Secure-by-Construction Controller Synthesis for Stochastic Systems under Linear Temporal Logic Specifications

Yifan Xie[1], Xiang Yin[1], Shaoyuan Li[1], Majid Zamani[2,3]

1. Department of Automation, Shanghai Jiao Tong University
2. Computer Science Department, University of Colorado Boulder
3. Computer Science Department, Ludwig Maximilian University of Munich

xyfan1234@sjtu.edu.cn

60th Conference on Decision and Control

December 13-17, 2021, Austin, Texas, USA

Introduction

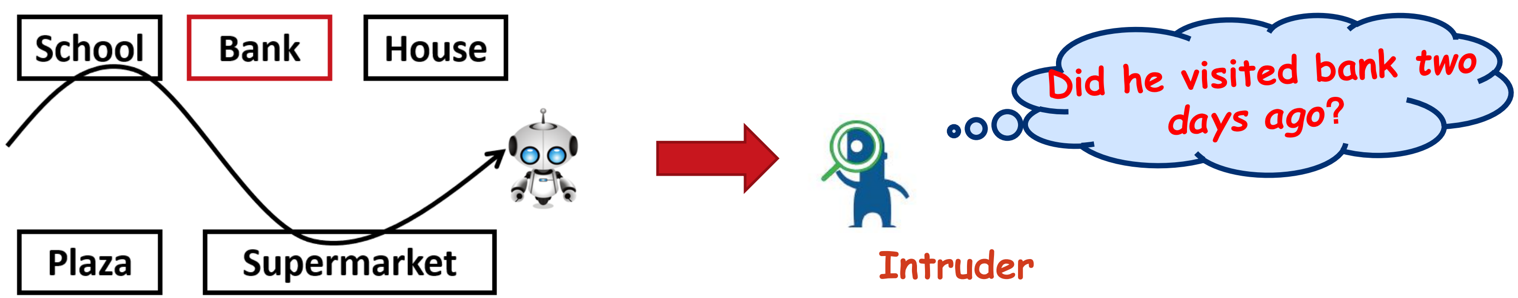
Warehouse Logistics

Rescue robot

Transportation

Industrial manufacture

- Controller synthesis in complex systems
- Linear temporal logic (LTL) to describe complex tasks
- Verification and synthesis of control strategies for LTL
- Security concerns in temporal-logic-based planning
- Outside intruder may infer system's secret information



Preliminary

System Model: (Labeled MDP)

A stochastic system is modeled as a finite labeled MDP

$$\mathcal{M} = (S, s_0, A, P, AP, L)$$

- S is a finite set of states, $s_0 \in S$ is the initial state, A is a finite set of actions
- $P: S \times A \times S \rightarrow [0, 1]$ is the transition probability
- AP is a set of atomic propositions, $L: S \rightarrow 2^{AP}$ is a labeling function

□ Given a labeled MDP $\mathcal{M}$, a control policy is a mapping $\Gamma: S^* \rightarrow A$

- The labeled MDP under control is denoted by $\mathcal{M}_\Gamma$
- $\mathcal{M}_\Gamma$ is a Markov chain when Γ is a state-based policy $\Gamma: S \rightarrow A$

Preliminary

Syntax of linear temporal logic (LTL)

$$\varphi := True \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 U \varphi_2$$

Deterministic Rabin automaton (DRA)

$$R = (Q, \Sigma, \delta, q_0, Acc)$$

- Q is a finite set of states, Σ is a finite set of alphabets
- $q_0 \in Q$ is the initial state
- $\delta: Q \times \Sigma \to Q$ is a finite set of alphabets
- $Acc = \{(B_1, G_1), (B_2, G_2), \cdots (B_n, G_n)\}$ is a finite set of Rabin pairs

For any LTL formula φ, there always exists an DBA over 2^{AP} that accepts exactly all infinite words satisfying φ, i.e.,$\mathcal{L}(R) = \mathcal{L}_\varphi$.

Literature Review

Synthesize optimal control strategies for MDPs

- ☐ **LTL specifications:**
  - X. Ding, S. Smith, C. Belta, and D. Rus. Optimal control of Markov decision processes with linear temporal logic constraints. IEEE Trans. Automatic Control, 59(5):1244–1257, 2014.
- ☐ **Co-safe LTL specifications:**
  - B. Lacerda, D. Parker, and N. Hawes. Optimal and dynamic planning for Markov decision processes with co-safe ltl specifications. In IEEE/RSJ International Conference on Intelligent Robots and Systems, pages 1511–1516, 2014.
- ☐ **CTL specifications ……**

Literature Review

Synthesize optimal control strategies for MDPs

- **LTL specifications:**
  - X. Ding, S. Smith, C. Belta, and D. Rus. Optimal control of Markov decision processes with linear temporal logic constraints. IEEE Trans. Automatic Control, 59(5):1244–1257, 2014.
- **Co-safe LTL specifications:**
  - B. Lacerda, D. Parker, and N. Hawes. Optimal and dynamic planning for Markov decision processes with co-safe ltl specifications. In IEEE/RSJ International Conference on Intelligent Robots and Systems, pages 1511–1516, 2014.
- **CTL specifications ……**

Security and privacy constraints in temporal logic synthesis

- **Differential privacy:**
  - B. Ramasubramanian, L. Niu, A. Clark, L. Bushnell, and R. Poovendran. Privacy-preserving resilience of cyber-physical systems to adversaries. In 59th IEEE CDC, pages 3785–3792, 2020.
  - Z. Xu, K. Yazdani, M. T. Hale, and U. Topcu. Differentially private controller synthesis with metric temporal logic specifications. In American Control Conference, pages 4745–4750, 2020.
- **Opacity:**
  - Y. Wang, S. Nalluri, and M. Pajic. Hyperproperties for robotics: Planning via hyperltl. In IEEE International Conference on Robotics and Automation, pages 8462–8468, 2020.
  - S. Yang, X. Yin, S. Li, and M. Zamani. Secure-by-construction optimal path planning for linear temporal logic tasks. In 59th IEEE CDC, pages 4460–4466, 2020.

Initial-state Opacity, Current-state Opacity

Infinite-Step Opacity

- The system has **secrets**, modeled as a set of states $S_{secret} \subseteq S$
- **Intruder model**
  - Knows the system model $\mathcal{M}$
  - Observes the external observation, $H: S \to Y$
  - Does not know the control policy Γ

Security requirement: intruder can never determine for sure that the system is/was at secret states for any specific instant of time based on observations.

Definition: (Infinite-Step Opacity).

Given a labeled MDP $\mathcal{M}$ with a set of secret states $S_{secret} \subseteq S$, a control policy Γ, the MDP under control $\mathcal{M}_\Gamma$ is said to be infinite-step opaque if

$$\forall \tau_1 \tau_2 \in Path(\mathcal{M}_\Gamma): Last(\tau_1) \in S_{secret}$$
$$\exists \tau_1' \tau_2' \in Path(\mathcal{M}): Last(\tau_1') \notin S_{secret}$$
$$H(\tau_1) = H(\tau_1') \land H(\tau_2) = H(\tau_2')$$

Infinite-Step Opacity

Definition: (Delayed state estimate)

Let $\alpha\beta \in H(Path(\mathcal{M}_\Gamma)) \subseteq Y^*$ be a sequence of observations of the intruder,
$\hat{E}(\alpha|\alpha\beta) \coloneqq \{Last(\tau_1) \in S: \exists \tau_1\tau_2 \in Path(\mathcal{M}) \text{ s.t. } H(\tau_1) = \alpha \wedge H(\tau_2) = \beta\}$

Definition: (Infinite-Step Opacity)

Given a labeled MDP $\mathcal{M}$ with a set of secret states $S_{secret} \subseteq S$, a control policy Γ, the MDP under control $\mathcal{M}_\Gamma$ is said to be infinite-step opaque if

$$\forall \alpha\beta \in H\big(Path(\mathcal{M}_\Gamma)\big), \hat{E}(\alpha|\alpha\beta) \nsubseteq S_{secret}$$

The intruder can never know that the system was at a secret state

Problem formulation

Given a labeled MDP $\mathcal{M}$ controlled by a control policy Γ, an LTL formula φ, the **probability of satisfying φ** in the labeled MDP under Γ

$$Pr(\mathcal{M}_\Gamma \vDash \varphi) = Pr(\{\tau \in Path(\mathcal{M}_\Gamma) : L(\tau) \vDash \varphi\})$$

- **Synthesis Problem**

Given a labeled MDP $\mathcal{M}$ with a set of secret states $S_{secret} \subseteq S$ and an LTL specification φ, synthesize a control policy $\Gamma\colon S^* \to A$ such that

(1) $\mathcal{M}_\Gamma$ is infinite-step opaque

(2) For any control policy Γ' satisfying (1), $Pr(\mathcal{M}_\Gamma \vDash \varphi) \geq Pr(\mathcal{M}_{\Gamma'} \vDash \varphi)$

Synthesis Procedure

Construct a product MDP

Step 1: translate the LTL formula φ to a DRA R

Step 2: construct the information-state estimator T

Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Synthesis Procedure

Construct a product MDP

Step 1: translate the LTL formula φ to a DRA R

Step 2: construct the information-state estimator T

Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Definition: (Information-state estimator)

The information-state estimator w.r.t. the labeled MDP $\mathcal{M}$ is a transition system

$$T = (X, x_0, Y, \zeta)$$

- $X \subseteq 2^S \times 2^{2^{S \times S}}$ is the set of states, $x_0 \in X$ is the initial state
- Y is the set of inputs, the intruder's observation
- $\zeta: X \times Y \to X$ is a transition function, $\zeta(x, y) = x'$

$\alpha = y_1 y_2 \cdots y_n$

$$\boxed{x_0} \xrightarrow{y_1} \boxed{\hat{E}(y_1|\alpha)} \xrightarrow{y_2} \boxed{\hat{E}(y_1 y_2|\alpha)} \xrightarrow{y_3} \cdots \xrightarrow{y_n} \boxed{\hat{E}(y_1 y_2 \cdots y_n|\alpha)}$$

Update Rule

$$C(x') = \mathrm{Post}(C(x), y)$$

$$D\,(x') = \{\overline{\mathrm{Post}}(\theta, y) \in 2^{S \times S} : \theta \in D(x)\} \cup \{\odot(C\,(x'))\}$$

Product MDP

Definition: (Product MDP)

Given a labeled MDP $\mathcal{M}$, a DRA R accepting φ and the information-state estimator T, the product MDP

$$\widetilde{\mathcal{M}} = (\tilde{S}, \tilde{s}_0, A, \tilde{P}, \widetilde{Acc})$$

- $\tilde{S} \subseteq S \times Q \times X$ is a finite set of states
- $\tilde{s}_0 = (s_0, q, x_0)$ is the initial state such that $q = \delta(q_0, L(s_0))$
- A is a finite set of actions
- $\tilde{P}: \tilde{S} \times A \times \tilde{S} \to [0, 1]$ is the transition probability
- $\widetilde{Acc} = \{(\widetilde{B_1}, \widetilde{G_1}), (\widetilde{B_2}, \widetilde{G_2}), \cdots (\widetilde{B_n}, \widetilde{G_n})\}$ is a finite set of Rabin pairs

- Capture both the LTL specification and the security requirement
- Solve the problem by applying safety game as well as probabilistic model checking techniques over the product state-space

Induced policy

Given a product MDP $\widetilde{\mathcal{M}}$ and a policy $\tilde{\Gamma}: \tilde{S} \to A$, we can compute an induced policy Γ on the labeled MDP $\mathcal{M}$

Synthesis Procedure

Construct a product MDP

Step 1: translate the LTL formula φ to a DRA R

Step 2: construct the information-state estimator T

Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Enforcement of infinite-step opacity

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Step 5: remove all inconsistent states iteratively from $\widetilde{\mathcal{M}}_0$

Enforcement of Infinite-step opacity

Theorem $D_1(x) = \{\{s \in S: (s, s') \in \theta\}: \theta \in D(x)\}$

For any observation $\alpha = y_0 y_1 \cdots y_n \in H(Path(\mathcal{M}_\Gamma))$

$$D_1(\zeta(\alpha)) = \{\hat{E}(y_0 \cdots y_i | \alpha) \in 2^S: i = 0, 1, \cdots, n\}$$

Information-state estimator T yields the desired delayed state estimate

- Construct the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$
- Remove secret-revealing states $S_{rev} = \left\{\tilde{s} \in \tilde{S}: \exists \eta \in D_1\big(X(\tilde{s})\big)\ s.t.\ \eta \subseteq S_{secret}\right\}$ and get a new product MDP $\widetilde{\mathcal{M}}_0 = \widetilde{\mathcal{M}}|_{\tilde{S} \setminus S_{rev}}$
- Delete all inconsistent states and get $\widetilde{\mathcal{M}}^*$
  - at least one action defined at each state
  - the overall probability of transitions labeled with an action is 1

Synthesis Procedure

Construct a product MDP

Step 1: translate the LTL formula φ to a DRA R

Step 2: construct the information-state estimator T

Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Enforcement of infinite-step opacity

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Step 5: remove all inconsistent states iteratively from $\widetilde{\mathcal{M}}_0$

Generate the optimal policy

Step 6: compute the set of accepting states $\mathcal{E}$

Step 7: generate the optimal control policy by value iteration

Optimal Control Policy

Proposition For any control policy Γ, the maximal probability of satisfying the LTL formula is equal to the maximal probability of reaching accepting states $\mathcal{E}$

$$\max_{\Gamma} Pr(\mathcal{M}_{\Gamma} \vDash \varphi) = \max_{\Gamma} Pr(reach\ \mathcal{E})$$

Value iterations

- Initial value function $v^0(k) = \begin{cases} 1 & if\ \tilde{s}_k \in \mathcal{E} \\ 0 & if\ \tilde{s}_k \notin \mathcal{E} \end{cases}$
- Iteration function
  - For state $\tilde{s} \in \mathcal{E}_N$, the value remains 0, for state $\tilde{s} \in \mathcal{E}$, the value remains 1
  - For the remaining state

$$v^{i+1}(k) = \max\{\textstyle\sum_{\tilde{s}_t \in \tilde{S}} \widetilde{P}(\tilde{s}_k, a, \tilde{s}_t) v^i(t) | a \in A(\tilde{s}_k)\}$$

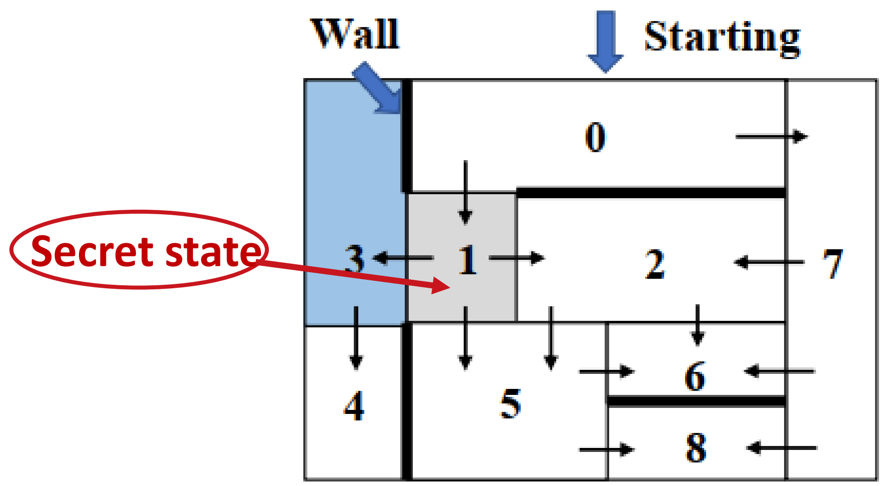
- Converge to v^*, compute $\tilde{\Gamma}: \tilde{S} \to A$ for each state $\tilde{s} \in \tilde{S} \setminus (\mathcal{E} \cup \mathcal{E}_N)$ by

$$v^*(k) = \sum_{\tilde{s}_t \in \tilde{S}} \widetilde{P}(\tilde{s}_k, a, \tilde{s}_t) v^*(t)$$

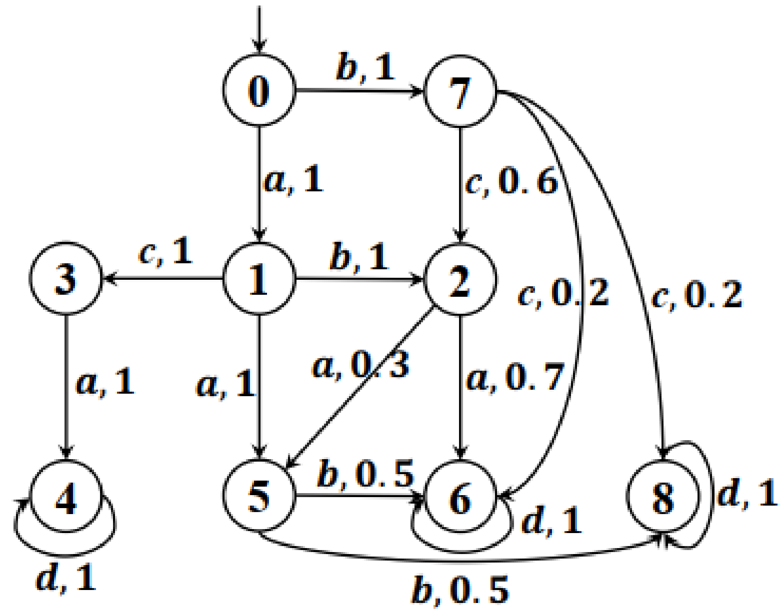
Case Study

Output function: $Y = \{D, \neg D\}, H(3) = D, H(s) = \neg D$

Labeling function: $AP = \{P_1, P_2\}, L(1) = \{P_1\}, L(4) = L(6) = \{P_2\}, L(s) = \emptyset$



Work space of the robot



Labeled MDP $\mathcal{M}$

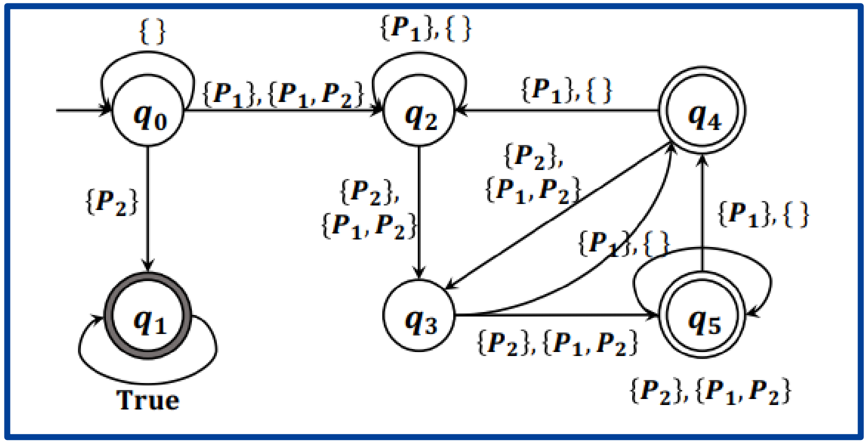
Goal: first go to region 1 and then visit in region 4 or region 6 infinitely often

$$\varphi = (\neg P_2 \mathcal{U} P_1) \wedge (\Box \Diamond P_2)$$

Case Study

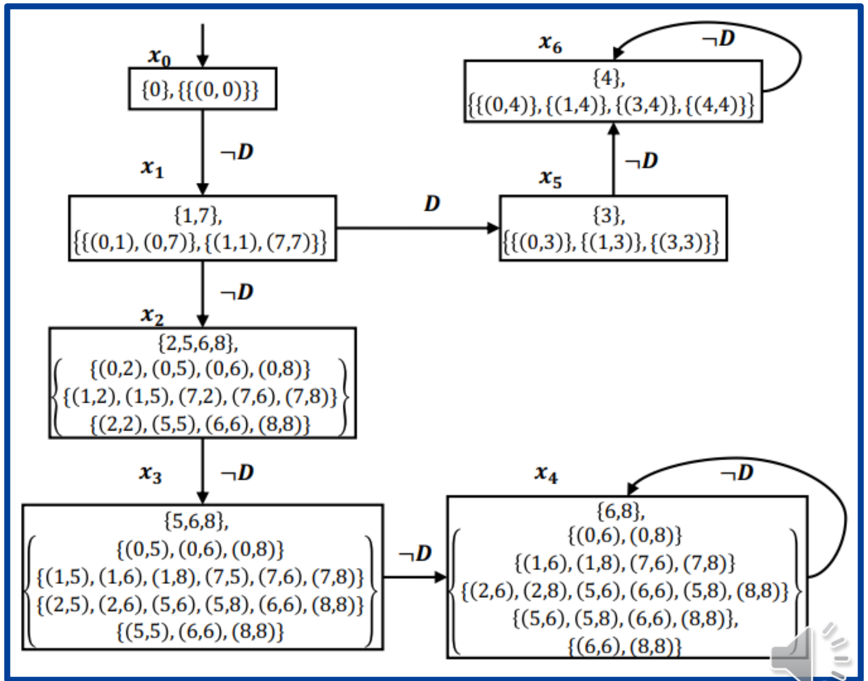
Step 1:

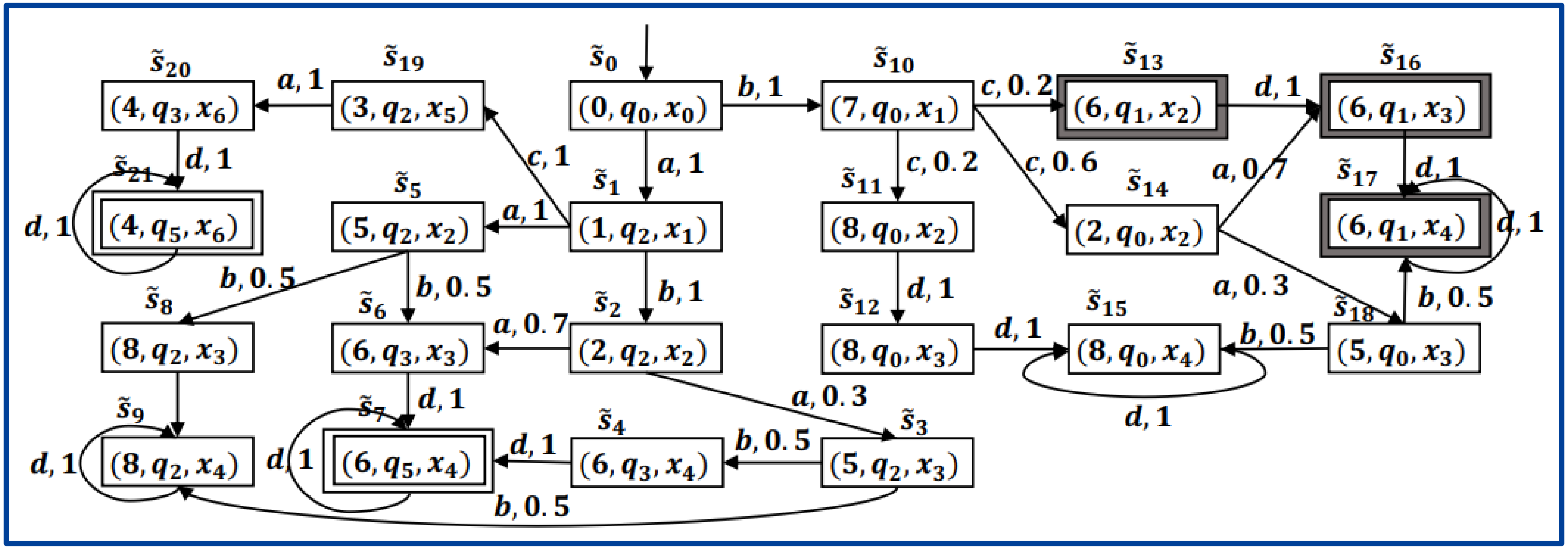
translate the LTL formula φ to a DRA R



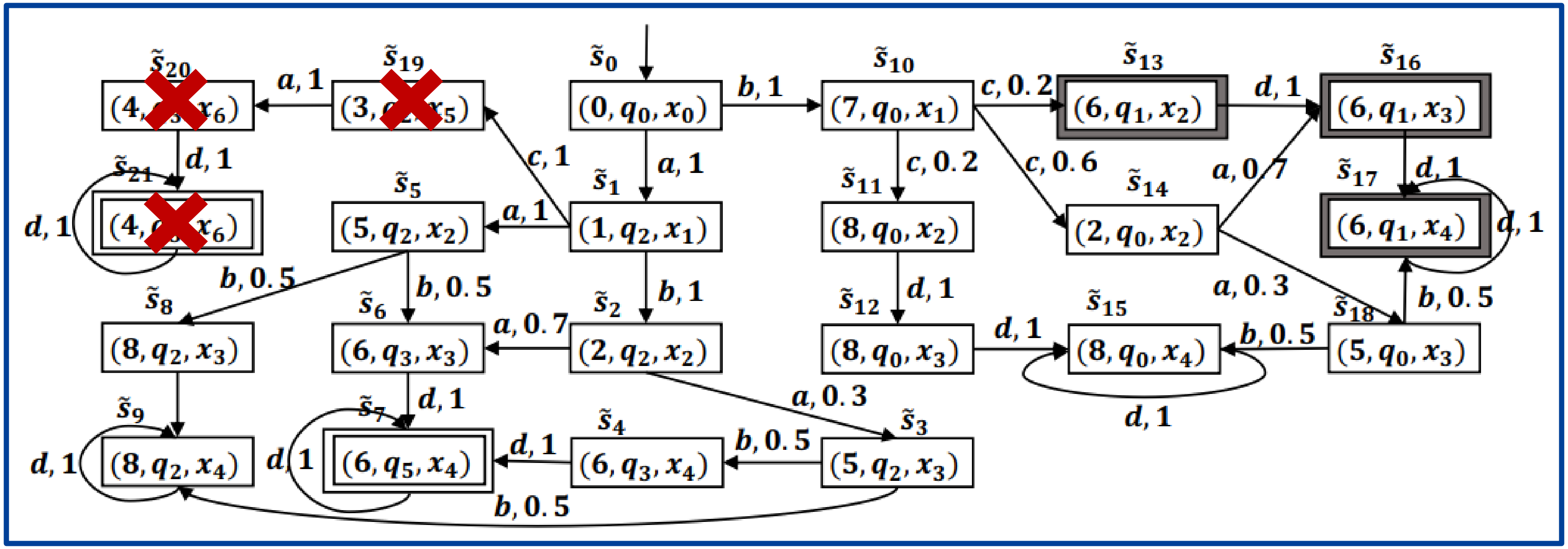
Step 2:

construct the information-state estimator T





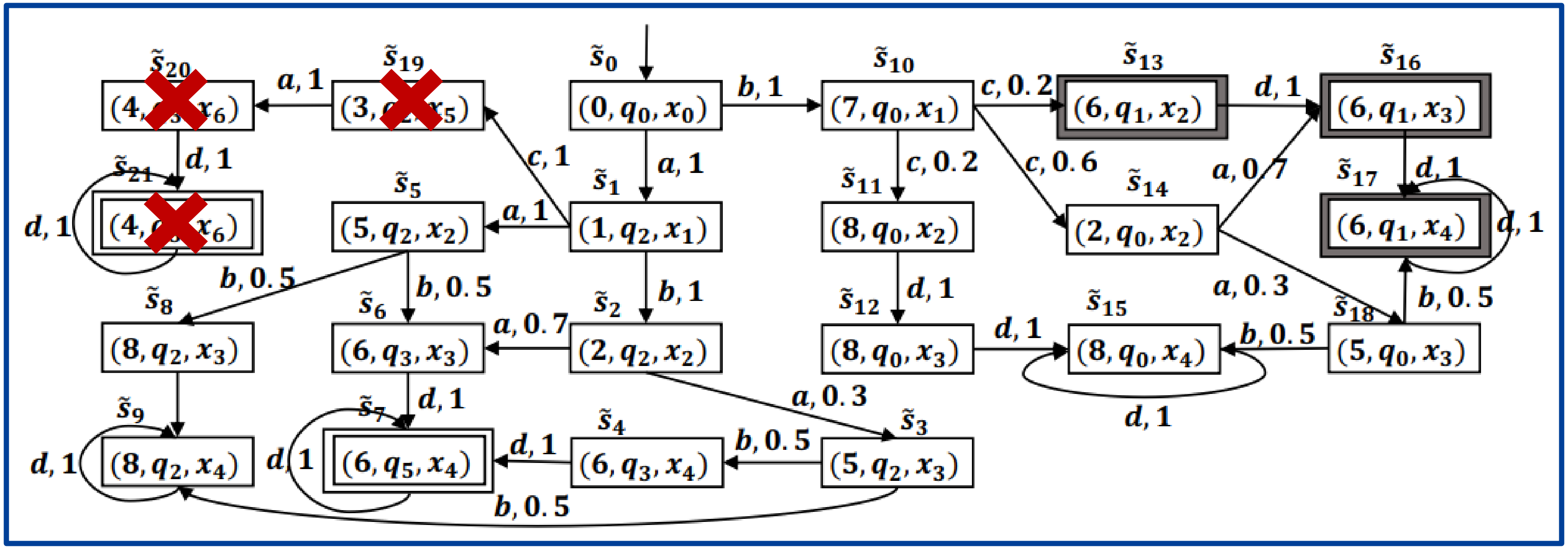
Step 3: **generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$**



Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Case Study

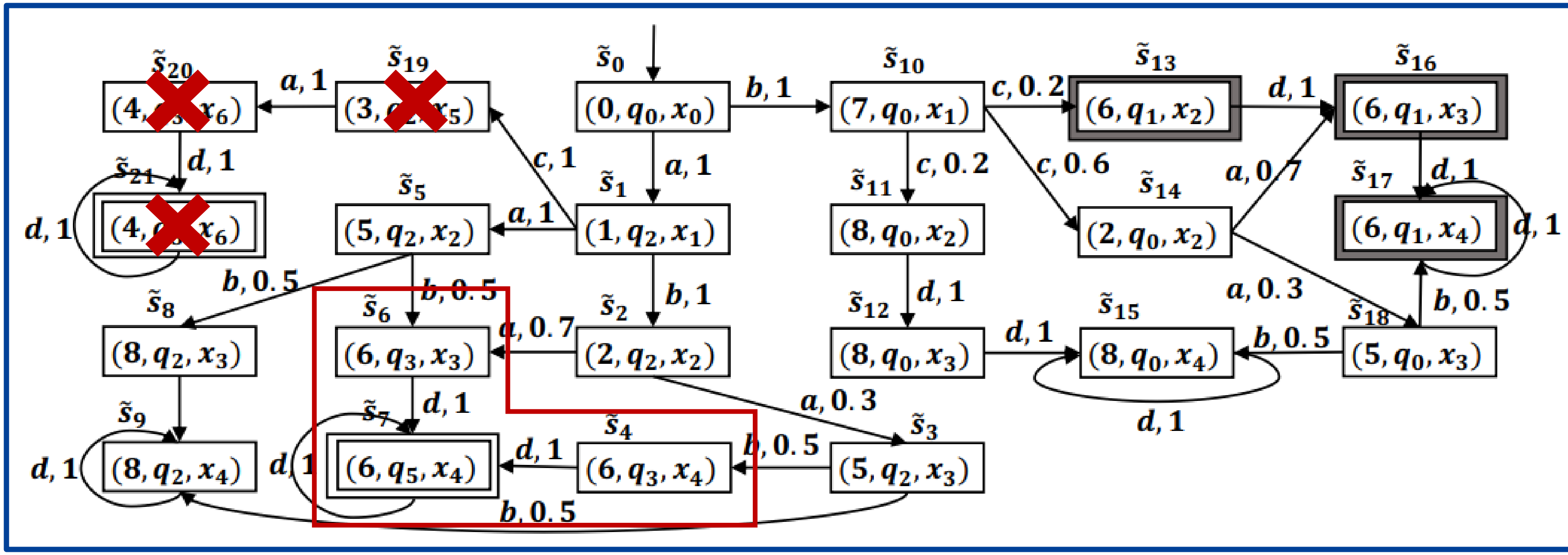


Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Step 5: remove all inconsistent states iteratively from $\widetilde{\mathcal{M}}_0$

Case Study

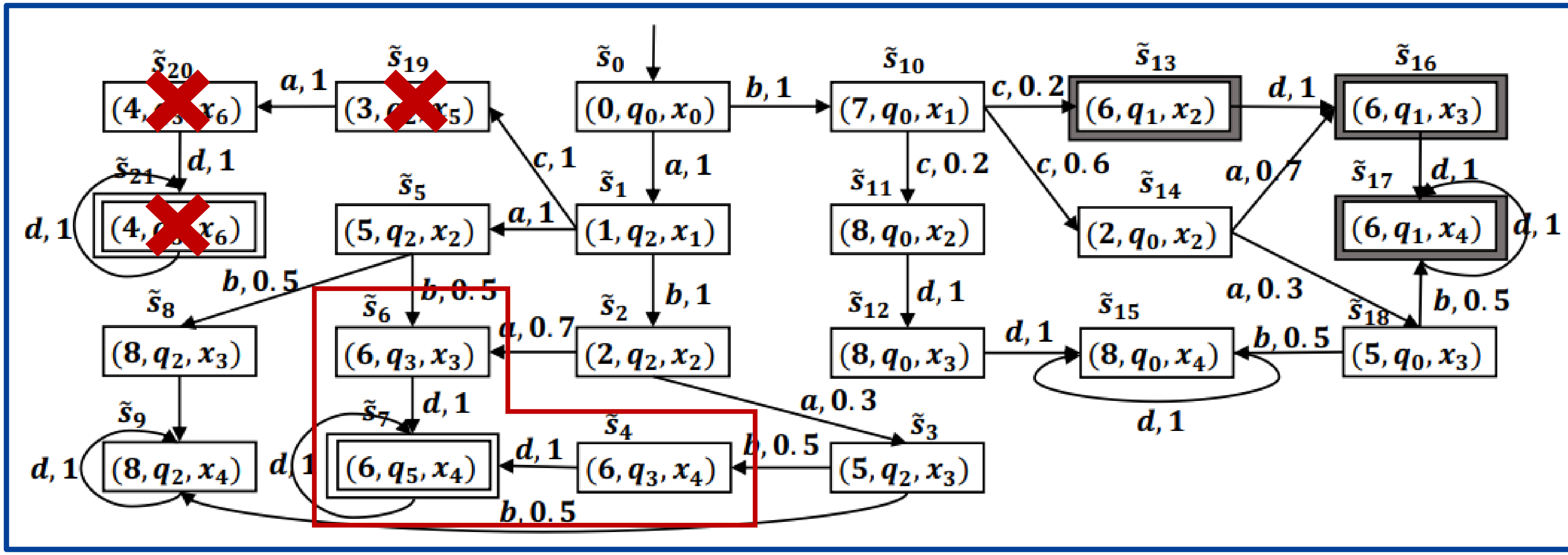


Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Step 5: remove all inconsistent states iteratively from $\widetilde{\mathcal{M}}_0$

Step 6: compute the set of accepting states $\mathcal{E}$



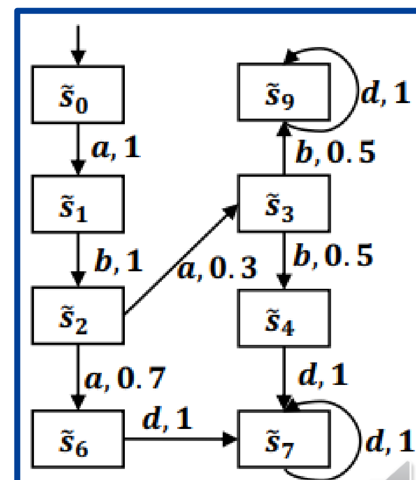
Step 3: generate the product MDP $\widetilde{\mathcal{M}} = \mathcal{M} \times R \times T$

Step 4: delete secret-revealing states from $\widetilde{\mathcal{M}}$ and get $\widetilde{\mathcal{M}}_0$

Step 5: remove all inconsistent states iteratively from $\widetilde{\mathcal{M}}_0$

Step 6: compute the set of accepting states $\mathcal{E}$

Step 7: generate the optimal control policy by value iteration



Conclusion

Contributions:

- Formulated a security-aware LTL synthesis problem for MDPs
- Proposed a new type of information-state estimator
- Solved the synthesis problem by solving safety game and using probabilistic model checking

Future Directions:

- Investigate the quantitative tradeoff between the probability of being secure and the probability of satisfying the LTL specification

Thank You!