一种基于IPSO-SVM算法的网络入侵检测方法

马占飞[1] 陈虎年[2] 杨 晋[2] 李学宝[1] 边 琦[3]

(包头师范学院信息科学与技术学院 内蒙古 包头 014030)[1]

(内蒙古科技大学信息工程学院 内蒙古 包头 014010)[2] (内蒙古师范大学传媒学院 呼和浩特 010022)[3]

摘 要 网络入侵检测一直是计算机网络安全领域的研究热点,当前网络面临着诸多的安全隐患。为了提高网络入侵检测的准确性,首先对粒子群优化(Particle Swarm Optimization,PSO)算法进行了改进,然后利用改进的PSO算法(IPSO算法)对支持向量机(Support Vector Machine,SVM)的参数进行了优化,并在此基础上设计了一种新型的基于IPSO-SVM算法的网络入侵检测方法。实验结果表明,相比于经典的SVM和PSO-SVM算法,IPSO-SVM算法不仅明显改善了网络训练的收敛速度,而且其网络入侵检测的正确率分别提高了7.78%和4.74%,误报率分别降低了3.37%和1.19%,漏报率分别降低了1.46%和0.66%。

关键词 网络安全,入侵检测,粒子群优化算法,最优参数,支持向量机

中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.040

Novel Network Intrusion Detection Method Based on IPSO-SVM Algorithm

MA Zhan-fei[1] CHEN Hu-nian[2] YANG Jin[2] LI Xue-bao[1] BIAN Qi[3]

(School of Information Science and Technology, Baotou Teachers College, Baotou, Inner Mongolia 014030, China)[1]

(School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou, Inner Mongolia 014010, China)[2]

(Vocational Skills Training Department, Inner Mongolia Normal University, Huhhot 010022, China)[3]

Abstract Network intrusion detection has always been the research focus in the field of computer network security, and the current network is facing many potential security problems. In order to improve the accuracy of network intrusion detection, this paper improved the particle swarm optimization (PSO) algorithm, and then optimized the parameters of support vector machine (SVM) by using the improved PSO algorithm. On this basis, this paper also designed a novel network intrusion detection method based on IPSO-SVM algorithm. The experiment results show that the proposed IPSO-SVM algorithm is efficient. Compared with the classical SVM algorithm and PSO-SVM algorithm, IPSO-SVM algorithm not only improves the convergence speed of the network training obviously, but also improves the accuracy rate of network intrusion detection by 7.78% and 4.74% respectively, decreases the false positive rate by 3.37% and 1.19%, and decreases the false negative rate by 1.46% and 0.66%.

Keywords Network security, Intrusion detection, Particle swarm optimization algorithm, Optimal parameter, Support vector machine

1 引言

随着互联网技术在科研、经济、军事、教育以及人们日常生活中的普及,人们越来越离不开互联网。与此同时,网络面临的安全问题也日益突出,因此,有效地防御网络安全已变得十分迫切。由于传统的网络安全防护技术存在一定的局限性,因此入侵检测系统(Intrusion Detection Systems,IDS)成为了当前网络安全技术的研究热点[1]。

IDS是一套集动态预防、监控和保护系统免遭入侵为一体的新型安全机制[2]。作为传统安全防御机制的补充,IDS不仅能主动地对入侵行为进行防护和识别,而且还能发出预警,并执行相应的响应动作。IDS可以防范更广泛意义上的对网络系统和计算机系统的非法攻击,包括检测内部合法用户超出使用权限的非法行为,以及来自外部非法入侵者的恶意攻击或诱惑。一般来说,入侵检测是针对计算机和网络资源上的一些恶意使用行为进行相应的识别和处理的过程[3],

到稿日期:2016-11-20 返修日期:2017-02-14 本文受国家自然科学基金项目(61762071,61163025),内蒙古自治区自然科学基金项目(2010BS0904,2016MS0614),内蒙古自治区高等学校科学研究基金项目(NJ10162,NJZY17287,NJZY201),包头市科学研究基金项目(2014S2004-3-1-26)资助。

马占飞(1973—),男,博士,教授,硕士生导师,CCF高级会员,主要研究方向为计算机网络与信息安全、人工智能、物联网安全与应用等,E-mail:mazhanfei@163.com(通信作者);**陈虎年**(1992—),男,主要研究方向为计算机网络与信息安全;**杨 晋**(1991—),男,主要研究方向为计算机网络与信息安全。

具有智能监控、动态响应、实时检测、易于配置等特点。虽然传统的入侵检测模型能够检测出入侵行为，但是在一定程度上，其在检测的速度、效率等方面均存在不足。为了尽可能地解决此类问题，本文提出了一种基于改进的 PSO-SVM(IPSO-SVM)算法的网络入侵检测方法。该方法通过 IPSO 算法优化 SVM 的相关参数。本文将其与经典 PSO-SVM 算法和 SVM 算法进行了比较，实验结果表明，该方法不仅能提高网络入侵检测的正确率，降低误报率和漏报率[4]，而且还可以满足网络安全的实际应用需求。

2 相关算法研究

2.1 SVM 算法简介

SVM 是一种基于统计学理论的机器学习方法[5-6]，将其描述为数学语言，即存在分类线性方程满足 $y_i[(\omega \cdot x_i+b)]-1\geqslant 0$。其中，$y_i=\pm 1$ 表示两种类别标识，$\omega\in R^n$，x_i 表示输入向量，b 为偏移量，$i=1,2,\cdots,n$。其结构如图 1 所示。

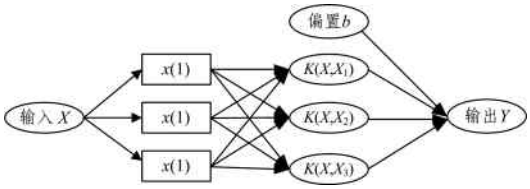

图 1 支持向量机的结构

Fig. 1 Structure of support vector machine

求解最优超平面可以简化为求解原始空间中的二次规划问题[7-8]，即有约束条件为：

$$\begin{cases}\min\ \varphi(\omega,\xi)=\dfrac{1}{2}\|x\|^2+C\sum\limits_{i=1}^{n}\xi_i \\ \text{s.t. } y_i[\omega\cdot x_i+b]-1+\xi_i\gg 0, i=1,2,\cdots,n,\xi_i\gg 0\end{cases} \tag{1}$$

其中，C 是误差惩罚系数。引入 Lagrange 乘子将问题转化为式(2)的对偶形式：

$$Q(\alpha)=\sum_{i=1}^{n}\alpha_i-\frac{1}{2}\sum_{i,j=1}^{n}\alpha_i\alpha_j y_i y_j K(x_i,x_j) \tag{2}$$

且满足如下约束条件：

$$\begin{cases}\sum\limits_{i=1}^{n}y_i\alpha_i=0 \\ 0\leqslant\alpha_i\leqslant C,\quad i=1,2,\cdots,n\end{cases} \tag{3}$$

其中，$K(x_i,x_j)$ 为核函数，α_i^* 表示与每个样本对应的 Lagrange 乘子。

相应的决策分类函数为：

$$f(x)=\mathrm{sgn}(\sum_{i=1}^{n}\alpha_i^* y_i K(x_i,x_j)+b^*) \tag{4}$$

其中，sgn()为符号函数。由于径向基核函数运行的时间短、分类精度高，因此选择径向基核函数作为 SVM 的核函数[9-10]。这样不仅能防止复杂的非线性变换，而且可以利用线性函数来对非线性问题进行求解。径向基核函数如式(5)所示：

$$K(x,y)=\exp(-|x-y|^2/d^2) \tag{5}$$

2.2 PSO 算法

PSO 算法是一种群体智能算法，源于对鸟类捕食行为的研究[11-12]。PSO 算法首先被初始化为一组随机粒子，可以用作随机初始解，初始群体在解空间中均匀分布。如果在 D 维目标搜索空间中存在 N 个粒子，则第 i 个粒子的位置和速度可分别表示为 $X_i=(x_{i_1},x_{i_2},\cdots,x_{i_D})$ 和 $V_i=(v_{i_1},v_{i_2},\cdots,v_{i_D})$，$i=1,2,\cdots,n$。然后该算法通过迭代搜索找到最优解。在每次迭代中，粒子通过跟踪这两个最优解来更新自己的速度和位置[13-14]。其中一个最优解是粒子本身迄今为止遇到的最佳值，称为个体最佳位置，记为 $P_{best}=(P_{best_1},P_{best_2},\cdots,P_{best_D})$；另一个最优解是种群迄今为止搜索到的最佳值，称为全局最佳位置，记为 $G_{best}=(G_{best_1},G_{best_2},\cdots,G_{best_D})$。粒子根据式(6)和式(7)来更新其速度和位置。

$$V_i^{k+1}=\omega\cdot V_i^k+c_1\cdot rand()\cdot(P_{best}-X_i^k)+c_2\cdot rand()\cdot(G_{best}-X_i^k) \tag{6}$$

$$X_i^{k+1}=X_i^k+V_i^{k+1} \tag{7}$$

其中，ω 为惯性权重；c_1 和 c_2 为学习因子；k 为当前迭代次数；$rand()$是一个 0 到 1 之间均匀分布的随机数，它反映了算法的随机性。

3 基于 IPSO-SVM 算法的设计

在 PSO 优化算法中，粒子表示待求解问题的可行性存在解[15]，它们都有位置，且以一定的速度在搜索空间中飞行。设粒子的位置和速度分别表示为 $X_i=(x_{i_1},x_{i_2},\cdots,x_{i_D})$ 和 $V_i=(v_{i_1},v_{i_2},\cdots,v_{i_D})$，粒子本身和种群的最优位置分别记为 P_{best} 和 G_{best}，粒子的飞行过程实质上就是问题的求解过程。

从 SVM 算法的基本原理可以得知，SVM 的两个参数对模型的诊断效果有很大的影响，一个参数是惩罚因子 C，另一个参数是核函数参数 d。这两个参数决定了 SVM 的泛化能力，因此想要得到最佳的诊断效果，就要得到最佳的 SVM 参数。优化 SVM 参数的传统方法主要有实验对比法、经验法、网格搜索法和交叉验证法，而这些方法都存在效率低、费时等缺点。为此，本文对 PSO 算法进行了改进，并利用改进的 PSO 算法(IPSO 算法)对 SVM 的参数进行优化；在此基础上，设计了基于 IPSO-SVM 算法的网络入侵检测方法，其目的是进一步改善网络的学习能力，提高收敛速度，从而提高入侵检测系统的整体性能。

3.1 IPSO 的算法设计

线性递减惯性加权法是一种广泛使用的研究方法，它可以较好地提高 PSO 算法的性能。除此之外，它还可以对 PSO 算法的全局与局部的寻优能力进行调节，但该方法存在一定的局限性，即不能真实地反映粒子的搜索过程，所达到的效果也并不理想。因此，为了提高 PSO 算法的收敛速度，本文引入了指数递减惯性权重，此时式(6)更新为：

$$\begin{cases}V_i^{k+1}=\beta\cdot V_i^k+c_1\cdot rand()\cdot(P_{best}-X_i^k)+c_2\cdot rand()\cdot(G_{best}-X_i^k) \\ \beta=\beta_{end}\cdot(\beta_{start}/\beta_{end})^{1/(1+10k/k_{\max})}\end{cases} \tag{8}$$

其中，k 为当前迭代次数；c_1 和 c_2 为学习因子；$k_{\max}$ 为允许的最大迭代次数；β_{start} 是初始惯性权重，β_{end} 是进化到最大迭代次数时的惯性权重。

在引入指数递减惯性权重的基础上，本文还引入了收缩因子，并使用指数递减惯性权重来达到更好的优化效果。然而，学习因子 c_1 和 c_2 不仅能确定粒子本身的经验信息和粒子

轨迹上其他粒子的经验信息，而且还能反映粒子群之间的信息交换。如果设置一个较大的 c_1 值，会使粒子在局部范围内徘徊；反之，如果设置较大的 c_2 值，将使粒子过早收敛到局部最小值。为了更加有效地控制粒子的飞行速度，并实现全局检测和局部挖掘之间的有效平衡，本文引入了收缩因子 φ。此时，式(8)更新为：

$$\begin{cases} V_i^{k+1}=\varphi\cdot[\beta\cdot V_i^k+c_1\cdot rand()\cdot(P_{best}-X_i^k)+c_2\cdot \\ \qquad rand()\cdot(G_{best}-X_i^k)] \\ \varphi=\dfrac{2}{|2-C-\sqrt{C^2-4C}|} \\ \beta=\beta_{end}\cdot(\beta_{start}/\beta_{end})^{1/(1+10k/k_{\max})} \end{cases} \tag{9}$$

其中，φ 是收缩因子，取经典值 $\varphi=0.729$；$C=c_1+c_2$。

通过引入指数递减惯性权重和收敛因子，可使 PSO 算法的性能得到较好的改善，由此构建一种新的 PSO 算法——IPSO 算法。

3.2　IPSO 对 SVM 参数的优化

通过将改进的粒子群优化算法与支持向量机回归算法相结合，构建了一种新的智能算法——IPSO-SVM 算法。对于给定的网络状态特征集合 $F=\{f_1,f_2,\cdots,f_n\}$，可以使用一个二进制向量来表示特征选择：$S=\{s_1,s_2,\cdots,s_n\}$，$s_i\in\{0,1\}$。其中，1 和 0 分别表示是否选择相应的特征，$i=1,2,\cdots,n$，n 表示网络特征集合的大小。网络特征选择的目的是提高网络入侵检测模型的性能，因此，将网络入侵检测精度(P)作为的特征选择的目标函数。网络状态特征的优化问题可以表述为：

$$\max_S P(S) \tag{10}$$

其约束条件为：

$$\begin{cases} S=\{s_1,s_2,\cdots,s_n\} \\ s_i\in\{0,1\} \\ i=1,2,\cdots \end{cases} \tag{11}$$

式(10)是一个多特征组合的选择问题，使用穷举法耗时长，且入侵检测的实时性差。而利用 IPSO 算法能够在短时间内搜索到最优解，适合解决网络特征选择问题。采用粒子位串代表选择的特征子集，适应度函数即为入侵检测精确率。当计算适应度值时，先根据 S 处理训练集，再通过 SVM 建模计算检测精确率(P)，但在计算 P 之前须设置 SVM 的相关参数。

SVM 的性能除了与核函数的参数 d 有关，还与惩罚参数 C 有关，C 用于调整最小经验风险和置信度。结合参数 C 和 d，SVM 的参数选择模型为：

$$M=\{d,C\} \tag{12}$$

把系统检测精确率(P)当作 SVM 的参数选择目标函数，SVM 相关参数的选择问题就可以表示为：

$$\max_M P(M) \tag{13}$$

其约束条件为：

$$\begin{cases} M=\{d,C\} \\ d>0 \\ C>0 \end{cases} \tag{14}$$

相比于网络入侵的特征选择问题，SVM 的参数选择问题也可以通过 IPSO 来求解。使用粒子位串表示 SVM 的训练模型参数(M)，检测精确率为适应度函数。需要注意的是，计算 P 时，要先确定网络的特征子集(S)。

将特征集和 SVM 参数组合进行选择的数学模型表示为：

$$\max_{S,M} P(S,M) \tag{15}$$

从式(15)可以看出，(S,M)同时描述了特征子集和 SVM 的参数，式(10)和式(13)只是其特殊情况，因此式(15)也可以通过 IPSO 算法来求解。粒子的个体位置是混合向量(S，M)，其适应度函数为检测精确率 P。当计算适应度值时，先根据混合向量(S,M)选择特征子集和 SVM 的参数，再通过 SVM 模型计算 P，这样能使得 S 和 M 的选择没有先后关系，并且相互关联。粒子编码设计如下。

粒子位串由三部分组成：第一部分表示网络特征子集；第二部分表示参数 C；第三部分表示参数 d。粒子位串的长度根据其精度的需要利用式(16)来调整：

$$j=\min_j+\frac{\max_j-\min_j}{2^l-1}\times e \tag{16}$$

其中，j 表示转换后的参数值，l 表示相应参数的位串长度，$\max_j$ 和 $\min_j$ 分别表示参数的最大值和最小值，e 表示二进制代表的精度。

从图 2 的粒子编码位串可知，第一部分表示特征编码，共 10 位，而第 1，5，6，7，8，9 位的变量构成了特征子集，后两部分即是在此特征集下的编码参数 C 和 d。

图 2　粒子编码

Fig. 2　Particle coding

特征选择与 SVM 参数优化相结合的目的是降低入侵检测系统的误报率和漏报率，从而提高网络入侵检测的精确率。因此，将粒子适应度函数定义为检测精确率，即

$$f(S,M)=\frac{\text{检测准确的样本数}}{\text{样本总数}}\times 100\% \tag{17}$$

IPSO 对 SVM 参数优化的步骤如下：

Step1　对粒子的初始值进行初始化。

Step2　评价粒子的适应度值。对于每个粒子，评价优化函数的适应度值。假设适应度函数为 $F=-\sum_{i=1}^{n}(y_i-\hat{y}_i)^2$，则对于粒子种群中的每一个粒子而言，其距离目标越近，就说明其适应度取值越大。其中，y_i，$\hat{y}_i$ 分别代表 SVM 模型的目标和实际输出结果。

Step3　更新个体最优 P_{best} 和全局最优 G_{best}。

Step4　更新粒子的速度与位置。

Step5　判断是否满足结束条件。若满足，则停止算法，并输出 SVM 的最优参数；若不满足，转向 Step2 进行循环，直到满足结束条件，循环结束。

Step6　在迭代结束之后，将此时得到的支持向量机的最优参数提取出来，并建立 IPSO-SVM 入侵检测模型，同时对需要测试的数据样本进行检测。

通过利用 IPSO 算法对 SVM 中的相关参数进行优化，以提高网络入侵检测系统的整体性能和检测效率。

3.3 IPSO-SVM 检测模型的构建

因为传统的 SVM 算法是针对二分类问题提出来的，但是在实际入侵检测中的攻击类型往往有多种，所以需要构造多分类器来实现分类。本文采用间接法，即通过利用多个二分类器进行组合来实现多类攻击类型的分类。此方法需要构造出 $n(n-1)/2$ 个 SVM，且每个 SVM 由相应的二分类样本进行训练。例如，在第 a 类和第 b 类中寻找最优超平面，则设相应的训练集为：

$$\begin{cases}(x_{ab,t},y_{ab,t}), & t=1,2,\cdots,n_{ab}\\ x_{ab,t}\in R^d, y_{ab,t}\in\{a,b\}\end{cases} \tag{18}$$

$$\min_{\omega_{ab},\xi_{ab}} \frac{1}{2}\|\omega_{ab}\|^2+C\sum_{a=1}^{m_{ab}}\xi_{ab,t} \tag{19}$$

$$\text{s.t.}\begin{cases}(\omega_{ab})^{\mathrm{T}}\varphi(x_{ab,t})+b_{ab}\geqslant 1-\xi_{ab,t}, & y_{ab,t}=a\\ (\omega_{ab})^{\mathrm{T}}\varphi(x_{ab,t})+b_{ab}\geqslant -1+\xi_{ab,t}, & y_{ab,t}=b\\ \xi_{ab,t}\geqslant 0\end{cases} \tag{20}$$

首先，通过使用相应的 SVM 的判决分类函数建立 $n(n-1)/2$ 个 SVM 模型；再利用投票法(Max-Wins Voting，MWV)对检测样本进行判别分类，即对 n 个类的训练样本的任意两类使用二分类 SVM_{ab} 进行比较；经过每轮竞争淘汰之后，最终优胜分类机输出的类别就是测试样本的类别。SVM 检测模型如图 3 所示。

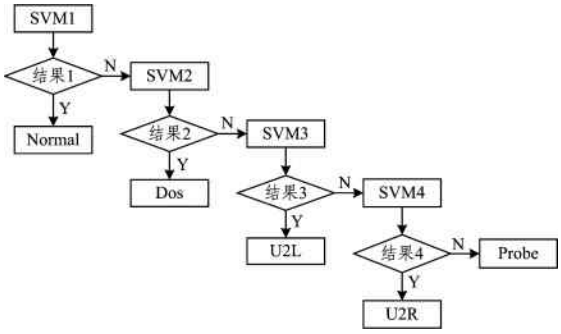

图 3 SVM 检测模型

Fig. 3 SVM detection model

基于 IPSO-SVM 算法的检测系统模型如图 4 所示。

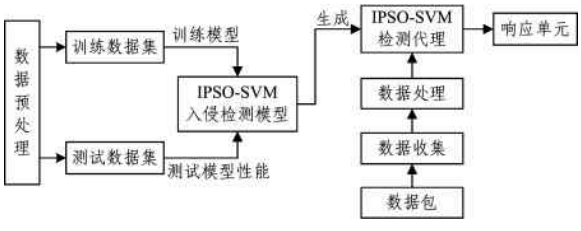

图 4 IPSO-SVM 检测系统模型

Fig. 4 IPSO-SVM detection system model

检测代理用于接收事件预处理单元的数据，并对数据加以分析和处理，其工作内容和责任分为两部分：在训练期间形成相应的分组检测模型；检测模型完成检测阶段的数据检测与处理。

基于 IPSO-SVM 算法的网络入侵检测过程如下：

Step1 采集原始数据。

Step2 对收集的原始数据进行归一化处理，其目的是对特别大或者特别小的样本矢量进行归一化，以减少网络数据的训练用时，加快收敛速度，提高数据的准确度。通过对数据的归一化处理能够极大地提高系统的检测性能。

Step3 将归一化网络入侵检测数据作为 SVM 的学习样本，通过 IPSO 优化 SVM 的参数，获得 SVM 的最优参数。

Step4 SVM 使用获得的最佳参数来训练网络入侵检测的训练样本，从而建模。也就是说，针对样本数较多的攻击类，采用基于边界样本的方法训练样本；而对于样本数量较少的攻击类，构造虚拟样本，使样本分布均匀。然后，通过组合这两种方法来构造一组新的网络训练样本。最后，建立一个最优网络入侵检测模型。

Step5 使用建立好的检测模型对测试样本进行检测。

Step6 输出网络的检测结果。

4 仿真实验与结果分析

4.1 实验环境

本系统选取的实验环境如下。

硬件配置：CPU 为 I5-3470 双核 3.20GHz，内存为 8.00GB，硬盘为 1TB；操作系统：Windows10；测试平台：MATLAB R2011a；实验数据：KDD CUP 99 数据集中的部分数据。

4.2 实验数据源

为了验证本文提出的基于 IPSO-SVM 算法的网络入侵检测系统的性能，采用 KDD CUP 99 数据集中的部分数据[16]。此数据集的入侵行为分为 4 种类型：拒绝服务攻击(DOS)、未授权使用本地超级权限访问攻击(U2R)、远程用户未授权访问攻击(U2L)、扫描攻击(Probe)。KDD CUP 99 数据集收集了 9 周的数据，包括大约 500 万条记录，每条记录包括 41 个特征属性(其中 7 个表示符号特征，34 个表示数字特征)，最后一个是标志属性；除了 Normal 表示正常事件之外，其余标志都表示为异常(Abnormal)。在本实验中，从 KDD CUP 99 数据集中随机选择 6000 条记录，其中测试数据 2900 条，训练数据 3100 条。

4.3 数据预处理

因为传统的 SVM 算法是在输入空间为内积的空间下诱导而出的，而在 DARPA 数据集上通常是无法定义内积的，所以不能直接利用 SVM 算法对 DARPA 数据集进行检测。本文采用 min-max 标准化(min-max Normalization)方法对原始数据进行归一化处理：

$$X^*=\frac{X-X_{\min}}{X_{\max}-X_{\min}} \tag{21}$$

其中，$X_{\max}$ 表示样本数据的最大值，$X_{\min}$ 表示样本数据的最小值。利用此方法将数据处理成[0,1]之间的实数。

4.4 入侵数据的训练与检测

利用 SVM 算法训练预先选择的训练数据集。将数据预处理部分获得的特征值发送到 IPSO-SVM 网络中，然后设置阈值(最大误差值)等参数，以确定输入分组是否为入侵分组。首先，将预处理后的数据发送到数据检测部分的 SVM 网络，训练之后，获得 IPSO 算法的输入(即粒子)；然后，搜索全局最优网络参数，将网络参数的最优值引入到 SVM 网络中，并用另一组数据测试入侵检测系统。检测结果分为两种情况：

1 表示正常，即未发生入侵行为；0 表示异常，即发生了入侵行为。通过上述过程即可完成对 SVM 参数的优化。

4.5　实验结果分析

为了验证本文提出的 IPSO 算法对 SVM 参数优化的有效性，本文采用相同的数据集，将经典 SVM 和 PSO-SVM 算法作为参考模型进行比较。为了确保实验的准确性，测试结果选择多次实验的平均值，其检测的正确率、误报率以及漏报率分别定义如下：

$$\text{正确率}=\frac{\text{检测准确的样本数}}{\text{样本总数}}\times 100\% \tag{22}$$

$$\text{误报率}=\frac{\text{误报为入侵的正常样本总数}}{\text{正常样本总数}}\times 100\% \tag{23}$$

$$\text{漏报率}=\frac{\text{误报为入侵的正常样本总数}}{\text{入侵样本总数}}\times 100\% \tag{24}$$

本文使用的测试函数是 Rastrigrin 标准测试函数，它是一个全局最优值为零、局部最优值随着正弦波动的多峰值函数。Rastrigrin 函数的表达式如下：

$$f(x)=\sum_{i=1}^{n}(x_i^2-10\cos(2\pi x_i)+10) \tag{25}$$

SVM，PSO-SVM，IPSO-SVM 3 种算法的仿真实验结果如表 1 所列。

表 1　SVM，PSO-SVM 和 IPSO-SVM 的仿真实验结果对比/%

Table 1　Comparison of simulation results of SVM，PSO-SVM and IPSO-SVM/%

模型	评价指标	Normal	DOS	Probe	R2L	U2R
SVM	正确率	85.52	82.66	77.65	80.70	81.82
	误报率	6.41	11.29	19.10	6.74	7.52
	漏报率	3.12	6.05	3.25	3.56	4.66
PSO-SVM	正确率	88.56	86.59	82.79	85.32	85.34
	误报率	4.23	10.56	17.23	5.27	4.96
	漏报率	2.32	4.65	2.95	2.96	3.56
IPSO-SVM	正确率	93.30	90.52	87.70	90.93	92.75
	误报率	3.04	9.95	15.56	4.73	2.27
	漏报率	1.66	3.53	2.74	2.34	2.98

从表 1 的实验结果可以看出，IPSO-SVM 算法对 Normal，DOS，Probe，R2L，U2L 的检测正确率分别为 93.30%，90.52%，87.70%，90.93% 和 92.75%，相比于 SVM 算法和 PSO-SVM 算法均有明显提高；同时误报率和漏报率也有所下降。由此可以看出，与经典 SVM 和 PSO-SVM 算法相比，IPSO-SVM 算法在网络入侵检测的整体性能方面均有不同程度的改善。

此外，本文还对 SVM，PSO-SVM 和 IPSO-SVM 3 种算法在不同类型的攻击平均建模时间上进行了验证。所谓建模时间就是建立网络入侵检测系统模型所需要的时间，其体现了建模与检测的效率。3 种算法的平均建模时间如图 5 所示。

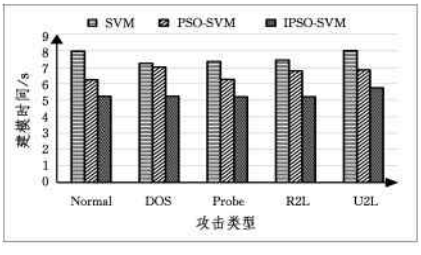

图 5　3 种算法的平均建模时间

Fig. 5　Average modelling time of three algorithms

从图 5 可以看出，相对于 SVM 算法和 PSO-SVM 算法，基于 IPSO-SVM 算法的网络入侵检测方法不仅具有更好的收敛性，而且建模时间明显缩短，其主要原因在于 IPSO-SVM 算法能够更快地找到支持向量机的参数；同时该算法在训练过程中的计算复杂度也明显下降，从而确保了网络入侵检测的效率能够得到显著提升。

结束语　随着网络技术的迅速发展，越来越多的人享受着网络为其带来的便利；与此同时，网络安全问题也成为了现实生活中一个不容忽视的核心问题。针对目前的网络入侵检测系统中存在的检测效率低、误报率和漏报率偏高等问题。本文提出了一种基于 IPSO-SVM 算法的网络入侵检测方法。该方法通过将 IPSO 算法引入到 SVM 参数的优化中，使网络入侵检测系统具有了较强的自学习和自适应能力。实验结果表明，相对于经典的 SVM 和 PSO-SVM 算法，基于 IPSO-SVM 算法的网络入侵检测方法不仅加快了其学习速度，而且提高了网络检测的正确率，降低了误报率和漏报率，同时也更适合用于现实的网络入侵检测系统。

参 考 文 献

[1] LUO B，XIA J. A novel intrusion detection system based on feature generation with visualization strategy[J]. Expert Systems with Applications，2014，41(9)：4139-4147.

[2] SINGH R，KUMAR H，SINGLA R K. An intrusion detection system using network traffic profiling and online sequential extreme learning machine[J]. Expert Systems with Applications，2015，42(22)：8609-8624.

[3] HUANG X，WAN R. The Construction Research of Security Computer Network System Based on the Distributed Intrusion Detection Technology[J]. International Journal of Security and Its Applications，2014，8(6)：185-196.

[4] WANG Y，GU D，LI W，et al. Network intrusion detection with workflow feature definition using bp neural network[C]// Proceedings of the IEEE International Symposium on Neural Networks. Springer Berlin Heidelberg，2009：60-67.

[5] ZHANG X H，LIN B G. Research on Internet Security Based on Balanced Binary Decision Tree SVM Algorithm[J]. Information Network Security，2015，36(8)：20-25.(in Chinese)
张晓惠，林柏钢. 基于平衡二叉决策树 SVM 算法的物联网安全研究[J]. 信息网络安全，2015，36(8)：20-25.

[6] WANG J，ZHU W，ZHANG W，et al. A trend fixed on firstly and seasonal adjustment model combined with the ε-SVR for short-term forecasting of electricity demand[J]. Energy Policy，2009，37(11)：4901-4909.

[7] AN W，LIANG M. A new intrusion detection method based on SVM with minimum within-class scatter[J]. Security and Communication Networks，2013，6(9)：1064-1074.

[8] LI Z G，GAN Q. Research on Network Intrusion Detection Model for Optimizing SVM Parameters by Improved Ant Colony Algorithm[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition)，2014，26(6)：785-789.(in Chinese)

(下转第 260 页)

[5] LI F,MIAO D Q,LIU C H,et al. Image segmentation algorithm based on the decision-theoretic rough set model[J]. CAAI Transactions on Intelligent Systems,2014,9(2):143-147. (in Chinese)
李峰,苗夺谦,刘财辉,等. 基于决策粗糙集的图像分割[J]. 智能系统学报,2014,9(2):143-147.

[6] LI R,GAO C Y,ZHANG L Y. The distributed fault diagnosis of power networks based on bayesian rough set method[J]. Journal of North China Electric Power University (Natural Science Edition),2010,37(3):1-7. (in Chinese)
栗然,高聪颖,张烈勇. 基于粗糙集-贝叶斯方法的分布式电网故障诊断[J]. 华北电力大学学报(自然科学版),2010,37(3):1-7.

[7] MISHRA H,MISHRA A,SHIV B. In praise of vagueness:malleability of vague information as a performance-booster[J]. Psychological Science,2011,22(6):733

[8] LIU D,LI T R,LIANG D C. Fuzzy Decision-theoretic Rough Sets[J]. Computer Science,2012,39(12):25-29. (in Chinese)
刘盾,李天瑞,梁德翠. 模糊数决策粗糙集[J]. 计算机科学,2012,39(12):25-29.

[9] LIU D,LI T R,LI H X. Interval-valued Decision-theoretic Rough Sets[J]. Computer Science,2012,39(7):178-181. (in Chinese)
刘盾,李天瑞,李华雄. 区间决策粗糙集[J]. 计算机科学,2012,39(7):178-181.

[10] LIANG D C,LIU D,WITOLD P,et al. Triangular fuzzy decision-theoretic rough sets[J]. International Journal of Approximate Reasoning,2013,54(8):1087-1106.

[11] ZHONG Y H,ZHANG P X. Generalized trapezoidal decision-theoretic rough sets[J]. Mathematics in Practice and Theory,2015,45(6):82-88. (in Chinese)
钟映竑,张培新. 广义梯形模糊数决策粗糙集[J]. 数学的实践与认识,2015,45(6):82-88.

[12] LIANG D C,LIU D. Deriving three-way decisions from intuitionistic fuzzy decision-theoretic rough sets[J]. Information Science,2015,300(C):28-48.

[13] LIANG D C,XU Z S,LIU D. Three-way decisions with intuitionistic fuzzy decision-theoretic rough sets based on point operators[J]. Information Science,2017,375:183-201.

[14] XUE Z A,ZHU T L,XUE T Y,et al. Model of three-way decision theory based on intuitionistic fuzzy sets[J]. Computer Science,2016,43(6):283-288. (in Chinese)
薛占熬,朱泰隆,薛天宇,等. 基于直觉模糊集的三支决策模型[J]. 计算机科学,2016,43(6):283-288.

[15] BURILLO P,BUSTINCE H,MOHEDANO V. Some definition of intuitionistic fuzzy number[C]// Fuzzy based expert systems. Bulgaria:fuzzy Bulgarian enthusiasts,1994:28-30.

[16] XU Z S,YAGER R R. Some geometric aggregation operators based on intuitionistic fuzzy sets[J]. International Journal of General Systems,2006,35(4):417-433.

[17] LV J H. The research of intuitionistic fuzzy numbers and its application in multi-attribute[D]. Fuxin:Liaoning Technology University,2011. (in Chinese)
吕金辉. 直觉模糊数的研究及在多属性决策中的应用[D]. 阜新:辽宁工程技术大学,2011.

[18] GUO S C,LV J H. The research of the intuitionistic fuzzy numbers[J]. Fuzzy Systems and Mathematics,2013,27(5):11-20. (in Chinese)
郭嗣琮,吕金辉. 直觉模糊数的研究[J]. 模糊系统与数学,2013,27(5):11-20.

(上接第 235 页)

李振刚,甘泉. 改进蚁群算法优化 SVM 参数的网络入侵检测模型研究[J]. 重庆邮电大学学报(自然科学版),2014,26(6):785-789.

[9] WU J Y,CHEN Z D. Research on Application of SVM Based on Improved PSO in Database Intrusion Detection[J]. Software Guide,2015,14(4):134-136. (in Chinese)
吴纪芸,陈志德. 基于改进 PSO 的 SVM 算法在数据库入侵检测中的应用研究[J]. 软件导刊,2015,14(4):134-136.

[10] ZHOU G,SHRESTHA A. Efficient intrusion detection scheme based on SVM[J]. Journal of Networks,2013,8(9):2128-2134.

[11] ZHU X M,ZHANG H B. Stability Analysis and Algorithm Improvement of PSO Algorithm[J]. Computer Science,2013,40(3):275-278. (in Chinese)
朱小明,张慧斌. PSO 算法的稳定性分析及算法改进[J]. 计算机科学,2013,40(3):275-278.

[12] LING S H,LU H H C,LEUNG F H F,et al. Improved hybrid particle swarm optimized wavelet neural network for modeling the development of fluid dispensing for electronic packaging[J]. IEEE Transactions on Industrial Electronics,2008,55(9):3447-3460.

[13] FARIA P,SOARES J,VALE Z,et al. Modified particle swarm optimization applied to integrated demand response and DG resources scheduling[J]. IEEE Transactions on Smart Grid,2013,4(1):606-616.

[14] ESMIN A A A,COELHO R A,MATWIN S. A review on particle swarm optimization algorithm and its variants to clustering high-dimensional data[J]. Artificial Intelligence Review,2015,44(1):23-45.

[15] SHAO P,WU Z J. A Particle Swarm Optimization Algorithm with Sine Function Factor[J]. Small Microcomputer System,2015,36(1):156-161. (in Chinese)
邵鹏,吴志健. 一种带正弦函数因子的粒子群优化算法[J]. 小型微型计算机系统,2015,36(1):156-161.

[16] CHO J,LEE C,CHO S,et al. A statistical model for network data analysis:KDD CUP 99'data evaluation and its comparing with MIT Lincoln Laboratory network data[J]. Simulation Modelling Practice and Theory,2010,18(4):431-435.