Journal of Computer Applications
计算机应用,2013,33(2):404-407
ISSN 1001-9081
CODEN JYIIDU
2013-02-01
http://www.joca.cn

文章编号:1001-9081(2013)02-0404-04
doi:10.3724/SP.J.1087.2013.00404

基于自律计算的网络安全态势感知模型

张　丹[1*],郑瑞娟[1],吴庆涛[1],代玉梅[2]
(1.河南科技大学 电子信息工程学院,河南 洛阳 471023;　2.商丘职业技术学院 软件学院,河南 商丘 476000)
(*通信作者电子邮箱 dandan2006_1213@126.com)

摘　要:针对当前网络安全管理的复杂性和态势感知过程缺乏自适应性等问题,提出一个基于自律计算的网络安全态势感知模型。利用自律反馈机制对态势提取进行实时分析;根据提取的态势信息,从攻击和防御两个角度出发,采用层次分析法建立多层次多角度的网络安全态势评估模型;依据过去和当前网络安全态势,采用改进的遗传神经网络方法建立网络安全态势预测模型。仿真实验结果表明,具有自律反馈机制的态势感知模型可以有效增强系统的自适应能力。

关键词:自律计算;网络安全态势感知;态势提取;态势评估;态势预测
中图分类号:TP393.08　　**文献标志码**:A

Network security situation awareness model based on autonomic computing

ZHANG Dan[1*], ZHENG Ruijuan[1], WU Qingtao[1], DAI Yumei[2]
(1. *Electronic and Information Engineering College, Henan University of Science and Technology, Luoyang Henan* 471023, *China*;
2. *College of Software, Shangqiu Polytechnic, Shangqiu Henan* 476000, *China*)

Abstract: Concerning the complexity of network security management and the absence of self-adaptation on situation awareness process, a Network Security Situation Awareness Model (NSSAM) based on autonomic computing was proposed. The situation extraction was analyzed in real-time by an autonomic feedback law. From the perspectives of attack and defense, a multi-level and multi-angle network security situation assessment model employing Analytic Hierarchy Process (AHP) was established according to the extracted situation information. The model of future network security situation prediction adopting improved genetic neural network was built on the basis of the past and current network security situation. Test results show that NSSAM with autonomic feedback mechanism can effectively enhance self-adaptation of the system.

Key words: autonomic computing; network security situation awareness; situation extraction; situation assessment; situation prediction

0　引言

近年来,随着网络的普及,计算机系统所面临的威胁程度越来越严重,木马程序、病毒、拒绝服务(Denial of Service, DoS)攻击/分布式拒绝服务(Distributed Denial of Service, DDoS)攻击日益猖獗。为保证网络的安全运行,目前所采用的入侵检测技术、防火墙技术、病毒检测技术等属于被动防御手段,而所获取的信息之间也缺乏关联性,并且这些技术手段只能检测系统局部。基于此种形势,自2000年网络安全态势感知[1]的概念被提出之后,相关模型与方法的研究迅速成为一个新的研究热点。

目前,对网络安全态势感知模型方面的研究多集中于框架结构的介绍,如Bass[1]提出的利用入侵检测系统的分布式多传感器进行数据融合的网络安全态势感知框架模型;Yin等[2]提出的基于Netflow网络安全态势感知框架模型。在感知与评估策略方面,刘念等[3]提出了一种基于免疫的网络安全态势感知方法,该方法采用基于免疫的入侵检测模型作为态势感知的基础,实现对网络中已知和未知入侵行为的检测;陈秀真等[4]提出了一种对网络安全威胁态势层次化量化评估的方法,根据入侵检测系统(Intrusion Detection System, IDS)报警信息以及网络的性能指标,并结合主机的漏洞信息,对网络系统进行层次化的定量评估,然后得到直观的网络安全态势图;Yegneswaran等[5]提出了利用Honeynets进行因特网安全态势评估的方法,该方法利用Honeynets收集到大量网络入侵信息,能够对当前网络的安全态势状况进行分析,但是该方法只对网络入侵信息进行分析,数据来源单一。

综合比较相关研究发现,尽管目前对网络安全态势感知的研究广受关注,在模型框架和评估策略方面也不断取得进展,但精确数学模型的建立和核心技术的实现则较少涉及。如何根据系统当前状态、安全性以及环境参数等的变化情况,融合自律特征,对网络安全态势感知系统的配置和相应运行参数进行动态调整以实现真正的自适应,成为制约网络安全态势感知研究的方法瓶颈。因此,本文将自律计算思想[6]引入到网络安全态势感知的研究中,提出了基于自律计算的网络安全态势感知模型,旨在对系统内外部环境变化进行实时监控,分析并及时动态调整系统中的参数,增强系统自适应能力。

1　基于自律计算的网络安全态势感知模型

网络安全态势感知是应网络安全监控需求而出现的一种

收稿日期:2012-08-13;**修回日期**:2012-09-27。　**基金项目**:国家自然科学基金资助项目(61003035,61142002,U1204614);河南省高等学校青年骨干教师资助计划项目(2009GGJS-050);河南省科技攻关项目(112102210187)。

作者简介:张丹(1988-),女,河南周口人,硕士研究生,主要研究方向:网络信息安全;　郑瑞娟(1980-),女,河南新乡人,副教授,博士研究生,主要研究方向:信息安全、自律计算;　吴庆涛(1975-),男,江西赣州人,副教授,博士研究生,主要研究方向:网络信息安全;　代玉梅(1979-),女,河南商丘人,助教,硕士研究生,主要研究方向:信息安全。

新技术,是对动态变化的网络安全态势元素进行获取、理解、评估和预测的过程。

据此,本文结合赖积保等[7]提出的网络安全态势感知概念模型,并借鉴自律计算系统工作机制[6]和自动控制中的反馈机制,提出一种基于自律计算的网络安全态势感知概念模型。模型原理如图 1 所示。

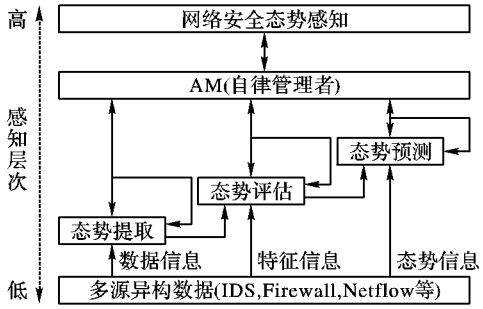


图 1　基于自律计算的网络安全态势感知模型

借鉴自律计算系统工作机制,该模型无须外力参与,能够实时监测来自多源异构环境的数据,并将各类传感器采集到的数据及分析得出的事件统一表示为 XML,为上层应用提供统一化的反映网络状态的安全数据以及经过分析的网络安全事件。然后,对这些安全数据及事件进行聚类分析,再将聚合后的安全信息融合,为态势评估提供实时数据,在此基础上,自主评估当前的网络安全态势,并预测未来网络安全态势。而自律管理者(Autonomic Manager,AM)负责根据系统内外部环境变化,对态势知识库中的态势值信息进行动态调整,从而使该模型具有自适应能力。

1.1　自律管理者

自律管理者[8]主要由监视功能模块、分析功能部件、计划部件、执行功能部件和知识库组成,如图 2 所示。其中,监视与分析模块主要提供自我觉察和外部环境状态觉察的能力,并在此基础上进行自主决策,从而确定系统的自适应目标;计划与执行功能部件主要实现系统状态偏离期望目标时的自适应功能。上述四个功能模块均是在知识库的支持下进行自律学习运作的。传感器具有收集应用模块状态和状态迁移信息的机制,效应器具有改变应用模块状态配置的功能。自律管理者的主要工作是监控反馈态势提取、态势评估和态势预测的运行状态,来进行综合分析判断系统的整体安全态势。

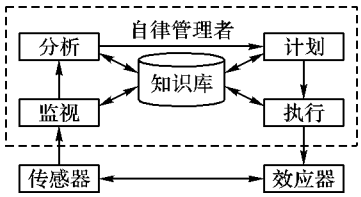


图 2　自律管理者

1.2　态势提取

网络安全态势要素提取是网络安全态势感知的基础,为态势感知提供实时的原始数据,即提取态势元素,并对态势元素进行分类,如图 3 所示。聚合模块主要是对来自多源异构环境的安全信息进行聚类分析,并将聚类判别结果反馈给自律管理者(AM),在 AM 的控制下,实现阈值的自主学习与调整,将判断满足阈值条件的安全信息划分为同一类别,并更新分类信息库;融合模块对聚合后的安全信息进行融合分析,进一步精简安全信息数量和识别攻击行为,然后将结果反馈给 AM,即完成安全要素提取,从而有效地提取态势信息,为态势评估做准备。

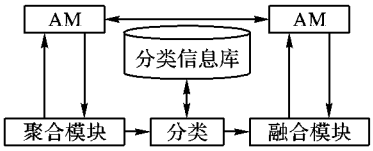


图 3　态势提取模块

1.3　态势评估

网络安全态势评估是态势感知的核心,是对当前安全态势的一个动态理解过程,将当前的安全态势状况反馈给自律管理者,自律管理者根据知识库中的态势值信息进行实时动态调整,以使系统适应当前网络环境的变化,从而使网络系统处于一个较稳定的状态,进而实现对当前网络安全态势的自主评估。

本文从攻击和防御的角度出发,采用层次分析法[9-10],建立了多层次多角度的网络安全态势评估模型[11]。该模型逐级分为网络层、主机层和攻防层三个层次:不同的主机构成网络层,主机上所运行的服务、安全措施等构成主机层,运行于主机上的服务和安全要素两部分在攻防层上被考虑,如图 4 所示。

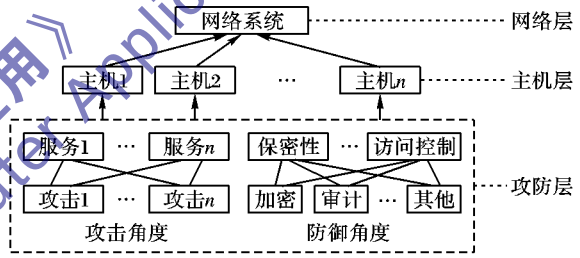


图 4　多层次多角度网络安全态势量化评估模型

综合采用文献[11-12]提供的服务安全态势、防御强度、主机安全态势和网络安全态势的量化计算方法对分层指标进行量化计算,并考虑其中的攻击威胁程度 D、服务重要性权重 $\boldsymbol{V}$、主机重要性权重 $\boldsymbol{W}$ 和安全属性的重要性权重 $\boldsymbol{W}_s$。

定义 1　函数 R_S 表示 t 时刻目标网络的服务安全态势状况,记为

$$R_S(S,C,N,D,t) = N(t) \cdot 10^{D(t)} \tag{1}$$

其中:S 表示目标网络当前所提供的某种服务,C 表示该服务受到的攻击种类,N 表示服务所受到的攻击的次数,D 表示攻击的严重程度,$N(t)$ 表示 t 时刻攻击所发生的次数,$D(t)$ 表示 t 时刻攻击的严重程度。

定义 2　函数 DF_H 表示 t 时刻目标网络的主机的防御强度,记为

$$DF_H(\boldsymbol{W}_s,SM,Ed,t) = \boldsymbol{W}_s \cdot Ed(t) \tag{2}$$

其中:$\boldsymbol{W}_s$ 表示安全属性在主机上的重要性权重,SM 表示主机上运行的安全措施,Ed 表示 SM 相对于安全属性的影响度。

定义 3　函数 R_H 表示 t 时刻目标网络的主机安全态势状况,记为

$$R_H(H,\boldsymbol{V},R_S,t) = \boldsymbol{V} \cdot R_S(t)/DF_H \tag{3}$$

其中:H 表示目标网络中的主机,$\boldsymbol{V}$ 表示运行在主机上的某服务在主机开通的所有服务中所占的权重,DF_H 表示防御强度。

定义 4　函数 R_L 表示 t 时刻目标网络的系统安全态势状况,记为

$$R_L(L,\boldsymbol{W},R_H,t) = \boldsymbol{W} \cdot R_H(t) \tag{4}$$

其中:目标局域网络中的系统为 L,在被评估局域网中主机所

占重要性的权重为 $\boldsymbol{W}$。

1.4 态势预测

态势预测依据过去安全态势信息与当前网络态势信息来对未来网络的安全态势进行预测（即已知 $t, t+1, \cdots, t+n$ 时刻的网络安全态势，预测 $t+(n+1)$ 时刻的网络安全态势），然后将未来网络的安全态势反馈给自律管理者，从而有效地指导未来的自主决策。

在评估历史和当前网络安全态势的基础上，建立态势预测的神经网络模型[12]，由于遗传算法具有很强的宏观搜索能力和良好的全局优化性能，因此本文采用改进的遗传神经网络算法（BP Neural Network with Genetic Algorithm, GA-BPNN）[13,15]对态势预测模型进行优化，以实现对未来网络安全态势的预测，具体步骤如下：

1）根据过去和当前的态势值信息，对态势预测模型 y_n^p 和相对应的误差函数 G 进行如下定义：

$$y_n^p = f\left(\sum_{k=1}^{K} \nu_{km} \cdot f\left(\sum_{n=1}^{N} \omega_{nk} \cdot x_n^p - \theta_k\right) - \gamma_m\right) \tag{5}$$

$$G = \frac{1}{P}\sum_{p=1}^{P}\sum_{m=1}^{M}(y_m^p - \hat{y}_m^p)^2 \tag{6}$$

其中：N 为输入层节点个数；K 为隐含层节点个数；M 为输出层节点个数；输入层与隐含层之间的连接权值用 ω_{nk} 来表示；隐含层与输出层之间的连接权值表示为 ν_{km}；隐含层和输出层的阈值分别表示为 θ_k 和 γ_m；f 表示隐含层到输出层的 Sigmoid 函数[12]，$f = \frac{1}{1+e^{-x}}$；第 p 个训练样本所对应的第 m 个实际输出和期望输出分别表示为 y_m^p 和 $\hat{y}_m^p$。

2）采用遗传优化算法对该预测模型进行优化，使得实际输出值与期望输出值一致，所定义的优化目标为

$$f(t) = \frac{1}{1+G(t)} \tag{7}$$

其中：$t = 1,2,3,\cdots$ 是种群中个体数；$f(t)$ 表示第 t 子代的个体适应度值；$G(t)$ 表示第 t 子代个体的误差情况。最后，输出训练后的态势预测模型，并对参数值进行动态调整，从而寻找出最优的参数组合，并输出预测的结果。

2 仿真实验及分析

为了进一步验证所建立的基于自律计算的网络安全态势感知模型的可行性和合理性，对其进行了仿真实验。该模型在受保护的 3 台主机（H1、H2、H3），配置为 Redhat Linux 9.0 操作系统，P4 3.0 CPU，1 024 MB 内存，160 GB 硬盘的计算机上予以实现，各个主机上运行着不同的服务和安全防御机制。实验环境包括华为 S5000 多层路由交换机、IDS 以及防火墙（Firewall），如图 5 所示。

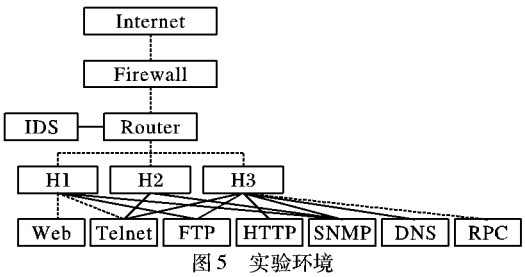


图 5 实验环境

2.1 实验过程

利用 Smurf、Ping of Death、portsweep 等攻击方法对受保护的服务器进行攻击，采集 IDS、防火墙和主机的日志信息并进行分析，每 24 h 对系统本身的安全态势作出评估，当前评估值与历史评估值一起建立时间序列作为输入量，进入遗传神经网络预测模型进行训练，得到态势预测值。

2.2 态势评估结果分析

本文中的攻击类别及威胁程度参考 Snort 手册[14]，其中威胁程度分为高、中、低、较低，对应数值为 4,3,2,1，如表 1 所示。

表 1 威胁程度与攻击类别

威胁程度	攻击类别
高(4)	Shellcode-detect
高(4)	Attempted-admin
中(3)	RPC-portmap-decode
中(3)	Attempted-DoS
低(2)	Network-scan
低(2)	Misc-activity
较低(1)	TCP-connection

如表 2 所示，给出了实验环境中各个主机上的安全措施和服务运行情况，并给出了防御强度[11]。从表中可以看出，H3 的防御能力最强，H2 的防御能力次之，H1 的防御能力最弱。

表 2 主机上安全措施、服务运行情况及防御强度

主机	安全措施	服务运行情况	防御强度
H1	加密，访问控制，鉴别	Web,Telnet,SNMP,FTP	6.6997
H2	数据完整性，访问控制	SNMP,FTP	8.6837
H3	加密，数字签名，访问控制	Http,SNMP,DNS, RPC,Telnet,FTP	9.3105

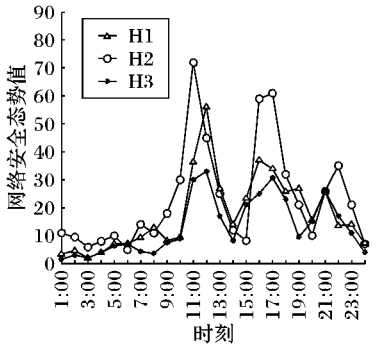
主机中服务权重和网络中主机权重的确立是一个动态、多变量、人为参与共同作用的综合评价过程。为了更加客观地评价各个服务和主机的重要性，采用改进的层次分析法（Improved Analytic Hierarchy Process, IAHP）[11]来确立服务权重和主机权重，H1 的服务权重 $\boldsymbol{V1}$ = (0.2535, 0.1170, 0.2327, 0.3968)，H2 的服务权重 $\boldsymbol{V2}$ = (0.2899, 0.7101)，H3 的服务权重 $\boldsymbol{V3}$ = (0.1739, 0.6636, 0.2458, 0.0971, 0.2458, 0.1739)；主机权重 $\boldsymbol{W}$ = (0.1234, 0.2877, 0.5889)，可以看出 H3 对应的权值最大，这与实际情况相吻合。

结合所确立的参数，依据式(1)～(3)计算出实验环境中主机的安全态势。如图 6 所示，分别给出了未考虑安全防御机制影响和考虑安全防御机制影响的主机安全态势图。从两个图的对比中可以看出，图(a)中所受威胁产生的波动最大的是主机 H2，而对于考虑了安全防御机制的图(b)中却显示所受威胁产生的波动最大的是主机 H1。究其原因是主机 H1 上所运行的安全防御机制相对较弱，而主机 H2 上所运行的安全防御机制则相对较强，因此，该结果能够更加真实地反映出网络中的主机所遭受威胁程度的状况。

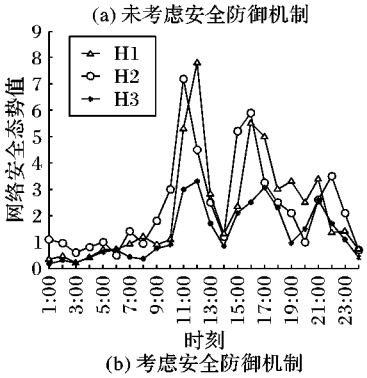
依据式(1)～(4)计算出网络的安全态势，如图 7 所示，给出了 2011 年 4 月 20 日全天网络安全态势情况。态势值越大则表明网络安全状况越严重，可以看出 10:00—18:00 的安全态势值较高，即攻击行为比较密集，说明这段时间较易受到攻击。

在实际过程中随机导入攻击来测试基于自律计算的网络安全态势感知模型的自适应性，对 10:00—18:00 这段时间，每隔 1 h 进行采样，得到 8 个采样点，通过图 7 可得出加载该模型前后的目标网络安全态势变化情况，如表 3 所示。从表

中可以直观地看出加载了该模型的目标网络的安全态势变化较平稳,究其原因是本文所提出的模型具有自律特性,对外部攻击具有自适应性,能够实时感知系统内外部环境变化,并根据系统内外部环境变化参数对态势值进行动态调整。



(a) 未考虑安全防御机制



(b) 考虑安全防御机制

图 6　主机安全态势

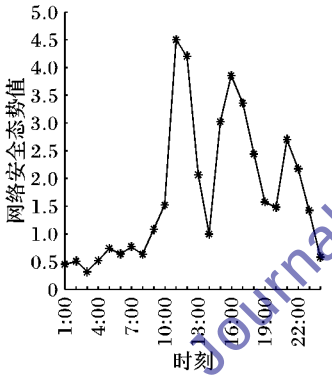


图 7　网络安全态势变化

表 3　加载该模型前后的网络安全态势变化情况

时刻	加载前	加载后	时刻	加载前	加载后
11:00	4.45	3.35	15:00	3.02	2.94
12:00	4.20	3.10	16:00	3.85	3.27
13:00	2.07	2.10	17:00	3.36	3.12
14:00	1.00	1.30	18:00	2.45	2.41

2.3　态势预测过程及结果分析

依据网络安全态势的评估结果,将连续的 80 个态势值作为样本,训练样本值为所取样本的前 50 个,测试样本值为后 30 个。神经网络的权值和阈值采用遗传算法(Genetic Algorithm,GA)来确定。种群个数初始为 $popu = 50$,最大训练代数 $gen = 100$,目标误差为 $goal = 0.001$,学习速率为 $LP.lr = 0.05$,大约 70 代时群体中个体的适应度逐渐趋于平稳,说明整个优化过程能达到预期的效果。为了对比分析,分别采用 BP 神经网络与本文优化后的预测模型对测试样本进行实验。图 8 给出了 GA-BPNN 和 BP 算法的预测曲线,可以看出,采用 GA-BPNN 算法预测得到的态势值与真实值最接近,说明采用该方法能够更准确地对未来网络安全态势进行预测。

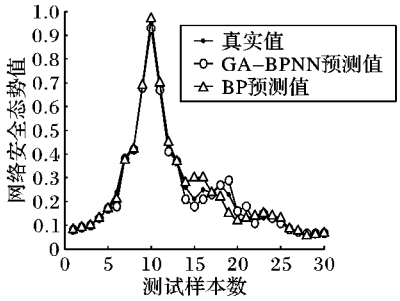


图 8　GA-BPNN 与 BP 方法的预测曲线

3　结语

本文借鉴了自律计算的思想和自动控制中的反馈机制,构建了一个基于自律计算的网络安全态势感知模型,该模型具备了较好的自适应性,能够有效地获取态势信息,准确了解网络的当前安全状况,快速预测未来网络安全态势,动态智能地适应复杂环境并有效地指导未来的自主决策;从而减轻了管理员的负担,降低了管理成本,进一步解决网络安全管理复杂性问题。仿真实验结果表明,具有自律反馈机制的态势感知模型可以有效增强系统的自适应能力。由于将自律计算引入到网络安全态势感知的研究还处在探索阶段,与之相关的方法和理论还需进一步的研究和完善。

参考文献:

[1] BASS T. Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness [J]. Communications of the ACM, 2000, 43(4): 99 - 105.

[2] YIN X X, YURCIK W, SLAGELL A. The design of VisFlowConnect-IP: a link analysis for IP security situational awareness [C]// Proceedings of the 3rd IEEE International Workshop on Information Assurance. Piscataway: IEEE, 2005: 141 - 153.

[3] 刘念,刘孙俊,刘勇,等.一种基于免疫的网络安全态势感知方法[J].计算机科学,2010,37(1):126 - 129.

[4] 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.

[5] YEGNESWARAN V, BARFORD P, PAXSON V. Using honeynets for Internet situation awareness [C]// Proceedings of the 4th Workshop on Hot Topics in Networks. New York: ACM, 2005: 1 - 6.

[6] 廖备水,李石坚,姚远,等.自主计算概念模型与实现方法[J].软件学报,2008,19(4):779 - 802.

[7] 赖积保,王慧强,朱亮.网络安全态势感知模型研究[J].计算机研究与发展,2006,43(Suppl.):456 - 460.

[8] 吴庆涛,华彬,郑瑞娟,等.基于自律计算的入侵容忍模型[J].计算机应用,2010,30(9):2386 - 2388.

[9] 朱丽娜,张作昌,冯力.层次化网络安全威胁态势评估技术研究[J].计算机应用研究,2011,28(11):4303 - 4306.

[10] 张焱,郭世泽,黄曙光,等.一种基于多源异构传感器的网络安全态势感知模型[J].计算机应用研究,2012,29(1): 286 - 289.

[11] 赖积保.基于异构传感器的网络安全态势感知若干关键技术研究[D].哈尔滨:哈尔滨工程大学,2009.

[12] 唐成华,余顺争.一种基于似然 BP 的网络安全态势预测方法[J].计算机科学,2009,36(11):97 - 100.

[13] 孟锦,马驰,何加浪,等.基于 HHGA-RBF 神经网络的网络安全态势预测模型[J].计算机科学,2011,38(7):70 - 72.

[14] Snort Users Manual 2.9.2. [EB/OL]. [2011 - 12 - 07]. http://www.snort.org/assets/166/snort_manual.pdf.

[15] 王慧强,赖积保,胡明明,等.网络安全态势感知关键实现技术研究[J].武汉大学学报:信息科学版,2008,33(10): 995 - 998.