



基于贝叶斯方法的网络安全态势感知模型

丁华东, 许华虎, 段 然, 陈 帆

(上海大学 计算机工程与科学学院, 上海 200444)

摘 要: 为全面、准确地分析既定网络的安全态势并给出态势等级评定, 提出一种基于贝叶斯方法的网络安全态势感知混合模型。对既定网络环境中收集到的态势指标数据进行离散化预处理, 利用不同的评价方法建立相应的态势指标分级模型, 并将分级模型底层的态势影响指标通过贝叶斯网络模型逐层向上融合至态势层, 得到最终评价指标进行网络态势评定。实验结果表明, 该模型满足实际应用要求, 评估结果准确、有效, 能够提高网络环境的稳定性和可靠性。

关键词: 网络安全态势感知; 态势指标; 贝叶斯网络; 分级模型; 数据融合

开放科学(资源服务)标志码(OSID):



中文引用格式: 丁华东, 许华虎, 段然, 等. 基于贝叶斯方法的网络安全态势感知模型[J]. 计算机工程, 2020, 46(6): 130-135.

英文引用格式: DING Huadong, XU Huahu, DUAN Ran, et al. Network security situation awareness model based on Bayesian method[J]. Computer Engineering, 2020, 46(6): 130-135.

Network Security Situation Awareness Model Based on Bayesian Method

DING Huadong, XU Huahu, DUAN Ran, CHEN Fan

(School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China)

[Abstract] To comprehensively and accurately analyze the security situation of a given network and evaluate the situation, this paper proposes a mixed Network Security Situation Awareness (NASS) model based on Bayesian method. The model preprocesses the situation indicator data collected from a given network environment by discretizing them. Then according to the different evaluation methods, the hierarchical model of situation indicators is established. Finally, the situation influence indicators at the bottom layer of the hierarchical model are merged upward layer by layer by using the Bayesian network model, and the final evaluation index of network security situation is obtained to give the status rating. Experimental results show that the proposed model meets the practical requirements of applications, and the evaluation results are accurate and effective, improving the stability and reliability of network environment.

[Key words] Network Security Situation Awareness (NSSA); situation indicator; Bayesian network; hierarchical model; data fusion

DOI: 10.19678/j.issn.1000-3428.0055219

0 概述

随着互联网的发展以及网络基础设施的不断完善, 基于互联网的网络信息技术带给人们越来越多的便利, 但与此同时也带来了潜在的安全隐患。为应对不断变化的网络安全威胁, 人们提出多种安全技术来防范应对, 如入侵检测、流量检测以及漏洞检测等^[1], 以期能从不同角度发现并消除网络中存在的安全隐患, 达到保护网络环境安全的目的。由于当前网络空间的基本安全态势是“易攻难守”^[2],

因此网络安全态势感知 (Network Security Situation Awareness, NSSA) 技术成为研究热点。

目前针对网络安全态势感知的研究仍处于初级阶段^[3]。文献[4]提出基于 Markov 博弈模型的网络安全态势感知方法, 通过对多传感器检测到的数据进行融合, 建立三方参与的博弈模型, 使得评估能够实时运行。但该方法对大规模网络的评估效率较低, 并且模型中的各个参数需要在真实的网络环境中不断测试, 以满足不同行业的应用需求。文献[5]构建基于神经网络的网络安全态势感知模型, 利用

基金项目: 赛尔网络下一代互联网技术创新项目“基于 IPv6 的智慧校园设备管理与可视化平台”(NGII20180617)。

作者简介: 丁华东 (1996—), 男, 硕士研究生, 主研方向为网络安全、大数据处理; 许华虎, 教授、博士生导师; 段 然、陈 帆, 硕士研究生。

收稿日期: 2019-06-17 修回日期: 2019-08-20 E-mail: ding-huadong@qq.com

神经网络找出网络态势值的非线性映射关系,采用自适应遗传算法对参数进行优化从而感知网络安全态势。但该模型不能实现对未来网络安全态势的准确预测。文献[6]构建非等时距灰色 Verhulst 残差修正态势感知模型,首先利用相关模型对网络中的风险值做出预测,然后基于多级残差对精度进行修正,最后通过修正后的模型得到态势感知预测结果。但该文没有考虑残差序列的选取方式以及模型实现的时空复杂度。

针对上述方法的不足,本文构建一种基于贝叶斯网络的网络安全态势感知模型。对数据源中影响网络安全态势的各个指标进行层次化处理,通过贝叶斯方法计算各个指标的后验概率,并据此将底层指标逐级向上混合,最终得到网络空间整体安全态势评价指标。

1 网络安全态势感知模型

网络态势是指网络内部系统状态、外部行为状态、内部用户状态之间相互平衡所构成的一个整体态势。态势感知最早来源于美国军方在军事对抗中所进行的研究^[7],目标是使得军事博弈的双方指挥官能够获悉对方的军事行为状态从而做出有利于己方的军事判断。文献[8-9]将态势感知定义为感知一定时间和空间范围内的状态并进行理解和分析。文献[10]将态势感知应用于网络空间,提出了初步的网络态势感知的概念(NetSA),但并没有给出网络安全态势感知的明确定义^[11]。

此后,许多研究人员开始对网络安全态势感知进行了研究。文献[12]将网络安全态势感知分为3个层次,即网络安全态势觉察、网络安全态势理解以及网络安全态势投射。其中:态势觉察主要完成对初始数据的提取并分辨初始数据中的关联信息,即对源数据进行降噪、规范化处理,得到具体有效的信息,主要目的是辨识出系统中的活动;态势理解主要对分辨出的关联信息进行理解,在此基础上分析当前的安全形势,判断是否发生安全攻击行为并对安全等级进行评定;态势投射主要完成这些活动意图是否会产生攻击的判断任务,即在前两步的基础上分析并评估各个活动对当前系统环境所造成的影响,判断其是否会对系统环境造成威胁,包括发现已经产生的威胁和预测可能产生的威胁。

本文将对源数据的预处理、数据信息的建模以及预信息的采集作为态势觉察层进行分类,而将与信息理解有关的机器学习模块以及初步态势的获取作为态势理解层进行分类。同时,对预信息的处理和对机器学习的评判之间需要不断进行反馈来修正最终的态势评级,将态势指标可视化和态势指标评级作为态势投射层进行分类。本文模型如图1所示,

其中提出了“预信息”的概念。预信息指的是外部信息首次通过数据预处理并经过建模后所得到的先验信息,能够反映数据指标最原始的特性。该模型经过与机器学习过程的不断反馈最终得出系统的初步态势^[13],然后经过数据可视化流程和相关专家知识得到系统的态势等级。

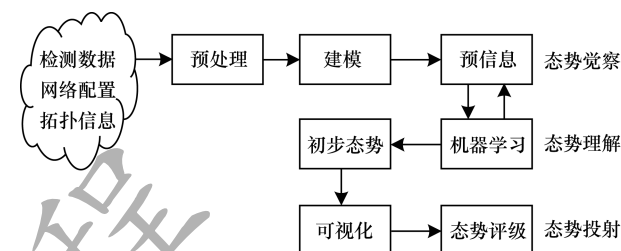


图1 网络安全态势感知模型示意图

Fig.1 Schematic diagram of network security situation awareness model

2 贝叶斯网络模型

贝叶斯网络是一种经典的概率图模型,其借助有向无环图刻画各个属性之间的相互依赖关系,并以条件概率表的方式表现属性之间的联合概率分布情况^[14]。贝叶斯网络作为不确定知识推理的重要工具,具有很强的理论基础,能够大幅降低推理的难度,从而在很多领域发挥重要作用。

一个贝叶斯网络可以表示为 $B = \langle G, P \rangle$ 的形式,需要说明如下:

- 1) $G = \langle V, A \rangle$ 是一个有向无环图,图中每个节点 V 对应于某一个属性,若两个属性之间存在依赖关系,则用一条有向边 A 连接属性。节点集合 $V = \{V_i\}_{i=1}^n$, 有向边 $A \subseteq V \times V$ 。
- 2) $P = \{P(V_i/P_B(V_i)), V_i \in V\}$ 是一组条件概率率的集合。参数 P 定量描述属性之间的依赖关系。假设属性 V_i 在 G 中的父节点集为 Q_i , 则 P 中含有条件概率 $P_{V_i|Q_i} = P_B(V_i|Q_i)$ 。

图2所示为一个比较基础的贝叶斯网络结构。从中可以看出,贝叶斯网络由有向无环图 G 和条件概率表两部分组成。

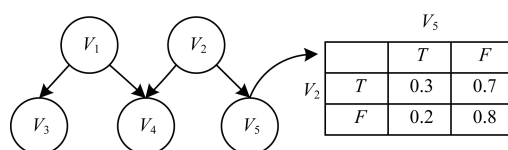


图2 贝叶斯网络结构

Fig.2 Bayesian network structure

在有向无环图 G 中可以有 N 个属性节点。对于具体的问题,每个属性节点可以是所求问题中的随机变量,而在网络安全态势感知中,属性节点可以是那些能够影响态势因素的影响因子,例如网络中

存在的漏洞、外部的匿名攻击以及一些 IDS 报警信息等。属性节点之间的有向边一般表示的是节点之间的因果关系,所以,贝叶斯网络有时也被称为“信念图”。在有向边 (V_i, V_j) 中, V_i 作为 V_j 的父节点存在, V_i 的所有父节点所构成的集合可以用 $P_B(V_i)$ 来表示。贝叶斯网络对每个节点都有条件独立的要求,任何节点 V_i 与非 V_i 子孙节点集合 $A(V_i)$ 中的所有节点条件独立,即 $I(V_i, A(V_i)/P_B(V_i))$, 可以表示为:

$$P(V_i/A(V_i), P_B(V_i)) = P(V_i/P_B(V_i)) \quad (1)$$

在贝叶斯网络结构中,用 P 表示条件概率表。给定父节点集,假设每个属性及其非子节点后裔属性条件独立,则将属性 v_1, v_2, \dots, v_n 的联合概率分布定义为:

$$P_B(v_1, v_2, \dots, v_n) = \prod_{i=1}^n P_B(v_i | q_i) \prod_{i=1}^n P_{v_i | q_i} \quad (2)$$

以图 2 为例,联合概率密度分布可以定义为:

$$P(v_1, v_2, v_3, v_4, v_5) = P(v_1)P(v_2)P(v_3 | v_1)P(v_4 | v_1, v_2)P(v_5 | v_2)$$

从上式可以看出, v_3 和 v_4 在给定 v_1 的取值时独立,而 v_4 和 v_5 在给定 v_2 的取值时独立。

贝叶斯网络模型由于具有良好的泛用性,因此使用率较高^[15-16],其主要优点如下:

1) 推理过程基于概率论。贝叶斯网络的建立严格基于概率推理,利用概率论计算有关节点的概率密度,从而增加了对于有关节点关联性之间的联系,对于不确定性知识的表述和推理更有把握。

2) 条件独立性。因为贝叶斯网络对节点之间具有条件独立的要求,所以在计算某些节点后验概率时只要针对所求节点有关的节点变量信息进行计算即可,这样可以减少参与计算的节点信息量,从而降低算法的复杂度。

3) 表示能力较强。贝叶斯网络能够处理定性的知识,也能够处理定量的知识,如某个特定节点和后验节点之间的因果关系就可以定性表达,而通过数学方法或相关专家经验得到的条件概率表就可以定量表达。

4) 计算较为简单。因为贝叶斯网络属性节点之间相互条件独立,在节点信息判别以及对所求节点进行归纳推理过程中的复杂性大幅降低。获取信息时只需要考虑与节点有关的网络图即可,在推理过程中也只需要考虑相关节点的概率信息。

3 基于贝叶斯网络的 NSSA 混合模型

针对目前多数网络安全态势感知模型存在的不足,本文提出一种基于贝叶斯网络的 NSSA 混合模型。首先对能够影响网络安全态势的因素进行分类和评级,建立一种层次化的多级贝叶斯网络模型架构,然后利用贝叶斯方法对底层的影响因子进行指标上的逐级向上融合,直至成功到达最顶层,即网络态势层,通过最终得到的影响指标对当前网络的安

全态势进行态势评估。若在融合过程中遇到变量连续化问题,则可考虑对连续属性采用概率密度函数^[17-18]进行计算,从而得到离散化、适合态势评估的数据。

3.1 态势指标

网络安全态势评估需要选取准确的数据来反映当前网络系统的态势。影响网络安全的因素较多,能够获取网络安全数据的形式也多种多样,例如系统日志记录、IDS 监测数据以及一些设备的基础信息等^[19]。本文根据以下原则来选取态势影响指标:

1) 危险性。危险性指的是所选取的影响指标能够对既定网络环境造成多大的危害。举例来说,有的网络攻击如 DoS 所造成的危害仅仅只是让服务器停止一段时间内向外提供服务,而有的网络攻击如后台利用却能够在暗处获取网络系统内部的资料信息,一旦让黑客获得价值量极大的资料信息,所造成的危害不可想象。

2) 普适性。普适性指的是所选取的影响指标应当能够反映网络态势中更普遍的信息,而不是仅仅反映态势的一面。例如,可以从各种设备中获取当前网络中的信息,但设备之间所反映的信息具有很大的差别,有的信息能够反映当前环境中的信息,而有的信息仅仅能够反映当前设备的信息。本文模型设计应当选取那些更能反映网络状况的信息。

3) 健壮性。健壮性指的是所选取的影响指标应当信息含量丰富且更易于获取。使用此原则主要是因为虽然影响网络安全态势的因素众多,但有些影响指标并不容易获取且内容信息极少,例如黑客攻击信息,在当今的网络环境中很难第一时间就获得黑客的攻击资料,大多依靠亡羊补牢的方法来获悉,所以,获取此类信息的难度极大。

利用以上 3 个基本原则,本文分析网络安全态势影响指标,并对指标进行分类,分类结果如表 1 所示。其中:网元信息包括节点主机的基本信息,网络黑客开始入侵时往往会针对节点主机的特征选取特定的攻击方案,如主机为何操作系统,当前开放了哪些端口等;流量信息主要包括与当前网络环境进行交互的流量情况,一些恶意的暴力扫描软件往往会通过网络对当前系统环境进行大量的访问,此时会造成大量的流量信息;报警信息主要是利用系统自身原有安全防御措施所生成的警告或处理信息,此类信息一般具有比较重要的参考价值;漏洞信息具有时效性,反映了当前环境所存在的漏洞,而不同的漏洞所造成的危害并不相同;配置信息主要反映当前系统的环境配置情况,包括网络拓扑结构、配置参数等,此类信息对黑客攻击具有一定的参考价值。

表 1 影响指标分类

Table 1 Classification of influence indexes

信息类别	具体指标
网元信息	主机数量、操作系统版本、主机开放端口
流量信息	带宽使用率、数据包的分布与变化率、数据流的总量与变化率、协议类型、数据流占比、数据源 IP 分布
报警信息	病毒攻击、木马攻击、DoS 攻击、蠕虫攻击、攻击发生频率、安全日志信息
漏洞信息	网络漏洞、主机漏洞、软件漏洞、设备漏洞
配置信息	网络拓扑结构、安全软件安装情况、安全设备情况

3.2 态势指标分级

为更好地突显不同影响指标对网络态势的影响程度, 本文采用对不同影响指标进行分级的处理方法, 即对影响程度较小的指标赋予较低的等级, 而对影响程度较大的指标赋予较高的等级。从分层的角度去考虑, 可将较低等级的指标放置在较低的层级, 将较高等级的指标放置在较高的层级, 这样能够使模型在进行融合处理时更重视比较重要的影响指标, 从而更准确地评估网络安全态势。因此, 在分级的过程中, 本文遵循以下原则:

1) 由于报警和漏洞信息类型的影响指标所带来的危害性较大, 因此尽量将此类信息放置在高层, 而尽量将其余信息类型的影响指标放置在低层。

2) 尽量将同一类型的影响指标进行分层分布, 而不是全部放置在某一层次, 从而避免层次分布过于集中所带来的态势评估片面的问题。

3) 低层的态势影响指标应尽可能多, 高层的态势影响指标应尽可能少, 使态势影响指标分级模型呈“金字塔”形。

基于以上 3 个基本原则和有关影响指标的重要程度, 本文给出如图 3 所示的影响指标分级模型。

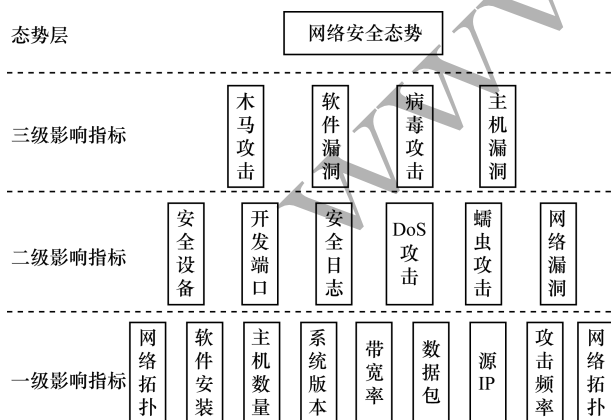


图 3 态势指标分级模型示意图

Fig. 3 Schematic diagram of hierarchical model of situation indicators

3.3 态势指标融合

在获得分级模型中各个层次所需要的原始数据后, 将每个数据源作为属性, 即贝叶斯网络中的随机变量来构建初始网络。在构建初始贝叶斯网结构时采用如下方法: 首先通过专家知识建立初步的贝叶斯网络, 然后通过计算后验概率的方法对网络进行重新修正^[20]。

假设数据集 $D = (d_1, d_2, \dots, d_n)$ 是关于 n 个变量 (x_1, x_2, \dots, x_n) 的观测值, 变量 G 是有向无环图。在给定拓扑结构 G 的情况下, 变量 θ_G 是与变量 G 对应的参数值。因此, 可用概率分布 $P(G)$ 来表示关于 G 的先验知识, 当 G 给定时, θ_G 用另一个概率分布 $P(\theta_G)$ 表示。修正函数表示为:

$$\log_a P(G, D) = \log_a P(D|G) + \log_a P(G) \quad (3)$$

其中, $P(G)$ 表示结构先验分布, 一般假设其为均匀分布。函数 $P(D|G)$ 称之为边缘似然函数, 展开式为:

$$P(D|G) = \int P(D|G, \theta_G) P(\theta_G|G) d\theta_G \quad (4)$$

选定修正函数后, 利用贪婪搜索算法搜索满足需求的网络结构。该算法的设计思想是在初始化的贝叶斯网络结构上, 每次从源中选取一条有向边加入, 然后利用公式计算评判值, 如果评判值变大, 就将该条边加入, 否则继续。利用贝叶斯方法计算后验概率时可能会遇到变量连续化的问题, 此处对连续属性可使用概率密度函数。假设 $p(x|c) \sim N(\mu_{c,i}, \sigma_{c,i}^2)$, 其中, $\mu_{c,i}$ 和 $\sigma_{c,i}^2$ 分别是第 c 类样本在第 i 个属性上取值的均值和方差, 则有:

$$p(x|c) = \frac{1}{\sqrt{2\pi}\sigma_{c,i}} \exp\left(-\frac{(x_i - \mu_{c,i})^2}{2\sigma_{c,i}^2}\right) \quad (5)$$

基于以上对态势指标的处理, 给出本文模型对于安全态势生成的算法, 该算法主要包括 3 个部分: 数据源的预处理, 态势指标的融合, 安全态势的生成。算法描述如下:

算法 顶层安全态势生成算法

输入 各级影响指标的初始样本数据 D

1) 采集样本中的连续数据, 构成连续数据集 G , 剩余的数据构成离散数据集 M 。

2) 利用概率密度函数(见式(3))对数据集 G 进行离散化预处理操作。

3) 对数据集 G 和数据集 M 进行重构, 组成新的数据集 D' 。

4) 对数据集 D' 中的数据按照态势指标分类表进行预分类。

5) 利用式(1)将底层态势指标逐层向上融合。

6) 生成网络安全态势评估值 V 。

4 实验结果及分析

本文实验采用 KDD-CUP99 网络入侵检测数据集。数据集被划分为两个部分:标识过的训练数据和未被标识的测试数据。训练数据集中包含 1 种正常的标识类型和 22 种训练攻击类型,如表 2 所示。

表 2 KDD-CUP99 标识类型

Table 2 Identification types of KDD-CUP99

标识类型	含义	指标
Normal	正常记录	normal
DoS	拒绝服务攻击	back,land,neptune,pod,smurf,teardrop
Probing	监视和嗅探攻击	ipsweep,nmap,portssweep,satan
R2L	远程非法访问	ftp_write, guess_passwd, imap, phf, spy, multihop
U2R	越级访问	buffer_overflow,loadmodule,perl,rootkit

首先通过上文提到的影响指标分级模型对数据集中的数据建立初步模型,然后运用贝叶斯方法对底层影响指标逐层向上进行融合。运用本文模型对 KDD-CUP99 中的数据集中的数据进行安全态势评估,其中网络环境主要影响指标分布如图 4 所示,可以看出,多数网络行为是正常的,但也有相当比例的网络攻击行为,如 smurf DoS 攻击、neptune DoS 攻击以及 satan 嗅探攻击等。

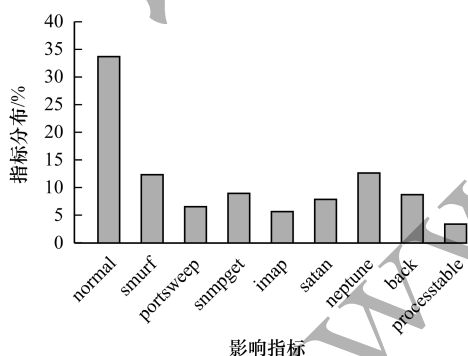


图 4 影响指标分布

Fig. 4 Influence indexes distribution

为进一步考察本文模型在时序上对于态势指标的生成情况,在数据集中提取一周时间内的网络入侵检测数据,以天为基本时间单位生成基于时序的态势指标评估结果。利用本文模型得到的指标评估网络环境所受到的攻击情况和基本网络态势,如图 5 所示。可以看出,周五、周六和周日的网络态势变化较大,而其余日期变化则较为平缓。

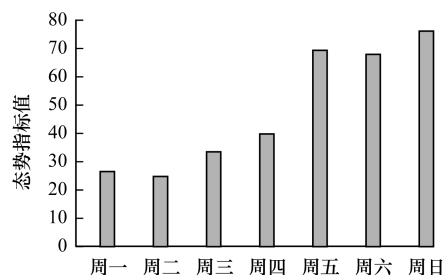


图 5 态势指标评估结果

Fig. 5 Assessment results of situation indicators

通过态势指标评估结果可以获得每一天的网络安全态势等级,分析网络安全态势的走势可以提前发现可能发生的网络安全危机,从而为网络系统的管理者提供预警,预防网络安全事件的发生,避免资产的损失。在实际的使用过程中,可以根据实时的数据分布情况调整相应分级模型的结构,将对特定网络影响指数较高的指标向上适当升级,而对特定网络影响指数较低的指标向下适当降级,从而动态适应网络环境,发挥更好的作用。

5 结束语

本文建立一种基于贝叶斯方法的网络安全态势感知混合模型。对影响网络安全环境的指标进行分类并建立分级结构。在此基础上,通过贝叶斯网络模型逐层向上融合,得到最终的网络安全态势评估指标。实验结果表明,该模型评估结果全面、客观,可准确把握网络态势的变化趋势,提高网络环境的稳定性和可靠性。目前对网络态势的影响因素较多,本文模型考虑的参数不足以支撑整体网络态势,评估结果仍有偏差并且其在进行数据离散化处理时默认使用概率密度函数,可能导致数据误差。下一步将针对这两方面不足,在真实网络环境中对模型进行测试和改进。

参考文献

- [1] QING Sihan, JIANG Jianchun, MA Hengtai, et al. Research on intrusion detection techniques; a survey [J]. Journal on Communications, 2004, 25(7): 19-29. (in Chinese)
卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述 [J]. 通信学报, 2004, 25(7): 19-29.
- [2] WU Jiangxing. Research on cyber mimic defense [J]. Journal of Cyber Security, 2016, 1(4): 1-6. (in Chinese)
邬江兴. 网络空间拟态防御研究 [J]. 信息安全学报, 2016, 1(4): 1-6.
- [3] GONG Zhenghu, ZHUO Ying. Research on cyberspace situational awareness [J]. Journal of Software, 2010, 21(7): 1605-1619. (in Chinese)
龚正虎, 卓莹. 网络态势感知研究 [J]. 软件学报, 2010, 21(7): 1605-1619.

- [4] ZHANG Yong, TANG Xiaobin, CUI Xiaolin, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3):495-508. (in Chinese)
张勇,谭小彬,崔孝林,等.基于Markov博弈模型的网络安全态势感知方法[J].软件学报,2011,22(3):495-508.
- [5] XIE Lixia, WANG Yachao, YU Jinbo. Research on network security situational awareness based on neural network[J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12):1750-1760. (in Chinese)
谢丽霞,王亚超,于巾博.基于神经网络的网络安全态势感知研究[J].清华大学学报(自然科学版),2013, 53(12):1750-1760.
- [6] ZHAO Guosheng, WANG Huiqiang, WANG Jian. A situation awareness model of network security based on gray Verhulst model[J]. Journal of Harbin Institute of Technology, 2008, 40(5):798-801. (in Chinese)
赵国生,王慧强,王健.基于灰色Verhulst的网络安全态势感知模型[J].哈尔滨工业大学学报,2008,40(5):798-801.
- [7] LIU Jian, SU Purui, YANG Min, et al. Software and cyber security: a survey[J]. Journal of Software, 2018, 29(1):42-68. (in Chinese)
刘剑,苏璞睿,杨珉,等.软件与网络安全研究综述[J].软件学报,2018,29(1):42-68.
- [8] ENDSLEY M R. Design and evaluation for situation awareness enhancement[J]. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 1988, 32(2):97-101.
- [9] ENDSLEY M R. Situation awareness global assessment technique[C]//Proceedings of IEEE National Aerospace and Electronics Conference. Washington D.C., USA: IEEE Press, 1988:789-795.
- [10] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems[C]//Proceedings of the IRIS National Symposium on Sensor and Data Fusion. Laurel, USA: [s. n.], 1999:24-27.
- [11] BASS T. Intrusion detection systems and multisensor data fusion: create cyberspace situation awareness[J]. Communications of the ACM, 2000, 43(4):99-105.
- [12] GONG Jian, ZANG Xiaodong, SU Qi. Survey of network security situation awareness[J]. Journal of Software, 2017, 28(4):1010-1026. (in Chinese)
龚俭,臧小东,苏琪.网络安全态势感知综述[J].软件学报,2017,28(4):1010-1026.
- [13] WANG Wei, ZENG Junjie, LI Guangsong, et al. Security analysis of dynamic heterogeneous redundant system[J]. Computer Engineering, 2018, 44(10):42-45, 50. (in Chinese)
王伟,曾俊杰,李光松,等.动态异构冗余系统的安全性分析[J].计算机工程,2018,44(10):42-45, 50.
- [14] ZHOU Zhihua. Machine learning[M]. Beijing: Tsinghua University Press, 2016. (in Chinese)
周志华.机器学习[M].北京:清华大学出版社,2016.
- [15] LI Shuohao, ZHANG Jun. Review of Bayesian networks structure learning[J]. Application Research of Computers, 2015, 32(3):641-646. (in Chinese)
李硕豪,张军.贝叶斯网络结构学习综述[J].计算机应用研究,2015,32(3):641-646.
- [16] HU Chunling. Research overview on Bayesian network[J]. Journal of Hefei University(Natural Science), 2013, 23(1):33-40. (in Chinese)
胡春玲.贝叶斯网络研究综述[J].合肥学院学报(自然科学版),2013,23(1):33-40.
- [17] WU Hong, WANG Weiping, YANG Feng. Discretization method of continuous variables in Bayesian network parameter learning[J]. Systems Engineering and Electronics, 2012, 34(10):2157-2162. (in Chinese)
吴红,王维平,杨峰.贝叶斯网络参数学习中的连续变量离散化方法[J].系统工程与电子技术,2012,34(10):2157-2162.
- [18] BRADSHAW J M, CARVALHO M, BUNCH L, et al. Sol: an agent-based framework for cyber situation awareness[J]. KI-Künstliche Intelligenz, 2012, 26(2):127-140.
- [19] LAI Jibao, WANG Ying, WANG Huiqiang, et al. Research on network security situation awareness system architecture based on multi-source heterogeneous sensors[J]. Computer Science, 2011, 38(3):144-149. (in Chinese)
赖积保,王颖,王慧强,等.基于多源异构传感器的网络安全态势感知系统结构研究[J].计算机科学,2011, 38(3):144-149.
- [20] CHEN Xinzhen, ZHENG Qinghua, GUAN Xiaohong, et al. Quantitative hierarchical threat evaluation model for network security[J]. Journal of Software, 2006, 17(4):885-897. (in Chinese)
陈秀真,郑庆华,管晓宏,等.层次化网络安全威胁态势量化评估方法[J].软件学报,2006,17(4):885-897.

编辑 金胡考