基于贝叶斯攻击图的 SDN 入侵意图识别算法的研究

罗智勇，张玉，王青，宋伟伟
（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：针对目前已有的软件定义网络（SDN）安全预测方法中未考虑攻击代价以及控制器漏洞对 SDN 安全所产生的影响，提出了一种基于贝叶斯攻击图的 SDN 入侵意图识别算法。利用 PageRank 算法求出设备关键度，并与漏洞价值、攻击成本、攻击收益以及攻击偏好相结合构建攻击图，建立风险评估模型，对入侵路径进行预测。通过实验对比可以看出，所提模型能更准确地预测入侵路径，有效地保证安全预测的准确性，并为 SDN 的防御提供依据。

关键词：SDN 安全预测；入侵意图；攻击图；PageRank 算法
中图分类号：TP393.4
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023073

Study of SDN intrusion intent identification algorithm based on Bayesian attack graph

LUO Zhiyong, ZHANG Yu, WANG Qing, SONG Weiwei
School of Computer Science and Technology, Harbin University of Science and Technology, Harbin 150080, China

Abstract: Since the existing software defined network (SDN) security prediction methods do not consider the attack cost and the impact of controller vulnerabilities on SDN security, a Bayesian attack graph-based algorithm to assessing SDN intrusion intent was proposed. The PageRank algorithm was used to obtain the criticality of the device, and combining with the vulnerability value, attack cost, attack benefit and attack preference, an attack graph was constructed, and a risk assessment model was established to predict the intrusion path. Through experimental comparison, it is obvious that the proposed model can more accurately predict the intrusion path, effectively ensure the accuracy of security prediction, and provide a basis for SDN defense.

Keywords: SDN security prediction, intrusion intention, attack graph, PageRank algorithm

0 引言

软件定义网络（SDN, software defined network）[1]是一种新型网络创新架构，可以利用软件编程的形式定义和控制网络，使控制平面和转发平面分离，并利用开放性可编程的特点，使网络变得更加灵活，被各方面的应用领域所采用。SDN 被认为是网络领域的一场历史性革命，为新型互联网体系结构研究提供了新的实验途径，加快了下一代网络的发展速度。

SDN 将实施网络决策的控制平面与传输数据包的数据平面分离。控制层使用 SDN 控制器通过南向接口与基础设施层（如网络交换机、路由器）进行通信，通过北向接口与应用程序进行通信，进而获取整个网络状态，并管理可编程网络进行网络的动态调整。但是 SDN 这种架构使安全问题、风险以及威胁变得更加扑朔迷离[2]。SDN 中引入了新的网络组件来支持新的网络功能，如 SDN 控制器和交换机，这就使 SDN 中出现了传统网络中未考虑的漏洞。

收稿日期：2022–11–03；**修回日期：**2023–03–06
基金项目：黑龙江省自然科学基金资助项目（No.LH2021F030）
Foundation Item: The Natural Science Foundation of Heilongjiang Province (No.LH2021F030)

在 SDN 架构中，控制器是核心组件之一，所以控制器的安全性是整个 SDN 正常运行的关键，因此本文着重对控制器安全进行分析。以往对于控制器安全性的研究介绍如下。针对 SDN 控制器中的欺骗式泛洪防御问题，提出基于关键特征多分类的泛洪检测机制和基于 SAVI（source address validation improvement）的泛洪缓解机制[3]。王涛等[4]以冗余、异构和动态为切入点，通过组合执行体冗余集构建策略、多维异构元素着色策略和动态反馈感知调度策略，有效增加 SDN 控制平面对攻击者所呈现的执行体时空不确定性（逆转攻防不对称性）。Varadharajan 等[5]提出了针对安全架构的设计，其中包括在 SDN 控制器中运行的用于指定和评估安全策略的安全管理应用程序，以及用于在网络流上执行这些安全策略的交换机中的安全组件，有助于在来自恶意终端主机的流量请求被转发到 SDN 控制器之前检测到攻击终端主机。在单链路故障研究中，Yang 等[6]提出了一种启发式算法来解决控制器安置问题。对于控制器中的多链路故障，则引入蒙特卡罗模拟来减少计算开销，陆以勤等[7]提出一种 SDN 拓扑攻击防御机制——PolicyTopo。该机制引入信息熵理论构建模型验证网络链路时延变化，同时定义数据设备端口的安全性，在防御传统拓扑攻击的同时进一步解决了网络状态变化下拓扑攻击的防御问题等。

在评估设备重要性研究中，谷歌公司针对网页提出了 PageRank 算法[8]。该算法不仅考虑了节点邻居数量关系对节点的影响，还考虑了其所在位置对节点重要性的影响。利用 PageRank 算法对网络中节点重要性的计算已得到实际的使用。

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，属于被动防御[9]，无法对网络进行系统的安全风险评估，也无法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[10]。故本文采用攻击图对网络攻击路径进行预测[11]，贝叶斯攻击图是最常用的预测方法之一。关于贝叶斯攻击图的研究有很多，具体介绍如下。Munoz-Gonzalez 等[12]提出在贝叶斯攻击图中使用有效的算法，启用静态和动态网络风险评估对攻击进行预测，并验证了其在预测中的优势和可靠性。Zeng 等[13]将基于攻击图的分析方法总结为 5 类，即图算法、贝叶斯网络、Markov 模型、成本优化算法和不确定性算法，并指出基于 Markov 模型的分析方法能够识别出高威胁度节点，评估最可能的入侵路径，具有训练容易和预测效果理想的优势。Pokhrel 等[14]通过分析主机的漏洞利用关系，依据漏洞利用评分构建各主机间的状态转移矩阵，然后根据 Markov 模型评估主机安全。Sun 等[15]提出了一种概率方法，并实现了一个原型系统 ZePro，用于零日攻击路径识别。该系统基于实例图构建了贝叶斯网络，通过将入侵证据作为输入，贝叶斯网络能够计算对象实例被感染的概率，通过依赖关系将高概率实例连接起来形成一条路径，这就是零日攻击路径。王辉等[16]提出了删除节点次序算法 DNO_Alg 确定消元顺序，并利用团树传播算法动态计算节点的后验风险概率，从而实时评估网络风险。

上述研究对 SDN 进行研究并利用攻击图建立了不同的网络安全风险评估模型，但一部分对于原子路径预测过于单一，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；另一部分没有考虑到设备之间的横向关系，以至于预测不准确。本文针对 SDN 利用贝叶斯攻击图预测攻击者的入侵意图，利用 PageRank 算法求出设备关键度，并与漏洞价值、攻击成本、攻击收益以及攻击偏好相结合构建 SDN 攻击图，以此建立风险评估模型，对入侵路径进行预测，最后利用仿真实验验证了该模型的有效性。

本文的贡献主要有以下 3 个方面。

1) 考虑到攻击者的攻击行为具有目的性，利用 PageRank 算法求出设备关键度，结合攻击经验计算攻击成本，再与漏洞价值、攻击收益以及攻击偏好相结合对设备攻击概率进行计算，更准确地预测攻击者的攻击路径。

2) 提出偏好函数的概念，将设备父节点到设备子节点的路径条件概率更加详细化，提高设备属性节点之间转移概率的准确性，避免路径转移行为的遗漏。

3) 对网络进行风险评估并生成入侵路径，计算路径中各个设备的可达概率，实现对入侵路径的预测，提高预测的准确性。

1　SDN 攻击图建立

SDN 攻击图在传统的贝叶斯攻击图的基础上增加了 SDN 控制器中的设备信息，使设备属性更加完善，并且运用了攻击图中的属性攻击图，对 SDN 中的复杂情况具有更好的适应性。为了更准确地计算出 SDN 攻击图中各个顶点被入侵的概率和可能的入侵路径，本文运用 PageRank 算法计算出设备的重要性，

并进行风险评估，对入侵路径进行预测。

定义 1 SDN 攻击图。SDN 攻击图是一个有向无环图，由设备信息集合 I、节点属性集合 B、攻击设备偏好 F、攻击过程集合 E、节点关系组合 S 以及可达概率 P 六元组组成，表示为 SDNBAG=(I,B,F,E,S,P)，其定义介绍如下。

1) I 为设备信息集合，$I=\{I_i|i=1,2,\cdots,n\}$，其中，$I_i=(h,W,Q,C)$，h 为设备名称，W 为设备重要性，Q 为设备影响度，C 为范围作用大小。

2) B 为节点属性集合，$B=B_{\text{start}}\cup B_{\text{process}}\cup B_{\text{target}}$，其中，$B_{\text{start}}$ 表示攻击者攻击的起始节点，B_{process} 表示攻击者攻击路径中的过程节点，B_{target} 表示攻击者攻击的目标设备节点。

3) F 为攻击设备偏好，表示攻击者对某个设备子节点进行攻击的偏好程度。

4) E 为攻击过程集合，$E=\{e_i|i=1,2,\cdots,n\}$，其中，e_i 为攻击者利用系统设备漏洞从一个节点攻击到另一个节点的攻击过程，表示为 $e_i\in B_{\text{pre}}\rightarrow B_{\text{next}}$，$E$ 属于有向边的集合。

5) S 为节点关系组合，到达目标设备节点的关系可以表示为二元组$<B_j,d_j>$，其中，$B_j\in B_{\text{target}}$，$d_j\in\{\text{AND,OR}\}$，d_j=AND 表示到达 B_j 的所有设备父节点均能到达 B_j 节点，所进行的攻击才能成功。同理，d_j=OR 表示 B_j 的某一设备父节点能到达 B_j，攻击就能成功。

6) P 为可达概率，即攻击者从设备父节点入侵到设备子节点的可达概率。

2 SDN 安全评估

为了对 SDN 的安全性做出更加全面的评估，本节通过给出 SDN 设备的漏洞价值和关键度定义，利用提出的攻击成本和攻击收益结合 PageRank 算法对 SDN 中每个网络设备的重要性进行评估。

2.1 漏洞价值分析

节点的漏洞价值与其本身漏洞被攻击者利用的难易程度和此漏洞对节点本身的影响有关，通常利用通用漏洞评分系统（CVSS, common vulnerability scoring system）对漏洞进行量化。本文利用 CVSS 对攻击向量（AV, access vector）、攻击复杂度（AC, access complexity）、权限要求（PR, privileges required）以及机密性（C, confidentiality）、完整性（I, integrity）和可用性（A, availability）6 个指标进行衡量[17]，其所对应的具体评分标准如表 1 所示。

表 1 CVSS 具体评分标准

指标	属性度量值	因素评分
AV	网络关系(N)	0.85
	相邻设备(A)	0.62
	本地设备(L)	0.55
	物理(P)	0.20
AC	低复杂度(L)	0.71
	中复杂度(M)	0.61
	高复杂度(H)	0.35
PR	无权限要求(N)	0.85
	权限要求较低(L)	0.64
	权限要求较高(H)	0.33
C, I, A	无(N)	0
	低(L)	0.22
	高(H)	0.56

根据以上指标对漏洞价值进行量化，求出对应的漏洞评分 grade，其对应的计算式为

$$\text{grade}=\min(\text{exp}+\text{impact},10) \tag{1}$$

其中，

$$\text{exp}=8.22\text{AV}\times\text{AC}\times\text{PR}$$

$$\text{impact}=6.42\text{iscbase}$$

$$\text{iscbase}=1-\big((1-\text{C})(1-\text{I})(1-\text{A})\big)$$

其中，impact 表示漏洞影响因子，这里默认其作用域为固定的；exp 表示漏洞利用因子，其大小表示受到攻击的难易程度；iscbase 表示临时的中间变量。

定义 2 漏洞价值。由于 CVSS 评分标准的物理范围为[0,10]，本文用 worth 对漏洞价值进行量化，计算式为

$$\text{worth}=\frac{\text{grade}}{10}\times 100\% \tag{2}$$

2.2 SDN 设备重要性分析

肖云鹏等[18]详细介绍了 PageRank 算法及其代码实现，故本文参考此书所用的 PageRank 算法对设备关键度进行分析与定义。

由于 SDN 与传统的网络结构不同，SDN 中的控制平面和数据平面是分离的，故 SDN 重要性的计算方式也不同。根据 SDN 的特点可知，每个设备都有其特定的功能，所以重要性有轻有重，由于控制器在整个 SDN 中起到了核心的作用，因此其重要性最高，其次是交换机、服务器以及主机。

定义 3 SDN 设备关键度 PR。PR 表示 SDN 设备在整个 SDN 中的关键程度，由其给定的网络

拓扑中所扮演的角色决定。由于 SDN 具有特殊性，因此本文将初始的设备关键度设置为[1,10]的整数。

在初始阶段，将主机的 PR 值设置为 4，交换机和服务器的 PR 值设置为 7，控制器的 PR 值设置为 10，并根据 PageRank 算法，对设备关键度重新进行计算，网络设备 B_j（j=1,⋯,n）的 PR(B_j)为

$$\mathrm{PR}(B_j)=\frac{1-d}{N}+d\sum_{c=1}^{M(B_j)}\frac{\mathrm{PR}(B_i)}{O(B_i)} \tag{3}$$

其中，d 表示阻尼系数，默认为 d=0.85；N 表示设备数量；PR(B_i)表示设备 B_j 的设备父节点 B_i 的设备关键度；$O(B_i)$表示设备 B_i 连接到设备 B_j 的数量；$M(B_j)$表示设备父节点到设备 B_j 的设备总数。

经过迭代后，当设备属性节点的 PR 值小于所设置的阈值 τ 时，可以得到最后的设备属性节点的 PR 值。如式(4)所示。

$$|\mathrm{PR}^{n+1}-\mathrm{PR}^{n}|<\tau \tag{4}$$

其中，PR^n 表示第 n 次迭代所得到的 PR 值。

根据 SDN 拓扑关系构建设备属性节点的初始化矩阵 $\boldsymbol{S}_{N\times N}$，其中 S_{xy} 表示设备父节点 x 到设备子节点 y 的攻击概率，取 $\boldsymbol{e}$ 为所有分量都为 1 的列向量，所得到的过渡矩阵 $\boldsymbol{K}$ 的计算式为

$$\boldsymbol{K}=d\boldsymbol{S}+\frac{1-d}{N}\boldsymbol{e}\boldsymbol{e}^{\mathrm{T}} \tag{5}$$

设置单位列向量为 $\boldsymbol{X}$ 进行迭代，如果 $\boldsymbol{X}$ 与 **PR** 值相似或者相同，结束迭代，得到最终的全部设备关键度，即$|\mathbf{PR}-\boldsymbol{X}|\leqslant\tau$，$\tau$ 为无穷小量。迭代计算式为

$$\mathbf{PR}=\boldsymbol{K}\boldsymbol{X} \tag{6}$$

利用设备关键度和漏洞价值计算出设备重要性 EIm_j，然后对其进行量化，量化后的设备重要性 EIm_j 的计算式为

$$\mathrm{EIm}(B_j)=\frac{\mathrm{PR}(B_j)\mathrm{worth}(B_j)}{10} \tag{7}$$

SDN 设备重要性算法如算法 1 所示。

算法 1　SDN 设备重要性算法

输入　阻尼系数 d，设备数量 N，单位列向量 $\boldsymbol{X}$，单位列向量 $\boldsymbol{e}$，漏洞价值 worth，无穷小量 τ，初始矩阵 $\boldsymbol{S}$

输出　SDN 设备重要性 **EIm**

1) 初始化 $\boldsymbol{S}$，$d=0.85$，$N=20$，$\tau=0.000\,001$，$\boldsymbol{X}=(1,\cdots,1)^{\mathrm{T}}$，worth，$\boldsymbol{e}=(1,\cdots,1)^{\mathrm{T}}$

2) $\boldsymbol{E}=\boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}$

3) $C=\dfrac{1-d}{N}$

4) 查找过渡矩阵

5) $\boldsymbol{K}=d\boldsymbol{S}+C\boldsymbol{E}$

6) while $|\mathbf{PR}-\boldsymbol{X}|>\tau$

7) 　记录　$\boldsymbol{U}=\mathbf{PR}$

8) 　更新　$\mathbf{PR}=\boldsymbol{K}\boldsymbol{X}$

9) 　记录　$\boldsymbol{X}=\boldsymbol{U}$

10) 记录　$\mathbf{EIm}=\dfrac{\mathbf{PR}\times\mathrm{worth}}{10}$

2.3　攻击成本分析

攻击者在对网络中的设备进行攻击时，除了付出人力资源、物力资源以外，还要承担攻击所带来的攻击代价。攻击代价主要由攻击者发动攻击时由被攻击网络的安全软件发现的概率系数（本文称之为风险系数 β），以及攻击者对该节点的攻击经验 ξ 两部分共同决定。风险系数 β 由被攻击设备的重要性 EIm(B_j)决定，该节点重要性越大，被发现的可能性越高，风险系数就越大。攻击经验的量化标准如表 2 所示。

表 2　攻击经验的量化标准

编号	经验值	经验信息描述
A_1	0.1	攻击者内部信息没有对该设备以往的攻击记录，但可能会找到该设备漏洞
A_2	0.2	攻击者内部信息没有对该设备以往的攻击记录，但知道其漏洞，不知道攻击方法
A_3	0.3	攻击者内部信息没有对该设备以往的攻击记录，但会参考可能用到的攻击方法
A_4	0.4	攻击者内部信息有粗略的攻击方法
A_5	0.5	有大概的攻击步骤，但没有攻击工具
A_6	0.6	有详细的攻击步骤，但没有攻击工具
A_7	0.7	有攻击代码和详细的工具步骤，但没有攻击工具
A_8	0.8	有攻击代码、详细的工具步骤以及攻击工具
A_9	0.9	所有都具备，且都已准备好

由以上分析可以得出，设备风险系数 $\beta(B_j)$的计算式为

$$\beta(B_j)=\mathrm{EIm}(B_j)\zeta(B_j) \tag{8}$$

定义 4　设备攻击成本 cost(B_j)。Cost(B_j)表示攻击者对目标网络中的设备发动一次攻击时所需要付出的成本。由于攻击者对设备属性节点进行攻击时攻击经验会逐步增加，因此增加系数 f 这个由专家根据不同网络环境给出的不同数值。本文默认攻击每一个设备所需要的人力资源、物力资源的攻击成本 HrACost(B_j)为 0.01，根据对风险系数和攻击经

验的全面分析，可以得到设备攻击成本的计算式为

$$\text{cost}(B_j)=f^{n-1}\beta(B_j)+\text{HrACost}(B_j) \tag{9}$$

2.4 攻击收益分析

定义 5 设备攻击收益 profit。Profit 表示攻击者对目标网络中的设备发动一次攻击时所获取的收益。本文的攻击收益衡量指标根据马春光等[19]提出的攻击收益方法进行定义。攻击收益衡量指标如表 3 所示。

表 3 攻击收益衡量指标

收益水平	衡量信息	收益值
PL_1	内部信息泄露	0.30~0.55
PL_2	远程登录设备	0.55~0.70
PL_3	认证绕过	0.70~0.85
PL_4	临时访问	0.85~0.95
PL_5	获取 Root 权限	1.00

攻击收益 profit 会根据衡量信息进行收益值判断，根据信息泄露的多少得到一个准确的收益值。泄露的信息越重要，所获得的收益就越高，具体情况由管理员根据设备所处的网络情况来设置。

2.5 攻击偏好分析

定义 6 偏好函数（PF, preference function）。PF 表示攻击者对目标设备节点进行攻击的偏好程度，偏好程度越高，攻击者对目标设备节点进行攻击的可能性就越高。

偏好函数主要由攻击成本与攻击收益的比值来评判，比值越高说明偏好函数越低，对目标设备节点进行攻击的可能性就越小，反之，可能性就越高。用 λ 表示攻击成本与攻击收益的比值，则 λ 的计算式为

$$\lambda=\frac{\text{cost}(B_j)}{\text{profit}(B_j)} \tag{10}$$

偏好函数 PF 的计算式为

$$\text{PF}(B_j)=\begin{cases}0,\lambda\geqslant 1\\ 1-\lambda,0<\lambda<1\\ 1,\lambda=0\end{cases} \tag{11}$$

由式(11)可知，$\text{PF}(B_j)\in[0,1]$，当 $\lambda\geqslant 1$ 时，偏好函数为 0，这时成本远大于收益，攻击者对该设备不可能进行攻击；当 $\lambda=0$ 时，相当于收益远大于成本，偏好函数为 1，这时攻击者必会对该设备发动攻击。

2.6 设备攻击概率分析

根据上述对设备重要性、攻击成本和攻击代价的分析，以及对其量化的结果，能够得到攻击者对所要攻击的设备发动攻击的概率，即该设备被攻击的概率，其范围为[0,1]，概率越高，被攻击的可能性就越大。

定义 7 设备攻击概率。设备攻击概率表示攻击者对目标设备实施攻击，并成功占领目标设备节点的概率。对于设备 B_j，其设备攻击概率 $P(B_j)$的计算式为

$$P(B_j)=\min\left(\frac{\text{worth}(B_j)\text{profit}(B_j)+\text{PF}(B_j)}{\text{cost}(B_j)},1\right) \tag{12}$$

2.7 条件概率分析

定义 8 条件概率。条件概率表示每一个设备属性节点都会在其设备父节点的影响下产生被攻击的可能性。其中，每个节点的条件概率也叫局部条件概率分布函数。对于设备属性节点 B_j，其局部条件概率可以表示为 $P_c(B_j|P_a(B_j))$，设备父节点集合表示为 $P_a(B_j)$，设备父节点到设备子节点的攻击表示为 v_j。

1) 当 $S=<B_j,d_j=\text{AND}>$时，设备父节点必须全部能到达设备子节点，攻击才能成功，此时计算式为

$$P_c(B_j|P_a(B_j))=\begin{cases}0,\exists B_j\in P_a(B_j),B_j=0\\ \prod_{j=1}^{n}P_a(v_j),\text{其他}\end{cases} \tag{13}$$

2) 当 $S=<B_j,d_j=\text{OR}>$时，只需存在一个设备父节点能到达设备子节点，攻击就可以成功，此时计算式为

$$P_c(B_j|P_a(B_j))=\begin{cases}0,\forall B_j\in P_a(B_j),B_j=0\\ 1-\prod_{j=1}^{n}[1-P_a(v_j)],\text{其他}\end{cases} \tag{14}$$

定义 9 设备可达概率。设备可达概率表示在 SDN 中的各个设备属性节点的可达概率，是当前设备属性节点中被攻击的初始节点所经过节点的联合条件概率，即对于 $B_j\in B_{\text{process}}\cup B_{\text{target}}$，设备属性节点 B_j 的设备可达概率计算式为

$$P_c(B_j)=\prod_{j=1}^{n}P_c(B_j|P_a(B_j)) \tag{15}$$

其中，$P_a(B_j)$表示设备属性节点 B_j 的设备父节点集合。

定义 10 入侵路径概率。入侵路径概率表示攻击者在入侵到目标设备所走的某一条攻击路径上的所有设备可达概率的乘积。入侵路径概率的计算式为

$$P(\mathrm{IV}_i)=\prod P_c(B_i),\ B_i \in \mathrm{IV}_i \tag{16}$$

3　SDN 风险评估及入侵路径

3.1　SDN 风险评估分析

为了能够更精准地预测攻击者对 SDN 设备的攻击路径，通过计算求得设备属性节点的条件概率和先验概率，结合贝叶斯理论以及所提出的攻击成本、攻击收益和攻击偏好对 SDN 攻击图中的参数进行赋值，得到最终的 SDN 攻击图，如算法 2 所示，具体步骤如下。

1) 将 SDN 攻击图中设备信息集合 I、节点属性集合 B、攻击过程集合 E、节点关系组合 S 进行初始化。

2) 利用式(12)计算攻击者从有向边攻击的设备攻击概率。

3) 利用式(11)计算攻击设备偏好函数，利用式(13)和式(14)计算攻击者从设备父节点攻击到设备子节点的条件概率，以及利用式(15)计算设备可达概率。

4) 将得到的攻击设备偏好和可达概率复制到参数 P 中，返回最终 SDN 攻击图。

算法 2　SDN 风险评估算法

输入　SDN 中的设备信息集合 I、节点属性集合 B、攻击设备偏好 F、节点关系组合 S

输出　$\mathrm{SDNBAG}=(I,B,F,E,S,P)$

1) 初始化 SDN 攻击图中的设备信息集合 I，节点属性集合 B，攻击设备偏好 F 以及节点关系组合 S
2) for (SDNBAG 中的每个有向边)
3)　　使用式(12)计算 $P(B_i)$
4) end for
5) for (在 SDNBAG 中的每个设备属性节点 B_i)
6)　　使用式(11)计算攻击设备偏好 F
7)　　if($F=1$)
8)　　$P_c(B_i)=P$
9)　　else
10)　　使用式(13)和式(14)计算 $P_c(B_i \mid P_a(B_i))$
11)　　使用式(15)计算设备可达概率 $P_c(B_i)$
12)　　end if
13) end for
14) 将 $P_c(B_i)$ 复制到参数 P 中
15) 记录 $\mathrm{SDNBAG}=(I,B,F,E,S,P)$

3.2　入侵路径分析

定义 11　入侵路径。根据 3.1 节得到的 SDN 攻击图可知，攻击者从起始设备属性节点 B_{start} 攻击到目标设备节点 B_{target} 所走过的路径，称为入侵路径。其中，设备属性节点组成的路径为 SDN 攻击图的入侵路径 IP，入侵路径算法如算法 3 所示。

算法 3　入侵路径算法

输入　SDN 攻击图中的参数

输出　$\mathrm{IntPath}=\{\mathrm{IP}_1,\cdots,\mathrm{IP}_n\}$

1) 初始化 SDN 攻击图中的参数
2) for (每个设备属性节点 $B_i \in B_{\text{target}}$)
3) 将 B_i 加入 IP_i 中
4)　if ($P_a(B_i)$!=None)
5)　　if ($d_i=\mathrm{OR}$)
6)　　n=len ($P_a(B_i)$)
7)　　复制 IP_i 到 $(\mathrm{IP}_{i-1},\cdots,\mathrm{IP}_{i-n})$
8)　　for (每个设备属性节点 $B_j \in P_a(B_j)$)
9)　　将 B_j 加入 IP_{i-j} 中
10)　　end for
11)　else
12)　将 $P_a(B_i)$ 加入 IP_i 中
13)　$B_i \in P_a(B_i)$
14)　end if
15) else
16) 返回 IP_i;
17) end if
18) 将 IP_i 加入 IntPath 中
19)end for
20) 返回 IntPath

根据算法 3 中所求得的所有入侵路径，找出概率风险最大的一条路径，即攻击者所攻击设备的路径。

4　仿真实验

4.1　实验环境搭建

为了验证 SDN 攻击图对攻击路径预测的有效性，本文利用 2 台虚拟机，搭建了如图 1 所示的仿真网络环境进行实验，包括 SDN 控制平面、数据平面以及外部网络。其中，SDN 控制平面包含 3 台控制器，分别为 S_1、S_2 和 S_3。数据平面包含 5 台服务器、6 台交换机、2 台虚拟机以及防火墙，在防火墙上安装入侵检测系统 Snort，对网络流量进行监控。运用 Web 服务器、FTP 服务器、VPN 服务器、SSH 服务器和数据库服务器，对业务网环境进行模拟。利用 Open vSwitch 软件创建虚拟交换机，对 Open Flow

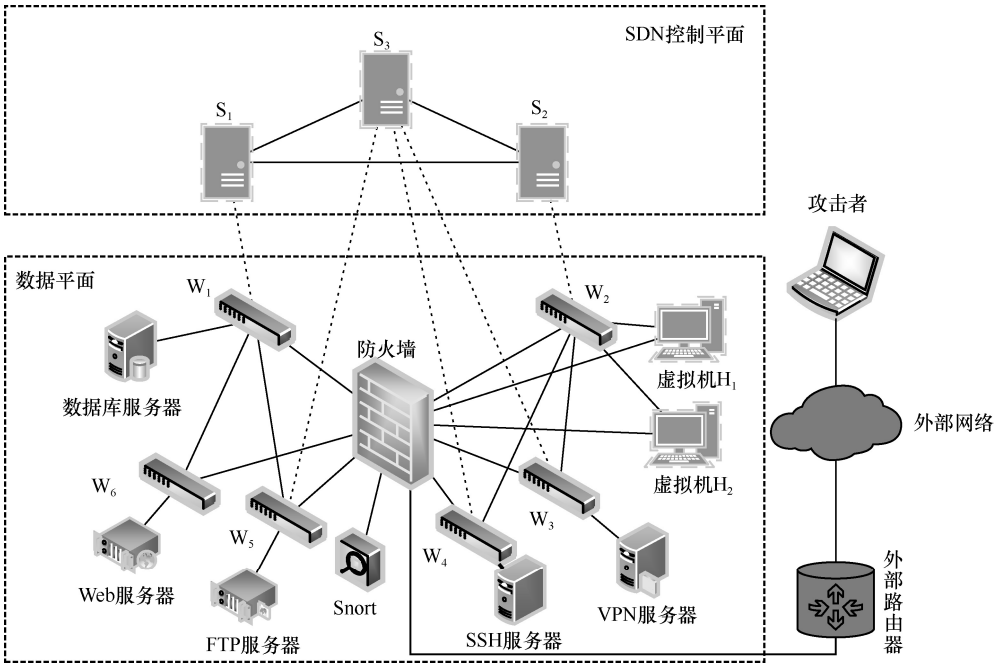


图 1　仿真网络环境

交换机进行模拟，用 W={W$_i$|i=1,2,⋯,6}表示。外部网络由攻击者所用主机以及外部路由器组成。

本文利用 OpenVAS 对设备属性节点进行扫描，得到 SDN 中各个设备属性节点的漏洞信息，并根据式(1)和式(2)得到对应设备属性节点的漏洞价值，然后对其进行汇总，得到表 4 所示的关系。

表 4　　漏洞信息及漏洞价值

设备名	设备 ID	操作系统或程序	漏洞描述	漏洞编号	CVE 编号	worth(v_i)
虚拟机 H_1	H_1	LINUX (Ubantu16.04)	缓冲区溢出	v_1	CVE-2014-1443	0.41
		LINUX (Ubantu16.04)	执行任意代码	v_2	CVE-2015-1635	0.43
虚拟机 H_2	H_2	LINUX (Ubantu16.04)	访问限制绕过	v_3	CVE-2015-8467	0.35
		LINUX (Ubantu16.04)	跨站脚本	v_4	CVE-2015-8622	0.39
VPN 服务器	T_1	WebVPN	授权后堆溢出漏洞	v_5	CVE-2018-13383	0.43
FTP 服务器	T_2	Titan FTP Server6.0.3	任意命令执行漏洞	v_6	CVE-2014-8517	0.43
SSH 服务器	T_3	LINUX (Ubantu16.04)	登录验证绕过漏洞	v_7	CVE-2018-10933	0.57
Web 服务器	T_4	LINUX (Ubantu16.04)	漏洞复现	v_8	CVE-2018-8715	0.39
数据库服务器	T_5	Postgre SQL (postgresql-11)	SQL 注入	v_9	CVE-2020-7471	0.52
		Postgre SQL (postgresql-11)	缓冲区溢出	v_{10}	CVE-2014-1669	0.41
交换机 W_1	W_1	Open vSwitch2.13	资源管理错误	v_{11}	CVE-2017-14970	0.55
交换机 W_2	W_2	Open vSwitch2.13	用户安全漏洞	v_{12}	CVE-2020-27827	0.62
交换机 W_3	W_3	Open vSwitch2.13	输入验证漏洞	v_{13}	CVE-2018-17205	0.57
交换机 W_4	W_4	Open vSwitch2.13	缓冲区溢出	v_{14}	CVE-2016-2074	0.41
交换机 W_5	W_5	Open vSwitch2.13	用户安全漏洞	v_{15}	CVE-2020-35498	0.62
交换机 W_6	W_6	Open vSwitch2.13	缓冲区溢出	v_{16}	CVE-2017-9265	0.41
控制器 S_1	S_1	NGINX1.21.0	其他	v_{17}	CVE-2021-23019	0.37
控制器 S_2	S_2	NGINX1.21.0	安全特征问题	v_{18}	CVE-2021-23020	0.52
控制器 S_3	S_3	ONAP SDNC	操作系统命令注入	v_{19}	CVE-2019-12113	0.55

4.2　攻击图和入侵路径的生成

对于攻击者来说，由于主机内的数据库存放着大量信息，入侵目的主机的数据库服务器所得到的收获最大，本次实验假设虚拟机 H_1 内部最先与外部网络进行通信，因此攻击者对虚拟机 H_1 最先进行入侵，并将数据库服务器设为目标最终攻击的设备。由于本文考虑的是 SDN 控制平面中的控制器和数据平面中的设备的关联关系整体分析攻击路径，故根据漏洞信息和 SDN 关系等数据生成攻击图，如图 2 所示。

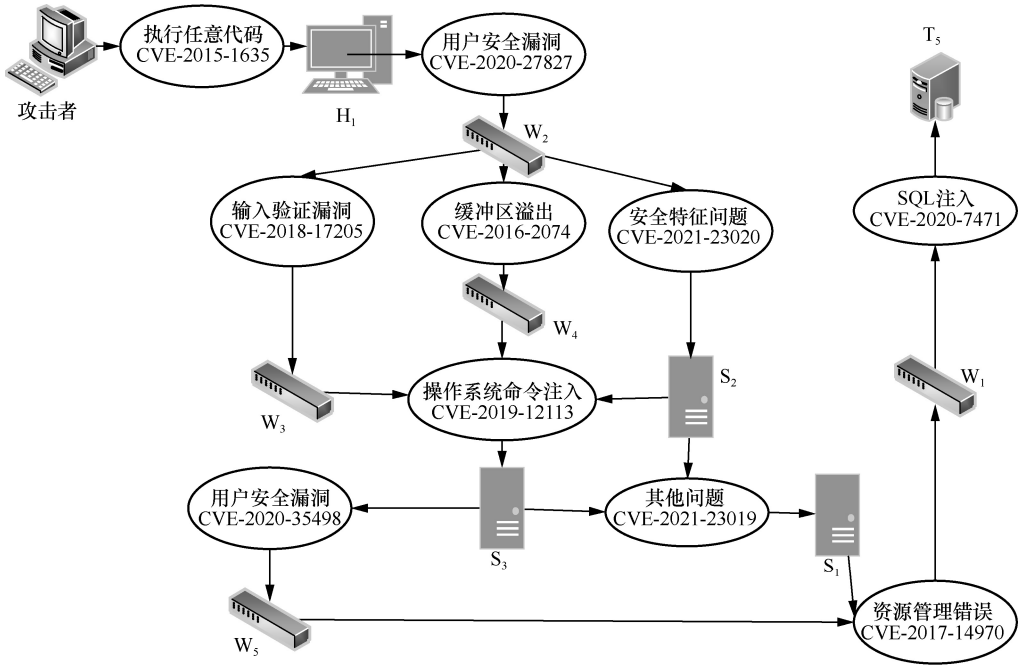


图 2　实验环境下的攻击图

由图 2 可知，当设备子节点存在多个设备父节点时，攻击者可从多个设备父节点中的任意一个设备父节点成功入侵目的设备子节点，故 d_j=OR。

根据本文提出的攻击路径分析方法，利用入侵路径算法对图 2 的攻击图进行预测，生成 7 条可行的入侵路径，如表 5 所示。

表 5　　入侵路径

路径编号	入侵路径	入侵设备数
IV_1	<H_1, W_2, W_3, S_3, S_1, W_1, T_5>	7
IV_2	<H_1, W_2, W_3, S_3, W_5, W_1, T_5>	7
IV_3	<H_1, W_2, S_2, S_3, S_1, W_1, T_5>	7
IV_4	<H_1, W_2, S_2, S_1, W_1, T_5>	6
IV_5	<H_1, W_2, S_2, S_3, W_5, W_1, T_5>	7
IV_6	<H_1, W_2, W_4, S_3, W_5, W_1, T_5>	7
IV_7	<H_1, W_2, W_4, S_3, S_1, W_1, T_5>	7

4.3　仿真风险计算

为了得到每条入侵路径中设备属性节点受到的设备攻击概率，本文先利用 PageRank 算法求出设备关键度，再利用攻击成本、攻击收益以及攻击偏好来对设备攻击概率进行计算。其中，攻击成本由攻击经验和设备重要性组成，由表 2 查找到设备的攻击经验并利用算法 1 计算出设备重要性，代入式(8)和式(9)中，得到攻击成本，即攻击者每次对设备发动攻击时的成本消耗，结果如图 3 所示。

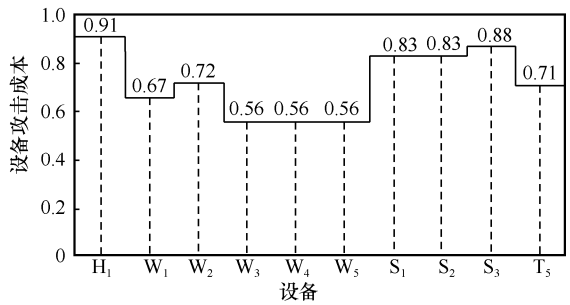


图 3　设备的攻击成本

将图 3 中各个设备的攻击成本、表 4 中各个设备的漏洞价值、表 3 中各个设备的攻击收益以及攻击者对设备的攻击偏好代入式(12)中，计算各个设备的攻击概率，结果如表 6 所示。

表 6 设备攻击概率

设备	攻击概率
H_1	0.44
W_1	0.63
W_2	0.72
W_3	0.65
W_4	0.52
W_5	0.66
S_1	0.41
S_2	0.70
S_3	0.77
T_5	0.52

根据式(15)计算每条入侵路径的设备可达概率，如图 4 所示。由于路径 IV_4 的入侵设备数低于其余路径，对实验结果存在影响，故本文忽略路径 IV_4 的实验结果，只对其余路径进行预测。从图 4 中可以看出，路径 IV_5 的入侵风险是最高的，故推断入侵路径为<H_1,W_2,S_2,S_3,W_5,W_1,T_5>，且所经过设备的漏洞价值和偏好程度越高，设备攻击概率越高。

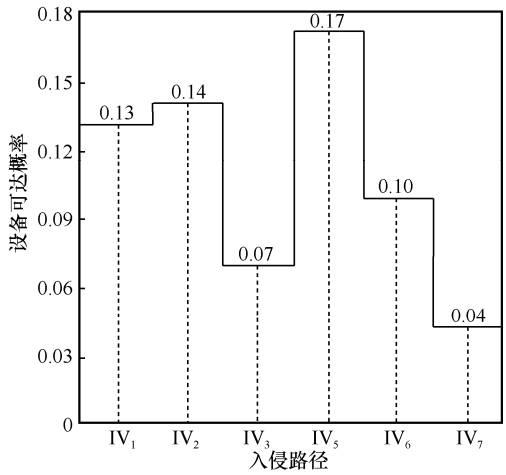


图 4 入侵路径的设备可达概率

4.4 算法比较

由于设备可达概率是 SDN 安全风险评估的关键，入侵路径的预测可以为 SDN 管理员提供入侵防御的可靠依据。为了充分证明本文算法的有效性和正确性，在完全相同的 SDN 环境下，将本文算法与文献[16]和文献[20]所提出的算法进行比较。

文献[16]和文献[20]同样采用贝叶斯攻击图对设备间的攻击行为进行描述，但是只考虑了部分因素进行评估，没有考虑到攻击设备所消耗的成本与所得到的收益、攻击者对设备的偏好所造成的影响以及设备之间的关系所带来的影响，导致对入侵路径预测不准确。图 5 为在相同的实验环境条件下，本文算法与文献[16]和文献[20]算法对实验中的各个设备攻击概率。

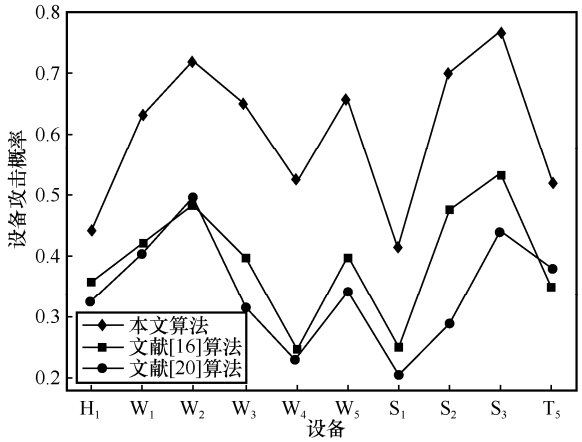


图 5 设备攻击概率

在得到 3 种算法的设备攻击概率对比后，为了进一步凸显本文算法的优越性，根据图 5 中每个设备的设备攻击概率，再根据式(16)对这 3 种算法所选择的攻击路径的入侵路径概率进行计算，可以得出本文算法对最高概率的入侵路径的入侵路径概率为 0.29%，文献[16]算法为 0.08%，文献[20]算法为 0.06%。可以看出，在添加了本文所提出的攻击偏好，以及对攻击成本进行重新评估后，入侵路径概率提高了，这验证了本文算法的优越性。

5 结束语

为了保护 SDN 中所有的信息和设备安全，针对入侵意图量化网络安全风险，给 SDN 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 SDN 入侵意图识别算法。首先，利用 PageRank 算法求出设备关键度，然后与漏洞价值、攻击成本、攻击收益以及偏好函数相结合构建攻击图，建立风险评估模型，对入侵路径进行预测。通过与以往实验对比，证实了本文研究的可行性。在现实的 SDN 中，漏洞间的关联性也会影响设备攻击概率，下一步将对此展开研究，优化 SDN 安全风险评估的算法和模型。

参考文献：

[1] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[2] CHICA J C C, IMBACHI J C, BOTERO J F. Security in SDN: a comprehensive survey[J]. Journal of Network and Computer Applications, 2020, 159: 102595.1-102595.23.

[3] 周启钊, 于俊清, 李冬. SDN 控制层泛洪防御机制研究:检测与缓解[J]. 通信学报, 2021, 42(11): 41-53.
ZHOU Q Z, YU J Q, LI D. Research on flood defense mechanism of SDN control layer: detection and mitigation[J]. Journal on Communications, 2021, 42(11): 41-53.

[4] 王涛, 陈鸿昶. 基于多维异构特征与反馈感知调度的 SDN 内生安全控制平面[J]. 电子学报, 2021, 49(6): 1117-1124.
WANG T, CHEN H C. An SDN endogenous security control plane based on multi-dimensional heterogeneous features and feedback-aware scheduling strategy[J]. Acta Electronica Sinica, 2021, 49(6): 1117-1124.

[5] VARADHARAJAN V, TUPAKULA U. Counteracting attacks from malicious end hosts in software defined networks[J]. IEEE Transactions on Network and Service Management, 2020, 17(1): 160-174.

[6] YANG S, CUI L Z, CHEN Z T, et al. An efficient approach to robust SDN controller placement for security[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1669-1682.

[7] 陆以勤, 毛中书, 程喆, 等. SDN 拓扑攻击及其防御[J]. 华南理工大学学报(自然科学版), 2020, 48(11): 114-122.
LU Y Q, MAO Z S, CHENG Z, et al. Research on SDN topology attack and its defense mechanism[J]. Journal of South China University of Technology (Natural Science Edition), 2020, 48(11): 114-122.

[8] PAGE L, BRIN S, MOTWANI R, et al. The PageRank citation ranking: bringing order to the Web[R]. 1999.

[9] 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.

[10] CHEN Y Y, XU B, LONG J, et al. Information security assessment of wireless sensor networks based on Bayesian attack graphs[J]. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 2021, 41(3): 4511-4517.

[11] HUSÁK M, KOMÁRKOVÁ J, BOU-HARB E, et al. Survey of attack projection, prediction, and forecasting in cyber security[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 640-660.

[12] MUNOZ-GONZALEZ L, SGANDURRA D, BARRERE M, et al. Exact inference techniques for the analysis of Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(2): 231-244.

[13] ZENG J P, WU S, CHEN Y Y, et al. Survey of attack graph analysis methods from the perspective of data and knowledge processing[J]. Security and Communication Networks, 2019, 2019: 1-16.

[14] POKHREL N R, TSOKOS C P. Cybersecurity: a stochastic predictive model to determine overall network security risk using Markovian process[J]. Journal of Information Security, 2017, 8(2): 91-105.

[15] SUN X Y, DAI J, LIU P, et al. Using Bayesian networks for probabilistic identification of zero-day attack paths[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2506-2521.

[16] 王辉, 张娟, 赵雅, 等. 一种新型贝叶斯模型的网络风险评估方法[J]. 小型微型计算机系统, 2020, 41(9): 1898-1904.
WANG H, ZHANG J, ZHAO Y, et al. Network risk assessment method of a new type of Bayesian model[J]. Journal of Chinese Computer Systems, 2020, 41(9): 1898-1904.

[17] RUOHONEN J. A look at the time delays in CVSS vulnerability scoring[J]. Applied Computing and Informatics, 2019, 15(2): 129-135.

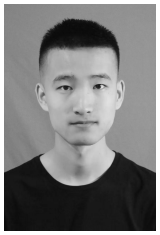
[18] 肖云鹏, 卢星宇, 许明, 等. 机器学习经典算法实践[M]. 北京: 清华大学出版社, 2018.
XIAO Y P, LU X Y, XU M, et al. Classical algorithm practice of machine learning[M]. Beijing: Tsinghua University Press, 2018.

[19] 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.

[20] 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.
WANG Y, WU J Y, HUANG J L, et al. Network intrusion intention recognition method based on Bayesian attack graph[J]. Computer Engineering and Applications, 2019, 55(22): 73-79.

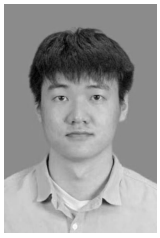
[作者简介]

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、网络优化等。



张玉（1996– ），男，黑龙江尚志人，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、网络优化等。

王青（1998– ），女，黑龙江伊春人，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、自然语言处理等。



宋伟伟（1998– ），男，山西临汾人，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、网络优化等。