入侵检测灰色空间模型及应用

彭云峰[1]，何模雄[2]，隆克平[1,2]

(1. 北京科技大学计算机与通信工程学院 北京 海淀区 100083;

2. 电子科技大学通信与信息工程学院 成都 611731)

【摘要】建立了基于粗糙集理论的入侵检测灰色空间模型，根据信息增益设计等价类获取和约简算法，提出了一种新的入侵检测系统模型。运用KDDCUP99数据集对网络入侵检测进行了测试。分析和对比实验结果表明，该模型具有分类规则简单、检测时间短和准确率高等特点，克服了检测系统不能有效判别未知行为的瓶颈。

关 键 词 灰色空间模型; 信息增益; 入侵检测; 粗糙集理论; 白化处理

中图分类号 TP393.08 文献标识码 A doi:10.3969/j.issn.1001-0548.2012.03.025

Gray Space Model and Application for Intrusion Detection

PENG Yun-feng[1], HE Mo-xiong[2], and LONG Ke-ping[1,2]

(1. School of Computer and Communication Engineering，University of Science and Technology Beijing Haidian Beijing 100083;

2. School of Communication and Information Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract An intrusion detection gray space model is presented based on rough set theory. Information gain is used to equivalence rule discovery and reduction algorithm. As a result, a new intrusion detection model is designed. According to the analyses and validation based on KDDCUP 99, the experimental results show that the model is good for networks intrusion detection with simple classification rules, short detection time and high detection accuracy, and it overcomes the bottleneck that the detection system can not effectively determine the unknown behavior.

Key words gray space model; information gain; intrusion detection; rough set theory; whitening process

入侵检测系统(intrusion detection system, IDS)是深度防御体系的关键技术。从1980年出现入侵检测概念至今，该技术已经从单学科研究转向交叉学科研究，从集中式管理模式延伸到分布式代理模式，从基于主机的入侵检测架构扩展到基于网络的入侵检测架构[1-2]。但于大部分IDS认为所有的行为模式都可以有效、绝对地划分为自我(合法用户、程序、服务等)与非我(非法的用户、程序、服务等)的对立关系[3]，却忽略了实际应用中知识的不完备性和动态性。因而当前的IDS只能对其经验范围内的行为做出准确判断，而对未知行为无能为力。由这些不能被检测系统有效识别的行为模式将构成一个灰色空间，是导致IDS具有较高漏报率和虚警率的根本原因。因此，建立入侵检测灰色空间的数学模型并提出有效的处理机制是提高IDS检测率的关键。

文献[4]提出的粗糙集理论是解决不确定、不完备、不精准数学问题的新方法。因为无需提供问题所需处理数据集合之外的任何先验信息，所以对问题的处理比较客观[5]。在入侵检测方面，粗糙集理论也已有了一些应用。文献[6]将粗糙集和混合遗传算法用于网络入侵检测，改进了传统网络IDS的检测性能。文献[7]提出一种结合粗糙集和支持向量机的分类器生成方法，提高了分类能力。文献[8]将粗糙集理论和隐马尔可夫模型用于异常检测缩短了训练时间。这些研究表明，粗糙集用于IDS不确定信息的处理具有明显的效果。

但是对不确定的灰色空间的准确描述还需要约简属性，挖掘分类规则。虽然一个数据集的所有约简可以通过粗糙集理论构造的分辨矩阵及其导出的分辨函数化简而得到，但寻找所有约简或者最小约

收稿日期：2010－02－15； 修回日期：2010－11－27

基金项目：国家自然科学基金(61071101)

作者简介：彭云峰(1971－)，男，教授，主要从事互连网络的生存性设计和应用等方面的研究.

简都已被证明是NP问题。由于信息增益不但在属性约简、规则生成时计算简单，而且可以对属性的重要性进行了排序和生成最小决策树等优点，使其成为目前最有影响和使用最多的一种数据挖掘技术之一。文献[9]对基于信息增益生成的决策树进行了评估，通过与基于卡方和基尼系数生成的决策树相比，证明该方法不仅具有很高的分类精度，分类器的训练时间也更短。文献[10]提出了一种基于粗糙集的理论的信息增益决策树生成法，有效地解决了子树可能在一棵决策树中重复多次出现的问题，提高了分类效率。

为了控制误报率和虚警率，本文提出一种基于灰色空间模型的入侵检测系统架构。其基本思想是根据粗糙集理论建立入侵检测灰色空间模型，将已知入侵行为、已知正常行为和未知行为进行了分离处理。新的检测方案设有异常检测模块和误用检测模块，同时兼具了两种检测方法的优点，用于提高系统对已知行为的检测率；灰色空间和白化处理方法的引入，改变了传统IDS二值分类法的缺陷，降低了系统对不确定行为误判的风险；采用信息增益对检测行为等价关系进行挖掘和约简，继而简化分类规则，减少计算步骤，提高检测的实时性。

1 灰色空间模型

1.1 基本思想

总体而言，根据分析方法的不同，入侵检测可分为误用检测和异常检测两类。误用检测通过匹配攻击特征来发现入侵，而异常检测则是通过分析被检测行为是否违背正常模式来判断攻击发生与否。误用检测能够检测到大部分已有的攻击，异常检测也可以在一定程度上发现新的攻击。

规则库或特征库是IDS的核心，精确定义安全行为模式是IDS准确判定每一个行为对象的前提条件。但复杂、多变的检测环境决定了认知的局限性和知识获取的不完备性。因而在实际检测时，IDS并不能如愿地将所有检测对象都进行有效的分类。异常检测容易将正常业务误认为是攻击，误用检测也不能检测到新的攻击，即存在这样一些行为模式——利用已有的知识既不能绝对地将它们判定为安全，也不能绝对地判定为危险，如果武断地对其判别就存在误判的风险。

波兰数学家Z.Pawlak于1982年提出粗糙集理论，给出了该类不确定、不精准、不完备数学问题的一般性研究方法。其主要思想是利用等价类，将每一个不确定的概念X用一对精确的概念来描述，即X的下近似和X的上近似，并把那些无法确认的对象都归集到边界域进行处理。

按照上述思想可以建立一个不确定集合的属性模型并据此设计新的检测系统。与传统IDS的二值对立分类法截然不同，新的系统将整个行为空间分为已知安全模式、已知攻击模式和未知模式3个子集。并分离出在已有知识范围内不能进行准确判别的模式集合进行单独处理。为了形象地区分表征安全的白色和表征危险的黑色，称其为灰色空间。新系统工作流程如图1所示。

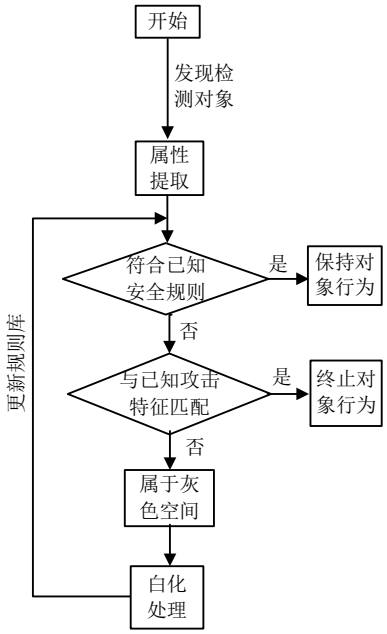

图1 基于灰色空间模型的入侵检测系统工作流程

IDS一开始处于低功耗的休眠状态，当且仅当待检测行为发生时才会被触发。该系统首先提取分类所需的特征并初始化数据。然后IDS启动异常检测模块，根据第一步获得的数据判断该行为是否正常，如果正常则检测终止，并保留此行为；如果检测未通过，则IDS进入下一环节，误用检测模块判断其是否为攻击。若发现提取的特征向量与库中的某一特征向量相匹配，则认为攻击发生，立即予以报警和阻止并结束检测；否则该行为只能属于灰色空间。系统随后检测对象白化处理并返回新的判决规则，更新规则库。

1.2 灰色空间模型的建立

IDS的对象论域M就是所有需要检测的行为构成的集合。为了描述和区分这些行为需选择既定的指标。在IDS的设计中，这些指标就是行为对象的等价关系(或属性)。但根据适用场景的不同，需要采集

的属性也会有所不同。如基于主机的误用检测系统需要通过审计系统日志、CPU利用率、内存占用情况等主机特征来检测主机运行是否正常；而基于网络的异常检测系统则主要通过sflow数据来表征网络的状况。

对象论域M可以被一组等价关系$A=[a_1, a_2, \cdots, a_n]$分成若干个等价类$[x]_A$，且使同属一个等价类的两元素之间不可分辨。IDS信息系统可以表示为：

$$I=(M,A,V,f) \tag{1}$$

式中，A表示由属性及属性值构成的等价关系，用a_j表示属性集A的第j个属性，$j=1, 2, \cdots, J$；V表示值域，用$v(a_{ij})$表示第j个属性的第i个取值$j=1, 2, \cdots, J$；$i=1,2, \cdots, I$；f为信息函数，使每一个二元组$(a\in A, x\in M)$，$f(x,a)=V_a$。

划分等价类的目的是为了精确描述对象论域中的特殊子集。然而，并非所有对象论域的子集都能被某些等价类$[x]_A$的并准确定义。IDS中的安全就是一个模糊的概念，没有一组等价关系可以有效地将安全行为集S表示出来。粗糙集理论称这类不可定义集为粗糙集。粗糙集虽然不能用等价关系精确定义，但可以用两个精确集(粗糙集的上近似和下近似)近似表示[11]。

定义 1　设R为对象论域U的等价关系，则粗糙集X的R下近似(R lower approximation)和R上近似(R upper approximation)分别定义为：

$$R\_(X)=\bigcup[x]=\{x\in U,[x]\subseteq X\} \tag{2}$$

即所有能确切地分类到X的等价类的并集。

$$R^-(X)=\bigcup[x]=\{x\mid x\in U,[x]\cap X\neq\phi\} \tag{3}$$

即所有包含x元素的等价类的并集。在粗糙集理论中有 $\mathrm{Pos}_R(X)=R\_(X)$，称为X的R正域。而 $\mathrm{Neg}_R(X)=U-R^-(X)$ 表示完全不属于集合X的元素的集合，称为X的R负域。IDS中粗糙集S可以用其上近似和下近似表示为$(A_(X), A^-(X))$。

因此既不能完全归入S，也不能完全归入 $\overline{S}$ 的元素的集合，即入侵检测灰色空间的数学模型可以表示为：

$$\mathrm{Bnd}_A(S)=A^-(S)-A\_(S)=M-[\mathrm{Neg}_A(S)+\mathrm{Pos}_A(S)] \tag{4}$$

式中，$\mathrm{Pos}_A(S)=A\_(S)$ 表示已知的正常行为模式集合，其规则被异常检测模块用于判断一个行为是否正常；$A^-(S)$ 表示可能安全的行为模式的集合；$\mathrm{Neg}_A(S)$ 表示已知的攻击行为模式的集合，其特征被误用检测模块用来判断攻击是否发生。灰色空间模型示意图如图2所示。

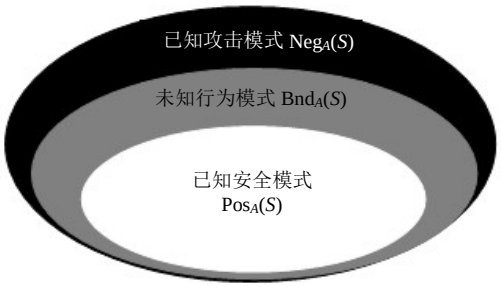

图2 灰色空间模型示意图

确定一个行为是否属于灰色空间，需要利用已有知识即已知的安全模式和攻击模式。因此，应用灰色空间模型将不确定问题转化为确定问题的求解，首先需要获取有效的等价关系A。一个好的等价关系不但可以提高分类器的分类能力，还能缩小灰色空间的规模、充分发挥模型在检测速度上的优势。

2　数据约简和分类器构建方法

为了尽可能有效地描述一个行为模式，IDS往往需要采集海量的信息，但是这些信息中可能存在冗余甚至噪声。因而IDS在对特征库进行持续搜索和匹配运算时，会耗费较多的时间去审核毫无意义的冗余信息，进而加重了系统的负担。为了减轻系统的负担和描述的简洁性，需要约简属性。

基于信息增益的数据挖掘技术是目前最有影响和使用最多的一种数据挖掘技术，它通过决策树的形式展现的规则不仅直观而且属性重要性的排序，有效地解决了模式匹配计算过程中需要提取一切可能属性的缺陷。

2.1　数据初始化

为了统一属性标准和简化计算的复杂度，需要对数据信息初始化。按照各属性的不同取值，它们将按需要被分为n+1个等级，则有：

$$V'(a_{ij})=\begin{cases}0 & v(a_{ij})-(m_j-e_j)\leqslant 0\\ \mathrm{round}\left(n\times\dfrac{v(a_{ij})-(m_j-e_j)}{(m+e_j)-(m-e_j)}\right) & \\ n & v(a_{ij})-(m_j+e_j)\geqslant 0\end{cases} \tag{5}$$

式中，V'为新的值域空间；round表示四舍五入取整；n表示最大分类值；$(m-e)$表示估计最小值，$(m+e)$表示估计最大值，括弧中的分式是归一化的一般计算方法；m和e分别为统计均值和一阶绝对中心矩，其计算公式分别为：

$$m=\frac{1}{L}\sum_{l=1}^{L}v(\alpha_{il}) \tag{6}$$

$$e=\frac{1}{L}\sum_{l=1}^{L}|v(\alpha_{il})-m| \tag{7}$$

2.2 属性约简

属性约简的关键是量化特征的重要性。在信息论中，信息增益(information gain)被用来表示条件选取前后信息熵的变化量。它也被广泛用于决策树生成过程中属性分类能力的衡量。基于信息增益的决策树构建方法已在文献[12]中有了详细的阐述。本文也采用这个统计量来对IDS检测行为对象属性的分类能力进行量化和排序，并构建出分类器。

计算信息增益首先需要计算信息熵，即有：

$$H(D)=-\sum_{k}P(d_k)\log_2 P(d_k) \tag{8}$$

式中，$P(d_k)$表示M的第d_k个等价分类的概率。而第j个属性的分类能力由其条件信息熵表示为：

$$H(D|a_J)=-\sum_{s}P(\alpha_{js})\sum_{k}P(d_k|\alpha_{js})\log_2 P(d_k|\alpha_{js}) \tag{9}$$

那么，第j个属性的信息增益定义为：

$$G(\alpha_j)=H(D)-H(D|\alpha_j) \tag{10}$$

信息增益越大说明属性越重要。

2.3 分类器训练算法

综上所述，算法的计算量主要集中在属性的选择上，也即是信息增益$G(a_j)$的计算。计算的结果是去除冗余属性后，剩下属性按重要性的大小生成的一颗决策树。分类器的训练算法伪代码如下：

INPUT： 训练样本数据
OUTPUT：约简后的属性集构成的决策树

DO 所有的数据去除冗余属性，剩余J个；
FOR 初始化每一个样本；
初始化$m=J$；
REPEAT
FOR 每一个属性a_j，$j=1, 2,\cdots, m$；
分别计算出信息增益$G(a_j)$；
选出信息增益最大的属性a_k作为根节点，并根据子节点的不同取值，将训练集划分为若干等价类；
IF 本属性下的样本不可分辨；
THEN 将该属性设为叶子并停止生成子节点返回本过程；
ELSE 将该属性设为子节点；
FOR 每一个等价类在树中向上追溯至根结点，选出还没有分枝的属性$a_1, a_2,\cdots, a_m$；
对各属性再递归执行本过程。
UNTILL 所有属性不能再向下分类。

2.4 灰色空间的白化处理

在灰色空间模型下，已知行为可以通过异常检测模块和误用检测模块实现有效的检测。分离出来的不确定行为还需要白化处理，本文提出以下3种白化处理的方式：

1) 基于不确定性越大威胁程度越高的思想提出的方式。系统为每一个不确定的行为设置一个ID和TTL。以该行为的ID被建立开始计时，若在达到TTL时依然不能进行判决。那么，系统将其判断为危险当作黑色空间的对象进行处理；

2) 基于生物免疫学中Toll样受体识别病原体的免疫原理[13]设计的方式。当本地出现灰色空间中的未知模式时，可以向邻节点求助，由网络进行群决策；同理，本地节点也参与到其他节点发送的判决请求，并实时更新决策系统，达到规则共享。

3) 特别针对过渡性连接设计的方式。现有的入侵检测主要是入侵结果和入侵过程的检测。更高层次的检测方法应是能检测到入侵的企图。研究发现当一个行为的状态从已知安全域向已知的攻击域过渡时是极度危险的。因此，该方法强调对过渡行为的处理。

3 模型的验证和性能检测

在网络入侵检测方面，为了评估网络入侵检测系统的检测性能，在美国国防高级研究计划署和美国空军研究实验室的赞助下，MIT林肯实验室于1998年成功构造出一套描述网络行为的完整数据集，即KDDCUP99数据集。作为最完整和权威的网络特征数据集，KDDCUP99数据集采用TCP dump的格式，每条记录包含34个数值型字段和7个非数值型字段[14]。

根据前文分类器训练算法得出的分类器为一颗最小决策树，如图3所示。1) 图中圈内的数字i表示第i个属性，属性的排序按样本记录特征顺序给出。如37表示取第37个属性作为判决条件，处于中心的节点13为根节点，是系统进行判决时首先选择的属性。2) 每个节点(叶子除外)有5个分支，按照逆时针方向每个分支分别表明属性取0、1、2、3、4个值，表示该属性初始化的5个等级。3) 节点可具有4种模式状态：① 已知攻击模式(图3中表示为节点所分出的实心圆点)；② 已知安全模式(图3中表示为节点所分出的空心方块)；③ 当前信息不足以判断状态(图3中表示为节点所分出的灰色空心圆点)，需进一步确认，属于灰色空间；④ 根节点13，也属于不确定状态灰色空间。

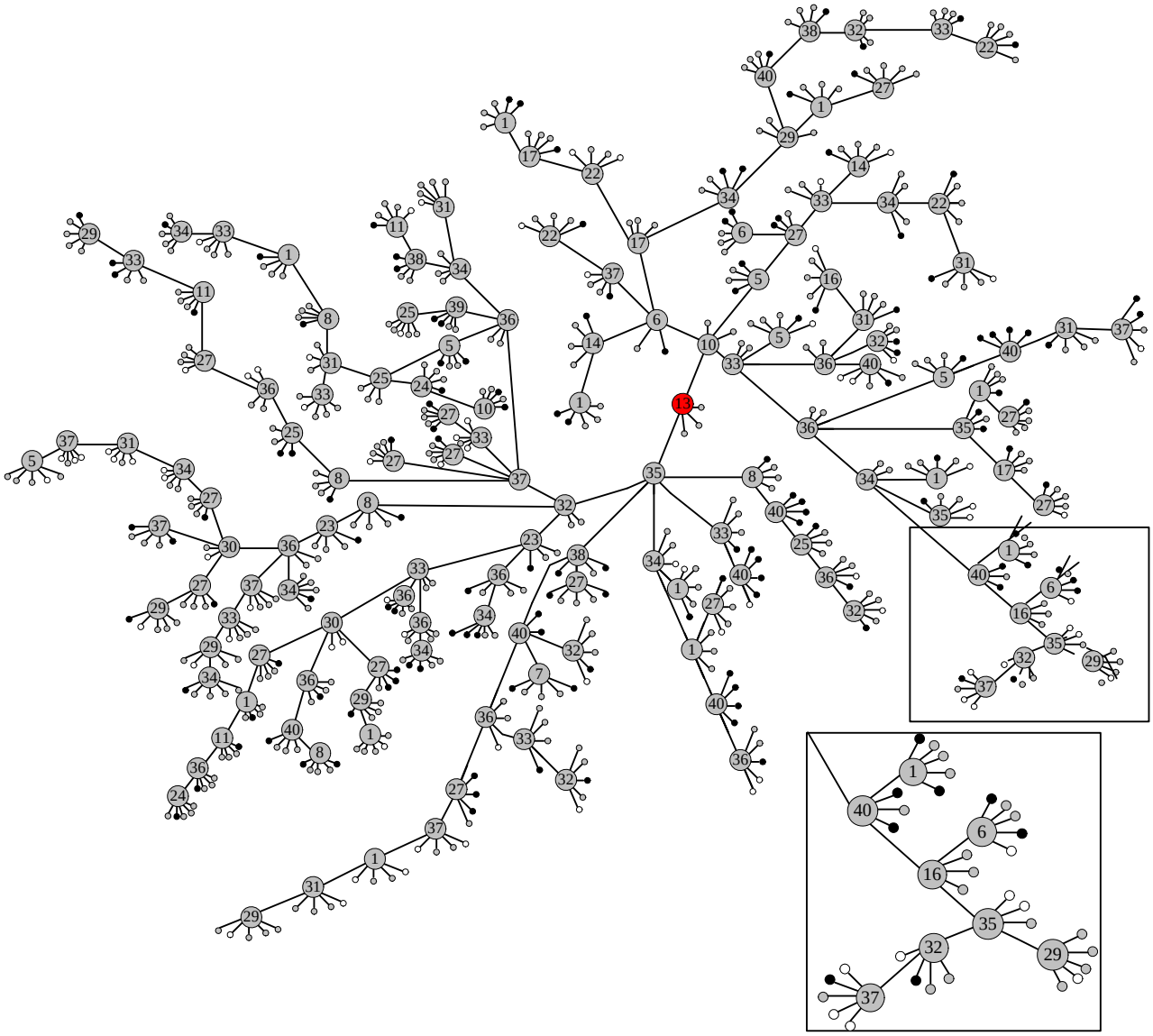

图3　基于灰色空间模型构建的网络入侵检测决策树

本文的实验选取KDDCUP 99中的10%训练样本和corrected测试样本进行实验。在训练过程中精选了各类攻击数据和约3.5万条正常数据，它们分别被标记为Normal、DOS、U2R、R2L、Probe等5大类，在信息增益计算中分别对应d_k＝0,1,2,3,4。训练和测试用到的数据如表1所示。

表1　网络入侵检测实验效果表

检测类别	检测样本数	实测数	误检数	检测率/(%)	误检率/(%)
Normal	4 900	4 722	178	96.37	3.63
DOS	13 010	12 629	381	97.07	2.93
U2R	27	26	1	98.04	1.96
R2L	595	579	16	97.34	2.66
Probe	2 010	1 856	154	92.34	7.64
合计	20 542	19 812	730	96.47	3.53

分类器训练环境为Matlab 7.6 Intel Xeon CPU E7320 2.13 GHz 4 GB内存，测试和环境为Matlab 7.6 Intel Pentium 4 CPU 3.2 GHz 480内存。约简后，网络行为模式空间M的等价关系为A = [1, 5, 6, 7, 10, 12, 13, 15, 17, 21, 25, 27, 29, 31, 32, 33, 34, 35, 36, 37, 38, 40]，少于文献[15]中的29个。

模型用于网络入侵检测时，系统首先收集该连接的信息并初始化。接着根据第12个属性logged_in的值判定该连接所属的域或决定需要读取的下一条属性。如a_{13}=0，说明了下一个需要读取第35条属性dst_host_diff_srv_rate。以此类推，直到没有可选择的属性为止。从图中可以看出最多需要12个步骤就可以得出结论。

实验的结果相对其他方法检测率有了明显地提高[15]，对随机选取的20 542条数据的检测误报率仅为3.53%。

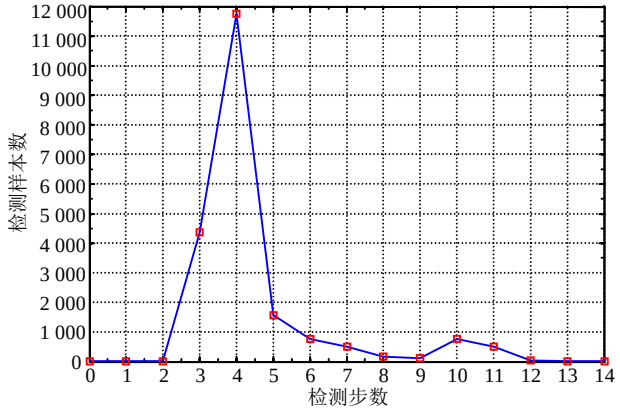

图4 样本检测步数统计图

对样本检测时所需检测步骤的一个统计如图4所示。从图中可以看出，系统在检测时需要至少3个属性才能做出判决。但大部分在第4、5步才能做出判定，而只有极少数会需要12个步骤。

4 结 束 语

本文采用粗糙集理论建立了入侵检测的灰色空间模型，并分析了该模型在网络入侵检测方面的应用。将灰色空间模型用于网络入侵检测的实验具有以下优点：1) 优化后的模型将原来KDDCUP数据集的41个属性约简到23个，缩小了规则库的规格；2) 系统的判决非常简单，最多12个步骤就可作出判定，而大部分都可以在第4、5步便做出判决，为提高检测的实时性创造了有利的条件；3) 灰色空间的独立处理摆脱了传统一分为二的检测模式的缺陷，不仅充分发挥了异常检测系统和误用检测系统的长处，还降低了对不确定行为误判的风险。

然而，灰色空间的白化处理是一个动态的过程，本文的实验所采用的都是静态数据。因此，未能充分体现其在处理未知行为方面的优越性。但这是一种有潜力的方法，将会在未来的工作中得到进一步的验证。

参 考 文 献

[1] LU Hong. Immune mechanism based intrusion detection systems[C]//International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC 2009. Wuhan, China: IEEE, 2009.

[2] XUE Ming, ZHU Chang-jun. Applied research on data mining algorithm in network intrusion detection[C]// International Joint Conference on Artificial Intelligence, JCAI 2009. Pasadena, California, USA: IEEE, 2009.

[3] FORREST S, PERELSON A S, ALLEN L, et al. Self-nonself discrimination in a computer[C]//Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, California, USA: IEEE, 1994.

[4] PAWLAK Z. Rough sets[J]. International Journal of Computer and Information Science, 1982, 11: 341-356.

[5] 王珏. 粗糙集理论及其应用研究[D]. 西安: 西安电子科技大学, 2005.
WANG Jue. Theory and applications on rough sets[D]. Xi'an: Xidian University, 2005.

[6] 陈伟统, 钱沄涛. 基于粗糙集理论的网络入侵检测方法[J]. 计算机工程, 2006, 32(16): 133-135.
CHEN Wei-tong, QIAN Yun-tao. Methods of network intrusion detection based on rough sets theory[J]. Computer Engineering, 2006, 32(16): 133-135.

[7] 张红梅. 基于粗糙集特征约简的SVM集成入侵检测模型[C]//2009中国控制与决策会议. 沈阳:《控制与决策》杂志社, 2009.
ZHANG Hong-mei. Integrate intrusion detection model for SVM based on rough sets theory[C]//Conference on Control and Decision of China 2009. Shenyang: Control and Decision Press, 2009.

[8] ZENG Fan-ping, YIN Kai-tao, CHEN Ming-hui, et al. A new anomaly detection method based on rough set reduction and HMM[C]//Eighth IEEE/ACIS International Conference on Computer and Information Science, ICIS 2009. Shanghai, China: IEEE, 2009.

[9] BALA M, AGRAWAL R K. Evaluation of decision tree SVM framework using different statistical measures[C]// International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom 2009. Kottayam, Kerala, India: IEEE, 2009.

[10] DING Bao-shi, ZHENG Yong-qing, ZANG Shao-yu. A new decision tree algorithm based on rough set theory[C]// Asia-Pacific Conference on Information Processing, APCIP 2009. Shenzhen, China: IEEE, 2009.

[11] 安利平. 基于粗集理论的多属性决策分析[M]. 北京: 科学出版社, 2008.
AN Li-ping. Analysis of multiple attributions based on rough sets theory[M]. Beijing: Science Press, 2008.

[12] 胡智喜, 唐学忠. 基于信息增益法的决策树构造方法.[J]. 计算机与现代化, 2006, 7(3): 28-30.
HU Zhi-xi, TANG Xue-zhong. Decision tree construction based on information gain mathed[J]. Journal of Computer and Modernization. 2006, 7(3): 28-30.

[13] 王海坤, 韩代书. Toll样受体(TLRs)的信息转导与免疫调节[J]. 生物化学与生物物理进展, 2006, 33(9): 820-827.
WANG Hai-kun, HAN Dai-shu. Information conversion and immunision controlling for Toll like receptors[J]. Advancement of Biochemistry and Biophysics, 2006, 33(9): 820-827.

[14] SALVATORE J, FAN W. Results of the JAM project [EB/OL]. [2009-05-22]. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[15] CHEN Rung-Ching, CHENG Kai-fan, CHEN Ying-hao, et al. Using rough set and support vector machine for network intrusion detection system[C]//First Asian Conference on Intelligent Information and Database Systems, ACIIDS 2009. Dong hoi, Quang binh, Vietnam: IEEE, 2009.

编 辑 黄 莘