·热点与综述·　　文章编号：1000-3428(2020)11-0035-07　　文献标志码：A　　中图分类号：TP309

一种基于 DBN-RF 的电网工控系统异常识别方法

舒　斐[1]，陈　涛[2]，王　斌[1]，杨慧婷[1]，李明轩[1]

（1. 国网新疆电力有限公司电力科学研究院，乌鲁木齐 830011；2. 国网新疆电力有限公司，乌鲁木齐 830063）

摘　要：电网作为国家关键基础设施，对其进行网络安全防护至关重要，而通过对电网工控系统流量预警可达到维护电网安全的目的。结合深度置信网络（DBN）和随机森林（RF）算法，提出一种电网工控系统异常识别方法。通过构建 DBN 模型完成对多个流量特征之间关联特性的深度挖掘，学习适用于电网工控系统流量的特征提取模式。在此基础上，将特征学习后的流量与恶意攻击流量输入 RF 检测模型，并逐步调优模型参数，学习得到最优检测模型。根据电网流量特性，从经典入侵检测数据集 KDD99 中筛选出相似数据集进行测试。实验结果表明，该方法检测率达到 96.16% 而误报率仅为 3.49%，与逻辑回归模型、多分类支持向量机模型、DBN 模型及 K-means 算法相比，能够更准确地识别电网工控系统中的异常流量。

关键词：电网安全；电网工控系统；流量异常检测；深度置信网络；随机森林算法

开放科学（资源服务）标志码（OSID）：

中文引用格式：舒斐，陈涛，王斌，等. 一种基于 DBN-RF 的电网工控系统异常识别方法[J]. 计算机工程，2020，46(11)：35-41.

英文引用格式：SHU Fei，CHEN Tao，WANG Bin，et al. An anomaly identification method for power grid industrial control system based on DBN-RF[J]. Computer Engineering，2020，46(11)：35-41.

An Anomaly Identification Method for Power Grid Industrial Control System Based on DBN-RF

SHU Fei[1]，CHEN Tao[2]，WANG Bin[1]，YANG Huiting[1]，LI Mingxuan[1]

（1. Electric Power Science Research Institute of State Grid Xinjiang Electric Power Co.，Ltd.，Urumqi 830011，China；
2. State Grid Xinjiang Electric Power Co.，Ltd.，Urumqi 830063，China）

【Abstract】It is crucial to provide network security protection for power grid，one kind of national key infrastructure. Network security can be maintained by providing traffic warnings for the power grid Industrial Control System（ICS）. To this end，this paper proposes an abnormal identification method that combines Deep Belief Network（DBN） with the Random Forest（RF） algorithm for the power grid ICS. The method constructs a DBN model to implement the in-depth mining of the correlation characteristics between multiple traffic characteristics and learn the feature extraction modes applicable to the traffic of power grid ICS. On this basis，the traffic whose characteristics are learnt and the malicious attack traffic are input into the RF detection model，and the model parameters are gradually adjusted for learning to obtain the optimal detection model. Tests are carried out on the data sets that are selected based on the features of power grid traffic from the classic intrusion detection data set，KDD99. Experimental results show that the accuracy rate of this method reaches 96.16% while the false alarm rate is only 3.49%. Compared with logistic regression model，multi-classification support vector machine model，DBN model and K-means algorithm，the proposed method can more accurately identify abnormal traffic in power grid ICS.

【Key words】power grid security；power grid Industrial Control System（ICS）；traffic anomaly detection；Deep Belief Network（DBN）；Random Forest（RF） algorithm

DOI：10.19678/j.issn.1000-3428.0057541

基金项目：国网新疆电力有限公司基金“电力行业工业控制系统安全监测与深度检测技术研究”（5230DK18000V）。

作者简介：舒　斐（1988—），男，工程师、硕士，主研方向为工控安全、大数据安全、物联网安全；陈　涛，高级工程师；王　斌、杨慧婷，硕士；李明轩，高级工程师。

收稿日期：2020-03-02　　**修回日期：**2020-04-16　　**E-mail：**shufei_88@163.com

计算机工程 www.ecice06.com

0 概述

随着国内外工业化和信息化的融合发展,各行业数字化、网络化和智能化水平稳步提升。作为全球工业体系智能化的重要推手,工业互联网正助力能源电力行业开拓全新发展方向。在此过程中,电力系统自动化技术已经逐步应用在电力生产和电力供应系统中,并且提供了快捷、方便、安全、稳定的电力传输途径[1]。但与此同时,电力行业也成为一些网络攻击组织的重点目标。2016 年 12 月,乌克兰电网工控系统(Industrial Control System,ICS)先后遭受 3 次恶意网络攻击,引发了大规模停电,影响涉及数十万人,给当地人民的生活带来不便并严重威胁社会稳定。2019 年 3 月 7 日,委内瑞拉发生全国性大规模停电事件,调查表明此次事件的发生极有可能是反对派对古里水电站发动了蓄意的网络攻击。由此可见,能否在电网工控系统运行过程中及时发现突发性、针对性的恶意攻击,对于保障电力系统的正常运行至关重要[2]。

在网络安全防护中,通过检查网络流量来检测针对特定目标的恶意活动是一项关键技术。通过对特定目标网络流量的分析,可以及时掌握当前网络的状态,发现潜在的恶意威胁。因此,从流量分析的角度出发及时发现电网工控系统在运行过程中潜在的网络安全问题,对保障电力系统持续稳定运行具有重要意义。

电网工控系统中的通信流量具有多源异构、数据长度小、周期性、数据流向固定和时序性强等特点,并且存在正常流量和异常流量分布不平衡的现象。本文提出一种基于深度置信网络(Deep Belief Network,DBN)[3]和随机森林(Random Forest,RF)算法[4]的电网工控系统异常识别方法,以实现对系统中异常通信流量的准确识别。利用深度学习强大的数据学习能力和有监督学习准确的分类能力,对深度置信网络中多个受限玻尔兹曼机(Restricted Boltzmann Machine,RBM)逐个进行训练,自学习得到流量中蕴含的更高级特征[5]。在此基础上,利用随机森林算法以监督方式检测流量中的异常情况,从而发现针对电网工控系统的多种威胁源。

1 电网工控系统

工业控制系统是涵盖电力、水利、石油、天然气等多种行业的控制系统[6],主要包括监控和数据采集系统(Supervisory Control and Data Acquisition,SCADA)、分布式控制系统(Distributed Control System,DCS)、过程控制系统(Process Control System,PCS)和可编程逻辑控制器(Programmable Logic Controller,PLC)。在电力行业中,电网工控系统由电力监控与信息采集系统、电力通信和数据网组成[7]。电力监控与信息采集系统负责监视和控制整个能源产生、输电、变电、配电以及调度过程中各个软硬件设备的运行状态,完成对设备信息的记录采集。电力通信和数据网包括电力调度数据网、电力企业数据网等,负责行业内部的数据通信和保障整个电力系统的畅通运行。

1.1 电网工控系统安全分析

传统的电网工控系统大多建立在一个相对封闭的环境中,利用电子机械、软件、通信协议的组合实现特定功能。此类系统主要关注功能、性能和稳定性的保障,以监测网络设备/平台日志为主,较少注重基于流量异常检测和全方位的防护措施。在“互联网+”以及“两化融合”(信息化和工业化融合)的背景和趋势下,电网工控系统将智能设备、人和数据三者有机结合,这种转变使得电网工控系统成为网络攻击者的主要目标,面临着比传统攻击更强、更广的破坏威胁。针对电网工控系统一次典型的攻击过程如图 1 所示,攻击者通过网络开展对目标系统的攻击,借助病毒与恶意代码、多种不同的协议漏洞、系统漏洞以及策略和管理漏洞,实现对系统的攻击,进而影响电力的配送。

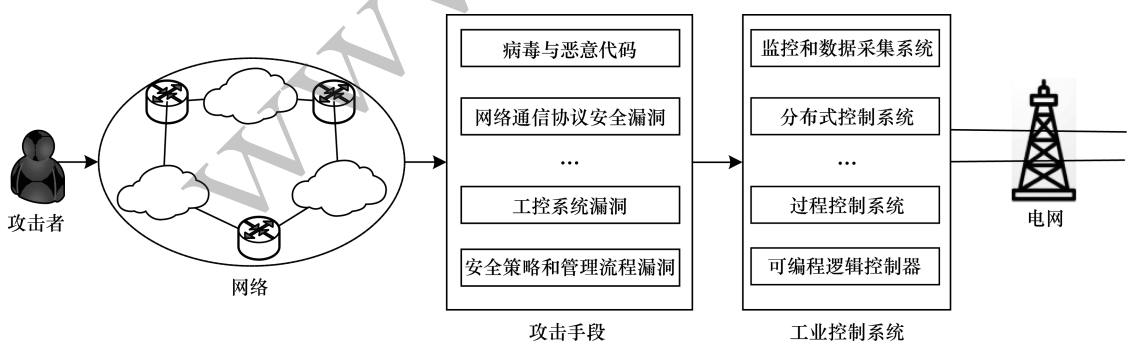


图 1 电网工控系统攻击示意图

Fig. 1 Schematic diagram of attack on power grid industrial control system

1.2 电网工控系统杀伤链

电网工控系统杀伤链模型[8]包括 2 个阶段,即网络入侵的准备与执行阶段以及工控攻击载荷的研发与执行阶段。

计算机工程 www.ecice.com

1)网络入侵的准备与执行阶段。此阶段是一个广泛攻击的设计和实现过程,可细化为电网信息搜集、能力准备、入侵实施、权限激活和持续控制 5 个部分。在电网信息搜集阶段,恶意攻击者主要开展对电网工控系统的侦察工作,这也是高级定向[9]威胁实施的第一步,攻击手段为通过外部网络扫描或利用内部社会工程学,侦察的信息包括工控系统使用的设备类型、设备版本、内部配置等重要信息。在能力准备阶段,攻击者根据搜集到的情报数据制定相应的攻击计划,确定攻击行动的先后顺序,设置渗透需要投递和使用的工具。在入侵实施、权限激活和持续控制 3 个阶段中,攻击者针对系统中存在的 0day 漏洞、木马、未修复的漏洞等利用已有的工具不断尝试进入目标系统,获取更高的权限,在得到更有价值信息的同时,充分考虑隐蔽性,尽量避免自身身份信息泄露。

2)工控攻击载荷的研发与执行阶段。在获得内部控制网络访问权限的基础上,攻击者在此阶段对特定工业主机、控制设备和通信协议开展定向攻击,从而建立控制,主要过程包括工具研发、验证测试及载荷应用。攻击者不断地调整和测试攻击方法,模拟网络常见的协议构建命令控制信道,绕过电网内部安全系统的监测。借用此类信道,攻击者试图将特定的载荷投递到目标系统,并通过载荷满足自己更多、更细化的攻击需求,包括修改系统默认配置、注入恶意代码、篡改通信指令等,从而造成电网工控系统监视与控制通信中断、监控画面与功能安全指令拒绝响应、电网基础设施被远程操控等。此外,该信道也用于服务器收集的信息加密回传。

综上可知,电网系统杀伤链是一个完整的攻击体系,在各个过程中都可以从流量中发现攻击者的一些恶意操作行为。因此,为增强系统对网络恶意攻击的感知能力,扩大系统的防护面,流量异常检测具有一定的理论研究价值。

2　电网工控系统面临的安全问题

基于对电网工控系统杀伤链模型的分析,笔者认为当前电网工控系统的安全防护需要考虑以下 3 个方面的问题:

1)与传统信息系统的安全防护需求存在差异。传统信息系统对突发的威胁可以采取入侵容忍甚至中断运行的方式,进而时常进行信息安全软件补丁和系统更新,而电网工控系统需要保证持续不间断的服务,不能及时下载软件补丁并进行系统更新,这使得电网工控系统面临严重的安全威胁[10]。

2)抵御各类高级攻击是防护趋势。物理隔离已不再是抵御网络攻击的最后一道防线,需要加强对软硬件漏洞和协议风险的重视。例如,攻击者会通过 U 盘、供应链以及其他渠道,以间接的方式入侵电网内部。因此,需要能够有效检测可能出现的更高级威胁。

3)对应急响应能力的要求更高。与其他工控系统相比,电网工控系统具有规模大、距离远、覆盖范围广、交叉感染性强的特点[11],系统中的各个环节紧密关联,一个环节出现安全问题,就可能造成其他环节的连锁反应。因此,其对故障范围控制、系统自愈能力、实时响应及灾备等要求更高。

由此可见,需要依据自身特点设置完备的电网工控系统安全防护策略,在“安全分区、网络专用、横向隔离、纵向认证”原则[12]的基础上,增强对电网工控系统潜在安全风险的检测能力。

3　电网工控系统检测技术分析

针对电网工控系统安全问题,我国相继出台了一系列系统化的工作方案,包括国家发改委颁布的《电力监控系统安全防护规定》、国家能源局颁布的《电网工控信息安全专项监管工作方案》和《电力监控系统安全防护总体方案》等,具有重要的指导意义。在实际电网安全防御过程中,主要对策是对网络和设备进行安全防护,对数据安全加密[13]。首先以边界隔离与加密的方式,降低不同区域、系统、生产区与地方系统之间的安全风险;其次在不同区域之间采用安全审计、恶意代码防范、入侵检查和访问控制等手段有效感知系统内部的风险。内部风险的核查大多基于系统流量,与互联网流量不同,工控系统的流量是由工控设备按照系统指令产生,具有数据长度小、周期性、数据流向固定、时序性强等特点[14],这与传统互联网流量存在较大差异。按照检测角度的不同,系统流量的安全检测可划分为基于统计分析的检测方法和基于机器学习的检测方法 2 种。

1)基于统计分析的检测方法

基于统计分析的检测主要依赖的是先验知识,针对流量内容、协议等提取特征码或是根据对系统数据进行长期分析设定的规则策略[15],实现黑白名单的构建以及特征数据和规则策略的匹配。文献[16]设计一种基于协议解析的电网工控安全检测系统,其包括对 IEC 60870-5-103 规约通信的深度解析,利用配置的大量安全策略,发现系统中的违规通信。文献[17]设计的工控网络安全检测系统包含规则模块和安全样本数据库,其中:规则模块在扫描模块执行初始化扫描前,向扫描模块下发安全扫描规则,通过这些安全扫描规则对目标环境进行安全扫描;安全样本数据库对扫描模块提取的文件特征进行数据匹配,并基于数据匹配的结果分发安全检测组件。该系统具有较高的准确性,但对新型威胁检测存在漏报和误报。

2)基于机器学习的检测方法

基于机器学习的检测是在深度分析系统流量的

www.eeacs.com

基础上,采用有监督、半监督或无监督的机器学习算法,发现系统存在的威胁[18]。有监督学习需要大量有标签的数据作为输入,从中提取源主机到目标主机的双向数据传输的字节数、周期性规律、连接来自/送达同一主机/端口的属性值和错误分段的数量等特征,从而发现威胁。该方法具有较高的准确性,但对未知威胁发现效果较差。常见的无监督[19]算法如 K-means、PCA、Auto-Encoder 等,能够有效识别未知威胁,但是单独使用时准确性不高。由此可见,半监督的方法更适合用于电网工控系统流量的检测。文献[20]提出一种基于熵的动态半监督 K-means 算法并以单类向量机辅助实现对半监督 K-means 算法的改进,有效提高了对未知攻击的检测率,降低了误报率。深度学习是无监督学习方法,其可使计算机自动学习深层特征,从而降低人为设计特征造成的不完备性。因此,本文利用深度学习中的深度置信网络对特征进行自学习,同时结合有监督算法进一步提高对系统异常流量的检测率,降低漏检率。

4 基于 DBN-RF 的异常识别

本文通过构建混合深度置信网络模型 DBN-RF,实现对电网工控系统网络异常流量的检测。如图 2 所示,其中左侧为电网工控系统架构,右侧为本文提出的检测模型。该模型通过初始数据的预处理完成对电网工控网络流量协议类型、网络服务类型、网络连接状态和攻击类型等特征的提取。本文利用深度置信网络模型挖掘多个流量特征之间的关联特性,学习适用于电网工控流量的特征提取模式。在此基础上,将特征学习后的电网工控流量与恶意攻击流量输入到随机森林模型中,通过参数的逐步调优,构建适用于检测电网工控系统流量中常见攻击异常的模型,实现流量异常报警。在实际使用中,将工控系统收集到的实时流量输入到检测模型中,经过混合深度置信网络模型的检测,发现流量中的多种威胁。下文将对基于 DBN 的流量处理和基于 RF 的异常检测两部分分别进行介绍。

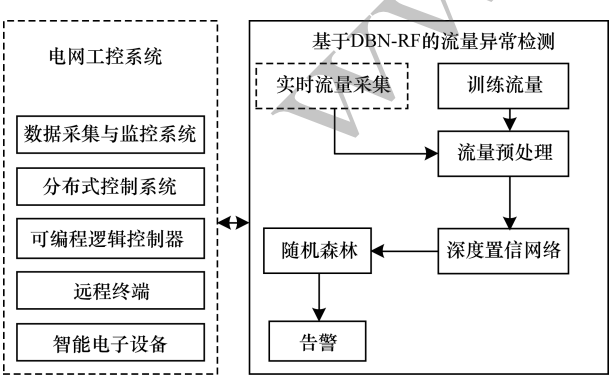


图 2 基于 DBN-RF 的异常识别过程

Fig. 2 Anomaly identification process based on DBN-RF

4.1 基于 DBN 的流量处理

深度置信网络的形成依赖于多层受限玻尔兹曼感知机(RBM)和前馈反向传播网络,进而完成网络的预训练以及对 RBM 堆叠网络的优化。RBM 是一种神经感知器,其由一个显层(v)和一个隐层(h)构成,显层与隐层的神经元之间为双向全连接。RBM 仅提供纵向层与隐藏层和可见层之间神经元的连接,同一层的各神经元之间没有连接。如图 3 所示,每个 RBM 有一个显层,也可称为输入层,与显层相连接的为隐层。

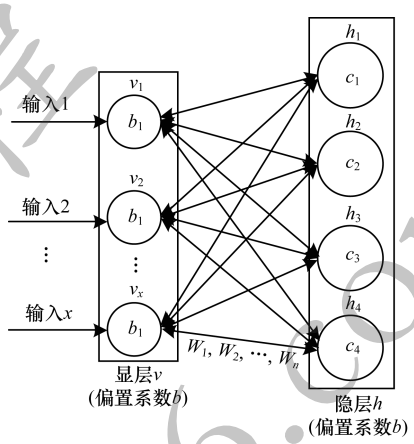


图 3 受限玻尔兹曼机结构

Fig. 3 Structure of restricted Boltzmann machine

RBM 的训练可分为 2 个阶段:首先是向前,其次是后向或者重构。在 RBM 中,包含 3 个通过数据不断学习得到的参数,分别是 w、b 和 c。w 代表两个神经元之间的连接强度。每个显层神经元和隐层神经元都有各自代表自身权重的偏置系数,显层神经元的偏置系数用 b 表示,隐层神经元的偏置系数用 c 表示。

RBM 是一种概率图模型,对于给定的状态(v,h),能量函数如式(1)所示:

$$E(v,h) = \sum_{i=1}^{N_v} b_i v_i - \sum_{j=1}^{N_h} c_j h_j - \sum_{i,j=1}^{N_v,N_h} W_{ij} v_i h_j \tag{1}$$

通过能量函数,可以定义一个显层 v 和隐层节点 h 的联合概率。RBM 中第 j 个隐层神经元被激活的概率如式(2)所示,其中,σ 为 Sigmoid 函数。同理,显层神经元 i 被隐层神经元激活的概率如式(3)所示:

$$P(h_j|v) = \sigma\left(b_j + \sum_i W_{i,j}x_i\right) \tag{2}$$

$$P(v_i|h) = \sigma\left(c_i + \sum_j W_{i,j}h_j\right) \tag{3}$$

对于一条 n 维流量样本数据 $X(x_1,x_2,\cdots,x_n)$,经过 RBM 编码后得到 m 维的样本 $Y(y_1,y_2,\cdots,y_m)$。训练过程如下:

1)获取初始神经元激活概率。输入数据 X 经过显层 v_1 的所有节点,传递到隐藏层 h_1。在隐藏层的

www.ecocn.com

节点上,X 乘以 w 再加 b,此结果再通过 sigmoid 函数产生节点的输出或者状态。因此,每个隐层神经元将有一个概率输出表示被激活的概率。

2)显层和隐层互相重构。采取吉布斯采样从计算的概率分布中抽取一个样本:$h_1 \sim P(h_1 \mid v_1)$。利用 h_1 重构显层,计算显层中每个神经元被激活的概率,并从计算得到的概率分布中采取吉布斯采样抽取一个样本:$v_2 \sim P(v_2 \mid h_1)$,通过 v_2 再次计算隐层中每个神经元被激活的概率,得到概率分布 $P(h_2 \mid v_2)$。

3)更新 RBM 中 3 个重要的权重 w、b 和 c:

$$w \leftarrow w + \lambda(P(h_1 \mid v_1)v_1 P(h_2 \mid v_2)v_2) \tag{4}$$

$$b \leftarrow b + \lambda(v_1 - v_2) \tag{5}$$

$$c \leftarrow c + \lambda(h_1 - h_2) \tag{6}$$

4)重复上述过程,得到隐层输出的样本 $Y(y_1, y_2, \cdots, y_m)$,此时该样本已充分学习到了显层数据的内部特点。

多个 RBM 的堆叠组成了 DBN。如图 4 所示,该 DBN 由 3 个 RBM 堆叠而成。训练 DBN 的过程是逐层进行的。在每一层中,用数据向量来推断隐层,再将这一隐层作为下一层的数据向量。

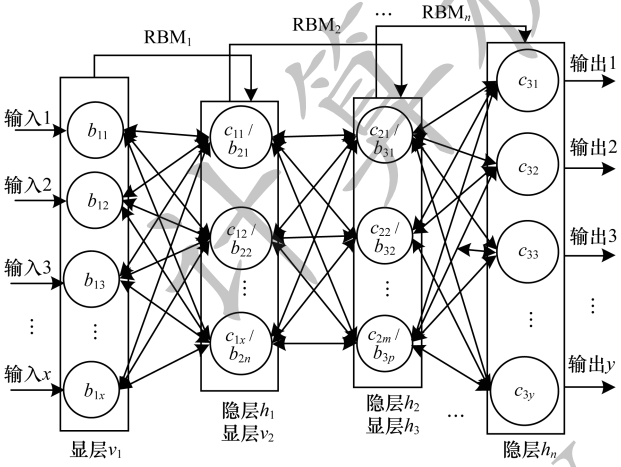


图 4　深度置信网络模型结构

Fig. 4　Structure of deep belief network model

初始的 DBN 模型依赖于原始无标签的数据集,采用无监督学习的方式生成。生成初始模型后,对整个模型进行微调。此阶段基于初始的 DBN 模型,保留其中各个 RBM 之间的权重和偏置,以数据集中的标签作为标准计算网络误差,利用 BP 算法得到各层误差,通过梯度下降法实现对各层权重和偏置的调节。

4.2　基于 RF 的异常检测

混合深度置信网络的检测综合了深度置信网络对数据深度学习的能力以及有监督学习分类的准确性。深度置信网络模型的生成实现了对电网工控系统中多个流量特征之间关联特性的自动深度挖掘,适用于电网工控流量的特征提取,可应用于后续检测。

基于 RF 的流量异常检测用于寻找一种最优的投票表决器,实现对大量混杂样本(多种类型攻击、正常通信流量)的差异化学习,满足大规模流量输入后需要及时发现其中异常情况的要求。如图 5 所示,经过深度置信网络对数据进行流量特征自学习后,将新生成的学习样本输入到 RF 模型中。RF 模型能够利用多棵树(弱分类器)对样本进行初始训练,再将所有弱分类器结果相结合,从而得到最终的决策结果,完成对异常流量的检测。

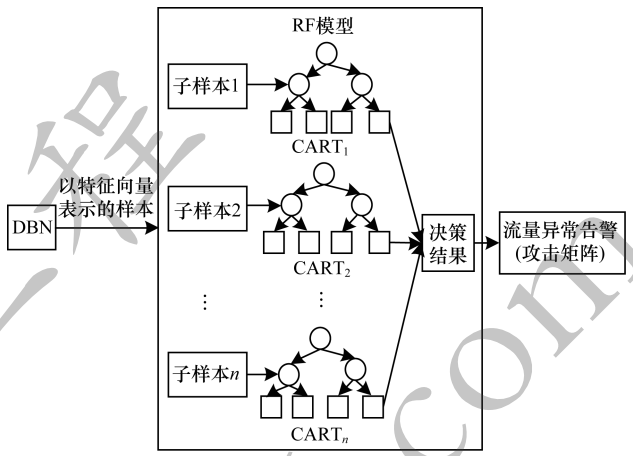


图 5　随机森林算法异常检测过程

Fig. 5　Anomaly detection process of random forest algorithm

为得到更优的异常识别模型,RF 算法利用网格搜索方法选择最优的模型参数,再通过交叉验证的方法完成对不同参数模型的评估,从而得到最优模型。

5　实验结果及分析

5.1　实验数据集

电网工控系统的流量由多种工控设备按照系统指令产生,这些流量具备一定的周期性,实时性较强,数据流较为规律,指令发送也较为频繁,而传统的网络流量具有很强的随机性,其连接的持续时间和响应时间较长,数据内容更随机,很难从中找到一定的规律性。本文从经典入侵检测数据集 KDD99 中筛选出相似的数据集,其中包含了电网工控系统可能遭受的不同网络攻击类型,例如端口攻击扫描探测目标各端口所提供服务的流量 port-scan、ping-sweep,以及拒绝服务攻击致瘫系统的流量 ping-of-death、syn flood、smurf 等。

针对电网工控系统受到的网络攻击,基于电网工控系统流量特征的角度,从数据集中存储有标签样本的 kddcup. data_10_percent 和 corrected 文件已有的 41 维特征中筛选出 18 维特征,然后根据数据集中的不同攻击类型,筛选出 3 050 个正常样本和 2 663 个异常样本组成新的数据集,数据集中异常样本的类型涵盖了拒绝服务(DDoS)、远程用户攻击(R2L)、提权攻击(U2R)和端口攻击(Probing)4 种

www.ecr06.com

电网工控系统受到的典型攻击类型。测试的样本中有 1 343 个正常样本和 860 个异常样本,其中有3 种攻击未出现在训练集中,用于测试模型对于未知攻击的检测能力。

5.2 评价指标

为有效评估本文提出的 DBN-RF 模型,使用检测率(ACC)和误报率(FPR)评价指标,并定义所有异常样本数为 M,所有正常样本数为 N,算法识别出的样本数为 m,将正常样本误判为异常的正常样本数为 f。2 种评价指标的计算公式如下:

$$\mathrm{ACC}=\frac{m}{M}\times 100\% \tag{7}$$

$$\mathrm{FPR}=\frac{f}{N}\times 100\% \tag{8}$$

5.3 检测结果对比

通过多次改变 RBM 的迭代次数并观察训练效果,发现当 DBN 模型的参数设置为 42-36-20-16-5 且 RBM 的迭代次数设置为 120 次时,实验数据最符合实际情况。为达到最佳的检测效果,本文同时使用了网络搜索[21]的方法优化随机森林算法的模型参数,使模型达到最优化。不同方法用于流量检测得到的各项指标如表 1 所示。实验结果表明,本文方法检测率和误报率分别为 96.16% 和 3.49% ,与其他检测方法相比,DBN-RF 模型能够更准确地识别电网工控系统中的异常流量。

表 1 5 种检测方法的检测率与误报率对比

Table 1 Detection rate and false alarm rate comparison of five detection methods %

检测方法	检测率	误报率
逻辑回归模型	71.05	6.92
多分类 SVM 模型	83.95	8.10
K-means 算法	88.26	5.81
DBN 模型	89.20	6.40
DBN-RF 模型	96.16	3.49

6 结束语

本文对电网工控系统中异常流量的识别方法进行研究,通过分析当前电网工控系统面临的安全问题,评估现有检测方法的优势与不足,并构建一种基于 DBN 模型与 RF 算法的检测模型 DBN-RF。该模型基于电网工控系统网络通信流量的特性,能够快速学习特征提取模式,无需大量标记样本即可完成对海量流量的检测,并根据实际情况在线更新输出权重,提升训练效率。实验结果表明,本文方法能够改善传统深度置信网络的多类检测效果,其检测率达到96.16% ,而误报率仅为 3.49% ,可准确识别异常流量。下一步拟将该方法应用于真实业务场景,评估其实时检测性能。

参考文献

[1] Research Institute of Foresight Industry. Analysis on the development trend of electric power automation in China in 2018[J]. China Electrical Equipment Industry,2018,10(1):29-32. (in Chinese)
前瞻产业研究院. 2018 年中国电力自动化发展趋势分析[J]. 电器工业,2018,10(1):29-32.

[2] SAEED A, XIAO T, HEIDAR M, et al. Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints[J]. IEEE Access, 2019, 7: 27376-27388.

[3] HINTON G E, OSINDERO S, TEH Y W. A fast learning algorithm for deep belief nets[J]. Neural Computation,2006,18(7):1527-1554.

[4] WU Lingyun, QIN Guihe, YU He. Anomaly detection method for in-vehicle CAN bus based on random forest[J]. Journal of Jilin University(Science Edition), 2018,56(3):663-668. (in Chinese)
吴玲云,秦贵和,于赫. 基于随机森林的车载 CAN 总线异常检测方法[J]. 吉林大学学报(理学版),2018,56(3):663-668.

[5] ARSA D M S,JATI G,MANTAU A J,et al. Dimensionality reduction using deep belief network in big data case study: hyperspectral image classification[C]//Proceedings of International Workshop on Big Data and Information Security. Washington D. C.,USA:IEEE Press,2016:71-76.

[6] WEISS J. Industrial Control System(ICS) cyber security for water and wastewater systems[M]//CLARK R M, HAKIM S. Securing water and wastewater systems. Berlin,Germany:Springer,2014:87-105.

[7] GE Bingyu. Security protection of power grid industrial control system[C]//Proceedings of Digital China Energy Interconnection-2018 Annual Conference of Power Industry Informatization. Beijing: Electric Power Information Committee of China Electrical Engineering Society,2018:85-88. (in Chinese)
葛冰玉. 电网工业控制系统安全防护[C]//数字中国能源互联-2018 电力行业信息化年会论文集. 北京:中国电机工程学会电力信息化专业委员会,2018:85-88.

[8] ZHAO Guicheng. Research on intrusion detection platform and algorithm based on industrial control network traffic analysis[D]. Hangzhou: Zhejiang University, 2019. (in Chinese)
赵贵成. 基于工业控制网络流量分析的入侵检测平台与算法研究[D]. 杭州:浙江大学,2019.

[9] DONG Na,ZHANG Junyan,LIU Weina,et al. Problem and countermeasures on APT defense in power grid enterprises[J]. Hebei Electric Power,2016,35(4):25-27,37. (in Chinese)
董娜,张君艳,刘伟娜,等. 电网企业 APT 攻击防御存在的问题及防御措施[J]. 河北电力技术,2016,35(4):25-27,37.

[10] ZHANG Wei. Preliminary discussion on information security of industrial control system under smart grid

计算机工程 www.ecice06.com

environment[J]. Technology Innovation and Application, 2016(27):194. (in Chinese)
张伟. 智能电网环境下工控系统信息安全初探[J]. 科技创新与应用,2016(27):194.

[11] YING Huan, LIU Songhua, HAN Lifang, et al. Overview of power industry control system security technology [J]. Electric Power Information and Communication Technology, 2018,16(3):56-63. (in Chinese)
应欢,刘松华,韩丽芳,等. 电网工业控制系统安全技术综述[J]. 电力信息与通信技术,2018,16(3):56-63.

[12] ZHU Shishun, LIU Xing. Research on network security protection system of power industry control system under the new situation[J]. Secrecy Science and Technology, 2017(5):62-64. (in Chinese)
朱世顺,刘行. 新形势下电网工业控制系统网络安全防护保障体系研究[J]. 保密科学技术,2017(5):62-64.

[13] ZHU Shishun, LIU Hang. The development and challenges of smart grid network security[J]. Electrotechnics Electric, 2019(7):5-8,54. (in Chinese)
朱世顺,刘行. 智能电网网络安全的发展与挑战[J]. 电工电气,2019(7):5-8,54.

[14] GAO Chunmei. Traffic anomaly detection based on industrial control network[D]. Beijing: Beijing University of Technology,2014. (in Chinese)
高春梅. 基于工业控制网络的流量异常检测[D]. 北京:北京工业大学,2014.

[15] HUO Xuesong, LÜ Chao, PEI Pei, et al. Smart grid communication network traffic anomaly detection based on entropy analysis [C]//Proceedings of the 2nd IEEE International Conference on Computer and Communications. Washington D.C., USA: IEEE Press, 2016:1-5.

[16] YU Haiguo, MA Xian, XU Yourui, et al. Design and application of security threat monitoring system for power grid industrial control system [J]. Electric Power Information and Communication Technology, 2016, 14(7): 76-80. (in Chinese)
俞海国,马先,徐有蕊,等. 电网工业控制系统安全威胁监测系统设计及应用[J]. 电力信息与通信技术,2016,14(7):76-80.

[17] LI Mingxuan. An industrial control network security detection system: CN109714371 [P]. 2019-03-12. (in Chinese)
李明轩. 一种工控网络安全检测系统:CN109714371[P]. 2019-03-12.

[18] OZAY M, ESNAOLA I, VURAL F T Y, et al. Machine learning methods for attack detection in the smart grid[J]. IEEE Transactions on Neural Networks and Learning Systems, 2015, 27(8):1773-1786.

[19] ZHONG Zhichen. Security monitoring technology of power grid industrial control system based on network traffic anomaly detection[J]. Electric Power Information and Communication Technology, 2017, 15(1):98-102. (in Chinese)
钟志琛. 基于网络流量异常检测的电网工控系统安全监测技术[J]. 电力信息与通信技术,2017,15(1):98-102.

[20] LIU Yali, MENG Lingyu, DING Yunfeng. Application and algorithm improvement of abnormal traffic detection in smart grid industrial control system [J]. Computer Systems and Applications, 2018, 27(3):173-178. (in Chinese)
刘亚丽,孟令愚,丁云峰. 电网工控系统流量异常检测的应用与算法改进[J]. 计算机系统应用,2018,27(3):173-178.

[21] FRIEDMAN J H. Greedy function approximation: a gradient boosting machine [J]. Annals of Statistics, 2001,29(5):1189-1232.

编辑　金胡考

北京机工程