文章编号:1006-2475(2023)09-0105-10

# 基于随机Petri网的RFID系统安全性分析模型

肖 航[1],李 鹏[1,2],马荟平[1],朱 枫[1,2]

(1.南京邮电大学计算机学院,江苏 南京 210023; 2. 南京邮电大学网络安全和可信计算研究所,江苏 南京 210023)

**摘要:**针对日益频发的RFID系统攻击给RFID系统带来瘫痪风险问题,提出一种采用基于层次广义随机Petri网的RFID系统安全性分析模型。该模型利用已有的知识储备模拟真实的RFID虚拟环境,对攻击RFID系统过程进行准确有效的实验推演,并量化分析RFID系统风险。首先,利用攻击层次、攻击权限和基于权限的攻击等信息构建RFID攻击者模型;其次,对攻击者的行为进行建模描述,刻画其对RFID系统状态的影响;最后,基于所构建的模型对目标RFID系统的攻击概率、脆弱节点等方面进行风险评估。实验结果表明,本文提出模型可有效地对RFID系统进行风险评估,并且大大降低了评估时间和复杂度。

**关键词:**随机Petri网; 安全评估; 时间复杂度; 组合攻击

**中图分类号:**TP393.08 **文献标志码:**A **DOI:**10.3969/j.issn.1006-2475.2023.09.017

## RFID System Security Analysis Model Based on Stochastic Petri Net

XIAO Hang[1], LI Peng[1,2], MA Hui-ping[1], ZHU Feng[1,2]

(1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; 2. Institute of Network Security and Trusted Computing of Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

**Abstract:** To solve the problem of RFID system breakdown risk caused by frequent RFID system attacks, this paper proposes a RFID system security analysis model based on hierarchical generalized stochastic Petri net. The model uses the existing knowledge reserve to simulate the real RFID virtual environment, accurately and effectively deduces the attack process in the RFID system, and quantifies the risk of the RFID system. Firstly, the RFID attacker model is constructed using the information of attack hierarchy, attack authority and permission-based attacks. Secondly, the description of the attacker's behavior is modeled and described its impact on the RFID system state. Finally, based on the constructed model, the attack probability, weak nodes and other aspects of the RFID system are assessed. The experimental results show that the proposed model can effectively evaluate the risk of RFID system, and greatly reduce the complexity of evaluation time.

**Key words:** stochastic Petri net; safety assessment; time complexity; combination of attack

## 0 引 言

随着现代物流和物联网技术应用的逐渐普及,RFID(Radio Frequency Identification)系统与人们衣食住行的联系日益紧密,RFID系统安全的重要性就日益凸显。近年来,针对RFID系统安全性的研究主要以基于多种算法的轻量级RFID安全认证协议[1-2]为主,相较而言,对攻击者的行为建模并分析的却不多。由于目前RFID安全领域中评估类标准匮乏,现有的研究者很难对RFID系统实施较为全面的安全评估。为了解决上述研究困境,本文参照传统计算机网络中入侵者行为建模的方法[3-4],本文针对RFID系统中特有的攻击分析,建立RFID系统的攻击者模型。

目前,在RFID攻击建模方面,缺乏对并发性和协作性攻击方式表达恰当的模型,本文提出一种基于层次广义随机Petri网的攻击模型HGSPN(Hierarchical Generalized Stochastic Petri Net)。该模型较为系统全面地表达了RFID系统攻击的原子性和宏观性,对RFID多种类并发协作攻击行为进行模拟,同时在模型状态节点的数量爆炸问题上得以有效的缓解。本文模型相较于攻击图等模型具有以下优点:

1)本文模型能准确地描述攻击过程和RFID系统状态,可实现RFID系统协同攻击建模,清晰地表达出复杂攻击中系统脆弱点之间的利用逻辑和时序关系。

2)本文模型在一定程度上缓解了模型状态规模随节点的增加带来的指数型上升的问题,在确保对RFID系统安全状态尽可能完整表达的基础上,合理地规划设计模型层级间的连接和构造能对状态规模

**收稿日期:**2022-08-15; **修回日期:**2022-10-28

**基金项目:**国家自然科学基金资助项目(61872196, 61872194, 61902196, 62102194, 62102196); 江苏省六大人才高峰高层次人才项目(RJFW-111)

**作者简介:**肖航(1998—),男,安徽广德人,硕士研究生,研究方向:物联网安全,E-mail: 1020041127@njput.edu.con; 通信作者:李鹏(1979—),男,福建长汀人,教授,博士生导师,研究方向:网络安全,云计算技术,E-mail: lipeng@njupt.edu.cn; 马荟平(1998—),男,甘肃白银人,硕士研究生,研究方向:物联网安全,E-mail: 1020041117@njput.edu.con; 朱枫(1986—),男,安徽合肥人,讲师,博士,研究方向:系统安全,E-mail: zhufeng@njupt.edu.cn。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

进行适当的剪枝。

3)本文模型中的状态节点概率可以在短时间内迅速收敛,同一般的Petri网模型相比,该模型在多目标攻击的稳态求解时间上快一个数量级。

## 1 相关工作

对RFID攻击进行科学、有效的建模是维护RFID系统安全的重要措施。目前,李辉等人[5]针对给出的RFID系统中防伪安全协议的复杂性提出了智能伪造攻击模型,形式化分析了复杂防伪协议的设计。李俊霖等人[6]对物联网安全协议攻击者能力进行了形式化构建,分析了攻击者模型的攻击行为,但文中缺乏相应的对比实验。黄义夫[7]提出了面向RFID协议的安全检测攻击图模型和基于层次分析法的RFID安全漏洞顶级策略,实现了对EPC C1 G2标准协议的仿真、攻击检测、安全评估,但文中并未对RFID非标准协议进行仿真和攻击检测。杨晓明[8]提出了基于图的RFID攻击模型,该模型能够动态地模拟攻击者可能采取的攻击步骤,直观地体现了RFID系统的安全状态,但在RFID攻击规则方面还有待完善。Wang等人[9]针对RFID的4种攻击方法,构建了RFID安全检测模型,研究分析了RFID系统的漏洞和可能的攻击路径。Ai等人[10]通过引入克隆标签的攻击概率概念,提出了IPCA协议,研究了大规模RFID系统中克隆攻击概率的识别问题。

Petri网是一种描述复杂系统(包括计算机网络和协议)的有效工具,基于Petri网所建立的模型既能表达出系统所处在的不同状态,还能对系统或网络中的攻击行为进行模拟。在近几年的研究中,Chen等人[11]提出了一种组合式Petri网的方法对大型网络物理系统进行攻击建模,文中虽未提出精确的智能电网威胁模型,但是为复杂系统攻击建模提供了相应的思路。高翔等人[12]提出了一种基于广义随机着色Petri网的网络攻击组合模型,对攻击行为之间的关联关系进行了清晰的表述,但文中仅根据时间代价对网络系统的脆弱性进行了分析,缺乏对攻击概率的量化评估。Almutairi等人[13-14]提出了一种基于广义随机Petri网的软件定义网络(SDN)攻击模型,评估了SDN多控制器的风险。毋泽南等人[15]提出了一种网络系统评估模型NSA-SPN,对网络安全相应指标进行了合理评估,但模型的攻击路径较为单一,对恶意用户针对系统的攻击不能够充分的表达。He等人[16]提出了基于GSPN模型的网络空间模拟DNS抗攻击模型并分析了其可靠性、可用性和抗攻击性。

目前,利用Petri网对系统进行建模分析时,模型规模问题一直未能得到很好的解决,缩减模型的规模往往伴随着状态特征的丢失,而对模型的规模进行适当地扩充虽然保留了部分状态特征,并在一定程度上降低了状态转移之间的耦合性,但是面对较为复杂的系统,攻击规模也就随之增大,模型的状态数量呈指数级增长。同时,就RFID的安全性研究而言,现有的文献大多是针对RFID的安全隐私、协议认证[17-19]方面进行相关的研究,缺乏从RFID攻击者模型构建方面来提高RFID安全性的研究。针对这些问题,本文提出一种基于层次广义随机Petri网的RFID系统安全评估模型HGSPN-RFID,通过对RFID攻击的并发性、协作性、递进性过程进行描述,发掘攻击者意图,评估RFID系统风险。该模型从攻击者角度出发,自顶向下从3个层次对RFID系统协作性、并发性攻击进行建模,对RFID系统所处的攻击状态进行准确的表达,在时间和空间规模上性能也进行了优化。

## 2 基于层次广义随机Petri网的RFID系统安全性分析模型

### 2.1 基本概念

广义随机Petri网GSPN(Generalized Stochastic Petri Net)[20]是在随机Petri网的基础上进行的改进,将变迁划分为2种,一种是表示耗时的事件的时间变迁;一种是表示逻辑选择的瞬时变迁,对随机Petri网的状态规模随着求解问题节点数量增加而产生指数爆炸问题进行有效地缓解,避免了同构的马尔可夫过程求解困难的问题。

广义随机Petri网是对随机Petri网功能的改进,相较于传统随机Petri网,其针对实际场景中的逻辑关系表述的更为恰当,对于和时间无关而在逻辑策略上具备选择的事件,将其建模为瞬时变迁;针对在时间上具有连贯性和先后顺序的事件,将其建模为时间变迁。

### 2.2 层次广义随机Petri网

首先给出层次广义随机Petri网的相关概念[21]。

**定义1** 顶层父Petri网(FPN)。顶层父Petri网由三元组FPN=$(P,T,F)$构成,其中:$P=\{p_1,p_2,\cdots,p_n\}$代表关键位置集合;$T=\{t_1,t_2,\cdots,t_n\}$代表摘要变迁集合;$P\cap T\neq\varnothing$且$P\cup T\neq\varnothing$,$F\subseteq\{P\times T\}\cup\{T\times P\}$是弧的集合。

**定义2** 权限子Petri网(PASPN)。PASPN=$\{P^{\mathrm{p}},T^{\mathrm{p}},F^{\mathrm{p}},M_0,v\}$,其中$P^{p}=\{p_0^{\mathrm{p}},p_1^{\mathrm{p}},\cdots,p_n^{\mathrm{p}}\}$是攻击者具有的权限集合;$T^{\mathrm{p}}=\{T_0^{\mathrm{p}},T_1^{\mathrm{p}},\cdots,T_n^{\mathrm{p}}\}$代表变迁集合,$T_k^{\mathrm{p}}=T_k^{\mathrm{p}}\{a_{\mathrm{p}},\pi_{\mathrm{p}},q_{\mathrm{p}}\}$表示某一具体行为,$\pi_{\mathrm{p}}$表示权限转移的概率,$q_{\mathrm{p}}$表示权限提升的概率;$F^{\mathrm{p}}$是有向弧集合,PASPN中由弧连接的起始位置到目标的连通图代表攻击权限提升路径;$M_0$代表初始状态;$v$代表变迁触发速率,反映了攻击者获取权限的能力。

**定义3** 基于权限的攻击子网(AASPN)。AASPN=$\{P^{\mathrm{a}},T^{\mathrm{a}},F^{\mathrm{a}}\}$,其中:$P^{\mathrm{a}}$是攻击集合;$T^{\mathrm{a}}=\{T_0^{\mathrm{a}},T_1^{\mathrm{a}},\cdots,T_n^{\mathrm{a}}\}$代表变迁集合,$T_k^{\mathrm{a}}=T_k^{\mathrm{a}}\{a_{\mathrm{a}},\pi_{\mathrm{a}},q_{\mathrm{a}}\}$代表某一攻击行为,$\pi_{\mathrm{a}}$表示攻击触发的概率,$q_{\mathrm{a}}$表示攻击成功的概率;$F^{a}$是有向弧集合,AASPN中由弧连接的起始位置到目标的连通图代表攻击路径。

**定义4** 层次广义随机Petri网模型(HGSPN)。HGSPN=$\{P',T',F',M_0',v'\}$,对于父Petri网FPN中的$t\in$T、PASPN, AASPN$\}$,通过细化组合操作,得到

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

HGSPN，其中：$P' = P \cup P^{p} \cup P^{a}$，$T' = (T - t) \cup T^{p} \cup T^{c}$，$F' = F - 2(t \times \{t\}) - (\{t\} \times t) \cup (F^{p} \cup (t \times T_i^{p}) \cup (T_o^{p} \times t)) + (F^{a} \cup (t \times T_i^{a}) \cup (T_o^{a} \times t))$，$t = \{y | (y,t) \in F\}$为$t$的前置集，$t = \{y | (t,y) \in F\}$为$t$的后置集，$T_i^{p}$和$T_o^{p}$分别为PASPN的入口和出口，$T_i^{a}$和$T_o^{a}$分别为AASPN的入口和出口。

### 2.3　攻击模型层次化结构

RFID系统主要由3个物理实体（电子标签、阅读器、后端数据库）和2种通信信道（无线通信信道、网络通信信道）组成。不同于有线网络中计算系统通常具备基于主机的集中式防御能力（防火墙），RFID系统中阅读器和标签都处于一个相对不够稳定且会被噪声干扰的环境中运行。攻击者可从后端数据库、网络通信信道、阅读器、前向通信信道、反向通信信道、标签等各方面对RFID系统进行攻击。目前在数据库安全、网络安全和计算机安全方面已经具备较为成熟的安全防护手段。

如图1所示，将RFID攻击按照攻击所属范围不同划分成感知层、网络传输层、应用层和多层次攻击[22]。

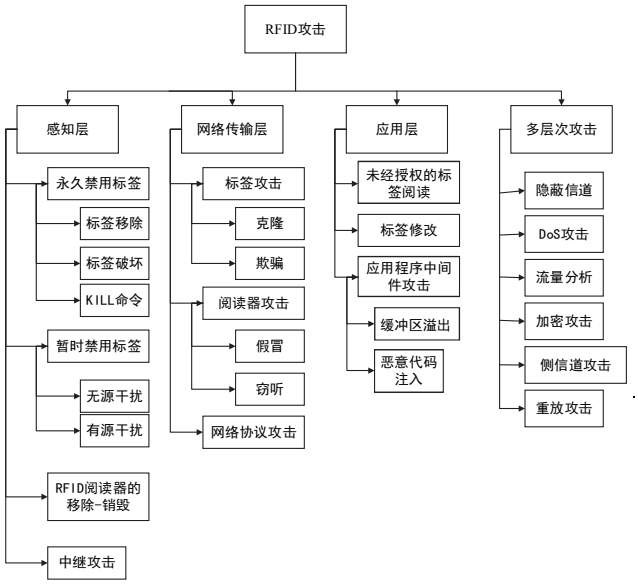



图1　RFID攻击的分类

一步构建RFID攻击模型会因规模庞大而难以实现，为此将描述RFID攻击系统的Petri网进行层次化扩展，分别构建顶层父Petri网、中间层权限Petri网和底层攻击Petri网。把表述RFID系统攻击的单一Petri网拓展为多方面多层次Petri网模型，从而缩减单一模型中的节点个数。将模型中的攻击方式分为全局攻击和原子攻击，就整体而言分析不同攻击间的联系，建立攻击间的连接，获取总体攻击路径；就局部而言，分析每一个独特节点的攻击方式和危害系数。系统把控RFID攻击间的紧密程度和不同攻击所造成的危害程度，可以对RFID系统中的脆弱性节点进行分析掌控，并根据这些脆弱点信息求解攻击路径，为RFID系统的安全性提供有力的保障。本文使用自顶层至权限层到攻击层的建模思路，令顶层父Petri网展现RFID攻击模型中各层次和系统安全之间的关系；中间层权限Petri网展现RFID系统中攻击者在发起攻击的过程中逐步利用当前权限获取更高级权限的提升关系；在攻击Petri网上，详细描述攻击者在利用权限层所获取到的权限后所具体发起的攻击形式。利用顶层网络、权限网络和攻击子网，实现对RFID系统的全网攻击描述。

### 2.4　攻击权限

攻击者发起攻击时处于初始节点，在该节点上攻击者只具有最低层次的系统权限。攻击者发起攻击并获取到更高级别的权限，就把获取后的权限当作新的状态点。

从攻击者的角度出发建立攻击者在不同层次上的权限模式。

分析现有的RFID攻击形式，并将RFID系统脆弱性分析过程中所涉及的权限分为感知层权限、网络传输层权限、应用层权3类，如表1所示。

**表1　RFID攻击者权限**

| 感知层权限 | 网络传输层权限 | 应用层权限 |
|---|---|---|
| 对RFID信道进行监听 | 伪装合法阅读器 | 获取标签权限 |
| 接近标签 | | |
| 接近阅读器 | 窃听信道并截获消息 | 破解标签安全机制，获取内部信息 |
| 手动操作标签 | | |
| 手动操作阅读器 | 非法读取标签信息 | 修改标签内容 |
| 对信道进行干扰 | | |

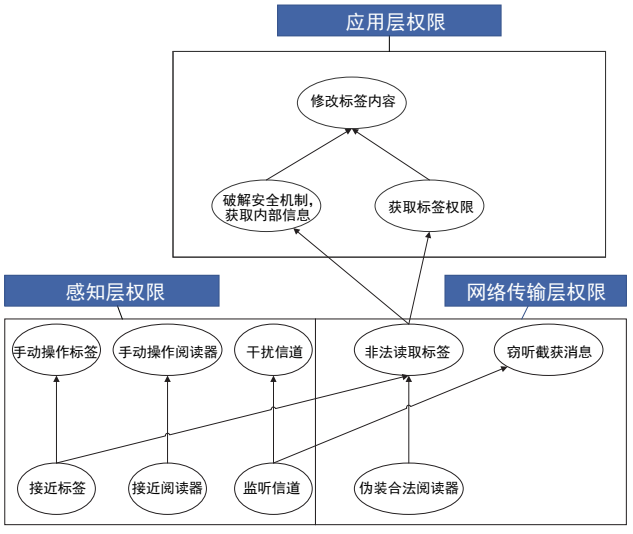



图2　RFID攻击权限提升模式

参考文献[7-8]，并总结已有的RFID攻击方式，获取不同攻击的攻击特征以及攻击权限之间的联系，根据RFID攻击者权限建立权限提升模式，如图2所示，同一个矩形中节点视为同一层次权限，没有入度的节点视为初始节点。攻击者最开始只具备初始节点的权限。然后攻击者利用自己已有的权限对系统发起攻击从而获取更高级别的权限。该行为对应到权限Petri上，即是权限提升变迁和权限库所的生成。

### 2.5　目标攻击

目标攻击是攻击者通过一系列攻击所要达到的

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

最终状态。调研分析现阶段主流的RFID系统攻击方式，依据攻击权限、区域等属性的不同将其划分为不同层次。根据图1对RFID系统的攻击按照攻击目标所处的不同层次可以分为3个大类，即感知层、网络传输层、应用层，建立如表2~表5所示的RFID感知层、网络传输层、应用层和多层次原子攻击规则库。

**表2 RFID感知层原子攻击规则库**

| 攻击类型 | | 攻击简述 |
|---|---|---|
| 永久禁用标签 | 标签移除 | 将标签从指定物品上移除 |
| | 标签破坏 | 以外力对标签进行破坏（包括物理破坏、化学腐蚀、放电和极端环境影响） |
| | KILL命令 | 破解标签密码执行KILL命令 |
| 暂时禁用标签 | 无源干扰 | 标签在不稳定和噪声环境中收到无线电干扰源的干扰和碰撞 |
| | 有源干扰 | 阅读器范围内产生信号，造成电磁干扰 |
| 阅读器的禁用 | RFID阅读器的移除 | 窃取阅读器以便攻击者访问RFID标签和后端系统 |
| | RFID阅读器的销毁 | 以外力对RFID阅读器进行破坏（包括物理破坏、化学腐蚀、放电和极端环境影响） |

**表3 RFID网络传输层原子攻击规则库**

| 攻击类型 | | 攻击简述 |
|---|---|---|
| 标签攻击 | 克隆 | 将标签的ID和任何相关数据复制到克隆标签（难易受标签安全特性影响） |
| | 欺骗 | 攻击者将伪装阅读器获取的标签信息发送给合法阅读器 |
| | 追踪 | 攻击者对标签中存储的数据进行标记，以达到对标签追踪的目的 |
| | 数据泄露 | 攻击者获取标签ID或标签上存储的用户敏感信息 |
| 阅读器攻击 | 假冒 | 攻击者根据RFID的认证强度在一定程度上假冒合法阅读器的身份，从而获取敏感信息以及修改RFID标签上的数据 |
| | 窃听 | 攻击者使用天线来记录合法的RFID标签和阅读器之间的通信 |
| | 中继攻击 | 攻击者拦截并修改合法标签和阅读器之间的无线电信号 |

**表4 RFID应用层原子攻击规则库**

| 攻击类型 | | 攻击简述 |
|---|---|---|
| 未经授权的标签读取 | | 接近RFID标签对未经身份验证的标签进行读操作 |
| 标签篡改 | | 对用户可写内存的标签修改或删除有价值的信息（难以依赖于RFID使用的标准和所采用的读写保护） |
| 中间件攻击 | 缓冲区溢出 | 使用RFID标签重复发送相同数据块的命令，使后端RFID中间件的缓冲区溢出 |
| | 恶意代码注入 | RFID标签对使用Web协议和脚本语言的RFID应用程序执行代码插入或SQL注入 |

RFID通信中的感知层由物理接口、使用的无线电信号和RFID设备组成。在该层攻击者利用了RFID通信的无线特性、物理安全性差以及对物理操纵缺乏弹性对系统进行攻击，感知层攻击并未获取标签所包含的信息，却对RFID系统的日常运行造成了危害。安全威胁主要包括永久禁用标签、暂时禁用标签和阅读器的禁用等物理攻击。

**表5 RFID多层次原子攻击规则库**

| 攻击类型 | | 攻击简述 |
|---|---|---|
| 隐蔽通道 | | 攻击者利用RFID标签创建未经授权的通信通道来秘密传输信息 |
| DoS攻击 | 使用“blocker tag” | 攻击者获得标签权限，利用标签自带保护机制故意阻止标签的访问 |
| | 使用LOCK命令 | 攻击者未经授权使用LOCK命令，防止未经授权写入RFID标签的内存 |
| | 攻击中间件 | 向中间件发送数据包流，使网络的带宽或处理能力被淹没，从而拒绝访问常规客户端 |
| 流量分析 | | 攻击者通过窃听截获消息并从通信模式中提取信息 |
| 加密攻击 | | 攻击者破坏系统采用的加密算法，并泄露或操纵敏感信息 |
| 侧信道攻击 | | 利用系统的时间、功耗、电磁场信息以及加密算法获取密文信息 |
| 重放攻击 | | 攻击者复制RFID通信中的有效应答，并在稍后广播给一方或多方 |

网络传输层包括所有基于RFID系统通信方式和RFID网络实体（标签、读卡器）之间数据传输方式的攻击，该层攻击主要是对信息在来回传输的过程中造成破坏。安全威胁主要包括标签攻击、读卡器攻击和中继攻击等对传输过程中信息的攻击。

应用层包括针对与应用程序相关的信息以及用户与RFID标签之间绑定的所有攻击。在该层，攻击者利用未经授权的标签读取、修改标签数据以及应用程序中间件来进行攻击。

然而，许多针对RFID通信的攻击并不局限于单一层。多层次攻击包括影响RFID感知层、网络传输层、应用程序层的多维攻击。在该层包括隐蔽通道、拒绝服务、流量分析、加密、侧通道攻击和重放攻击。

### 2.6 攻击事件描述

攻击事件的定义为：

Attack_event=（PN（Permission_name），PP（Pre_permission），NP（Next_permission），A（Attack））

在此定义下的符号含义为：

PN：针对RFID系统的攻击权限名称。

PP：获取当前权限的前提条件。

NP：基于当前权限进行攻击可以获取的下一个权限。

A：攻击者基于当前权限可以完成的原子攻击。

原子攻击规则库如表6所示。

### 2.7 基于层次广义随机Petri网的RFID攻击模型

RFID攻击Petri网的构造思想是自顶向下，逐步精细的过程。父Petri网描述RFID系统攻击中层次之间的关系；权限Petri网描述RFID系统中的权限提升关系，把攻击权限视为对象，那么权限Petri网由攻击权限和攻击权限间的权限变迁生成；权限Petri网上的对象可按攻击权限规则库扩展为攻击子网。对应RFID攻击权限库，可建立如图2所示的RFID攻击Petri网。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

**表6　RFID原子攻击规则库**

| PN | PP | NP | A |
|---|---|---|---|
| 监听RFID信道 | Null | 干扰RFID信道、窃听截获消息 | 有源干扰、无源干扰 |
| 接近标签 | Null | 对标签进行手动操作 | |
| 对标签进行手动操作 | 接近标签 | | 标签移除、标签破坏、KILL |
| 接近阅读器 | Null | 对阅读器进行手动操作 | |
| 对阅读器进行手动操作 | 接近阅读器 | | 阅读器的移除、销毁 |
| 伪装合法阅读器 | Null | 非法读取标签 | 中间人攻击、欺骗攻击 |
| 非法读取标签 | 接近标签、伪装合法阅读器 | 破解安全机制、获取内部信息、获取标签权限 | |
| 破解安全机制、获取内部信息 | 非法读取标签 | 修改标签内容 | 重放攻击、加密攻击、 |
| 获取标签权限 | 非法读取标签 | 修改标签内容 | DoS攻击 |
| 修改标签内容 | 破解安全机制、获取内部信息、获取标签权限 | | 篡改攻击、注入恶意代码 |
| 窃听截获消息 | 监听RFID信道 | | 流量分析、侧信道攻击 |

攻击者从根节点出发，查询已具备的起始权限，根据该权限查询能发起的攻击方式，生成状态节点和攻击节点，然后依次查询每个攻击对权限的提升关系，获取进一步的攻击权限，重复上面的过程，直到没有进一步的权限可以获取。

根据定义1~定义4，首先构建顶层父Petri网模型，如图3所示，攻击者从感知层、网络传输层、应用层关键位置对RFID系统进行攻击。其次，根据RFID攻击者权限提升模式构建权限子Petri网模型，如图4所示，攻击者在不同层次间可以获取权限以此达到对RFID系统进一步攻击的目的。最后，根据RFID原子攻击规则库构建基于权限的攻击子Petri网模型，每一个原子攻击都是在攻击者获取了相应的一个或多个攻击权限的基础上发起的。

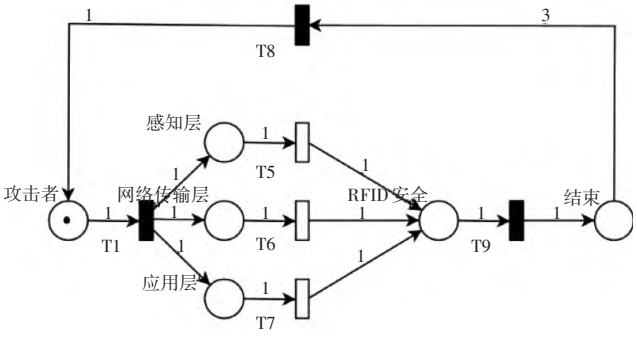



图3　顶层父Petri网模型FPN

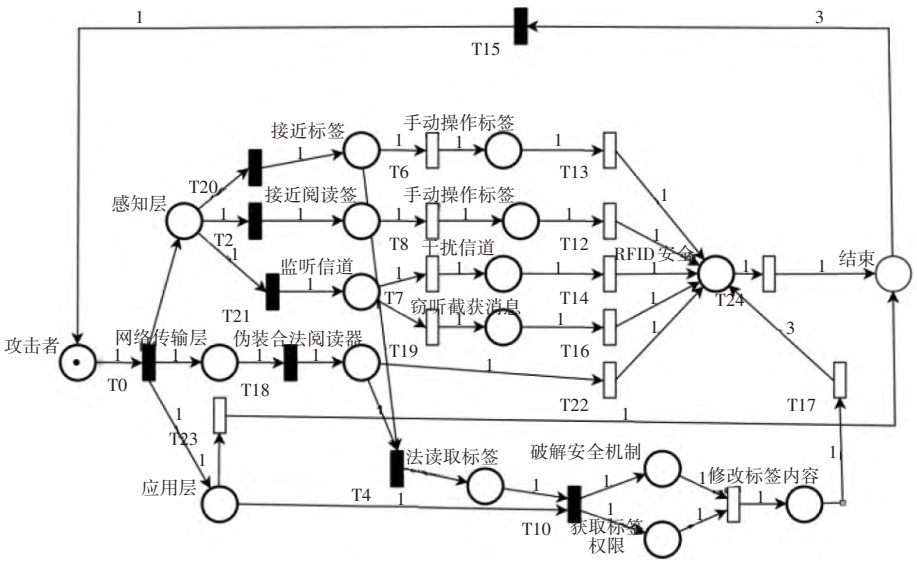



图4　权限子Petri网PASPN

基于层次广义随机Petri网的RFID攻击模型通过建立RFID不同层次段攻击的Petri网，拓展顶层Petri网的内容获得基于RFID攻击权限的Petri网，针对权限Petri网建立攻击子网并整合后，如图5所示，获取较为综合的RFID安全分析模型。层次化Petri网模型有效地避免了Petri网模型因整体节点过多而产生的组合爆炸问题。

在基于层次广义随机Petri网的RFID攻击模型的构建过程中，使用瞬时变迁来表示攻击权限的获取以及攻击状态的重置过程，使用延时变迁来表示攻击者已经获取了部分攻击权限，并根据权限发起相应的攻击，但如果攻击者有机会获取更高级别的权限，那么基于当前权限的攻击将不会被选择，即该延时变迁不会触发，进而选择更高级别的权限并在此基础上选择高级权限的攻击。

攻击者的攻击具有递进性，攻击者需要先获取相应的权限，基于权限来获取更高级别的权限或者基于当前权限发起对RFID系统的攻击。攻击者的攻击具

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

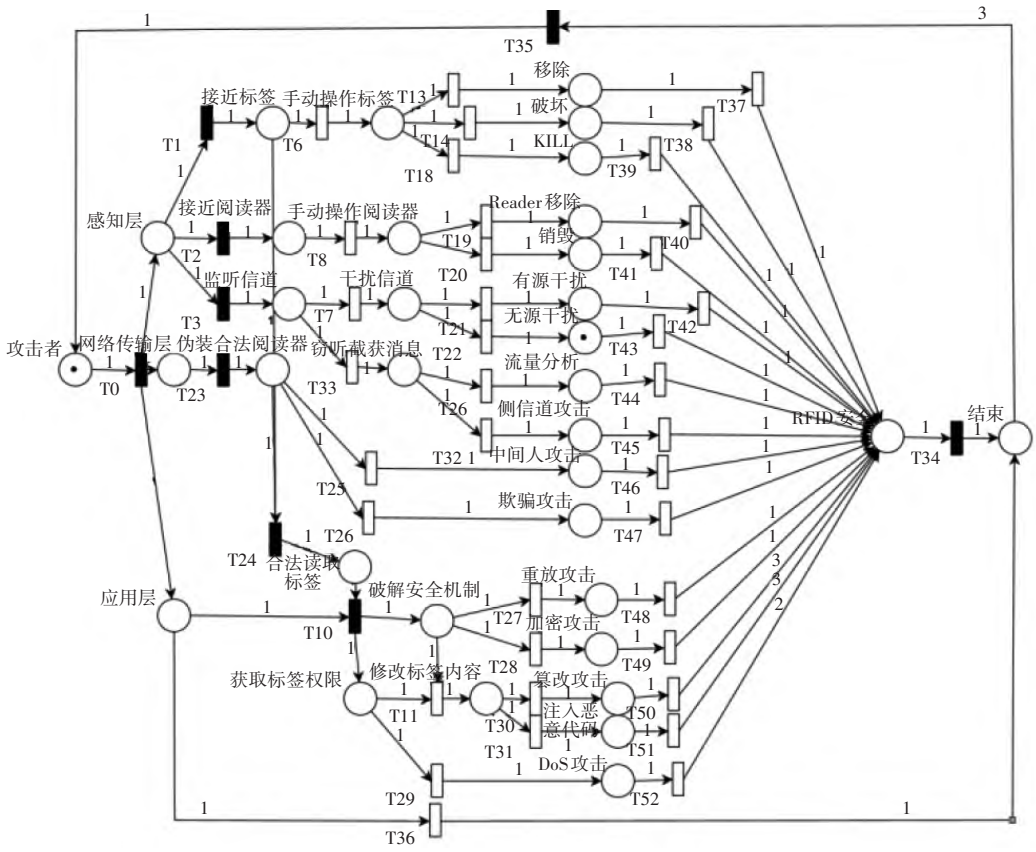



图5 基于权限的攻击子网AASPN

有并发性,攻击者从初始节点开始,分别获取感知层、网络传输层和应用层的相应低级权限,攻击者在每一层的攻击都是时间上并行的。攻击者的攻击具有协作性,攻击者基于所获取的低级权限可以选择进行攻击或者进一步获取高级权限,多种低级权限之间进行相互协作,进而获取更为高级的权限,对系统发起更具威胁的攻击。

在AASPN中,库所描述如表7所示。

**表7 AASPN中库所说明**

| 库所 | 描述 | 库所 | 描述 | 库所 | 描述 |
|---|---|---|---|---|---|
| p0 | 攻击者 | p12 | 中间人攻击 | p24 | 破坏 |
| p1 | 感知层 | p13 | 欺骗攻击 | p25 | KILL |
| p2 | 网络传输层 | p14 | 非法读取标签 | p25 | Reader移除 |
| p3 | 应用层 | p15 | 破解安全机制 | p27 | 销毁 |
| p4 | 接近标签 | p16 | 获取标签权限 | p28 | 有源干扰 |
| p5 | 接近阅读器 | p17 | 修改标签内容 | p29 | 无源干扰 |
| p6 | 监听信道 | p18 | 重放攻击 | p30 | 流量分析 |
| p7 | 伪装合法阅读器 | p19 | 加密攻击 | p31 | 侧信道攻击 |
| p8 | 手动操作标签 | p20 | 篡改攻击 | p32 | RFID安全 |
| p9 | 手动操作阅读器 | p21 | 注入恶意代码 | p33 | 结束 |
| p10 | 干扰信道 | p22 | DoS攻击 | | |
| p11 | 窃听截获消息 | p23 | 移除 | | |

## 3 稳态分析与仿真评估

研究Petri网模型的性能一般包括可达树[23]、可达标识图[24]、矩阵方程求解、分层或化简等方法。可达树和可达标识图可简洁直观地分析系统的可达性、有界性、活性等各种动态特性,并可以对Petri网的大部分特性进行验证。该方法通过分析层次广义随机Petri网模型的活性、有界性以及是否具有完全可达性来验证攻击的正确性。

### 3.1 稳态分析

根据文献[25],一个随机Petri网同构于一个连续时间Markov链,本文所建立的顶层父Petri网、权限子Petri网、基于权限的攻击子网也同构于一个连续时间Markov链。与顶层父Petri网同构的Markov链如图6所示。在图中,S0、S2、S3、S4、S8、S9、S10、S14、S15为消失状态,因为它关联的库所触发瞬时变迁,不存在稳态概率,其中S0表示初始状态;S1、S5、S6、S7、S11、S12、S13为有形状态,存在稳态概率。根据同构马尔科夫链中有形状态之间的转换关系,可以得到顶层父Petri网稳定状态的可达标识集,如表8所示。

对图6进行可达性、有界性及或许分析如下:

1)图6是一个全连通图,该模型是完全可达的,该可达树中的任一标识都是从S0可达。

2)如表8所示,每一个库所的Token数都未超过3,库所的Token数是动态守恒的,不存在凭空产生的Token,也不存在凭空消失的Token,该模型是安全的,也是有界的。

3)图6中的每一个状态节点,既有入度,也有出度,换言之,该模型不存在死锁或结束状态,该模型是活性的。

综上所述,该评估模型是有效可行的。

对顶层父Petri网、权限子Petri网、基于权限的攻击子网分别进行可达图构建,结果如表9和图7所示。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

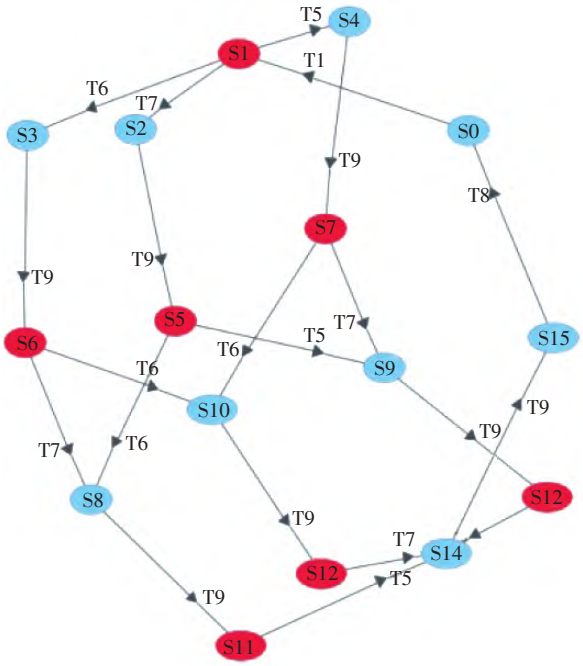



图6　顶层父Petri网可达标识图

**表8　顶层父Petri网可达标识集**

| 状态 | 结束 | RFID安全 | 感知层 | 攻击者 | 网络传输层 | 应用层 |
|---|---|---|---|---|---|---|
| S0 | 0 | 0 | 0 | 1 | 0 | 0 |
| S1 | 0 | 0 | 1 | 0 | 1 | 1 |
| S2 | 0 | 1 | 1 | 0 | 1 | 0 |
| S3 | 0 | 1 | 1 | 0 | 0 | 1 |
| S4 | 0 | 1 | 0 | 0 | 1 | 1 |
| S5 | 1 | 0 | 1 | 0 | 1 | 0 |
| S6 | 1 | 0 | 1 | 0 | 0 | 1 |
| S7 | 1 | 0 | 0 | 0 | 1 | 1 |
| S8 | 1 | 1 | 1 | 0 | 0 | 0 |
| S9 | 1 | 1 | 0 | 0 | 1 | 0 |
| S10 | 1 | 1 | 0 | 0 | 0 | 1 |
| S11 | 2 | 0 | 1 | 0 | 0 | 0 |
| S12 | 2 | 0 | 0 | 0 | 1 | 0 |
| S13 | 2 | 0 | 0 | 0 | 0 | 1 |
| S14 | 2 | 1 | 0 | 0 | 0 | 0 |
| S15 | 3 | 0 | 0 | 0 | 0 | 0 |

**表9　库所数量、状态数量、状态间变迁数量**　　单位：个

| 网络类型 | 库所数量 | 状态数量 | 状态间变迁数量 |
|---|---|---|---|
| 顶层父Petri网 | 6 | 16 | 21 |
| 权限子Petri网 | 18 | 50 | 80 |
| 基于权限的攻击子网 | 34 | 158 | 343 |

根据表9和图7的结果可知，随着由顶层父Petri网到权限子Petri网再到基于权限的攻击子网进行层次扩充的过程，模型的库所数量呈较为稳定的线性增长，状态数量呈近似于3的指数级增长，状态间变迁数量呈近似于4的指数级增长。通过逐层构建RFID攻击模型的过程，顶层父Petri网模型的构建很大程度上决定了权限子Petri网和基于权限的攻击子网的状态数量，对顶层父Petri网的精简在一定程度上可以对状态爆炸问题进行适当的缓解。

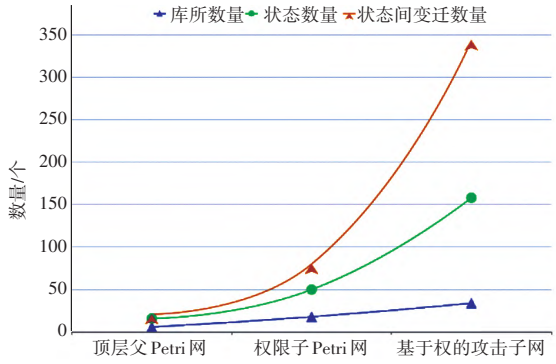



图7　库所数量、状态数量、状态间变迁数量图

### 3.2　稳态概率求解

随着时间的推移，顶层父Petri网马尔科夫链的节点概率趋于稳定，如图8所示，在初始时间点最上方的线条显示了S1状态的概率变化趋势，中间的线条显示了状态S5、S6、S7的概率变化趋势，最下方线条显示了状态S11、S12、S13的概率变化趋势。

其中，“p1　p2　p3”表示S1状态，“p1　p3　p5”、“p1　p2　p5”、“p2　p3　p5”分别表示S5、S6、S7状态，“p1　p5　p5”、“p2　p5　p5”、“p3　p5　p5”分别表示S11、S12、S13状态，其稳态概率如表10所示。

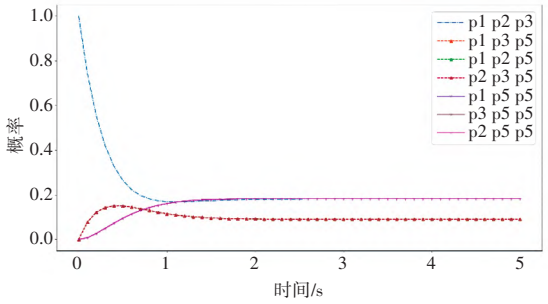



图8　顶层父Petri网稳态概率

**表10　稳态概率**

| 状态 | Value |
|---|---|
| S1、S11、S12、S13 | 0.182 |
| S5、S6、S7 | 0.092 |

权限子Petri网马尔科夫链稳态概率如图9所示。

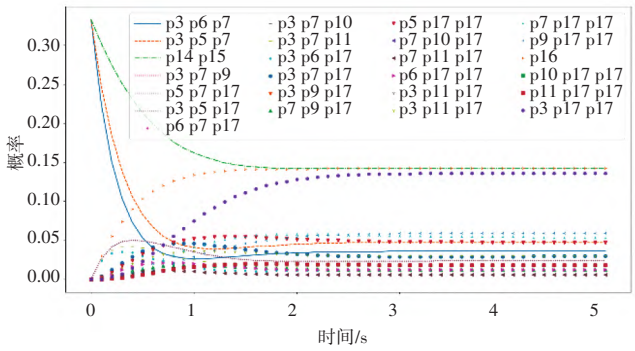
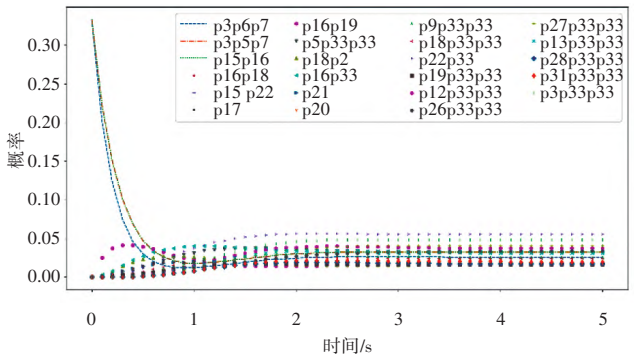


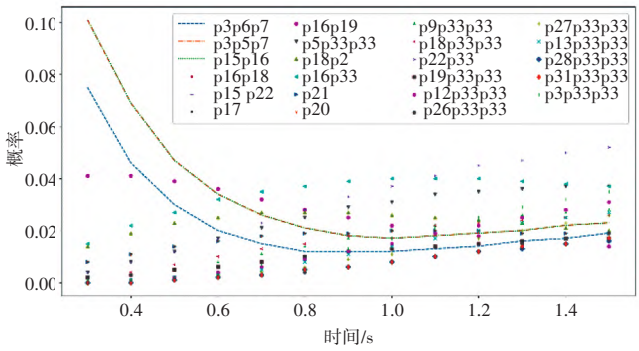

图9　权限子Petri网稳态概率

基于权限的攻击子网马尔科夫链稳态概率如图10所示，其中由于状态较多，筛选出初始概率大于0.1或者稳态概率大于0.15的状态。

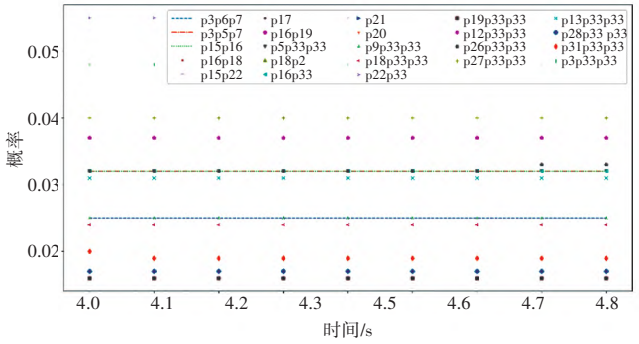
(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net




（a）1~5 s基于权限的攻击子网稳态概率




（b）0.4~1.4 s基于权限的攻击子网稳态概率




（c） 4~4.8 s基于权限的攻击子网稳态概率

图10 基于权限的攻击子网稳态概率

根据图10结果可知，本文所构建的顶层父Petri网、权限子Petri网、基于权限的攻击子网均可以在单位时间内得到稳态概率，其都相应地同构于一个马尔可夫链，可以求得对应的平稳状态概率。

### 3.3 模型的评估

引入3个属性来评估RFID攻击模型：攻击成本$c$、技术难度$d$和发现几率$s$。表11展示了相应的等级标准[26]。根据以下规则为每一个变迁属性赋值。

表11 等级标准

| 攻击成本$c$ | 级别 | 技术难度$d$ | 级别 | 发现几率$s$ | 级别 |
|---|---|---|---|---|---|
| >10 | 5 | 非常困难 | 5 | 非常困难 | 5 |
| 6~10 | 4 | 困难 | 4 | 困难 | 4 |
| 3~6 | 3 | 中等 | 3 | 中等 | 3 |
| 0.5~3 | 2 | 简单 | 2 | 简单 | 2 |
| <0.5 | 1 | 非常简单 | 1 | 非常简单 | 1 |

1）攻击者可以对系统的任何节点发起攻击，对攻击者来说，在较高级别的节点上进行攻击比在较低级别的节点上进行攻击更为困难，而且攻击的成本也会更高。

2）攻击者应该考虑变迁的前置状态来发动攻击，所需状态的数量和难度会给攻击者后续的攻击带来更高的难度和成本。

使用多属性效用理论将$c$、$d$、$s$属性转换成攻击者的效用值$P$，计算公式如式（1）：

$$P=w_1u_1(c)+w_2u_2(d)+w_3u_3(s) \tag{1}$$

其中，$u_1(c)$、$u_2(d)$、$u_3(s)$是变迁属性的效用函数，它们的范围在0~1之间。$w_1$，$w_2$，$w_3$是变迁属性的权重，其中$w_1+w_2+w_3=1$。为了计算模型中每个转换的总体效用，设置$w_1+w_2+w_3=1/3$，效用函数$u_1(c)=u_2(d)=u_3(s)=u(c_x)=c/x$，其中$c=0.2$来确保效用值分布在0和1之间。

### 3.4 应用实例和分析

下面以某图书馆RFID门禁系统为目标，应用前文提到的模型和分析方法，在实验环境下进行攻击概率计算，RFID系统架构如图11所示。

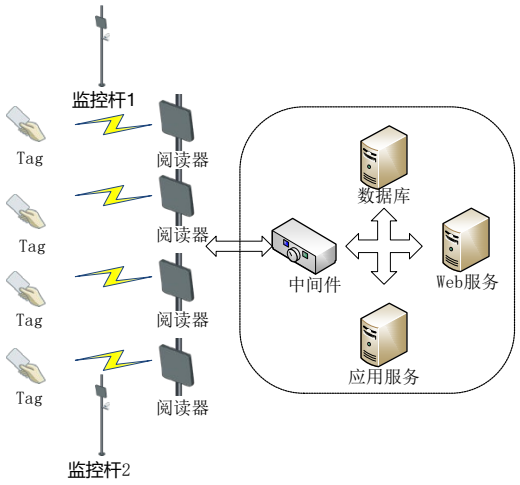



图11 RFID系统架构

该门禁系统具体配置如下：

1）EPC标准结构采用96位EPC编码，标头8位，EPC管理者代码28位，对象类别24位，系列号36位。

2）ISO15693标准，工作频率为13.56 Mhz±7 KHz。

3）高频阅读器型号为C5000W-A/C5000W-I系列。

4）安全协议为随机Hash Lock协议。

模型中部分过渡的发生概率如表12所示。

在PIPE[27]中建立RFID攻击模型，如图5所示。接着，根据表9，为每个变迁分配权重。为部分变迁设置$w=1$。在这种情况下没有时间转换，可以获得可达图、稳态分析和每个位置的平均令牌个数，此外，可达性图显示了该模型的无死锁有界稳态。

考虑到仿真时间和仿真结果的准确性，所设计的RFID攻击GSPN模型使用不同的初始随机点火次数（100、300、500、700、1000和1200）进行了50次模拟（一次点火过程表示模型中将有一个变迁满足可实施条件，消耗输入库所的令牌，并为输出库所产生令牌），最终再求解每个攻击的加权平均概率。

表13是仿真结果的一个示例。图12是不同的攻击概率在点火次数为100、300、500、700、1000和1200次时的仿真结果。其中，针对标签的攻击，包括移除、破坏、KILL，仿真结果均为0，在结果图中将不予显

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

示。根据实验结果，点火次数低于300时的攻击概率与高于300时的攻击概率有一定的出入。而普遍看来，欺骗攻击和中间人攻击这2种攻击的概率仍是最高的，均在4%~8%区间内浮动；DoS攻击的概率稳定在4%~5%区间；而Reader移除、销毁、无源干扰、重放攻击、加密攻击的概率则以2%为中心，小幅度浮动；有源干扰、流量分析、篡改攻击、注入恶意代码攻击则低于1%的概率。

**表12　变迁属性值**

| 变迁 | 属性 | | | 触发概率 |
|---|---|---|---|---|
| | 攻击成本 | 技术难度 | 发生几率 | |
| T1 | 1 | 1 | 1 | 0.2 |
| T2 | 1 | 2 | 1 | 0.167 |
| T3 | 2 | 3 | 2 | 0.089 |
| T6 | 2 | 3 | 3 | 0.078 |
| T7 | 3 | 3 | 3 | 0.067 |
| T8 | 3 | 3 | 2 | 0.078 |
| T13 | 2 | 2 | 2 | 0.1 |
| T14 | 3 | 3 | 3 | 0.067 |
| T18 | 4 | 4 | 4 | 0.05 |
| T19 | 3 | 3 | 3 | 0.067 |
| T20 | 4 | 4 | 4 | 0.05 |
| T21 | 3 | 4 | 4 | 0.056 |
| T22 | 3 | 4 | 4 | 0.056 |
| T16 | 4 | 5 | 5 | 0.043 |
| T32 | 3 | 5 | 5 | 0.049 |
| T33 | 3 | 3 | 3 | 0.067 |
| T25 | 3 | 4 | 5 | 0.052 |
| T26 | 3 | 5 | 4 | 0.052 |
| T24 | 5 | 5 | 5 | 0.04 |
| T10 | 3 | 5 | 5 | 0.049 |
| T11 | 4 | 5 | 4 | 0.047 |
| T27 | 2 | 5 | 5 | 0.06 |
| T28 | 2 | 5 | 5 | 0.06 |
| T30 | 5 | 5 | 5 | 0.04 |
| T31 | 3 | 5 | 5 | 0.049 |

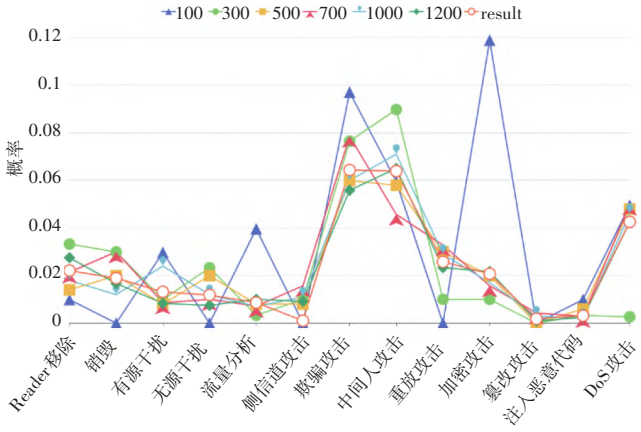



图12　100、300、500、700、1000和1200次点火次数下的令牌分布图

在第$i$次实验中，点火次数为$f_i$，攻击令牌$x$平均数量为$t_i(x)$，那么的加权概率如式(2)：

$$p(x)=\frac{\sum f_i t_i(x)}{\sum f_i} \tag{2}$$

加权概率如图13所示。

根据仿真结果，对系统威胁最大的2项攻击为欺骗攻击和中间人攻击。根据图12，当仿真点火次数较少(100次)时，加密攻击和流量分析的概率明显高于后续仿真点火次数较多的概率，说明点火次数较少的结果具有偶然性。使用加权概率进行计算后，加密攻击和流量分析的概率得到了明显的修正，符合实验预期。

**表13　使用PIPE对模型进行100次过渡点火和50次运行的模拟结果**

| 库所 | 令牌平均数量 | 95%置信区间 |
|---|---|---|
| Dos攻击 | 0.0495 | 0.05178 |
| KILL | 0 | 0 |
| Reader移除 | 0.0099 | 0.04066 |
| 侧信道攻击 | 0 | 0.03884 |
| 篡改攻击 | 0 | 0.01115 |
| 非法读取标签 | 0.0495 | 0.03013 |
| 干扰信道 | 0.0099 | 0.0409 |
| 感知层 | 0.09901 | 0.02291 |
| 攻击者 | 0.08911 | 0.00461 |
| 获取标签权限 | 0.0891 | 0.07533 |
| 加密攻击 | 0.11881 | 0.05367 |
| 监听信道 | 0.0396 | 0.09927 |
| 接近标签 | 0.08911 | 0.05193 |
| 接近阅读器 | 0.0396 | 0.12126 |
| 结束 | 0.64356 | 0.15443 |
| 流量分析 | 0.0396 | 0.03414 |
| 破坏 | 0 | 0 |
| 破解安全机制 | 0.05941 | 0.05111 |
| 欺骗攻击 | 0.0297 | 0.08016 |
| 窃听截获消息 | 0.0099 | 0.03587 |
| 手动操作标签 | 0 | 0 |
| 手动操作阅读器 | 0.0099 | 0.04803 |
| 网络传输层 | 0.13861 | 0.02567 |
| 伪装合法阅读器 | 0.15842 | 0.07395 |
| 无源干扰 | 0 | 0.02893 |
| 销毁 | 0 | 0.03768 |
| 修改标签内容 | 0.0099 | 0.01612 |
| 移除 | 0 | 0 |
| 应用层 | 0.34683 | 0.10982 |
| 有源干扰 | 0.0297 | 0.02689 |
| 中间人攻击 | 0.05941 | 0.07454 |
| 重放攻击 | 0 | 0.03877 |
| 注入恶意代码 | 0.0099 | 0.01164 |

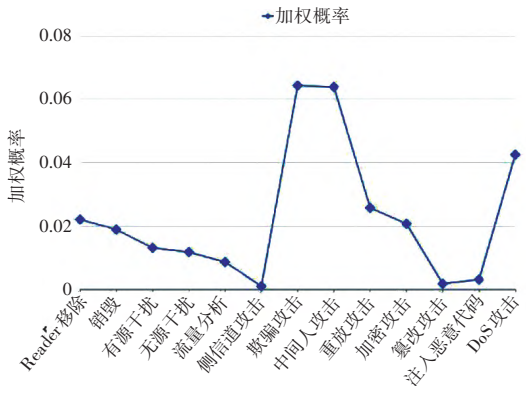
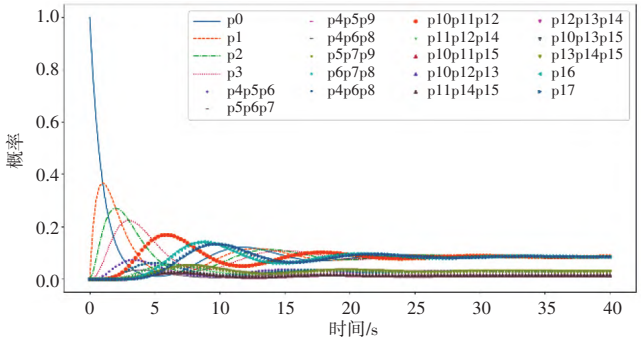


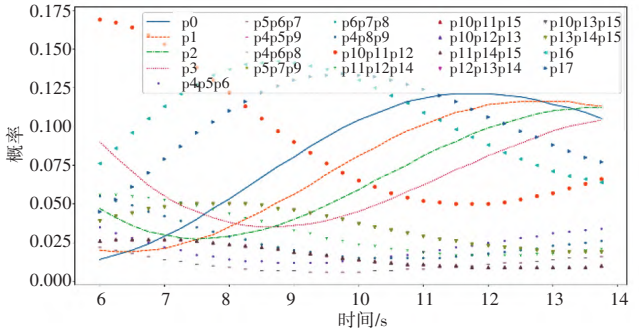

图13　加权攻击概率

对文献[12]中的基于广义随机着色Petri网的网络攻击组合模型(GSCPN)进行分析，结果如图14和表14所示。

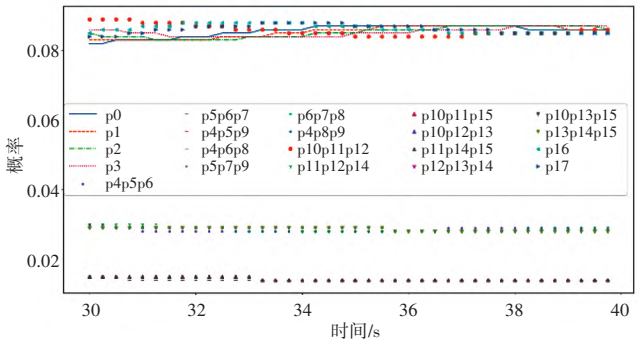
(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net




（a）0~40 s GSCPN模型稳态概率




（b）6~14 s GSCPN模型稳态概率




（c）30~40 s GSCPN模型稳态概率

图14 GSCPN模型稳态概率

**表14 实验结果表**

| 模型 | 库所数量/个 | 状态数量/个 | 状态间变迁数量/个 | 稳态求解时间/s |
|---|---|---|---|---|
| AASPN | 34 | 158 | 343 | 3.5 |
| GSCPN | 18 | 22 | 32 | 38.1 |

根据表14可知，本文所建立的模型虽然在库所数量、状态数量和状态间变迁数量上明显高于GSCPN模型，并且在稳态概率求解上所花费的时间明显优于GSCPN模型，其效率高于GSCPN模型一个数量级。根据图14可知，GSCPN模型在进行稳态概率求解时，不同状态的概率随时间呈上下波动形变化，很大一部分时间耗费在了对概率值进行收敛的过程。实验结果表明，本文所建立的模型中不同状态的概率值可以在短时间内迅速达到收敛，时间效率上优于GSCPN模型。

## 4 结束语

本文针对RFID系统安全分析工作的需求，以攻击者的视角分析并建立RFID攻击模型。首先给出了随机Petri网的RFID系统安全性分析模型的定义，主要包括3个不同的层次：顶层父Petri网、权限子网和基于权限的攻击子网。然后研究分析了RFID不同的攻击方式之间的关联关系，根据这些关系提出了RFID攻击权限提升模式。基于随机Petri网的RFID系统安全性分析模型可以对RFID攻击在逻辑层面的关联性、协作性和在事件层面的并发性进行很好表述。最后对模型的性能进行了分析，通过多属性效用理论分析RFID攻击中的风险分数，将其转换成概率设置为变迁参数，从建模分析的效果来看，本文所建立的模型中稳态求解时间效率优于一般的Petri网模型一个数量级，本文提出的安全评估模型是有效可行的。下一步工作就是对本文所建立的模型参数进行优化，使其更具有准确性和通用性。

**参考文献：**

[1] 高通. RFID安全认证协议的研究[D]. 呼和浩特:内蒙古大学, 2017.
[2] 肖亮. RFID系统的轻量级安全认证协议研究与设计[D]. 南京:南京邮电大学, 2021.
[3] 魏忠. 基于本体的网络攻击建模与分析方法研究[D]. 上海:上海交通大学, 2018.
[4] 乐成利,高秀峰. 基于Perti网的移动AdHoc网络改进攻击网建模方法研究[J]. 兵器装备工程学报, 2020,41(4):148-155.
[5] 李辉,侯义斌,黄樟钦,等. 一种智能攻击模型在RFID防伪协议中的研究[J]. 电子学报, 2009,37(11):2565-2573.
[6] 李俊霖,周华,夏金虎,等. 物联网安全协议攻击者模型形式化构建研究[J]. 云南大学学报(自然科学版), 2013,35(S2):147-151.
[7] 黄义夫. RFID系统安全检测关键技术研究[D]. 成都:电子科技大学, 2014.
[8] 杨晓明. RFID攻击建模及安全技术研究[D]. 成都:电子科技大学, 2015.
[9] WANG Y S, SHEN J J, GUO X F, et al. Research on RFID attack methods[C]// 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE). 2020:433-437.
[10] AI X, CHEN H L, LIN K, et al. Nowhere to hide: Efficiently identifying probabilistic cloning attacks in large-scale RFID systems[J]. IEEE Transactions on Information Forensics and Security, 2021,16:714-727.
[11] CHEN T M, SANCHEZ-AARNOUTSE J C, BUFORD J. Petri net modeling of cyber-physical attacks on smart grid[J]. IEEE Transactions on Smart Grid, 2011,2(4):741-749.
[12] 高翔,祝跃飞,刘胜利. 一种基于广义随机着色Petri网的网络攻击组合模型[J]. 电子与信息学报, 2013,35(11):2608-2614.
[13] ALMUTAIRI L M, SHETTY S. Generalized stochastic Petri Net model based security risk assessment of software defined networks[C]// IEEE Military Communications Conference (MILCOM). 2017:545-550.
[14] ALMUTAIRI L M, HONG L, SHETTY S. Security analysis of multiple SDN controllers based on stochastic Petri nets[C]// 2019 Spring Simulation Conference (SpringSim). 2019:1-12.
[15] 毋泽南,田立勤,陈楠. 基于随机Petri网的系统安全性量化分析研究[J]. 信息网络安全, 2020,20(9):27-31.
[16] HE L, REN Q, MA B, et al. Anti-attacking modeling and analysis of cyberspace mimic DNS[J]. China Communications, 2022,19(5):218-230.
[17] 李鹏,郑田甜,徐鹤,等. 基于区块链技术的RFID安全认证协议[J]. 信息网络安全, 2021,21(5):1-11.
[18] 雷璨,陈治宇. 基于RFID的物联网轻量级安全认证方案[J]. 电子技术与软件工程, 2021(24):252-254.
[19] 王小骥,杨竞,刘瑶,等. 基于PUF的轻量级RFID安全认证协议[J]. 信息安全与通信保密, 2022(1):74-80.
[20] 翟禹尧,史贤俊,秦玉峰,等. 基于层次广义随机Petri网的测试性建模新方法[J]. 兵工学报, 2020,41(1):161-170.
[21] 崔文岩,孟相如. 基于层次Petri网的信息物理融合系统安全博弈建模[J]. 计算机应用研究, 2017,34(8):2439-2442.
[22] MITROKOTSA A, RIEBACK M R, TANENBAUM A S. Classifying RFID attacks and defenses[J]. Information Systems Frontiers, 2010,12(5):491-505.
[23] 王振,杜玉越,亓亮. 扩展颜色逻辑Petri网及其可达性分析[J]. 山东科技大学学报(自然科学版), 2020,39(3):84-98.
[24] 韩耀军. 基于带标记的并发可达标识图的关键路径的求解方法[J]. 计算机科学, 2016,43(11):121-125.
[25] 何炎祥,沈华. 随机Petri网模型到马尔可夫链的转换规则与实现[J]. 计算机科学与探索, 2013,7(1):55-62.
[26] RAHULAMATHAVAN Y, RAJARAJAN M, RANA O F, et al. Assessing data breach risk in cloud systems[C]// 2015 IEEE 7th International Conference on Cloud Computing Technology and Science. 2015:363-370.
[27] DUBA D. Refitting PIPE: Extending the Petri Net Tool PIPE 5[R]. Leiden: Leiden University, 2016.

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net