**融合位置信息的恶意流量识别方法**

**摘要：**针对现有网络流量入侵检测中模型鲁棒性不足、特征选择不稳定以及数据噪声干扰显著等问题，本文提出了一种融合位置信息的异常检测方法。首先，通过滑动窗口方法对流量数据进行分片处理，分别构建网络流量的时序特征和相应的标签序列；随后，采用本文提出的，融合位置信息的频谱生成方法SSPE，对标签序列进行转换，生成频谱标签，用以捕捉和表征攻击的行为模式；最后，使用时序特征和频谱标签训练模型，并通过模型识别入侵行为和攻击类型。实验结果表明，采用SSPE方法训练的XGBoost模型在二分类任务中的准确率达到96.3%，相比传统方法提升了4.8%，在多分类任务中，在90%噪声比例的情况下仍保持了84%的准确率，显著优于基准方法。

**关键词：**网络流量异常检测；滑动窗口；标签频谱分析；离散二值化；相似度度量

网络环境的日益复杂和攻击形式的不断演变，使得网络异常检测技术面临巨大的挑战。传统异常检测方法在处理复杂网络流量时[1][2]，难以有效提取和捕捉动态特征，进而影响检测的可靠性。此外，网络流量中的噪声干扰普遍存在，这使得模型在实际应用中的鲁棒性较差，容易受到干扰，导致检测结果不稳定。面对新型威胁和不断变化的攻击手段，传统技术在适应性方面存在不足，限制了其在多变网络环境中的应用效果。

目前，基于机器学习的网络流量异常检测方法[3][4]因其在复杂特征提取方面的优势而受到广泛关注。然而，现有方法在面对动态的网络流量特征和不稳定的数据环境时仍显不足，主要存在以下两个问题：问题一：对时序特征的捕捉能力有限。尽管深度学习模型在特征提取方面展现了卓越的能力，但在处理网络流量的时序特性时仍面临较大挑战，尤其是在长时间序列数据中，难以有效捕捉全局和局部的时序依赖性，导致检测精度下降。问题二：模型的鲁棒性不足。现有模型在面对噪声数据时表现出鲁棒性不足，容易受到噪声干扰，降低异常检测的准确性。这主要是由于特征的不稳定性和随机噪声未得到有效处理导致的。

针对以上两个问题，本文提出了一种融合位置信息的恶意流量识别方法。对于问题一，使用滑动窗口对网络流量进行分片，构造时序特征，在保留流量时序信息的同时，捕捉网络流量中的全局和局部时序特征。对于问题二，使用SSPE算法融合原始标签信息和位置信息，构造频谱标签，将原始离散的二值标签转换为连续的频谱标签，增强模型的抗噪性。具体来说，先采用正弦位置编码对数据包的位置信息进行编码，然后以位置编码为权重，对原始标签进行加权求和运算得到频谱值。通过SSPE生成的频谱标签融合了数据包的位置信息和原始的攻击信息，增强了模型对噪声数据的抗扰能力，从而提升了异常检测的鲁棒性。

本文的贡献主要有以下四点：

1. 提出了SSPE算法，对原始的离散标签序列进行转换，构造出连续的频谱标签，频谱标签融合位置信息，提升标签的表达能力。
2. 使用滑动窗口，对原始流量进行转换，构造出时序特征，保留了流量中的时间信息，提升了特征的表达能力。
3. 使用构造出的时序特征和频谱标签训练模型，通过模型预测的频谱值分布识别攻击行为，提升了模型鲁棒性。
4. 实验表明，在Edge-IIoTset数据集[5]上，采用SSPE方法训练的模型有更好的鲁棒性，如XGBoost模型在二分类任务中的准确率达到96.3%，比传统方法提升了4.8%，并且在90%噪声比例下仍保持了84%的准确率，显著优于基准方法。
5. **文献综述**

在早期研究中，Gupta等人[6]提出了一种基于树分类器的网络入侵检测模型，专注于物联网中的安全问题，并验证了该方法在物联网环境下的有效性。Ma等人[7]结合支持向量机与聚类方法，通过对流量特征进行分类，提高了在复杂网络环境中检测异常的能力。基于特征选择的机器学习方法依照预设规则选取对流量重要性较高的特征，形成最优特征子集，从而降低数据维度和计算成本。接着，通过机器学习算法训练分类器，实现检测和分类的目的。

然而，传统的机器学习方法往往忽略特征之间的相互关系，仅选择与网络流量最相关的部分特征。由于网络数据流量庞大且结构复杂，机器学习方法的处理能力有限，导致误报和漏报情况较为严重。随着攻击类型的复杂化，传统机器学习方法在处理高维数据和多样化攻击模式时表现出一定的局限性，在应对新兴的复杂网络环境时其表现力逐渐不足，难以取得稳定的检测效果[8]。

目前，深度学习方法逐渐成为网络流量分析的主流手段。Wang等人[9]提出了一种结合生成对抗网络（Generative Adversarial Network, GAN）与Transformer的模型，以提高对复杂网络流量中恶意行为的识别精度。Jung等人[10]则基于深度学习方法，使用自编码器（Autoencoder）来捕捉数据中的连续与非连续模式，并通过重构误差检测异常行为，从而能够有效处理大规模网络流量。Zamanzadeh等人[11]指出，深度学习方法通过捕捉时间和空间特征，有效识别复杂的时间序列异常，显著提升了异常检测的准确性与鲁棒性。

此外，Feng等人[12]通过卷积神经网络（Convolutional Neural Network, CNN）进行VPN流量分类，解决了传统方法在应对加密和伪装流量时的低效问题。通过CNN对原始流量数据进行特征提取，提升了加密网络流量的分类精度，尤其在真实网络环境中取得了更高的识别准确率。相比之下，长短期记忆网络（Long Short-Term Memory, LSTM）的显著特点在于其输出不仅依赖当前输入，还与前一时刻的输入密切相关，这使其更适合处理长距离序列数据。由于流量数据集通常具有时间特性[13]，例如时间戳和持续时间，LSTM在流量分析任务中表现出优异的适应性。Bahe等人[14]基于LSTM对真实网络流量数据进行时间序列预测，研究表明，LSTM在聚合流量预测中表现优异，能够更充分理解特征间的内在关联。

现有文献表明，传统机器学习方法和深度学习方法在网络流量异常检测中各具优势。传统方法如支持向量机和聚类技术在早期阶段取得了显著成效，但在应对高维和复杂流量时表现出一定的局限性[8]。尽管深度学习方法在特征提取和时序建模方面表现优异，但由于其训练过程对数据量和数据质量依赖较大，在处理可能含有噪声的现实应用数据时，模型的稳定性容易受到影响[15][16]。

为提升模型的鲁棒性，可以结合对抗性训练和数据增强等方法[17]，但网络流量数据集通常存在样本分布不均衡的问题，即正常样本多、异常样本少，构建均衡数据集需要较高的时间和人力成本。此外，深度学习方法对计算资源需求较高，其响应速度难以满足实时分析的要求。

深度学习技术在捕捉复杂特征和时序依赖性方面展现了显著优势，时间序列特征对提升模型的异常流量分析能力起到了关键作用。为了更有效地捕捉异常检测中的时间序列特征，Tang等人[18]提出了一种结合标签神经网络和长短期记忆网络的多网络异常检测架构，通过自学习业务逻辑标签优化了模型的鲁棒性和检测精度。Sørbø等人[19]深入探讨了不同标签生成策略对异常检测结果的影响，强调了标签频谱生成在提升检测效果中的重要性。Pekar等人[20]则提出了一种基于高级流标签生成的网络流量异常检测方法，通过改进数据流标记和频谱分析，使异常检测模型在面对真实世界中的动态流量时具备更强的适应能力

1. 研究方法
2. 总体框架

总体框架如图1所示。框图分为“数据集构造”和“模型训练”两个部分。“数据集构造”是将原始网络报文和标签转换为可以用来训练模型的数据集，“模型训练”是训练回归或分类模型并评估他们的性能。

数据集构造：首先，从PCAP文件中提取网络流量数据，并通过滑动窗口方

法将流量数据划分为多个流量序列和对应标签序列，每个流量序列是一组由网络报文组成的序列，每个标签序列是一组由原始标签组成的序列。然后，通过特征选择和Flatten操作，将二维的流量序列，转换为流量特征；通过SSPE算法将标签序列转换为频谱标签。最后，使用流量特征和频谱标签构造新的数据集，用于后续模型训练。

模型训练：本研究通过两组实验，分别通过训练分类模型和回归模型，来验证SSPE对异常流量的识别效果：首先，对数据集进行了采样，划分为训练集和测试集。然后，对于二分类模型，将频谱标签二值化作为训练标签，训练模型并评估模型的性能；对于回归模型，直接使用频谱标签作为训练标签，通过模型输出的频谱值分布识别攻击行为。

图示, 形状

描述已自动生成

图1 方法总体框架图

* 1. 流量特征构造

流量特征构造包括“缺失时序点填充”、“特征选择”、“流量序列和标签序列生成”和“特征聚合”四个步骤。

缺失时序点填充：为应对原始流量数据中的缺失时序点，采用了插值技术，随机采样正常流量填充缺失的数据点，确保时间序列的连续性。这种填充操作旨在提高时序数据的完整性，从而更好地提取特征。图2展示了填充结果。

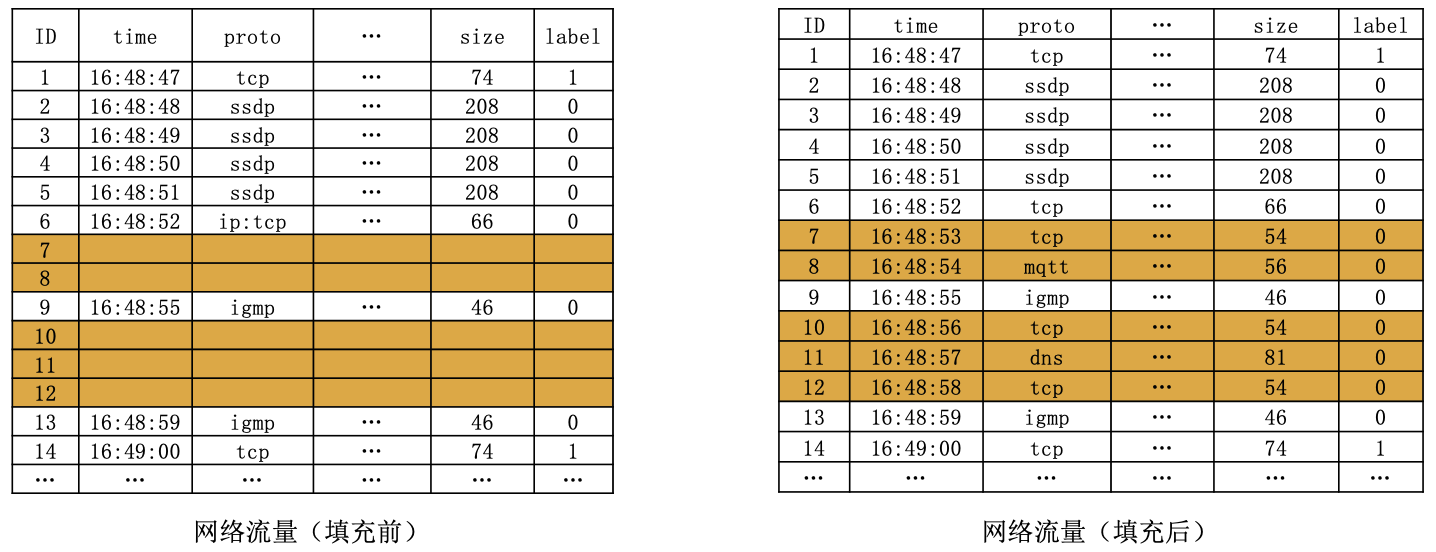


图2 网络流量填充

特征选择：本研究首先对各攻击类型的特征进行筛选，去掉原始包中与攻击无关的内容。表1中为各攻击类型选取的特征数量。

表1 各攻击类型选取的特征数量

|  |  |  |  |
| --- | --- | --- | --- |
| 攻击类型 | 特征数量 | 攻击类型 | 特征数量 |
| 端口扫描攻击 | 37 | 勘察软件攻击 | 40 |
| 漏洞利用 | 56 | DDoS HTTP 洪水攻击 | 48 |
| 密码攻击 | 48 | 后门攻击 | 37 |
| 上传攻击 | 40 | 中间人攻击（ARP欺骗+DNS） | 23 |
| DDoS UDP 洪水攻击 | 9 | SQL注入攻击 | 37 |
| DDoS ICMP 洪水攻击 | 15 | 跨站脚本攻击 | 48 |
| DDoS TCP SYN 洪水攻击 | 32 | 操作系统指纹识别攻击 | 35 |

流量序列和标签序列生成：为保留时序信息，采用滑动窗口的方式将网络流量划分为多个流量序列和标签序列。随着滑动窗口在流量序列上移动，每次移动后，窗口内的特征为一个流量序列、窗口内的标签为标签序列。流量序列和标签序列保留了流量中的时序信息，使得模能更好地捕捉攻击行为的时序特征。图3展示了流量序列和标签序列的生成过程。

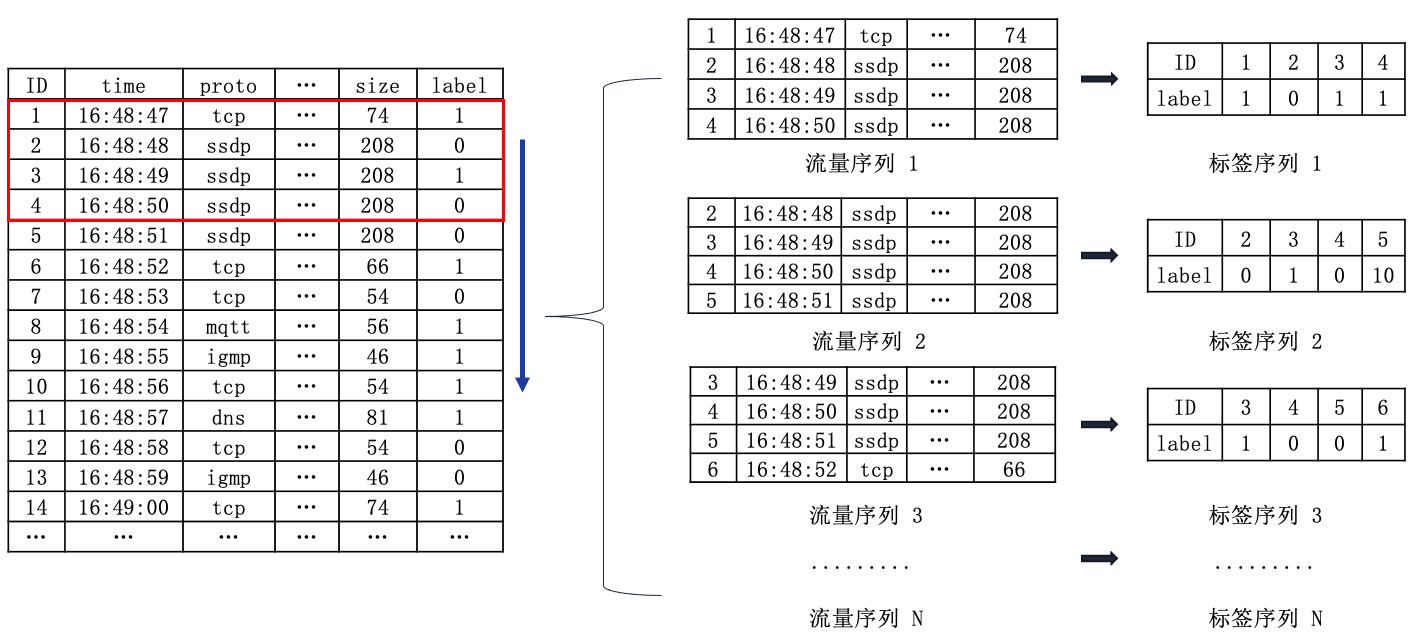


图3 使用滑动窗口生成流量序列和标签序列

特征聚合：采用Flatten Aggregation方法对滑动窗口内的数据进行处理，将滑动窗口内的二维数据展平为一维特征向量，保留流量片段中的全部特征信息，包括协议类型、包大小等。图4展示了特征聚合的过程。

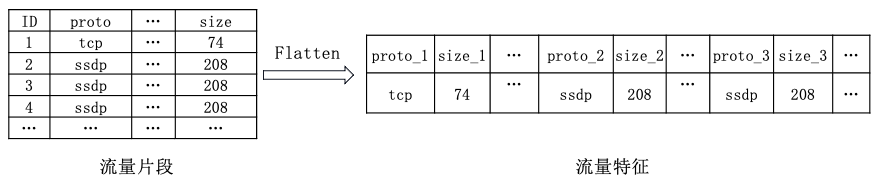


图4 特征聚合

* 1. 频谱标签构造

标签序列为二值时间序列（Binary Time Series），其中0表示正常流量，1表示攻击流量。频谱标签构造是将标签序列转换为一个实数，并将这个实数作为流量片段对应的标签。本研究共采用了两种频谱标签生成方法：COAP（ Count of Attack Packets）方法与SSPE（Sum of Sinusoidal Positional Encoding）方法。

COAP方法：忽略序列中的位置信息，直接统计攻击数据包的数量，COAP能直观地反映攻击强度，适合快速评估攻击频率的场景。计算方法如公式所示。

其中，为标签序列的长度，表示第个包的标签，标签为0代表正常流量，标签为1则代表异常流量，表示频谱标签。



SSPE方法：为了解决COAP方法中存在的位置信息丢失的问题，本研究

参考论文[21]使用的正弦位置编码方法，通过正弦和余弦函数为序列中的位置进行编码，再将位置编码与相应的标签值相乘后求和。由于标签序列为二值时间序列（Binary Time Series），通过乘法运算可以屏蔽掉正常流量（标签值为0）的影响，只保留攻击流量的信息。SSPE能够更精细地描述攻击行为在时序上的变化。计算方法如公式所示。



其中，为标签序列的长度，表示第个包的标签，标签为0代表正常流量，标签为1则代表异常流量，表示频谱标签。



表示第个包的位置编码值，计算方法如公式所示。其中，为超参数表示编码维度，表示维度索引。



* 1. 数据预处理

使用Z-Score对特征值进行标准化处理，计算方法如公式所示。其中是第个样本，第个特征；是第个特征的均值；是第个特征的标准差；是标准化后的第个样本，第个特征。

* 1. 模型训练

分别通过攻击检测和攻击识别来验证SSPE算法的抗噪能力，攻击检测使用二分类模型只识别正常流量或攻击流量，不识别攻击的类型。攻击识别使用回归模型输出攻击频谱，通过攻击频谱的分布识别攻击的类型。

频谱值二值化：构造的频谱标签为连续值，在训练二分类模型前，使用阈值对频谱标签进行二值化处理。处理方法如公式所示，其中，是频谱标签，是设定的阈值（threshold），是二值化后的标签。

攻击频谱识别：通过计算模型输出频谱的分布与真实频谱分布的相似度识别攻击的类别。相似度度量使用余弦相似度[22]，计算公式如下。

其中，其中，为攻击类型，表示模型输出的频谱分布向量，表示样本中、第个攻击类型的频谱分布向量，当表达式取最小值时的类别为攻击类型。



模型选择：本文使用AutoML工具H2O(V3.46.0.4)进行训练，修改部分超参数见表2（未修改部分使用默认值）。

表2 模型与参数

|  |  |  |
| --- | --- | --- |
| 模型类型 | 二分类模型参数 | 回归模型参数 |
| ANN | hidden：[100, 100] | hidden：[100, 100] |
| GBM | ntrees：50 | ntrees：50 |
| GLM | Family：binomial | Family：gaussian |
| RF | ntrees:25  max\_depth:10  sample\_rate:0.5  nbins:5  min\_rows:50 | ntrees:25  max\_depth:10  sample\_rate:0.5  nbins:5  min\_rows:50 |
| xgboost | n\_estimators:100 | n\_estimators:100 |

* 1. 模型评估

在攻击检测任务中，二分类模型输出分类的结果，使用常用的分类指标进行评估，包括准确率（Accuracy）、精确率(Precision)、召回率(Recall)、F1值(F1-score)。在攻击识别任务中，通过相似度进行识别，评价指标为识别的准确率，计算方法如公式所示。

1. 仿真实验
   1. 数据集和评测标准

本研究使用了Edge-IIoTset数据集[5]，这是一个专门为工业物联网（Industrial Internet of Things，IIoT）准备的网络安全数据集。Edge-IIoTset数据集通过使用tcpdump工具捕获网络包生成PCAP文件，随后使用Zeek和TShark等工具进行Session数据生成和特征提取。该数据集包含与IoT和IIoT连接协议相关的14种攻击，分为五大类威胁：拒绝服务（DoS/DDoS）攻击、信息收集、中间人攻击、注入攻击和恶意软件攻击，具体分布见图6。此外，从不同来源（如警报、系统资源、日志、网络流量）中提取了特征，并从1176个特征中筛选出61个高相关性的特征用于实验分析。

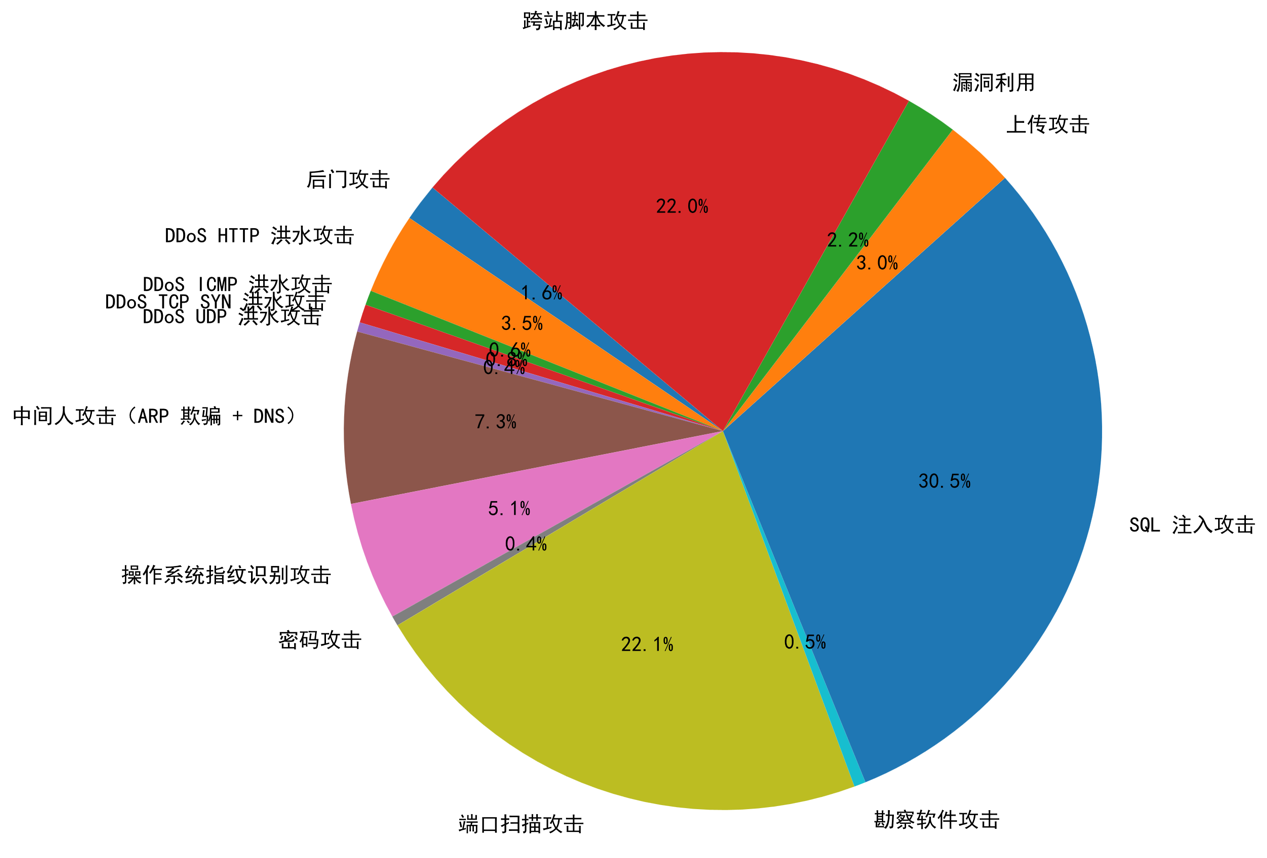


图6 数据集攻击类型分布

3.2 实验方法与基准

本研究在在复现论文[5]实验的基础上，通过向特征值上添加随机噪声的方法，模拟真实的应用场景。评估在不同比例噪声的环境中，使用SSPE/COAP方法带来的抗噪效果。

噪声环境构造：首先，按一定比例随机选择待加噪声的样本，然后，对选中的样本的特征值添加随机噪声。本文分别以0%至100%，10%为增量共11种不同的比例进行加噪声处理，共得到11个带有不同噪声比例的测试集，如表所示。

表3 测试集

|  |  |
| --- | --- |
| 测试集 | 说明 |
| 1 | 无噪声 |
| 2 | 10%样本有噪声 |
| 3 | 20%样本有噪声 |
| … | …. |
| 11 | 100%样本有噪声 |

3.3 实验结果

3.3.1 频谱标签的分布

SSPE和COAP在构造频谱标签时，我们重点研究了滑动窗口大小、正弦位置编码维度对结果的影响。我们分别以不同大小（10,20,30,40,50,60）的滑动窗口，不同大小(2、4、8、16、32、64、128、236、256)的正弦编码维度，进行了多次实验。通过实验发现，选取合适的滑动窗口和正弦编码维度，与COAP相比，使用SSPE生成的频谱具有更多的细节，更接近一个或多个正态分布。本文选择的参数见表5，生成的频谱标签的分布如图所示。

表5 不同攻击类型的最佳位置编码维度和滑动窗口大小

|  |  |  |
| --- | --- | --- |
| 攻击类型 | 位置编码维度 | 滑动窗口大小 |
| Vulnerability scanner attack | 8 | 30 |
| Password attacks | 236 | 30 |
| Uploading attack | 8 | 60 |
| DDoS UDP Flood Attacks | 256 | 30 |
| DDoS ICMP Flood Attacks | 8 | 30 |
| Ransomware attack | 128 | 30 |
| Backdoor\_attack | 256 | 60 |
| MITM (ARP spoofing + DNS) Attack | 128 | 60 |
| SQL injection attack' 'XSS attacks | 128 | 60 |
| OS Fingerprinting attack | 64 | 60 |
| Port Scanning attack | 128 | 60 |
| DDoS TCP SYN Flood Attacks | 64 | 60 |
| DDoS HTTP Flood Attacks | 16 | 60 |
| XSS attacks | 256 | 60 |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

图7 使用COAP和SSPE生成频谱直方图

* + 1. 二分类异常检测结果

在二分类任务中，我们使用了COAP和SSPE两种频谱生成方法，并采用ANN、RF、XGBoost等机器学习模型对异常流量进行检测。对于每种特征生成方法，我们分别评估了模型在准确率、精确率、召回率和F1分数等指标上的表现。实验结果见表3。

表3 分类结果

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 模型 | 准确率 | 精确率 | 召回率 | F1值 |
| 传统方法 | ANN | 82.3% | 76.1% | 73.4% | 0.744 |
| RF | 87.8% | 81.2% | 78.6% | 0.796 |
| XGBoost | 91.5% | 86.3% | 84.7% | 0.853 |
| 传统方法+COAP | ANN | 91.6% | 92.2% | 91.6% | 0.92 |
| RF | 89.3% | 90.4% | 89.2% | 0.898 |
| XGBoost | 95.2% | 93.0% | 92.0% | 0.941 |
| 传统方法+SSPE | ANN | 93.1% | 93.3% | 93.1% | 93.2 |
| RF | 92.1% | 92.8% | 92.2% | 92.5 |
| XGBoost | 96.3% | 94.5% | 93.0% | 91.7 |

从表X中，可以得到以下3点结论：

首先，从整体表现来看，COAP和SSPE频谱生成方法明显优于传统特征生成方法。在传统方法中，XGBoost模型的准确率最高，达到了91.5%，但依然低于COAP和SSPE的结果。COAP结合XGBoost的表现达到95.2%，而SSPE结合XGBoost的表现更为突出，达到了96.3%。这表明基于频谱的特征生成方法能够更有效地捕捉异常流量的特征，尤其是SSPE，得益于其位置编码特征的加入，进一步提升了对时序数据的表达能力。

其次，从模型的对比来看，ANN在采用频谱生成方法时也展现出极佳的性能提升。在COAP和SSPE的频谱生成下，ANN模型的准确率分别达到91.6%和93.1%，相比传统特征生成方法下的82.3%有了显著提升。这说明频谱特征的提取能够更好地适应深度学习框架，通过更有效的特征表达提升其对异常流量的识别能力。

最后，对比COAP和SSPE两种频谱生成方法，SSPE整体表现优于COAP。以XGBoost为例，SSPE的准确率为96.3%，精确率为94.5%，均高于COAP下的95.2%和93.0%。SSPE方法通过结合正弦和余弦位置编码，能够有效保留和利用时序信息，因此在不同模型的应用中均展现出更强的泛化能力和更高的分类性能。此外，SSPE在多个指标上相对于COAP的显著优势表明，其在复杂时序数据的表达和攻击模式的捕捉方面更具优势，是一种更为适合网络异常流量检测的频谱生成方法。

* + 1. 攻击类型识别结果

在攻击类型识别任务中，我们采用SSPE方法生成频谱特征，并通过余弦相似度匹配不同攻击类型的频谱特征，以识别数据集中包含的14种不同攻击类型。传统方法识别攻击类型的平均准确率为79.68%[5]，本文方法实验结果见表4。

表4 攻击类型识别结果

|  |  |
| --- | --- |
| 攻击类型 | 准确率 |
| 后门攻击 | 46.5 |
| DDoS HTTP洪水攻击 | 84.3 |
| DDoS ICMP洪水攻击 | 84.8 |
| DDoS TCP SYN洪水攻击 | 84.7 |
| DDoS UDP洪水攻击 | 73.5 |
| 中间人攻击（ARP欺骗 + DNS） | 84.3 |
| 操作系统指纹识别攻击 | 83.3 |
| 密码攻击 | 85.4 |
| 端口扫描攻击 | 84.5 |
| 勒索软件攻击 | 84.6 |
| SQL注入攻击 | 83.9 |
| 上传攻击 | 75.5 |
| 漏洞利用 | 77.0 |
| 跨站脚本攻击 | 83.5 |

分析表4可知，模型对于大部分攻击具有较强的识别能力。密码攻击的识别精度最高（85.4%），其次是DDoS ICMP洪水攻击（84.8%）、DDoS HTTP洪水攻击（84.3%）和DDoS TCP SYN洪水攻击（84.7%），大部分攻击类型识别准确率均明显优于传统方法。这表明，SSPE结合频谱特征和余弦相似度能够有效捕捉这些攻击的特征。后门攻击的识别效果最差（46.5%），说明其特征更复杂且隐蔽性更强，频谱特征难以充分描述，需要更多特征或增强训练数据以提升分类性能。

1. 验证泛化能力

为了验证融合位置信息后的模型的泛化能力，我们在数据集中随机加入了多种类型和不同程度的噪声，具体来说，对于布尔型特征，随机进行了取反操作；对于整数型特征，添加了正态分布噪声后取整；对于浮点型特征，直接添加正态分布噪声。以二分类模型为例，通过在不同比例的噪声环境下评估模型的准确率变化情况，实验在基准方法中表现最优的XGBoost模型上加入COAP和SSPE进行测试。实验结果见图7。

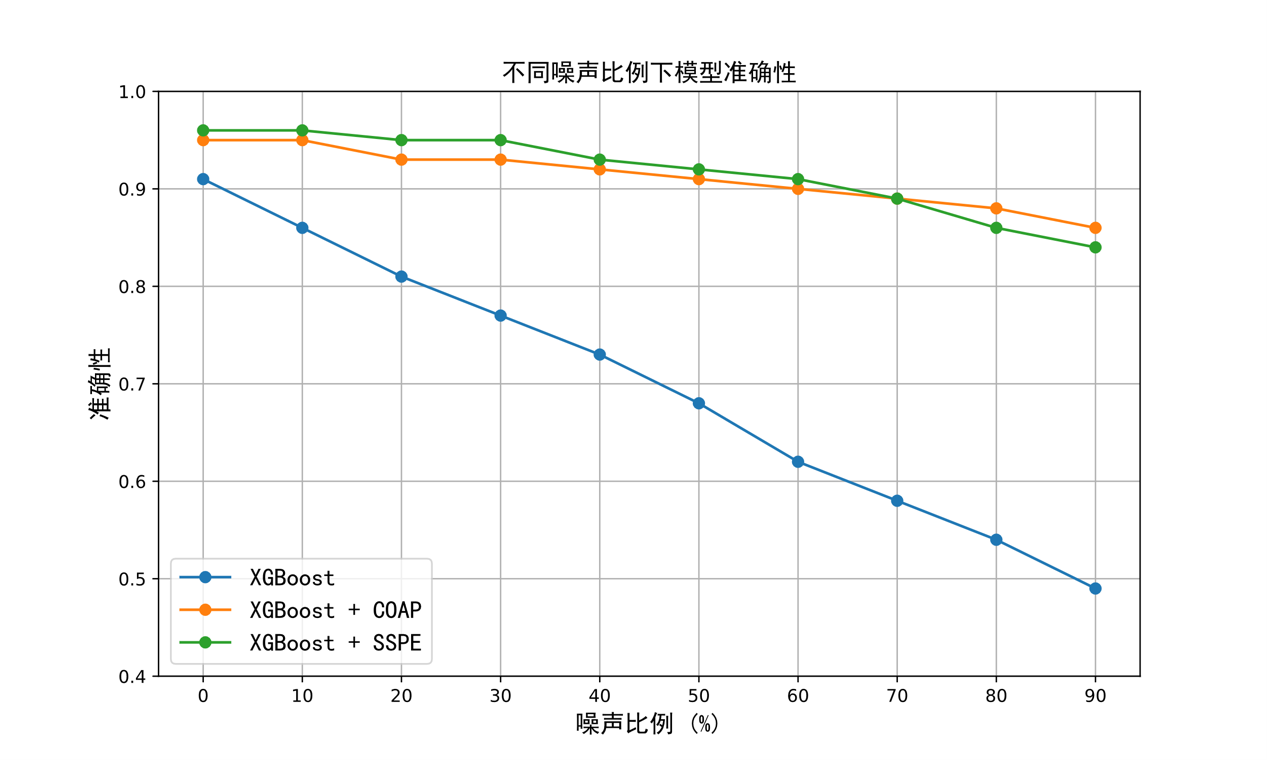


图7 加入不同比例噪声后模型表现

从图7中可以看出，随着噪声比例的增加，所有模型的准确性均逐渐下降。然而，XGBoost结合COAP和SSPE的模型表现明显优于单独使用XGBoost模型，说明频谱特征生成方法能够有效增强模型对噪声的抗扰性。这表明COAP和SSPE特征不仅能够捕捉流量的核心信息，还能在噪声环境中保持较高的特征识别能力。

1. 参数敏感性分析

在参数敏感性分析中，我们重点研究了滑动窗口大小、正弦位置编码维度对模型性能的影响。

滑动窗口的大小从10到60进行了多次实验，每10为增量，探讨不同窗口大小在捕捉时间序列特征上的表现。较小的窗口可以捕捉更多细粒度的信息，但可能导致噪声过多；较大的窗口则可以增强模型的鲁棒性，但有可能忽略重要的细节。

对于正弦位置编码维度，选择了多种维度值进行实验，包括7、8、16、32、64、128、236、256等，以观察不同维度对频谱生成的影响。从实验中发现，SSPE生成的频谱在较高维度时表现出更强的特征表达能力，并且生成的频谱更接近一个或多个正态分布。

具体参数选择见表5。

表5 不同攻击类型的最佳位置编码维度和滑动窗口大小

|  |  |  |
| --- | --- | --- |
| 攻击类型 | 正弦位置编码 | 滑动窗口大小 |
| 漏洞扫描器攻击 | 8 | 30 |
| 密码攻击 | 236 | 30 |
| 文件上传攻击 | 8 | 60 |
| 分布式拒绝服务 (DDoS) UDP 泛洪攻击 | 256 | 30 |
| 分布式拒绝服务 (DDoS) ICMP 泛洪攻击 | 8 | 30 |
| 勒索软件攻击 | 128 | 30 |
| 后门攻击 | 256 | 60 |
| 中间人攻击（ARP 欺骗 + DNS 欺骗） | 128 | 60 |
| SQL 注入攻击 | 128 | 60 |
| 操作系统指纹识别攻击 | 64 | 60 |
| 端口扫描攻击 | 128 | 60 |
| 分布式拒绝服务 (DDoS) TCP SYN 泛洪攻击 | 64 | 60 |
| 分布式拒绝服务 (DDoS) HTTP 泛洪攻击 | 16 | 60 |
| 跨站脚本攻击 (XSS) | 256 | 60 |

1. 结论

本文提出了一种融合位置信息的标签频谱分析方法，旨在解决现有网络流量异常检测中模型鲁棒性不足、特征选择不稳定以及数据噪声干扰显著等问题。通过滑动窗口对流量进行分片处理，提取时序特征并生成标签序列，结合COAP和SSPE频谱生成方法，提升了模型对攻击特征的捕捉能力。实验结果表明，所提方法在二分类和多分类任务中的表现均优于传统机器学习方法，尤其在高噪声环境下具备显著的抗干扰能力，验证了本文方法在复杂网络环境中的有效性和泛化性能。

未来，我们将从以下两个方面进一步推进研究。首先，探索频谱生成方法与深度神经网络的结合，进一步提升对复杂攻击类型的检测能力；其次，其次，针对不同的网络应用场景，如工业物联网、智慧城市等，我们将对模型结构进行优化，选择适合具体场景的数据处理和特征提取策略，同时调整模型参数以降低计算开销，从而提高系统的实时性，增强其对大规模网络数据的处理效率和响应速度。

1. Zhao H, Wang Y, Duan J, et al. Multivariate time-series anomaly detection via graph attention network[C]//2020 IEEE international conference on data mining (ICDM). IEEE, 2020: 841-850.
2. Wang S, Balarezo J F, Kandeepan S, et al. Machine learning in network anomaly detection: A survey[J]. IEEE Access, 2021, 9: 152379-152396.
3. LI H T,WANG R M,DONG W Y,et al.A GRU-based method for semi-supervised network traffic anomaly detection[J].Computer Science,2023,50(3):380-390.
4. 陈向效,崔鑫,杜秦,等.基于机器学习的异常流量检测模型优化研究[J].计算机科学,2024,51(S1):994-998.
5. Ferrag M A, Friha O, Hamouda D, et al. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning[J]. IEEE Access, 2022, 10: 40281-40306.
6. Gupta K, Sharma D K, Gupta K D, et al. A tree classifier based network intrusion detection model for Internet of Medical Things[J]. Computers and Electrical Engineering, 2022, 102: 108158.
7. Ma Q, Sun C, Cui B, et al. A novel model for anomaly detection in network traffic based on kernel support vector machine[J]. Computers & Security, 2021, 104: 102215.
8. 顾伟,行鸿彦,侯天浩.基于网络流量时空特征和自适应加权系数的异常流量检测方法[J].电子与信息学报,2024,46(06):2647-2654.
9. Wang Z, Zhou J, Hei X. Network traffic anomaly detection based on generative adversarial network and transformer[C]//The International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery. Cham: Springer International Publishing, 2022: 228-235.
10. Sharma K, Chaudhary M, Yadav K, et al. Anomaly Detection in Network Traffic using Deep Learning[C]//2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET). IEEE, 2023: 1-5.
11. Zamanzadeh Darban Z, Webb G I, Pan S, et al. Deep learning for time series anomaly detection: A survey[J]. ACM Computing Surveys, 2022.
12. Feng R, Hu T, Jia X. VPN traffic classification based on CNN[C]//2022 14th International Conference on Computer Research and Development (ICCRD). IEEE, 2022: 94-99.
13. Kanna P R, Santhi P. Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features[J]. Knowledge-Based Systems, 2021, 226: 107132.
14. Bahe M, Yamane K D S, Großegesse N, et al. Traffic Prediction of Real Network Traffic Data with LSTM Neural Networks[C]//Future of Information and Communication Conference. Cham: Springer Nature Switzerland, 2024: 311-326.
15. Iqbal A, Amin R, Alsubaei F S, et al. Anomaly detection in multivariate time series data using deep ensemble models[J]. Plos one, 2024, 19(6): e0303890.
16. Pang G, Shen C, Cao L, et al. Deep learning for anomaly detection: A review[J]. ACM computing surveys (CSUR), 2021, 54(2): 1-38.
17. Rasheed B, Masood Khattak A, Khan A, et al. Boosting adversarial training using robust selective data augmentation[J]. International Journal of Computational Intelligence Systems, 2023, 16(1): 89.
18. Tang X, Xu S, Ye H. Labeling expert: A new multi-network anomaly detection architecture based on LNN-RLSTM[J]. Applied Sciences, 2022, 13(1): 581.
19. Sørbø S, Ruocco M. Navigating the metric maze: A taxonomy of evaluation metrics for anomaly detection in time series[J]. Data Mining and Knowledge Discovery, 2024, 38(3): 1027-1068.
20. Pekar A, Jozsa R. Evaluating ML-Based Anomaly Detection Across Datasets of Varied Integrity: A Case Study[J]. arXiv preprint arXiv:2401.16843, 2024.
21. Vaswani A. Attention is all you need[J]. Advances in Neural Information Processing Systems, 2017.
22. de Vos I M A, Boogerd G L, Fennema M D, et al. Comparing in context: Improving cosine similarity measures with a metric tensor[J]. arXiv preprint arXiv:2203.14996, 2022.