Università degli Studi di Napoli Federico II

Carlo Motta

Security Assessment and Enforcement Strategies for Event-Driven Cyber-Physical Systems

Tutor: Prof. G. De Tommasi

co-Tutor: Prof. S. Santini

Cycle: XXXVI

Year: 2024

Background information

- **MSc degree in Automation Engineering, University of Naples Federico II**
- **Working team: DAiSYLab**
- **Period Abroad: Swinburne University of Technology (SUT), Melbourne 18/10/2023 - 04/06/2024**
- **Collaboration: UniSa (Prof. Francesco Basile); DIETI (RO group)**
- **PhD start-end date: 01/11/2020 – 31/01/2024**
- **Scholarship type: "UNINA"**

Summary of study activities

During This 3 years I have been focusing my activities on dealing with Discrete Event Systems and optimization problems.

This are some of the courses I have attended:

- From observability to privacy and security in discrete event systems
- Scientific Programming and Visualization with Python
- Operational Research: Mathematical Modelling, Methods and Software Tools for Optimization Problems

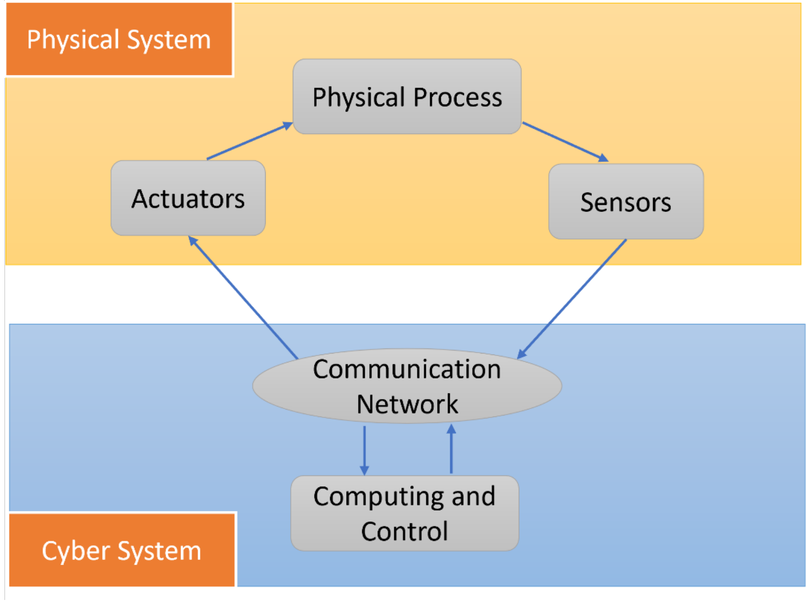
I also attended AIRO PhD school:

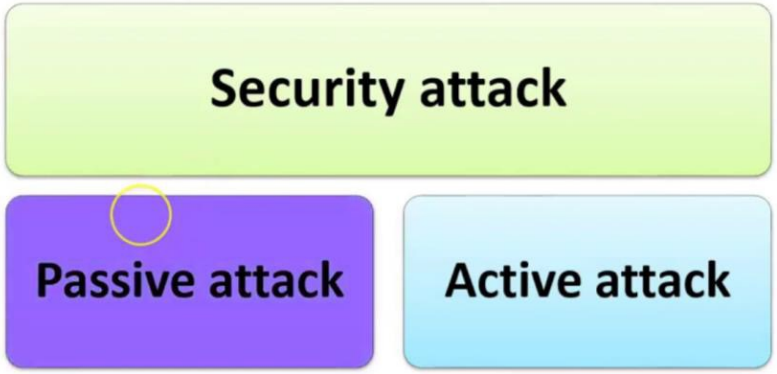
Optimization and Data Science: Trends and Applications

Cyber-Physical System

- In our modern technological society, intricate systems are prevalent, comprised of numerous intelligent elements and devices that interact through communication networks, commonly referred to as distributed Cyber-Physical Systems (CPS).

- A CPS is a complex integration of both a physical system and a cyber system, achieved through the amalgamation of physical processing, sensing, computation, communication, and control





- Given the adaptability of these CPSs in diverse environments, they are exposed to potential vulnerabilities that can be exploited by adversaries, leading to cyber attacks which have the potential to degrade system performance.

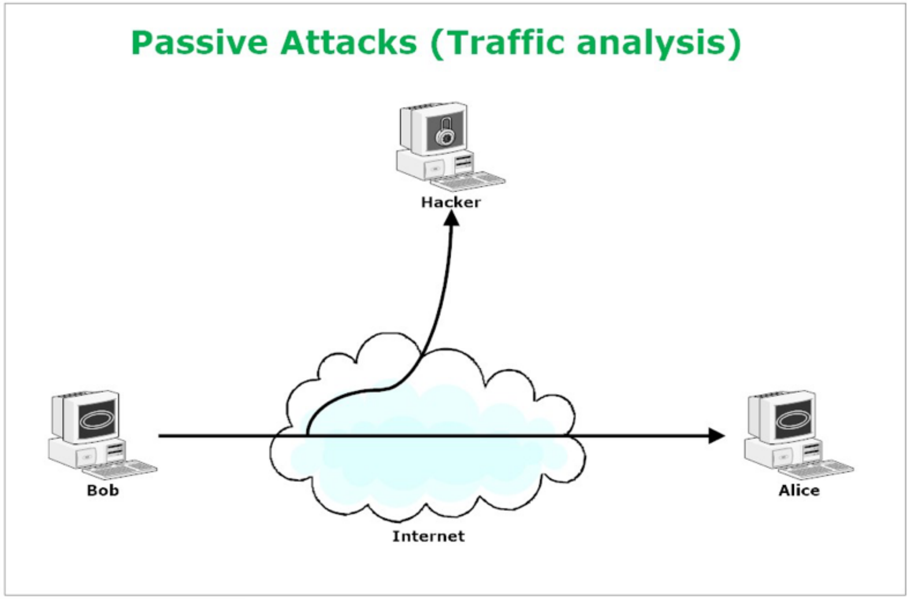
- Attacks can be divided into Passive attacks, when the objective is inferring secrets, and Active attacks, when the objective is to compromise the correct functioning.

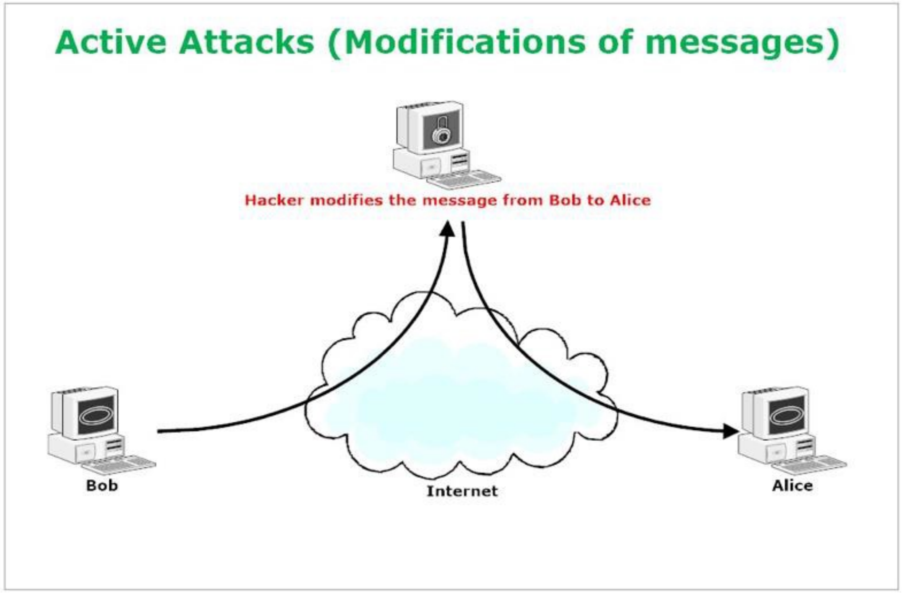
Research results

By modeling the Cyber-Physical System as a Discrete Event System, the results of the research are:

The introduction of Necessary and Sufficient conditions to conclude if a DES is resilient to passive cyber attacks in terms of opacity and non-interference

The design of supervisory control systems that are resilient (robust) to Active cyber-attacks and communication delays.




Active Attacks (Modifications of messages)
Hacker modifies the message from Bob to Alice
Bob
Internet
Alice

Research products

Journal Paper:

[J1]	F. Basile, M. Boccia, G. De Tommasi, C. Motta, C. Sterle **An optimization-based approach to assess non-interference in labeled and bounded Petri net Systems;** Nonlinear Analysis: Hybrid Systems, vol. 44, pp. 101153, 2022
[J2]	F. Basile, G. De Tommasi, C. Motta, C. Sterle **Necessary and Sufficient Condition to Assess Initial-State-Opacity in Live Bounded and Reversible Discrete Event Systems**. IEEE Control System Letters, vol. 6, pp. 2683-2688, 2022
[J3]	A. Coppola, G. De Tommasi, C. Motta, A. Petrillo, S. Santini **Double-Layer Control Architecture for Motion and Torque Optimisation of Autonomous Electric Vehicles.** Transportation Research Interdisciplinary, vol. 21, pp. 100866, 2023
[J4]	F. Basile, G. De Tommasi, C. Motta **Assessment of initial-state-opacity in live and bounded labeled Petri net systems via optimization techniques.** Automatica , vol.152, pp 110911, 2023

Research products

Conference Paper:

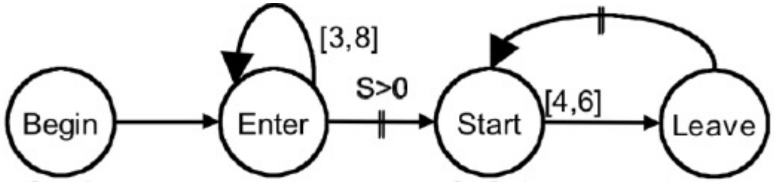
[C1]	F. Basile, G. De Tommasi, C. Motta, A. Petrillo, S. Santini **Assessment of Initial-State-Opacity in Live Bounded and Reversible Discrete Event Systems via Integer Linear Programming.** The 30th Mediterranean Conference on Control and Automation, Athens, Greece, Jul. 2022
[C2]	G. De Tommasi, C. Motta, A. Petrillo, S. Santini **Design of Resilient Supervisory Control for Autonomous Connected Vehicles Approaching Unsignalized Intersection in presence of Communication Delays.** IEEE International Conference on Networking, Sensing and Control (ICNSC), Shanghai, China, Jan. 2023
[C3]	G. De Tommasi, C. Motta, A. Petrillo, S. Santini **Design of Resilient Supervisory Control for Autonomous Connected Vehicles Approaching Unsignalized Intersection in presence of Cyber-Attacks.** International Federation of Automatic Control (IFAC), Yokohama, Japan, Sep. 2023, pp. 587-592
[C4]	G. De Tommasi, C. Motta, A. Petrillo, S. Santini **Optimization-based assessment of Initial-State Opacity in Petri Nets.** Italian Association of Operations Research - Optimization and Decision Science, AIRO Conference Naples, Italy, Aug. 2021
[C5]	R. Brancati, G. Di Massa, C. Motta, S. Pagano, A. Petrillo, S. Santini **A Test Rig for Experimental Investigation on a MRE Vibration Isolator.** The International Conference of IFToMM ITALY, Ischia, Italy, Sep. 2022

Awards:

[A1]	Third Best Paper Award - 30th Mediterranean Conference on Control and Automation (MED 2022).
[A2]	Silver Best Application Paper Award – Fourth International Conference of IFToMM Italy (2022).
[A3]	Best Emerging Technology Paper Award - IEEE Systems, Man, and Cybernetics Society – 19th IEEE International Conference on Networking, Sensing, and Control (IEEE ICNSC 2022).

PhD thesis overview

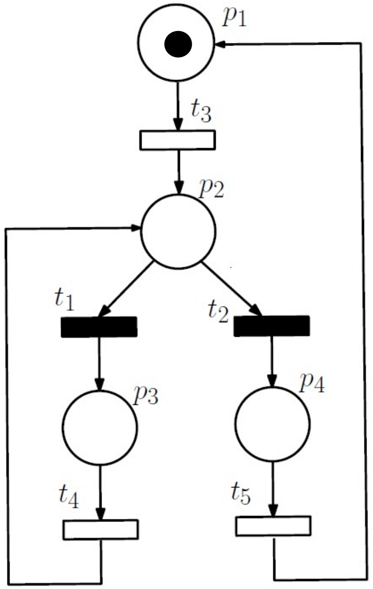
Discrete Event System (DES) is a discrete-state, event-driven dynamic system of which the state evolution depends entirely on the occurrence of asynchronous discrete events over time



Opacity is a confidentiality property that captures whether an intruder can infer a “secret”.

Passive attacks: the system is *opaque* if a user cannot infer any secret if granted a partial observation of the system.
the system’s initial state represents the *secret* →*Initial State Opacity (ISO)*

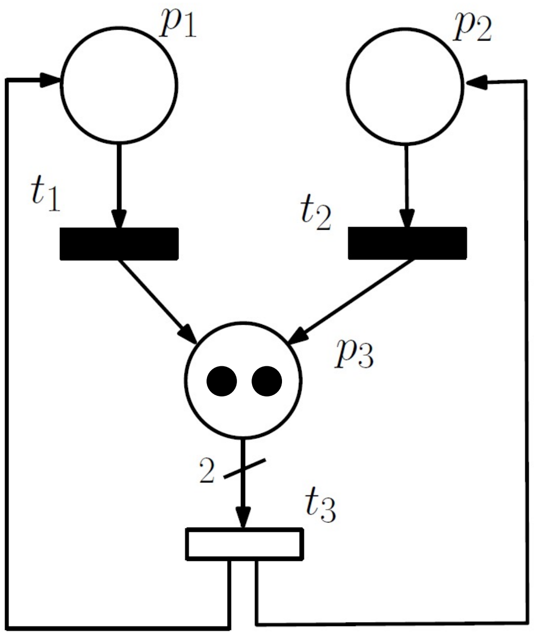
- Introduced a Necessary and Sufficient condition to conclude if a DES modeled as a Petri net (PN) is ISO based on the solution of Integer Linear Programming Problems.



Initial Stat Opacity (ISO)

Initial-state opacity property is a state property that relates to the membership of the system's initial state within a set of secret states. The system is initial-state opaque if the observer is never sure whether the system's initial state is a secret state or not.

Among the different Discrete Event System modeling tools, we decided to use Petri Nets (PNs)



The PN is defined by the 4-tuple N= (P ,T , Pre, $Post$):
P: the set of «p» places (represented by circles);
T: the set of «t» transitions (represented by boxes);
Pre: the pre-incidence matrix of dimensions (p,t), a transition is enabled when $m \geq Pre(\cdot,t_i)$;
$Post$: the post-incidence matrix of dimensions (p,t).

$$m' = m + Post(\cdot,t) - Pre(\cdot,t) = m + C(\cdot,t)$$

Initial Stat Opacity (ISO)

Opacity is a confidentiality property that captures whether an intruder can infer a “secret”.

Initial-state opacity property is a state property that relates to the membership of the system’s initial state within a set of secret states. The system is initial-state opaque if the observer is never sure whether the system’s initial state is a secret state or not.

Among the different Discrete Event System modeling tools, we decided to use Petri Nets (PNs)

The PN is defined by the 4-tuple N= (P ,T , Pre, $Post$):
P: the set of «p» places (represented by circles);
T: the set of «t» transitions (represented by boxes);
Pre: the pre-incidence matrix of dimensions (p, t), a transition is enabled when $m \geq Pre(\cdot, t_i)$;
$Post$: the post-incidence matrix of dimensions (p, t).

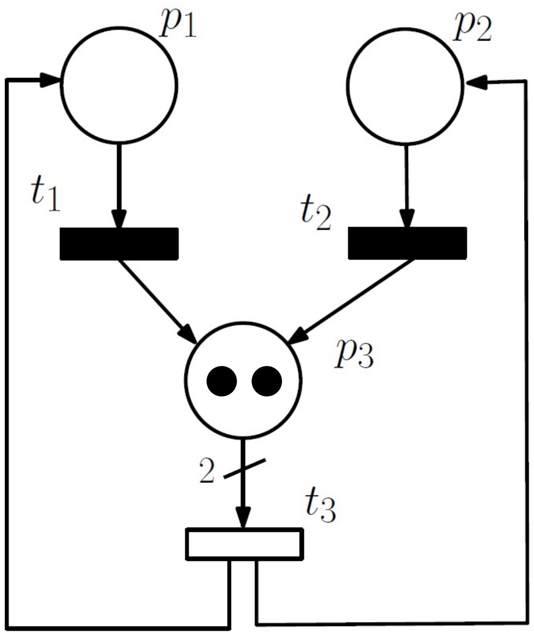
$$m' = m + Post(\cdot, t) - Pre(\cdot, t) = m + C(\cdot, t)$$

We can extend the concept by introducing firing sequenceces σ and the firing count vector $\vec{\sigma}$:

$$\sigma = t_3 t_1 \qquad \vec{\sigma} = [1 \quad 0 \quad 1]^T$$

$$m' = m_0 + C \cdot \vec{\sigma}$$

$$m' = \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & 1 & -2 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$



Initial Stat Opacity (ISO)

The information we want to hide is a Secret Initial marking

First let us introduce some notations:

- Unobservable Transitions T_{uo}: Is the set of transitions whose firing cannot be seen by an outside observer. $T = T_o \cup T_{uo}, \quad T_o \cap T_{uo} = \emptyset$

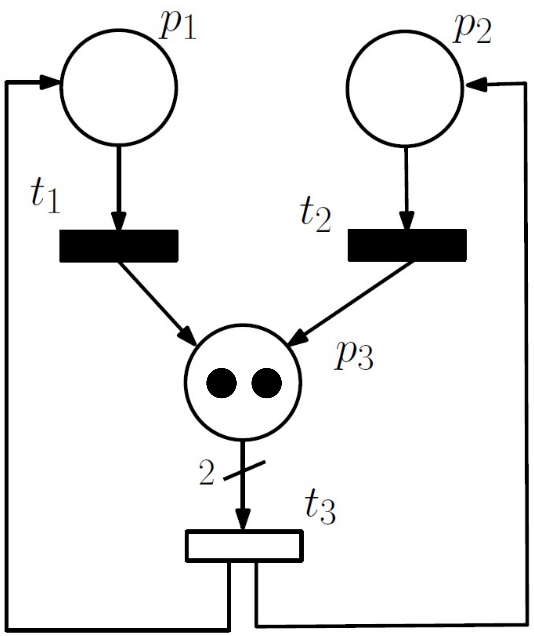
  Pre_o (Pre_{uo}) is the pre-incidence matrix restricted to observable (unobservable) transitions. The same applies for $Post_o$ $(Post_{uo})$and $C_0(C_{uo})$

- Language: A language is the set of finite-length strings formed from transitions in T.

$$L = \{t_3, t_3t_1, t_3t_2t_1\}$$

- Projection: The vector obtained from L by removing all the unobservable components.

$$\Pr(L) = \{\epsilon, t_1, t_2t_1\}$$



- T-invariant: It is a sequence $\vec{y}$ whose occurrence generates a null net marking variation $(C\vec{y} = 0)$

$$\vec{y} = \{t_{1,} t_2, t_3\} = (1\ 1\ 1)'$$

Initial Stat Opacity (ISO)

Garcia-Valles Constraints (1998):

There exists ρ integer vectors $\vec{s}_1, \ldots, \vec{s}_\rho \in N^n$ with $\rho \leq |\sigma|$ such that the following linear constraints are fulfilled.

$$\vec{m}_0 \geq Pre \cdot \vec{s}_1$$
$$\vec{m}_0 + C \cdot \vec{s}_1 \geq Pre \cdot \vec{s}_2$$
$$\ldots$$
$$\vec{m}_0 + C \cdot \sum_{i=1}^{\rho} \vec{s}_i \geq Pre \cdot \vec{s}_2$$
$$\sum_{i=1}^{\rho} \vec{s}_i = \pi(\sigma)$$

if and only if there exists at least one sequence σ, which is enabled under the marking $\vec{m}_0$

A system with uncertain initial state belonging to M_0 is ISO <u>if and only if</u>

$$\forall \vec{m}_s \in M_S \; and \; \forall \sigma \in L(N, \vec{m}_s) \; \exists \, \vec{m}_{ns} \in M_{ns} \; and \; \exists \, \sigma' \in L(N, \vec{m}_{ns}) \quad s.t.$$
$$\Pr(\sigma) = \Pr(\sigma')$$

Mathematical Characterization

$\forall \vec{m}_s \in M_s$ and for each T-invariant $\vec{y} \in T$ the solution to the following ILP problem is needed to find the minimum number of firing count vectors $\vec{s}_j$ that cover the observable part of the MS T-invariant:

$$\max \left\{ \sum_{j=1}^{J} \left[\boxed{(J-j+1)\cdot \sum_{\tau\in\|\vec{y}\|_o} \vec{s}_j(\tau)} + \boxed{B\cdot b_j} \right] \right\}$$

Unknown firing count vectors $\vec{\epsilon}_{s_j}$, $\vec{s}_j$ represent the unobservable and observable part of a sequence enabled from $\vec{m}_s$ for $\vec{y}$

$$\left\{\begin{array}{l}
\vec{m}_s \geq Pre_{uo}\cdot \vec{\epsilon}_{s_1} \\
\vec{m}_s + C_{uo}\cdot \vec{\epsilon}_{s_1} \geq Pre_o \cdot \vec{s}_1 \\
\vec{m}_s + C_{uo}\cdot \vec{\epsilon}_{s_1} + C_o\cdot \vec{s}_1 \geq Pre_{uo}\cdot \vec{\epsilon}_{s_2} \\
\qquad \cdots \\
\vec{m}_s + C_{uo}\cdot \sum_{j=1}^{J} \vec{\epsilon}_{s_j} + C_o \cdot \sum_{j=1}^{J-1} \vec{s}_j \geq Pre_o\cdot \vec{s}_J \\
\sum_{j=1}^{J} \vec{s}_j(\tau) \geq \vec{y}(\tau)\,, \quad \forall \tau \in T_o \\
\vec{s}_j \leq \boxed{B(1-b_j)}\cdot \vec{1}\,, \quad j=1,\dots,J \\
\vec{\epsilon}_{s_j}, \quad \vec{s}_j \in \mathcal{N}^n\,, \quad j=1,\dots,J \\
b_j \in \{0,1\}\,, \quad j=1,\dots,J
\end{array}\right.$$

Garcia-Valles constraints to check progression of the evolution. Between two observable transitions $\vec{s}_j$, it is possible to fire as many unobservable transitions $\vec{\epsilon}_{s_j}$ as needed to get to optimize the ILP problem solution

Makes the firing count vector $\vec{s}_j$ cover the observable part of $\vec{y}$

The number of not null firing count vectors $\vec{s}_j$ is minimized by the presence of the term B which is intended as a sufficiently big number

The number of firings in each not null $\vec{s}_j$ is maximized, as far as this is compatible with the enabling constraints

Mathematical Characterization

Given $\vec{s}_k^*$, **solution to the previous optimization problem**, the system is ISO ***if and only if*** this feasibility problem admits a solution

$$
\left\{
\begin{array}{l}
\vec{\mu} \geq Pre_{uo} \cdot \vec{\epsilon}_1^{\,1} \\
\vec{\mu} + C_{uo} \cdot \vec{\epsilon}_1^{\,1} \geq Pre_{uo} \cdot \vec{\epsilon}_1^{\,2} \\
\dots \\
\vec{\mu} + C_{uo} \cdot \displaystyle\sum_{j=1}^{J-1} \vec{\epsilon}_1^{\,j} \geq Pre_{uo} \cdot \vec{\epsilon}_1^{\,J} \\
\vec{\mu} + C_{uo} \cdot \displaystyle\sum_{j=1}^{J} \vec{\epsilon}_1^{\,j} \geq Pre_{o} \cdot \vec{s}_1^{\,\star} \\
\vec{\mu} + C_{uo} \cdot \displaystyle\sum_{j=1}^{J} \vec{\epsilon}_1^{\,j} + C_o \vec{s}_1^{\,\star} \geq Pre_{uo} \cdot \vec{\epsilon}_2^{\,1} \\
\dots \\
\vec{\mu} + C_{uo} \cdot \displaystyle\sum_{k=1}^{K} \sum_{j=1}^{J} \vec{\epsilon}_k^{\,j} + C_o \cdot \sum_{k=1}^{K-1} \vec{s}_k^{\,\star} \geq Pre_{o} \cdot \vec{s}_K^{\,\star} \\
\hline
\vec{\mu} = \displaystyle\sum_{i=1}^{card(\mathcal{M}_{ns})} \vec{m}_{ns_i} \circ (\mu_i \cdot \vec{1}) \\
\displaystyle\sum_{i=1}^{card(\mathcal{M}_{ns})} \mu_i = 1 \\
\vec{\epsilon}_k^{\,j} \in \mathcal{N}^n \,, \quad j = 1\,, \dots \,, J\,, k = 1\,, \dots \,, K \\
\mu_i \in \{0, 1\} \,, \quad i = 1\,, \dots \,, card(\mathcal{M}_{ns})
\end{array}
\right.
$$

This Garcia-Valles constraints, with alternation of observable and unobservable firing count vectors, are used to check is the firings held in each firing count vector $\vec{s}_k^*$ are then ***justified*** by the firing of $\vec{\epsilon}_k^{\,j}$ which represents the ***unobservable explanations*** starting from the non-secret initial marking $\vec{\mu}$.

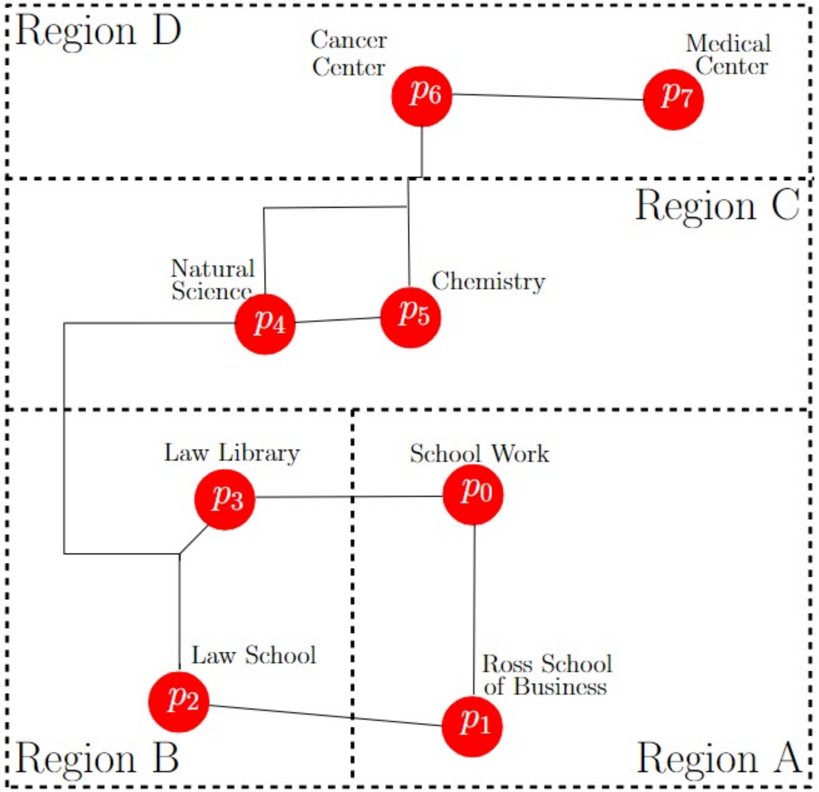
These unobservable explanations are enabled starting from one of the non-secret markings $\vec{m}_{ns_i}$, since these constraints are equivalent to an exclusive “or”, thus forcing the marking vector $\vec{\mu}$ to be equal to one of the non-secret markings.

Case Study

We can extend the result to a labeled case by by inserting new constraints to the ILP problem.

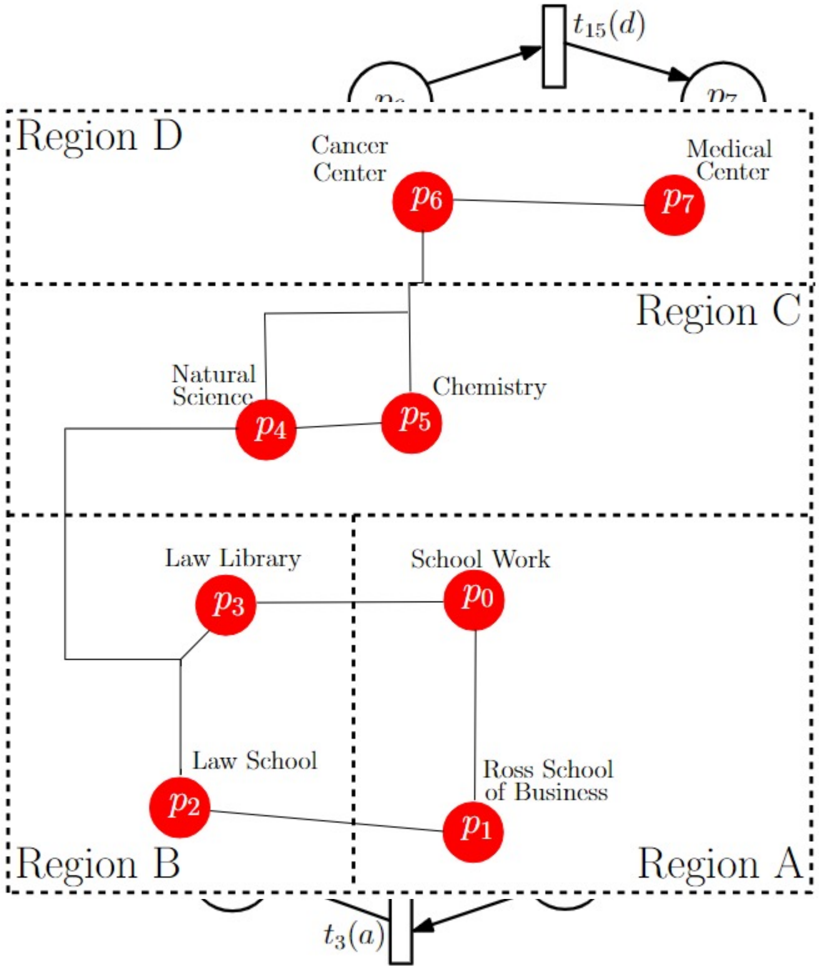
- Let us consider the campus map shown.
- The campus is covered by four coarse regions, namely A, B, C, D.
- In each region two points of interest are selected.
- People moving in the campus are traced by a Location-Based Service (LBS).

There is a privacy concern, since a malicious intruder may infer users' location by observing the events exchanged with the LBS.



Case Study

- The labeled net system models the events generated by a LBS user
- Each transition is labeled with the name of the coarse region a user is moving from, i.e. the source position.
- The events of the model are those monitored by the LBS, that can be also potentially intercepted by a malicious user.



The net is consistent; thus, it is covered by T-invariants:

$$Y' = \begin{pmatrix} \overrightarrow{y}_1^T \\ \overrightarrow{y}_2^T \\ \overrightarrow{y}_3^T \\ \overrightarrow{y}_4^T \\ \overrightarrow{y}_5^T \\ \overrightarrow{y}_6^T \\ \overrightarrow{y}_7^T \\ \overrightarrow{y}_8^T \\ \overrightarrow{y}_9^T \\ \overrightarrow{y}_{10}^T \end{pmatrix} = \begin{pmatrix} 1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \\ 1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0 \end{pmatrix} .$$

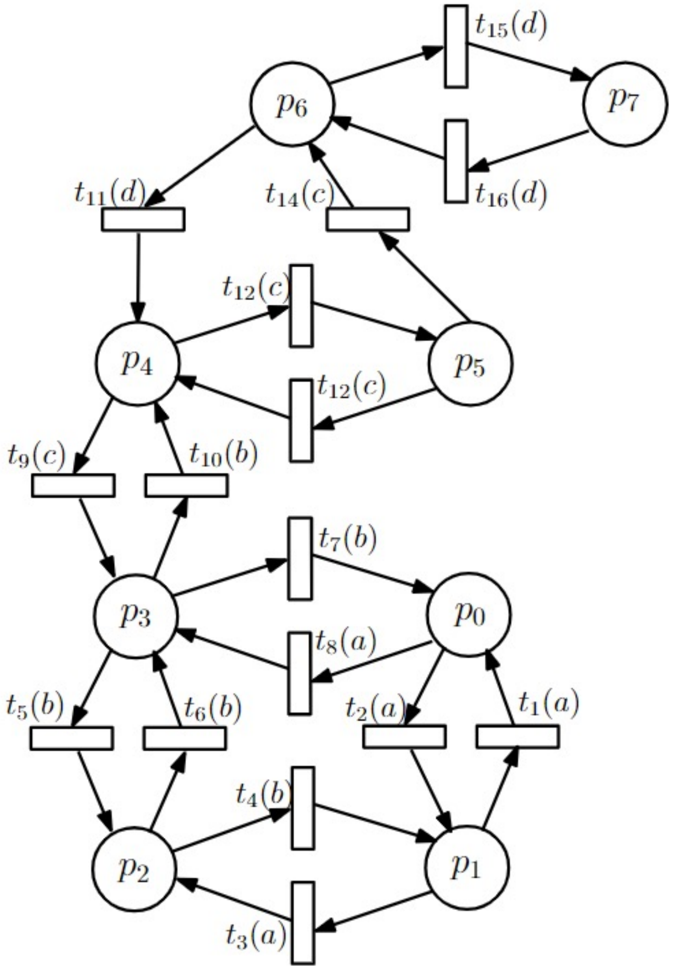
Case Study

Let us recursively select the secret marking as follows:

$$\vec{m}_{s_n}(p_i) = \begin{cases} 0, & i \neq n \quad for\ n = 1, \dots, 8 \\ 1, & i = n \end{cases}$$

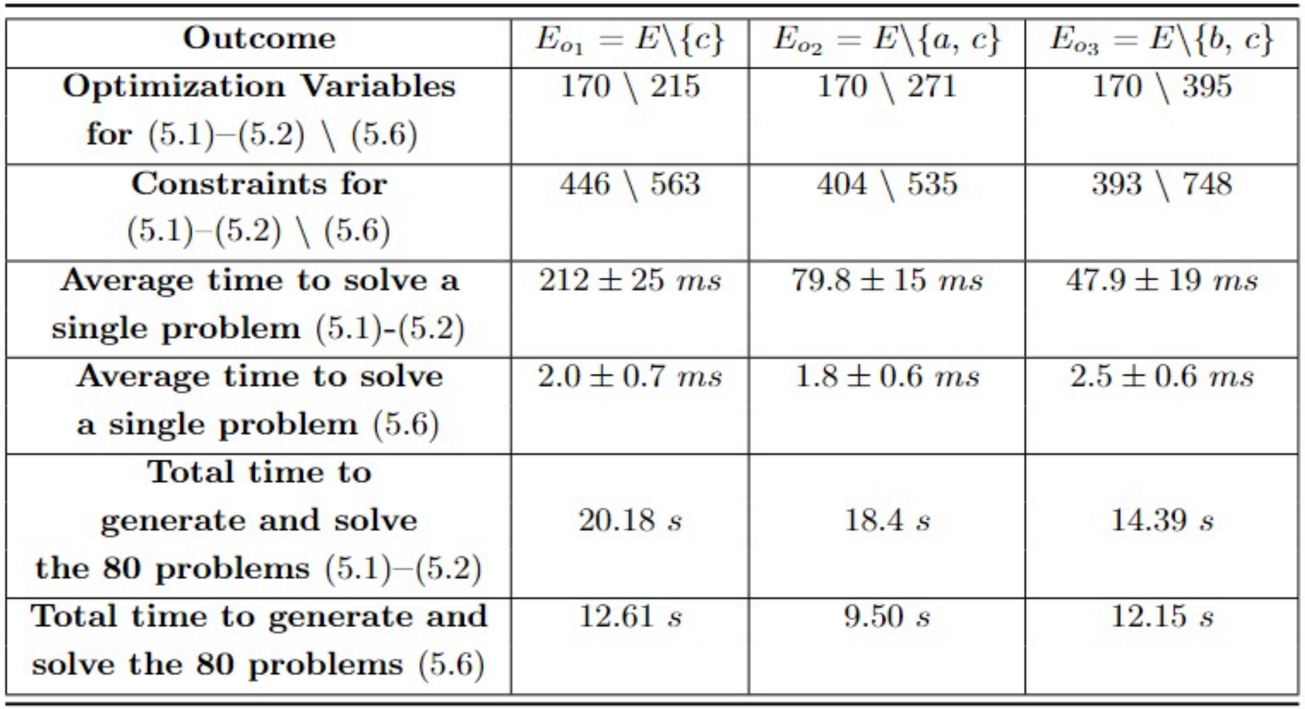
For each of those secret markings there are seven non-secret ones each of which is obtained by positioning one token in other places p_j

By selecting and selecting $E_{uo} = \{c\}$ and by applying the Theorem, the system turns out to be ***not ISO*** $\forall n \in [1,8]$.
This can be checked by considering $n = 1$ as $\sigma = a\ b\ c\ c\ d$ obtained by considering $\vec{y}_6 = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0)^T$, the projection: ($\Pr_\sigma = a\ b\ d$) cannot be mimicked when starting from any of the non-secret markings.

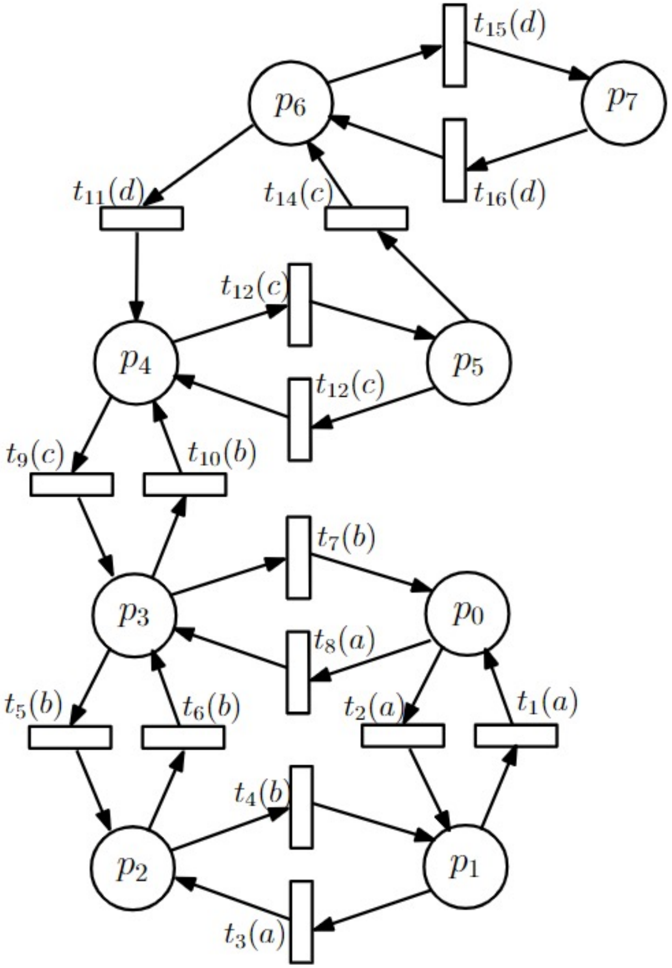


It is needed to shrink the observable subspace by letting $\boldsymbol{E_{uo1} = \{a, c\}}$ ***or*** $\boldsymbol{E_{uo2} = \{b, c\}}$

Case Study



Outcome	$E_{o_1} = E\setminus\{c\}$	$E_{o_2} = E\setminus\{a, c\}$	$E_{o_3} = E\setminus\{b, c\}$
Optimization Variables for (5.1)–(5.2) \ (5.6)	170 \ 215	170 \ 271	170 \ 395
Constraints for (5.1)–(5.2) \ (5.6)	446 \ 563	404 \ 535	393 \ 748
Average time to solve a single problem (5.1)-(5.2)	$212 \pm 25\ ms$	$79.8 \pm 15\ ms$	$47.9 \pm 19\ ms$
Average time to solve a single problem (5.6)	$2.0 \pm 0.7\ ms$	$1.8 \pm 0.6\ ms$	$2.5 \pm 0.6\ ms$
Total time to generate and solve the 80 problems (5.1)–(5.2)	$20.18\ s$	$18.4\ s$	$14.39\ s$
Total time to generate and solve the 80 problems (5.6)	$12.61\ s$	$9.50\ s$	$12.15\ s$



Conclusions

- This work has addressed the problem of designing resilient supervisor controller for managing both Active and Passive cyber attacks in Cyber-Physical Systems;

- A necessary and sufficient condition to assess ISO in labeled and unlabeled live and bounded systems has been given;

- Regarding Initial State Opacity, future lines of research include the extension of the approach to both current and initial-and-final opacity

- Future research directions could include the integration of the proposed supervisor within a more complex and hybrid control architecture.

THANKS FOR YOUR ATTENTION