Journal of Computer Applications
计算机应用,2021,41(7):1996 - 2002
ISSN 1001-9081
CODEN JYIIDU
2021-07-10
http://www.joca.cn

文章编号:1001-9081(2021)07-1996-07
DOI:10.11772/j.issn.1001-9081.2020081217

基于改进三元组网络和K近邻算法的入侵检测

王　月*,江逸茗,兰巨龙
(战略支援部队信息工程大学,郑州 450001)
(*通信作者电子邮箱tomato_wy1996@163.com)

摘　要:入侵检测一直以来被视作是保证网络安全的重要手段。针对网络入侵检测中检测准确率和计算效率难以兼顾的问题,借鉴深度度量学习思想,提出了改进三元组网络(imTN)结合K近邻(KNN)的网络入侵检测模型imTN-KNN。首先,设计了适用于解决入侵检测问题的三元组网络结构,以获取更有利于后续分类的距离特征;其次,为了应对移除传统模型中的批量归一化(BN)层造成过拟合进而影响检测精度的问题,引入了Dropout层和Sigmoid激活函数来替换BN层,从而提高模型性能;最后,用多重相似性损失函数替换传统三元组网络模型的损失函数。此外,将imTN的距离特征输出作为KNN算法的输入再次训练。在基准数据集IDS2018上的对比实验表明:与现有性能良好的基于深度神经网络的入侵检测系统(IDS-DNN)和基于卷积神经网络与长短期记忆(CNN-LSTM)的检测模型相比,在Sub_DS3子集上,imTN-KNN的检测准确率分别提高了2.76%和4.68%,计算效率分别提高了69.56%和74.31%。

关键词:网络安全;入侵检测;深度学习;三元组网络;K近邻;多重相似性损失函数
中图分类号:TP309.1　　**文献标志码**:A

Intrusion detection based on improved triplet network and K-nearest neighbor algorithm

WANG Yue*, JIANG Yiming, LAN Julong
(*Information Engineering University, Zhengzhou Henan* 450001 *China*)

Abstract: Intrusion detection is one of the important means to ensure network security. To address the problem that it is difficult to balance detection accuracy and computational efficiency in network intrusion detection, based on the idea of deep metric learning, a network intrusion detection model combining improved Triplet Network (imTN) and K-Nearest Neighbor (KNN) was proposed, namely imTN-KNN. Firstly, a triplet network structure suitable for solving intrusion detection problems was designed to obtain the distance features that are more conducive to the subsequent classification. Secondly, due to the overfitting problem caused by removing the Batch Normalization (BN) layer from the traditional model which affected the detection precision, a Dropout layer and a Sigmoid activation layer were introduced to replace the BN layer, thus improving the model performance. Finally, the loss function of the traditional triplet network model was replaced with the multi-similarity loss function. In addition, the distance feature output of the imTN was used as the input of the KNN algorithm for retraining. Comparison experiments on the benchmark dataset IDS2018 show that compared with the Deep Neural Network based Intrusion Detection System (IDS-DNN) and Convolutional Neural Networks and Long Short Term Memory (CNN-LSTM) based detection model, the detection accuracy of imTN-KNN is improved by 2.76% and 4.68% on Sub_DS3, and the computational efficiency is improved by 69.56% and 74.31%.

Key words: network security; intrusion detection; deep learning; triplet network; K-Nearest Neighbor (KNN); Multi-Similarity loss function

0　引言

信息通信系统(包括服务器、网络通信设备等)通常要处理大量敏感的用户数据,而这些数据容易受攻击。网络威胁和攻击带来了严重的安全问题由此激发了组织和个人对安全工具和系统越来越大的需求[1]。灵活、可靠、检测准确率高的实时入侵检测系统随着网络攻击技术的不断更新而成为应对安全问题的基本需求。

入侵检测系统根据网络数据来源可以分为基于网络的入侵检测系统和基于主机的入侵检测系统。基于网络的入侵检测系统通过从网络设备如交换机、路由器等收集获得的网络流量分析和检测攻击行为;基于主机的入侵检测系统可以从不同种类的日志文件、计算机资源利用率中提取系统活动事件,进而对异常进行检测。基于网络流量的入侵检测是本文的主要关注点。近年来,深度学习技术在入侵检测领域迅速发展并且出现了很多包括有监督分类方法[1-5]和无监督聚类方法[6-8]在内的相关方法。在基于深度学习的入侵检测方法中,基于深度神经网络的入侵检测系统(Deep Neural Network in Intrusion Detection System, IDS-DNN)和基于卷积神经网络与长短期记忆(Convolutional Neural Networks and Long Short Term Memory, CNN-LSTM)的检测模型是其中的典型代表。

收稿日期:2020-08-14;**修回日期**:2020-12-15;**录用日期**:2020-12-28。　**基金项目**:国家重点研发计划项目(2018YFB0804002)。
作者简介:王月(1996—),女,四川眉山人,硕士研究生,主要研究方向:网络空间安全;　江逸茗(1984—),男,江苏南通人,助理研究员,博士,主要研究方向:网络虚拟化、网络架构;　兰巨龙(1962—),男,河北张北人,教授,博士生导师,博士,主要研究方向:新一代信息网络。

IDS-DNN的特点是具有多层隐藏层并且相邻隐藏层之间是全连接方式,使得该模型具有很强的表征能力;但IDS-DNN的网络规模会随着输入样本的维度线性增加并且计算效率降低。在CNN-LSTM模型中,CNN的共享卷积核能够缩小神经网络规模并提高计算效率,LSTM能够学习时序特征;但CNN中的池化层会丢失大量有价值的信息,而且LSTM模型的计算复杂度较高。本文对目前的网络入侵检测方法进行调研,重点关注基于深度学习的网络入侵检测方法的研究,发现仍存在以下问题:1)大部分方法所用数据集比较过时,年代久远的KDD99数据集被大量用于验证,因此无法反映不断更新变化的攻击特征而缺乏实用性;2)现有的基于异常的入侵检测统存在高误报率并且在较新的数据集上由于复杂的网络攻击行为表现出较低的检测准确率;3)在分类任务中,尽管数据特征很重要,但有些表示形式和相应的诱导度量可能对分类起副作用。以上述三个问题为研究动机,为进一步提升分类模型的检测准确率和计算效率,利用三元组网络模型学习高效的距离表示,并且学习对检测结果更有用的特征,进而基于距离特征进行正常和异常攻击行为的识别[9]。本文提出一种改进三元组网络(improved Ttriplet Nnetwork, imTN)结合K近邻(K-Nearest Neighbor, KNN)算法的网络入侵检测模型imTN-KNN,以提升检测准确率和计算效率,并在最近公开的入侵检测数据集CSE-CIC-IDS2018(以下简称IDS2018)进行了验证。

本文的主要工作包括:

1)将经典的深度度量学习模型三元组网络引入网络入侵检测领域并对其进行多方面改进,而且通过实验验证了三元组网络适用于入侵检测领域。

2)结合KNN进一步提升检测准确率,将三元组模型输出的待测样本与各个正例样本的距离向量,以及待测样本与各个负例样本的距离向量作为KNN分类器的输入,由KNN分类器进一步学习得到更加准确的分类结果。

3)采用最近的公开数据集IDS2018进行实验评估,并与多个表现良好的模型进行比较。

1　相关研究

1.1　入侵检测方法

网络入侵检测方法可以分为基于统计的检测方法、基于信息论的检测方法、基于传统机器学习的检测方法和基于深度学习的检测方法。

1.1.1　基于统计和信息论的方法

基于统计的方法大多广泛地应用于信息技术发展初期,包括混合模型和主成分分析[10]等。基于信息论的方法,主要使用信息熵、条件信息熵、信息增益、信息成本作为数据集的特征衡量指标[11]。

1.1.2　基于传统机器学习的方法

传统机器学习包括有监督分类方法和无监督聚类方法。Heller等[12]将支持向量机(Support Vector Machine,SVM)用于网络异常检测,但假设训练集中不能存在噪声,在实际中不可行。Yang等[13]将基于规则的方法用于采用深度分析协议的IEC 60870-5-104数据采集与监视控制网络。基于传统机器学习的无监督聚类包括K均值聚类和层次聚类等方法。吴剑[14]提出了一种将遗传算法和K均值聚类结合的入侵检测方法以解决入侵检测中的特征选择问题。Noorbehbahani等[15]提出一种半监督流分类算法,使用增量聚类算法和监督方法创建初始分类模型,支持不平衡数据,并使用数量有限的带标签实例和有限的存储来实现高性能。传统机器学习入侵检测方法存在的主要问题包括:缺乏一套协商一致的输入特征以实现特定目标,例如网络安全、异常检测和流量分类等;与深度学习模型相比,传统机器学习方法的检测准确率不够高。因此在需要智能分析和高维数据学习时,传统机器学习通常不符合要求。

1.1.3　基于深度学习的方法

近年来,出现了很多基于深度学习的网络入侵检测方法,在检测性能上更具优势。Kim等[2]采用长短期记忆(Long Short Term Memory, LSTM)模型进行网络入侵检测,可以很好地检测到攻击,但未能解决误报率高的问题。在此基础上,Zhu等[16]在LSTM中引入注意力模型,在多分类问题上提高了准确性。Li等[3]在NSL-KDD公开数据集和边界网关协议(Border Gateway Protocol, BGP)路由数据集上对比了多种LSTM模型和门控循环单元(Gated Recurrent Unit, GRU)模型的检测准确率。Vinayakumar等[1]设计了一种深度神经网络入侵检测模型,并对网络结构和参数进行优化设计。另有一些研究提出的混合神经网络模型能取得良好检测效果,如Yuan等[17]和Saaudi等[18]将卷积神经网络与长短期记忆(CNN-LSTM)模型用于内部威胁检测,对日志文本数据进行用户行为建模分析;Agarwal等[19]同样利用CNN和LSTM的组合优势实现流量数据的攻击检测。但是这些方法大部分仍然使用过时的网络数据集进行验证,对当前现实世界的网络流量变化缺乏考虑。深度学习模型的计算效率远低于传统的机器学习方法,需要进一步提升深度学习模型计算效率以满足入侵检测的实时性要求。

1.2　三元组网络

深度度量学习已经广泛应用于图像识别和人脸检测等领域,利用不同对象的相似度分析来完成任务。三元组网络是由Hoffer等[9]提出的一种典型深度度量学习模型,核心思想是通过学习使相似样本之间的距离尽可能小而不相似样本之间的距离尽可能大。实验表明在多个图像数据集上三元组网络的分类准确率比CNN等模型更突出,为进一步利用三元组网络的性能优势,很多改进算法被提出。如Ustinova等[20]提出了基于直方图损失函数的三元组网络。在直方图损失函数中,相似样本对和不相似样本对排列组成概率分布,将相似样本对和不相似样本对的累计密度分布相乘,再进行积分得到直方图损失函数。通过直方图损失函数可以缩小相似样本和不相似样本之间的重叠。实验表明,在行人重识别数据集上基于直方图损失函数的方法拥有较好的识别率;但该方法的局限是相似性评估仍采用单一方式,即样本对的自相似性。Song等[21]认为采用传统的方法可能会使同类别相似性差异较大,并且提出了一种基于簇的相似度度量方法;但该方法需要采用大量贪婪搜索操作寻找簇中心以获得局部最优值,计算效率较低。Wang等[22]认为现有深度度量学习模型的不足之处是普遍采用单一的相似度度量,因此提出了一种多重相似度损失函数,结合了样本对之间的自相似性、负样本对之间的相对相似性以及正样本对之间的相对相似性等多种相似度衡量方式。实验表明该方法在多个图像检索数据集上的性能优于其他方法。

不少相关研究证明了三元组网络的表现优于传统的深度学习模型,目前主要应用于图像处理领域。本文探索了如何

将三元组网络用于入侵检测领域，并通过优化设计网络结构、损失函数以进一步提升入侵检测方法的检测准确率、计算效率等性能指标。

2 算法设计

深度度量学习过程中产生了相似度距离特征，可用于分类。在此首次将一种典型的名为三元组网络的深度度量模型应用于网络入侵检测，并改进了传统三元组网络以在网络入侵检测中发挥优势，而且结合KNN分类器进一步学习得到二分类结果，实现高精度网络入侵检测。

2.1 传统三元组网络

三元组网络中，三个样本$\boldsymbol{a}$、$\boldsymbol{b}$和$\boldsymbol{c}$作为输入。其中，样本$\boldsymbol{a}$和$\boldsymbol{b}$属于同一类别，样本$\boldsymbol{c}$属于不同类别。假设样本$\boldsymbol{a}$和样本$\boldsymbol{b}$间的距离为d_1，样本$\boldsymbol{a}$和样本$\boldsymbol{c}$间的距离为d_2。学习目标是最小化同类样本之间的距离而最大化不同类样本之间的距离。

$$\begin{cases} d_1 = \| \boldsymbol{a} - \boldsymbol{b} \| \\ d_2 = \| \boldsymbol{a} - \boldsymbol{c} \| \end{cases} \tag{1}$$

其中距离d_i用欧氏距离计算，公式如下：

$$d_i = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{2}$$

距离特征d_1和d_2归一化后，距离向量中各元素和等于1，产生输出向量：

$$\boldsymbol{p} = \mathrm{softmax}([d_1, d_2]) \tag{3}$$

每个($\boldsymbol{a}$,$\boldsymbol{b}$,$\boldsymbol{c}$)三元组所对应的输出向量的取值范围是[0，1]。传统三元组网络架构如图1所示。

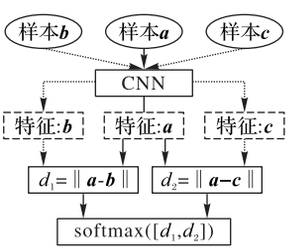

图1 三元组网络架构

Fig. 1 Architecture of triplet network

在2.3节中详细描述了对传统三元组网络的改进，包括卷积层结构和参数、批量归一化(Batch Normalization，BN)层和损失函数以最大化入侵检测准确率和计算效率。

2.2 KNN

KNN因为简单有效且容易实现而广泛应用[23]。KNN算法的基本思想：首先，把训练样本作为欧氏空间的点存放，所有样本对应于n维空间的点，根据客观事实或专家经验，给训练数据设定分组；然后，挑选训练样本集中与待分类样本距离最近的k个样本；最后，根据这距离最近的k个样本的类别标签对待预测样本进行分类。

近邻数k是KNN的参数，对模型训练精度起决定性作用，本文主要通过实验确定最优k值。

2.3 改进三元组网络和KNN组合模型

三元组网络预测模型输出样本间的距离向量，将待测样本与正例样本距离求和得到d_1，待测样本与负例样本距离求和得到d_2。理想情况下，当$d_1 \leqslant T$，认为待测样本是正例；当$d_1 > T$，认为待测样本是负例。用于网络入侵检测时，由于正例样本间也存在较大差异，难以确定合适的阈值T。为解决这个问题，将三元组模型输出的距离向量作为KNN分类器的输入，由KNN分类器进一步学习得到二分类结果。

为提升KNN的计算效率和检测精度，将得到的距离向量按照先后次序分成s组，对每组向量求平均值，将这s个平均距离向量作为KNN的输入。imTN-KNN模型架构如图2所示。

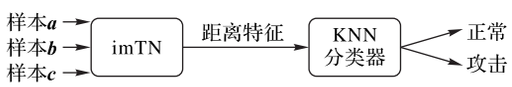

图2 imTN-KNN架构

Fig. 2 imTN-KNN architecture

适用于网络入侵检测领域的改进三元组网络模型中CNN网络结构设计如表1所示。

表1 改进三元组网络采用的CNN结构

Tab. 1 CNN structure employed by improved triplet network

层序	CNN
1	卷积层(32个神经元，卷积核大小3)
2	卷积层(32个神经元，卷积核大小3)
3	卷积层(32个神经元，卷积核大小3)
4	卷积层(32个神经元，卷积核大小3)
5	池化层(池化大小为2)
6	卷积层(64个神经元，卷积核大小3)
7	卷积层(64个神经元，卷积核大小3)
8	卷积层(64个神经元，卷积核大小3)
9	卷积层(64个神经元，卷积核大小3)
10	池化层(池化大小为2)

在改进三元组网络中移除了BN层。BN层在图像处理领域主要应用于输入图像的数据分布和输出数据的分布不一致或有很大变动的情况，它在该应用领域具有良好的表现；但在网络入侵检测领域，输入与输出的数据分布一般一致，因此去掉它影响不大。相反，加入了BN层导致输入输出的数据分布发生了不必要的变化从而造成了信息损失，进而给检测准确率的提升带来了负面影响。此外，移除BN层可以减小内存消耗并提升计算效率[24]。

损失函数一般用于机器学习中预测模型的预测准确率衡量。损失函数的选择需要考虑很多问题，并且发现一个适合于大部分数据集的损失函数比较困难。

在三元组网络中，损失函数的设计对于提升模型性能指标比较关键，近年来出现了不少有关三元组损失函数的研究。Hoffer等[9]提出了主要关注同类样本和不同类样本的相似性的经典三元组损失函数，通过训练减小同类样本的相似距离而增大不同类样本之间的相似距离。这种方法生成的大量成对样本是高度冗余的且包含很多无信息样本。后来又出现了很多其他类型的用于度量学习的损失函数，包括提升结构损失函数[25]、直方图损失函数[20]、层次三元组损失函数[26]等。经典三元组损失函数在批量训练大小较小时很难利用所有的样本对之间的关系，为了应对这个问题，研究者提出了提升结构损失函数；但结构损失函数仅随机采样相等数量的正例样本对和负例样本对，依然损失了大量信息。直方图损失函数将同类样本对和不同类样本对进行排列组成概率分布，通过概率分布使得不同类样本的相似性远小于同类样本的相似

性。直方图损失函数的优点是不需要额外参数,并且不需要困难样本挖掘,但缺点是计算复杂度较高。在层次三元组损失函数中,建立了所有类的层次树,样本对的选择依据一个动态的边界阈值。层次三元组损失函数虽然提升了检测准确率等性能但实现比较复杂。Wang等[22]对度量学习中的损失函数进行了全面深入分析,研究了这些损失函数的共性,发现关键的影响因素是数据样本的包含自相似度和相对相似度在内的多种相似度,其中相对相似度主要取决于其他样本对。但大多数现有方法仅探索了自相似度和相对相似度其中的一个因素,于是提出了多重相似性损失函数。本文最终采用Wang等[22]提出的多重相似性损失函数,它从多个角度对相似性进行衡量,克服了以往对相似度衡量的片面性。具体地,多重相似性损失函数能够从自相似性、负例相对相似性和正例相对相似性三方面评估损失值,该损失函数表达式为:

$$L_{\mathrm{MS}}=\frac{1}{m}\left\{\frac{1}{\alpha}\log\left[1+\sum_{j\in P_i}\mathrm{e}^{-\alpha(S_{ij}-\lambda)}\right]+\frac{1}{\beta}\log\left[1+\sum_{j\in N_i}\mathrm{e}^{\beta(S_{ij}-\lambda)}\right]\right\} \tag{4}$$

其中:m为训练样本数,S_{ij}表示两个样本i和j的相似度。在改进三元组网络模型中采用多重相似函数获得了两方面的收益:一是通过对嵌入大小*embedding_size*进行调参的方式明显提升实验部分的检测准确率;二是提升了模型训练的收敛速度,训练过程中经过第一次迭代就获得了最好的检测准确率,大幅节省了训练时间、提升了计算效率。

此外,使用高效的自适应学习率优化器Adam[27],为不同的参数设计独立的自适应性学习率。学习率值设定为0.000 1,$\beta_1=0.9$,$\beta_2=0.999$。

2.4　imTN-KNN算法流程

算法主要包括数据预处理、模型训练和模型测试等主要步骤,模型训练和模型测试阶段通过不断迭代来得到最优的网络参数(如图3所示)。

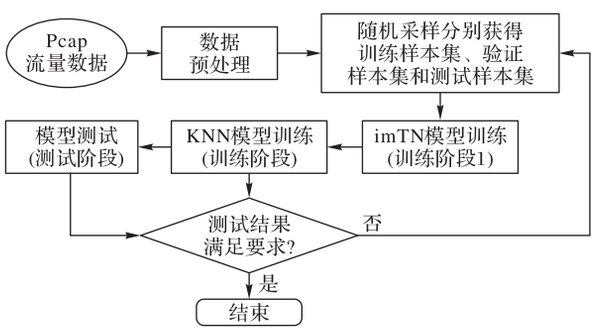

图3　imTN-KNN流程

Fig. 3　Flowchart of imTN-KNN

公开基准数据集IDS2018包含了提取的80多个特征数据,这些数据需要预处理,包含两个操作:一是将无穷大或者空值异常数据进行修正和补齐;二是进行归一化处理。为保证数据尽量不损失信息并且确保数据均映射到[0,1]区间内,采用最小值-最大值函数(Min-Max)进行归一化以实现对原始数据的等比缩放。函数Min-Max定义为:

$$x_{\mathrm{norm}}=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{5}$$

经过预处理的数据集被分成训练数据集和测试数据集分别用于训练和测试阶段。以上所有样本子集都从总样本集中随机选取,不作人为筛选。

3　实验评估

实验硬件环境包括:Intel Xeon(Cascade Lake) Platinum 82692.5 GHz/3.2 GHz的4核心中央处理单元(Central Processing Unit, CPU),8 GB内存。在基准数据集IDS2018上进行实验评估,与现有性能良好的深度学习算法进行对比,验证imTN-KNN的有效性。此外,imTN-KNN还与浅层学习方法主成分分析(Principal Component Analysis,PCA)和KNN相结合的PCA+KNN、SVM[28]、PCA+SVM[28]和朴素贝叶斯(Naive Bayes,NB)[29]进行了对比,验证了改进三元组网络模型进行特征提取的高效性。

3.1　数据集

IDS2018是一个包含大量网络流量和系统日志的数据集,通过10天的数据采集获得,每天的数据形成一个数据子集,总大小超过400 GB。该数据集包括7种攻击类型和16种子类型攻击的有场景标记的数据,包括暴力破解、拒绝服务(Denial of Service,DoS)攻击、监视网络攻击和渗透攻击等。通过特征生成工具CICFlowMeter-V3[30]分析IDS2018数据集,生成约80种特征数据,表征了网络流量和数据包的活动行为。在相关研究基础上,本文选取两个检测精度比较高的数据子集(分别简写为Sub_DS1和Sub_DS2)和一个检测精度比较低的数据子集(简写为Sub_DS3)作为实验的测试集。这三个数据子集在已有模型中的检测准确率差异较大,对验证模型具有代表意义,数据子集的说明如表2所示。

表2　IDS2018三个数据子集概要

Tab. 2　Summary of three data subsets of IDS2018

数据子集	采集时间	攻击类型	样本总数
Sub_DS1	Wednesday-14-02-2018	Benign	663 808
		FTP-BruteForce	193 354
		SSH-Bruteforce	187 589
Sub_DS2	Thursday-15-02-2018	Benign	988 050
		DoS-GoldenEye	41 508
		DoS-Slowloris	10 990
Sub_DS3	Thursday-01-03-2018	Benign	235 778
		Infilteration	92 403

3.2　对比算法

基于深度学习的入侵检测算法近年来得到广泛研究,相关研究表明:IDS-DNN和CNN-LSTM在性能指标上达到了良好的效果,前者能够自动提取高级特征,后者在捕捉时间和空间特征上具有优势。基于上述原因,本文选择IDS-DNN和CNN-LSTM两种深度学习模型作为对比模型。

IDS-DNN结构包含6个Dense层和1个激活层。为防止过拟合,Dense层之间加入Dropout层。每个Dense层的维数如表3所示。激活层采用Sigmoid函数,Dense层激活函数采用线性整流单元(Rectified Linear Unit,ReLU)函数。损失函数为二元交叉熵函数,优化函数为Adam[27]。

CNN-LSTM[19]混合网络结构如表4所示,其损失函数为稀疏分类交叉熵函数,优化函数为Adam。

表 3 IDS-DNN 结构

Tab. 3 Structure of IDS-DNN

层序	层描述
1	Dense 层(神经元个数:1024)
2	Dropout 层(丢弃比率:0.01)
3	Dense 层(神经元个数:768)
4	Dropout 层(丢弃比率:0.01)
5	Dense 层(神经元个数:512)
6	Dropout 层(丢弃比率:0.01)
7	Dense 层(神经元个数:256)
8	Dropout 层(丢弃比率:0.01)
9	Dense 层(神经元个数:128)
10	Dropout 层(丢弃比率:0.01)
11	Dense 层(神经元个数:1)
12	激活层(Sigmoid 函数)

表 4 CNN-LSTM 结构

Tab. 4 Structure of CNN-LSTM

层序	层描述
1	卷积层(32 个神经元,卷积核大小 3)
2	卷积层(32 个神经元,卷积核大小 3)
3	卷积层(32 个神经元,卷积核大小 3)
4	卷积层(32 个神经元,卷积核大小 3)
5	池化层(池化大小为 2)
6	卷积层(64 个神经元,卷积核大小 3)
7	卷积层(64 个神经元,卷积核大小 3)
8	卷积层(64 个神经元,卷积核大小 3)
9	卷积层(64 个神经元,卷积核大小 3)
10	池化层(池化大小为 2)
11	LSTM 层(70 个单元)
12	Dropout 层 丢弃比率:0.01
13	Dense 层 (神经元个数:1)
14	激活层(Sigmoid 函数)

3.3 衡量指标

采用全局准确率 *Acc*(Accuracy)、正例准确率 *AccP*(Accuracy of Positives)、负例准确率 *AccN*(Accuracy of Negtives)、假正率 *FPR*(False Positive Rate)、真正率 *TPR*(True Positive Rate)和模型训练时间 *Training_Time* 等指标对模型进行对比分析[1]。

Acc = (真阳性 + 真阴性)/样本总数

AccP = 真阳性/正例总数

AccN = 真阴性/负例总数

FPR = 假阳性/(假阳性 + 真阴性)

TPR = 真阳性/(真阳性 + 假阴性)

本文将训练时间用作易于衡量的计算效率的指标。减少模型的训练时间不是提高计算效率的唯一目标,但训练时间通常与其他计算效率指标呈正相关关系,例如模型测试时间或在线响应时间。He 等[31]详细分析了 CNN 模型的在训练阶段的时间复杂度。该文献中涉及到的相同的理论公式同样适用于分析训练时间和测试时间。基于以上考虑,本文采用训练时间作为检测计算效率的衡量指标。

3.4 实验对比分析

首先,与检测准确率较高的浅层机器学习方法 SVM、PCA-SVM 以及 NB 进行对比,imTN-KNN 只采用一层包含 32 个单元的卷积层就能够获得最高准确率,而且对比时已将 SVM[28]、PCA-SVM[28]、NB[29]方法中的参数调整到最优值。在这种情形下,尽管因为深度学习模型本身的复杂性导致 imTN-KNN 的归一化训练时间大于其他浅层机器学习方法,但在调整检测计算效率与检测准确率性能的平衡方面,imTN-KNN 具有更强的自由度(如表 5 所示)。关注检测准确率的网络入侵检测应用场合更适合采用 imTN-KNN 等深度学习模型。此外,对于某些动态复杂场景可以将 imTN-KNN 深度学习模型和 PCA+SVM 等浅层学习模型结合起来使用。

表 5 imTN-KNN 与浅层机器学习模型性能对比

Tab. 5 Performance comparison between imTN-KNN and shallow machine learning models

模型	全局准确率	归一化训练时间
imTN-KNN	0.762	1.000
SVM	0.722	0.328
PCA+SVM	0.723	0.221
NB	0.713	0.173

图 4 呈现了 imTN-KNN、IDS-DNN、CNN-LSTM 和 PCA-KNN 在数据子集上的 *Acc* 对比,图 5 和图 6 分别为不同数据集上四个算法的 *AccP* 和 *AccN* 分析。可以看出,在 Sub_DS1、Sub_DS2 和 Sub_DS3 三个数据子集上,imTN-KNN 的性能都优于其他方法。其中在 Sub_DS3 数据子集上,相比 IDS-DNN、CNN-LSTM 和 PCA-KNN,imTN-KNN 的 *Acc* 分别提升 2.76%、4.68% 和 6.53%。值得注意,在 Sub_DS3 数据子集上所有模型的表现都不够理想,说明渗透攻击和正常流量的区分度不高,现有模型对这种攻击类型的检测率依然偏低。

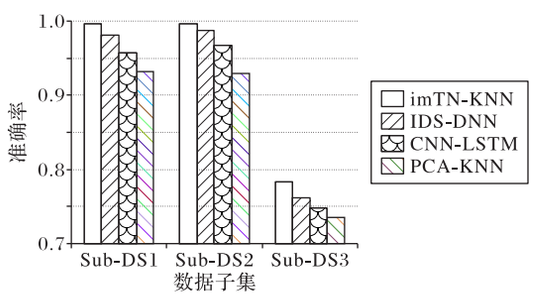

图 4 识别准确率对比图

Fig. 4 Comparison of Acc

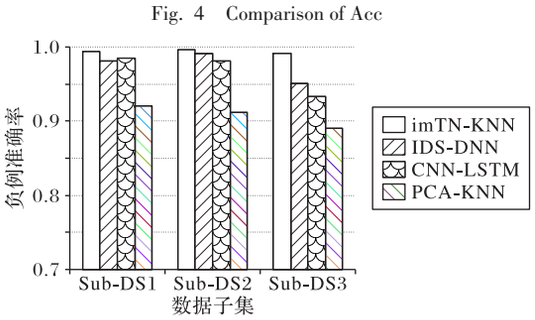

图 5 负例识别准确率对比

Fig. 5 Comparison of AccN

在数据集 Sub_DS3 上,检测模型的 *Acc* 随训练样本个数的变化如图 7 所示。可以看出,imTN-KNN 和 IDS-DNN 在小样本训练时比 CNN-LSTM 更具优势,但随着训练样本数增多,imTN-KNN 和 IDS-DNN 的 *Acc* 逐渐缓慢降低,而 CNN-LSTM 的 *Acc* 开始缓慢上升至逐渐超过 DNN 并接近 imTN-KNN。训练样本数在从 2 000 到 140 000 变化的过程中,imTN-KNN 的 *Acc* 总是高于其余三个方法,尤其在训练样本数为 2 000 时,imTN-

KNN 的 *Acc* 明显高于 IDS-DN、CNN-LSTM 和 PCA-KNN,说明 imTN-KNN 更适合小样本场景,这与在图像检测领域的性能表现一致。

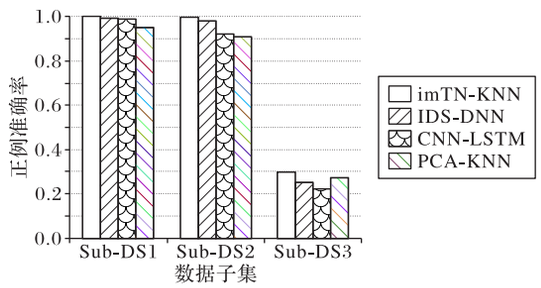

图6　正例识别准确率对比

Fig. 6　Comparison of AccP

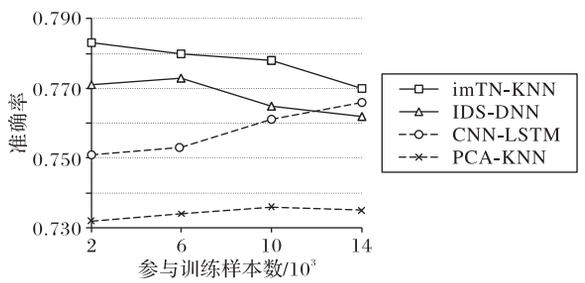

图7　训练样本数对检测准确率的影响

Fig. 7　Influence of training sample number on detection accuracy

图8展示了其他参数保持不变的情况下,KNN中参数 k 值在10到170变换过程中,imTN-KNN 和 PCA-KNN 检测准确率的变化。从图中可以看出两个方法的检测准确率都随着 k 值的变大先变大再变小并且变化较大,最优 k 值都是50。虽然 imTN-KNN 的检测准确率受 k 值的影响更大,但 imTN-KNN 的检测准确率总是明显高于PCA-KNN。

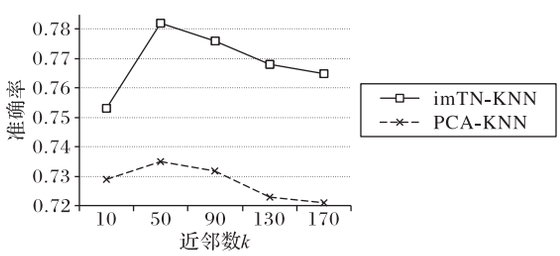

图8　KNN中参数 k 对检测准确率的影响

Fig. 8　Influence of parameter k in KNN on Acc

在数据子集 Sub_DS3 上,四个方法的受试者工作特征(Receiver Operating Characteristic, ROC)曲线由图9所示,可以看出 imTN-KNN 的总是优于其余方法。相比 IDS-DNN、CNN-LSTM 和 PCA-KNN,imTN-KNN 的 ROC 曲线下面的面积(Area Under ROC Curve, AUC)分别提升了 6.53%、7.03%、8.10%。

图10呈现了在训练迭代次数 e 从1到10变化过程中,imTN-KNN、IDS-DNN 和 CNN-LSTM 三个模型 *Acc* 的变化。这三个模型取得最优 *Acc* 值时,对应 e 的值分别为1、7、9,说明在模型训练时 imTN-KNN 的收敛速度远快于 IDS-DNN 和 CNN-LSTM;这三个模型在达到最优 *Acc* 时所用的归一化训练时间分别为0.256 9,0.843 9和1。imTN-KNN 的归一化训练时间远小于其余两个模型,相较于 IDS-DNN 和 CNN-LSTM,imTN-KNN 缩短训练时间分别高达69.56%和74.31%。

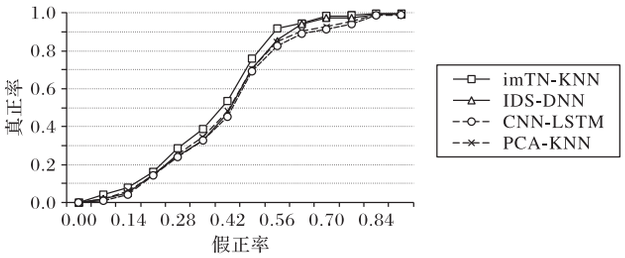

图9　ROC对比

Fig. 9　Comparison of ROCs

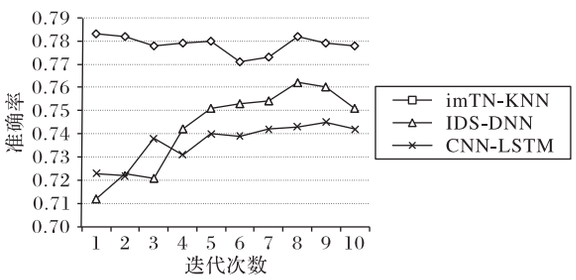

图10　迭代次数对模型准确率的影响

Fig. 10　Influence of iteration number on accuracy

4　结语

针对用深度学习解决网络入侵检测问题时计算效率普遍低下的问题,本文借鉴深度度量学习思想,以距离特征作为分类标准,提出了 imTN-KNN 模型。从 CNN 结构和参数角度改进了传统三元组网络,用 Dropout 层和 Sigmoid 激活函数层替换了 BN 层。此外,利用高效的 KNN 分类算法学习距离特征,解决了依据特定阈值进行简单分类导致检测精度不高的问题。在公开数据集 IDS2018 上的实验结果表明,与其他算法相比,imTN-KNN 能更好地兼顾检测准确率和计算效率。在后续研究中,为提高对渗透攻击的识别率,需要在保证检测率的计算效率的同时尽可能多地学习原始流量中包含的信息以进一步提高入侵检测模型的检测准确率和检测计算效率等多种性能。

参考文献(References)

[1] VINAYAKUMAR R, ALAZAB M, SOMAN K P, et al. Deep learning approach for intelligent intrusion detection system [J]. IEEE Access, 2019, 7: 41525-41550.

[2] KIM J, KIM J, THI THU H L, et al. Long short term memory recurrent neural network classifier for intrusion detection [C]// Proceedings of the 2016 International Conference on Platform Technology and Service. Piscataway: IEEE, 2016: 1-5.

[3] LI Z, RIOS A L G, XU G, et al. Machine learning techniques for classifying network anomalies and intrusions [C]// Proceedings of the 2019 IEEE International Symposium on Circuits and Systems. Piscataway: IEEE, 2019:1-5.

[4] KIM J, SHIN Y, CHOI E. An intrusion detection model based on a convolutional neural network [J]. Journal of Multimedia Information System, 2019, 6(4): 165-172.

[5] GURUNG S, GHOSE M K, SUBEDI A. Deep learning approach on network intrusion detection system using NSL-KDD dataset [J]. International Journal of Computer Network and Information Security, 2019, 11(3): 8-14.

[6] ZONG B, SONG Q, MIN M R, et al. Deep autoencoding Gaussian

mixture model for unsupervised anomaly detection[EB/OL]. [2020-11-12]. https://openreview.net/pdf? id=BJJLHbb0-.

[7] LUDWIG S A. Intrusion detection of multiple attack classes using a deep neural net ensemble [C]// Proceedings of the 2017 IEEE Symposium Series on Computational Intelligence. Piscataway: IEEE, 2017: 1-7.

[8] ESKIN E. Anomaly detection over noisy data using learned probability distributions [C]// Proceedings of the 17th International Conference on Machine Learning. San Francisco: Morgan Kaufmann Publishers Inc., 2000:255-262.

[9] HOFFER E, AILON N. Deep metric learning using triplet network [C]// Proceedings of the 2015 International Workshop on Similarity-Based Pattern Recognition, LNCS 9370. Cham: Springer, 2015: 84-92.

[10] FADLULLAH Z M, TANG F, MAO B, et al. State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems [J]. IEEE Communications Surveys and Tutorials, 2017, 19(4): 2432-2455.

[11] SHYU M L, CHEN S C, SARINNAPAKORN K, et al. A novel anomaly detection scheme based on principal component classifier [EB/OL]. [2020-11-12]. https://homepages.laas.fr/owe/METROSEC/DOC/FDM03.pdf.

[12] HELLER KA, SVORE K M, KEROMYTIS A D, et al. One class support vector machines for detect anomalous windows registry accesses [EB/OL]. [2020-11-12]. https://angelosk.github.io/Papers/ocsvm.pdf.

[13] YANG Y, McLAUGHLIN K, LITTLER T, et al. Rule-based intrusion detection system for SCADA networks [C/OL]// Proceedings of the 2nd IET Renewable Power Generation Conference. Stevenage: IET, 2013 (2013-09-09) [2020-03-15]. https://digital-library.theiet.org/content/conferences/10.1049/cp.2013.1729.

[14] 吴剑. 基于特征选择的无监督入侵检测方法[J]. 计算机工程与应用, 2011, 47(26): 79-82. (WU J. Unsupervised intrusion detection based on feature selection [J]. Computer Engineering and Applications, 2011, 47(26): 79-82.)

[15] NOORBEHBAHANI F, FANIAN A, MOUSAVI R, et al. An incremental intrusion detection system using a new semi-supervised stream classification method [J]. International Journal of Communication Systems, 2017, 30(4): No. e3002.

[16] ZHU M, YE K, WANG Y, et al. A deep learning approach for network anomaly detection based on AMF-LSTM [C]// Proceedings of the 2018 IFIP International Conference on Network and Parallel Computing, LNCS 11276. Cham: Springer, 2018: 137-141.

[17] YUAN F, CAO Y, SHANG Y, et al. Insider threat detection with deep neural network [C]// Proceedings of the 2018 International Conference on Computational Science, LNCS 10860. Cham: Springer, 2018: 43-54.

[18] SAAUDI A, AL-IBADI Z, TONG Y, et al. Insider threats detection using CNN-LSTM model [C]// Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence. Piscataway: IEEE, 2018: 94-99.

[19] AGARWAL S, TYAGI A, USHA G. A deep neural network strategy to distinguish and avoid cyber-attacks [M]// DASH S S, LAKSHMI C, DAS S, et al. Artificial Intelligence and Evolutionary Computations in Engineering Systems. Singapore: Springer, 2020:673-681.

[20] USTINOVA E, LEMPITSKY V. Learning deep embeddings with histogram loss [C]// Proceedings of the 30th International Conference on Neural Information Processing Systems. Red Hook, NY: Curran Associates Inc., 2016:4177-4185.

[21] SONG H O, JEGELKA S, RATHOD V, et al. Deep metric learning via facility location [C]// Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2017: 2206-2214.

[22] WANG X, HAN X, HUANG W, et al. Multi-similarity loss with general pair weighting for deep metric learning [C]// Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2019: 5017-5025.

[23] 孙岩,吕世聘,王秀坤,等. 基于结构学习的KNN分类算法[J]. 计算机科学, 2007, 34(12):184-186, 237. (SUN Y, LYU S P, WANG X K, et al. K-nearest neighbor algorithm based on learning structure [J]. Computer Science, 2007, 34(12): 184-186, 237.)

[24] IOFFE S, SZEGEDY C. Batch normalization: accelerating deep network training by reducing internal covariate shift [EB/OL]. [2020-08-12]. https://arxiv.org/pdf/1502.03167.pdf.

[25] GE W, HUANG W, DONG D, et al. Deep metric learning with hierarchical triplet loss [C]// Proceedings of the 2018 European Conference on Computer Vision, LNCS 11210. Cham: Springer, 2018: 2772-288.

[26] SONG H O, XIANG Y, JEGELKA S, et al. Deep metric learning via lifted structured feature embedding [C]// Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2016: 4004-4012.

[27] KINGMA D P, BA J L. Adam: a method for stochastic optimization [EB/OL]. [2020-08-12]. https://arxiv.org/pdf/1412.6980.pdf.

[28] GLASS-VANDERLAN T R, IANNACONE M D, VINCENT M S, et al. A survey of intrusion detection systems leveraging host data [EB/OL]. [2020-08-12]. https://arxiv.org/pdf/1805.06070.pdf.

[29] ADEK R T, ULA M. A survey on the accuracy of machine learning techniques for intrusion and anomaly detection on public data sets [C]// Proceedings of the 2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics. Piscataway: IEEE, 2020:19-27.

[30] CICFlowMeter [CP/OL]. [2020-05-29]. https://www.unb.ca/cic/research/applications.html#CICFlowMeter.

[31] HE K, SUN J. Convolutional neural networks at constrained time cost [C]// Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE, 2015: 5353-5360.

This work is partially supported by the National Key Research and Development Program of China (2018YFB0804002).

WANG Yue, born in 1996, M. S. candidate. Her research interests include cyberspace security.

JIANG Yiming, born in 1984, Ph. D., research assistant. His research interests include network virtualization, network architecture.

LAN Julong, born in 1962, Ph. D., professor. His research interests include new generation information networks.