FM Milano 2024

The Opacity of Timed Automata

Jie An[1,3], Qiang Gao[1], Lingtai Wang[1], Naijun Zhan[2,1], Ichiro Hasuo[3]

[1] Institute of Software, Chinese Academy of Sciences, Beijing, China
[2] School of Computer Science, Peking University, Beijing, China
[3] National Institute of Informatics, Tokyo, Japan

2024-09-12 @ FM 2024, Milan

ISCAS 中国科学院软件研究所 Institute of Software Chinese Academy of Sciences

北京大學 PEKING UNIVERSITY

NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 National Institute of Informatics

Outline

- Introduction to opacity problem

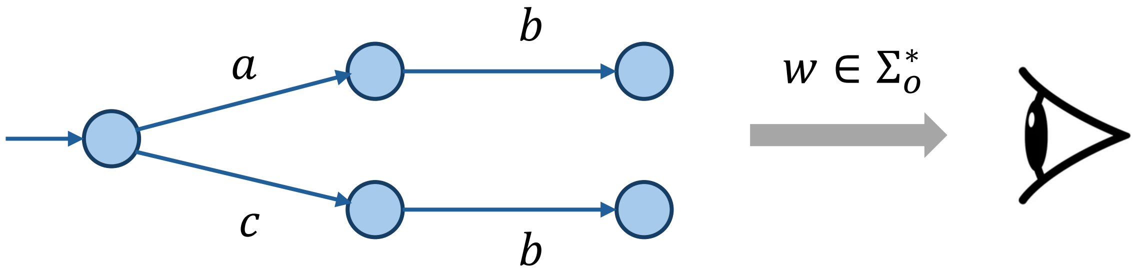
- Introduction to timed opacity
  - The dark side of timed opacity

- Revisiting the opacity of timed automata
  - The transformation of three kinds of timed opacity problems (language, initial-location, current-location)
  - One-clock timed automata, TA under discrete-time semantics
  - Sufficient condition, necessary condition

What is opacity?

Opacity serves as a critical security and confidentiality property, which concerns whether an intruder can unveil a system's secret based on structural knowledge and observed behaviors.

Example



- An intruder knows the system M.
- The behaviors of the system $L = \{ab, cb\}$.
- The observable actions $\Sigma_o = \{b\}$.
- The secret $S = \{ab\}$.

Question: For every observation w, if the intruder can infer that w is produced by a secret in S.

M is opaque w.r.t Σ_o and S.

The opacity problems:

- **Language-based opacity**: the secret is a set of system languages
- **Initial-state opacity**: the secret is a set of initial states
- **Current-state opacity**: the secret is a set of states
- ....

Decidable!

Discrete-Event Systems

Outline

- Introduction to opacity problem

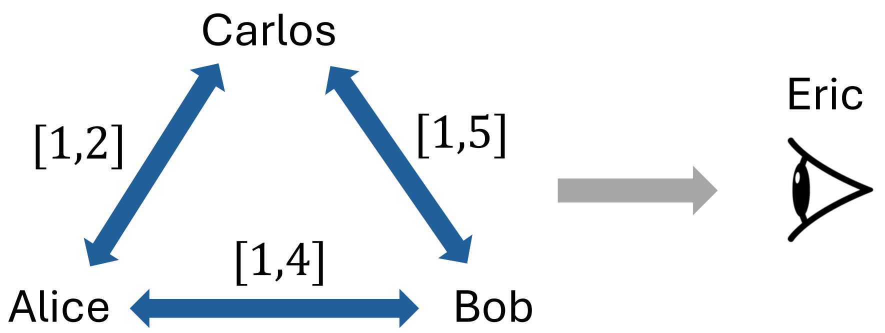
- Introduction to timed opacity
  - The dark side of timed opacity

- Revisiting the opacity of timed automata
  - The transformation of three kinds of timed opacity problems (language, initial-location, current-location)
  - One-clock timed automata, TA under discrete-time semantics
  - Sufficient condition, necessary condition

What is timed opacity?

Considering opacity problems in timed systems.

Example



- Alice, Bob, and Carlos can send messages to each other, and Carlos is a secret participant.
- Eric can only observe Alice and Bobs' behaviors
  - A system behavior: Alice $\xrightarrow{1.2}$ Carlos $\xrightarrow{2.1}$ Bob
  - Corresponding observation: Alice $\xrightarrow{3.3}$ Bob

Question: if Eric can infer that there is a third participant in the system.

Yes, when observing Alice $\overset{t}{\leftrightarrow}$Bob where $t > 4$

J. An et al. <anjie@iscas.ac.cn>

What is timed opacity?

Considering opacity problems in timed systems.

- **Dark side**: the opacity problem of timed automata is **undecidable.** [Cassez09]

The universality problem of TA $\xrightarrow{\text{reduction}}$ The opacity problem of TA

Motivation

- The decidability for the opacity problems of one-clock timed automata.
  - The universality problem of one-clock timed automata is decidable.
- Conjecture in [Cassez09]: the opacity of TA under the discrete-time semantics is decidable.
- The decidability for the opacity problems of specific subsets of TA.
  - Sufficient condition and necessary condition for the decidability.

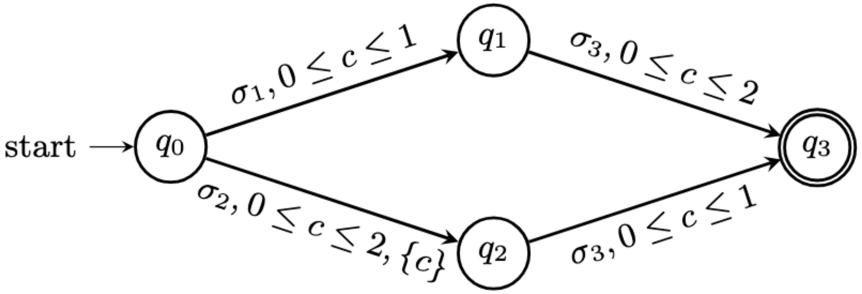
Outline

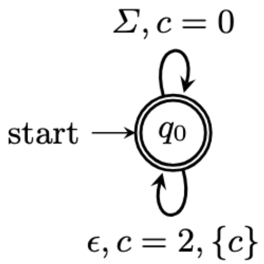
- Introduction to opacity problem
- Introduction to timed opacity
  - The dark side of timed opacity
- Revisiting the opacity of timed automata
  - The transformation of three kinds of timed opacity problems (language, initial-location, current-location)
  - One-clock timed automata, TA under discrete-time semantics
  - Sufficient condition, necessary condition

Timed automata

Extending finite-state automata with a finite set of clock variables.

Example





- **Timed word** $\omega \in (\Sigma \times \mathbb{R}_{\ge 0})^*$: $(\sigma_1, t_1)\,(\sigma_1, t_2)\,\ldots(\sigma_n, t_n)$, where $t_1 \le t_2 \ldots \le t_n$.
  - $(\sigma_2, 1)(\sigma_3, 2)$ is an accepting timed words.
- A **timed language** is a set of timed words.
  - $\mathcal{L} = \{(\sigma_1, t_1)(\sigma_3, t_2) | 0 \le t_1 \le 1 \wedge 0 \le t_2 \le 2\} \cup \{(\sigma_2, t_1)(\sigma_3, t_2) | 0 \le t_1 \le 2 \wedge 0 \le t_2 - t_1 \le 1\}$

- ϵ-TA $\supset$ TA
- $\mathcal{L}_\epsilon = \{(\sigma_1, t_1) \cdots (\sigma_n, t_n) \in (\Sigma \times \mathbb{R}_{\ge 0})^* | \forall i \ge 0, t_i \in 2\mathbb{N}\}$

- Given a subset $\Sigma_o \subseteq \Sigma$, a **projection** on timed words $P_{\Sigma_o}: (\Sigma \times \mathbb{R}_{\ge 0})^* \longrightarrow (\Sigma_o \times \mathbb{R}_{\ge 0})^*$ s.t.

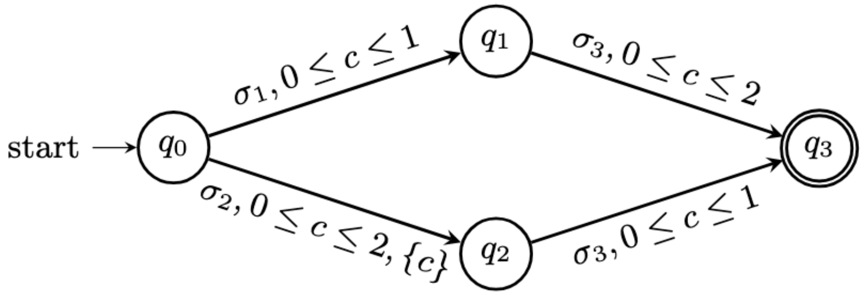
$$P_{\Sigma_o}(\epsilon) = \epsilon \qquad\qquad P_{\Sigma_o}((\sigma, t) \cdot \omega) = \begin{cases} (\sigma, t) \cdot P_{\Sigma_o}(\omega) & if\ \sigma \in \Sigma_o \\ P_{\Sigma_o}(\omega) & otherwise \end{cases}$$

The opacity problems of timed automata

Language-based timed opacity : given a TA $\mathcal{A} = (\Sigma, Q, Q_0, Q_f, C, \Delta)$, an *observable alphabet* $\Sigma_o \subseteq \Sigma$, and *a secret timed language* $\mathcal{L}_s$, then $\mathcal{A}$ is **language-based timed opaque (LBTO)** w.r.t Σ_o and $\mathcal{L}_s$ iff

$$\forall \omega \in \mathcal{L}(\mathcal{A}) \cap \mathcal{L}_s, \exists \omega' \in \mathcal{L}(\mathcal{A}) \backslash \mathcal{L}_s \text{ s.t. } P_{\Sigma_o}(\omega) = P_{\Sigma_o}(\omega')$$

Example



- $\Sigma_o = \{\sigma_3\}$
- $\mathcal{L}_s = \{(\sigma_2, t_1)(\sigma_3, t_2) | 0 \leq t_1 \leq 2 \wedge 0 \leq t_2 - t_1 \leq 1\}$

LBTO?

- $\omega = (\sigma_2, 2)(\sigma_3, 3)$, $P_{\Sigma_o}(\omega) = (\sigma_3, 3)$
- Not exists $\omega' \in \mathcal{L}(\mathcal{A}) \backslash \mathcal{L}_s$ s.t. $P_{\Sigma_o}(\omega) = P_{\Sigma_o}(\omega')$

The opacity problems of timed automata

Location-based timed opacity : given a TA $\mathcal{A} = (\Sigma, Q, Q_0, Q_f, C, \Delta)$, an *observable alphabet* $\Sigma_o \subseteq \Sigma$, and *a secret set of locations* $Q_s \in Q$, then

- $\mathcal{A}$ is **initial-location timed opaque (ILTO)** w.r.t Σ_o and $Q_s \in Q_o$ iff

$$\forall \omega \in Tr_{\mathcal{A}}(Q_s), \exists \omega' \in Tr_{\mathcal{A}}(Q_0 \backslash Q_s) \text{ s.t. } P_{\Sigma_o}(\omega) = P_{\Sigma_o}(\omega')$$

- $\mathcal{A}$ is **current-location timed opaque (CLTO)** w.r.t Σ_o and $Q_s \in Q$ iff

$$\forall \omega \in Tr_{\mathcal{A}}(Q_o, Q_s), \exists \omega' \in Tr_{\mathcal{A}}(Q_0, Q \backslash Q_s) \text{ s.t. } P_{\Sigma_o}(\omega) = P_{\Sigma_o}(\omega')$$

Transformation between LBTO, ILTO, and CLTO

Results

(1) The LBTO, ILTO, and CLTO problems of one-clock timed automata (OTA) are undecidable.

The universality problem of OTA with ϵ-transitions $\xrightarrow{\text{reduction}}$ The CLTO problem of OTA

(2) A constructive proof for the decidability of timed opacity under discrete-time semantics.

TA Under Discre. → Region Automata → Integral Automata → ϵ-NFA

The opacity problem of TA under Discre. $\xrightarrow{\text{reduction}}$ The language-inclusion problem of ϵ-NFA

For example, $\omega = (\sigma_1, 2)(\sigma, 3), Tick(\omega) = \checkmark\checkmark\sigma_1\checkmark\sigma_2$

PSPACE-complete

Results

(3) A sufficient condition and a necessary condition for the decidability of timed opacity of $\mathcal{X}$-automata

Sufficient condition

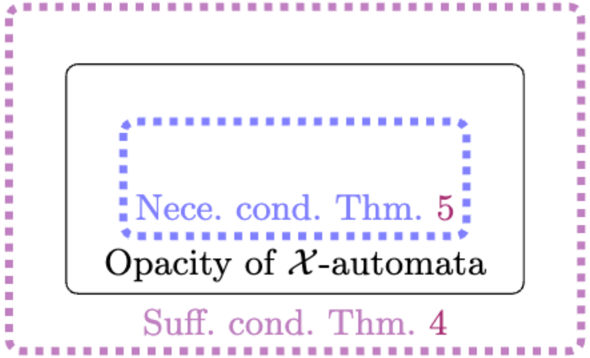
$\mathcal{X}$-automata are closed under product, complementation, and projection.

The LBTO problem of $\mathcal{X}$-automata

↓

The emptiness problem of $\mathcal{X}$-automata

PSPACE



Necessary condition

The universality problem of $\mathcal{X}$-automata is decidable.

The universality problem of $\mathcal{X}$-automata

↓

The CLTO problem of $\mathcal{X}$-automata

Thank you!