文章编号：2096-1472(2019)-04-17-04
DOI:10.19644/j.cnki.issn2096-1472.2019.04.005

基于深度学习的改进贝叶斯网络入侵检测算法

孙惠丽[1]，陈维华[2]，刘东朝[2]
(1.河北大学继续教育学院，河北 保定 071002；
2.河北软件职业技术学院，河北 保定071002)

摘　要：针对传统的朴素贝叶斯网络入侵检测技术存在训练数据集中属性冗余的问题，以及没有考虑到网络环境的变化导致贝叶斯网络结构改变的问题，提出一种结合深度学习和滑动窗口改进贝叶斯网络入侵检测方法。利用深度学习提取特征属性，降低数据集维数；采用滑动窗口技术实时更新贝叶斯网络参数，并利用特征属性的互信息计算各属性之间的相对欧氏距离，根据相对欧氏距离的大小及时更新贝叶斯网络，以提高检测率。实验结果表明，改进后的贝叶斯网络能够提高运算效率和检测率。

关键词：朴素贝叶斯；属性冗余；深度学习；滑动窗口；相对欧氏距离
中图分类号：TP393　**文献标识码**：A

Improved Bayesian Network Intrusion Detection Technology Based on Deep Learning

SUN Huili[1],CHEN Weihua[2],LIU Dongzhao[2]
(1.*Hebei University Continuing Education College*, *Baoding* 071002,*China*;
2.*Hebei Software Institute*, *Baoding* 071002,*China*)

Abstract: In view of the problem of training data set attribute redundancy and the lack of considering the changes in the network environment of the traditional Naive Bayesian network intrusion detection technology,this paper proposes an improved Bayesian network intrusion detection method,combining deep learning and sliding window.In this method,deep learning is utilized to extract feature attribute,reducing dimension data sets;the sliding window technology updates Bayesian network parameters,calculating the relative Euclidean distance between the various properties;the Bayesian network is updated according to the size of the relative Euclidean distance in order to improve the detection rate.The experimental results show that the improved Bayesian network can improve the operation efficiency and detection rate.

Keywords: Naive Bayesian Model;attribute redundant;deep learning;sliding window;relative Euclidean distance

1 引言(Introduction)

随着互联网的兴起和各种智能终端设备的普及，网络数据流量与日俱增，网络安全问题也是层出不穷，如何提高网络的安全性能，增强对网络流量的监控和异常网络流量的鉴别成了人们亟待解决的问题之一。目前存在的一些入侵检测技术能够精准地识别出入侵攻击，但当检测数据集发生变化或出现大量未知攻击时，检测精度急剧下降，效果达不到预期。因此，建立一个有效性与自适应性都不错的入侵检测模型成为以后研究的课题[1]。

深度学习是机器学习的一个重要分支，近些年来被广泛应用于图像分类，语音识别等众多领域。机器学习经历了浅层学习和深度学习两次浪潮。20世纪，学者Rumelhart、Hinton和Williams等人提出了反向传播算法(Back Propagation算法，BP算法)[2]，给机器学习带来了活力。20世纪90年代，各种浅层机器学习模型相继出现，并在机器学习领域取得巨大成功。多层神经网络因当时不够成熟的理论和相对匮乏的经验而相对沉寂，直到2006年Hinton和Salakhutdinov在发布在《科学》上的一篇文章中首次提出了

基金项目：河北省科技支撑计划项目“传统产业网上俱乐部的设计研究”(项目编号：13210905),主持人：孙惠丽.

深度学习的概念[3]，才拉开新的序幕。在深度学习研究领域，Google走在世界前列。2016年3月，基于深度学习的人工智能程序AlphaGo大比分击败围棋世界冠军李世石；2017年，其升级版智能程序Master连续击败中日韩等60名围棋高手，震惊世界。

贝叶斯网络以其强大的理论基础和优秀的信息提取的能力，广泛应用于入侵检测、文本分类、垃圾电子邮件过滤、模式识别等领域。朴素贝叶斯是一种基于属性之间相互条件独立所建立的贝叶斯方法，只需要少量必要数据就能进行建模，但面临属性冗余和计算成本过高的问题。文献[4]介绍了半监督式的朴素贝叶斯算法，该算法在处理大量数据时效果不错，但对小型网络的入侵检测效果不佳。局部加权朴素贝叶斯[5]结合频率估计，利用朴素贝叶斯对缩小的空间区域进行分类，提高了准确率，但时间与空间复杂度过高。文献[6]结合了朴素贝叶斯和权重，先估计特征数值，再利用海量数据来进行特征选取，最终实现属性减少，有效降低时间复杂度并提高准确率。但该算法特征提取稳定性差，泛化能力有待提升。

本文结合前人理论，对时间复杂度过高、泛化能力不强等问题，提出了一种基于深度学习和滑动窗口的改进贝叶斯网络入侵检测方法。该方法引入了被广泛认可和使用的深度学习和经典的滑动窗口思想，降低了数据集的维度，提高了网络扩展性，同时提升了检测效率和准确率。

2 深度学习(Deep learning)

2.1 神经学研究启示

深度学习源于对人类大脑神经网络连接结构的不断探索。机器学习通过一套规则，并通过大量数据训练，使机器学习到数据之间的关联，从而进行分类或判别。深度学习的发展源于生物神经网络学的进步。大脑神经研究结果显示，人类大脑分层次处理视觉信号，从低层提取边缘特征，在下一层提取形状，一直到最高层的特征提取[7]。人类大脑对视觉信号的处理是逐层转化、逐层提取的。这种多层次的结构极大地降低了处理的数据维数，而且最大程度地保留了有用信息。

2.2 特征提取的需要

机器学习通过大量数据的训练，从中找寻重要规律特征，并用于其他数据，实现分类预测。因此，如何寻找和描述数据特征是工作的重点。以往采用人工方式手动提取，该方法严重依赖于经验，耗时长、稳定性差。而深度学习克服了这个缺点，可以从大量数据中自动寻找有效特征，效率和准确率都远高于人工选择。

深度学习需要进行多层次的学习，在特征表达方面优于单隐含层节点的浅层学习。如图1所示，深度学习是一个逐层学习的过程，把每一层的输出作为下一层的输入，以此方式实现对信息的逐层表达。类似于生物学中从分子、细胞到器官、生物体的表达方式，深度学习的实质就是模拟大脑神经网络，实现对输入数据从低级到高级的特征提取表达，从而在不同维度抽象数据。

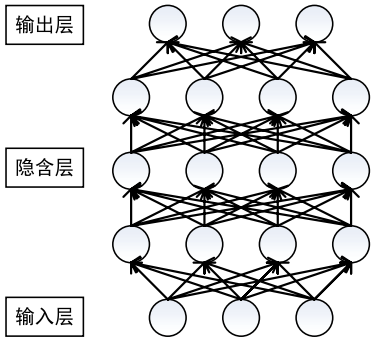

图1 含有多个隐含层的深度学习模型

Fig.1 A deep learning model with multiple hidden layers

2.3 卷积神经网

卷积神经网是深度学习的一种，属于前馈深度网络模型。1962年，Hubel等[8]通过研究猫的视觉机制，提出感受野的概念。1984年，Fukushima[9]基于感受野提出神经感知机，这是第一次在ANN领域成功运用CNN模型。LeCun[10]等将BP算法应用于CNN模型之中，并在图像识别领域取得成功。

卷积神经网由多个单层卷积神经网构成，主要包含卷积层，非线性变换和下采样层。CNN中采用局部连接、权值共享的方式，每层神经网络有一对二维平面，每个二维平面有多个独立的神经元。每个二维平面上的神经元只与上一层的部分神经元相连接，负责提取局部特征。每一层卷积层和下采样层都有多个二维特征平面，每一层的特征平面都共享权值参数，不同的特征平面提取特定的特征，在提升特征表达的同时又大大减少了计算量，提高了网络泛化能力。

如图2所示，上一层的特征图与卷积核进行卷积操作，输出的结果经过激活函数后输入给下一层。使用多个不同的卷积核可以提取某一层特征图不同的特征，形成良好的特征表达。卷积层和下采样层交替出现，一般地，卷积层计算公式为：

$$X_j^l = \sigma(\sum_{m_j} X^{l-1} * Kernel_j^l + b_l) \quad (1)$$

式中，l为网络层数，Kernele为卷积核，每层对应的卷积核不同，m_j为特征图的一个选项，每层有可训练的偏置参数b_1,$\sigma(z) = 1/(1+\exp(-z))$。

非线性变换是把卷积操作后的数据作为输入，进行非线性映射。传统的四种非线性操作函数公式为

Sigmoid：

$$R = \frac{1}{1+e^{-y}} \quad (2)$$

Tanh：

$$R = \frac{e^{y}-e^{-y}}{e^{y}+e^{-y}} \quad (3)$$

Softsign：

$$R = \frac{y}{1+|y|} \quad (4)$$

ReLU：

$$R = \max(0, y) \quad (5)$$

下采样功能简单，负责对每个特征图独立操作，采用平均池化或者最大池化方法降低数据规模。池化操作在尽量保留原特征图特征表达的同时，尽量降低了特征图分辨率，减

少了计算量。下采样层神经元的计算公式是：

$$X_j^l = \sigma(g_{m_j}(X^{l-1}) + b_l) \tag{6}$$

其中，$g(z)$表示对信息z的下采样，可以是取区域内的平均值或最大值。

输出层是最后一层，其连接着全连接层或者下采样层，是对输入层数据的高度抽象表达。

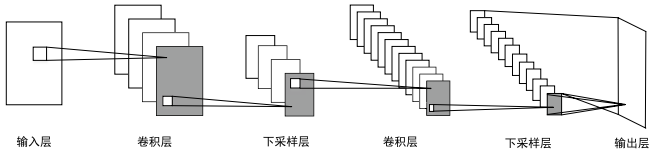

图2 CNN模型

Fig.2 CNN model

训练卷积神经网经常采用反向传播算法，以及有监督的训练方式，流程图如图3所示。卷积神经网的输入层为X，输出层位O。将输出特征O与理想特征T比较，将产生的误差E反向传递到上一层的每个节点，并依据权值公式进行权值更新。在有监督训练过程中，网络误差随着迭代次数的增加而逐渐减小，直至收敛或趋于稳定。

对于卷积神经网络的任意一层L，其第i个输入特征X_i和第j个输出特征Y_j之间的权值w_{ij}的更新公式[11]为：

$$\Delta w_{ij} = \alpha \delta_j X_i \tag{7}$$

当L层是最后一层时，式(7)中δ_j为：

$$\delta_j = \left(T_j - Y_j\right) h_L'(X_i) \tag{8}$$

式中，T_j为第j个预期特征；$h'(x)$为非线性映射函数的导数；j=1,2,⋯,N_L。

当L层不是最后一层时，式(7)中δ_j为：

$$\delta_j = h_L'(X_i) \sum_{m=1}^{N_{L+1}} \delta_m \omega_{jm} \tag{9}$$

式中，N_{L+1}为第L+1层的输出特征个数；ω_{jm}是L层的第j个输出和L+1层第m个输出之间的权值。

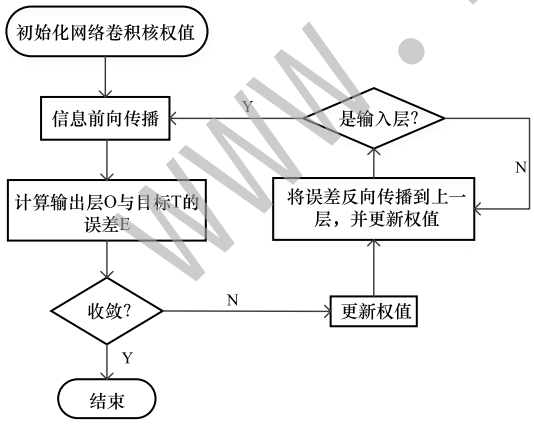

图3 卷积神经网络训练过程

Fig.3 Training process of convolution neural network

3 贝叶斯网络(Bayesian network)

朴素贝叶斯是一种利用先验概率和样本信息计算出后验概率，把样本归分到后验概率最大那一组中的方法，理论基础是贝叶斯公式和简单的条件假设。

根据贝叶斯公式，假设A_1，A_2，A_3，⋯，A_n为一互不相容的事件组，事件B能且只能与上述事件组中某一个事件同时发生，则下式成立：

$$P(A_i/B) = \frac{P(B/A_i)P(A_i)}{P(B)} = \frac{P(B/A_i)P(A_i)}{\sum_{i=1}^{n} P(B/A_i)P(A_i)} \tag{10}$$

假设$x = \{a_1, a_2, a_3, \ldots, a_m\}$是待分类项，$a$是样本属性。类别集合$c = \{y_1, y_2, y_3, \ldots, y_n\}$。统计和计算训练样本集在各类别前提下的条件概率或先验概率，即$P(a_1|y_1), P(a_2|y_1), \cdots, P(a_m|y_1)$；$P(a_1|y_2)$，$P(a_2|y_2)$，⋯，$P(a_m|y_2)$；⋯；$P(a_1|y_n)$，$P(a_2|y_n), \cdots, P(a_m|y_n)$。简单假设各特征属性之间是条件独立的，根据贝叶斯定理，得到公式(11)：

$$p(y_i|x) = \frac{p(x|y_i)p(y_i)}{p(x)} \tag{11}$$

公式(11)中，因为分母$P(x)$为固定值，只需计算分子中的最大值。因为各特征属性条件独立，所以：

$$P(x|y_i)P(y_i) = P(a_1|y_i)P(a_2|y_i) \ldots P(a_m|y_i)P(y_i) = P(y_i)\prod_{j=1}^{m} P(a_j|y_i) \tag{12}$$

根据计算，如果$P(y_k|x) = \max\{P(y_1|x), P(y_2|x), \ldots, P(y_n|x),\}$，则样本$x \in y_k$。

朴素贝叶斯网络中包含一个类节点与若干个属性节点，属性节点彼此之间独立，如图4所示。

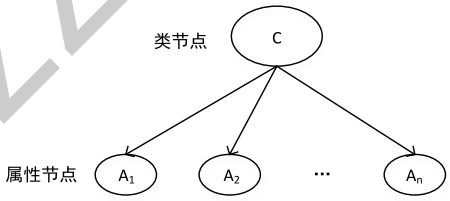

图4 朴素贝叶斯分类模型

Fig.4 Naive Bayesian Classification model

4 基于深度学习和贝叶斯网络的入侵检测算法 (Intrusion detection algorithms based on deep learning and Bayesian networks)

朴素贝叶斯算法在对数据集进行训练时，没有考虑到训练集的特征属性冗余，造成计算量增大且分类精度下降。传统的基于贝叶斯网络的入侵检测算法，根据训练集构造分类器，在测试相关度较高的测试集时表现出较好的性能。由于贝叶斯网络没有自学习能力，所以当测试集和训练集相关度下降或出现大量未知攻击时，传统算法的分类精度急剧下降。

针对上述不足，本文采用卷积神经网络对训练数据集进行属性越减，降维处理。然后采用基于互信息的构造算法[12]构造贝叶斯网络、参数学习，最后结合滑动窗口和相对欧式距离自更新网络并测试分类。

滑动窗口最早应用于OSI分层协议中的传输层和数据链路层，用于流量控制。本文借鉴此概念用于实时更新训练集，以提高对测试集的分类正确率。由于训练集更新，仅仅依靠参数学习已经不能满足贝叶斯网络的表达，所以本文定义了相对欧式距离，来度量训练集更新时互信息之间的差异，当差异超过某个阈值，更新贝叶斯网络结构。相对欧式距离公式如下：

$$q_{tk}=\frac{d_{tk}}{m_k}=\frac{\sqrt{\sum_{i,j}(I_{w_t}^{ij}-I_{w_k}^{ij})^2}}{\sqrt{\sum_{i,j}(I_{w_k}^{ij})^2}} \tag{13}$$

其中，d_{tk}表示窗口W_t和W_k之间互信息的欧氏距离；W_k表示当前网络所处窗口，初始状态为W_1；W_t表示第t个滑动窗口；$I_{w_t}^{ij}$表示在当前窗口下i、j两列特征属性之间的互信息($i\neq j$)。

本文算法步骤如下：

步骤1：对训练集T_0进行预处理(如：离散化、数值化)得到数据集T_1。

步骤2：利用卷积神经网对数据集T_1进行降维处理，得到数据集T_2。

步骤3：基于数据集T_2，采用文献[12]中的贝叶斯网络结构生成算法构造贝叶斯网络，并进行参数学习。

步骤4：结合滑动窗口机制和相对欧式距离，对测试集进行分类。具体步骤如下：

将测试集连接到训练集的尾部；设置四个指针$P_1P_2P_3P_4$，分别指向训练集的首部、尾部和测试集的首部、尾部。

(1)将指针P_1P_2之间的数据集T作为训练集构造贝叶斯网络并进行参数学习。令t=1，初始窗口为W_1。

(2)对指针P_3指向的样本进行检测，$P_3=P_3+1$。

(3)重复(2)，直到$P_3=P_4$或$P_3=P_2+N+1$，$t=t+1$，其中N为实验设置的滑动窗口的大小。

(4)如果$P_3=P_4$，转到(5)；否则，$P_2=P_2+N$，并计算当前窗口和初始窗口之间的欧氏距离q_{tk}，如果欧氏距离大于阈值ε，转到(1)，否则转到(2)。

(5)测试完毕，计算总正确率。

5 实验结果及分析(Experimental results and analysis)

5.1 入侵检测数据集

本实验采用KDD CPU 1999数据集，该数据集收集了9周的网络连接数据。其中，前两周收集的训练数据集大约含有500万个网络连接，后两周的测试数据集大约含有200万个网络连接。每个连接都有41个特征属性和1个标签属性。每个标签标记着正常或异常，异常类型中又总共包括4大类、39小类攻击类型，其中有22小类出现在训练集中，17小类出现在测试集当中。异常类型的详细描述如表1所示。

表1 异常类型

Tab.1 Types of exceptions

四种攻击类型	描述	22种攻击类型
DOS	拒绝服务攻击	Ping-of-death,syn flood, smurf etc.
R2L	来自近程主机的未授权访问	Guess password
U2R	未授权的本地超级用户特权访问	Buffer overflow Attacks etc.
Probe	端口监视或扫描	Port-scan,Ping-sweep etc.

5.2 实验结果与分析

本文从KDD CPU 1999数据集的训练集中随机抽取了4万条数据作为训练集，从该数据集中随机抽取了2万条数据作为本次实验的测试集。对数据预处理之后，采用深度学习进行降维处理，将原数据集中的42个属性约减成了9条属性(包含标签属性)，然后用改进的贝叶斯网络进行建模和分类。

实验在Matlab 2015b中编程完成，并将本文算法和已有的贝叶斯网络算法进行比较。实验表明，在本文算法中，当滑动窗口N为1000时，检测效果最好，得到的准确率对比结果，如表2所示。在窗口滑动过程中，贝叶斯网络发生了多次变化，仅选取其中四次贝叶斯网络结构图，如图5所示。

表2 准确率对比

Tab.2 Accuracy comparison

算法	记录类型/%				
	Normal	DOS	R2L	U2R	Probe
朴素贝叶斯	92.59	89.12	83.1	80.74	85.22
改进算法	96.59	91.98	87.5	92.19	91.11

与传统贝叶斯方法相比，改进的算法在减少计算量的同时，大大提升了贝叶斯网络检测的正确率。

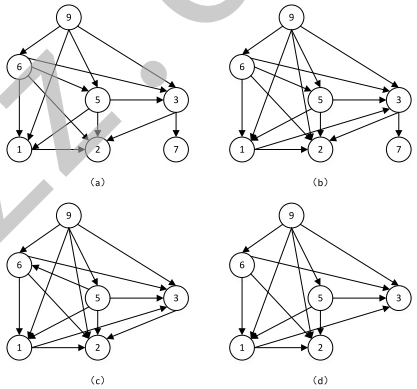

图5 贝叶斯网络结构变化图

Fig.5 Bayesian network structure change diagram

6 结论(Conclusion)

本文基于KDD CPU 1999数据集，使用深度学习对数据集进行降维处理，并引入滑动窗口和欧氏距离来实时更新贝叶斯网络，来提高正确率。实验证明，本文的改进算法能有效降低计算量和提高分类正确率。经过分析，分类错误的信息大部分是未知攻击类型。虽然深度学习具有从多维数据中提取高级抽象特征表达的能力，但依然很难学习到高层应用行为中复杂的逻辑行为。如何结合应用层的特征行为来检测未知攻击或异常数据需要进一步的学习和研究。

参考文献(References)

[1] 冯祖洪,李静.基于主成分分析的改进贝叶斯网络入侵检测研究[J].现代电子技术,2012,35(19):73-75.

[2] Rumelhart D,Hinton G,Williams R.Learning representations by back-propagating errors[J].Nature,1986,323(6088):533-536.

[3] Hinton G,Salakhutdinov R.Reducing the dimensionality of data with neural networks[J].Science,2006,313(5786):504-507.

[4] 江凯,高阳.并行化的半监督朴素贝叶斯分类算法[J].计算机科学与探索,2012,06(10):912-918.

(下转第16页)