Flots d’information, opacité – et quelques remarques sur le diagnostic

Béatrice Bérard

Sorbonne Université, LIP6

Based on joint work with:

MSR, 14 novembre 2019
General context: Security Properties

Information flow:
Transmission of information from a high level user to a low level user, in a possibly illegal and/or indirect way.

A class of Security Properties:

Goals:
Enforce those properties. [Lafortune 12-19, with many co-authors], [Marchand 11-15, with many co-authors], [Tong, Ma, Li, Seatzu, Giua 16].
visit to a red state is hidden from observer

observing $ad^*$ discloses a visit

$acd^*$ is ambiguous
Partially Observable System

- Visit to a red state is hidden from observer
- Observing $ad^*$ discloses a visit
- $acd^*$ is ambiguous

Goals: hide or detect information

- Opacity: the visit is a secret which must be kept
  [Bryans et al. 08]
- Diagnosis: the visit is a faulty event which must be detected
  [Sampath et al. 95]

No black box: Observer knows the system
Outline

Qualitative properties of Diagnosability and Opacity

Rational Information Flow Properties

Probabilistic Disclosure
  Probabilistic disclosure for Markov Chains
  Disclosing a secret under strategies
A common framework

A system with set $L$ of behaviours

- A subset $M \subseteq L$ with $\overline{M} = L \setminus M$,
- An external agent observing the system via a function $O$ on $L$.

Requirements: ordering ambiguity

\[
\begin{align*}
O(M) &= O(\overline{M}) \\
O(M) &\subseteq O(\overline{M}) & O(\overline{M}) &\subseteq O(M) \\
O(M) \cap O(\overline{M}) &\neq \emptyset \\
O(M) \cap O(\overline{M}) &= \emptyset
\end{align*}
\]

- $M$ symmetrically opaque
- $M$ opaque $|$ $\overline{M}$ opaque
- $M$ weakly opaque or not diagnosable
- $M$ diagnosable
\[ O(M) \subseteq O(\overline{M}) \]

\[ O(M) \cap O(\overline{M}) = \emptyset \]
## Verification

<table>
<thead>
<tr>
<th>Model</th>
<th>Diagnosability</th>
<th>Opacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>finite LTS</td>
<td>NL-c.</td>
<td>PSPACE-c. [Cassez et al. 09]</td>
</tr>
<tr>
<td>safe (WF-)PN</td>
<td>PSPACE-c.</td>
<td>ESPACE-c. det. space $2^{O(n)}$</td>
</tr>
<tr>
<td>weak-fairness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PN</td>
<td>EXPSPACE-c.</td>
<td>undecidable</td>
</tr>
<tr>
<td></td>
<td>+ [Yin et al. 17]</td>
<td></td>
</tr>
<tr>
<td>strict WF-PN</td>
<td>$\leq^P \neg \text{Diag} \leq^\text{EXP} \text{Reach}$</td>
<td></td>
</tr>
<tr>
<td>no fair faults</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[B., Haar, Schmitz, Schwoon 17]
Weak Fairness

A WF-Petri net

is a PN $\mathcal{N} = (P, T, w, m_0)$ with a subset $W \subseteq T$ of weakly fair transitions. Trace $\sigma = t_1 t_2 \ldots \in Tr^\omega$ with markings $m_0 m_1 \ldots$ is weakly fair if $\forall t \in W$:

**WF1** either there are infinitely many $i$ with $t = t_i$

**WF2** or there are infinitely many $i$ where $t_i$ conflicts with $t$ in $m_{i-1}$:

$m_{i-1}(p) - w(p, t_i) < w(p, t)$ for some place $p$.

For safe PNS, equivalent to:

For each $i$, if $t$ is enabled in $m_{i-1}$, there is a $j \geq i$ with $\bullet t \cap \bullet t_j \neq \emptyset$. 
WF Diagnosability = Finite Diagnosability restricted to WF traces

for any \( \sigma \in \text{Fty}_{WF}(A) \)
there is a prefix \( \hat{\sigma} \) s.t.
any \( \rho \in \text{Tr}_{WF}(A) \)
with \( O(\hat{\sigma}) < O(\rho) \)
is also faulty

WF Opacity = Finite Opacity restricted to WF traces

for each \( \sigma \in \text{Sec}^\ast(A) \)
there is \( \rho \in \text{Pub}_{WF}(A) \)
such that \( O(\sigma) \leq O(\rho) \)
\( s \in S_{WF} \rho \)
WF Diagnosability and WF Opacity

**WF Diagnosability** = Finite Diagnosability restricted to WF traces

- For any $\sigma \in Fty_{\text{WF}}^ω(\mathcal{A})$, there is a prefix $\hat{\sigma}$ such that for any $\rho \in Tr_{\text{WF}}^ω(\mathcal{A})$ with $O(\hat{\sigma}) < O(\rho)$, the trace is also faulty.

**WF Opacity** = Finite Opacity restricted to WF traces

- For each $\sigma \in Sec^*(\mathcal{A})$, there is $\rho \in Pub_{\text{WF}}^ω(\mathcal{A})$ such that $O(\sigma) \leq O(\rho)$. 
### Properties

$\mathcal{W} = \emptyset$ corresponds to the standard notion

For a convergent WF PN $(\mathcal{N}, \mathcal{W})$:
- $(\mathcal{N}, \emptyset)$ is WF diagnosable iff $\mathcal{N}$ is diagnosable.
- Secret is WF opaque in $(\mathcal{N}, \emptyset)$ iff it is opaque in $\mathcal{N}$.
\( W = \emptyset \) corresponds to the standard notion

For a convergent WF PN \((\mathcal{N}, W)\):

- \((\mathcal{N}, \emptyset)\) is WF diagnosable iff \(\mathcal{N}\) is diagnosable.
- Secret is WF opaque in \((\mathcal{N}, \emptyset)\) iff it is opaque in \(\mathcal{N}\).

**WF Opacity is more discriminating than Opacity**

For secret trace \(\sigma = s_1 a\), any infinite WF trace \(\rho\) such that \(\mathcal{O}(\sigma) < \mathcal{O}(\rho)\) belongs to \(s_1 a^\omega + u_1 a^* s_2 a^\omega\) hence contains a secret transition.
Properties

\( W = \emptyset \) corresponds to the standard notion

For a convergent WF PN \((\mathcal{N}, W)\):
- \((\mathcal{N}, \emptyset)\) is WF diagnosable iff \(\mathcal{N}\) is diagnosable.
- Secret is WF opaque in \((\mathcal{N}, \emptyset)\) iff it is opaque in \(\mathcal{N}\).

Weak fairness increases diagnosability

\[ \begin{array}{c}
  f \\
  \downarrow a \\
  \downarrow b \\
  \downarrow !WF \\
\end{array} \quad \begin{array}{c}
  u \\
  \downarrow \\
\end{array} \quad \begin{array}{c}
  c \\
  \downarrow \\
  \downarrow \text{not Diag because } O(fc^\omega) = O(uc^\omega) \\
  \text{but Diag without } c \\
  \text{and WF-diag} \\
\end{array} \]

For WF faulty traces in \(fc^*ac^\omega\), finite prefixes containing \(a\) have observations in \(c^*ac^*\), hence all infinite WF extensions are faulty.
Summary

Good news:

- Weak fairness for Diagnosability and Opacity comes at no additional cost in safe Petri nets;
- Standard Diagnosability is EXPSPACE-complete for Petri nets.

Bad news:

- Other strong undecidability results for the verification of Opacity in Petri nets;
- Non Diagnosability is equivalent to reachability when faults are not weakly fair.

Open problem: the complexity of verifying WF Diagnosability
Outline

Qualitative properties of Diagnosability and Opacity

Rational Information Flow Properties

Probabilistic Disclosure
  Probabilistic disclosure for Markov Chains
  Disclosing a secret under strategies
Examples

Given actions in $A$ and set of traces $L \subseteq A^*$

- $A = V \cup C \cup N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:
An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in $w$ results in a behaviour still in $L$. 

$A = V \cup P$ a partition into visible actions and participant actions.

Strong anonymity of participants:
for any $w \in L$, replacing in $w$ an action $a \in P$ by any other action in $P$ produces a behaviour still in $L$. 
Examples

Given actions in $A$ and set of traces $L \subseteq A^*$

- $A = V \cup C \cup N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:
An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in $w$ results in a behaviour still in $L$.

Insertion of $X$-admissible confidential actions, with $X \subseteq A$:
for any $w = w_1 w_2 \in L$ such that $w_2$ contains no confidential action and there exists $w_3 \in A^*$ and $c \in C$ with $w_3 c \in L$ and the $X$-letters in $w_1$ and $w_3$ are the same, then $w_1 cw_2$ also belongs to $L$. 
Examples

Given actions in $A$ and set of traces $L \subseteq A^*$

- $A = V \cup C \cup N$ a partition into visible, confidential and neutral actions.

Removal of confidential actions:
An observer cannot see if the confidential actions are erased: for any $w \in L$, erasing all confidential actions in $w$ results in a behaviour still in $L$.

Insertion of $X$-admissible confidential actions, with $X \subseteq A$:
for any $w = w_1w_2 \in L$ such that $w_2$ contains no confidential action and there exists $w_3 \in A^*$ and $c \in C$ with $w_3c \in L$ and the $X$-letters in $w_1$ and $w_3$ are the same, then $w_1cw_2$ also belongs to $L$.

- $A = V \cup P$ a partition into visible actions and participant actions.

Strong anonymity of participants:
for any $w \in L$, replacing in $w$ an action $a \in P$ by any other action in $P$ produces a behaviour still in $L$. 
Rational observers

- An automaton is a finite Labelled Transition System over a set of labels $\text{Lab}$. With final states and $\text{Lab}$ is alphabet $A$, it accepts a regular language in $A^*$. 

\[ L = a^+ b \{a, b\}^* \cup b^+ a \{a, b\}^* \]
Rational observers

▶ An automaton is a finite Labelled Transition System over a set of labels $Lab$. With final states and $Lab$ is alphabet $A$, it accepts a regular language in $A^*$. 

▶ A transducer is an automaton with set of labels $Lab \subseteq A^* \times B^*$. With final states, it accepts a rational relation in $A^* \times B^*$. 

$L = a^+ b\{a, b\}^* \cup b^+ a\{a, b\}^*$ \quad \quad R = \{(a, a), (b, b)\}^* (\varepsilon, b)(a, a)^*$
Rational observers

- An automaton is a finite Labelled Transition System over a set of labels \( Lab \). With final states and \( Lab \) is alphabet \( A \), it accepts a regular language in \( A^* \).

- A transducer is an automaton with set of labels \( Lab \subseteq A^* \times B^* \). With final states, it accepts a rational relation in \( A^* \times B^* \).

\[
L = a^+ b \{ a, b \}^* \cup b^+ a \{ a, b \}^*
\]

\[
R = \{(a, a), (b, b)\}^*(\varepsilon, b)(a, a)^*
\]
Rational observers

- An automaton is a finite Labelled Transition System over a set of labels $Lab$. With final states and $Lab$ is alphabet $A$, it accepts a regular language in $A^*$.  

- A transducer is an automaton with set of labels $Lab \subseteq A^* \times B^*$. With final states, it accepts a rational relation in $A^* \times B^*$.

$$L = a^+ b\{a, b\}^* \cup b^+ a\{a, b\}^*$$

$$R = \{(a, a), (b, b)\}^*(\varepsilon, b)(a, a)^*$$
### Rational observers

#### A rational observer

A rational observer is a rational relation $O \subseteq A^* \times B^*$.  

Observation of $w \in A^*$: $O(w) = \{ w' \in B^* \mid (w, w') \in O \}$.  

Observation of $L \subseteq A^*$: $O(L) = \bigcup_{w \in L} O(w)$.

#### Example: an Orwellian observer

Over $A = \{a, b\}$:  
- $O(\varepsilon) = \varepsilon$ and $O(w) = \begin{cases} \pi\{b\}(w) \text{ if } w \text{ ends with } a \\ \pi\{a\}(w) \text{ if } w \text{ ends with } b \end{cases}$

Then $O = O_a \sqcup O_b \sqcup O_\varepsilon$ with:

- $a|\varepsilon, \ b|b$
- $a|a, \ b|\varepsilon$

In $L = (a+b)(a^*+b^*)(a+b)$, the subset $M = a(a^*+b^*)(a+b)$ is opaque.
A rational information flow property (RIFP) for $L$ is any relation $L_1 \subseteq L_2$, where $L_1$ and $L_2$ are given by:

$$L_1, L_2 ::= L | \mathcal{O}(L_1) | L_1 \cup L_2 | L_1 \cap L_2$$

where $\mathcal{O}$ is a rational observer.

$\text{RIF}(\mathcal{L})$ for a class of languages $\mathcal{L}$ is the set of rational information flow properties for languages $L \in \mathcal{L}$. 


Example 1: Removal of confidential actions

\( A = V \cup C \cup N \) a partition into visible, confidential and neutral actions.

An observer cannot see if the confidential actions are erased: for any behaviour \( w \in L \), erasing all confidential actions in \( w \) results in a behaviour still in \( L \).

Translates as

\[
\pi_C(L) \subseteq L
\]

where \( \pi_C \) is the projection from \( A^* \) onto \( (A \setminus C)^* \):

\[
\pi_C(a) = \begin{cases} 
\varepsilon \text{ if } a \in C \\
 a \text{ otherwise}
\end{cases}
\]

\( c \mid \varepsilon, c \in C \\
 a \mid a, a \in V \cup N \)
Example 1: Removal of confidential actions

\[ A = V \cup C \cup N \] a partition into visible, confidential and neutral actions.

An observer cannot see if the confidential actions are erased: for any behaviour \( w \in L \), erasing all confidential actions in \( w \) results in a behaviour still in \( L \).

Translates as

\[ \pi_C(L) \subseteq L \]

where \( \pi_C \) is the projection from \( A^* \) onto \( (A \setminus C)^* \):

\[
\pi_C(a) = \begin{cases} 
\varepsilon \text{ if } a \in C \\
\varepsilon, c \in C \\
a \mid a, a \in V \cup N \\
a \text{ otherwise}
\end{cases}
\]

Proposition

Since \( \pi_C \) is a rational observer, removal of confidential actions is an RIFP.
Example 2: Insertion of confidential actions

\[ A = V \cup C \cup N \text{ and } X \subseteq A. \]

For any \( w = w_1w_2 \in L \) such that \( w_2 \) contains no confidential event and there exists \( w_3 \in A^* \) and \( c \in C \) with \( w_3c \in L \) and the \( X \)-letters in \( w_1 \) and \( w_3 \) are the same, then \( w_1cw_2 \) also belongs to \( L \).

Translates as

\[
\bigcup_{c \in C} (l-ins_c(L) \cap O_c^X(L)) \subseteq L
\]

where for each \( c \in C \),

- \( l-ins_c \) is the rational relation inserting \( c \) after the last confidential action,
- \( O_c^X \) is defined by \( O_c^X(u) = \pi_X^{-1}(\pi_X(c^{-1}u)) \cdot (V \cup N)^* \) for \( u \in A^* \).
Example 2: Insertion of confidential actions

\[ A = V \uplus C \uplus N \text{ and } X \subseteq A. \]

For any \( w = w_1w_2 \in L \) such that \( w_2 \) contains no confidential event and there exists \( w_3 \in A^* \) and \( c \in C \) with \( w_3c \in L \) and the \( X \)-letters in \( w_1 \) and \( w_3 \) are the same, then \( w_1cw_2 \) also belongs to \( L \).

Translates as
\[
\bigcup_{c \in C} (l\text{-}ins_c(L) \cap O_c^X(L)) \subseteq L
\]

where for each \( c \in C \),

- \( l\text{-}ins_c \) is the rational relation inserting \( c \) after the last confidential action,
- \( O_c^X \) is defined by \( O_c^X(u) = \pi_X^{-1}(\pi_X(c^{-1}u)).c.(V \uplus N)^* \) for \( u \in A^* \).

Proposition

All operations are rational observers, hence insertion of \( X \)-admissible confidential actions is an RIFP.
Example 3: Strong anonymity

\[ A = V \cup P. \]

For any \( w \in L \), replacing in \( w \) an action in \( P \) by another produces a behaviour in \( L \).

Translates as \( O^{P}_{SA}(L) \subseteq L \)
where \( O^{P}_{SA} \) is a substitution:

\[ O^{P}_{SA}(a) = \begin{cases} P \text{ if } a \in P \\ \{a\} \text{ otherwise} \end{cases} \]

\[ v\mid v, v \in V \]
\[ a\mid a', (a, a') \in P \times P \]
**Example 3: Strong anonymity**

\[ A = V \cup P. \]

For any \( w \in L \), replacing in \( w \) an action in \( P \) by another produces a behaviour in \( L \).

Translates as \( \mathcal{O}_\text{SA}^P(L) \subseteq L \)
where \( \mathcal{O}_\text{SA}^P \) is a substitution:

\[
\mathcal{O}_\text{SA}^P(a) = \begin{cases} 
  P & \text{if } a \in P \\
  \{a\} & \text{otherwise}
\end{cases}
\]

**Proposition**

A substitution is a rational observer, hence strong anonymity is an RIFP.
Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

For the class $\text{Reg}$ of regular languages:

The problem of deciding a property in $RIF(\text{Reg})$ is PSPACE-complete. Because regular languages have all the required closure properties and inclusion is decidable in PSPACE in $\text{Reg}$.

PSAPCE-hardness comes from the fact that $\Omega(w) = \{w\} \cap \mathcal{K}$ is a rational relation if and only if $\mathcal{K}$ is a regular language.

Consequence:

Strong (and weak) anonymity [BKMR 2008], as well as all Basic Security Predicates [Mantel 2000], are decidable (in PSPACE) for regular languages.

We retrieve results from [D’Souza et al., 2011].
Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

For the class $\mathcal{R}_{\text{eg}}$ of regular languages:

The problem of deciding a property in $RIF(\mathcal{R}_{\text{eg}})$ is PSPACE-complete.

Because regular languages have all the required closure properties and inclusion is decidable in PSPACE in $\mathcal{R}_{\text{eg}}$.

PSAPCE-hardness comes from the fact that $O_K(w) = \{w\} \cap K$ is a rational relation if and only if $K$ is a regular language.
Verification of RIFPs

For a class of languages $\mathcal{L}$:

If $\mathcal{L}$ is closed under union, intersection, and rational transductions, and if the inclusion is decidable in $\mathcal{L}$, then any property in $RIF(\mathcal{L})$ is decidable.

For the class $\text{Reg}$ of regular languages:

The problem of deciding a property in $RIF(\text{Reg})$ is PSPACE-complete.

Because regular languages have all the required closure properties and inclusion is decidable in PSPACE in $\text{Reg}$.

PSAPCE-hardness comes from the fact that $O_K(w) = \{w\} \cap K$ is a rational relation if and only if $K$ is a regular language.

Consequence:

Strong (and weak) anonymity [BKMR 2008], as well as all Basic Security Predicates [Mantel 2000], are decidable (in PSPACE) for regular languages. We retrieve results from [D’Souza et al., 2011].
The case of Opacity

For $M \subseteq L$ a regular subset of secret behaviours and $\mathcal{O}$ a functional rational observer

From $\mathcal{O}(M) \subseteq \mathcal{O}(\overline{M})$:

Rational opacity for regular secrets is an RIFP.

Consequence:

We recover the decidability result (in PSPACE) for rational opacity with regular languages and regular secrets [Cassez et al., 2009].

Remark: Strong Anonymity translates as Opacity [BKMR08]

$\mathcal{O}$ is the morphism into $(\Sigma \cup \{\#\})^*$ defined by:

$\mathcal{O}(a) = \#$ if $a \in P$ and $\mathcal{O}(a) = a$ otherwise

$\pi_P$ the projection on $P^*$

$L$ is strongly anonymous w.r.t. $P$ iff for any $u \in P^*$,

$Sec_u = \{w \in L \mid \pi_P(w) \neq u \land |\pi_P(w)| = |u|\}$

is opaque for $\mathcal{O}$. 
The case of Weak Non Inference

From [D’Souza et al., 2011]

With $A = V \cup C \cup N$,

**WNI**

$L$ satisfies WNI if for all $w \in L$ there exists $w' \in L$ such that if $w$ contains confidential actions, then $\pi_V(w) = \pi_V(w')$ and $\pi_C(w) \neq \pi_C(w')$.

**WNI is undecidable on regular languages.**

**Consequence:**

WNI is NOT an RIFP.
Summary

Good news:

- Many security properties from the literature are RIFPs;
- The complexity of verification is always in PSPACE for regular languages, whatever the (rational) observation.

To do:

- Find other classes satisfying the closure properties leading to decidability;
- Find links with model checking extensions of LTL like SecLTL [DFKRS12] or even CTL* like HyperCTL* [CFKMRS14].
- What about Opacity with a general rational observer?
Outline

Qualitative properties of Diagnosability and Opacity

Rational Information Flow Properties

Probabilistic Disclosure

Probabilistic disclosure for Markov Chains
Disclosing a secret under strategies
A quantitative problem for opacity...

No disclosing path iff

\[ V = \text{Sec} \setminus \mathcal{O}^{-1}(\mathcal{O}(\text{Sec})) \text{ is empty} \]

Measuring the disclosure set \( V \)
...under uncertainty

- Probabilistic choice: Markov Chains
  [B., Mullins, Sassolas 10,15] [Saboori, Hadjicostis 14]
...under uncertainty

- Probabilistic choice: Markov Chains
  [B., Mullins, Sassolas 10,15] [Saboori, Hadjicostis 14]
- Combined with nondeterministic choice:
  [B., Chatterjee, Sznajder 15] for MDPs and POMDPs,
  [B., Haddad, Lefaucheux 17] for MDPs,
- Underspecification: [B., Kouchnarenko, Mullins, Sassolas 16] for IMCs.
A toy example

Access control to a database inspired from [Biondi et al. 13]

\[ M_2 : \]

\[ \begin{array}{ccc}
0, 1 & \rightarrow & 0, 1 \\
0.2, 1 & \rightarrow & 0.2, 1 \\
0.2, 1 & \rightarrow & 0.2, 1
\end{array} \]

\[ \begin{array}{ccc}
q_0 & \rightarrow & q_1 \\
q_2 & \rightarrow & q_3 \\
q_4 & \rightarrow & q_3
\end{array} \]

\[ M_1 : \]

\[ \begin{array}{ccc}
0.2, 0.4 & \rightarrow & 0.1, 1 \\
0.2, 0.4 & \rightarrow & 0.1, 1 \\
0.2, 0.4 & \rightarrow & 0.1, 1
\end{array} \]

\[ \begin{array}{ccc}
r_0 & \rightarrow & r_1 \\
r_2 & \rightarrow & r_1' \\
r_3 & \rightarrow & r_4
\end{array} \]

0: input user name, 1: input password, 3: access granted if correct
2: not on the list of authorized users, 4: reject
\[ Sec = \{0.1.3^\omega\} ; \text{ All states except } 1 \text{ and } 1' \text{ are observable.} \]
A Markov Chain $\mathcal{A} = (S, \Delta, O)$ over $\Sigma$:

- countable set $S$ of states,
- $\Delta : S \rightarrow \text{Dist}(S)$,
- $O : S \rightarrow \Sigma \cup \{\varepsilon\}$ observation function.

equipped with an initial distribution $\mu_0$. 

Example with Sec: visiting $s_1$ or $s_2$, hidden by $O$
Disclosure for MCs

ω-Disclosure of Sec in \((A, \mu_0)\):

\[
Disc_\omega(A, \mu_0, Sec) = P_{A,\mu_0}(V) \text{ for } V = Sec \setminus O^{-1}(O(Sec)).
\]

Example with Sec: presence of \(s_1\) or \(s_2\), hidden by \(O\)

\[
Disc_\omega(A, 1_{s_0}, Sec) = \frac{1}{3}
\]
Restricting Sec to the set of pathes visiting states from a given subset assuming a path remains secret once a secret state has been visited.

Observation sequence $w$ in $\Sigma^*$ is:
- **disclosing** if all pathes in $O^{-1}(w)$ are secret,
- **minimal disclosing** if disclosing with no strict disclosing prefix.

$Disc(A, \mu_0, Sec)$: probability of minimal disclosing observations

$$Disc_\omega = \frac{1}{2}$$

$$Disc = 0$$

$Disc \leq Disc_\omega$

equality if $A$ is convergent and finitely branching.
Interactions with the system

Active attacker

The attacker consists of two components:
- The passive external observer,
- Some piece of code inside the system.

Worst case corresponds to maximal disclosure.

System designer

The designer has provided a first version with the required functionalities. He must develop the access policy...

... to obtain minimal disclosure.
Constraint Markov Chains

M = (S, T, O)

ients set of states S,
▶ T : S → 2^{Dist(S)}.
### Subclasses of CMCs

**MDP: Markov Decision Processes**

For each $s \in S$, $T(s)$ is a finite set.

**LCMC: Linear CMCs**

For each $s \in S$, $T(s)$ is the set of distributions that are solutions of a linear system.

**IMC: Interval MC**

For each $s$, $T(s)$ is described by a family of intervals $(l(s, s'))_{s' \in S}$.

#### Relations

- IMC is a strict subclass of LCMC,
- Any LCMC can be transformed in an exponentially larger MDP.
Examples

LCMC $\mathcal{M}_2$:

- Initial state: Idle
- Transitions:
  - $x_1$ to Success
  - $x_2$ to Error
  - $x_3$ to Failure
- States:
  - Idle
  - Error
  - Failure

- Time constraints:
  - $x_2 \geq 2x_3$
  - $x_2 + x_3 \leq \frac{1}{2}$
  - $0 \leq x_1, x_2, x_3 \leq 1$
  - $x_1 + x_2 + x_3 = 1$

- Mappings:
  - $\mu_1 = (1, 0, 0)$
  - $\mu_2 = (\frac{1}{2}, \frac{1}{2}, 0)$
  - $\mu_3 = (\frac{1}{2}, \frac{1}{3}, \frac{1}{6})$

IMC $\mathcal{M}_3$:

- Initial state: Idle
- Transitions:
  - $x_1$ to Success
  - $x_2$ to Error
  - $x_3$ to Failure
- States:
  - Idle
  - Error
  - Failure

- Time constraints:
  - $\frac{1}{2} \leq x_1 \leq 1$
  - $0 \leq x_2 \leq \frac{1}{2}$
  - $0 \leq x_3 \leq \frac{1}{6}$

- Mappings:
  - $\mu_4 = (\frac{5}{6}, 0, \frac{1}{6}) \in T_3(s_0)$
  - $\mu_4 \notin T_2(s_0)$
From LCMCs to MDPs

\[
\begin{align*}
\mu_1 &= (1, 0, 0) \\
\mu_2 &= \left(\frac{1}{2}, \frac{1}{2}, 0\right) \\
\mu_3 &= \left(\frac{1}{2}, \frac{1}{3}, \frac{1}{6}\right)
\end{align*}
\]
Strategies on CMCs

A strategy for $M = (S, T, O)$ with initial distribution $\mu_0$:

$\sigma : \text{Runs}(M) \rightarrow \text{Dist}(S)$

For $\rho = s_0 \mu_1 \rightarrow s_1 \ldots \mu_n \rightarrow s_n$, $\sigma(\rho) \in T(s_n)$.

Scheduling $M$ with $\sigma$ produces a (possibly infinite) MC $M_\sigma$. 
A strategy for \( \mathcal{M} = (S, T, \mathcal{O}) \) with initial distribution \( \mu_0 \):

\[
\sigma : FRuns(\mathcal{M}) \rightarrow Dist(S)
\]

For \( \rho = s_0 \xrightarrow{\mu_1} s_1 \ldots \xrightarrow{\mu_n} s_n \), \( \sigma(\rho) \in T(s_n) \).

Scheduling \( \mathcal{M} \) with \( \sigma \) produces a (possibly infinite) MC \( \mathcal{M}_\sigma \).
A strategy for $\mathcal{M} = (S, T, \mathcal{O})$ with initial distribution $\mu_0$:

$\sigma : \text{FRuns}(\mathcal{M}) \rightarrow \text{Dist}(S)$

For $\rho = s_0 \xrightarrow{\mu_1} s_1 \ldots \xrightarrow{\mu_n} s_n$, $\sigma(\rho) \in T(s_n)$.

Scheduling $\mathcal{M}$ with $\sigma$ produces a (possibly infinite) MC $\mathcal{M}_\sigma$. 
Randomized strategies on MDPs

An MDP with distributions $\mu_1$ and $\mu_2$ for $s_0$ and secret states $\{s_2, s_3\}$

$Disc = \frac{1}{2}$ with the two strategies choosing $\mu_1$ or $\mu_2$ in $s_0$
if they are known by the observer.

![Diagram](image)

But $Disc = 0$ with randomized strategies $\sigma_p$ such that
$\sigma_p(s_0) = p\mu_1 + (1 - p)\mu_2$ with $0 < p < 1$. Necessary for minimisation.

A randomized strategy associates $\sigma(\rho) \in \text{Dist}(T(s_n))$

with $\rho = s_0 \xrightarrow{\mu_1} s_1 \ldots \xrightarrow{\mu_n} s_n$ (instead of $\sigma(\rho)$ in $T(s_n)$).
Maximal and minimal disclosure

For Sec in $\mathcal{M}$ with initial distribution $\mu_0$:

- $Disc_{\text{max}}(\mathcal{M}, \mu_0, \text{Sec}) = \sup_{\sigma \in \text{Strat}(\mathcal{M})} Disc(\mathcal{M}_\sigma, \mu_0, \text{Sec})$
- $Disc_{\text{min}}(\mathcal{M}, \mu_0, \text{Sec}) = \inf_{\sigma \in \text{Strat}(\mathcal{M})} Disc(\mathcal{M}_\sigma, \mu_0, \text{Sec})$

Several disclosure problems for a given $\mathcal{M}$

- **Value problem**: compute the disclosure $Disc_{\text{max}}$ or $Disc_{\text{min}}$.
- **Quantitative decision problems**: Given a threshold $\theta \in [0, 1]$, is $Disc_{\text{max}} \geq \theta$? is $Disc_{\text{min}} \leq \theta$?
- **Qualitative decision problems**:
  - Limit-sure disclosure: the quantitative problem with $\theta = 1$ for maximisation and $\theta = 0$ for minimisation.
Maximal Disclosure

[BCS15] On MDPs, if observer ignores the strategies or if no edge can be blocked by a strategy,

- The value can be computed in polynomial time;
- All problems are decidable.

[BHL17] On MDPs, if observer knows the strategies:

- Deterministic strategies are sufficient;
- The problem asking whether there exists a strategy producing value 1 is EXPTIME-complete;
- But the quantitative and limit-sure problems are undecidable.

Consequence:
The quantitative problem is undecidable for general LCMCs.
[BHL17] On MDPs, if observer knows the strategies:

- Families of randomized strategies are necessary;
- The value can be computed in EXPTIME;
- All problems are decidable.
Summary

Linear CMCs form a good class for compact specifications of probabilistic systems with:

- nice closure properties;
- an increased security criterion with schedulers as adversaries;
- But the quantitative problem is undecidable unless the structure is fixed.

Minimisation on MDPs

- requires randomized strategies;
- and all quantitative problems are decidable.
Conclusion

A lot of work to be done... on qualitative and quantitative aspects
Conclusion

A lot of work to be done... on qualitative and quantitative aspects

Thank you