研究与开发

基于贝叶斯攻击图的 SDN 安全预测方法

尹彦尚，索同鹏，董黎刚，蒋献
（浙江工商大学信息与电子工程学院（萨塞克斯人工智能学院），浙江 杭州 310018）

摘　要：现有研究者采用威胁建模和安全分析系统的方法评估和预测软件定义网络（software defined network，SDN）安全威胁，但该方法未考虑 SDN 控制器的漏洞利用概率以及设备在网络中的位置，安全评估不准确。针对以上问题，根据设备漏洞利用概率和设备关键度结合 PageRank 算法，设计了一种计算 SDN 中各设备重要性的算法；根据 SDN 攻击图和贝叶斯理论设计了一种度量设备被攻击成功概率的方法。在此基础上设计了一种基于贝叶斯攻击图的 SDN 安全预测算法，预测攻击者的攻击路径。实验结果显示，该方法能够准确预测攻击者的攻击路径，为安全防御提供更准确的依据。

关键词：SDN 安全预测；漏洞利用概率；攻击图；PR 算法
中图分类号：TP393.0
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021212

SDN security prediction method based on bayesian attack graph

YIN Yanshang, SUO Tongpeng, DONG Ligang, JIANG Xian
School of Information and Electronic Engineering (Sussex Artificial Intelligence Institute), Zhejiang Gongshang University, Hangzhou 310018, China

Abstract: Existing researchers use threat modeling and security analysis system to evaluate and predict SDN (software defined network) security threats, but this method does not consider the vulnerability utilization of SDN controller and the location of devices in the network, so the security evaluation is not accurate. In order to solve the above problems, according to the probability of device vulnerability utilization and device criticality, combined with PageRank algorithm, a algorithm to calculate the importance of each device in SDN was designed; according to SDN attack graph and Bayesian theory, a method to measure the success probability of device being attacked was designed. On this basis, a SDN security prediction method based on Bayesian attack graph was proposed to predict the attack-

收稿日期：2021−04−09；**修回日期**：2021−09−11
通信作者：董黎刚，donglg@zjgsu.edu.cn
基金项目：浙江省重点研发计划项目（No.2020C01079，No.2021C01036）；国家自然科学基金资助项目（No.61871468）；浙江省自然科学基金资助项目（No.LY18F010006）；浙江省新型网络标准与应用技术重点实验室基金资助项目（No.2013E10012）；大学生科技成果推广项目（No.1120KZN0220031G）
Foundation Items: Zhejiang Province Key Research and Development Program (No.2020C01079, No.2021C01036), The Natural Science Foundation of China (No.61871468), Zhejiang Provincial Natural Science Foundation of China (No.LY18F010006), Zhejiang Provincial Key Laboratory of New Network Standards and Application Technology (No.2013E10012), University Students' Scientific and Technological Achievements Promotion Project (No.1120KZN0220031G)

er's attack path. Experimental results show that this method can accurately predict the attacker's attack path and provide more accurate basis for security defense.

Key words: SDN security prediction, vulnerability utilization probability, attack graph, PR algorithm

1 引言

软件定义网络[1]（software defined network，SDN）解决了传统网络部署、维护复杂和不可编程等问题，加速了网络的发展。SDN 在物理上和逻辑上将网络控制平面和数据平面分开，使网络变得敏捷灵活，被许多应用领域所采用，但 SDN 体系架构带来了许多未知且额外的安全问题、风险和威胁[2-3]。SDN 引入了新的网络组件支持新的网络功能，如 SDN 控制器和交换机，这会使 SDN 中存在着传统网络中未考虑的漏洞[4]。

被攻击的网络主机会利用SDN控制器中的漏洞，通过发送包含负载的特制的网络数据包，在 SDN 控制器上安装 SDN 恶意软件，会造成恶意应用程序威胁[5]。所有 OpenFlow 交换机都允许任何人通过被动监听端口从任何网络连接，大多数 OpenFlow 交换机使用这些被动侦听端口进行远程调试，而且这些端口允许访问流表。因此，攻击者有可能使用某些工具或通用实用程序（如 dpctl）通过这些被动侦听器端口连接到 OpenFlow 交换机。dpctl 是一种管理实用程序，可控制 OpenFlow 交换机来修改其配置[6-7]，造成中间人攻击威胁。针对以上安全威胁问题，为了增强 SDN 抵御网络攻击的安全性，目前已经提出了许多安全解决方案。其中最主要的是使用图形安全模型系统地评估和评价 SDN 的安全性。

与现有网络不同，SDN 控制器在 SDN 应用和通信协议方面存在漏洞，这些新的漏洞具有安全风险，而图形安全模型安全评估方法无法准确地分析这些漏洞。在评估传统网络设备脆弱性中采用了 PageRank（PR）算法[8]，此算法不仅考虑了节点邻居数量，还考虑了其质量对节点重要性的影响，但未考虑到网络设备漏洞[9]的差异，在这种情况下评估 SDN 中设备的重要性不够准确。

目前研究者大多采用贝叶斯攻击图[10]预测网络攻击路径，贝叶斯攻击图采用系统和自动化的方法构建攻击图，并对给定网络上所有潜在的原子攻击步骤建模。在贝叶斯攻击图中，每一个节点代表在该网络的当前配置与状态下可能被攻击者利用的条件，每条边对应一个或多个漏洞被利用的概率，每条路径代表潜在的被攻击路径。贝叶斯攻击图保留了网络中所有攻击路径信息，给大中型网络带来了很好的可扩展性，在不确定的条件下将攻击者被成功攻击的可能性嵌入攻击图的边缘权重分配中。目前，尚未发现在 SDN 中使用贝叶斯攻击图预测攻击者攻击路径的相关文献，而且在 SDN 中不同角色的网络设备所拥有的功能是有所差异的，相应地被攻击成功的概率有所差异，所以需要考虑 SDN 设备的多种角色。

为了全面准确地评估SDN设备的重要性以及预测 SDN 的攻击路径，本文提出了一个新的 SDN 安全评估方法，该方法根据 SDN 设备漏洞被利用的概率、设备在网络中的角色和 PR 算法度量了 SDN 设备的重要性，构建了 SDN 攻击图并结合贝叶斯理论度量了设备被攻击成功的概率。在评估模型基础上提出了一种安全预测算法，整合所有 SDN 设备信息，结合贝叶斯攻击图得出网络的安全风险态势，预测攻击者采取的攻击路径，通过实验验证本文所提方法的有效性。

2 SDN 安全评估与网络安全预测

本节主要围绕SDN安全评估和基于贝叶斯攻击图的网络安全预测两方面进行研究。

SDN 安全评估目前大体分为两类：使用图形安全模型或自定义的 SDN 安全指标评估。文献[11]

提出了一种使用预计算图形安全模型的SDN实时入侵响应框架，在该文献中采用分层攻击图模型以及通用漏洞评分系统评估设备的脆弱性。文献[12]提出了一种 SDN 威胁建模和安全分析的系统方法，在该文献中定义了 3 个新的安全指标表示SDN 的安全性，分别为网络度中心性、漏洞评分和攻击影响。文献[13]讨论了软件定义网络的移动网络的安全评估问题，结合移动自组网的特性提出了一种基于攻击图和层次分析法的安全评估方法。文献[14]提出了 3 层攻击图模型，该模型利用主机的漏洞信息评估主机的受损概率。图形安全模型存在可伸缩性和适应性问题，自定义安全指标未考虑到 SDN 控制器的漏洞被利用的概率，SDN 安全评估不够全面准确。

贝叶斯攻击图提供了一种比传统方法更紧凑的攻击路径表示方法，包含了网络中所有攻击路径信息，在不确定的条件下根据网络的漏洞率和设备信息结合贝叶斯推理方法为预测攻击路径提供了依据。文献[15]最早提出了一种利用贝叶斯网络对潜在攻击路径建模的方法。该方法通过将度量标准与贝叶斯网络的后验条件概率相关联实现对主机网络地定量脆弱性评估，使用桶消除算法更新，最大概率解释算法来计算相对于攻击者和攻击机制的先验知识的攻击路径的最优子集。文献[10]在静态贝叶斯双层网络结构模型的基础上，提出了一种基于贝叶斯的动态网络攻击行为预测方法。文献[11]根据正在进行的攻击使用预计算预测未来攻击的可能性。文献[16]提出了一种基于贝叶斯网络的加权攻击路径建模技术，结合基于关键点和关键边的多源最短路径优化算法找到最短路径。根据以上方法，结合 SDN 特性，在 SDN 安全评估基础上结合贝叶斯攻击图预测攻击者的攻击路径。

3　SDN 安全评估

为了对 SDN 的安全性做出全面准确的评估，本文通过给出 SDN 设备的漏洞利用概率和 SDN 设备关键度定义，结合 PR 算法评估 SDN 中每个设备的重要性，并根据 SDN 设备信息定义了 SDN 攻击图，结合贝叶斯理论评估设备被攻击成功的概率。

3.1　设备重要性度量

通过对 SDN 设备重要性的分析，设计了一种计算 SDN 设备重要性的算法。

3.1.1　设备重要性度量分析

安全评估可以量化或定性描述信息的安全风险，使管理者能够根据风险的严重性对安全风险进行排序，体现信息资产的价值，反映存在或可能存在的威胁和漏洞，确保现有控制措施及其对所识别风险的影响，确定潜在后果并最终确定其优先级[17-18]。PR 算法是 Google 提出的一个判断网页相对重要性级别的算法，该算法主要考虑了网络的拓扑链路关系和设备在网络中的位置。对于 SDN 集中控制的特性而言，每个网络设备的重要程度是有区别的，控制器对 SDN 来说是至关重要的，而且每个网络设备的漏洞被利用的概率也有差异。结合设备的漏洞利用概率、设备关键度和网络拓扑链路关系采用 PR 算法评估 SDN 设备的重要性，PR 值越高，说明设备越重要。

定义 1（SDN 设备漏洞利用概率） 每个 SDN 设备的一个漏洞可能被攻击者利用的概率。

通用漏洞评分系统[19]（common vulnerability scoring system，CVSS）基于定性和定量的指标，定义了安全漏洞的影响，计算过程整合了 3 个维度，即计算机系统的内在共性特征、时间特征及其环境因素。在 SDN 中，使用一个 CVSS 进行漏洞或风险分析，以评估安全漏洞的影响。利用 CVSS 的漏洞得分来度量 SDN 设备的漏洞利用概率 C_j。

虽然SDN设备漏洞利用概率在一定程度上评估了设备的安全风险，但有一些特定于 SDN 的重要因素并未包括在其中，这些因素影响着 SDN 的

安全性，扩大了 SDN 的脆弱性。如控制器的集中化管理将其数据转换为其他 SDN 设备的共享数据；OpenFlow 交换机允许所有使用者连接并进行流表修改、下发等操作。所以，SDN 中每个设备都扮演着不同的角色，拥有不同的功能，相应地重要性也不在一个级别上。文献[14]根据主机的角色设定其关键度，但主要针对数据平面的设备，没有将控制平面的关键设备控制器考虑在内，给出的设备关键度不够准确。本文将控制器考虑进去重新定义了 SDN 设备关键程度。

定义 2（SDN 设备关键度） 根据 SDN 设备在给定网络拓扑中的角色来设置其关键程度，控制器在网络中起着核心作用，关键度最高，其次是交换机，再者服务器，最后主机。

用 S 表示设备关键度级别，它是一个在[1,10]范围内的整数。主机的关键度级别 S_h 在 0～4 范围内，交换机和服务器的关键度级别 S_s 在 5～7 范围内，控制器的关键度级别 S_c 在 8～10 范围内。

PR 算法在初始时刻，根据 SDN 拓扑和链路关系构建初始概率矩阵，考虑到 SDN 设备的漏洞利用概率和关键度级别，本文在计算出 PR 值之后乘以SDN设备漏洞利用概率和关键度得出每个设备的重要性。将网络设备 e_j（j=1,…,N）的 PR 值记为 PR_j，计算式如下：

$$\mathrm{PR}_j(t)=c\sum_{i=1}^{j_a}\frac{\mathrm{PR}_j(t-1)}{K_j}+\frac{(1-c)}{N} \tag{1}$$

其中，N 表示网络设备总数；c 表示阻尼系数，这里取值为 0.85；K_j 表示设备 e_j 连接到其他设备的链路总数；j_a 表示连接到设备 e_j 的链路总数。不断迭代此计算式，直到满足式（2）时，算法终止。

$$\left|\mathrm{PR}_j(t)-\mathrm{PR}_j(t-1)\right|\leqslant\varepsilon \tag{2}$$

其中，ε 为无穷小量。

3.1.2 算法详细步骤

（1）根据 SDN 拓扑和链路关系构建初始概率矩阵 $\boldsymbol{G}_{N\times N}$，$\boldsymbol{G}$ 是一个 N 阶矩阵，G_{ij} 表示从设备 i 到设备 j 的转移概率。

（2）求归一化邻接矩阵 $\boldsymbol{M}$。

$$\boldsymbol{M}=c\boldsymbol{G}+(1-c)\boldsymbol{e} \tag{3}$$

其中，c 为阻尼系数，e 为特征向量。

（3）求 PR 值。

$$\mathrm{PR}=\boldsymbol{M}\times\boldsymbol{X} \tag{4}$$

其中，$\boldsymbol{X}$ 为 N 维列向量，初始时刻 $\boldsymbol{X}=\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}$，迭代执行式（4）直到 $\left|\mathrm{PR}-\boldsymbol{X}\right|\leqslant\varepsilon$ 算法结束，得到各网络设备的 PR 值。

（4）求 SDN 设备重要性 W_j。

$$W_j=\mathrm{PR}_j\times S_j\times C_j \tag{5}$$

算法 1 计算 SDN 设备重要性算法

输入初始概率矩阵 $\boldsymbol{G}$，阻尼系数 c，特征向量 $\boldsymbol{e}$，无穷小量 ε，N 维单位列向量 $\boldsymbol{X}$，N 维零列向量 PR，设备关键度 S

输出 SDN 设备的权重值 W

Initialization $\boldsymbol{G}$

$c=0.85,\varepsilon=0.00001,\boldsymbol{X}=\begin{bmatrix}1\\ \vdots\\ 1\end{bmatrix}$

For i =1 to N {

  For j=1 to N {

    Finding normalized adjacency matrix $\boldsymbol{M}_{ij}=c\boldsymbol{G}_{ij}+(1-c)\boldsymbol{e}_{ij}$ }}

For i =1 to N {

  For j=1 to N {

    Update $\mathrm{PR}_i=\boldsymbol{M}_{ij}\times\boldsymbol{X}_{i-1}$ }}

Record $\boldsymbol{X}_i=\mathrm{PR}_i$

While $\left|\mathrm{PR}_i-\boldsymbol{X}_{i-1}\right|\leqslant\varepsilon$

Record $W_i=\mathrm{PR}_i\times S_i\times C_i$

Return W_i

3.2 设备被攻击成功概率度量

基于提出的 SDN 攻击图定义，设计了一种计算设备被攻击成功的概率度量方法。

3.2.1　SDN 设备攻击图定义

参考 Poolsappasit 等[20]关于攻击图的定义修改为描述 SDN 中的攻击。以下所有节点代表 SDN 设备。

定义 3（SDN 攻击图）　SDN 攻击图是一个有向无环图，表示了 SDN 多步攻击之间的关系，图中每一个节点表示设备被攻击的属性状态，边值表示攻击成功的概率。

SDN 攻击图由四元组组成，设备信息集合 H、节点集合 N、攻击过程集合 E 和关系组合 β，表示为 SBAG=（H,N,E,β）。

（1）设备信息集合 H：表示一个 SDN 域内的资源设备的集合，$H=\{h_1,h_2,h_3,\cdots,h_n\}$，其中，$H=$（$h$,$r$,$W$,Impact）。

（2）节点集合 N：使用离散的随机变量表示攻击者在网络攻击过程中所拥有的资源和设备。$N=N_{\text{pro}}\cup N_{\text{post}}$，其中，$N_{\text{pro}}$ 代表初始节点，N_{post} 代表攻击者的目标节点，$N_i=\{<r,h>|r\in\mathbf{R}, h\in H\}$。

（3）攻击过程集合 E：$E=\{e_1,e_2,e_3,\cdots,e_n\}$，$e_i$ 表示攻击图中攻击者利用有限的资源从一个节点攻击到另一节点的中间过程，$e_i: N_{\text{pro}}\rightarrow N_{\text{post}}$，$\{N_{\text{pro}},N_{\text{post}}\in N$ 且 $N_{\text{pro}}\neq N_{\text{post}}\}$，$e_i=\{<r,h_s,h_d>|r\in\mathbf{R}, h_s\in H, h_d\in H\}$，$E$ 是有向边集合。

（4）β 表示关系组合（N_j,s_j），其中 $N_j\in N_{\text{post}}$，$s_j\in\{\text{AND,OR}\}$，节点到达 N_j 需要满足一定的条件，s_j 为到达节点的条件，如 s_j=AND，要求到达 N_j 的所有节点为可达状态，才能攻击成功。同理，s_j= OR，则到达 N_j 的节点状态中至少一个节点可达才能攻击成功。

3.2.2　设备被攻击成功的概率度量方法

将贝叶斯理论应用于 SDN 攻击图中，给出以下定义度量 SDN 设备被攻击成功的概率。

定义 4（条件概率）　每一个属性节点受其父节点的影响。因此，图中每一个节点都有一个条件概率分布，被称为局部条件概率分布函数。其中，属性节点 $N_j\in N_{\text{post}}$，$N_{\text{pro}}\in\text{parents}(N_j)$，在攻击 e_i: $N_{\text{pro}}\rightarrow N_{\text{post}}$ 中，属性节点 N_j 的条件概率计算式如下。

（1）当 $\beta=(N_j, s_j=\text{AND})$时：

$$P_e(N_j\,|\,\text{parents}(N_j))=\begin{cases}0,\ \exists\text{parents}(N_j)=0\\ P_e(\bigcap e_i),\ \text{其他情况}\end{cases}\tag{6}$$

（2）当 $\beta=(N_j,s_j=\text{OR})$时：

$$P_e(N_j\,|\,\text{parents}(N_j))=\begin{cases}0,\ \forall\text{parents}(N_j)=0\\ P_e(\bigcup e_i),\ \text{其他情况}\end{cases}\tag{7}$$

攻击事件之间通常是离散的，对于 s_j=AND 而言，同一攻击事件中同一层属性节点中的漏洞被利用是独立事件，目标节点被攻陷的概率取决于所有攻击轨迹中的漏洞被成功利用的概率，属性节点 N_j 的条件概率表示为：

$$P_e(\bigcap e_i)=\prod P_e(e_i)\tag{8}$$

而对 s_j=OR，目标节点被攻陷的条件为所有攻击轨迹中至少有一个漏洞被成功利用，节点 s_j 的条件概率表示为：

$$P_e(\bigcup e_i)=1-\prod[1-P_e(e_i)]\tag{9}$$

定义 5（无条件概率）表示属性节点的静态安全风险，无条件概率分布可以直观地展示网络系统的静态安全风险情况。对于节点 $N_j\in N_{\text{post}}$，被入侵的概率由其根节点被入侵的条件概率联合计算得到，计算式如下：

$$P_e(N_j)=\prod P_e(N_j\,|\,\text{parents}(N_j))\tag{10}$$

其中，parents(N_j)是属性节点 N_j 的父节点集合，$P_e(N_j|\text{parents}(N_j))$表示属性节点 N_j 受攻击的无条件概率，也称为先验概率，计算时需要将节点 N_j 受其父节点影响的条件概率与 $P_e(N_j)$受其根节点影响的条件概率关联起来。

4　SDN 安全预测

为了预防 SDN 设备被攻击，能够更准确地预测攻击者的攻击路径，通过算法模拟攻击状态变

迁过程，将 SDN 安全风险量化。根据状态发生概率矩阵转移次数，结合贝叶斯理论和 SDN 设备权重值预测攻击者采取的攻击路径。

4.1 SDN 安全风险态势值

基于 SDN 环境信息，利用工具 MulVAL（multi-host、multi-stage vulnerability analysis）生成攻击图。通过对攻击能力与防御策略的分析，结合 SDN 攻击图，判断攻击者的状态转移，以攻击为驱动，模拟攻击状态变迁过程，并将 SDN 安全风险量化。算法详细步骤如下。

（1）根据 SDN 攻击图初始化网络设备信息 H、攻击次数 r、节点概率 P、状态转移矩阵 NP。

（2）定期检测安全事件是否发生，发生时记录此次安全事件转移 SDN 设备 $N_i \rightarrow N_j$。

（3）根据当前发生的状态转换，以及状态转移矩阵，更新当前 SDN 设备的概率 P。

（4）根据贝叶斯条件概率、先验概率和已经发生的状态转移，进行递归计算，更新 SDN 设备 N_j 发生概率 P_j，并记录到 $\boldsymbol{M}_{r+1,j}$ 矩阵中。其中，⊕的运算规则依据定义 4 与 5 中的方法。

（5）根据设备一个漏洞的影响分数、权重值 W 和 SDN 设备发生概率矩阵 $\boldsymbol{M}$ 计算该 SDN 中每个网络设备的风险态势值 $\mathrm{NSM}_{r+1,j}$。

算法 2 预测 SDN 设备风险态势值算法

输入 SDN 攻击图 SBAG=（H,N,E,β）

输出 SDN 设备风险态势值矩阵 NSM，攻击次数 round

Initialization r=0, NP, P, H according to definition in the SBAG

Upon event state transition $N_i \rightarrow N_j$

Update $\mathrm{NP}_{i,j}$, P_j

For$i$ =1 to n {

For j=1 to n {

Update $P_j = P_1 \times \mathrm{NP}_{1,j} \oplus P_2 \times \mathrm{NP}_{2,j} \oplus \cdots \oplus P_n \times \mathrm{NP}_{n,j}$ and record $\boldsymbol{M}_{r+1,j} = P_j$ }}

Record round=r+1

For$j$=1 to n {

$\mathrm{NSM}_{r+1,j} = M_{r+1,j} W_j \mathrm{Impact}_j$ }

Record $\mathrm{NSM}_{r+1,j}$

Return NSM，round

4.2 攻击路径预测

在上一节算法执行过程中，算法每执行一次都会被记录到攻击次数 round 中。根据攻击次数 round 来预测攻击者多步攻击的步长，结合 SDN 攻击图中的所有攻击路径，找出相同步长的攻击路径。根据路径中每个设备的风险态势值算出每一条攻击路径风险值，找出风险值最大的攻击路径，预测此路径为攻击者将要走的攻击路径。

5 实验分析

本节搭建了一个实验拓扑环境，进行 SDN 安全评估和预测，分析实验结果，验证该安全评估和预测方法的有效性。

5.1 实验场景

假设搭建的网络拓扑如图 1 所示，网络中包括 SDN 控制平面上 3 台 SDN 控制器、6 台交换机、2 台虚拟机（virtual machine，VM）、4 台服务器和防火墙，其中防火墙上装有入侵检测系统（intrusion detection system，IDS）Snort。Snort IDS 包含由代理组成的 IDS 实例，IDS 实例负责分析网络流量以检测入侵或通信管理，网络流量分析通过检测器代理执行，通信管理通过代理执行。通过攻击图关联进行安全预测，由 IDS 生成的每个警报都将发送到 SDN 安全预测模块。在 SDN 安全预测模块，有安全预测算法，功能是通过攻击图映射和关联警报，对 SDN 进行安全预测，减少攻击带来更多的损失。通过查询漏洞数据库[21]（national vulnerability database，NVD），可以得到各网络设备的漏洞信息，见表 1。

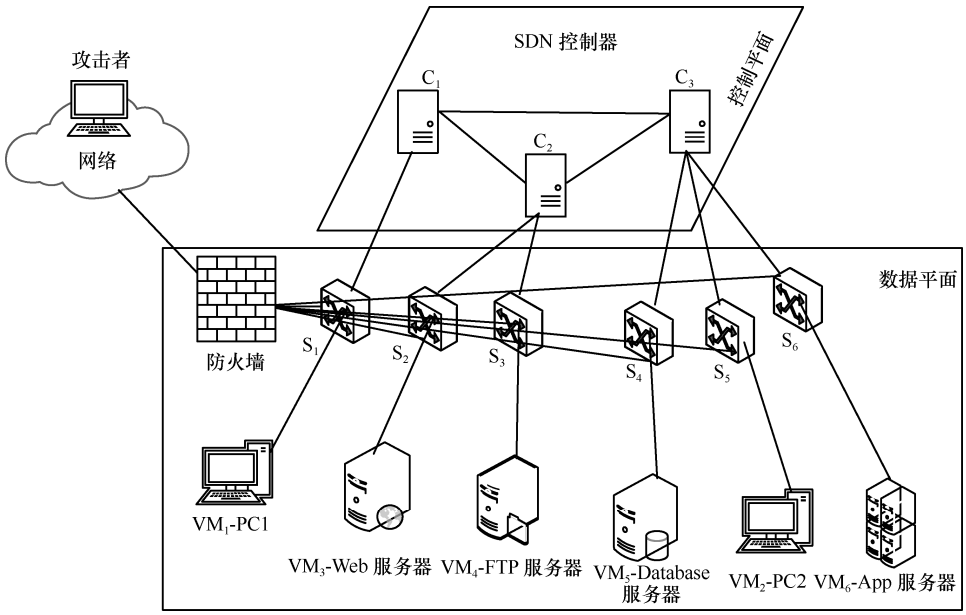


图 1　实验网络拓扑

表 1　SDN 设备信息及漏洞信息

Host	主机配置	服务	CvE ID	CVSS	Impact
VM_3	Windows Server 2008	apache	CVE-2014-0098	7	2.9
VM_4	RedHat Linux	Linux	CVE-2014-0038	7	10.0
VM_5	MySQL Server 2003	postgresql	CVE-2014-0063	6.5	6.4
VM_6	RedHat Enterprise Linux	Linux	CVE-2015-4002	9	8.5
S_1	OpenFlow Spec 1.3.0	Open vSwitch	CVE-2016-2074	7.5	6.4
S_2	OpenFlow Spec 1.3.0	Open vSwitch	CVE-2017-9265	7.5	6.4
S_3	OpenFlow Spec 1.3.0	Open vSwitch	CVE-2017-9263	3.3	2.9
VM_1	RedHat Linux	Linux	CVE-2014-0098	0.73	2.9
C_1	RedHat Linux	ONOS	CVE-2018-1000616	7.5	6.4
C2	RedHat Linux	ONOS	CVE-2018-1000615	5.0	2.9
C_3	RedHat Linux	ONOS	CVE-2018-1000614	7.5	6.4

5.2　实验结果分析

通过 IDEA 编写的 Java 程序和编写的 MATLAB 程序，根据部署的网络拓扑结构以及漏洞数据集，对 MulVAL 设置[22]。在一个 input.p 文件中定义谓词与事实，在 Linux 终端上执行输入文件，生成攻击图。由于 MulVAL 生成的攻击图比较复杂，对 MulVAL 生成的攻击图进行简化，如图 2 所示。图 2 中的椭圆表示原子攻击的节点，边值表示攻击发生的概率和攻击转移标识。图 2 中的节点标号与实际的 SDN 设备的对应关系见表 2。设置 IDEA 运行 Java 程序，用于生成攻击图的文件作为参数提供给 Java 程序计算度量。根据 SDN 设备漏洞，利用概率得到攻击图中 SDN 设备的转移概率见表 3。由攻击图得到所有可能的攻击路径

见表 4。

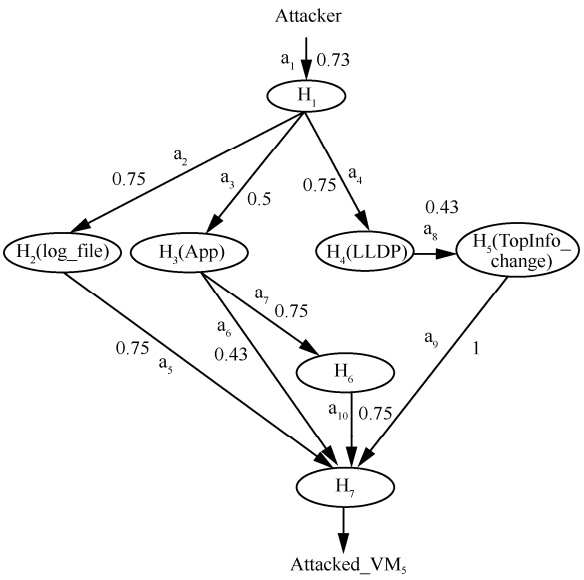


图 2　实验网络攻击图

表 2　攻击图节点与 SDN 设备对应关系

攻击图中的节点	SDN 设备名称
H_1	VM_1 主机
H_2	C_1 控制器
H_3	C_1 控制器
H_4	S_1 交换机
H_5	C_1 控制器
H_6	C_2 控制器
H_7	C_3 控制器

表 3　攻击图中 SDN 设备漏洞转移概率

状态转移	CVE#	转移概率
a_1	CVE 2014-0098	0.73
a_2	CVE-2018-1000616	0.75
a_3	CVE-2018-1000615	0.5
a_4	CVE-2017-9265	0.75
a_5	CVE-2018-1000614	0.75
a_6	CVE-2018-12691	0.43
a_7	CVE-2018-1000614	0.75
a_8	CVE-2017-13762	0.43
a_{10}	CVE-2018-1000616	0.75

表 4　攻击图中的所有攻击路径

路径编号	攻击路径
1	$H_0 \rightarrow H_1 \rightarrow H_2 \rightarrow H_7$
2	$H_0 \rightarrow H_1 \rightarrow H_3 \rightarrow H_6 \rightarrow H_7$
3	$H_0 \rightarrow H_1 \rightarrow H_3 \rightarrow H_7$
4	$H_0 \rightarrow H_1 \rightarrow H_4 \rightarrow H_5 \rightarrow H_7$

利用网络中的防火墙、Snort IDS 和主机安全审计日志采集网络中的异常信息，得到告警信息。利用自动化的工具分析告警数据，得到攻击路径，计算各阶段的攻击成功的概率。假设攻击者攻击 VM_1 主机，要通过此主机对 VM_5 攻击。

为了对 VM_5 进行攻击破坏，攻击者对目标网络进行 IP 地址扫描，搜寻有效主机。搜到主机 VM_1 会对其端口进行扫描，发现其通信端口为 80，并利用漏洞 CVE 2014-0098 获得 H_1 的 root 权限，成功概率为 0.73。攻击者可能有很多攻击途径对目标进行攻击破坏。攻击者可能利用恶意应用对控制器 C_1 进行攻击，对 C_1 控制器进行修改配置，利用多控制器之间的关系对 C_3 控制器进行攻击，从而达到对 VM_5 的破坏；通过 GUI 界面从北向接口入侵控制器 C_1，访问 C_1 控制器的日志文件，并对控制器 C_3 进行攻击；对交换机 S_1 进行攻击，修改链路层发现协议（link layer discovery protocol，LLDP），改变控制器 C_1 的拓扑信息，由于控制器之间的通信，将拓扑更改信息发送到 C_3 控制器，实现对控制器 C_3 的攻击，达到攻击目的。

对上述攻击的可能性，验证上一节算法对 SDN 设备地安全预测的有效性，分析攻击的可能性，并与实际的攻击状态比较。

（1）设备重要性分析

根据图 2 攻击图中设备在图 1 的链路拓扑关系构造初始概率矩阵 $\boldsymbol{G}$ 执行算法 1 得到各网络设备的权重值见表 5。

表 5　攻击图中 SDN 设备权重值

攻击图中的节点	SDN 设备权重值 W	关键度
H_1	0.179 404 8	4
H_2	0.910 372 5	9
H_3	0.910 372 5	9
H_4	1.318 03	7
H_5	0.910 372 5	9
H_6	0.691 12	8
H_7	1.166 265	9

（2）攻击行为模拟

由表 3 可知共有 10 种不同的状态转移情况，当发现攻击状态转移 a_1 时，初始状态的发生概率向量为 $P=\{1,0.73,0,0,0,0,0,0\}$，构造初始状态转移矩阵 NP，如下：

$$\begin{bmatrix} 1 & 0.73 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0.75 & 0.5 & 0.75 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0.75 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0.75 & 0.43 \\ 0 & 0 & 0 & 0 & 1 & 0.43 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0.75 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

根据生成的攻击图，对攻击图中所有 SDN 设备 N_j（j=1,…,N）计算被攻击成功的概率 P_j 并记录到概率发生矩阵 $\boldsymbol{M}_{r+1,j}$ 中，利用 MATLAB 进行仿真，执行算法 2 得到攻击过程中的状态发生概率矩阵如下：

$$\begin{bmatrix} 1 & 0.73 & 0.54 & 0.36 & 0.54 & 0.23 & 0.27 & 0.63 \\ 1 & 0.73 & 0.54 & 0.36 & 0.54 & 0.23 & 0.42 & 0.72 \\ 1 & 0.73 & 0.54 & 0.36 & 0.54 & 0.23 & 0.32 & 0.69 \end{bmatrix}$$

（3）SDN 风险态势分析

根据每个设备一个漏洞的影响分数、权重值 W 和 SDN 设备发生概率矩阵 $\boldsymbol{M}$，计算 SDN 设备风险态势值 $NSM_{r+1,j}$，如图 3 所示。

由图 3 可以看出，在 3 次攻击中各 SDN 设备的风险态势值。在每次攻击中，网络设备 H_7 的风险态势值最高，此结果与攻击者最后攻击目标是 H_7 相一致，验证了此算法的有效性。

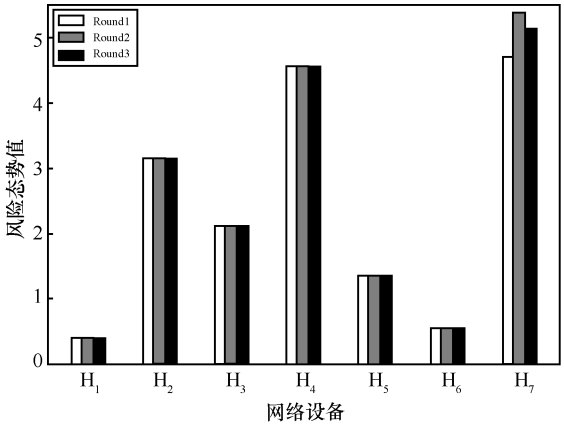


图 3　攻击图中 SDN 设备风险态势值

图 4 展示了攻击图中 4 个攻击路径中每个 SDN 设备的安全风险态势值、不同的攻击路径攻击者所采取的步长（3 步或 4 步）和每一个攻击路径中所攻击的网络设备及其风险态势值。网络设备 H_7 的风险最大，其次是网络设备 H_4，再者控制器 H_2。应该重点对设备 H_4 和 H_2 进行防御。

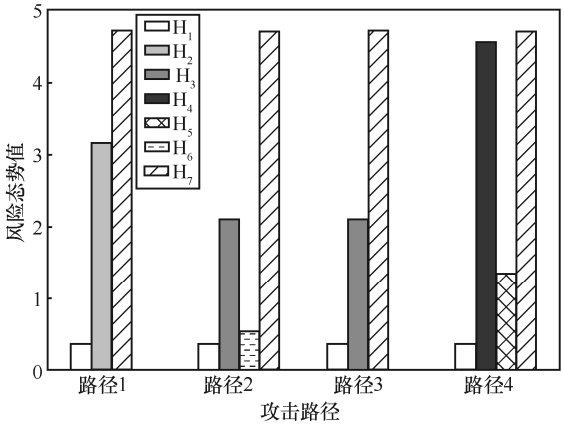


图 4　每个攻击路径中网络设备风险态势值

（4）攻击路径预测

在后续攻击状态转移过程中，状态发生概率矩阵转移了 3 次，预测整个攻击路径的长度为 4。攻击路径长度为 4 的攻击路径有路径 2 和路径 4，路径 2=H_0→H_1→H_3→H_6→H_7；路径 4=H_0→H_1→H_4→H_5→H_7。根据路径中每个设备的风险态势值计算出路径 2 的风险值为 2.22，路径 4 的风

险值为 11.93，因此，预测攻击者将要走路径 4。路径 4 中攻击者利用主机 VM_1 对交换机 S_1 进行攻击，修改 LLDP，改变控制器 C_1 的拓扑信息，利用多控制器之间的通信关系，将拓扑更改信息发送到 C_3 控制器，实现对控制器 C_3 的攻击，与实际情况一致，验证了此预测算法的准确性。从图 5 中看出路径 2 和路径 4 在第一步攻击之后，路径 4 的风险值都比路径 2 的风险值要大，第二步攻击是关键转折点，路径 4 第二步攻击对象是设备 H_4，下一步要对设备 H_4（交换机 S_1）重点防御。

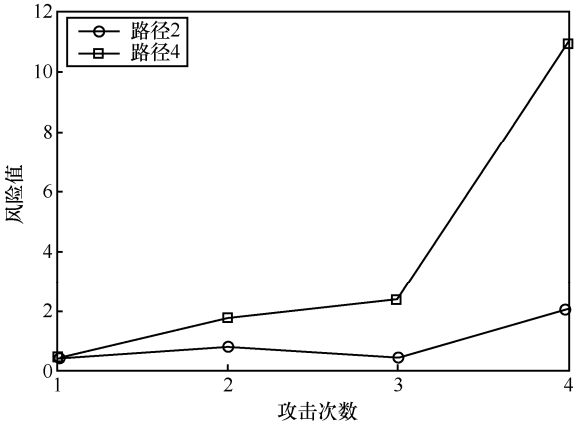


图 5　路径 2、路径 4 风险值对比

6　结束语

本文首先设计了一个新的评估SDN各设备安全性的方法，从 SDN 重要性和被攻击成功的概率两个方面进行评估，SDN 设备重要性从设备角色、漏洞被利用的概率和网络拓扑链路关系 3 方面进行度量，设备被攻击成功的概率在构建的 SDN 攻击图基础上结合贝叶斯理论进行度量。其次，提出了一种基于贝叶斯攻击图的 SDN 安全预测方法，通过算法模拟攻击者状态变迁过程，将 SDN 安全风险量化，根据状态发生概率矩阵转移次数预测攻击者的步长，结合 SDN 设备风险态势值计算出路径的风险值，预测出风险值最大的攻击路径为攻击者将要采取的攻击路径。最后，实验结果表明所提评估和预测方法准确，为 SDN 安全防御提供可靠的依据。

参考文献：

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

[2] SCHEHLMANN L, ABT S, BAIER H. Blessing or curse? Revisiting security aspects of Software-Defined Networking[C]//10th International Conference on Network and Service Management (CNSM) and Workshop. Piscataway: IEEE Press, 2014: 382-387.

[3] SCOTT-HAYWARD S, NATARAJAN S, SEZER S. A survey of security in software defined networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 623-654.

[4] KREUTZ D, RAMOS F M V, VERISSIMO P. Towards secure and dependable software-defined networks[C]//Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking - HotSDN '13. New York: ACM Press, 2013: 55–60.

[5] LEE S, YOON C, SHIN S. The smaller, the shrewder: a simple malicious application can kill an entire SDN environment[C]//Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. New York: ACM Press, 2016: 23-28.

[6] FERNANDES E L. Dpctl documentationcpqd/ofsoftswitch13 wiki github [EB]. 2018.

[7] ANTIKAINEN M, AURA T, SÄRELÄ M. Spook in your network: attacking an SDN with a compromised OpenFlow switch[C]//Secure IT Systems. Piscataway: Springer Press, 2014: 229-244.

[8] 任晓龙. 网络节点重要性排序算法及其应用研究[D]. 杭州: 杭州师范大学, 2015.
REN X L. The study of ranking algorithm of the important node in networks and its applications[D]. Hangzhou: Hangzhou Normal University, 2015.

[9] 游梦娜. 基于攻击图的网络脆弱性评估技术研究与实现[D]. 北京: 北京邮电大学, 2018.
YOU M N. Research and implementation of network vulnerability assessment technology based on attack graph[D]. Beijing: Beijing University of Posts and Telecommunications, 2018.

[10] 朱禹铭. 基于贝叶斯的动态网络攻击行为预测方法研究[D]. 秦皇岛: 燕山大学, 2019.
ZHU Y M. Research on dynamic network attack behavior prediction method based on Bayesian[D]. Qinhuangdao: Yanshan University, 2019.

[11] EOM T, HONG J B, AN S, et al. A framework for real-time intrusion response in software defined networking using precomputed graphical security models[J]. Security and Communication Networks, 2020: 1-15.

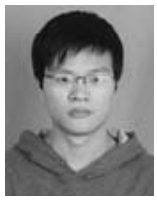
[12] EOM T, HONG J B, AN S, et al. A systematic approach to threat modeling and security analysis for software defined networking[J]. IEEE Access, 2019, 7: 137432-137445.
[13] LUO S, DONG M, OTA K, et al. A security assessment mechanism for software-defined networking-based mobile networks[J]. Sensors (Basel, Switzerland), 2015, 15(12): 31843-31858.
[14] YOON S, CHO J H, KIM D S, et al. Attack graph-based moving target defense in software-defined networks[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1653-1668.
[15] LIU Y, MAN H. Network vulnerability assessment using Bayesian networks[C]//Defense and Security. Proc SPIE 5812, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005.Piscataway: Society of Photo-Optical Instrumentation Engineers (SPIE) Press, 2005, 5812: 61-71.
[16] ZIMBA A, CHEN H S, WANG Z S. Bayesian network based weighted APT attack paths modeling in cloud computing[J]. Future Generation Computer Systems, 2019, 96: 525-537.
[17] Information security risk assessment[EB].2019.
[18] Definition - what does risk analysismean? [EB].2019.
[19] JOHNSON P, LAGERSTRÖM R, EKSTEDT M, et al. Can the common vulnerability scoring system be trusted? A Bayesian analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(6): 1002-1015.
[20] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic security risk management using Bayesian attack graphs[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(1): 61-74.
[21] Information Technology Labortory.National vulnerability database version 2.5[S]. 2018.
[22] OU X, GOVINDAVAJHALA S, APPEL A W. MulVAL: alogic-based network security analyzer[C]//USENIX Security Symposium. Piscataway: USENIX Press, 2005: 113-128.

[作者简介]

尹彦尚（1998− ），女，浙江工商大学硕士生，主要研究方向为软件定义网络。

索同鹏（1995− ），男，浙江工商大学硕士生，主要研究方向为软件定义网络。

董黎刚（1973− ），男，博士，浙江工商大学信息与电子工程学院院长、教授、硕士生导师，中国电子学会高级会员，浙江省计算机学会理事，主要研究方向为新一代网络和分布式系统。



蒋献（1988− ），男，浙江工商大学实验师，主要研究方向为数字电路和模拟电路。