基于IQPSO-IDE算法的网络入侵检测方法

马占飞[1],杨 晋[2],金 溢[2],边 琦[3]
1.内蒙古科技大学 包头师范学院,内蒙古 包头 014030
2.内蒙古科技大学 信息工程学院,内蒙古 包头 014010
3.内蒙古师范大学 传媒学院,呼和浩特 010022

摘 要:为了提高网络入侵检测的准确性与检测效率,弥补由单一优化算法带来的计算精度低、易陷入局部极值等不足,将差分算法的思想引入量子粒子群算法中,提出了一种改进量子粒子群算法(Improved Quantum Particle Swarm Optimization algorithm,IQPSO)和改进差分算法(Improved Difference Evolution,IDE)相融合的IQPSO-IDE算法,并将IQPSO-IDE算法对支持向量机(Support Vector Machine,SVM)的参数进行优化。以此为基础,设计了一种基于IQPSO-IDE算法的网络入侵检测方法。实验结果表明,IQPSO-IDE算法与传统的QPSO、GA-DE、QPSO-DE算法相比,不仅在效率上有了明显的改善,而且在网络入侵检测的正确率上分别提高了5.12%、3.05%、2.26%,在误报率上分别降低了3.31%、1.54%、0.93%,在漏报率上分别降低了1.26%、0.73%、0.52%。

关键词:网络安全;入侵检测;量子粒子群算法;差分算法;支持向量机
文献标志码:A **中图分类号:**TP393.08 doi:10.3778/j.issn.1002-8331.1802-0218

马占飞,杨晋,金溢,等.基于IQPSO-IDE算法的网络入侵检测方法.计算机工程与应用,2019,55(10):115-120.
MA Zhanfei, YANG Jin, JIN Yi, et al. Network intrusion detection method based on IQPSO-IDE algorithm. Computer Engineering and Applications, 2019, 55(10):115-120.

Network Intrusion Detection Method Based on IQPSO-IDE Algorithm

MA Zhanfei[1], YANG Jin[2], JIN Yi[2], BIAN Qi[3]
1.Baotou Teachers College, Inner Mongolia University of Science and Technology, Baotou, Inner Mongolia 014030, China
2.School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou, Inner Mongolia 014010, China
3.Vocational Skills Training Department, Inner Mongolia Normal University, Huhhot 010022, China

Abstract: In order to improve the testing efficiency and accuracy of network intrusion detection, and make up for the disadvantages of low computing precision and easy to get into local extremum caused by a single optimization algorithm, this paper introduces the idea of the difference algorithm into the quantum particle swarm algorithm, and proposes an IQPSO-IDE algorithm based on the Improved Quantum Particle Swarm Optimization algorithm(IQPSO) and the Improved Difference Evolution algorithm(IDE). In addition, the IQPSO-IDE algorithm also optimizes the parameters of support vector machines. Based on this, this paper designs a network intrusion detection method based on IQPSO-IDE algorithm. The experimental results show that the efficiency of the IQPSO-IDE algorithm is better than traditional QPSO algorithm, GA-DE algorithm, QPSO-DE algorithm, and the accuracy of network intrusion detection of this algorithm is increased by 5.12%, 3.05% and 2.26%, the rate of false positives is reduced by 3.31%, 1.54% and 0.93%, the non-response rate is decreased by 1.26%, 0.73% and 0.52%.

基金项目:国家自然科学基金(No.61762071,No.61163025);内蒙古自治区自然科学基金(No.2016MS0614);内蒙古自治区高等学校科学研究基金(No.NJZY17287,No.NJZY201)。

作者简介: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;杨晋(1991—),男,研究方向为计算机网络与信息安全;金溢(1994—),女,研究方向为计算机网络与信息安全;边琦(1976—),副教授,硕士生导师,研究方向为教育软件。

收稿日期:2018-02-28 **修回日期:**2018-04-27 **文章编号:**1002-8331(2019)10-0115-06
CNKI **网络出版:**2018-10-15, http://kns.cnki.net/kcms/detail/11.2127.tp.20181009.1623.002.html

Key words: network security; intrusion detection; quantum particle swarm optimization; differential evolution; support vector machine

1 引言

入侵检测系统(Intrusion Detection System,IDS)是指鉴别出对于网络、系统威胁或破坏的行径,然后对这一行径有所响应的过程[1]。IDS作为一种主动式的网络安全防御系统,是近些年飞速发展起来的一种动态的集预防、监控和抵御为一体的新型安全防御机制[2]。虽然IDS是网络安全领域的研究热点,但是其检测性能仍存在很多不足,如主动防御功能存在局限性,误报率和漏报率高等问题。

针对网络入侵检测的不足,许多学者从优化算法与入侵检测分类的角度进行分析研究,以此来提高入侵检测的性能。其中,支持向量机[3](Support Vector Machine,SVM)作为入侵检测分类方法的热门课题,因其具有较高的检测率和较强的推广性等特点,近年来被广泛应用于入侵检测领域。常见的优化算法有:量子粒子群(Quantum Particle Swarm Optimization,QPSO)算法[4]、遗传(Genetic Algorithm,GA)算法[5]、DE(Differential Evolution,DE)算法[6]等。其中,QPSO算法、GA算法作为相对高效的智能优化算法,具有较好的全局优化能力,但是单一使用这些算法仍不可避免地陷入“早熟”收敛的困境。相比于其他优化算法,DE算法作为一种启发式的全局搜索算法,在目标优化、混合算法设计等方面有较好的应用[7],但是传统的DE算法参数的依赖性选择也不可避免地影响着该算法的性能。

根据上述研究,为了更好地避免由单一优化算法导致陷入局部极值,从而影响入侵检测整体性能等问题,本文将差分算法思想引入量子粒子群算法中,提出一种基于改进量子粒子群算法(Improved QPSO,IQPSO)和改进差分算法(Improved DE,IDE)相融合的IQPSO-IDE算法,并提出一种基于IQPSO-IDE算法的网络入侵检测方法。该方法主要利用SVM的机器学习方法建立各类网络入侵的检测分类器,然后通过IQPSO-IDE算法对支持向量机的参数进行优化调整,从而提高网络入侵检测系统的检测性能。实验测试结果与性能分析验证了本文构建的入侵检测方法具有较好的实用性。

2 相关算法研究

2.1 量子粒子群算法简介

粒子群算法(Particle Swarm Optimization,PSO)是一种群体智能算法,由Kennedy博士和Eberhart博士研究发明,此源于对鸟群捕食的行为研究[8]。与PSO算法相类似,量子行为粒子群优化算法(QPSO)是由Sun等人受到量子力学的启发,于2004年提出了PSO算法的新型变体,也是一种基于迭代的优化工具[9]。相比于其他优化算法,QPSO算法在收敛精度与收敛速度的求解上是一种简单而有效的优化算法。该算法通过建立经量子化的吸引势场来约束粒子群中的粒子,使处于量子束缚态的粒子以一定的概率密度覆盖解空间的任何点,进而在很大程度上缓解了粒子过早地陷入局部极值,为系统寻优提供了新的途径[10]。

QPSO算法使得具有量子行为的粒子更加呈现多样性的状态。该算法的基本原理如下:

$$mbest=\frac{1}{m}\sum_{i=1}^{m}P_i=\left(\frac{1}{m}\sum_{i=1}^{m}P_{i1},\frac{1}{m}\sum_{i=1}^{m}P_{i2},\cdots,\frac{1}{m}\sum_{i=1}^{m}P_{iD}\right) \tag{1}$$

$$P_{iD}=\frac{r_1\times P_{iD}+r_2\times P_{gD}}{r_1-r_2} \tag{2}$$

式中,$mbest$(Mean Best Position)表示粒子群中所有粒子的平均最好位置点;m表示粒子群中粒子的数量;D表示粒子的空间维数;r_1与r_2表示值在$[0,1]$上均匀分布的随机数;P_i为第i个粒子的$pbest$;P_g为群体的$gbest$。最后可得到QPSO算法的位置变化方程为:

$$L_{id}(t+1)=\begin{cases}P_{id}-w\left|mbest-L_{id}(t)\right|\ln\left(\frac{1}{u}\right), u>0.5\\ P_{id}+w\left|mbest-L_{id}(t)\right|\ln\left(\frac{1}{u}\right), u<0.5\end{cases} \tag{3}$$

式中,w称为惯性权重,一般取$w=0.5+0.5\times\frac{T_{\max}-t}{T_{\max}}$;$T_{\max}$为粒子的最大进化代数;$t$为粒子的当前迭代次数。

2.2 差分算法简介

差分算法是由Price和Storn在1997年提出用于全局优化的浮点数编码进化算法,现已被成功地应用于并行计算、多目标优化、约束优化等[11]。差分算法的实现过程如下:

(1)生成初始种群

在多维空间随机产生N个个体,其公式如下:

$$x_{ij}(0)=x_{ij}^{\mathrm{L}}+rand(0,1)\left(x_{ij}^{\mathrm{U}}-x_{ij}^{\mathrm{L}}\right) \tag{4}$$

其中,$rand(0,1)$表示在$[0,1]$上服从均匀分布的随机数。

(2)变异操作

作为整个算法过程中的重要步骤,随机从粒子群中选择x_{P_1}、x_{P_2}、x_{P_3}且$P_1\neq P_2\neq P_3$粒子进行变异,则粒子进行变异操作为:

$$h_{ig}(g)=x_{P_1}+F\times\left(x_{P_{2j}}-x_{P_{3j}}\right) \tag{5}$$

其中,F表示缩放因子。

(3)交叉操作

$$v_{ig}(g+1)=\begin{cases}h_{ig}(g), rand(0,1)\leqslant CR \text{ or } j=rand(1,n)\\ x_{ig}(g), rand(0,1)>CR \text{ or } j\neq rand(1,n)\end{cases} \tag{6}$$

式中，CR 表示交叉概率，CR 取值范围同 $rand(0,1)$ 一样。这种交叉操作可以保证 $v_{ig}(g+1)$ 产生的子个体由 $h_{ig}(g)$ 贡献。

(4)选择操作

通过对 $f(v_i(g+1))$ 与 $f(x_i(g))$ 关系的比较，对分量 $v_i(g+1)$ 和分量 $x_i(g)$ 进行选择，从而对粒子进行优劣的筛选，让具有最优适应度的个体进入下一代。

$$x_i(g+1)=\begin{cases}v_{ig}(g), f(v_i(g+1))<f(x_i(g))\\ x_i(g), f(v_i(g+1))\geqslant f(x_i(g))\end{cases} \tag{7}$$

3　IQPSO-IDE算法设计

3.1　IQPSO算法

传统的QPSO算法在迭代寻优过程中会出现粒子群聚集度不断提高，种群的多样性快速下降的现象，此时迭代过程中粒子群将可能陷入局部极值的困境，因此本文提出了IQPSO算法。首先在粒子平均最优位置加入高斯扰动来弥补粒子在迭代后期多样性不足的缺陷，从而提高粒子的寻优能力；其次引入粒子“早熟”收敛的判定标准，通过判定使“早熟”收敛的粒子及时跳出局部最优。

IQPSO算法设计中引入高斯扰动过程如下：

$$mbest(t)=mbest(t)+\tau\times randn;\ t=1,2,\cdots,m \tag{8}$$

$$mbest=\frac{1}{m}\sum_{i=1}^{m}P_i=\left(\frac{1}{m}\sum_{i=1}^{m}P_{i1},\frac{1}{m}\sum_{i=1}^{m}P_{i2},\cdots,\frac{1}{m}\sum_{i=1}^{m}P_{iD}\right) \tag{9}$$

式中，$mbest$ 为所有粒子最优位置的平均值；τ 为常数；$randn$ 表示满足高斯分布的随机数，且取值范围在均值0与标准方差1之间。

在算法迭代过程中，粒子的位置决定了其适应度值，并通过粒子群的适应度方差 s^2 反映粒子群中粒子的状态。当 s^2 值越大时，粒子“聚集”程度就越小，算法的搜索性能就好；当 s^2 值越小趋于0时，粒子“聚集”程度就越大，粒子群在迭代过程中陷入局部最值，此时算法将不能搜寻出全局最优值。

因此，本文通过选择适应度方差 s^2 值来判定是否跳出局部最优。设种群的适应度方差为 s^2，其公式为：

$$s^2=\sum_{m=1}^{M}\left(\frac{f_m-f_{\text{avg}}}{f}\right)^2 \tag{10}$$

$$f=\begin{cases}\max|f_m-f_{\text{avg}}|, \max|f_m-f_{\text{avg}}|>1\\ 1, \text{else}\end{cases} \tag{11}$$

式中，m 是粒子种群规模；f 为归一化因子；f_m 为第 m 个粒子的适应度；f_{avg} 为当前粒子群的平均适应度；s^2 表示适应度方差。在这步操作过程中，设定一个阈值 e，当算法在迭代寻优过程中，若判定 $s^2<e$，则认为陷入局部最优；反之，没有陷入局部最优。

3.2　IDE算法

差分算法中，粒子数量 N 一般介于 $5\times D$ 与 $10\times D$ 之间；CR 为交叉概率因子，可控制个体从父代继承选择变异的概率大小；参数 F 表示缩放因子，是可变参数中最重要的一个。为了充分发挥差分算法在混合优化算法设计中的全局优化性能，本文对参数缩放因子 F 进行了优化，提出了IDE算法。

参数 F 通过差分矢量的大小影响粒子群中父代个体变异的程度。通过对参数 F 进行调控，可以更好地增强粒子群体的多样性。在差分算法迭代初期，粒子之间差异性较大，此时 F 趋于较大值，可有利于算法的全局搜索能力；在算法迭代后期，粒子群的聚集度不断提高，种群的多样性会快速下降，此时通过调控，当 F 趋于较小值时，更有利于提高算法的局部搜索能力。因此，为了提高算法在不同迭代时期的搜索性能，增强差分算法在混合算法设计中全局优化的性能，本文在差分算法中引入控制参数 F 的自适应变化策略，即在算法的不同时期可以动态调整缩放因子的值，从而增强差分算法在混合算法设计中目标优化的应用。缩放因子 F 的动态调整如下：

$$F=a\times(e^b-1) \tag{12}$$

式中，a 表示常数且取值范围在 $[0.2,0.6]$ 之间；b 为可变参数，$b=\frac{C_{\max}}{C_{\max}+C}$，$C$ 为当前迭代次数，$C_{\max}$ 为最大迭代次数。

3.3　IQPSO-IDE算法的设计

在IQPSO算法中，粒子表示的是待求解问题的可行性存在解，粒子位置状态变化的过程实质上就是问题的求解过程。而在IQPSO算法设计中，除了在平均最优位置引入高斯扰动来增强粒子群的多样性外，还通过判定机制来判断增加高斯扰动的粒子是否跳出局部最优，从而达到全局寻优的能力。若粒子不满足条件，仍未全部跳出局部最优，则转入IDE算法进行迭代寻优来增强算法的寻优能力。一方面通过利用差分算法的变异策略丰富粒子群体的多样性；另一方面利用差分算法的“贪婪”搜索策略，更好地使其应用于目标优化问题中，满足最优值问题的求解。若粒子满足条件跳出局部最优，则粒子转入IDE算法进行迭代寻优来增强算法求解的收敛精度。

根据上述研究，为了更好地增强IQPSO算法的全局寻优能力与收敛精度，本文提出了一种新的IQPSO-IDE算法。该算法的主要思想是将优化以后的IQPSO算法与优化以后的IDE算法进行融合。IQPSO-IDE算法首先通过对IQPSO算法在平均最优位置加入高斯扰动的优化与改进，弥补粒子在迭代后期多样性快速下降、粒子可能收敛于局部极值的缺陷。其次通过方差值与阈值 e 的大小来判定IQPSO算法是否陷入局部最优。若

$s^2<e$，则认为陷入局部最优，此时转入IDE算法进行迭代寻优操作，利用IDE算法的变异、交叉、选择操作来引导陷入局部最优值的粒子偏离局部最优点，找到全局最优的值，直到满足IDE算法最大迭代次数，结束迭代，输出最优值。反之，则认为没有陷入局部最优，继续执行IQPSO算法进行迭代搜索，直到满足IQPSO算法最大迭代次数，结束迭代并转入IDE算法进行迭代寻优操作，直至迭代结束输出最优值。

IQPSO-IDE算法设计的具体描述如下：

第一阶段IQPSO算法寻优操作，具体步骤为：

步骤1　设定IQPSO算法参数，如搜索维数、种群规模和迭代次数等，并初始化粒子种群。

步骤2　对IQPSO算法中粒子群进行迭代搜索，并根据式(1)、(2)记录粒子状态，并计算粒子的适应度值，由初始适应度评价每个粒子的优劣，若粒子当前位置优于历史最优位置，用当前目标更换；若当前种群全局位置优于历史最优位置，则用当前位置更换。

步骤3　根据粒子的局部最优值和全局最优值确定最优粒子，并根据式(8)对种群进行高斯扰动操作，提高粒子群的多样性，并根据式(3)更新粒子状态。

步骤4　判断IQPSO算法是否满足终止条件，若是，转入第二阶段IDE算法步骤6；否则执行步骤5。

步骤5　根据式(10)计算种群的适应度方差，并判断s^2是否大于阈值e，若是，则认为算法陷入局部最优，转入第二阶段IDE算法迭代寻优；否则，转入步骤2更新粒子状态。

第二阶段IDE算法寻优操作，具体步骤为：

步骤6　通过式(4)确定初始化粒子群规模，以及确定IDE算法基本参数，如迭代次数G，缩放因子的最小值$F_{\min}$，最大值$F_{\max}$；交叉因子的初始值CR_0，最大值$CR_{\max}$，最小值$CR_{\min}$等。

步骤7　变异操作。结合式(5)，并利用式(12)优化IDE算法中的变异操作，并随机从粒子群中选取粒子进行变异，从而使聚集程度较高的粒子群脱离陷入局部最优的缺陷，进而使粒子群向所期望的方向发展变化。

步骤8　交叉操作。在上述变异操作的基础上，利用式(6)进行交叉操作来保证粒子个体是由变异操作产生的子个体。

步骤9　选择操作。通过评价函数$v_i(g+1)$和$x_i(g)$之间的比较，对粒子进行优劣选取，从而让具有最优适应度的个体进入下一代。

步骤10　判断IDE算法是否满足终止条件，若是，结束迭代，输出最优值；否则，转入步骤7，继续迭代寻优，直至满足迭代终止条件，结束迭代。

基于IQPSO-IDE算法的流程结构如图1所示。

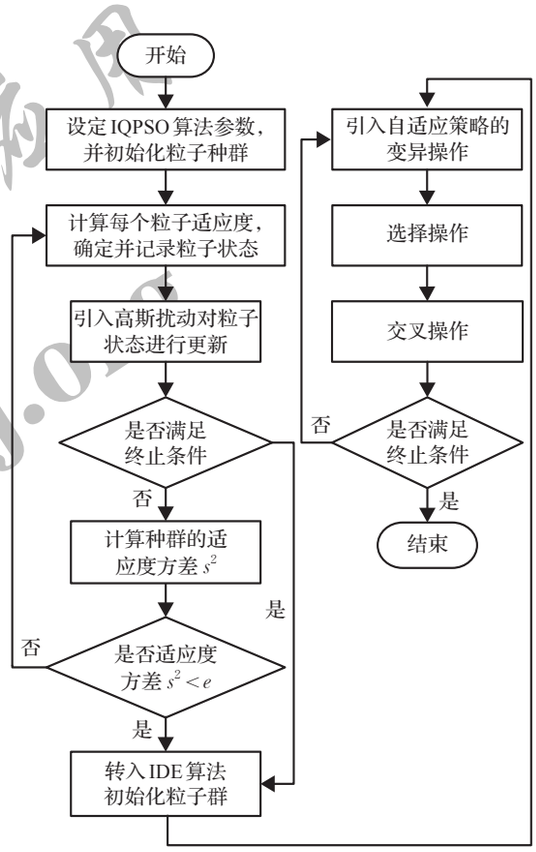

图1　IQPSO-IDE**算法的流程结构图**

4　基于IQPSO-IDE算法的入侵检测模型设计

SVM为热门的入侵检测分类方法，其具有很好的推广性、较高的检测率等特点。因此，本文选取SVM作为入侵检测分类器，并将IQPSO-IDE算法与支持向量机分类模型相结合，构造了一种新的入侵检测方法——基于IQPSO-IDE算法的入侵检测方法。

基于IQPSO-IDE算法的入侵检测方法的本质是利用IQPSO-IDE算法优化SVM，以匹配出SVM的最佳参数值为基础而设计的最优网络入侵检测方法。而SVM的分类性能除了与选取的核函数参数g有关外，还与惩罚参数C有关。其中，参数g的取值影响输入空间与特征空间之间的映射。参数C的值既影响着平衡训练误差，又影响着模型复杂度。

基于IQPSO-IDE算法的入侵检测方法是由$n(n-1)/2$个SVM组合来实现多类攻击类型的分类。因为传统的SVM主要应用于解决二分类问题，无法满足多样化攻击种类的检测，所以需通过构造多个SVM分类器来实现样本分类。数据检测是利用SVM机器学习的分类功能，通过投票法(Max-Wins Voting，MWV)对检测数据进行优胜劣汰选择，从而输出测试样本的类别。测试样本的类别则通过每一层SVM检测到的结果进行判别[12]。如第1层对检测样本进行判别，划分为Normal和Abnormal两大类；第2~4层开始依次将异常数据送入SVM进行分类。第2层SVM检测的入侵类型为Dos，

第3层SVM检测的入侵类型为R2L，第4层SVM检测的入侵类型为两种，分别是U2R与Probe[13]。检测结果可分为两种状态：1表示检测结果为正常，未发生入侵行为；-1表示检测结果为异常，发生入侵行为。其中，SVM核函数选取运行时间短、分类准确率高的径向基核函数 $K(x,y)=\exp(-|x-y|^2/d^2)$。

基于IQPSO-IDE算法的入侵检测方法主要包括数据预处理、训练与测试三个步骤。首先，在数据预处理步骤中，将数据集处理成[0，1]之间的实数；其次，在训练步骤中，通过本文设计的基于IQPSO-IDE算法的入侵检测模型对预先选定好的训练数据集进行入侵行为的判别测试，并通过训练数据集训练出最优网络入侵检测模型参数值；最后，在测试步骤中，通过基于IQPSO-IDE算法的最优网络入侵检测模型对测试数据进行分析，输出网络入侵检测结果。

基于IQPSO-IDE算法入侵检测方法的检测过程如下：

步骤1　截获网络数据包。

步骤2　数据预处理。利用网络数据特征属性，对数据集进行标准化、归一化。由于针对输入差异性较大的样本矢量，将会出现训练建模过程时间增大，或者样本无法收敛等问题，因此需对其进行标准化、归一化处理。数据预处理的优势在于既加快了最优解求解过程的速度，又提高了数据的精度。

步骤3　训练数据集。将预处理的部分数据作为训练数据集，利用步骤1~步骤10迭代寻优步骤来完成IQPSO-IDE算法对SVM分类器的优化，即完成IQPSO-IDE算法对SVM参数值的优化，并训练出SVM最佳参数值。通过匹配得出的最佳参数值作为基于IQPSO-IDE算法的入侵检测模型的最优参数，从而建立最优网络入侵检测模型。

步骤4　测试数据。利用预处理的剩余数据作为测试数据，对步骤3得出的IQPSO-IDE算法最佳入侵检测模型进行性能测试。

步骤5　通过测试数据在基于IQPSO-IDE算法最佳入侵检测模型中的测试，输出最终的测试结果。

基于IQPSO-IDE算法入侵检测模型结构如图2所示。

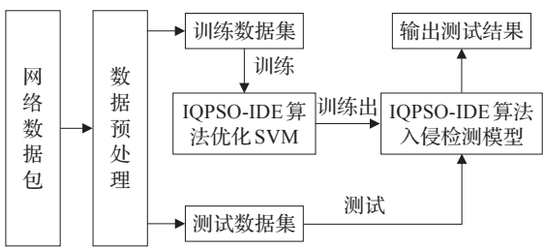

图2　基于IQPSO-IDE算法入侵检测模型结构图

5　仿真实验与结果分析

5.1　实验环境

本文在Windows 7系统测试环境下，以Matlab 2012软件为实验测试平台。选取改进的KDD CUP 99数据集[14]作为实验测试依据，以满足当下多样化、复杂化的网络攻击手段以及网络环境。改进的KDD CUP 99数据集通过降低数据特征属性提取难度，为研究人员对数据集应用到真实网络环境中提供更便利的条件，并确保实验的有效性和真实性。为了验证本文提出的IQPSO-IDE算法的正确性和有效性，从改进的KDD CUP 99数据集随机抽取20 000条记录。其中，测试数据12 000条。数据集中Normal表示正常事件，异常(Abnormal)表示入侵行为。主要包括四种攻击类型：拒绝服务攻击(DOS)、本地权限提升攻击(U2R)、远程攻击(R2L)和探测攻击(Probe)[15]。

5.2　实验结果分析

实验过程采用相同的数据集，QPSO算法、GA-DE算法、QPSO-DE算法作为参考模型，并与IQPSO-IDE算法进行比较。QPSO算法作为主流代表的单一优化算法与本文提出的IQPSO-IDE混合算法相比较，实验检测结果可以更加直观地表述算法的优劣。其次IQPSO-IDE算法与传统的QPSO-DE算法和较流行的检测方法GA-DE算法相比较，则可从实验测试结果对比检验算法改进是否有效，以便更为全面地验证本文提出的基于IQPSO-IDE算法入侵检测方法的有效性。

本次实验测试中，设定实验测试函数的维数 $D=20$，粒子群体数量 $m=50$，最大迭代次数的取值为100；IQPSO算法的阈值取 5×10^{-6}；DE算法中缩放因子 $Fc=0.5$，交叉概率 $CR=0.6$，$c_1=c_2=2$；GA算法中，位置交叉概率 $P_c=0.7$，位置变异概率 $P_m=0.5$。SVM的参数搜索范围是：惩罚因子 $C\in[0,1\,000]$，$g\in[0.01,100]$。

为了确保IQPSO-IDE算法与QPSO算法、GA-DE算法、QPSO-DE算法实验测试的有效性，本文从入侵检测方法的检测正确率、误报率、漏报率以及平均建模时间对四种算法进行评判，且分别选取各自最优入侵模型参数值与200次测试数据中检测率的平均值作为参考值进行对比。其中检测率的三个评价指标分别定义如下：

$$\text{误报率}=\frac{\text{被误报为入侵的正常样本数}}{\text{正常样本数}}\times100\%$$

$$\text{正确率}=\frac{\text{检测准确的样本数}}{\text{样本总数}}\times100\%$$

$$\text{漏报率}=\frac{\text{被误报为入侵的正常样本数}}{\text{入侵样本总数}}\times100\%$$

基于IQPSO-IDE、QPSO-DE、QPSO、GA-DE算法的仿真实验结果如表1所示。

表1　四种算法的仿真实验结果

模型	攻击类型	正确率/%	误报率/%	漏报率/%	C	g
QPSO	Normal	89.56	5.41	2.42	112.70	12.11
	DOS	88.42	9.39	5.05		
	Probe	86.16	14.64	2.84		
	R2L	87.42	5.62	2.66		
	U2R	87.78	5.48	3.66		
GA-DE	Normal	91.63	3.64	1.89	72.30	16.14
	DOS	90.52	8.89	4.31		
	Probe	89.33	11.06	2.71		
	R2L	90.41	4.71	2.53		
	U2R	90.88	2.63	2.84		
QPSO-DE	Normal	92.42	3.03	1.68	83.06	17.30
	DOS	91.48	8.56	3.55		
	Probe	90.54	10.23	2.65		
	R2L	90.62	4.07	2.36		
	U2R	91.64	2.26	2.56		
IQPSO-IDE	Normal	94.68	2.10	1.16	58.61	4.13
	DOS	93.75	7.24	2.63		
	Probe	93.58	8.32	2.04		
	R2L	93.93	2.83	1.84		
	U2R	94.03	1.97	1.68		

从表1的实验测试结果可知，IQPSO-IDE算法不仅检测的正确率提高之外，实验测试指标误报率和漏报率也随之下降。与传统的QPSO、GA-DE、QPSO-DE算法相比，入侵检测的正确率分别提高了5.12%、3.05%、2.26%，误报率分别降低了3.31%、1.54%、0.93%，漏报率分别降低了1.26%、0.73%、0.52%。因此，通过与多种不同类型的算法相比较，本文提出的IQPSO-IDE算法可以更好地避免粒子陷入“早熟”收敛，提高算法全局寻优的能力，从而更好地优化SVM，并匹配出SVM中惩罚因子 C 与核函数参数 g 的最佳参数值，增强SVM的分类性能，提高基于IQPSO-IDE算法入侵检测方法的检测性能。

本文还对IQPSO-IDE、GA-DE、QPSO-DE、QPSO四种算法在该实验的平均建模时间进行了对比分析。平均建模时间是指实验测试过程中建立网络入侵检测系统模型所花费的时间，它的大小体现了建模与检测结果的效率。实验结果如图3所示，相比于QPSO、GA-DE、QPSO-DE算法，IQPSO-IDE算法的平均建模时间明显减少，反映了该算法的寻优速度更快。

6　结束语

网络技术的迅猛发展，给日常生活带来了前所未有的帮助，但是不容忽视的是网络安全也日益成为现实生活中的热点话题。本文针对网络入侵检测的局限性，从单一优化算法的缺陷出发，提出基于IQPSO-IDE算法的网络入侵检测方法。与多种检测方法进行对比，实验结果验证了本文提出的算法应用在网络入侵检测中的有效性，并可为网络优化和入侵检测提供依据。但是网络入侵检测技术仍存在很多可研究的空间。在下一步的研究工作中，将继续探索更为有效的入侵检测方法。

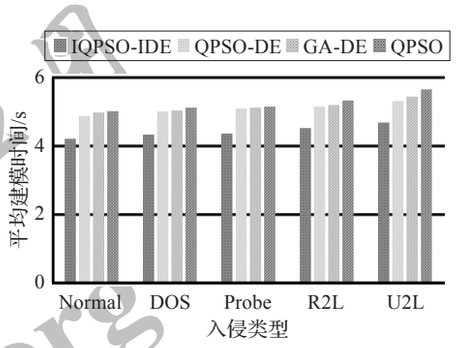

图3　四种算法平均建模时间对比图

参考文献：

[1] Luo S 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.

[2] Ambusaidi M A, He X, Nanda P, et al.Building an intrusion detection system using a filter-based feature selection algorithm[J].IEEE Transactions on Computers, 2016, 65(10): 2986-2998.

[3] Aburomman A A, Reaz M B I.A novel SVM-*k*NN-PSO ensemble method for intrusion detection system[M].[S.l.]: Elsevier Science Publishers, 2016.

[4] Fan Q, Wang T, Chen Y, et al.Design and application of fuzzy logic system based on QPSO intelligent algorithm[J]. ICIC Express Letters, 2017, 11(1): 133-149.

[5] Aslahi-Shahri B M, Rahmani R, Chizari M, et al.A hybrid method consisting of GA and SVM for intrusion detection system[J].Neural Computing & Applications, 2016, 27(6): 1-8.

[6] Yang S, Wang W, Lin Q, et al.A novel PSO-DE co-evolutionary algorithm based on decomposition framework[C]// International Conference on Smart Computing and Communication, Cham, 2016: 381-389.

[7] Zheng L M, Zhang S X, Zheng S Y, et al.Differential evolution algorithm with two-step subpopulation strategy and its application in microwave circuit designs[J].IEEE Transactions on Industrial Informatics, 2017, 12(3): 911-923.

[8] Zhang H, Liang Y, Ma J, et al.An improved PSO method for optimal design of subsea oil pipelines[J].Ocean Engineering, 2017, 141: 154-163.

（下转第204页）