Privacy Verification in POMDPs via Barrier Certificates

Mohamadreza Ahmadi* Bo Wu* Hai Lin Ufuk Topcu

Abstract— **Privacy is an increasing concern in cyber-physical systems that operates over a shared network. In this paper, we propose a method for privacy verification of cyber-physical systems modeled by Markov decision processes (MDPs) and partially-observable Markov decision processes (POMDPs) based on barrier certificates. To this end, we consider an opacity-based notion of privacy, which is characterized by the beliefs in system states. We show that the belief update equations can be represented as discrete-time switched systems, for which we propose a set of conditions for privacy verification in terms of barrier certificates. We further demonstrate that, for MDPs and for POMDPs, privacy verification can be computationally implemented by solving a set of semi-definite programs and sum-of-squares programs, respectively. The method is illustrated by an application to privacy verification of an inventory management system.**

I. INTRODUCTION

Privacy is becoming a rising concern in many modern engineering systems which are increasingly connected over shared infrastructures, such as power grids [1], healthcare systems [2], smart home [3], transportation systems [4], and etc. Potentially malicious intruders may have access to the information available publicly or privately based on which they attempt to infer some "secret" associated with the system, such as personal activity preferences, health conditions, and bank account details. If the privacy is compromised, it could lead to substantial social or economic loss. Therefore, it is of fundamental importance to design cyber-physical systems that are provably safe against privacy breaches.

In recent years, a privacy notion called "opacity" has received significant attention. Generally speaking, opacity is a confidentiality property that characterizes a system's capability to conceal its "secret" information from being inferred by outside observers. These observers are assumed to have full knowledge of the system model, often as a finite automaton, and can observe or partially observe the behaviors of the system, such as the actions performed, but not the states of the system directly. Various notions of opacity, depending on whether the secret is the behavior of the system in regular languages, initial states, or the current states, have been proposed [5] and their verification and enforcement are studied in deterministic and probabilistic systems [6].

M. Ahmadi and U. Topcu are with the Department of Aerospace Engineering and Engineering Mechanics, and the Institute for Computational Engineering and Sciences (ICES), University of Texas, Austin, 201 E 24th St, Austin, TX 78712. B. Wu and H. Lin are with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA. e-mail: ({mrahmadi, utopcu}@utexas.edu,{bwu3, hlin1}@nd.edu).

* M. Ahmadi and B. Wu contributed equally to this work.

Most existing results on opacity only consider the absolute certainty of the occurrence of the secret as the privacy violation. However, in practice, in many (partially observable) probabilistic systems, the intruder may only maintain a belief over the system secrets through Bayesian inference, which may still pose a security threat if the intruder has a high confidence that a secret has been observed. Hence, a new opacity notion was introduced in [7] for Markov decision processes (MDPs), where the system is considered opaque, if the intruder's confidence that the current state is a secret state never exceeds a given threshold.

In this paper, in addition to studying privacy verification in MDPs, we study partially observable MDP (POMDP) models with the privacy metric based on opacity. POMDPs generalize MDPs with partial observability and are popular in sequential decision-making [8]. Existing studies on POMDPs mostly consider model checking against a given specification [9], or policy synthesis to optimize a given performance metric [10]. Privacy issues in POMDP planning have gained interest only recently. For example, in [11], privacy is quantified as the average conditional entropy to be minimized while optimizing the task-related reward in a power grid. An accumulated discounted minimal Bayesian risk was defined in [12] as the privacy breach metric to be optimized. Like these two papers, most existing work focuses on privacy measures that are averaged over time. However, minimizing a time average may not be sufficient in some circumstances, because it does not guarantee that the intruder will not have a fairly high confidence about the secret at *some time instant*. In contrast, our notion of privacy is supposed to be satisfied *at any time*.

A key observation we use in [7] is that the intruder's belief update dynamics can be characterized as an autonomous discrete-time switched system whose switching signals are the observed actions. Then, the privacy verification problem can be equivalently cast into verifying whether the solutions of the belief switched system avoid a privacy unsafe subset of the belief space, where the privacy specification is violated.

Safety verification is a familiar subject to the control community [13], [14], [15], [16], [17]. One of the methods for safety verification relies on the construction of a function of the states, called the *barrier certificate* that satisfies a Lyapunov-like inequality [15]. The barrier certificates have shown to be useful in several system analysis and control problems running the gamut of bounding moment functional of stochastic systems [18] to collision avoidance of multi-robot systems [19]. It was also shown in [20] that any safe dynamical system admits a barrier certificate.

In this paper, we propose conditions for privacy veri-

fication of MDPs and POMDPs using barrier certificates. From a computational stand point, we formulate a set of semi-definite programs (SDPs) and sum-of-squares programs (SOSP) to verify the privacy requirement of MDPs and POMDPs, respectively. We apply the proposed method to a case study of privacy verification of an inventory management system.

The rest of this paper is organized as follows. In the subsequent section, we present some definitions related to MDPs, POMDPs, belief dynamics and privacy. In Section III, we propose a set of conditions for privacy verification of belief equations represented as discrete-time switched systems based on barrier certificates. In Section IV, we apply the method based on barrier certificates to the privacy verification problem of MDPs and POMDPs, and present a set of SDP and SOSP sufficient conditions, respectively. In Section V, we elucidate the proposed privacy verification methodology with an inventory management example. Finally, in Section VI, we conclude the paper and give directions for future research.

Notation: The notations employed in this paper are relatively straightforward. $\mathbb{R}_{\geq 0}$ denotes the set $[0, \infty)$ and $\mathbb{Z}_{\geq 0}$ denotes the set of integers $\{0, 1, 2, \ldots\}$. For a finite set A, we denote by $|A|$ the cardinality of the set A. Given a matrix Q, we denote by Q^T the transpose of Q. The notation $0_{n\times m}$ is the $n \times m$ matrix with zero entries. For two vectors, a and b with the same size, $a \succeq b$ implies entry-wise inequality. $\mathcal{R}[x]$ accounts for the set of polynomial functions with real coefficients in $x \in \mathbb{R}^n$, $p : \mathbb{R}^n \to \mathbb{R}$ and $\Sigma \subset \mathcal{R}$ is the subset of polynomials with an SOS decomposition; i.e., $p \in \Sigma[x]$ if and only if there are $p_i \in \mathcal{R}[x],\ i \in \{1, \ldots, k\}$ such that $p = p_i^2 + \cdots + p_k^2$.

II. Preliminaries

A. MDP

MDPs [21] are decision-making modeling framework in which the actions have stochastic outcomes. An MDP $\mathcal{M} = (Q, \pi, A, T)$ has the following components:

- Q is a finite set of states with indices $\{1, 2, \ldots, n\}$.
- $\pi : Q \to [0, 1]$ defines the distribution of the initial states, i.e., $\pi(q)$ denotes the probability of starting at $q \in Q$.
- A is a finite set of actions.
- $T : Q \times A \times Q \to [0, 1]$ is the probabilistic transition function where

$$T(q, a, q') := P(q_t = q' | q_{t-1} = q, a_{t-1} = a), \quad \forall t \in \mathbb{Z}_{\geq 1}, q, q' \in Q, a \in A.$$

B. POMDP

POMDPs provide a more general mathematical framework to consider not only the stochastic outcomes of actions, but also the imperfect state observations [22]. Formally, a POMDP $\mathcal{P} = (Q, \pi, A, T, Z, O)$ is defined with the following components:

- Q, π, A, T are the same as the definition of an MDP.
- Z is the set of all possible observations. Usually $z \in Z$ is an incomplete projection of the world state q, contaminated by sensor noise.
- $O : Q \times A \times Z \to [0, 1]$ is the observation function where

$$O(q, a, z) := P(z_t = z | q_t = q, a_{t-1} = a), \quad \forall t \in \mathbb{Z}_{\geq 1}, q \in Q, a \in A, z \in Z.$$

Furthermore, we assume that there is a set of secret states $Q_s \subset Q$ and we would like to conceal the information that the system is currently in some secret state $q \in Q_s$.

C. Belief Update Equations as Discrete-Time Switched Systems

In [7], we considered the case that given a system modeled as an MDP $\mathcal{M}$, there is an intruder with potentially malicious intention that can observe the actions executed but not the states of the system, and tries to determine whether the system is currently in some secret state with a high confidence. If all the actions are available at every state, then from the intruder's point of view, the system is actually a POMDP with trivially the same observation for every state (since it cannot observe the states at all). In this case, the intruder may maintain a belief $b_{t-1} : Q \to [0, 1], \sum_{q\in Q} b_t(q) = 1$ over Q at time $t-1$. The belief at $t = 0$ is defined as $b_0(q) = \pi(q)$ and $b_t(q)$ denotes the probability of system being in state q at time t. At time $t+1$, when action $a \in A$ is observed, the belief update can be described as

$$b_t(q') = \sum_{q\in Q} P(q, a, q') b_{t-1}(q). \tag{1}$$

We also consider systems modeled as a POMDP, where we assume that the intruder may have access to the observations in addition to the executed actions. Therefore, the intruder has to consider a complete history of the past actions and observations to update its belief with Bayes rule:

$$\begin{aligned} b_t(q') &= P(q' | z_t, a_{t-1}, b_{t-1}) \\ &= \frac{P(z_t | q', a_{t-1}, b_{t-1}) P(q' | a_{t-1}, b_{t-1})}{P(z_t | a_{t-1}, b_{t-1})} \\ &= \frac{P(z_t | q', a_{t-1}, b_{t-1}) \sum_{q\in Q} P(q' | a_{t-1}, b_{t-1}, q) P(q | a_{t-1}, b_{t-1})}{P(z_t | a_{t-1}, b_{t-1})} \\ &= \frac{O(q', a_{t-1}, z_t) \sum_{q\in Q} T(q, a_{t-1}, q') b_{t-1}(q)}{\sum_{q'\in Q} O(q', a_{t-1}, z_t) \sum_{q\in Q} T(q, a_{t-1}, q') b_{t-1}(q)}. \end{aligned} \tag{2}$$

D. Privacy in Belief Space

Our notion of privacy is defined on the belief space of the intruder, where we require that the intruder, even with access to the actions and observations since $t = 0$, is never confident that the system is in a secret state with a probability larger than or equal to a constant $\lambda \in [0, 1]$, at any time t:

$$\sum_{q\in Q_s} b_t(q) \leq \lambda, \forall t. \tag{3}$$

The notion of privacy used in this paper is closely related to the current-state opacity (CSO) in discrete event systems [6]. The CSO definition provides a deterministic notion

of privacy in that privacy is breached when the intruder is absolutely sure that the system is currently in a secret state. On the other hand, in our formulation, the privacy requirement is violated when the intruder is confident with a probability over some threshold.

III. Privacy Verification Using Barrier Certificates

The belief update equations for MDPs (1) and POMDPs (2) are discrete-time switched system where the actions $a \in A$ define the switching modes. In the sequel, we develop a technique based on barrier certificates for privacy verification of belief update equations represented as discrete-time switched systems.

Consider the following belief dynamics

$$b_t = f_a(b_{t-1}), \tag{4}$$

where b denote the belief vector belonging to the belief space hyper-cube $[0,1]^{|Q|}$, $a \in A$ is the action that can be interpreted as the switching mode index, $t \in \mathbb{Z}_{\geq 1}$ denote the discrete time instances, the vector fields $\{f_a\}_{a\in A}$ with $f_a : [0,1]^{|Q|} \to [0,1]^{|Q|}$, and $b_0 \in \mathcal{B}_0 \subset [0,1]^{|Q|}$ representing the set of initial beliefs. We also define a privacy unsafe set $\mathcal{B}_u \subset [0,1]^{|Q|}$, where the privacy requirement is violated. Verifying whether all the belief evolutions of (4) starting at $\mathcal{B}_0$ avoid a given privacy unsafe set $\mathcal{B}_u$ at a pre-specified time T or for all time is a cumbersome task in general and requires simulating (4) for all elements of the set $\mathcal{B}_0$ and for different sequences of $a \in A$. Furthermore, POMDPs are often computationally intractable to solve exactly [23]. To surmount these challenges, we demonstrate that we can find a barrier certificate which verifies that a given privacy requirement is not violated without the need to solve the belief update equations or the POMDPs directly.

Theorem 1: Consider the belief update equation (4). Given a set of initial beliefs $\mathcal{B}_0 \subset [0,1]^{|Q|}$, an unsafe set $\mathcal{B}_u \subset [0,1]^{|Q|}$ ($\mathcal{B}_0 \cap \mathcal{B}_u = \emptyset$), and a constant T, if there exists a function $B : \mathbb{Z} \times [0,1]^{|Q|} \to \mathbb{R}$ such that

$$B(T, b_T) > 0, \quad \forall b_T \in \mathcal{B}_u, \tag{5}$$

$$B(0, b_0) < 0, \quad \forall b_0 \in \mathcal{B}_0, \tag{6}$$

and

$$B(t, f_a(b_{t-1})) - B(t-1, b_{t-1}) \leq 0, \quad \forall t \in \{1, 2, \ldots, T\},\ \forall a \in A, \tag{7}$$

then there exist no solution of belief update equation (4) such that $b_0 \in \mathcal{B}_0$, and $b_T \in \mathcal{B}_u$ for all $a \in A$.

Proof: The proof is carried out by contradiction. Assume at time instance T there exit a solution to (4) such that $b_0 \in \mathcal{B}_0$ and $b_T \in \mathcal{B}_u$. From inequality (7), we have

$$B(t, b_t) \leq B(t-1, b_{t-1})$$

for all $t \in \{1, 2, \ldots, T\}$ and all actions $a \in A$. Hence, $B(t, b_t) \leq B(0, b_0)$ for all $t \in \{1, 2, \ldots, T\}$. Furthermore, inequality (6) implies that

$$B(0, b_0) < 0$$

for all $b_0 \in \mathcal{B}_0$. Since the choice of T can be arbitrary, this is a contradiction because it implies that $B(T, b_T) \leq B(0, b_0) < 0$. Therefore, there exist no solution of (4) such that $b_0 \in \mathcal{B}_0$ and $b_T \in \mathcal{B}_u$ for any sequence of actions $a \in A$. ■

Theorem 1 checks whether the privacy requirement is not violated at a particular point in time T. We can generalize this theorem to the case for verifying privacy for all time. In this case, the barrier certificate is time-invariant.

Corollary 1: Consider the belief switched dynamics (4). Given a set of initial conditions $\mathcal{B}_0 \subset [0,1]^{|Q|}$, and an unsafe set $\mathcal{B}_u \subset [0,1]^{|Q|}$ ($\mathcal{B}_0 \cap \mathcal{B}_u = \emptyset$), if there exists a function $B : [0,1]^{|Q|} \to \mathbb{R}$ such that

$$B(b) > 0, \quad \forall b \in \mathcal{B}_u, \tag{8}$$

$$B(b) < 0, \quad \forall b \in \mathcal{B}_0, \tag{9}$$

and

$$B\left(f_a(b_{t-1})\right) - B(b_{t-1}) \leq 0, \tag{10}$$

then there exist no solution of (4) such that $b_0 \in \mathcal{X}_0$ and $b_t \in \mathcal{X}_u$ for all $t \in \mathbb{Z}_{\geq 1}$ and any sequence of actions $a \in A$. Hence, the privacy requirement is not violated.

IV. Privacy Verification in MDPs and POMDPs

In the previous section, we discussed conditions for privacy verification of general belief update equations using barrier certificates. Next, we show that the barrier certificates can be used for privacy verification of MDPs and POMDPs. To this end, we define the privacy unsafe set $\mathcal{B}_u$ to be the complement of the privacy requirement (3) inspired by the notion of opacity. That is,

$$\mathcal{B}_u = \left\{ b \in \mathbb{R}^{|Q|} \mid \sum_{q \in Q_s} b_t(q) > \lambda \right\}. \tag{11}$$

Hence, given a set of initial beliefs $\mathcal{B}_0$, if there exists a barrier certificate verifying privacy with respect to $\mathcal{B}_u$, then we infer that the privacy requirement is satisfied, i.e., $\sum_{q\in Q_s} b_t(q) \leq \lambda$.

In the following, we formulate a set of conditions in terms of SDPs or SOSPs (refer to Appendix A for more details on SOSPs) to verify whether a given MDP or a POMDP, respectively, satisfies a privacy requirement.

A. Privacy Verification for MDPs via SDPs

For MDPs, the belief update equation can be described as a linear discrete-time switched system

$$b_{t+1}(q') = H_a\ b_t(q') = \sum_{q \in Q} P(q, a, q') b_t(q), \tag{12}$$

where $H_a \in \mathbb{R}^{|Q|\times|Q|}$, $a \in A$. Furthermore, the privacy requirement (11) describes a half-space in the belief space hyper-cube. Denote by $\bar{b}$ the augmentation of the belief states by 1, i.e., $\bar{b} = \begin{bmatrix} b^T & 1 \end{bmatrix}^T \in \mathbb{R}^{|Q|+1}$. We define the set of initial beliefs to be a convex polytope represented by the

intersection of a set of half-spaces in the augmented belief space

$$\mathcal{B}_0 = \left\{ b_0 \in \mathbb{R}^{|Q|} \mid \bar{E}_0^T \bar{b}_0 \succeq 0_{n_0} \right\}, \tag{13}$$

where $\bar{E}_0 \in \mathbb{R}^{n_0 \times (|Q|+1)}$.

The privacy unsafe set can be re-written, respectively, as

$$\mathcal{B}_u = \left\{ b \in \mathbb{R}^{|Q_s|} \mid \bar{b}^T \bar{W} \bar{b} > 0 \right\}, \tag{14}$$

where

$$\bar{W} = \begin{bmatrix} 0_{|Q| \times |Q|} & 0_{1\times 1} \\ \boldsymbol{w}^T & -\lambda \end{bmatrix},$$

with $\boldsymbol{w} \in \mathbb{R}^{|Q|}$ and $\boldsymbol{w}(i) = 1$ for $i = q \in Q_s$ and $\boldsymbol{w}(i) = 0$ otherwise.

At this point, we are ready to state the SDP conditions for verifying privacy of a given MDP.

Corollary 2: Consider the MDP belief update dynamics as given in (12), the unsafe set (14), and the set of initial beliefs (13). If there exist a matrix $V \in \mathbb{S}^{|Q|+1}$, a matrix with positive entries $U \in \mathbb{S}^{n_0}$, and a positive constant s^u such that

$$V - s^u \bar{W} > 0, \tag{15}$$

$$-V - \bar{E}_0 U \bar{E}_0^T > 0, \tag{16}$$

and

$$H_a^T V H_a - V < 0, \quad \forall a \in A, \tag{17}$$

then the privacy requirement (3) is satisfied for all time.

Proof: We show that each of the SDP conditions of (15)-(17) correspond to conditions (8)-(10), respectively, for the barrier certificate

$$B(\bar{b}) = \bar{b}^T(q)\ V\ \bar{b}(q).$$

Multiplying both sides of (15) from left and right respectively with $\bar{b}^T(q)$ and $\bar{b}(q)$, respectively, gives

$$\bar{b}^T(q) V \bar{b}(q) - s^u \bar{b}^T(q) \bar{W} \bar{b}(q) > 0.$$

Since $s^u > 0$, from S-procedure, we conclude that $\bar{b}^T(q) V \bar{b}(q) > 0$ only if $\bar{b}^T(q) \bar{W} \bar{b}(q) > 0$ (because $\bar{b}^T V \bar{b}(q) > s^u \bar{b}^T(q) \bar{W} \bar{b}(q)$). Moreover, $\bar{b}^T(q) \bar{W} \bar{b}(q) > 0$ implies that $\sum_{q \in Q_s} b_t(q) > \lambda$. Therefore, condition (8) is satisfied. Similarly, we can show, via S-procedure [24], that if the linear matrix inequality (16) is satisfied, condition (9) holds. This is due to the fact that the polytope $\mathcal{B}_0$ is contained in the ellipsoid represented by $\bar{b}^T \bar{E}_0 U \bar{E}_0^T \bar{b} > 0$ and the positive entries of U are the S-procedure coefficients based on the construction in [25, p. 76].

Finally, multiplying both sides of (17) from left and right respectively with $\bar{b}^T(q)$ and $\bar{b}(q)$ yields

$$\bar{b}^T(q) \left(H_a^T V H_a - V \right) \bar{b}(q) < 0, \quad \forall a \in A.$$

That is,

$$\bar{b}^T(q) H_a^T V H_a \bar{b}(q) - \bar{b}^T(q) V \bar{b}(q) < 0, \quad \forall a \in A,$$

which in turn implies that (10) holds for $B(\bar{b}) = \bar{b}^T(q)\ V\ \bar{b}(q)$. Therefore, from Corollary 1, the solutions of the MDP belief update equation (12) are safe with respect to the privacy unsafe set (14). Hence, the privacy requirement is satisfied. ■

B. Privacy Verification for POMDPs via SOSP

The belief update equation (2) for a POMDP is a rational function in the belief states $b_t(q)$, $q \in Q_s$

$$\begin{aligned} b_t(q') &= \frac{S_a\left(b_{t-1}(q')\right)}{R_a\left(b_{t-1}(q')\right)} \\ &= \frac{O(q', a_{t-1}, z_t) \sum_{q \in Q} T(q, a_{t-1}, q') b_{t-1}(q)}{\sum_{q' \in Q} O(q', a_{t-1}, z_t) \sum_{q \in Q} T(q, a_{t-1}, q') b_{t-1}(q)} \end{aligned} \tag{18}$$

Moreover, the privacy unsafe set (11) is a semi-algebraic set, since it can be described by a polynomial inequality. We further assume the set of initial beliefs is also given by a semi-algebraic set

$$\mathcal{B}_0 = \left\{ b_0 \in \mathbb{R}^{|Q_s|} \mid l_i^0(b_0) \leq 0,\ i = 1, 2, \ldots, n_0 \right\}. \tag{19}$$

At this stage, we are ready to present conditions based on SOSP to verify privacy of a given POMDP.

Corollary 3: Consider the POMDP belief update dynamics (18), the privacy unsafe set (11), the set of initial beliefs (19), and a constant $T > 0$. If there exist polynomial functions $B \in \mathcal{R}[t, b]$ with degree d, $p^u \in \Sigma[b]$, $p_i^0 \in \Sigma[b]$, $i = 1, 2, \ldots, n_0$, and constants $s_1, s_2 > 0$ such that

$$B\left(T, b_T\right) - p^u(b_T) \left(\sum_{q \in Q_s} b_T(q) - \lambda \right) - s_1 \in \Sigma\left[b_T\right], \tag{20}$$

$$-B\left(0, b_0\right) + \sum_{i=1}^{n_0} p_i^0(b_0) l_i^0(b_0) - s_2 \in \Sigma\left[b_0\right], \tag{21}$$

and

$$\begin{aligned} -R_a\left(b_{t-1}\right)^d \left(B\left(t, \frac{S_a\left(b_{t-1}\right)}{R_a\left(b_{t-1}\right)}\right) - B(t-1, b_{t-1}) \right) \\ \in \Sigma[t, b_{t-1}], \quad \forall t \in \{1, 2, \ldots, T\}, \end{aligned} \tag{22}$$

then the privacy requirement (3) is satisfied for all $t \in \{1, 2, \ldots, T\}$.

Proof: SOS conditions (20) and (21) are a direct application of Propositions 1 and 2 in Appendix A to verify conditions (5) and (6), respectively. Furthermore, condition (7) for system (18) can be re-written as

$$B\left(t, \frac{S_a\left(b_{t-1}\right)}{R_a\left(b_{t-1}\right)}\right) - B(t-1, b_{t-1}) > 0.$$

Given the fact that $R_a\left(b_{t-1}(q')\right)$ is a positive polynomial of degree one, we can relax the above inequality into an SOS condition given by

$$\begin{aligned} -R_a\left(b_{t-1}\right)^d \left(B\left(t, \frac{S_a\left(b_{t-1}\right)}{R_a\left(b_{t-1}\right)}\right) - B\left(t-1, b_{t-1}\right) \right) \\ \in \Sigma[t, b_{t-1}]. \end{aligned}$$

Hence, if (22) holds, then (7) is satisfied as well. Then, from Theorem 1, we infer that there is no $b_t(q)$ at time T such that $b_0(q) \in \mathcal{B}_0$ and $\sum_{q\in Q_s} b_T(q) > \lambda$. Equivalently, the privacy requirement is satisfied at time T. That is, $\sum_{q\in Q_s} b_T(q) \leq \lambda$. ■

We can also verify privacy for all time for a given POMDP, which is based on Corollary 1.

Corollary 4: Consider the POMDP belief update dynamics (18), the privacy unsafe set (11), and the set of initial beliefs (19). If there is exist polynomial functions $B \in \mathcal{R}[b]$ with degree d, $p^u \in \Sigma[b]$, $p_i^0 \in \Sigma[b]$, $i = 1, 2, \ldots, n_0$, and constants $s_1, s_2 > 0$ such that

$$B(b) - p^u(b)\left(\sum_{q\in Q_s} b(q) - \lambda\right) - s_1 \in \Sigma[b], \tag{23}$$

$$-B(b_0) + \sum_{i=1}^{n_0} p_i^0(b_0) l_i^0(b_0) - s_2 \in \Sigma[b_0], \tag{24}$$

and

$$-R_a(b_{t-1})^d \left(B\left(\frac{S_a(b_{t-1})}{R_a(b_{t-1})}\right) - B(b_{t-1})\right) \in \Sigma[b_{t-1}], \tag{25}$$

then the privacy requirement (3) is satisfied for all time.

V. Numerical Example: Privacy in an Inventory Management System

In this section, we illustrate the proposed privacy verification method by applying it to an inventory management system. The numerical experiments are carried out on a MacBook Pro 2.9GHz Intel Core i5 and 8GB of RAM. The SDPs are solved using YALMIP [26] and the SOSPs are solved using the SOSTOOLs [27] parser and solvers such as Sedumi [28].

A. Example I

We use the same example from [7]. Suppose the MDP $\mathcal{M}$ has three states $Q = \{q_1, q_2, q_3\}$ representing different inventory levels of a company. The states $q_2, q_3 \in Q_s$ correspond to the low and high inventory levels, respectively, and are the secret states. If the intruder, say a competitor or a supplier, has information over the current inventory levels being high or low, they may manipulate the price of the goods, and thus negatively affect the company's profit. Therefore, it is of the company's interest to conceal the inventory levels from the potential intruders. q_1 is a non-secret state representing the normal inventory level. $A = \{\sigma_1, \sigma_2\}$ represents two different actions denoting different purchasing quantities. The initial condition is $\pi(s_1) = 0.1, \pi(s_2) = 0.2, \pi(s_3) = 0.2$. The transition probabilities are as shown in the following matrices for action σ_1 and σ_2, $H_{\sigma_a}(i,j) = T(q_j, \sigma, q_i)$.

$$H_{\sigma_1} = \begin{bmatrix} 0.15, & 0.2, & 0.3 \\ 0.45, & 0.2, & 0.2 \\ 0.4, & 0.6, & 0.5 \end{bmatrix}, H_{\sigma_2} = \begin{bmatrix} 0.25, & 0.35, & 0.1 \\ 0.25, & 0.1, & 0.5 \\ 0.5, & 0.55, & 0.4 \end{bmatrix} \tag{26}$$

The randomness of the inventory level after the purchasing action is due to the random demand levels. The privacy requirement is

$$b_t(q_2) + b_t(q_3) \leq \gamma, \forall t. \tag{27}$$

Based on Corollary 2, we check whether the above privacy requirement is satisfied for $\gamma = 0.85$. The SDPs (15) to (17) are solved certifying that the privacy requirement (27) is satisfied, where we found the following barrier certificate (up to 0.01 precision) in 2.5803 seconds

$$B(\bar{b}) = \begin{bmatrix} b(q_1) \\ b(q_2) \\ b(q_3) \\ 1 \end{bmatrix}^T \begin{bmatrix} 2.98 & -0.83 & -0.61 & 0 \\ -0.83 & 0.07 & 3.89 & 0.92 \\ -0.61 & 3.89 & -1.33 & -0.74 \\ 0 & 0.92 & -0.74 & 1.72 \end{bmatrix} \begin{bmatrix} b(q_1) \\ b(q_2) \\ b(q_3) \\ 1 \end{bmatrix}.$$

Therefore, the high and low inventory levels are private. Furthermore, in order to find the best achievable privacy requirement, we decrease γ and search for a barrier certificate based on Corollary 2. We could find the smallest value for $\gamma^* = 0.42$ below which no certificate for privacy verification could be found.

B. Example II

Following our MDP example, besides the purchasing action, the intruder may also have access to the intervals between the two consecutive purchases, which suggests a POMDP $\mathcal{P}$ model that has the same state space Q, initial condition π, action set A, transition probabilities T. Additionally, $\mathcal{P}$ has the observation set $Z = \{z_0, z_1\}$ which represents a short and a long purchasing intervals respectively. The observation function is defined as below where $O_\sigma(i,j) = O(q_i, \sigma, z_j)$

$$O_{\sigma_1} = \begin{bmatrix} 0.7, & 0.3 \\ 0.5, & 0.5 \\ 0.8, & 0.2 \end{bmatrix}, O_{\sigma_2} = \begin{bmatrix} 0.8, & 0.2 \\ 0.6, & 0.4 \\ 0.2, & 0.8 \end{bmatrix}. \tag{28}$$

The privacy requirement is (27) with $\gamma = 0.42$ to make sure that the inventory level being too high or too low is not disclosed with confidence larger than 0.42. We check the SOSPs (23) to (25) where fix the degree d of the barrier certificate. We could not find a certificate for privacy even for $d = 10$. In order to find an upper-bound on the achievable privacy requirement, we increase the degree of the barrier certificates from 2 to 10 and look for the smallest value of γ, for which privacy verification could be certified. Table I outlines the obtained results. As it can be observed from the table, by increasing the degree of the barrier certificate, we can find a tighter upper-bound on the best achievable privacy level. The barrier certificate of degree 2 (excluding terms smaller than 10^{-4}) constructed using Corollary 4 is provided below

$$\begin{aligned} B(b) = {} & 0.1629b(q_1)^2 - 3.9382b(q_2)^2 + 09280b(q_3)^2 \\ & - 0.0297b(q_1)b(q_2) - 4.4451b(q_2)b(q_3) - 0.0027b(q_1) \\ & - 2.0452b(q_2) + 9.2633. \end{aligned}$$

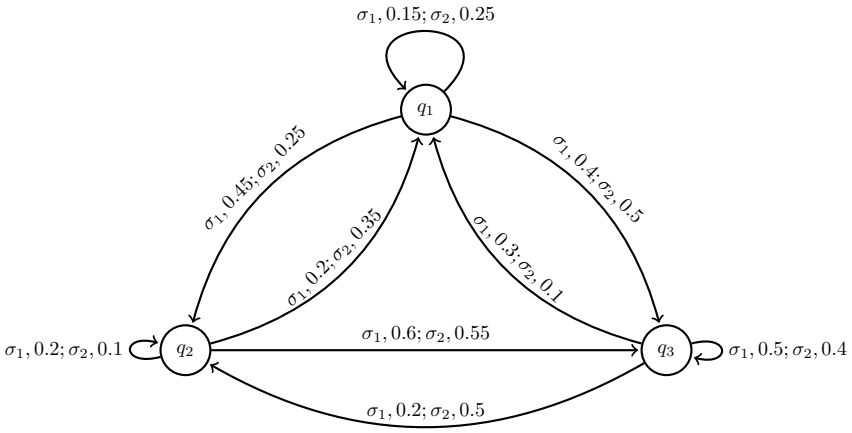

Fig. 1: The MDP in Example I

TABLE I: Numerical results for Example II.

d	2	4	6	8	10
γ^*	0.93	0.88	0.80	0.74	0.69
Computation Time (s)	5.38	8.37	12.03	18.42	27.09

VI. CONCLUSIONS AND FUTURE WORK

We proposed a method for privacy verification of MDPs and POMDPs based on barrier certificates. We demonstrated that the privacy verification can be carried out in terms of an SDP problem for MDPs and an SOSP problem for POMDPs. The method was applied to the privacy verification problem of an inventory management system.

The formulation presented here assumes a unified barrier certificate for all actions $a \in A$. A more conservative but more computationally efficient approach to address the privacy verification problem of MDPs and POMDPs is to consider non-smooth barrier certificates, which are composed of a the convex hull, max, or min a set of local barrier certificates for different actions [29], [30].

In addition to privacy verification, the proposed method based on barrier certificates can be used to design a sequence of actions such that some given privacy requirement is satisfied. To this end, we follow the footsteps of the contributions on synthesizing switching sequences such that some cost is minimized [31].

REFERENCES

[1] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009.

[2] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2018.

[3] K. L. Courtney, "Privacy and senior willingness to adopt smart home information technology in residential care facilities," 2008.

[4] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[5] Y.-C. Wu and S. Lafortune, "Comparative analysis of related notions of opacity in centralized and coordinated architectures," *Discrete Event Dynamic Systems*, vol. 23, no. 3, pp. 307–339, 2013.

[6] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annual Reviews in Control*, vol. 41, pp. 135–146, 2016.

[7] B. Wu and H. Lin, "Privacy preserving controller synthesis via belief abstraction," *arXiv preprint arXiv:1802.10051*, 2018.

[8] A. R Cassandra, "A survey of pomdp applications," vol. 1724, January 1998.

[9] K. Chatterjee, M. Chmelík, and M. Tracol, "What is decidable about partially observable markov decision processes with ω-regular objectives," *Journal of Computer and System Sciences*, vol. 82, no. 5, pp. 878–911, 2016.

[10] S. Junges, N. Jansen, R. Wimmer, T. Quatmann, L. Winterer, J.-P. Katoen, and B. Becker, "Permissive finite-state controllers of pomdps using parameter synthesis," *arXiv preprint arXiv:1710.10294*, 2017.

[11] J. Yao and P. Venkitasubramaniam, "The privacy analysis of battery control mechanisms in demand response: Revealing state approach and rate distortion bounds," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2417–2425, 2015.

[12] Z. Li, T. J. Oechtering, and M. Skoglund, "Privacy-preserving energy flow control in smart grids," in *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on*. IEEE, 2016, pp. 2194–2198.

[13] H. Guéguen, M. Lefebvre, J. Zaytoon, and O. Nasri, "Safety verification and reachability analysis for hybrid systems," *Annual Reviews in Control*, vol. 33, no. 1, pp. 25 – 36, 2009.

[14] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986–1001, July 2003.

[15] S. Prajna, "Barrier certificates for nonlinear model validation," *Automatica*, vol. 42, no. 1, pp. 117 – 126, 2006.

[16] S. Han, U. Topcu, and G. J. Pappas, "A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems," in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 2049–2054.

[17] M. Ahmadi, G. Valmorbida, and A. Papachristodoulou, "Safety verification for distributed parameter systems using barrier functionals," *Systems & Control Letters*, vol. 108, pp. 33 – 39, 2017.

[18] M. Ahmadi, A. W. K. Harris, and A. Papachristodoulou, "An optimization-based method for bounding state functionals of nonlinear stochastic systems," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 5342–5347.

[19] L. Wang, A. D. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Transactions on Robotics*, vol. 33, no. 3, pp. 661–674, June 2017.

[20] R. Wisniewski and C. Sloth, "Converse barrier certificate theorems," *IEEE Transactions on Automatic Control*, vol. 61, no. 5, pp. 1356–1361, May 2016.

[21] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming*. John Wiley & Sons, 2014.

[22] G. Shani, J. Pineau, and R. Kaplow, "A survey of point-based pomdp solvers," *Autonomous Agents and Multi-Agent Systems*, vol. 27, no. 1, pp. 1–51, 2013.

[23] M. Hauskrecht, "Value-function approximations for partially observable Markov decision processes," *Journal of Artificial Intelligence Research*, vol. 13, no. 1, pp. 33–94, Aug. 2000.
[24] I. Polik and T. Terlaky, "A survey of the S-lemma," *SIAM Review*, vol. 49, no. 3, pp. 371–418, 2007.
[25] M. Johansson, "Piecewise linear control systems," Ph.D. dissertation, Lund Institute of Technology, 1999.
[26] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in MATLAB," in *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004. [Online]. Available: http://control.ee.ethz.ch/~joloef/yalmip.php
[27] S. Prajna, A. Papachristodoulou, P. Seiler, and P. Parrilo, "SOSTOOLS: Sum of squares optimization toolbox for MATLAB V3.00," 2013.
[28] J. F. Sturm, "Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones," 1998.
[29] P. Glotfelter, J. Cortés, and M. Egerstedt, "Nonsmooth barrier functions with applications to multi-robot systems," *IEEE Control Systems Letters*, vol. 1, no. 2, pp. 310–315, Oct 2017.
[30] M. Ahmadi, A. Israel, and U. Topcu, "Controller synthesis for safety of physically-viable data-driven models," *arXiv preprint arXiv:1801.04072*, 2018.
[31] B. Stellato, S. Ober-Blöbaum, and P. J. Goulart, "Second-order switching time optimization for switched dynamical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 5407–5414, Oct 2017.
[32] P. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, California Institute of Technology, 2000.
[33] M. Choi, T. Y. Lam, and B. Reznick, "Sums of squares of real polynomials," in *Proceedings of Symposia in Pure mathematics*, vol. 58. American Mathematical Society, 1995, pp. 103–126.
[34] G. Chesi, A. Tesi, A. Vicino, and R. Genesio, "On convexification of some minimum distance problems," in *5th European Control Conference*, Karlsruhe, Germany, 1999.
[35] M. Nie, J.and Schweighofer, "On the complexity of Putinar's positivstellensatz," *Journal of Complexity*, vol. 23, no. 1, pp. 135–150, 2007.
[36] J. B. Lasserre, *Moments, Positive Polynomials and Their Applications*. Imperial College Press, London, 2009.
[37] G. Chesi, "LMI techniques for optimization over polynomials in control: a survey," *IEEE Transactions on Automatic Control*, vol. 55, no. 11, pp. 2500–2510, 2010.

APPENDIX

A. Sum-of-Squares Polynomials

A polynomial $p(x)$ is a sum-of-squares polynomial if $\exists p_i(x) \in \mathcal{R}[x]$, $i \in \{1, \dots, n_d\}$ such that $p(x) = \sum_i p_i^2(x)$. Hence $p(x)$ is clearly non-negative. A set of polynomials p_i is called *SOS decomposition* of $p(x)$. The converse does not hold in general, that is, there exist non-negative polynomials which do not have an SOS decomposition [32]. The computation of SOS decompositions, can be cast as an SDP (see [33], [32], [34]). The Theorem below proves that, in sets satisfying a property stronger than compactness, any positive polynomial can be expressed as a combination of sum-of-squares polynomials and polynomials describing the set.

For a set of polynomials $\bar{g} = \{g_1(x), \dots, g_m(x)\}$, $m \in \mathbb{N}$, the *quadratic module* generated by m is

$$M(\bar{g}) := \left\{ \sigma_0 + \sum_{i=1}^{m} \sigma_i g_i | \sigma_i \in \Sigma[x] \right\}. \tag{29}$$

A quadratic module $M \in \mathcal{R}[x]$ is said *archimedean* if $\exists N \in \mathbb{N}$ such that

$$N - |x|^2 \in M.$$

An archimedian set is always compact [35]. It is the possible to state [36, Theorem 2.14]

Theorem 2 (Putinar Positivstellensatz): Suppose the quadratic module $M(\bar{g})$ is archimedian. Then for every $f \in \mathcal{R}[x]$,

$$f > 0 \ \forall \ x \in \{x | g_1(x) \geq 0, \dots, g_m(x) \geq 0\} \Rightarrow f \in (\bar{g}).$$

The subsequent proposition formalizes the problem of constrained positivity of polynomials which is a direct result of applying Positivstellensatz.

Proposition 1 ([37]): Let $\{a_i\}_{i=1}^k$ and $\{b_i\}_{i=1}^l$ belong to $\mathcal{P}$, then

$$p(x) \geq 0 \qquad \forall x \in \mathbb{R}^n : a_i(x) = 0, \forall i = 1, 2, ..., k \quad \text{and} \quad b_j(x) \geq 0, \forall j = 1, 2, ..., l \tag{30}$$

is satisfied, if the following holds

$$\exists r_1, r_2, \dots, r_k \in \mathcal{R}[x] \quad \text{and} \quad \exists s_0, s_1, \dots, s_l \in \Sigma[x]$$
$$p = \sum_{i=1}^k r_i a_i + \sum_{i=1}^l s_i b_i + s_0 \tag{31}$$

Proposition 2: The multivariable polynomial $p(x)$ is strictly positive ($p(x) > 0 \quad \forall x \in \mathbb{R}^n$), if there exists a $\lambda > 0$ such that

$$\big(p(x) - \lambda\big) \in \Sigma[x]. \tag{32}$$