文章编号：1001－9081(2009)08－2227－03

基于遗传优化与模糊规则挖掘的异常入侵检测

徐东升[1]，艾晓燕[1]，阎世梁[2]
(1.榆林学院 信息技术系，陕西 榆林 719000；2.西南科技大学 工程技术中心，四川 绵阳 621010)
(yl_xuds@163.com)

摘 要：提出一种基于智能体进化计算框架与遗传模糊规则挖掘的异常入侵检测方法。通过应用模糊集分布策略、解释性的控制策略和模糊规则生成策略，实现了 Agent之间的模糊集信息交换，从而有效地从网络数据中抽取正确的、可解释的模糊 IF-THEN分类规则，优化了模糊系统的可解释性，并提高了系统的紧凑性。采用 KDD-Cup99数据集进行测试，并与现有方法进行了比较，结果表明该方法对 R2L的攻击检测性能稍弱，对 DoS、Probe和 U2R的攻击均具有较高的分类精度与较低的误报率。

关键词：遗传模糊系统；多目标优化；遗传算法；规则提取；入侵检测
中图分类号：TP393.08　　文献标志码：A

Anomaly intrusion detection based on genetic optimization and fuzzy rules mining

XU Dong-sheng[1]，AI Xiao-yan[1]，YAN Shi-liang[2]
(1. Department of Information Technology，Yulin University，Yulin Shaanxi 719000，China；
2. Engineering and Technology Center，Southwest University of Science and Technology，Mianyang Sichuan 621010，China)

Abstract：A genetic-fuzzy rule mining approach applied to anomaly intrusion detection was proposed，with an Agent-based evolutionary computing framework. Due to the exchanging of fuzzy sets information among the fuzzy sets Agents，accurate and interpretable fuzzy IF-THEN rules could be extracted from network traffic data for optimizing the interpretability and improving the compactivity of the fuzzy system，s by using three strategies including fuzzy sets distribution，interpretable regulation and fuzzy rules generation. All the training and testing datasets were based on the KDD CUP99 intrusion detection benchmark data set. Compared with the current methods，the experimental results show that the proposed approach can provide higher detection accuracy and lower false alarm rate for DoS，Probe and U2R attacks with a slightly poorer performance for R2L attacks.

Key words：genetic-fuzzy system；multi-objective optimization；genetic algorithm；rule extraction；intrusion detection

0 引言

随着互联网规模的不断扩大与用户数量的日益激增，使得计算机网络的安全性变得尤为重要。为解决网络安全问题，各种安全机制、策略和工具被广泛研究和应用。入侵检测系统（Intrusion Detection System，IDS）作为一种有效的网络安全策略，通过分析被保护的计算机系统，发现网络中已知的或潜在的入侵威胁。近年来，基于统计模式识别方法的入侵检测引起广泛了关注与研究。

入侵检测方法分为误用检测方法与异常检测方法。误用检测方法利用已知的入侵方法结合系统弱点进行编码，通过与审计数据的匹配来检测入侵行为，一般情况下不能检测出新型或未知的攻击。异常入侵检测方法使用概率分析方法描述行为特征，将当前行为特征与特征数据库中的特征进行偏差比对，以识别非正常或潜在的入侵行为，且能够发现一些新的未知的入侵行为；然而，相对误用检测方法，它通常会具有较高的误报率。近年来，一些学者提出了基于数据挖掘[1]遗传算法[2]和强化规则学习[3]等智能方法用于异常入侵检测。

文献[4]提出使用关联规则来捕获程序执行与用户行为之间的关系，使用频繁情节算法对系统审计序列模式进行建模，在进行异常和正常划分时需要将入侵数据分割为若干离散区间，因此，易导致所谓的“尖锐边界问题”，文献[5]提出了一种结合模糊集合的模糊数据挖掘技术来解决该问题，并取得了一定的效果。文献[6]使用模糊关联规则先对每一个分类生成大量的模糊规则，再使用 Boosting遗传算法对各个分类实现模糊规则的搜索，该方法仅对分类的精确性进行了优化，而忽略了对解释性优化的必要性。

通常，在精确性与可解释性之间总存在一个折中，具有良好精度的模糊规则并不意味着具有良好的可解释性[7]。因此，在综合考虑系统精确性与解释性的基础上。本文提出一种多目标遗传模糊规则挖掘方法，将基于智能体的进化计算框架用于生成精确的与可解释的模糊知识库，并提取模糊 IF-THEN规则。同时，由于特征子集的优化能够提高分类器的可解释性，因此，该方法进一步也可从网络流量数据中搜索近优特征子集，从而减少分类的计算量。

1 基于规则的遗传模糊系统

基于规则的模糊系统（Fuzzy Rule-Based System，FRBS）源于模糊集合论，通过建立模糊 IF-THEN规则，成功地解决了许多复杂的非线性问题。基于规则的遗传模糊系统（Genetic Fuzzy Rule-Based System，GFRBS）使用进化方法从训练数据中学习和提取知识，其优化准则包括语言变量、模糊

收稿日期：2009－02－14；修回日期：2009－04－17。　基金项目：陕西省榆林市科技计划项目（shf200820）。
作者简介：徐东升（1970－），男，陕西清涧人，副教授，硕士，主要研究方向：人工智能、网络安全；　艾晓燕（1967－），女，陕西西安人，讲师，硕士，主要研究方向：人工智能、模糊系统；　阎世梁（1980－），男，四川绵阳人，讲师，硕士，主要研究方向：智能计算。

隶属度函数参数以及模糊规则及其数量。

1.1 模糊集划分的完备清晰性

对于一个模糊变量，模糊集划分应具有完备清晰性，若特征向量 $X=[x_1, x_2, \cdots, x_n]^T$中的每一个输入变量 x_i存在 M_i个模糊集，即 $A_1(x_i), A_1(x_i), \cdots, A_{M_i}(x_i)$，若满足式(1)，并且对于每一个有效的输入变量组合，至少有一个模糊集被触发，则模糊集的划分是完备的：

$$\forall x_i \in U_i,\ i \in [0, \cdots, n];\quad \exists A_j(x_i) > 0,\ j \in [1, \cdots, M_i] \tag{1}$$

这里 U_i是 x_i的全体，其完备清晰性通过模糊相似性测度进行解释，模糊集 A B之间的相似性可通过式(2)来计算[8]：

$$S(A,B)=\frac{\sum_{j=1}^{m}[\mu_A(x_j)\wedge \mu_B(x_j)]}{\sum_{j=1}^{m}[\mu_A(x_j)\vee \mu_B(x_j)]} \tag{2}$$

其中 $\wedge$ 和 $\vee$ 分别表示最小最大算子，$S(A,B)$为定义在[0,1]的相似性测度，如果 S大于给定的门限值，那么集合 A B将不具备良好的可辨识性。

1.2 模糊规则的一致性与紧凑性

模糊规则的一致性是指，若两个或两个以上的模糊规则具有相似前提，那么它们的结论也应当是相似的[9]。具有紧凑性的模糊系统能够使其更易于被理解，它与以下三个方面有关：

1)模糊变量具有的模糊集合数；

2)规则库中具有的模糊规则数；

3)在规则前件中具有的条件数。

当系统具有较高维数时，模糊规则的紧凑性将变得尤为重要。因此，提高系统的紧凑性对于改善模糊系统的可解释性以及降低模糊推理过程中的计算开销是有益的。同时应注意到，即使模糊系统具有完备清晰性，但也可能存在模糊集合没有任何一条规则的使用情况，因此，从规则库中去除未被使用的模糊集也是必要的。

2 基于智能体的知识提取

本文提出了使用智能体的进化计算框架来构建 GFRBS，该方法可看作是一个多智能体学习系统，由模糊集 Agent与决策 Agent构成。其中，每一个自治模糊集 Agent使用 3层策略来建立模糊系统：首先，通过模糊集分布策略来初始化模糊集信息；然后，使用解释性的控制策略和模糊规则生成策略来产生可解释的模糊规则，父代模糊集 Agent通过对递阶结构的染色体进行交叉、变异操作来实现模糊集信息的交换，从而得到其子代；最后，模糊集 Agent将各自的模糊集的多目标信息(即精确性与可解释性的适应值)传递给决策 Agent，并采用 NSGA-II[10]对父代和子代的模糊集 Agent进行评价，从而选择出最优模糊集 Agent个体。

2.1 模糊集分布策略

这里，我们采用了递阶遗传算法(Hierarchical Genetic Algorithm, HGA)，主要是考虑到该方法可以有效减少模糊集合数量与模糊规则数。其染色体的递阶结构由控制基因和参数基因构成，参数基因处于最低级，控制基因处于上级，下级基因受上级基因的控制[11]。由于染色体的基因型结构在 HGA中并不是固定的，对染色体的操作不仅可改变本级基因结构，而且将引起下一级基因结构的改变，因此在训练过程中模糊系统的参数和模糊系统规则数目可同时得到优化，并能够用于模糊集分布的优化过程。

2.2 模糊规则的解释性控制策略

式(2)中，通常门限值的取值范围为[0.4,0.7]，这里将门限值设定为 0.55。假设 A和 B分别具有隶属度函数 $\mu_A(x; a_1, a_2, a_3, a_4)$和 $\mu_B(x; b_1, b_2, b_3, b_4)$，其中 a_1, a_2, a_3, a_4分别表示双边高斯隶属度函数控制参数的下界、左中心、右中心和上界，且满足 $a_1 \leqslant a_2 \leqslant a_3 \leqslant a_4$。同样，对于 b_1, b_2, b_3, b_4也是如此，集合 C的隶属度函数 $\mu_C(x; c_1, c_2, c_3, c_4)$定义如下[12]：

$$\begin{cases} c_1 = \min(a_1, b_1) \\ c_2 = \eta_1 a_2 + (1-\eta_1) b_2 \\ c_3 = \eta_2 a_3 + (1-\eta_2) b_3 \\ c_4 = \max(a_4, b_4) \end{cases} \tag{3}$$

其中 $\eta_1, \eta_2 \in [0,1]$。依此规则，集合 A B将被合并为一个新的集合 C，如图 1所示。

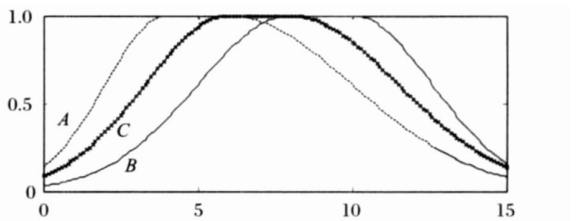

图 1 相似集 A B合并为集合 C

对于全集 U，若存在一个模糊集的相似性测度大于上限或小于下限，那么我们就将其从规则库中去除，前者表明该集合与全集相似，而后者说明该集合与单点集相似。

2.3 模糊规则生成策略

模糊规则库的遗传优化方法，通常包括 Michigan法、Pittsburgh法和迭代规则学习方法[13]。本文采用 Pittsburgh方法，假设有 N个模糊变量，M_i是关于变量 x_i的有用模糊集数量，每一条模糊规则的编码长度为 N，第 i个元素 c_i的取值范围为 $[0, M_i]$。当 $c_i > 0$时，表示第 c_i个模糊集起作用；当 $c_i = 0$时，表示第 i个模糊变量不起作用。规则集中，个体表示为大小为 $N \times N_{pop}$的级联字符串，N_{pop}为模糊规则库的初始规模，其中每一个长度为 N的子串代表一条独立的模糊规则。

子代规则集通过交叉与变异操作生成，这里，采用单点交叉算子。由于交叉与变异操作可能会引入多余的规则，因此模糊集 Agent还需要对生成的规则集进行检验，以保证模糊系统的一致性与紧凑性。如前所述，模糊集 Agent通过相互间传递其模糊集信息来产生子代，因此，子代也可用同样的策略来产生可解释的规则库，然后，在决策 Agent收集了其适应值信息后，用 NSGA-II算法来评价模糊集 Agent的父代与子代，并选择最优个体成为下一代种群。

3 实验结果分析

在实验测试中，采用了 KDD Cup99网络数据集，该数据集包含多种网络环境下的模拟入侵，其中每条连接记录含有 41维特征，被广泛用于 IDS评价测试。我们从 10%的训练数据选取含有“Normal”、“Smurf”和“Neptune”三类的 21 076条数据为训练数据样本，使用 311 029条记录为测试数据，并设置了 10个模糊集 Agent，每一个模糊集 Agent含有 10个模糊规则集。最终，在 100个模糊集中得到了 15个非支配解，模糊集数目和模糊规则数与精度之间的变化趋势如图 2所示，可以看出，所提取的模糊规则数目在 50到 300之间，其平均准确度为 80% ~98.5%，当生成 196条模糊规则时，具有最高

精度为 98.46%。

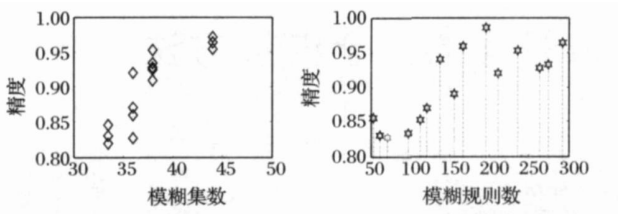

图 2　模糊集数和模糊规则数与精度之间的关系

如图 3所示，本文方法对模糊集 Agent进行 60次迭代后，通过对比模糊集分布策略、解释性的控制策略以及模糊规则生成策略的应用情况，可以明显看出在使用了 3层策略的情形下（图 3(a~b)），相比未使用时（图 3(c~d)），能明显减少模糊规则数与规则前件总长度，从而提高了系统的紧凑性。

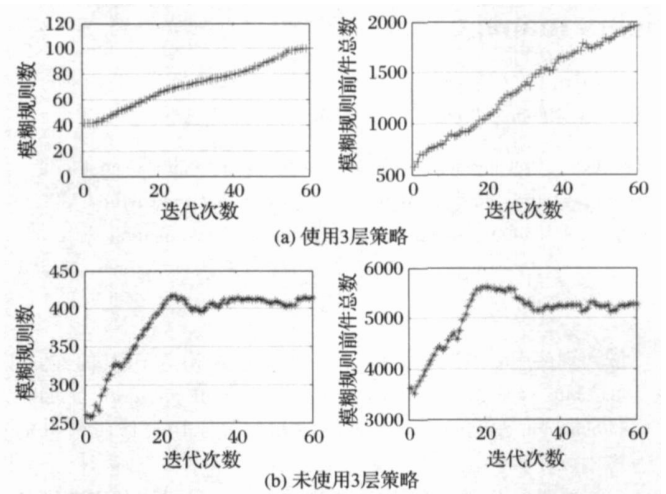

图 3　在模糊集 Agent进化过程中模糊规则生成情况对比

其次，为综合考虑检测性能，采用式（4）中的查全率（Recall）、查准率（Precision）与调和平均 F_measure值[14]作为检测精度的目标函数：

$$\mathrm{Recall}=\frac{TP}{TP+FN}$$

$$\mathrm{Precision}=\frac{TP}{TP+FP} \qquad (4)$$

$$F\_measure=\frac{2\cdot \mathrm{Precision}\cdot \mathrm{Recall}}{\mathrm{Precision}+\mathrm{Recall}}$$

表 1给出了本文方法与文献[15－17]的测试数据对比。其中，R代表查全率，P代表查准率，F代表 F_measure值，“—”表示该文献没有给出对应项的数据测试与评价。

由表 1可以看出，文献[15]中的 KDD-Cup 99 winner方法在划分 Normal类中具有较好的检测性能，并在其他攻击类测试中表现出较高的查准率，然而对于所有攻击类别的预报，若综合考虑查全率和 F-measure指标，则本文方法要稍优于该方法。文献[16]所提出的改进 PNrule方法在 Probe和 R2L攻击检测中优于本文方法，但相比之下在广泛的 DoS攻击检测中却明显处于劣势。文献[17]采用多分类器模型方法将多层感知神经网络、高斯分类与 K均值聚类算法相结合，对 Probe、DoS和 U2R攻击获得了较高的查全率，然而该方法并没有给出其他指标的数据结果，同时也未考虑 Normal类中误报率的最小化，从而可能会降低安全性分析的可解释性。

综合以上分析及数据结果，可以看出本文方法对 DoS、Probe和 U2R的攻击具有较好的检测性能，对 R2L的攻击检测性能稍弱。同时，实验表明本文方法对正常网络行为的检测具有 97.86%的查全率与 74.37%的查准率，以及较低的误报率，因而相比之下其整体性能在不同程度上要优于其他三种方法。

表 1不同方法的实验数据比较　　%

攻击类别	指标	本文方法	文献[15]方法	文献[16]方法	文献[17]方法
Probe	R	87.97	83.30	89.01	88.70
	P	73.48	64.81	82.11	—
	F	79.42	72.90	85.42	—
DoS	R	96.80	97.10	21.74	97.3
	P	98.65	99.88	96.68	—
	F	97.57	98.47	35.30	—
U2R	R	14.64	13.20	11.40	29.81
	P	59.03	71.43	53.06	—
	F	24.76	22.28	18.77	—
R2L	R	10.39	8.41	13.05	9.60
	P	67.60	98.84	82.37	—
	F	18.22	15.48	22.53	—
Normal	R	97.86	99.50	—	—
	P	74.37	74.61	—	—
	F	84.68	85.28	—	—

4　结语

本文在建立了具有精确性与解释性的模糊系统的基础上，对基于规则的模糊系统进行了必要的解释性优化，所提出的基于 3层策略的 Agent进化计算架构，通过模糊集 Agent间的适应值交互与遗传操作，以及决策 Agent的评价机制，能够有效地从网络流量数据中提取模糊 IF-THEN规则。同时，从多目标优化角度出发，利用 HGA中染色体的递阶结构，使得系统的参数和模糊规则数目能够同时得到优化，有效地提高了系统的紧凑性。实验结果表明该方法对于 DoS、Probe和 U2R的攻击具有较好的检测性能，对于异常入侵检测具有较高的分类精度以及较低的误报率。

参考文献：

[1] LEE W, STOLFO S J, MOK K W. Adaptive intrusion detection: A data mining approach[J]. Artificial Intelligence Review, 2000, 14(6): 533－567.

[2] BALAJINATH B, RAGHAVAN S V. Intrusion detection through learning behavior model[J]. Computer Communications, 2001, 24(12): 1202－1212.

[3] 杨武，云晓春，李建华. 一种基于强化规则学习的高效入侵检测方法[J]. 计算机研究与发展，2006，43(7)：1252－1259.

[4] GLOREZ G, BRIDGES S M, VAUGHN R B. An improved algorithm for fuzzy data mining for intrusion detection[C]// Proceedings of North American Fuzzy Information Processing Society Conference: NAFIPS 2000. New Orleans, LA: [s.n.], 2002: 457－462.

[5] 张箭，龚俭. 一种基于模糊综合评判的入侵异常检测方法[J]. 计算机研究与发展，2003，40(6)：776－782.

[6] ABRAHAM A, KOPPEN M, FRANKE K. Design and Application of Hybrid Intelligent Systems[M]. Amsterdam: IOS Press, 2003: 983－992.

[7] JULISCH K, DACIER M. Mining intrusion detection alarms for actionable knowledge[C]// Proceedings of the Eighth ACM International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2002: 366－375.

（下转第 2239页）

$\alpha=10, \beta=2, P_{min}=10, p^-=5, p^+=10, p=15, f=0.1\%$, $n=1$, $DF=0.2$

试验一　比较陷阱邮箱动态分布策略使用前后,蠕虫邮件的捕获率,结果见表 1。

表 1　动态分布策略使用前后捕获率比较

传播类型	PF	捕捉率/%	
		采用策略前	采用策略后
基于本地邮件服务器的传播类型	0.1	1.57	18.64
	0.3	1.77	18.80
	0.5	1.89	19.01
	0.7	1.92	19.26
基于自带邮件服务器的传播类型	0.1	1.29	18.17
	0.3	1.43	18.18
	0.5	1.66	18.28
	0.7	2.36	18.51

试验一中,暂不考虑行为监测对邮件捕获的辅助作用。结果表明,陷阱邮箱动态分布策略的采用大幅度提高了蠕虫邮件的捕获率。

试验二　测试陷阱诱骗与行为模型匹配的互补效果。

传播因子分别为 0.1、0.3、0.5、0.7的两种传播类型的邮件蠕虫,其附着邮件的捕获率试验结果分别如图 3和 4所示。试验二结果表明,对于不同传播因子的未知邮件蠕虫,陷阱邮箱与行为监测能够很好地互补过滤大多数蠕虫邮件,并在免疫机制生成前最大限度地控制邮件蠕虫的传播。

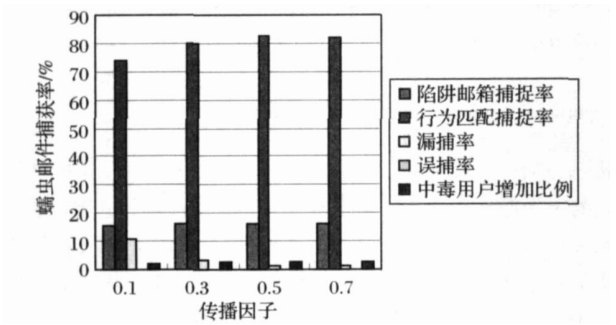

图 3　本地邮件服务器传播类型的蠕虫邮件捕获率

现有行为识别方法多用于垃圾邮件的过滤,其捕捉率在 97%左右[5]。本文将行为识别方法与陷阱邮箱相结合,用于蠕虫邮件的过滤。从以上两个模拟试验的结果来看,除对传播因子为 0.1的邮件蠕虫所发邮件的捕捉率较低以外,对于其他邮件蠕虫所发邮件的捕捉率均高于现有行为识别方法。若将本文所提的行为模型进一步细化,蠕虫邮件的捕捉效果将更好。此外,由于仅在服务器端进行监测,从而避免了监测方法客户端与服务器端的通信负载,节省了网络资源。

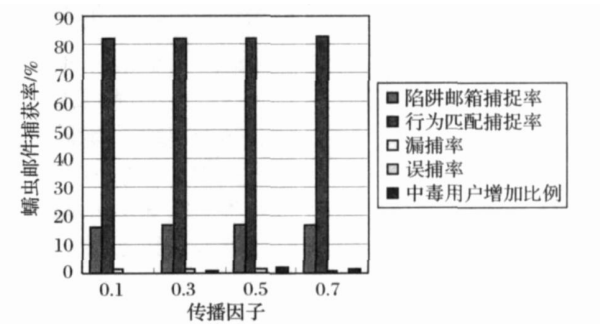

图 4　自带邮件服务器传播类型的蠕虫邮件捕获率

5　结语

本文提出了一种基于陷阱邮箱的蠕虫邮件行为模式识别方法。该方法首先利用动态分布的陷阱邮箱诱捕蠕虫邮件,进而获取大量蠕虫邮件的特征信息。而后根据本文所提出的蠕虫邮件行为模型,对所有邮件的特征信息进行模型匹配,从而最大限度地分离蠕虫邮件。由于方法采用了模型匹配的思路,摆脱了传播因子的影响,因而不存在对传播延时较长的邮件蠕虫活动敏感度不高的缺点。从模拟试验结果来看,陷阱诱骗与行为模型匹配能够很好地对邮件进行互补过滤。

参考文献:

[1] MARTIN S, SEWANI A. Semi-supervised learning on E-mail characteristics for novel worm detection[D]. Berkeley: University of California, 2004.

[2] WONG C, BIELSKI S, MCCUNE J M, et al. A study of mass mailing worms[D]. Pittsburgh: Carnegie Mellon University, 2004.

[3] BARRENO M, NELSON B, SEARS R, et al. User model transfer for email virus detection[D]. Berkeley: University of California Computer Science Division, 2006.

[4] HUANG C-T, JOHNSON N L, JANIES J, et al. On capturing and containing e-mail worms[D]. Colombia: University of South Carolina Department of Computer Science and Engineering, 2006.

[5] 赵治国, 谭敏生, 丁琳. 垃圾邮件行为识别技术的研究与实现[J]. 计算机应用研究, 2007, 24(11): 228－231.

(上接第 2229页)

[8] 张永, 吴晓蓓, 向峥嵘, 等. 基于多目标进化算法的高维模糊分类系统的设计[J]. 系统仿真学报, 2007, 19(1): 210－215.

[9] 阎岭, 郑洪涛, 蒋静坪. 基于进化策略生成可解释性模糊系统[J]. 电子学报, 2005, 33(1): 70－73.

[10] DEB K, PRATAP A, AGRARWAL S, et al. A fast and elitist multiobjective genetic algorithm: NSGA-II[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(2): 182－197.

[11] 周辉仁, 郑丕谔. 模糊系统的递阶遗传算法设计新方法[J]. 系统仿真学报, 2008, 20(3): 678－681.

[12] TSANG C-H, KWONG S, WANG HANLIN. Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection[J]. Pattern Recognition, 2007, 40(9): 2373－2391.

[13] MAGDALENA L, CORDON O, GOMIDE F, et al. Ten years of genetic fuzzy systems: current framework and new trends[J]. Fuzzy Sets and Systems, 2004, 141(1): 5－31.

[14] 俞研, 黄皓. 面向入侵检测的基于多目标遗传算法的特征选择[J]. 计算机科学, 2007, 34(3): 197－200.

[15] ELKAN C. Results of the KDD'99 classifier learning[J]. ACM SIGKDD Explorations Newsletter, 2000, 1(2): 63－64.

[16] AGARWAL R, JOSHI M V. PNrule: A new framework for learning classifier models in data mining (a case-study in network intrusion detection)[C/OL]// Proceedings of First SIAM Conference on Data Mining. Chicago: [s.n.], 2001[2009－02－01]. http://www.siam.org/meetings/sdm01/pdf/sdm01_30.pdf.

[17] MAHESHKUMAR S, GURSEL S. Application of machine learning algorithms to KDD intrusion detection dataset within misuse detection context[C]// Proceedings of International Conference on Machine Learning: Models, Technologies and Applications. Las Vegas, Nevada, USA: [s.n.], 2003: 209－215.