遗传禁忌算法优化 BP 网络用于入侵检测

王艳萍
(郑州铁路职业技术学院 信息工程系, 郑州 450052)

摘 要: 针对入侵检测系统存在的高漏报率和误报率,提出一种基于遗传禁忌神经网络的入侵检测模型。该模型基于遗传禁忌算法的全局搜索和 BP 网络局部精确搜索的特性,将遗传禁忌算法和 BP 算法有机结合,利用遗传禁忌算法优化 BP 网络初始权重,同时引入小生境技术改进遗传禁忌算法。实验表明,改进的遗传禁忌算法优化 BP 网络用于入侵检测能提高入侵检测的效率,降低误警率,可在一定程度上提高入侵检测系统的准确率。

关键词: 入侵检测; BP 神经网络; 遗传禁忌算法; 小生境技术; 网络安全
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2010)03-1086-03
doi:10.3969/j.issn.1001-3695.2010.03.077

Genetic tabu algorithm for BP network intrusion detection

WANG Yan-pin
(*Dept. of Information Engineering, Zhengzhou Railway Vocational & Technical College, Zhengzhou* 450052, *China*)

Abstract: For high omission rate and false alarm rate in intrusion detection system, this paper proposed a tabu-based genetic neural network intrusion detection model. The model was based on genetic tabu algorithm of global search and BP global network of local search precision features, combined genetic tabu algorithm and BP algorithm, and used genetic tabu algorithm initial weights of BP network, at the same time, used niching technology to improve genetic tabu algorithm. Experiments show that the improved genetic tabu algorithm optimizing the BP network for intrusion detection can improve the efficiency of intrusion detection, lower false positive rate, improve the accuracy in the intrusion detection system to some extent.

Key words: intrusion detection; BP neural network; genetic tabu algorithm; niche technology; network security

随着网络互连程度的日益扩大,Internet 得到迅速发展。尤其是近年来网络上电子商务等业务的快速发展,网络的重要性及其对社会的影响也越来越大,网络与人们的日常生活密不可分。同时,通过网络犯罪对国家安全、企业安全和个人安全造成的损失也日益严重,网络安全已成为人们最为关心的问题。入侵检测是近十年发展起来的一种动态监测、预防或抵御系统入侵行为的安全机制[1]。目前入侵检测有许多模型和方法,而模式识别和数据挖掘等技术的引入使入侵检测的智能性研究成为热点[2,3]。神经网络和模式识别技术具有自学习、自适应的能力,只要提供系统的审计数据或网络数据包,神经网络就可以通过自学习从中提取正常的用户或系统活动特征模式,并检测出异常活动的攻击模式[4]。神经网络的这些特性使其在入侵检测中得到了很好的应用。最流行的神经网络学习算法是 BP 算法(back-propagation algorithm),它的收敛速度慢,存在局部最优问题[5,6],故基于神经网络的入侵检测面临的一个主要任务是效率问题和准确性问题[7,8]。

1 相关概念介绍

1.1 入侵检测

入侵是指系统的未授权用户试图或已经窃取了系统的访问权限,以及系统的授权用户超越或滥用了系统所授予的访问权限,从而威胁或危害了网络资源的完整性、机密性或有效性的行为集合[9]。其中,完整性是指防止网络资源被非法删改和破坏;机密性是指防止网络系统内信息的非法泄露;有效性是指网络系统数据资源可以被授权用户随时正常地访问,以及程序资源能够按期望的方式和作用正常地运行。从分类角度可将入侵划分为信息收集(如路由探测、拓扑重建、系统探查、端口扫描等)、系统侵入、系统渗透、伪装隐形、系统攻击(如洪流、邮件炸弹等)和恶意使用等类型。

入侵检测是通过对系统数据的分析,有效地发现非授权的访问和攻击行为。它通过从计算机系统中的日志文件、计算机网络中的若干关键节点等处收集相关信息并分析这些信息,检查系统或网络中是否有违反安全策略的行为和遭到袭击的迹象,在不影响系统性能的情况下能对网络进行监测[10]。

入侵检测系统(intrusion detection system, IDS)[11]是一种计算机软件系统,用于自动检测上述入侵行为,并收集入侵证据,为数据恢复和事故处理提供依据。有些入侵检测系统在检测到入侵特征后还试图作出某些响应,以遏制或阻止对系统的威胁或破坏。该系统通常包括以下功能:a)检查系统的配置和系统存在的脆弱性;b)评估关键系统和数据文件的完整性和一致性;c)分析用户和系统的活动情况;d)检测并响应正在进行的或已经实现的违反系统安全策略的入侵活动;e)收集入侵证据。

在设计网络入侵检测系统时,要特别对来自组织机构内部的入侵行为予以更多的重视。据 FBI 的研究,80% 的入侵和攻击行为来自于组织机构内部。由于内部人员具有访问系统资源的合法身份、了解系统数据的价值和熟悉系统的安全措施,

收稿日期: 2009-06-15; **修回日期**: 2009-07-15
作者简介: 王艳萍(1970-),女,河南郾城人,讲师,硕士,主要研究方向为网络安全、数字图像(wangyanpin2009@163.com).

从而可以使用某些系统特权或调用比审计功能更低级的操作来逃避审计。

1.2　禁忌搜索算法

禁忌搜索算法(TS)最早是由 Glover 于 1986 年提出的,它是一种"局部搜索"的修正方法[12],通过一个灵活的记忆功能和藐似准则达到搜索解空间的目的。与传统的优化算法相比,其主要特点是:a)在搜索过程中可以接受劣解,所以具有较强的"爬山"能力;b)新解不是在当前解的领域中随机产生,而是从中选取最好解,即最好解的产生概率远远大于其他解。

禁忌搜索算法的缺陷是对于初始解具有较强的依赖性。一个较好的初始解可使禁忌搜索在解空间中搜索到更好的解,而一个较差的初始解则会降低禁忌搜索的收敛速度,搜索到的解也相对较差。此外,其搜索只是单对单操作,即在搜索过程中初始解只能有一个,在每代也只是把一个解移动到另一解。

1.3　遗传算法与禁忌搜索算法的混合优化算法

Glover 等人从广义的角度对遗传算法(GA)和禁忌搜索算法(TS)进行了比较和分析,指出了两者结合的可能性,为 GA 和 TS 算法的结合应用提供了理论基础[13]。为了保持 GA 和 TS 算法的优点,提高算法的计算效率,在实际应用时人们提出各种改进策略。本文将两者混合使用,提出一种将 GA 和 TS 算法混合的策略,并在其中引入小生境技术。先将小生境技术融入 GA 中,使 GA 的种群保持较高的多样性,从而避免 GA 陷入局部最优;用这种融入了小生境的 GA 进行全局搜索,可以使群体中的个体分布在解空间的大部分区域,待收敛到一定程度后,各个体的位置相对比较固定,再用 TS 算法进行局部搜索,使算法快速地收敛到全局最优解。

2　改进的遗传禁忌算法优化 BP 网络

2.1　融入小生境的技术

在用 BP 神经网络进行入侵检测时,有一个重要问题就是网络连接权值的确定问题,因为初始权值选择不当,不仅会影响到网络的收敛速度,而且可能对最终网络的性能有很大影响。对这类问题的解决方法目前主要是凭经验进行选择。针对以上问题,本文提出了用遗传禁忌算法来初始化 BP 网络的权值。由于遗传算法采用根据适应度值的大小来决定个体是否被复制的选择机制,这样容易出现来源于同一种群的个体被大量繁衍的情况,形成近亲繁殖,造成算法的局部搜索和过早收敛,从而导致全局寻优过程失败,特别是对于多峰值函数容易出现这种现象。为了避免 GA 陷入局部最优,将小生境技术引入到算法中。小生境技术通过海明距离定义的排挤策略能够保证种群的多样性。

2.2　改进遗传禁忌算法优化 BP 网络的初始权值

本文提出的入侵检测模型(图 1),首先通过分类器对捕捉到的数据进行特征分析,然后将出现的未知类型投入到训练样本中,进行改进的遗传禁忌算法优化 BP 网络的学习后,再次使用神经网络分类器进行分类。根据采集可控网络流量数据,每一分钟计算一次这段时间内的各流量特征的统计值作为神经网络的输入,通过网络流量异常的可视化分析。利用遗传禁忌算法优点来克服 BP 算法收敛慢和易局部收敛的缺陷,同时与 BP 算法的结合也解决了单独利用遗传禁忌算法往往不能在短时间内寻找到接近最优解的这一问题,引入 BP 算法的梯度信息将会避免这种现象。因此可将 BP 神经网络的训练分成两部分:a)用遗传禁忌算法来优化网络的初始权值;b)用 BP 算法来训练入侵检测数据得到网络模型。本文将融入小生境的遗传禁忌算法简称为 NGATS。

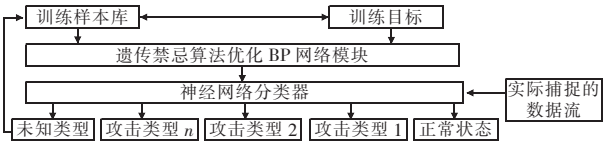

图 1　改进的遗传禁忌算法优化 BP 网络入侵检测模型

NGATS 算法优化 BP 网络具体步骤如下:

a)确定初始参数,包括最大迭代次数 T、种群规模 N、交叉概率 P_c 和变异概率 P_m 等,并确定编码方式,令 $t=0$。

b)随机产生 N 个初始个体组成初始种群 $p(t)=\{a_1,a_2,\cdots,a_i,\cdots,a_N\}$,并求出各个个体的适应度 $F_{a_i}(i=1,2,\cdots,N)$,记录最好的个体。

c)依据各个个体的适应度进行降序排列,并计算每个个体被选择的概率 $P_{a_i}=F_{a_i}/\sum_{i=1}^{M}F_{a_i}(i=1,2,3,\cdots,M)$。选择过程中使用保优原则(即上一代最优的个体以概率 1 保存至下一代),产生种群 $P(1)(t)$。

d)根据交叉概率 P_c 对群体中的个体进行交叉运算,得到 $P(2)(t)$。

e)根据变异概率 P_m 对群体中的个体进行变异运算,产生新一代种群 $P(3)(t)=\{b_1,b_2,\cdots,b_i,\cdots,b_N\}$。

f)小生境淘汰运算。按照下式[9]求出 $P(3)(t)$ 中每两个个体 b_i 和 b_j 之间的海明距离:

$$\|b_i-b_j\|=\sum_{k=1}^{\text{chromlen}}(b_{i_k}-b_{j_k})^2$$

其中,$i=1,\cdots,N-1$;$j=i+1,\cdots,N$;chromlen 为染色体长度。

当 $\|b_i-b_j\|<L$(L 为设置的最小海明距离)时,比较个体 b_i 和 b_j 的适应度大小,并对其中适应度比较低的个体处以罚函数:$\min(F_{b_i},F_{b_j})=\text{penalty}$。其中 penalty 为一个很小的正数,得到种群 $P(4)(t)$,并重新依据各个个体的适应度进行降序排列,记录种群中最好的个体。

g)判断是否满足遗传算法终止规则,即在规定连续代数 Q 内均满足 $|\text{eval}(U_{t\max})-\text{eval}(U_{(t-1)\max})|\leqslant\varepsilon$。其中:$\varepsilon$ 为一适当小的正数;$\text{eval}(U_{t\max})$ 为第 t 代的最大适应度值;$\text{eval}(U_{(t-1)\max})$ 为 $t-1$ 代的最大适应度值。则遗传算法终止,继续下一步迭代,否则转步骤 c)。

h)把遗传算法得到的最优解作为禁忌搜索的初始解,进行禁忌搜索算法。

i)若 $t<T$,令 $t=t+1$,转 h);否则停止运算,输出结果。

重复以上步骤,直到进化代数达到要求或网络误差满足条件时结束改进的遗传禁忌算法,选择网络误差最小的一组权值作为 BP 网络训练的初始权值,再利用 BP 算法进行训练,使最终误差达到要求。

3　仿真实验结果与分析

3.1　实验数据与实验环境

目前,用于网络入侵检测的生物算法很多[14,15],如前面提

到的传统 BP 算法[16]、遗传算法[17]以及粒子群算法[18]等。本文把基于遗传禁忌算法的 BP 网络应用到网络入侵检测中,期望改进入侵检测系统的性能。

为了验证本文所提出方法的有效性,本文采用 KDD Cup 1999 标准入侵检测数据集[19]进行实验。KDD Cup 1999 数据集是由 Defence Advanced Research Projects Agency(DARPA)和麻省理工学院的 Lincoln 实验室提供的入侵数据集采集样本,该数据集共有近 500 万条数据样本,每个样本包含了 41 个特征属性。其中 7 个符号特征(离散属性)、34 个数值特征(连续属性)。这些实验数据除包含正常连接数据 normal 外,还包含了四大类入侵行为,分别是 DoS(拒绝服务)、R2L(远程攻击)、U2R(获取根权限)和 Probe(刺探攻击)。实验从 KDD Cup 1999 数据集中随机选取了训练数据 7 032 条,测试数据 16 408 条。训练集中 DoS 攻击 1 114 条、R2L 攻击 9 条、Probe 攻击 38 条、U2R 攻击 20 条;测试数据中 DoS 攻击 2 581 条、R2L 攻击 11 条、U2R 攻击 33 条、Probe 攻击 78 条。

神经网络采用如下结构:输入层的节点数为 40 个,隐含层的节点数为 10 个,输出节点数为 4 个。采用 GA 优化初始神经网络权重的方法,GA 操作的参数为:选择种群 $N=50$,最大进化代数 gen = 500,选择概率 $P_s=0.095$。BP 算法参数为:初始学习率 $l_r=0.005$,设定的误差(输出值与真实输入之间的差值的绝对值)为 0.000 01,最大循环数为 1 000。

实验在 Intel Celeron 3.0 GHz CPU、512 MB 内存、Windows XP 操作系统、MATLAB 语言编程环境下进行,同时对 BP 网络、GA-BP、PSO-BP、本文算法进行比较分析。

3.2　实验结果与分析

实验分别是对于同一组混合数据的四种方法 BP 训练,示意图如图 2 ~5 所示。

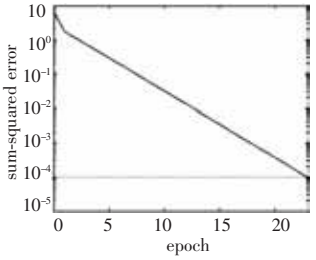

图 2　NGATS-BP 训练示意图

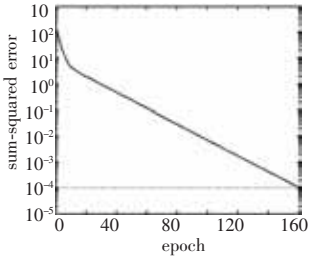

图 3　PSO-BP 训练示意图

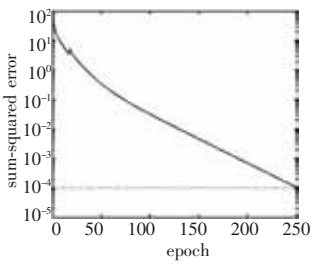

图 4　GA-BP 训练示意图

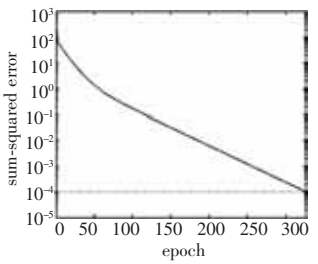

图 5　BP 训练示意图

如图 2 ~5 所示,在这组数据中,NGATS-BP 训练步数为 23 步,时间为 12.238 000 s,均方误差为 1.378 6e-003;PSO-BP 训练步数为 161 步,时间为 19.212 100 s,均方误差为 1.378 6e-003;GA-BP 训练步数为 251 步,时间为 22.219 000 s,均方误差为 1.378 6e-003;BP 训练步数为 327 步,时间为 26.612 000 s,相对收敛较慢,均方误差为 0.11。对 NGATS-BP 来讲,无论是从训练时间上还是从降低误差上都有明显的提高。

在实验中笔者发现,四种训练算法训练神经网络与权值和阈值的初始值都有一定的关系,而 BP 算法表现最为明显。如果初始值比较好,则很快就能得到最佳结果,反之,则得不到最佳结果,误差会越来越大,最后到达某一结果后停下来。NGATS 在训练过程中一直向理想结果靠近,表现出较好的全局寻优能力。实验证明,利用本文提出的 NGATS 算法训练神经网络用于入侵检测能取得较好的性能,针对几种攻击类型与其他几种算法相比,检测率都有不同程度的提高(表 1)。

表 1　基于四种算法的检测率

攻击类型	攻击名称	检测率/%			
		NGATS-BP	PSO-BP	GA-BP	BP
DoS	Smurf	99.05	96.72	76.47	72.84
PROBE	Satan	99.37	93.20	85.62	86.55
R2L	Guess_passwd	99.60	91.56	73.87	67.23
U2R	Perl	98.79	89.35	65.71	72.58

4　结束语

通过分析表明,遗传禁忌算法在 BP 网络学习中,相对于 PSO 算法、GA 和传统 BP 算法,不仅速度快、算法简单,而且测试精确率高。特别是最后经过网络入侵数据的仿真实验的比较,进一步证明了基于遗传禁忌算法的 BP 网络学习算法的优越性和实用性。

参考文献:

[1] DE Den-ning. An intrusion detection model[J]. IEEE Trans on Software Engineering,1987,139(2):222-232.

[2] 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.

[3] 林果园,黄皓,张永平.入侵检测系统研究进展[J].计算机科学,2008,35(2):69-74.

[4] 唐勇,卢锡城,王勇军.攻击特征自动提取技术综述[J].通信学报,2009,30(2):96-105.

[5] SHUN J,MALKI H A. Network intrusion detection system using neural networks[C]//Proc of the 4th International Conference on Natural Computation. 2008:242-246.

[6] SONG Guang-jun, ZHANG Jia-lin, SUN Zhen-long. The research of dynamic change learning rate strategy in BP neural network and application in network intrusion detection[C]//Proc of the 3rd International Conference on Innovative Computing Information and Control. 2008:513-513.

[7] TIAN Jing-wen, GAO Mei-juan. Network intrusion detection method based on high speed and precise genetic algorithm neural network [C]//Proc of International Conference on Networks Security, Wireless Communications and Trusted Computing. 2009:619-622.

[8] WANG Hui-ran, MA Rui-fang. Optimization of neural networks for network intrusion detection[C]//Proc of the 1st International Workshop on Education Technology and Computer Science. 2009:418-420.

[9] YU Zhen-wei, TSAI J J P, WEIGERT T. An automatically tuning intrusion detection system[J]. IEEE Trans on Systems, Man, and Cybernetics, Part B, Cybernetics, 2007, 37(2):373-384.

[10] PARIKH D, CHEN T. Data fusion and cost minimization for intrusion detection[J]. IEEE Trans on Information Forensics and Security, 2008, 3(3):381-389.

(下转第 1091 页)

b)对于 $i=j+1,\cdots,d,l,\cdots,j-1$,计算 $C_{i+1}=H_i(m,L,Tr(g_i^{s_l}g_i^{kc_i}))$。这里 $s_i\in_R Z_{q_i}$,$1<a<q_i-2$。

c)计算 $s_j=a-\delta c_j \bmod q_j$。

d)V_j 对 m 和 L 的签字 $\sigma=(m,L,c_1,M',s_1,\cdots,s_d)$。

e)验证者根据 σ 计算 $C_{i+1}=H_i(m,L,Tr(g_i^{s_l}g_i^{kc_i}))$,$i=1,2,\cdots,d$,如果 $C_{d+1}=C_1$ 则接收,否则拒绝。

签名算法的安全性与效率分析如下:

a)安全性与真实性。数字签名用来确保一个节点不能否认它已经发出的信息,确保信息是由签名者发出的且没有作过任何修改,它对检查和孤立被占领节点具有特别重要的意义。在该签名方案中,当节点 A 验证通过了节点 B 的签名,即可保证消息确实由节点 B 发出;当节点 A 接收到来自被占领节点 B 的错误信息时,数字签名保证节点 A 能够利用该信息告知其他节点 B 已被占领,再加上 XTR 密码体制的安全性,从而保证节点间数据传输的安全性与真实性。

b)机密性与可靠性。在用户私钥的分发过程中,随机数 k 和 ψ 的任意选取和安全通道确保了签名私钥的保密性。引入离线可信任机构可以使系统有较高的信任度。因为没有可信任方的参与,系统的可信度不高,不适用于军事、消防和警用车辆通信等安全性要求较高的环境中。

该签名方案利用车辆用户的身份 ID 直接计算出用户的公钥,而无须公钥证书的存在,极大地减少了公钥认证的计算量和通信开销,减少了用户的存储容量,提高了系统的运行效率。

同时,在典型实现环境(相应于同等安全的 RSA-1024 bit,DL-160 bit 和 XTR-170 bit)下的 XTR-环签字及基于 RSA 和离散对数的环签字在计算量和签字长度方面作一对比[10],结果如表 2 所示。从表中可以看出,XTR-环签字与 RSA 环签字在签字长度和计算量方面具有明显优势,与 DL 环签字相比,签字长度大致相当,但计算上比其约快 1.75 倍,具有明显优势。

表 2　XTR 环签字与其他环签字比较表

比较项	签字长度/bit	产生签字的计算量	验证签字的计算量
XTR 环签字	$170+170n$	$1.14\times10^8\times n$	$1.14\times10^8\times n$
DL 环签字	$160+160n$	$2.0\times10^8\times n$	$2.0\times10^8\times n$
RSA 环签字	$(1024+160)+1184n$	$110\times10^9+1.6\times10^7\times n$	$116\times10^7\times n$

3　恶意节点的发现

由于系统中增加了身份认证功能和信息验证功能,故能发现不正常的节点,从而能将恶意仿冒节点和恶意发送虚假信息节点快速地从系统中分离出来。本文引入信誉值的概念来剔除恶意节点。

在某个节点收到另一个节点所提供的服务(消息)之后,前者根据后者所提供服务的质量给后者一个评价值(如对满意的服务提供 +1 的评价值,对恶意的服务提供 -1 的评价值)。在对某个节点的可信程度进行评估时,通过其他节点对该节点的历史评价值来计算一个信誉值,信誉值越高表明该节点越可信。在这种情况下,提供恶意服务(虚假消息等)的节点的信誉值通常要低于善意节点的信誉值,随着恶意节点信誉值的降低,它们将从网络中被分离出来。

4　结束语

XTR 公钥体制是一种基于子群离散对数问题的密码体制,在保证安全性不变的前提下,与 RSA 公钥体制相比,它的密钥长度短、传输效率高;与椭圆曲线公钥体制相比,它的密钥选取简单、计算速度快。本文参考移动自组网中基于身份的认证方法,结合当前最高效的 XTR 密码体制,提出了基于 XTR 的认证私钥的安全签发和环签名算法,并对其特性和效率进行了分析,同时引入信誉值的概念来剔除网络中的恶意节点。本文给出的方案具有分布式实现和安全高效的特点,相信对 VANET 中车辆节点间安全认证有一定的参考价值。

参考文献:

[1] 常促宇,向勇,史美林. 车载自组网的现状与发展[J]. 通信学报,2007,28(11):116-126.

[2] KHALILI A,KATZ J,ARBAUGH W,*et al*. Toward secure key distribution intruly Ad hoc networks[C]//Proc of Symposium on Application and the Internet Workshops. [S. l.]:IEEE Computer Society,2003:1-5.

[3] 陈炜,龙翔,高小鹏. 一种基于身份的移动自组网认证机制[J]. 北京航空航天大学学报,2006,32(7):869-872.

[4] 杜春来,胡铭曾,张宏莉. 在椭圆曲线域中基于身份认证的移动 Ad hoc 密钥管理框架[J]. 通信学报,2007,28(12):53-59.

[5] 庞辽军,姜正涛,王育民. 基于一般访问结构的多重秘密共享方案[J]. 计算机研究与发展,2006,43(1):33-38.

[6] 代锦秀,唐小虎,郑宇,等. XTR 公钥密码体制概述[J]. 计算机工程与应用,2005,41(29):63-65,99.

[7] LENSRA A K,VERHEUL E R. The XTR public key system[C]//Prpc of the 20th Annual International Cryptology Conference on Advances in Cryptology. London:Springer-Verlag,2000:1-19.

[8] LENSTRA A K,VERHEUL E R. Key improvements to XTR[C]//Proc of the 6th International Conference on the Theory and Application of Cryptology and Information Security:Advances in Cryptology. London:Springer-Verlag,2000:220-233.

[9] MENZES A J. Comparing the security of ECC and RSA[EB/OL]. (2000). http://www. cacr. math. uwaterloo. ca/~ajmeneze.

[10] 王继林,伍前红,高虎明,等. 基于 XTR Schnorr 签字与环签字算法[J]. 西安电子科技大学学报,2004,31(3):454-458.

(上接第 1088 页)

[11] CHEN L,LENEUTRE J. Game theoretical framework on intrusion detection in heterogeneous networks[J]. IEEE Trans on Information Forensics and Security,2009,4(2):165-178.

[12] GLOVER F,KELLY J,LAGUNA M. Genetic algorithm and tabu search:hybrids for optimizations[J]. Computers and Science,1995,22(1):111-134.

[13] 蒋泰,杨海. 定位—路线问题的遗传禁忌混合优化算法[J]. 计算机应用,2008,28(3):688-691.

[14] 刘衍珩,田大新,余雪岗,等. 基于分布式学习的大规模网络入侵检测算法[J]. 软件学报,2008,19(4):993-1003.

[15] 易晓梅,陈波,蔡家楣. 入侵检测的进化神经网络研究[J]. 计算机工程,2009,35(2):208-209,213.

[16] 许朋飞,沈磊. 改进 BP 算法在入侵检测系统中的应用[J]. 计算机工程,2008,34(6):151-152.

[17] 徐仙伟,叶小岭. 遗传算法优化 BP 网络初始权重用于入侵检测[J]. 计算机应用研究,2005,22(3):127-128,132.

[18] 肖晓丽,黄继红,刘志朋. 基于 MPSO 的 BP 网络及其在入侵检测中的应用[J]. 计算机工程,2008,34(15):168-169,210.

[19] KDD Cup 1999 data set [EB/OL]. http://archive. ics. uci. edu/ml/databases/kddcup99/kddcup99. html.