基于隐马尔科夫模型的网络安全风险评估方法

王增光[1]，卢　昱[1]✉，赵东昊[2]
(1.陆军工程大学石家庄校区装备指挥与管理系，石家庄，050003；
2.陆军工程大学石家庄校区装备模拟训练中心，石家庄，050003)

摘要　为了能实时准确地评估网络安全风险，提出一种基于隐马尔科夫模型的网络安全风险评估方法。该方法基于隐马尔科夫模型对目标网络进行建模，通过节点的直接风险和相关性引起的间接风险来量化节点的安全风险；考虑节点在网络中的重要性程度，结合节点安全风险，量化目标网络的整体安全风险。通过实验对所提方法进行验证。实验结果表明：该方法能够对由节点相关性和节点重要性程度所带来的网络安全风险进行量化，使得网络安全风险评估结果更加准确、可信。与传统的网络安全风险评估方法相比，该方法能够更加及时地发现网络中的异常风险变化情况，为网络安全防御策略的及时调整提供依据。

关键词　风险评估；隐马尔科夫模型；节点安全风险；网络安全风险
DOI　10.3969/j.issn.1009-3516.2019.03.012
中图分类号　TP309　　**文献标志码**　A　　**文章编号**　1009-3516(2019)03-0071-06

Network Security Risk Assessment Method Based on Hidden Markov Model

WANG Zengguang[1], LU Yu[1]✉, ZHAO Donghao[2]
(1. Equipment Command and Administration Department, Shijiazhuang Campus of Army Engineering University, Shijiazhuang 050003, China; 2. Equipment Simulation Training Center, Shijiazhuang Campus of Army Engineering University, Shijiazhuang 050003, China)

Abstract: A new network security risk assessment method based on hidden Markov model is proposed in order to accurately assess the network security risk in real time. The method is based on Hidden Markov model to model the target network. The security risk of node is quantified by direct risk and indirect risk caused by correlation of the node. Considering the importance of nodes in the network, the overall security risk of the target network is quantified on the basis of node security risk. The experimental results show that the method can quantify the network security risk caused by the correlation and importance of the node, which makes the network security risk assessment results more accurate and credible. Compared with traditional network security risk assessment methods, this method can detect abnormal risk changes in the work more timely ,which can provide the basis for the timely adjustment of the network security defense strategy.

Key words: risk assessment; hidden Markov model; node security risk; network security risk

收稿日期：2018-06-10
基金项目：国家自然科学基金(61271152)；国家社会科学基金(15GJ003-184)
作者简介：王增光(1991—)，男，河南省驻马店人，博士生，主要从事装备保障信息化研究。E-mail：wang1223797579@163.com
通信作者：卢　昱(1960—)，男，河南洛阳人，教授，主要从事网络安全研究。E-mail：wzg6410@163.com

引用格式：*王增光，卢昱，赵东昊. 基于隐马尔科夫模型的网络安全风险评估方法[J]. 空军工程大学学报(自然科学版)，2019，20(3)：71-76. WANG Zengguang, LU Yu, ZHAO Donghao. Network Security Risk Assessment Method Based on Hidden Markov Model[J]. Journal of Air Force Engineering University (Natural Science Edition), 2019, 20(3): 71-76.*

网络安全是确保网络能够为人们提供便捷服务的基础。随着网络攻击手段的日益多样化,网络安全问题面临越来越严峻的考验[1]。网络安全风险评估能够在攻击行为发生之前对网络安全风险进行准确评估,为实现网络主动防御进而确保网络安全提供技术支撑[2-3]。

作为网络安全领域的研究热点之一,网络安全风险评估技术取得了丰硕的研究成果[4]。文献[5]构建了风险评估指标体系,结合层次分析法和灰色聚类法对无线网络安全风险进行评估,解决了网络评估过程中评价指标的子因素较多的问题,但是指标体系的构建主观性较强,且该方法不能实时评估网络安全风险。文献[6]基于贝叶斯攻击图对目标网络进行风险评估,结合入侵检测信息对生成的贝叶斯攻击图进行动态更新达到实时评估网络安全风险的目的,但是在评估的过程中没有考虑网络节点相关性对网络安全风险的影响。文献[7]提出了一种优化的实时网络安全风险评估方法,减小了评估过程中的输入参数规模,但是在评估过程中通过主机风险相加的方式来量化网络的整体风险,没有考虑网络中主机的重要性程度,与网络实际情况不符。

针对上述研究成果中存在的问题,提出了一种基于隐马尔科夫模型(Hidden Markov Model, HMM)的网络安全风险评估方法。该方法通过不同时刻网络节点的安全状态和状态风险值来量化节点的直接风险;考虑节点之间的相关性,来量化节点的间接风险;根据直接风险和间接风险的量化结果来评估节点的实际风险情况;结合节点的权重,对网路的整体安全风险进行评估。

1 基于 HMM 的网络安全风险评估模型

1.1 网络安全风险评估框架

在实际运行的网络环境中,节点状态的变化符合 HMM 模型的规律[8-9];节点之间的特殊逻辑关系,如控制关系、访问关系等会对网络安全风险评估的结果带来一定的影响;节点在网络中地位不同,受到攻击时所带来的安全风险也不尽相同。因此,本文提出了网络安全风险评估框架,如图 1 所示。

该框架采用自底向上结构,首先根据网络中节点在某时刻处于某种安全状态的概率和该种安全状态的风险值来计算节点的直接安全风险;考虑节点的相关性对网络安全风险评估的影响,结合节点的相关性系数和相关节点的安全风险,计算节点的间接安全风险;进而根据节点的直接风险和间接风险来评估节点的安全风险。最后,结合节点在网络中的权重,对整个网络的安全风险进行评估。

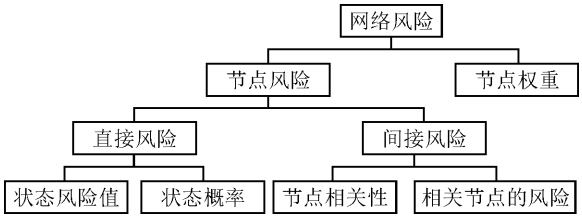

图 1 网络安全风险评估框架

1.2 隐马尔科夫模型

目标网络的安全风险可以通过隐马尔科夫模型来体现,隐马尔科夫模型可以通过五元组 $Mar=\{S,Y,\boldsymbol{Q},\boldsymbol{T},\boldsymbol{\lambda}\}$来定义[10-11]。其中:

1)$S=\{s_1,s_2,\cdots,s_m\}$为网络节点安全状态的集合。由于网络是一个不断变化的复杂系统,节点的安全状态会随着时间的变化而不断变化[12]。因此,采用随机过程$\{X_t|X_t\in S\}$来表示 t 时刻节点所处的安全状态。在实际的评估过程中,为了降低转移矩阵的规模,可以根据网络安全等级保护的思想对网络节点安全状态进行合理分类。

2)$Y=\{y_1,y_2,\cdots,y_m\}$为能够检测到的网络中不同种类攻击的集合。网络中的攻击行为会随着时间的变化而不断变化[13]。因此,采用随机过程$\{Z_t|Z_t\in Y\}$来表示 t 时刻检测到的攻击种类。为了降低观测矩阵的规模,也可以将攻击行为进行合理分类。

3)$\boldsymbol{Q}=[a_{ij}]$为安全状态转移矩阵。其中,$a_{ij}=P(x_{t+}1=s|X_t=s_i)$,$1\leqslant i,j\leqslant m$,表示节点在 t 时刻的安全状态为 s_i,在 $t+1$ 时刻转化为 s_j 的概率。

4)$\boldsymbol{T}=[b_j(k)]$为安全状态观测矩阵。其中,$b_j(k)=P(y_k|s_j)$,$1\leqslant k\leqslant n$,$1\leqslant j\leqslant m$,表示节点处于状态 s_j 时,受到 y_k 攻击的概率。

5)$\boldsymbol{\lambda}=[\lambda_1,\lambda_2,\cdots,\lambda_m]$为初始安全状态向量。其中,$\lambda_1=P(X_0=s_i)$,$1\leqslant i\leqslant m$,表示节点在时刻 0 处于安全状态 s_i 的概率。

2 节点风险计算

节点之间的相关性会对节点的风险值带来一定的影响[14]。传统的网络安全风险评估方法只对节

点自身的安全风险进行评估，会导致评估结果不够准确[15]。因此，本节从直接风险和间接风险两方面对节点风险进行计算。

2.1　直接风险

直接风险指节点自身所处安全状态所带来的风险，记为 $DR_k(t,j)$。$DR_k(t,j)$的计算不考虑节点的相关性，可以通过 t 时刻节点 k 所在某种安全状态的概率与该状态下的风险值来计算。

节点 k 的在时刻 t 处于状态的 S_i 概率定义为 $\lambda_{k,t}=\{\lambda_{k,t}(i,j),1\leqslant i\leqslant m,1\leqslant j\leqslant n\}$。$\lambda_{k,t}(i,j)$可以通过式(1)进行计算：

$$\lambda_{k,t}(i,j)=P(X_i=s_i\mid Z_t=y_j)=\frac{P(X_i=s_i,Z_t=y_j}{P(z_t=y_j))}=\frac{P(Z_t=y_j\mid X_t=s_i)P(X_t=s_i)}{\sum_{k=1}^{N}[P(Z_t=y_j\mid X_t=s_k)P(X_t=s_k)]}\tag{1}$$

式中：

$$P(X_i=s_i)=\sum_{j=1}^{N}P(x_t=s_i,X_0=s_j)=\sum_{j=1}^{N}P(X_t=s_i\mid X_0=s_j)P(X_0=s_j)=\sum_{j=1}^{N}a_{ji}^{(t)}\lambda_j\tag{2}$$

式中：$s_i\in S$，$y_j\in Y$，$a_{ji}^{(t)}$ 表示节点 k 的第 t 步的转移概率。

针对节点所处的安全状态，引入节点状态风险值向量 $\boldsymbol{R}=(r_1,r_2,\cdots,r_m)$来表示节点所处安全状态的风险值[10]。$r_i$ 表示节点在安全状态 s_i 时的风险值，可以根据具体的网络环境进行具体定义。

根据节点 k 在时刻 t 所处安全状态的概率和该状态下的风险值，$DR_k(t,j)$的计算公式为：

$$DR_k(t,j)=\sum_{i=1}^{M}\lambda_{k,t}(i,j)r_i\tag{3}$$

2.2　间接风险

节点的相关性是基于物理连接关系上的一种特殊访问关系。间接风险是指由节点之间的相关性而引起的网络安全风险，记为 $IR_k(t,j)$。与节点 k 具有相关性关系的节点共有 m 个，记为 $k_1,k_2,\cdots,k_m$。为了更好的体现相关性对节点风险的影响程度，参照文献[16]中对节点关联性的研究，引入了相关性量化值的概念，记为 $W_{k_l,k}$。$W_{k_l,k}$表示利用相关性关系攻击成功的概率，可以根据具体的网络环境、实践经验等确定不同的取值。$W_{k_l,k}$ 的取值范围为[0，1]，取值越大节点 k 的风险受相关节点的影响程度越大。与节点 k 具有相关性关系的节点在 t 时刻的风险值，记为 $r_{k_l}(t,j)$，$1\leqslant l\leqslant m$，$1\leqslant j\leqslant n$。具有相关性关系的节点对节点 k 的风险影响值记为 $\Delta r_{k_l}(t,j)$，$1\leqslant l\leqslant m$，$1\leqslant j\leqslant n$，可以通过相关性量化值和相关节点的风险值来计算，具体计算公式如下：$\Delta r_{k_l}(t,j)=W_{k_l,k}r_{k_l}(t,j)$。节点 k 的间接风险是由节点间的特殊访问关系带来的。因此，间接风险的取值可以通过风险影响值的叠加获得，即：

$$IR_k(t,j)=\sum_{l=1}^{M}\Delta r_{k_l}(t,j)=\sum_{l=1}^{M}\{W_{k_l,k}r_{k_l}(t,j)\}\tag{4}$$

2.3　节点风险

节点的风险由 $DR_k(t,j)$和 $IR(t,j)$共同决定。根据网络运行的实际情况不同，$DR(t,j)$和 $IR_k(t,j)$对节点风险的影响程度不同。因此，节点风险的计算不能简单的通过将 $DR_k(t,j)$和 $IR_k(t,j)$相加求得，需要选择合适的函数 $f(x)$来体现 $DR_k(t,j)$和 $IR_k(t,j)$对节点风险的影响程度，以便得到更加符合网络实际情况的节点风险值。当节点的之间的关联性较强时，节点的风险值主要由间接风险决定；反之，节点的风险主要由直接风险决定。节点风险 $R_k(t)$的计算公式为：

$$R_k(t)=f(x)DR_x(t,j)+[1-f(x)]IR_k(t,j)\tag{5}$$

式中：$f(x)$是间接风险的权重函数，代表间接风险在节点风险中所占的比重，x 对应 $IR_k(t,j)$所对应的相关性量化值。函数 $f(x)$的选取可以根据网络的具体环境选择不同的形式，但需要满足以下特性：①与相关性量化值有关；②[0，1]区间上的单调递减函数；③$f(x)$的取值范围在 0 和 1 之间。

3　网络风险计算

在实际的网络环境中，节点在网络中的位置不同，其对网络整体风险的影响也不尽相同[17-18]。显然，核心节点被攻陷要比边缘节点被攻陷对网络安全的影响更大。因此，在评估目标网络的整体安全风险时，采取单个节点风险累加求和的评估方式所得到的结果并不准确。需要结合节点在网络中的权重，来对目标网络进行整个风险评估。

3.1　节点权重

节点的权重主要用来衡量节点在网络中的重要性程度，取决于节点提供服务的种类和服务的重要性。一个节点提供的服务种类越多，服务的重要性程度越到，则节点越重要[19]。因此，节点 k 的权重 V_k 的计算公式为：

$$V_k = \sum_{j=1}^{n} N_j \tag{6}$$

式中:n 为节点 k 所提供的服务的种类数;N_j 为该服务在整个网络服务中所占的权重。为了确保节点的权重之和为 1,当几个节点提供同一种服务时,将给服务的权重平均分配给该节点。

服务的重要性主要取决于服务的主流性,其次取决于服务涉及到的用户数目,最后受用户访问频率的影响。这符合帕累托分析法的思想。因此,依照帕累托分析法的原则,将服务的主流性、涉及到的用户数据和用户访问的频率对服务的重要性的影响系数分别设为 4/5,4/25,1/25。服务的重要性 M 的计算公式为:

$$M=\frac{4}{5}M_{ms}+\frac{4}{25}M_{un}+\frac{1}{25}M_{af} \tag{7}$$

式中:M_{ms} 为服务的主流性值,主流性的判断是一个布尔变量;M_{un} 表示服务涉及到的用户数据所对应的量化值;M_{af} 表示用户访问频率对应的量化值。上述参量对应的量化值可以根据网络的具体情况设定合适的取值区间。对 M 进行归一化处理,即可得到服务在整个网络服务中所占的权重 N_j:

$$N_j = \frac{M_j}{\sum_{t=1}^{n} M_t} \tag{8}$$

3.2 网络风险

当目标网络中有 m 个节点时,通过第 2 节中的节点风险的计算方法对节点的安全风险进行量化,记为 $R_k(t)$。为了能够更加真实地反应网络的风险值,不采用传统的单个主机风险直接相加的方式来计算网络风险值。结合节点在网络中权重和节点的风险值来评估网络风险值 $R(t)$,具体计算公式为:

$$R(t) = \sum_{k=1}^{m} V_k R_k(t) \tag{9}$$

4 实验验证

4.1 实验环境

搭建了典型的实验环境来验证本文提出的基于隐马尔科夫模型的网络安全风险评估方法的可行性和有效性,实验环境的网络拓扑图见图 2。防火墙将网络分为两部分:外网和内网。外网中的终端通过 Internet 对内网中的节点进行访问,为了便于说明问题,实验环境中外网由 5 个相同地位的终端组成,将其统称为 A;内网由终端 B、Web 服务器 C、内部管理员 D 和数据库服务器 E 组成。

在实验环境中,防火墙只允许外网中的终端 A 访问 Web 服务器 C 的网路服务和内部管理员 D、终端 B 的所有端口;内网节点对外网的访问不受限制。在内网中,内部管理员 D 能够通过 SNMP 服务对数据库服务器 E 进行管理,同时能够访问 Web 服务器;终端 B 能够在内部管理员 D 上发布或者获取信息,并能够访问 Web 服务器 C,但是不能执行系统命令;Web 服务器 C 能够向数据库服务器读写信息,但是不能管理数据库服务器。攻击者通过外部网络对内网发动攻击,最终的目的是获得能够修改数据库服务器的权限。

为了便于验证本文所提出的方法,结合具体的实验环境,将网络的安全状态划分为 4 类,即安全状态 G、刺探状态 P、攻击状态 A 和攻陷状态 C。同理,为了降低观测矩阵的规模,参照文献[20]对原始报警信息的分类方法,根据报警信息的严重程度,将原始报警信息分为了 10 类。

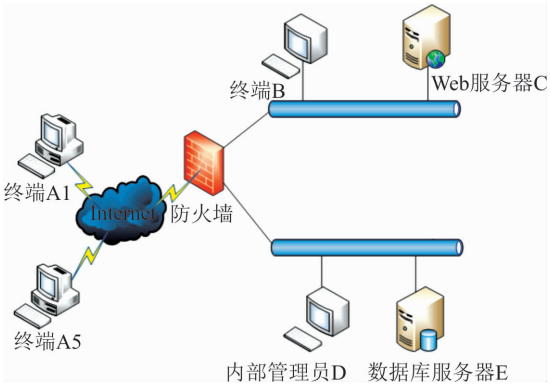

图 2 实验环境的网络拓扑图

4.2 实验结果分析

借助 CNSIS 局域网模拟实验环境中的外部终端 A_i,$1\leqslant i\leqslant 5$ 所组成的局域网。在 12 h 内通过 A_i 持续与内部网路中的不同节点进行通信,记录提供服务的相关参量,根据节点权重的量化方法,对实验环境中节点的重要性程度进行量化:$V_{A_i}=0.056$,$1\leqslant i\leqslant 5$;$V_B=0.086$;$V_C=0.198$;$V_D=0.104$;$V_E=0.332$。

根据文中所提出的方法对网络安全风险进行量化,以节点 B 为例进行说明。根据文献[21]提出的原则,结合实验环境的运行情况,将节点 B 的初始安全状态概率分布设置为 $\boldsymbol{\lambda}_B=(0.8,0.1,0.05,0.05)$,状态风险值为 $\boldsymbol{R}_B=(1,5,15,25)$。根据采集到的网络状态变化情况和报警信息,配置节点 B 的安全状态转移矩阵和观测矩阵:

$$\boldsymbol{Q}_B=\begin{bmatrix} 0.948 & 0.018 & 0.024 & 0.01 \\ 0.014 & 0.944 & 0.022 & 0.02 \\ 0.011 & 0.013 & 0.966 & 0.01 \\ 0.012 & 0.014 & 0.004 & 0.97 \end{bmatrix}$$

$$\boldsymbol{T}_B=\begin{bmatrix}0.2 & 0.1 & 0.15 & 0.1 & 0.15 & 0.1 & 0.05 & 0.05 & 0.025 & 0.075\\ 0.25 & 0.015 & 0.1 & 0.15 & 0.1 & 0.1 & 0.08 & 0.035 & 0.02 & 0.015\\ 0.27 & 0.15 & 0.1 & 0.14 & 0.12 & 0.03 & 0.06 & 0.06 & 0.045 & 0.025\\ 0.3 & 0.1 & 0.12 & 0.14 & 0.05 & 0.05 & 0.08 & 0.07 & 0.055 & 0.035\end{bmatrix}$$

间接风险的权重函数设置为 $f(x)=x^2-2x+1$。根据实验环境的访问规则，节点 B 的相关性量化值见表 1。

表 1　节点 B 的相关性量化值

相关节点	量化值
A_1B	0.2
A_2B	0.2
A_3B	0.2
A_4B	0.2
A_5B	0.2
CB	0.3
DB	0.5

根据 IDS 给出的报警信息，对节点 B 的安全风险进行量化；同理，对其他节点的安全风险进行量化；进而对网络安全风险进行量化。采用相同的数据集，将本文所提出的网络安全风险评估方法（以下简称本文方法与考虑节点重要程度但不考虑节点相关性的网络安全风险评估方法（以下简称方法 1）和不考虑节点相关性和节点重要程度的网络安全风险评估方法（以下简称方法 2）进行对比，网络安全风险评估结果见图 3。

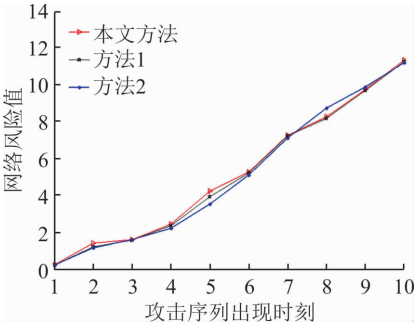

图 3　网络安全风险评估结果

由图 3 可知，本方法得到的网络风险值的变化趋势与方法 1 和方法 2 的变化趋势基本吻合，说明本文方法能够有效的网络中的安全风险进行评估。与方法 1 和方法 2 相比，本文方法由于在评估的过程中考虑了节点相关性和节点权重对网络安全风险的影响，网络安全风险值变化更加明显，有利于管理人员更加及时地发现网络风险情况，调整网路安全策略。在时刻 5 和 8，本文方法和方法 1 的评估结果相对于方法 2 的评估结果有较大的波动，是因为本文方法和方法 1 在评估的过程中考虑了节点权重的影响，某些风险值很低但权重较大或风险值较高但权重较低的节点的出现会导致以上情况发生。在时刻 2 和 5，本文方法相对于方法 1 的评估结果有明显变化，是因为本文方法在评估的过程中考虑了节点相关性对网络安全风险的影响，相关节点的风险会带来网络安全风险的变化。

因此，相对于传统的网络安全风险评估方法，本方法更加详细的考虑了实际网络的运行情况，能够更加准确的评估网络的安全风险，及时发现网络中的异常风险变化情况，为网络安全防护策略的制定与调整提供依据。

5　结语

本文提出了一种基于隐马尔科夫模型的网络安全风险评估方法。该方法基于隐马尔科夫模型对目标网络进行建模，从网络安全状态出发来评估网络的实时风险状况。在评估的过程中考虑了节点之间相关性和节点权重对网络安全风险的影响，更加符合网络运行的实际情况。对比实验证明，该方法能够更加准确的评估网络安全风险，为网络安全风险策略的制定和调整提供支撑。

参考文献(References)：

[1] 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. (in Chinese)

[2] 张利，彭建芬，杜宇鸽，等. 信息安全风险评估的综合评估方法综述[J]. 清华大学学报(自然科学版)，2012，52(10)：1364-1369.
ZHANG L, PENG J F, DU Y G, et al. Information Security Risk Assessment Survey [J]. Journal of Tsinghua University (Science&Technology), 2012, 52(10):1364-1369. (in Chinese)

[3] LIU G, LI Q M, ZHANG H. Reliability Vector Orthogonal Projection Decomposition Method of Network Security Risk Assessment [J]. Journal of Electronics & Information Technology, 2012 34(8):1934-1938.

[4] 陈建莉. 基于未确知数学的网络安全风险评估模型[J]. 空军工程大学学报(自然科学版)，2014，15(2)：91-94.
CHEN J L. A Network Security Risk Assessment Model Based on Unascertained Mathematics [J]. Journal of Air Force Engineering University (National Science Edition), 2014, 15(2):91-94. (in Chinese)

[5] 傅建新，黄联芬，姚彦. 基于层次分析法-灰色聚类的无

线网络安全风险评估方法[J].厦门大学学报(自然科学版),2010,49(5):622-626.
FU J X, HUANG L F, YAO Y. Risk Evaluation of Wireless Network Security Based on AHP-Grey Clustering Method [J]. Journal of Xiamen University (Natural Science), 2010,49(5):622-626. (in Chinese)

[6] POOLSAPPASIT N, DEWRI R, RAY I. Dynamic Security Risk Management Using Bayesian Attack Graphs [J]. IEEE Trans on Dependable and Secure Computing, 2012, 9(1):61-74.

[7] 龙门,夏靖波,张子阳,等.节点相关的隐马尔科夫模型的网络安全评估[J].北京邮电大学学报,2010,33(6):121-124.
LONG M, XIA J B, ZHANG Z Y, et al. Network Security Assessment Based on Node Correlated HMM [J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(6):121-124. (in Chinese)

[8] 吴建台,刘光杰,刘伟伟,等.一种基于关联分析和HMM的网络安全态势评估方法[J].计算机与现代化,2018(6):30-36.
WU J T, LIU G J, LIU W W, et al. Cyber Security Situation Evaluation Method Based on Association Analysis and Hidden Markov Model [J]. Computer and Modernization, 2018(6):30-36. (in Chinese)

[9] 王笑,李千目,戚湧.一种基于马尔科夫模型的网络安全风险实时分析方法[J].计算机科学,2016,43(11A):338-341.
WANG X, LI Q M, QI Y. Real Time Analysis Method of Network Security Risk Based on Markov Model [J]. Computer Science, 2016, 43(11A):338-341. (in Chinese)

[10] 李伟明,雷杰,董静,等.一种优化的实时网络安全风险量化方法[J].计算机学报,2009,32(4):793-804.
LI W M, LEI J, DONG J, et al. An Optimized Method for Real Time Network Security Quantification [J]. Chinese Journal of Computers, 2009, 32(4):793-804. (in Chinese)

[11] 周末,张宏, 李博涵.基于攻防状态图模型的网络风险评估方法[J].东南大学学报(自然科学版),2016,46(4):688-694.
ZHOU W, ZHANG H, LI B H. Network Risk Assessment Method Based on Attack-Defense Graph Model [J]. Journal of Southeast University (Natural Science Edition), 2016, 46(4):688-694. (in Chinese)

[12] 刘建峰,陈健.基于模糊博弈规则的网络节点入侵风险评估[J].计算机科学,2018,45(10):138-141.
LIU J F, CHEN J. Evaluation of Network Node Invasion Risk Based on Fuzzy Game Rules [J]. Computer Science, 2018, 45(10):138-141. (in Chinese)

[13] 刘刚.网络安全风险评估、控制和预测技术研究[D].南京:南京理工大学,2014.
LIU G. Research on Network Security Risk Assessment Control and Prediction Technology [D]. Nanjing: Nanjing University of Science &Technology, 2014. (in Chinese)

[14] 葛海慧,肖达,陈天平,等.基于动态关联分析的网络安全风险评估方法[J].电子与信息学报,2013,35(11):2630-2636.
GE H H, XIAO D, CHEN T P, et al. Quantitative Evaluation Approach for Real-Time Risk Based on Attack Event Correlating [J]. Journal of Electronics & Information Technology, 2013, 35(11):2630-2636. (in Chinese)

[15] SEN A, MADRIA S. Risk Assessment in a Sensor Cloud Framework Using Attack Graphs [J]. IEEE Transactions on Services Computing, 2017, 10(6):942-955.

[16] 张永铮,方滨兴,迟悦,等.网络风险评估中网络节点关联性的研究[J].计算机学报,2007,30(2):234-240.
ZHANG Y Z, FANG B X, CHI Y, et al. Research on Network Node Correlation in Network Risk Assessment, 2007, 30(2):234-240. (in Chinese)

[17] 陈天平,孟相如,崔文岩,等.基于网络可生存性态势感知的主动服务漂移模型[J].空军工程大学学报(自然科学版),2015,16(6):64-68.
CHEN T P, MENG X R, CUI W Y, et al. A Proactive Service Migration Model Based on Network Survivability Situation Awareness [J]. Journal of Air Force Engineering University (National Science Edition), 2015, 16(6):64-68. (in Chinese)

[18] 刘玉岭,冯登国,连一峰,等.基于时空维度分析的网络安全态势预测方法[J].计算机研究与发展,2014,51(8):1681-1694.
LIU Y L, FENG D G, LIAN Y F, et al. Network Situation Prediction Method Based on Spatial-Time Dimension Analysis [J]. Journal of Computer Research and Development, 2014, 51(8):1681-1694. (in Chinese)

[19] 陈天平,许世军,张串绒,等.基于攻击检测的网络安全风险评估方法[J].计算机科学,2010,37(9):94-96.
CHEN T P, XU S J, ZHANG C R, et al. Risk Assessment Method for Network Security Based on Intrusion Detection System [J]. Computer Science, 2010, 37(9):94-96. (in Chinese)

[20] 席荣荣,云晓春,张永铮,等.一种改进的网络安全态势量化评估方法[J].计算机学报,2015,38(4):749-758.
XI R R, YUN X C, ZHANG Y Z, et al. An Improved Quantitative Evaluation Method for Network Security [J]. Chinese Journal of Computers, 2015, 38(4):749-758. (in Chinese)

[21] ÅRNES A, VALEUR F, VIGNA G, et al. Using Hidden Markov Models to Evaluate the Risks of Intrusions [C]//Proceedings of the Recent Advances in Intrusion Detection. Hamburg: Springer, 2006: 145-164.

(编辑:徐楠楠)