基于深度学习的配电网无线通信入侵检测系统

刘文军[1],郭志民[2],吴春明[3],阮 伟[4],周伯阳[2],周 宁[2],吕 卓[2]
(1. 国网河南省电力公司,河南郑州 450000;2. 国网河南省电力公司电力科学研究院,河南郑州 450000;
3. 浙江大学计算机科学与技术学院,浙江杭州 310027;4. 浙江大学控制科学与工程学院,浙江杭州 310027)

摘 要: 在采用无线通信接入的配电网中,入侵检测系统(IDS)通过分析通信网中传输数据来判断入侵事件.为提高检测的准确性,本文将深度学习理论应用于 IDS,提出了一种面向配电网无线通信网络新型入侵检测系统,由带有门控循环单元、多层感知器和 Softmax 的循环神经网络组成.攻击测试基准实验结果表明 IDS 防御的有效性,在 KDD99 测试数据集上,其误报率为 0.06%,总检出率为 96.43%;在 NSL-KDD 测试数据集上,其误报率低至 0.86%,总检出率则为 99.33%.

关键词: 配电网;无线网;入侵检测;深度学习;递归神经网络
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112(2020)08-1538-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.08.011

A Deep Learning Based Intrusion Detection System for Electric Distribution Grids

LIU Wen-jun[1], GUO Zhi-min[2], WU Chun-ming[3], RUAN Wei[4], ZHOU Bo-yang[2], ZHOU Ning[2], LÜ Zhuo[2]
(1. *State Grid Henan Electric Power Company, Zhengzhou, Henan* 450000, *China*;
2. *State Grid Henan Electric Power Research Institute, State Grid Henan Electric Power Company, Zhengzhou, Henan* 450000, *China*;
3. *College of Computer Science and Technology, Zhejiang University, Hangzhou, Zhejiang* 310027, *China*;
4. *College of Control Science and Engineering, Zhejiang University, Hangzhou, Zhejiang* 310027, *China*)

Abstract: In an electric power distribution grid using wireless communication access, IDS is used to decide system the intrusive event through analyzing the network transmission data. In this paper, to improve the detection accuracy, a deep learning theory is studied for the IDS in the wireless communication network of a power distribution grid. The proposed Recurrent Neural Network (RNN) model is composed of Gated Recurrent Unit (GRU), Multi-Layer Perceptron (MLP) and Softmax. The experimental results on the attack testing baseline demonstrate the effectiveness of the IDS defenses. In the KDD99 test data, its negative error rate and accuracy are with 0.06% and 96.43%, and in the NSL-KDD test data, those statistics are 0.86% with 99.33%, respectively.

Key words: electric distribution network; wireless network; intrusion detection; deep learning; recurrent neural network (RNN)

1 引言

配电网主要实现 110kV 及以下的台区用户端的供电覆盖,近年来随着智能电网的建设,配电网终端 DTU(Distribution Terminal Unit)、FTU(Feeder Terminal Unit)和 TTU(Transformer Terminal Unit)等大量采用了无线通信方式接入到配电网主站中,无线通信信道承载着遥控、遥测和遥信等重要的业务信息,无线攻击会造成信息篡改或泄露,可导致电网控制失去准确性和可信性,引发级联式的电网故障或设备损坏问题,进而造成经济损失,更会危及人身和社会安全,相关安全防御问题已逐渐成为目前的研究热点问题.

收稿日期:2018-04-18;修回日期:2018-06-06;责任编辑:诸叶梅

入侵检测系统(Intrusion Detection System,简称IDS)是一种用于检测网络入侵的安全管理系统,能主动保护系统应对网络攻击. IDS 的检测方法主要分为两类:误用检测和异常检测[1]. 误用检测是一种基于知识库的检测技术,通过匹配特征或规则来识别入侵,需要构建一个特征库以确认入侵行为,无法检测未知的攻击. 相比之下,异常检测是一种基于行为的检测技术,通过检查网络实际行为是否偏离其正常的行为来检测未知的攻击.

许多关于机器学习的研究已经开发出具有机器智能的入侵检测技术,取得了良好的效果,如向量机、人工神经网络和遗传算法. 然而,由于配电网需要考虑无线通信结合电力业务检测的复杂性,维度较大、规则复杂,因此传统基于人工设计特征的机器学习方法越来越难以适应,需要设计和实现一种能够自动提取入侵特征和分析的学习方法. 近年来,循环神经网络(Recursive Neural Networks,RNN)技术开始进入一个快速发展时期,RNN 建立多个隐藏的非线性神经元层,变换多维数据空间实现准确分类,配电入侵行为可被抽象为来自于底层无线网络的特定时间序列事件. 因此,RNN 能为配网业务的入侵事件识别分类带来更高的准确性,适合于构建相应的 IDS 入侵识别技术.

为了提高配电网无线通信下 IDS 检测准确性,本文提出了一种适用于智能配电网的基于深层循环神经网络的 IDS 模型,该模型由门控循环单元(Gated Recurrent Unit,简称 GRU)、多层感知模块和 Softmax 传输模块构成. 本文的主要贡献包括:提出了一种新的基于深层神经网络的 IDS,它利用门控循环单元作为记忆单元,结合多层感知模块来识别网络入侵. 目前,将门控循环单元用于入侵检测在学术界和工业界尚不多见.

本文对所提出的系统进行了详细的评价,并利用 KDD99[2] 和 NSL-KDD[3] 的数据集进行了详细的评估. 这两个数据集在以前的工作中得到了广泛的应用,因此可以直接用这两个数据集进行性能比较. 实验结果表明,相对于 IDS 经典的长短时记忆(Long Short-Term Memory,LSTM)单元,GRU 单元更加适合于用作 RNN 的主要记忆单元. 该 IDS 系统不需要借助于人工来对特征进行选择,从而能够显著地减少网络安全防御的工作量.

2　相关工作

自从 Denning 首次提出入侵检测模型[4],近年来,学者们已经使用了各种不同的入侵检测方法. 从概率统计到机器学习和数据挖掘方法,尝试提取特定的模式,从而实现攻击流量的区分.

不少工作采用支持度向量机(Supporting Vector Machine,SVM)的经典数据分类方法来识别异常流量. 最近的研究工作是 Hussain 等人[5] 所提出的一种两阶段混合分类方法,在第一阶段,采用 SVM 进行异常检测,第二阶段采用人工神经网络进行误用检测. 然而,经典的分类算法不能自主调整预处理和特征提取的参数,需要专家的人工参与来完成学习和分类的目标.

深度学习是神经网络研究的一个新热点,在入侵检测领域取得了良好的效果. Ma 等人[6] 采用了光谱聚类从网络流量提取特征,并使用多层深神经网络(Deep Neural Networks,简称 DNN)来检测攻击类型. Kang 等人[7] 提出了基于 DNN 车载网络的有效 IDS. 在控制器区域网络的总线上,系统使用 DNN 来提供每个类辨别正常和攻击数据包的概率. 为了充分利用深度学习,系统通过预先训练的深度信任网络(Deep Belief Network,简称 DBN)对参数进行初始化,从而提高了检测精度. Erfani 等人[8] 提出了一个混合模型,把深度信任网络(DBN)与一个单类向量机结合在一起. Javaid 等人[9] 采用了一种称为自学学习的深度学习技术来构建网络入侵检测系统(Network IDS,简称 NIDS),实现了基于 NIDS 和 Softmax 回归的 IDS 系统. Staudemeyer[10] 首次指出,一个 LSTM 的循环神经网络可用于入侵检测. LSTM 可以学会回溯时间,从时间角度发现一些关联. Kimet-al[11] 也使用 LSTM 结构去构建一个 IDS 模型,该模型由 KDD99 数据集训练得出,表明该 IDS 的入侵检测准确性高,证明了 LSTM 结构适合于入侵检测. 然而,相对于传统的机器学习算法,该方法对诸如检测率等性能指标的改进没有起到特别显著的效果. 所以需要进一步改进. 此外,LSTM 是一个相对复杂的结构,这对 IDS 的实时处理性能有一定的负面作用.

3　系统局部组件

3.1　循环神经网络

RNN 是传统前馈神经网络的一种后续扩展. 在传统的 RNN 模型中,数据流是单向的,即从输入层到隐藏层,最后到输出层. 虽是相邻的层也可能完全连接,但同一层中的节点不是完全连接的. 因此,在处理与时间相关的数据方面,传统的神经网络受到许多限制. 然而,RNN 却有不同之处:在后续时间点($t+1$,$t+2\cdots$)进行计算的时候,它还能记住之前时间点 t 时刻的相关信息. RNN 的特点是,同一层中的节点是连通的(图 1). 因此,隐藏层的输入不仅包括上层的输出,还包含最后一个时间点的同一层的输出.

RNN 可以展开形成一个完整的网络(图 2). 一般的 RNN 模型包含输入层、隐藏层和输出层. 输入集可以表示为$\{i_0,i_1,\cdots,i_{t-1},i_t,i_{t+1},\cdots\}$和输出设置为$\{o_0,o_1,$

$\cdots, o_{t-1}, o_t, o_{t+1}, \cdots\}$. 对于每个隐藏层,输入集可以表示为$\{x_0, x_1, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots\}$和输出设置为$\{h_0, h_1, \cdots, h_{i-1}, h_i, h_{i+1}, \cdots\}$. $\boldsymbol{U}$、$\boldsymbol{V}$和$\boldsymbol{W}$分别是从输入层到隐藏层、隐藏层到输出层、以及隐藏层内的权重矩阵. 在RNN中,那些隐藏的单位完成了最重要的工作. 虽然从输入层到隐藏层的信息流是单向的,但是隐藏的节点是自联和互联的,以便完全交换信息(如图2所示).

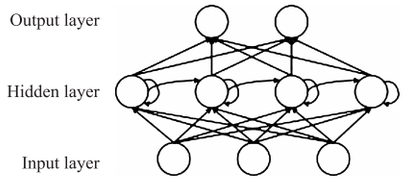

图1 循环神经网络

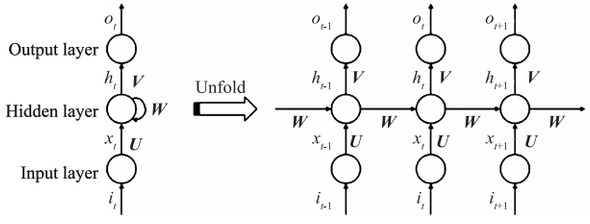

图2 循环神经网络的展开结构

RNN的一个重要扩展是Shuster和Paliwal所提出的双向RNN(BRNN)[19](图3). 其基本思想是将两个相反的RNNs放在一起,但共享相同的输入和输出层. 这样,经过训练的数据可以与过去和将来的信息相关联. BRNN的显著特征是它具有两个隐藏层:向前和向后层(图3). 其他元件与一般与RNNs大体一致. BRNN通常用五重矩阵来表示:$\boldsymbol{W}_1, \boldsymbol{W}_2, \cdots, \boldsymbol{W}_5$. 由于两个隐藏层之间没有连接,所以展开的网络中没有循环.

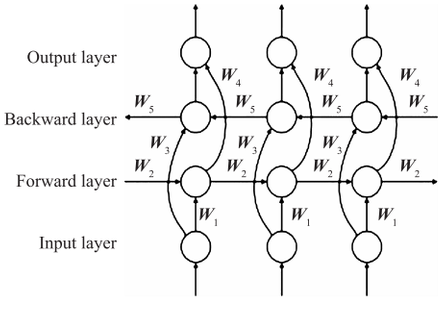

图3 双向循环神经网络

传统RNNs在实际使用过程中会遇到梯度消失或复杂度爆炸的问题[20]. 这就使得RNN只能够记住一些短期信息. 传统的RNN不能充分利用长期信息. 为了缓解这些问题,本文提出了一些特定的RNN结构,比如说LSTM和GRU,其基本的思想是使用多个门来控制记忆内存并防止梯度下降.

3.2 门控循环单元

在性能上,GRU与LSTM相当[21],GRU可被看作是LSTM[22]在结构上的简化版. 在GRU中,隐藏单元是最重要的组件,负责记忆或获取特定信息. 图4展示的是一种常见的LSTM的结构图[23],其连接关系由式(1)给出. 在式(1)中,$\boldsymbol{x}$是输入向量,$\boldsymbol{h}$是输出向量,$\boldsymbol{C}$是单元状态. 下标t表示当前时间,$t-1$是最末时间. σ是一个s型函数,°是Hadamard积,$\boldsymbol{W}$表示待定参数. 在式(1)中,f被称作舍弃门,由它决定哪些信息需要从单元状态中舍弃. i是输入门,决定哪些信息需要存储在单元中. o是输出门,决定输出哪些信息需要输出.

$$\begin{cases} \boldsymbol{f}_t = \sigma(\boldsymbol{W}_{xf}\boldsymbol{x}_t + \boldsymbol{W}_{hf}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{cf}\boldsymbol{C}_{t-1}) \\ \boldsymbol{i}_t = \sigma(\boldsymbol{W}_{xi}\boldsymbol{x}_t + \boldsymbol{W}_{hi}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{ci}\boldsymbol{C}_{t-1}) \\ \boldsymbol{C}_t = \boldsymbol{f}_t \circ \boldsymbol{C}_{t-1} + \boldsymbol{i}_t \circ \tanh(\boldsymbol{W}_{xc}\boldsymbol{x}_t + \boldsymbol{W}_{hc}\boldsymbol{h}_{t-1}) \\ \boldsymbol{o}_t = \sigma(\boldsymbol{W}_{xo}\boldsymbol{x}_t + \boldsymbol{W}_{ho}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{co}\boldsymbol{C}_{t-1}) \\ \boldsymbol{h}_t = \boldsymbol{o}_t \circ \tanh(\boldsymbol{C}_t) \end{cases} \quad (1)$$

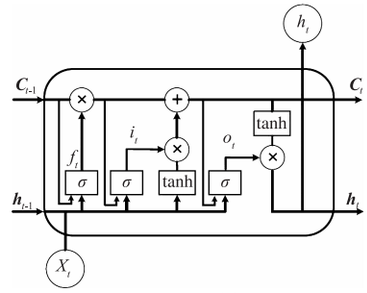

图4 LSTM结构图

图5中给出了GRU的结构,其内部的连接关系由式(2)给出. 在式(2)中,$\boldsymbol{x}$是输入向量,$\boldsymbol{h}$是输出向量和$\bar{\boldsymbol{h}}$是候选输出. 其他符号的表示和含义与之前相同. GRU有两个门:r被表示为复位门和z作为更新门. 与LSTM相比,GRU的门更少. 这是因为GRU没有单元状态,并将输入门和舍弃门组合成一个新的单一门,也就是更新门z. 因此,GRU在结构上要比LSTM简单得多,参数也较少,因此在性能和收敛性方面具有很大的优势. 在随后的实验验证中,GRU也体现出了很大的优势.

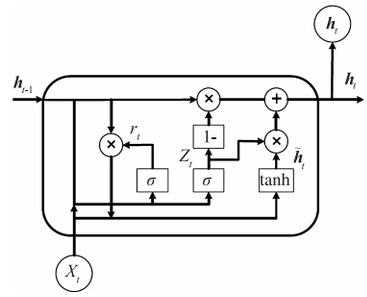

图5 GRU结构图

$$\begin{cases} \boldsymbol{r}_t = \sigma(\boldsymbol{W}_r \boldsymbol{x}_t + \boldsymbol{U}_r \boldsymbol{h}_{t-1}) \\ \boldsymbol{z}_t = \sigma(\boldsymbol{W}_z \boldsymbol{x}_t + \boldsymbol{U}_z \boldsymbol{h}_{t-1}) \\ \tilde{\boldsymbol{h}}_t = \tanh(\boldsymbol{W}_h \boldsymbol{x}_t + \boldsymbol{U}(\boldsymbol{r}_t \circ \boldsymbol{h}_{t-1})) \\ \boldsymbol{h}_t = (-\boldsymbol{z}_t)\boldsymbol{h}_{t-1} + \boldsymbol{z}_t \tilde{\boldsymbol{h}}_t \end{cases} \tag{2}$$

3.3　多层感知器

多层感知器(Multilayer Perceptron,MLP)是一个由多个层组成的单向 ANN[24]. 利用非线性激活函数,MLP 可以识别线性不可分的数据. MLP 的主要特征是:信号前向传播,误差反向传播,以及 BP 算法训练. 标准 BP 算法是一种经典的学习算法,它计算实际输出和期望输出之间的差异,将差异点返回到每个层,从而调整每个层的参数以达到完成学习的目的.

一个典型的 MLP 由三个组件构成:一个输入层、多个隐藏层和一个输出层. 相邻层完全连接,但同一层中的节点相互独立. MLP 所使用的激活函数需要具备连续和单调增加的属性,如 S 型函数.

3.4　Softmax 函数回归

Softmax 回归是逻辑回归的一种扩展. 它从一个 k 维向量 $\boldsymbol{x}$ 中产生一个位于[0,1]取值区间的 k 维向量 $\sigma(\boldsymbol{x})$[30]. 该方程由公式(3)给出.

$$\sigma(\boldsymbol{x})_j = \frac{e^{x_j}}{\sum_{k=1}^{K} e^{x_k}}, j = 1, \cdots, K \tag{3}$$

网络攻击的类型多种多样,因此每个特定的记录都应归因于其中的一个或多个攻击(或正常).

在 IDS 中,一种比较好的方法是使用多路区分器(multi-classifier). 在一个多路区分器中,对于给定的输入 x,需要一个假设函数来估计每个类 j 的概率 $P(y=j|x)$. 即需要估计每种可能分类输出的概率. 具体说,假设函数应输出一个 $kh_\theta(x^{(i)})$ 维向量(向量元素的总和是 1)来表示估计的概率. 公式(4)给出了假设函数的具体表达方式.

$$\begin{aligned} h_\theta(x^{(i)}) &= \begin{vmatrix} P(y^{(i)}=0|x^{(i)};\theta) \\ P(y^{(i)}=1|x^{(i)};\theta) \\ \vdots \\ P(y^{(i)}=k-1|x^{(i)};\theta) \end{vmatrix} \\ &= \frac{1}{\sum_{j=0}^{k-1} e^{\theta_j^T x^{(i)}}} \begin{vmatrix} e^{\theta_0^T x^{(i)}} \\ e^{\theta_1^T x^{(i)}} \\ \vdots \\ e^{\theta_{k-1}^T x^{(i)}} \end{vmatrix} \end{aligned} \tag{4}$$

在公式(4)中,假设函数被表示为 $h_\theta(x^{(i)})$,其中 $\theta_0, \theta_1, \cdots \theta_{k-1}$ 是待定的参数. 另,如果 $\theta \to \infty$,则 Softmax 成为最大函数. 当输入不同的有限值,Softmax 是一个带参数的、弱化的最大函数.

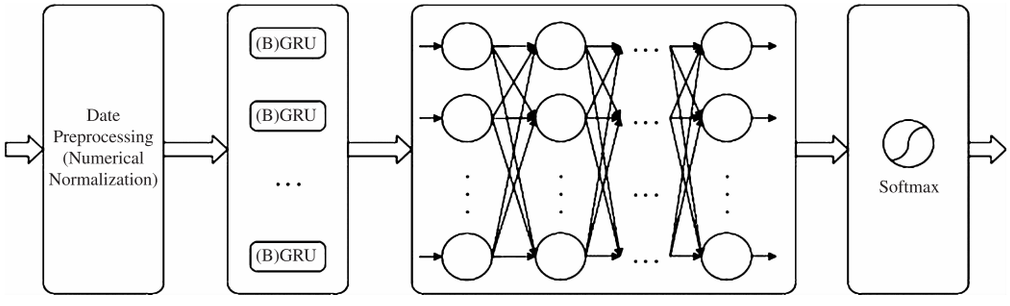

图6　基于深层循环神经网络的IDS模型结构图

4　系统整体设计

要构造一个 DNN,每个组件都应被视为一个层,并级联在一起. 图 6 是本文所提出的基于深层循环神经网络的 IDS 模型结构图. 该模型由预处理模块、GRU 模块、MLP 模块和输出模块组成. 预处理模块可将数据处理成适合输入神经网络的归一化值,并且保证不改变数据的维数. GRU 模块由一个或多个 GRU(或双向 GRU,记作 BGRU)层组成,用以提取和存储特征. 这是整个系统的核心. MLP 模块是一个 n 层感知器,对 GRU 模块的输出进行非线性映射,从而做出非线性的分类决策. 输出模块是一个 Softmax 层. 它对分类概率进行归一化,并将其输出为最终结果.

在这些组件中,GRU 和 MLP 模块对整体性能的影响起着至关重要的作用. 这两个模块属于两个不同类型的神经网络. GRU 不仅有记忆,还有相对来说更为复杂的结构和更加强大的计算能力. MLP 则具有结构简单、计算速度快、易于叠加的特点. 二者的结合构成了一个新型的深层网络,可以实现对结果的更多优化.

5　实验和分析

5.1　基准数据集

评估 IDS 的最佳方法是使用通用数据集进行测试,以便可以对不同系统进行公平的比较.

在对 IDS 的系统评估方面,DARPA/KDDCup99 数据集(通常缩写为 KDD99)已广泛使用,并开始成为标

准的测试基准[18]. 麻省理工学院林肯实验室在“DARPA98 IDS Evaluation Program”这个项目中获得了一批数据,KDD99 数据集则是建立在此数据集之上[2]. 它包含了七周的训练数据和两周的测试数据. 此数据集包括 39 种类型的攻击:其中有 22 种包含在训练数据集中;其余 17 种则只作为未知攻击类型出现在测试数据集中,用于测试算法的泛化性能. 所有这些攻击可分为四类:

(1)DOS:拒绝服务攻击,阻止用户访问某项业务,如泛洪攻击;

(2)R2L:从远程计算机进行未经授权的访问,如猜测密码;

(3)U2R:未经授权访问本地 *root* 权限,例如缓冲区溢出;

(4)PROBING:监视和其他探测,例如端口扫描.

此外,考虑到正常(即没有遭受攻击的情况),每个记录都被分配到这五个类别的其中之一. 在 KDD99 中,每个记录有 41 个特征:34 个连续特征和 7 个离散特征. 所有的特征可分为四大类:

(1)单个 TCP 连接的基本特征. 这些特征直接从数据包标题中提取;

(2)基于内容派生出来的特征. 比如说,由领域知识所建议的那些内容功能;

(3)“同一主机”特征. 这些特征只检查过去 2 秒内与当前连接具有相同目标主机的连接

(4)“同一服务”功能. 这些特征只检查过去 2 秒中与当前具有相同服务的连接.

“同一主机”和“同一服务”功能一起被称为基于时间的流量特征. 在参考文献[3]给出了有关此数据集的更多详细信息.

Tavallaee 等人[3]提出了一个改进版本的 KDD99 数据集,叫做 NSL-KDD. NSL-KDD 克服了 KDD99 中的一些不足. 例如,它不包括冗余或重复记录. NSL-KDD 从每个不同级别选择一定的记录. 由于 NSL-KDD 选择的数量更加合理,所以它能够进行更高效的公平评估. NSL-KDD 所选择的记录总数比较合理,使得其可以在完整的数据集上运行,而不是只能运行在随机选择一小部分数据集之上. 因此,它可以更容易用于针对不同研究的评估和比较. 本文使用 KDD99 和 NSL-KDD 的数据集来评估所提出的 IDS.

5.2 评估指标

对于分类问题,分类的结果可能是正确的或不正确的,并且所有可能的结果可分为以下四种情况:

(1)真阳性(TP):实际攻击被做正确划分为攻击;

(2)真阴性(TN):实际正常记录被正确划分为正常;

(3)假阳性(FP):实际正常记录被错误划分为攻击,这种情况也为假警报;

(4)假阴性(FN):实际攻击被错误划分为正常记录.

简便起见,TP、TN、FP 以及 FN 用于表示四条件的数量. 在此基础上,公式(5)给出了准确度(Accuracy)、精密度(Precision)、检出率(Detection Rate)、假阳性率(False Positive Rate)、F-测量值 F-measure 等指标的具体计算方式. 准确性指的是正确分类的数量占记录总数的比率. 精度指的是实际攻击的数量相对于被划分为攻击的数量的比率. 检测率(DR)是被划分为攻击的数量相对于实际攻击的比率. 假阳性率(FRR)是被划分为攻击的数量相对于所有正常记录数量的比率.

$$\begin{cases} \text{Accuracy} = \dfrac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FN}+\text{FP}} \\ \text{Precision} = \dfrac{\text{TP}}{\text{TP}+\text{FP}} \\ \text{DetectionRate(DR)} = \dfrac{\text{TP}}{\text{TP}+\text{FN}} \\ \text{FalsePositiveRate(FPR)} = \dfrac{\text{FP}}{\text{FP}+\text{TN}} \\ \text{F}-\text{measure} = \dfrac{2(\text{Precison} * \text{DR})}{\text{Precision}+\text{DR}} \end{cases} \tag{5}$$

一方面,从分类的角度来看,精度和检测率是一对矛盾的度量. 较高的精确度意味着存在着较少误报的情况,但较高的检测率意味着存在着较少假阴性的情况. 例如,如果更多的疑似攻击被划分为攻击(一种极端情况是所有记录都被划分为攻击),那么检测率将会增加,但精确度会降低,反之亦然. 因此,单一的高精度或检测率是没有意义的. 另一方面,从入侵检测的角度来看,一些严格的环境对入侵的容忍度很低,因此单独的检测率也是一个重要的度量指标. F-测量值是对精度和检测率的综合考虑. 这是基于两者的调和平均值. 较高的 F-测量值意味着更高的精确度和检测率.

5.3 实验结果

仿真实验平台的软硬件环境配置如下. 硬件采用了英特尔酷睿 i7 @ 3.4GHz、64GBRAM 以及 NVIDIAK40. 软件采用了 Ubuntu16.04LTS, CUDA8.0, cuDNN5.1, TensorFlow0.11,所有的软件都可以从互联网上免费下载.

KDD99 和 NSL-KDD 两个数据集均进行了 10 倍的交叉验证. 因为它是一个 DNN,所以在 DNN 训练阶段使用了随机梯度下降(SGD)[19]. 为了提高效率,使用了交叉熵作为成本函数,而不是使用最小平方误差(MSE)函数来作为成本函数[20]. 实验中的学习率和迭代次数则是由实际经验决定的.

在所提出的系统中,因为 GRU 和 MLP 模块最为重

要,所以下面的实验着重于验证这两个模块的有效性和必要性.

实验 1 评价了 GRU + MLP 性能. 作为参考,在同一实验环境中,LSTM 模块被 GRU 模块取代. 此外,考虑到必要性,还增加了双向 RNN 实验. 在实验结果中,前缀 B 表示它是双向 RNN.

实验 2 对每个模块独立运行时的情况进行了评估. 在进行类似的实验之前,RNN 模块或 MLP 模块首先被移除,然后再开始实验过程.

实验 1 和 2 分别对 KDD99 和 NSL-KDD 数据集进行了研究. 表 1 和 2 分别对相关的实验结果进行了总结.

从上述结果,能够得出如下结论,在 KDD99 和 NSL-KDD 两种数据集中,BGRU + MLP 的结果是最好的. 实验 1 表明,在 KDD99 测试数据集中,由于 GRU 的使用,其总体性能比 LSTM 有所改进. 这种改进可以在准确度、检出率和误报率这三个指标上得到体现. 此外,总体来说,双向 BGRU 的总体性能要比单向 GRU 好. 双向 RNN 可以进一步提高 RNN 的性能. 实验 2 表明,RNN 和 MLP 的结合是比较有效的. 其实验结果比单独使用 RNN(GRU 和 LSTM)或单独使用 MLP 的情形更好.

表 1　基于 KDD99 的实验结果

System	Accuracy(%)	DR(%)	FPR(%)
BGRU + MLP	**99.26**	**99.33**	**0.86**
GRU + MLP	99.21	99.37	1.02
BLSTM + MLP	96.41	95.65	2.67
LSTM + MLP	95.22	93.97	3.24
GRU	94.96	94.78	4.86
LSTM	94.1	95.65	7.58
MLP	90.56	86.61	3.49

表 2　基于 NSL-KDD 的实验结果

System	Accuracy(%)	DR(%)	FPR(%)
BGRU + MLP	**99.85**	**99.43**	**0.06**
GRU + MLP	99.29	96.74	0.08
BLSTM + MLP	98.57	93.78	0.17
LSTM + MLP	98.51	94.77	0.53
GRU	92.29	71.78	0.14
LSTM	91.91	70.77	0.10
MLP	91.88	70.92	0.31

图 7 比较了不同算法的收敛性. 结合前面的结果,可以看出,采用 BGRU + MLP 或 GRU + MLP 的系统,其收敛速度更快.

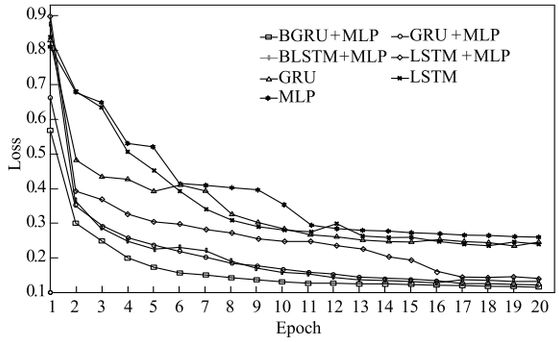

图7　基于收敛性的相关比较

表 3 中将结果与先前的研究进行了比较. 从表 3 中可以发现,BGRU + MLP 在两个数据集上都表现良好. 其在 KDD99 测试数据集上获得了最佳的准确度和误报率,在 NSL-KDD 测试数据集上获得了最高的检出率.

表 3　相关性能比较

System	Dataset	Accuracy (%)	DR (%)	FPR (%)
LSTM(2015)[9]	KDD99	94.11	77.07	0.18
LSTM-RNN(2016)[21]	KDD99	96.93	98.88	10.04
LSSVM + FMIFS(2016)[22]	KDD99	99.79	99.46	0.13
TVCPSO + MCLP(2016)[5]	NSL-KDD	N/A	97.23	2.41
OS-ELM(2015)[23]	NSL-KDD	N/A	97.67	1.74
LSSVM + FMIFS(2016)[22]	NSL-KDD	99.91	98.76	0.28
BGRU + MLP(proposed)	**KDD99**	**99.85**	**99.43**	**0.06**
BGRU + MLP(proposed)	**NSL-KDD**	**99.26**	**99.33**	**0.86**

需要注意的是以上的比较仅当作一个参考,而不是用以对不同算法的绝对区分. 不同的入侵检测系统,其对入侵的响应有所不同,因此很难找到一个能够在任何情况下都能够达到最佳性能的系统. 此外,评价方法也总有细微的差别. 比如说,数据集的不同随机抽样,也会导致最终结果可能有所不同. 通过与最近研究的全面比较,本文所提出的新型系统,在准确度、检出率和误报率等多个方面,都有一定的优势.

6　结论

本文设计了适合配电网无线通信业务的一个新型 IDS 并提出了一种新的 DNN 模型,利用 GRUs 作为记忆单元,结合 MLP 来识别网络入侵,也采用深度学习技术进行训练,同时取得了良好的效果. 对 KDD99 和 NSL-KDD 数据集的攻击仿真实验表明,该系统具有领先性. 本文对所提出的系统主要进行了理论验证. 为了验证其实际应用,接下来需要投入到大量的工程中运行. 下一步的工作重点是优化系统,使其可以更有效地应用于配电网无线通信 IDS 的实际环境中.

参考文献

[1] Allen J H, Christie A, Fithen W, Willke B. State of the practice of intrusion detection technologies[R]. Carnegie Mellon Software Engineering Institute. 2000.

[2] MIT-Lincoln-Labs. DARPA intrusion detection datasets [DB/OL]. https://www.ll.mit.edu/ideval/data/,2016-12-25.

[3] Tavallaee M, Bagheri E, Lu W, Ghorbani A. A detailedanalysis of the kdd cup 99 data set[A]. IEEE Symposium on Computational Intelligence for Security and Defense Applications[C]. IEEE,2009. 1 – 6.

[4] Denning D E. An intrusion-detection model [J]. IEEE Trans on Software Engineering,1987,13(2):222 – 232.

[5] Hussain J, Lalmuanawma S, Chhakchhuak L. A two-stage hybrid classification technique for network intrusion detection system[J]. International Journal of Computational Intelligence Systems,2016,9(5):863 – 875.

[6] Ma T, Wang F, Cheng J, Yu Y, Chen X. A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks[J]. Sensors, 2016, 16(10):1701.

[7] Kang M J. Kang W. Intrusion detection system using deep neural network for in-vehicle network security[J]. PloSone 11,2016,(6):e0155781.

[8] Erfani S M, Rajasegarar S, Karunasekera S, Leckie C. High-dimensional and large-scale anomaly detection using alinear one [J]. Pattern Recognition, 2016, 58 (C): 121 – 134.

[9] Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system [A]. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies[C]. New York City:ICST,2015. 35:2126.

[10] Staudemeyer R C. Applying long short-term memory recurrent neural networks to intrusion detection[J]. South African Computer Journal,2015,56(1):136 – 154.

[11] Kim J, Kim J, Thu LHT, Kim H. Long short term memory recurrent neural network classifier for intrusion detection [A]. 2016 International Conference on Platform Technology and Service[C]. Jeju:IEEE,2016. 1 – 5.

[12] Schuster M, Paliwal K K. Bidirectional recurrent neural networks[J]. IEEE Transactions on Signal Processing, 1997,45(11):2673 – 2681.

[13] Schmidhuber J. Deep learning in neural networks: An overview[J]. Neural Networks,2015,61:85 – 117.

[14] Chung J, Gulcehre C, Cho KH, Benqio Y. Empirical evaluation of gated recurrent neural networks on sequence modeling[A]. NIPS 2014 Deep Learning and Representation Learning Workshop [C]. Montréal: NIPS, 2014. 1 – 9.

[15] Hochreiter S, Schmidhuber J. Longshort-term memory [J]. Neural Computation,1997,9(8):1735 – 1780.

[16] Gers F A, Schmidhuber J, Cummins F. Learning to forget: Continual prediction with LSTM[J]. Neural Computation,2000,12(10):2451 – 2471.

[17] Pal S K, Mitra S. Multilayer perceptron, fuzzy sets, and classification [J]. IEEE Transactions on Neural Networks,1992,3(5):683 – 697.

[18] KDDcup1999 data[DB/OL]. http://kdd.ics.uci.edu/datab ases/kddcup99/kddcup99.html,2016-12-21.

[19] Bottou L. Large-scale machine learning with stochastic gradient descent[A]. Proceedings of COMPSTAT[C]. Paris:Physica-Verlag HD,2010. 177 – 186.

[20] Shore J, Johnson R. Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy[J]. IEEE Transactions on Information Theory, 1980,26(1):26 – 37.

[21] Staudemeyer R C. Applying long short-term memory recurrent neural networks to intrusion detection[J]. South African Computer Journal,2015,56(1):136 – 154.

[22] Ambusaidi M A, He X, Nanda P, Tan Z. Building an intrusion detection system using a filter-based feature selection algorithm [J]. IEEE Transactions on Computers, 2016,65(10):2986 – 2998.

[23] Singh R, Kumar H, Singla R. An intrusion detection system using network trac profiling and online sequential extreme learning machine[J]. Expert Systems with Applications,2015,42(22):8609 – 8624.

作者简介

刘文军 男,1967 年出生,华北电力大学通信工程专业毕业,高级工程师,国网河南省电力公司科信部通信处处长,从事电力通信工作 29 年.

郭志民 男,1977 年出生,本科,教授级高级工程师,国网河南省电力公司电力科学研究院设备状态评价中心副主任,研究方向为电力系统自动化、电力信息安全.

阮 伟(通信作者) 男,1969 年出生,工学博士,教授级高级工程师. 2000 年浙江大学能源系硕士、博士毕业,现工作于浙江大学控制学院. 长期从事自动控制系统软硬件、优化控制策略的研究、现场工程应用等,承担多项科技部、工信部工业控制系统信息安全领域重大研究项目.

E-mail:ruanwei@zju.edu.cn