

# 基于神经网络和 CFS 特征选择的网络入侵检测系统<sup>\*</sup>

## A Network Intrusion Detection System Based on Neural Networks and the CFS-Based Feature Selection

孙宁青

SUN Ning-qing

(广西工业职业技术学院, 广西 南宁 530003)

(Guangxi Vocational and Technical Institute of Industry, Nanning 530003, China)

**摘 要:**本文提出了一种新型的基于 CFS 特征选择和神经网络的高效入侵检测模型。通过使用该模型对经过特征提取后的攻击数据的训练学习,可以有效地识别各种入侵。在经典的 KDD Cup 1999 入侵检测数据集上的测试说明,该模型能够高效地对攻击模式进行训练学习,从而正确有效地检测网络攻击。

**Abstract:** This paper introduces a novel intrusion detection model based on neural networks and the CFS (correlation-based feature selection) based feature selection mechanism. It can effectively detect several types of attacks by combining neural networks and the CFS-based feature selection. The experiments upon the well-known KDD Cup 1999 intrusion detection dataset demonstrate that the model is actually effective in practice.

**关键词:**入侵检测;特征选择;神经网络;CFS

**Key words:** intrusion detection; feature selection; neural network; correlation-based feature selection

**doi:** 10. 3969/j. issn. 1007-130X. 2010. 06. 010

**中图分类号:** TP393. 08

**文献标识码:** A

## 1 引言

入侵检测系统是当前网络安全领域的研究热点,在保障网络安全方面起着重要的作用。当前,有两类比较成熟的入侵检测系统:基于异常(Anomaly-Based)的入侵检测和基于特征(Signature-Based)的入侵检测。异常入侵检测系统记录用户在系统上的活动,并且根据这些记录创建活动的统计报告,如果报告表明它与正常用户的行为有明显的不同,那么检测系统就会将这种活动视为入侵。特征入侵检测是事先对已知的入侵方式进行定义(即定义入侵方式的特征),并且将这些方式写进系统中,将网络上检测到的攻击与系统定义的已知入侵方式进行对比,如果两者相同,则认为发生了入侵<sup>[1]</sup>。

由于传统的入侵检测技术存在着规则库难于管理、统

计模型难以建立以及较高的误报率和漏报率等诸多问题,制约了入侵检测系统在实际应用中的效果。并且,我们通过研究发现,提取和处理的特征数目过多是导致当前网络入侵检测系统速度下降的主要原因之一。特征和检测算法之间并不存在线性关系,当特征数量超过一定限度时,会导致检测算法性能变坏。实际上,有些特征没有包含或者包含极少的系统状态信息,它们对检测结果几乎没有影响。所以,使用特征选择去除冗余特征,保留能够反映系统状态的重要特征是提高检测速度的一个有效方法。

在这种背景下,我们在本文首先提出并实现了一个基于神经网络技术的网络入侵检测系统;并且,我们还采用了基于关联特征的 CFS(Correlation-Based Feature Selection, 简称 CFS)特征选择技术对它所使用的特征进行选择 and 约简,以提高整个系统的性能。

<sup>\*</sup> 收稿日期:2009-09-12;修订日期:2009-12-10

作者简介:孙宁青(1963-),男,广西南宁人,副教授,研究方向为计算机应用技术。

通讯地址:530003 广西南宁市广西工业职业技术学院计算机与信息工程系; Tel: (0771) 4212633, 13910017089; E-mail: superzhou-junpeng@163.com

Address: Department of Computer and Communication Engineering, Guangxi Vocational and Technical Institute of Industry, Nanning, Guangxi 530003, P. R. China

## 2 后向传播神经网络(BPNN)

### 2.1 基本原理

人工神经网络方法是现在模拟大脑智能所采用的主要技术手段。人们在许多人类智能问题采用人工神经网络方法进行模拟时,出于对不同问题的考虑,提出了许多种针对某类问题能有效解决的不同的人工神经网络模型,这些模型虽然不尽相同,但就其基本结构而言都是类似的。

BP神经网络,也称误差后向传播神经网络(Back Propagation Neural Network,简称 BPNN),是一种由非线性变换单元组成的多层前馈网络,一般由输入层、输出层和隐含层组成<sup>[2]</sup>。1989年 Robert Hecht-Nielson 证明了对于闭区间内的任一个连续函数都可以用一个隐含层的 BP 网络来逼近,因而一个三层的 BP 网可以完成任意的  $n$  维到  $m$  维的映射。该论点的证明不属本文的研究范围,在此不再赘述。但是,这实际上已经给了我们一个基本的设计 BP 网络的原则,即一个三层的 BP 网络在解决问题时已经基本可以满足要求。虽然增加层数可以进一步降低误差、提高精度,但同时使网络复杂化,从而增加了网络的训练时间,在很大程度上是得不偿失的。误差精度的提高实际上也可以通过增加隐含层中的神经元数目来获得,其训练效果也比增加层数更容易观察和调整,所以一般情况下,当问题难以解决时,应首先考虑增加隐含层的神经元数目,而不是增加隐含层。

### 2.2 算法流程

神经网络在实际工作之前必须进行学习,通过学习神经网络获得了一定的“智能”,才可以在实际的应用中取得良好的效果。下面是 BPNN 算法的简单流程<sup>[3]</sup>:

(1) 选定权重系数初始值。通常取较小的随机数(例如 ±0.25 区间)作为初始值。

(2) 重复下述 5 个步骤直至收敛(对各个样本依次计算):

① 从前向后各层计算各单元  $O_j$  :

$$Net_j = \sum_i w_{ji} o_i \quad (1)$$

$$O_j = \frac{1}{1 + e^{-net_j}} \quad (2)$$

② 对输出层计算  $\delta_j$  :

$$\delta_j = (y - O_j) O_j (1 - O_j) \quad (3)$$

③ 从后向前计算各隐含层  $\delta_j$  :

$$\delta_j = O_j (1 - O_j) \sum_k w_{jk} \delta_k \quad (4)$$

④ 计算并保存各权值修正量:

$$\Delta W_{ij}(t) = \alpha \Delta W_{ij}(t-1) \eta \delta_j o_i \quad (5)$$

⑤ 修正权值:

$$W_{ij}(t+1) = W_{ij}(t) + \Delta W_{ij}(t) \quad (6)$$

## 3 基于 CFS 的特征选择模型

### 3.1 特征选择算法概述

特征选择有三种模式:过滤器模式、封装器模式和混合器模式<sup>[4]</sup>。过滤器模式利用数据本身的特性作为特征子集

的度量指标,而封装器模式利用机器学习算法的准确率作为特征子集的度量指标。一般来说过滤器模式的效率比较高,结果与采用的学习算法没有关系,但效果稍差;封装器模式效率比较低,需要交叉认证和大量的计算资源,结果依赖于采用的分类算法,效果一般较好。为了解决两种特征选择模式存在的问题,发挥它们的优势,提出了混合器模式。

本节主要介绍基于过滤器模式的特征选择方法,其详细流程见图 1。图 1 中出现的变量定义为:  $D(F_0, F_1, \dots, F_{N-1})$  为具有特征数量为  $N$  的数据集;  $S_0$  为特征搜索空间的初始子集;  $S$  为生成的特征子集;  $\gamma$  为评价函数值;  $\delta$  为评估停止条件;  $M$  为与分类器无关的评价函数;  $S_{best}$  为符合最终要求的特征子集;  $\gamma_{best}$  为最优评价函数值;  $C$  为分类器;  $TrD$  为训练数据集;  $TeD$  为测试数据集。图 1 中出现的函数定义为:  $Generate(D)$ : 根据数据集  $D$  生成一个特征子集  $S$ ;  $Eval(S, D, M)$ : 根据数据集  $D$ 、评价函数  $M$ , 对特征子集  $S$  进行评估, 返回  $\gamma$ ;  $Build(TrD, S_{best})$ : 通过  $TrD$  和选择后的特征  $S_{best}$ , 建立分类器  $C$ ;  $Test(TeD, C)$ : 通过测试集  $TeD$  检测分类器  $C$  的性能。

通过特征选择,找到  $S_{best}$  之后,在  $S_{best}$  和  $TrD$  上建立分类器  $C$ ,这样建立的分类器计算资源耗用少,性能优于在全部特征上建立的分类器。

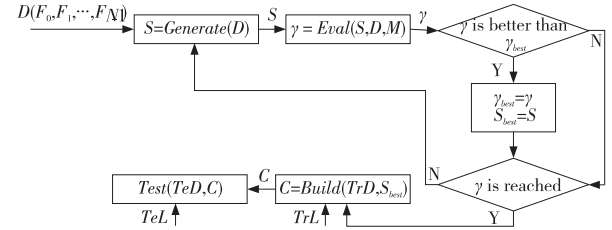


图 1 基于过滤器模式的特征选择方法流程

### 3.2 基于 CFS 的特征选择方法

CFS 方法是一种经典的过滤器模式的特征选择方法<sup>[5,6]</sup>,它启发式地对单一特征对应于每个分类的作用来进行评价,从而得出最终的特征子集,其形式化的评估方法如下:

$$Merit_s = \frac{k \bar{r}_{cf}}{\sqrt{k + k(k-1) \bar{r}_{ff}}} \quad (7)$$

其中,  $Merit_s$  表示一个包含  $k$  个特征的特征子集  $S$  的一个评价;  $\bar{r}_{cf}$  则表示对应于该子集的特征-子集平均相关度,其中  $f \in S$ ;  $\bar{r}_{ff}$  则表示特征-特征的平均相关度。事实上,式(7)给出的是一个 Pearson 相关,所有的变量都是经过标准化的。该评价指标能够有效地给出特征对于分类的贡献度,并从而清除不相关的或者是贡献度非常小的特征,而这些特征往往与其它特征相关度极高。

在式(7)中,需要通过熵计算方式来对特征间的相关性进行评价。并且,这些特征都必须是离散的随机变量,如果是数值型变量,需要首先使用指导的离散性方法对其进行离散化<sup>[7]</sup>。

## 4 基于 BPNN 和 CFS 的入侵检测模型总体结构

依据第 2 节所述的神经网络模型的特点,我们使用

CFS 特征选择方法,构建了一个高效的网络入侵检测系统,如图 2 所示。该系统主要包含如下几个部分:

- (1)报文捕获引擎捕获所有流经系统监测网段的网络数据流。
- (2)CFS 特征选取模块对捕获到的网络数据流进行分析处理,提取出可以完备而准确代表该数据流的特征向量,并采用本文所述的 CFS 选择方法对特征空间进行选择 and 约简,并将该特征向量提交给神经网络分类引擎以作为神经网络分类引擎的输入向量。
- (3)神经网络分类引擎对这一特征向量进行分析和处理,从而判别出是否为入侵行为,如果神经网络分类引擎经过分析处理以后认为是一种攻击行为,则向用户发出警告信息。如果报警信息对于攻击样本库的完善和更新有较大价值,比如发现了未知类型攻击行为(指神经网络未曾学习过的攻击类型),可以在用户参与下将该次攻击事件加入到训练数据里,以备神经网络分类引擎的再学习。这体现了神经网络所具备的不断学习以识别更多类型攻击行为的能力,也是神经网络入侵检测系统相比于一般的基于规则入侵检测系统的突出优势和亮点,对入侵检测系统的实际应用具有很大的价值。

特别需要注意的是:神经网络分类引擎的训练工作是离线进行的,它将依据管理员设定的时间间隔根据攻击数据库的信息进行再训练,以适应不断变化的攻击方式,能够较好地保证检测效率。

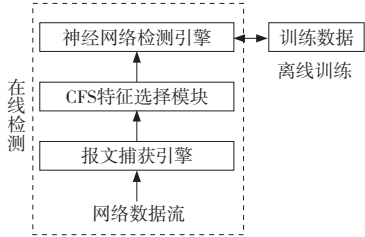


图 2 基于 BPNN 和 CFS 特征选择的高效入侵检测模型

## 5 实验及结果

为了验证我们提出的入侵监测系统的性能和效率,我们采用较为通用的 KDD 1999 数据集<sup>[8]</sup>来进行测试。在实验前,我们对该数据集进行了预处理。首先,考虑到神经网络训练的时间比较长以及 KDD 数据集的庞大,我们对其进行了随机采样,得到了 98 673 条实验数据,这些数据当中包含了 DoS(拒绝服务攻击)、Probe(探测攻击)、R2L(Remote to Local 攻击)、U2R(User to Root 攻击)四类攻击类型以及正常数据(Normal 类型);其次,根据本文第 3 节所述,我们采用 CFS 的特征选择方法选择了 KDD 数据集中的 6 个主要特征作为 BPNN 模型的输入,并且将采用得来的数据的其他属性进行了去除处理。在实验中,我们采用了十折交叉验证(Ten Fold Cross-Validation)的方法,得到如表 1 和表 2 所示的实验结果。

从表 1 的测试结果可以看出,对于训练过的攻击类型,神经网络具有很高的识别率,而误报率和漏报率都很低。并且,由于 KDD 1999 数据集中包含的 DoS 和 Probe 攻击的种类以及数据量都相对比较大,因而检测正确率较高,因

此神经网络模型对于训练数据量充足的入侵检测下的应用应该是非常适合的。

从表 2 的测试结果来看,相对于传统的入侵检测技术而言,神经网络具有很高的识别效率、很低的漏报率和误报率;对于未知类型的攻击行为,神经网络具备一定的检测能力,在一定程度上克服了基于规则入侵检测系统只能检测已知攻击行为的缺陷。并且,我们还对本文所述方法与文献[3]中所采用的 BPNN 结合独立主成份分析 ICA(Independent Component Analysis,简称 ICA)方法进行了实验对比,实验结果表明:BPNN 结合 CFS 进行入侵检测的效果无论在正确率还是误报率上都要比 BPNN 结合 ICA 方法的实验检测效果好,这也极大地验证了本文所述方法的正确性和有效性。

表 1 检测率实验结果 %

类型	正确率	误报率	漏报率
Normal	100	0	0
Probe	99.89	0.11	0
DoS	100	0	0
U2R	99.80	0.05	0.15
R2L	99.78	0	0.22

表 2 对比实验结果 %

检测模型	正确率	误报率
SVM	99.53	0.42
BPNN	99.62	0.18
BPNN+CFS	99.95	0.05
BPNN+ICA	99.73	0.27

## 6 结束语

本文提出了一种基于 BPNN 和 CFS 特征选择的入侵检测模型,并针对该模型进行了深入的分析和实验验证,证明了其正确性和有效性。目前,我们已经完成了基于本文所述 CFS 特征选择方法和神经网络算法的网络入侵检测系统原型,并将他们用于实际的恶意流量检测中,取得了比较好的实践效果。当然,在实践过程中,还是存在着部分漏报和误报问题;并且,神经网络的计算开销在一定程度上还比较大,并且本文所研究的特征选择和神经网络的训练方式还只适用于离线模式。这些都需要我们在下一阶段的工作中进行完善和优化。

### 参考文献:

- [1] Bykova M, Ostermann S, Tjaden B. Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics[C]//Proc of the 33rd Southeastern Symp on System Theory, 2001.
- [2] 戴葵. 神经网络实现技术[M]. 长沙:国防科技大学出版社, 1998.
- [3] Sun N Q, Li Y. Intrusion Detection Based on Back-Propagation Neural Network and Feature Selection Mechanism[C]//Proc of FGIT'09, 2009: 151-159.
- [4] Yu L, Liu H. Efficient Feature Selection via Analysis of Relevance and Redundancy[J]. Journal of Machine Learning Research, 2004(5): 1205-1224.

(下转第 117 页)