Non-Interference Control Synthesis for Security Timed Automata*

Guillaume Gardey[1], John Mullins[2] and Olivier H. Roux[1]**

[1] IRCCyN/CNRS
BP 92101 1 rue de la Noë 44321 Nantes Cedex 3 France.
[2] École Polytechnique de Montréal
P.O. Box 6079, Station Centre-ville, Montreal (Quebec), Canada, H3C 3A7.

Abstract. In this paper, the problem of synthesizing controllers that ensures non interference for multilevel security dense timed discrete event systems modeled by an extension of timed automata, is addressed for the first time. We first discuss a notion of non interference for dense real-time systems that refines notions existing in the literature and investigate decidability issues raised by the verification problem for dense time properties. We then prove the decidability of the problem of synthesis of the timed controller for some of these timed non interference properties, providing so a symbolic method to synthesize a controller that ensures them.

1 Introduction

Non interference. Nowadays computing environments allow users to employ programs that are sent or fetched from different sites to achieve their goal, either in private or in an organization. Such programs may be run as a code to do simple calculation task or as interactive communicating programs doing IO operations or communications. Sometimes they deal with secret information such as a private data of a user or as classified data of an organization. Similar situations may occur in any computing environments where multiple users share common computing resources. One of the basic concerns in such context is to ensure programs not to leak sensitive data to a third party, either maliciously or inadvertently. This is one of the key aspects of the security concerns, that is often called *secrecy*. The *information flow analysis* addresses this concern by clarifying conditions when a flow of information in a program is safe (i.e. high-level information never flows into low-level channels). These conditions named *non interference* properties, capture any causal dependency between high-level actions and low-level behavior. Their characterization has appeared rapidly out of the scope of the safety-liveness classification of system properties achieved by the system verification community during the last twenty five years. Also, in recent years, verification of information flow security has become an emergent field of research in computer science with a success story in its application to the analysis of cryptographic protocols where numerous uniform and concise characterizations of information flow security properties (*e.g.* confidentiality, authentication, non-repudiation or anonymity) in terms of non-interference have been proposed.

Timed non interference verification problem. The growing importance of verification for real-time systems, leads naturally to the next question of whether proof techniques developed in the untimed setting can be generalized for timed systems in order to be able to capture,

* Work supported by an NSERC grant (Canadian Government) and by an ACI grant (French Government) on Control and Observation of Real-Time Open Systems (CORTOS) `http://www.lsv.ens-cachan.fr/aci-cortos/`

** Currently at the École Polytechnique de Montréal

besides the logical information flows, also the *time dependent* interference, *e.g.* timing covert channel [FS00]. Some untimed bisimulation-based non interference properties for information flow studied in [FG01] have been reformulated in [RFM03] in a discrete time setting. In [BT03], some state-based and trace-based non interference properties have been introduced in a dense time setting using timed automata.

Timed non interference control problem. A natural generalization of security verification is *control of security* which is useful in the context of automated security system design. The problem here is not to verify that the system meets a given security policy, but to *control* the system in such a way that the security policy is met. In this framework, a system, often called a plant, is usually viewed as *open* and interacting with a "hostile" environment. The problem then is to synthesize a controller such that no matter how the environment behaves, the controlled plan satisfies the given security policy. The controller can control only a subset of actions of the plant, referred to as the controllable actions while the non-controllable actions represent the environment actions. In a real-time framework, the plant is modeled using discrete or continuous clocks. Recent researches have presented symbolic control synthesis algorithms for Timed Automata [MPS95,AT02,DM02].

Organization of the paper and contributions. In this paper, we complete the dense time picture for non interference started in [BT03] by reformulating in this setting some untimed bisimulation-based non interference properties for information flow studied in [FG01] and by introducing a cosimulation-based notion of timed non interference (section 3). Also, we investigate decidability issues raised by the problem of their verification as real-time requirements of finite-state systems. We then focus (section 4) on the state-based and cosimulation-based timed non interference properties and prove the decidability of the problem of synthesis of their timed controller. The main result of the paper is a symbolic method to synthesize a controller that ensures these properties. In the next section we give a short presentation of the notion of Timed Automata used in this paper.

2 Timed Automata

In this section we recall the definitions of Timed Automata (section 2.2) and some of their constructors. But first, some preliminaries about Timed Transition Systems and their behavior are given in section 2.1 in order to express semantics of Timed Automata.

2.1 Timed Transition Systems

Definition 1 (Timed Transition Systems). *A* timed transition system (TTS) *over the set of actions Σ is a tuple $S = (Q, Q_0, \Sigma, \longrightarrow)$ where Q is a set of states, $Q_0 \subseteq Q$ is the set of initial states, Σ is a finite set of actions disjoint from $\mathbb{R}_{\geq 0}$, $\longrightarrow \subseteq Q \times (\Sigma \cup \mathbb{R}_{\geq 0}) \times Q$ is a set of edges. If $(q, e, q') \in \longrightarrow$, we also write $q \xrightarrow{e} q'$.*

Definition 2 (Timed Similation). *Let $S_1 = (Q_1, Q_0^1, \Sigma, \longrightarrow_1)$ and $S_2 = (Q_2, Q_0^2, \Sigma, \longrightarrow_2)$ be two TTS and $\sqsubseteq$ be a binary relation over $Q_1 \times Q_2$. We write $s \sqsubseteq s'$ for $(s, s') \in \sqsubseteq$. $\sqsubseteq$ is a* strong (timed) simulation relation *of S_1 by S_2 if: 1) if $s_1 \in Q_0^1$ there is some $s_2 \in Q_0^2$ s.t. $s_1 \sqsubseteq s_2$; 2) if $s_1 \xrightarrow{d}_1 s_1'$ with $d \in \mathbb{R}_{\geq 0}$ and $s_1 \sqsubseteq s_2$ then $s_2 \xrightarrow{d}_2 s_2'$ for some s_2', and $s_1' \sqsubseteq s_2'$; 3) if $s_1 \xrightarrow{a}_1 s_1'$ with $a \in \Sigma$ and $s_1 \sqsubseteq s_2$ then $s_2 \xrightarrow{a}_2 s_2'$ and $s_1' \sqsubseteq s_2'$.*

A TTS S_2 strongly simulates S_1 *if there is a strong (timed) simulation relation of* S_1 *by* S_2. *We write* $S_1 \sqsubseteq_{\mathcal{S}} S_2$ *in this case.*

When there is a strong simulation relation $\sqsubseteq$ of S_1 by S_2 and also a strong simulation $\sqsubseteq'$ of S_2 by S_1, we have a *strong (timed) cosimulation relation.* When $\sqsubseteq'=\sqsubseteq^{-1}$, we have a *strong (timed) bisimulation relation* and we write $S_1 \approx_{\mathcal{S}} S_2$.

Let $S = (Q, Q_0, \Sigma^\varepsilon, \longrightarrow)$ be a TTS. We now use the ε-abstract TTS $S^\varepsilon = (Q, Q_0^\varepsilon, \Sigma, \longrightarrow_\varepsilon)$ (with no ε-transitions).

Definition 3 (Weak Timed Similation). *Let* $S_1 = (Q_1, Q_0^1, \Sigma_\varepsilon, \longrightarrow_1)$ *and* $S_2 = (Q_2, Q_0^2, \Sigma_\varepsilon, \longrightarrow_2)$ *be two TTS and* $\sqsubseteq$ *be a binary relation over* $Q_1 \times Q_2$. $\sqsubseteq$ *is a* weak (timed) simulation relation *of* S_1 *by* S_2 *if it is a strong timed simulation relation of* S_1^ε *by* S_2^ε. *A TTS* S_2 weakly simulates S_1 *if there is a weak (timed) simulation relation of* S_1 *by* S_2. *We write* $S_1 \sqsubseteq_{\mathcal{W}} S_2$ *in this case.*

When there is a weak simulation relation $\sqsubseteq$ of S_1 by S_2 and also a weak simulation $\sqsubseteq'$ of S_2 by S_1, we have a *weak (timed) cosimulation relation.* When $\sqsubseteq'=\sqsubseteq^{-1}$, we have a *weak (timed) bisimulation relation* and we write $S_1 \approx_{\mathcal{W}} S_2$.

Remark 1. Remark that if $S_1 \sqsubseteq_{\mathcal{S}} S_2$ then $S_1 \sqsubseteq_{\mathcal{W}} S_2$ and if $S_1 \sqsubseteq_{\mathcal{W}} S_2$ then $\mathcal{L}(S_1) \subseteq \mathcal{L}(S_2)$. In particular, weak timed bisimulation refines weak timed cosimulation that refines timed language (or trace) equivalence.

Definition 4 (TTS induced by a set of states). *Let* $\mathcal{S} = (Q, Q_0, \Sigma, \rightarrow)$ *a TTS and* $Y \subseteq Q$. *The TTS* induced by Y on $\mathcal{S}$ *is the TTS* $\mathcal{S}^Y = (Y, Q_0 \cap Y, \Sigma, \rightarrow_i)$ *where* $\rightarrow_i$ *is defined by:* $(q, \bullet, q') \in \rightarrow_i \Leftrightarrow q \in Y \wedge q' \in Y \wedge (q, \bullet, q') \in \rightarrow$

2.2 Timed Automata

Timed Automata (TA) were introduced by Alur & Dill [AD94] and have since been extensively studied. This model is an extension of finite automata with (dense time) *clocks* and enables one to specify real-time systems.

Definition 5 (Timed Automaton). *A* Timed Automaton $\mathcal{A}$ *is a tuple* $(L, l_0, X, \Sigma^\varepsilon, E, Inv)$ *where:* L *is a finite set of* locations*;* $l_0 \in L$ *is the* initial location*;* X *is a finite set of positive real-valued* clocks*;* $\Sigma^\varepsilon = \Sigma \cup \{\varepsilon\}$ *is a finite set of* actions *and* ε *is the* silent *action;* $E \subseteq L \times \mathcal{C}(X) \times \Sigma^\varepsilon \times 2^X \times L$ *is a finite set of* edges*,* $e = \langle l, \gamma, a, R, l' \rangle \in E$ *represents an edge from the location* l *to the location* l' *with the guard* γ*, the label* a *and the reset set* $R \subseteq X$*;* $Inv \in \mathcal{C}(X)^L$ *assigns an* invariant *to any location. We restrict the invariants to conjuncts of terms of the form* $x \preceq r$ *for* $x \in X$ *and* $r \in \mathbb{N}$ *and* $\preceq \in \{<, \leq\}$.

Definition 6 (Semantics of a Timed Automaton). *The semantics of a timed automaton* $\mathcal{A} = (L, l_0, X, \Sigma^\varepsilon, E, Inv)$ *is a timed transition system* $S^{\mathcal{A}} = (Q, q_0, \Sigma^\varepsilon, \rightarrow)$ *with* $Q = L \times (\mathbb{R}_{\geq 0})^X$*,* $q_0 = (l_0, \mathbf{0})$ *is the initial state and* $\rightarrow$ *is defined by:*

$$(l, v) \xrightarrow{a} (l', v') \text{ iff } \mathbf{Fired}(l, \gamma, a, R, l') \in E \text{ s.t. } \begin{cases} \gamma(v) = \mathit{tt}, \\ v' = v[R \mapsto 0] \\ Inv(l')(v') = \mathit{tt} \end{cases}$$

$$(l, v) \xrightarrow{t} (l', v') \text{ iff } \begin{cases} l = l' \qquad v' = v + t \quad \textit{and} \\ \forall\, 0 \leq t' \leq t,\ Inv(l)(v + t') = \mathit{tt} \end{cases}$$

We denote $Q^{\mathcal{A}}$, for the set of states of $\mathcal{A}$. A run ρ of $\mathcal{A}$ is an initial run of $S^{\mathcal{A}}$. The timed language accepted by $\mathcal{A}$ is $\mathcal{L}(\mathcal{A}) = \mathcal{L}(S^{\mathcal{A}})$.

Lets finally introduce some constructors over Timed Automata in order to express timed information flow in concurrent timed systems.

To describe a system as a parallel composition of timed automata, we use the classical composition notion based on a *synchronization function à la* Arnold-Nivat. Let $X = \{x_1, \cdots, x_n\}$ be a set of clocks, $\mathcal{A}_1$, ..., $\mathcal{A}_n$ be n timed automata with $\mathcal{A}_i = (N_i, l_{i,0}, X, \Sigma, E_i, Inv_i)$. A *synchronization function* f is a partial function from $(\Sigma \cup \{\bullet\})^n \hookrightarrow \Sigma$ where $\bullet$ is a special symbol used when an automaton is not involved in a step of the global system. We denote by $(\mathcal{A}_1 | \ldots | \mathcal{A}_n)_f$ the parallel composition of the $\mathcal{A}_i$'s w.r.t. f. The configurations of $(\mathcal{A}_1 | \ldots | \mathcal{A}_n)_f$ are pairs $(\mathbf{l}, \mathbf{v})$ with $\mathbf{l} = (l_1, \ldots, l_n) \in N_1 \times \ldots \times N_n$ and $\mathbf{v} = (v_1, \cdots, v_n)$ where each v_i is the value of the clock $x_i \in X$.

Definition 7 (Hiding Timed Automata). *Let $\mathcal{A} = (L, l_0, X, \Sigma^{\varepsilon}, E, Inv)$ be a TA and $\Gamma \subseteq \Sigma$. We define the Γ-hiding TA $\mathcal{A}_{/\Gamma} = (L, l_0, X, (\Sigma \setminus \Gamma)^{\varepsilon}, E_{/\Gamma}, Inv)$ (with hided Γ-transitions) by $\langle l, \gamma, a, R, l' \rangle \in E_{/\Gamma}$ iff*

1. *$a \in (\Sigma \setminus \Gamma)^{\varepsilon}$ and $\langle l, \gamma, a, R, l' \rangle \in E$ or,*
2. *$a = \epsilon$ and there is a transition $\langle l, \gamma, b, R, l' \rangle \in E$ with $b \in \Gamma$.*

Definition 8 (Restriction Timed Automata). *Let $\mathcal{A} = (L, l_0, X, \Sigma^{\varepsilon}, E, Inv)$ be a TA and $\Gamma \subseteq \Sigma$. We define the Γ-restriction TA $\mathcal{A}_{\setminus\Gamma} = (L, l_0, X, (\Sigma \setminus \Gamma)^{\varepsilon}, E_{\setminus\Gamma}, Inv)$ (without Γ-transitions) by $\langle l, \gamma, a, R, l' \rangle \in E_{\setminus\Gamma}$ iff*

$$a \in (\Sigma \setminus \Gamma)^{\varepsilon} \text{ and } \langle l, \gamma, a, R, l' \rangle \in E.$$

3 Timed Non Interference for Security Timed Automata

In this section, we reformulate some non interference properties for information flow analysis in dense time discrete event systems previously studied in an untimed [FG01] or discrete time [RFM03] setting. So we refine the notion of timed non interference for Timed Automata introduced in [BT03]. We start with *Strong Non-deterministic Non Interference* (SNNI). The basic idea of SNNI is that the public behavior of a system is not affected by the effects of its private behavior. We define this property on different behavior notions in section 3.3: trace equivalence, weak cosimulation, weak bisimulation and reachability equivalence. We then classify these properties among them and address decidability issues raised by their verification. A timed security model based on timed automata is presented in section 3.2.

3.1 An introductory example

Let start by considering informally how information flow prohibition arises in interacting transition systems, taking a simple example. Consider first the transition system depicted on the left-hand side of the Figure 1. Suppose we attach secrecy levels to each action, for example $h_1 \in \Sigma_{priv}$ and $l_1 \in \Sigma_{pub}$. Intuitively this means that we wish interaction at h_1 to be secret, while interaction at l_1 may be known by a wider public: any private action may interact at h_1 and l_1, while a public action may interact only at l_1. None of the public observers *i.e.* observers allowed to observe (or react) only the public actions, has the possibility to know

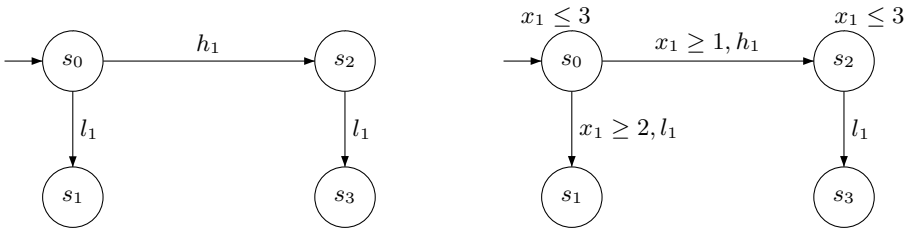

Fig. 1. Non-interferent automaton and interferent Timed Automaton

whether an interaction with h_1 happened or not. Otherwise stated, no causal dependency from private behavior may be inferred by any public observer. However adding timing constraints on this transition system could introduce prohibited information flow from the private level to the public one. As an illustration suppose that l_1 cannot occurs from s_0 before 2 time units as depicted by the time automata on the right-hand side of the Figure 1, then any public observer has the possibility to know whether an interaction with h_1 happened or not in the eventuality of l_1 occurring from s_2 before 2 time units *i.e.* there is a correlation between some private behavior and some public observation.

3.2 A Timed Security Model

We are looking at extended timed automata to model processes and computations of computing entities interacting at different trust levels.

Definition 9 (Security Timed Automaton). A *Security Timed Automaton* is a timed automaton whose the set of visible actions Σ are partitioned in 2 sets Σ_{pub}, Σ_{priv}.

3.3 Timed Information Flow Properties

The introductory example discussed in the section 3.1 motivates the following definitions.

3.3.1 Timed Strong Non-deterministic Non Interference

SNNI has been first proposed by Focardi [FG01] as a trace-based generalization of non interference for concurrent systems.

Definition 10 (Timed SNNI). Let $\mathcal{A}$, a security timed automaton. $\mathcal{A}$ satisfies *timed strong non-deterministic non interference* (timed SNNI) if and only if

$$\mathcal{L}(\mathcal{A}_{/\Sigma_{priv}}) = \mathcal{L}(\mathcal{A}_{\setminus\Sigma_{priv}})$$

3.3.2 Timed Cosimulation-based SNNI

We now give a weak timed cosimulation non interference definition.

Definition 11 (Timed Cosimulation-based SNNI). Let $\mathcal{A}$, a security timed automaton. $\mathcal{A}$ satisfies *timed cosimulation non-deterministic non interference* (timed CSNNI) if and only if

$$S^{\mathcal{A}_{/\Sigma_{priv}}} \sqsubseteq_{\mathcal{W}} S^{\mathcal{A}}$$

The next result presents an algebraic characterization of timed cosimulation non-deterministic non interference (timed CSNNI):

Theorem 1 (Unwinding Theorem for CSNNI). *A security timed automaton $\mathcal{A}$ satisfies timed cosimulation non-deterministic non interference (timed CSNNI) iff*

$$S^{\mathcal{A}/\Sigma_{priv}} \sqsubseteq_{\mathcal{W}} S^{\mathcal{A}\setminus\Sigma_{priv}} \tag{1}$$

$$S^{\mathcal{A}\setminus\Sigma_{priv}} \sqsubseteq'_{\mathcal{W}} S^{\mathcal{A}/\Sigma_{priv}} \tag{2}$$

Proof. Equation 1 is obtained from definition 11: as $\mathcal{A}_{/\Sigma_{priv}}$ is defined over Σ_{pub} we have $S^{\mathcal{A}/\Sigma_{priv}} \sqsubseteq_{\mathcal{W}} S^{\mathcal{A}} \Leftrightarrow S^{\mathcal{A}/\Sigma_{priv}} \sqsubseteq_{\mathcal{W}} S^{\mathcal{A}\setminus\Sigma_{priv}}$. Equation 2 is obtained directly from definitions of timed automata, hiding and restriction: for any TA over $\Sigma = \Sigma_{priv} \cup \Sigma pub$, we have $S^{\mathcal{A}\setminus\Sigma_{priv}} \sqsubseteq'_{\mathcal{W}} S^{\mathcal{A}/\Sigma_{priv}}$. Furthermore $\sqsubseteq'_{\mathcal{W}}$ is not necessarily equal to $\sqsubseteq^{-1}_{\mathcal{W}}$.

3.3.3 Timed Bisimulation-based SNNI

We now give a timed version of the bisimulation-based definition of strong non-deterministic non interference proposed in [FG01]. Actually, any bisimulation-based information flow property presented in [FG01] could be recast in a similar manner. Differences between CSNNI and BSNNI are illustrated in appendix A with figures Fig. 4 and Fig. 5.

Definition 12 (Timed Bisimulation-based SNNI). Let $\mathcal{A}$, a security timed automaton. $\mathcal{A}$ satisfies *timed bisimulation-based strong non-deterministic non interference* (timed BSNNI) if and only if

$$S^{\mathcal{A}/\Sigma_{priv}} \approx_{\mathcal{W}} S^{\mathcal{A}\setminus\Sigma_{priv}}$$

3.3.4 Timed State NNI

In [BT03], authors propose a decidable notion of timed non deterministic non-interference based on states. We reformulate it as follows :

Definition 13 (Timed State NNI). *Let $\mathcal{A}$ be a Security Timed Automaton over Σ ($\Sigma = \Sigma_{pub} \cup \Sigma_{priv}$). $\mathcal{A}$ is said to be Timed State Non Deterministic Non Interfering (timed StNNI) if and only if:*

$$Q^{\mathcal{A}/priv} = Q^{\mathcal{A}\setminus priv} \text{ i.e. } Q^{\mathcal{A}} = Q^{\mathcal{A}\setminus priv}$$

Let us note that as $Q^{\mathcal{A}\setminus priv} \subseteq Q^{\mathcal{A}}$, then timed StNNI is equivalent to $Q^{\mathcal{A}/priv} \subseteq Q^{\mathcal{A}\setminus priv}$ i.e. $Q^{\mathcal{A}} \subseteq Q^{\mathcal{A}\setminus priv}$.

3.4 Ordering relation among properties

Theorem 2 (Timed non interference classification).

$$\textit{timed-BSNNI} \Rightarrow \textit{timed-CSNNI} \Rightarrow \textit{timed-SNNI} \tag{3}$$

$$\textit{timed-SNNI} \not\Rightarrow \textit{timed-CSNNI} \not\Rightarrow \textit{timed-BSNNI} \tag{4}$$

Proof. Equation 3 follows directly Remark 1 while counterexamples proving that implications are strict (Equation 4) are provided in Appendix A.

Remark 2. There is no ordering between Timed StNNI and any of the previous non interference definitions presented here.

Remark 3. It can be proved that 0-trace-non-interference introduced in [BT03] is equivalent to Timed StNNI.

3.5 Decidability results

Theorem 3 (Timed SNNI decidability). *Timed SNNI is undecidable.*

Proof. We prove that the universality problem for TA can be expressed as a timed SNNI problem. Let $\mathcal{A}$ be a TA over Σ and $\mathcal{A}_u$ be a TA that accepts universal language over Σ ($\mathcal{A}_u$ have one locality ℓ_u and for each action $a \in \Sigma$, a loop from ℓ_u to ℓ_u with label a). We construct a security timed automaton $\mathcal{A}_f$ with $\Sigma_{pub} = \Sigma$ and $\Sigma_{priv} = \{h\}$ as follows : 1) We start $\mathcal{A}_f$ with $\mathcal{A}$, 2) we add $\mathcal{A}_u$ to $\mathcal{A}_f$ and we add an arc from the initial state of $\mathcal{A}$ with label h leading to the locality ℓ_u. Thus $\mathcal{A}$ accepts universal language (i.e. $\mathcal{L}(\mathcal{A}_u) \subseteq \mathcal{L}(\mathcal{A})$) iff $\mathcal{A}_f$ is timed trace non-interfering. As universality problem is known to be undecidable for TA, it follows that timed SNNI problem is also undecidable.

Theorem 4 (Timed BSNNI, CSNNI and StNNI decidability). *timed BSNNI, timed CSNNI and timed StNNI are decidable.*

Proof. Simulation [AIPP00] and bisimulation [LLW95] are decidable for TA and then timed BSNNI and timed CSNNI are decidable. As reachability [AD94] is decidable for TA, timed StNNI is also decidable.

4 Timed Non-Interference Controllability

4.1 Introduction

Recent researches have presented symbolic control synthesis algorithms for Timed Automata [WTH91,MPS95,AT02]. The aim of such algorithms is to design an agent (also named controller or supervisor) that restricts the behavior of the initial system so that a property of interest is modeled by the controlled system (closed-loop system).

In such frameworks, the set of actions of the model is classically partitioned into controllable and uncontrollable actions. Controllable can be disabled by the controller whereas uncontrollable actions can not be restricted.

Definition 14 (Controllable and uncontrollable actions). *Let $\mathcal{A}$ be a Security Timed automaton. The set of actions Σ is partitioned in 2 sets Σ_{pub}, Σ_{priv}. Σ_{pub} is the set of uncontrollable actions and Σ_{priv} is the set of controllable actions.*

We formalize the controller of a Security Timed Automaton in the following definition:

Definition 15 (Controller). *Let $\mathcal{A} = (L, l_0, X, \Sigma, E, Inv)$ be a Security Timed Automaton over Σ ($\Sigma = \Sigma_{pub} \cup \Sigma_{priv}$). A controller $\mathcal{C} = (L^C, l_0^C, X, \Sigma, E^C, Inv^C)$ for $\mathcal{A}$ is a Timed Automaton over Σ such that $\mathcal{A}_C = \mathcal{A}|\mathcal{C}_{f_c})$ where $\mathcal{A}_C = (L_C, (l_0, l_0^C), X, \Sigma, E_C, Inv_C))$ with $L_C \in L \times L^C$ and f_c is a control synchronization function defined by $f_c(priv, priv) = priv$, $f_c(pub, pub) = pub$.*

The controller mustn't restrict uncontrollable behavior in the following meaning :

Let (l_a, l_c) a locality of $\mathcal{A}_\mathcal{C}$,

1. $\forall \langle l_a, \gamma, a, R, l'_a \rangle \in E$ *s.t.* $a \in \Sigma_{pub}$, *there is an edge* $\langle (l_a, l_c), \gamma, a, R, (l'_a, l'_c) \rangle \in E_C$,
2. *if* $\nexists \langle (l_a, l_c), \gamma, a, R, (l'_a, l'_c) \rangle \in E_C$ *with* $a \in \Sigma_{priv}$ *then* $Inv_C(l_a, l_c) = Inv(l_a)$

4.2 Timed Non-interference control problems

In this section we define and propose solutions for some timed non-interference control problem. We prove the decidability of control problems of *timed-StNNI* and *timed-CSNNI* by giving algorithms for the synthesis of controller guaranteeing these two properties. As well as the safety control problem for Timed Automata, the TTS solution given by the algorithm can be both interpreted as the system in closed-loop and the controller. For all these problems, the controller that forbids any controllable actions is a solution but not necessarily the most permissive.

4.2.1 Timed-StNNI Control Problem

First, we consider the *Timed State Non-Interference Control Problem.*

Definition 16 (Timed-StNNI Control Problem). *Let $\mathcal{A}$ be a Security Timed Automaton over Σ ($\Sigma = \Sigma_{pub} \cup \Sigma_{priv}$). A StNNI controller $\mathcal{C}$ for $\mathcal{A}$ (according to def. 15) is a Timed Automaton over Σ such that :*

$$Q^{((\mathcal{A}|\mathcal{C})_{fc})_{/\Sigma_{priv}}} = Q^{((\mathcal{A}|\mathcal{C})_{fc})_{\setminus \Sigma_{priv}}}$$

$$i.e.\ Q^{(\mathcal{A}|\mathcal{C})_{fc}} = Q^{((\mathcal{A}|\mathcal{C})_{fc})_{\setminus \Sigma_{priv}}}$$

Let us consider the solution of the safety control problem on $\mathcal{A}$ that is to find a controller C such that $Q^{(A|C)_{fc}} \subseteq Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$.

Proposition 1. *If C is the solution of the control problem $Q^{(A|C)_{fc}} \subseteq Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$, C is a solution of timed-StNNI if and only if:*

$$\forall q \in Q^{(A|C)_{fc}} \exists \rho = \tau_1 \cdot low_1 \ldots \tau_n \cdot low_n \in \mathcal{S}^{(A|C)_{fc}}, low_i \in \Sigma_{pub} \text{ such that } q_0 \xrightarrow{\rho} q$$

Proof. Let C the solution of the safety control problem $Q^{(A|C)_{fc}} \subseteq Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$.

If C is the solution of the timed-StNNI problem then $Q^{(A|C)_{fc}} \subseteq Q^{((A|C)_{fc})_{\setminus \Sigma_{priv}}}$. Since the property holds for all states of $Q^{((A|C)_{fc})_{\setminus \Sigma_{priv}}}$, it also holds for any state of $Q^{(A|C)_{fc}}$.

The converse is straightforward.

This characterization can give a decision procedure for the timed-StNNI control problem. Let us consider the following algorithm:

Definition 17 (Algorithm State-Alg). *We note State-Alg the following fix-point algorithm:*

$X_0 \leftarrow Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$
repeat
  $X_{i+1} \leftarrow \pi(X_i)$
  $X_{i+1} \leftarrow X_{i+1} \cap \overrightarrow{Post_{\Sigma_{pub}}}^*(Q_0, X_{i+1})$
until $X' = X_i$

where $\pi(X)$ is the classical controllable predecessor operator [MPS95,AT02,Tri98] (see appendix B) and $\overrightarrow{Post_\Sigma}^*(X,Y) = \{q \in Y \mid \exists(\tau_i)_n \in (\mathbb{R}_{\geq 0})^n,\ \exists(low_i)_n \in (\Sigma_{pub})^n,\ \exists q_0 \in X$ such that $q_0 \xrightarrow{\tau_1 \cdot low_1} q_1 \ldots \xrightarrow{\tau_n \cdot low_n} q_n = q$ and $\forall i,\ q_i \in Y\}$

This is the classical controllable predecessors algorithm extended with a step that ensures that all states computed are reachable from the initial states by a sequence of low level actions (Σ_{pub}), that is states of $((\mathcal{A}|\mathcal{C})_{f_c})_{\setminus \Sigma_{priv}}$.

It follows from this algorithm this theorem:

Theorem 5 (Timed-StNNI Control Problem Decidability). *The timed-StNNI control problem is decidable and there exists a state-based controller $\mathcal{C}$ such that $(\mathcal{A}|\mathcal{C})_{f_c}$ is timed-StNNI.*

Proof. Let us consider the algorithm State-Alg.

1. *State-alg terminates in a finite number of iterations.* Actually, let us consider the region graph of $\mathcal{A}$: $\mathcal{R}^*$ [AD94]. $\mathcal{R}^*$ has a finite number of regions. The sequence of X_i is monotone ($X_{i+1} \subseteq X_i$). State-Alg is then a fix-point algorithm over a finite domain with a monotone function, then converges in a finite number of iterations. We note X^* the solution.
2. *The TTS induced by X^* on $\mathcal{A}$ is timed-StNNI.* It is straightforward that $\forall i X_i \subseteq Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$ and that the TTS verifies the condition of the proposition 1

4.2.2 Timed-CSNNI Control Problem

Intuitively, the method we propose consists first in computing the (controllable as well as uncontrollable) non interfering behavior of the STA $\mathcal{A}$ that is to say the intersection of behavior of $\mathcal{A}$ with the the behavior of $\mathcal{A}_{\setminus priv}$ given by the product $(\mathcal{A}|\mathcal{A}_{\setminus priv})_f$ synchronized on actions of Σ_{pub} and free on actions of Σ_{priv}. The controllable behavior guaranteeing the non-interference property is then extracted from this result.

Definition 18 (Timed-CSNNI Control Problem). *Let $\mathcal{A}$ be a Security Timed automaton over $\Sigma = \Sigma_{pub} \cup \Sigma_{priv}$. A CSSNI controller $\mathcal{C}$ for $\mathcal{A}$ (according to def. 15) is a timed automaton over Σ such that:*

$$\mathcal{S}^{(\mathcal{A}|\mathcal{C})_{/\Sigma_{priv}}} \sqsubseteq_{\mathcal{W}} \mathcal{S}^{(\mathcal{A}|\mathcal{C})_{\setminus \Sigma_{priv}}}$$

We will prove that the following theorem holds:

Theorem 6 (Timed-CSNNI Control Problem Decidability). *Timed-CSNNI is decidable and a controller is computable.*

Definition 19. *Let $\mathcal{A}$ a STA. We denote $\mathcal{A}' = (\mathcal{A}|\mathcal{A}_{\setminus priv})_f$ where f is defined by: $f(priv, \bullet) = priv$, $f(pub, pub) = pub$ (see figure 3). $\mathcal{A}'$ is Timed-CSNNI.*

First we define the simulation relation by:

Definition 20 (Simulation relation). *Let $q = (l_1, l_2, v) \in Q^{(\mathcal{A}|\mathcal{C})_{/\Sigma_{priv}}}$ and $q' = (l'_1, l'_2, v') \in Q^{(\mathcal{A}|\mathcal{C})_{\setminus \Sigma_{priv}}}$: $q \sqsubseteq q' \Leftrightarrow l_2 = l'_2 \wedge v = v'$*

Since $\mathcal{S}^{(\mathcal{A}|\mathcal{C})_{\setminus \Sigma_{priv}}} \sqsubseteq \mathcal{S}^{\mathcal{A}_{\setminus \Sigma_{priv}}}$ (the controller restrict the behavior of $\mathcal{A}$), we will also note $q \sqsubseteq q'$ for any $q = (l_1, l_2, v) \in Q^{(\mathcal{A}|\mathcal{C})_{\setminus \Sigma_{priv}}}$ and $q' = (l'_2, v') \in Q^{\mathcal{A}_{\setminus \Sigma_{priv}}}$ if and only if $l_2 = l'_2$ and $v = v'$.

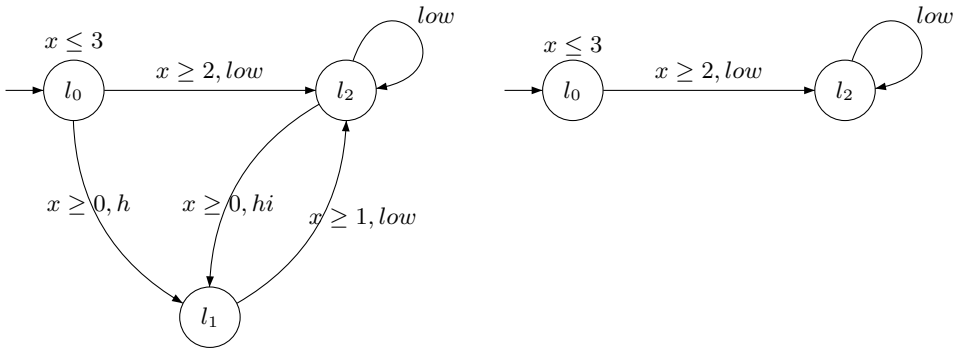

Fig. 2. $\mathcal{A}$ and $\mathcal{A}_{\setminus \Sigma_{priv}}$

Definition 21 (Unfolding of $\mathcal{A}$ over $(\mathcal{A}|\mathcal{A}_{\setminus \Sigma_{priv}})_f$). *Let $\mathcal{A} = (L, \ell_0, X, \Sigma, E, Inv)$ be a TA over $\Sigma = \Sigma_{pub} \cup \Sigma_{priv}$. Let $\mathcal{A}' = (L', (l'_0, l'_0), X, \Sigma, E', Inv'))$ with $L' \in L \times L$ be a TA defined by $\mathcal{A}' = (\mathcal{A}|\mathcal{A}_{\setminus \Sigma_{priv}})_f$.*

The TA $\mathcal{A}'' = (L'', (l_0, l_0), X, \Sigma, E'', Inv'')$ with $L'' \in (L \times L) \cup \{bad\}$ is the unfolding of $\mathcal{A}$ over $\mathcal{A}'$ iff :

1. $L'' = L' \cup \{bad\}$
2. $\forall e' = \langle (l_i, l_j), \gamma', a, R', (l'_i, l'_j) \rangle \in E'$ *such that* $e = \langle l_i, \gamma, a, R, l'_i \rangle \in E$
   we have $\langle (l_i, l_j), \gamma, a, R, (l'_i, l'_j) \rangle \in E''$,
3. $\forall e = \langle l, \gamma, a, R, l' \rangle \in E$ *such that* $a \in \Sigma_{pub}$, $\forall (l, l_i) \in L'$ *and* $(l', l_j) \in L'$
   we have $\langle (l, l_i), \gamma, a, R, (l', l_j) \rangle \in E''$,
4. $\forall e = \langle l, \gamma, a, R, l' \rangle \in E$ *such that* $a \in \Sigma_{pub}$, $\forall (l, l_i) \in L'$ *and* $(l', l_j) \notin L'$
   we have $\langle (l, l_i), \gamma, a, R, (bad) \rangle \in E''$,
5. $\forall l = (l_i, l_j) \in L'', Inv(l) = Inv(l_i)$

The second and the fifth requirements relax the constraints inherited from $\mathcal{A}_{\setminus \Sigma_{priv}}$. The third and the fourth requirements add edges over public actions removed by $(\mathcal{A}|\mathcal{A}_{\setminus \Sigma_{priv}})_f$. We use the location *bad* as destination of edges leading to location not in L'.

Definition 22 (States of $\mathcal{A}''$ similar to states of $\mathcal{A}_{\setminus \Sigma_{priv}}$). *Let us consider the Timed Automaton $\mathcal{A}''$ and the set of states of $\mathcal{A}'$: $Q^{\mathcal{A}'} \subseteq Q^{\mathcal{A}''}$. We note $SiSt(\mathcal{A}')$ the set of states defined by:*

$$SiSt(\mathcal{A}') = \{q \in Q^{\mathcal{A}'} \mid \text{if } \exists low \in \Sigma_{pub} \text{ st. } q \xrightarrow{low} \in E'' \text{ then } \exists q' \in Q^{\mathcal{A}_{\setminus \Sigma_{priv}}} \text{ st. } q \sqsubseteq q' \wedge q' \xrightarrow{low} \in E^{\mathcal{A}_{\setminus \Sigma_{priv}}}\}$$

$SiSt(\mathcal{A}')$ contains all states that are weakly similar to a state of $\mathcal{A}_{\setminus \Sigma_{priv}}$. That is, for every state $q = (l_1, l_2, v)$ such that the transition low is possible in the TTS defined by $\mathcal{A}''$, there exists also such a transition $(l_2, v) \xrightarrow{low}$ in the TTS defined by $\mathcal{A}_{\setminus \Sigma_{priv}}$. Considering the example of the figure 3, $(l_1, l_0, x = 1) \notin SiSt(\mathcal{A}')$ since $(l_0, x = 1) \not\xrightarrow{low}$ for $\mathcal{A}_{\setminus \Sigma_{priv}}$.

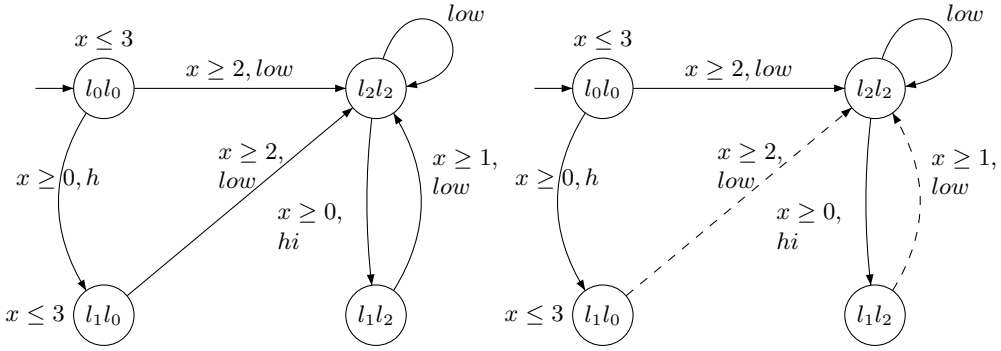

Fig. 3. $\mathcal{A}' = (\mathcal{A}|\mathcal{A}_{\setminus \Sigma_{priv}})_f$ and A''

Let us consider the algorithm 23 where $R_{\setminus \Sigma_{priv}}(X) = \{q \in X \mid \exists q_0 \in Q_0, \exists(\tau_i) \in (\mathbb{R}_{\geq 0})^n,\ \exists(low_i) \in (\Sigma_{pub})^n,\ q_0 \xrightarrow{\tau_1} q_1 \xrightarrow{low_1} q'_1 \cdots \xrightarrow{low_n} q'_n = q \wedge \forall i,\ q_i, q'_i \in X\}$ is the set of states that are reachable only by elapsing of time or low level actions (Σ_{pub}) such that all intermediary states remain in X, $Pred_{\Sigma^*_{priv}}(X) = \{q \in Q \mid q \xrightarrow{\rho}, \rho \in \Sigma^*_{priv}\}$ is the set of predecessors of X by a sequence of discrete controllable transitions (Σ_{priv}), $Pred_{low}(X) = \{q \in Q \mid \exists q' \in X\ q \xrightarrow{low} q', low \in \Sigma_{pub}\}$, is the set of discrete predecessors of X by an uncontrollable transition, $Pred^Y_{\Sigma_{priv}}(X) = \{q \in Y \mid q \xrightarrow{hi_1} q_1 \xrightarrow{hi_2} q_2 \ldots \xrightarrow{h_n} q_n \wedge q, q_1, \ldots q_n \in Y \ \wedge \forall i,\ hi_i \in \Sigma_{priv}\}$ is the set of predecessors of X by a sequence of discrete controllable transitions such that all intermediary states remain in Y, $\pi(X)$ is the classical controllable predecessor operator [MPS95,AT02,Tri98] (see appendix B) and $Sim(X, Y) = \{q \in X \mid \exists q' \in Y q \sqsubseteq q'\}$ is the set of states X similar to Y.

Definition 23 (Algorithm *Alg*). *We note Alg the following fix-point algorithm:*

1: $X_0 \leftarrow SiSt(\mathcal{A}')$
2: ***repeat***
3: $\quad X_{i+1} \leftarrow \pi(X_i)$
4: $\quad X_{i+1} \leftarrow Sim(X_{i+1}, R_{\setminus \Sigma_{priv}}(X_{i+1}))$
5: $\quad$ ***for all*** $l \in \Sigma_{pub}$ ***do***
6: $\quad\quad Y \leftarrow Pred_{\Sigma^*_{priv}}(Pred_l(X_{i+1}))$
7: $\quad\quad Z \leftarrow Pred^{X_{i+1}}_{\Sigma^*_{priv}}(Pred^{X_{i+1}}_l(X_{i+1}))$
8: $\quad\quad X' \leftarrow X_{i+1} \setminus (Z \setminus Y)$
9: ***until*** $X' = X_i$

Proposition 2. *If Alg converges, we note X^* the solution. The TTS induced by X^* on $\mathcal{S}_{\mathcal{A}''}$ is SCNNI.*

Proof. We have to prove that $(\mathcal{S}^{X^*}_{A''})_{/\Sigma_{priv}} \sqsubseteq_{\mathcal{W}} (\mathcal{S}^{X^*}_{A''})_{\setminus \Sigma_{priv}}$.

Let $q \in Q^{\mathcal{S}^{X^*}_{A''}}$. According to line 4 of the algorithm, $\exists q' \in Q^{\mathcal{S}^{X^*}_{A''} \setminus \Sigma_{priv}}$ such that $q \sqsubseteq q'$. It there exists a firing sequence $q \xrightarrow{hi_1 \ldots hi_n} s \xrightarrow{low_1} r$ then $q \sqsubseteq s$ (and so $q' \sqsubseteq s$) and $\exists r' \in Q^{\mathcal{S}^{X^*}_{A''} \setminus \Sigma_{priv}}$ such that $r \sqsubseteq r'$ (line 4). We also have with lines 5–8, $s, r \in X^*$. Since $s \xrightarrow{low_1} r$ and $q' \sqsubseteq s$, $q' \xrightarrow{low_1} r'$. So $q' \xrightarrow{low_1} r'$ and $r \sqsubseteq r'$. Consequently, q and q' fulfill the weak timed simulation (by replacing all hi_i by ϵ).

The proof would be similar for continuous transitions.

Proposition 3. *The algorithm Alg terminates.*

Proof. The convergence of the algorithm is ensured by the *region graph* $\mathcal{R}^*$ [AD94]: the family sequence (X_i) is monotone ($X_{i+1} \subseteq X_i$) over a finite domain $\mathcal{R}^*$.

Consequently, propositions 2 and 3 prove our theorem 6, that is: Timed-CSNNI control problem is decidable and a controller is computable. Since the synchronization function (f_c) is total, the TTS solution given by the algorithm can be both interpreted as the system in closed-loop and the controller for the system (as for safety control problem on TA).

The method is illustrated on a simple example in appendix C.

5 Conclusion and future works

In this paper we have reformulated SNNI in dense time setting for four semantics of Security Timed Automata and addressed the decidability issues of their associate verification problem. We have also addressed, for the first time, the control synthesis problem for Timed CSNNI and Timed StSNNI and, in each cased, provided algorithms computing an associated controller.

In the following we would like to highlight four specific aspects we intend to focus our attention on, in view of further developments: Timed BSNNI controller, verification and controller synthesis for Timed BNDC and timed intransitive non interference and timed control with partial observability.

Control synthesis techniques for Timed BSNNI. Of course it remains to extend control synthesis to Timed BSNNI to complete the picture depicted in this paper

Proof and control synthesis techniques for Timed BNDC. In [FG01] it is proposed *Bisimulation-based nondeducibility on Composition* (BNDC) as the most natural untimed information flow property: a system $\mathcal{S}$ satisfies BNDC if for any private level user Π, the public behavior of $\mathcal{S}$ is not affected by its interaction with Π. A next issue is the extension to a dense time reformulation of BNDC in our theory together with related proof and control synthesis techniques.

Timed intransitive non interference control synthesis. Another important issue is the extension to dense time reformulation of *intransitive non interference*. Indeed, absence of information flow is rarely very interesting as a description of confidentiality, as many practical applications are intended to preserve confidentiality, but nonetheless leak information. A clever and complete development of channel control can be found in [Rus92] for the deterministic case. Channel control is formulated therein in terms of noninterference in which the interference relation over the set of security levels is intransitive. This has been characterized in [HALL$^+$04] using notions and techniques from the observability theory of supervisory control of Discrete Event System (DES) as introduced by Lin and Wonham [LW88]. A nondeterministic generalization for intransitive non interference has been proposed in [Mul00].

Timed non interference control synthesis with partial observability. Depending on the nature of the plant, the non-controllable actions could be observable (*full observability*) or only a proper subset (*partial observability*) may be observable by the controller. In the timed setting, partial observability assumption applies not only to uncontrollable actions but also to the clocks of the security system.

References

[AD94] R. Alur and D.L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[AIPP00] Luca Aceto, Anna Ingólfsdóttir, Mikkel Lykke Pedersen, and Jan Poulsen. Characteristic formulae for timed automata. *RAIRO - Theoretical Informatics and Applications*, 34(6):565–584, 2000.

[AT02] K. Altisen and S. Tripakis. Tools for controller synthesis of timed systems. In *RT-TOOLS'02*, 2002.

[BT03] R. Barbuti and L. Tesei. A decidable notion of timed non-interference. *Fundamenta Informaticae*, 54:137–150, 2003.

[DM02] D. D'Souza and P. Madhusudan. Timed control synthesis for external specifications. In *Proc. STACS '02*, number 2285 in LNCS, 2002.

[FG01] Riccardo Focardi and Roberto Gorrieri. Classification of security properties (part I: Information flow). In Riccardo Focardi and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design I: FOSAD 2000 Tutorial Lectures*, volume 2171 of *Lecture Notes in Computer Science*, pages 331–396, Heidelberg, 2001. Springer-Verlag.

[FS00] Edward W. Felten and Michael A. Schneider. Timing attacks on web privacy. In *CCS '00: Proceedings of the 7th ACM conference on Computer and communications security*, pages 25–32, New York, NY, USA, 2000. ACM Press.

[HALL+04] N. Ben Hadj-Alouane, S. Lafrance, F. Lin, J. Mullins, and M. Yeddes. Characterizing intransitive non-interference in security policies with observability. *IEEE Trans. on Automatic Control*, 2004.

[LLW95] François Laroussinie, Kim G. Larsen, and Carsten Weise. From timed automata to logic – and back. In Jirí Wiedermann and Petr Hájek, editors, *Proceedings of the 20th International Symposium on Mathematical Fundations of Computer Science (MFCS'95)*, volume 969 of *Lecture Notes in Computer Science*, pages 27–41, Prague, Czech Republic, August 1995. Springer.

[LW88] F. Lin and W. M. Wonham. On observability of discrete-event systems. *Information Sciences*, 44:173–198, 1988.

[MPS95] Oded Maler, Amir Pnueli, and Joseph Sifakis. On the synthesis of discrete controllers for timed systems. In E.W. Mayr and C. Puech, editors, *Proc. STACS '95*, number 900 in LNCS, pages 229–242. Springer–Verlag, 1995.

[Mul00] J. Mullins. Nondeterministic admissible interference. 6(11):1054–1070, 2000.

[RFM03] R. Gorrieri R. Focardi and F. Martinelli. Real-time information flow analysis. *IEEE Journal on Selected Areas in Communications*, 21(1):20–35, 2003.

[Rus92] J. Rushby. Noninterference, transitivity and channel-control security policies. Technical Report CSL-92-02, SRI International, Menlo Park CA, USA, december 1992.

[Tri98] Stavros Tripakis. *The analysis of timed systems in practice*. PhD thesis, Universit Joseph Fourier, Dec 1998.

[WTH91] H. Wong-Toi and G. Hoffmann. The control of dense real-time dicrete event systems. In *Proc. 30th IEEE Conf. Decision and Control*, 1527–1528, 1991.

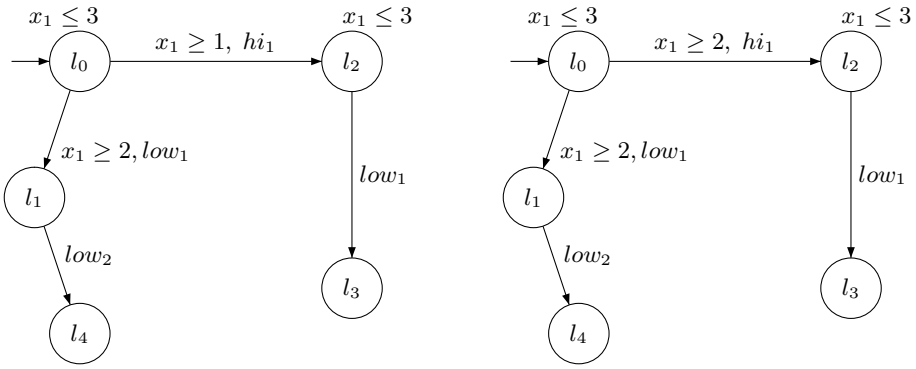

Fig. 4. Timed CSNNI : a interferent and a non-interferent TA

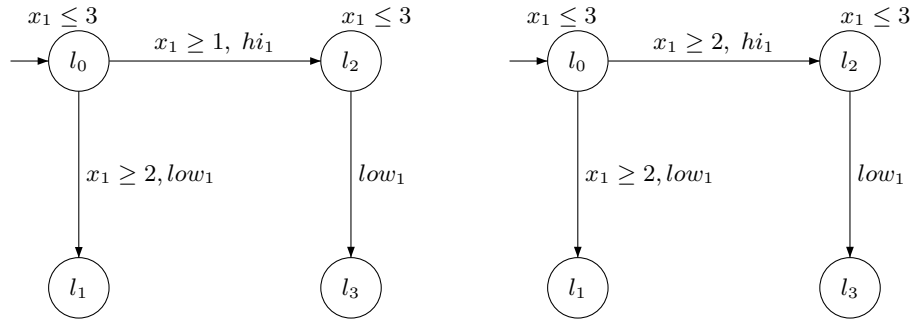

Fig. 5. Timed BSNNI : a interferent and a non-interferent TA

A An illustration of timed CSNNI and timed BSNNI

In order to show that timed CSNNI does not imply timed BSNNI, consider the Timed Automaton depicted on the right hand side of the Figure 4. It is easy to see that it is timed CSNNI. Indeed, the capability of a public observer to interact at low_1 is not correlated to the occurrence of hi_1 while such a correlation exists for the Timed Automata depicted on the left hand side of the Figure 4 and 5. Indeed any public interaction at low_1 for $1 \leq x_1 < 2$ is correlated to the occurrence of hi_1.

However, the Timed Automaton depicted on the right hand side of the Figure 4 is not timed BSNNI since a public observer after interacting with low_1 has now the capability to detect the deadlock correlated to the occurrence of hi_1. It is worthwhile to mention that this correlation has disappeared in the Timed Automaton depicted on the right hand side of the Figure 5 which is clearly timed BSNNI.

B Controllable Predecessors

Let $X \subseteq Q$ be a set of states of a Security Timed Automaton S. The set of controllable predecessors of X is defined by:

$$\pi(X) = \{q \in Qs.t.((\exists \delta \in \mathbb{R}_{\geq 0}\ \exists t \in T\ \exists q' \in X,\ q \xrightarrow{\delta} \xrightarrow{t} q') \vee (\exists \delta \in \mathbb{R}_{\geq 0}\ \exists q' \in X,\ q \xrightarrow{\delta} q'))$$
$$\wedge \forall \delta_u \in \mathbb{R}_{\geq 0} \text{ if } \exists t_u \in T_u, q'_u \notin X, q \xrightarrow{\delta} \xrightarrow{t_u} q'_u$$
$$\text{then } \exists \delta_c < \delta_u\ t_c \in T_c, \exists q'_c \in X\ q \xrightarrow{\delta_c} \xrightarrow{t_c} q'_c\}$$

Informally, q is a controllable predecessor of X iff:

- a state q' of X is reachable by time elapsing and firing of a transition,
- for any uncontrollable transition diverging from X, the controller can take a decision at an earlier date to constraint the system in X.

The controllable predecessors operator can be rewritten using the following simpler operators [Tri98,AT02]:

- $Pred_t(X) = \{q \in Qs.t.q \xrightarrow{t} q',\ q' \in X\}$, the set of all states that can lead to a state in X by the firing of the transition t.
- $Pred_T(X)$, $Pred_{T_c}(X)$, $Pred_{T_u}(X)$ respectively represent the set of discrete predecessors ($\bigcup_{t \in T} Pred_t(X)$), controllable discrete predecessors ($\bigcup_{t \in T_c} Pred_t(X)$) and uncontrollable discrete predecessors ($\bigcup_{t \in T_u} Pred_t(X)$).
- $Pred_\delta(X) = \{q \in Qs.t.\exists \delta \in \mathbb{R}_{\geq 0},\ q \xrightarrow{\delta} q',\ q' \in X\}$, the set of continuous predecessors of X.
- $while - not(X, Y) = \{q \in Qs.t.\exists \delta \in \mathbb{R}_{\geq 0}, q \xrightarrow{\delta} q', q' \in Y \text{ and } \forall \delta' < \delta,\ q \xrightarrow{\delta'} \notin X\}$, the set of continuous predecessors of Y from which there is no possibility to reach a state in X.

Then,

$$\pi(X) = Pred_\delta(X \cup Pred_T(X)) \setminus while - not(Pred_{T_c}(X), Pred_{T_u}(\overline{X}))$$

$while - not(Pred_{T_c}(X), Pred_{T_u}(\overline{X}))$ contains all the states that are time predecessors of $Pred_{T_u}(\overline{X})$ not avoidable by the firing of a controllable transition.

C CSNNI Control Problem - A simple example

Let us consider the Security Timed Automaton $\mathcal{A}$ of figure 6 and the CSNNI control problem on $\mathcal{A}$.

Following the method proposed in section 4.2.2, we compute $\mathcal{A}' = (\mathcal{A}|\mathcal{C})_{\{\rfloor}$. $\mathcal{A}'$ is represented in figure 7. We are then able to compute $Q^{\mathcal{A}'}$ (table C).

Given $Q^{\mathcal{A}'}$ and $\mathcal{A}''$ we can then compute $SiSt(\mathcal{A}')$(table C. For instance, at state $(l_2, l_0, x_1 = 1)$ the firing of low_1 is possible for $\mathcal{A}''$ while it is not possible for the state $(l_0, x_1 = 1)$ in $\mathcal{A}'$. So this state must be discarded. The aim of the controller will be to prevent this state to be reachable.

The solution of the algorithm 23 is the set of states of table C which can be transformed into the Timed Automaton of the figure 9.

Localities	Clock Space
$l_0 l_0$	$x_1 \leq 3$
$l_1 l_1$	$x_1 \geq 2$
$l_4 l_4$	$x_1 \geq 2$
$l_2 l_0$	$1 \leq x_1 \leq 3$
$l_3 l_1$	$2 \leq x_1$
$l_5 l_1$	$1 \leq x_1$

Table 1. $Q^{\mathcal{A}'}$

Localities	Clock Space
$l_0 l_0$	$x_1 \leq 3$
$l_1 l_1$	$x_1 \geq 2$
$l_4 l_4$	$x_1 \geq 2$
$l_2 l_0$	$2 \leq x_1 \leq 3$
$l_3 l_1$	$1 \leq x_1$
$l_5 l_1$	$1 \leq x_1$
bad	$\emptyset$

Table 2. $SiSt(\mathcal{A}')$

Localities	Clock Space
$l_0 l_0$	$x_1 \leq 3$
$l_1 l_1$	$x_1 \geq 2$
$l_4 l_4$	$x_1 \geq 2$
$l_2 l_0$	$2 \leq x_1 \leq 3$
$l_3 l_1$	$2 \leq x_1$
$l_5 l_1$	$\emptyset$
bad	$\emptyset$

Table 3. Solution of control algorithm 23

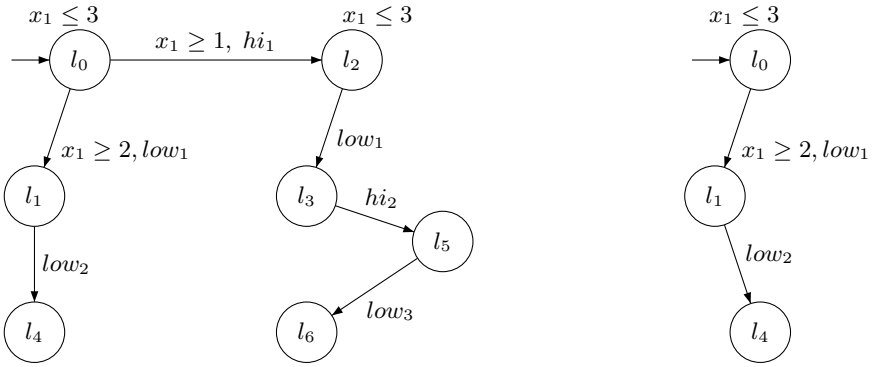

Fig. 6. Control example :$\mathcal{A}$ and $\mathcal{A}_{\setminus \Sigma_{priv}}$

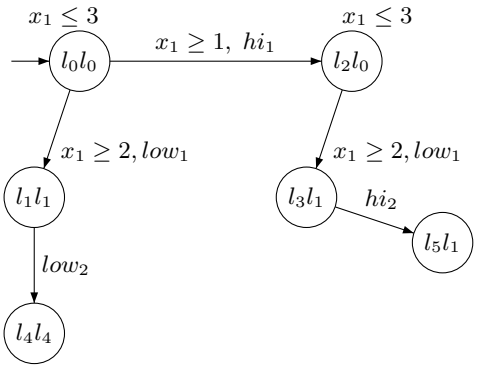

Fig. 7. Control example : $\mathcal{A}'$

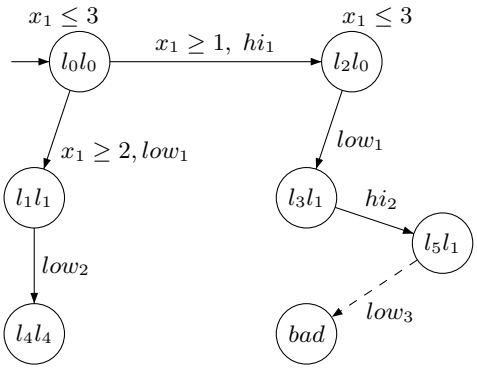

Fig. 8. Control example : $\mathcal{A}''$

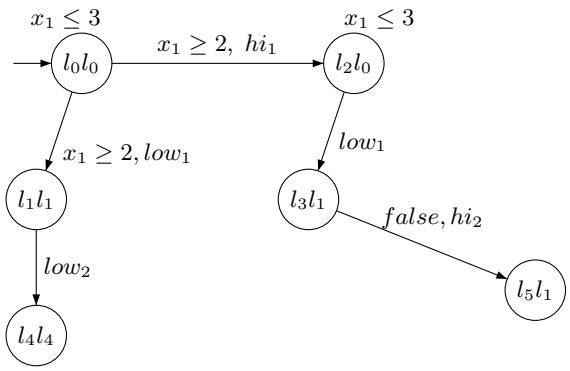

Fig. 9. Solution of the CSNNI control problem on $\mathcal{A}$