# 用于安全运行时监控的鲁棒马尔可夫模型学习

Antonina Skurka 查尔姆斯理工大学和哥德堡大学 瑞典哥德堡 skurka@chalmers.se

Luko van der Maas 拉德堡德大学奈梅亨分校，荷兰 luko.vandermaas@ru.nl

Sebastian Junges 拉德堡德大学奈梅亨分校，荷兰 sebastian.junges@ru.nl

Hazem Torfah 查尔姆斯理工大学和哥德堡大学 瑞典哥德堡 hazemto@chalmers.se

arXiv:2602.14987v1 [cs.LO] 16 Feb 2026

**摘要**

我们提出了一种基于模型的方法，用于为自主系统学习鲁棒运行时监控器。运行时监控器通过观察系统行为并预测潜在的安全违规，在提升保障水平方面发挥着关键作用。在我们的方法中，我们提出使用区间隐马尔可夫模型（区间隐马尔可夫模型）来刻画系统的（随机）行为。随后，监控器利用所学习的区间隐马尔可夫模型，为潜在的安全违规推导风险估计。本文有三项主要贡献：（1）对学习鲁棒运行时监控器的问题进行了形式化；（2）提出了一种新颖的框架，利用基于一致性测试的细化来学习具有收敛保证的鲁棒区间隐马尔可夫模型；（3）提出了一种高效的监控算法，用于计算区间隐马尔可夫模型上的风险估计。我们的实证结果证明了采用该方法学习的监控器的有效性，尤其是与无模型监测方法相比更为突出；后者完全依赖收集的数据，无法访问系统模型。

**关键词**

基于模型的运行时监控、不确定性下的决策、学习区间隐马尔可夫模型

## 1 引言

运行时监控对于提高信息物理系统（CPS）的保障水平至关重要 [7, 19]。运行时监控器持续观察系统，以发现可能不安全的情况。当此类情况发生时，运行时监视器会发出警报，并可能随之触发备用故障安全方案，以保持系统安全。在现代自主信息物理系统中，运行时监视器对于确保安全性变得更加不可或缺，尤其是在集成机器学习（ML）组件时 [13]。在这些场景中，运行时监视器必须应对各种不确定性，既包括机器学习模型所作决策中的不确定性，也包括这些系统运行所处环境中的不确定性。系统动力学往往是概率性的，且环境状态无法被完全观测。运行时监视器在预测安全违规时必须将这些方面考虑在内，同时在假阳性（警报过多）与假阴性（危险情况未被察觉）之间取得平衡。监控器所能获得的关于系统中不确定性的信息类型，对实现这一平衡具有重大影响。

考虑一个自主飞机在存在地面交通的情况下接近跑道的例子。该飞机配备了基于摄像头的感知传感器。一项关键的安全关键程序是观察地面交通的行为，并决定着陆是安全的，还是应当中止着陆。安全规范规定飞机与地面交通在任何时候都必须保持的最小距离。车辆行为始终存在不确定性；由于诱发噪声，所感知的传感器数据中同样存在不确定性。运行时监视器必须（隐式或显式地）估计风险水平：即着陆过程中规范被违反的概率，以及若被违反，其程度有多大。若该风险水平超过某个阈值，运行时监视器必须发出警报。监控器的准确性在很大程度上取决于能够提供关于地面车辆和传感器（随机）行为的何种信息。

在本文中，我们研究在不确定性下鲁棒估计违反安全规范之风险的监视器构造问题。我们特别提出一种用于学习鲁棒运行时监视器的新颖基于模型的方法。在该方法中，我们提出一种数据驱动方法，以区间隐马尔可夫模型（*iHMMs*）的形式学习鲁棒的不确定性模型；这是隐马尔可夫模型的一种变体，其中转移概率以区间而非固定值表示。在所学区间隐马尔可夫模型之上，我们开发了一种高效的监控算法，用于谨慎（或保守）地估计风险等级。我们的方法始于一个基于细化的学习过程，该过程根据从受观测系统收集的仿真运行逐步构建区间隐马尔可夫模型。随后，所得模型被集成到一个能够在系统执行期间估计风险的监测框架中。学习区间隐马尔可夫模型并将其集成到监测框架中的总体流程如图1所示。

我们的方法弥补了学习运行时监视器这一当前最先进领域中的空白。当前最先进的方法大致可分为两类。第一类假设存在一个已知的模型，该模型使用预定义模型来刻画系统和环境中的不确定性。通常，这些模型是隐马尔可夫模型（HMM）或其变体 [3, 10, 18]。这类方法面临的一项关键挑战是获取足够准确的模型。第二类方法，即无模型方法，则避开了这一挑战。此类方法直接从数据中学习分类器，而不依赖显式的系统模型 [9, 29, 35]。尽管前景可期，无模型方法通常样本复杂度较高，而且往往准确率较低

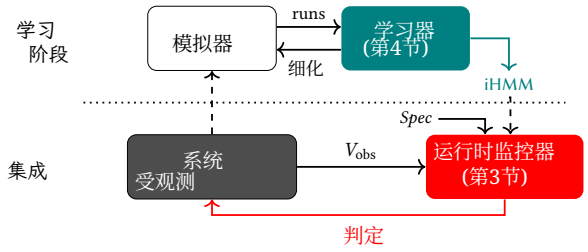



**图 1：在信息物理系统中学习并集成鲁棒监视器**

，因为它们仅根据可观测数据学习监控器，缺乏对系统更深层的结构性认识。

在我们的工作中，我们倡导学习模型，并提出一种方法，克服获取不确定性模型这一难题；这一难题阻碍了基于模型的方法在运行时监视器中的应用。具体而言，我们提出一种数据驱动策略，用于学习一个可作为系统可行抽象的无限隐马尔可夫模型。随后，我们构建一个运行时监视器，对这一已学习的抽象进行（逻辑）推理。尽管监视器仍基于观测序列运行，但其决策如今以已学习的无限隐马尔可夫模型为依据，从而有效地将数据驱动学习与基于模型的推理结合起来。我们对基于模型的学习方法的兴趣，源于它们在其他领域的成功。可以将监测视为一种不确定性下的序贯决策，其中基于模型的方法对应专用的（经典）规划器，而无模型方法则对应强化学习的专用数据驱动变体 [20]。研究表明，基于模型的方法对提高安全性具有显著影响 [8]。此外，在不确定性下的序贯决策中，基于模型的学习方法以样本高效著称。事实上，在我们的实验中，我们表明，在数据量相同的情况下，我们的模型能够达到较高的安全性和准确率，而无模型方法无法企及。

区间隐马尔可夫模型使我们能够显式地对转移动态中的不确定性进行建模。我们提出了一种基于细化的方法来学习区间隐马尔可夫模型。在这种方法中，通过线性调整概率区间 [28]，迭代更新模型。我们的细化方法融入了由一致性测试驱动的反馈回路。该回路评估迄今已学习模型的监控决策不确定性，并通过细化模型表现欠佳的部分来指导学习过程。我们特别证明，随着细化次数增加，细化过程会收敛到最优模型。最后，为了实现高效监测，我们进一步引入了一种受 [18] 启发、适用于区间隐马尔可夫模型的可处理监测方法。我们的监测过程相对于观测序列的长度在多项式时间内运行。我们在自主系统领域的一组基准测试上评估了我们的方法。这些基准测试尤其证实了基于模型的运行时监视器设定相较于无模型方法的优势。

## 2 问题陈述

我们的目标是构建一个监控器，在安全违规即将发生时发出警报。我们所处的环境中，系统动力学和监控器获取的观测都存在不确定性。

我们首先给出关键符号和定义。对于集合 $X$，我们使用 $X^*$ 定义 $X$ 上的有限序列集合，并使用 $X^{\leq h}$ 表示长度不超过 $h$ 的序列集合。在基于状态的系统中，状态集合 $\Sigma_{\text{sys}}$ 通过系统变量集合 $V_{\text{sys}}$ 上的赋值来定义。监控器不一定观测 $V_{\text{sys}}$ 上的赋值，而是观测 $V_{\text{obs}}$ ——观测变量集合（见图1 - 集成）。下文中，我们区分系统执行序列和观测执行序列，将 $\Sigma^*_{\text{sys}}$ 中的序列称为路径，将 $\Sigma^*_{\text{obs}}$ 中的序列称为轨迹。对于可数集合 $X$，令 $Dist(X) \subset (X \to [0,1])$ 定义 $X$ 上的概率分布集合。概率分布 $d \in Dist(X)$ 特别满足 $\sum_{x \in X} d(x) = 1$。

定义 1（被观测系统（SuO））。离散时间系统是一个元组 $\mathcal{S} = (V_{sys}, V_{obs}, d, \text{观测})$，其中 $V_{sys}$ 和 $V_{obs}$ 分别是系统变量集和观测变量集，动态 $d$ 是定义在 $\Sigma^*_{sys}$ 上的概率分布，而观测：$\Sigma^*_{sys} \to Dist(\Sigma^* \text{ 观测})$ 是路径到观测轨迹概率分布的映射。

受观测系统隐含地刻画了系统与其环境之间的交互。在上述定义中，$d$ 定义了某条路径发生的概率，从而刻画了环境行为中的不确定性。观测映射 $obs$ 刻画了传感器的（含噪）行为；对于给定路径，传感器可能根据其随机行为输出不同的轨迹。

定义 2（规范）。我们将安全约束定义为有限线性时间性质 *[5, 14]*。定义在 $\Sigma_{sys}$ 上的规范 $\varphi$ 是一个集合 $\varphi \subseteq \Sigma^*_{sys}$。如果 $\pi \in \varphi$，则称 $\pi$ 满足 $\varphi$，也记作 $\pi \models \varphi$。

根据上述安全性定义，我们可以定义违反安全规范的概率。我们将其称为风险函数 [18][1]。

定义 3（风险函数）。给定 $\mathcal{S} = (V_{sys}, V_{obs}, d, obs)$ 以及定义在 $\Sigma_{sys}$ 上的规范 $\varphi$，对于时域 $h \in \mathbb{N}^+$，风险函数 $r^h_\varphi$：$\Sigma^*_{sys} \to [0,1]$ 给出给定初始路径 $\pi \in \Sigma^*_{sys}$ 在 $h$ 步的时域内违反 $\varphi$ 的概率。若 $d(\pi) = 0$，则令 $r^h_\varphi(\pi) = 0$；否则

$$r^h_\varphi(\pi) = Pr(\{\pi' \in \Sigma^{\leq h}_{sys} \mid \pi \cdot \pi' \not\models \varphi\}) = \frac{1}{d(\pi)} \sum_{\pi' \in \Sigma^{\leq h}_{sys}} (\pi \cdot \pi' \not\models \varphi) \cdot d(\pi \cdot \pi')$$

右侧的表达式是通过对条件概率 $d(\pi' \mid \pi)$ 应用贝叶斯定律推导得出的。规范和风险函数定义在系统层级上，通常无法将它们提升到观测层级而不损失精确性。以引言中的着陆场景为例，我们可以根据飞机和地面车辆的轨迹来定义（近）碰撞的风险；然而，监控器并不知道地面车辆的真实位置，只能获知其感知到的位置。也就是说，监测面临的挑战在于，我们无法直接观测系统路径，因此不可能直接计算相关风险。接下来，我们将系统状态空间与监控器的观测联系起来，以应对这一挑战。

SuO 的监控器只是一个函数 $M$：$\Sigma^*_{\text{obs}} \to [0,1]$，它为系统中的每条轨迹赋予一个介于 0 和 1 之间的值，用以表示观测轨迹的风险。为了将监控器与系统级规范联系起来，我们引入理想监视器的概念。

[1]风险通常定义为违规概率乘以影响。事实上，可以轻松细化这一界定，使其也能考虑影响程度的差异。

定义 4（理想监视器）。给定 $\mathcal{S}=(V_{sys}, V_{obs}, d,$ 观测)和规范 $\varphi$，对于时域 $h$ 和损失函数 $L^{\varphi,h,\mathcal{S}}$，理想监视器 $M^*$: $\Sigma^*$ 观测 $\to [0,1]$ 满足以下条件：

$$M^* \in \underset{M':\Sigma^*_{obs}\to[0,1]}{\arg\min} \; L^{\varphi,h,\mathcal{S}}(M').$$

理想监视器 $M^*$的概念，以及由此产生的对下述问题陈述的解答，都取决于损失函数的具体实例化。在本文中，我们考虑均方误差损失函数。对于某个监控器 $M \in \mathbb{M}$:

$$L^{\varphi,h,\mathcal{S}}_{\mathrm{MSE}}(M) = \sum_{\tau\in\Sigma^*_{\mathrm{obs}}} Pr(\tau) \sum_{\pi\in\Sigma^*_{\mathrm{sys}}} Pr(\pi \mid \tau)\big(M(\tau) - r^h_\varphi(\pi)\big)^2$$

其中 $Pr(\tau) = \sum_{\pi\in\Sigma^{*}sys} d(\pi)\cdot obs(\pi)(\tau)$，且 $Pr(\pi\mid\tau) = {}^{d}(\pi)\cdot \underline{obs(\pi)(\tau)\, Pr(\tau)}$。

利用理想监视器的概念，我们还定义了保守监控器的集合，即与理想监视器相比高估风险的监视器。

定义 5（保守监控器）。给定 $SuO\ \mathcal{S}$ 和理想监视器 $M^*$，如果对于所有$\tau \in \Sigma^*$ $obs$，监视器 $M$ 满足 $M^*(\tau) \le M(\tau)$，则称其为保守监控器。我们将保守监控器的集合称为$\mathcal{M}^C$。

备注。由于系统与观测世界之间存在不匹配，理想监视器仍可能产生错误的风险评估；我们只是要求保守监控器的风险评估至少与理想监视器一样保守。

理想监视器可能无法简洁地表示，也可能不符合其他重要约束，因而无法部署到系统 [30] 中。我们假设存在一类可接受监控器，它们实现函数 $\Sigma^*_{\mathrm{obs}} \to [0,1]$，并且存在一个用于比较两个监控器的距离函数 $\delta$。本文的目标是通过算法找到一个与理想监视器最接近的可接受保守监控器：

**问题陈述** 给定一个理想监视器 $M^*$、一组可接受监控器 $\mathbb{M}$、一组保守监控器 $\mathbb{M}^C$，以及一个距离函数 $\delta$: $(\Sigma^*_{\mathrm{obs}} \to [0,1])^2 \to \mathbb{R}$，求一个监控器 $M \in \mathbb{M} \cap \mathbb{M}^C$，使得：

$$M \in \underset{\mathbb{M}\cap\mathbb{M}^C}{\text{参数最小值}}\ \delta(M^*, M')_{M'\in}$$

距离函数 $\delta$ 可以有多种定义方式；本文采用所有轨迹上的平均距离。

解决上述问题的关键在于能够访问理想监视器 $M^*$。这又在很大程度上取决于能否将系统级风险函数转换到观测层级，即能否准确表示函数 $obs$（见定义 4）。

## 3 iHMM 监测器

本节研究由（已知）隐马尔可夫模型（HMM）描述的 SuO。我们将介绍必要的背景知识，定义 HMM 上的（理想）监控器，然后讨论如何通过定义基于所谓的 区间 HMM 的监控器，来考虑 HMM 转移概率中的不确定性。

### 3.1（区间）隐马尔可夫模型

定义 6（隐马尔可夫模型（隐马尔可夫模型））。 隐马尔可夫模型是一个元组 $H=(S, \iota, P, Z, O)$，其中 $S$是一个有限状态集，$\iota$: $S \to [0,1]$ 是初始分布，$P$: $S\times S \to [0,1]$ 是转移概率函数，且 $O$: $S \to Distr(Z)$是观测函数，其中 $Z$ 是观测集合。转移概率函数满足：对于每个 $s \in S$，均有 $\sum_{s'\in S} P(s,s') = 1$。

HMM H 中的路径是一个有限序列 $\pi_{\mathrm{H}} = s_0 s_1 \dots s_n$，其中对于所有 $0 \le i < n$、$P(s_i, s_{i+1}) > 0$。令 $\Pi_{\mathrm{H}}$ 表示 H 的路径集。令 $\Pi^n_{\mathrm{H}}$ 表示 H 中长度为 $n \in \mathbb{N}$ 的路径集。与某条路径 $\pi_{\mathrm{H}}$ 相关联的 H 的观测轨迹是一个序列 $\tau_{\mathrm{H}} = z_0 z_1 \dots z_n$，其中对于所有 $0 \le i \le n$，$\mathrm{O}(s_i)(z_i) > 0$。令 $T_{\mathrm{H}}$ 表示观测轨迹集。令 $T^n_{\mathrm{H}}$ 表示长度为 $n \in \mathbb{N}$ 的观测轨迹集。注意，存在一个映射 $obs_{\mathrm{H}}$： $\Pi_{\mathrm{H}} \to Distr(T_{\mathrm{H}})$，它根据标记函数 O，为每条路径指定一个观测轨迹上的分布。如果 H 的状态集定义在 $V_{sys}$上，H 的观测函数映射到 $V_{obs}$上的分布，并且映射 $obs_{\mathrm{H}}$ 等价于该系统的 $obs$，则受观测系统由 HMM H 建模。因此，系统与模型的路径集和轨迹集相同。在本文余下部分中，我们用 $\Pi$ 和 $T$ 表示系统及其模型 H 的路径集和轨迹集。

定义 7（区间隐马尔可夫模型（$iHMM$））。区间隐马尔可夫模型是一个元组 $iH=(S, \iota_l, \iota_u, P_l, P_u, Z, O)$，其中 $S$、$Z$ 和 $O$ 与 $H$ 中的相同，$\iota_l, \iota_u$: $S \to [0,1]$，且对于所有 $s \in S$，$\iota_l(s) \le \iota_u(s)$，它们是初始分布的上下界；而 $P_l, P_u$: $S\times S \to [0,1]$，且对于所有 $s, s' \in S$，$P_l(s,s') \le P_u(s,s')$，它们是转移概率的上下界。我们将路径和轨迹等概念从隐马尔可夫模型推广到区间隐马尔可夫模型。

如果区间隐马尔可夫模型 iH 与隐马尔可夫模型 H 具有相同的状态集合和观测集合，并且对于所有 $\iota_l(s) \le \iota(s) \le \iota_u(s)$，以及对于所有状态对 $s$，$t \in S$，$s \in S$和 $P_l(s,t) \le P(s,t) \le P_u(s,t)$，则称 iH 被 H细化。令 $\mathrm{H}_{\mathrm{iH}}$表示所有细化给定区间隐马尔可夫模型 iH 的隐马尔可夫模型的集合。

### 3.2 HMM 监测器

HMM H 上的监控器是一个函数 $M_{\mathrm{H}}$: $T_{\mathrm{H}} \to [0,1]$。前向滤波 [27, 32] 是此类监控器的一种实现，它根据给定轨迹计算风险函数 $r^h_\varphi$ 的期望值：$\mathrm{R}_{\mathrm{H}}(\tau) = \mathbb{E}_\pi\left[r^h_\varphi(\pi) \mid \tau\right]$.。如果我们选择均方误差作为损失函数，那么该期望值就是针对所选损失函数的最优估计量 [24],，因而也是 H 的最优监控器。

当 H 对 SuO 建模时，$\mathrm{R}_{\mathrm{H}}$ 对应于$L^{\varphi}$ 的理想监视器，$h$ H 。我们将此监控器记为 $M^*_{\mathrm{H}}$。 $MSE$

引理 1。 给定一个对 $SuO\ S$ 建模的 $HMM\ H$、一个规范 $\varphi$ 和时域 $h$，$L^{\varphi}$ 的$h$理想监视器$^{H}$ 为 $M^*_H$。

### 3.3 iHMM 监测器

对区间隐马尔可夫模型的监测遵循与监测隐马尔可夫模型相同的一般原则，但存在一个额外挑战：一个 iHMMiH 对应于一组可能的隐马尔可夫模型 $\mathrm{H}_{\mathrm{iH}}$。在计算一条轨迹的风险时，我们因此必须决定使用哪一个 H $\in \mathrm{H}_{\mathrm{iH}}$。为保持谨慎，我们会高估轨迹的风险。

定义 8（iHMM 监测器）。给定一个 $iHMM$ $iH$、规范 $\varphi$、时域 $h$ 和观测轨迹 $\tau$，$iHMM$ 监测器定义为 $M_{iH}(\tau) = \max_{H\in\mathcal{H}} \mathrm{R}_H(\tau)$。

与保守监控器的关系。安全规范 $\varphi$、时域 $h$和由隐马尔可夫模型 H 建模的 SuO S 共同确定了状态上的风险函数$r_\varphi^h$、理想隐马尔可夫模型监视器 $M_{\mathrm{H}}^*$以及一组保守监控器 $\mathrm{M}^C$。任何 iHMM 监测器 $M_{\mathrm{iH}}$，只要我们的系统模型 H 细化了 iH，都是一个保守监控器。

引理 2. 给定一个由隐马尔可夫模型 $H$ 建模的 $SuO$，任何被 $H$ 细化的无限隐马尔可夫模型 $iH$ 都会导出一个谨慎监控器 $M_{iH} \in \mathcal{M}^C$。

证明。我们知道 $\mathrm{H} \in \mathrm{H}_{\mathrm{iH}}$。因此，对于每条轨迹 $\tau \in T_{\mathrm{H}}$，

$$M_{\mathrm{iH}}(\tau) = \max_{\mathrm{H}' \in \mathcal{H}} \sum_{\pi \in \Pi_{\mathrm{H}'}^{|\tau|}} Pr_{\mathrm{H}'}(\pi \mid \tau) \cdot r_\varphi^h(\pi) \geq \sum_{\pi \in \Pi_{\mathrm{H}}^{|\tau|}} Pr_{\mathrm{H}}(\pi \mid \tau) \cdot r_\varphi^h(\pi) = M_{\mathrm{H}}^*$$

满足 $M_{\mathrm{iH}} \in \mathrm{M}^C$的条件。 □

我们现在证明，通过对无限隐马尔可夫模型进行最大有界可达性性质的模型检测，可以在多项式时间内计算风险。据此，使用来自 [18] 的展开算法，可以在多项式时间内计算无限隐马尔可夫模型的监视判定。

定理 1. 判定问题 $M_{iH}(\tau) > \lambda$ 对于阈值 $\lambda \geq 0$可在多项式时间内计算。

定理 1 的证明结合了来自 [6, 16, 18, 25] 的工作。我们在本节剩余部分以图 2a 所示的小型无限隐马尔可夫模型为例，说明多项式时间判定过程。该无限隐马尔可夫模型有三个状态：初始状态 $s_0$ 的观测恰好为蓝色，以及状态 $s_1$、$s_2$ 的观测恰好为橙色。定义 6 中隐马尔可夫模型的概率观测可以在多项式时间内变换为此处所用的精确观测 [11]。任何单点区间都写成单一概率。设规范为 $\varphi = \neg s_2$，时域为 $h = 1$。最大化风险函数于是变为 $r = [s_0 \mapsto 0.3, s_1 \mapsto 0, s_2 \mapsto 1]$。假设我们观测到轨迹 $\tau = (blue)(orange)$。为计算 $M_{\mathrm{iH}}(\tau)$，我们执行如图 2b 所示的变换。我们按轨迹长度展开模型，$|\tau| = 2$。这给出状态 $s_i^j$，其中 $j$为该状态的展开深度。在时域处，我们添加指向两个新状态 $\top$ 和 $\bot$ 的转移，其中 $P(s_i^h, \top) = r(s_i)$，$P(s_i^h, \bot) = 1 - r(s_i)$。在此变换后的模型中，对轨迹的监测归结为一个条件可达性问题，

$$M_{\mathrm{iH}}((blue)(orange)) = Pr_{\mathrm{iH}}^{\max}(Reach(\top) \mid (blue)(orange)).$$

现在，我们对从区间隐马尔可夫模型到马尔可夫决策过程应用标准转换 [16]。该马尔可夫决策过程中的策略与区间隐马尔可夫模型细化后的隐马尔可夫模型之间存在一一对应关系。[25, 命题2] 表明，在马尔可夫决策过程中允许采用随机化策略时，二者的概率测度相等。因此，现在我们得到了一个带有随机化策略的马尔可夫决策过程 mdp，其中 $Pr_{\mathrm{iH}}^{\max}(\mathrm{Reach}(\top) \mid (blue)(orange)) = Pr^{\max}\,\mathrm{mdp}(\mathrm{Reach}(\top) \mid (blue)(orange))$。现在，[6]已证明，在马尔可夫决策过程中使条件概率最大的策略是确定性的，因此我们可以应用他们的转换，得到一个新的马尔可夫决策过程，在其中$Pr^{\max}\,\mathrm{mdp}(\mathrm{Reach}(\top) \mid (blue)(orange))$可以通过非条件可达概率模型检测来计算。因此，我们可以计算$M_{\mathrm{iH}}^{\max}((blue)(orange))$。

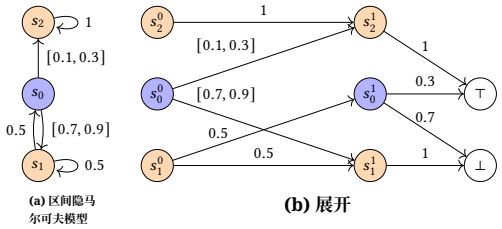



**图2：监测区间隐马尔可夫模型的变换**

## 4 学习理想监测器模型

上文中，我们从区间隐马尔可夫模型推导出了保守监控器。本节中，我们使用从 SuO 采样得到的路径，迭代地学习并细化区间隐马尔可夫模型。我们采用一种适配方法——线性更新区间 [28]——来学习区间隐马尔可夫模型，然后使用符合性检查来判断这些区间隐马尔可夫模型是否能提供足够精确的监控器。

### 4.1 学习区间隐马尔可夫模型

我们介绍一种从SuO中采样的路径数据集学习区间隐马尔可夫模型的过程。我们的方法密切遵循用于学习马尔可夫决策过程的线性更新区间（LUI）方法 [28]。为了支持学习观测分布，我们将关于这些分布的不确定性编码到转移中，其动机来源于变换 [11]。与用于马尔可夫决策过程的LUI一样，我们假设已知模型的状态空间和转移空间。我们使用相关变量定义状态空间（$V_{sys}$ 以及上文所述的进一步变量 $V_{obs}$）。我们利用领域知识（例如牛顿力学）推导出已有的转移。与 [28], 不同，我们不假设存在一个已知且唯一的初始状态。

现在我们概述初始化过程。我们通过为每个转移分配一个初始区间来初始化转移概率区间。例如，对于状态 $i$ 和 $j$之间的转移，我们分配$I_{i,\,j} = [I_{i,j}^{\downarrow}, I_{i,j}^{\uparrow}]$。此外，我们引入一个强度区间$[n_{i,j}^{\downarrow}, n_{i,j}^{\uparrow}]$，用于表示当前版本的概率区间所依据的样本数量的最小值和最大值。

为了估计转移概率，我们计算转移频率。具体而言，$N_i$ 表示某个状态 $i$在数据集中出现的总次数。$k_{i,\,j}$表示状态$j$在数据集中紧接着 $i$出现的次数。因此，给定转移的经验转移频率为$k_{i,\;\;j}/N_i$。概率区间按如下方式更新：

$$I_{i,j}^{\downarrow} := \begin{cases} \dfrac{n_{i,j}^{\uparrow} \times I_{i,j}^{\downarrow} + k_{i,j}}{n_{i,j}^{\uparrow} + N_i} & \forall x.\, \dfrac{k_{i,x}}{N_i} \geq I_{i,j}^{\downarrow} \\ \dfrac{n_{i,j}^{\downarrow} \times I_{i,j}^{\downarrow} + k_{i,j}}{n_{i,j}^{\downarrow} + N_i} & \exists x.\, \dfrac{k_{i,x}}{N_i} < I_{i,j}^{\downarrow} \end{cases} \qquad I_{i,j}^{\uparrow} := \begin{cases} \dfrac{n_{i,j}^{\uparrow} \times I_{i,j}^{\uparrow} + k_{i,j}}{n_i^{\uparrow} + N_i} & \forall x.\, \dfrac{k_{i,x}}{N_i} \leq I_{i,j}^{\uparrow} \\ \dfrac{n_{i,j}^{\downarrow} \times I_{i,j}^{\uparrow} + k_{i,j}}{n_i^{\downarrow} + N} & \exists x.\, \dfrac{k_{i,x}}{N_i} > I_{i,j}^{\uparrow} \end{cases}$$

我们根据规则 $0.5 \geq \epsilon > 0$ 将所有初始区间设为 $[\epsilon, 1-\epsilon]$，并根据 $0 \leq n_i^{\downarrow}$、$_j \leq n_i^{\uparrow}$、$_j$ 选择强度区间值。我们采用较小的 $\epsilon$，以不对先验知识作任何假设，并采用较低的强度值，使数据集中的信息能够迅速产生影响。如果给定状态的所有经验频率都落在先验区间内，则使用强度区间的上界计算后验区间

。否则，改用强度区间的下界。使用不同的强度值，可以在新数据不符合根据先前数据推导出的概率区间时，采取更为保守的响应。更新概率区间后，强度区间按如下方式更新：$[n^{\downarrow}_{i,j}, n^{\uparrow}_{i,j}] := [n^{\downarrow}_{i,j} + N_i, n^{\uparrow}_{i,j} + N_i]$。

初始状态概率区间的学习方式与此相同，其中 $N_i$ 对应数据集中的路径数量，而$k_{i,\ j}$表示以状态 $j$开头的轨迹数量。

随着新数据的不断获取，学习过程以迭代方式进行。LUI 方法会生成有效的概率区间，即这些区间始终满足：$0 \le I^{\downarrow}_{i,\ j} \le I^{\uparrow}_{i,\ j} \le 1$。此外，该方法还保证收敛到真实概率。我们现在在所采用的方法的背景下重述 [28],中的收敛性结论。

定理 2. 对于状态空间与某个隐马尔可夫模型相同的无限隐马尔可夫模型，使用 *LUI* 学习该无限隐马尔可夫模型的转移概率和初始分布，可保证当已处理的隐马尔可夫模型路径样本总数趋于无穷时，区间将收敛到精确的转移概率，而与每次迭代处理的样本数量无关。

因此，在极限情况下应用 LUI 方法将得到一个能够导出理想监视器的模型。

推论 1. *LUI* 会生成一个 *iHMM* 序列，通过逐点应用定义 *8*，该序列会导出一个监视器序列。该序列收敛于理想监视器。

## 4.2 基于符合性测试的细化

我们提出一种用于学习 iHMM 的基于符合性测试的细化框架，该框架建立在上一节介绍的 LUI 流程之上。该框架包含一个迭代流程：不断更新转移区间，直到基于 iHMM 的监控器给出的结果满足我们稍后定义的停止条件。我们尤其针对 LUI 的一些不足进行处理。LUI 方法保证收敛到真实 HMM，但不一定能高效地收敛到该 HMM。根据经验，来自经常访问状态的转移会很快收敛到较窄的区间，而来自很少访问状态的转移则会长时间保持较宽。这会导致 iHMM 监视器给出的结果很可能与理想监视器给出的结果不同。为了避免持续采样并学习那些转移概率近似值已经足够准确的邻域，我们引入一种基于符合性测试的细化方法，引导采样过程，进而引导学习过程，转向探索不足的邻域。实际应用中，我们希望尽可能少地处理样本，就能学习到一个与某个 iHMM 监视器相对应的 iHMM，且该监视器尽可能接近理想监视器。这正是细化框架的核心动机。

框架架构如图 3 所示。它由一个区间学习器组成，该学习器使用 LUI 更新当前 iH；一个轨迹采样器，用于从 SuO 中采样观测轨迹，以供一致性测试使用；以及一个一致性测试器，它接收当前 iHMM iH 的监控器 $M_{\text{iH}}$和一组轨迹 $T$，并检查是否满足停止条件。我们使用的停止条件定义为一个阈值 $\theta$，它作用于我们所称的“风险区间”的平均宽度。

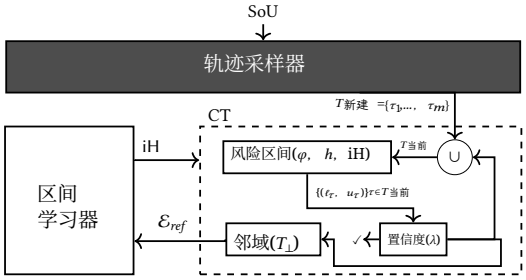



**图3：基于iHMM细化的学习。**

对于每条轨迹，区间边界分别为最小风险和最大风险（$\ell_\tau$， $u_\tau$）=（$M^{\min}_{\text{iH}}$（$\tau$） $M^{\max}_{\text{iH}}$（$\tau$）），其中 $u_\tau$是第3.3节中定义的 iHMM 监测器的结果，而 $\ell_\tau$是对应的风险最小化监视器的结果。如果所有待考察轨迹的风险区间平均宽度低于停止条件阈值 $\theta$，则 iHMM学习终止。

如图 3 所示，细化学习从一个初始iH和一组采样轨迹 $T_{new}$开始。初始iH的转移区间和初始分布区间均设为 $[\epsilon, 1-\epsilon]$。采样轨迹被送入风险区间分析；除非满足停止条件，否则每条未达到阈值的轨迹都会被送入邻域采样器。

邻域采样器从该轨迹 $\tau$的扩展邻域中采样路径；也就是说，对于 $\tau$的子序列 $\tau'$，我们以概率 $Pr(\pi \mid \tau')$采样路径 $\pi$。采样方法的详细内容见附录A。

所有邻域样本 E$^{ref}$ 都会被转发给区间学习器，以执行必要的更新。风险区间高于停止条件 $\theta$ 的轨迹 $T_\perp \subseteq T_{new}$会与构成集合 $T_{curr} = T_{new} \cup T_\perp$的最新采样新轨迹一同保留，用于下一轮一致性测试。当满足停止条件时，学习过程结束。

由于细化过程不涉及区间学习方法，而只会影响采样，因此以下结果成立。

推论 2. 在所学习的无限隐马尔可夫模型与真实*HMM*具有相同状态且 $\theta = 0$的假设下，应用基于符合性测试的细化过程，可以保证当处理的样本总数趋于无穷时，无论每次迭代处理多少样本，区间都会收敛至精确的转移概率。

## 5 实验评估

我们将探讨三个研究问题。首先，我们的基于模型的方法是否优于无模型方法？（5.2）其次，使用鲁棒模型能否在保持准确性的同时提高安全性？（5.3）第三，基于符合性测试的细化是否能更好地逼近理想监视器？（5.4）

## 5.1 实验设置

术语。 假阴性率 (FNR)、假阳性率 (FPR)、曲线下面积 (AUC)、停止条件 (SC)。

实现。我们为图 3 所示的框架以及第 3.3 节所述的基于无限隐马尔可夫模型的监测提供了原型实现。监控算法的实现

基于 Premise [18], 这一基于模型检测的监控工具，并将其适配到无限隐马尔可夫模型。该工件可在 [1] 获取。

基准测试。 我们使用改编自 [18, 31] 的基准测试。下表列出了这些基准测试。机场基准测试模拟了这样一个场景：一架自主飞机下降着陆，同时地面车辆横穿跑道。该场景考虑飞机与跑道之间的距离、地面车辆的位置以及观测到的这些车辆的位置。机场B模型包含了机场A中所使用噪声模型的更大版本。evadeV 基准测试模拟两个机器人的行为，其中一个机器人观测另一个机器人的位置。同一基准测试不同版本之间的差异（例如机场-A-7-10-10和机场-A-7-40-20）在于状态和观测信息的详细程度。SnL 是一个用于模拟蛇梯棋的玩具基准测试，主要用于合理性检查。

对于每个基准测试，我们都会监控可达性属性；在机场和 evade 基准测试中，这意味着我们估计未来发生碰撞的风险，而在 SnL-10x10 中，则是估计到达游戏最终状态的风险。

| Name | 状态 | 转移 | $\|\tau\|$ | $h$ |
|---|---|---|---|---|
| SnL-10x10$^{(*)}$ | 101 | 502 | 15 | 5 |
| evadeV-5-3 | 1001 | 3878 | 10 | 20 |
| evadeV-6-3$^{(*)}$ | 2 161 | 8 667 | 12 | 20 |
| airport-A-7-10-10$^{(*)}$ | 1 170 | 5 557 | 15 | 25 |
| 机场-A-7-40-20 | 10 760 | 56 577 | 125 | 35 |
| 机场-B-7-40-20$^{(*)}$ | 21 520 | 152 170 | 125 | 35 |

带星号标记的基准 $(*)$ 还在“粗粒度”变体下进行了测试，其中部分系统变量不会提供给学习器。我们使用这些变体研究状态空间缩减对学习得到的监视器准确性的影响。请注意，定理 2 和推论 2 中讨论的收敛保证不适用于粗粒度模型。

学习设置。我们使用第4.1节所述的改进版 LUI 方法，通过邻域采样学习无限隐马尔可夫模型，并根据这些模型构建监控器，具体如第3.3节所述。监控器通过长度为 $|\tau| + h$ 的路径数据集进行学习。测试时，我们使用长度为 $|\tau|$ 的轨迹，并将监测时域设为 $h$。$|\tau|$ 和 $h$ 的取值见基准测试表。学习得到的监控器在 500 条轨迹上进行测试。出于内存方面的考虑，机场-A-7-40-20 和 airport-B-7-40-20 基准在 200 条轨迹上进行测试。基准 airportB-7-40-20 在 12 小时内未能完成，因此省略其结果。每种方法在每个基准上运行 10 次。除非另有说明，图中展示的是平均值和以阴影标示的 $\pm 1$ 个标准差范围。所有实验均使用 Intel Xeon Gold 6338 CPU（16 核）和 NVIDIA A100 GPU，并设有 12 小时超时。只有保形预测在 GPU 上运行，其他所有计算均基于 CPU。

## 5.2 基于模型与无模型的监测

在本实验中，我们将基于模型的方法与两种无模型监测方法进行比较。我们考察了两种无模型方法：（1）通过 sklearn 库学习得到的随机梯度下降（SGD）回归器 [22],，以及（2）一种共形预测方法[9],，该方法专门用于在不确定性下进行监测；该方法采用神经网络方法来估计风险，并通过共形预测验证计算出的风险。

无模型方法使用细化学习所用的最高样本数进行一次性训练。我们的比较依据不同阈值下的假阳性率（用于评判保守性）和假阴性率（用于评判安全性）进行。对于所有基准测试，我们根据基准的规模，在风险区间宽度上选择安全置信度。为较小的基准选择较低的安全置信度，可确保学习需要非平凡数量的数据。

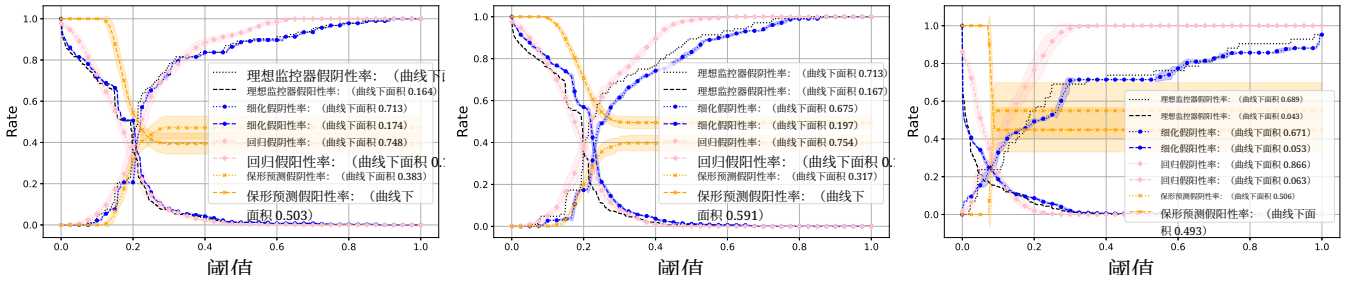
我们在所有基准测试上进行了该实验。在图4中，我们展示了airportA-7-10-10和SnL-10x10的一组代表性结果。其余结果见第B.1节。我们的目标是创建一个尽可能接近理想监视器$M^*$的谨慎监控器。在图4中，$M^*$ 的假阴性率和假阳性率分别用黑色点线和虚线表示。我们绘制了随阈值增大而变化的比率，其中阈值为1表示没有任何轨迹被视为不安全。我们的目标是使监视器的假阴性率曲线接近并始终低于 $M^*$的假阴性率，从而使假阴性率曲线下面积略低于 $M^*$的曲线下面积。

我们观察到，基于 *iHMM* 的监测器在支持安全性方面具有优势，同时又不会过于保守。图表清楚地显示，在除粗粒度 SnL-10x10 以外的所有基准测试中，针对每个基准测试和所有阈值，iHMM 监测器的假阴性率始终低于 $M^*$。对于某些阈值，iHMM 监控器的假阴性率高于 $M^*$（图 4c）。假阴性率高于 $M^*$ 表明，对于某些轨迹，学习得到的监控器低估了风险，导致轨迹被错误地归类为安全。尽管在粗粒度 SnL-10x10 基准测试中，iHMM 监控器有时的假阴性率高于 $M^*$ 这一点令人担忧，但其他替代方案的表现要差得多，其中回归的假阴性率远高于它。假阳性率保持在较低水平，并且与 $M^*$ 的假阳性率非常接近（图 4a）。其他基准测试中也观察到了这一点（附录 B.1）。总体而言，在考虑真实状态空间时，iHMM 监测器的准确性有所提高；图 4a 显示，iHMM 监测器几乎完美地模仿了 $M^*$ 的行为。

无模型监控器缺乏准确性，并会损害安全性。 保形预测监控器在准确性方面表现严重不佳。我们将其归因于这样一个事实：这些监控器是为具有确定性动力学的系统设计的。回归监控器同样在准确性方面表现不佳。回归方法在所有实验中都存在一个缺陷，即无法拟合 $M^*$的行为。FPR 和假阴性率曲线过于平滑，无法拟合 $M^*$曲线的形状。

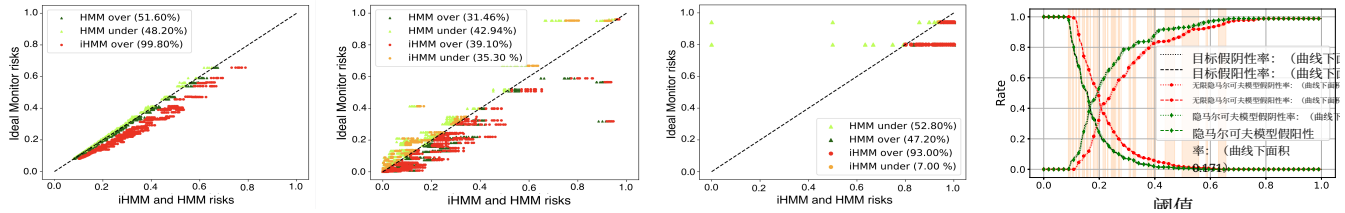
### 5.3 无限隐马尔可夫模型与基于隐马尔可夫模型的监测

在本节中，我们探讨使用鲁棒模型进行安全监测所产生的影响。我们将 iHMM 和基于 HMM 的监测器近似得到的风险值与来自 $M^*$ 的风险值进行比较，并将其归类为下近似或上近似。此外，我们考察假阳性率和假阴性率，以研究不同阈值下的监测结果。我们使用细化学习所用的最大样本数来学习 HMM 模型。我们将数据集划分为 10 个相等的批次，并逐步增加用于学习的批次数，因此每次运行会得到 10 个 HMM 模型。HMM 使用简单的频率学派方法进行学习。



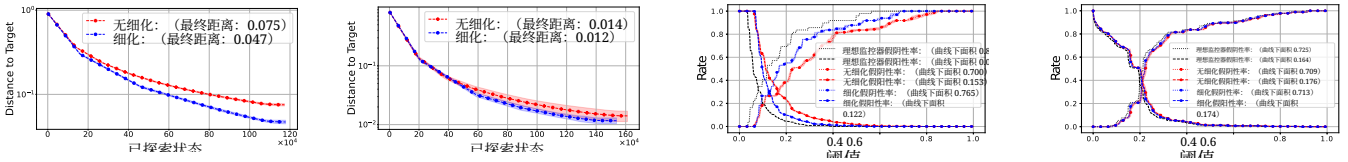

（a）airportA-7-10-10，安全置信度 = 0.001　（b）粗粒度 airportA-7-10-10，安全置信度 = 0.01　（c）粗粒度 SnL-10x10，安全置信度 = 0.01

**图4：比较基于模型的方法与无模型方法的假阴性率和假阳性率。**




(a) evadeV-5-3，安全置信度= 0.01　(b) 粗粒度 SnL-10x10，安全置信度= 0.01　(c) Unlikely-15，安全置信度= 0.01　(d) evadeV-5-3 安全置信度 = 0.01

**图5：无限隐马尔可夫模型与基于 HMM 的监测器在风险估计（a-c）以及假阴性率和假阳性率（d）方面的比较。散点图（a-c）绘制了每种方法全部 10 次运行的数值。**




(a) 粗粒度 evadeV-6-3，安全置信度 = 0.01　(b) airportA-7-10-10，SC = 0.001　(c) 粗粒度 evadeV-6-3，SC= 0.01　(d) airportA-7-10-10，SC= 0.001

**图6：比较　　有无细化的学习效果，在距离 $M^*$ (a-b)、假阴性率和假阳性率方面的比较 (c-d　　)**

对于所有基准测试（附录 *B.2*），我们观察到基于 *iHMM* 的监测器在安全性方面具有积极效果。 EvadeV-5-3（图 5a）是一个展示 iHMM 和 HMM 监测典型性能的基准。图中绘出了 HMM 和 iHMM 监视器近似得到的风险，并将其与理想监视器的风险进行比较；其中每个点代表一个理想监视器风险值，以及一个 iHMM（红色）或 HMM 风险值（绿色）。我们观察到，基于 iHMM 和基于 HMM 的监测器在下近似和上近似方面存在显著差异。如图 5a 所示，对于近一半的轨迹，基于 HMM 的监测器会低估风险，而基于 iHMM 的监测器几乎总是高估风险，因此能够支持安全性。由此产生了许多阈值，在这些阈值下，基于 HMM 的监测器的假阴性率高于 $M^*$（图 5d 中的橙色区域）。因此，对于这些阈值，我们可以预期 HMM 监测器会将一些不安全轨迹错误分类为安全轨迹。基于 iHMM 的监测器则不会出现这种情况。唯一一个观察到基于 iHMM 的监测器产生显著风险下近似的基准是粗粒度 SnL-10x10（图 5b）。不过，对于这个基准，与基于隐马尔可夫模型的监控器相比，基于无限隐马尔可夫模型的监控器在轨迹较少时会低估风险。

基于 *HMM* 的监测器可能会严重低估风险。虽然隐马尔可夫模型中的许多轨迹都会导致风险被低估，但差异通常很小。不过，这并不总是如此。我们引入了另一个基准 Unlikely-15，用来展示 HMM 监控器未能识别高风险情形的情况。Unlikely-15 的结构使得其中某些邻域极少被遇到，因此无限隐马尔可夫模型在这些邻域中的概率区间较宽，从而导致风险被高估。然而，HMM 可用的样本很少，学到的概率与真实值相差甚远，有时会大幅低估风险。图 5c 绘制了通过拒绝采样识别出的 100 条具有正风险的轨迹，其中包括一些轨迹示例：HMM 监控器将高风险轨迹误判为低风险，这可能导致违反安全规范。

## 5.4 无细化与细化学习

最后，我们考察基于精化的无限隐马尔可夫模型学习对监测结果的影响。我们考察到 $M^*$ 的距离变化以及假阳性率与假阴性率之间的差异。在这项实验中，我们还使用细化学习所用的最大样本数，在不进行细化的情况下学习无限隐马尔可夫模型。我们将数据集分成 10 个等量批次，并通过依次添加批次进行学习，因此每次运行会得到 10 个无限隐马尔可夫模型。

采用细化进行学习，始终能使监控器在学习过程结束时更接近 $M^*$。请注意，所用的距离度量为 $\delta = \frac{\sum_{\tau \in T_{\mathrm{H}}} |M^*(\tau) - M(\tau)|}{|T_{\mathrm{H}}|}$；在实验评估中，我们仅考虑 $T_{\mathrm{H}}$ 的一个采样子集。正如预期，距 $M^*$ 的距离与假阴性率和假阳性率数值之间存在关联。对于那些细化方法在距 $M^*$ 的距离方面产生显著影响的基准测试，我们发现细化方法能使假阴性率与假阳性率曲线更接近理想假阴性率与假阳性率曲线（图 7、9）。细化过程的优势在于提高了样本效率。例如，在图 7 的情形中，我们只需探索非精化方法所需状态数的约三分之二，就能学到与无细化学习方法同样出色的监控器。

细化过程对不同基准的影响各不相同。对于粗粒度 evadeV-6-3 基准，经过细化学习得到的区间隐马尔可夫模型所对应的监控器，比未经细化时显著更接近 $M^*$（图 7）。这使得细化后的监控器能够更好地近似理想假阴性率与假阳性率曲线（图 9）。另一方面，对于 airportA-7-10-10 基准，细化与不细化之间的差异很小，如图 8 和图 10 所示。

我们还考虑了一种替代采样方法，该方法在实验评估中几乎没有表现出差异。我们在附录A中介绍了这种方法，并在附录5.3中对两种采样方法进行了实验比较。

## 5.5 进一步说明

最大基准上的结果。为两个最大的基准 airportA-7-40-20 和 airport-B-7-40-20 学习监控器颇具挑战。因此，我们将分别讨论这些基准上的监控器学习。此前的一些结论仍然成立，即细化对与 $M^*$ 的距离有积极影响。我们还观察到，与基于 HMM 的监测器不同，无限隐马尔可夫模型能够给出安全风险近似。尽管结果令人鼓舞，但我们不对这些实验得出强有力的结论，因为所有学习方法得到的监控器都输出了与 $M^*$ 相去甚远的结果。我们推测，原因在于 SC 过高，以及这些基准中的违规路径出现频率显著更低。附录C中给出了详细讨论。

参数敏感性。我们注意到，粗粒度状态空间和较低的停止条件阈值会产生影响。实验结果凸显了识别相关状态变量的重要性，以及为学习能够紧密近似 $M^*$的监控器选择较低停止阈值的重要性。

计算成本。所有实验的超时时间均设为 12 小时，但大多数基准测试所需时间要短得多。以安全置信度为 =0 的 evadeV-6-3 为例，学习一个经过细化的无限隐马尔可夫模型需要约 110 秒，学习一个未经细化的无限隐马尔可夫模型需要约 220 秒，学习一个隐马尔可夫模型需要约 9 秒，训练一个回归模型需要约 10 秒，而训练一个保形预测模型需要约 345 秒。值得注意的是，只有保形预测方法是在图形处理器上训练的。所评估的监控器在执行速度方面也各不相同。仍以 evadeV-6-3 为例，在长度为 12、时域设为 20 的轨迹上进行测试时，隐马尔可夫模型、无限隐马尔可夫模型、回归和保形预测监控器生成风险估计所需的时间分别为 1.8、20、0.003 和 1.6 毫秒。值得注意的是，优化无限隐马尔可夫模型监控器的学习和执行速度并非本研究的重点。

## 6 相关工作

不确定性下的监控系统已在许多场景中得到研究，涵盖从基于模型的方法 [2, 3, 10, 17, 18, 34] 到无模型方法 [9, 29, 35]。基于学习马尔可夫模型的方法包括 [3], , 该方法提出了一种针对已学习隐马尔可夫模型的监控算法，在监测过程中依赖于选择最可能的单个隐状态。与考虑可能状态上的分布相比，这种做法无法在不确定性下实现准确监测所需的精度。[2] 进一步扩展了这一方法，引入重要性采样（IS），以更高效地学习稀有事件，这与我们的细化过程类似。然而，他们的IS基于使用经过修改的仿真，其中稀有事件以已知的更高概率发生，因此不适用于我们的场景。无模型方法的一个例子见 [9], , 该方法采用神经网络方法进行状态估计，并在此基础上使用保形预测进行风险估计。这种方法的一个瓶颈是，它专为具有确定性动力学的监控系统而设计，这与我们的方法形成对照。文献中还包括若干研究，探讨如何从数据中学习马尔可夫模型。其中包括用于学习马尔可夫决策过程的主动学习方法 [4] ，以及一种学习隐马尔可夫模型的方法 [3]。这两种方法都基于 Baum-Welch算法，因此对所用训练先验高度敏感。强化学习中的屏蔽也与此相关，并已应用于部分可观测系统[12, 21]。然而，与我们的方法不同，屏蔽需要（预先）计算部分信息调度器，最重要的是还需要模型。另有若干研究致力于运行时保障（执行），探讨如何利用监控器判定进一步改变系统行为 [15, 23, 26, 33]。我们的重点是监测，而我们的方法可以集成到这些方法中，构成完整的保障流程。

## 7 结论

我们提出了一种用于学习鲁棒的基于马尔可夫模型的监控器的框架。我们的方法能够保证收敛到理想监视器。实验结果表明，学习得到的监测器在准确且谨慎的监测方面优于其他方法，尤其是相比无模型方法。

## 致谢

本研究部分由克努特与爱丽丝·瓦伦堡基金会资助的瓦伦堡人工智能、自主系统与软件计划（WASP）以及荷兰科学研究组织的 FuRoRe 项目资助（OCENW.M.22.282）。

计算工作使用了瑞典国家学术超级计算基础设施（NAISS）提供的资源；该基础设施部分由瑞典研究理事会通过编号为 2022-06725 的资助协议提供资金。

## 参考文献

[1] Skurka Antonina、Luko van der Maas、Sebastian Junges 和 Hazem Torfah。2026。《用于安全运行时监控的鲁棒马尔可夫模型学习》的工件》。*https://doi.org/*。*/zenodo*。*Reza Babaee*、*Vijay Ganesh* 和 *Sean Sedwards*。*2019*。针对罕见故障的预测性运行时监视器加速学习。载于*RV*（计算机科学讲义，第*11757*卷）。施普林格，111–128。[3] Reza Babaee、Arie Gurfinkel 和 Sebastian Fischmeister。2018。Prevent：一种采用统计学习的预测性运行时验证框架。第*16*届软件工程与形式化方法国际会议，205–220。[4] Giovanni Bacci、Anna Ingolfsdottir、Kim G. Larsen 和 Raphaël Reynouard。2021。使用Baum-Welch算法主动学习马尔可夫决策过程。载于《论文集——第*20*届*IEEE*国际机器学习与应用会议（*ICMLA 2021*）》（《论文集——第*20*届*IEEE*国际机器学习与应用会议（*ICMLA 2021*）》），M. Arif Wani、Ishwar K. Sethi、Weisong Shi、Guangzhi Qu、Daniela Stan Raicu 和 Ruoming Jin（编）。IEEE（电气与电子工程师协会），美国，1203–1208。https: //doi.org/ 10 1109 52953 2021 00195 。/ICMLA。。Christel Baier 和 Joost-Pieter Katoen[5] 2008。。《模型检测原理》（表征与心智丛书）。麻省理工学院出版社。[6] Christel Baier、Joachim Klein、Sascha Klüppelholz 和 Steffen Märcker。2014。高效计算马尔可夫模型中的条件概率。载于*TACAS*（计算机科学讲义，第*8413*卷）。施普林格，515–530。[7] Ezio Bartocci、Jyotirmoy Deshmukh、Alexandre Donzé、Georgios Fainekos、Oded Maler、Dejan Ničković 和 Sriram Sankaranarayanan。2018。基于规范的网络物理系统监控：理论、工具与应用综述。施普林格国际出版，开姆尼茨，135–175。https://doi.org/10.1007/978-3-319-75632-5 5[8] Felix Berkenkamp、Matteo Turchetta、Angela P. Schoellig 和 Andreas Krause。2017。具备稳定性保证的安全的基于模型的强化学习。载于第*31*届神经信息处理系统国际会议论文集 （美国加利福尼亚州长滩）（*NIPS' 17*）。Curran Associates Inc.，美国纽约州雷德胡克，908–919。[9] Francesca Cairoli、Luca Bortolussi 和 Nicola Paoletti。2021。部分可观测条件下的神经预测监控。载于运行时验证国际会议。施普林格，121–141。[10] Matteo Camilli、Raffaela Mirandola 和 Patrizia Scandurra。2021。弹性网络物理系统的运行时均衡验证。载于*2021*年*IEEE*自主计算与自组织系统国际会议（*ACSOS*）。IEEE, 71 80 10 1109 52086 2021 00025 –。[11] https://doi.org/。/ACSOS。。Krishnendu Chatterjee、Martin Chmelik、Raghav Gupta 和 Ayush Kanodia。2015。部分可观测马尔可夫决策过程中的最优成本几乎必然可达性。载于*AAAI*。AAAI出版社，3496–3502。[12] Krishnendu Chatterjee、Petr Novotn`y、Guillermo Pérez、Jean-François Raskin 和 Đorđe Žikelić。2017。部分可观测马尔可夫决策过程中的期望优化与保证。载于*AAAI*。3725–3732。[13] David Dalrymple、Joar Skalse、Yoshua Bengio、Stuart Russell、Max Tegmark、Sanjit Seshia、Steve Omohundro、Christian Szegedy、Ben Goldhaber、Nora Ammann、Alessandro Abate、Joe Halpern、Clark W. Barrett、Ding Zhao、Tan Zhi-Xuan、Jeannette M. Wing 和 Joshua B. Tenenbaum。2024。迈向有安全保证的人工智能：确保人工智能系统鲁棒可靠的框架。*CoRR* abs/2405.06624（2024）。[14] Giuseppe De Giacomo 和 Moshe Y. Vardi。2013。有限轨迹上的线性时序逻辑与线性动态逻辑（*IJCAI '13*）。AAAI出版社，854–860。[15] Ankush Desai、Shromona Ghosh、Sanjit A. Seshia、Natarajan Shankar 和 Ashish Tiwari。2019。SOTER：用于安全机器人系统编程的运行时保障框架。载于*2019*年第*49*届*IEEE/IFIP*可靠系统与网络国际年会（*DSN*）。138–150。https://doi.org/10.1109/DSN. 2019.00027[16] Garud N. Iyengar。2005。鲁棒动态规划。数学运筹学30，2（2005），257–280。[17] Sebastian Junges、Sanjit A. Seshia 和 Hazem Torfah。2024。《不确定条件下运行时监视器的主动学习》。载于集成形式化方法——第*19*届国际会议，*IFM 2024*，英国曼彻斯特，*2024*年*11*月*13*日至*15*日，论文集（计算机科学讲义，第*15234*卷），Nikolai Kosmatov 和 Laura Kovács（编）。施普林格, 297 306 10 1007 978 3 031 76554 4_18 – 。[18] 2021 https://doi.org/ 。 / - - - - Sebastian Junges、Hazem Torfah 和 Sanjit A. Seshia。。马尔可夫决策过程的运行时监视器。载于*CAV*（*2*）（计算机科学讲义，第*12760*卷）。施普林格，553–576。[19] Stefan Mitsch 和 André Platzer。2016。ModelPlex：对经验证的信息物理系统模型进行经验证的运行时验证。形式化方法与系统设计49，1-2（2016），33–74。https://doi.org/10.1007/s10703-016-0241-z [20] Thomas M. Moerland、Joost Broekens、Aske Plaat 和 Catholijn M. Jonker。2023。基于模型的强化学习：综述。机器学习趋势16，1 2023 1 118( )，– 。[21] Wonhong Nam 和 Rajeev Alur。2010。部分可观测条件下针对安全性和可达性目标的计划主动学习。*IEEE*系统、人类与控制论汇刊*B*辑（控制论）40，2（2010），412–420。https://doi.org/10. 1109/TSMCB.2009.2025657[22] F. Pedregosa、G. Varoquaux、A. Gramfort、V. Michel、B. Thirion、O. Grisel、M. Blondel、P. Prettenhofer、R. Weiss、V. Dubourg、J. Vanderplas、A. Passos、D. Cour- nap eau、M. Brucher、M. Perrot 和 E. Duchesnay。2011。Scikit-learn：Python中的机器学习。机器学习研究期刊12（2011），2825–2830。[23] Dung Phan、Junxing Yang、Matthew Clark、Radu Grosu、John Schierman、Scott Smolka 和 Scott Stoller。2017。面向高可信信息物理系统的基于组件的单纯形架构。载于*2017*年第*17*届并发在系统设计中的应用国际会议（*ACSD*）。IEEE计算机学会，洛斯阿拉米托斯，加利福尼亚州，美国, 49 58 10 1109 2017 23 – 。[24] 2014 https://doi.org/ 。 /ACSD. 。Hossein Pishro-Nik。。概率、统计学与随机过程导论。Kappa Research, LLC，布卢贝尔，宾夕法尼亚州，美国。[25] Koushik Sen、Mahesh Viswanathan 和 Gul Agha。2006。在存在不确定性的情况下对马尔可夫链进行模型检测。载于*TACAS*（计算机科学讲义，第*3920*卷）。施普林格，394–410。[26] Lui Sha。2001。用简洁性控制复杂性。*IEEE*软件18，4（7月 2001 20 28 10 1109 2001 936213 ），– 。https://doi.org/ 。 /[27] MS. 。Scott D. Stoller、Ezio Bartocci、Justin Seyster、Radu Grosu、Klaus Havelund、Scott A. Smolka 和 Erez Zadok。2011。基于状态估计的运行时验证。载于*RV*（计算机科学讲义，第*7186*卷）。施普林格，193–207。[28] Marnix Suilen、Thiago D Simão、David Parker 和 Nils Jansen。2022。马尔可夫决策过程的鲁棒随时学习。神经信息处理系统进展35（2022），28790–28802。[29] Hazem Torfah、Aniruddha R. Joshi、Shetal Shah、S. Akshay、Supratik Chakraborty 和 Sanjit A. Seshia。2023。运行设计域的监视器集成学习。载于第*23*届运行时验证国际会议（*RV*）（计算机科学讲义，第*14245*卷），Panagiotis Katsaros 和 Laura Nenzi（编）。施普林格，271–290。[30] Hazem Torfah、Carol Xie、Sebastian Junges、Marcell Vazquez-Chanlatte 和 Sanjit A. Seshia。2022。可信自主的可监视运行设计域学习。施普林格出版社，柏林，海德堡，3–22。https://doi.org/ 10 1007 978 3 031 19992 9_1 . / - - - - Luko van der Maas 和 Sebastian Junges。[31] 2025。隐马尔可夫模型的经验证监视器学习。*CoRR* abs/2504.05963（2025）。[32] Cristina M. Wilcox 和 Brian C. Williams。2010。随机故障系统的运行时验证。载于*RV*（计算机科学讲义，第*6418*卷）。施普林格，452–459。[33] Beyazit Yalcinkaya、Hazem Torfah、Ankush Desai 和 Sanjit A. Seshia。2023。Ulgen：用于安全信息物理系统编程的运行时保障框架。*IEEE*计算机辅助设计与集成电路系统汇刊42，11（2023），3679 3692 10 1109 2023 3246386 – 。[34] https://doi.org/ 。 /TCAD. 。Hansol Yoon、Yi Chou、Xin Chen、Eric W. Frew 和 Sriram Sankaranarayanan。2019。线性随机系统的预测性运行时监控及其在无人机地理围栏执行中的应用。载于*RV*（计算机科学讲义，第*11757*卷）。施普林格，349–367。[35] Yiqi Zhao、Bardh Hoxha、Georgios Fainekos、Jyotirmoy V. Deshmukh 和 Lars Lindemann。2024。分布偏移下用于STL运行时验证的鲁棒保形预测。载于第*15*届*ACM/IEEE*网络物理系统国际会议，*ICCPS 2024*，香港，*2024*年*5*月*13*日至*16*日。IEEE，169–179。https: //doi.org/10.1109/ICCPS61052.2024.00022

## 关于细化框架的扩展讨论

下面我们将详细介绍第4.2节中提出的邻域路径采样方法。邻域采样分为两个步骤：第一步寻找一个不良邻域，第二步从该不良邻域中采样。

ˆ 第一步是识别不良轨迹 $T_\perp$ 的不良前缀 $\tau \in T_\perp$。我们采用两种不同的方法来识别不良前缀，从而区分两种细化方法（“无拆分细化”和“拆分细化”）。

在第一种方法中，我们选择 $N_{neigh} = \{0, \ldots, 10\}$ 个大小线性递增的前缀 $\hat{T}_\perp = \bigcup_{\tau \in T_\perp} \{\tau^{\leq N_{neigh}} | n \in N_{neigh}\}$。

在第二种方法中，我们将模型视为由两个可能重叠的部分组成。第一部分称为初始部分，用于对轨迹到达某个状态的概率建模；第二部分称为时域部分，用于对所到达状态的风险建模。对于每条不良轨迹，我们判断初始部分和时域部分中哪一部分更差。具体来说，我们比较沿着该不良轨迹可到达的随机抽样状态的最小风险和最大风险。如果该风险区间的宽度大于停止条件的阈值，我们就将完整轨迹加入不良前缀；否则加入空轨迹。因此，我们将相应地从轨迹终点处开始的邻域，或该轨迹所经过的邻域中进行抽样。

使用任一方法识别出不良前缀后，我们会在观测到前缀 $\tau'$ 的条件下，从状态中随机采样；也就是说，我们以概率 $\sum_{\pi \in \Pi^{|\tau'|-1}} Pr(\pi s \mid \tau')$ 采样一个状态 $s$。我们将采样状态的集合称为 $S_\perp$。至此，第一步完成。

第二步中，我们从以 $S_\perp$ 中的状态为起点的 SuO 中采样，得到路径 E$ref$。

第一种方法的目标是从该轨迹的整个邻域中均匀采样。第二种方法旨在判断较宽风险区间的根源是风险估计不足，还是对产生该轨迹的路径分布估计不佳，并着重解决根本问题。

## A.1 实验比较

从实验结果来看，拆分细化的平均表现略优于无拆分细化，如图 7、8、9 和 10 所示。哪些条件下精化方法有益，以及如何开发改进的精化方法，留待后续研究。实验比较中两种精化方法的其余结果——

法可参见附录 B.4。B.1 中的实验评估包含了两种细化方法的结果。

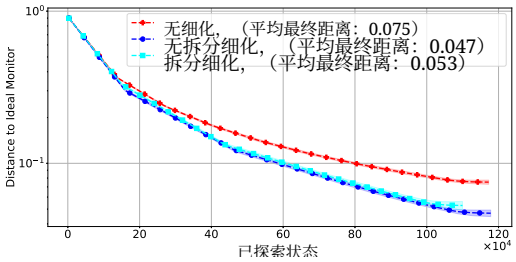



**图 7：比较采用和不采用细化的学习结果，以到 IM 的距离、粗粒度 evadeV-6-3、SC = 0.01 为指标**

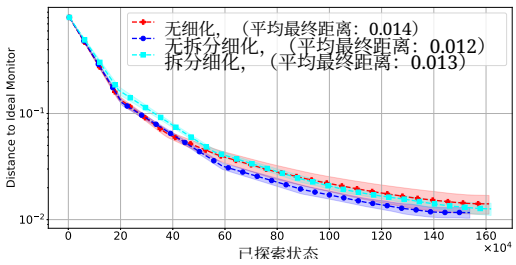



**图 8：比较采用和不采用细化的学习结果，以到 IM 的距离、airportA-7-10-10、SC = 0.001 为指标**

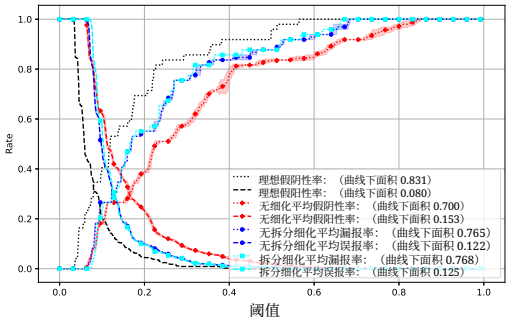



**图 9：比较细化前后的学习效果，以假阴性率和假阳性率衡量，coarseevadeV-6-3，SC= 0.01**

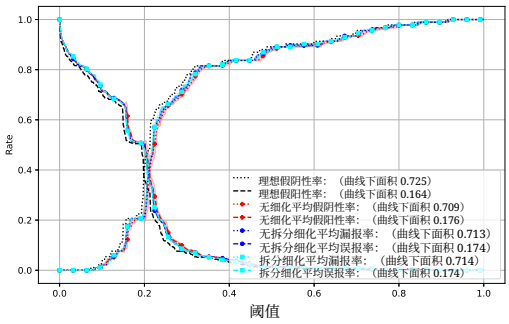



**图10：比较细化前后的学习效果，以假阴性率和假阳性率衡量，airportA-7-10-10，SC= 0.001**

## B 补充实验结果

## B.1 基于模型与无模型监控——其余实验结果

对于第 5.2 节未纳入的每个基准测试，我们都补充了相应的分析，比较基于模型和无模型监控器在不同阈值下的假阴性率和假阳性率。

基准 airportA-7-40-20 和粗略 airportB-7-40-20 的监视器实验评估见第 C 节。

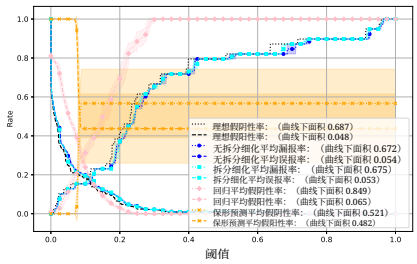



**图 11：SnL-10x10，安全置信度 = 0.001——基于模型方法与无模型方法的假阴性率和假阳性率对比**

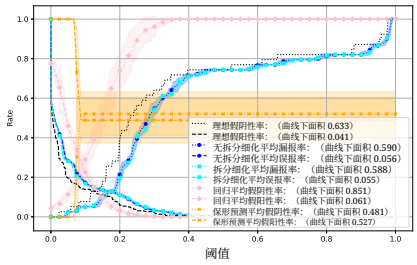



**图 12：SnL-10x10，安全置信度 = 0.01——基于模型方法与无模型方法的假阴性率和假阳性率对比**

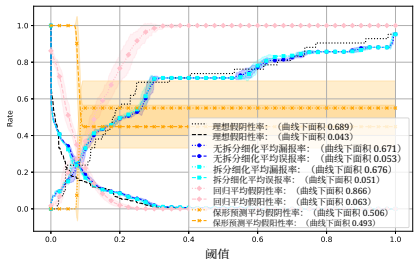



**图 13：粗粒度 SnL-10x10，安全置信度 = 0.01——基于模型与无模型方法的假阴性率和假阳性率比较**

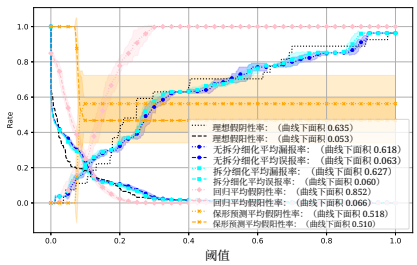



**图 14：粗粒度 SnL-10x10，安全置信度 = 0.1——基于模型与无模型方法的假阴性率和假阳性率比较**

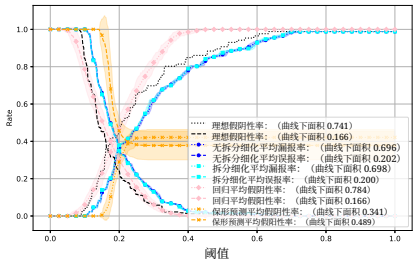



**图 15：evadeV-5-3，安全置信度 = 0.01——基于模型与无模型方法的假阴性率和假阳性率比较**

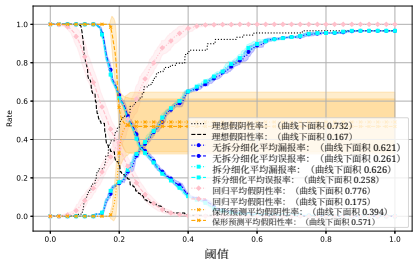



**图 16：evadeV-5-3，安全置信度 = 0.1——基于模型与无模型方法的假阴性率和假阳性率比较**

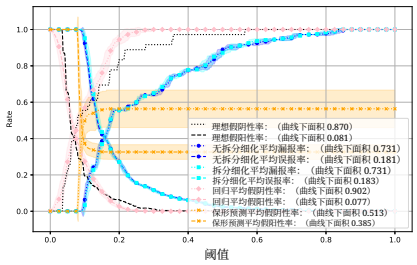



**图 17：evadeV-6-3，安全置信度 = 0.01——基于模型与无模型方法的假阴性率和假阳性率比较**

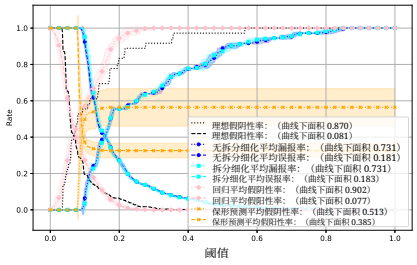



**图 18：evadeV-6-3，安全置信度 = 0.1——基于模型与无模型方法的假阴性率和假阳性率比较**

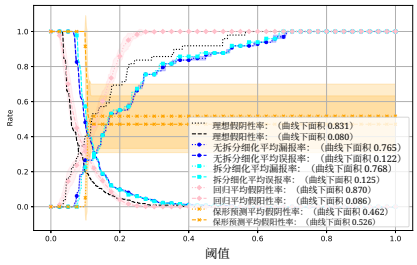



**图19：粗粒度 evadeV-6-3，安全置信度 = 0.01 - 基于模型与无模型方法的假阴性率和假阳性率比较**

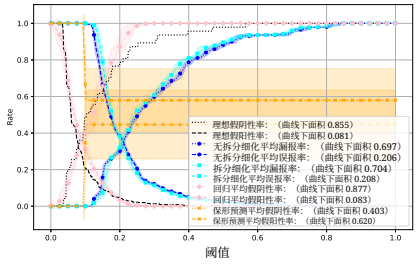



**图20：粗粒度 evadeV-6-3，安全置信度 = 0.1 - 基于模型与无模型方法的假阴性率和假阳性率比较**

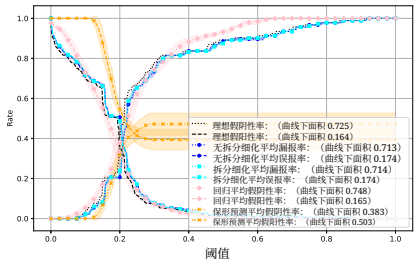



**图21：airportA-7-10-10，安全置信度 = 0.001 - 基于模型与无模型方法的假阴性率和假阳性率比较**

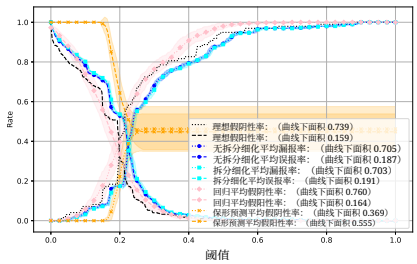



**图22：airportA-7-10-10，安全置信度 = 0.01 - 基于模型与无模型方法的假阴性率和假阳性率比较**

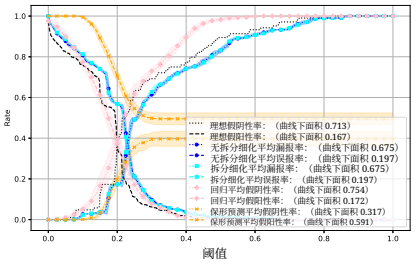



**图23：粗粒度 airportA-7-10-10，安全置信度 = 0.01 - 基于模型与无模型方法的假阴性率和假阳性率比较**

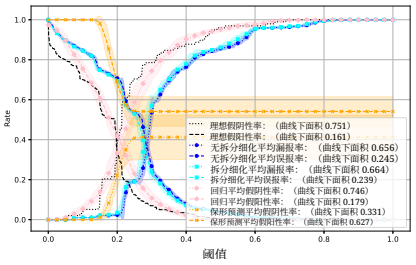



**图24：粗粒度 airportA-7-10-10，安全置信度 = 0.1 - 基于模型和无模型方法的假阴性率与假阳性率对比**

### B.2 基于无限隐马尔可夫模型与隐马尔可夫模型的监测

对于第5.3节未包含的每个基准测试，我们补充了相应分析，包括无限隐马尔可夫模型与隐马尔可夫模型监视器在不同阈值下的假阴性率和假阳性率对比，以及将风险分类为低估或高估。基准测试 airportA-7- 40-20 和粗略 airportB-7-40-20 的监视器实验评估见第C节。

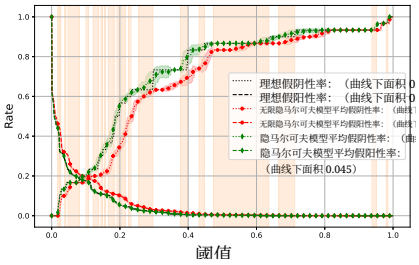



**图25：SnL-10x10，安全置信度 = 0.001 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率对比**

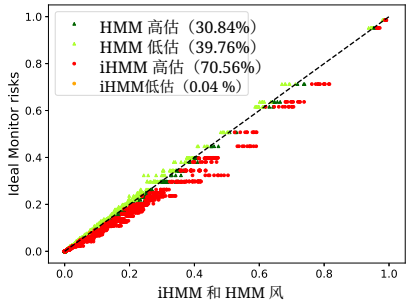



**图26：SnL-10x10，安全置信度 = 0.001 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

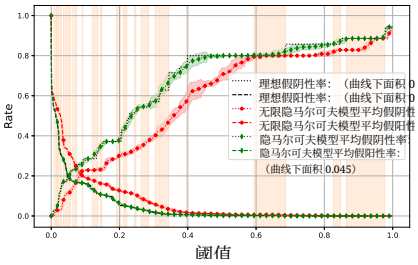



**图27：SnL-10x10，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

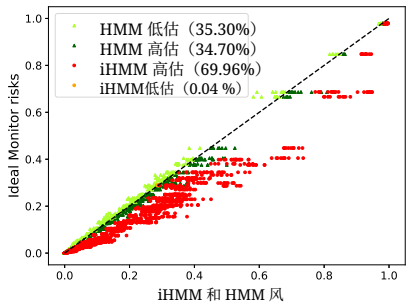



**图28：SnL-10x10，安全置信度 = 0.01 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

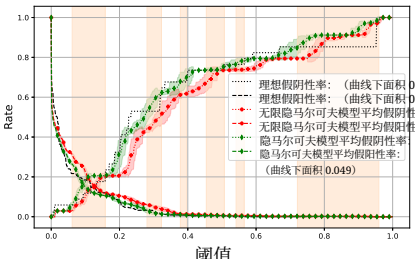



**图29：粗粒度 SnL-10x10，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

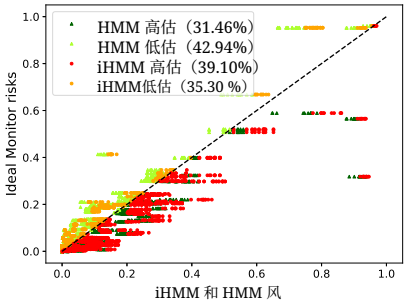



**图30：粗粒度 SnL-10x10，安全置信度 = 0.01 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

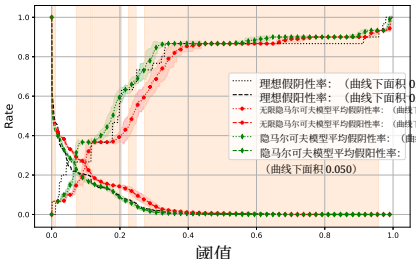



**图31：粗粒度 SnL-10x10，安全置信度 = 0.1 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

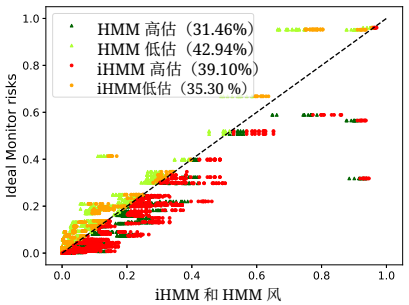



**图32：粗粒度 SnL-10x10，安全置信度 = 0.1——针对目标的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

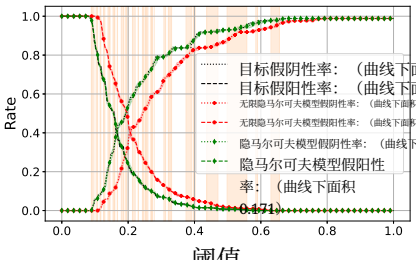



**图33：evadeV-5-3，安全置信度 = 0.01——无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

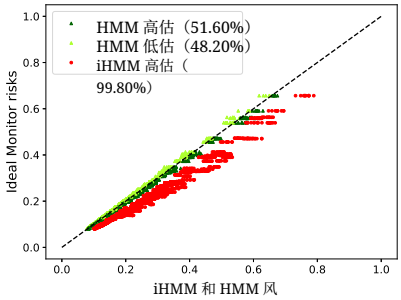



**图34：evadeV-5-3，安全置信度 = 0.01 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

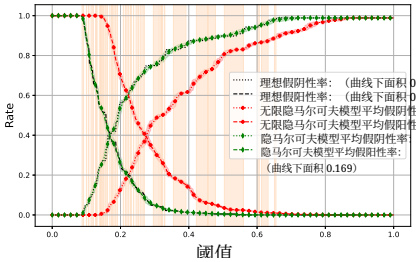



**图35：evadeV-5-3，安全置信度 = 0.1 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

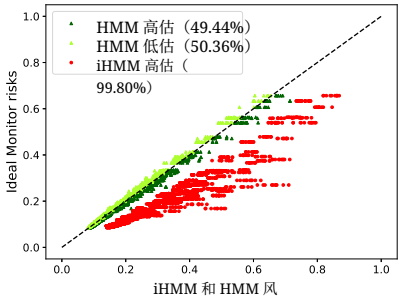



**图36：evadeV-5-3，安全置信度 = 0.1 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

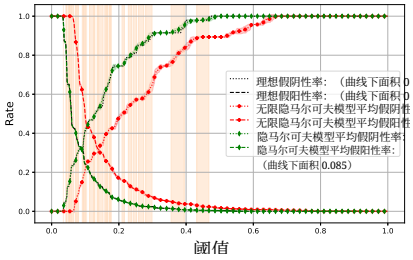



**图37：evadeV-6-3，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

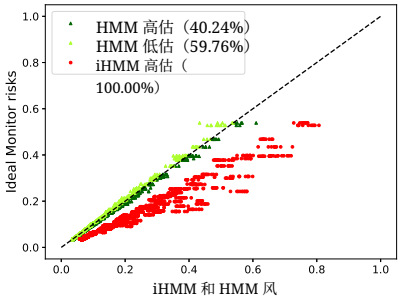



**图38：evadeV-6-3，SC = 0.01 - 以目标为条件的风险估计，有限隐马尔可夫模型与隐马尔可夫模型的比较**

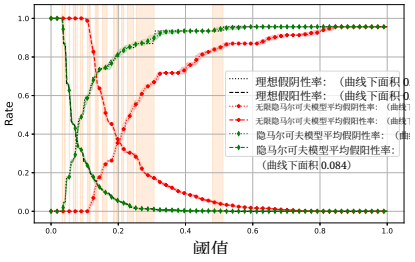



**图39：evadeV-6-3，SC = 0.1 - 有限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

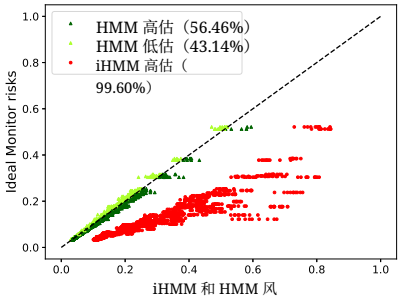



**图40：evadeV-6-3，SC = 0.1 - 以目标为条件的风险估计，有限隐马尔可夫模型与隐马尔可夫模型的比较**

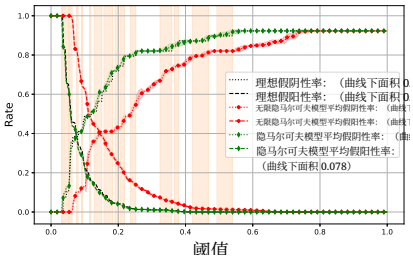



**图41：粗粒度 evadeV-6-3，SC = 0.01 - 有限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

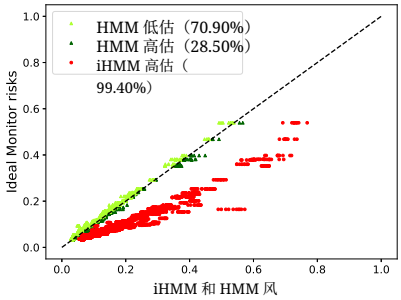



**图42：粗粒度 evadeV-6-3，SC = 0.01——以目标为条件的风险估计，比较无限隐马尔可夫模型与隐马尔可夫模型**

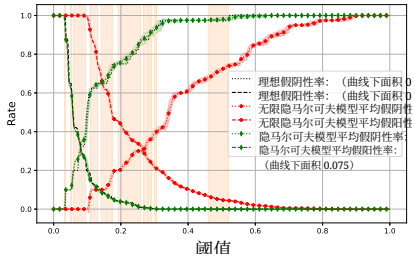



**图43：粗粒度 evadeV-6-3，SC = 0.1——无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

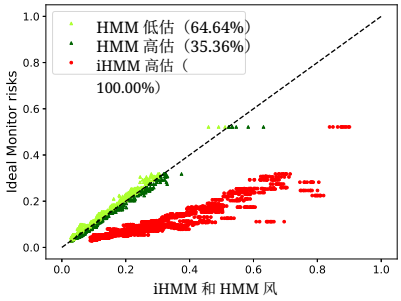



**图44：coarseevadeV-6-3，安全置信度 = 0.1 - 相对于目标的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

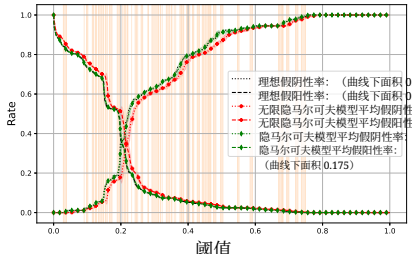



**图45：airportA-7-10-10，安全置信度 = 0.001 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

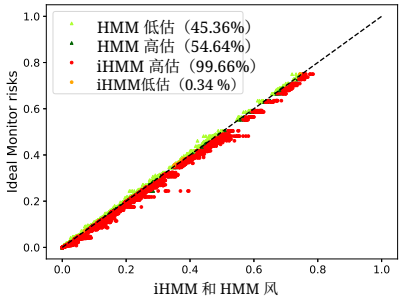



**图46：airportA-7-10-10，安全置信度 = 0.001 - 相对于目标的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

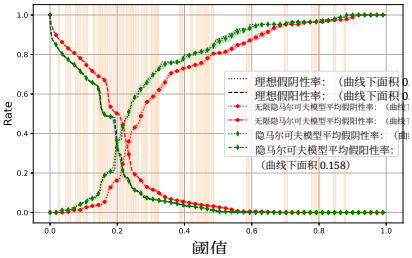



**图47：airportA-7-10-10，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

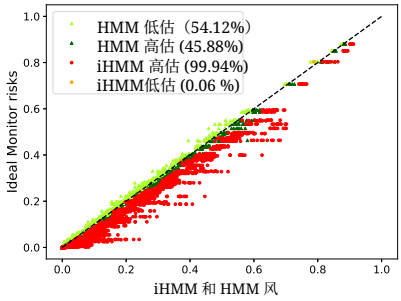



**图48：airportA-7-10-10，安全置信度 = 0.01 - 相对于目标的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较**

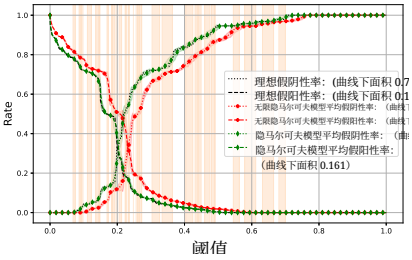



**图49：粗粒度 airportA-7-10-10，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

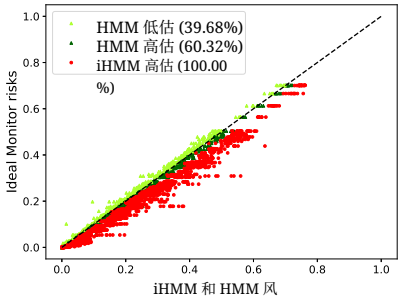



**图50：粗粒度 airportA-7-10-10，安全置信度 = 0.01 -以目标为条件的风险估计，比较无限隐马尔可夫模型与隐马尔可夫模型**

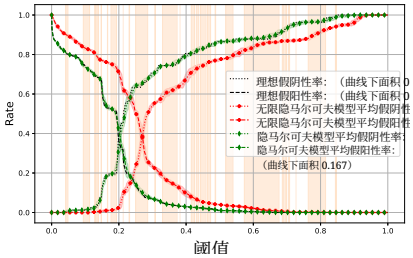



**图51：粗粒度 airportA-7-10-10，SC = 0.1——iHMM 与 HMM 的假阴性率和假阳性率对比**

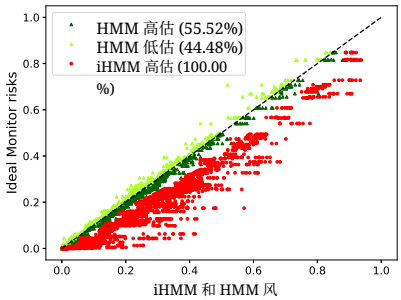



**图52：粗粒度 airportA-7-10-10，SC = 0.1——iHMM 与 HMM 的以目标为条件的风险估计对比**

## B.3 Unlikely-15 基准

我们进一步介绍第5.3节中引入的 Unlikely-15 基准的结构。

Unlikely-15 包含越来越难以采样的区段，每个区段都需要多个样本来学习其转移，以便我们能够准确预测该区段的风险。每个区段都有一条独特的轨迹通向其中，因此产生了许多难以预测其风险的轨迹。

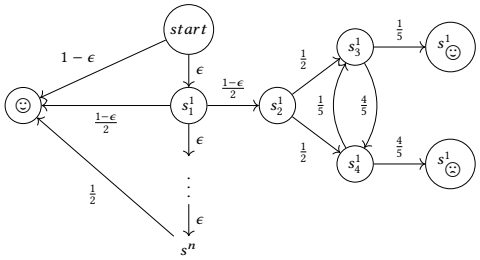



**图53：不太可能基准示意图。良好状态用 ☺ 表示，坏状态用 ☹ 表示。状态 $s_i^j$ 的观测为 $j$ 的值，以及 $i \geq 2$ 或 $i \in \{☺, ☹\}$。其他状态均完全可观测。我们的规范是永不处于坏状态，时域为 2。我们将示意图中的 $s^1$ 部分复制 $n$ 次；在实验中，我们选择了 $n = 15$。**

## B.4 精化与不精化

对于第5.4节未涵盖的每个基准测试，我们补充相应的分析：比较其与理想监视器的距离，并比较采用和不采用细化进行学习时，在不同阈值下的假阴性率和假阳性率。基准测试 airportA- 7-40-20 和粗略 airportB-7-40-20 的监视器实验评估见 C节。

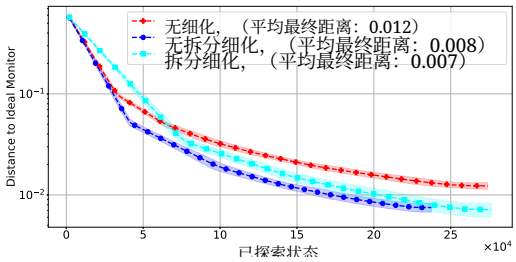



**图54：SnL-10x10，安全置信度 = 0.001 - 比较有细化和无细化时的学习效果，以与理想监视器的距离衡量**

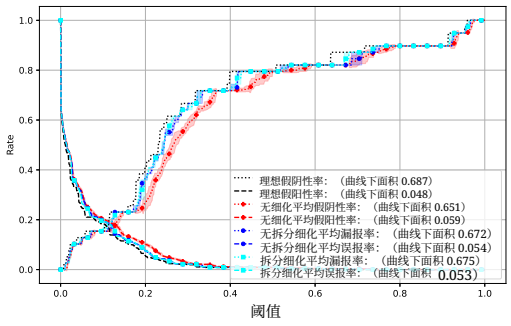



**图55：SnL-10x10，安全置信度 = 0.001 - 比较有细化和无细化时的学习效果，以假阴性率和假阳性率衡量**

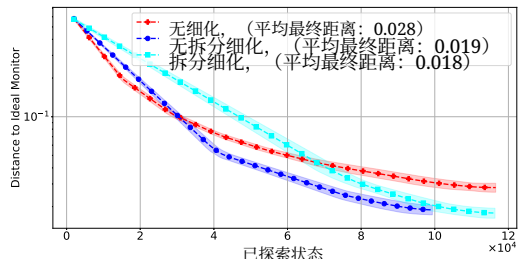



**图56：SnL-10x10，安全置信度 = 0.01——比较有无细化时的学习效果，衡量指标为与理想监视器的距离**

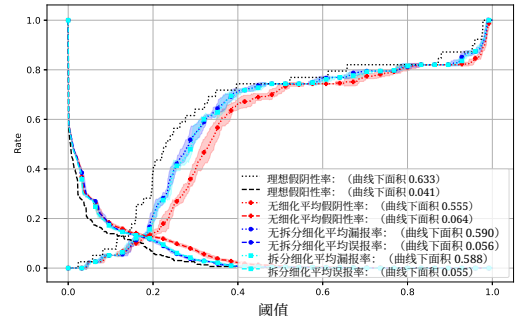



**图57：SnL-10x10，安全置信度 = 0.01——比较有无细化时的学习效果，衡量指标为假阴性率和假阳性率**

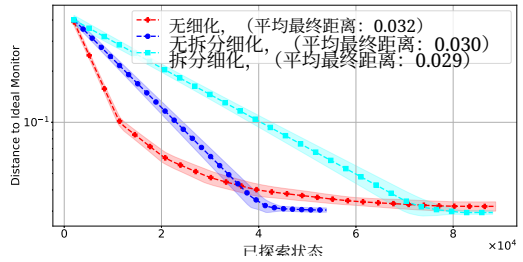



**图58：粗粒度 SnL-10x10，安全置信度 = 0.01，有无细化时的学习效果对比，衡量指标为与理想监视器的距离**

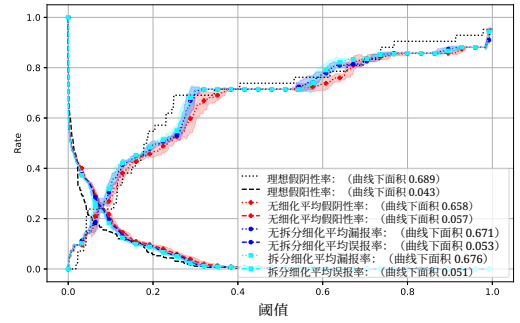



**图59：粗粒度 SnL-10x10，安全置信度 = 0.01，有无细化时的学习效果对比，衡量指标为假阴性率和假阳性率**

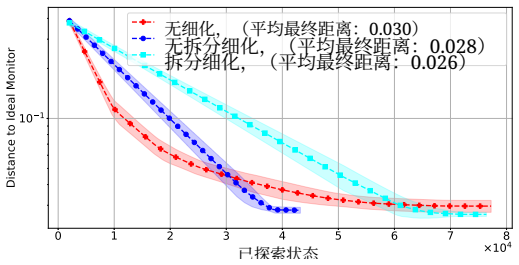



**图60：粗粒度 SnL-10x10，安全置信度 = 0.1——比较有无细化时的学习效果，衡量指标为与理想监视器的距离**

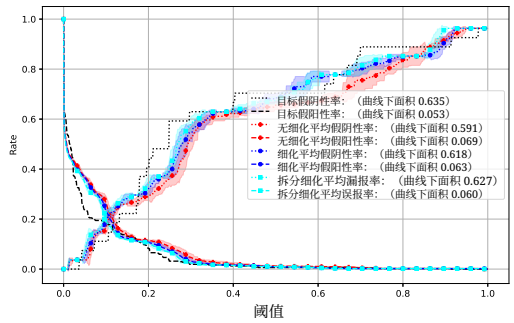



**图61：粗粒度 SnL-10x10，安全置信度 = 0.1——比较有无细化时的学习效果，以假阴性率和假阳性率为指标**

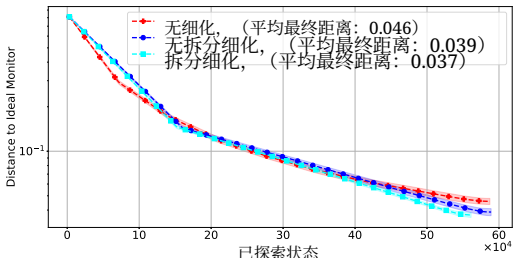



**图62：evadeV-5-3，安全置信度 = 0.01——比较有无细化时的学习效果，以与理想监视器的距离为指标**

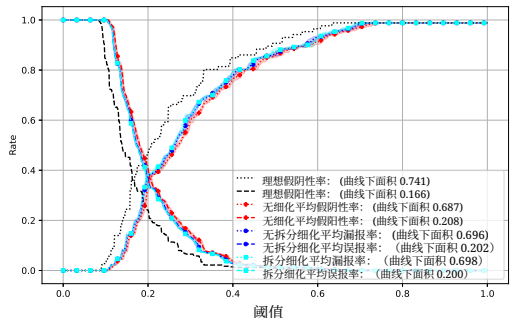



**图63：evadeV-5-3，安全置信度 = 0.01——比较有无细化时的学习结果，比较指标为与假阴性率和假阳性率的距离**

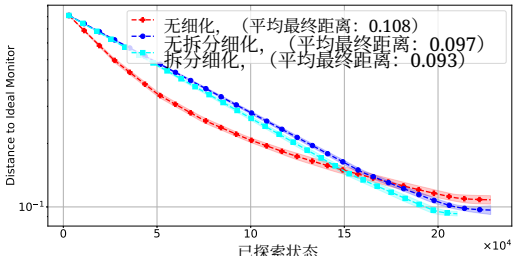



**图64：evadeV-5-3，安全置信度 = 0.1——比较有无细化时的学习结果，比较指标为与理想监视器的距离**

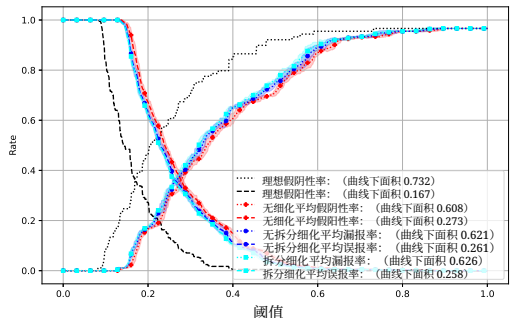



**图65：evadeV-5-3，安全置信度 = 0.1——比较有无细化时的学习结果，比较指标为与假阴性率和假阳性率的距离**

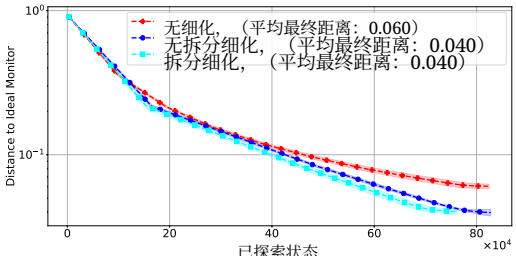



**图66：evadeV-6-3，安全置信度 = 0.01——比较有无细化时的学习结果，比较指标为与理想监视器的距离**

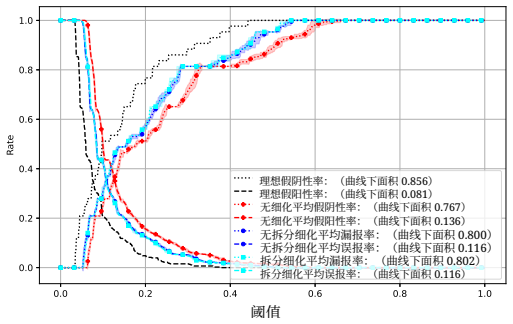



**图67：evadeV-6-3，安全置信度 = 0.01——比较有无细化时的学习结果，比较指标为与假阴性率和假阳性率的距离**

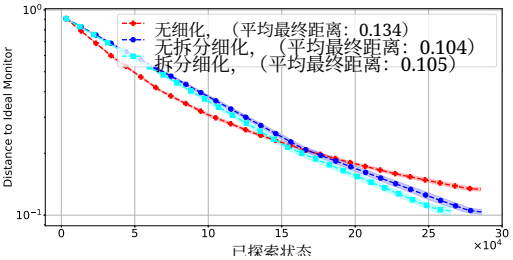



**图68：evadeV-6-3，安全置信度 = 0.1——比较有无细化时的学习结果，比较指标为与理想监视器的距离**

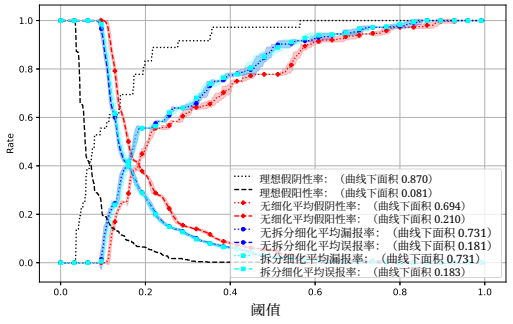



**图69：evadeV-6-3，安全置信度 = 0.1——从假阴性率和假阳性率的角度比较采用与不采用细化的学习**

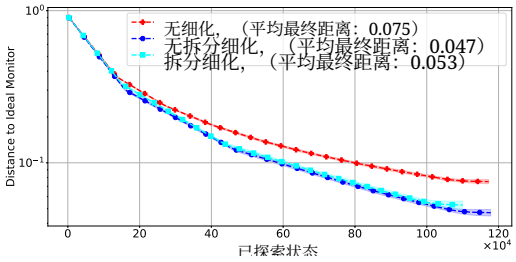



**图70：粗粒度coarseevadeV-6-3，安全置信度 = 0.01——从与理想监视器的距离方面比较采用和未采用细化的学习**

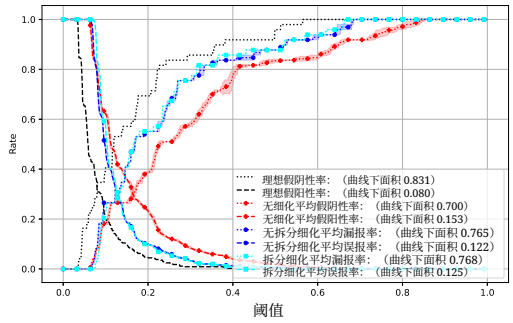



**图71：粗粒度coarseevadeV-6-3，安全置信度 = 0.01——从假阴性率和假阳性率方面比较采用和未采用细化的学习**

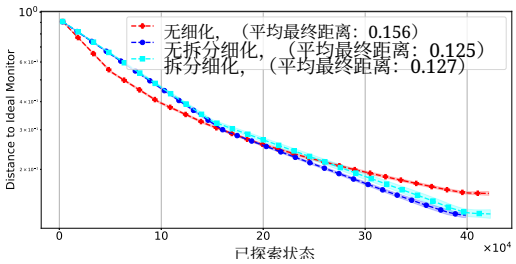



**图 72：粗粒度 evadeV-6-3，安全置信度 = 0.1——从与理想监视器的距离方面比较采用和未采用细化的学习**

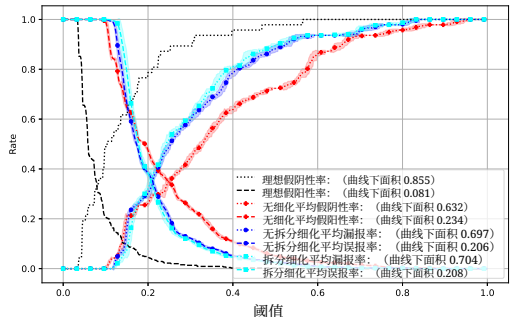



**图 73：粗粒度 evadeV-6-3，安全置信度 = 0.1——从假阴性率和假阳性率方面比较采用和未采用细化的学习**

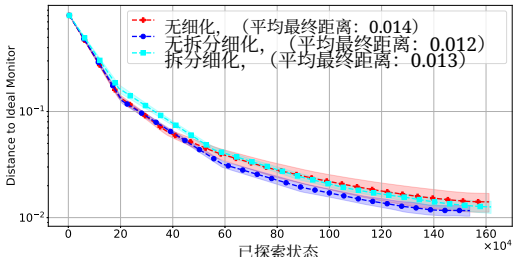



**图 74：airportA-7-10-10，安全置信度 = 0.001——从与理想监视器的距离方面比较采用和未采用细化的学习**

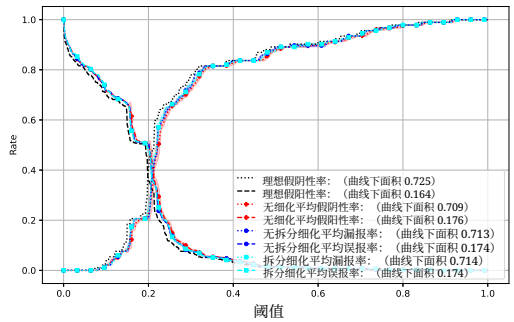



**图 75：airportA-7-10-10，安全置信度 = 0.001 - 比较有无细化的学习效果，依据假阴性率和假阳性率**

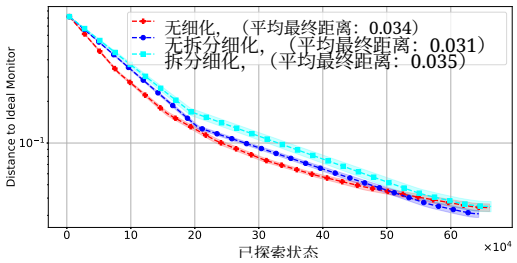



**图 76：airportA-7-10-10，安全置信度 = 0.01 - 比较有无细化的学习效果，依据与理想监视器的距离**

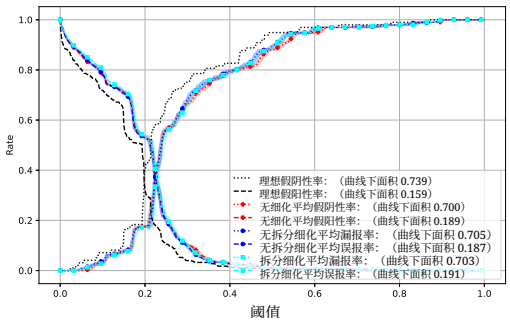



**图 77：airportA-7-10-10，安全置信度 = 0.01——从假阴性率和假阳性率方面比较有细化和无细化的学习**

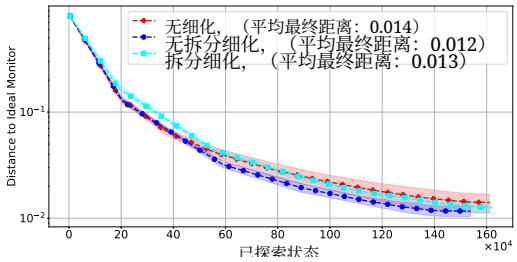



**图 78：粗粒度 airportA-7-10-10，安全置信度 = 0.01——从与理想监视器的距离方面比较有细化和无细化的学习**

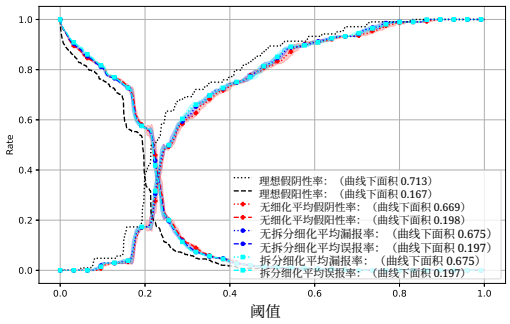



**图 79：粗粒度 airportA-7-10-10，SC = 0.01——比较有无细化时的学习效果（以假阴性率和假阳性率衡量）**

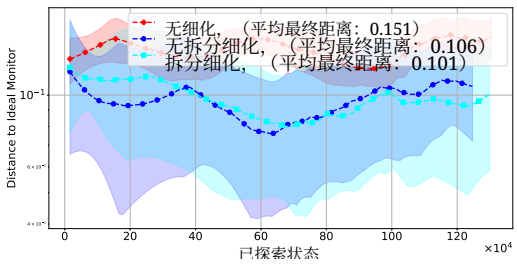



**图 80：粗粒度 airportA-7-10-10，SC = 0.1——比较有无细化时的学习效果（以与理想监视器的距离衡量）**

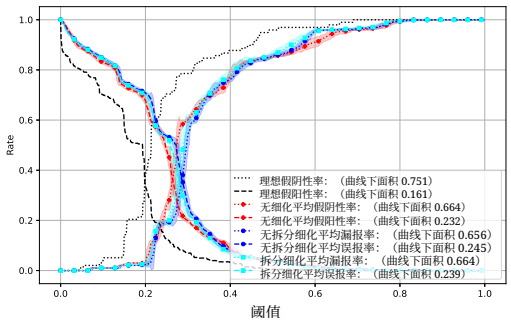



**图 81：粗粒度 airportA-7-10-10，SC = 0.1——比较有无细化时的学习效果（以假阴性率和假阳性率衡量）**

## C AIPORTA-7-40-20 和粗粒度 AIPORTB-7-40-20 基准测试的监视器实验评估

基准 aiportA-7-40-20 和粗粒度 aiportB-7-40-20 的实验评估将单独讨论。这是因为所考虑的方法均未能为这些基准学习到合理的监视器。

### C.1 基于模型与无模型监控

我们纳入了针对 aiportA-7-40-20 以及粗粒度 aiportB-7-40-20 基准测试的基于模型监控器与无模型监控器的实验比较结果。

图 84 由于内存问题，原因是基于 100 个测试样本。

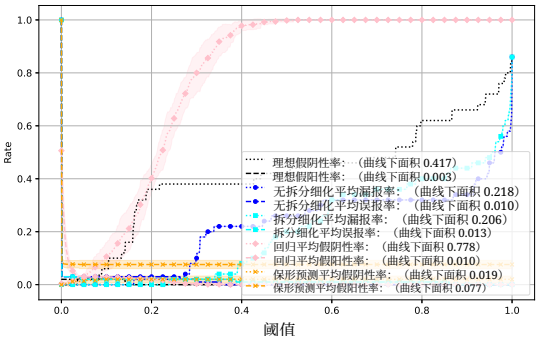



**图 82：airportA-7-40-20，安全置信度 =0.01 - 基于模型方法与无模型方法的假阴性率和假阳性率比较**

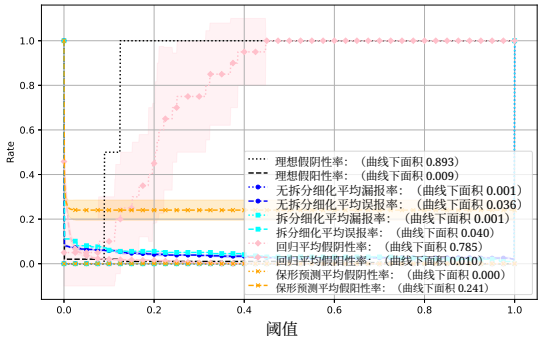



**图 83：airportA-7-40-20，安全置信度 = 0.1——基于模型与无模型方法的假阴性率和假阳性率比较**

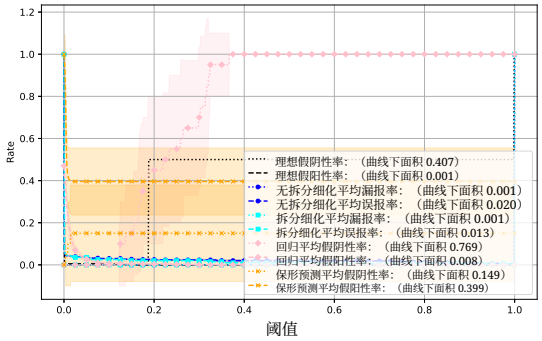



**图 84：粗粒度 airportB-7-40-20，安全置信度 = 0.01——基于模型与无模型方法的假阴性率和假阳性率比较**

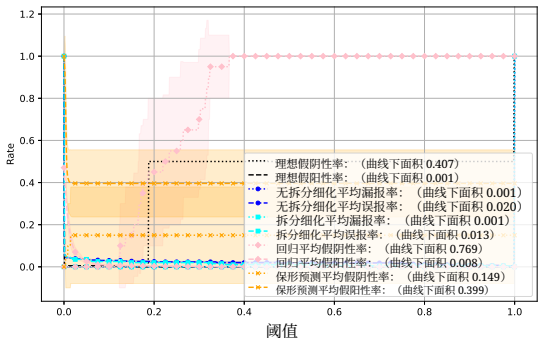



**图 85：粗粒度 airportB-7-40-20，安全置信度 = 0.1——基于模型与无模型方法的假阴性率和假阳性率比较**

### C.2 无限隐马尔可夫模型与隐马尔可夫模型监测

我们列出了 airportA-7-40-20 和粗略 airportB-7-40-20 的无限隐马尔可夫模型与隐马尔可夫模型监控结果比较。

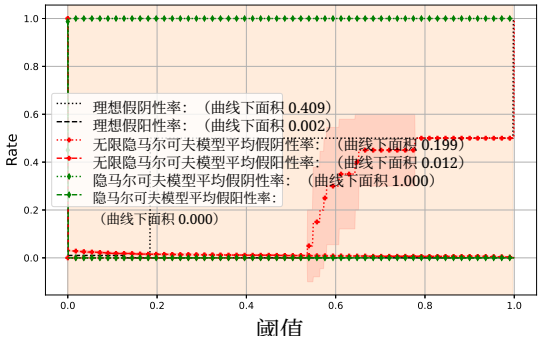



**图 86：airportA-7-40-20，SC =0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

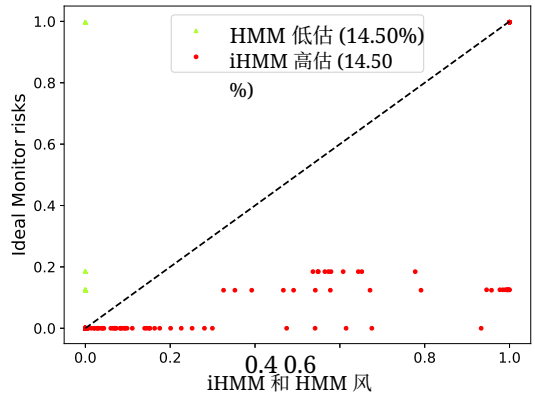



**图87：airportA-7-40-20，SC = 0.01 - 在目标条件下的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较0.0 0.2 0.4**

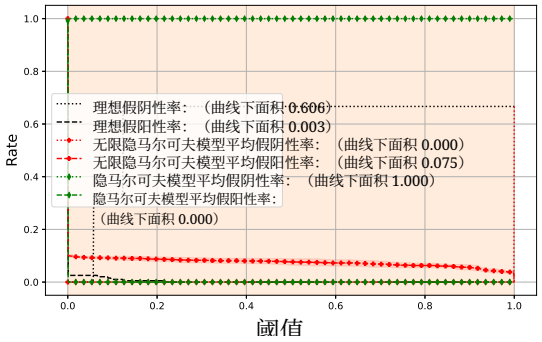



**图 88：airportA-7-40-20，SC = 0.1 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

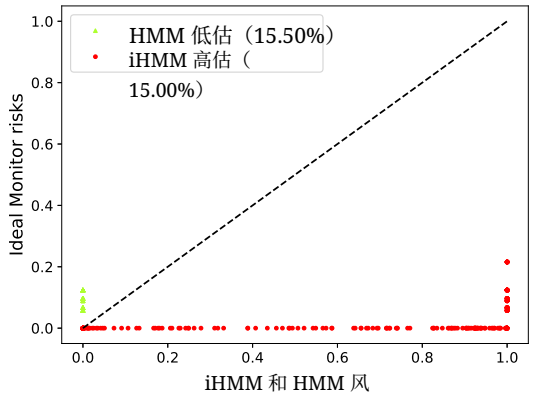



**图 89：airportA-7-40-20，安全置信度 = 0.1 - 以目标为条件的风险估计，比较无限隐马尔可夫模型与隐马尔可夫模型0.0 0.2 0.4**

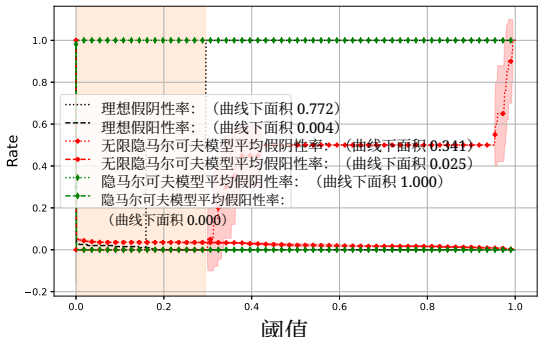



**图 90：粗略 airportB-7-40-20，安全置信度 = 0.01 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

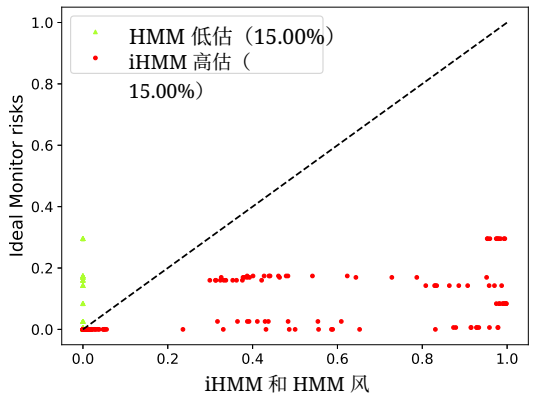



**图 91：粗略 airportB-7-40-20，安全置信度 = 0.01 - 以目标为条件的风险估计，比较无限隐马尔可夫模型与隐马尔可夫模型0.0 0.2 0.4**

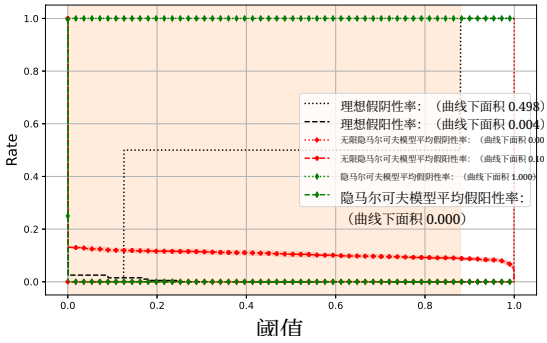



**图 92：粗粒度 airportB-7-40-20，安全置信度 = 0.1 - 无限隐马尔可夫模型与隐马尔可夫模型的假阴性率和假阳性率比较**

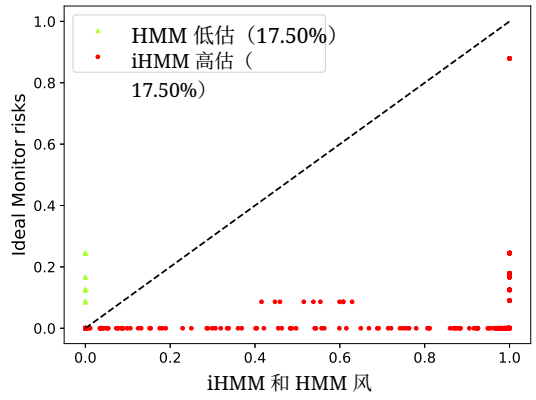



**图 93：粗粒度 airportB-7-40-20，安全置信度 = 0,1 - 以目标为条件的风险估计，无限隐马尔可夫模型与隐马尔可夫模型的比较0.0 0.2 0.4**

## C.3 无细化与细化学习

我们列出了 airportA-7-40-20 和粗略 airportB-7-40-20 的细化学习与无细化学习对比结果。

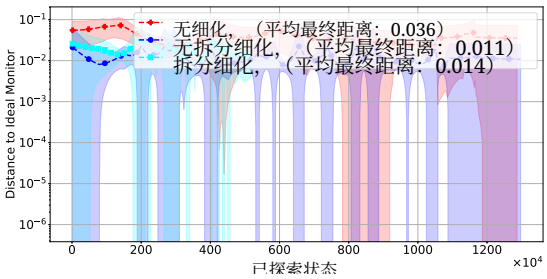



**图 94：airportA-7-40-20，安全置信度 =0.01 - 有细化与无细化的学习方式在与理想监视器的距离方面的比较**

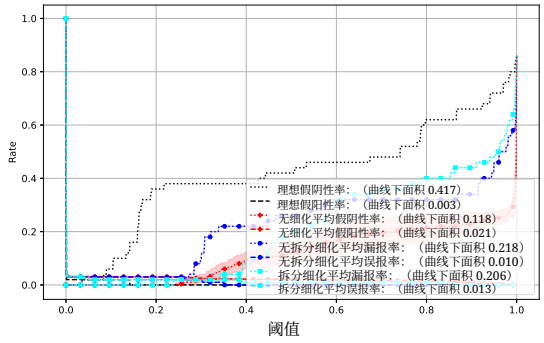



**图 95：airportA-7-40-20，SC = 0.01 - 比较有细化和无细化的学习在假阴性率和假阳性率方面的表现**

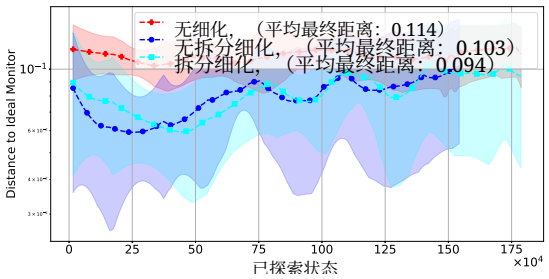



**图 96：airportA-7-40-20，SC = 0.1 - 比较有细化和无细化的学习与理想监视器的距离**

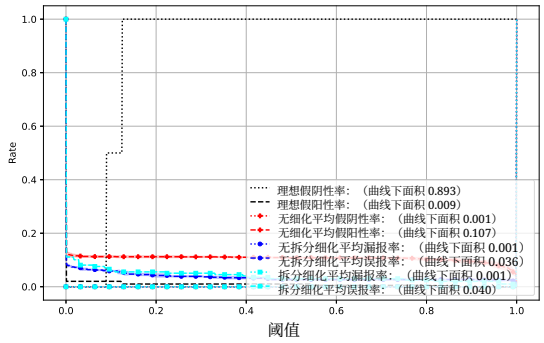



**图 97：airportA-7-40-20，SC = 0.1 - 比较有细化和无细化的学习在假阴性率和假阳性率方面的表现**

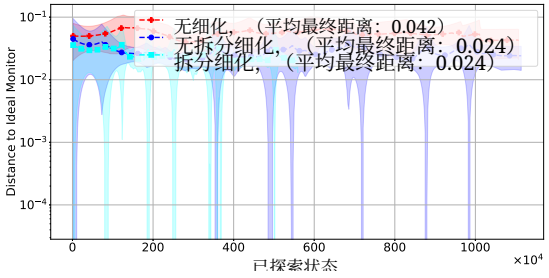



**图 98：粗略 airportB-7-40-20，SC = 0.01 - 比较有细化和无细化的学习与理想监视器的距离**

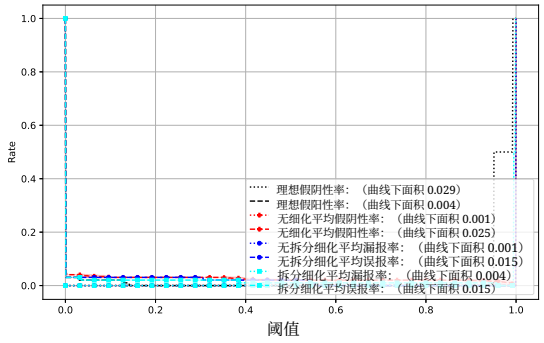



**图 99：粗略 airportB-7-40-20，SC = 0.01 - 比较有细化和无细化的学习在假阴性率和假阳性率方面的表现**

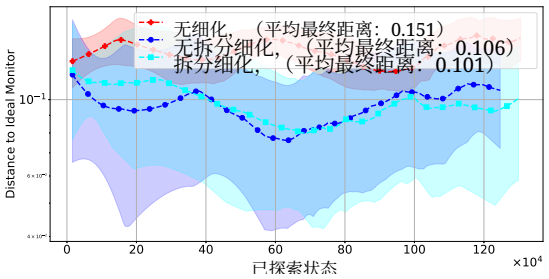



**图 100：粗略 airportB-7-40-20，SC = 0.1 - 比较有细化和无细化的学习与理想监视器的距离**

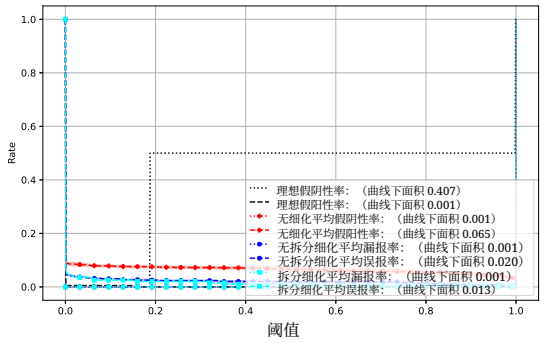



**图 101：粗略 airportB-7-40-20，SC = 0.1——比较细化与未细化情况下的学习结果，以假阴性率和假阳性率为指标**