基于贝叶斯攻击图的网络入侵意图分析模型

罗智勇，杨旭，刘嘉辉，许瑞
（哈尔滨理工大学计算机科学与技术学院，黑龙江 哈尔滨 150080）

摘 要：针对目前网络风险评估模型中忽略攻击代价和入侵意图对网络安全产生影响的问题，为了准确评估目标网络风险，提出一种基于贝叶斯攻击图的网络入侵意图分析方法。利用由漏洞价值、攻击成本和攻击收益计算出的原子攻击概率，结合贝叶斯信念网络量化攻击图，建立静态风险评估模型，并利用入侵意图动态更新模型，实现对网络风险的动态评估，为攻击面动态防御措施提供了依据。实验表明，所提模型不但可以有效地评估网络整体的安全性，而且在预测攻击路径方面也具有可行性。

关键词：贝叶斯信念网络；攻击图；网络安全；入侵意图；风险评估
中图分类号：TP393.4
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020172

Network intrusion intention analysis model based on Bayesian attack graph

LUO Zhiyong, YANG Xu, LIU Jiahui, XU Rui
School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

Abstract: Aiming at the problem of ignoring the impact of attack cost and intrusion intention on network security in the current network risk assessment model, in order to accurately assess the target network risk, a method of network intrusion intention analysis based on Bayesian attack graph was proposed. Based on the atomic attack probability calculated by vulnerability value, attack cost and attack benefit, the static risk assessment model was established in combination with the quantitative attack graph of Bayesian belief network, and the dynamic update model of intrusion intention was used to realize the dynamic assessment of network risk, which provided the basis for the dynamic defense measures of attack surface. Experiments show that the model is not only effective in evaluating the overall security of the network, but also feasible in predicting attack paths.

Key words: Bayesian belief network, attack graph, network security, intrusion intention, risk assessment

1 引言

信息技术的飞速发展，使现代社会对互联网更加依赖，但是也使网络攻击更加复杂，更具有危害性。传统的入侵检测系统（IDS, intrusion detection system）只能在攻击发生后对节点漏洞间的依赖关系进行分析，进而监控攻击行为，这属于被动防御[1]。因此 IDS 无法对网络进行系统的安全风险评估，针对未知网络中潜在的风险，如轨迹隐蔽的多部攻击进行有效防护[2]。20 世纪 90 年代，Phillips 等[3]最早提出了攻击图的概念，利用受攻击节点的配置信息、节点间的因果关系和攻击者的能力生成攻击图，并将其应用于对网络脆弱性的分析。攻击图是一种由顶点和有向边组成的有向图，根据模型的不同，顶点可以表示主机、服务、漏洞、权限、网络安全状态的要素，有向边表示攻击者攻击路径的攻击顺序[4]。攻击图可以直观地图形化地展示攻击行为的细节，如目标网络、漏洞、攻击路径等[5]，为

收稿日期：2020−06−12；**修回日期**：2020−07−19
基金项目：国家自然科学基金资助项目（No.61403109）
Foundation Item: The National Natural Science Foundation of China (No.61403109)

预测攻击者的攻击意图和后续攻击行为提供支撑，便于管理员及时应对突发的网络入侵事件[6]。

胡浩等[7]提出的状态转移概率归一化算法将攻击图映射为吸收马尔可夫链，利用马尔可夫链的马尔可性和漏洞评分系统计算状态转移概率，对各个节点的可能访问次数和通向目标节点的路径长度做出预测。雷程等[8]为了对网络中的移动目标进行防御并计算出成本和收益，利用攻击图建立分层网络资源图，结合变点检测方法，提出了一种基于变点检测的网络移动目标防御效能评估方法，有效提高了网络资源图的构建效率。Hu 等[9]利用不同维度的告警信息和实时攻击行为，计算出漏洞利用率，评估攻击者的能力，提出基于动态贝叶斯攻击图的威胁预测算法，实现量化网络威胁和遭受持续攻击的风险。王辉等[10]利用贝叶斯理论计算各节点的可达概率，描述单步攻击发生概率，动态预测网络中潜在的风险，结合攻击图提出一种基于改进型攻击图的入侵预测算法，简化告警证据和攻击行为的联系，提高预测的准确性。秦虎等[11]用矩阵描述主机间的关系和状态转移过程中攻击者权限的提升，提出一种基于权限提升矩阵的攻击图生成方法，该方法对于复杂网络的攻击图生成问题具有更好的适应性。

上述研究基于攻击图建立了不同的网络安全风险评估模型，但对于原子攻击概率的评估指标过于单一，无法真实地反映攻击者对目标网络和攻击路径选择的可能性，且没有针对攻击者的意图量化网络节点的风险情况。本文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，主要工作和创新如下。

1) 考虑到影响攻击者攻击行为的复杂因素，从漏洞价值、攻击成本和攻击收益 3 个指标对原子攻击概率进行计算，更真实地反映了漏洞在实际网络中被利用的情况。

2) 将贝叶斯信念网络和攻击图结合，针对攻击者的攻击意图，建立动态风险评估模型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。

3) 生成攻击路径并计算出路径总体可达概率，实现对攻击路径的预测，避免了单个网络节点漏洞对路径选择的影响，提高了预测的准确性。

2　贝叶斯攻击图建立

攻击图可以分为状态攻击图和属性攻击图。状态攻击图中顶点表示网络状态信息，边表示状态的迁移方向和过程，但是状态攻击图无法应对快速增长的状态节点，并且结构上不够直观，因此不适用于大规模网络。属性攻击图中每个属性顶点代表一个独立的安全要素，避免了状态攻击图的状态爆炸问题[12]，因此，属性攻击图对复杂的大规模网络具有更好的适应性。为了计算出攻击图中顶点到达概率和可能的攻击路径，本文利用贝叶斯信念网络来描述攻击间的因果关系，结合攻击图的图形化结构，生成贝叶斯攻击图对目标网络进行风险评估。

2.1　贝叶斯攻击图定义

贝叶斯攻击图（BAG, Bayesian attack graph）是一个有向无环图，可以表示为 BAG=(S,A,E,R,P)，具体定义如下。

1) S 为属性节点集合，分为三类，即 $S=S_{\text{start}}\cup S_{\text{transition}}\cup S_{\text{target}}$，其中，$S_{\text{start}}$ 为网络攻击的发起节点，$S_{\text{transition}}$ 为攻击行为的过程节点，S_{target} 为攻击者的目标节点。其中，S_i={0,1}，1 表示攻击者已经成功利用该属性节点漏洞占用该节点，0 表示该节点未被占用。

2)$A=\{A_i|i=1,2,\cdots,n\}$为原子攻击集合，表示攻击者对节点漏洞的攻击行为，即属性节点的迁移方式，可表示为 $A_i{:}S_{\text{pre}}\rightarrow S_{\text{next}}$。

3)$E=\{E_i|i=1,2,\cdots,n\}$为攻击图中的有向边集合，表示属性节点间攻击行为的因果关系，其中(S_{pre}，S_{next})$\in E_i$ 表示从 S_{pre} 攻击 S_{next} 的一条有向边。

4)R 表示父子属性节点间的关系，可用二元组 $<S_j,d_j>$表示，其中 $d_j\in$ {AND,OR}。AND 表示只有到达 S_j 的所有父节点状态为真，攻击才能完成；OR 表示只要其中一个父节点状态为真即可。

5)P 为攻击图中属性节点的可达概率；P_1 为攻击图中节点属性的静态可达概率；P_2 为攻击图中节点属性的动态可达概率。

2.2　贝叶斯攻击图结构建立

贝叶斯攻击图的结构与一般攻击图的结构类似，本文采用模型化方法生成攻击图的主要结构，示例如图 1 所示。

图 1 中，S_0 为攻击的发起节点，S_1 和 S_2 为过程属性节点，S_3 和 S_4 为攻击者的目标网络节点，A_1、A_2、A_3、A_4、A_5、A_6 为原子攻击。AND 表示原子攻击 A_5 和 A_6 到达 S_4 的攻击策略全部为真，攻击才可实现；OR 表示原子攻击 A_3 和 A_4 到达 S_3 的攻击策略只要有一个为真，攻击就可实现，即图例所示 2 条

攻击路径完成其中任意一个，就可完成对目标节点 S_3 的攻击。

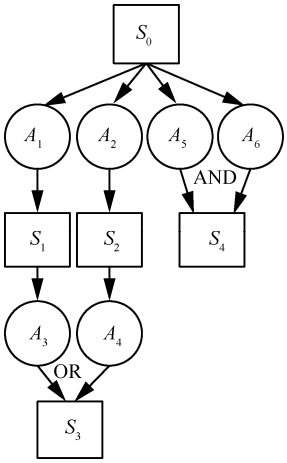

图 1 贝叶斯攻击图示例

2.3 贝叶斯攻击图量化

2.3.1 漏洞价值

漏洞价值与该属性节点漏洞被利用的难易程度和影响大小有关，一般采用美国国家通用漏洞数据库（NVD, national vulnerability database）提供的通用漏洞评分系统（CVSS, common vulnerability scoring system）[13]进行量化。CVSS 能提供完整的评分参数和开放的评分框架，将动态评估和属性节点间漏洞的依赖关系结合，量化漏洞被利用的难易程度。本文根据 CVSS 量化标准，从可利用性、影响度和范围 3 个指标进行量化，其中，可利用性包括攻击途径（AV, access vector）、攻击复杂度（AC, access complexity）、权限要求（PR, privileges required）和用户验证（UI, user interaction）；影响度包括机密性（C, confidentiality）、完整性（I, integrity）和可用性（A, availability）；范围表示漏洞的影响是否会扩大到其他组件。CVSS 指标评分如表 1 所示。

攻击者攻击漏洞时会依据漏洞的可利用性和影响度两方面来考虑漏洞价值，所以为了量化漏洞价值，首先计算出代表漏洞价值的漏洞评分 Score，其计算式为

$$\text{Score}=\begin{cases}\min\left(1.08\left(\text{Exp}+\text{Impact}\right),10\right),\text{Scope}=\text{C}\\ \min\left(\text{Exp}+\text{Impact},10\right),\text{Scope}=\text{U}\end{cases}$$

$$\text{Impact}=\begin{cases}7.52\left(\text{ISC}-0.029\right)-3.25\left(\left(\text{ISC}-0.02\right)^{15}\right),\text{Scope=C}\\ 6.42\text{ISC},\text{Scope}=\text{U}\end{cases}$$

$$\text{ISC}=1-\left(\left(1-\text{C}\right)\left(1-\text{I}\right)\left(1-\text{A}\right)\right)$$

$$\text{Exp}=8.22\text{AV}\cdot\text{AC}\cdot\text{PR}\cdot\text{UI} \tag{1}$$

其中，Impact 表示漏洞影响因子，Exp 表示漏洞利用因子，ISC 表示中间变量，常数 10 表示 Score 的最大取值为 10，其他常系数取值由 CVSS 根据安全策略进行设置。

表 1 CVSS 指标评分

基础指标	因素	度量值	评分
可利用性	AV	网络(N)	0.85
		相邻(A)	0.62
		本地(L)	0.55
		物理(P)	0.20
	AC	低(L)	0.77
		高(H)	0.44
	PR	无(N)	0.85
		低(L)	0.62
		高(H)	0.27
	UI	无(N)	0.85
		所需(R)	0.62
影响度	C, I, A	无(N)	0.00
		低(L)	0.22
		高(H)	0.56
范围	S	不变(U)	
		变动(C)	

定义 1 漏洞价值表示攻击者利用某漏洞的可能性对于漏洞 v_i，用 value(v_i)表示其漏洞价值，大小与漏洞评分有关。由于 CVSS 标准的漏洞评分取值范围是[0,10]，为了方便后续概率的计算，value(v_i)的计算式为

$$\text{value}(v_i)=\frac{\text{Score}}{10}\times 100\% \tag{2}$$

2.3.2 攻击成本与收益

攻击者对某网络节点发起攻击时，不仅会考虑该节点漏洞的价值，还会考虑攻击该节点的成本与攻击完成后所带来的收益。攻击的成本与收益不会影响节点间原本的状态转移性质，但是会影响攻击者对攻击节点的选择，一个理性的攻击者会选择攻击成本低、收益高的节点。本文参考马春光等[14]的方法对攻击成本与收益进行定义。

定义 2 攻击者在发起一次攻击行为时，会投入人力资源、物力资源、攻击代价等必要的成本，

对于原子攻击 A_i，用 cost(A_i)表示该次攻击所消耗的成本，即攻击成本。

本文从攻击代码信息（SI, shellcode information）、攻击代码对应平台（SP, shellcode platform）、攻击操作需求（Or, operation requirement）、信息收集需求（IR, information requirement）4 个指标对攻击成本进行评估，具体评分如表 2 所示。

表 2　攻击成本评分指标

成本	度量值	评分
SI	完整/功能/空	0.1/0.3/0.7
SP	普通/特殊/特定	0.15/0.35/0.6
Or	工具/脚本/手册/团体	0.1/0.25/0.45/0.7
IR	空/普通/配置/关键	0/0.2/0.55/0.8

利用 SI、SP、Or、IR 这 4 个指标的评分可以对攻击成本进行量化，计算式为

$$\text{cost}(A_i)=1-\big((1-\text{SI})(1-\text{SP})(1-\text{Or})(1-\text{IR})\big) \quad (3)$$

定义 3　对于某一原子攻击 A_i，攻击者通过该攻击完成对节点的攻击时，所能获得的收益称为攻击收益，用 income(A_i)表示，具体评分如表 3 所示。

表 3　攻击收益评分指标

度量值	评分
信息泄露	0.3~0.55
远程注册	0.55~0.7
认证绕过	0.7~0.8
有限访问	0.85~0.95
完整权限	1.0

攻击完成后的属性节点最终状态价值等同于该次攻击的收益 income(A_i)，本文给出的每个最终状态价值评分是一个范围值，在不同实际运行的网络环境中，具体的值可由管理员根据经验来赋值。

2.3.3　原子攻击概率

综合对节点漏洞价值、攻击成本与收益的量化，可以计算出攻击者在当前属性节点对其子节点发起攻击的概率，即某一原子攻击的概率，取值范围为[0,1]。当攻击概率为 0 时表示该次攻击对于攻击者无收益，攻击者不会发动攻击；攻击概率为 1 时表示该次攻击可获得的收益远远大于成本，攻击者必定会发起攻击。

定义 4　攻击者通过漏洞 v_i 完成一次原子攻击 A_j 的概率称为原子攻击概率，用 $P(A_j)$表示，计算式为

$$P(A_j)=\min\left(\frac{\text{value}(v_i)\text{income}(A_j)}{\text{cost}(A_j)},1\right) \quad (4)$$

2.3.4　条件概率

在攻击图中，属性节点并非是独立的，能否被占用还受其父节点的影响，所以需要计算该节点在整个攻击图中的条件概率。

定义 5　条件概率表示某属性节点在其父节点的影响下被攻击的可能性，对于属性节点 S_j，条件概率用 $P(S_j|\text{Par}(S_j))$表示，其中 $\text{Par}(S_j)$表示 S_j 的父节点集合。根据 d_j 的不同，条件概率的计算式分别如式(5)和式(6)所示。

1) 当 d_j=AND 时，有

$$P(S_j|\text{Par}(S_j))=\begin{cases}0, \exists S_i\in\text{Par}(S_j), S_i=0\\ \prod_{i=1}^{n}\text{Par}(A_i), \text{其他}\end{cases} \quad (5)$$

2) 当 d_j=OR 时，有

$$P(S_j|\text{Par}(S_j))=\begin{cases}0, \forall S_i\in\text{Par}(S_j), S_i=0\\ 1-\prod_{i=1}^{n}[1-\text{Par}(A_i)], \text{其他}\end{cases} \quad (6)$$

2.3.5　静态可达概率

利用贝叶斯攻击图中全部属性节点的条件概率，可计算出每个节点的可达概率，即静态可达概率。静态可达概率可以对网络风险进行静态评估，展示网络的静态风险情况。

定义 6　静态可达概率表示静态网络中各个属性节点的可达概率，是当前节点与其祖先节点的联合条件概率，即对于 $S_j\in S_{\text{transition}}\cup S_{\text{target}}$，用 $P_1(S_j)$表示该节点的静态可达概率，计算式为

$$P_1(S_j)=\prod_{j=1}^{n}P(S_j|\text{Par}(S_j)) \quad (7)$$

在图 1 中，属性节点 S_1、S_2 的静态可达概率由其条件概率结合 S_0 静态可达概率计算得出。属性节点 S_3 的静态可达概率同样依赖 S_1、S_2 的静态可达概率，具体如图 2 所示。

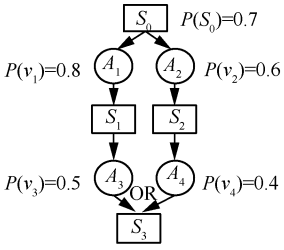

图 2　贝叶斯攻击图漏洞利用概率

S_1、S_2、S_3 的静态可达概率为

$$P_1(S_1)=P(S_1\mid S_0=1)P(S_0)=0.7\times 0.8=0.56$$

$$P_1(S_2)=P(S_2\mid S_0=1)P(S_0)=0.7\times 0.6=0.42$$

$$P_1(S_3)=\{P(S_3\mid S_1=1,S_2=1)P(S_1\mid S_0=1)\cdot P(S_2\mid S_0=1)P(S_0)+P(S_3\mid S_1=1,S_2=0)\cdot P(S_1\mid S_0=1)P(S_2\mid S_0=0\mid S_0=1)P(S_0)+P(S_3\mid S_1=0,S_2=1)P(S_1=0\mid S_0=1)\cdot P(S_2\mid S_0=1)\ P(S_0)\}=0.5\times 0.8\times 0.6\times 0.7+0.5\times 0.8\times 0.4\times 0.7+0.4\times 0.2\times 0.6\times 0.7=0.313\,6$$

2.3.6 动态可达概率

网络并非是静态的，任何网络安全要素的变化都会影响到静态可达概率，当攻击者的攻击意图已知（即 $S_{\text{target}}=1$）时，整个攻击图中属性节点的可达概率都可能随之发生改变，所以为了针对攻击者的意图量化网络风险，需要结合已知目标属性节点来更新其他节点的可达概率。

定义 7 将贝叶斯攻击图中属性节点集合 $S=\{S_i|i=1,2,\cdots,n\}$ 分为目标节点集合 $S_{\text{update}}=\{S_j\in S|S_j=0\}$和需要更新的节点集合 $S_{\text{target}}=S-S_{\text{update}}$。动态可达概率表示已知目标节点为 $S_a(S_a\in S_{\text{target}})$ 后，对更新集中节点 $S_b(S_b\in S_{\text{update}})$的可达概率进行动态更新后的概率，用 $P_2(S_b|S_{\text{target}})$表示，计算式为

$$P_2\left(S_b\mid S_{\text{target}}\right)=\frac{P\left(S_{\text{target}}\mid S_b\right)P_1\left(S_b\right)}{P_1\left(S_{\text{target}}\right)} \tag{8}$$

其中，$P\left(\mathrm{S}_{\text{target}}\mid S_b\right)=\prod_b \mathrm{P}\left(S_b=1\mid S_a\right)$，$P_1\left(S_{\text{target}}\right)=\prod_b P\left(S_b=1\right)$。

在图 1 中，假设已知攻击者的目标属性节点为 S_3，则属性节点 S_2 的动态可达概率为

$$P_2(S_2\mid S_3)=\frac{P(S_3\mid S_2)P_1(S_2)}{P_1(S_3)}=\frac{\sum_{S_1=0,1}[P(S_3\mid S_1,S_2)P(S_1)]P_1(S_2)}{P_1(S_3)}=\frac{0.5\times 0.42}{0.313\,6}=0.669\,6$$

3 贝叶斯攻击图风险分析方法

3.1 静态风险评估

计算出属性节点的条件概率和静态可达概率后，可在原始攻击图的基础上构建静态风险评估模型，静态风险评估可以评估网络中的潜在风险，构建算法如算法 1 所示。

算法 1 STATIC_BAG(AG,p)

输入 攻击图 AG=(S,A,E,R)，初始属性节点 S_1 的静态可达概率 p 可根据专家经验赋值

输出 静态风险评估攻击图 S_{BAG}=(S,A,E, R,P_1)

1) 初始化 S_{BAG} 中的参数，将 AG 中的属性节点、原子攻击、有向边和依赖关系复制到 S_{BAG} 中

2) for S_{BAG} 中的每条有向边 E_i

3) 利用式(4)计算出原子攻击概率 $P(A_i)$

4) end for

5) for S_{BAG} 中的每个属性节点 S_i

6) if S_i 为开始节点

7) $P_1(S_1 = 1) = p$

8) else

9) 利用式(5)和式(6)计算出条件概率 $P(S_i|\text{Par}(S_i))$

10) 利用式(7)计算出静态可达概率 $P_1(S_i)$

11) end if

12) 将 $P_1(S_i)$复制到参数 P_1 中

13) end for

14) 返回静态贝叶斯攻击图 S_{BAG}(S,A,E, R,P_1)

3.2 动态风险评估

现实的复杂网络中，网络安全要素会随着网络的运行不断发生变化，在知道攻击者的攻击目标时，静态风险评估的准确率会降低。因此，必须结合根据贝叶斯理论计算出的动态可达概率不断更新属性节点的可达概率，构建动态风险评估模型。构建算法如算法 2 所示。

算法 2 DYNAMIC_BAG(S_{BAG})

输入 静态风险评估攻击图 S_{BAG} = (S,A,E, R,P_1)

输出 动态风险评估攻击图 D_{BAG} = (S,A,E, R,P_2)

1)初始化 D_{BAG} 中的参数，将 S_{BAG} 中的属性节点、原子攻击、有向边、依赖关系和参数 P_1 复制到 D_{BAG} 中

2) for S_{BAG} 中的每个属性节点 S_i

3) if S_i 的值为 0

4) $S_i\in S_{\text{update}}$

5) end if

6) end for

7) for S_{BAG} 中的每个属性节点 S_j

8)　if S_j 的值为 1

9)　　for S_j 的每个父节点 S_k

10)　　利用式(8)计算出动态可达概率 $P_2(S_k|\ S_j)$

11)　　将 $P_2(S_k|\ S_j)$复制到参数 P_2 中

12)　 end for

13)　end if

14) end for

15)返回动态贝叶斯攻击图 $D_{BAG}(S,A,E,R,P_2)$

3.3　攻击路径生成

对网络进行入侵风险评估时，需要针对攻击者的意图预测出攻击者可能发起攻击的攻击路径。依据 3.2 节和 3.3 节中的攻击图算法，以目标节点为起点，自下向上查找，得到可对此目标节点发起攻击的攻击路径。需要注意的是，对于某一目标节点 S_i，如果其有 3 个父节点且父子间得依赖关系是 OR 时，需要再生成 2 条攻击路径来容纳另外 2 个父节点，即通向该节点的路径至少有 3 个。

定义 8　攻击路径表示在生成的贝叶斯攻击图中，入侵者可由初始属性节点 S_{start} 沿着一组属性节点入侵至目标节点 S_{target}，则该组节点组成的路径为贝叶斯攻击图的一条攻击路径 AP_i，攻击图中的攻击路径集合记为 Attack Path，具体算法如算法 3 所示。

算法 3　Attack Path(S_{BAG},D_{BAG})

输入　风险评估攻击图 S_{BAG} 或 D_{BAG}

输出　攻击路径 Attack Path={$AP_1,\cdots, AP_n$}

1)初始化 Attack Path 中的参数

2) for S_{target} 中的每个目标节点 S_i

3)　将 S_i 添加到路径 AP_i 中

4)　if S_i 的父节点不为空

5)　　if 父子节点间的关系为 OR

6)　　生成等同于父节点个数的路径($AP_{i-1},\cdots,AP_{i-n}$)

7)　　将父节点分别添加到路径($AP_{i-1},\cdots$, AP_{i-n})中

8)　　else

9)　　将父节点添加到 AP_i 中

10)　　end if

11)　　将父节点赋值给 S_i，重复步骤 4)

12)　else

13)　　返回路径 AP_i

14)　 end if

15)　将路径 AP_i 添加到 Attack Path

16) end for

17)　返回 Attack Path

定义 9　为了比较不同路径被攻击者攻击的概率，将某条路径上所有节点的可达概率进行乘积运算，其积为该路径的总体可达概率，即对于 AP_i，总体可达概率计算式为

$$P(AP_i)=\prod P(S_i),\ \ S_i \in AP_i \tag{9}$$

4　实验分析与优化评估

4.1　实验建立

为了验证基于贝叶斯攻击图的入侵意图分析模型的准确率，本文建立了如图 3 所示的网络拓扑结构。该结构主要包含 D_1 域、D_2 域、D_3 域和 DMZ 域，通过安装防火墙划分网络区域，并制定子网间的通信规则，保证外部访问无法到达内网区域。具体访问规则介绍如下。

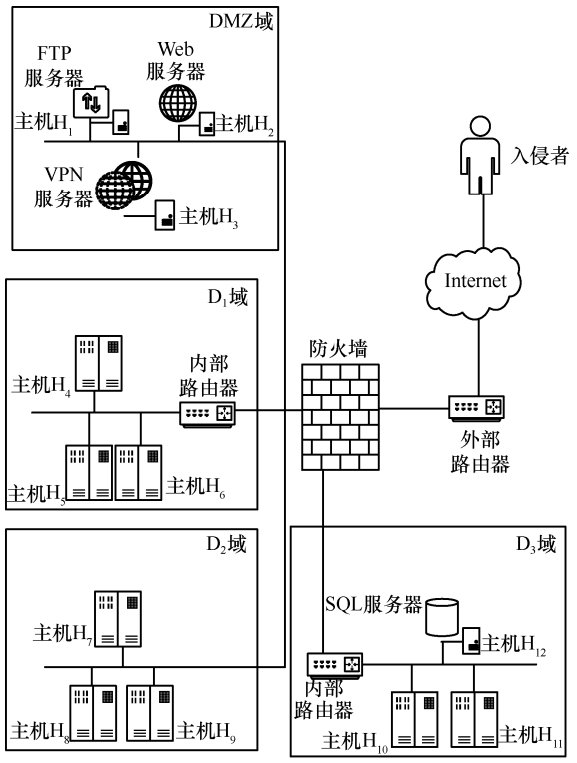

图 3　实验网络拓扑结构

1) D_1 域内只有主机 H_6 可以访问 SQL 数据库。

2) D_2 域内只有主机 H_9 可以访问 SQL 数据库。

3) D_1 域和 D_2 域的主机可以与 DMZ 域内的服务器相互访问。

4) D_1 域访问 D_2 域只能通过主机 H_6 访问主机 H_7。

5) 域内主机可以相互访问，禁止其他跨域访问。

4.2 攻击图生成

利用 OVAL 漏洞扫描器对实验网络进行扫描，得到各主机与服务器存在的漏洞信息，并利用式(1)和式(2)计算出漏洞价值，如表 4 所示。

表 4 漏洞信息和漏洞价值

主机	操作系统或程序	漏洞编号	CVE 编号	value(v_i)
H_1	Titan FTP Server6.0.3	v_1	CVE-2013-4465	46%
H_1	Windows 2003 Server	v_2	CVE-2004-0575	53%
H_2	Windows 2003 Server	v_3	CVE-2002-0364	35%
H_2	IIS 5.0 Web Server	v_4	CVE-2006-2379	39%
H_3	Check Point VPN-1 Server4.1	v_5	CVE-2009-0241	43%
H_6	Windows 2000	v_6	CVE-2007-0038	55%
H_7	Windows XP	v_7	CVE-2006-2370	25%
H_9	Windows XP	v_8	CVE-2003-0252	39%
H_{12}	Windows XP	v_9	CVE-2004-1306	51%
H_{12}	SQL Server	v_{10}	CVE-2004-0893	36%
H_{12}	SQL Server	v_{11}	CVE-2015-1762	41%

在图 3 的实验网络中，SQL 数据库服务器存在着重要数据，可以将 H_{12} 看作攻击者的入侵意图，利用扫描到的漏洞信息、漏洞间的关系、主机与服务器信息、网络配置等数据生成并输出图形化的攻击图，如图 4 所示。

图 4 所示的攻击图中，属性节点表示主机信息或者漏洞信息，原子攻击表示属性节点状态迁移的方式。当某一节点拥有多个父节点时，父子节点间的关系全为 OR，即 d_f=OR。

4.3 风险评估

为了计算出不同原子攻击的概率，首先要计算出对应的攻击成本。根据表 2 的评分标准，利用式(3)可以计算出攻击图中每次原子攻击的消耗成本，如图 5 所示。

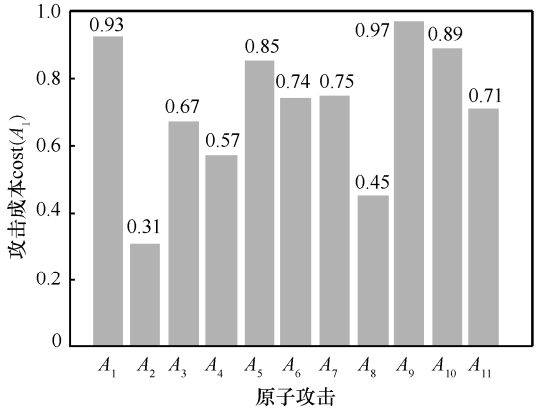

图 5 原子攻击成本

将计算出的攻击成本与表 4 所示漏洞价值以及实验攻击图中原子攻击的收益代入式(4)，计算出各

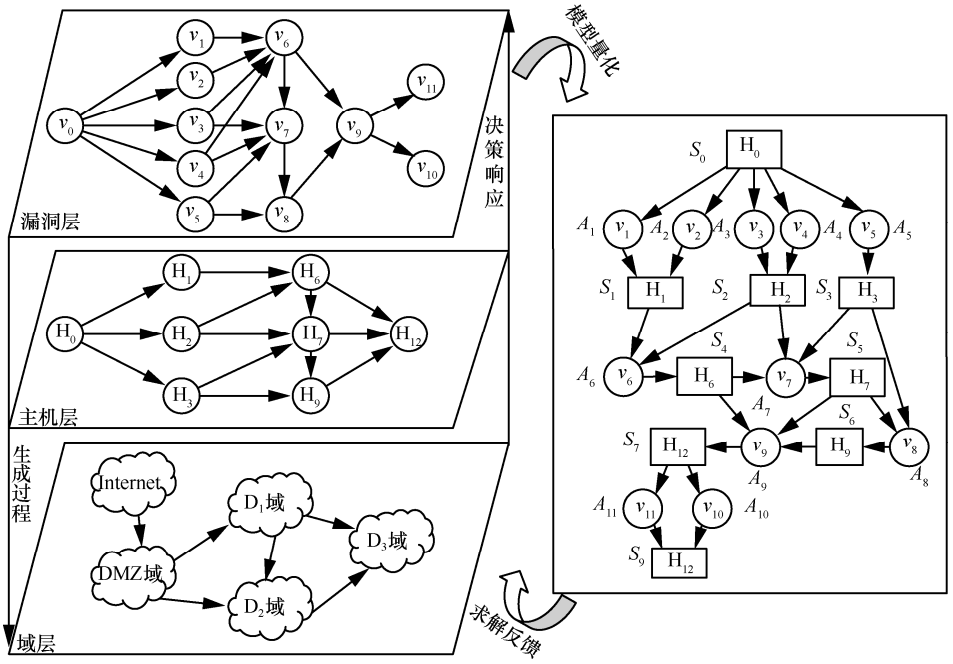

图 4 实验环境下的攻击图

个原子攻击概率，如图 6 所示。

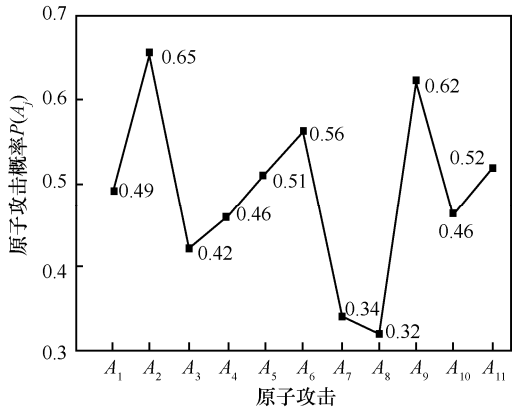

图 6　原子攻击概率

结合图 6 中获得的攻击图上每个原子攻击的概率，计算出每个属性节点的条件概率，再利用条件概率联合攻击轨迹依据算法 1 得出各个节点的静态可达概率，对实验网络进行静态风险评估。其中，节点 S_0 的静态可达概率初始化为 $P(S_0)$=0.7。确定攻击目标为 S_8 后，按照 3.3 节提出的算法 2 和式(8)对攻击图中各个属性节点的可达概率进行更新，得到动态风险评估攻击图中各个节点的动态可达概率。其中，每个节点的静态可达概率和动态可达概率分布如图 7 所示。

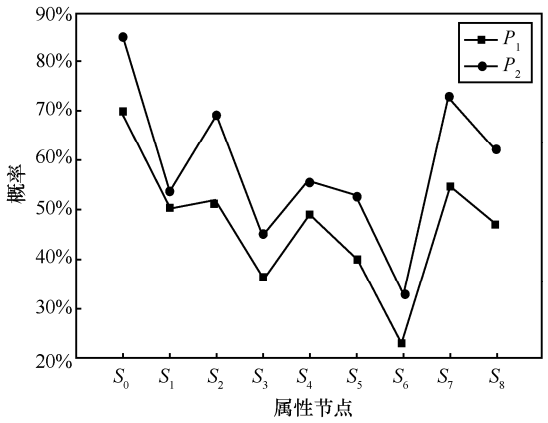

图 7　属性节点可达概率

在知道攻击者的目标节点后，实验网络中各个属性节点的可达概率都呈现上升趋势，即网络的入侵风险有明显的提升，目标节点 S_8 的可达概率也由 47%上升到 62%，中间属性节点 S_2、S_7 的被入侵风险最高，需要采取措施更新主机补丁。所以在真实的网络环境中，动态评估方法对网络风险评估的准确性明显高于静态评估，可以为管理员进行网络风险管理提供良好的支撑。

4.4　攻击路径

利用算法 3 对图 4 所示的攻击图进行查找，得到 7 条攻击路径，如表 5 所示。

表 5　　攻击路径

编号	攻击路径
AP_1	S_0—S_1—S_4—S_7—S_8
AP_2	S_0—S_2—S_4—S_7—S_8
AP_3	S_0—S_2—S_4—S_5—S_7—S_8
AP_4	S_0—S_2—S_5—S_7—S_8
AP_5	S_0—S_3—S_5—S_7—S_8
AP_6	S_0—S_3—S_6—S_7—S_8
AP_7	S_0—S_3—S_5—S_6—S_7—S_8

利用式(9)计算出每条路径在静态攻击图和动态攻击图中的总体可达概率，如图 8 所示。从图 8 可以看到，无论在静态模型还是动态模型中，攻击路径 AP_2 被入侵的风险最高。当明确攻击者的目标后，各条路径的总体可达概率均有所提高，特别是攻击路径 AP_4，通过该条路径入侵节点 S_8 的风险已经接近 AP_2。数据表明，在确定攻击者的意图后，网络风险发生了变化，动态风险评估能够更加准确地分析网络风险。

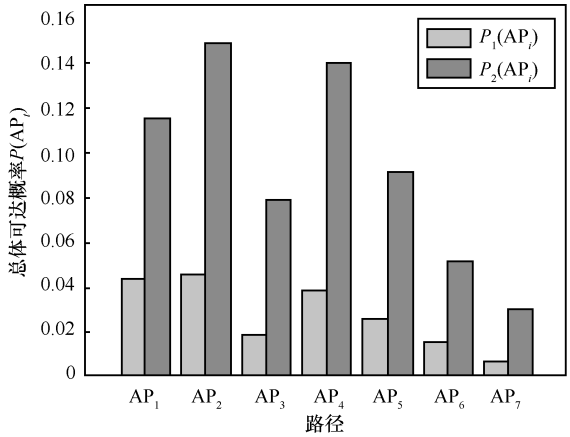

图 8　攻击路径总体可达概率

4.5　方法对比

攻击图中各属性节点的可达概率是对网络安全风险评估的主要指标，攻击路径的预测可以为网络管理员提供入侵防御依据。为了验证本文模型的优越性，在同样的网络环境下，分别给出文献[15]方法、文献[16]方法与本文方法的实验数据对比。

图 9 给出了同样在图 5 所示的网络环境下，3 种方法中不同属性节点的动态可达概率分布。文献[15]和文献[16]的评估模型也是采用贝叶斯信念网络来描述网络攻击行为间的因果关系，但是由于其对漏洞的评估指标过于单一，且没有考虑到攻击的成本与收益，导致二者的漏洞利用率并没有真实地反映网络中漏洞的被利用情况。由图 9 可以看出，本文评估模型的准确性明显优于二者，因为本文从多个指标对原子攻击概率进行计算，评估更加准确。

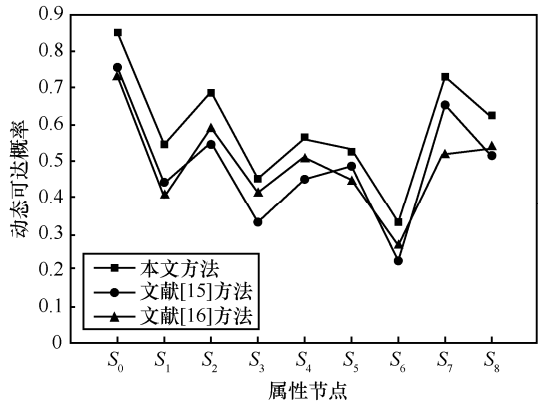

图 9 动态可达概率对比

预测攻击者实施攻击行为的攻击路径选择是对网络风险的进一步分析。本文分别利用 3 种方法进行攻击路径的预测，在相同网络环境下，预测攻击者对目标节点所选择的攻击路径。图 10 展示了 3 种方法分别在静态网络和动态网络下对目标节点 S_8 预测被攻击路径的总体可达概率对比。

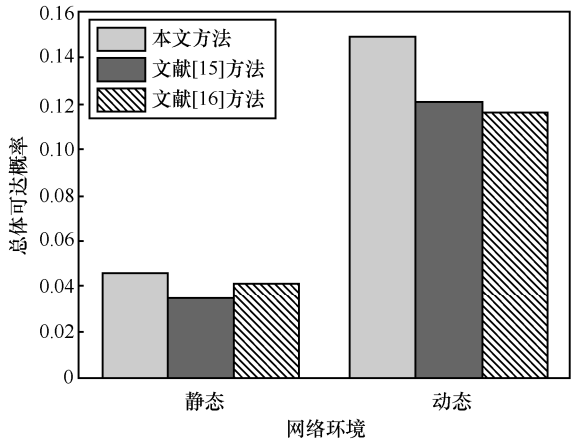

图 10 预测路径可达概率对比

虽然 3 种方法都对攻击者可能利用的攻击路径进行了预测，但是很明显，本文方法预测的路径总体可达概率高于另外二者。这是因为，首先，二者对于原子攻击概率的量化过于单一，导致属性节点的可达概率计算并不准确。其次，二者预测攻击路径的方法是从目标节点开始，不断向上查找可达概率最大的属性节点，但是忽略了单个节点对攻击路径预测的影响。例如，通向某目标节点有 2 条攻击路径，其中各属性节点可达概率分别是(0.9,0.9,0.5,0.4,0.3)和(0.7,0.7,0.6,0.4,0.3)，如果按照文献[15]和文献[16]方法预测的结果应该为后者，但是从整体性上考虑，攻击者对攻击路径的选择应该更倾向于前者。

5 结束语

为了保护重要的网络节点，针对攻击意图量化网络安全风险，给网络安全管理员提供安全策略支撑，提出了一种基于贝叶斯攻击图的网络入侵意图分析方法。首先，利用漏洞价值、攻击成本和收益 3 个评估指标计算出原子攻击概率，通过原子攻击概率得到静态可达概率和动态可达概率量化攻击图，构建基于入侵意图的风险分析模型；其次，利用构建的风险分析模型计算出每条攻击路径总体可达概率，预测可能的攻击路径；最后，从属性节点的可达概率和预测路径的总体可达概率 2 个方面和其他文献的评估方法进行对比，验证本文方法的优越性。在实际网络中，漏洞间的关联性也会影响原子攻击的概率，下一步将对此展开研究，优化网络入侵风险评估模型。

参考文献：

[1] 罗智勇, 杨旭, 孙广路, 等. 基于马尔可夫的有限自动机入侵容忍系统模型[J]. 通信学报, 2019, 40(10): 79-89.
LUO Z Y, YANG X, SUN G L, et al. Finite automaton intrusion tolerance system model based on Markov[J]. Journal on Communications, 2019, 40(10): 79-89.

[2] 王帆. 基于贝叶斯攻击图的网络安全风险评估方法研究[D]. 西安: 西北大学, 2018.
WANG F. Research on network security risk assessment method based on Bayesian attack graph[D]. Xi'an: Northwest University, 2018.

[3] PHILLIPS C, SWILER L P. A graph-based system for networ-k vulnerability analysis[C]//1998 Workshop on New Security Paradigms. New York: ACM Press, 1998: 71-79.

[4] 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.
YE Z W, GUO Y B, WANG C D, et al. Survey on application of attack graph technology[J]. Journal on Communications, 2017, 38(11): 121-132.

[5] 吴晨思, 谢卫强, 姬逸潇, 等. 网络系统安全度量综述[J].通信学报,

2019, 40(6): 14-31.
WU C S, XIE W Q, JI Y X, et al. Survey on network sy-stem security metrics[J]. Journal on Communications, 2019, 40(6): 14-31.

[6] 王硕, 汤光明, 王建华, 等. 基于因果知识网络的攻击场景构建方法[J]. 计算机研究与发展, 2018, 55(12): 2620-2636.
WANG S, TANG G M, WANG J H, et al. Attack scenarioconstruction method based on causal knowledge net[J]. Journal of Computer Research and Development, 2018, 55(12): 2620-2636.

[7] 胡浩, 刘玉岭, 张红旗, 等. 基于吸收 Markov 链的网络入侵路径预测方法[J]. 计算机研究与发展, 2018, 55(4): 831-845.
HU H, LIU Y L, ZHANG H Q, et al. Route prediction method for network intrusion using absorbing Markov chain[J]. Journal of Computer Research and Development, 2018, 55(4): 831-845.

[8] 雷程, 马多贺, 张红旗, 等. 基于变点检测的网络移动目标防御效能评估方法[J]. 通信学报, 2017, 38(1): 126-140.
LEI C, MA D H, ZHANG H Q, et al. Performance assessment approach based on change-point detection for network moving target defense[J]. Journal on Communications, 2017, 38(1): 126-140.

[9] HU H, ZHANG H, YANG Y, et al. Security risk situation quantification method based on threat prediction for multimedia communication network[J]. Multimedia Tools and Applications, 2018, 77(11): 1-31.

[10] 王辉, 鹿士凯, 王银城. 基于关联攻击图的入侵预测算法[J]. 计算机工程, 2018, 44(7): 131-138.
WANG H, LU S K, WANG Y C. Intrusion prediction algorithm based on correlation attack graph[J]. Computer Engineering, 2018, 44(7): 131-138.

[11] 秦虎, 王建利, 彭逍遥. 基于权限提升矩阵的攻击图生成方法[J]. 北京理工大学学报, 2019, 39(1): 101-105.
QIN H, WANG J L, PENG X Y. Attack graph generation method based on privilege escalation matrix[J]. Transactions of Beijing Institute of Technology, 2019, 39(1): 101-105.

[12] 李艳, 王纯子, 黄光球, 等. 网络安全态势感知分析框架与实现方法比较[J]. 电子学报, 2019, 47(4): 927-945.
LI Y, WANG C Z, HUANG G Q, et al. A survey of architecture and implementation method on cyber security situation awareness analysis[J]. Acta Electronica Sinica, 2019, 47(4): 927-945.

[13] JUKKA R. A look at the time delays in CVSS vulnerability scoring[J]. Applied Computing and Informatics, 2019, 15(2):1-18.

[14] 马春光, 汪诚弘, 张东红, 等. 一种基于攻击意愿分析的网络风险动态评估模型[J]. 计算机研究与发展, 2015, 52(9): 2056-2068.
MA C G, WANG C H, ZHANG D H, et al. A dynamic network risk assessment model based on attacker's inclination[J]. Journal of Computer Research and Development, 2015, 52(9): 2056-2068.

[15] 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(工程科学版), 2016, 48(1): 111-118.
GAO N, GAO L, HE Y Y, et al. Dynamic security risk assessment model based on bayesian attack graph[J]. Journal of Sichuan University (Engineering Science Edition), 2016, 48(1): 111-118.

[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.
ZHOU Y Y, CHENG G, GUO C S. Risk assessment method for network attack surface based on Bayesian attack graph[J]. Chinese Journal of Network and Information Security, 2018, 4(6): 11-22.

[作者简介]

罗智勇（1978− ），男，山东平度人，博士，哈尔滨理工大学教授，主要研究方向为计算机网络与信息安全、网络优化。

杨旭（1995− ），男，安徽定远人，哈尔滨理工大学硕士生，主要研究方向为计算机网络与信息安全、网络优化。

刘嘉辉（1974− ），男，黑龙江牡丹江人，博士，哈尔滨理工大学教授，主要研究方向为计算机网络与信息安全、网络优化。

许瑞（1997− ），女，河南驻马店人，哈尔滨理工大学硕士生，主要研究方向为计算机网络与信息安全、网络优化。