# 改进的免疫克隆算法在入侵检测中的应用

牛永洁,薛宁静
(延安大学 数学与计算机学院,陕西 延安 716000)

**摘 要**:为了提高入侵检测系统的正确率,降低误检率,对基本的免疫克隆选择算法采用抗体的克隆数目与亲和度成正比且克隆数目线性递减、变异概率线性递减、新的替换策略、变异概率和抗体克隆数量突变进行改进。对抗体克隆策略的改进保证了算法的收敛速度,避免了算法后期的震荡,变异概率的自适应变化加强了算法后期的收敛,新的替换策略、变异概率和抗体克隆数量突变能够有效地避免算法陷入局部最优。经过 KDD Cup 1999 数据集的训练和检验数据的仿真测试,改进后的算法具有较高的检测正确率和较低的误检率,而且新算法收敛速度快,不易“早熟”。

**关键词**:入侵检测;克隆选择;变异概率;克隆策略;自适应
**中图分类号**:TP301.6 **文献标识码**:A **文章编号**:1673-629X(2016)05-0086-05
doi:10.3969/j.issn.1673-629X.2016.05.018

# Application of Improved Immune Clonal Selection Algorithm in Intrusion Detection

NIU Yong-jie, XUE Ning-jing
(College of Mathematics & Computer Science, Yan'an University, Yan'an 716000, China)

**Abstract**: In order to improve the correct rate of intrusion detection system and reduce false positive rate, on the basic immune clonal selection algorithm using antibody clone number and affinity is proportional to the degree and the number of clones linear decreasing, mutation probability decreasing linearly, new replacement strategy, the number of mutation probability and antibody clonal mutation for improvement. The improvement of antibody cloning strategy to ensure the convergence speed of the algorithm and avoid the shock of the late. Adaptive changes in the mutation probability strengthen the convergence of the algorithm for the late. New replacement strategy and the number of mutation probability and antibody clonal mutations can effectively avoid the algorithm into a local optimum. After the training and testing for Cup KDD 1999 data set, the improved algorithm has the advantages of higher detection accuracy rate and lower false detection rate, with fast convergence speed, and it is not easy to "premature".

**Key words**: intrusion detection; clonal selection; mutation probability; cloning strategy; adaptive

## 1 概 述

目前,计算机网络已经渗透到人们工作生活的各个方面,特别是最近电子商务的兴起和普及,越来越多的敏感信息在网络中传输,为了保证这些信息的安全性,网络安全问题越来越受到人们的关注。随着网络技术的发展,新型的网络攻击方法层出不穷,让现有的防御技术防不胜防,因此用户的计算机系统可能随时都有被新型的攻击方法攻击的危险。

入侵检测系统(Intrusion Detection System,IDS)是一种能够主动发现并进行防御的系统,它能发现新型、现有未知的攻击方法。相对于其他安全措施而言,入侵检测系统不仅在防御性上具有主动性的优点,而且还具有能够识别新型的、未知的攻击方法的特性。一般的入侵检测系统能够同时防御系统内外两个方面的攻击,其运行的基本原理是首先在计算机系统或者外部网络的关键点位置放置探测装置收集相关的信息,然后对收集的信息使用相关技术进行分析,从而得出系统是否遭到攻击的判断。一旦发现受到攻击,系统将会根据受攻击的类别或者严重程度依据事先制定好的规则做出不同的反应,如:报警、拦截运行或者直接删除、丢弃相应的数据。因此得出结论:入侵检测系统的整个关键步骤是对收集的相关信息进行信息解析、

**收稿日期**:2015-06-19 **修回日期**:2015-09-24 **网络出版时间**:2016-05-05
**基金项目**:陕西省自然科学研究项目(14JK1828)
**作者简介**:牛永洁(1977-),男,硕士,讲师,CCF 会员,研究方向为数据挖掘、智能算法、网络安全。
**网络出版地址**:http://www.cnki.net/kcms/detail/61.1450.TP.20160505.0815.036.html

分析处理,然后得出这些行为是否异常[1-3]。

对流经计算机系统的数据包进行抓取和数据处理,然后使用适当的数据分析算法,判断出数据包属于正常或者非正常数据,针对非正常的数据采取报警或者其他的措施对用户进行警告或者提示。所以对数据包进行分析,用来分辨数据是否正常的算法是入侵检测系统的核心。

在对人体免疫系统运行机理进行深入研究的基础上,按照仿生学的原理,研究人员提出了人工免疫系统算法。目前已经发展成多种不同的算法,比较典型的有克隆选择算法、B 细胞网络算法、阴性选择算法和免疫遗传算法。其中应用最为广泛和经典的算法是免疫克隆选择算法,该算法由 De Castro 等根据生物免疫系统理论中的克隆选择学说而提出[4-5]。这种算法被人们称为 CLONALG 算法。CLONALG 算法在应用过程中逐渐暴露出很多的缺点和弊端,比如收敛速度慢、搜索能力差而且容易陷入局部最优,也就是通常所说的“早熟”现象。

虽然 CLONALG 有上述的一些缺点,但是本身也有很多其他算法不具有的独特优势,比如算法本身具有并行性、自适应性,能够主动学习、识别和记忆,所以该算法被迅速地应用到很多领域。这些领域主要包括复杂函数的优化[6-7]、多维数据的特征选择[8-9]、网络安全监测[10]、图像的分割[11-12]和机器学习[13]等。

文中将免疫克隆算法应用到入侵检测系统中。为了避免 CLONALG 算法的缺点进而获得较高的正确率和较低的误检率,详细研究了 CLONALG 算法的运行过程并对造成其缺陷的原因进行了深入分析,对算法进行了四个方面的优化和改进。改进后的算法不仅收敛速度快、全局搜索能力强,而且不易陷入局部最优点,即使算法陷入到局部最优点,算法仍有较大的几率跳出并继续进行全局搜索,在算法运行后期,能够迅速收敛到最优值,不会造成算法后期运行的震荡。最后通过在模拟数据下的仿真实验,发现算法运行高效、快捷,效果良好。

## 2　入侵检测

入侵是指除了正常使用计算机资源的各种活动的集合,这些活动往往企图对计算机资源在完整性、机密性和可用性等方面进行破坏。入侵检测系统的任务就是从各种使用计算机的活动中识别出入侵的活动。为了进行识别,系统必须对通信数据或用户的行为进行实时监视并检测这些数据,以此来判断是否有入侵行为的发生。

入侵检测技术按照检测方法可以分为两种基本的方法,分别是误用检测(misuse detection)和异常检测(anomaly detection)。

误用检测是指识别入侵者使用现有已经知道的攻击方法或者利用系统安全漏洞采用合法的命令进行攻击的检测过程。异常检测主要检测的攻击方式是利用系统正常运行的日志记录或者利用网络交互数据中具有识别性的数据来假冒系统正常运行这两种方式。IDS 根据对数据的侦听策略不同又可以分为基于网络的入侵检测系统和基于主机的入侵检测系统。网络入侵检测系统是在网络上利用网络侦听技术抓取数据包,然后对收集的数据包进行信息解析,从里面分析行为是否异常。而基于主机的 IDS 的数据来源主要是主机系统和系统本地用户的审计数据和系统的日志。

文中研究的入侵检测系统的数据来源于网络中的数据包[11],所以是一种基于网络的 IDS。系统的运行原理机制如图 1 所示。

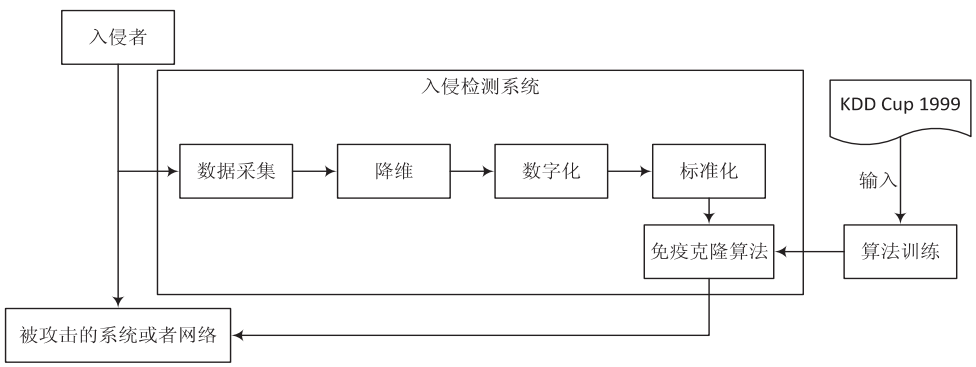


图 1　入侵检测系统的运行机制

为了进行入侵检测,首先应该得到需要分析的数据,即数据采集。对网络数据的采集使用一种叫嗅探器的工具。嗅探器有硬件和软件两种实现方式。硬件网络嗅探器灵活性比较差,但是其性能高而且价格比较昂贵。软件网络嗅探器具有实现方便、布置灵活和成本低的优势。不同的软件版本需要不同的平台支持,比较常见的嗅探器有:Linux 系统下的 Tcpdump,HP-UX 系统平台下的 NfSwatch 和 Windows 系统平台下的 lpman、FoxSniffe、Wireshark、WinPcap 等。SharpPcap 是一个基于著名的 WinPcap 库,在. NET 环境下

开发而成的网络包捕获应用程序包。该开发包提供了网络包的捕获、数据注入、数据包解析和生成的功能，适用于. NET 开发平台。文中对数据包的抓取基于 SharpPcap 库进行。

对抓取的数据包进行数据预处理的过程主要包含 3 个步骤，它们分别是降维、数字化、标准化。由于抓取的数据包一般维数比较大，为了减少后续算法的运算量，同时还不能影响算法的准确度，文中采用主成分分析(Principal Component Analysis，PCA)方法对网络数据包进行降维处理。在获得的网络数据包中，每一条记录中，对有些属性的描述往往会采用字符串进行，这些字符串对后面要进行的数据分析和处理不利，因此首先需要对这些属性进行数字化处理，如为了表示目标主机的网络服务类型，会对记录的网络服务类型标记为 HTTP、SMTP、SQL_NET、POP_3 等。为了后续更好地进行数据处理和分析，需要对文本字符进行转换，使之成为数值型数据。最后还需要考虑每条记录中不同属性采用的量纲不同，数值大小的不同会严重影响数据处理过程中属性权重的大小，所以需要消除不同属性量纲的不同，因此还需要对转换以后的数据进行标准化处理。处理过程使用式(1)、(2)进行。

$$\bar{x}_j = \frac{1}{n}\sum_{i=1}^{n} x_{ij}, S_j = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{ij} - \bar{x}_j)^2} \quad (1)$$

$$x'_{ij} = \frac{x_{ij} - \bar{x}_j}{S_j} \quad (2)$$

式中：$x_{ij}$ 表示第 $i$ 行、第 $j$ 列的一个标量数据；$\bar{x}_j$ 表示第 $j$ 列的算术平均值；$S_j$ 表示第 $j$ 列的标准方差；$x'_{ij}$ 表示数据标准化处理后的新数据。

经过标准化处理消除了不同属性之间量纲对数据分析的影响。

## 3 免疫克隆算法的改进

### 3.1 基本免疫克隆算法

对人工免疫系统(Artificial Immune System，AIS)的研究，起步相对较晚，但近年来发展迅速。人工免疫算法将抗原视为问题域中需要进行优化的问题的目标函数，而抗体恰好是该目标函数对应的可行解。不同的抗体对抗原的亲和力不同，而问题域中，可行解对目标函数的匹配程度恰好可以使用这种亲和力来表示：抗体对抗原亲和力的不同能够保证问题域中可行解的多样性，计算不同抗体的期望生存率，使用期望生存率高的抗体进行下一代抗体的遗传，为了防止可行解陷入局部最优，遗传下来的抗体必须保持一定的变异率，用来继续保证抗体对抗原亲和力的多样性，但是变异概率不应过大，不然算法很容易陷入震荡而造成算法最后的不收敛。同时使用记忆细胞记录这些优秀的可行解，记忆细胞中的数据可以用来防止后续可行解产生过程中相似可行解的继续出现，进而可以使算法快速地搜索到全局最优解，保证了算法的收敛速度。当算法再次遇到相似问题时，可以从记忆细胞中快速地产生与抗原亲和力很高的抗体，能快速地产生问题的较优解甚至最优解，这就是算法的免疫性。

比较经典的人工免疫算法—克隆选择算法主要步骤为：算法起始阶段、优良抗体的选择、抗体的复制克隆、变异、种群抗体替换等。在算法的起始化步骤中，采用随机化的方法随机产生 $N$ 个抗体，这些抗体对应于问题域中的 $N$ 个可能解，随机产生的抗体群又被分为功能不同的两个子群体，其中一个子群体作为记忆细胞 $M$，而剩下的群体被称为剩余种群 $R$。然后计算每个抗体与抗原的亲和度，这个亲和度用来作为每个抗体优劣性的衡量指标，亲和度高的抗体表示是抗原表示问题的优秀解，即亲和度高的抗体更可能是问题域的可能解，从抗体群中筛选出 $n$ 个结合度较高的抗体，下一步对这 $n$ 个抗体进行复制即为克隆。为了预防算法的局部最优，需要对复制后的抗体进行高概率的随机变异。在变异后的群体中随机选择其中的 $C$ 个抗体，然后重新随机生成 $C$ 个抗体，用新生成的 $C$ 个抗体替换掉变异后群体中被选中的 $C$ 个抗体，然后算法再次进入起始化阶段，计算抗体对抗原的亲和度，选择，复制克隆，等等。算法进入迭代循环，直到算法找到最优解或者循环达到一定要求为止。

经典的克隆选择算法的运行步骤如下：

(1)候选抗体集合 $H$ 的生成。根据问题的定义域要求，使用随机化的方法，得到一个含有 $N$ 个抗体的种群集合 $H$。其中 $N$ 即为候选抗体种群的大小，即在定义域中得到 $N$ 个可行解的点。

(2)计算抗体集合 $H$ 中每个抗体对抗原的亲和度，即计算每个可行解在适应度函数中的值，根据值的大小从抗体集合 $H$ 中选择 $n$ 个最优的抗体，选中的抗体称为集合 $R_n$，其中选择的 $n$ 与抗体规模满足 $n \leqslant N$ 的要求。

(3)克隆复制操作。将集合 $R_n$ 中的每个抗体重复克隆复制 $k$ 个，$n$ 个抗体复制的个数为 $n*k$，$n*k$ 个抗体组成了临时的克隆集合 $C$。

(4)对克隆集合 $C$ 以一定的概率 $m$ 进行高频变异，变异后抗体群构成了一个新的集合 $C_n$。

(5)对集合 $C_n$ 中变异后的每个抗体再次计算适应度函数值，选择与集合 $R_n$ 相同个数的最优抗体，选中的变异后的这些抗体就构成了另一个集合，这个集合被称为记忆细胞集合 $M$，然后将集合 $M$ 的抗体替换掉集合 $R_n$ 中的抗体。

(6)从集合 $H$ 中选择 $d$ 个低亲和度的抗体，将这

些抗体丢弃,然后使用完全随机化的方法重新生成 $d$ 个新的抗体,将这些新抗体加入集合 $H$ 中,同时将原先选中的 $d$ 个低亲和度的抗体丢掉。

### 3.2　新的免疫克隆算法

新的免疫克隆算法对经典的算法进行了四个方面的优化和改进[13]。

(1)采用新的抗体克隆方法[14]。

新的抗体克隆方法分两个阶段进行。经典的免疫克隆算法对集合 $R_n$ 中的每个抗体采用相同的克隆办法,即每个抗体都复制 $c$ 个,新的方法为了让优秀的抗体更多地带到下一代,采用根据抗体自身的亲和度大小进行正比例的复制,亲和度越大复制的数量越多,而亲和度低的抗体复制的数目要少。对任意一个抗体 $t$ 的克隆数量的计算使用式(3)。

$$C_t = \alpha \times \frac{f_t}{f_{\max}} \times N \tag{3}$$

式中:$C_t$ 为第 $t$ 个抗体需要克隆复制的个数;$f_t$ 为该抗体的亲和度;$f_{\max}$ 为所有种群的最大亲和度;$N$ 为种群数量的大小;$\alpha$ 为对克隆进行调节的参数。

随着算法的迭代进行,一方面保持按照亲和度正比例克隆的方法,同时根据迭代次数递减抗体的克隆数目,即在上一代中抗体 $t$ 的亲和度为 $q$,复制的数量为 $p'$,但是在下一代的克隆过程中,有一个抗体的亲和度也为 $q$,但是其复制的数量为 $p''$,其中 $p''$ 和 $p'$ 满足 $p'' < p'$ 的关系。

新的抗体克隆方法总体上能够保证算法是收敛的,而且能够保证算法的收敛速度。在算法的运行后期,由于采用复制克隆数量递减的策略,避免了算法在收敛到全局最优点时的震荡现象。对式(3)进行调整,用来递减克隆抗体,调整以后为:

$$C_t = \left(\alpha \times \frac{f_t}{f_{\max}} + \beta \times \mathrm{Iter} + \lambda\right) \times N \tag{4}$$

式中:Iter 为算法的迭代次数;$\beta$ 为一个负值的调节参数;$\lambda$ 为复制克隆阶段第一次迭代时的复制克隆数值。

因此新算法在进行抗体克隆时,一方面要保持抗体克隆数量与自己亲和度的正比例关系,而且随着算法的迭代,使得每个抗体的克隆数量呈线性递减趋势。

(2)变异概率的自适应[15]。

克隆复制后的集合 $R_n$ 为了保持种群的多样性,对集合中的抗体进行高频变异操作。经典的算法其变异的概率始终保持不变,新的算法采用在算法的初期采用比较高的变异概率,用来保持种群的多样性,对问题的空间进行充分搜索,但是在算法运行后期,算法已经进入收敛阶段,如果仍然采用高的变异概率,这些新的种群往往会造成算法的震荡,使算法在长时间内得不到收敛。因此在新算法中采用变异概率的自适应变化,即随着算法的迭代运行,变异概率随着迭代次数线性递减。新算法的变异概率为:

$$m^{k+1} = \rho \times m^k \tag{5}$$

式中:$m^k$ 为算法第 $k$ 次运行时采用的变异概率;$m^{k+1}$ 为第 $k+1$ 次循环步骤使用的变异概率;参数 $\rho$ 满足 $0<\rho<1$。

(3)抗体更新的新限制[16]。

经典的克隆选择算法采用算法初始化时的方法随机产生 $d$ 个新的抗体,新产生的抗体直接替换掉集合 $H$ 中的 $d$ 个低亲和度的抗体,没有对新产生的 $d$ 个抗体做任何限制。而新算法为了使算法在运行上向收敛的方向进行,对 $d$ 个新产生的抗体提出了新的要求,即重新随机生成 $d$ 个新的抗体以后,计算每个抗体的亲和度,求这些新抗体亲和度的平均值,要求新抗体的平均亲和度要大于等于目前种群的平均亲和度,否则,重新随机生成 $d$ 个新的抗体。如果连续生成的 $d$ 个抗体平均亲和度都不符合要求的次数超过某个次数,采用基本的算法方式进行,这样保证算法能够向收敛的方向更快地进行。

(4)突变机制的引入[17-18]。

为了防止算法在运行过程中出现“早熟”现象,受到遗传算法中的小生境的启发,文中引入早熟检测指数 $D_p$。当早熟指数小于等于某一个数值 $\xi$ 时,使用将变异概率突然放大为原先概率 $k$ 倍的方法,同时将抗体的替换方法转变为完全初始化的方式进行,即取消替换抗体集合的平均亲和度必须大于等于种群平均亲和度的要求。这个策略是在算法陷入早熟的情况下,引入新的群体来增加算法跳出局部最优的一个常识,由于变异概率的突然增大和替换总群的完全初始化,引入的新群体将有机会带领算法向全局最优收敛。而当早熟检测指数 $D_p$ 重新大于 $\xi$ 时,抗体的变异规律和替换策略继续方法(2)和(3)进行。文中 $\xi$ 取值为 1.2。早熟检测指数采用式(6)计算。

$$D_p = \frac{f_{\max} - f_{\min}}{f_{\mathrm{ave}}} \tag{6}$$

式中:$f_{\max}$ 为本次迭代中抗体种群亲和度的最大值;$f_{\min}$ 为亲和度的最小值;$f_{\mathrm{ave}}$ 为本次迭代中抗体种群亲和度的平均适应度。

## 4　仿真实验

采用 KDD Cup 1999 网络数据集对新算法的效果进行了仿真实验。该数据集是第三届数据挖掘大会采用的官方测试入侵检测的数据集,具有很高的通用性,实验结果也具有很强的对比性,同时也有很高的问题说服力。数据集来源于美国麻省理工学院,是在对美

国军方的网络环境模拟的情况下进行了各种网络攻击实验,同时抓取了网络流量数据包,进行整理而得到。

整个数据集被分成两个部分,一部分是包含由 500 万条记录组成的训练集,另一部分是由 300 万条记录组成的测试集。数据集中的每条记录中由 34 个数值型字段和 7 个非数值型字段组成,这些记录被分为五类,分别为正常、Probing 攻击、DoS 攻击、R2L 攻击和 U2R。此次仿真实验从训练集中随机抽取了 4 500 条正常的记录,同时等比例抽取了攻击数据记录共 2 000条,将这两个集合合在一起作为整体训练集。

算法运行过程中,相关的参数设置如下:

种群的规模个数为 150,从抗体群中筛选出的结合度较高的抗体数量为种群规模的 1/3,克隆调节参数 $\alpha$ 取值为 0.9,克隆数量递减的负值调节参数取值 -0.001,复制克隆阶段第一次迭代时的复制克隆数为 3,变异概率的线性递减系数 $\rho$ 取 0.75,算法初始的变异概率设置成 1% 的概率。在抗体替换的步骤中,每次替换掉选中种群整体的 1/5;在变异概率突变的步骤中,概率突变放大的倍数采用 1.4 倍。

为了进行对比,经典算法和改进算法分别独立运行 20 次,每次运行算法的循环次数规定为 150 代。最后,对每种算法运行的结果求平均值作为其算法的最终结果。

表 1 列出了经典算法和改进算法在入侵检测系统中应用后的检测正确率和误报率结果。

表 1 经典算法与改进免疫克隆算法的对比结果

| 攻击类型 | 经典算法 | | | 改进后的算法 | | |
|---|---|---|---|---|---|---|
| | 检测率/% | 误检率/% | 运行时间/s | 检测率/% | 误检率/% | 运行时间/s |
| DoS | 91.47 | 2.64 | 8.53 | 99.22 | 0.26 | 7.21 |
| Probing | 92.35 | 2.71 | 7.79 | 98.46 | 1.07 | 6.37 |
| R2L | 89.63 | 3.03 | 9.75 | 98.66 | 1.67 | 8.78 |
| U2R | 90.16 | 2.47 | 8.35 | 98.83 | 1.26 | 7.15 |

## 5 结束语

通过新的抗体克隆、变异概率的自适应、抗体更新的新限制和突变机制的引入,得到一种改进的新算法,并将新算法应用到了入侵检测系统的数据分析过程中。新算法通过采用抗体的克隆数目与亲和度成正比及克隆数目逐渐递减的策略,能够更有效地保留优良抗体,加速算法的收敛速度,克隆数目的递减能够有效地减少算法计算工作量;变异概率的自适应递减策略能够保证算法在运行初期有充分的搜索算法空间,而且由于克隆数目与亲和度的正比关系,能够保证优良抗体的充分保留;替换策略的改进保证了算法在运行期间既能引入新的抗体,又避免了算法运行后期的震荡;变异概率和克隆数量的突变能够有效防止算法的“早熟”现象。最后,通过 KDD Cup 1999 数据集对算法进行了仿真实验。结果表明,改进后的新算法能够有效地提高入侵检测的正确率、降低错误率且具有收敛速度快和不易“早熟”的优势。

**参考文献:**


[1] 牛永洁,赵耀锋. 改进的 LF 算法在入侵检测中的应用[J]. 计算机与现代化,2013(6):57-59.

[2] 肖 敏,柴 蓉,杨富平,等. 基于可拓集的入侵检测模型[J]. 重庆邮电大学学报:自然科学版,2010,22(3):345-349.

[3] 吴思远,刘孙俊,王电钢. 一种基于免疫的入侵检测动态响应模型[J]. 重庆邮电大学学报:自然科学版,2007,19(5):635-638.

[4] de Castro L N, Tmanis J. Artificial immune systems: a new computational intelligence approach [M]. British: Springer Press,2002.

[5] 罗印升,李人厚,张 雷,等. 人工免疫算法在函数优化中的应用[J]. 西安交通大学学报,2003,37(8):840-843.

[6] 陈 曦,贺建军,万 力,等. 基于改进克隆选择算法的函数优化问题[J]. 湖南理工学院学报:自然科学版,2012,25(1):34-37.

[7] 张向荣,焦李成. 基于免疫克隆选择算法的特征选择[J]. 复旦学报:自然科学版,2004,43(5):926-929.

[8] 王 俊,田玉玲. 用于入侵检测的动态克隆选择算法的研究[J]. 计算机与数字工程,2010,38(6):108-110.

[9] 刘 倩,仇 宾. 基于克隆选择算法的花卉图像分割[J]. 计算机工程与应用,2012,48(14):185-189.

[10] 丛 琳,沙宇恒,焦李成. 基于免疫克隆选择算法的图像分割[J]. 电子与信息学报,2006,28(7):1169-1173.

[11] 徐 佳,张 卫. 人工免疫系统中的抗体生成与匹配算法[J]. 计算机工程,2010,36(9):181-183.

[12] 牛永洁,陈 莉. 基于混合神经网络的入侵检测技术[J]. 微计算机信息,2006,22(12-3):92-95.

[13] 牛永洁,马亚玲. 一种改进的免疫克隆选择算法[J]. 电子设计工程,2014,22(4):23-25.

[14] 刘 琼,吴小俊. 一种改进的免疫克隆选择算法[J]. 山东大学学报:工学版,2009,39(6):8-12.

[15] 高新龙. 免疫入侵检测邻域空间检测算法研究[D]. 哈尔滨:哈尔滨理工大学,2015.

[16] 方贤进,李龙澍,钱 海. 基于人工免疫的网络入侵检测中疫苗算子的作用研究[J]. 计算机科学,2010,37(1):239-242.

[17] 冯 翔,马美怡,赵天玲,等. 基于复合免疫算法的入侵检测系统[J]. 计算机科学,2014,41(12):43-47.

[18] 伍海波,高劲松,唐启涛,等. 基于生物免疫原理的网络入侵检测研究[J]. 计算机技术与发展,2013,23(7):167-170.