invariant for a given net.

3.2 Measuring visibility

We can give a measure of the uncertainty related to visibility. Intuitively, visible or invisible conditions are opposite ends of some kind of *spectrum* of visibility and, in Def. 9, we do not weight the relative persistence of the invisible condition p in marking m or m'.

For example, in Table 2, attacker case S_{0A}, condition b_{0N1} is more frequently un-marked than marked. Consequently, we could consider b_{0N1} as a random variable whose average information content — persistence in a given local state — depends on the chosen marking of the attacker.

Traditionally, entropy is a measure of the uncertainty associated with a random variable. Consequently, a measure of the uncertainty of the marking for a given defender condition in a given attacker marking can be given, as usual in information science, by using Shannon's entropy:

the entropy H of a discrete random variable $X = \{x_1, ..., x_n\}$ with p denoting the probability mass function of X is $H(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i)$.

Obviously, when $H(X) = 1$ condition X seen as random variable is totally invisible on the attacker marking considered while when $H(X) = 0$ it is visible.

For example, with reference to Table 2, let us calculate the entropy of b_{0N1} seen as variable with possible values in $\{0, 1\}$ with respect to the attacker marking S_{0A}. Marking S_{0A} "covers" $\{S_0, S_2, S_5, S_8, S_9, S_{11}\}$ and, with reference to Table 1, we can divide this set in two subsets: one in which $b_{0N1} = 0$, $\{S_0, S_2, S_8, S_9, S_{11}\}$, and one with $b_{0N1} = 1$, $\{S_5\}$. By plain computation of the relative frequencies of persistence in a state, the entropy is $H(b_{0N1}) =$

$-\sum_{i=1}^{2} p(x_i) \log_2 p(x_i) = -5/6 \log_2 5/6 - 1/6 \log_2 1/6 = 0,65$. So b_{0N1} in S_{0A} is invisible at 65%.

4 Conclusion

We aimed at defining structurally the notion of *visibility* between composed subsystems in order to isolate the unwanted information flows between an hypothetical *defender* system and an *attacker* system whose interactions are coordinated by an *interface*. The composition of these three subsystems is formally defined in terms of morphisms. In the context of information science, our work is naturally placed in the field of *non-interference* as reported in the introduction.

We managed to use traditional tools in the study of Petri Nets like *invariants*, for the definition of the properties of our interest. In the context of this work we did not use T-invariants because their are more related to the concept of controlling the defender than to the concept of visibility. Unfortunately we failed in having a full structural description since, for proving theorem 1, we had to make an hypothesis of *bisimulation* between the *defender* and the *interface*. Nevertheless, we reached a preliminary result in a direction worth to be explored further. Next steps will be in the direction of a finer characterization of the statistical dependency between the subsystems, in proving the conjecture concerning the dependence between all the possible *attackers* and the *interface*, and in using different kinds of morphisms for the definition of the composition in order to avoid the use of bisimilarity relations in the proofs.

Acknowledgments Work partially supported by MIUR.

References

1. Luca Bernardinello, Elena Monticelli, and Lucia Pomello. On preserving structural and behavioural properties by composing net systems on interfaces. *Fundam. Inform.*, 80(1-3):31–47, 2007.
2. Eike Best, Philippe Darondeau, and Roberto Gorrieri. On the decidability of non interference over unbounded petri nets. In Konstantinos Chatzikokolakis and Véronique Cortier, editors, *SecCo*, volume 51 of *EPTCS*, pages 16–33, 2010.
3. Nadia Busi and Roberto Gorrieri. A survey on non-interference with petri nets. In J. Desel, W. Reisig, and G. Rozenberg, editors, *Lectures on Concurrency and Petri Nets*, volume 3098 of *Lecture Notes in Computer Science*, pages 328–344. Springer, 2003.
4. Riccardo Focardi and Roberto Gorrieri. Classification of security properties (part I: Information flow). In Riccardo Focardi and Roberto Gorrieri, editors, *FOSAD*, volume 2171 of *Lecture Notes in Computer Science*, pages 331–396. Springer, 2000.
5. Robin Milner. *Communication and concurrency*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989.
6. Edward F. Moore. Gedanken-experiments on sequential machines. In Claude Elwood Shannon and John McCarthy, editors, *Automata Studies*, volume 34 of *Annals of mathematics studies*, pages 129–153. Princeton University Press, 1956.

7. Mogens Nielsen, Grzegorz Rozenberg, and P. S. Thiagarajan. Elementary transition systems. *Theor. Comput. Sci.*, 96(1):3–33, 1992.
8. Lucia Pomello and Luca Bernardinello. Formal tools for modular system development. In J. Cortadella and W. Reisig, editors, *ICATPN*, volume 3099 of *Lecture Notes in Computer Science*, pages 77–96. Springer, 2004.
9. Lucia Pomello, Grzegorz Rozenberg, and Carla Simone. A survey of equivalence notions for net based systems. In Grzegorz Rozenberg, editor, *Advances in Petri Nets: The DEMON Project*, volume 609 of *Lecture Notes in Computer Science*, pages 410–472. Springer, 1992.
10. Grzegorz Rozenberg and Joost Engelfriet. Elementary net systems. In Wolfgang Reisig and Grzegorz Rozenberg, editors, *Petri Nets*, volume 1491 of *Lecture Notes in Computer Science*, pages 12–121. Springer, 1996.