•可信计算与信息安全•

DOI:10.15961/j.jsuese.201700642

融合杜鹃搜索的灰狼优化算法在网络入侵检测特征选择中的应用

徐　慧,付迎春,刘　翔,方　策,苏　军

(湖北工业大学 计算机学院,湖北 武汉 430068)

摘　要:针对当前网络入侵检测技术由于特征冗余引起的检测效率低和准确率低等问题,将一种融合杜鹃搜索的灰狼优化算法应用于网络入侵检测的特征选择中,旨在减少特征冗余,进而提高网络入侵检测的性能。首先,在每次迭代过程中采用杜鹃搜索算法中的莱维飞行机制对适应度值最好的3只灰狼的位置进行扰动,避免在搜索最优解的过程中陷入局部最优。然后,采用灰狼优化算法的更新机制来更新灰狼的位置信息,使狼群朝着猎物的方向聚集。最后,根据预先设定的概率值对狼群的位置进行随机更新,迫使狼群在不断逼近猎物的过程中,能随机地跳出局部最优,从而提高灰狼优化算法在网络入侵检测特征选择中的全局搜索能力。使用网络入侵检测NSL-KDD测试集进行验证实验,并与灰狼优化算法、杜鹃优化算法以及传统的信息增益算法从特征选择的角度进行对比,结果表明,将融合杜鹃搜索的灰狼优化算法应用于网络入侵检测的特征选择时,分类准确率及特征子集的选择都取得较好的效果。融合杜鹃搜索的灰狼优化算法在全局搜索能力方面有较为显著的提升,将其应用于特征选择中,可以有效地提高网络入侵检测的性能。

关键词:网络入侵检测;特征选择;灰狼优化算法;杜鹃搜索算法

中图分类号:TP393.08　　**文献标志码**:A　　**文章编号**:2096-3246(2018)05-0160-07

Applying Improved Grey Wolf Optimizer Algorithm Integrated with Cuckoo Search to Feature Selection for Network Intrusion Detection

XU Hui, *FU Yingchun*, *LIU Xiang*, *FANG Ce*, *SU Jun*

(School of Computer Sci., Hubei Univ. of Technol., Wuhan 430068, China)

Abstract: In order to solve the problem of low detection efficiency and low accuracy caused by feature redundancy in current network intrusion detection technology, an improved Grey Wolf Optimizer algorithm integrated with Cuckoo Search was applied to feature selection for network intrusion detection, which aimed at reducing the feature redundancy and improving the performance of network intrusion detection. First, the Levy flight mechanism in the Cuckoo Search algorithm was adopted to disturb the position of three grey wolves with the best fitness values, which avoided the local optimum in the process of searching the optimal solution. Then, the updating mechanism of the Grey Wolf Optimizer algorithm was utilized to update the location information of grey wolves, ensuing these wolves could gather in the direction of their prey. Finally, the location of the grey wolf group was randomly updated according to the predetermined probability value. Hence, the grey wolf group could randomly jump out of the local optimum in the process of continuous approximation of the prey, which improved the global-search ability of the Grey Wolf Optimizer algorithm in feature selection for network intrusion detection. The NSL-KDD dataset in network intrusion detection was used for the verification, and the Grey Wolf Optimizer algorithm, the Cuckoo Search algorithm and the traditional Information Gain algorithm were compared in the experiments from the viewpoint of feature selection. The experimental results showed that, when applying the improved Grey Wolf Optimizer algorithm integrated with Cuckoo Search to feature selection for network intrusion detection, it could achieve good results in both the classification accuracy and the selection of feature subsets. In summary, the improved Grey Wolf Optimizer algorithm integrated with Cuckoo Search had a relatively significant improvement in the ability of global search, and its application in feature selection could effectively improve the per-

收稿日期:2017 – 08 – 08

基金项目:国家自然科学基金资助项目(61602162;61440024)

作者简介:徐　慧(1983—),女,副教授,博士. 研究方向:网络与服务管理. E-mail:xuhui@mail.hbut.edu.cn

网络出版时间:2018 – 08 – 30 00 : 20 : 00　　**网络出版地址**:http://kns.cnki.net/kcms/detail/51.1773.TB.20180830.0020.008.html

formance of network intrusion detection.

Key words: network intrusion detection; feature selection; Grey Wolf Optimizer algorithm; Cuckoo Search algorithm

如今，计算机和网络深入到人们生活的方方面面。然而，随着黑客和网络恐怖组织发动的网络攻击在不断的增加，使得网络安全形势十分严峻。为了保证网络的安全运行，网络入侵检测已成为近年来的研究热点。

由于网络入侵检测数据集的特征数量较多，使得入侵检测的时间效率和检测的准确率下降。因此，特征选择成为提升网络入侵检测性能的一个重要手段[1]。对此国内外学者做了许多研究[2−4]，比如传统的特征选择方法（相关性特征选择、信息增益等）、群体智能优化算法（遗传算法、粒子群算法、杜鹃搜索算法等）等来解决网络入侵检测的特征问题。李安等[5]提出将自适应遗传算法与信息增益相结合的特征选择方法应用于网络入侵。袁开银等[6]提出一种混合粒子群算法选择特征的入侵检测模型。虽然这些算法已经广泛的应用，但仍然存在着一些不足有待改进。

灰狼优化（grey wolf optimizer，GWO）算法是Mirjalili等[7]于2014年提出的一种智能优化算法。近年来，GWO算法已被广泛应用在各领域中。吕新桥等[8]将改进后的混合GWO算法用以解决置换流水线调度问题，通过引入局部搜索策略，提高了算法的收敛能力。毛森茂等[9]通过对GWO算法改进，使之能够应用到多目标优化中。王钛等[10]提出了离散GWO算法，并用该算法求解以Kapur分割函数为目标函数的全局优化问题。Seth等[11]将GWO算法应用到入侵检测领域中，使用二进制GWO算法解决数据集的特征选择问题。Emary等[12]将GWO算法应用于特征选择领域，使用UCI数据集作为实验数据并与传统的粒子群和遗传算法进行了对比。

鉴于GWO算法具有良好的寻优性能，比较适合应用于特征选择问题。然而，GWO算法在处理数据维数较多的问题时，容易陷入局部最优，搜寻到的解往往并不理想[13]。而杜鹃搜索（cuckoo search，CS）算法是Yang等[14]在2009年研究杜鹃的繁殖行为时，结合莱维飞行（Levy flights）特征提出的一种群智能优化算法。Jiang等[15]提出一种用于特征选择的改进的二进制杜鹃搜索算法。Aziz等[16]提出将杜鹃搜索算法与粗糙集理论结合在名义数据集中进行特征选择。Raj等[17]提出基于粒子群和杜鹃搜索优化的特征选择方法，来改善网页的分类。

因此，结合网络入侵检测数据集特征维数较多的特点，将一种融合杜鹃搜索的灰狼优化算法应用于网络入侵检测的特征选择中，该算法在迭代过程中融合莱维飞行机制对种群进行位置的扰动更新，使算法避免陷入局部最优。采用网络入侵检测测试集与现有的标准算法及传统算法进行对比实验，以验证该算法在网络入侵检测特征选择中的有效性。

1　基础算法

1.1　灰狼优化算法

GWO算法源自于自然界中的灰狼种群的捕食机制与灰狼种群的等级制度。一般来说，灰狼的种群数量被控制在5到12只之间，它们有着严格的等级划分。在灰狼的种群中主要划分有α、β、δ、ω这4种等级。其中，α灰狼为领导阶层，负责领导种群中其它灰狼的行动。β灰狼为第二阶层，负责帮助领导阶层的灰狼制定各种决策和活动行为。δ灰狼为第三阶层，它们听从α和β灰狼的命令，并且对下级灰狼进行管理。ω灰狼则为种群中的最低层。在实际问题中，α、β、δ对应的是适应度最好的3个解。

灰狼种群的猎食行为主要分为以下3个阶段。

1）包围猎物阶段

灰狼包围猎物的行为由式（1）和（2）表示：

$$\boldsymbol{D} = |\boldsymbol{C} \cdot \boldsymbol{X}_P(t) - \boldsymbol{X}(t)| \tag{1}$$

$$\boldsymbol{X}(t+1) = \boldsymbol{X}_p(t) - \boldsymbol{A} \cdot \boldsymbol{D} \tag{2}$$

其中，t为算法当前迭代的次数，$\boldsymbol{A}$和$\boldsymbol{C}$是系数向量，其计算方式如式（3）和（4）所示：

$$\boldsymbol{A} = 2 \cdot a \cdot \boldsymbol{r}_1 - a \tag{3}$$

$$\boldsymbol{C} = 2 \cdot \boldsymbol{r}_2 \tag{4}$$

其中，a的值随着算法迭代次数的增加从2到0之间线性减少，$\boldsymbol{r}_1$和$\boldsymbol{r}_2$是[0, 1]之间的随机向量。

2）狩猎阶段

当灰狼发现猎物的位置时，狼群会逐渐包围猎物。通常假设α、β、δ灰狼在狩猎过程中知道猎物的位置，狼群会根据它们的位置利用式（5）～（7）和（8）进行位置更新。

$$\boldsymbol{X}(t+1) = \frac{\boldsymbol{X}_1 + \boldsymbol{X}_2 + \boldsymbol{X}_3}{3} \tag{5}$$

$$\boldsymbol{X}_1 = |\boldsymbol{X}_\alpha - \boldsymbol{A}_1 \cdot \boldsymbol{D}_\alpha| \tag{6}$$

$$\boldsymbol{X}_2 = \left|\boldsymbol{X}_\beta - \boldsymbol{A}_2 \cdot \boldsymbol{D}_\beta\right| \tag{7}$$

$$\boldsymbol{X}_3 = |\boldsymbol{X}_\delta - \boldsymbol{A}_3 \cdot \boldsymbol{D}_\delta| \tag{8}$$

其中：式（5）表示灰狼$\boldsymbol{X}$在算法第$t+1$代时的位置；$\boldsymbol{X}_\alpha$、$\boldsymbol{X}_\beta$、$\boldsymbol{X}_\delta$代表的是在狩猎过程中α、β、δ灰狼的位置，

即是问题的最优的3个解。式(6)、(7)和(8)中的$\boldsymbol{A}_1$、$\boldsymbol{A}_2$、$\boldsymbol{A}_3$由式(3)计算得出。$\boldsymbol{D}_\alpha$、$\boldsymbol{D}_\beta$、$\boldsymbol{D}_\delta$的定义如式(9)、(10)和(11)所示,其中$\boldsymbol{C}_1$,$\boldsymbol{C}_2$,$\boldsymbol{C}_3$由式(4)计算得出。

$$\boldsymbol{D}_\alpha = |\boldsymbol{C}_1 \cdot \boldsymbol{X}_\alpha - \boldsymbol{X}| \tag{9}$$

$$\boldsymbol{D}_\beta = \left|\boldsymbol{C}_2 \cdot \boldsymbol{X}_\beta - \boldsymbol{X}\right| \tag{10}$$

$$\boldsymbol{D}_\delta = |\boldsymbol{C}_3 \cdot \boldsymbol{X}_\delta - \boldsymbol{X}| \tag{11}$$

3)攻击猎物阶段

当灰狼停止移动的时候便开始攻击猎物。a的值随着算法迭代次数的增加而不断减少,其值的更新如式(12)所示:

$$a = 2 - 2\left(\frac{t}{T_{\max}}\right) \tag{12}$$

其中,$T_{\max}$代表的是最大迭代次数。

由式(12)可知,收敛因子a是随着迭代次数的增加从2到0之间线性减少的。

1.2 杜鹃搜索算法

CS算法具有搜索路径优以及全局搜索能力强的特点,可以用来改进GWO算法容易陷入局部最优的不足。

杜鹃鸟的繁殖行为比较特殊,它不自己孵化后代,而是通过将卵产入其它鸟巢,借助其他鸟为其孵化养育后代。这种繁殖方式存在着一定的风险,鸟巢主人可能会发现这些外来鸟蛋,于是会将其抛弃或重新筑巢。CS算法中的莱维飞行是自然界中许多动物和昆虫的一种典型的随机游走的方式,游走的步长满足重尾分布。

杜鹃鸟寻找鸟巢的位置进行更新,如式(13)所示:

$$x_i(t+1) = x_i(t) + \alpha \oplus L(\lambda), 1 < i \le n \tag{13}$$

其中,$x_i(t+1)$为第i个鸟巢更新后的位置,$\alpha > 0$为控制步长的变量,$L(\lambda)$为代表莱维分布随机数,如式(14)所示:

$$L \sim u = t^{-\lambda},\ 1 < \lambda < 3 \tag{14}$$

2 融合杜鹃搜索的灰狼优化算法

在迭代过程中,GWO算法始终跟随α、β、δ灰狼对狼群的位置进行更新,导致其全局搜索能力较弱,容易陷入局部最优。特别地,在应用于网络入侵检测领域时,由于数据集的维数较高,GWO算法更容易出现局部最优问题。而CS算法结合莱维飞行模式寻找鸟巢并且根据预先给定的概率Pa随机地对鸟巢位置进行更新,这使得它很容易从当前的区域跳入到其它区域,全局搜索能力较强。因此,本文尝试在已有工作[18]的基础上,进一步深化GWO算法与CS算法的融合思想,在GWO算法对位置的更新方式中融入CS算法中出现的两次扰动过程,结合CS算法的莱维飞行模式和对鸟巢位置随机更新的特点,最终将改进后的融合杜鹃搜索的灰狼优化(CS-GWO)算法应用于网络入侵检测的特征选择中。

2.1 编码方式

由于标准的GWO算法是用于求解连续变量问题,而特征选择是一个典型的离散空间的组合优化问题,无法直接使用标准的GWO算法。因此,有效的编码是GWO算法应用于特征选择的关键步骤之一。

设狼群中的灰狼数量为m,原始数据集的特征数量为d,对于需要优化的特征选择问题,以适应度值作为待寻优变量,每只灰狼的位置对于一个可行解,对灰狼的每一维采用二进制方式编码,由于数据集的特征数量为d,因此狼群的位置矩阵为一个$m \times d$维的0,1二进制矩阵,如矩阵$\boldsymbol{G}$所示。

$$\boldsymbol{G} = \begin{bmatrix} G_{11} & G_{12} & \cdots & G_{1d} \\ G_{21} & G_{22} & \cdots & G_{2d} \\ \vdots & \vdots & \vdots & \vdots \\ G_{m1} & G_{m2} & \cdots & G_{md} \end{bmatrix}。$$

矩阵$\boldsymbol{G}$中,$G_{m1}, G_{m2}, \cdots, G_{md}$为狼群中各灰狼每一维度的编码。由于数据集的特征数量为d,因此,每只灰狼有d个二进制编码,其中,“0”为该只灰狼所代表的可行解不选择该特征,“1”为该只灰狼所代表的可行解选择该特征。

2.2 初始种群的生成

为了保证初始灰狼种群的多样性,通过随机的方式来对种群中的灰狼个体进行初始化,初始化公式如式(15)、(16)所示:

$$\boldsymbol{G}_i = [G_{ij}], 1 \le i \le m, 1 \le j \le d \tag{15}$$

$$G_{ij} = \begin{cases} 0, & \text{if} \quad rand < 0.5; \\ 1, & \text{if} \quad rand \ge 0.5 \end{cases} \quad 1 \le i \le m, 1 \le j \le d \tag{16}$$

其中,$\boldsymbol{G}_i$为狼群$\boldsymbol{G}$中第i只狼,$\boldsymbol{G}_{ij}$为第i只狼的第j维特征。对于每只灰狼G_i的每一维特征G_{ij},当生成的随机数小于0.5时,将这一维置为0,其它情况置为1。$rand$是区间[0, 1]上的随机数。

2.3 适应度函数

适应度函数又称评价函数,它用于评判种群中每只灰狼的适应度值。在网络入侵检测领域中,适应度与2个因素有关:一个是分类的正确率,另一个是所选用的特征数量。根据适应度值可以选出适应度较高的3只灰狼,由它们指引狼群的位置更新,使狼群朝着猎物的方向移动。选用的适应度函数如式(17)所示。

$$F_i = \frac{ac}{1+\eta \cdot n(i)} \tag{17}$$

式中，F_i为第i只灰狼所代表的可行解的适应度值，ac为该可行解的分类正确率，$n(i)$为此可行解所选择的特征总数，η是一个权重参数，取值为0.01。

2.4 算法流程

基于CS-GWO的网络入侵检测特征选择流程图如图1所示。CS-GWO算法的更新机制主要分为三步。

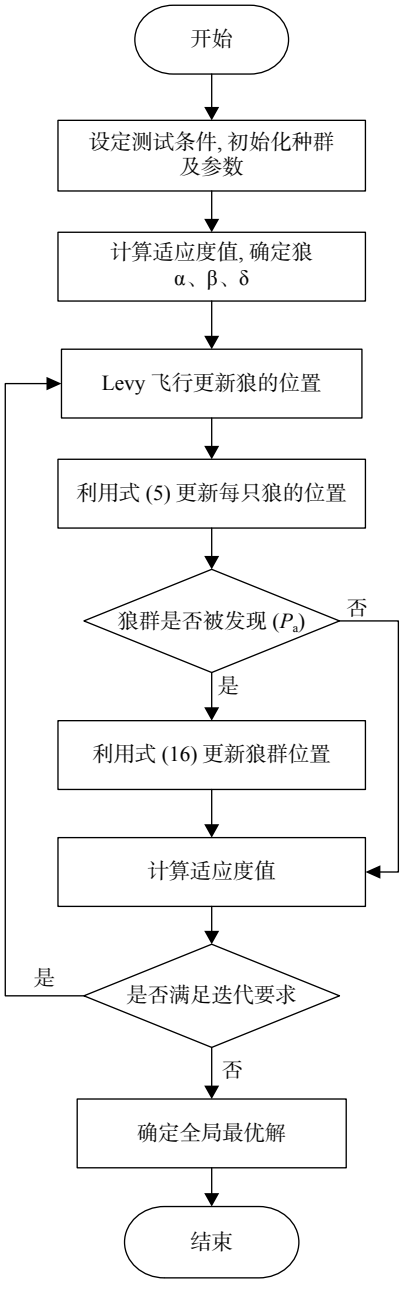

图 1　CS-GWO算法的特征选择流程图

Fig. 1　Feature selection flowchart of CS-GWO

第一步，采用莱维飞行机制对适应度值最好的3只灰狼的位置进行扰动。

第二步，采用GWO算法的更新机制来更新灰狼位置信息，使狼群朝着猎物的方向聚集。

第三步，根据预先设定的概率值Pa对灰狼种群的位置进行随机更新。

通过第一步和第三步分别对适应度值最好的3只灰狼和整个灰狼种群的位置进行扰动，迫使狼群在逼近猎物的过程中能随机地跳出局部最优，增强GWO算法在网络入侵检测特征选择中的全局搜索能力。

对于连续问题转化为特征选择的离散问题，在此采取陈昌帅提出的转换函数[13]，将GWO算法的更新机制转换到二进制中。根据该转换函数，首先对狼群位置的更新如式(18)所示：

$$\boldsymbol{X}(t+1) = round\left(\frac{\boldsymbol{X}_\alpha(t)+\boldsymbol{X}_\beta(t)+\boldsymbol{X}_\delta(t)}{3}\right) \tag{18}$$

其中，$\boldsymbol{X}_\alpha(t)$, $\boldsymbol{X}_\beta(t)$, $\boldsymbol{X}_\delta(t)$的计算如式(19)～(23)所示：

$$\boldsymbol{X}_i(t) = [x_j], i = \alpha、\ \beta、\ \delta, 1 \le j \le d \tag{19}$$

$$x_j = \begin{cases} 0, & \text{if } rand < S(\boldsymbol{X}_i(t)); \\ 1, & \text{if } rand \ge S(\boldsymbol{X}_i(t)) \end{cases} \quad i = \alpha、\ \beta、\ \delta, 1 \le j \le d \tag{20}$$

$$S(\boldsymbol{X}_\alpha(t)) = \frac{1}{1+\exp(|\boldsymbol{X}_\alpha(t)|)} \tag{21}$$

$$S(\boldsymbol{X}_\beta(t)) = \frac{1}{1+\exp(|\boldsymbol{X}_\beta(t)|)} \tag{22}$$

$$S(\boldsymbol{X}_\delta(t)) = \frac{1}{1+\exp(|\boldsymbol{X}_\delta(t)|)} \tag{23}$$

式(19)～(23)可以实现狼群位置在0和1之间的更新转换。进而采用CS算法对最优α、β、δ灰狼的位置进行扰动，按照Rodrigues等提出的二进制变化公式[19]进行变换，如式(24)和(25)所示：

$$S\left(\boldsymbol{X}_i^j(t)\right) = \frac{1}{1+e^{X_i^j(t)}} \tag{24}$$

$$\boldsymbol{X}_i^j(t+1) = \begin{cases} 1, & \text{if } S\left(\boldsymbol{X}_i^j(t)\right) > \sigma; \\ 0, & \text{else} \end{cases} \tag{25}$$

3 验证分析

3.1 实验环境

实验使用网络入侵检测NSL-KDD测试集[20]，相较于原始的KDD Cup 1999数据集，该数据集清除了原数据集中的许多重复记录，改进了原数据集中存在的一些缺陷。数据集中的每一条连接记录都可以归类为 Normal、Probing、DOS、U2R、R2L这5种类别之一。每一个记录都包含有41个特征，以及1个类别标签，其中38个为数值型特征，3个为字符型特征。

采取从KDDTest.arff文件以及KDDTrain+_20Percent.arff文件中随机抽取10%的数据分别作为测试集和训练集。首先，需要对数据集进行预处理，将3个字符型特征映射为数值型特征。由于数据集中的“Service”特征具有几十个不同的取值，根据先验知识该特征会引起较大的误报，因此在实验中不使用这个特征。对于其它的40个特征则全部保留，以减少人工因素对算法结果的干扰。最后，对所有的特征做最小-最大规范化处理将特征值都规范化到[0，1]区间之中。

实验采用Java作为编程语言，Weka工具提供的SMO算法作为分类算法。实验参数设置为：最大迭代次数为50，种群数量为20，实验次数均为50。

3.2 结果分析

为了验证CS-GWO算法的性能，分别与原始算法和传统算法进行对比实验。

3.2.1 原始算法对比实验

将CS-GWO算法分别与GWO算法和CS算法在网络入侵检测NSL-KDD测试集上进行比较实验，通过对迭代过程的分析，以证明CS-GWO算法有较强的跳出局部最优的能力。

图2～4是GWO、CS和CS-GWO算法在迭代过程中适应度值的变化情况，其中包括最好的适应度值和平均适应度值。

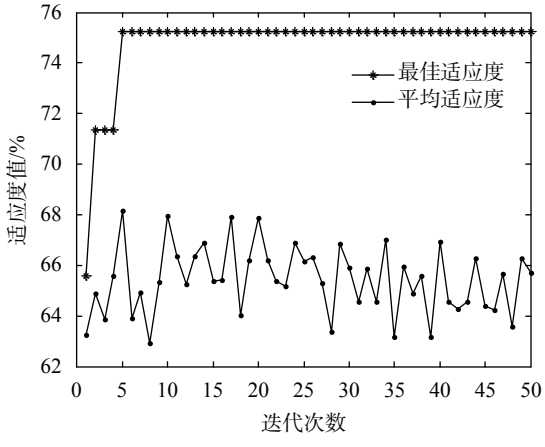

图 2 GWO算法的特征选择图

Fig. 2 Feature selection graph using the GWO algorithm

如图2所示，GWO算法的最佳适应度值在迭代后期没有变化，说明此时狼群可能陷入局部最优，找到的解可能为局部最优解。如图3所示，CS算法有较好的跳出局部最优的能力，即使在迭代的后期也有进化的现象。如图4所示，狼群最优个体在前、中、后期适应度值都有所提高，说明CS-GWO算法的狼群最优个体避免了陷入局部最优的困境，且最佳适应度值比CS算法与GWO算法的最佳适应度值都高。

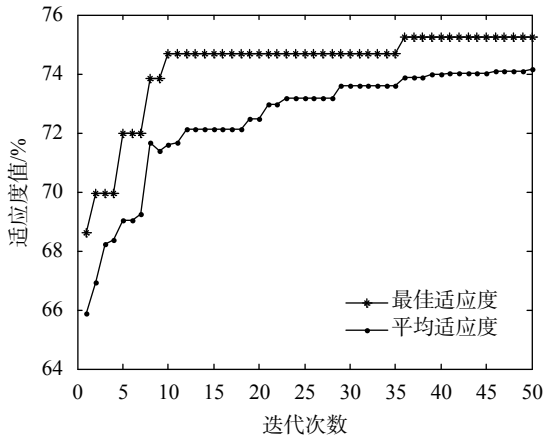

图 3 CS算法的特征选择图

Fig. 3 Feature selection graph using the CS algorithm

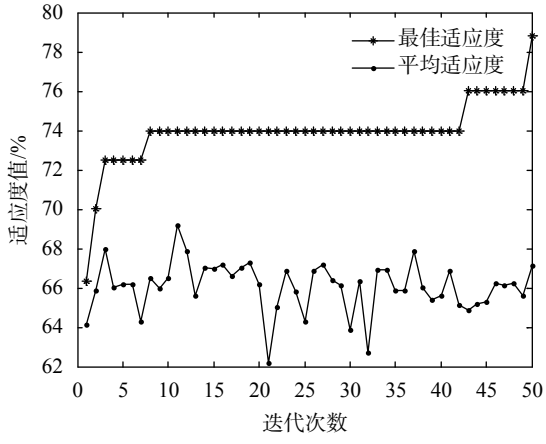

图 4 CS-GWO算法的特征选择图

Fig. 4 Feature selection graph using the CS-GWO algorithm

图5是GWO、CS、CS-GWO算法和未进行特征选择在特征维度和正确率方面的结果对比图。

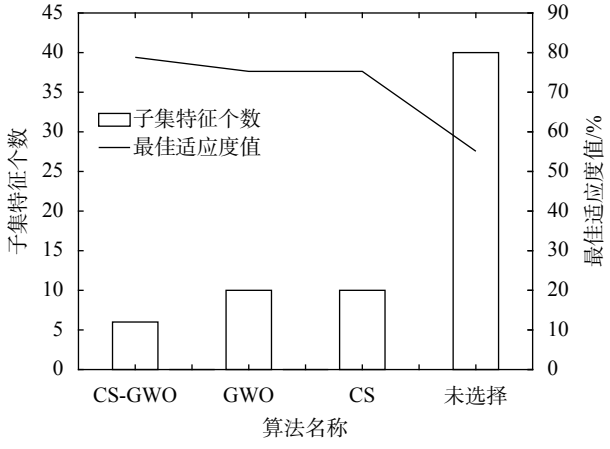

图 5 CS-GWO算法、GWO算法、CS算法和未选择的实验结果对比图

Fig. 5 Comparison of experimental results by the CS-GWO algorithm, the GWO algorithm, the CS algorithm and the unselected case

如图5所示，柱状图表示的是算法选择的特征个数，折线图是所对应的正确率。与未进行特征选择（55.107%）相比，CS-GWO算法（78.811%）、GWO算法（75.261%）和CS算法（75.261%）的最佳适应度值都有所提高，且CS-GWO算法选择的子集特征个数最少，最佳适应度值更高。由此可见，较之GWO算法和CS算法，CS-GWO算法在网络入侵检测特征选择中搜索到的解最优，其全局搜索能力最强。

3.2.2　传统算法对比实验

为了验证CS-GWO算法的有效性，将CS-GWO与传统的IG算法进行比较。表1是IG算法的特征选择结果。

表 1　IG算法的特征选择结果

Tab. 1　Feature selection results by the IG algorithm

名称	名称对应的取值
特征序号	4、5、10、11、29、38
特征名称	src_bytes、dst_bytes、num_failed_logins、logged_in、diff_srv_rate、dst_host_srv_serror_rate
分类正确率/%	80.12
适应度值/%	75.588

表2是IG算法与CS-GWO算法在分类正确率和适应度值的结果对比。

表 2　IG算法与CS-GWO算法的特征选择结果比较

Tab. 2　Comparison of feature selection results by the IG algorithm and the CS-GWO algorithm

名称	正确率/%	适应度值/%	特征数
IG算法	80.12	75.588	6
CS-GWO算法	83.54	78.811	6

如表2所示，传统的IG算法和CS-GWO算法在特征选择数量方面均为6个特征；在分类正确率方面，前者的正确率比后者低3.42%；在适应度值方面，前者比后者低3.223%。由此可见，在应用于网络入侵检测的特征选择时，CS-GWO算法比传统IG算法的性能更好。

4　结　论

为了改善标准的GWO算法在网络入侵检测数据集容易陷入局部最优的不足，将一种CS-GWO算法应用于网络入侵检测的特征选择中。该算法通过CS算法对GWO算法中灰狼位置进行扰动，使狼群能跳出局部最优。最后在NSL-KDD测试集上验证，并与标准的GWO算法和CS算法比较，验证了CS-GWO算法在搜索能力方面有较为显著的提升，在网络入侵检测的特征选择中能取得较好的效果。

由于CS-GWO算法结合了GWO算法和CS算法的特点，CS-GWO算法在应用于网络入侵检测的特征选择时的时间复杂度高于GWO算法和CS算法，这是需要进一步研究和改进之处。

参考文献：

[1] Mi Hong,Yang Xibei.Network anomaly detection model based on intrusion feature selection[J].Modern Electronics Technique,2017,40(12):69–71.[米洪,杨习贝.基于入侵特征选择的网络异常数据检测模型[J].现代电子技术,2017,40(12):69–71.]

[2] Ramakrishnan S,Devaraju S.Attack's feature selection-based network intrusion detection system using fuzzy control language[J].International Journal of Fuzzy Systems,2017,19(2):316–328.

[3] Khammassi C,Krichen S.A GA-LR wrapper approach for feature selection in network intrusion detection[J].Computers & Security,2017,70:255–277.

[4] Liu Bailu,Yang Yahui,Shen Qingni.Method of intrusion early feature selection based on genetic algorithm[J].Journal of Chinese Computer Systems,2015,36(1):111–115.[刘白璐,杨雅辉,沈晴霓.一种基于遗传算法的入侵早期特征选择方法[J].小型微型计算机系统,2015,36(1):111–115.]

[5] Li An,Jiang Jiahe.A feature selection method for intrusion detection using the adaptive genetic algorithm[J].Applied Science and Technology,2016,43(3):49–53.[李安,江加和.基于自适应遗传算法的入侵检测特征选择方法[J].应用科技,2016,43(3):49–53.]

[6] Yuan Kaiyin,Fei Lan.Detection of network intrusion based on hybrid particle swarm optimization algorithm selection features[J].Journal of Jilin University(Science Edition),2016,54(2):309–314.[袁开银,费岚.混合粒子群优化算法选择特征的网络入侵检测[J].吉林大学学报(理学版),2016,54(2):309–314.]

[7] Mirjalili S,Mirjalili S M,Lewis A.Grey wolf optimizer[J].Advances in Engineering Software,2014,69:46–61.

[8] Lv Xinqiao,Liao Tianlong.Permutation flow-shop scheduling based on the grey wolf optimizer[J].Journal of Wuhan University of Technology,2015,37(5):111–116.[吕新桥,廖天龙.基于灰狼优化算法的置换流水线车间调度[J].武汉理工大学学报,2015,37(5):111–116.]

[9] Mao Senmao,Qu Kaiping,Chen Yixuan,et al.Grey wolf multi-objective optimizer for optimal carbon-energy combined-flow[J].The Journal of New Industrialization,2016,6(9):11–17.[毛森茂,瞿凯平,陈艺璇,等.基于灰狼多目标算法的电网碳-能复合流优化调度[J].新型工业化,

2016,6(9):11–17.]

[10] Wang Tai,Xu Bin,Li Linguo,et al.A multi-threshold image segmentation algorithm based on discrete grey wolf optimization[J].Computer Technology & Development,2016,26(7):30–35.[王钛,许斌,李林国,等.基于离散灰狼算法的多级阈值图像分割[J].计算机技术与发展,2016,26(7):30–35.]

[11] Seth J K,Chandra S.Intrusion detection based on key feature selection using binary GWO[C]//Proceeding of International Conference on Computing for Sustainable Global Development.Piscataway,NJ:IEEE Press,2016:3735–3740.

[12] Emary E,Zawbaa H M,Grosan C,et al.Feature subset selection approach by gray-wolf optimization[C]//Proceedings of Afro-European Conference for Industrial Advancement.Switzerland:Springer,Cham:2014:1–13.

[13] 陈昌帅.二进制灰狼优化算法的研究与分析[J].信息系统工程,2016,28(7):136–138.

[14] Yang X S,Deb S.Cuckoo search via Lévy flights[C]//Proceedings of Nature & Biologically Inspired Computing,2009.Piscataway,NJ:IEEE Press,2009:210–214.

[15] Jiang Y,Liu X,Yan G,et al.Modified binary cuckoo search for feature selection:a hybrid filter-wrapper approach[C]//Proceedings of International Conference on Computational Intelligence and Security.Washington DC:IEEE Computer Society,2017:488–491.

[16] Aziz M A E,Hassanien A E.Modified cuckoo search algorithm with rough sets for feature selection[J].Neural Computing & Applications,2018,29(4):925–934.

[17] Raj A M J,Francis F S,Benadit P J,et al.Particle swarm and cuckoo search (PSCS) optimization based feature selection method to improve the web page classification[J].Journal of Advanced Research in Dynamical & Control Systems,2017,9(6):1125–1140.

[18] Xu H,Liu X,Su J.An improved grey wolf optimizer algorithm integrated with cuckoo search[C]//Proceedings of IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems:Technology and Applications.Piscataway,NJ:IEEE,2017:490–493.

[19] Rodrigues D,Pereira L A M,Almeida T N S,et al.BCS:A binary cuckoo search algorithm for feature selection[C]//Proceedings of IEEE International Symposium on Circuits and Systems.Piscataway,NJ:IEEE,2013:465–468.

[20] Canadian Institute for Cyber security.NSL-KDD dataset [EB/OL].(2009-07-08) [2018-07-05].http://www.unb.ca/cic/datasets/nsl.html.

（编辑　张凌之）

引用格式:Xu Hui,Fu Yingchun,Liu Xiang,et al.Applying improved grey wolf optimizer algorithm integrated with cuckoo search to feature selection for network intrusion detection[J].Advanced Engineering Sciences,2018,50(5):160–166.[徐慧,付迎春,刘翔,等.融合杜鹃搜索的灰狼优化算法在网络入侵检测特征选择中的应用[J].工程科学与技术,2018,50(5):160–166.]