WiP Abstract: Towards Approximate Opacity of Cyber-Physical System

Xiang Yin
Department of Automation, Shanghai Jiao Tong University
Key Lab of System Control & Information Processing
Ministry of Education, Shanghai, China
yinxiang@sjtu.edu.cn

Majid Zamani
Department of Computer Science
University of Colorado Boulder, USA
majid.zamani@colorado.edu

ABSTRACT

Opacity is an important information-flow security property in the analysis of cyber-physical systems. In this abstract, we extend the concept of opacity to systems whose output sets are equipped with metrics. A new concept called approximate opacity is proposed in order to quantitatively evaluate the security guarantee level with respect to the measurement precision of the intruder. Then we propose a new simulation-type relation called approximate opacity preserving simulation relations, which characterizes how close two systems are in terms of the satisfaction of approximate opacity. We also discuss how to construct approximate opacity preserving symbolic models for a class of discrete-time control systems.

CCS CONCEPTS

• **Security and privacy** → **Formal security models**; *Logic and verification*; • **Theory of computation** → Abstraction;

KEYWORDS

Opacity, Approximate Simulation Relation, Finite Abstractions

ACM Reference Format:
Xiang Yin and Majid Zamani. 2019. WiP Abstract: Towards Approximate Opacity of Cyber-Physical System. In *ICCPS '19: ACM/IEEE International Conference on Cyber-Physical Systems, April 16–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3302509.3313316

1 INTRODUCTION

Security and privacy have becoming increasingly important issues for cyber-physical systems (CPS) in the past few years. In this abstract, we investigate an important information-flow security property called *opacity*. Roughly speaking, a system is said to be opaque if it always has the plausible deniability for any of its secret behavior [2]. Since opacity is an information-flow property, its definition strictly depends on the information model of the system. Most of the existing works formulate opacity by adopting the event-based observation model. This essentially assumes that the output of the system is symbolic in the sense that we can precisely distinguish different output labels. Hereafter, we will also refer to opacity under this setting as *exact opacity*. However, for many real-world systems whose outputs are physical signals, instead of just saying that two events are distinguishable or indistinguishable, we may have a measurement to quantitatively evaluate how close two outputs are. Such systems are referred to as *metric systems*, where the output sets are equipped with appropriate metrics. For metric systems, if two signals are very close to each other, then it will be very hard to distinguish them unambiguously due to the measurement precision or potential measurement noises.

In this abstract, we propose a new concept called *approximate opacity* that is more applicable to metric systems. We treat two outputs as "indistinguishable" outputs if their distance is smaller than a given threshold parameter $\delta \geq 0$. Intuitively, δ-approximate opacity says that the intruder can never determine that the system is initiated from a secret state if it does not have an enough measurement precision captured by parameter δ. In other words, our new definition provides a relaxed version of opacity with a quantitative security guarantee level with respect to the measurement precision of the intruder. Then we propose the notion of ε-approximate opacity preserving (ε-OP) simulation relation, which characterizes how close two systems are, specified by parameter $\varepsilon \geq 0$, in terms of the satisfaction of approximate opacity. We show that if system S_a is ε-OP simulated by system S_b, then S_b being δ-approximate opaque implies that S_a is $(\delta + 2\varepsilon)$-approximate opaque. In particular, for a class of incrementally input-to-state stable discrete-time control systems with possibly infinite state-spaces, we propose an effective approach to construct symbolic models (a.k.a. finite abstractions) that approximately simulate the original systems in the sense of opacity preserving and vice versa.

2 APPROXIMATE OPACITY

We employ a notion of "*system*" introduced in [3] as the underlying model of CPS describing both continuous-space and finite control systems. Specifically, a system S is a tuple $S = (X, X_0, U, \longrightarrow, Y, H)$, where X is a set of states, $X_0 \subseteq X$ is a set of initial states, U is a set of inputs, $\longrightarrow \subseteq X \times U \times X$ is a transition relation, Y is a set of outputs, and $H : X \to Y$ is an output map. A transition $(x, u, x') \in \longrightarrow$ is also denoted by $x \xrightarrow{u} x'$.

The system may have some "secrets" that do not want to be revealed to intruders. We adopt a state-based formulation of secrets by assuming that $X_S \subseteq X$ is a set of *secret states*. Due to the imperfect measurement precision, it is very difficult to distinguish two observations if their difference is very small. Therefore, it will be useful to define a "robust" version of opacity by characterizing under which measurement precision the system is opaque.

ICCPS '19, April 16–18, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6285-6/19/04.
https://doi.org/10.1145/3302509.3313316

Definition 2.1. *Let $S = (X, X_0, X_S, U, \longrightarrow, Y, H)$ be a metric system, with the metric $\mathbf{d}$ defined over the output set, and a constant $\delta \geq 0$. System S is called δ-approximate opaque if for any $x_0 \in X_0 \cap X_S$ and finite state run $x_0 \xrightarrow{u_1} x_1 \xrightarrow{u_2} \cdots \xrightarrow{u_n} x_n$, there exist $x_0' \in X_0 \setminus X_S$ and a finite state run $x_0' \xrightarrow{u_1'} x_1' \xrightarrow{u_2'} \cdots \xrightarrow{u_n'} x_n'$ such that $\max_{i\in\{0,\ldots,n\}} \mathbf{d}(H(x_i), H(x_i')) \leq \delta$.*

Intuitively, approximate opacity can be interpreted as "*the initial secret of the system cannot be revealed to an intruder that does not have an enough measurement precision related to parameter δ*". In general, verifying approximate opacity is a PSPACE-hard problem. To mitigate the verification complexity, we introduce a new notion of approximate opacity preserving simulation relations, inspired by the one in [1]. The newly proposed simulation relations will also provide the basis for abstraction-based verification of approximate opacity.

Definition 2.2. *Consider two metric systems $S_a = (X_a, X_{a0}, X_{aS}, U_a, \xrightarrow[a]{}, Y_a, H_a)$ and $S_b = (X_b, X_{b0}, X_{bS}, U_b, \xrightarrow[b]{}, Y_b, H_b)$ with the same output sets $Y_a = Y_b$ and metric $\mathbf{d}$. For $\varepsilon \in \mathbb{R}_0^+$, a relation $R \subseteq X_a \times X_b$ is called an ε-approximate opacity preserving simulation relation (ε-OP simulation relation) from S_a to S_b if*

(1)(a) $\forall x_{a0} \in X_{a0} \cap X_{aS}, \exists x_{b0} \in X_{b0} \cap X_{bS} : (x_{a0}, x_{b0}) \in R$;
(b) $\forall x_{b0} \in X_{b0} \setminus X_{bS}, \exists x_{a0} \in X_{a0} \setminus X_{aS} : (x_{a0}, x_{b0}) \in R$;
(2) $\forall (x_a, x_b) \in R : \mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$;
(3) For any $(x_a, x_b) \in R$, we have
(a) $\forall x_a \xrightarrow[a]{u_a} x_a', \exists x_b \xrightarrow[b]{u_b} x_b' : (x_a', x_b') \in R$;
(b) $\forall x_b \xrightarrow[b]{u_b} x_b', \exists x_a \xrightarrow[a]{u_a} x_a' : (x_a', x_b') \in R$.

We say that S_a is ε-OP simulated by S_b, denoted by $S_a \preceq_\varepsilon S_b$, if there exists an ε-OP simulation relation R from S_a to S_b.

Although the above relation is similar to the approximate bisimulation relation proposed in [1], it is still a one sided relation here because condition (1) is not symmetric. We refer the interested readers to [5] to see why one needs strong condition (3) to show preservation of opacity in one direction when $\varepsilon = 0$.

Theorem 2.3. *Let S_a and S_b be two metric systems with the same output sets and metric $\mathbf{d}$ and let $\varepsilon, \delta \in \mathbb{R}_0^+$. If $S_a \preceq_\varepsilon S_b$ and $\varepsilon \leq \frac{\delta}{2}$, then the following implication hold:*

S_b is $(\delta - 2\varepsilon)$-approximate opaque $\Rightarrow$ S_a is δ-approximate opaque.

Remark 2.4. *Note that δ and ε are parameters specifying two different types of precision. Parameter δ is used to specify the measurement precision under which we can guarantee opacity for a single system, while parameter ε is used to characterize the "distance" between two systems in terms of being approximately opaque.*

3 OPACITY OF CONTROL SYSTEMS

We show how to analyze approximate opacity for a class of discrete-time control systems. Specifically, we deal with discrete-time control system described by difference equations of the form

$$\Sigma : \begin{cases} \xi(k+1) = f(\xi(k), \upsilon(k)), \\ \zeta(k) = h(\xi(k)), \end{cases} \tag{3.1}$$

where $\xi : \mathbb{N}_0 \to \mathbb{X}$, $\zeta : \mathbb{N}_0 \to \mathbb{Y}$, and $\upsilon : \mathbb{N}_0 \to \mathbb{U}$ are the state, output, and input signals, respectively, and $\mathbb{X}$, $\mathbb{Y}$, and $\mathbb{U}$ are bounded state, output, and input sets, respectively. We denote by $\mathbb{S} \subseteq \mathbb{X}$ the set of secret states of control system Σ. We assume that the output map $h : \mathbb{X} \to \mathbb{Y}$ satisfies the following Lipschitz condition: $\|h(x) - h(y)\| \leq \alpha(\|x - y\|)$ for some $\alpha \in \mathcal{K}_\infty$ and all $x, y \in \mathbb{X}$. Also, we assume Σ is incrementally input-to-state stable (δ-ISS), i.e., there exist a $\mathcal{KL}$ function β and $\mathcal{K}_\infty$ function γ such that $\forall x, x' \in \mathbb{X}$ and $\forall \upsilon, \upsilon' : \mathbb{N}_0 \to \mathbb{U}$, the following inequality holds for any $k \in \mathbb{N}$:

$$\|\xi_{x\upsilon}(k) - \xi_{x'\upsilon'}(k)\| \leq \beta(\|x - x'\|, k) + \gamma(\|\upsilon - \upsilon'\|_\infty). \tag{3.2}$$

For any control system Σ, we define an associated metric system $S(\Sigma) = (X, X_0, X_S, U, \longrightarrow, Y, H)$, where $X = \mathbb{X}$, $X_0 = \mathbb{X}$, $X_S = \mathbb{S}$, $U = \mathbb{U}$, $Y = \mathbb{Y}$, $H = h$, and $x \xrightarrow{u} x'$ if and only if $x' = f(x, u)$. We assume that the output set Y is equipped with the infinity norm: $\mathbf{d}(y_1, y_2) = \|y_1 - y_2\|$, $\forall y_1, y_2 \in Y$. Then let $\mathrm{q} = (\eta, \mu)$ be a tuple of parameters, where $0 < \eta \leq \min\{span(\mathbb{S}), span(\mathbb{X} \setminus \mathbb{S})\}$ is the state set quantization and $0 < \mu \leq span(\mathbb{U})$ is the input set quantization; see [4] for a formal definition of *span* and η-approximation $[\cdot]_\eta$, for $\eta > 0$. We introduce the symbolic system

$$S_{\mathrm{q}}(\Sigma) = (X_{\mathrm{q}}, X_{\mathrm{q}0}, X_{\mathrm{q}S}, U_{\mathrm{q}}, \xrightarrow[\mathrm{q}]{}, Y_{\mathrm{q}}, H_{\mathrm{q}}), \tag{3.3}$$

where $X_{\mathrm{q}} = X_{\mathrm{q}0} = [\mathbb{X}]_\eta, X_{\mathrm{q}S} = [\mathbb{S}]_\eta, U_{\mathrm{q}} = [\mathbb{U}]_\mu, Y_{\mathrm{q}} = \{h(x_{\mathrm{q}}) \mid x_{\mathrm{q}} \in X_{\mathrm{q}}\}$, $H_{\mathrm{q}}(x_{\mathrm{q}}) = h(x_{\mathrm{q}})$, and $x_{\mathrm{q}} \xrightarrow[\mathrm{q}]{u_{\mathrm{q}}} x_{\mathrm{q}}'$ iff $\|x_{\mathrm{q}}' - f(x_{\mathrm{q}}, u_{\mathrm{q}})\| \leq \eta$.

The following result shows that, under some condition over the quantization parameters η and μ, $S_{\mathrm{q}}(\Sigma)$ and $S(\Sigma)$ are related under an approximate opacity preserving simulation relation.

Theorem 3.1. *Let $\Sigma = (\mathbb{X}, \mathbb{S}, \mathbb{U}, f, \mathbb{Y}, h)$ be a δ-ISS control system. For any desired precision $\varepsilon > 0$, and any tuple $\mathrm{q} = (\eta, \mu)$ of quantization parameters satisfying $\beta\left(\alpha^{-1}(\varepsilon), 1\right) + \gamma(\mu) + \eta \leq \alpha^{-1}(\varepsilon)$, we have $S(\Sigma) \preceq_\varepsilon S_{\mathrm{q}}(\Sigma) \preceq_\varepsilon S(\Sigma)$.*

4 CONCLUSION

We extended the concept of opacity to metric systems by proposing the notion of approximate opacity. Approximate relation that preserves approximate opacity were also provided. We also discussed how to construct finite abstractions that approximately simulates a class of control systems in terms of opacity preserving.

ACKNOWLEDGMENTS

This work was supported in part by the NSFC (61803259, 61833012), the H2020 ERC Starting Grant AutoCPS, and the German Research Foundation (DFG) through the grant ZA 873/1-1.

REFERENCES

[1] A. Girard and G. J. Pappas. Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, 52(5):782–798, May 2007.
[2] R. Jacob, J.-J. Lesage, and J.-M. Faure. Overview of discrete event systems opacity: Models, validation, and quantification. *Annual Rev. Control*, 41:135–146, 2016.
[3] P. Tabuada. *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer Publishing Company, 1st edition, 2009.
[4] M. Zamani, P. Mohajerin Esfahani, R. Majumdar, A. Abate, and J. Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.
[5] K. Zhang, X. Yin, and M. Zamani. Opacity of nondeterministic transition systems: A (bi)simulation relation approach. *https://arxiv.org/abs/1802.03321*, 2018.