DOI:10. 3969/j. issn. 1674-1951. 2021. 02. 001

结合KNN和优化特征工程的AMI通信入侵检测研究

Research on AMI communication intrusion detection combining KNN and optimized feature engineering

卢官宇,田秀霞*,张悦
LU Guanyu,TIAN Xiuxia*,ZHANG Yue

(上海电力大学 计算机科学与技术学院,上海 200090)
(School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China)

摘 要:随着互联网技术在智能电网的广泛应用,识别电力系统中的入侵攻击行为显得尤为重要。基于高级量测体系(AMI)中的通信网络架构,根据智能电网入侵检测需求,提出了一种结合K最邻近算法(KNN)和优化特征工程的AMI通信入侵检测方案,通过数据采集、数据预处理、特征工程和模型训练4个模块识别入侵攻击流量。特征工程部分,采用文本特征提取方法对输入KNN训练模型的特征进行优化,并基于信息增益值移除冗余特征向量。模型训练部分,通过k个最近邻训练实例的标签来判断待检测数据的类型。将该方案在公开的入侵检测数据集ADFA-LD上进行测试,得到了各类入侵攻击的检测准确率。试验结果表明,该方案在检测结果性能上显著优于传统的入侵检测方案,最优特征提取下模型的分类准确率提高了21.96%。

关键词:智能电网;入侵检测;高级量测体系;KNN;特征工程;ADFA-LD;能源互联网;电力信息安全
中图分类号:TM 732 **文献标志码**:A **文章编号**:1674-1951(2021)02 - 0001 - 08

Abstract: With the widespread use of internet technology in smart grids, it is particularly important to identify intrusion attacks in power systems. Based on the communication network architecture in Advanced Metering Infrastructure (AMI), an AMI communication intrusion detection scheme combining K Nearest Neighbor (KNN) and optimized feature engineering is proposed in response to the smart grid intrusion detection requirements. Intrusion attack flow can be identified through four modules: data collection, data preprocessing, feature engineering and model training. In feature engineering module, the features inputted into KNN training model are optimized by text feature extraction method, and the redundant feature vectors are removed based on the information gain values. In model training part, the types of data are judged by the labels of the k nearest neighbour training samples. The proposed scheme was tested on public intrusion detection data sets ADFA-LD, and the detection accuracy of various intrusion attacks was obtained. The experimental results show that the detection performance of this scheme is superior to the traditional intrusion detection scheme, with an 21.96% increase in the classification accuracy under the optimal feature extraction model.

Keywords: smart grid; intrusion detection; Advanced Metering Infrastructure; KNN; feature engineering; ADFA-LD; Energy Internet; power information security

0 引言

随着智能电网(Smart Grid, SG)、能源互联网(Energy Internet, EI)以及智联网(Internet of Intelligence, IoI)等一系列能源与电力发展概念的提出,网络通信在电力系统中的应用越来越广泛,识别交互流量是否可靠,给电网通信入侵检测带来了巨大挑战。同时,相量测量单元(PMU)、智能电表采集系统、数据采集与监控(SCADA)系统等产生了指数级增长的数据[1]。快速处理这些数据、识别异常数据从而维护系统稳定运行一直是电力信息领域的研究热点。

层出不穷的入侵攻击可能引发电力系统大规模停电事故,对电力信息安全产生了巨大威胁[2]。国内外对智能电网入侵检测已进行了大量的相关

收稿日期:2020-08-04;**修回日期**:2021-01-23
基金项目:国家自然科学基金面上项目(61772327);国家自然科学基金重点项目(61532021)

研究。在20世纪初,美国和欧洲各国相继开展智能电网相关研究,以提高电网安全性、稳定性和能源利用率[3]。我国也提出了建设坚强智能电网的总体发展目标,实现信息化、自动化和互动化的“智能”技术特征。在智能变电站三层两网的结构中,通信设备基于面向通用对象的变电站事件(GOOSE)管理技术,实现了集中配置[4]和通信过程中的异常数据检测,对智能变电站的稳定运行起到了重要作用。文献[5]对信息熵、相对熵、条件熵以及活跃熵4者在入侵检测领域的应用进行了概述,并汇总了常见的基于熵的入侵检测方法的优缺点。文献[6]对比分析了决策树、支持向量机(SVM)和神经网络等机器学习方法在入侵检测上的应用,并通过仿真试验来验证不同模型的性能变化。文献[7]提出了一种基于决策树的攻击检测算法,并在公开的入侵检测数据集UNSW-NB15和KDD99上进行试验验证。通过对2个数据集的检测精度和误报率进行对比,分析数据集的优劣性。但以上3个方案只提供了网络入侵检测的方法,并未针对电力系统中的通信入侵检测结果提出相应的解决方案。文献[8]利用SVM算法,设计了智能电网中邻域网入侵检测方案,结合邻域网网络结构特性,根据信任度白名单实现了分级协作的入侵检测。但是该方案依赖于电网的结构拓扑,且SVM分类性能的优劣主要取决于核函数的选取,目前尚未有更客观的选取方案。文献[9]基于隐马尔科夫模型(Hidden Markov Model,HMM)对智能电网系统网络安全攻击检测算法进行研究,但试验部分只是对服务器上的各种攻击进行了简单统计,没有具体分析算法的性能。文献[10-11]采用的是神经网络的方法对入侵电力系统中的行为进行检测。但在电力信息数据的交互过程中,由于入侵行为产生的异常流量所占比重较小,反向传播(BP)神经网络和长短期记忆网络的训练效果并不好。

通过分析智能电网中高级量测体系(Advanced Metering Infrastructure, AMI)的通信交互过程,结合入侵检测系统的设计理念,提出了结合K最邻近算法(KNN)和优化特征工程的AMI通信入侵检测方案。该方案的实施基于数据采集、数据预处理、特征工程、模型训练4个步骤。在特征工程到模型训练中,优化了输入到KNN模型的抽象特征向量提取过程,并计算出各特征向量的信息增益值,采用滤波法过滤信息增益值较小的特征,减少了特征空间的维度。在试验部分,模拟AMI中通信数据报文的获取方法,并在公开入侵检测数据集(ADFA-LD)对提出的方案进行了测试。测试得到了在不同优化特征提取方法下各种攻击类型数据的检测结果,并拟合出该组训练数据下模型的最优k值。

1 AMI通信入侵检测研究

在电网通信架构中最典型的是AMI中的通信系统,它负责传输、测量管理设备收集、储存的用户用电信息。鉴于交互信息以及用户隐私数据的价值,AMI通信过程受到大量安全威胁。基于智能检测模型的设计思想,各类入侵检测系统可应用于识别入侵攻击流量和系统的防御维护的过程。

1.1 AMI通信网络

AMI一般由智能电表、集中器、电网计量管理服务器和其通信网络组成[12],是智能电网中最重要的组成部分。通过该体系,可以实现能源消费者和电力公司之间的数据交互,为电表端与电力企业端间的信息自动双向流通提供了渠道。

在AMI通信网络层级结构中:AMI最底层的组件是智能电表,智能电表负责采集家庭区域网络(HAN)、商业区域网络(BAN)和工业区域网络(IAN)的用户信息,同时监控和记录用电数据和其他统计数据;该体系的中间组件是部署在邻居区域网络(NAN)中的数据收集器,负责汇总从智能电表收到的数据信息;最上层组件是AMI头端设备,部署在广域网(WAN)中,它负责收集从多个数据收集器汇总的数据(如图1所示)。每个层次都存在多种可行的通信方式和协议,例如在HAN中使用的是紫蜂协议(ZigBee)、蓝牙通信协议栈等;而在NAN中,用到了无线通信技术(WiFi)标准;WAN中通信方式众多,可以使用数字用户线路(DSL)、光纤通信和通用无线分组业务(GPRS)等。

1.2 入侵检测系统

入侵检测系统(Intrusion Detection System, IDS)在信息安全综合防御系统中扮演了重要角色,可检测网络中可能的入侵行为并及时报警[13],阻止安全威胁攻击并针对漏洞进行防御。IDS是继防火墙系统后的第2道安全防线。

IDS按照不同的方式有多种分类结果。最常见的是按照检测结果分为误用检测和异常检测:在误用检测中,IDS把入侵攻击数据作为训练数据集,对比检测数据特征和入侵攻击数据特征,如果特征相似就将该类数据判断为入侵攻击数据;异常检测则是将通信过程中正常的数据作为训练数据集,若检测数据特征与正常数据特征明显不符,则判断该类数据为入侵攻击数据。除了上述方法,其他IDS分类标准见表1。

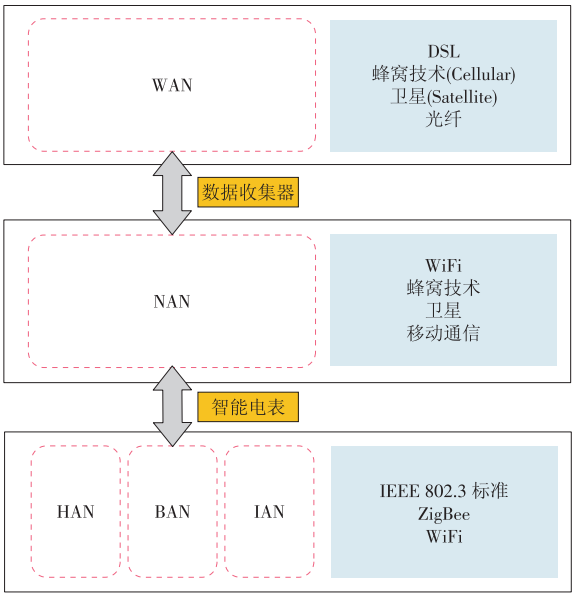

图1　AMI通信网络层级结构

Fig. 1　AMI communication network hierarchy

表1　IDS其他分类标准

Tab. 1　Other classification standards for IDS

分类标准	入侵检测系统类型
数据源	基于主机式 基于网络式 基于应用式
体系结构	集中式 等级式 协作式
使用频率	在线 离线
反应机制	主动反应 被动反应

1.3　针对AMI的入侵检测

AMI中通信系统对安全的需求可以描述为机密性、完整性、有效性和不可否认性4个特征。智能电表端收集的数据涉及用户的隐私，敏感数据需要相应的授权认证才可以进行访问；网络体系内传输数据必须保证其真实、有效且可以被授权用户在任意时刻获取。智能电网中应用了一系列的异构技术。根据安全需求，每一种技术都受到各种安全威胁，这些威胁可能导致破坏性的后果，例如，拒绝服务(DoS)和分布式拒绝服务(DDoS)攻击可能会损害系统的有效性；虚假数据注入(FDI)攻击可能危及信息的完整性；中间人(MiTM)攻击可能会威胁到系统的机密性[14]。分布式拒绝服务攻击通过发送大量的伪造请求数据包到目标主机或服务器，耗尽主机资源且占用大量网络带宽，使主机处于瘫痪状态不能处理正常请求；虚假数据的注入则是利用了电力信息系统中的异常数据漏洞，篡改状态参数估计结果，影响电力系统的安全、可靠运行；中间人攻击可以篡改和窃取通信双方的交互信息，并可以通过域名系统(DNS)欺骗和会话劫持的方式来进行虚假数据的传输，进而控制电力系统中的正常调度。

在智能电网系统中，正常行为模式下的数据流量种类复杂，界定不符合正常流量特征的方法若过于主观，会使异常检测误报率较高。所以本文的误用检测方案通过将输入数据的特征向量和入侵攻击数据的特征向量进行匹配，判断该组流量的安全性。由于数据源为电网中AMI通信网络，因此该设计方案为基于网络的入侵检测系统。

目前，智能入侵检测系统应用普遍，采用机器学习的方法实现了良好的入侵攻击检测效果，如决策树、神经网络、SVM和各种聚类算法都可以应用到智能入侵检测领域。由于在所有层次部署IDS成本较高，因此，在电网智能检测中通常在数据收集器等集成位置处部署IDS。

2　结合KNN和优化特征工程的检测方案

各类入侵攻击给电力系统通信安全带来了巨大挑战，基于分类思想来识别链路上正异常数据流量，实现AMI通信过程中的入侵检测具有非常重要的意义。结合KNN和优化特征工程的检测方案通过深入研究入侵攻击数据流量的特征，进而探索和正常数据流量的行为区别，通过KNN方法对这些特征在向量空间内的距离进行计算，最终区分入侵攻击流量和正常数据流量，检测到入侵攻击行为。

对电网的通信入侵检测分为4步：数据采集、数据预处理、特征工程以及模型训练，设计流程如图2所示。文本在进行特征提取时，使用自然语言处理中的词袋(Bag of Words，BoW)模型、TF-IDF模型和N-gram模型。

2.1　数据采集

在传统网络通信过程中，可以采用Wireshark或NetFlow分析软件从公共网络中获取通信报文数据，也可以采取相同的方法提取电网中通信报文。但直接从实际环境中采集到的数据存在异常流量数据过少以及各种入侵攻击形式复杂等问题，不利于数据的特征提取和模型的训练。因此，以往很多研究会采用一些公开的数据集，这些数据集已经对数据进行了简单处理操作，方便展开研究。

典型的用于网络入侵检测的公开数据集有DARPA98，KDD99和ADFA-LD。和其他用于入侵检测的数据集相比，数据集ADFA-LD的结构与智能电网攻击更为类似[15]，所以本文采用公开入侵检测数据集ADFA-LD。

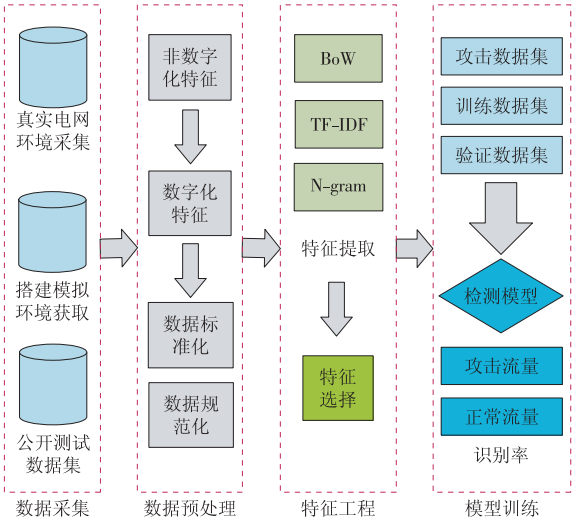

图2　AMI通信入侵检测方案设计流程

Fig. 2　Design process of the AMI communication intrusion detection scheme

2.2　数据预处理

在对网络流进行数据处理时，为后续的数据聚类和预测，需要对数据集中的特征值进行数字化处理。传统的网络信息交互过程中所具有的五元组特征为：源网络协议（IP）地址、源端口号、目的IP地址、目的端口号和协议类型字段。对于数据中源端口号这类数字化特征，依据数据标准化以及规范化方法进行处理；对于协议类型等非数字化特征，要首先进行数字化处理，然后进行标准化操作。AMI网络通信过程中，除了上述五元组特征外，还有数据报文长度、数据包传送时间、消息传递频率以及消息传送命令等特征。由于数据的评价指标、维度和大小不同，为了消除相似性和差异性的影响，通常采用数据标准化和规范化处理[16]。数据标准化和规范化常采用Min-Max和Z-score这2种方法。

（1）假定一组数据集为$X=\{x_1,x_2,\cdots,x_n\}$，使用Min-Max方法对该集合中某一数据x_i进行标准化，

$$x_i'=\frac{x_i-x_{\mathrm{Min}}}{x_{\mathrm{Max}}-x_{\mathrm{Min}}},\tag{1}$$

式中：x_i'为x_i标准化后的数据；x_{Max}，x_{Min}为这组数据的最大值与最小值。

（2）在一组数据的最大值和最小值未知的情况下，可以采取Z-score数据规范化的方法预处理数据。Z-score方法归一化后的值符合正态分布，

$$x_i'=\frac{(x_i-\mu)}{\sigma},\tag{2}$$

式中，μ和σ为该组数据的均值和标准差。

2.3　特征工程

数据特征会直接影响模型训练准确率，特征工程即是把预处理后的数据转化为特征向量的过程，包括特征提取和特征选择2个部分。在传统的入侵检测方案中，会人工设定输入KNN训练模型的特征，这种方法依赖于专家经验和后续试验结果的验证，很多入侵检测模型都会直接选择数据流量特征的五元组。但是在这种特征设定方案下，模型对入侵攻击的检测准确率并不高。本文基于自然语言处理中的文本特征提取方法，从原始数字文本中获取重要的抽象表示，对输入训练模型的特征向量进行了优化。

ADFA-LD已经处理为数字文本格式。在特征提取时，可使用BoW模型、TF-IDF模型和N-gram模型：BoW模型将文本词袋中词出现的次数转变为向量形式表达；TF-IDF模型在BoW模型的基础上考虑了词频（TF）和逆文本频率（IDF）对词进行加权，区分了词频高和词频低的词；N-gram模型考虑了词的关联关系以及否定关系。利用这3个模型对ADFA-LD数据集进行文本特征提取，提取的特征向量用于对入侵攻击流量的检测。在AMI通信入侵检测过程中，提取的特征向量可能对检测结果的影响较小，或2个特征对模型训练的影响效果相类似，这类特征即为冗余特征，需要采取特征选择的方法进行移除。通过计算信息增益的方式进行特征选择，使用熵的概念计算信息增益值，基本计算步骤如下。

（1）计算输出集合Y的熵值

$$H(Y)=-\sum_{i=1}^{n}P(y_i)\log P(y_i),\tag{3}$$

式中：y_i为特征的可能输出；$P(y_i)$为输出概率。

（2）给定输入特征X，计算输出集合Y的条件熵值

$$H(Y|X)=-\sum_{i=1}^{n}\sum_{j=1}^{n}P(x_i,y_i)\log P(y_i|x_i),\tag{4}$$

式中，$P(y_j\mid x_i)$表示输入为x_i的条件下输出为y_j的概率。

（3）计算得到Y和X之间的信息增益

$$Gain(Y,X)=H(Y)-H(Y|X)。\tag{5}$$

基于上述过程，可以计算得到每个特征的信息增益值。在入侵检测数据集中，X表示不同的特征输入，Y表示输出的入侵攻击类型。选择当前信息增益大的特征来检测入侵数据流量，因为该类特征划分得到的子集纯度较高，不确定性较小。根据特征选择过程得到的数据集特征见表2。

通过特征工程阶段实现对预处理数据特征的提取和选择，对输入训练模型的初始化特征进行了优化。如果直接将全部特征作为KNN模型的输入向量，会降低检测的准确率，并会增加分类预测的

表2　根据信息增益值选择的特征值

Tab. 2　Eigenvalues selected according to information gains

特征	描述
Src_ip	传输数据源IP地址
Des_ip	传输数据目的IP地址
Src_port	传输数据源端口号
Des_port	传输数据目的端口号
Pack_length	传输数据报文长度
Pack_frequency	数据报文传送频率
Pack_ttl	数据报文TTL值
Pack_command	传输数据报文命令

时间成本，所以改进的特征优化部分对AMI通信入侵检测方案是十分必要的。

2.4　模型训练

在使用KNN方法进行异常识别决策时，只涉及周围相邻的少量样本，不需要估计参数，适用于分离极少出现的异常数据，且可以处理多类问题。AMI通信过程中各种入侵攻击属于小概率事件，数据总线上的大部分流量为正常流量，用于发送指令以及调度控制设备等。由于攻击类型的多样性，电网通信入侵检测也是一个多分类问题，因此采用KNN方法具有明显的优势。使用KNN进行电力系统通信入侵检测的模型训练过程如图3所示。

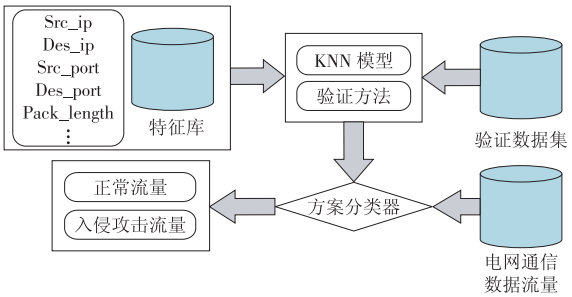

图3　AMI入侵检测模型训练过程

Fig. 3　Training process of AMI intrusion detection model

特征库中负责存储特征工程部分优化好的特征向量，从库中提取用于KNN模型的特征进行训练，使用验证数据集检测提出方案的准确性。利用训练得到的方案分类器对AMI通信流量进行检测，最终分离正常流量和入侵攻击流量，实现入侵攻击异常的识别。通过KNN方法比较检测数据的k个最近邻训练实例的类别，得到该类数据的检测结果，基本步骤如下。

步骤1。将数据集中数据实例进行矩阵化，把特征向量作为输入，可以得到数据矩阵

$$\boldsymbol{X}=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1m} \\ x_{21} & x_{22} & \cdots & x_{2m} \\ \vdots & & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nm} \end{pmatrix}=(x_1 \quad x_2 \quad \ldots \quad x_m)\ , \tag{6}$$

式中：n为该类数据数量；m为该类数据特征数量。

步骤2。计算测试数据和训练数据之间的距离。在向量空间中有2种距离计算表达，采用欧式距离计算的距离

$$d\left(x_1,x_2\right)=\sqrt{\sum_{k=1}^{n}\left(x_{1k}-x_{2k}\right)^2}\ , \tag{7}$$

采用曼哈顿距离计算的距离

$$d\left(x_1,x_2\right)=\sum_{k=1}^{n}\left|x_{1k}-x_{2k}\right|\ 。 \tag{8}$$

步骤3。按照$d(x_1,\ x_2)$的递增对数据点进行排序。

步骤4。选择距离最小的k个数据点，k的取值需要不断测试，因为会直接影响入侵数据流量和正常数据流量的分类准确率，选取最优k值作为提出方案的参数。

步骤5。确定前k个数据点所在类型的出现频率，返回前k个数据点中出现频率最高的类别作为检测数据的预测分类。

经过上述步骤可以得到该点代表的测试数据的数据类型，计算验证数据集中所有数据的预测结果，和已知标签进行比较，得出基于KNN的检测方案的分类精确度。

3　试验验证

使用公开的入侵检测数据集对提出的方案进行测试，并设计AMI通信系统中实际获取通信交互数据的试验环境，将实际数据预处理为公开数据集示例的文本格式。通过调试参数k，得到检测方案的最优k值，并计算出优化特征提取方法下不同类型入侵攻击数据的检测准确率。

3.1　数据集准备

在电力信息系统网络中，设计试验的数据采集环境如图4所示，主要包括可编程逻辑控制单元（PLC）以及数据获取单元，通过交换机和数据总线上的通信服务器相连。数据总线上的潜在入侵攻击威胁设备在通信过程中发送异常数据流量，实施各类攻击，影响正常设备之间的通信过程。数据库服务器负责存储设备之间的通信日志文件，数据获取单元负责收集正常数据流量和入侵攻击数据流量。对数据获取单元采集的数据进行数据预处理，将非数字化特征转化为数字化特征，转换完成后进行标准化和规范化。

在真实的电网通信环境中，可以按照上述步骤得到入侵检测需要的数据集，本文对提出的AMI通信入侵检测方案进行测试的数据集是公开数据集ADFA-LD。ADFA-LD数据集是澳大利亚国防学院

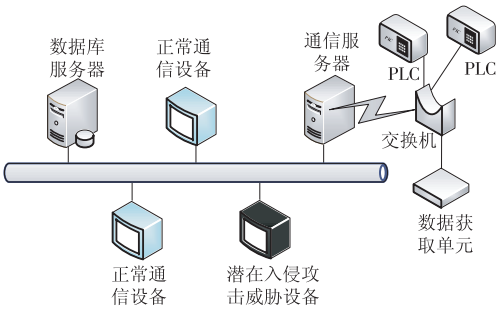

图4　试验数据采集环境

Fig. 4　Experimental data collection environment

在对网络入侵事件检测时获得整理的一套数据集，包含了入侵事件系统调用syscall序列的数据。该数据集主要包括攻击数据集、训练数据集和验证数据集3个部分。攻击数据集中包含了6种不同的攻击类型，数据集中不同类型数据的标注和数据量见表3。

表3　ADFA-LD中不同类型数据信息

Tab. 3　Different types of data information in ADFA-LD

数据类型	标注类型	数据量
Training_Data	训练数据	833
Validation_Data	验证数据	4 373
Adduser	攻击数据	91
Hydra_FTP		162
Hydra_SSH		148
Java_Meterpreter		125
Meterpreter		75
Web_Shell		118

3.2　评价标准

对于检测方案中的设计模型，需要设定相应的模型评价标准，来评测电网通信入侵检测的准确率。本文将入侵攻击数据流量定义为正例，正常数据流量定义为负例，评价标准中各指标定义见表4。

表4　评价指标含义解释

Tab. 4　Explanation of the meaning of evaluation indicators

评价指标	解释
N_{TP}	入侵攻击数据流量被方案检测为正例的个数
N_{TN}	正常数据流量被方案检测为负例的个数
N_{FP}	正常数据流量被方案检测为正例的个数
N_{FN}	入侵攻击数据流量被方案检测为负例的个数

计算检测准确率的表达式为

$$R_{accuracy}=\frac{N_{TP}+N_{TN}}{N_{TP}+N_{TN}+N_{FP}+N_{FN}}。\tag{9}$$

3.3　结果分析

首先对检测方案中的k参数进行不同取值，分析对结果的影响；然后评估了采取优化特征提取方法的AMI通信入侵检测方案的性能；最后比较了本文提出的方案和传统AAFID入侵检测系统在ADFA-LD数据集上的检测效果。

3.3.1　选取k值

通过调试程序，设置循环来输入k的取值集合。从1开始，测试到训练数据数量的平方根，选取最优k值作为提出方案的参数。不同k值下，不同特征提取方法的检测准确率如图5所示。

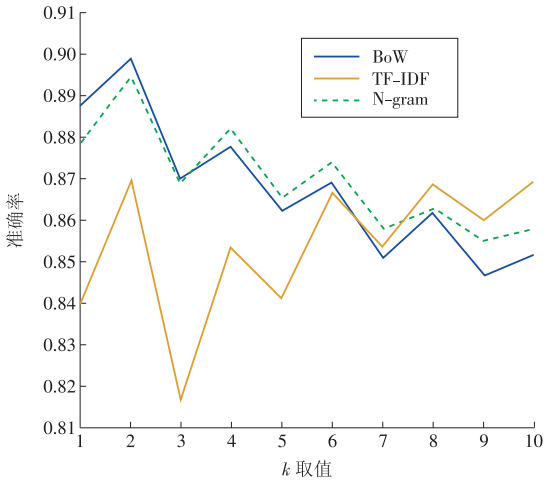

图5　不同k值下各方案检测准确率

Fig. 5　Accuracy of detection schemes with different values of k

从图5可以看出，确定特征提取方法的情况下，模型训练中选取距离最小数据点的个数为2时，检测效果要优于k值取集合内的其他值。经过代码调试，当k值继续增加时，对入侵攻击数据的检测准确率呈现波动下降趋势。在实际电网环境中，若将采集到的数据处理成和ADFA-LD相同格式的数据集，使用本文提出方案进行入侵攻击检测时，可将KNN分类模型中的k值取为2。

3.3.2　不同特征提取方法下的检测结果

当攻击数据集选取特定入侵攻击类型的数据集合，使用BoW，TF-IDF，N-gram等3种特征提取方法，优化输入KNN模型的特征向量，检测准确率如图6所示。

从图6可以看出，除了在检测Meterpreter攻击时，采用TF-IDF方法进行特征提取的检测效果略微优于BoW和N-gram方法，检测其他5种类型的入侵攻击数据时，BoW和N-gram的特征提取的检测效果更好。在使用TF-IDF方法对ADFA-LD数据集中数据进行文本特征提取时，由于该数据集是一个数据特征信息已经处理为数字格式的良好数据集，所以IDF算法在试图抑制噪声数据的加权过程中，会倾向于文本中频率较小的词，进而导致对各类入侵攻击数据的检测准确率较低。在智能电网AMI

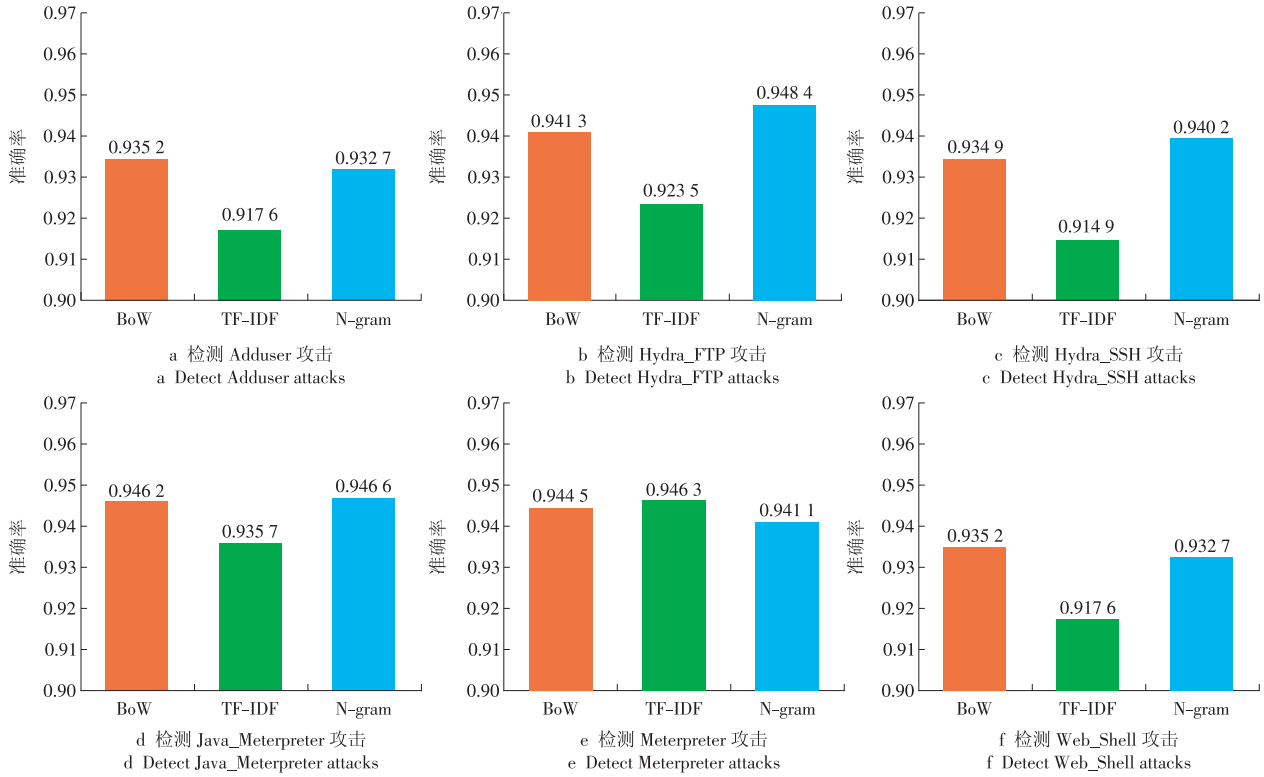

图 6　数据集中各攻击类型检测准确率

Fig. 6　Detection accuracy rate of each attack type in the data set

架构进行入侵检测过程中，选用文本特征提取相关模型需要注意词频和逆文本频率指数加权等改进机制的合理性，否则入侵攻击数据识别准确率反而可能会降低。

3.3.3　入侵检测方式对比

AAFID是一种典型的入侵检测系统，采用了自治代理的思想，可用于分布式入侵检测。在AAFID中，特征工程部分采用专家经验设定的方式，并没有对特征进行抽象提取的过程。本文方案和传统的AAFID检测效果对比见表5。

表 5　提出方案和AAFID的检测对比

Tab. 5　Comparison between the proposed detection scheme and AAFID detection

对比方案	选用特征提取方法	检测准确率/%
本文方案	BoW	87.77
	TF-IDF	85.31
	N-gram	88.20
传统的AAFID检测		66.24

传统的AAFID在对划分好的数据集进行检测时，检测度函数平均结果取值可达到66.24%[17]。在BoW，TF-IDF，N-gram等3种不同的优化特征提取方法下，结合KNN和优化特征工程的AMI通信入侵检测方案的检测准确率可分别达到87.77%，85.31%和88.20%。试验证明这种方案应用于AMI通信入侵检测具有良好的性能。

4　结束语

本文基于智能电网高级量测体系中通信架构的特点，分析了入侵攻击对电网通信的安全威胁，提出了一种结合KNN和优化特征工程的AMI通信入侵检测方案。特征工程部分应用BoW，TF-IDF，N-gram等3种不同的文本特征提取方法，并计算得到各特征数据的信息增益值，选取信息增益值较大的特征作为KNN模型训练的输入特征向量，对AMI通信中的异常入侵数据流量进行模型训练和分类识别。在试验部分，设计了AMI通信过程获取数据的仿真试验环境，通过公开入侵检测数据集ADFA-LD检验提出方案对入侵攻击数据流量的预测准确率，调试k值得到了KNN模型对该组数据集检测的最优参数，并比较了3种优化模型输入特征的提取方法对检测结果准确率的影响。在提取特征向量较多的情况下，后续将针对降低检测算法的复杂度进行研究，尝试采用深度学习方法节省特征工程阶段时间，同时提高对样本类别分布不均衡数据集的检测准确率。

参考文献：

[1]王德文，杨力平.智能电网大数据流式处理方法与状态监测异常检测[J].电力系统自动化，2016，40(14)：122-128.

WANG Dewen, YANG Liping. Stream processing method and condition monitoring anomaly detection for big data in smart grid[J]. Automation of Electric Power Systems, 2016, 40(14): 122-128.

[2]鄢晶, 高天露, 张俊, 等. 边云链协同技术在能源互联网数据管理中的应用及展望[J]. 华电技术, 2020, 42(8): 41-47.
YAN Jing, GAO Tianlu, ZHANG Jun, et al. Application and prospect of edge-cloud-chain collaboration technologies for energy internet data management [J]. Huadian Technology, 2020, 42(8): 41-47.

[3]张文亮, 刘壮志, 王明俊, 等. 智能电网的研究进展及发展趋势[J]. 电网技术, 2009, 33(13): 1-11.
ZHANG Wenliang, LIU Zhuangzhi, WANG Mingjun, et al. Research status and development trend of smart grid [J]. Power System Technology, 2009, 33(13): 1-11.

[4]张宪军, 赵谦, 梁志宝, 等. 智能变电站交换机基于GOOSE管理技术设计与实现[J]. 华电技术, 2020, 42(2): 42-49, 57.
ZHANG Xianjun, ZHAO Qian, LIANG Zhibao, et al. Design and implementation of GOOSE management technology on smart substation switches[J]. Huadian Technology, 2020, 42(2): 42-49, 57.

[5]韦尧, 王昌达. 基于熵的入侵检测研究综述[J]. 计算机应用与软件, 2020, 37(4): 297-302.
WEI Yao, WANG Changda. A review of entropy-based intrusion detection[J]. Computer Applications and Software, 2020, 37(4): 297-302.

[6]和湘, 刘晟, 姜吉国. 基于机器学习的入侵检测方法对比研究[J]. 信息网络安全, 2018(5): 1-11.
HE Xiang, LIU Sheng, JIANG Jiguo. Comparative study of intrusion detection methods based on machine learning[J]. Net Information Security, 2018(5): 1-11.

[7]MOUSTAFA N, SLAY J. The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems [C]//2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Kyoto, Japan, 2015.

[8]李雅洁. 智能电网邻域网入侵检测技术研究与实现[D]. 北京: 北京邮电大学, 2018.

[9]ZHOU C, WANG Z, HUANG W, et al. Research on network security attack detection algorithm in smart grid system[C]// 2017 International Conference on Computer Technology, Electronics and Communication, Dalian, China, 2017.

[10]HE H. Intrusion detection method based on improved neural network [C]//2018 International Conference on Smart Grid and Electrical Automation, Changsha, 2018.

[11]OUYANG X, MA Z. Using LSTM Networks to identify false data of smart terminals in the smart grid [C]// 2017 IEEE 23rd International Conference on Parallel and Distributed Systems, Shenzhen, China, 2017: 765-768.

[12]蒋南允, 程光. 智能电网入侵检测综述[J]. 网络空间安全, 2018, 9(1): 93-98.
JIANG Nanyun, CHENG Guang. A review of intrusion detection in smart grid[J]. Cyberspace Security, 2018, 9(1): 93-98.

[13]王贵珍, 曲天光. 入侵检测系统研究与发展概述[J]. 保密科学技术, 2019(2): 30-35.
WANG Guizhen, QU Tianguang. Overview of research and development of intrusion detection system [J]. Secrecy Science and Technology, 2019(2): 30-35.

[14]RADOGLOU-GRAMMATIKIS P I, SARIGIANNIDIS P G. An anomaly-based intrusion detection system for the smart grid based on CART decision tree [C]//2018 Global Information Infrastructure and Networking Symposium, Thessaloniki, Greece, 2018.

[15]郝建军, 王启银, 张兴忠. 基于支持向量机的电网通信入侵检测技术[J]. 电测与仪表, 2019, 56(22): 109-114.
HAO Jianjun, WANG Qiyin, ZHANG Xingzhong. Intrusion detection technology based on support vector machine for power grid communication [J]. Electrical Measurement & Instrumentation, 2019, 56(22): 109-114.

[16]REN B, HU M, YAN H, et al. Classification and prediction of network abnormal data based on machine learning [C]// 2019 International Conference on Robots & Intelligent System, Haikou, China, 2019.

[17]刘金辉, 李娜, 葛丽娜, 等. 改进的神经网络应用于入侵检测的方案[J]. 网络新媒体技术, 2017, 6(6): 54-60, 53.
LIU Jinhui, LI Na, GE Lina, et al. Improved neural network applied to intrusion detection computer engineering and applications[J]. Journal of Network New Media, 2017, 6(6): 54-60, 53.

(本文责编: 陆华)

作者简介:

卢官宇(1997—), 男, 山东德州人, 在读硕士研究生, 从事电力终端安全、基于机器学习电网异常流量检测方面的研究(E-mail: lgy18521035808@163.com)。

田秀霞*(1976—), 女, 河南安阳人, 教授, 博士, 从事数字图像篡改检测、数据库安全、隐私保护、安全机器学习、面向电力用户的安全计算方面的研究(E-mail: xxtian@shiep.edu.cn)。

张悦(1998—), 女, 安徽宿州人, 在读硕士研究生, 从事信息安全、访问控制方面的研究工作(E-mail: zy17621817238@163.com)。