·安全技术· 文章编号:1000-3428(2017)07-0175-07 文献标志码:A 中图分类号:TP393.08

基于文化算法的层次属性约减入侵检测模型

申 元,高 岭,高 妮,王 帆

(西北大学 信息科学与技术学院,西安 710069)

摘 要: 为有针对性地区分入侵攻击类别,提高入侵检测系统(IDS)整体的分类准确率,提出一种层次属性约减模型。该模型采用文化算法的双层进化思想,结合粗糙集和遗传算法进行属性约减。对数据进行预处理并分层划分子空间,形成决策子表规则集 f_D。运用文化算法在信念空间进行知识更新,并将层次评价知识库的进化数据传入种群空间。在种群空间利用粗糙集和遗传算法进行进化和约减,得到各层的优选属性集 f_{opt},设计出层次 Bayes 分类器验证模型性能。实验结果表明,该模型可将属性约减前的 Bayes 分类正确率提高至 98.21%,并能较好地识别出流量特征不明显的 R2L,U2R 类别的入侵攻击。

关键词: 入侵检测;文化算法;粗糙集;遗传算法;层次属性约减

中文引用格式: 申 元,高 岭,高 妮,等. 基于文化算法的层次属性约减入侵检测模型[J]. 计算机工程,2017,43(7):175-181.

英文引用格式: Shen Yuan, Gao Ling, Gao Ni, et al. Hierarchical Attribute Reduction Model for Intrusion Detection Based on Cultural Algorithm[J]. Computer Engineering, 2017, 43(7):175-181.

Hierarchical Attribute Reduction Model for Intrusion Detection Based on Cultural Algorithm

SHEN Yuan, GAO Ling, GAO Ni, WANG Fan

(School of Information Science and Technology, Northwest University, Xi'an 710069, China)

【Abstract】 In order to distinguish detection attack categories pertinently and improve the classification accuracy of Intrusion Detection System (IDS), a hierarchical attributes reduction model used for IDS is proposed. This model reduces attributes by adopting dual structure of culture algorithms and combined with rough sets as well as genetic algorithm. Firstly, the data is preprocessed and divide it into hierarchies, which forms the rule of decision subset f_D. Secondly, using cultural algorithm, knowledge is updated in belief space, and evolving data of hierarchical evaluation knowledge is introduced into population space. Thirdly, the optimal subser of each layer is acquired by using rough sets and genetic algorithm which can evolve knowledge and reduce attributes in belief space. Finally, model performance is verified by designing Bayes hierarchical classifier. Experimental results show that the algorithm can improve the accuracy of the Bayes classification before attributes reducting to 98.21%, and it is better to identify the intrusion categories whose traffic characteristics is not obvious such as R2L and U2R.

【Key words】 intrusion detection; cultural algorithm; rough set; genetic algorithm; hierarchical attribute reduction

DOI: 10.3969/j.issn.1000-3428.2017.07.029

0 概述

入侵检测是通过监控主机和网络的状态、资源利用、网络连接等行为,检测用户的越权使用以及安全缺陷对系统进行入侵的企图[1]。入侵检测系统(Intrusion Detection System, IDS)作为保证网络安全的重要手段,一直受到安全领域的重视和关注。近年来,入侵检测技术得到了长足发展,但在误报、漏检、时间性能和协调性等方面仍存在问题[2-3]。

数据挖掘应用于入侵检测必须依赖于大量的数据,训练时间长,建立模型困难。采用特征选择的方法可以消除无关因素,提高检测性能。文献[4]采用

基金项目: 国家自然科学基金(61373176,61572401);陕西省重大科技创新专项资金项目(2012ZKC05-2)。

作者简介: 申 元(1991—),女,硕士研究生,主研方向为网络与信息安全;高 岭,教授、博士、博士生导师;高 妮,博士研究生;王 帆,硕士研究生。

收稿日期: 2016-06-06 **修回日期:** 2016-07-12 **E-mail:** gl@nwu.edu.cn.

粗糙集方法进行属性约减,检测率提高了 10% 左右。文献[5]通过信息增益和约登指数删减数据集的特征属性确定特征属性容量。文献[6]对属性重要性进行数值化并利用信息增益进行属性约减。但针对全局的属性约减没有差异和针对性,某些特征对一种或几种入侵类别有区分性,而对其他类型产生干扰,降低整体的分类性能[7],且针对不同的入侵类别,特征选择的维度也会有所不同,而传统的属性约减方法只是简单的整体约减,导致整体分类准确率不高,且异常检测效果不佳。此外,特征选择对于分类起到很重要的作用,而现阶段相关研究很少重点研究正常与入侵攻击之间的特征区别[8]。

文化算法[9]是一种模拟社会进化的算法,用于解决复杂计算并进行全局最优搜索。目前越来越多的问题通过文化算法与已有机器学习方法结合获得了更优的解。文献[10]采用了文化算法的双重进化结构,构建了一种反映人们认知和偏好的广义知识模型。文献[11]将文化算法里的信念空间设为网格结构用于求解多目标优化问题。

针对以上问题,本文提出基于文化算法的属性约减方法,针对入侵类别网络连接特点,将入侵类别进行层次划分。借鉴文化算法的双层进化模式,得到双层进化的粗糙集遗传算法并进行属性约减,从而获得特定的优选集(f_{opt}),即针对不同类别得到不同维度具有针对性的规则集。根据 f_{opt} 设计层次贝叶斯分类器进行训练,最终构成层次属性约减贝叶斯入侵检测模型(HRGA-IDS)用于入侵检测。

1 模型结构框架

基于层次属性约减的入侵检测模型由预处理、层次属性约减、入侵检测器三部分构成,如图 1 所示。

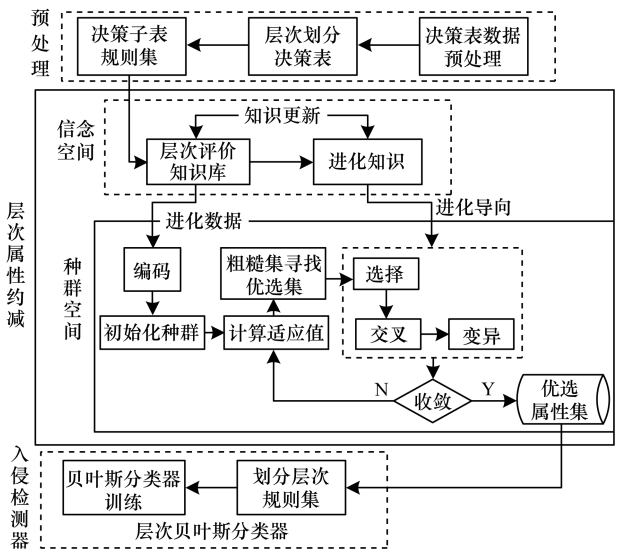


图 1 HRGA-IDS 模型执行过程

预处理模块负责对输入决策表进行处理,进行分层划分子空间。首先对信息系统里面的数据去除重复,并且编码,根据数据集的数据属性,结合先验知识以及专家经验,根据不同决策属性显著特征,层次划分决策表,生成决策子表规则集(f_D),用以表示层次的特征分布。

层次属性约减模块采用文化算法进化模型,由知识更新的信念空间和个体进化的种群空间构成,实现优化粗糙集遗传算法、有效约减属性并快速收敛的目的。信念空间中的层次评价知识库,利用预处理产生的 f_D 控制属性约减的约减层数,以实现针对相似类别约减优选属性的目的。通过进化知识来动态引导进化方向,并通过进化反馈进行动态更新。在种群空间,实现粗糙集遗传算法的属性约减目的。通过粗糙集计算重要属性,通过遗传算法快速寻优。最终形成不同维度的优选属性集。

入侵检测器模块对优选属性集进行层次划分,分层进行贝叶斯分类器训练,获得参数用于测试决策表。子节点在父节点划分的基础上选定优选属性集继续进行划分。

1.1 决策子表规则集

根据决策属性 D 及特征,依据专家经验,人工将决策属性分成决策子表规则集 f_D。

$$f_D=\{\{D,d_1,d_2,\cdots\},\{d_1,d_{11},d_{12},\cdots\},\{d_2,d_{21},d_{22},\cdots\},\cdots\} \tag{1}$$

其中,D 为整个决策表的决策属性;d_1,d_2 为其子集合,每一个子集合的第一个元素为其父节点,其余元素为子节点。决策表根据决策属性 D 的 f_D 进行同等划分。

1.2 层次属性约减方法

层次属性约减模块参考文化算法思路,采用文化算法的双层进化机制,上层信念空间实现对进化过程隐含信息的提取,并以知识的形式对种群进化状况加以描述[12],底层种群空间通过进化操作和性能评价进行自身的迭代。本文采用遗传算法作为主群体空间的进化过程,结合粗糙集进行属性约减。

训练数据可以看作一个决策表,用一个四元组描述 $S=\{U,C\cup D=A,V,\rho\}$,其中,U 为非空有限集,表示论域;A 表示属性集;C 为条件属性 $C=\{M_i\mid i=1,2,\cdots,k\}$;$D$ 为决策属性 $D=\{d\}$;V 为属性值;ρ 则表示映射函数 $U\times A\rightarrow V,\rho(o_i,a_j)=v_{ij}$ 表示 o_i 在 a_j 上的取值为 v_{ij},其中,$o_i\in U,a_j\in A,v_{ij}\in V$。

1.2.1 文化算法

信念空间用于控制种群空间的进化发展。本文模型中信念空间由层次评价知识库和进化知识两部分组成。f_D 充当层次评价知识库。进化知识指隐含

在交互式操作中不能直接获得的隐含知识[10]。

定义 1　层次评价知识库是 i 层层次规则集 f_D^i 到解空间 X 的一个映射,记作 $F_h:f_D^i\rightarrow X$,本文根据 f_D 划分决策表,形成层次解空间。每访问一层解空间,形成相应种群空间 $S(g)$ 和进化知识 $K(g)$。

定义 2　进化知识描述进化种群的基本情况,定义为第 g 代进化知识 $K(g)$[10]:

$$K(g)=[avg(g),x_{\max}(g),\rho_{\max}(g),x_{\min}(g),\rho_{\min}(g),sim(g)] \tag{2}$$

其中,$avg(g)$ 为种群平均适应度;$x_{\max}(g)=\arg\max_{i=1,2,\cdots,M}\rho(x_i(g))$,$n$ 为种群规模,且 $\rho_{\max}(g)=\rho(x_{\max}(g))$;$x_{\min}(g)=\arg\min_{i=1,2,\cdots,n}\rho(x_i(g))$;$\rho_{\min}(g)=\rho(x_{\min}(g))$;$sim(g)$ 为进化相似度,表示为:

$$sim(g)=\frac{\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\sqrt{\sum_{k=1}^{n}(x_{ik}(t)-x_{jk}(g))^2}}{n(n-1)} \tag{3}$$

定义 3　进化导向函数影响控制进化,在进化选择中,以流量记录个体作为约束条件限制子代相似个体的数目,以提高种群多样性[12]。因此,需要采用一定措施抑制浓度较高的相似个体。这里采用相似个体浓度 $C^g(x_i)=\frac{m_i}{n}$ 和种群多样性 σ 来表示。

$$\sigma=\frac{1}{n}\sum_{i=1}^{n}\left[x_i-\frac{1}{n}\sum_{j=1}^{m}x_j\right]^2 \tag{4}$$

进化导向函数为:

$$D_s(x_i(g+1))=\lambda\sigma+[(1-\lambda)C^g(x_i)]$$

如果满足 $D_s(x_i(g+1))\neq 0$,则 $x_i(g+1)$ 进入下一代。

种群空间中的操作是将粗糙集中的约减原理与遗传算法的寻优进行结合,进行知识的分类和约减。

1.2.2　粗糙集理论

本文的粗糙集属性约减利用文献[13]中的 Reduct 算法,该算法通过计算可辨析矩阵对可辨析矩阵进行等价项约减、吸收规则运算、膨胀规则运算,最终达到属性约减的目的。

定义 4　属性的依赖度定义为 $r(d)=|pos_B(d)|/|U|$,其中,$|pos_B(d)|$ 为正域 $pos_B(d)$[14] 元素的个数;$|U|$ 为整个决策表对象集合的个数。

定义 5(可辨识矩阵)给定一个决策信息表 $SD=\{U,C\cup D=A,V,\rho\}$,可辨识矩阵 $\boldsymbol{M}$ 是一个 $|U|\times|U|$ 的矩阵:

$$\boldsymbol{M}=\begin{cases}m_{ij},C(x_i)\neq C(x_j)\\ \varphi,C(x_i)=C(x_j)\end{cases} \tag{5}$$

其中,$m_{ij}=\{a\in C:a(x_i)\neq a(x_i)\wedge(d\in D,d(x_i)\neq d(x_j))\}$,$i,j=1,2,\cdots,n$,$m_{ij}$ 表示一个属性集合,利用划分 U/D 将 x_i 和 x_j 划分到不同的决策类别中。其物理意义是样本 x_i 和 x_j 可以被 m_{ij} 中的任何属性区分。可辨识矩阵是一个对称矩阵,因此,只需要考虑上三角或者下三角部分。

定义 6(吸收规则)如果一个只有合取运算的项是另一个项的子集,那么该最小属性数目的项被保留,其余约掉。

定义 7(膨胀规则)应用膨胀规则算法保留在划分过程中经常使用的属性。

膨胀规则算法过程如下:

1)从吸收规则约减后的 $f(s)$ 中找到出现最频繁的属性(至少出现 2 次)。

2)将具有频繁属性的项用合取,并只保留频繁属性,其余项用析取。

3)将具有频繁属性的项中频繁属性去掉,并将其他属性用析取连接,项与项用合取连接。

4)利用合取连接过程 2)、过程 3)中剩余的项。

算法 1　Reduct 算法[13]

输入　待约减的信息系统 SD

输出　属性约减集合

1)计算可辨识矩阵 $\boldsymbol{M}$。

2)用析取逻辑表达式 Or_{ij} 表示可辨识矩阵中的 m_{ij},即:

$$Or_{ij}=\bigvee_{c\in m_{ij}}c \tag{6}$$

3)将所有析取逻辑表达式用合取运算连接,表示可辨析:

$$f(s)=\bigwedge_{m_{ij}\neq\varphi}Or_{ij} \tag{7}$$

4)利用吸收规则约减 $f(s)$。

5)利用膨胀规则算法约减 $f(s)$。

6)得到约减结果。

1.2.3　遗传算法

在特征选择过程中,每个染色体对应一个 0,1 向量来表示特征是否被选。若为 1,则表示被选,反之为 0。

定义 8　设属性 c 中可能的取值为 pr_i,出现的概率为 $p(pr_i)$,则称属性 c 的信息熵为 $H(c)=\sum_{i=1}^{n}p(pr_i)\ln p(pr_i)$,表示含有的攻击信息量。

为了衡量个体的攻击性能,建立适应度函数指导搜索。设 $p(x)$ 为样本 x 中基因对应的特征中攻击信息大于阈值 ε 的比例,$p(x)$ 越大,说明个体中优良基因数目越多,被选中的可能性也就越大;$N(x)$ 为个体 x 中含有基因“1”的个数;t 为当前进化代数,T 为进化总代数,则适应度函数表示为:

$$fitness(t)=\frac{p(x)}{1+e^{N(x)}}\mathrm{lb}\frac{t}{T}+r(d) \tag{8}$$

2　模型实现

2.1　基于层次属性约减的入侵检测算法

算法 2　基于层次属性约减的入侵检测算法(HRGA-IDS)

输入 KDD99 信息系统(K_S)

输出 分类结果以及准确率

1)去除重复。

2)二进制编码。

3)利用数据特点,人工将 K_S 划分成 f_D。

4)循环遍历 f_D,执行过程 5)~过程 12)。

5)利用 KUD 函数产生 G_D 和 $K(g)$。

6)迭代执行过程 7)~过程 11)。

7)利用 TPS 算法计算优选属性集 f_{opt}。

8)保存 f_{opt}。

9)利用 Bayes 对 f_{opt} 进行分类,并将结果进行保存。

10)计算正确率(accuracy)、检验率(detection)、误警率(false alarm)。

11)利用 y_d = accuracy-false alarm 计算约登指数 y_d。

12)根据 y_d 保存最优 f_{opt}。

$Dis(x_t(i),x_t(j))$ HRGA-IDS 描述了整个模型的工作过程,对信息系统进行预处理,并依据决策子表规则集对其进行分层处理,在信念空间中进行知识更新,形成知识库,并在种群空间中进行属性约减,最后利用贝叶斯进行分类来验证模型性能并找到每一层的最优解。其中,KUD 表示知识更新函数;TPS 表示种群更新函数。

2.2 知识更新函数

算法 3 知识更新函数(KUD)

输入 决策子表规则集(f_D),访问层数 g

输出 进化数据 G_D,初始化进化知识 $K(g)$

1)循环访问 f_D。

2)如果 ${f_D}^i$ 决策子集合未被访问过。

3)将该子集的第一个元素划为父决策属性:$D_F = f_D^i(1)$。

4)根据 D_F 计算其种群空间 S_F:

$$S_F = \{S(x) \mid \forall x \in U, D(x) = D_F\}$$

5)访问父节点 $U_F = S_F.U$。

6)对于 f_D^i 剩下的每一个元素 $f_D^i(j)$,执行过程 7)~过程 9)。

7)划分子决策属性 $D_S^j = f_D^i(j)$。

8)根据 D_S^j 计算其相对应的种群空间:

$$S_s^i = \{S_F(x) \mid \forall x \in U_F, D(x) = D_S^j\}$$

9)将该决策子集设置被访问标志:

$$flag(f_D^i) = ture$$

10)进化数据 $G_D = S_s$。

11)根据式(2)初始化进化知识 $K(g)$ 以初始化第一代进化知识。

KUD 是知识更新函数,主要负责层次评价知识库和进化知识之间的知识更新,根据决策子表规则集获取分层的知识并进行处理。

2.3 进化导向函数

算法 4 进化导向函数(AD)

输入 进化知识 $K(g)$

输出 进化标志 $OS(x_i(t+1))$

1)遍历所有样本,计算两两样本之间的距离 $Dis(x_t(i),x_t(j))$,执行过程 2)~过程 3)。

2)如果距离 $Dis(x_t(i),x_t(j))$ 小于阈值 thred。

3)则设置样本相似函数 $Similarity(i,j)$ 为 1。

4)利用定义 3 计算种群个体浓度 $C(x_i)'$ 和多样性 σ。

5 计算进化导向函数 $D_s(x_i(t+1))$。

6)如果 $D_s(x_i(t+1)) \neq 0$。

7)则进入下一代,设置进化标志为 1 :$OS(x_i(t+1)) = 1$。

8)否则继续留在本代,设置进化标志为 0:$OS(x_i(t+1)) = 0$。

AD 算法通过进化知识控制种群空间中遗传算法的进化,通过进化导向函数控制抑制浓度高的相似个体,保持进化的种群多样性。

2.4 种群空间函数

算法 5 种群空间函数(TPS)

输入 进化数据 G_D

输出 优选属性集 f_{opt}

1)根据 $r(d) = |pos_B(d)|/|U|$ 计算决策属性 D 关于条件属性 C 的支持度 $r(d)$。

2)初始化种群 G_D。

3)初始化当前进化代数 t 为 0。

4)计算适应度函数 $fitness(t)$。

5)如果连续 t_c 代 *fitness* 不收敛并且 $t > maxgen$,则执行过程 6)~过程 11)。

6)执行 Reduct 算法。

7)进化代数 $t++$。

8)利用轮盘赌方法选择属性 f_s,用交叉概率 p_c 以及变异概率 p_m 产生新代种群 $S(t)$,该属性对应的等位基因不发生变异。

9)计算 $fitness(t)$。

10)利用进化导向函数 AD 指导进化。

11)依据最优保存策略将 f_s 中最优属性集 f_{opt} 复制到下一代种群中,并保存。

12)输出 f_{opt}。

TPS 算法实现种群空间中粗糙集和遗传算法结合进行属性约减功能。若适应度函数值连续 t_c 代收敛,结束算法,输出 f_{opt}。

3　实验仿真与分析

3.1　数据预处理

本文采用 KDD-Cup99 中的 10% 数据集作为模型的样本数据,其中,41 维特征包含了 9 个基本流量特征、13 个连接内容特征和 19 个网络流量特征,采用该数据的 20% 作为训练数据,其余 80% 作为测试数据。实验环境为 Windows,Intel(R) Core(TM) i5 CPU,64 位操作系统,利用 Matlab 进行仿真。

首先,由于重复数据会淹没其他类型的特征,因此去除原始数据集中的重复数据[5],去重后的类型分布如表 1 所示。将去重的数据集转换成二进制字符串用来标示样本编码。编码构造参考文献[1]。

表 1　样本去重后类型分布数量

数据记录	Normal	DOS	Probe	U2R	R2L
原始数据	97 277	391 458	4 107	52	1 126
删除数据	9 445	336 886	1 977	0	127
保留数据	87 832	54 572	2 130	52	999

在本文中数据来源于 KDD99 数据集,其中,每个网络连接可以分为正常和异常 2 种状态,在异常状态中,通过合法的手段使服务器不能提供正常服务的攻击手段都属于 DOS 范畴[15],该攻击通过大量的通信量或连接请求冲击网络,使得网络资源消耗殆尽;R2L 通过改变配置方式、漏洞方式等获取用户权限。该攻击模式在网络连接上没有显著特征;U2R 攻击通过缓冲区溢出方式、系统环境恶化等方式获取用户 shell,该方式也没有大量网络连接;Probe 通过滥用方式造成系统脆弱,发生此类攻击时网络中会有大量探寻连接。因为 U2R 和 U2L 这 2 种连接行为的特征在数据集中记录较少,且没有大量的连接特征,只是具有一些 TCP 的内容特征,与正常连接非常相似[2],所以 U2R 和 U2L 这 2 种连接与正常态连接分为流量无关类(Non-traffic Related,NTR),其余 2 类分为流量相关类(Traffic Related,TR),网络连接层次预处理如图 2 所示。经过层次划分决策表之后,形成决策子表规则集 f_D。

$$f_D = \{\{D, NTR, TR\}, \{NTR, Normal, U2R, R2L\}, \{TR, DOS, Probe\}\} \tag{11}$$

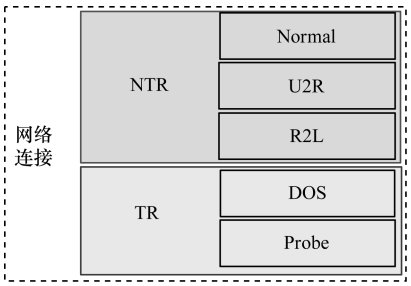
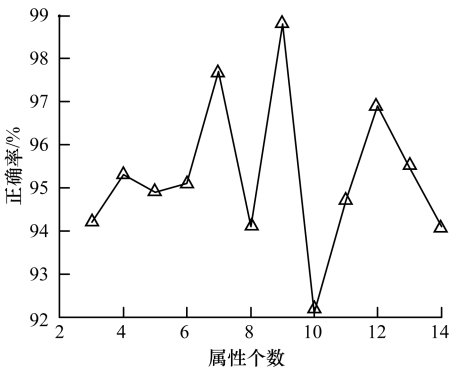


图 2　f_D 的层次结构

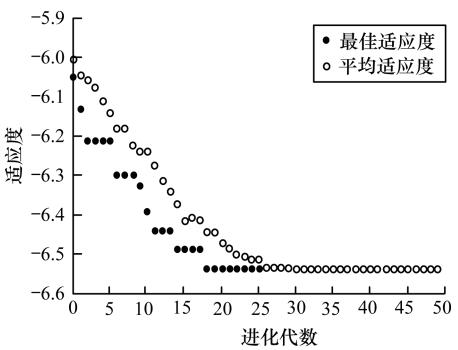
3.2　结果分析

本文采用正确率、检测率、误警率验证模型的性能。检测率与误警率之差作为结果的约登指数来评价分类结果的优良,并迭代 500 次计算约减的平均准确率。

图 3 ~ 图 5 描述的是 f_D 的属性约减个数和正确率以及最优约减集的适应度值与进化代数,其中,图 3(a)展示的是 f_D^1 的属性约减及正确率;图 3(b)描述最优属性集的进化代数,可以看到,f_D^1 的正确率最高约减属性集个数为 9。图 4 表示的是 f_D^2 的信息,图 5 表示的是 f_D^3 的信息,从图中可以看到,f_D 的每一层的最优约减集都是不一样的,第一层中的最优约减集的属性个数是 9 个,f_D^2 的最优约减集的属性个数是 6 个,f_D^3 的最优约减集的属性个数是 7 个。因此,在测试数据时,选取以上最优约减集。此外,从图 3(b)、图 4(b)、图 5(b)中也可以看出,各个最优约减集也均迭代 45 次 ~ 60 次就达到收敛,也说明了选择最优约减个数可以减少迭代次数。

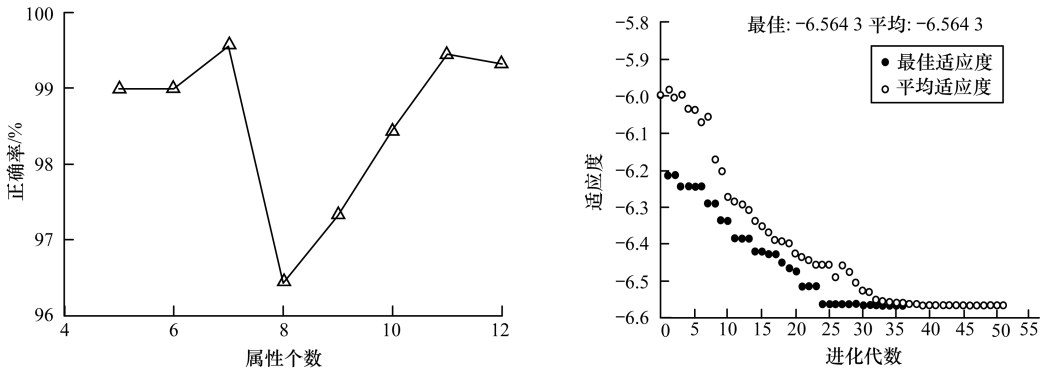


(a)f_D^1的属性约减及正确率



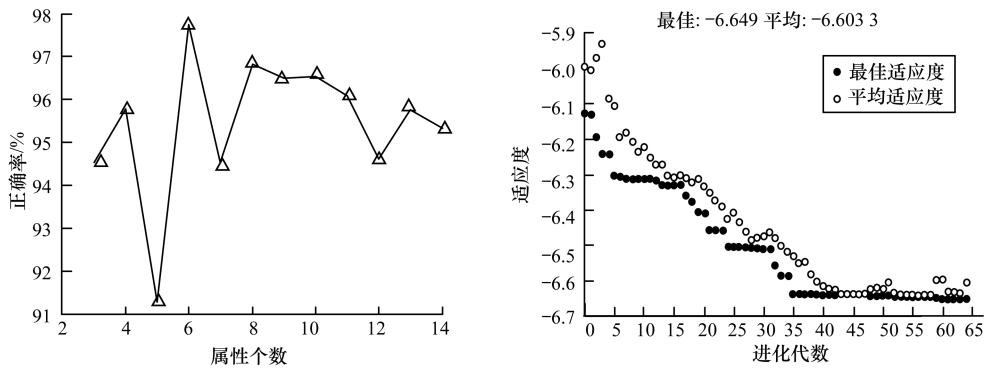
(b)f_D^1最优属性集的进化代数

图 3　f_D^1 的属性约减以及最优约减集的进化情况



(a)f_D^2的属性约减及正确率　(b)f_D^2最优属性集的进化代数

图 4　f_D^2 的属性约减以及最优约减集进化情况



(a)f_D^3的属性约减及正确率　(b)f_D^3最优属性集的进化代数

图 5　f_D^3 的属性约减以及最优约减集进化情况

在图 3(b) ~ 图 5(b)中,最佳适应度分别为 −6.537 2, −6.564 3, −6.649,平均适应度分别为 −6.537 1, −6.564 3, −6.603 3。每一层选取最优约减集得到该模型整体的层次约减集,以及模型的正确率、检测率、误警率,如表 2和表 3 所示。

表 2　检测率、误警率和约登指数

检测类别	检测率/%	误警率/%	约登指数
Normal	99.12	0.06	0.991
DOS	99.35	0.05	0.993
R2L	98.34	0.08	0.983
U2R	98.26	0.15	0.991
Probe	98.75	0.03	0.985
整体	99.28	0.08	0.992

表 3　属性约减前后正确率对比

方法	正确率/%	约登指数
约减前 Bayes	96.95	0.987
约减后 Bayes	98.21	0.992

从表 2 和表 3 可以看出,利用 HRGA-IDS 模型进行属性约减并且分类,能够较好地识别 Normal, DOS 以及 Probe,且对于 R2L 和 U2R 流量特征不明显的攻击种类,也能够很好识别。表 2 中 Normal 的约登指数为 0.991,DOS 的约登指数为 0.993,其余 3 类的约登指数均在 0.98 以上,并且整体的约登指数为 0.992,说明了该方法的分类结果较为显著。同时,从表 3 可以看出,属性进行层次约减后,Bayes 方法分类的正确率得到了显著提升,由 96.95% 提升到 98.21% 。

4　结束语

本文针对当前网络入侵的热点问题,设计层次属性约减贝叶斯入侵检测模型。采用基于文化算法的属性约简入侵检测模型对流量数据进行分层次属性约减,利用贝叶斯分类器检验模型的约减属性性能。实验结果表明,基于文化算法的双层进化属性约减方法能够有效识别 KDD99 数据集中的不同攻击类别,并对攻击类别定制不同的特征集进行分类识别,对于攻击类别尤其是 R2L,U2R 流量特征不明显的类别能够很好地识别。但本文模型仍存在不足,f_D 是人工依据专家经验划分的,存在一定的主观性,下一步将重点解决自动生成 f_D 算法,对具有针对性的规则集归纳分析,形成更加细化的入侵检测规则,用于优化入侵检测。

参考文献

[1] 张　玲,白中英,罗守山,等. 基于粗糙集和人工免疫的集成入侵检测模型[J]. 通信学报,2013,34(9):166-176.

[2] Li M. Change Trend of Averaged Hurst Parameter of Traffic Under DDOS Flood Attacks[J]. Computers & Security,2006,25(3):213-220.

[3] Wang W, Guyet T, Quiniou R, et al. Autonomic Intrusion Detection: Adaptively Detecting Anomalies over Unlabeled Audit Data Streams in Computer Networks[J]. Knowledge-based Systems, 2014, 70: 103-117.

[4] 赵曦滨,井然哲,顾　明. 基于粗糙集的自适应入侵检测算法[J]. 清华大学学报(自然科学版),2008,48(7):1165-1168.

[5] 唐成华,刘鹏程,汤申生,等. 基于特征选择的模糊聚类异常入侵行为检测[J]. 计算机研究与发展,2015,52(3):718-728.

[6] Saxena H, Richariya V. Intrusion Detection in KDD99 Dataset Using SVM-PSO and Feature Reduction with Information Gain[J]. International Journal of Computer Applications,2014,98(6):25-29.

[7] 李丹丹,田春伟,李佰洋,等. 基于子空间聚类的网络流量分类方法[J]. 哈尔滨理工大学学报,2015,20(2):63-68.

[8] Lin W C, Ke S W, Tsai C F. CANN: An Intrusion Detection System Based on Combining Cluster Centers and NearestNeighbors[J]. Knowledge-based Systems, 2015,78(1):13-21.

[9] Reynolds R G. An Introduction to Cultural Algorithms[C]//Proceedings of the 3rd Annual Conference on Evolutionary Programming. San Diego, USA: World Scientific,1994:131-139.

[10] 郭一楠,巩敦卫. 双层进化交互式遗传算法的知识提取与利用[J]. 控制与决策,2007,22(12):1329-1334.

[11] Coello C A C, Becerra R L. Evolutionary Multiobjective Optimization Using a Cultural Algorithm [C]// Proceedings of IEEE Swarm Intelligence Symposium. Washington D. C., USA: IEEE Press,2003:6-13.

[12] 郭一楠,王　辉,程　建. 自适应免疫克隆选择文化算法[J]. 电子学报,2010,38(4):966-972.

[13] Sengupta N, Sen J, Sil J, et al. Designing of On-line Intrusion Detection System Using Rough Set Theory and Q-learning Algorithm [J]. Neurocomputing, 2013, 111(6):161-168.

[14] Lashin E F, Kozae A M, Khadra A A A, et al. Rough Set Theory for Topological Spaces[J]. International Journal of Approximate Reasoning,2005,40(12):35-43.

[15] Chang R K C. Defending Against Flooding-based Distributed Denial-of-Service Attacks: A Tutorial[J]. IEEE Communications Magazine,2002,40(10):42-51.

编辑　刘　冰　索书志

(上接第 174 页)

参考文献

[1] 谢　平,邹传伟. 互联网金融模式研究[J]. 金融研究,2012(12):11-22.

[2] 上海金融信息行业协会. 互联网金融网络与信息安全技术指引[EB/OL]. (2010-11-21). https://www.watchf.cn/.

[3] 公安部等级保护评估中心. 信息安全等级保护基本要求[EB/OL]. (2008-11-01). http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getJcbz&id=402886e4353223cb013551fa78170050.

[4] 公安部等级保护评估中心. 信息系统安全管理要求[EB/OL]. (2006-05-31). http://www.djbh.net/webdev/web/PolicyStandardsAction.do?p=getJcbz&id=402886e4353223cb0135520045ce0055.

[5] 中国软件测评中心,中国电子技术标准化研究院,中国信息安全测评中心. 公共及商用服务信息系统个人信息保护指南[EB/OL]. (2012-11-05). http://www.pipa.gov.cn/NewsDetail.asp?ID=1002.

[6] 国家信息中心信息安全研究与服务中心,中国电信股份有限公司北京研究院. 信息安全风险管理指南[EB/OL]. (2009-12-01). https://wenku.baidu.com/view/52d4c724ccbff121dd368377.html.

[7] 康　维. 网络安全体系结构[M]. 田　果,刘丹宁,译. 北京:人民邮电出版社,2007.

[8] Satty T. L. How to Make a Decision: The Analytic Hierarchy Process [J]. European Journal of Operational Research,1990(48):9-26.

[9] 汪培庄. 模糊系统理论与模糊计算机[M]. 北京:科学出版社,1996.

[10] Zimmermann H J. Fuzzy Set Theory and its Applications[M]. Berlin, Germany: Springer,1996.

[11] 冯登国,张　阳,张玉清. 信息安全风险评估综述[J]. 通讯学报,2004,25(7):10-18.

[12] 范　红,冯登国,吴亚非. 信息安全风险评估方法与应用[M]. 北京:清华大学出版杜,2006.

[13] 李　杨,聂晓伟,杨鼎才. 一个基于等级保护的有效风险评估方法[J]. 计算机应用研究,2005,22(7):39-41.

[14] 邓　平,范科峰,张素兵,等. 一种安全操作系统风险评估模型[J]. 计算机工程,2011,37(9):57-58.

[15] 姜政伟,赵文瑞,刘　宇,等. 基于等级保护的云计算安全评估模型[J]. 计算机科学,2013,40(8):151-156.

编辑　刘　冰　陆燕菲