Time and Probability based Information Flow Analysis

Angelo Troina

Dipartimento di Informatica, Università di Pisa, Italy

Joint work with:
Ruggero Lanotte (University of Insubria at Como)
Andrea Maggiolo Schettini (University of Pisa)

Outline

- **Multilevel Security**
  - Non-Interference [Goguen and Meseguer,1982]
- **The Model**
  - Probabilistic Timed Automata
  - Weak Bisimulation for Probabilistic Timed Automata
- **Information Flow Analysis**
  - Probabilistic and/or Timed Security Properties

Security in Multilevel Systems

- **General setting**: a multilevel system, i.e. a system of interacting agents where every agent is confined in a bounded security level.
- **Access rules**: can be imposed to control direct unwanted transmissions from higher levels to lower levels.
- **Covert channels**: information could be transmitted from higher levels to lower levels by using system side effects.
- **Aim**: to control the whole flow of information
- **Non-interference**: low level agents are not able to deduce anything about the activity of high level agents.

Non-deterministic systems

- J. A. Goguen, J. Meseguer: *Security Policy and Security Models*. Proc. of Symp. on Research in Security and Privacy, IEEE CS Press, 11–20, 1982.
- D. McCullough: *Noninterference and the Composability of Security Properties*. Proc. of Symp. on Research in Security and Privacy, IEEE CS Press, 177–186, 1988.
- R. Focardi, R. Gorrieri: *A Classification of Security Properties*. Journal of Computer Security 3, 5–33, 1995.

Timed systems

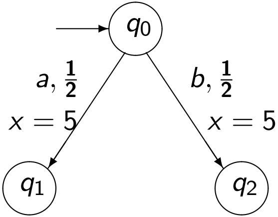
- R. Focardi, R. Gorrieri, F. Martinelli: *Information Flow Analysis in a Discrete-Time Process Algebra*. Proc. of 13th CSFW, IEEE CS Press, 170–184, 2000.
- N. Evans, S. Schneider: *Analysing Time Dependent Security Properties in CSP Using PVS*. Proc. of Symp. on Research in Computer Security, Springer LNCS 1895, 222–237, 2000.
- R. Barbuti, L. Tesei: *A Decidable Notion of Timed Non-interference*. Fundamenta Informaticae 54, 137–150, 2003.

Probabilistic systems

- J. W. Gray III. *Toward a Mathematical Foundation for Information Flow Security*. Journal of Computer Security 1, 255–294, 1992.
- A. Aldini, M. Bravetti, R. Gorrieri: *A Process-algebraic Approach for the Analysis of Probabilistic Non-interference*. Journal of Computer Security 12, 191–245, 2004.
- A. Di Pierro, C. Hankin, H. Wiklicky: *Approximate Non-Interference*. Journal of Computer Security 12, 37-82, 2004.

The Model of PTA

A Probabilistic Timed Automaton (PTA) is $A = (\Sigma, X, Q, q_0, \delta, \pi)$.



A *configuration* of a PTA is a pair $s = (q, v)$, where $q \in Q$ is a state, and v is a valuation over X.

Weak Bisimulation of Probabilistic Timed Automata

A *weak bisimulation* is a bisimulation which does not take care of internal moves.

For a PTA $A = (\Sigma, X, Q, q_0, \delta, \pi)$ a *weak bisimulation* is an equivalence relation $\mathcal{R}$ such that, for all $(s, s') \in \mathcal{R}$ and equivalence classes $\mathcal{C}$ of $\mathcal{R}$:

$$Prob(s, \tau^*\alpha, \mathcal{C}) = Prob(s', \tau^*\alpha, \mathcal{C}) \qquad \forall \alpha \in \Sigma \cup \{\tau\} \cup \mathbb{R}^{>0}$$

Two configurations s, s' are *weak bisimilar* ($s \approx s'$) iff $(s, s') \in \mathcal{R}$ for some weak bisimulation $\mathcal{R}$.

Weak Bisimulation of Probabilistic Timed Automata (2)

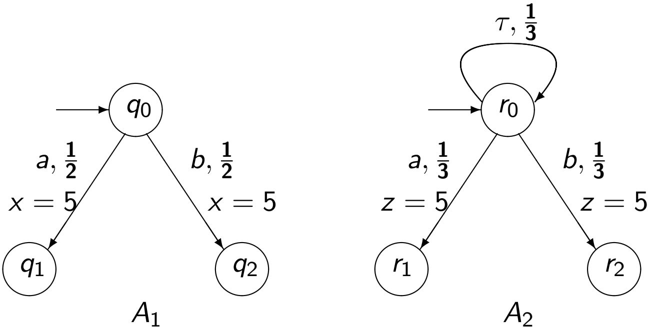


Figure: $A_1 \approx A_2$.

Auxiliary operators for Probabilistic Timed Automata

Given two PTA A_1 and A_2, $L \subseteq \Sigma$ set of synchronization actions and $p \in]0,1[$ advancing speed parameter, $A_1||_L^p A_2$ denotes the *parallel composition*. The composition is a PTA obtained by normalizing probabilities and hiding with the τ label the synchronized actions.

The *restriction* of a PTA A with respect to the set of actions L is $A \setminus L$, obtained from A by removing transitions and normalization of probabilities.

The *hiding* of a PTA A with respect to the set of actions L is A/L where each transition label $a \in L$ is replaced by label τ.

Non-interference

A system S satisfies the *Non-interference* property ($S \in NI$) if high level agents do not interfere with the observable behavior of the system from the low level point of view:

$$S \in NI \qquad \Leftrightarrow \qquad S/\Sigma_H \approx S \setminus \Sigma_H$$

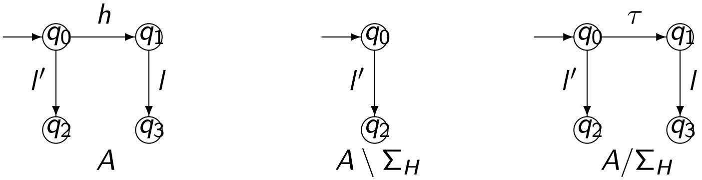
where Σ_H is the set of high level actions.

(The observable behavior of the isolated system is bisimilar to the behavior of the system which communicates with high level agents in an invisible manner for the low agent point of view).

Proposition. It is decidable to check whether a system S satisfies the NI property.

Non-deterministic Non-interference

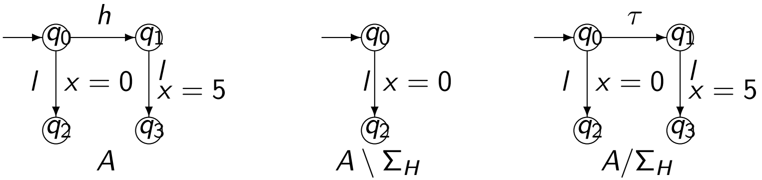
An example of non-deterministic covert channel.



The high level action h interferes with the observation of the action l. In $A \setminus \Sigma_H$ the low level agent observes only the execution of l, whereas, in A/Σ_H also action l' may be observed. A low level agent, observing the event l knows that action h has occurred.

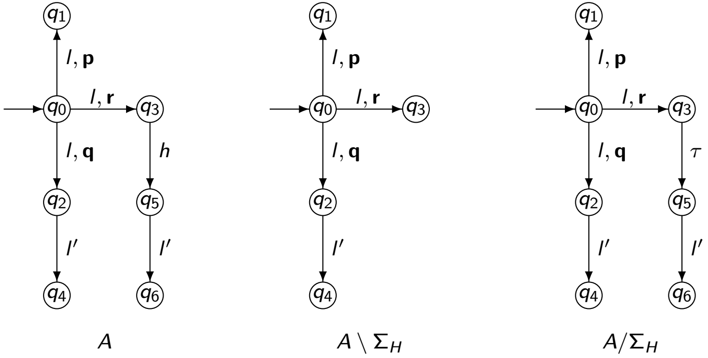
Timed Non-interference

An example of timing covert channel.



The high level action h interferes with the time of observing the action l. In $A \setminus \Sigma_H$ the low level agent observes l executed immediately, whereas, in A/Σ_H l could either be observed immediately or when the clock x reaches value 5. A low level agent, observing the event l when clock x has value 5 knows that action h has occurred.

Probabilistic Non-interference



$A \setminus \Sigma_H$: l is obsevred with probability $\mathbf{p} + \mathbf{r}$, ll' with probability $\mathbf{q}$.

A / Σ_H: l is observed with probability $\mathbf{p}$, ll' with probability $\mathbf{r} + \mathbf{q}$.

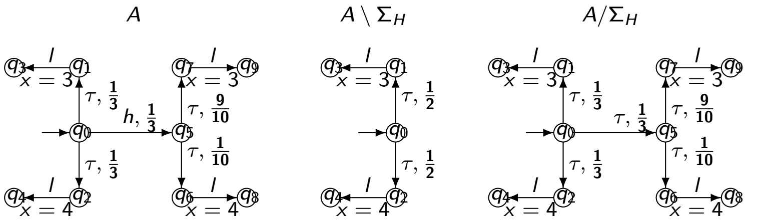
A Classification of Quantitative Security Properties

Given NNI, TNI, PNI and PTNI be non-interference properties defined for the models of non-deterministic automata, timed automata, probabilistic automata and probabilistic timed automata, respectively, the following implications hold:

- $A \in PNI \Rightarrow unprob(A) \in NNI$
- $A \in TNI \Rightarrow untime(A) \in NNI$
- $A \in PTNI \Rightarrow unprob(A) \in TNI \wedge untime(A) \in PNI$.

A Classification of Quantitative Security Properties (2)

$\exists A : A \notin PTNI \wedge unprob(A) \in TNI \wedge untime(A) \in PNI$



$A \setminus \Sigma_H$: l when $x = 3$ or when $x = 4$ with probability $\frac{1}{2}$.
A/Σ_H: l when $x = 3$ with probability $\frac{19}{30}$, l when $x = 4$ with probability $\frac{11}{30}$.

A Classification of Quantitative Security Properties (3)

The following diagram summarizes our results.

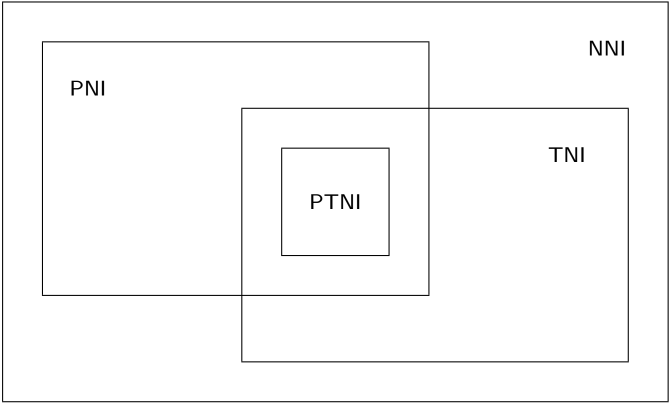


Figure: Relations among Non-Interference security properties.

Non Deducibility on Composition

A system S satisfies the *Non Deducibility on Composition* (NDC) if the system in isolation has not to be altered when considering all the potential interactions with the high level agents of the external environment, formally:

$$S \in NDC \;\Leftrightarrow\; \forall \Pi \in \Gamma_H, \forall p \in]0,1[,\; \forall L \subseteq \Sigma_H$$
$$S/\Sigma_H \approx (S||^p_L \Pi) \setminus \Sigma_H$$

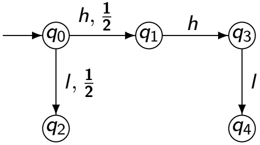
where Γ_H is the set of high level agents.

(The observable behavior of the isolated system is bisimilar to the behavior of the system communicating with the high level agent Π in an invisible manner for the low agent point of view).

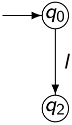
Note. Decidability of NDC depends on the possibility of reducing all the high level automata in Γ_H to a finite case for the particular automaton S considered.

Non Deducibility on Composition (2)

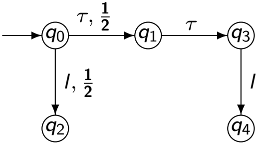
Theorem. $S \in mNDC \Rightarrow S \in mNI$.



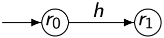
A



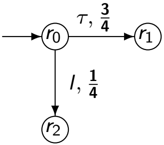
$A \setminus \Sigma_H$



A/Σ_H



Π



$(A||^p_L\Pi) \setminus \Sigma_H$

A is $PTNI$ secure, since $A/\Sigma_H \approx A \setminus \Sigma_H$. But A is not $PTNDC$ secure as $(A||^p_L\Pi) \setminus \Sigma_H$ reaches with probability $\frac{3}{4}$ a state where it cannot perform any visible action.

A Classification of Quantitative Security Properties(4)

Given NNDC, TNDC, PNDC and PTNDC be non-deducibility on composition properties defined for the models of non-deterministic automata, timed automata, probabilistic automata and probabilistic timed automata, respectively, the following implication holds:

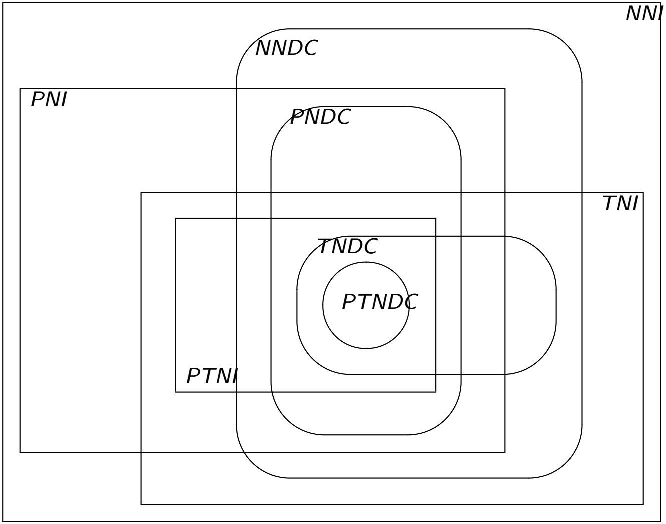
$A \in PTNDC\ (PNDC,\ TNDC,\ NNDC) \Rightarrow A \in PTNI\ (PNI,\ TNI,\ NNI)$.

Moreover, as for the NI properties, we have that:

- $A \in PNDC \Rightarrow unprob(A) \in NNDC$;
- $A \in TNDC \Rightarrow untime(A) \in NNDC$;
- $A \in PTNDC \Rightarrow unprob(A) \in TNDC \wedge untime(A) \in PNDC$.

and that $\exists A : A \notin PTNDC \wedge unprob(A) \in TNDC \wedge untime(A) \in PNDC$.

A Classification of Quantitative Security Properties (5)



Observations and Future Work

- Introduce an approximated notion of weak bisimulation for PTA.
- We can formulate other well known information flow security properties within our framework.
- Extend the model with cryptographic primitives in order to analyze security protocols.
- Develop an automatic technique to "adjust" unsecure systems.

Bibliography

[1] R. Lanotte, A. Maggiolo-Schettini, A. Troina
A Classification of Time and/or Probability Dependent Security Properties
Proc. QAPL'05, Elsevier ENTCS, to appear.
[2] R. Lanotte, A. Maggiolo-Schettini, A. Troina
Information Flow Analysis for Probabilistic Timed Automata
Proc. FAST'04, Springer IFIP series 173, pp. 13–27, 2004.
[3] R. Lanotte, A. Maggiolo-Schettini, A. Troina
Weak Bisimulation for Probabilistic Timed Automata and Applications to Security
Proc. SEFM'03, IEEE Computer Society Press, pp. 34–43, 2003.