研究提出随机系统容忍障碍函数方法

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/43011.html

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

研究提出随机系统容忍障碍函数方法
。近日，中国科学院软件研究所针对传统随机系统安全规约难以容纳短暂、可恢复的非安全访问问题，提出容忍安全与容忍到达—规避性质及相应的容忍障碍函数方法，为随机系统的定量安全验证提供了新的理论工具和算法支撑。

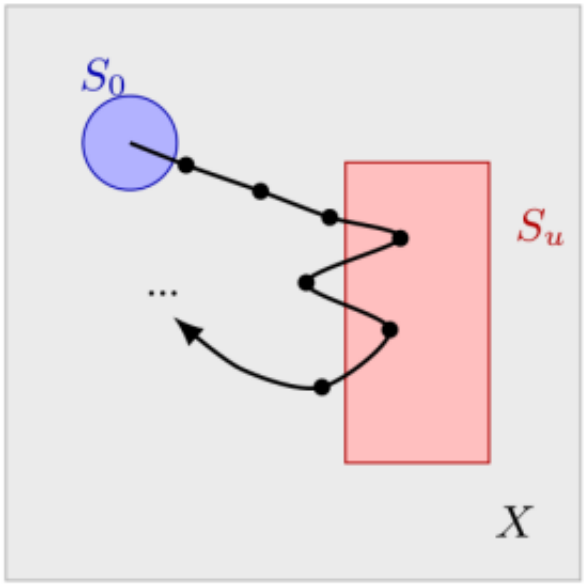
随机动态系统广泛应用于机器人、嵌入式系统和信息物理系统等，描述受噪声、误差等随机因素影响的过程。传统安全规约要求系统始终避开非安全区域，任何一次越界即判定失败。而这类短暂的非安全偏离并不一定表示任务失败，更合理的指标是控制累计越界次数或停留时间。现有随机障碍函数难以直接给出累计非安全访问超过指定阈值的概率上界，动态规划和概率模型检测等方法也难以扩展到非线性、连续状态随机系统。

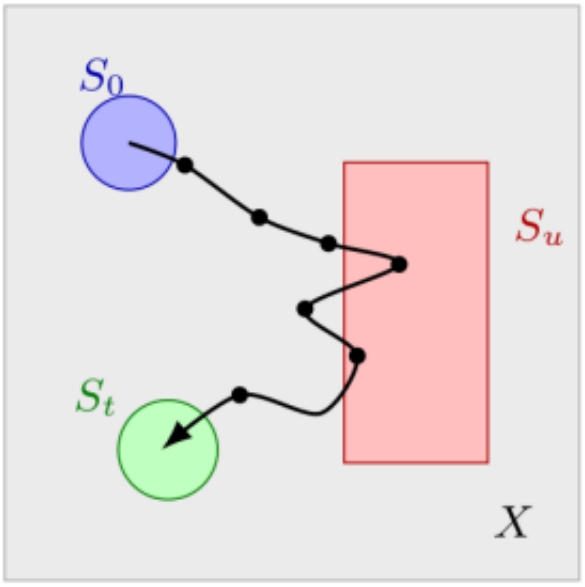
研究团队提出面向随机系统的容忍安全验证框架，通过累计非安全访问刻画系统的安全风险，区分离散、连续系统的统计指标，并定义容忍安全和容忍到达—规避性质，将安全规约由“零违规”拓展为累计非安全访问不超过给定阈值的概率性判断。团队进一步构建容忍障碍函数方法，将障碍函数与累计访问次数或占用时间结合构造超鞅，推导非安全访问超过给定阈值的概率上界。针对具有多项式动力学和半代数状态集合的随机系统，团队将容忍障碍函数的合成转化为平方和规划问题，并实现了原型工具。

在四类任务上，该方法在各基准中均成功合成障碍函数，并获得容忍安全性质的概率估计。实验表明，代表性案例计算得到的概率界与经验分布处于相近量级。可扩展性实验验证了6至16维耦合随机系统，在16维情形下四类任务的求解时间均不超过约137秒。与计数器增广方法相比，该方法直接在原状态空间中合成单个障碍函数，并可复用于不同非安全访问阈值，为含噪声嵌入式系统和信息物理系统的可靠性分析提供了新的形式化验证手段。

相关论文被第26届嵌入式软件国际会议（EMSOFT 2026）录用。

论文链接





容忍安全与容忍到达—规避性质

研究团队单位：软件研究所

更多 科学进展 请访问 https://www.iikx.com/news/progress/

本文版权归原作者所有，请勿用于商业用途，爱科学iikx.com转发