计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190300045

基于改进隐马尔可夫模型的网络安全态势评估方法

李 欣 段詠程
中国人民公安大学信息技术与网络安全学院 北京 100038
(ndlixin@sina.com)

摘 要 网络安全态势感知作为网络安全防护措施的有效补充,是近年来的研究热点之一,而准确地评估网络安全状态已成为网络安全领域的一个重要课题。隐马尔可夫模型(Hidden Markov Model,HMM)可用于网络安全态势评估,能实时评估网络状态,但其存在模型参数难以配置、评估准确率较低等问题。因此,文中提出了一种改进隐马尔可夫模型的态势评估方法,将模型 Baum-Welch(BW)参数优化算法与人群搜索算法(Seeker Optimization Algorithm,SOA)相结合,利用 SOA 随机搜索能力强的特点,解决传统参数优化算法容易陷入局部最优解的问题,将优化后的参数代入 HMM 中,通过量化分析得出网络安全态势值。基于 DARPA2000 数据集采用 MATLAB 软件对提出的方法进行实验验证,结果表明,与 BW 算法相比,所提方法能够提高模型准确率,对网络安全态势的量化更加合理。

关键词:态势评估;HMM;SOA;参数优化;态势感知
中图法分类号 TP393

Network Security Situation Assessment Method Based on Improved Hidden Markov Model

LI Xin and DUAN Yong-cheng
College of Information Technology and Network Security,People's Public Security University of China,Beijing 100038,China

Abstract Cyber security situation awareness,as an effective supplement in cyber security protection measures,is one of the research focus in recent years. In particular,network security situation assessment has become an important research topic in the field of network security. Hidden Markov Model (HMM) can be used in network security situation assessment,which can evaluate network status in real time,but there are problems such as difficult to configure model parameters and low evaluation accuracy. Therefore,this paper proposes a situation assessment method for improving the Hidden Markov Model,combining the Baum-Welch (BW) parameter optimization algorithm with the Seeker Optimization Algorithm (SOA). Taking advantage of the strong random search ability of SOA,the traditional parameter optimization algorithm is easy to fall into local optimal solution. The optimized parameters are substituted into the HMM,and the network security situation value is obtained through quantitative analysis. Based on the DARPA2000 dataset,this paper uses MATLAB software to verify the proposed method. The experimental results show that compared with BW algorithm,this method can improve the accuracy of the model,and it makes the quantification of the network security situation more reasonable.

Keywords:Situation assessment;HMM;SOA;Parameter optimization;Situational awareness

为了有效应对日益复杂、隐蔽的网络威胁,宏观地把握整个网络的安全状况,网络安全态势评估越来越受到重视。网络安全态势评估的目标是完成从安全数据集合到网络态势结果的映射。从目标网络环境中的各类安全监测和检测设备中获取数据并对其进行处理,根据相关的经验和知识,利用数学模型或工具量化计算网络的安全状态,给出特定时间段内网络当前状态的合理性解释,以便安全管理者把握整体安全态势,为决策提供支撑。

国外的研究团队对网络安全态势评估的研究起步较早。Gorodetsky 等[1]提出了基于多源且周期有限的输入数据异步流的实时网络安全态势评估方法。首先采集有多个来源且生命周期有限的网络数据流,然后通过数据的异步流量分析各种安全事件,最后以网络安全领域的异常检测为例进行实证研究。Arnes 等[2]提出使用隐马尔可夫模型对网络安全状态进行评估,将主机的各种安全状态和转换关系转换成一个含有隐含未知参数的马尔可夫过程问题,通过安全状态转换过程和观察到的安全事件来评估整个网络的安全态势。Haslum 等[3]在文献[2]的基础上提出了隐马尔可夫模型的状态转移矩阵应基于安全事件的持续时间来确定;Poolsappasit 等[4]提出了利用贝叶斯网络进行网络安全风险评估的框架,其能够动态地帮助系统管理员量化系统网络在各个层次上的网络安全风险,该模型在网络部署阶段具有动态分析的能力。

到稿日期:2019-03-13 返修日期:2019-05-12
基金项目:国家重点研发计划(2017YFC0803700)
This work was supported by the National Key R&D Program of China(2017YFC0803700).
通信作者:段詠程(443130851@qq.com)

国内网络安全态势评估的研究以院校为主。Chen 等[5]提出了利用层次分析法对网络威胁态势进行量化评估，建立了从上至下的网络层次评估模型，并计算每层的安全指数，通过每层的权值进行加权汇聚，据此整体把握网络安全态势，从而得到态势值。Li 等[6]提出了基于遗传算法的隐马尔可夫模型的风险量化方法，该方法利用遗传算法自动生成状态转移矩阵和观测概率矩阵，在一定程度上解决了配置复杂的问题。Zhang 等[7]提出利用马尔可夫博弈模型的方法对网络安全态势进行评估，该模型由安全威胁、普通人员和管理人员三方组成，能动态、实时地把握网络的安全态势，通过对网络内的安全威胁的传播方式进行分析，来找到危害程度最大的威胁，进而提高系统的安全性。Xi 等[8]在文献[7]的基础上依据入侵检测系统中 snort 警报的质量来获取初始观测序列参数，通过系统防御事件、攻击完成概率、安全威胁措施三方共同确定状态转移矩阵的参数，该算法使网络安全态势值的量化更加合理。Wen 等[9]针对网络安全态势评估中信息来源异构、安全事件发生的时间和空间不同、评估时间较长、模型参数难以获取，以及评估准确度不高等问题，提出了一种基于聚类分析的方法。Tian 等[10]针对能源互联网的态势评估问题，提出了威胁传播和图理论相结合的评估方法，量化网络态势并绘制网络整体安全态势的变化趋势图。Zhao 等[11]针对大数据环境中的多源数据，提出了一种基于属性重要性矩阵的并行约简算法来减少数据属性，并通过基于粒子群的优化方法优化小波神经网络参数，应用基于粒子群优化的小波神经网络进行态势评估。针对分层网络安全态势评估模型存在主观指标权重系数大、评价指标体系大、计算量大、效率低等问题，Wang 等[12]提出了一种基于 AHP 的网络安全态势评估模型和量化方法。该方法首先利用 D-S 证据理论融合多源设备的模糊结果，解决单一信息源、准确度偏差大的问题；然后通过建立风险状况、基本运行情况和损害情况 3 个评价指标，解决了评价指标体系较大、评价效率较低的问题；最后利用 AHP 层次分析法确定不同指标项的权重，以避免权重系数的主观性和随机性问题。Liu 等[13]提出了网络安全态势感知的认知意识控制模型，该模型采用跨层架构和认知环，可以突破不同网络层之间的交互障碍。首先，利用决策级融合方法为不同的数据源分配不同的权重，从而提高融合精度；其次，利用分层量化方法得到网络组件之间的复杂关系；最后，利用认知调节机制解决自动控制问题。

本文是对基于隐马尔可夫模型的网络安全态势评估方法的改进和优化，通过改进 HMM 初始参数的获取和优化方法，提出了基于改进 HMM 的态势评估方法。该方法将 BW 算法与 SOA 相结合，利用 SOA 适用于连续空间的全局优化的特点，来避免模型陷入局部最优解，从而得到最优参数，提升了模型的精度；最后将优化后的参数代入 HMM 中，得到更优的网络安全态势量化分析结果。

1 基于 HMM 的网络安全态势评估

基于 HMM 的方法认为：网络安全状态与实际观察到的网络安全事件不是一一对应的关系，网络安全事件与网络安全状态之间通过一组概率分布相联系，网络安全事件的序列能够展示状态的变化过程。本文将网络安全态势评估问题映射成一个 HMM，其中隐含状态序列为网络安全状态的转移过程，观测序列为按照时间序列获取的态势要素，因此网络安全态势评估被转换成一个含有隐含未知参数的马尔可夫过程的问题，然后通过隐含状态序列和观测序列训练模型，最后利用量化模型对网络安全的态势进行评估。

网络安全态势的 HMM 由一个五元组 (N,M,π,A,B)[14]构成。

(1)N 表示模型中网络安全状态的集合。记 n 个状态为 $N_1,N_2,\cdots,N_n$，记 t 时刻马尔可夫链所处状态为 q_t，$q_t\in\{N_1,N_2,\cdots,N_n\}$。本文依据安全事件的等级进行划分，设 4 种可能的安全状态为 $N=\{G,P,A,C\}$，其定义如下：

1)良好 G(good)，表示主机没有受到任何攻击。

2)被探测 P(probe)，表示主机受到扫描等活动。该状态可以导致主机可用性降低，增加了攻击的可能性。

3)被攻击 A(attacked)，表示主机受到一方或多方的攻击。该状态可以导致可用性降低，并且增加了入侵的可能性。

4)被入侵 C(compromised)，表示主机遭到入侵。该状态可能导致主机失去机密性、完整性和可用性。

(2)M 表示每个安全状态对应的可能的观测集合。记 m 个观测值为 $M_1,M_2,\cdots,M_m$，记 t 时刻的观察值为 O_t，$O_t\in\{M_1,M_2,\cdots,M_m\}$。网络安全状态是不能被直接观测到的，但可以直接观测到警报事件，本文采取文献[8]的方法，选取高质量警报，依据 snort 警报用户手册，对入侵检测警报进行分类，$M=\{1,2,3,4\}$，其定义如下：

1)1 表示周期内没有任何入侵警报。

2)2 表示扫描类警报信息。

3)3 表示入侵类警报信息。

4)4 表示已经获取权限警报信息。

(3)π 表示初始状态概率矢量，$\pi=(\pi_1,\pi_2,\cdots,\pi_i)$，其中 $\pi_1=P(q_1=N_i)(1\leqslant i\leqslant n)$ 表示初始安全状态处于 N_i 的概率。

(4)$\boldsymbol{A}$ 表示状态转移概率矩阵，$\boldsymbol{A}=(a_{ij})_{n\times n}$，$a_{ij}=P(q_{t+1}=N_j/q_t=N_i)(1\leqslant i,j\leqslant n)$表示 t 时刻状态为 N_i 且 $t+1$ 时刻状态为 N_j 的概率。

(5)$\boldsymbol{B}$ 表示可观察值的概率分布，$\boldsymbol{B}=\{b_{ijk}\}(1\leqslant i,j\leqslant n,1\leqslant k\leqslant m)$表示在 N_j 状态输出的可观察值为 b_k 的概率。

在确定 HMM 参数之后，根据网络在周期内检测到的一系列警报对应的观测值 O_t，可实时更新网络在 t 时刻处于状态 q_t 的概率 $\gamma_t(i)$。再引入一个权值 $C(i)$，则任意 t 时刻网络态势 R_t 可按下式计算：

$$R_t=\sum_{i=1}^{n}\gamma_t(i)C(i) \tag{1}$$

其中，$\gamma_t(i)$ 表示 t 时刻网络处于状态 q_t 的概率，该值由前向后向算法计算[15]，$C(i)$ 表示状态 q_t 相对应的权值，n 表示网络安全状态的数目。

基于隐马尔可夫模型的网络安全态势评估方法如图 1 所示。基于 HMM 的网络安全态势评估方法的准确性取决于模型的初始参数。当前，模型初始参数的优化一般使用 BW 算法，因此难以获取模型的最优参数，导致模型评估的准确性不高。为解决上述问题，本文提出了一种基于改进 HMM 的

态势评估方法，将 SOA 与 BW 算法相结合，提高了初始参数的有效性。

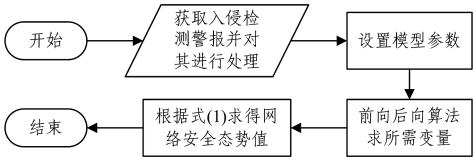


图 1　基于隐马尔可夫模型的网络安全态势评估方法

Fig. 1　Network security situation assessment method based on hidden Markov model

2　基于 SOA 的 HMM 训练

HMM 模型中，通常使用 BW 算法[16]完成 HMM 参数估计，即给定一个观察值序列 $O=O_1,O_2,\cdots,O_t$，该算法能够确定一个 $\lambda=(\pi,\boldsymbol{A},\boldsymbol{B})$，使得 $P(O/\lambda)$最大。BW 算法由 EM(Expectation Maximization)算法实现，是通过迭代进行极大似然估计的优化算法，该算法只能迭代至局部最优解，而不能达到全局最优解。在态势评估中，观测概率矩阵 $\boldsymbol{B}$ 的确立是影响评估准确性的关键，也是影响目标函数 $P(O/\lambda)$的主要因素，而参数 π 和参数 $\boldsymbol{A}$ 的影响效果甚微[17]。因此，在 HMM 的训练过程中，应对参数 $\boldsymbol{B}$ 的取值进行优化，而且 BW 算法是一个迭代的过程，参数 $\boldsymbol{B}$ 的改变也会导致参数 $\boldsymbol{A}$ 改变，从而避免了算法陷入局部最优。

SOA[18]是一种新的基于种群的启发式随机搜索算法，该算法通过对人的随机搜索行为进行研究，凭借认知科学、AI 等多种学科的科研成果，分析研究人的各种智能行为，将人的搜索行为与进化思想相结合，并对人特有的经验理论进行建模以确定搜索方向，对人特有的模糊推理理论进行建模以计算步长，完成位置的更新，实现对所求问题解的全局优化。为解决 HMM 参数优化容易陷入局部最优的问题，本文将 SOA 与 BW 算法相结合，利用 SOA 在搜索空间进行全局性搜索的能力得到最优参数，从而提高量化模型的准确性。基于 SOA 的 HMM 的态势评估总流程如图 2 所示。

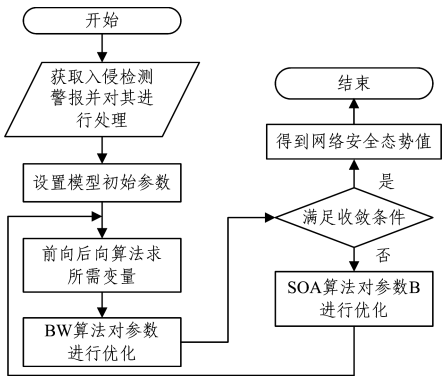


图 2　基于 SOA 的 HMM 的态势评估总流程

Fig. 2　SOA-based HMM situation assessment process

如图 2 所示，当设置完模型的初始参数后，利用 BW 算法优化参数。若满足收敛条件则直接将参数代入量化模型求得网络安全态势值；若不满足收敛条件，则通过 SOA 算法对参数 $\boldsymbol{B}$ 进行优化，再将参数传入 BW 算法，直至满足收敛条件。人群搜索算法的流程如图 3 所示。

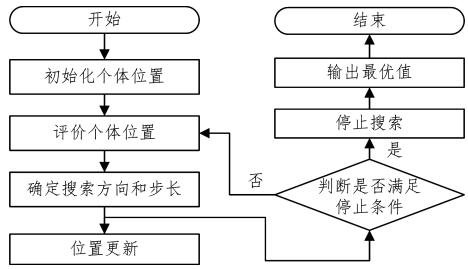


图 3　人群搜索算法的流程图

Fig. 3　Flowchart of seeker optimization algorithm

人群搜索算法的实现过程如下：

(1)初始化个体位置

在可行解域随机产生 n 个初始位置，即随机产生 n 个观测概率矩阵 $\boldsymbol{B}$，并对矩阵进行归一化处理。

(2)评价个体位置

计算每个位置的目标函数值，即 $P(O/\lambda)$值。

(3)计算每一个个体 i 在每维 j 的搜索方向和步长

采用线性隶属函数，根据模糊推理来确定目标函数值和步长的关系：

$$\mu_i=\mu_{\max}-\frac{s-I_i}{s-1}(\mu_{\max}-\mu_{\min}),i=1,2,\cdots,s \tag{2}$$

$$\mu_{ij}=rand(\mu_{ij},1),j=1,2,\cdots,D \tag{3}$$

$$\alpha_{ij}=\delta_{ij}\sqrt{-\ln(\mu_{ij})} \tag{4}$$

其中，$\mu_{\max}=1.0$ 和 $\mu_{\min}=0.0111$ 分别为最佳隶属度和最差隶属度，μ_i 为个体 i 的隶属度，μ_{ij} 为 j 维方向个体 i 的隶属度；I_i 是 $P(O/\lambda)$按降序排列后的编号；D 为方向维数；s 为个体规模；α_{ij} 为 j 维方向的步长；δ_{ij} 可由下式确定：

$$\vec{\delta}_{ij}=\omega\cdot\mathrm{abs}(\vec{x}_{\min}-\vec{x}_{\mathrm{rand}}) \tag{5}$$

$$\omega=(T_{\max}-t)/T_{\max} \tag{6}$$

其中，$x_{\min}$是个体最佳位置，x_{rand}为个体随机产生的不同于个体中最佳位置的位置；ω 是变化权值，其随着 T 的增加而线性减少；t 为当前进化次数；$T_{\max}$ 为最大进化次数；函数 abs()为取绝对值函数。

搜索方向$\vec{d}_i(t)$由利己方向(式(7))、利他方向(式(8))和预动方向(式(9))共同确定：

$$\vec{d}_{i,\mathrm{ego}}(t)=\vec{p}_{i,\mathrm{best}}-\vec{x}_i(t) \tag{7}$$

$$\vec{d}_{i,\mathrm{alt}}(t)=\vec{g}_{i,\mathrm{best}}-\vec{x}_i(t) \tag{8}$$

$$\vec{d}_{i,\mathrm{pro}}(t)=x_i(t_1)-x_i(t_2) \tag{9}$$

$$\vec{d}_i(t)=\mathrm{sign}(\omega\vec{d}_{i,\mathrm{ego}}+\varphi_1\vec{d}_{i,\mathrm{alt}}+\varphi_2\vec{d}_{i,\mathrm{pro}}) \tag{10}$$

其中，$x_i(t_1)$和 $x_i(t_2)$分别为$\{x_i(t-2),x_i(t-1),x_i(t)\}$中的最佳位置；$\vec{g}_{i,\mathrm{best}}$为第 i 个个体历史最佳位置；$\vec{p}_{i,\mathrm{best}}$ 为全局最佳位置；sign()为符号函数；φ_1 和 φ_2 为随机产生的介于 0 和 1 之间的数；ω 是变化权值，其随着 T 的增加而线性减少。

(4)个体位置更新

按下式更新每个个体位置：

$$\Delta x_{ij}(t+1)=\alpha_{ij}(t)d_{ij}(t) \tag{11}$$

$$x_{ij}(t+1)=x_{ij}(t)+\Delta x_{ij}(t+1) \tag{12}$$

3　实验验证与分析

本文使用网络安全领域普遍认可的林肯实验室 DAR-

PA2000 数据集进行实验分析。DARPA2000 数据集包含两个 DDos 攻击场景，分别为 LLDOS1.0 和 LLDOS2.0.2。本文选取 LLDOS1.0 攻击场景作为目标网络系统进行网络安全态势的评估与分析。

实验中，LLDOS1.0 是由一次真实的多步骤攻击所产生的，该过程分为 5 个步骤。第 1 步，扫描网络中的 IP 地址，尝试发现在线主机，开始时间为 9:51:36，结束时间为 9:52:00；第 2 步，嗅探所有在线主机，发现开启了 sadmind 服务的主机，开始时间为 10:08:07，结束时间为 10:18:10；第 3 步，对已经运行了 sadmind 服务的主机(Locke，Pascal 和 mill)发动基于 Sadmind Buffer Overflow 漏洞的缓冲区溢出攻击，并获得这些主机上的代码执行权限，开始时间为 10:33:10，结束时间为 10:35:01；第 4 步，在已经获得代码执行权限的主机(Locke，Pascal 和 mill)上安装 mstream 程序，开始时间为 10:50:01，结束时间为 10:50:54；第 5 步，远程操控安装了 mstream 程序的主机，发起了对 www.af.mil 主机的基于 SYN Flood 漏洞的 DDOS 攻击，开始时间为 11:26:15，结束时间为 11:34:21。LLDOS1.0 所有数据流的开始时间为 9:21:36，结束时间为 12:35:48。

本文采用流量重放技术，采取文献[8]的方法，将原始数据流导入 snort，从 snort 产生的警报流中选取质量最高的警报作为观测向量，设定选取的周期为 5 min。

为了验证算法的有效性，实验中，$N=4$，$M=4$，初始参数 $\pi_0=(1,0,0,0)$，$\boldsymbol{A}=\begin{bmatrix}0.5000 & 0.5000 & 0 & 0\\ 0.3000 & 0.4000 & 0.3000 & 0\\ 0 & 0.3000 & 0.4000 & 0.3000\\ 0 & 0 & 0.5000 & 0.5000\end{bmatrix}$，$\boldsymbol{B}=\begin{bmatrix}0.8999 & 0.02 & 0.08 & 0.0001\\ 0.6699 & 0.25 & 0.08 & 0.0001\\ 0.7350 & 0.1 & 0.16 & 0.005\\ 0.8000 & 0.04 & 0.11 & 0.05\end{bmatrix}$，$C=(0,25,50,100)$。

分别使用 BW 算法和 SOA-BW 算法进行训练，结果如图 4 所示。

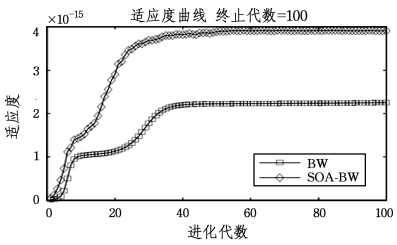
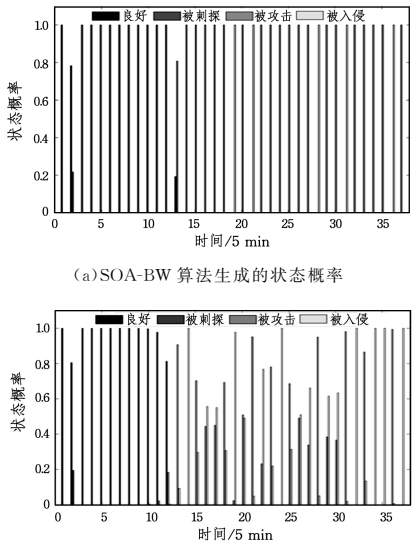


图 4 不同算法的 $P(O/\lambda)$ 值的变化情况

Fig. 4 Changes in $P(O/\lambda)$ values of different algorithms

由图 4 可知，首先，使用 SOA-BW 算法后，态势评估模型的 $P(O/\lambda)$ 值显著提升，优化后的模型能够更加准确地评估网络所处安全状态。其次，使用 BW 算法进行参数优化需经历 44 次重复迭代才能达到收敛，适应度为 2.2×10^{-15}，而使用 SOA-BW 算法只需要 17 次迭代就超过了 BW 算法的最高适应度，且收敛时的适应度为 3.9×10^{-15}，是使用 BW 算法的 1.77 倍。由此表明，将 BW 算法与全局搜索能力强的 SOA 算法相结合，能使 BW 算法最终趋于全局最优解，因此 SOA-BW 算法可以避免陷入局部最优解，得到最优参数，且优化能力更强。

为了量化评估网络的安全态势，采用算法 1 实时更新在 t 时刻网络处于状态 q_t 的概率 $\gamma_t(i)$，实验结果如图 5 所示。结合每个状态所对应的权值 C，可以得到 t 时刻网络的安全态势值，实验结果如图 6 所示。



(a)SOA-BW 算法生成的状态概率

(b) BW 算法生成的状态概率

图 5 SOA-BW 算法和 BW 算法生成的状态概率

Fig. 5 State probability generated by SOA-BW algorithm and BW algorithm

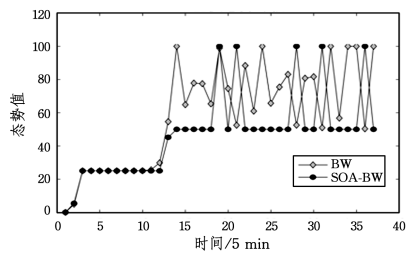


图 6 改进算法生成的网络安全态势值

Fig. 6 Network security situation value generated by improved algorithm

通过图 5(a)可以看出，在 15 min 之前，网络处于良好状态的概率更高，表明网络没有受到任何攻击；在 15 min 到 60 min 之间，网络处于被探测状态的概率为 1，表明网络受到扫描等活动；在 60 min 到 90 min 之间网络处于被攻击状态的概率为 1，表明网络受到一方或多方的攻击；在 95 min 时，网络处于被入侵状态的概率为 1，表明网络已遭到入侵；在 95 min 之后网络交替处于被攻击和被入侵状态，表明网络状态异常。通过图 5(b)可以看出，在 15 min 之前，网络处于良好状态的概率更高，表明网络没有受到任何攻击；在 15 min 到 60 min 之间网络处于被探测状态的概率为 1，表明网络受到扫描等活动；在 65 min 时网络处于被攻击状态的概率更高，表明网络已遭到攻击；在 70 min 时网络处于被入侵状态的概率为 1，表明网络已遭到入侵；在 65 min 之后网络交替处于被

攻击和被入侵状态，表明网络状态异常。上述分析表明，相比BW算法生成的状态概率，SOA-BW算法生成的状态概率与攻击场景的描述更为相符。

通过图6可以看出，经过BW算法优化后，由于其在70 min时被入侵的概率就达到了1，其产生的态势值在14 min时提前出现了小波峰，与实际情况不符。经过SOA算法优化后，在0到12 min之间，网络态势值较低；在12 min到18 min之间时，网络态势值升高，与网络处于被刺探和被攻击的状态相符；在19 min时出现小波峰，表明网络状态异常，与网络受到攻击后被入侵的实际情况相符。上述分析表明，使用通过改进算法优化得到的参数能使模型更加准确，生成的态势值更加符合LLDOS1.0攻击场景的描述，且提出的模型对网络安全态势的量化更为合理。

结束语　本文将隐马尔可夫模型的BW算法与SOA算法相结合，提出了一种改进隐马尔可夫模型的态势评估方法，解决了参数难以选择和BW算法容易陷入局部最优解的问题，使态势评估模型更加准确。实验结果表明，改进算法判定的网络安全状态变化趋势与实际情况相符，能准确量化网络安全态势，验证了算法的有效性。但该模型还存在一些问题，例如观测序列的获取主要依赖于入侵检测警报，而警报中存在大量不相关的警报和误报，后续可对观测序列的确定问题展开研究。

参 考 文 献

[1] GORODETSKY V, KARSAEV O, SAMOILOV V. On-line update of situation assessment based on asynchronous data streams [C]// International Conference on Knowledge-Based and Intelligent Information and Engineering Systems. Berlin: Springer, 2004: 1136-1142.

[2] ÅRNES A, VALEUR F, VIGNA G, et al. Using hidden markov models to evaluate the risks of intrusions [C] // International Workshop on Recent Advances in Intrusion Detection. Berlin: Springer, 2006: 145-164.

[3] HASLUM K, MOE M E G, KNAPSKOG S J. Real-time intrusion prevention and security analysis of networks using HMMs [C]// 2008 33rd IEEE Conference on Local Computer Networks (LCN). IEEE, 2008: 927-934.

[4] 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.

[5] CHEN X Z, ZHENG Q H, GUAN X H, et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2006, 17(4): 885-897.

[6] 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.

[7] ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on Markov game model [J]. Journal of Software, 2011, 22(3): 495-508.

[8] 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.

[9] WEN Z C, CHEN Z G, TANG J. Network Security Assessment Method Based on Cluster Analysis [J]. Journal of Shanghai Jiaotong University, 2016, 50(9): 1407-1414, 1421.

[10] TIAN J W, TIAN Z, QI W H, et al. Threat Propagation Based Security Situation Quantitative Assessment in Multi-Node Network [J]. Journal of Computer Research and Development, 2017, 54(4): 731-741.

[11] ZHAO D M, LIU J X. Study on Network Security Situation Awareness based on Particle Swarm Optimization Algorithm [J/OL]. Computers & Industrial Engineering. https://www.sciencedirect.com/science/article/abs/pii/S036083521830007X.

[12] WANG H, CHEN Z F, FENG X, et al. Research on Network Security Situation Assessment and Quantification Method Based on Analytic Hierarchy Process [J/OL]. Wireless Personal Communications. https://link.springer.com/article/10.1007%2Fs11277-017-5202-3.

[13] LIU X W, YU J G, LV W F, et al. Network security situation: From awareness to awareness-control [J]. Journal of Network and Computer Applications, 2019, 139(8): 15-30.

[14] WU X, YAN Y S, LIU X R. Program Behavior Anomaly Detection Method Based on Improved HMM [J]. Netinfo Security, 2016, 1(9): 108-112.

[15] SRIVASTAVA A, KUNDU A, SURAL S, et al. Credit card fraud detection using hidden Markov model [J]. IEEE Transactions on Dependable and Secure Computing, 2008, 5(1): 37-48.

[16] YANG L Q, MENG K, WANG B, et al. A New Detection Technique of SQL Injection Based on Hidden Markov Mode [J]. Netinfo Security, 2017, 1(9): 115-118.

[17] LI F W, LI Q, ZHU J. Improved method of situation assessment method based on hidden Markov model [J]. Journal of Computer Applications, 2017, 37(5): 1331-1334, 1340.

[18] DAI C H. Seeker Optimization Algorithm and Its Applications [D]. Chengdu: Southwest Jiaotong University, 2009.

LI Xin, born in 1977, Ph. D, associate professor. His main research interests include cyber security and so on.

DUAN Yong-cheng, born in 1995, master. His main research interests include situational awareness and so on.