·安全技术· 文章编号：1000-3428(2019)04-0142-06 文献标志码：A 中图分类号：TP391

基于云模型与决策树的入侵检测方法

郭 慧[1]，刘忠宝[2]，柳 欣[1]

（1. 山西大学商务学院 信息学院，太原 030031；2. 中北大学 软件学院，太原 030051）

摘 要： 针对入侵检测系统中传统决策树分类算法仅能处理离散化数据的情况，提出一种改进的入侵检测方法。通过云模型对数据集连续属性进行离散化，利用遗传算法引入加权选择概率函数，使得决策树分类算法能检测出 DoS、R2L、U2R、PRB 攻击。KDDCUP 99 数据集上的实验结果表明，与基于贝叶斯、支持向量机与云模型离散化的检测方法相比，该方法具有更好的入侵检测与分类性能。

关键词： 云模型；决策树；离散化；遗传算法；入侵检测；连续属性

开放科学（资源服务）标志码（OSID）：

中文引用格式： 郭慧，刘忠宝，柳欣. 基于云模型与决策树的入侵检测方法[J]. 计算机工程，2019，45(4)：142-147.

英文引用格式： GUO Hui，LIU Zhongbao，LIU Xin. Intrusion detection method based on cloud model and decision tree[J]. Computer Engineering，2019，45(4)：142-147.

Intrusion Detection Method Based on Cloud Model and Decision Tree

GUO Hui[1]，LIU Zhongbao[2]，LIU Xin[1]

（1. School of Information，Business College of Shanxi University，Taiyuan 030031，China；
2. School of Software，North University of China，Taiyuan 030051，China）

【Abstract】 Aiming the problem that the traditional decision tree classification algorithm in intrusion detection system can only deal with discrete data，an improved intrusion detection method is proposed. The cloud model is used to discretize the continuous attribute of datasets and the genetic algorithm is used to introduce the weighted selection probability function so that the decision tree classification algorithm can detect the attack of DoS，R2L，U2R and PRB. Experimental result of the KDDCUP 99 dataset shows that this method has better intrusion detection and classification performance compared with detection method based on Bayes，Support Vector Machine（SVM）and cloud model discretization.

【Key words】 cloud model；decision tree；discretization；genetic algorithm；intrusion detection；continuous attribute

DOI： 10.19678/j.issn.1000-3428.0052276

0 概述

计算机网络是信息传输、交换和资源共享的虚拟平台。网络安全是其重要的研究领域[1]。入侵检测系统（Intrusion Detection System，IDS）能保护自动化入侵检测过程的系统免受各种攻击威胁，保证其机密性、完整性和可用性。由于网络流量的特殊性，因此在 IDS 上下文中分析网络流量和机器学习是一项具有挑战性的任务。IDS 处理的数据集具有多层次（不同类型的攻击）、多功能（多个网络流量属性）、高度不平衡（许多网络流量正常，但极少有罕见攻击实例）的特点。IDS 的核心算法是对入侵数据进行分类。决策树分类算法不仅具有良好的分类效果，还结合了决策树的决策规则简单、便于理解的特点。然而，该算法通常会生成结构复杂的决策树，而且只能处理离散化的数据。在实际生活中存在大量的连续属性数据，数据集的连续属性离散化成为分类挖掘的一个前置处理过程。针对以上决策树分类算法中存在的问题，本文在分析与比较各种连续属性离散化方法的基础上，引入基于云模型的连续属性离散化方法，解决传统决策树分类算法不能处理连续属性的问题。另外，根据遗传算法具有全局优先搜索的特点，将遗传算法运用到决策树算法中，对决策树分类算法进行优化。

基金项目： 山西省自然科学基金（201601D011042）。

作者简介： 郭 慧（1980—），女，讲师、硕士，主研方向为网络安全、人工智能；刘忠宝，副教授、博士；柳 欣，副教授、硕士。

收稿日期： 2018-07-31 **修回日期：** 2018-09-26 **E-mail：** guozihui80@163.com

1　相关概念

1.1　云模型

云模型是一种定量数值和定性概念之间可以进行双向转化的认知模型,既可从定量数值转化为定性概念,也可从定性概念转化为定量数值[2]。云模型有 3 个数字特征,分别为期望 Ex、熵 En 和超熵 He[3]。云滴构成的随机变量 x 的期望为 $E(x)=Ex$,方差为 $D(x)=En^2+He^2$,其中,Ex 代表图形中心值,En 代表云滴距离中心值的远近程度,He 代表云层的厚度。在 $Ex=25$、$En=1$、$He=0.1$ 下的云模型示意图如图 1 所示。

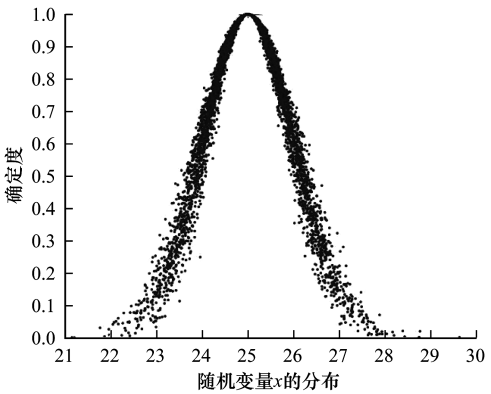

图 1　$Ex=25$、$En=1$、$He=0.1$ 下的云模型示意图

1.2　决策树

决策树(Decision Tree,DT)是决策支持系统的分类模型[4]。内部节点($f_1,f_2,\cdots,f_n$)表示测试条件数据集中实例的属性值,其目的是推断实例所属的类。每一片叶子代表一个类[5]。根节点($Root$)对实例的某一属性进行测试,并将实例分配到相应的叶子节点(A,B,C)[6],具体如图 2所示。

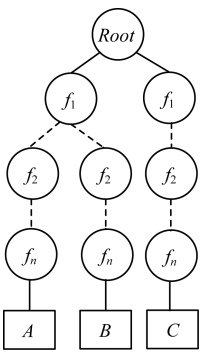

图 2　决策树示意图

每个分支从树的根部到叶子,可以表示为:

$\text{if}(f_1=v_1 \wedge f_2=v_2 \wedge \cdots \wedge f_n=v_n)$

$\text{then}\{Class=C\}$

其中,if 子句中的条件是多个分支节点的联合,输出的是分类,用叶子节点表示[7]。规则的 if 部分作为先行词,用序列 < 特征,运算符,值 > 表示。

1.3　遗传算法

遗传算法引入达尔文进化原理,从代表问题可能潜在的解集的种群开始,一般由以下基本步骤组成[8]。

步骤 1　初始化 M 个个体,种群为 $P(0)$,初始化进化代数为 $t=0$,t 的最大值为 T。

步骤 2　对群体进行选择运算,把优化的个体直接遗传到下一代或通过配对交叉产生新的个体再遗传到下一代。

步骤 3　对群体进行交叉运算。

步骤 4　对群体个体串中某些基因值做改动。

步骤 5　群体 $P(t)$ 经过选择、交叉、变异运算后得到下一代群体 $P(t+1)$。

终止条件判断:若 $t=T$,则以进化过程中得到的具有最大适应度的个体作为最优解输出,终止计算。遗传算法是一种优化机制,可以提高分类模型的性能。

2　评估指标

入侵检测方法的评估指标具体如下:

TP_i:被正确分配到第 i 类中的样本数。

FP_i:其他类被错误分配到第 i 类的样本数。

FN_i:第 i 类中的样本数,但被错误分配到其他类中。

精度:$precision_i=\dfrac{TP_i}{TP_i+FP_i}$。

召回率:$recall_i=\dfrac{TP_i}{TP_i+FN_i}$。

准确率:$accuracy=\dfrac{\sum_{i=1}^{|C|}TP_i}{N}$。

平均度量值用于测量预测值与召回值之间的平衡关系。

$$Mean\ \ F\text{-}measure=\frac{\sum_{i=1}^{|C|}F\text{-}measure_i}{|C|}$$

$$F\text{-}measure=\frac{2Recall_i\cdot Precision_i}{Recall_i+Precision_i}$$

3　入侵检测方法

由于决策树只能处理离散属性,因此将云模型用于数据集 KDDCUP 99 的连续属性离散化。同时,为进一步提高分类准确度,利用遗传算法进化决策树种群,优化分类模型。将云模型、决策树和遗传算法相结合,用于生成入侵检测规则。检测规则便于理解,且检测精度高。

3.1　连续属性离散化

本文利用云变换将连续属性的个体域分解为多个云所对应的区域。云模型可以将属性值同时映射到多个区间上,每个区间具有不同的隶属度,符合边界模糊性。基于云模型的连续属性离散化算法流程如图 3所示。

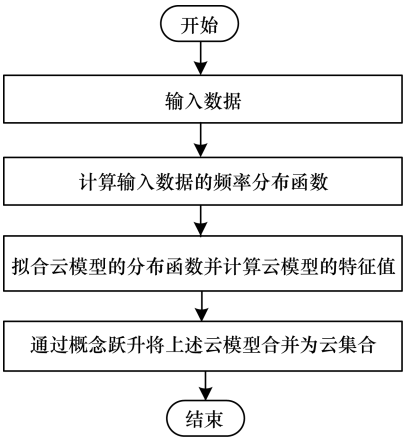

图 3 基于云模型的连续属性离散化算法流程

输入为条件属性 $G_k, k=1,2,\cdots,m$,定义域为 $[g_1,g_m]$,输出为离散化的若干个云的集合(属性值)。具体离散化步骤如下:

步骤 1 对于属性取值 G_k 定义域中的每一个可能属性值 $x, x\in[g_1,g_m]$,计算属性 $[g_1,g_m]$ 范围内 G_k 等于该属性值 x 的数据个数 y,由此得出 G_k 的频率分布函数 $g(x)$[9]。

步骤 2 根据步骤 1 得到的属性值频率分布函数 $g(x)$,确定 $g(x)$ 具体的波峰值。波峰值定义为第 i 个云的期望值 $Ex_i(i=1,2,\cdots,n)$。计算以 Ex_i 为期望,用于拟合为 $g(x)$ 的云模型分布函数 $g_i(x)$。

步骤 3 从频率分布函数 $g(x)$ 中去除步骤 2 得到的第 i 个云模型的数据分布函数 $g_i(x)$,由此得出一个新的属性值频率分布函数 $g(x)$,重复步骤 2、步骤 3,得出若干基于云模型的频率数据分布函数。

步骤 4 得出误差函数 $g'(x)$ 和各个云模型的属性值频率分布函数 $g_i(x)$,计算基于云模型的定性概念的 3 个特征值以及含混度。

步骤 5 通过概念跃升,将步骤 4 得到的所有云模型合并为 7±2 个云组成的云集合。

步骤 6 按照含混度顺序,对每个正态云的含混度 CD 进行判断,取含混度阈值为 0.500 4,在含混度为 0.500 4 时,相邻概念间的基本区不会有交叉区。如果 $CD>0.500\ 4, k=1,2,\cdots,n$,则概念数 $n=n-1$,跳转至步骤 2;否则,输出 n 个含混度小于等于 0.500 4 的正态云。

从步骤 6 中可看出,每次变换的结果中只要出现一个概念的含混度大于 0.500 4,概念的数目就要减少 1 个,重复上述步骤,反复调用云变换算法,直至满足终止条件为止。

3.2 决策树进化

3.2.1 初始种群生成

初始种群由最小决策树组成,只能对一类中的实例进行分类且节点条件正确[10],且初始种群的树中没有分支。如果将任何数据集实例提交给此类树,则所有属性都将满足节点上的条件,因此,分类结果为树中叶子节点的值。决策树通过交叉和变异逐步进化。

初始种群尺寸 $|p|$ 由数据集中的类别数 $|C|$ 和每类中的个体数 λ 得出,具体如式(1)所示。

$$|p|=|C|\cdot\lambda \tag{1}$$

DT 节点序列是个体分类准确度的一个重要方面。决策节点优先级由信息增益驱动。本文利用 infoGainAttributeEval 以信息增益为依据对属性值进行评估。通过将重要的决策节点放置在接近根(*Root*)的位置构造个体,测试条件数据集中实例的属性值 $(f_1,f_2,\cdots,f_n)$ 按照信息增益从大到小的顺序进行排序 $(f_{i1},f_{i2},\cdots,f_{in})$,如图 4 所示。一旦创建初始种群,其将作为遗传进化过程的一个输入来执行进化过程,使个体分类准确率达到最高。

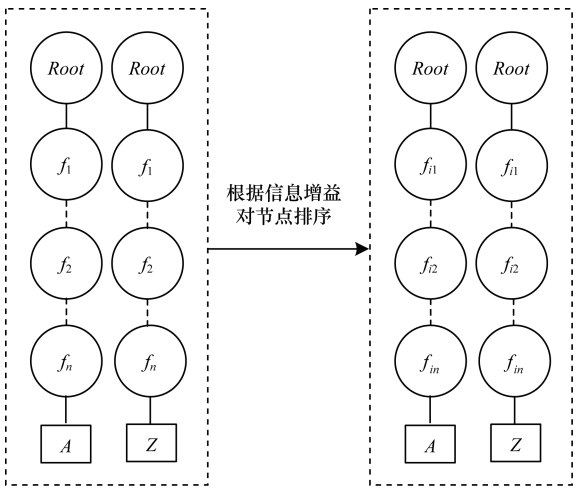

图 4 初始种群生成过程

3.2.2 选择算子

遗传算法涉及一个逐步的选择过程,选择过程由概率方法驱动[11]。选择的父节点 $\{parent_1, parent_2\}$ 将在之后步骤中进行交叉和变异构造 2 个新的个体[12]。

连续属性经过云模型变换形成二进制位串的消息。由于云模型的不确定性,属性在一定程度上属于多个云,即属于不同消息[13]。

定义 1 属性数据 $x_k=\{x_{k1},x_{k2},\cdots,x_{kn}\}$ 与消息 M_i 的符合度为:

$$\mu_i(x_k)=\min\{\mu_{i1}(x_{k1}),\mu_{i2}(x_{k2}),\cdots,\mu_{in}(x_{kn})\} \tag{2}$$

其中,$\mu_{ij}(x_{kj})$ 为属性数据 x_{kj} 与消息 M_i 中云 A_{kj} 的符合度。

根据云模型的隶属度计算公式,属性数据 x_{kj} 与云 $A_{ij}(Ex,En,He)$ 的符合度 $\mu_{ij}(x_{kj})$ 计算具体如下:

1)以 En 为期望、He 为方差,计算得到一个正态随机数 En'。

2)计算符合度值 $\mu_{ij}=e^{\frac{-(x-Ex)^2}{2(En')^2}}$。

根据式(2)及选择规则 $R=\max\{\mu_i(x_k)\times F(\tau_i)\}$,得到选择规则具有与数据符合度及选择概率乘积的最大值。

种群中每个个体 τ_i 的选择概率计算如下:

$$F(\tau_i)=\alpha\cdot g_1(\tau_i)+\beta\cdot g_2(\tau_i)+\gamma\cdot g_3(\tau_i) \quad (3)$$

其中,$g_1(\tau_i)\in[0,1]$是第 i 代个体的实际适应度函数,$g_2(\tau_i)\in[0,1]$是第 i 代个体基于类的选择函数,$g_3(\tau_i)\in[0,1]$是个体缺失的类函数,$\alpha,\beta,\gamma\in[0,1]$分别是 g_1、g_2、g_3 的权重,$\alpha+\beta+\gamma=1$。

进化论中的适应度 $g_1(\tau_i)$用来度量群体中的个体分类能力,根据所求问题的目标函数进行评估。模型采用平均度量值(Mean F-measure)作为适应度函数,平等对待数据集中的类。Mean F-measure 保证了召回率和精度的平衡。召回率和精度分别考虑了 FNS 和 FPS[14]。基于类的选择函数 $g_2(\tau_i)$使得个体包含更多的少数类,最大化非数据集的选择概率。

$$g_2(\tau_i)=\sum_{j=1}^{|C|}\left((1-p_j)\frac{|l_j|}{|l|}\right) \quad (4)$$

其中,$|C|$表示数据集中类的个数,p_j 表示数据集中第 j 代分类实例占比,$|l_j|$表示第 j 代个体 τ_i 的类别数,$|l|$表示个体 τ_i 的类别数。

缺失的类函数 $g_3(\tau_i)$的目标是使包含缺失类的最优个体选择概率最大。

$$g_3(\tau_i)=\frac{\sum_{j=1}^{m}(|l_j|)}{|l|} \quad (5)$$

其中,m 为最优个体缺失类的数目。

为调整系统结果,在 $F(\tau_i)$方法中,α、β、γ 分别为 g_1、g_2、g_3 的权重,α、β 在初始化过程中进行调整。当且仅当最优个体有缺失类时,γ 是非零值。当最优个体为正常时,决策树的叶子代表所有的类别,$\gamma=0$。

$$\gamma=1-\frac{m}{|C|}(\alpha+\beta) \quad (6)$$

其中,α 和 β 权重互补($\alpha+\beta=1$),而且在种群进化过程中逐渐变化。为增加选择概率,生成的叶子较少,初始配置可以设置较高的 β 值(例如 $\alpha=0.05$ 和 $\beta=0.95$)。通过进化最终达到 $\alpha=1$ 和 $\beta=0$。在渐进过程中,当且仅当最优个体中有丢失类时,从式(6)可以推断,基于数据集中 $|C|$类的总和及最优个体中的缺失类数 m,γ 得到特定的值。当 $\gamma\neq0$ 时,为满足 $\alpha+\beta+\gamma=1$,α 和 β 都要进行归一化处理,具体计算如下:

$$\alpha=\alpha\cdot\frac{m}{|C|} \quad (7)$$

$$\beta=\beta\cdot\frac{m}{|C|} \quad (8)$$

传统分类方法忽略了数据集的次要类,分类精度较低。为解决该问题,引入选择函数 $F(\tau_i)\in[0,1]$,结合 α、β、γ 的权重,引入 α、β、γ 时考虑到数据集的次要类,按顺序引入 γ 比重可保证数据集中所有类的存在,提高分类准确度。初始决策树是单类,最终的分类模型能够推断出所有类的实例,从而通过进化保证所有类的存在。采用轮盘选择技术选择父母节点,可提高选择的可能性,并考虑到少数类的选择可能性。

3.2.3　深度选择

深度选择利用均值为 μ 的高斯分布,μ 从 0 变化到决策树的最大深度(最大深度为数据集 $|F|$属性的总和)。每选中 2 个父母,μ 加 1。当 μ 达到最大值时,重新初始化为 0。父母节点将在更高的叶子节点上重新开始交叉和变异。标准差 σ 做相应调整。深度选择方法的目标是逐步在多个层次(节点)上创建分支个体,以更有效的方式探索问题的搜索空间。

3.2.4　交叉算子

交叉算子应用于 2 个父节点。进化策略综合个体特征,通过在选定的个体之间按照交叉概率和决策树的深度交换随机选择分支,构造高方差个体。将虚线分支交叉,产生 2 个新的个体,$f_1,f_2,\cdots,f_n$ 表示测试条件数据集中实例的属性值,根节点为 *Root*,叶子(A、B、C)代表该实例的分类,如图 5 所示。

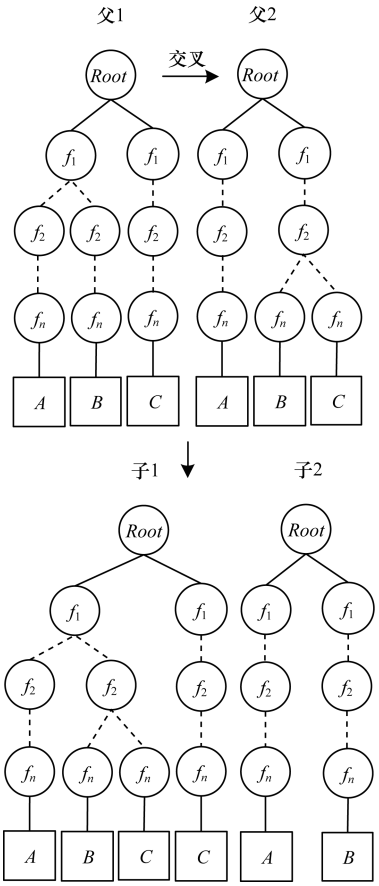

图 5　交叉操作

3.2.5　变异算子

变异算子应用于交叉个体中,在特定个体上创建新的分支,属性值 f_1 的值集由$\{v_1,v_2,v_3,v_4\}$变异为 2 个集合$\{v_1,v_2,v_3\}$、$\{v_4\}$,如图 6 所示。一个数据集属性由一个节点代替,数据集中的属性是离散或连续,变异操作需要将特定节点分离,并引入云模型对连续属性进行离散化。

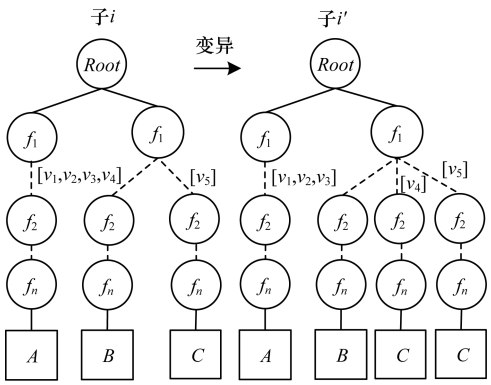

图 6 变异操作

每个分离决策点属性根据信息增益产生新的分支。如果一个分裂点不能再分,或者它不能产生信息增益,则不能应用变异操作。在交叉过程中,突变基于特定的突变概率和由深度选择过程决定的突变深度。变异个体将加入临时种群。交叉和变异操作重复进行,直到临时种群的尺寸达到初始种群为止。

3.2.6 种群替换

在初始种群和临时种群之间,选择最适合的个体形成下一代种群,继续进化。在该过程中,计算每一个个体的分类准确率。每个个体按照数据符合度以及选择概率的乘积进行排序,具有最高乘积的个体最终移到下一代种群中作为进化过程的输入。

在替换过程中,检查种群中可能缺失的类。如果有缺失类,则继续从先前的种群中添加额外的个体,使得个体中包含缺失的类。在下一代种群中,增加相同个体的实例,该类在进化过程中被选择为父类的概率以及下一代种群中个体的数量。当算法满足迭代次数、分类精度的特定值时,得到最终模型并对攻击类型进行分类。

4 实验结果与分析

本文采用 KDDCUP 99 数据集对本文提出的入侵检测方法和传统入侵检测方法进行对比分析。

4.1 评测数据集

KDDCUP 99 是一个标准的入侵检测数据集,分为 5 个主要类别:正常类(Normal),拒绝服务(DoS),探测监控手段(PRB),未经授权的远程访问(R2L),未经授权的本地访问(U2R)[15-16]。从数据集中选取 U2R 50% 的实例,其他类别选取 10% 的实例,从部分数据集中删除所有重复项。手工提取 flag、service、src _ byte、dst_byte、dst_host_srv_count、diff_srv_rate 条件属性作为分类对象。预处理后的典型数据如表 1 所示。

表 1 预处理后的典型数据

flag 属性	service 属性	src_byte 属性	dst_byte 属性	dst_host_srv_count 属性	diff_srv_rate 属性	数据所属类别
S0	telnet	0	0	0.13	15	1
S1	telnet	490	3 525	0.00	17	0
RSTO	telnet	126	179	0.00	19	2
REJ	private	0	0	0.57	1	4
SF	time	0	4	0.00	2	3

在表 1 中,第 7 列为每个数据所属的分类,其中,0 代表正常连接,1 代表 DoS 攻击,2 代表 R2L 攻击,3 代表 U2R 攻击,4 代表 PRB 攻击。由于预处理后的部分数据属性为连续属性,需要对连续属性离散化,以适应决策树分类算法的要求。数据离散化后的典型数据如表 2 所示。在表 2 中,每个属性经过离散化后再编码成6 位二进制数。以第 1 条数据为例,该数据的 flag 属性编码为 000011,service 属性编码为 000101,以此类推,类别为 DoS 攻击。利用离散化后的数据对决策树分类器进行训练得到分类模型。

表 2 数据离散化后的典型数据

flag 属性编码	service 属性编码	src_byte 属性编码	dst_byte 属性编码	dst_host_srv_count 属性编码	diff_srv_rate 属性编码	数据所属类别
000011	000101	000000	000000	000101	000010	1
000001	000101	000101	010000	000000	000010	0
000101	000101	000010	000001	000000	000010	2
000111	001010	000000	000000	001010	000000	4
000000	001010	000000	000000	000000	000000	3

4.2 结果分析

本文模型采用平均度量值作为适应度函数,KDDCUP 99 迭代 1 350 次,测试数据集混淆矩阵及精度与召回率见表 3、表 4。入侵检测分类精度见图 7。入侵检测召回率、准确率与平均度量值见表 5、表 6。

表 3 测试数据集混淆矩阵

数据集	Normal	DoS	PRB	U2R	R2L
Normal	78 259	291	202	17	280
DoS	440	48 440	235	0	0
PRB	72	220	1 620	4	2
U2R	2	2	0	22	0
R2L	78	11	2	1	807

表 4　测试数据集检测精度与召回率　%

数据集	精度	召回率
Normal	99.25	99.00
DoS	98.93	98.63
PRB	78.68	84.46
U2R	50.00	84.62
R2L	74.10	89.77

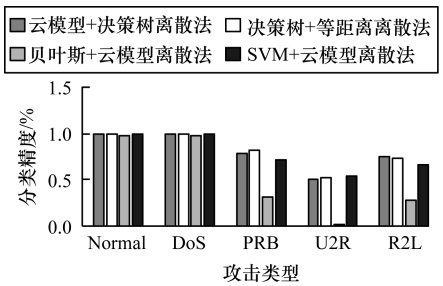

图 7　入侵检测分类精度

表 5　入侵检测召回率　%

入侵检测方法	Normal	DoS	PRB	U2R	R2L
云模型 + 决策树离散法	99.00	98.63	84.46	84.62	89.77
决策树 + 等距离离散法	99.38	98.93	69.86	76.92	88.65
贝叶斯 + 云模型离散法	95.59	92.82	54.22	76.92	66.41
SVM + 云模型离散法	99.13	98.93	64.65	80.77	88.43

表 6　入侵检测准确率与平均度量值　%

入侵检测方法	准确率	平均度量值
云模型 + 决策树离散法	98.58	84.68
决策树 + 等距离离散法	98.70	83.20
贝叶斯 + 云模型离散法	93.74	55.05
SVM + 云模型离散法	98.47	81.29

综上所述,本文提出的基于云模型和决策树的离散化入侵检测方法的平均度量值优于其他方法,分类准确率也较高,是一种有效的入侵检测与分类方法。

5　结束语

现有入侵检测方法只能处理 IDS 中的离散属性,为此,本文引入云模型对连续属性进行离散化,同时通过遗传算法对决策树进行优化,降低决策树的复杂度。通过 KDDCUP 99 数据集验证了该入侵检测方法的有效性。本文在属性选择方面,根据经验手工选择了 21 个属性。下一步将对离散属性选择方法进行优化,提高入侵检测算法的通用性。

参考文献

[1] WANG P,CHAO K M,LIN H C,et al. An efficient flow control approach for SDN-based network threat detection and migration using support vector machine[C]//Proceedings of IEEE International Conference on E-business Engineering. Washington D.C.,USA:IEEE Press,2016:56-63.

[2] 秦昆,李德毅,许凯. 基于云模型的图像分割方法研究[J]. 测绘信息与工程,2006,31(5):3-5.

[3] 宋运忠,范丽媛. 基于云变换的混沌动力系统逼近性研究[J]. 河南理工大学学报(自然科学版),2015,34(5):659-664.

[4] LI J,MA S,LE T,et al. Causal decision trees[J]. IEEE Transactions on Knowledge and Data Engineering,2017,29(2):257-271.

[5] CATALTEPE Z,EKMEKCI U,CATALTEPE T,et al. Online feature selected semi-supervised decision trees for network intrusion detection[C]//Proceedings of IEEE/IFIP Network Operations and Management Symposium. Washington D.C.,USA:IEEE Press,2016:1085-1088.

[6] XIANG C,YONG P C,MENG L S. Design of multiple-level hybrid classifier for intrusion detection system using Bayesian clustering and decision trees[J]. Pattern Recognition Letters,2008,29(7):918-924.

[7] BARROS R C,BASGALUPP M P,DE CARVALHO A C P L F,et al. A survey of evolutionary algorithms for decision-tree induction[J]. IEEE Transactions on Systems,Man,and Cybernetics,Part C,2012,42(3):291-312.

[8] SOLTANI H,SHAFIEI S. Adiabatic reactor network synthesis using coupled genetic algorithm with Quasi linear programming method[J]. Chemical Engineering Science,2015,137:601-612.

[9] WANG J Q,PENG J J,ZHANG H Y,et al. An uncertain linguistic multi-criteria group decision-making method based on a cloud model[J]. Group Decision and Negotiation,2015,24(1):171-192.

[10] BONDARENKO A,ALEKSEJEVA L,JUMUTC V,et al. Classification tree extraction from trained artificial neural networks[J]. Procedia Computer Science,2017,104(C):556-563.

[11] ROSTAMI M,MORADI P. A clustering based genetic algorithm for feature selection[C]//Proceedings of the 6th Conference on Information and Knowledge Technology. Washington D.C.,USA:IEEE Press,2014:112-116.

[12] 袁琴琴,吕林涛. 基于改进蚁群算法与遗传算法组合的网络入侵检测[J]. 重庆邮电大学学报(自然科学版),2017,29(1):84-89.

[13] 韩伟,马邕文,万金泉,等. 基于云模型在废水处理 pH 控制中的仿真研究[J]. 计算机仿真,2015,32(5):432-440.

[14] SINGH 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.

[15] 郝晓弘,张晓峰. 入侵检测分类技术的比较研究[J]. 微型机与应用,2017,36(15):8-11,15.

[16] ABDELRAHMAN S M,ABRAHAM A. Intrusion detection using error correcting output code based ensemble[C]//Proceedings of the 14th International Conference on Hybrid Intelligent Systems. Washington D.C.,USA:IEEE Press,2014:181-186.

编辑　陆燕菲