控制与决策
Control and Decision

针对无穷步不透明性的传感器主动攻击

丘瑞明, 肖存涛

引用本文:
丘瑞明, 肖存涛. 针对无穷步不透明性的传感器主动攻击[J]. 控制与决策, 2026, 41(1): 123-132.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2025.0278

针对无穷步不透明性的传感器主动攻击

丘瑞明，肖存涛†

(广东工业大学 数学与统计学院，广州 510520)

摘　要: 不透明性在信息安全领域取得了许多成功的应用, 针对离散事件系统不透明性的攻击问题引起了国内外学者的广泛关注. 在监督控制背景下, 研究针对离散事件系统无穷步不透明性的传感器主动攻击可行性问题. 根据能否对系统中秘密状态全面攻击, 分别给出强可攻击与弱可攻击的形式化定义. 针对增强无穷步不透明性的闭环受控系统, 提出一种新的全攻击信息流结构模型来记录攻击者与监督器的前后状态估计, 并以此判断主动攻击者能否通过篡改监督器的观察, 在监督器未检测到其存在的前提下完成对系统无穷步不透明性的攻击, 并以此模型分别推导出针对无穷步不透明性强可攻击和弱可攻击的充分必要条件. 结论及实例均表明所提出的传感器主动攻击策略可以有效实现对系统安全性的主动攻击.

关键词: 离散事件系统；信息物理系统；监督控制；主动攻击；无穷步不透明性；基于位置服务

中图分类号: TP273　　**文献标志码:** A

DOI: 10.13195/j.kzyjc.2025.0278

引用格式: 丘瑞明, 肖存涛. 针对无穷步不透明性的传感器主动攻击 [J]. 控制与决策, 2026, 41(1): 123-132.

Active sensor attacks against infinite-step opacity

QIU Rui-ming，*XIAO Cun-tao*†

(School of Mathematics and Statistics，Guangdong University of Technology，Guangzhou 510520，China)

Abstract: The problem of opacity has been successfully applied in the field of information security for cyber-physical systems, and recently the attack problem of opacity in discrete event systems has attracted extensive attention of scholars. This paper studies the feasibility of active attacks against infinite-step opacity in the context of supervisory control of discrete event systems. According to whether the attacker can fully attack the secret states in the system, the formal concepts of strong attackability and weak attackability are respectively given. For the closed-loop controlled system with enhanced infinite-step opacity, a new all attack structure model is proposed to record the pre-state and post-state estimations of the attacker and the supervisor, and determines whether the active attacker can complete the attack against infinite-step opacity of the system by tampering with the supervisor's observations without being detected by the supervisor. Based on this model, the necessary and sufficient conditions for strong attackability and weak attackability of infinite-step opacity are respectively deduced. The conclusions and examples demonstrate that the proposed sensor active attack strategy can effectively achieve active attacks against system security.

Keywords: discrete event systems； cyber-physical systems； supervisory control； active attacks； infinite-step opacity；location based services

0 引　言

近年来, 随着计算机、网络通信以及传感器技术的发展, 信息物理系统已成为推动各行业智能化转型的关键力量. 信息物理系统具有随时间推移和事件转移异步发展的特点, 因此可被视为一个状态及空间均离散的系统, 这种情况下系统可被建模为一个离散事件系统 (DES). 离散事件系统具有事件驱动特点, 通过离散事件的激活触发状态转移, 并记录事件序列和系统状态的变化, 因此离散事件系统是一类适合由自动机建模和形式化方法刻画的动态系统[1], 进而实现对系统的运行逻辑进行分析和研究. 离散事件系统模型广泛应用于文件管理系统、终端数据交换、自动导引车路径规划等领域[2-4].

在信息物理系统中, 传感器和执行器可以通过网络通信实时交换信息, 一方面这使得控制架构更加灵活和智能, 但另一方面, 这也给系统的信息安全与隐私性带来挑战. 一旦网络通信成为网络攻击的弱点, 系统可能面临隐私和机密信息的泄露, 偏离正

收稿日期: 2025-03-16；**录用日期:** 2025-08-07.
基金项目: 国家自然科学基金面上项目 (12271112).
†通信作者. E-mail: xiaocuntao@gdut.edu.cn.

常或预期的行为, 从而导致高昂的运营成本. 出于上述原因, 国内外学者探索通过离散事件系统建模, 研究构造系统攻击的方法以及检测攻击的发生, 并提供针对此类威胁的弹性技术, 其目的是预防攻击者窃取隐私和机密信息, 确保在正常操作期间和攻击发生后都不会违反系统规范.

对于不满足信息保护要求的系统, 可以通过监督控制方法避免系统执行不希望的操作. 此时, 攻击者可以通过向目标系统注入虚假信息以破坏系统与监督器的正常交互, 进行主动攻击. 文献 [5] 研究了合成传感器隐形欺骗攻击的问题, 作者假设入侵者完全知道系统和监督器的模型, 传感器通道容易受到攻击. 入侵者的意图是在入侵者与监督者的交互中操纵传感器数据, 诱导系统到达不安全状态. 文献 [6] 在入侵者可有限次地插入监督器观察的情形下, 提出了一种判断是否可使系统进入不安全状态的全插入-删除模型; 文献 [7] 将系统的安全行为扩展到初始秘密状态保护上, 提出了验证所有可能攻击方式可行性的全攻击模型; 文献 [8-9] 考虑了在 Petri 网模型下的传感器攻击问题. 除传感器攻击外, 也可假设入侵者能够修改系统发出的部分控制命令以进行执行器攻击[10-11]. 此外, 亦有学者研究了容忍攻击的安全策略问题[12-13]. 文献 [14] 对信息物理系统中攻击策略的设计、攻击检测以及攻击鲁棒性监控器设计的研究现状进行了总结分析.

在离散事件系统中, 不透明性已成为系统信息安全的重要性质, 在一个离散事件系统中, 部分信息属于秘密信息, 不能够被外部非法获取. 例如, 系统中部分状态属于秘密状态, 系统运行者不希望他人能确定系统进入过秘密状态. 2005 年, Bryans 等[15] 提出了基于 Petri 网的初始状态不透明性和当前状态不透明性概念; 文献 [16] 提出了无穷步不透明性和k步不透明性的形式化定义, 通过记录k步观察内状态估计得到了k步不透明性的验证算法; 文献 [17] 通过构造初始状态估计验证器, 用以验证无穷步不透明性; 文献 [18] 提出了基于事件串的不透明性概念, 包括强不透明性和弱不透明性; 文献 [19] 通过构造双向观测器, 分别对前后观察进行状态估计, 提出了一种无穷步与k步不透明性的验证算法, 降低了复杂度; 文献 [20] 基于鲁棒监控方法研究了强制隐蔽性的监控综合问题.

相比于文献 [6] 和文献 [7], 本文研究针对无穷步不透明性的传感器主动攻击问题. 无穷步不透明性要求攻击者在系统任意时刻都无法通过有限步观察确定系统曾进入秘密状态, 相比于当前状态不透明性和初始状态不透明性, 涉及更复杂的动态行为和状态估计; 本文所提出的全攻击模型记录攻击者与监督器的前后状态估计, 并以此作为攻击隐蔽性的判断条件.

本文提出了针对无穷步不透明性的强可攻击与弱可攻击形式化概念以及验证可攻击性的算法. 通过构造全攻击模型, 推导出针对无穷步不透明性强可攻击和弱可攻击的充要条件. 若确定系统对无穷步不透明性可攻击, 模型则给出具体的攻击方式.

1 预备知识

离散事件系统是一种状态和空间离散、事件驱动的动态模型, 通常用自动机$G=(Q,\Sigma,\delta,x_0)$进行建模. 其中: Q为状态集, Σ为事件集, $\delta: Q\times\Sigma\to Q$为状态转移函数, $x_0\in Q$为初始状态, Σ^*表示包括空串ϵ在内的所有有限长字符串的集合. 系统在状态 q 下的可触发事件集记为$\Delta_G(q)$, 系统生成的语言定义为$L(G)=\{s\in\Sigma^*:\delta(x_0,s)!\}$, 其中符号“!”表示有定义. 对于事件串$s=\sigma_1\sigma_2\ldots\sigma_n$, 记$s_j=\sigma_1\sigma_2\ldots\sigma_j$. 对于一个二元组$(a,b)$, 记$\varphi(a,b)=a$, $\psi(a,b)=b$.

事件集Σ通常被划分为可观事件集Σ_o和不可观事件集$\Sigma_{\rm uo}$, 以及可控事件集Σ_c和不可控事件集$\Sigma_{\rm uc}$, 满足$\Sigma=\Sigma_o\bigcup\Sigma_{\rm uo}=\Sigma_c\bigcup\Sigma_{\rm uc}$. 自然映射 $P:\Sigma^*\to\Sigma_o^*$定义为

$$P(\epsilon)=\epsilon,\ P(se)=\begin{cases}P(s),\ e\in\Sigma_{\rm uo};\\ P(s)e,\ e\in\Sigma_o.\end{cases}\tag{1}$$

其逆映射$P^{-1}:\Sigma_o^*\to\Sigma^*$定义为$P^{-1}(t)=\{s\in\Sigma^*:P(s)=t\}$.

离散事件系统的监督控制理论是指监督器S通过控制事件发生使闭环受控系统S/G满足规范要求. 监督器控制行为记为$S:P(L(G))\to\Gamma$, 其中$\Gamma=\{\gamma\subseteq\Sigma,\Sigma_{\rm uc}\subseteq\gamma\}$, 监督器控制行为可建模为确定自动机 $H=(Z,\xi,z_0,\Sigma)$, 从而给定$s\in L(G)$, 有$S(P(s))=\Delta_H(\xi(z_0,s))$. 受控系统$S/G$可通过$G\times H$得到, 其中$\times$是标准复合乘积运算.

给定状态集$X\subseteq Q$和控制模式$\gamma\subseteq\Sigma$, 以及可观事件$\sigma\in\Sigma_o$, 在控制模式γ下, 状态集X的不可观到达定义为

$$\begin{aligned}&{\rm UR}_\gamma(X)=\\&\{\delta(q,s)\in Q:q\in X,s\in(\Sigma_{\rm uo}\bigcap\gamma)^*\}.\end{aligned}\tag{2}$$

状态集X在σ发生后的可观到达定义为

$${\rm NX}_\sigma(X)=\{\delta(q,\sigma)\in Q:q\in X\}.\tag{3}$$

控制模式γ下状态集X的下一可观事件集定义为

$$\Omega_\gamma(X)=\{\sigma\in\Sigma_o:\exists q\in X,\ \exists\omega\in(\Sigma_{\rm uo}\bigcap\gamma)^*,\delta(q,\omega\sigma)!\}. \quad (4)$$

通常系统G中部分状态可能包含秘密信息, 秘密状态记为$X_s\subseteq Q$, 若攻击者能够通过外部观察确定系统曾进入过秘密状态, 则可能导致隐私泄露. 如果系统进入秘密状态后, 攻击者无法通过外部观察确定系统曾进入秘密状态, 则称系统具有无穷步不透明性.

定义 1[17] (无穷步不透明性)　给定系统G, 可观事件集Σ_o, 秘密状态集X_s, 称系统G是无穷步不透明的, 如果下列条件成立:

$$(\forall st\in L(G):\delta(x_0,s)\in X_s)(\exists s't'\in L(G))[\delta(x_0,s')\notin X_s\bigwedge P(s')=P(s)\bigwedge P(t')=P(t)]. \quad (5)$$

对于$st\in P(L(G))$, 观察到s时的延迟状态估计定义为

$$\hat{X}_{|s|}(st)=\{x\in Q:\exists t_1t_2\in L(G),x=\delta(x_0,t_1)\bigwedge P(t_1)=s\bigwedge P(t_2)=t\}. \quad (6)$$

引理 1[19]　系统 G 是无穷步不透明的, 当且仅当

$$\forall st\in P(L(G)):\hat{X}_{|s|}(st)\not\subseteq X_s. \quad (7)$$

2　针对无穷步不透明性的主动攻击

对于标准的无穷步不透明性问题, 攻击者行为可看作是被动的, 仅能通过观察窃取秘密信息, 不对系统本身的运行进行干扰. 然而, 某些攻击者可能具有更强的能力, 能主动篡改传感器的观察, 误导监督器决策, 这种攻击方式被称为传感器主动攻击.

假设攻击者可以观察到系统中所有的可观测事件, 并且能够对部分可观测事件进行篡改或删除, 将这些易受攻击的事件记为 $\Sigma_v\subseteq\Sigma_o$. 为了区分攻击者和监督器的观察, 定义$\hat{\Sigma}_o=\{\hat{\sigma}:\sigma\in\Sigma_o\}\bigcup\{\hat{\epsilon}\}$为攻击者篡改观察后监督器观察到的事件, 监督器无法区分σ和$\hat{\sigma}$.

定义 2[7] (攻击者行动空间映射)　给定易受攻击事件集Σ_v以及可观事件集Σ_o, 定义$V:\Sigma_o\to\hat{\Sigma}_o$为攻击者行动空间映射, 有

$$V(\sigma)=\begin{cases}\{\hat{\sigma}_a:\sigma_a\in\Sigma_v\}\bigcup\{\hat{\epsilon}\},\ \sigma\in\Sigma_v;\\ \{\hat{\sigma}\},\ \sigma\notin\Sigma_v.\end{cases} \quad (8)$$

也就是说, 对于每个易受攻击事件$\sigma\in\Sigma_v$, 攻击者可以将其替换为一个新的事件$\hat{\sigma}_a$(此时监督器观察到的是事件σ_a), 或者删除这一事件, 即监督器没有观察到任何事件的发生. 攻击者不能对非易受攻击事件进行篡改.

若攻击者任意篡改系统的观察$s\in P(L(G))$, 当篡改后的观察$s'\notin P(L(S/G))$时, 攻击者将被检测到, 此时监督器可能会终止系统运行以避免进一步攻击. 因此在攻击者实现攻击目标前, 应确保篡改后的观察在 $P(L(S/G))$内, 以保证攻击的隐蔽性. 对于事件串$s\in L(G)$, 攻击者将其篡改为一个新的事件串s', 因此监督者产生控制决策$S(P(s'))$, 随后系统生成新的事件$\sigma\in S(P(s'))$, 当σ是可观事件时, 攻击者将其篡改为$\hat{\sigma}_a\in V(\sigma)$.

定义 3 (攻击方案)　给定系统G、可观事件集Σ_o、易受攻击事件集$\Sigma_v\subseteq\Sigma_o$、监督器$S$, 定义非确定攻击方案$A:L(G)\to 2^{(\hat{\Sigma}_o\cup\Sigma_{\rm uo})^*}$, 有:

1) $A(\epsilon)=(S(\epsilon)\bigcap\Sigma_o)^*$.

2) 对于任意的$s\in L(G)$, 若已知$A(s)=t\in L(S/G)$, $\sigma\in S(P(t))$, 则

$$A(s\sigma)=\begin{cases}t\hat{\sigma}',\ \hat{\sigma}'\in V(\sigma),\ \sigma\in\Sigma_o;\\ t\sigma',\ \sigma'\in S(P(t))\bigcap\Sigma_{\rm uo},\ \sigma\in\Sigma_{\rm uo}.\end{cases}$$

定义 4 (攻击者无穷步延迟状态估计)　给定系统G、可观事件集Σ_o、易受攻击事件集Σ_v、监督器S, 对于$st\in P(L(G))$, 定义攻击者无穷步延迟状态估计为$\hat{X}^A_{|t|}(st)$, 有

$$\hat{X}^A_{|t|}(st)=\{x\in Q:\exists t_1t_2\in L(G):A(t_1t_2)!,\ x=\delta(x_0,t_1)\bigwedge P(t_1)=s\bigwedge P(t_2)=t\}. \quad (9)$$

下面给出针对无穷步不透明性的弱可攻击与强可攻击的形式化定义.

定义 5 (针对无穷步不透明的弱可攻击性)　给定系统G、可观事件集Σ_o、易受攻击事件集Σ_v、监督器S、秘密状态X_s, 称攻击器A是对无穷步不透明性弱可攻击的, 如果

$$(\exists st\in L(G))[P(A(st))\bigcap P(L(S/G))\neq\varnothing\bigwedge\hat{X}^A_{|P(s)|}(P(st))\subseteq X_s]. \quad (10)$$

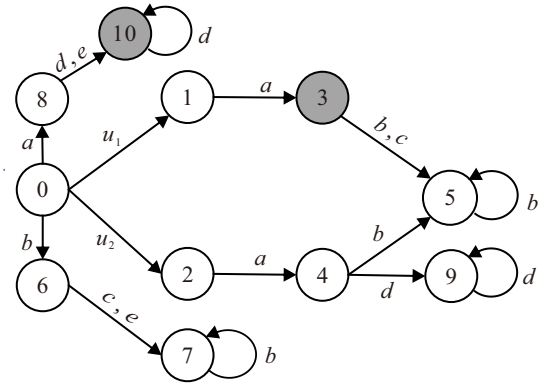
定义 6 (针对无穷步不透明的强可攻击性)　给定系统G、可观事件集Σ_o、易受攻击事件集Σ_v、监督器S、秘密状态X_s, 称攻击器A是对无穷步不透明性强可攻击的, 如果

$$(\forall x\in X_s)(\exists st\in L(G):x=\delta(x_0,s))[P(A(st))\bigcap P(L(S/G))\neq\varnothing\bigwedge\hat{X}^A_{|P(s)|}(P(st))\subseteq X_s]. \quad (11)$$

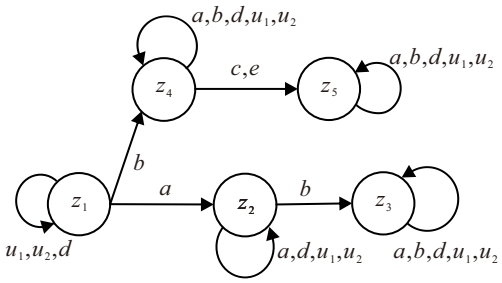
直观上, 弱可攻击性要求能够找到系统中至少一个事件串, 每次篡改观察后保证攻击者隐蔽, 确保进程不会终止, 并在最后一次观察后破坏系统的无穷步不透明性. 强可攻击指对于任何一个秘密状态, 攻击者都能够找到一种攻击方式, 在隐身的前提下确定系统曾进入过秘密状态. 即弱可攻击指攻击者能找到至少一个事件序列实现攻击, 而强可攻击则

要求对系统中的任意秘密状态都能找到有效攻击方案. 弱可攻击性与强可攻击性统称为可攻击性.

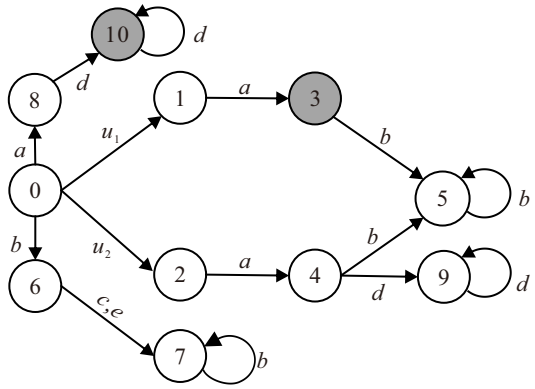
例 1 如图 1(a) 所示, 给定系统$G=(Q,\Sigma,\delta,x_0)$. 其中: 可观事件集$\Sigma_o=\{a,b,c,d,e\}$, 不可观事件集$\Sigma_{\rm uo}=\{u_1,u_2\}$, 可控事件集$\Sigma_c=\{c,e\}$, 易受攻击事件集$\Sigma_v=\{a,b\}$, 秘密状态集$X_s=\{3,10\}$.



(a) 离散事件系统G



(b) 监督器H



(c) 受控系统S/G

图1 离散事件系统监督控制图

当取$st=u_1ac\in L(G)$, $s=u_1a$, $t=c$, 此时$\hat{X}_{|a|}(ac)=\{3\}\subseteq X_s$; 当取$st=ae\in L(G), s=ae$, $t=\epsilon$时, $\hat{X}_{|ae|}(ae)=\{10\}\subseteq X_s$. 因此, 系统$G$不满足无穷步不透明性.

监督器H如图 1(b) 所示, 受控系统S/G如图 1(c) 所示, 任意经过秘密状态 3 的语言为u_1ab^*, 有$P^{-1}(P(u_1ab^*))=\{u_1ab^*,u_2ab^*\}$, u_2ab^*不经过秘密状态; 任意经过秘密状态 10 的语言为ad^*, 有$P^{-1}(P(ad^*))=\{u_2ad^*,ad^*\}$, 其中$u_2ad^*$不经过秘密状态. 因此, 受控系统$S/G$满足无穷步不透明性.

现验证针对无穷步不透明性的强可攻击性和弱可攻击性. 取$a\in S(\epsilon)$作为攻击者观察到的第 1 个事件, 将其替换为$\hat{b}\in V(a)$, 此时监督器观察到b, 并作出控制决策$S(b)$, 取$c\in S(b)$, 此时有$bc\in P(L(S/G))$, $\hat{X}^A_{|a|}(ac)=\{3\}$; 若发生事件$e\in S(b)$, 此时有$be\in P(L(S/G))$, $\hat{X}^A_{|ae|}(ae)=\{10\}$. 因此, 对于任意一种秘密状态都存在攻击方式确定系统曾进入秘密状态, 即系统是针对无穷步不透明性强可攻击的.

3 针对无穷步不透明性的全攻击模型

step 1: 构造反转自动机. 通过文献 [19] 的方法对系统G、监督器H、受控系统S/G分别构造反转自动机G_R、H_R、$(S/G)_R$. 其中: $G_R=(Q,\Sigma,\delta_R,Q)$, 其初始状态定义为原系统状态集全体$Q$; 转移函数$\delta_R: Q\times\Sigma\to 2^Q$, 有$y=\delta(x,\sigma)$, 当且仅当$x\in\delta_R(y,\sigma)$, 即将原系统对应转移反转. 对于$s=\sigma_1\sigma_2\dots\sigma_n$, 定义$s_R=\sigma_n\sigma_{n-1}\dots\sigma_1$.

step 2: 构造受控系统和反转自动机的观察器. 对于受控系统S/G, 其观察器定义为

$$\mathrm{obs}(S/G)=(Q_{(S/G)\mathrm{obs}},\Sigma_o,f_{\mathrm{obs}(S/G)},q_{\mathrm{obs}(S/G),0}). \tag{12}$$

其中: $Q_{(S/G)\mathrm{obs}}\subseteq 2^Q$, $q_{\mathrm{obs}(S/G),0}=\mathrm{UR}(x_0)$. 对于任意的$q\in 2^Q$, $\sigma\in\Sigma_o$, 有$f_{\mathrm{obs}(S/G)}(q,\sigma)=\mathrm{UR}(\mathrm{NX}_\sigma(q))$.

监督者在观察到$s\in\hat{\Sigma}_o^*$时的状态估计定义为

$$\hat{X}^S_{S/G}(s)=\{x\in Q:\exists t\in L(S/G),\ P(t)=s\bigwedge\delta(x_0,t)=x\}. \tag{13}$$

易知, $\hat{X}^S_{S/G}(s)=f_{\mathrm{obs}(S/G)}(q_{\mathrm{obs}(S/G),0},s)$.

对于攻击者, 观察到$s\in\Sigma_o^*$时的状态估计定义为

$$\hat{X}^A_G(s)=\{x\in Q:\exists t\in L(G):A(t)!\bigwedge x=\delta(x_0,t)\bigwedge P(t)=s\}. \tag{14}$$

$\hat{X}^A_G(s)$ 可以通过以下方式递归得到:

1) $\hat{X}^A_G(\epsilon)=\mathrm{UR}_{s(\epsilon)}(x_0)$;

2) 对于任意$s\in\Sigma_o^*$, $\sigma\in\Sigma_o$, 取$\hat{t}\in A(P^{-1}(s))$, $\hat{\sigma}_a\in V(\sigma)$, 有

$$\hat{X}^A_G(s\sigma)=\mathrm{UR}_{S(P(\hat{t})\hat{\sigma}_a)}(\mathrm{NX}_\sigma(\hat{X}^A_G(s))).$$

step 2 的目的是得到攻击者和监督者在观察到可观事件序列后的状态估计.

step 3: 构造全攻击模型. 全攻击的模型定义如下.

定义 7 (全攻击模型) 给定系统$G=(Q,\Sigma,\delta,x_0)$、

可观事件集$\Sigma_o \subseteq \Sigma$、可控事件集$\Sigma_c$、易受攻击事件$\Sigma_v \subseteq \Sigma_o$以及监督器$H=(Z,\Sigma,\xi,z_0)$, 则全攻击模型$M$可定义为一个确定性有限状态自动机

$$M=(Y,\Sigma_M,f,y_0). \tag{15}$$

$\Sigma_M=\Sigma_M^a\bigcup\Sigma_M^s$是事件集合, $\Sigma_M^a=(\Sigma_o,\epsilon)\bigcup(\epsilon,\Sigma_o)$, $\Sigma_M^s=(\hat{\Sigma}_o,\epsilon)\bigcup(\epsilon,\hat{\Sigma}_o)$.

$Y=Y_e\bigcup Y_a$ 包含如下两种非交的状态集:

1) $Y_e\subseteq Q_{(S/G)\text{obs}}\times Q_{(S/G)\text{obs},R}\times 2^Q\times 2^Q\times Z\bigcup z_{\text{att}}\times 2^{Z\cup z_{\text{att}}}$表示环境状态集合, 即监督者和攻击者的双向状态估计和监督者在当前情形下可行的控制模式, 其中z_{att}表示当前情况下攻击者的攻击被暴露, 定义 $\Delta_H(z_{\text{att}})=\varnothing$.

2) $Y_a\subseteq Q_{(S/G)\text{obs}}\times Q_{(S/G)\text{obs},R}\times 2^Q\times 2^Q\times Z\bigcup z_{\text{att}}\times 2^{Z\cup z_{\text{att}}}\times\Sigma_M^a$表示可攻击的状态集合.

$y_0=(q_{(S/G)\text{obs},0}\times Q\times \text{UR}_{S(\epsilon)}(x_0)\times Q\times z_0\times Z)$ 是攻击模型M 的初始状态.

$f:Y\times\Sigma_M\to Y$包含如下 4 种类型的转移函数:

1) $f_{e1}:Y_e\times(\Sigma_o,\varepsilon)\to Y_a$ 是前向状态估计下, 从环境状态到攻击状态的转移函数: 对于任意的$y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 有$\Delta_M(y)=\Omega_{\Delta_H(z)}(q_1)$, 对于任意的$\sigma\in\Delta_M(y)$, 有

$$f_{e1}(y,(\sigma,\varepsilon))=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z,(\sigma,\varepsilon)).$$

2) $f_{e2}:Y_e\times(\varepsilon,\Sigma_o)\to Y_a$是后向状态估计下, 从环境状态到攻击状态的转移函数: 对于任意的$y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 有 $\Delta_M(y)=\Omega_{\Delta_{H_R}(Z)}(q_2)$, 对于任意$\sigma\in\Delta_M(y)$, 有

$$f_{e2}(y,(\varepsilon,\sigma))=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z,(\varepsilon,\sigma)).$$

3) $f_{a1}:Y_a\times(\hat{\Sigma}_o,\varepsilon)\to Y_e$是前向状态估计下, 从攻击状态到环境状态的转移函数: 对于任意的$y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z,(\sigma,\varepsilon))\in Y_a$, 有 $\Delta_M(y)=V(\sigma)$, 对于任意的 $\hat{\sigma}\in\Delta_M(y)$, 有

$$f_{a1}(y,(\hat{\sigma},\varepsilon))=(f_{(S/G)_{\text{obs}}}(\hat{q}_1,\hat{\sigma}),\hat{q}_2,\ \text{UR}_{\Delta_H(z')}(\text{NX}_\sigma(q_1)),q_2,z',Z).$$

其中

$$z'=\begin{cases}\xi(z,\hat{\sigma}),\ f_{(S/G)_{\text{obs}}}(\hat{q}_1,\hat{\sigma})\neq\varnothing\bigwedge\xi(z,\hat{\sigma})!;\\ z_{\text{att}},\ \text{otherwise.}\end{cases} \tag{16}$$

4) $f_{a2}:Y_a\times(\varepsilon,\hat{\Sigma}_o)\to Y$是后向状态估计下, 从攻击状态到环境状态的转移函数: 对于任意的$y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z,(\varepsilon,\sigma))\in Y_a$, 有 $\Delta_M(y)=V(\sigma)$, 对于任意的 $\hat{\sigma}\in\Delta_M(y)$, 有

$$f_{a2}(y,(\varepsilon,\hat{\sigma}))=(\hat{q}_1,f_{(S/G)_{\text{obs},R}}(\hat{q}_2,\hat{\sigma}),q_1,\ \text{UR}_{\Delta_{H_R}(Z')}(\text{NX}_\sigma^{G_R}(q_2)),z,Z').$$

其中

$$Z'=\begin{cases}\xi_R(Z,\hat{\sigma}),\ f_{(S/G)_{\text{obs},R}}(\hat{q}_2,\hat{\sigma})\neq\varnothing\bigwedge\xi_R(Z,\hat{\sigma})!;\\ z_{\text{att}},\ \text{otherwise.}\end{cases} \tag{17}$$

攻击者的攻击流程如图 2 所示, 系统首先运行第 1 个事件σ_1, $\sigma_1\in S(\epsilon)\bigcap\Delta_H(1)$. 若$\sigma_1$是可观事件, 攻击者则根据是否是易受攻击事件作出攻击决策, 使监督者观察到的序列为$\hat{\sigma}_1$. 若监督者的观测序列属于$P(L(S/G))$, 则监督者根据观察到的序列作出决策$S(P(\hat{\sigma}_1))$, 从而系统的下一个运行事件$\sigma_2\in S(P(\hat{\sigma}_1))\bigcap\Delta_H(2)$, 攻击者再继续作篡改操作. 依此类推, 假设系统到第i次时进入秘密状态, 但此时攻击者还不能确定系统是否进入到秘密状态, 则系统可继续运行. 若系统运行到第n次时, 攻击者通过外部观察破坏受控系统无穷步不透明性, 则攻击成功.

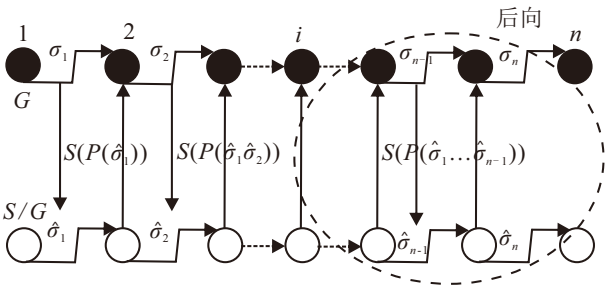


图2　攻击流程示意图

全攻击模型运行过程如图 3 所示. 模型首先确定第 1 个事件σ_1(若不可观, 则不发生转移), 经过转移到达对应的攻击状态, 随后攻击者确定攻击策略, 使监督者观察到的事件为$\hat{\sigma}_1$; 经转移, 到第 2 个环境状态y_2, 若攻击未被发现 (未出现z_{att}), 则经i次前向转移可以到y_i, 此时根据全攻击模型的状态能得到攻击者和监督器的前向状态估计; 随后转变方向, 先发生实际最后发生的事件σ_n和篡改的$\hat{\sigma}_n$, 到最后得到的y_n, 就有攻击者和监督器的后向状态估计.

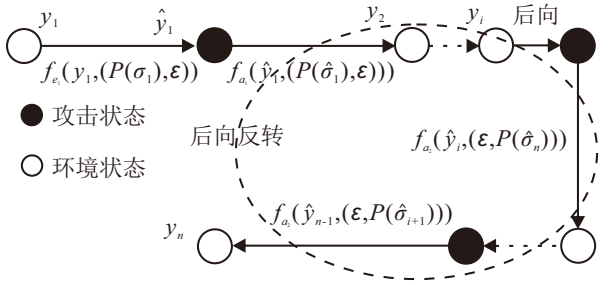


图3　全攻击模型运行示意图

4 无穷步不透明性可攻击的充要条件

为更好地给出针对无穷步不透明性可攻击的充分必要条件, 下面给出几个形式化标记. 对于构建的全攻击模型$M=(Y,\Sigma_M,f,y_0)$, $y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 记 $\mu(y)=(\hat{q}_1,\hat{q}_2),\eta(y)=(q_1,q_2),\lambda(y)=(z,Z)$.

定义函数M_a: $L(M)\to(\Sigma_M^a)^*$, 如果$\sigma\in\Sigma_M^a$, 则$M_a(\sigma)=\sigma$; 如果$\sigma\in\Sigma_M^s$, 则$M_a(\sigma)=\varepsilon$. 定义函数M_s: $L(M)\to(\Sigma_M^s)^*$, 如果$\sigma\in\Sigma_M^s$, 则$M_s(\sigma)=\sigma$; 如果$\sigma\in\Sigma_M^a$, 则$M_s(\sigma)=\varepsilon$. 对于$s\in L(M)$, 定义a_1、a_2分别为$M_a(s)$第 1 分量和第 2 分量上的字符串, 即攻击模型发生 s 时, 攻击者前后观察到的事件串; 定义s_1、s_2分别为$M_s(s)$第 1 分量和第 2 分量上的字符串, 即攻击模型发生s时, 监督者前后观察到的事件串. 若有事件串$t=(a,\varepsilon)(\hat{b},\varepsilon)(\varepsilon,b)(\varepsilon,\hat{a})$, 则有$a_1=a,a_2=b,s_1=\hat{b},s_2=\hat{a}$.

引理 2 对于任意的$s\in L(M)$, 令$y=f(y_0,s)=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 则有

$$q_1=\hat{X}_G^A(a_1),\ q_2=\hat{X}_{G_R}^A(a_2); \tag{18}$$

$$\hat{q}_1=\hat{X}_{S/G}^S(s_1),\ \hat{q}_2=\hat{X}_{(S/G)_R}^S(s_2). \tag{19}$$

证明 只证明$q_1=\hat{X}_G^A(a_1)$, 其余情况可用类似方法得出.

令 $a_1=\sigma_1\sigma_2\dots\sigma_n\in\Sigma_o^*$, $s_1=\hat{\sigma}_1\hat{\sigma}_2\dots\hat{\sigma}_n\in\hat{\Sigma}_o^*$, 有 $A(a_1)=s_1$, 记 $\varphi(\eta(f(y_0,\sigma_1\hat{\sigma}_1\dots\sigma_i\hat{\sigma}_i)))=q_i$, $\varphi(\lambda(f(y_0,\sigma_1\hat{\sigma}_1\dots\sigma_i\hat{\sigma}_i)))=z_i$. 当 $i=0$时, 有$\hat{X}_G^A(\varepsilon)=\mathrm{UR}_{S(\varepsilon)}(x_0)=q_0$, 此时条件成立.

假设对于$0\leqslant i\leqslant n-1$, 命题成立, 则对于$j=i+1$, 若$s_1^j\in P(L(S/G))$, 则有

$$\hat{X}_G^A(a_1^j)=\mathrm{UR}_{S(s_1^j)}(\mathrm{NX}_{\sigma_j}(q_i))=\mathrm{UR}_{\Delta_H(z_j)}(\mathrm{NX}_{\sigma_j}(q_i))=q_j.$$

当$s_1^j\notin P(L(S/G))$时, 必有 $z_j=z_{\mathrm{att}}$, 因此有$j=n$, 以及

$$\hat{X}_G^A(a_1^n)=\mathrm{UR}_{\Delta_H(z_n)}(\mathrm{NX}_{\sigma_n}(q_i))=\mathrm{UR}_{\Delta_H(z_{\mathrm{att}})}(\mathrm{NX}_{\sigma_n}(q_i))=\mathrm{NX}_{\sigma_n}(q_i)=q_n.$$

综上, 对于任意的$0\leqslant i\leqslant n$, 命题均成立, 证明成立. □

引理 2 说明, 对于全攻击模型的环境状态, $\hat{q}_1$、$\hat{q}_2$为监督器的前后状态估计, q_1、q_2为攻击者的前后状态估计.

引理 3 给定攻击模型$M=(Y,\Sigma_M,f,y_0)$, 对于任意的$s\in L(M)$, 令$y=f(y_0,s)=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 有

$$q_1\bigcap q_2\neq\varnothing\Rightarrow(\exists t\in L(G))[a_1(a_2)_R=P(t)], \tag{20}$$

$$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing\Rightarrow(\exists t'\in L(S/G))[s_1(s_2)_R=P(t')]. \tag{21}$$

证明 只证明式 (20), 式 (21) 可用类似方法得出.

由引理 2, $q_1=\hat{X}_G^A(a_1),q_2=\hat{X}_{G_R}^A(a_2)$, 令$x\in q_1\bigcap q_2$是$Q$中的状态, 由此可以得到

$$[\exists t_1\in L(G):A(t_1)!\bigwedge x=\delta(x_0,t_1)\bigwedge P(t_1)=a_1][\exists x'\in Q,\exists t_2\in L(G_R,x'):A_{G_R}(t_2)!\bigwedge x\in\delta_{G_R}(x',t_2)\bigwedge P(t_2)=a_2].$$

由$x\in\delta_{G_R}(x',t_2)$可知$\delta(x,(t_2)_R)=x'$, 由$P(t_2)=a_2$可知 $P((a_2)_R)=(t_2)_R$. 因此, 存在 $t=t_1(t_2)_R\in L(G)$, 有$P(t)=P(t_1)P((t_2)_R)=a_1(a_2)_R$, 证明成立. □

引理 4 对于任意的$s\in L(M)$, 令$y=f(y_0,s)=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 若$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$, 则 $\exists t_1t_2\in L(G)$, $P(t_1)=a_1,P(t_2)=(a_2)_R$, 满足

$$A(t_1t_2)!\Leftrightarrow A(t_1)!,A_{G_R}((t_2)_R)!. \tag{22}$$

证明 先证必要性, 显然有$A(t_1)!$, 因为$A(t_1t_2)!$, 因此$P(A_{G_R}((t_2)_R))=s_2$, 即$\exists s'\in L(G_R)$, $P(s')=s_2,A_{G_R}((t_2)_R)=s'$.

再证充分性, 由$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$和引理 3 可知, $(\exists t'\in L(S/G))[s_1(s_2)_R=P(t')]$, 即$A(t_1t_2)!$, 证明成立. □

引理 5 对于任意的$s\in L(M)$, 令$y=f(y_0,s)=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e$, 若 $\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$, 则有

$$\hat{X}_{|a_1|}^A(a_1(a_2)_R)=q_1\bigcap q_2, \tag{23}$$

$$\hat{X}_{|s_1|}^S(s_1(s_2)_R)=\hat{q}_1\bigcap\hat{q}_2. \tag{24}$$

证明 只证明式 (23), 式 (24) 可用类似方法得出. 由引理 4 可推得

$$\begin{aligned}&x\in\hat{X}_{|a_1|}^A(a_1(a_2)_R)\Leftrightarrow\\&\exists t_1t_2\in L(G):A(t_1t_2)!,x=\delta(x_0,t_1)\bigwedge\\&P(t_1)=a_1\bigwedge P(t_2)=(a_2)_R\Leftrightarrow\\&[\exists t_1\in L(G):A(t_1)!\bigwedge x=\delta(x_0,t_1)\bigwedge P(t_1)=a_1]\bigwedge\\&[\exists x'\in Q,\exists t_2\in L(G,x'):A_{G_R}((t_2)_R)!\bigwedge\\&x'=\delta(x,t_2)\bigwedge P(t_2)=(a_2)_R]\Leftrightarrow\\&[\exists t_1\in L(G):A(t_1)!\bigwedge x=\delta(x_0,t_1)\bigwedge P(t_1)=a_1]\bigwedge\\&[\exists x'\in Q,\exists(t_2)_R\in L(G_R,x'):A_{G_R}((t_2)_R)!\bigwedge\\&x\in\delta_{G_R}(x',(t_2)_R)\bigwedge P((t_2)_R)=a_2]\Leftrightarrow\\&x\in\hat{X}_G^A(a_1)\bigcap\hat{X}_{G_R}^A(a_2).\end{aligned}$$

由引理 2 得到$\hat{X}_{|a_1|}^A(a_1(a_2)_R)=q_1\bigcap q_2$, 证明成立. □

引理 4 和引理 5 说明, 若$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$, 则存在满

足$P(t_1)=a_1, P(t_2)=(a_2)_R$的语言$t_1t_2\in L(G)$是可攻击的语言, 此时$q_1\bigcap q_2$是攻击者的延迟状态估计.

定理 1　针对无穷步不透明的弱可攻击性充要条件. 给定系统G、可观事件集Σ_o、监督器S、秘密状态X_s、易受攻击事件Σ_v, 令$M=(Y,\Sigma_M,f,y_0)$是全攻击模型, 则系统是无穷步不透明性弱可攻击的, 当且仅当

$$(\exists y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e)[q_1\bigcap q_2\subsetneq X_s\bigwedge\hat{q}_1\bigcap\hat{q}_2\neq\varnothing]. \tag{25}$$

证明　先证必要性, 若系统是无穷步不透明性弱可攻击的, 则存在事件串$st\in L(G)$, 有$\hat{X}^A_{|s|}(P(st))\subseteq X_s$, 则由引理 5 可知

$$\hat{X}^A_{|s|}(P(st))=\hat{X}^A_G(P(s))\bigcap\hat{X}^A_{G_R}(P(t_R)),$$

同时, 由$st\in L(G)$和$A(st)$!可知, 在全攻击模型中, 存在$u\in L(M)$, 使得下列条件成立: $f(y_0,u)=y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_e, a_1=P(s), a_2=P(t_R)$.

由式 (23) 可知, $q_1\bigcap q_2\subsetneq X_s$.

对于$P(A(st))\bigcap P(L(S/G))\neq\varnothing$, 可知$P(A(s))P(A_{G_R}(t_R))_R\in P(L(S/G))$, 令到达$y$的语言为$s$, 有$P(A(s))=s_1, P(A_{G_R}(t_R))=s_2$, 因此有$s_1(s_2)_R\in P(L(S/G))$, 即$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$.

再证充分性, 由$q_1\bigcap q_2\subsetneq X_s$和引理 3 可知$(\exists t_1t_2\in L(G))[a_1=P(t_1), (a_2)_R=P(t_2)]$, 则有$\hat{X}^A_{|P(t_1)|}(P(t_1t_2))=\hat{X}^A_G(a_1)\bigcap\hat{X}^A_{G_R}(a_2)=q_1\bigcap q_2$, 因此, $\hat{X}^A_{|P(t_1)|}(P(t_1t_2))\subseteq X_s$.

由$\hat{q}_1\bigcap\hat{q}_2\neq\varnothing$和引理 3 可知$P(A(st))\bigcap P(L(S/G))\neq\varnothing$, 证明成立. □

定理 2　针对无穷步不透明的强可攻击性充要条件. 给定系统G、可观事件集Σ_o、监督器S、秘密状态X_s、易受攻击事件Σ_v, 令$M=(Y,\Sigma_M,f,y_0)$是全攻击模型, 则系统是无穷步不透明性强可攻击的, 当且仅当

$$\bigcup_{y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y_s}(q_1\bigcap q_2)=X_s, \tag{26}$$

其中$Y_s=\{y=(\hat{q}_1,\hat{q}_2,q_1,q_2,z,Z)\in Y: q_1\bigcap q_2\subsetneq X_s\bigwedge\hat{q}_1\bigcap\hat{q}_2\neq\varnothing\}$.

证明　对于$y\in Y_s$, 由定理 1 可知, 对于任意的$x\in q_1\bigcap q_2\subseteq X_s$, 当且仅当能找到一种攻击方式, 使秘密状态$x$暴露. $\bigcup\limits_{y\in Y_s}(q_1\bigcap q_2)=X_s$时, 当且仅当对任意的$x\in X_s$, 能找到一种攻击方式, 使秘密状态$x$暴露, 证明成立. □

定理 1 表明, 若全攻击模型存在一个状态, 其攻击者前后状态估计交集真包含于秘密状态, 而监督者前后状态估计交集非空, 则攻击者可找到一条攻击路径破坏系统无穷步不透明性. 从引理 3 可以看出, 若到达这一状态的语言为s, 则将系统观察$a_1(a_2)_R$篡改为$s_1(s_2)_R$是一个破坏系统安全性的攻击方案. 定理 2 说明, 若对每个秘密状态, 都能在全攻击模型中找到能够破坏系统安全的路径, 则系统是无穷步不透明性强可攻击的.

例 2　对例 1 中的系统构造全攻击模型, 全攻击模型如图 4 所示. 对于状态$Y_2=\{\hat{X}_3,\hat{X}_3,X_2,X_3,z_4,Z_2\}$, 有$X_2\bigcap X_3=\{3\}\subseteq X_s$且$\hat{X}_3\bigcap\hat{X}_3=\{6\}\neq\varnothing$; 对于状态$Y_3=\{\hat{X}_5,\hat{X}_4,X_5,X_4,z_5,Z_1\}$, 有$X_5\bigcap X_4=\{10\}\subseteq X_s$且$\hat{X}_5\bigcap\hat{X}_4=\{7\}\neq\varnothing$. 因此有$(X_2\bigcap X_3)\bigcup(X_5\bigcap X_4)=X_s$, 由定理 2 可知系统是无穷步不透明性强可攻击的.

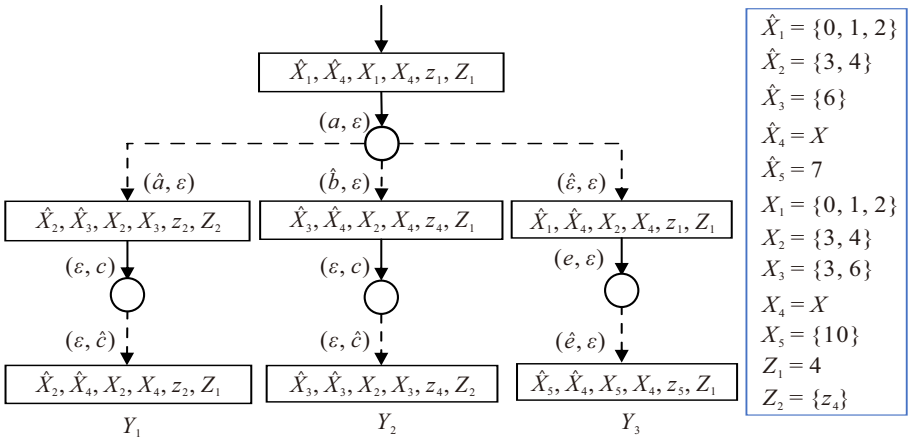


图4　全攻击模型M(部分)

注意到对于状态$Y_1=\{\hat{X}_2,\hat{X}_3,X_2,X_3,z_2,Z_2\}$, 尽管$X_2\bigcap X_3=\{3\}\subseteq X_s$, 但$\hat{X}_2\bigcap\hat{X}_3=\varnothing$, 因此不篡改系统观察$ac$的方式不能破坏受控系统的无穷步不透明性, 实际上$ac\notin P(L(S/G))$.

全攻击模型的监督器状态估计由攻击者根据系统运行时的决策而定, 因此模型状态数量最大值为

$2^{2^{|Q|+|Z|}} \times |Z| \times (|\Sigma_v|+1)^2$, 而算法复杂度为 $O(2^{2^{|Q|+|Z|}} \times |Z| \times |\Sigma_v|^2 \times 4|\Sigma_o|)$. 全攻击模型状态空间可能的个数的确增长迅速, 但在针对无穷步不透明性这一问题上, 由于破坏系统无穷步不透明性的事件串其前向估计必含秘密状态, 所以只需关注攻击者前向估计含秘密状态的情形, 再以此对可能含秘密状态的估计做后向估计. 因此, 模型状态数量最大值将有所下降至$(2^{|Q|}-2^{|Q-X_s|}) \times 2^{|Q|+|Z|} \times |Z| \times (|\Sigma_v|+1)^2$. 若秘密状态占比较低, 状态空间可能的个数将下降较多.

5 实例分析

本节通过基于位置服务 (LBS)[21] 保护用户的位置隐私来说明对无穷步不透明性传感器主动攻击的应用.

随着移动性传感器和线上交易体系的普及, 越来越多的应用开始要求用户提供实时位置信息, 以寻求为用户提供个性化和及时的信息, 这种服务被称为基于位置服务 (LBS). LBS 在为用户提供更加优质服务的同时, 也加大了隐私暴露的危害性, 攻击者可以通过这些信息了解到用户的家庭住址、工作地点, 甚至是身体状况. 为保护用户的位置隐私, 目前 LBS 最常使用的技术是基于位置匿名服务的位置匿名器, 位置匿名器会将用户的准确位置信息转化成一个包含多个虚假位置信息并且比准确位置范围更大的位置区域, 再提供给 LBS 服务器, 其工作流程如图 5 所示.

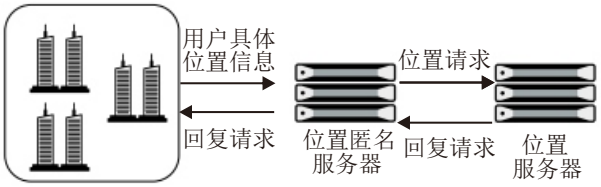
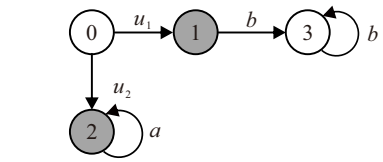


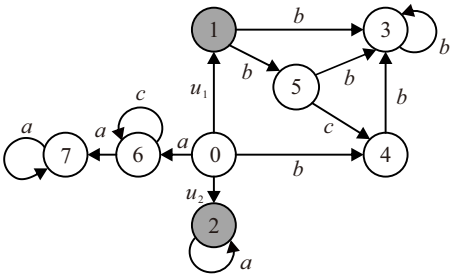
图5 位置匿名器工作流程

特别是当用户处于运动状态时, 由于提供的 LBS 数据仅是一些位置区域, 可能会出现用户轨迹不连贯的情况. 因此, 除了设置虚假位置之外, 还需要设置虚假路径. 在监督控制框架下, 监督器能够通过控制位置匿名方案来满足对用户信息保护的要求.

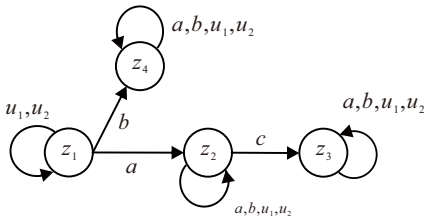
假设某用户运动轨迹如图 6(a) 所示. 其中: $\{a,b\}$ 为可观事件, $\{u_1,u_2\}$ 为不可观事件, 状态$\{1,2\}$为秘密位置. 用户不希望被外部入侵者发现自己曾到过这些位置. 当用户从位置 1 到位置 3 时, 入侵者观察到事件b, 能确定用户曾到过位置 1, 因此这一运动轨迹本身不满足无穷步不透明性的要求.



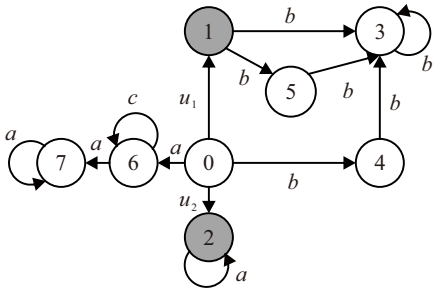
(a) 某用户运动轨迹



(b) 位置匿名系统提供的方案



(c) 监督者针对匿名控制方案的监督控制行为H



(d) 受控下位置匿名系统提供的方案 S/G

图6 基于位置服务实例

将状态 0 看作 0 区, 状态 1 看作 1 区, 依次类推, 位置匿名系统为用户轨迹提供的虚假位置和虚假路径如图 6(b) 所示. 其中: 状态$\{6,7\}$是 2 区的虚假位置, 状态$\{4,5\}$是 3 区的虚假位置. 各事件含义如表 1 所示. 其中: $\{u_1,u_2\}$为不可观事件, $\{a,b,c\}$为可观事件, $\{c\}$为可控事件. 当入侵者观察到事件串bc时, 能确定用户曾到过位置 1, 因此不满足无穷步不透明性的要求. 图 6(c) 为监督者对匿名方案的控制方案 (监督器), 得到的受控系统如图 6(d) 所示, 满足无穷

表1 位置匿名系统的事件描述

事件	描述
u_1	表示从位置0移动到位置1
u_2	表示从位置0移动到位置2
a	表示移动到2区
b	表示移动到3区
c	表示位置匿名方案, 即监督器可对其进行控制, 包括从虚假位置5到虚假位置4和长时间停在位置6

步不透明性的要求.

例 3　针对图 6 的位置匿名方案构造全攻击模型, 其模型如图 7 所示. 对于状态$Y_1=\{\hat{X}_1,\hat{X}_5,X_1,X_9,z_1,Z_3\}$, 有$X_1\bigcap X_9=\{1\}\subseteq X_s$, 且$\hat{X}_1\bigcap\hat{X}_{10}\neq\varnothing$, 因此对于秘密位置 1, 将系统的观察$b$篡改为$\hat{a}$, 然后系统观察到 c, 通过这种攻击策略即可在系统进入位置 1 一步观察后暴露位置信息, 破坏位置匿名系统无穷步不透明性. 根据定理 1, 该位置匿名服务系统是对无穷步不透明性弱可攻击的. 而对于秘密位置 2, 全攻击模型中没有相应满足要求的环境状态, 由定理 2 可知, 该位置匿名服务系统不是对无穷步不透明性强可攻击的.

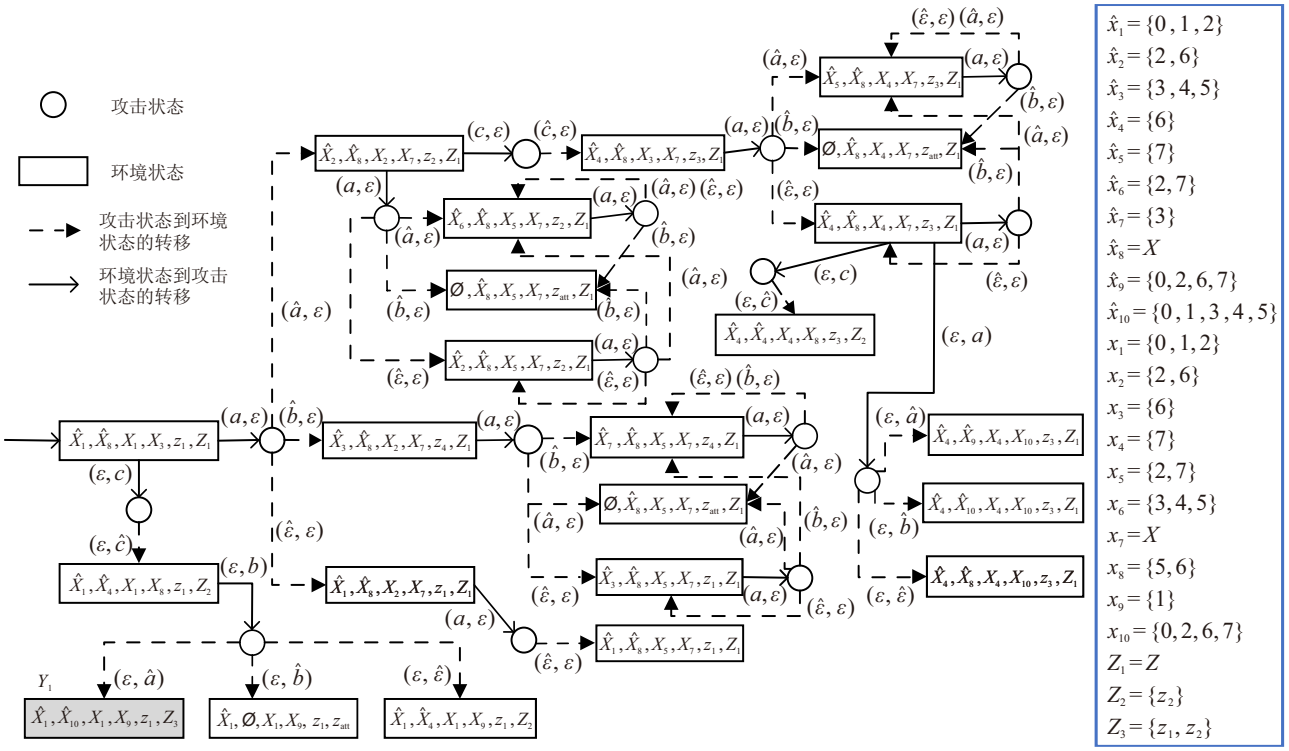


图7　全攻击模型M

通过上述示例可知, 对于给定的用户运动轨迹和受控下位置匿名系统方案, 可以判断系统对无穷步不透明性是否可攻击. 当前, 许多学者对不透明可攻击性进行了广泛研究, 提出了多种判断可攻击性的方案. 本文选取了一些具有代表性的文献进行对比, 如表 2 所示.

表2　不透明可攻击性方法比较

文献	不透明性	模型	监督控制
本文	无穷步不透明性	全攻击模型	是
文献[6]	当前不透明性	插入-删除模型	是
文献[7]	初始不透明性	全攻击模型	是
文献[8]	当前不透明性	估计器	否

文献 [8] 构造攻击情形的估计器, 并未考虑监督控制, 系统运行者无法控制系统运行, 当遇到攻击时, 无法及时做出对策; 文献 [6] 针对插入和删除事件两种攻击方式提出插入-删除模型, 并未考虑修改事件的情况, 攻击方式不够全面. 文献 [6-8] 适用于当前状态不透明性或初始状态不透明性; 而本文以监督控制为框架, 考虑了修改事件的攻击方式, 提高了方法的适用性. 相比于当前状态不透明性和初始状态不透明性, 无穷步不透明性要对系统运行过程中的状态做延迟状态估计, 估计过程更复杂, 本文解决了对监督者和攻击者同时做延迟状态估计的问题.

6　结　论

本文研究了在离散事件系统监督控制框架下, 针对无穷步不透明性的传感器主动攻击可行性问题. 通过构造全攻击模型, 记录攻击者与监督器的前后状态估计, 从而为攻击者提供了破坏受系统的攻击方法, 并以此模型得到了针对无穷步不透明性强可攻击和弱可攻击的充分必要条件. 在本文的基础上, 后续可继续研究针对无穷步不透明性的容忍攻击问题, 探索如何设计更强大的监督器, 使其在遭受攻击时仍保持系统的不透明性, 从而提高系统的鲁棒性.

参考文献 (References)

[1]　Cassandras C G, Lafortune S. Introduction to discrete event systems[M]. Boston: Springer, 2008: 26-43.

[2]　黄楠, 刘富春, 赵锐, 等. 基于动态观测的随机离散事件系统故障诊断[J]. 控制与决策, 2022, 37(2): 417-423.

(Huang N, Liu F C, Zhao R, et al. Failure diagnosis of stochastic discrete event systems based on dynamic observations[J]. Control and Decision, 2022, 37(2): 417-423.)

[3] 刘慧敏, 黎良. 基于标签时间 Petri 网的 DES 故障概率及发生时间预测[J]. 控制与决策, 2025, 40(2): 581-589.
(Liu H M, Li L. Prediction of fault probability and occurrence date for discrete event systems based on labeled time Petri nets[J]. Control and Decision, 2025, 40(2): 581-589.)

[4] 于绍琪, 田玉平. 基于 Petri 网与多智能体深度强化学习的 AGV 路径规划[J]. 控制与决策, 2025, 40(5): 1438-1446.
(Yu S Q, Tian Y P. AGV path planning based on Petri net and multi-agent deep reinforcement learning[J]. Control and Decision, 2025, 40(5): 1438-1446.)

[5] Meira-Góes R, Kang E, Kwong R H, et al. Stealthy deception attacks for cyber-physical systems[C]. 2017 IEEE 56th Annual Conference on Decision and Control. Melbourne, 2017: 4224-4230.

[6] Meira-Góes R, Kang E, Kwong R H, et al. Synthesis of sensor deception attacks at the supervisory layer of Cyber-Physical Systems[J]. Automatica, 2020, 121: 109172.

[7] Yao J S, Li S Y, Yin X. Sensor deception attacks against security in supervisory control systems[J]. Automatica, 2024, 159: 111330.

[8] Habbachi S, Zaghdoud A, Li Z W, et al. Secret inference and attacktability analysis of discrete event systems[J]. Information Sciences, 2022, 609: 1221-1238.

[9] Zhang Q, Seatzu C, Li Z W, et al. Stealthy sensor attacks for plants modeled by labeled Petri nets[J]. IFAC-PapersOnLine, 2020, 53(4): 14-20.

[10] Tai R C, Lin L Y, Zhu Y T, et al. Synthesis of distributed covert sensor-actuator attackers[J]. IEEE Transactions on Automatic Control, 2024, 69(8): 4942-4957.

[11] Lin L Y, Su R. Synthesis of covert actuator and sensor attackers[J]. Automatica, 2021, 130: 109714.

[12] Zheng S B, Shu S L, Lin F. Modeling and control of discrete event systems under joint sensor-actuator cyber attacks[C]. 2021 6th International Conference on Automation, Control and Robotics Engineering. Dalian, 2021: 216-220.

[13] Meira-Góes R, Lafortune S, Marchand H. Synthesis of supervisors robust against sensor deception attacks[J]. IEEE Transactions on Automatic Control, 2021, 66(10): 4990-4997.

[14] 王寿光, 赵玉美, 尤丹, 等. 离散事件系统框架下信息物理系统攻击问题综述[J]. 控制与决策, 2022, 37(8): 1934-1944.
(Wang S G, Zhao Y M, You D, et al. Survey on attacks in cyber physical systems based on discrete event systems[J]. Control and Decision, 2022, 37(8): 1934-1944.)

[15] Bryans J W, Koutny M, Ryan P Y A. Modelling opacity using Petri nets[J]. Electronic Notes in Theoretical Computer Science, 2005, 121: 101-115.

[16] Saboori A, Hadjicostis C N. Notions of security and opacity in discrete event systems[C]. 2007 46th IEEE Conference on Decision and Control. New Orleans, 2007: 5056-5061.

[17] Saboori A, Hadjicostis C N. Verification of infinite-step opacity and complexity considerations[J]. IEEE Transactions on Automatic Control, 2012, 57(5): 1265-1269.

[18] Lin F. Opacity of discrete event systems and its applications[J]. Automatica, 2011, 47(3): 496-503.

[19] Yin X, Lafortune S. A new approach for the verification of infinite-step and K-step opacity using two-way observers[J]. Automatica, 2017, 80: 162-171.

[20] 戴茵茵, 王飞, 罗继亮. 基于离散事件系统鲁棒监控的强制隐蔽综合[J]. 控制理论与应用, 2025, 42(4): 847-854.
(Dai Y Y, Wang F, Luo J L. Opacity-enforcing synthesis on robust supervisory control of discrete event systems[J]. Control Theory & Applications, 2025, 42(4): 847-854.)

[21] Aparicio J, Álvarez F J, Hernández Á, et al. A survey on acoustic positioning systems for location-based services[J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 8505336.

作者简介

丘瑞明 (2000−), 男, 硕士生, 主要研究方向为离散事件系统监督控制、信息物理系统安全控制, E-mail: qiuruim@163.com;

肖存涛 (1979−), 男, 副教授, 博士, 硕士生导师, 主要研究方向为控制理论与应用、形式化方法、算法设计, E-mail: xiaocuntao@gdut.edu.cn.