王戈.基于混沌算法的地震信息网络入侵检测研究[J].地震工程学报,2020,42(3):799-805.doi:10.3969/j.issn.1000－0844.2020.03.799

WANG Ge.Intrusion Detection of the Seismic Information Network Based on the Chaos Algorithm[J].China Earthquake Engineering Journal,2020,42(3):799-805.doi:10.3969/j.issn.1000－0844.2020.03.799

# 基于混沌算法的地震信息网络入侵检测研究

王 戈[1,2]

(1. 开封文化艺术职业学院 计算机学院，河南 开封 475000；
2. 河南大学 计算机与信息工程学院，河南 开封 475000)

**摘要**：为改善传统的基于机器学习的网络入侵检测方法只能检测已知入侵行为，对于未知入侵行为的检测存在误警率高、时效性差的不足，提出一种基于混沌算法的地震信息网络入侵检测方法。创建候选地震信息网络特征-混沌变量映射模型，实现变量之间的转化；采用混沌变量迭代演化算法进行地震信息网络特征选择；使用支持向量机对最优特征进行学习，为提高地震信息网络入侵检测精度，利用柯西蜂群算法对支持向量机参数进行寻优，建立网络入侵检测优化模型。仿真实验证明，基于混沌算法的地震信息网络入侵检测方法能有效实现高检测率、低误报率的入侵检测，具有很高的应用优势。

**关键词**：混沌算法；地震信息网络；特征提取；入侵检测

**中图分类号**：TP393.08 **文献标志码**：A **文章编号**：1000－0844(2020)03－0799－07

DOI:10.3969/j.issn.1000－0844.2020.03.799

# Intrusion Detection of the Seismic Information Network Based on the Chaos Algorithm

WANG Ge[1,2]

(*1.School of Computer, Kaifeng Vocational College of Culture and Arts, Kaifeng 475000, Henan, China;*
*2.School of Computer and Information Engineering, Henan University, Kaifeng 475000, Henan, China*)

**Abstract**: The traditional machine-learning-based network intrusion detection method can only detect the known intrusion behavior and has the disadvantages of high false alarm rate and poor timeliness when detecting unknown intrusion behavior. In this study, a new seismic information network intrusion detection method based on the chaos algorithm is proposed. First, the candidate seismic information network feature - chaos variable mapping model is created to enable the transformation between variables, and the chaos variable iterative evolution algorithm is used to select seismic information network features. Then, the support vector machine is used to learn optimal features. Finally, to improve the detection accuracy of seismic information network intrusion, the Cauchy bee colony algorithm is adopted to optimize the parameters of the support vector machine, and the optimization model of network intrusion detection is established. The simula-

**收稿日期**:2019-12-16

**基金项目**:国家自然科学基金项目(51186259)

**第一作者简介**:王 戈(1981－),女,河南开封人,硕士,讲师,主要研究领域为计算机网络安全。E-mailuniverse1302764@163.com。

tion experiment results show that the seismic information network intrusion detection method based on the chaos algorithm can effectively implement intrusion detection with high detection rate and low false alarm rate, thus having high application advantage.

**Keywords**: chaos algorithm; seismic information network; feature extraction; intrusion detection

## 0 引言

入侵检测技术可有效解决传统地震信息网络入侵防御系统无法解决的问题,提高了地震信息网络安全防御架构的完整性,因此越来越受到人们的关注。目前入侵检测技术是实现地震信息网络安全防护常采用的方案。文献[1]提出一种特征和分类器参数组合优化的网络入侵检测方法,先获取目标网络特征、分类器参数,分析这两项参数与入侵检测结果之间的关系,创建入侵检测模型,利用多目标优化算法种群优化过程对入侵检测模型的最优解进行优化,得到最佳的入侵特征和分类器参数组合,完成入侵检测。文献[2]提出一种基于 Makov 链状态转移概率矩阵的网络入侵检方法,采用 K 均值聚类方法设定目标网络当前状态,基于设定的状态创建隐马尔科夫模型。通过该模型实时检测输入到目标网络中的运行状态数据,完成实时入侵检测。

但上述的网络入侵检测方法普遍存在检测率不够精准的问题,因此提出一种基于混沌算法的地震信息网络入侵检测方法。设计思路如下:构建候选地震信息网络特征-混沌变量映射模型,然后采用混沌变量迭代演化算法筛选网络特征,在此基础上通过支持向量机深度学习最优特征,并利用柯西蜂群算法完成寻优过程,实现网络入侵检测。仿真实证结果证明该检测方法对地震入侵信息的检测速度更快,检测精度较高、误报率较低。

## 1 地震信息网络特征选择

混沌算法由特征信息映射和混沌变量、混沌向量部分组成[3],其构成如图 1 所示。

地震信息网络特征-混沌变量映射实质是为后续检测过程提供有效的混沌变量,通过候选地震信息网络数据特征与混沌变量之间的转化关系,将混沌变量任务量化为采用地震信息网络数据特征映射过程实现特征选取。设定混沌变量的目的是估测地震信息网络数据特征用于后续分类过程的性能,方便及时确定入侵数据。同时,地震信息网络数据与混沌变量之间的转化过程重复执行,直至达到迭代次数要求截止。

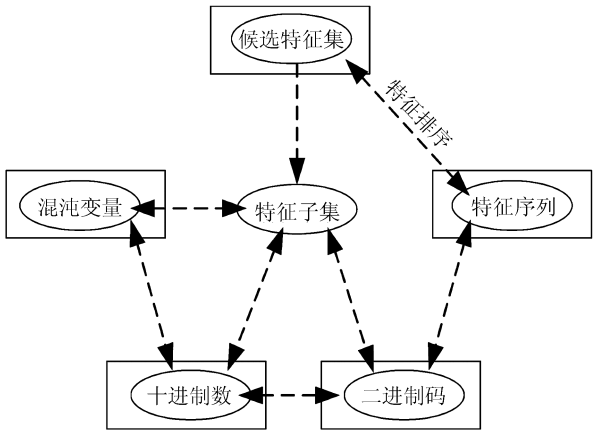


图 1 混沌算法构成

Fig.1 Chaos algorithm structure

### 1.1 候选信息特征与混沌变量映射

在采用混沌算法对网络入侵信息进行搜索前,需要将候选地震信息网络特征转变为混沌变量,将两者之间的转换过程称之为特征映射[4]。特征映射过程极为重要,可直接影响后续地震信息网络特征选择的精准度。

为提高检测时效性和有效性,采用分组排序法把候选特征信息集进行特征信息排序,将多个特征信息进行排序变成一个候选特征信息序列。具体过程如下,设由 $n$ 个候选地震信息网络特征信息组成的特征集描述为:

$$X=\{x_1,x_2,\cdots,x_i,\cdots,x_n\} \tag{1}$$

式中:$x_i$ 为特征信息,且 $i=1,\cdots,n$。采用 $f(x_i)$ 表示特征信息 $x_i$ 相对应的特征信息序列编码。$f(x_i)$ 取值为:

$$f(x_i)=\begin{cases}1, & x_i \text{ 被选中}\\ 0, & x_i \text{ 未被选中}\end{cases} \tag{2}$$

由式(2) 可知,候选特征信息序列对应的特征信息序列编码可表示为 $f(x_1)f(x_2),\cdots,f(x_n)$ 则通过选择可以得到特征信息子集:

$$S=\{x_i \mid x_i \in X, f(x_i)=1, i \in (0,n)\} \tag{3}$$

在特征信息序列编码完成后,将此二进制数码看作一个二进制数 $f$,利用特征信息和映射信息数制为完成特征信息序列与混沌变量的相互转化[5]:

$$y=\frac{\text{decimal}(f)}{2^n} \tag{4}$$

在式(4)中:$y$ 为特征信息;decimal($f$) 为 $f$ 将转为十进制数。

### 1.2　混沌特征搜索

混沌是自然界中非常普遍的现象,由于混沌变量具有规律性,因此可将其应用于地震信息网络数据分析中。经 Logistic 回归分析,混沌映射并非在所有阶段均处于完全混沌状态,仅在初始阶段为完全混沌状态,此时其均匀分布在区间[0,1]内。该区间的分布不受初始变量的影响,因此利用 Logistic 混沌映射完成地震信息网络数据搜索[6]。经 Logistic 映射生成混沌变量,即:

$$y_{j+1}=\mu y_j(1-y_j),\ j=1,2,\cdots,m \tag{5}$$

在式(5)中:$\mu$ 为常数;$y_j$ 为混沌变量;$m$ 混沌迭代次数。CSFS 方法步骤如下:

(1) 令 $y_0=\dfrac{\mu-1}{\mu}$;

(2) 运用公式(5)完成混沌变量 $y_{j+1}(j=1,\cdots,2^n-1)$;

(3) 将混沌变量 $y_j$ 从区间[0,1]映射到区间[0,$2^n$],并通过二进制编码[7-8]转化结果描述经混沌搜索获得的特征子集。

## 2　网络入侵检测模型

给定数据样本集 $T=\{x_i,y_j \mid i=1,2,\cdots,n,\ j=1,2,\cdots,m\}$,其中 $x_i\in R^n$ 表示输入矢量;$y_j\in\{+1,-1\}$ 表示期望输出矢量。通过非线性映射参数[9]将输入到支持向量机中的地震信息网络呈现于高维线性空间中,在该空间内建立分类超平面:

$$f(x)=w\varphi(x)+b=0 \tag{6}$$

式中:$w$ 为权值矢量;$b$ 为阀值。

特征分类要面对所有特征信息样本正确分类,所以有限制条件:

$$y_j[w\varphi(x)+b]\ \ j=1,2,\cdots,m \tag{7}$$

为避免在特征信息样本中线性不可分的情况,在最小化的目标函数中添加惩罚项 $C\sum_{i=1}^{l}\xi_i$,此时的优化问题变为:

$$\begin{cases}\min\psi(w)=\dfrac{1}{2}\|w\|^2+C\sum\limits_{i=1}^{l}\xi_i \quad i=1,2,3,\cdots,n\\ \text{s.t. } y_i=[(wx_i+b)]\geqslant 1-\xi_i\end{cases} \tag{8}$$

在式(8)中:$\xi_i$ 为松弛变量;$C$ 为惩罚因子。

引入 Lagrangian 乘子 $a_i$ 将上述问题转换为二次分类的优化问题:

$$\begin{cases}\min L(a)=\sum\limits_{i=1}^{n}a_i-\dfrac{1}{2}\sum\limits_{j=1}^{m}a_iy_jK(x_i,y_j)\\ \text{s.t. }\sum\limits_{i=1}^{m}a_iy_i=0\geqslant 0\ \ i=1,2,3,\cdots,n\ \ j=1,2,\cdots,m\end{cases} \tag{9}$$

通过求解式(10)来获取分类决策函数:

$$f(x)=\operatorname{sgn}\Big(\sum_{i,j=1}^{\infty}a_iK(x_i,y_j)+b\Big) \tag{10}$$

网络入侵检测建模阶段,惩罚函数 $C$ 以及核函数 $b$ 选取的好坏对入侵检测结果有直接影响,为提升检测模型精度,利用柯西蜂群算法对支持向量机参数进行寻优,以提升分类模型的性能。

## 3　入侵检测模型设计

在模拟实际自然算法中,人工蜂群算法是应用较多的算法之一,其模仿蜜蜂工作分类包含:引导蜂、追随蜂和勘察蜂,种群初始化阶段,设定食物源的数量与采蜜蜂的数量一致,人工蜂群算法初始化时设食物源个数与采蜜蜂的个数相等,而食物源则代表问题的最优解,并且会根据问题随机产生一种初始种群,进行竞争对比的方式在较优的食物源附近进行搜索,并会淘汰较差的食物源;此后追随蜂进行搜索,在最优个体邻近区域采用轮盘赌[10-11]算法搜索生成另一个个体;最终由勘察蜂对剩余个体进行搜索,若当前勘察蜂没有搜索到食物源,则生成新的勘察蜂,获取新的食物源。

设定食物源总数为 $N$,其随机生成的位置可描述为:

$$X_i=X_{i\min}+\text{rand}(0,1)(X_{i\max}-X_{i\min}) \tag{11}$$

式中:$X_{i\max}$ 表示种群搜索区间的最外围边界,$X_{i\min}$ 表示种群搜索区间的内围边界 rand(0,1) 为搜索区间内的任意常数。引导蜂搜索食物源过程中,通过种群交叉操作[12-13],更新已搜索到的食物源并生成一个新解,计算新解的适应度值时,采用贪婪准则对生成的解以及当前阶段的全局最优解进行选取。

$$v_{ij}=x_{ij}+\varphi_{ij}(x_{ij}-x_{kj}) \tag{12}$$

式中:$k\in\{1,2,\cdots,n/2\}$,$j\in\{1,2,\cdots,n\}$,且 $k\neq i$;$\varphi_{ij}$ 为[-1,1]之前的随机数。

人工蜂群算法中跟随蜂进行搜索时以概率 $P_i$ 并采用轮盘赌式的选择策略选出合适的蜜源采蜜,由式(13)、(14)计算跟随蜂在相邻区域进行搜索时得到的最佳适应值,利用贪婪准则对当前获得的最新解以及全局最优解进行选取。

$$P_i=f_{iti}/\sum_{i=1}^{n}f_{iti} \tag{13}$$

式中：$f_{iti}$ 为 $X_i$ 的适度函数值。

$$f_{iti}=\begin{cases}\dfrac{1}{1+f_i} & f_i\geqslant 0\\ 1+abs(f_i) & f_i<0\end{cases} \tag{14}$$

式中：$f_i$ 用于描述 $i$ 相应的适应度函数值。当蜜源所在空间位置 $X_i$ 通过多次迭代搜索仍无任务变化时，此时放弃该蜜源，采蜜蜂转换成勘察蜂，利用公式(12)随机生成新的蜜源替换当前搜索的蜜源进行迭代计算。

(1) 根据蜂群搜索步长进行动态调整

种群搜索计算，由于采蜜蜂的步长是随机变化的，追随蜂在所选取的蜜源周围搜索其他蜜源时，无法保证其搜索的结果为全局最优结果，在之后的搜索过程中也难以保证搜索的结果为全局最优结果。因此，在种群寻优阶段，期望在初始阶段扩展搜索区间，在种群迭代后期，即搜索到全局最优解后，为保证搜索精度，在最优解邻近区间内缩小搜索区间。本文引入一种动态因子 $w$，该因子可对搜索步长进行动态调整，调整后的搜索步长可描述为：

$$w=w_{\min}+(w_{\max}-w_{\min})f_{iti} \tag{15}$$

$$t=f_i/\sum_{i=1}^{n}f_i \tag{16}$$

式中：$w_{\min}$ 为最小惯性权值，$w_{\max}$ 为种群每次迭代搜索对应的适应度函数值，$f_i$ 表示种群迭代阶段的最大惯性权重值，通过该权重值的调整，种群中引导蜂和追随蜂位置更新为：

$$v_{ij}=x_{ij}+w(x_{ij}-x_{kj}) \tag{17}$$

由式(15)可知，在初始阶段 $t$ 较小 $w$ 值较大，可通过扩展动态因子增加种群搜索区间，使蜂群算法获取的解并非局部最优解，保证搜索结果的多样性；在种群搜索后期调整动态因子，增强蜂群引导者在全局最优解邻近区域的搜索性能，进一步提高种群全局寻优性能。

(2) 引入柯西因子

种群个体摘采相同蜜源的次数已达到设定的摘采极限时，引导蜂转换成勘察蜂生成一个新解，会导致随机性较强、扰动性较差。为此本引入柯西分布因子，目的是为提高种群全局搜索能力，辅助蜂群中的个体跳出局部最优解，以下给出柯西分布因子：

$$f(x)=\frac{1}{\pi}\frac{t}{t+x^2}\quad -\infty<x<+\infty \tag{18}$$

由式(18)可知，当 $t$ 为 1 时，$f(x)$ 就是标准柯西分布 Cauthy(0,1)，此时柯西分布随机变量形成函数为 $\beta=\tan[(a-1/2)\pi]$，式中 $a$ 是[0,1]区间的随机变量。

图 2 表示的是基准正态分布概率密度函数曲线、基准柯西分布概率密度函数曲线。

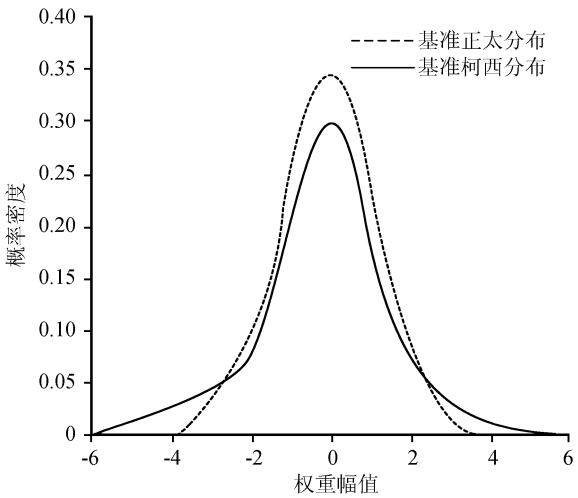


图 2 基准正态分布和柯西分布

Fig.2 Reference normal distribution and Cauchy distribution

由图可以看出基准柯西分布概率密度函数曲线左右两侧逼近于 0 的速度比基准正态分布概率密度函数要慢。从图中可以看出引入柯西因子后，避免种群个体搜索到的最优解为局部最优解，并非全局最优解，同时可以看出基准柯西分布概率密度函数曲线中峰值处要比基准正态分布概率密度函数曲线峰值处低，说明引入柯西因子后能够提高算法扰动能力。

## 4 仿真实验与结果分析

### 4.1 实验数据来源

为验证基于混沌算法的地震信息网络入侵检测方法的有效性，设计如下实验进行验证。

仿真实验环境为 CPU：双核 2.53 GHz，内存：4.0 G，操作系统：64 位 Windows7，开发环境：Matlab R2010a。选取的实验数据为 Marmousi 合成的地震信息数据集。地震信息网络数据入侵可划分为以下几种不同的攻击类型：

(1) DoS 攻击。这种入侵攻击模式主要是入侵者根据目标网络服务请求使用服务资源，致使目标网络用户服务请求难以得到准确应答的攻击模式，是当前阶段入侵者采用的攻击手段之一。

(2) Probe 攻击。这种入侵攻击模式主要通过入侵计算机来获取部分已知的服务漏洞。

(3) R2L 攻击。这种入侵攻击模式是通过截取地震信息数据包来攻击目标网络终端访问权限的入侵方式。

(4) U2R 攻击。这种入侵攻击模式是入侵者采用目标网络登陆信息访问系统,搜索系统中最脆弱的防火墙得到系统权限的行为。仿真实验过程中,从 Marmousi 合成的地震信息网络数据集中任意选择训练样本和测试样本,对样本内部属性信息进行归一化处理后获得实验样本如表 1 所列。

**表 1　入侵信息实验样本集**

**Table 1　Sample set of intrusion information experiment**

| 攻击类型 | 实验数据 | | | 测试数据 | | |
|---|---|---|---|---|---|---|
| | 样本数目/个 | 正常数目/个 | 入侵数目/个 | 样本数目/个 | 正常数目/个 | 入侵数目/个 |
| Dos | 9 015 | 6 346 | 2 669 | 3 202 | 2 274 | 928 |
| Probe | 6 512 | 5 189 | 1 323 | 2 345 | 1 876 | 469 |
| R2L | 4 762 | 3 756 | 1 006 | 1 472 | 1 254 | 218 |
| U2R | 2 476 | 2 271 | 205 | 762 | 714 | 48 |

### 4.2　数据特征选择

由 Marmousi 合成的地震信息数据集属性特征繁多。无关属性、冗余属性等会对地震信息网络入侵检测准确性产生影响,增加运算量导致检测速度降低,所以在实验中要进行特征选择,地震信息网络数据特征选取的目的就是保留有效的属性特征,去除无用的属性特征,进一步提取出优质的地震信息网络数据特征,提高目标网络入侵检测精度及效率。

文献[1]和文献[2]中的检测方法检测时间相对较短,但由于所选取的数据特征中包含较多的冗余特征,使得最终的入侵检测精度有所降低。为避免这种情况,要在保持检测精度的基础上,删除无效的属性特征,保证后续检测过程中使用的属性特征均为优质特征,引入粗糙集属性约简方法对地震信息网络数据属性特征进行有效约简。先将由 Marmousi 合成的地震信息数据集中的 50 个属性特征进行约简,剔除无效属性来提高最终的入侵检测精度。约简后的特征子集生成过程利用图 3 进行表示。

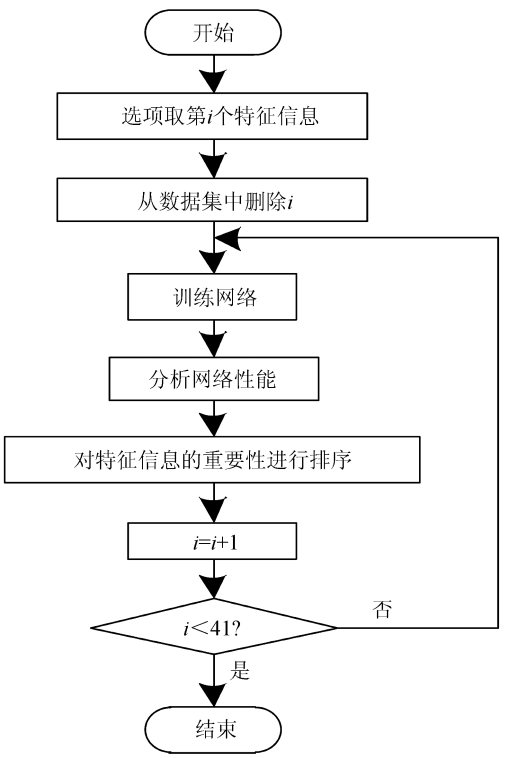


图 3　特征子集生成流程图

Fig.3　Flow chart of feature subset generation

根据图 3 可知,在选取第 i 个特征信息后,在原数据集中删除 i,在完成网络训练的基础上,按顺序排列特征信息的重要性,并计算 $i$ 的值。若 $i<41$,则生成特征子集,否则,则重新训练网络。

50 个属性特征按照图 3 所示过程有效约简后,入侵攻击类型对应的属性个数分别为 3、7、12、8,特征选择结果如表 2 所列。

**表 2　特征信息选择结果**

**Table 2　Selection results of feature information**

| 攻击类型 | 属性序号 |
|---|---|
| Dos | 6,18,31 |
| Probe | 4,12,22,28,32,38,42 |
| R2L | 1,6,11,14,19,22,27,32,37,41,43,45 |
| U2R | 2,9,15,21,26,30,35,39 |

### 4.3　检测结果与分析

将检测率和误报率作为评估对比指标,对文献[1]方法、文献[2]方法和所提检测方法进行评价。其中,检测率为地震信息网络信息检测量与地震信息网络信息总量的比值,误报率为入侵结果错误报警次数与总入侵次数的比值。检测结果分别如表 3、表 4 所列。

由表 3 的检测结果可得知,文献[1]方法除了 U2R 攻击的检测率稍高以外其他攻击类型的检测率明显低于本文所提出的检测方法。

由表 4 的检测结果可得知,在对入侵检测系统的误报率的检测中,本文方法明显比其他 2 中检测方法更加精准,Dos、Probe、R2L、U2R 这几种攻击类型中,对 DoS 攻击类型的检测率是最高的,并且

在所有攻击类型中误报率最低。

**表 3 三种入侵检测方法检测率对比结果**

**Table 3 Comparison result of detection rates of three intrusion detection methods**

| 方法 | 攻击类型 | 检测率/% |
|---|---|---|
| 文献[1] | Dos | 90.48 |
| | Probe | 86.41 |
| | R2L | 77.1 |
| | U2R | 70.02 |
| 文献[2] | Dos | 90.69 |
| | Probe | 86.38 |
| | R2L | 72.6 |
| | U2R | 69.95 |
| 本文方法 | Dos | 95.36 |
| | Probe | 89.12 |
| | R2L | 77.27 |
| | U2R | 69.98 |

**表 4 三种入侵检测方法误报率对比结果**

**Table 4 Comparison result of false alarm rates of three intrusion detection methods**

| 方法 | 攻击类型 | 误报率/% |
|---|---|---|
| 文献[1] | Dos | 2.69 |
| | Probe | 2.48 |
| | R2L | 1.69 |
| | U2R | 3.04 |
| 文献[2] | Dos | 2.61 |
| | Probe | 2.49 |
| | R2L | 1.62 |
| | U2R | 3.01 |
| 本文方法 | Dos | 0.86 |
| | Probe | 1.96 |
| | R2L | 1.27 |
| | U2R | 2.06 |

将所提的基于混沌算法的地震信息网络入侵检测方法通过在公开的数据样本集中进行测试，也同样验证了该检测方法的各项指标都优于另外 2 种检测方法。

## 5 结束语

本文将混沌算法引入到地震信息网络入侵检测过程中，增强了地震信息入侵检测的能力，取得较高的检测率以及较低的误报率。但该检测方法在计算复杂度、算法自身鲁棒性等方面不够理想，未来阶段将继续深入研究，提出更加全能的检测方法。

## 参考文献(References)


[1] 王战红.特征和分类器参数组合优化的网络入侵检测[J].南京理工大学学报，2017，41(1)：59-64.
WANG Zhanhong. Network Intrusion Detection by Using Combination Optimizing Features and Classifier Parameters [J].Journal of Nanjing University of Science and Technology，2017，41(1)：59-64.

[2] 韩红光，周改云.基于 Makov 链状态转移概率矩阵的网络入侵检测[J].控制工程，2017，24(3)：698-704.
HAN Hongguang，ZHOU Gaiyun.A Network Intrusion Detection Method Based on Fusion of Markov Chain State Transfer Probability Matrix[J].Control Engineering of China，2017，24(3)：698-704.

[3] 贺静，徐成武，任密林.基于概率神经网络的 IPv6 入侵检测技术研究[J].太原理工大学学报，2017，48(6)：969-972，983.
HE Jing，XU Chengwu，REN Milin.Research on IPv6 Intrusion Detection Technology Based on PNN[J].Journal of Taiyuan University of Technology，2017，48(6)：969-972，983.

[4] 张国华，刘文龙.基于压缩感知的星型拓扑结构无线传感网络信号检测算法[J].太原理工大学学报，2018，49(3)：473-476.
ZHANG Guohua，LIU Wenlong.A Compressed Sensing Based Detection for Star Topology WSNs[J].Journal of Taiyuan University of Technology，2018，49(3)：473-476.

[5] 封化民，李明伟，侯晓莲，等.基于 SMOTE 和 GBDT 的网络入侵检测方法研究[J].计算机应用研究，2017，34(12)：3745-3748.
FENG Huamin，LI Mingwei，HOU Xiaolian，et al.Study of Network Intrusion Detection Method Based on SMOTE and GBDT[J].Application Research of Computers，2017，34(12)：3745-3748.

[6] 刘田天，龙士工，冯金明.一种基于双线性对的云存储数据安全保护协议[J].贵州大学学报(自然科学版)，2017，34(5)：66-70.
LIU Tiantian，LONG Shigong，FENG Jinming.Data Security Protection Protocol for Cloud Storage Based on Bilinear Pairings[J].Journal of Guizhou University(Natural Sciences)，2017，34(5)：66-70.

[7] 王传栋，叶青，姚橹，等.基于大数据的网络恶意行为及特征关联分析[J].太原理工大学学报，2018，49(2)：264-273.
WANG Chuandong，YE Qing，YAO Lu，et al.Analysis of Network Malicious Behavior and Feature Association Based on Big-Data[J].Journal of Taiyuan University of Technology，2018，49(2)：264-273.

[8] 刘海燕，张钰，毕建权，等.基于分布式及协同式网络入侵检测技术综述[J].计算机工程与应用，2018，54(8)：1-6，20.
LIU Haiyan，ZHANG Yu，BI Jianquan，et al.Review of Technology Based on Distributed and Collaborative Network Intrusion Detection[J].Computer Engineering and Applications，2018，54(8)：1-6，20.

[9] 李静毅，杨雪梅，晁晓洁.高密度特征的网络分布式入侵检测技术仿真[J].计算机仿真，2018，35(10)：453-456.
LI Jingyi，YANG Xuemei，CHAO Xiaojie.Network Distributed Intrusion Detection Technology Simulation with High Density Characteristics[J].Computer Simulation，2018，35(10)：453-456.

[10] 陈俊，陈孝威.基于关联规则挖掘的 IPv6 入侵检测系统研究

[J].贵州大学学报(自然科学版),2013,30(2):60-65.
CHEN Jun,CHEN Xiaowei.Intrusion Detection System Research Based on Association Rule Mining for IPv6[J].Journal of Guizhou University (Natural Sciences),2013,30(2):60-65.

[11] 王广.基于改进差分进化的 K 均值聚类算法在入侵检测中的研究[D].北京:北京化工大学,2016.
WANG Guang.Research on K Means Clustering Algorithm Based on Modified DE Algorithm in Intrusion Detection[D].Beijing:Beijing University of Chemical Technology,2016.

[12] 朱琨,张琪.机器学习在网络入侵检测中的应用[J].数据采集与处理,2017,32(3):479-488.
ZHU Kun,ZHANG Qi.Application ofMachine Learning in Network Intrusion Detection[J].Journal of Data Acquisition and Processing,2017,32(3):479-488.

[13] 唐瑜穗,许道云.基于卷积的安全双方计算问题[J].贵州大学学报(自然科学版),2016,33(1):52-57.
TANG Yusui,XU Daoyun.A Secure Two-party Computation Problem Based on the Convolution[J].Journal of Guizhou University (Natural Sciences),2016,33(1):52-57.

[14] 黄永华,林振衡,宋骆林.基于改进 Hough 变换的刹车蹄块片安装孔定位检测法[J].贵州大学学报(自然科学版),2019,36(1):76-81.
HUANG Yonghua,LIN Zhenheng,SONG Luolin.A Method of Locating Detection for the Installation Holes of Brake Pads Based on Modified Hough Transform[J].Journal of Guizhou University (Natural Science),2019,36(1):76-81.

[15] 张富贵,付静,孟辉,等.基于 SIFT 算法的无人机烟株图像快速拼接方法[J].贵州大学学报(自然科学版),2019,36(3):62-68.
ZHANG Fugui,FU Jing,MENG Hui,et al.Fast Image Stitching Method of UAV Tobacco Plants Based on SIFT Algorithm[J].Journal of Guizhou University (Natural Science),2019,36(3):62-68.

[16] 席仕军,左宇军,孙文吉斌,等.基于数字图像处理的含分叉裂纹花岗岩破裂过程研究[J].贵州大学学报(自然科学版),2019,36(5):95-99.
XI Shijun,ZUO Yujun,SUN Wenjibin,et al.Study on the Fracture Process of Granite with Split Crack Based on Digital Imaging[J].Journal of Guizhou University(Natural Science),2019,36(5):95-99.