DOI：10.16667/j.issn.2095-1302.2020.02.015

基于深度学习的病毒检测综述

赵晨洁[1,2]，吴　恋[1]，左　羽[1,2]，王永金[1,2]
（1. 贵州师范学院 数学与大数据学院，贵州 贵阳 550018；
2. 贵州大学 计算机科学与技术学院，贵州 贵阳 550025）

摘　要：随着数据的增多，病毒的类型也随之增加。病毒的不确定性及其攻击的复杂性，使传统的机器学习已经不能满足大量高维信息的处理，数据安全问题就越来越引人注意。人工神经网络的进一步发展，使深度学习在语音、视觉等领域飞速发展。深度学习的技术越来越成熟，对病毒检测领域有着重要的意义，将在病毒检测领域也有很大的提升。该文着重于深度学习的每一个过程的不同方法，探究是否适用于病毒检测，介绍常用的深度学习模型，剖析深度学习对电脑病毒检测的现状，分析病毒检测中常用的数据集及其每个数据集的优缺点，以及需要经过数据预处理、特征学习和分类识别的整体流程及其每个过程中的常用技术。最后用经典案例分析深度学习在病毒检测中的准确率，结果表明准确率得到明显提升。

关键词：深度学习；病毒检测；识别分类；特征降维；高维信息；人工神经网络
中图分类号：TP391.4　　**文献标识码：**A　　**文章编号：**2095-1302（2020）02-0060-03

0　引　言

随着网络迅速发展，数据指数般的增长，数据安全问题成为人们关注的重点。病毒检测系统是维持互联网安全的一种防护措施，也是抵抗病毒入侵的一道重要保障，病毒检测系统能准确识别出病毒，对网络安全起着至关重要的作用。病毒主要分为黑客入侵和恶意软件等。传统的病毒检测方法是针对带有标签及样本数据量少的情况下有理想的分类效果，可是在信息数据指数增长的时期，病毒入侵将要面对新的挑战——大量非线性高维数据[1]。随着深度学习的不断发展，其能应用于多种领域，在病毒检测方面，主要采用深度信念网络、卷积神经网络等分类算法[2]。特征学习是深度学习的实质，用低维特征表示重要特征，能更好地解决维数灾难问题，同时在高维庞杂的网络数据中有着较好的检测结果。

1　深度学习技术

深度学习中有很多模型，实质是经过训练神经网络的参数，从而得到权重，调整权重值最后学到特征。深度学习从不同角度可以分为多种：在有无监督层面分为 Supervised Learning（有监督学习）和 Unsupervised Learning（无监督学习）；在使用场景[3]层面分为 Generation Model（生成模型）、Recognition Model（识别模型）和 Hybrid Mode（混合模型）。其中 Hybrid Mode 是指 Generation Model 和 Recognition Model 的混合，代表模型深度神经网络。常见的深度信念网络（DBN）属于 Unsupervised Learning，Generation Model；卷积神经网络（CNN）属于 Supervised Learning，Recognition Model。

深度信念网络由 Hinton 等人提出，在结构上是由多层无监督的 RBM（受限玻尔兹曼机）网络和有监督的 BP（反向传播）网络组成的一种深层神经网络[4]。卷积神经网络采用感受野，及用局部信息得到全部信息从而减少连接数目。权值共享需要减少求解参数，降低网络复杂性。pooling 对原图像进行下采样降低维度，减少计算量，防止过拟合。

2　病毒检测

2.1　基于深度学习的病毒检测现状

20 世纪 90 年代初期，Debar 等人初次在网络入侵检测病毒中加入神经网络[5]；21 世纪初，Creech 等人尝试在主机的入侵检测中加入神经网络[6]。在前人实验的基础上，病毒检测开始用深度学习技术[7]。但深度学习在病毒检测中并没有发展完善，还需要更深层的探究。在测试病毒监测模型时，通常用到 KDD Cup1999（KDD99）数据集[8]。该数据集数量多，类型丰富，每条数据有 41 种特征，其中包含 9 种 TCP（传输控制协议）连接基本特征、13 种内容特征、9 种

收稿日期：2019-08-13　　**修回日期：**2019-09-12
基金项目：贵州省科技厅2018年度国家科技部和国家自然科学基金奖励补助项目（黔科合平台人才[2017]5790-09）；贵州师范学院一流大学建设一流平台项目（贵师院发[2018]100号）；贵州师范学院信息工程专业专业建设项目（贵师院发[2018]99号）；贵州省科技厅基础研究计划项目（黔科合基础[2018]1121）

基于时间的网络流量统计特征、10 种主机的网络流量统计特征。KDD99 数据集为大量研究入侵检测的专家们提供了便利，但同时该数据集也出现了一系列冗余问题。NSL-KDD 数据集 [9] 删除了 KDD99 数据集中冗余数据，为病毒检测的实验准确性做出重要贡献。

2.2 基于深度学习的病毒检测原理

构建病毒检测模型的总体框架，分为 3 个步骤。

（1）数据预处理。将数据集（KDD99 或 NSL-KDD）[8] 的符号型转化为数值型，再对数值型数据做归一化。

（2）数据特征提取。将归一化后的数据，作为模型训练的输入，对高维数据进行降维，在对其关键特征提取。在此步骤主要是针对模型的选择及优化，对过拟合等问题进行解决。

（3）分类识别。将学习到的病毒特征值对其分类，输入到分类器中与训练好的数据集（KDD99 或 NSL-KDD）进行对比，识别出病毒类型。将识别出的病毒类型对用户做出相应的提示，如禁止访问等措施，保障了用户使用互联网的安全。

病毒检测整体流程如图 1 所示。

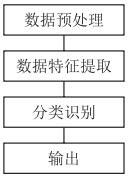

图 1 病毒检测流程

2.2.1 数据预处理

将“图像数据”（是指将异常代码以图像的形式来处理）转换成矩阵像素数据输入到神经网络。不同的“图像数据”有不同的规范，为了使模型精度提高，将对“图像数据”进行归一化处理，以及将“图像数据”压缩至 [0，1]。采用以下方法为数据进行归一化处理 [10]：

$$a=\frac{a-\mathrm{MIN}}{\mathrm{MAX}-\mathrm{MIN}} \tag{1}$$

式中：a 代表处理数据的特征属性值；MIN 是该数据属性的最小值；MAX 是该数据属性的最大值。

2.2.2 特征学习

对预处理后的病毒“图像数据”进行高维向低维的映射 [11]，学习数据的特征。将选取好的网络模型进行优化操作，如加入正则化、优化算法；再对模型进行训练、调参等使模型提取特征更为精确；最后对其数据进行降噪处理，获取优质特征值。经过这一步特征提取和选择，并采用更加稳定的网络模型进行训练，学习更深层的病毒特征，病毒检测系统将会具有更高的病毒识别率。

2.2.3 病毒识别分类器

分类器的任务是将上层有效特征进行自学习，学习到特征，然后给出最后的检测结果。分类器有贝叶斯、Logistic 回归、支持向量机（SVM）、Softmax 等，常用于病毒分类的有 Softmax，支持向量机等。

Softmax 将多分类的输出数值转化为相对概率，更容易理解和比较。Softmax[12] 分类器定义如下：

$$y_p=\frac{e^{\boldsymbol{\theta}_p x^{(i)}}}{\sum e^{\boldsymbol{\theta}} k^{x^{(i)}}} \tag{2}$$

式中：$\boldsymbol{\theta}_p$ 为第 p 个权重向量；$x(i)$ 为第 i 个数据样本。

SVM[13] 是解决小样本和非线性问题的一种高效的二分类机器学习算法，在病毒分类中将采用多类 SVM 分类，在 SVM1 中确定是正常类型还是攻击类型，从而在 SVM2，SVM3…中进一步确定具体属于哪种病毒。

朴素贝叶斯分类器 [14] 用贝叶斯来估计后验概率，定义为：

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)} \tag{3}$$

对所有特征做独立性假设，其样本 X 标记分类错误的后验概率为：

$$P(C|X)=\frac{P(C)P(X|C)}{P(X)}=\frac{P(C)}{P(X)}\prod_{i=1}^{d}P(X_i|C) \tag{4}$$

朴素贝叶斯分类器表达式为：

$$h_{\mathrm{nb}}(X)=\underset{C\in Y}{\arg}P(X)=\prod_{i=1}^{d}P(X_i|C) \tag{5}$$

式中：d 为属性数目；X_i 是 X 在第 i 个属性上的取值。朴素贝叶斯分类器主要是解决离散型病毒数据，在离散数据中提取病毒框架，进行区分不同网络攻击行为，有较高的精确度。

2.3 基于深度学习的病毒检测典型案例

2.3.1 案例一：基于深度信念网络的入侵检测模型 [15]

本文阐述了一种基于深度信念网络的病毒检测模型，网络模型如图 2 所示。该模型主要用深度信念网络为特征降维，将学到的数据用支持 SVM（支持向量机）的方法进行分类，并用 NSL-KDD 数据集评估。在实验中，保持 SVM 参数为默认值，用两层的受限玻尔兹曼机（RBM）作为深度信念网络的结构，将迭代次数设置为 150；特征数量由高层到低层分别是 4，13，41。实验结果见表 1 所列。通过实验发现，DBN-SVM 的准确率比单个的 SVM（支持向量机）和 DBN（深度信念网络）高。在速度上，本文提出的深度学习模型 DBN-SVM 比传统单独的 SVM 识别速度要快，很大程度上提高了处理时间。总的来说，在准确率和高效性上，DBN-SVM 都有突出的优势，能大幅提升对病毒检测的能力。

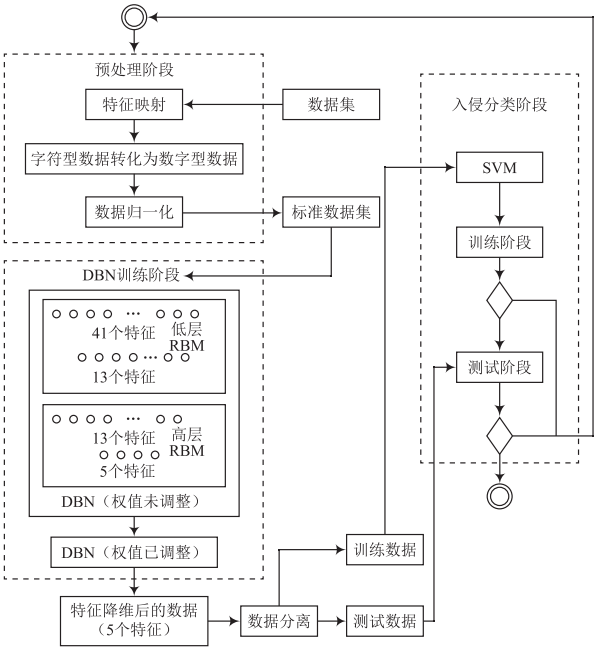

图 2　DBN-SVM 网络模型

表 1　不同分类模型间的对比

训练数据 /%	SVM		DBN		DBN-SVM	
	准确率 /%	时间 /s	准确率 /%	时间 /s	准确率 /%	时间 /s
20	82.30	10.4	89.63	0.31	90.06	2.54
40	87.60	11.7	89.44	0.43	91.50	3.96
60	88.33	20.87	89.54	0.57	92.84	5.07
100	89.25	32.30	89.60	0.76	93.14	7.75

2.3.2　案例二：基于卷积神经网络的入侵检测算法 [16]

贾凡等研究者对于病毒检测提出一个新的算法，将典型的卷积神经网络引入到病毒检测中，卷积神经网络模型如图 3 所示。利用卷积神经网络在处理图片时采用 3 维数据接收输入的数据，对高维数据的特征提取更为有效。根据特征的局部相关性提取特征，确保提取特征的准确率。该研究者提出的 CNN 网络模型囊括了 3 个卷积层、3 个池化层、1 个全连接层、1 个分类层，经过 CNN（卷积神经网络）提取特征后用 Softmax 分类器进行分类识别病毒类型，设置模型迭代次数为 10。利用本文模型与传统模型对准确率（AC）、检测率（DR）和误报率（FA）三方面指标进行评估，比较结果如表 2 所示。结果显示，CNN 模型在准确率和检测率中都高于传统方法，误报率相对下降很多。总之，CNN 模型比其他传统方法对于病毒检测有较大的性能提升。

3　结　语

本文讨论了病毒检测的必要性、深度学习的基本方法及深度学习用于病毒检测的模型，研究分析各网络模型对于病毒检测的效果。在互联网和物联网的结合下，越来越多的数据被存储，个人信息需要被保护，但是病毒检测还未能发展成熟，如在线攻击意图识别算法、网络多步攻击识别算法等都有待研究。

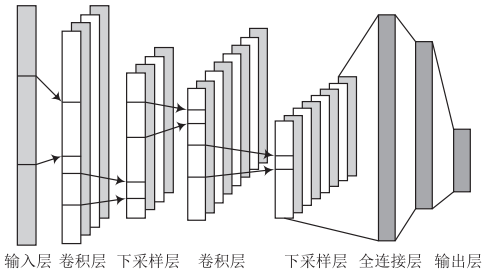

图 3　卷积神经网络模型结构

表 2　CNN 与其他算法性能比较　%

模　型	AC	DR	FA
本文	92.18	90.95	0.97
SOM[9]	90.82	89.57	1.16
NN[9]	82.30	81.63	2.31
SVM[9]	86.82	86.57	1.96

参　考　文　献

[1] 高妮，高岭，贺毅岳 . 面向入侵检测系统的 Deep Belief Nets 模型 [J]. 系统工程与电子技术，2016，38（9）：2201-2207.
[2] 张玉清，董颖，柳彩云，等 . 深度学习应用于网络空间安全的现状、趋势与展望 [J]. 计算机研究与发展，2018，55（6）：1117-1142.
[3] BIERMANN E，CLOETE E，VENTER L M. A comparison of Intrusion Detection systems [J]. Computers & security，2001，20（8）：676-683.
[4] HINTON G E，OSINDERO S，THE Y W. A fast learning algorithm for deep belief nets [J]. Neural computation，2006，18（7）：1527-1554.
[5] DEBAR H，BECKER M，SIBONI D. A neural network component for an intrusion detection system [C]// IEEE Symposium on Security & Privacy. Oakland：IEEE，1992：240-250.
[6] CREECH G，HU J K. A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns [J]. IEEE transactions on computers，2014，63（4）：807-819.
[7] FIORE U，PALMIERI F，CASTIGLIONE A，et al. Network anomaly detection with the restricted boltzmann machine [J]. Neurocomputing，2013，122：13-23.
[8] TAVALLAEE M，BAGHERI E，LU W，et al. A detailed analysis of the KDD CUP 99 data set [C]// IEEE International Conference on Computational Intelligence for Security & Defense Applications. Ottawa，Canada：IEEE，2009：1-6.
[9] Canadian Institute for Cybersecurity. NSL-KDD dataset [EB/OL]. [2017-08-18]. http：//www.unb.ca/cic/research/datasets/nsl.html.
[10] 于洋 . 入侵检测系统中特征选择算法与模型构建方法的研究 [D]. 兰州：兰州大学，2017.
[11] 高妮 . 网络安全多维动态风险评估关键技术研究 [D]. 西安：西北大学，2016.

（下转第 65 页）

8 KB FLASH，主频为 16 MHz，具有简单的 20 管脚封装，完全能满足项目需求。由于智能插座无需高精度的时钟源，因此晶振部分采用内部振荡器，以节省外部晶振的成本 [10]。

计量电路采用深圳合力为公司设计的 HLW8032 芯片，该芯片内置频率振荡器、参考电压源和电源监控电路，能实时测量有功功率、有效电流和有效电压，采用 UART 的方式同单片机通信，在 1 000 ： 1 的动态范围内，具有 0.5% 以上的测量精度，且无需校正，使用方便、可靠 [11-12]。

外部通信控制接口用于和视频测温系统进行通信控制。需要注意的是，外部控制信号接入系统需要进行光电隔离。

4 手机 APP 设计

手机端用来设定温度阈值、接收过温报警信号，并实时呈现设备图像和温度数据。APP 在获取图像和温度数据后，可以只显示图像，也可以对图像数据和温度数据进行融合，使温度值叠加在图像上，方便用户直观看到被测设备各点的温度，为判断设备是否处于安全运行状态提供依据。图 5 所示为某实验室用本系统监控大功率商用电磁炉样机电路的 APP 截图。其中，图 5（a）为只显示图像的截图；图 5（b）为图像、温度融合后的截图。从图片可以看出，该样机电路中变压器为最强的热源，温度超 50 ℃。

（a）显示图像截图　　（b）图像、温度融合后的截图

图 5　APP 显示界面截图

5 结　语

从实验室安全角度出发，设计了一套适用于实验室设备安全监测的软硬件系统，借助该系统可以实现设备的 24 h 监控，及时发现设备存在的安全隐患，并做相应的处理，降低实验室发生火灾等危险的概率。用户能通过手机 APP 实时查看设备的运行情况和关键部位的温度情况。特别对于新研发的设备而言，配备一套类似的监测设备十分必要。经过测试，系统运行稳定，用户界面友好，得到了实验室同行的广泛认可。同时，系统选用的方案具有很高的性价比，推广价值和市场潜力较大。

参　考　文　献

[1] 刘健 . 高校实验室火灾成因及预防 [J]. 消防技术与产品信息，2008（11）：47-49.
[2] 刘音，王瑞雪，刘洋，等 . 基于模糊综合评价法的实验室火灾风险评价 [J]. 实验室研究与探索，2018（8）：321-325.
[3] 崔琳，朱磊，刘小龙，等 . 基于 STM32F407 的以太网通信模块设计 [J]. 计算机测量与控制，2018（1）：260-263.
[4] 谢志文，许睿，黄小雪，等 . 基于 LwIP 的嵌入式 Web 服务器的设计与实现 [J]. 桂林电子科技大学学报，2014（4）：305-309.
[5] 熊雪艳，梁光胜，赖程鹏，等 . 基于 OV2640 模块的网络视频监控系统设计 [J]. 单片机与嵌入式系统应用，2015（12）：23-26.
[6] 黄健，罗国平，杜丽君 . 基于 STM32F407 平台 OV2640 驱动程序设计 [J]. 通讯世界，2015（10）：246-247.
[7] 孙宇贞，胡超，方永辉 . 基于 MLX90621 红外传感器的开关柜温度无线监测系统设计 [J]. 红外，2016（12）：13-18.
[8] 王维佳，喻青，段航，等 . 基于 MLX90621 的电梯电机及控制回路温度采集系统设计 [J]. 工业安全与环保，2019，45（3）：17-20.
[9] 刘鹏，熊卫华 . 基于 POE 供电的双目成像检测系统设计 [J]. 工业控制计算机，2019（1）：23-24.
[10] 项粤生，高瑞霞，邬杨波，等 . 基于单片机的智能插座的设计与实现 [J]. 工业控制计算机，2012（9）：129-131.
[11] 周晓，田瑞清，李永清 . 用电设备运行状态监控系统设计与实现 [J]. 计算机测量与控制，2019（2）：52-55.
[12] 徐钰琨 . 基于 STC 和 HLW8012 的电视节能插座设计 [J]. 电子世界，2016（20）：90-92.

作者简介：季瑞松（1978—），男，江苏海门人，硕士研究生，高级工程师，主要从事电工电子学实验教学和嵌入式设备的研发。

（上接第 62 页）

[12] 张思聪，谢晓尧，徐洋 . 基于 dCNN 的入侵检测方法 [J]. 清华大学学报（自然科学版），2019，59（1）：44-52.
[13] 王佳林，童恩栋，牛温佳，等 . 基于 CNN-NSVM 的入侵检测模型 [J]. 信息通信技术，2018，12（6）：48-55.
[14] 席海龙，刘海燕，张钰 . 应用于入侵检测的机器学习现状与发展分析 [J]. 价值工程，2018（34）：269-272.
[15] 杨昆朋 . 基于深度信念网络的入侵检测模型 [J]. 现代计算机（专业版），2015（2）：10-14.
[16] 贾凡，孔令智 . 基于卷积神经网络的入侵检测算法 [J]. 北京理工大学学报，2017，37（12）：1271-1275.

作者简介：赵晨洁（1995—），女，硕士，研究方向为深度学习。
吴　恋，女，硕士，讲师。
左　羽，男，教授，硕士生导师，CCF高级会员。
王永金，男，硕士。