基于贝叶斯攻击图的 RFID 系统安全评估模型

马荟平[1],李 鹏[1,2],肖 航[1],朱 枫[1,2]
(1. 南京邮电大学 计算机学院,江苏 南京 210023;
2. 江苏省无线传感网络高技术研究重点实验室,江苏 南京 210023)

摘 要:针对目前 RFID(Radio Frequency Identification,射频识别技术)系统安全分析中忽略攻击事件对系统安全状态动态影响的问题,为了有效实现 RFID 系统的安全风险评估,文章提出了一种基于贝叶斯攻击图的 RFID 系统安全评估模型。该模型首先通过对 RFID 系统结构、所用协议进行分析确定系统的脆弱性漏洞及其依赖关系,建立攻击图。针对攻击图模型只能进行定性分析的问题,构建出相应的攻击图模型结构后可以结合贝叶斯理论对其进行量化。依据漏洞的利用难易度和影响程度建立 RFID 漏洞量化评价指标,计算出对应的原子攻击概率,然后以条件转移概率的形式将攻击节点与 RFID 系统的安全属性节点联系在一起,不仅能推断攻击者能够成功到达各个属性节点的风险概率,而且能够依据攻击者的不同行为动态展示系统风险状况的变化,实现评估不同状态下目标 RFID 系统的整体风险状况。实验表明,所提模型可以有效地计算出 RFID 系统整体的风险概率,为后续实施对应的安全策略提供理论依据。

关键词:贝叶斯;射频识别技术;攻击图;原子攻击;属性节点;安全评估
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2024)02-0113-07
doi:10.3969/j.issn.1673-629X.2024.02.017

RFID System Security Evaluation Model Based on Bayesian Attack Graph

MA Hui-ping[1],LI Peng[1,2],XIAO Hang[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,Nanjing 210023,China)

Abstract:Aiming at the problem of ignoring the dynamic influence of attack events on the system security state in the current RFID system security analysis,in order to effectively realize the security risk assessment of RFID system,we propose a security assessment model of RFID system based on Bayesian attack graph. The model firstly determines the vulnerability and dependence of the system by analyzing the RFID system structure and the protocol used,and establishes the attack diagram. For the problem that the attack graph model can only be qualitatively analyzed,the corresponding attack graph model structure can be quantified by combining Bayes theory. The RFID vulnerability quantitative evaluation index is established according to the exploit difficulty and impact degree of the vulnerability,the corresponding atomic attack probability is calculated,and then the attack node is associated with the security attribute node of the RFID system in the form of conditional transfer probability,which can not only infer the risk probability that the attacker can successfully reach each attribute node. Moreover,it can dynamically display the changes of the system risk status according to the different behaviors of the attacker,and realize the overall risk status of the target RFID system under different states. The experiment shows that the proposed model can effectively calculate the risk probability of the whole RFID system,and provide a theoretical basis for the subsequent implementation of the corresponding security strategy.

Key words:Bayesian;radio frequency identification;attack graph;atomic attack;attribute node;security evaluation

0 引 言

随着信息化的发展,基于 RFID 的信息系统大量出现,RFID 技术开始应用在社会的各行各业中。然而使用 RFID 技术给人们的生活带来便利的同时,RFID

收稿日期:2023-06-01 **修回日期**:2023-10-09
基金项目:国家自然科学基金(61872196,61872194,61902196);江苏省科技支撑计划项目(BE2019740,BK20200753,20KJB520001);江苏省高等学校自然科学研究重大项目(18KJA520008);江苏省六大人才高峰高层次人才项目(RJFW-111)
作者简介:马荟平(1998-),男,硕士研究生,研究方向为物联网安全;通信作者:李 鹏(1979-),男,博士,教授,CCF 会员(48573M),研究方向为网络安全。

系统内存在的诸多安全问题和安全隐患也日益突出。如何解决 RFID 系统的安全隐患[1],已经成为目前研究的热点。

目前大多数有关 RFID 安全的研究均围绕着安全认证协议这一领域进行[2],但是由于 RFID 标签本身计算能力的限制,大多安全认证协议不能实现大规模应用。不断改进 RFID 的认证协议是从防守的角度解决问题。除此之外,还可以尝试从攻击者的角度解决问题[3]:基于攻击模型对 RFID 系统进行安全性评估,通过主动地在威胁攻击发生之前评估网络或 RFID 信息系统中存在的安全隐患[4],提高 RFID 系统的安全性。例如,李景等[5]在文章中从标签端、阅读器、中间件以及后台服务器四个方面归纳了 RFID 的潜在安全问题,提出一种基于攻击树的 RFID 系统安全策略。杨晓明等[6]针对不同 RFID 通信协议进行安全检测,基于多决策树构建了 RFID 系统漏洞攻击模型,依据发掘出的漏洞信息提出了多种 RFID 漏洞检测算法。

同时,该文尝试结合传统计算机网络中的安全评估方法,通过主动地在威胁攻击发生之前评估 RFID 信息系统中存在的安全风险和安全隐患攻击,建立面向 RFID 的安全评估模型[7-9]。在传统网络中基于攻击图模型的安全评估方法较为成熟,攻击图是一种由节点和有向边组成的有向图,可以从攻击者的角度直观地、图形化地展示攻击行为[10-13]。杨英杰等[14]基于属性攻击图理论构建了一种针对传统计算机网络的动态威胁风险分析模型,根据网络中的漏洞信息和协议信息提出了动态威胁属性攻击图生成算法,在复杂网络中具有更好的适应性。Wu Hua 等[15]通过分析攻击者的攻击能力、网络资源和脆弱性因素的相关性建立了贝叶斯攻击图,实现了对网络攻击有效性的评估和对后续攻击路径的推测。周余阳等[16]基于贝叶斯攻击图建立了一种动态网络入侵意图分析模型,用来应对安全要素不断变化的复杂网络,提高了风险评估的准确性。顾士星等[17]基于生成的贝叶斯攻击图模型,提出使用团树的方式对贝叶斯网络进行推理,降低了计算复杂度。

基于上述研究可以看出,目前针对 RFID 系统构建的攻击模型比较缺乏相应的定量分析,也就是说不能较为明确和直观地观察系统脆弱性分析结果。同时部分研究中没有体现出 RFID 系统中多种原子漏洞之间的因果联系,忽视了漏洞攻击事件对 RFID 系统安全状态的动态影响。由于贝叶斯网络结合了图形结构以及条件概率集合,因此使用该方法不仅能够很好地描述 RFID 漏洞之间的依赖关系,同时也可以进行后续的概率量化评估。因此,该文提出了一种基于贝叶斯攻击图的 RFID 系统脆弱性评估模型,主要工作如下:

(1)基于 RFID 系统中存在的漏洞和脆弱因素构建 RFID 原子攻击库,确定原子攻击库中各脆弱性漏洞的依赖关系,建立基于贝叶斯攻击图的 RFID 系统攻击模型。

(2)基于 CVSS 评分系统提出了针对 RFID 系统的量化评估模型,对 RFID 原子攻击概率进行估算,然后结合 RFID 系统攻击模型计算属性节点的可达概率,对 RFID 系统的风险状况进行评估。

1 相关技术

1.1 贝叶斯攻击图

贝叶斯攻击图(Bayesian Attack Graph,BAG)是由节点和有向边构成的一个有向无环图,可将贝叶斯攻击图表示为:BAG=(S,A,E,P)。其中 S 表示属性节点集合,A 表示原子攻击集合,E 表示攻击图的有向边集合,P 代表攻击图中各属性节点的概率集合,具体定义如下:

(1) $A=\{A_i \mid i=1,2,\cdots,n\}$ 且 $A \in S \times S$,其中 A_i 代表攻击者利用系统漏洞进行的一次攻击,由此导致了属性节点的转换和迁移,因此有 $\forall a \in A, a=S_{pre}(a) \rightarrow S_{post}(a)$,其中 $S_{pre}(a)$ 代表原子攻击 a 的起始节点,$S_{post}(a)$ 代表原子攻击 a 的终止节点。

(2) $S=S_{start} \cup S_{mid} \cup S_{final}$,其中,$S_{start}$ 代表攻击者的初始状态节点或是攻击的起始节点,S_{mid} 代表攻击者的中间状态节点或是攻击的中间过程节点,S_{final} 代表攻击者的目标状态节点或是攻击的终止节点。对于任意的属性节点 S_i 均包含 $S_i=1$ 或 $S_i=0$ 两种状态,$S_i=1$ 代表攻击者已经成功实施相应的原子攻击占用了当前属性节点,$S_i=0$ 代表该节点还未被攻击者成功利用。

(3) $E=\{E_i \mid i=1,2,\cdots,n\}$ 为攻击图的有向边集合,$\forall S_i \in S_{mid} \cup S_{final}$,有 $S_k \in S$ 满足(S_k , S_i) $\in E$,表示存在一条以 S_k 为起点,以 S_i 为终点的有向边。

(4) P 代表攻击图中各属性节点的可达概率集合,$\forall S_i \in S$,P (S_i)代表状态节点 $S_i=1$ 时的可达概率。

1.2 贝叶斯攻击图结构

贝叶斯攻击图的结构类似于攻击图的结构,攻击图一般可以分为状态攻击图和属性攻击图。为避免了状态攻击图状态爆炸的问题,该文借鉴了属性攻击图的结构构建贝叶斯攻击图。

属性攻击图中通常包含两种节点:第一种节点为属性节点,代表系统中的具体资源属性,在攻击图中表示为方形节点;第二种为攻击节点,代表攻击者的具体

原子攻击,在攻击图中用圆形节点。

1.3　RFID 原子攻击

为构建针对 RFID 系统的贝叶斯攻击图,首先需调研现有的各种不同类型的 RFID 攻击,构建 RFID 系统的原子攻击库。该文总结各种 RFID 原子攻击,包括窃听、重放、鉴别数据包、克隆复制卡片、假冒攻击、信息篡改、边信道攻击[18]。

在确定 RFID 系统中存在的各种攻击手段后,可将单一的原子攻击事件 $a \in A$ 定义如下:

$$a = (\text{Att\_name}, \text{Att\_pre}, \text{Att\_next}, \text{Att\_ability})$$

其中,Att_name 代表该原子攻击的名称,Att_pre 代表为实现该攻击所需的前提条件或前序原子攻击,Att_next 代表只有在实现当前攻击后才能进行的下一步攻击,Att_ability 代表攻击者在成功实施该原子攻击后所能达到的结果,可以视作该攻击的结果属性,即攻击者在实现该原子攻击后所获得的新的攻击能力。

基于 RFID 系统内存在的各种攻击手段和相关攻击规则可构建针对 RFID 系统的原子攻击库,根据攻击库中各攻击之间的先后关系可以确定贝叶斯攻击图中原子攻击节点和属性节点之间的关系,从而确定贝叶斯攻击图的网络结构。

2　RFID 安全评估模型

2.1　贝叶斯攻击图生成

假定攻击者是聪明并且贪心的,因此攻击者必然会利用目标 RFID 系统中存在的漏洞发起攻击,且在攻击成功后必然会获得一定的系统资源有助于发起下一次的攻击。

将起始点设置为攻击者的初始状态,攻击者在此状态时所具有的攻击能力是最低级的攻击能力。每当攻击者成功实施上述攻击并获得一定的计算资源提升其攻击能力后,就把这个提升后的状态看作新的状态点。基于这种攻击者实施各种攻击并且提升其攻击能力直至达到目标的思想可以构建出 RFID 系统的贝叶斯攻击图模型,攻击者的状态和攻击行为构成了贝叶斯攻击图模型中的节点,攻击者每实施一次实例攻击行为都导致了攻击者状态的变迁,对应了贝叶斯攻击图模型中的边关系。

贝叶斯攻击图的构建流程如下:

(1)依据 RFID 攻击库中的信息,获取目标 RFID 系统中的漏洞信息,初始攻击者信息,将攻击者可能的各种实例攻击行为加入到攻击队列中;

(2)判断攻击队列是否为空,若不空,则进行下一步;若为空,生成最终的贝叶斯攻击图,转第 6 步;

(3)扫描攻击队列,查看攻击队列中各个实例攻击行为的前置条件或是发起该攻击行为所需的计算资源;

(4)查看是否存在攻击前提已经被满足的实例攻击行为,若存在,则进行下一步;若不存在则重新读取 RFID 攻击库,更新攻击队列,转第 2 步;

(5)攻击者发起满足条件的实例攻击行为,将该实例攻击行为作为新的原子攻击节点,将相应获得的计算资源作为节点,将该攻击事件作为边更新;

(6)得出最终的贝叶斯攻击图。

2.2　RFID 漏洞量化

2.2.1　原子攻击节点概率

为利用贝叶斯攻击图实现对 RFID 系统的脆弱性评估,在构建出针对 RFID 系统的贝叶斯攻击图的基础上,需对贝叶斯攻击图中的各个原子攻击进行分级评估并量化。在传统网络中,一般采用美国国家通用漏洞数据库(National Vulnerability Database,NVD)提供的通用漏洞评分系统(Common Vulnerability Scoring System,CVSS)进行量化。CVSS 能提供完整的评分参数和开放的评分框架,量化漏洞被利用的难易程度。该文借鉴 CVSS 评分系统的量化标准,在参考文献[19]的基础上结合 RFID 漏洞利用所需权限的思想,从利用难易度和影响程度对 RFID 系统中的漏洞进行量化。利用难易度可分为访问途径(AV)、访问复杂度(AC)、权限(PR),影响度包括机密性(CI)、完整性(IN)和可用性(AI),如表 1 所示。

表 1　指标描述

指标	等级	描述	评分
访问复杂度(AC)	简单	无需借助外部条件	0.71
	一般	介于简单和复杂之间	0.61
	复杂	需要借助外部条件,如需要大量的解密运算,反复的发送阻塞信号	0.35
访问路径(AV)	控制 RFID 系统环境	攻击者需对 RFID 信道中传送的消息进行读取,如:窃听、阻截等	0.85
	控制 RFID 会话实体	表示攻击者需要拥有合法实体的身份、密钥并且完成合法实体能进行的协议运算以及控制合法实体发起会话	0.62
	破译 RFID 协议口令	攻击者需利用安全协议对协议中所使用的弱口令或弱密钥进行破译并验证,实际上是暴力破解的攻击方式	0.55
	协议密码分析	指攻击者掌握了协议密码算法的核心内容,能够对传输密文进行分析判断并破译	0.2

续表 1

指标	等级	描述	评分
权限（PR）	无	攻击者在攻击前是未经授权的	0.85
	低	攻击者在发起攻击前只具有低级权限，可以访问非敏感信息	0.62
	高	攻击者利用该漏洞需要提供访问权限，进行多次认证	0.27
影响程度	轻微影响	安全漏洞对 RFID 系统保密性、完整性和可用性影响轻微；攻击者有能力对 RFID 通信进行监听	0.56
	部分影响	安全漏洞对 RFID 系统保密性、完整性和可用性影响相对较轻；攻击者有能力分辨窃听到的命令包的类型，有能力辨别命令包中各数据段的信息	0.22
	完全影响	安全漏洞对 RFID 系统的保密性、完整性以及可用性的影响较严重，攻击者有能力复制或篡改目标信息	0

基于上述指标和评分计算漏洞价值的计算式如下所示：

$$\text{BaseScore} = \min(\text{Exp} + \text{Impact}, 10) \tag{1}$$

$$\text{Impact} = 6.4 \times (1 - (1 - \text{CI}) \times (1 - \text{IN}) \times (1 - \text{AI})) \tag{2}$$

$$\text{Exp} = 8.22 \times \text{AC} \times \text{AV} \times \text{PR} \tag{3}$$

漏洞价值表示攻击者利用某一漏洞的可能性大小，即上述的 BaseScore 值，基于该值可计算出攻击者利用某一属性节点对其后续节点成功攻击的概率，即某一原子攻击节点的概率。由于按照上述评分系统计算出的值范围是[0,10]，为了后续的概率计算，需进行一定的缩放，因此原子攻击节点 $a_i \in A$ 的概率计算式为：

$$P(a_i) = \frac{\text{BaseScore}}{10} \times 100\% \tag{4}$$

2.2.2 属性节点可达概率

贝叶斯攻击图一般都描述了攻击者通过多步攻击最终实现目标的攻击行为，所以需要依据父节点与子节点之间的关系，计算某属性节点在其父节点影响下被攻击者成功利用的概率，即其对应的条件概率，表示为 $P(S_j \mid \text{Par}(S_j))$。由于子节点 S_j 与父节点 $\text{Par}(S_j)$ 之间存在两种关系："或"关系和"与"关系，故分两种情况讨论。

(1)若为"或"关系，则有：

$$P(S_j \mid \text{Par}[S_j]) = \begin{cases} 0 & \forall S_k \in \text{Par}[S_j], S_k = 0 \\ 1 - \prod_{S_k=1} (1 - P(a_k)) & \text{其它} \end{cases} \tag{5}$$

(2)若为"与"关系，则有：

$$P(S_j \mid \text{Par}[S_j]) = \begin{cases} 0 & \exists S_k \in \text{Par}[S_j], S_k = 0 \\ \prod_{S_k=1} P(a_k) & \text{其它} \end{cases} \tag{6}$$

依据父节点与子节点之间的关系，计算某属性节点对应的条件概率之后，就可得出该属性节点的静态可达概率，从该概率中可观察到对应 RFID 系统的静态风险情况，具体计算式如下：

$$P(S_j) = \prod_{i=1}^{j} P(S_i \mid \text{Par}[S_i]) \tag{7}$$

假设攻击者已经成功实现了某一原子攻击，即对应的属性节点 $S_j = 1$，则利用后验概率公式将属性节点 S_i 的动态到达概率表示为 $P(S_i \mid S_j)$，计算式如下：

$$P(S_i \mid S_j) = \frac{P(S_j \mid S_i) \times P(S_i)}{P(S_j)} \tag{8}$$

2.3 基于贝叶斯攻击图的 RFID 系统风险评估

基于 2.2 节计算出的 RFID 原子攻击节点量化概率和属性节点的可达概率，在无额外推理条件的情况下可进行静态的 RFID 风险状况评估，主要过程如下：

(1)基于表 1 量化原子攻击漏洞。

(2)基于式 5 和式 6 结合攻击模型计算条件概率表，然后依据式 7 更新图中各属性节点的可达概率。

(3)得出目标节点的可达概率，评估静态状况下的系统风险状况。

但是 RFID 系统的风险状态不会一直保持静态，当系统中的任何漏洞被攻击者成功利用后都会影响到模型中各属性节点的静态可达概率，因此当管理员观察到攻击者的攻击结果后需依据式 8 及时更新系统风险状况。

3 模型验证

3.1 实验设置

为了建立基于贝叶斯攻击图的 RFID 风险评估模型，该文针对如图 1 所示的某仓储 RFID 信息管理系统进行分析。

3.2 贝叶斯攻击图生成

图 2 为针对目标 RFID 系统安全评估建立的贝叶斯攻击图。

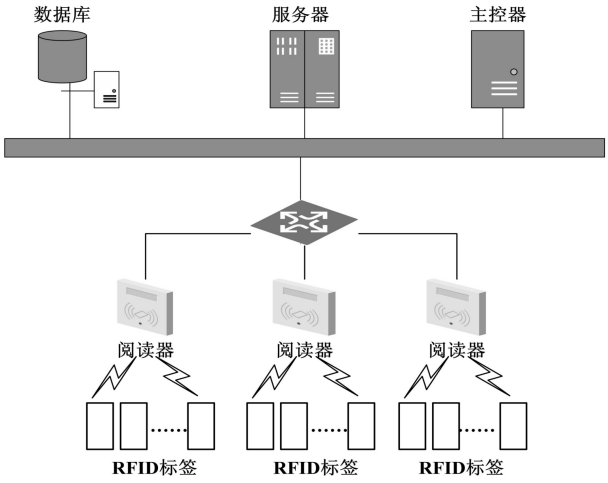

图 1　实验 RFID 系统结构

(1)攻击者可以通过未经授权的 RFID 阅读器强行读取标签,造成标签 ID 信息泄露,并复制克隆标签隐私信息获取目标系统的访问权限发起假冒攻击,篡改系统隐私数据。攻击者同样可以通过监听信道窃取到标签的隐私信息,依据上述攻击过程发起攻击。

(2)若攻击者可以监听信道,则可以通过窃听标签读写器发送的命令,获取到 RFID 读写器发送的各种命令包,然后可以按照标准协议命令包头定义的格式用来辨别命令包的类型,实现对敏感数据包的窃取或是发起重放攻击。

(3)攻击者可以发起 DOS 攻击,通过一些射频信号装置短时间内向阅读器端发送大量非法标签信息,导致 RFID 系统被大量信息淹没,系统中的阅读器无法与合法标签进行正常读写操作,阻塞通信信道,破坏 RFID 系统的可用性。

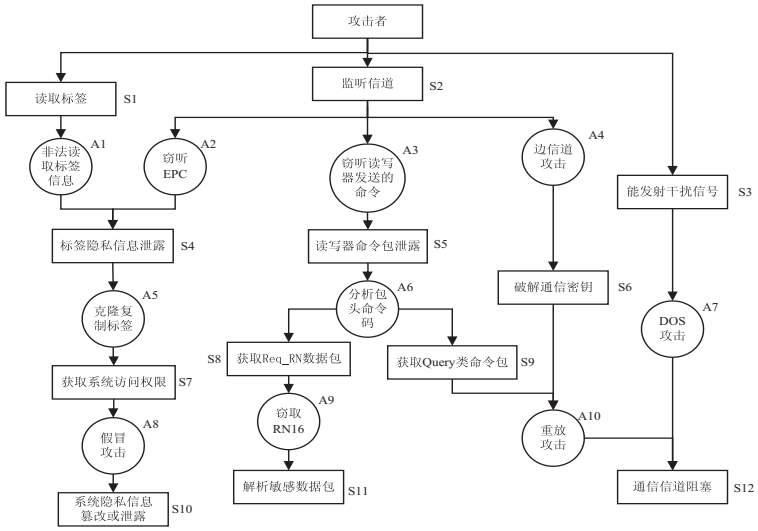

图 2　RFID 贝叶斯攻击模型

3.3　风险计算

依据 2.2 节所述的评分标准,首先对上述 RFID 贝叶斯攻击模型中的原子攻击节点进行概率量化。

依据表 2 所述的对各种原子攻击的分级标准可计算出各个原子攻击的概率,如图 3 所示。

根据表 2 所给定各攻击节点的成功利用概率可以对属性节点进行概率量化,首先计算攻击者到某一属性节点的静态可达概率表,其中将外部属性节点 S1,S2,S3 的静态概率初始化为 0.8。

表 2　RFID 原子攻击分级

原子攻击	攻击编号	危害程度			
		访问路径(AV)	访问复杂度(AC)	权限(PR)	影响程度
非法读取信息	A1	控制 RFID 协议会话实体	一般	无	部分影响
窃听攻击	A2、A3	控制 RFID 网络环境	复杂	无	部分影响
边信道攻击	A4	密码分析	复杂	无	部分影响
克隆复制标签	A5	控制 RFID 网络环境	复杂	低	部分影响
分析包头命令码	A6	控制 RFID 网络环境	复杂	低	部分影响
DOS 攻击	A7	控制 RFID 网络环境	一般	低	完全影响
假冒攻击	A8	控制 RFID 网络环境	复杂	高	完全影响
窃取 RN16	A9	控制 RFID 网络环境	复杂	高	完全影响
重放攻击	A10	控制 RFID 网络环境	一般	高	完全影响

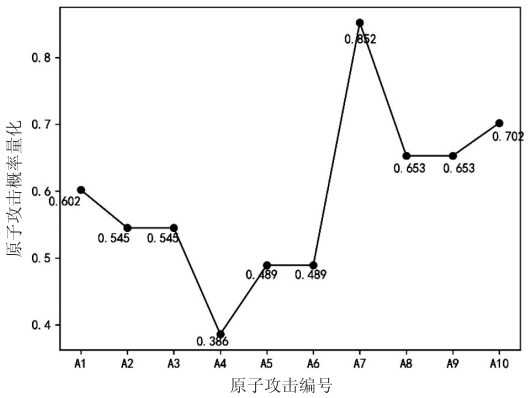

图 3 原子攻击概率

基于图 2 所示的图形结构和上述的可达概率计算过程,使用 Netica 工具集可构建出如图 4 所示的贝叶斯模型。

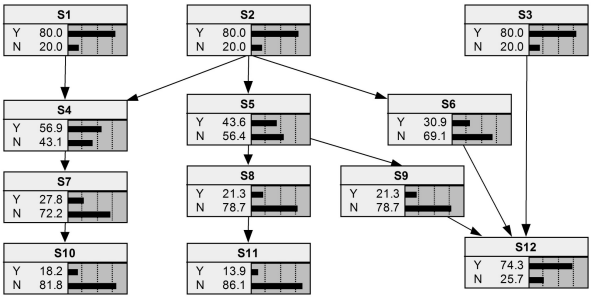

图 4 针对 RFID 系统的静态贝叶斯评估模型

图 4 可以直观展示出在无额外推理条件的情况下,攻击者可成功占用各个属性节点的成功概率,即该系统的静态风险状况。其中目标节点为 S10,S11,S12,攻击者可以成功占领各目标节点的概率分别为 18.2%,13.9%,74.3%,可以看出攻击者到达 S12 节点的概率最高,即攻击者更易实现的攻击结果为通过 DOS 攻击或者重放攻击阻塞 RFID 系统的通信信道。

RFID 系统的风险状态不会一直保持静态,需要考虑到攻击者的不同攻击行为对 RFID 系统安全状况造成的动态影响。在图 4 所示推理模型的基础上,若是系统管理员确认了攻击者的攻击目标或者观测到系统中已经发生的攻击行为,可按照式 8 所述的后验概率计算公式对部分属性节点概率进行更新。结果如图 5 所示。

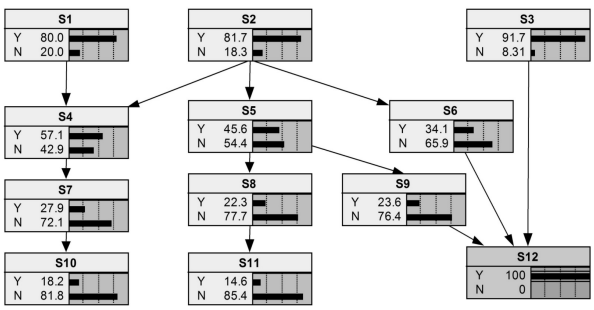

图 5 基于攻击者目标节点的动态概率评估

也可结合系统的实时安全事件对模型及节点可达概率进行动态更新,可以更好地反映 RFID 系统的风险状况。例如若是管理员观测到图 2 中的攻击事件 A3,则将节点 S5 的概率置为 1,同时更新其余节点的可达概率,结果如图 6 所示。

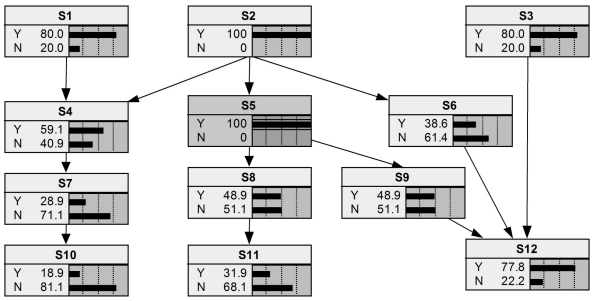

图 6 基于系统安全事件的动态概率评估

在图 5 所示的情况下,在已知攻击者目标节点为 S12 时,可以看出属性节点 S3,S6,S9 的攻击者可达概率有明显提升。在图 6 所示的情况下,攻击者已经成功实施原子攻击 A3 后,目标节点 S11 和 S12 的安全风险显著增加,通过这种动态更新系统可达概率的方式,也可以为预测攻击者的下一步攻击或是攻击目标提供依据。

3.4 方法对比

在基于贝叶斯攻击图的脆弱性评估方式中,模型中各属性节点的可达概率是反映 RFID 系统风险的主要指标。为了验证所提的 RFID-BAG-ATT 模型,在同样的系统实验环境下,给出了与文献[20]所提出的 DRABAG 模型的实验数据对比,如图 7 所示。图 7 给出了在图 1 所示的 RFID 系统环境下,RFID-BAG-ATT 模型和 DRABAG 模型对于贝叶斯攻击图中原子攻击节点的量化结果。

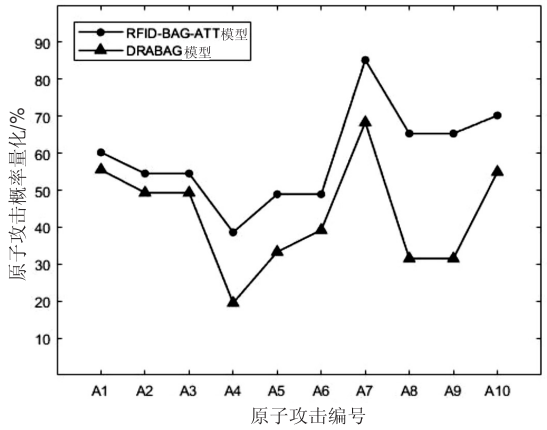

图 7 原子攻击概率量化对比

基于参考文献所提出的 DRABAG 模型以及上述量化概率可以构建出图 8 所示的量化结果图。

对比图 4 和图 8,观察图中所示的属性节点可达概率,可以看出 RFID-BAG-ATT 模型优于 DRABAG

模型,这是因为该模型在多个方面对原子攻击概率进行量化,评估更加准确。

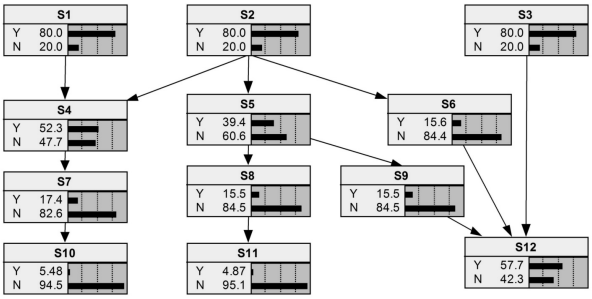

图 8　原子攻击概率量化对比

4　结束语

针对目前 RFID 系统面临的诸多安全问题和安全隐患,尝试从攻击者的角度建立起针对 RFID 系统的贝叶斯攻击图模型。首先,归纳总结了 RFID 系统内常见的各种攻击手段,建立 RFID 攻击库。然后,重点介绍了 RFID 贝叶斯攻击图模型的建立,在得出攻击图模型的基础上提出了针对 RFID 攻击的分级量化标准,得到原子攻击概率。通过原子攻击概率计算出贝叶斯攻击图中属性节点的静态可达概率和动态可达概率,从而衡量出 RFID 系统的风险状况。

在实际的 RFID 系统中,系统管理者也可能会根据攻击者的攻击进度选择相应的防御策略,所以如何优化 RFID 系统风险评估模型使其可以在复杂的情况下准确地评估出系统的风险状况将成为下一步的研究重点。

参考文献:

[1] HE Wenji,LIU Yifeng,YAO Haipeng,et al. Distributed variational Bayes-based in-network security for the internet of things[J]. IEEE Internet Things J.,2021,8(8):6293-6304.

[2] 黄可可. 面向物联网的 RFID 安全认证协议研究[D]. 扬州:扬州大学,2020.

[3] WU Tianshui,ZHAO Gang. A novel risk assessment model for privacy security in internet of things[J]. Wuhan University Journal of Natural Sciences,2014,19(5):398-404.

[4] 张　凯,刘京菊. 基于漏洞动态可利用性的网络入侵路径分析方法[J]. 信息网络安全,2021,21(4):62-72.

[5] 李　景,戴　桦. 射频识别系统的安全与检测方法研究[J]. 网络空间安全,2017,8(12):85-90.

[6] 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.

[7] 叶子维,郭渊博,王宸东,等. 攻击图技术应用研究综述[J]. 通信学报,2017,38(11):121-132.

[8] 王　洋,吴建英,黄金垒,等. 基于贝叶斯攻击图的网络入侵意图识别方法[J]. 计算机工程与应用,2019,55(22):73-79.

[9] 刘威歆. 基于攻击图的 APT 攻击检测和威胁评估研究[D]. 北京:北京邮电大学,2017.

[10] 李　欢. 基于贝叶斯网络攻击图的动态风险评估方法研究[D]. 秦皇岛:燕山大学,2019.

[11] JIAO Jian,WEI Mengwei,YUAN Yuan,et al. Risk quantification and analysis of coupled factors based on the Dematel model and a Bayesian network[J]. Applied Sciences,2020,10(1):317-337.

[12] MUÑOZ-GONZÁLEZ L,SGANDURRA D,BARRÈRE M,et al. Exact inference techniques for the analysis of Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing,2019,16(2):231-244.

[13] 罗智勇,杨　旭,刘嘉辉,等. 基于贝叶斯攻击图的网络入侵意图分析模型[J]. 通信学报,2020,41(9):160-169.

[14] 杨英杰,冷　强,常德显,等. 基于属性攻击图的网络动态威胁分析技术研究[J]. 电子与信息学报,2019,41(8):1838-1846.

[15] WU Hua,GU Yu,CHENG Guang,et al. Effectiveness evaluation method for cyber deception based on dynamic Bayesian attack graph[C]//2020 3rd international conference on computer science and software engineering. Beijing:ACM,2020:1-9.

[16] 周余阳,程　光,郭春生. 基于贝叶斯攻击图的网络攻击面风险评估方法[J]. 网络与信息安全学报,2018,4(6):11-22.

[17] 顾士星. 基于贝叶斯网络攻击图的安全分析算法的研究[D]. 镇江:江苏大学,2017.

[18] 朱珊珊. 物联网中 RFID 安全认证方法研究[D]. 西安:西安电子科技大学,2020.

[19] 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.

[20] 高　妮,高　岭,贺毅岳,等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报,2016,48(1):111-118.