文章编号: 1006-2475(2019) 10-0117-04

基于异卷积神经网络的入侵检测

李荷婷,冯仁君,陈海雁,景栋盛

(国网江苏省电力有限公司苏州供电分公司,江苏 苏州 215004)

摘要: 网络已经深入人们生产生活的各领域。然而,由于存在大量的非法入侵行为,网络所面临的安全问题也越来越严峻。因此,检测入侵以保障网络安全是一个亟待解决的问题。针对此,本文提出一种基于异卷积神经网络的入侵检测方法,采用深度学习的卷积神经网络模型完成对入侵数据的特征提取,然后根据 2 种不同结构的卷积神经网络训练数据,从而得到最优模型,用以判断网络入侵。最后,使用 KDD 99 数据进行对比实验,验证本文方法的准确性和精确性。

关键词: 深度学习; 卷积神经网络; 异卷积神经网络; 入侵检测; 网络安全

中图分类号: TP309 文献标识码: A doi: 10.3969/j.issn.1006-2475.2019.10.022

Intrusion Detection Based on Heterogeneous Convolutional Neural Network

LI He-ting, FENG Ren-jun, CHEN Hai-yan, JING Dong-sheng

(Suzhou Power Supply Branch, State Grid Jiangsu Electric Power Limited Company, Suzhou 215004, China)

Abstract: Network has penetrated into all fields of people's production and life. However, due to the existence of a large number of illegal intrusions, the network is facing more and more serious security problems. Therefore, detecting intrusion to ensure network security is an urgent problem to be solved. In order to solve this problem, an intrusion detection method based on heterogeneous convolution neural network is proposed. The convolution neural network model of deep learning is used to extract the intrusion data features. Then the optimal model is obtained according to the training data of convolution neural network with two different structures, which can be used to judge the network intrusion. Finally, experiment on KDD 99 verifies the accuracy and accuracy of the method proposed in this paper.

Key words: deep learning; convolutional neural network; heterogeneous convolutional neural network; intrusion detection; network security

0 引 言

随着大数据的发展,数据信息量之大使得安全过滤技术面临着全新的挑战。海量的数据使得安全分析遇到前所未有的困境,从大数据中获取恶意入侵的信息变得异常艰巨。庞大的网络入侵数量导致了网络空间面临着巨大的威胁。当前的入侵方式之多,未知入侵检测之难,传统的检测方式已经难以招架。每当出现新的入侵方式,往往不能及时发现,事后发现处理的被动局面将对国家企业造成巨大损失。因此,及时高效准确地检测入侵数据,判断入侵威胁将是在大数据时代的当务之急。

目前,常用的一些传统检测入侵方法有模式匹配、统计分析和完整性分析等。徐周波等人[1]针对入侵检测中模式匹配效率低的问题,改进了入侵检测系统的 BM 算法,节约了匹配时间并减少了匹配次数,提高了匹配效率。韩红光等人[2]针对网络攻击预测问题,先用 K 均值聚类定义网络状态,再构建状态概率转移矩阵和初始概率分布的隐马尔科夫模型,并以此检测异常。刘铭等人[3]针对传统参数优化算法在优化过程中会不同程度地陷入局部最优解,提出了基于交叉突变人工蜂群算法的支持向量机参数优化方法,有效提高了入侵检测的分类性能。雷宇飞等人[4]针对 BP 神经网络收敛速度慢、易陷入局部最优、系统稳定性差等问题,提出了基于粒子群优化的 BP 神经网络入侵检测技术优化算法。

收稿日期: 2019-03-19; 修回日期: 2019-03-29

基金项目: 江苏省高等学校自然科学研究重大项目(17KJA520004)

作者简介: 李荷婷(1990-) ,女,江苏常州人,助理工程师,硕士,研究方向: 信息安全,E-mail: loading.527@163.com; 冯仁君(1989-) ,男,江苏盐城人,硕士,研究方向: 软件智能化,信息安全,E-mail: frj1989@126.com; 陈海雁(1974-) ,男,江苏苏州人,工程师,硕士,研究方向: 信息安全,E-mail: 13372175016@189.cn; 景栋盛(1981-) ,男,江苏苏州人,高级工程师,硕士,研究方向: 信息安全,E-mail: jds19810119@163.com。

虽然上述方法从多方面着手,提高了入侵检测的准确率,但是,网络中不断涌现出大量新的入侵数据,由于这些数据都是无标签数据,导致绝大多数传统的方法无法有效地处理。深度学习是一种新的机器学习方法,近几年内理论基础日益完善,实际应用效果极佳,在语义分析[5-6]、图像处理[7]、语音识别[8]和医疗[9-10]等方面有着广泛的应用。深度学习的理论研究与实践的沉积对于处理大量无标签数据,挖掘数据特征打下了坚实的基础。因此,本文在深度学习的基础上,提出基于异卷积神经网络的入侵检测方法,通过卷积神经网络提取入侵数据的特征,然后使用 2 个不同结构的卷积神经网络训练数据,得到检测模型。

1 相关工作

1.1 深度学习

深度置信网络由 Hinton 等人[11]在 2006 年提出,由此开辟了划时代的深度学习研究。传统的神经网络中神经网络学习到的只是数据的一层特征,但是深度学习能够学习到数据的多层特征。"深度学习"中的"深度"表示连续层表征[12],通常涉及几十甚至上百个连续的表示层,这些表示层能够自主学习。对于机器学习的其他方法,比如浅层学习中的多层感知机,则更侧重于 1 层或者 2 层的数据特征学习。

当深度学习进行训练的时候,先是从输入到输出逐层对神经网络进行无监督训练,接着从输出到输入反向对参数进行微调,通过不断地循环从而收敛得到最优的参数解。随着硬件设施的升级,深度学习也在迅猛发展,在网络入侵检测方面深度学习的应用也在逐年增多。其中,最主流的模型包括深度置信网络(DBN)[13]、卷积神经网络(CNN)[14]和循环神经网络(RNN)[15]等。

1.2 卷积神经网络

卷积神经网络的深度学习模型是由多个卷积神经网络组成的多层卷积神经网络。卷积行为、下采样以及非线性变换构成了经典卷积神经网络。卷积过程如图 1 所示。

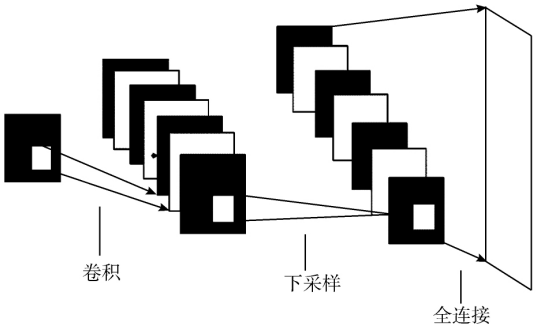

图 1 经典 CNN 结构图

在卷积网络进行卷积的过程中,卷积神经网络初始化输入信号的不同特征的卷积核。通过卷积核可以检测到输入信号的不同特定特征,并由此实现对于输入特征的权值共享。一般来说,对于某个深度卷积神经网络,采用不同的卷积核来提取不同的输入数据特征。对于图像作为输入的卷积网络,输入 x_i 为 m_1 个 $m_2 \times m_3$ 的二维数据特征,通过映射输出 y_j 为 n_1 个 $n_2 \times n_3$ 的特征数据。其中,映射的公式如式(1)所示:

$$y_j = \sum_i w_{ij} * x_i + b_j \tag{1}$$

其中,b 表示偏置向量,w 表示权重。

在进行下采样的过程中,卷积神经网络通常采用池化操作[16]处理数据特征,其中应用最广泛的是最大池化和平均池化这 2 种。最大池化操作是将限定的窗口内像素取最大值。相应地,平均池化操作是在邻域窗口内计算像素的平均值。通过一系列的池化操作后,在保证保持一定的原始数据总体特征下,降低了图片数据的分辨率,提高了神经网络计算速度。

当卷积完成后,卷积神经网络通过非线性函数 $f(y)$ 对卷积的输出进行非线性激活,激活函数常用的有 4 种:Relu 函数 $f(y) = \max(0, y)$、softsign 函数 $f(y) = y/(1 + |y|)$、tanh 函数 $f(y) = (e^y - e^{-y})/(e^y + e^{-y})$ 和 Sigmoid 函数 $f(y) = 1/(1 + e^{-y})$。

1.3 入侵检测

通常以异常检测和误用检测组合来提高入侵检测能力。异常入侵检测是指在正常的系统模式轮廓下,如果实时的用户轮廓值和正常值的差异超过了指定的阈值,就进行入侵报警。异常入侵检测可以不依赖攻击特征,直接根据被检测的目标发现入侵行为,而异常入侵检测的问题在于正常模式轮廓如何定义而降低误报率。误用检测取决于已有知识的完备性,可以根据已有知识库及时发现已知的攻击行为,它具有比较低的误报率,但其缺点在于,一旦有未知的入侵行为,误用检测并不能及时更新并检测出来。

异常检测的前提是存在异常行为,需要预先获取入侵的先验概率,从而依赖不同的异常模型而构成不同的检测方法。异常入侵检测的关键问题是在入侵行为和异常行为之间作出正确的判断,选出合适的度量子集,但是预先确定特定的度量将导致漏报行为。选择能够动态地进行判断和决策的度量集才是理想的。

误用检测的前提是能够按照某种方式进行特征编码,通过特征编码中的安全事件或其他误用事件的条件、特征、排列以及关系。误用检测可以通过观测一个事件发生的序列,应用贝叶斯定理来推测该行为是否为入侵行为[17]。一般可以用状态图来表示攻击特征,通过表征不同状态,获得某一阶段的特征。当

状态发生迁移,将导致系统陷入危险状态。

2　异卷积神经网络入侵检测

本文提出一种基于异卷积神经网络的入侵检测方法。目前,鲜有学者将深度学习应用于入侵检测。深度学习作为当代被广泛应用的技术,本文在应用深度学习进行入侵检测的基础上,新定义一种异卷积神经网络,将不同深度的卷积神经网络结构相结合,应用于入侵检测中,以期提高入侵检测的准确率。本章以 KDD 99 为数据集,分析了应用异卷积神经网络的入侵检测效果。

2.1　KDD 99 数据集

KDD 99 数据集是一个模拟军事网络中各种入侵的安全审计数据集,其中包含了 490 万次的攻击记录[18]。训练集中一共分为 5 大类: 正常、R2I(远程对本地攻击) 、Probe(探测攻击) [19]、DOS(拒绝服务攻击) [20]和 U2R(用户对管理员攻击) [21]。其中,每个样本都包含了 41 个固定属性特征和一个类标志符。在前 41 个固定属性中,32 个为连续类型,9 个为离散类型。KDD 99 的 4 种异常类型分别为 R2L、DOS、U2R 和 Probing,共有 39 种不同的攻击类型。整个数据集包含了 10% 的训练样本和测试集。测试集可用来模拟测试本文模型的泛化能力。本文使用 10% 的数据训练模型,用测试集测试并调整模型以得到最佳模型。下面是数据集中的一条记录样本:

0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,00,tcp,http,SF,334,1684,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,9,0.00,0.00,0.00,0.00,0.33,0,0,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,normal

2.2　数据预处理

由于 KDD 99 的特征包含了 32 个连续类型和 9 个离散类型,为了统一化处理,本文对 10% 的训练集采用了独热编码(one-hot) 预处理数据,将离散特征取值拓展到欧氏空间[22]。对于数据集中的符号型数据转化为数值型。

在 KDD 99 数据集的标签中,5 种主要攻击类型极其不均匀,其中,DOS 占据了极大多数,而 U2R、R2I 的比较少。在这种不均匀的情况用深度学习进行多分类学习,将导致效果往往不如支持向量机等传统的机器学习方法好。为了提高入侵检测的效果,本文将 5 种攻击类型都判定为非正常,编码为“0”,将“normal”编码为“1”。

因为数据特征中的各个数值差距很大,必须先将其进行数值标准化。标准化公式如下:

$$m' = \frac{m - AVG}{STAD} \tag{2}$$

其中,m 为特征值,m'为改变之后的特征值。AVG 为平均值,STAD 为平均绝对误差,由于训练集中存在孤立点,相比于标准误差,平均绝对误差具有更好的鲁棒性。值得注意的是,如果平均绝对误差为 0,则认为 m′为 0。

在标准化每个数值之后,为了加快梯度下降求最优解的速度同时提高精度,将标准化后的每个数值归一化到 [0,1] 区间。归一化公式如下:

$$m_{ij} = \frac{m'_{ij} - m_{\min}}{m_{\max} - m_{\min}} \tag{3}$$

$$m_{\min} = \min\{m'_{ij}\} \tag{4}$$

$$m_{\max} = \max\{m'_{ij}\} \tag{5}$$

其中,下标变量 $1 \leq i \leq n$,$1 \leq j \leq 32$。

经分析可以发现,数据集中存在大量的“0”,而太多的“0”将导致大量无效计算,浪费计算资源。因此,本文将所有数据归一化之后,将其视为灰度值,从而可以作为图像统一化处理,这样不仅可以在计算时忽略大量存在的“0”,而且突出了数据中非“0”元素的重要性。

图 2 显示了一个样本经过数据预处理之后的效果。在图中,非“0”元素将明显体现出来,从而提高训练效果。处理后的每个样本为 119 个数据,加上 2 位“0”填充,形成 11 × 11 大小的图像。将数据从一维转变为二维,将进一步提高卷积层的效果,更方便提取特征。

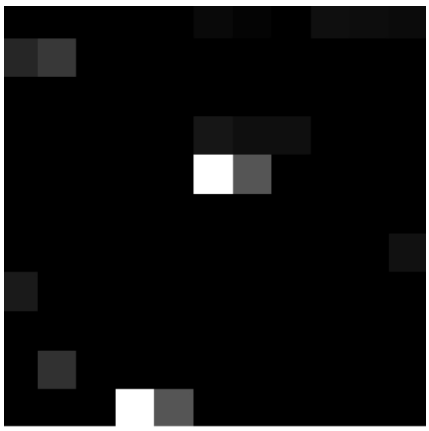

图 2　预处理之后的样本

2.3　模型结构和分析

目前最常用的多层卷积神经网络是一种三层卷积神经网络组成的通过对图像的 4 次卷积和 3 次池化,能够比较细腻地提取出图像的特征[23]。但由于归一化之后的数据在过于考虑图片局部特征的情况下,将导致模棱两可从而降低实验效果。因此本文添加一个相对的浅层卷积网络,它只有 3 层卷积网络和 1 个池化层构成,以期保留总体特征。最后通过 1 个全连接层使得 2 个网络并联。结构示意图如图 3 所示。

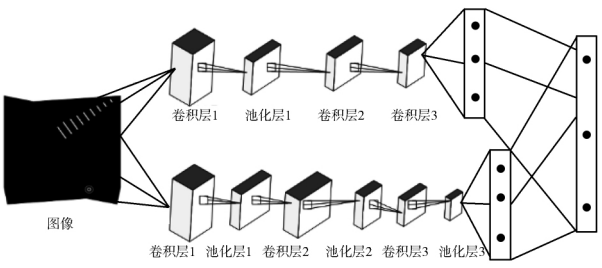

图 3 异卷积神经网络结构

通过上卷积神经网络，将训练样本的特征进行粗化提取特征，第一层卷积采用 5 ×5 的卷积核，步长为 2; 第二层和第三层采用 3 ×3 的卷积核，最后的全连接层包含 50 个隐层单元。通过下卷积神经网络，将训练样本的特征进行细化提取特征，第一层采用 7 × 7 的卷积核，步长为 2; 第二层和第三层采用 5 ×5 的卷积核，并对每一层卷积层都进行池化操作，最后的全连接层包含 5 个隐层单元。最后将 2 个全连接层用 1 个含有 100 个隐层单元的 softmax 层分类。

3 实验及结果分析

通过前面的分析，本文通过采用异卷积神经网络以期望提高入侵检测的各种性能。为了体现模型的高效性和优越性，本文选取一些经典的机器学习算法比如 K 近邻算法(KNN) 和支持向量机模型(SVM) ，非机器学习算法比如决策树算法(DT) ，以及经典的神经网络算法比如深度置信网络(DBN) 、长短期记忆网络(LSTM) 与本文模型(HCNNID) 进行比较。

为了体现异卷积神经网络的有效性，本文还比较了上层卷积网络(UpCNN) 的模型。所用的训练集为 KDD Cup 中 10% 数据集的 100000 个数据，并用 50000 个样本作为验证集以证明模型的泛化性能。实验指标采用精确率、准确率、F_1 值和召回率(Recall rate) 。对比 KNN、DT、SVM、LSTM、DBN 和 CNN 等方法所得结果如表 1 所示。

表 1 机器学习方法对比

方法	准确率/%	精确率/%	召回率/%	F_1
KNN	85.2	89.6	75.6	0.82
DT	91.94	98.9	75.6	0.92
DBN	93.49	92.3	93.7	0.93
SVM	82.4	74.0	80.3	0.77
LSTM	96.93	98.8	90.4	0.95
UpCNN	97.2	99.2	96.5	0.96
HCNNID	98.5	99.9	98.2	0.98

从表 1 中可以看出，经典的机器学习算法，比如 K 近邻算法、支持向量机等算法的实验效果比较差，应用决策树算法的结果也不是很理想; 深度置信网络、长短期记忆网络、普通卷积神经网络则实验指标比较高，本文算法利用上下 2 个不同的卷积神经网络相结合，在这 7 种算法中表现最佳，说明本文模型的先进性和高效性。

4 结束语

相比于用其他机器学习方法进行入侵检测，深度学习模型具有高准确性、高精确性特点。而针对深度学习过于专注于细节而极容易忽略总体特征从而一定程度上降低了模型的有效性，本文提出了一种用异卷积神经网络模型，通过一个深度神经网络和一个相对浅的神经网络相结合，提高了入侵检测的智能化水平，使其对于实时入侵拥有更精确的检测机制。经过对 KDD 99 数据集的测试，异卷积神经网络相比其他算法具有高效性、泛化性强等特点。随着社会的发展与进步，入侵检测必然越来越被人们所重视，而拥有准确、稳定且主动的入侵检测能力必然成为未来时代发展的潮流。

参考文献:

[1] 徐周波，张永超，古天龙，等. 面向入侵检测系统的模式匹配算法研究 [J]. 计算机科学，2017，44(9) : 125-130.
[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.
[3] 刘铭，黄凡玲，傅彦铭，等. 改进的人工蜂群优化支持向量机算法在入侵检测中的应用 [J]. 计算机应用与软件，2017，34(1) : 230-235.
[4] 雷宇飞，林玉梅. 基于 PSO-BP 神经网络的入侵检测技术优化算法的研究 [J]. 软件工程，2017，20(9) : 49-51.
[5] 何炎祥，孙松涛，牛菲菲，等. 用于微博情感分析的一种情感语义增强的深度学习模型 [J]. 计算机学报，2017，40(4) : 773-790.
[6] 郭东亮，刘小明，郑秋生. 基于卷积神经网络的互联网短文本分类方法 [J]. 计算机与现代化，2017(4) : 78-81.
[7] 李小薪，梁荣华. 有遮挡人脸识别综述: 从子空间回归到深度学习 [J]. 计算机学报，2018，41(1) : 177-207.
[8] 王山海，景新幸，杨海燕. 基于深度学习神经网络的孤立词语音识别的研究 [J]. 计算机应用研究，2015，32(8) : 2289-2291.
[9] 徐彦君，杜利民，侯自强，等. 一种用于立体匹配的改进的神经网络方法 [J]. 中国图象图形学报，1998，3(10) : 845-848.
[10] 林钦壮，钟映春，罗唯师. 面神经序列图像感兴趣区域识别 [J]. 计算机与现代化，2017(11) : 51-54.
[11] HINTON G E，SALAKHUTDINOV R. Reducing the dimensionality of data with neural networks [J]. Science，2006，313(5786) : 504-507.
[12] 傅天驹，郑嫦娥，田野，等. 复杂背景下基于深度卷积神经网络的森林火灾识别 [J]. 计算机与现代化，2016(3) : 52-57.

(下转第 126 页)

总是的关键技术之一,聚类分析算法是解决网络入侵检测的一种重要方法。由于数据维数越来越高,传统的数据聚类分析算法不适用于高维数据的聚类分析问题。鉴于此,本文提出了基于 Krylov 子空间方法的高维数据聚类分析算法,并将该算法应用在网络入侵检测问题中。实验表明,该方法具有良好的性能。

参考文献:

[1] BHUYAN M H, BHATTACHARYYA D K, KALITA J K. Network anomaly detection: Methods, systems and tools [J]. IEEE Communications Surveys & Tutorials, 2014,16(1):303-336.

[2] WU J S, ZHENG W S, LAI J H. Approximate kernel competitive learning [J]. Neural Networks, 2015,63:117-132.

[3] 姜洪权,王岗,高建民,等. 一种适用于高维非线性特征数据的聚类算法及应用 [J]. 西安交通大学学报, 2017,51(12):49-55.

[4] 刘晨赫,刘小晴,刘青,等. 针对高维数据的动态网格子空间聚类算法 HDGCLUS [J]. 小型微型计算机系统, 2018,39(9):1895-1899.

[5] SHAO J M, WANG X Z, YANG Q L, et al. Synchronization-based scalable subspace clustering of high-dimensional data [J]. Knowledge and Information Systems, 2016,52(1):83-111.

[6] CUNNINGHAM J P, YU B M. Dimensionality reduction for large-scale neural recordings [J]. Nature Neuroscience, 2014,17(11):1500-1509.

[7] CUI Y, ZHENG C H, YANG J. Dimensionality reduction for microarray data using local mean based discriminant analysis [C] // Proceedings of the 9th International Conference on Intelligent Computing Theories and Technology. 2013:267-276.

[8] SAHOO D, PETERCA M, AQAD E, et al. Losing supramolecular orientational memory via self-organization of a misfolded secondary structure [J]. Polymer Chemistry, 2018,9(18):2370-2381.

[9] LEVERS C, MÜLLER D, ERB K, et al. Archetypical patterns and trajectories of land systems in Europe [J]. Regional Environmental Change, 2015,18(3):715-732.

[10] LI C, FARKHOOR H, LIU R, et al. Measuring the Intrinsic Dimension of Objective Landscapes [EB/OL]. [2019-04-01]. https://arxiv.org/abs/1804.08838.

[11] ANDERSON C B, NICK H. Biodiversity monitoring, earth observations and the ecology of scale [J]. Ecology Letters, 2018,21:1572-1585.

[12] 向柳明,周渭博,钟勇. 基于高斯过程的 CLIQUE 改进算法 [J]. 计算机应用, 2015(S2):85-87.

[13] LIU S S, BREMER P T, THIAGARAJAN J J, et al. The grassmannian atlas: A general framework for exploring linear projections of high-dimensional data [J]. Computer Graphics Forum, 2016,35(3):1-10.

[14] 杨维永,何军,郑生军,等. 一种适宜于子空间聚类的离群点检测算法 [J]. 计算机与现代化, 2015(12):39-42.

[15] 琚书存,程文杰,徐建鹏,等. 基于密度峰和划分的快速聚类算法 [J]. 计算机与现代化, 2018(8):16-20.

[16] FARMANI F, PARVIZIMOSAED M, Monsef H, et al. A conceptual model of a smart energy management system for a residential building equipped with CCHP system [J]. International Journal of Electrical Power & Energy Systems, 2018,95:523-536.

[17] 徐聪,黄文准,黄世奇. 基于自组织映射的遗传聚类算法 [J]. 计算机与现代化, 2017(4):38-43.

[18] IRFAN S, DWIVEDI G, GHOSH S. Optimization of K-means clustering using genetic algorithm [C] // 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN). 2017.

[19] SHUKRI S, FARIS H, ALJARAH I, et al. Evolutionary static and dynamic clustering algorithms based on multi-verse optimizer [J]. Engineering Applications of Artificial Intelligence, 2018,72:54-66.

[20] XU X P, LI J, ZHOU M C, et al. Accelerated two-stage particle swarm optimization for clustering not-well-separated data [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018,48:1-2.

[21] 张新有,曾华燊,贾磊. 入侵检测数据集 KDD CUP 99 研究 [J]. 计算机工程与设计, 2010,31(22):4809-4812.

[22] RUAN Z H, MIAO Y T, LEI P, et al. Visualization for big data security: A case study on KDD Cup 99 data set [J]. Digital Communications and Networks, 2017,3(4):250-259.

[23] 刘春. 基于组合算法选择特征的网络入侵检测模型 [J]. 计算机与现代化, 2014(8):75-80.

[24] 陈路莹. 高维数据的聚类分析方法研究及其应用 [D]. 厦门:厦门大学, 2009.

(上接第 120 页)

[13] MNIH V, KAVUKCUOGLU K, SILVER D, et al. Human-level control through deep reinforcement learning [J]. Nature, 2015,518(7540):529-533.

[14] 周飞燕,金林鹏,董军. 卷积神经网络研究综述 [J]. 计算机学报, 2017,40(6):1229-1251.

[15] 杨祎玥,伏潜,万定生. 基于深度循环神经网络的时间序列预测模型 [J]. 计算机技术与发展, 2017,27(3):35-38.

[16] XU S J, CHENG Y, GU K, et al. Jointly attentive spatial-temporal pooling networks for video-based person re-identification [C] // Proceedings of IEEE International Conference on Computer Vision. 2017:4733-4742.

[17] 黄玉洁,唐作其. 基于改进贝叶斯模型的信息安全风险评估 [J]. 计算机与现代化, 2018(4):95-99.

[18] 刘春. 基于组合算法选择特征的网络入侵检测模型 [J]. 计算机与现代化, 2014(8):75-80.

[19] 梁鑫,桂小林,戴慧珺,等. 云环境中跨虚拟机的 Cache 侧信道攻击技术研究 [J]. 计算机学报, 2017,40(2):317-336.

[20] TAO W, CHEN H C. SGuard: A lightweight SDN safeguard architecture for DOS attacks [J]. China Communications, 2017,14(6):113-125.

[21] BEGHDAD R. Efficient deterministic method for detecting new U2R attacks [J]. Computer Communications, 2009,32(6):1104-1110.

[22] 叶衍,张凌,曹明明,等. 基于特征分布的图象信息抽取 [J]. 中国图象图形学报, 1998,3(3):189-193.

[23] 李钦,游雄,李科,等. 图像深度层次特征提取算法 [J]. 模式识别与人工智能, 2017,30(2):127-136.