沈阳农业大学学报,2024,55(3):354-362 http://syny.cbpt.cnki.net
Journal of Shenyang Agricultural University DOI:10.3969/j.issn.1000-1700.2024.03.011

王小宇,贺鸿鹏,马成龙,等.基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法[J].沈阳农业大学学报,2024,55(3):354-362.

WANG Xiaoyu, HE Hongpeng, MA Chenglong,et al.Application layer DDoS attack detection method based on multimodal neural network traffic characteristics[J].Journal of Shenyang Agricultural University,2024,55(3):354-362.

基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法

王小宇[1,2],贺鸿鹏[2],马成龙[2],陈欢颐[2]

(1.西安理工大学 电气工程学院,西安 710048;2.国网内蒙古东部电力有限公司,呼和浩特 010010)

摘　要:农业设备、传感器和监控系统与网络的连接日益紧密,给农村配电网带来了新的网络安全挑战。其中,分布式拒绝服务(DDoS)攻击是一种常见的网络威胁,对农村配电网的安全性构成了严重威胁。针对农村配电网的特殊需求,提出一种基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法。通过制定网络应用层流量数据包捕获流程并构建多模态神经网络模型,成功提取并分析了网络应用层DDoS攻击流量的特征。在加载DDoS攻击背景下的异常流量特征后,计算相关系数并设计相应的DDoS攻击检测规则,以实现对DDoS攻击的有效检测。经试验分析,所提出的方法在提取DDoS攻击相关特征上表现出色,最大提取完整度可达95%,效果明显优于对比试验中基于EEMD-LSTM的检测方法和基于条件熵与决策树的检测方法。

关键词:农村配电网;流量特征提取;DDoS攻击;网络应用层;多模态神经网络;攻击行为检测

中图分类号:TP393　　**文章编号**:1000-1700(2024)03-0354-09

文献标识码:A　　**开放科学(资源服务)标识码(OSID)**:

Application Layer DDoS Attack Detection Method Based on Multimodal Neural Network Traffic Characteristics

WANG Xiaoyu[1,2], HE Hongpeng[2], MA Chenglong[2], CHEN Huanyi[2]

(1. School of Electrical Engineering, Xi′an University of Technology, Xi′an 710048, China;
2. State Grid East Inner Mongolia Electric Power Supply Co., Ltd., Hohhot 010010, China)

Abstract: The increasing connectivity of agricultural equipment, sensors and monitoring systems to the network poses new cybersecurity challenges to rural distribution grids. Among them, distributed denial-of-service (DDoS) attacks are a common cyber threat that poses a serious threat to the security of rural power distribution networks. This study is dedicated to propose a network application layer DDoS attack detection method based on multimodal neural network traffic features for the special needs of rural power distribution networks. By formulating the web application layer traffic packet capture process and constructing a multimodal neural network model, the features of web application layer DDoS attack traffic are successfully extracted and analyzed. After loading the abnormal traffic features in the context of DDoS attack, the correlation coefficient is calculated and the corresponding DDoS attack detection rules are designed to achieve effective detection of DDoS attack. After experimental analysis, the proposed method performs well in extracting DDoS attack related features, with a maximum extraction completeness of up to 95%, which is significantly better than that of the DDoS attack

收稿日期:2024-02-20

基金项目:国网内蒙古东部电力有限公司科技项目(SGMD0000DDJS2200049)

第一作者:王小宇(1982-),男,硕士,高级工程师,从事电力系统自动化、继电保护、知识图谱及人工智能研究,E-mail:wangxiaoyu1005@163.com

通信作者:贺鸿鹏(1989-),男,硕士,高级工程师,从事电力调度自动化、电力系统及其自动化研究,E-mail:hehongpeng@126.com

detection methods based on EEMD-LSTM and those based on conditional entropy and decision tree in the comparison experiments.

Key words: rural power distribution networks; traffic feature extraction; DDoS attacks; network application layer; multimodal neural network; attack behavior detection

建设新型电力系统,是加强生态文明建设、保障国家能源安全、实现可持续发展作出的重大部署,也是践行“四个革命、一个合作”能源安全新战略和落实“双碳”目标的重要举措。在“双碳”目标引领下,建设新型电力系统是一道必答题。而配电网是新型电力系统的重要组成部分,配电网是传统电网的末端环节,在能源转型的背景下,配电网愈发成为了电力网络发展的未来方向[1]。农村配电网也正逐步由单纯接受、分配电能给用户的电力网络转变为源网荷储融合互动、与上级电网灵活耦合的电力网络。为推动新形势下配电网高质量发展,助力构建清洁低碳、安全充裕、经济高效、供需协同、灵活智能的新型电力系统。农村配电网在信息化和网络化的进程中扮演着至关重要的角色。然而,随着农业生产、管理和监测过程中数据量的急剧增加,网络安全问题愈发突出。

分布式拒绝服务(DDoS)攻击作为一种常见的网络威胁形式,正日益对农村配电网和相关基础设施构成严重挑战[2-3]。DDoS攻击不仅可能直接损害农业机构、农业供应链系统或农业物联网设备,导致服务中断或延迟,还有可能瘫痪重要的农业系统如农田灌溉系统、温室控制系统等,对农作物的生长和产量带来严重影响,进而损害整个农业生产和供应链的稳定性,给相关企业和个人带来巨大的经济损失和安全风险[4-6]。在这一背景下,本研究致力于探讨基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法,以为农村配电网的安全发展提供有效技术支持。通过深入研究网络应用层DDoS攻击的检测方法,将为农业生产网络安全领域带来新的理念和技术支持,有助于有效防范和抵御各类网络安全威胁。在当今信息化高速发展的背景下,确保农村配电网的安全发展不仅关乎农业生产和供应链的正常运转,更是对我国农村现代化进程的重要保障,因此,对网络应用层DDoS攻击的检测方法研究具有极其重要的现实意义和应用价值。

李彬等[7]引入集合经验模态分解与长短期记忆网络设计了一种DDoS攻击双重检测方法,利用集合经验模态分解攻击流量,对模态特征进行提取,利用改进的LSTM神经网络检测DDoS攻击。此种方法应用的长短期记忆网络改进程序较为复杂,容易陷入局部最优困境,致使DDoS攻击检测精度与效率均不理想;傅友等[8]以软件定义网络(SDN)作为研究对象,引入条件熵和决策树设计了一种全新的DDoS攻击检测方法,采用条件熵对SDN运行状态进行判断,深入分析DDoS攻击特点,并提取其6项重要特征,通过C4.5决策树算法分类处理网络流量数据,从而实现DDoS攻击的有效检测。此种方法提取的DDoS攻击特征数量较少,会降低DDoS攻击检测的准确性;还有外国学者以软件定义网络(SDN)作为研究对象,根据网络流量动态特性选取适当的动态阈值,在机器学习算法的支持下,有效区分DDoS攻击和正常流量,从而实现DDoS攻击的检测功能[9]。此种方法在动态阈值选取方面需要耗费大量的运算资源,致使攻击检测耗时较长,无法满足软件定义网络(SDN)的安全需求;SHALINI等[10]以CUSUM为基础,对闪存流量进行识别与分离,最大限度地减少将良性流量作为攻击错误检测事件的发生,从而完成DDoS攻击检测方法(DOCUS)的开发。此种方法考虑到了闪存流量的影响,虽然一定程度上提升了DDoS攻击检测的精度,但依然无法满足日益增长的DDoS攻击检测需求。

多模态神经网络流量特征通过综合分析不同模态的信息,能够更好地捕捉到攻击者在攻击期间留下的特征。同时,神经网络的特征提取和模式识别能力可以自动学习正常流量与攻击流量之间的差异,从而实现有效的攻击识别和分类。因此,为了能够有效地应对新型攻击和变种攻击,并且具有较低的误报率,为网络安全人员提供了强有力的帮助和保护,提出基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法。

1　基于多模态神经网络的网络应用层流量特征提取

1.1　网络应用层流量数据包捕获

网络应用层流量数据包捕获是网络应用层DDoS攻击检测过程中的关键环节[11],主要为DDoS攻

击检测提供基础数据支撑。从本质角度出发，网络应用层流量数据包捕获是一个较为复杂的过程，涉及步骤、环节较多，需要对其进行合理地规划与执行[12-13]。

此研究将网络应用层流量数据包捕获划分为两个阶段，分别为准备阶段与捕获阶段[14]。结合网络应用层的流量特性，制定流量数据包捕获流程，具体如图1。依据图1所示流程捕获网络应用层的流量数据包，将其整合为集合形式，记为$R=\{r_1,r_2,\cdots,r_i,\cdots,r_N\}$。其中，$r_i$表示第$i$种模态网络应用层流量数据子集；$N$表示数据包中流量数据模态的总数量。该集合中的模态网络指的是网络中具有不同特征或行为模式的应用层流量数据。

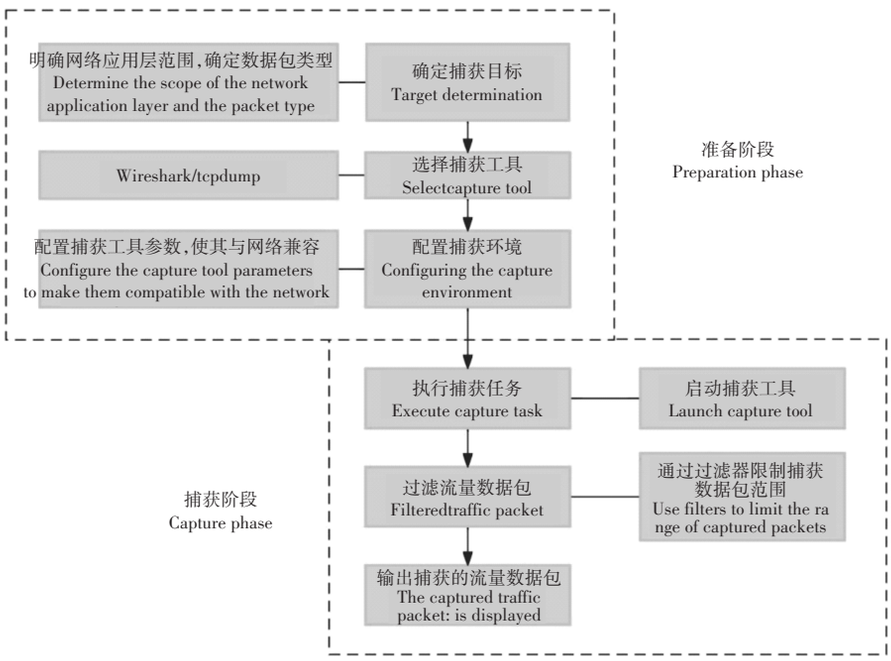

图1 网络应用层流量数据包捕获流程图

Figure 1 Flowchart for capturing web application layer traffic packets

上述过程完成了网络应用层流量数据包的捕获，为后续DDoS攻击相关流量特征提取奠定坚实的基础。

1.2 DDoS攻击相关流量特征提取

根据图1得到的网络应用层的流量数据包$R=\{r_1,r_2,\cdots,r_i,\cdots,r_N\}$数据量较大，且捕获的流量数据包中可能混杂有底层网络层的协议信息、无效的或冗余的数据包，这些数据对最终的DDoS攻击检测具有较大的负面影响。多模态神经网络由多个子网络组成，可以将来自不同模态的数据进行特征提取和融合，每个子网络处理一种模态的数据，并通过一定的机制将各个模态的特征进行融合。通过训练神经网络，可以学习到有效地表示网络应用层流量数据的特征，以用于后续的分类、识别和分析任务。故此研究构建多模态神经网络模型[15-18]，利用该模型提取DDoS攻击相关流量特征，为后续DDoS攻击相关流量特征提取提供支撑。

多模态神经网络模型如图2，构建的多模态神经网络模型主要分为以下3部分。

1.2.1 特征提取部分 $R=\{r_1,r_2,\cdots,r_i,\cdots,r_N\}$中每个模态的流量数据都会通过一个独立的子网络进行特征提取。此研究采用卷积神经网络（CNN）作为特征提取子网络，其数量与流量数据模态的总数量一致（N）。

1.2.2 特征融合部分 特征融合负责将来自子网络输出的不同模态流量特征进行整合。为了不影响流量特征内涵的关键信息，此研究只采用简单的拼接来融合流量特征。

1.2.3 特征决策部分 在流量特征融合后，对其进行分类，为后续流量特征应用提供便利，输出结果就是最终的网络应用层流量特征。

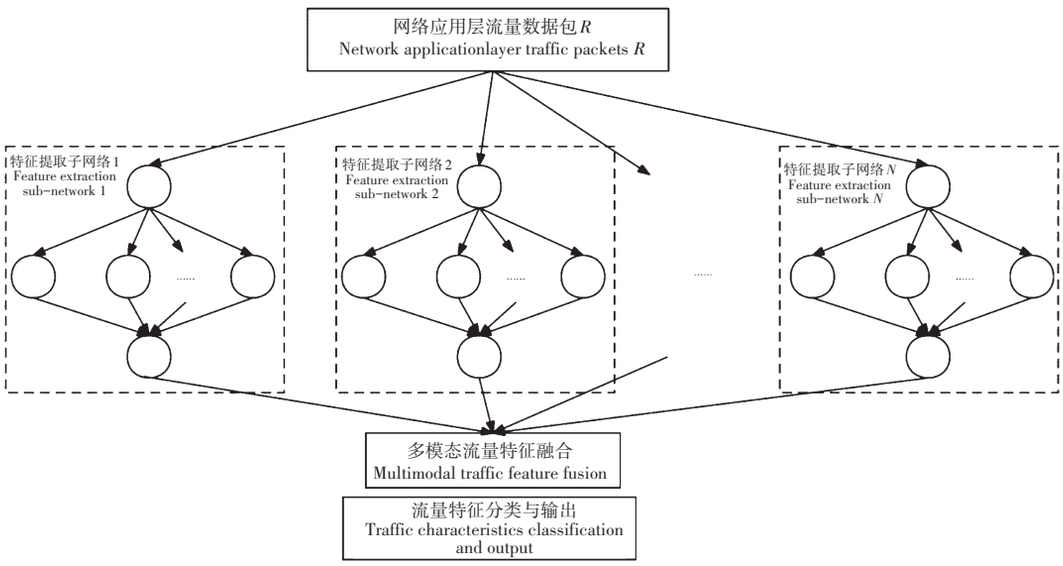

图 2　多模态神经网络模型示意图

Figure 2　Schematic diagram of a multimodal neural network model

上述过程完成了多模态神经网络模型构建[19-21],将 1.1 节捕获的网络应用层流量数据包 $R=\left\{r_1,r_2,\cdots,r_i,\cdots,r_N\right\}$ 输入至图2多模态神经网络模型中,提取DDoS攻击相关流量特征。

将多模态流量数据均分给多个独立的子网络(卷积神经网络),以某一模态流量数据子集 r_i 为例,阐明卷积神经网络提取DDoS攻击相关流量特征的全过程。此研究中卷积神经网络采用最简单的结构,其主要包括输入层、隐含层与输出层。输入层主要是对模态流量数据子集 $r_i=\left\{x_1,x_2,\cdots,x_j,\cdots,x_n\right\}$ (n 表示流量数据的总数量)进行接收与清洗,表达式为:

$$\begin{cases}\zeta\left(x_j\right)=\dfrac{x_j-mean\left(r_i\right)}{std\left(r_i\right)}\\ \begin{cases}\zeta\left(x_j\right)\geqslant\zeta^o & \text{保留}x_j\\ \zeta\left(x_j\right)<\zeta^o & \text{删除}x_j\end{cases}\end{cases}\tag{1}$$

式中:$\zeta\left(x_j\right)$ 为 x_j 的 Z 分数;x_j 为模态流量数据子集 r_i 中的第 j 个流量数据;$mean\left(r_i\right)$ 与 $std\left(r_i\right)$ 为模态流量数据子集 r_i 的平均值与标准差;ζ^o 为流量数据是否异常的判定阈值。

依据公式(1)中的判断条件,完成模态流量数据子集 r_i 中异常流量数据的清洗,剩余模态流量数据子集为 $r_{i1}=\left\{x_1,x_2,\cdots,x_j,\cdots,x_p\right\}=1-r_i$,$p$ 表示剩余流量数据的总数量。

隐含层对剩余模态流量数据子集 r_{i1} 内部的数据进行非线性变换,其输出结果为:

$$H_i=activation\left(\omega_i{}^*r_{i1}+\delta_i\right)\tag{2}$$

式中:H_i 为隐含层输出结果;$activation(\cdot)$ 为激活函数;ω_i 为权重系数;δ_i 为偏置项。

输出层对隐含层输出结果进行深度处理,获取模态流量特征,表达式为:

$$y_i=\hat{\omega}_i\times H_i+\hat{\delta}_i\tag{3}$$

式中:y_i 为输出层输出结果,即模态流量特征;$\hat{\omega}_i$ 为输出层的权重系数;$\hat{\delta}_i$ 为输出层的偏置项。

依据上述步骤获取DDoS攻击相关多模态流量特征,记为 $Y=\left\{y_1,y_2,\cdots,y_i,\cdots,y_N\right\}$,按照简单拼接原则对其进行融合处理,记为 $X=\left\{x_1,x_2,\cdots,x_j,\cdots,x_M\right\}$,$M$ 表示全部流量特征的数据量。融合后的多模态流量特征 X 数据量较多,并呈现着随机的特性,若是不对其进行处理,势必会增加DDoS攻击检测的运算量。因此,根据流量特征特性,对其进行分类处理,将最终的DDoS攻击相关多模态流量特征记为 $X=\left\{X_1,X_2,\cdots,X_k\right\}$,$X_k$ 表示第 k 种DDoS攻击相关流量特征。

上述过程完成了DDoS攻击相关多模态流量特征的提取与处理，为后续DDoS攻击检测提供有效的依据。

2 基于流量特征的DDoS攻击检测

DDoS攻击是一种分布式拒绝服务攻击，其目的是通过大量无用的请求拥塞目标网络，导致合法用户无法正常访问[22]。DDoS攻击通常是一种少数攻击者对大量受害者发起的攻击方式，导致正常流量与攻击流量的比例不平衡。在网络应用层发生该类攻击时，容易导致训练模型出现偏差，影响检测性能。因此，依据上述描述内容，获取DDoS攻击背景下网络应用层异常流量特征，记为$\eta=\{\eta_1,\eta_2,\cdots,\eta_5\}$，通过制定DDoS攻击检测规则，实现DDoS攻击检测。

以提取的DDoS攻击相关多模态流量特征$X=\{X_1,X_2,\cdots,X_k\}$与DDoS攻击背景下网络应用层异常流量特征$\eta=\{\eta_1,\eta_2,\cdots,\eta_5\}$为基础，衡量两者之间的相关系数，以此为基础，制定DDoS攻击检测规则，从而实现研究目标[23]。

DDoS攻击相关多模态流量特征集合与DDoS攻击异常流量特征集合相关系数计算公式为：

$$\xi=\frac{X\cap\eta}{X\cup\eta} \tag{4}$$

式中：ξ为X与η的相关系数。

以式(4)计算结果为基础，制定DDoS攻击检测规则[24-27]，具体公式为：

$$\begin{cases}\xi\geqslant\tilde{\Phi} & \text{存在DDoS攻击}\\ \xi<\tilde{\Phi} & \text{不存在DDoS攻击}\end{cases} \tag{5}$$

式中：$\tilde{\Phi}$为DDoS攻击检测阈值。

综上所述，在多模态神经网络模型与流量特征支持的基础上，完成了网络应用层DDoS攻击的有效检测，为网络的安全运行提供助力[28-29]。

3 试验设置与结果分析

本研究选取李彬等[7]的DDoS攻击检测方法(基于EEMD-LSTM的DDoS攻击检测方法)、傅友等[8]条件熵和决策树的DDoS攻击检测方法(基于条件熵和决策树的DDoS攻击检测方法)分别作为本研究的对比试验，结合提出方法共同进行网络应用层DDoS攻击检测对比试验，以此来测试提出方法的应用性能。

3.1 试验设置

为了避免应用层DDoS攻击造成系统瘫痪，在操作系统Ubuntu 20.04 LTS、3.8.10Python版本、TensorFlow 2.5.0深度学习框架、NVIDIA GeForce GTX 1080Ti的GPU环境中，模拟网络应用层攻击过程(图3)。

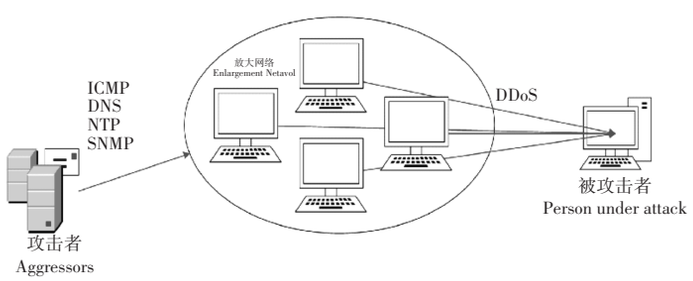

图 3 DDoS攻击过程

Figure 3 DDoS attack process

在试验过程中，考虑到提出方法构建了多模态神经网络模型对流量特征进行提取，其内部子网络隐含层节点数量是否合理直接影响着流量特征提取效率。因此，在试验进行之前，对子网络隐含层节

点数量进行确定。通过测试获得子网络隐含层节点数量与CNN训练迭代次数的关系如图4。

由图4可知,随着隐含层节点数量的增加,CNN训练迭代次数呈现先下降后上升的变化趋势。当隐含层节点数量为10个时,CNN训练迭代次数达到最小值5次,此时流量特征提取效率达到最大值。因此,确定子网络隐含层节点数量为10个。

除上述参数外,设定多模态神经网络参数如表1。

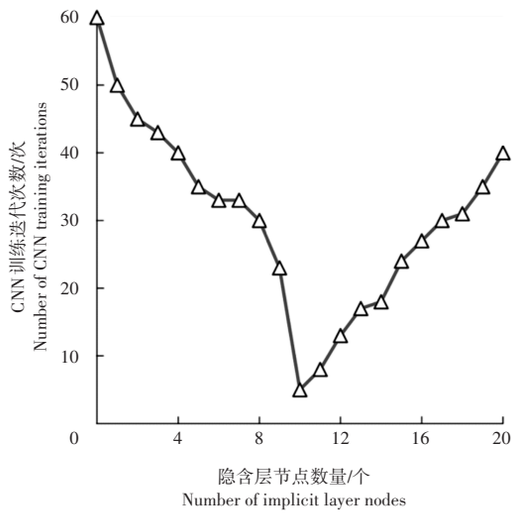

图4　神经网络隐含层节点数量与CNN训练迭代次数关系示意图

Figure 4　Relationship between number of nodes in hidden layer of neural network and number of CNN training iterations

表1 多模态神经网络参数

Table 1 Multimodal neural network parameters

参数 Parameters	值 Value
网络架构 Network infrastructure	MLP
输入层 Input layer	10
隐含层 Implicit layer	3
输出层 Output layer	Sigmoid
学习率 Learning rate	0.001
批大小 Batch size	64
迭代次数 Number of iterations	50
优化器 Optimizer	Adam
暂退层 Dropout	0.2
正则化 Regularization	L2 regularization (Weight decay factor: 0.001)

在试验数据采集方面,考虑数据的来源和质量,试验所采集的数据来自某农村配电网的真实网络系统。在上述参数设定后,采用Wireshark软件捕获试验对象不同时间背景下网络应用层流量数据包,具体如表2。

表2　流量数据包准备

Table 2　Traffic packet preparation

流量数据包采集时间/hh:mm Traffic packet acquisition time	流量数据包大小/GB Traffic packet size	异常流量数据占比/% Percentage of anomalous traffic data
8:00	56.46	2.30
8:30	42.13	10.20
9:00	30.15	4.56
9:30	26.89	18.12
10:00	45.12	9.56
10:30	51.29	7.45
11:00	45.32	8.26
11:30	47.82	8.45
12:00	53.23	5.42
12:30	58.90	6.23

对于网络应用层流量数据包的采集,经分析发现在采集时间、规模大小以及异常流量数据占比等方面存在一定程度的差异[30-31]。这种差异性反映了真实网络环境中数据流量的多样性和变化性,有助于更全面地评估提出的网络应用层DDoS攻击检测方法的有效性和适用性[22,32]。

3.2 试验结果分析

以上述准备的网络应用层流量数据包与确定的子网络隐含层节点数量为基础，进行网络应用层DDoS攻击检测对比实验。通过DDoS攻击相关特征提取完整度与DDoS攻击检测结果来反映提出方法的应用性能。

通过试验获得DDoS攻击相关特征提取完整度如表3。

表 3 DDoS攻击相关特征提取完整度

Table 3 DDoS attack related feature extraction completeness table

流量数据包采集时间/hh:mm Traffic packet acquisition time	本研究方法/% Methodology	EEMD-LSTM/%	条件熵和决策树/% Conditional entropy and decision trees
8:00	89	76	56
8:30	95	65	45
9:00	91	56	41
9:30	87	51	58
10:00	86	54	57
10:30	80	50	59
11:00	94	50	59
11:30	90	53	45
12:00	90	62	43
12:30	94	69	40

实际上，基于EEMD-LSTM和基于条件熵和决策树的DDoS攻击检测方法均存在一定的理论和实践问题。基于EEMD-LSTM的DDoS攻击检测方法首先通过集合经验模态分解攻击流量提取模态特征，其次基于改进的LSTM神经网络进行攻击检测[7]。这种方法虽然在一定程度上提高了基于单一LSTM神经网络的检测效率，但EEMD模型只能分解提取流量频域的暂态特征从而忽略流量数据的全局动态特征，并且当前DDoS攻击具有多特征、多形式等复杂特点，这些都限制了对比方法一对DDoS攻击特征的提取效果从而影响最后的检测效率。

基于条件熵和决策树的DDoS攻击检测方法利用条件熵判断当前网络状态，通过分析SDN中DDoS攻击特点，提取用于流量检测的多项重要特征，再使用C4.5决策树算法进行网络流量分类以实现对SDN网络中的DDoS攻击的检测[8]。该方法同样在提取DDoS攻击流量深层次特征效果及检测效率方面存在不足，往往难以提取出攻击流量的全部相关特征从而极大程度上影响检测结果。

由表3可知，本研究提出方法获得的DDoS攻击相关特征提取完整度远远高于对比基于EEMD-LSTM的DDoS攻击检测方法与基于条件熵和决策树的DDoS攻击检测方法，其最大值达到95%。这主要是因为本研究所提出的方法应用了多模态神经网络模型，通过结合多个不同维度的卷积神经网络捕捉到了更多DDoS攻击可能导致的异常模式，进而提高了特征提取的完整度，为后续DDoS攻击检测效果提供更好的理论基础。

通过试验获得实际DDoS攻击检测结果如图5。同时，为了确保准确分析检测效果，以图5的检测结果为依据，对比3种方法的检测效果，并进行量化处理，结果如图6。

由图5和图6可知，当应用本研究提出的方法来进行DDoS攻击检测时，其所得结果与实际情况完全吻合，这表明该方法具有高度的准确性和可靠性。相较之下，应用对比基于EEMD-LSTM的检测方法和基于条件熵和决策树的检测方法所得到的DDoS攻击检测结果，与真实情况存在一定的偏差，这种偏差可能会给网络安全带来潜在的风险和威胁。因此，从实际效果来看，本研究提出的方法在DDoS攻击检测上展现出了更为优越的性能。本研究提出的方法在利用多模态神经网络提取应用层DDoS攻击检测流量特征方面，有着独特的优势。多模态神经网络能够综合考虑不同维度的信息，从而更全面地反映流量的特性。在提取出特征后，本研究方法还根据预先制定的DDoS攻击检测规则，通过匹配异常流量特征的相关度，来判定是否发生了DDoS攻击。这种基于规则的匹配方法，能够更精确地识别出攻击行为，减少误报和漏报的可能性。本研究提出的方法不仅能够准确地判断DDoS攻

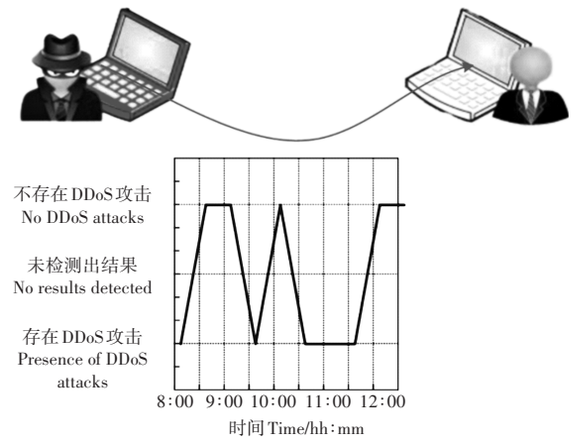

图5　DDoS攻击实际检测结果

Figure 5　Actual DDoS attack detection results

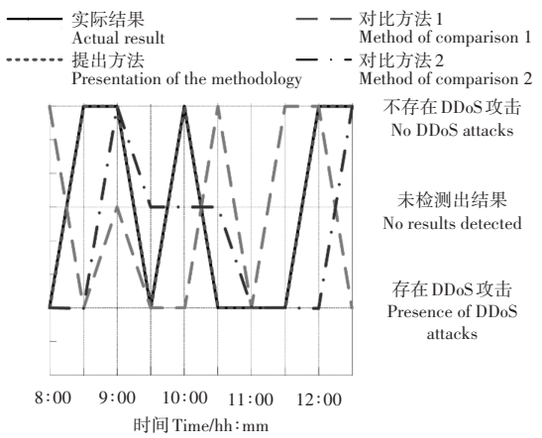

图6　DDoS攻击检测结果示意图

Figure 6　Diagram of DDoS attack detection results

击的发生,还能够提供有关攻击特征的详细信息,这对于后续的防御和应对措施制定具有重要的指导意义。因此,相较于其他方法,本研究提出的方法在DDoS攻击检测上不仅结果更可靠,而且具有更高的实用价值[33-34]。

4　讨论与结论

随着互联网的普及和网络技术的不断发展,DDoS对农业网络的攻击也在不断演进和变化,其已经成为威胁农业生产的关键因素之一。在该背景下,提出基于多模态神经网络流量特征的网络应用层DDoS攻击检测方法研究。试验数据显示:提出方法有效地提升了DDoS攻击相关特征提取完整度与DDoS攻击检测精度,能够为网络应用层的稳定运行提供更有力的支撑。

随着大语言模型的兴起与快速发展,DDoS攻击及恶意流量检测领域未来可能会有更多高效、轻量且准确率更高的方法。比如,探索如何赋予大语言模型自适应学习能力,使其能够随着时间不断提高对新型攻击和恶意流量的识别准确性。同时,需要关注增强模型对对抗性攻击的鲁棒性,以应对可能出现的攻击和干扰。最后,对于数据隐私与安全问题也需要深入研究,以确保在使用大语言模型进行DDoS攻击和恶意流量检测时不会牺牲用户数据的安全性和隐私保护。

参考文献:

[1] 耿立宏,冯义华.孙吉昌:建设新型农村配电网 赋能乡村振兴[J].农电管理,2024(2):11-13.

[2] HOANG TRONG V,GWANG-HYUN Y,THANH VU D,et al.Late fusion of multimodal deep neural networks for weeds classification[J].Computers and Electronics in Agriculture,2020,175:105506.

[3] ZHA L J,MIAO J Z,LIU J L,et al.State estimation for delayed memristive neural networks with multichannel round-robin protocol and multimodal injection attacks[J].IEEE Transactions on Systems,Man,and Cybernetics:Systems,2024,99:1-11.

[4] 贾　鹏,王平辉,陈品安,等.基于无监督学习的智能数据中心电力拓扑系统[J].清华大学学报(自然科学版),2023,63(5):730-739.

[5] 洪惠群,黄风华.基于轻量级神经网络的农作物病害识别算法[J].沈阳农业大学学报,2021,52(2):239-245.

[6] 吴尚智,周　运,王欢欢,等.利用粗糙集和双隐层BP神经网络的小麦籽粒品种分类[J].沈阳农业大学学报,2020,51(5):576-585.

[7] 李　彬,魏吟斌,祁　兵,等.基于EEMD-LSTM的需求响应终端DDoS攻击检测方法[J].电力建设,2022,43(4):81-90.

[8] 傅　友,邹东升.SDN中基于条件熵和决策树的DDoS攻击检测方法[J].重庆大学学报,2023,46(7):1-8.

[9] FOULADI R F,ERMIŞ O,ANARIM E.A DDoS attack detection and countermeasure scheme based on DWT and auto-encoder neural network for SDN[J].Computer Networks,2022,214:109140.

[10] SHALINI P V,RADHA V,SANJEEVI S G.DOCUS-DDoS detection in SDN using modified CUSUM with flash

traffic discrimination and mitigation[J].Computer Networks,2022,217:109361.
[11] 孔 芝,孙 琦,寇晓宇,等.基于属性信息和结构特性的网络节点重要度研究[J].东北大学学报(自然科学版),2022,43(5):625-631.
[12] 谢汶锦,张智斌,张三妞.基于软件定义网络的DDoS攻击检测方案[J].重庆邮电大学学报(自然科学版),2022,34(6):1032-1039.
[13] 杨亚红,王海瑞.基于Renyi熵和BiGRU算法实现SDN环境下的DDoS攻击检测方法[J].计算机科学,2022,49(增刊1):555-561.
[14] 白坚镜,顾瑞春,刘清河.SDN环境中基于Bi-LSTM的DDoS攻击检测方案[J].计算机工程与科学,2023,45(2):277-285.
[15] 陆 焰,刘 霞,苏 皑.基于多模态神经网络的直播推荐[J].南京理工大学学报,2023,47(5):658-664.
[16] 丁来旭,刘洪娟.复杂网络上基于多维特征表示学习的推荐算法[J].东北大学学报(自然科学版),2022,43(3):359-367.
[17] 陈心怡,陶小梅.基于多模态生理信号特征融合的情感识别方法[J].计算机仿真,2023,40(6):175-181,186.
[18] 李占山,宋志扬,花昀峤.一种基于自适应搜索的多模态多目标优化算法[J].东北大学学报(自然科学版),2023,44(10):1408-1415.
[19] 吴鸿敏,张国英,管贻生,等.基于多模态时间序列建模的机器人安全监控[J].哈尔滨工业大学学报,2020,52(1):126-132.
[20] 姚家琪,荆 华,赵春晖.一种面向噪声环境中旋转机械故障诊断的多模态耦合输入神经网络[J].控制与决策,2023,38(7):1918-1926.
[21] 宋 永,杨 阔,覃觅觅.基于循环神经网络的多模态无线传感数据自适应融合方法[J].传感技术学报,2023,36(1):141-146.
[22] 王飞雪,戴 蓉.基于投票ELM和黑洞优化的云计算DDoS攻击检测[J].西南大学学报(自然科学版),2022,44(8):205-215.
[23] 孙 涛,蔡江涛,郭政杰,等.SDN环境下基于动态阈值的DDoS攻击检测方法研究[J].内蒙古大学学报(自然科学版),2022,53(1):98-104.
[24] 倪洪杰,俞文海,张 丹.不确定DoS攻击下的异构多智能体系统异步控制器设计[J].哈尔滨工业大学学报,2021,53(8):153-162.
[25] 陈淑梅,余建波.卷积神经网络多变量过程特征学习与故障诊断[J].哈尔滨工业大学学报,2020,52(7):59-67.
[26] 宋宇波,杨慧文,武 威,等.软件定义网络DDoS联合检测系统[J].清华大学学报(自然科学版),2019,59(1):28-35.
[27] 梁 杰,陈嘉豪,张雪芹,等.基于独热编码和卷积神经网络的异常检测[J].清华大学学报(自然科学版),2019,59(7):523-529.
[28] 张婷婷,唐 勇,李云天,等.基于近攻击源部署的应用层DDOS检测方法[J].软件导刊,2022,21(11):104-109.
[29] 黄利军,翟登辉,李瑞生,等.未来多源农村配电网安全与防护技术研究与探讨[J].电力系统保护与控制,2019,47(2):167-174.
[30] 刘志虹,盛万兴,杜松怀,等.基于区域划分的农村有源配电网动态重构方法[J].农业工程学报,2021,37(20):248-255.
[31] 王勤全,朴在林,宋 野,等.基于CP原则的地方电力网络安全防御方法研究[J].沈阳农业大学学报,2009,40(3):373-375.
[32] 周奕涛,张 斌,刘自豪.基于多模态深度神经网络的应用层DDoS攻击检测模型[J].电子学报,2022,50(2):508-512.
[33] 张 伟,李文建,冯 晗,等.浅谈农村配电网规划存在的问题及改进措施[J].农村电气化,2022(6):95-96.
[34] 林 峰,梅 勇,朱益华,等.网络攻击对电力系统典型场景全过程影响综述[J].南方电网技术,2023,17(11):61-75.

[责任编辑 马迎杰]