研究与开发

基于流量特征重构与映射的物联网DDoS攻击单流检测方法

谢丽霞[1]，袁冰迪[1]，杨宏宇[1,2]，胡泽[2]，成翔[3]，张良[4]

（1. 中国民航大学计算机科学与技术学院，天津 300300；
2. 中国民航大学安全科学与工程学院，天津 300300；
3. 扬州大学信息工程学院，江苏 扬州 225127；
4. 亚利桑那大学信息学院，美国亚利桑那 图森 AZ 85721）

摘　要：针对现有检测方法对物联网（IoT）分布式拒绝服务（DDoS）攻击响应速度慢、特征差异性低、检测性能差等不足，提出了一种基于流量特征重构与映射的单流检测方法（SFDTFRM）。首先，为扩充特征，使用队列按照先入先出存储定长时间跨度内接收的流量，得到队列特征矩阵。其次，针对物联网设备正常通信流量与 DDoS 攻击流量存在相似性的问题，提出一种与基线模型相比更加轻量化的多维重构神经网络模型与一种函数映射方法，改进模型损失函数按照相应索引重构队列定量特征矩阵，并通过函数映射方法转化为映射特征矩阵，增强包括物联网设备正常通信流量与 DDoS 攻击流量在内的不同类型流量之间的差异和同类型流量的相似性。最后，使用文本卷积网络、信息熵计算分别提取映射特征矩阵和队列定性特征矩阵的频率信息，得到拼接向量，丰富单条流量的特征信息并使用机器学习分类器进行 DDoS 攻击流量检测。在两个基准数据集上的实验结果表明，SFDTFRM 能够有效检测不同类型的 DDoS 攻击，检测性能指标平均值与现有方法相比最多提升 12.01%。

关键词：DDoS 攻击检测；多维重构；函数映射；机器学习

中图分类号：TP393

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2024012

A single flow detection enabled method for DDoS attacks in IoT based on traffic feature reconstruction and mapping

XIE Lixia[1], YUAN Bingdi[1], YANG Hongyu[1,2], HU Ze[2], CHENG Xiang[3], ZHANG Liang[4]

1. School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China;
2. School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China;
3. School of Information Engineering, Yangzhou University, Yangzhou 225127, China;
4. School of Information, The University of Arizona, Tucson AZ 85721, USA

Abstract: To address the slow response time of existing detection modules to Internet of things (IoT) distributed de-

收稿日期：2023−09−02；**修回日期：** 2024−01−11

基金项目：国家自然科学基金资助项目（No.62201576, No.U1833107）；中央高校基本科研业务费项目（No.3122022050）；江苏省基础研究计划自然科学基金青年基金项目（No.BK20230558）

Foundation Items: The National Natural Science Foundation of China (No.62201576, No.U1833107), Fundamental Research Funds for the Central Universities (No.3122022050)，Jiangsu Provincial Basic Research Program Natural Science Foundation-Youth Fund Project (No.BK20230558)

nial of service (DDoS) attacks, their low feature differentiation, and poor detection performance, a single flow detection enabled method based on traffic feature reconstruction and mapping (SFDTFRM) was proposed. Firstly, SFDTFRM employed a queue to store previously arrived flow based on the first in, first out rule. Secondly, to address the issue of similarity between normal communication traffic of IoT devices and DDoS attack traffic, a multidimensional reconstruction neural network model more lightweight compared to the baseline model and a function mapping method were proposed. The modified model loss function was utilized to reconstruct the quantitative feature matrix of the queue according to the corresponding index, and transformed into a mapping feature matrix through the function mapping method, enhancing the differences between different types of traffic, including normal communication traffic of IoT devices and DDoS attack traffic. Finally, the frequency information was extracted using a text convolutional network and information entropy calculation and the machine learning classifier was employed for DDoS attack traffic detection. The experimental results on two benchmark datasets show that SFDTFRM can effectively detect different DDoS attacks, and the average metrics value of SFDTFRM is a maximum of 12.01% higher than other existing methods.

Key words: DDoS attacks detection, multidimensional reconstruction, function mapping, machine learning

0　引言

物联网（Internet of things，IoT）设备需要独占公网 IP 地址提供网络服务，这给僵尸网络提供了可利用的网络资源[1]。同时，由于物联网设备存在漏洞和弱密码问题，攻陷物联网设备的难度低于其他类型联网设备[2]。此外，物联网的供应链长、碎片化严重，部分物联网厂商不具备完善的安全能力，上述因素导致物联网设备安全性较低。

2020 年 1 月初，我国在物联网家用设备中首次检测到以流量劫持为主要攻击手段的僵尸网络木马家族——Pink，该家族通过计算机数控（computer numerical control，CNC）模式集中分发具有高及时性要求的指令，可发起分布式拒绝服务（distributed denial of service，DDoS）攻击[3]。而 DDoS 攻击作为网络安全的主要威胁之一，近年来呈现出持续增长的态势，给网络安全带来巨大挑战[4]。2022 年，DDoS 攻击峰值创下新高，达到历年之最[5]。

物联网设备的低安全性使其容易被组织成僵尸网络来发起 DDoS 攻击，并且对于攻击者来说该方法成本更低，带来的不利影响更加显著，如何有效检测出物联网环境中的 DDoS 攻击是目前的研究热点之一。

网络流量是源用户和目标用户通信状态信息的载体，可通过网络流量信息区分正常和攻击行为，但物联网设备正常通信流量与 DDoS 攻击发生时的网络流量存在相似性[6]，因此难以通过单条流量特征对 DDoS 攻击进行高效检测。DDoS 攻击具有周期性和频率性[7]特征，可用以区分正常行为和攻击行为，但通过聚合多条流量提取频率信息，通常仅能检测时间窗口内的攻击事件，无法检测出具体 DDoS 攻击流量。

定量特征表示流量的数值信息，如平均速率、数据包字段长度等。流量的定量特征是源 IP 地址和目标 IP 地址之间通信状态的数值体现，可以作为 DDoS 攻击和正常流量的划分依据，但只能体现 DDoS 攻击的部分特性，除此之外，DDoS 攻击还具有周期和频率性，这些特征无法通过单条流量进行提取。流量的定性特征表示流量属性而非数值信息，如源 IP 地址、目的端口号和传输协议等，但单条流量的定性特征无法用于检测，因此需要通过聚合多条流量进一步对定性特征集合进行统计分析提取信息作为补充特征，同时提取流量集合中蕴含的频率和周期信息。

针对上述问题，本文提出一种基于流量特征重构与映射的单流检测方法（single flow detection enabled method with traffic feature reconstruction and mapping，SFDTFRM）。SFDTFRM 的网络流量多层次特征提取方法利用定量特征和定性特征更加全面地提取反映攻击行为的特征。为使得定性特征能够用于检测，SFDTFRM 提取了定性特征矩阵进行统计分析获得数值作为补充特征。此外，SFDTFRM 提取了定量特征矩阵，在后续特征工程中通过深度学习技术深入挖掘潜在的特征，能够扩充单条流量特征。SFDTFRM 的多维重构和函数映射方法可以增强不同类型流量之间的差异和相同类型流量的相似度，因此该方法能够解决物联网设备正常通信流量与 DDoS 攻击流量相似带来的特征差异性低、检测性能差的问题，可有效检测单条流量是否异常及其攻击类型并快速提供检测结果。

本文的主要工作如下。

- 提出一种网络流量多层次特征提取方法，根据 DDoS 攻击的频率性和周期性，使队列动态地按照先入先出规则存储定长时间跨度内接收的流量，通过队列聚合流量提取深层特征信息。为丰富单条流量特征信息，提取队列中包括定量、定性和频率在内的多层次网络流量特征并使用队列整体信息代表当前待检测流量，能够扩充特征提高检测性能以及完成单条流量的检测。
- 提出一种特征差异增强方法，通过搭建多维重构网络并引入双曲正切函数的导函数进行特征差异增强。多维重构网络模型训练的优化方向为能够正确重构不同类型流量数据，通过改进的均方误差作为损失函数来评估模型重构输出与预期输出的差距。计算预训练模型重构输出与模型输入的向量差值并将差值作为流量特征引入双曲正切函数的导函数进行函数映射，能够在增强相同类型流量相似性的同时保留不同类型流量的区分度。
- 提出一种 DDoS 攻击流量检测方法，为提高检测方法性能，根据特征矩阵每行向量代表一条流量的特点，将定量特征矩阵视为每行均为一个词向量的文本，通过文本卷积网络提取整体特征；通过信息熵统计定性特征值在矩阵中出现的概率，信息熵将作为补充特征与定量特征频率信息共同作为当前待检测流量的特征表示，并使用机器学习分类器进行 DDoS 攻击检测。

1 相关工作

目前物联网 DDoS 攻击检测方法主要包括基于特征的检测方法和基于异常的检测方法。

1.1 基于特征的检测方法

基于特征的检测方法刻画已知攻击行为特征，将检测流量与特征进行匹配，可检测出已知攻击。Ahmed 等[8]提出一种面向网络应用程序的 DDoS 攻击检测方法。该方法应用基于直方图的加权平均算法以及信息熵，得到应用程序的指纹特征，正常应用程序与恶意程序流量的指纹特征在三维空间分布中交叠程度低，但该方法只能检测出已知应用程序产生的 DDoS 攻击流量。Doshi 等[6]提出的物联网 DDoS 攻击检测方法提取网络流量特性，如数据包长度、数据包时间间隔和协议；同时提取物联网特定的网络行为特征作为补充特征，但这些特征在正常和 DDoS 攻击流量间的差异很微小，而该方法未进行特征衍生。Das 等[9]提出基于特征选择的 DDoS 攻击检测框架，使用多数投票技术整合 7 种特征选择方法，提取特征的组合子集用于分类，但该方法的检测性能依赖于选取的既定特征，不能有效检测未知 DDoS 攻击。

1.2 基于异常的检测方法

基于异常的检测方法通过定义正常行为来检

测新的攻击[10]。由于 DDoS 攻击的周期性和频率性不可避免[7,11]，可通过流量集合的聚合状态提取统计特征[12-13]作为检测依据，通常需要设定阈值，这类方法[14-16]对于资源受限的物联网设备来说具有轻量和时效优势，但阈值的大小对检测效果具有决定性作用。物联网设备通信节点数量有限，目的 IP 地址集很少随时间变化[6,17]，这使得物联网设备正常状态下的网络流量与被组织成僵尸网络时产生的 DDoS 攻击流量非常相似，因此基于机器学习和深度学习的方法[18-20]可应用于 DDoS 攻击检测，利用微小差异提取深层信息[21-22]。Torabi 等[23]提出一种基于堆叠自编码器的 DDoS 攻击检测方法，为每个自编码器设置阈值，但需选取合适的阈值且内存开销较大，不适合部署在资源受限的物联网设备端。Orman 等[24]将长短期记忆网络作为检测模型，仅考虑与时间相关的序列关系，忽略了网络流量特征。Akgun 等[25]提出一种基于深度学习的 DDoS 攻击检测方法，利用信息增益属性评估方法降低特征维度，基于原始特征使用具有不同大小卷积核的深层卷积网络执行检测，未进行特征衍生。Jalili 等[26]提出一种 DDoS 攻击三阶段检测和防御机制，部署在用户端、服务器端和受害者端，通过用户评分机制来检测恶意用户，但该方法是基于用户的，只能判断是否为恶意用户，不能判断流量是否为 DDoS 攻击流量。

结合基于特征与基于异常的检测方法，本文提出一种基于流量特征重构与映射的单流检测方法，该方法通过神经网络模型和机器学习模型刻画正常行为与已知的不同类型 DDoS 攻击行为，可检测出新的攻击以及攻击类型。该方法包含队列结构，能够对单条流量进行检测；该方法充分进行特征构造与衍生，通过多维重构和函数映射增强相同类型流量的相似性同时保留不同类型流量的区分度，能够扩充特征，丰富单条流量的特征信息，提升检测效果。

2　检测框架

在目前的主流检测方法中，通过采集多条流量提取更丰富的特征信息提升检测效果，但往往只能检测采集的流量集合中是否出现攻击事件，无法判断具体由哪些流量引起攻击。随着网络规模的日益壮大，由物联网僵尸网络发起的 DDoS 攻击具有更强的破坏性，这就要求检测方法能快速检测。

已有文献探究了网络带宽负载可以用来表征物联网设备的网络流量模式，Doshi 等[6]按源设备划分网络流量，并计算了 10 s 时间窗口内的平均带宽，以测量与每个设备相关的瞬时带宽并分析了正常流量和攻击流量之间的带宽负载在 10 s 时间窗口内的变化趋势，显示正常流量和物联网 DDoS 攻击流量之间的带宽负载存在微小的分布差异。除此之外，物联网设备的特点之一是与之通信的端点数量有限[6]，例如，WeMo 智能交换机仅与 4 个端点通信，用于从云中激活、禁用、检索固件更新和记录其状态。物联网设备流量的另一个关键特征是，物联网设备流量的目标 IP 地址集很少随时间变化[17]，因为大多数物联网设备只需要向固定服务器提供数据和接收指令，因此物联网设备正常状态下的流量目标 IP 地址相对固定。而物联网 DDoS 攻击事件中，大量恶意主机或僵尸网络对目标受害者服务器发送请求，导致服务器充斥大量要求回复的信息，消耗网络带宽或系统资源导致服务器无法正常提供服务，在这种资源消耗型 DDoS 攻击中，物联网设备产生的网络流量中数据包的目标 IP 地址、目标端口等就不再是随机分布，而是相对固定的值。因此，当物联网设备由于低安全性被组织成僵尸网络发起 DDoS 攻击时，其正常流量和攻击流量表现形式的抽象状态为：源和目标 IP 地址等特征值相对集中，不是无规律的杂乱分布。

因此，本文基于流量特征重构与映射方法，

提出一种可增强流量差异、检测单条流量的异常检测方法。SFDTFRM 检测框架如图 1 所示，包括队列结构和单流检测两部分，其中，单流检测包括自编码器、多维重构与函数映射、文本卷积网络、信息熵计算和队列信息编码 5 个部分。

该方法框架可用于检测物联网设备端产生的通信流量是否异常，继而从源头检测 DDoS 攻击，有利于防范安全风险。流量的采样位置为物联网设备或物联网网关，流量采样数据为数据包格式，经过 CICFlowMeter 工具处理之后，生成 flow（数据流），该方法在 flow 形式的流量基础上进行特征构造与检测，最终可检测出单条 flow 是否为 DDoS 攻击流量。

为分析本文方法框架的优势，选取了现有研究中的 7 种框架与之进行对比，分别从特征选取完整性、特征衍生充分性、单流检测能力和物联网场景适用性几个方面描述 8 种对比方法框架的主要差异，对比结果见表 1。

由表 1 可见，在本文方法框架中，首先，通过队列结构获得流量的定性特征矩阵和定量特征矩阵，特征提取完整，能够扩充单条流量特征。其次，为增强物联网设备正常通信流量、不同类型 DDoS 攻击流量之间的差异，在方法框架中依次通过自编码器、多维重构编码器进行特征构造，计算得到重构误差特征和多维重构误差特征；在增强流量差异性的基础上，为

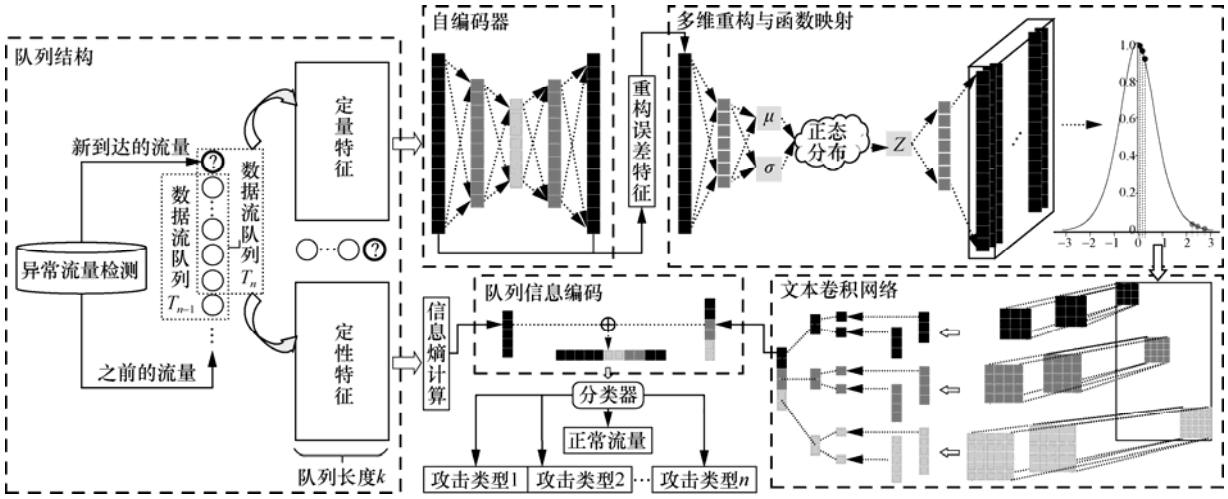

图 1 SFDTFRM 检测框架

表 1 方法框架主要差异对比结果

方法框架	定性特征	定量特征	特征衍生	单流检测	轻量化
SAF[8]	×	√	√	×	√
CIOT[6]	√	√	×	√	×
TETFS[9]	×	√	×	√	×
UVRE[23]	×	√	√	√	×
LSTM[24]	×	√	×	√	×
NDL[25]	×	√	×	√	×
RAD[26]	√	√	√	×	×
SFDTFRM	√	√	√	√	√

增强同一类型流量之间的相似性，在方法框架中通过双曲正切函数的导函数进行特征映射，得到映射特征，该特征在不同类型流量之间表现差异性同时在相同类型流量之间具有相似性。在本文方法框架中，上述充分的特征构造与衍生处理能够提升检测效果。除此之外，多维重构编码器的设计理念为简化模型使其更适用于部署在资源受限的物联网场景，同时保留差异化不同类型流量的功能，因此本文方法框架具有轻量化优势。最后，使用文本卷积网络将定量特征矩阵转化为一维向量作为待检测流量的特征表示，并通过计算定量特征信息熵提取频率信息作为待检测流量的补充特征，使用机器学习分类器进行检测，能够以高性能检测出单条流量是否异常。

2.1　队列结构

队列结构规则为先入先出，用以按时间顺序收集固定数量的流量，便于提取深层特征信息。固定队列长度为 k，新的流量到达时，将其加入队尾，队首流量出队，队列积累流量过程示意图如图 2 所示。

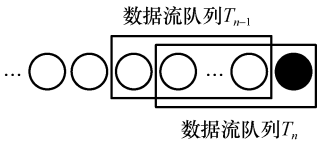

图 2　队列积累流量过程示意图

由队列生成的流量特征矩阵包括定性特征和定量特征两部分，分别用 Qt 和 Ql 表示，提取队列特征示意图如图 3 所示。定性特征是表示流量属性而非数值信息的特征，如源 IP 地址、目的端口号和传输协议等，定量特征表示流量的数值信息，如平均速率、数据包字段长度等。流量的定量特征是源 IP 地址和目标 IP 地址之间通信状态的数值体现，可以作为 DDoS 攻击和正常流量的划分依据，但只能体现 DDoS 攻击的部分特性，除此之外，DDoS 攻击还具有频率性。

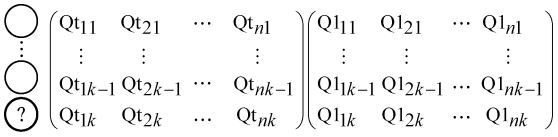

图 3　提取队列特征示意图

通过队列结构，不仅可以获得单条流量的通信状态特征信息，还可以捕获与时间相关的频率信息。

由队列获取到定性特征矩阵和定量特征矩阵是检测工作的基础。相比单条流量，借助队列提取到的矩阵信息更为丰富。

2.2　单流检测

单流检测包括自编码器、多维重构与函数映射、文本卷积网络、信息熵计算和队列信息编码 5 个部分，可将提取到的定性和定量特征矩阵转化为特征向量，便于分类器执行检测。

针对单条流量的定量特征数值表示，通过“自编码器”“多维重构与函数映射”等部分将定量特征转化为新的数值结果，增强不同类型流量的区分度和同一类型流量的相似性。针对单条流量的定性特征，根据每个定性特征值在矩阵中出现的概率来计算各定性特征的信息熵值作为补充特征。

首先，获取待检测流量的定量特征，经过“自编码器”和“多维重构与函数映射”处理，转化为一维特征向量，将其加入定量特征矩阵。定量特征矩阵更新后，每一行数据均为转化后的特征向量。更新后的定量特征矩阵将作为文本卷积网络的输入，经过卷积、池化转化为一维特征向量。其次，经过信息熵计算，得到定性特征矩阵的一维特征向量。最后，在“队列信息编码”部分拼接定性特征和定量特征一维特征向量，将其作为当前待检测流量最终的特征表示，输入机器学习分类器，检测其是否为 DDoS 攻击流量以及攻击类型。

3　自编码器和重构误差特征

如前文所述，获得待检测流量的定量特征后，

首先通过自编码器获得重构误差特征，增强正常流量和攻击流量之间的差异，区别于文献[23]中定义的单个数值重构误差，本文将重构误差定义为向量，可减少向量压缩为单个数值时的信息损失。

自编码器（auto-encoder，AE）模型在训练后可以学习到一种映射关系，记为：$f_\theta: x \to x$。自编码器可以将输入数据 x 编码为隐向量 $\mathbf{z}$，并通过解码器重构出 x，解码器的输出 x^r 能够以较小误差近似恢复出原来的输入，即 $x^r \approx x$。自编码器的优化目标（或损失函数）可表示为：

$$\text{Mnimizer} = \text{dist}(x, x^r) \tag{1}$$

$$x^r = f_\theta(x) \tag{2}$$

其中，$\text{dist}(x,x^r)$表示 x 和 x^r 的距离度量，通常使用均方误差，计算式如下。

$$\text{dist}(x, x^r) = \sqrt{\sum (x_i - x_i^r)^2} \tag{3}$$

综上，AE 模型在训练之后，能够以较小误差还原输入数据 x，将模型输出记为 x^r，假设将输入数据 x 和输出数据 x^r 之间的重构误差记为向量 **Er**，按式（4）～式（5）计算。

$$\mathbf{Er} = \left| x^r - x \right| \tag{4}$$

$$\left| X \right| = \left(\left| X_1 \right|, \left| X_2 \right|, \cdots, \left| X_n \right| \right) \tag{5}$$

其中，**Er** 近似零向量：$\mathbf{Er} \approx \mathbf{0}$。

仅将正常流量数据作为 AE 模型的训练数据，学习到映射关系 f_θ，将正常流量数据记为 x，攻击流量数据记为 x_a，通过训练好的 AE 模型可得到二者的重构输出，分别表示为 x^r、$x_a{}^r$，按照式（6）和式（7）计算，重构误差 **Er** 可表示为：

$$\mathbf{Er}(x) = \left| x^r - x \right| \approx \mathbf{0} \tag{6}$$

$$\mathbf{Er}(x_a) = \left| x_a^r - x_a \right| \ncong \mathbf{0} \tag{7}$$

将正常流量作为训练数据使 AE 模型能够以较小误差重构正常流量，因此，正常流量的 **Er** 较小，相应地，攻击流量的 **Er** 较大。因此，使用重构误差 **Er** 作为流量的特征表示可以达到放大攻击流量和正常流量差异的效果。

4 多维重构与函数映射

4.1 方法概述

在对定量特征矩阵进行卷积运算以提取频率特征之前，期望矩阵中单条流量的特征在正常流量和不同类型的攻击流量之间表现出更高的区分度，从而提升分类性能。为实现上述目标，本文提出“多维重构”与“函数映射”。

首先，将待检测流量的重构误差特征作为多维重构编码器的输入数据，计算多维重构编码器的输出与输入数据的“差值”，得到多维重构误差特征。其次，将多维重构误差特征作为双曲正切函数导函数的输入，得到映射后的双曲正切多维重构误差特征。最后，添加映射后的特征到定量特征矩阵中（先前到达的流量数据已被映射）。

4.2 多维重构编码器

如前文所述，仅将正常流量作为自编码器的训练数据得到的重构误差能够差异化正常流量和 DDoS 攻击流量。同样地，使用 K 种类型的流量训练 K 个自编码器，得到的 K 个重构误差能够差异化 K 种不同类型的流量[18]。为简化模型使其更适用于部署在资源受限的物联网设备端，同时保留差异化 K 种不同类型流量的功能，本文设计了一个多维重构编码器（multidimensional reconstruction encoder，MrE）。

多维重构编码器能够根据训练数据的类型，从相应索引位置重构输入数据，编码器的输出数据与输入数据的“差值”，即多维重构误差能够在不同类型流量之间体现差异性，检测效果得以提升。多维重构编码器按照有监督神经网络模型框架设计，使用反向传播算法更新梯度。其中，输入和输出数据维度由特征维度和样本类型数目决定。

MrE 模型由两个子网络构成。

首先，第一个子网络依据高维度的输入数据 x，生成低维度隐向量 $\boldsymbol{z}$ 的变分概率分布，由均值 μ 和均方差 σ 表示。

其次，依据正态高斯分布采样隐向量 $\boldsymbol{z}$。

最后，另一个子网络将隐向量 $\boldsymbol{z}$ 解码为多维度的 x^M（其维度为样本类型数目 K）。

MrE 模型结构如图 4 所示。

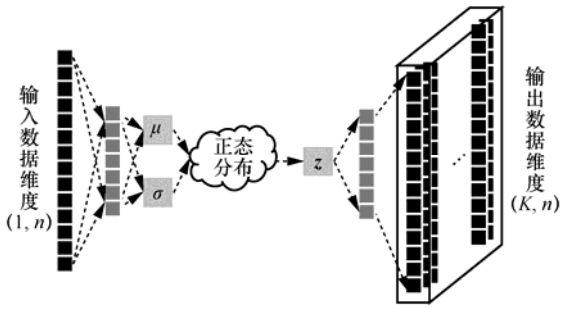

图 4　MrE 模型结构

在流量样本类型数为 K 的情况下，假设模型输入数据 x 的维度是$(1, n)$，模型输出数据 $\boldsymbol{x}^M$ 的维度是(K, n)，输出数据 $\boldsymbol{x}^M$ 用矩阵表示如下。

$$\boldsymbol{x}^M=\begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{K1} & \cdots & x_{Kn} \end{pmatrix}_{K\times n} \tag{8}$$

按式（9）和式（10）定义 MrE 模型的优化目标：

$$\text{Minimizer}=\text{dist}(x,x_i^M) \tag{9}$$

$$\text{label}(x)=i, i\in\{1,2,\cdots,K\} \tag{10}$$

其中，label(x)是类别标签，dist(x,x_i^M)表示 x 和 x_i^M 的距离度量，通常使用均方误差，按式（11）计算：

$$\text{dist}(x,x_i^M)=\sqrt{\sum(x_j-x_{ij}^M)^2} \tag{11}$$

对于输入数据 x，label(x)=i，$\boldsymbol{x}^M$ 的行向量 $\boldsymbol{x}_i^M$ 能够以较小误差重构 x。将 x 和 x_i^M 之间的重构误差记为 **Er**，计算方法如下。

$$\mathbf{Er}=\left|x_i^M-x\right| \tag{12}$$

$$|\alpha|=\left(|\alpha_1|,|\alpha_2|,\cdots,|\alpha_n|\right) \tag{13}$$

则 **Er** 近似零向量：**Er**≈**0**。

在模型训练阶段，将 K 类流量数据作为 MrE 模型的训练数据，将训练后模型的映射关系记为 f_θ^M，将流量数据记为 x^i，i=label(x^i)，通过训练好的 MrE 模型可得到多维重构输出，表示为 $f_\theta^M(x^i)=x^{iM}$，按式（14）定义矩阵 $\boldsymbol{X}^i$：

$$\boldsymbol{X}^i=\begin{pmatrix} x_1^i\,x_2^i & \cdots & x_n^i \\ \vdots\ \vdots & & \vdots \\ x_1^i\,x_2^i & \cdots & x_n^i \end{pmatrix}_{K\times n} \tag{14}$$

由式（12）和式（14）可知，利用多维重构编码器的输出矩阵可得到多维重构误差矩阵 $\mathbf{MEr}^i$，表示为：

$$\mathbf{MEr}^i=\begin{pmatrix} \left|\boldsymbol{x}_1^{iM}-X_1^i\right| \\ \vdots \\ \left|\boldsymbol{x}_i^{iM}-X_i^i\right| \\ \vdots \\ \left|\boldsymbol{x}_j^{iM}-X_j^i\right| \\ \vdots \\ \left|\boldsymbol{x}_K^{iM}-X_K^i\right| \end{pmatrix}_{K\times n} \tag{15}$$

由式（14）和式（15）可知，不同类型的输入数据 $x, x\in\{x^1,\cdots,x^i,\cdots,x^j,\cdots,x^K\}$ 的多维重构误差的近似表示为式（16）。

$$\mathbf{MEr}^1\approx\begin{pmatrix} \mathbf{0} \\ \vdots \\ \left|\boldsymbol{x}_i^{1M}-X_i^1\right| \\ \vdots \\ \left|\boldsymbol{x}_j^{1M}-X_j^1\right| \\ \vdots \\ \left|\boldsymbol{x}_K^{1M}-X_K^1\right| \end{pmatrix}\mathbf{MEr}^i\approx\begin{pmatrix} \left|\boldsymbol{x}_1^{iM}-X_1^i\right| \\ \vdots \\ \mathbf{0} \\ \vdots \\ \left|\boldsymbol{x}_j^{iM}-X_j^i\right| \\ \vdots \\ \left|\boldsymbol{x}_K^{iM}-X_K^i\right| \end{pmatrix}\mathbf{MEr}^j\approx\begin{pmatrix} \left|\boldsymbol{x}_1^{jM}-X_1^j\right| \\ \vdots \\ \left|\boldsymbol{x}_i^{jM}-X_i^j\right| \\ \vdots \\ \mathbf{0} \\ \vdots \\ \left|\boldsymbol{x}_K^{jM}-X_K^j\right| \end{pmatrix}\mathbf{MEr}^K\approx\begin{pmatrix} \left|\boldsymbol{x}_1^{KM}-X_1^K\right| \\ \vdots \\ \left|\boldsymbol{x}_i^{KM}-X_i^K\right| \\ \vdots \\ \left|\boldsymbol{x}_j^{KM}-X_j^K\right| \\ \vdots \\ \mathbf{0} \end{pmatrix} \tag{16}$$

将类别标签为 i 的输入数据 x^i 与 MrE 模型输出矩阵 $\boldsymbol{x}^{iM}$ 的行向量 $\boldsymbol{x}_i^{iM}$ 之间的重构误差作为损失函数参与目标优化，可以使 MrE 模型学习到：模型输出矩阵 $\boldsymbol{x}^{iM}$ 的行向量 $\boldsymbol{x}_i^{iM}$ 能够以较小误差重构输入数据 x^i。相应地，模型输出矩阵 $\boldsymbol{x}^{iM}$ 的其余行向量与输入数据 x^i 的重构误差较大，多维重构误差 $\mathbf{MEr}^i$ 在不同类型流量之间呈现差异性。利用搭建的 MrE 模型得到多维重构误差 $\mathbf{MEr}^i$，并将其作为类别标签为 i 的流量的特征表示，是增强不同类型流量差异的基础。

4.3 函数映射

函数映射包括相似度分析和映射函数两部分。相似度分析旨在分析相同类型流量的多维重构误差特征相似度低的问题以及多维重构误差数值特点，然后依据数值特点选取合适的函数对多维重构误差执行映射操作，提高相同类型流量特征相似性，同时保留不同类型流量特征差异性。

（1）相似度分析

在前文中定义的多维重构误差 $\mathbf{MEr}^i$ 在不同类型的流量之间具有差异性，但在同一类型的流量之间的相似度不高。

利用 MrE 模型可得到输入数据 x 的多维重构误差 $\mathbf{MEr}$。将类别标签为 i 的数据集合记为 X，假设 X^t，$X^r \in X$，X^t，X^r 作为 MrE 模型的输入数据，二者的输出结果分别记为 X^{tM}，X^{rM}，则 X^t，X^r 的多维重构误差的近似表示如式（17）所示。从式（17）可得，第 i 个行向量近似为零向量是 $\mathbf{MEr}^{X_t}$ 矩阵和 $\mathbf{MEr}^{X_r}$ 矩阵均具备的特点，虽然其他行向量均不近似于零向量，但其数据在两个矩阵之间不体现相似性。

$$\mathbf{MEr}^{(X^t)} \approx \begin{pmatrix} \left|X_1^{tM}-\chi_1^t\right| \\ \vdots \\ \mathbf{0} \\ \vdots \\ \left|X_j^{tM}-\chi_j^t\right| \\ \vdots \\ \left|X_K^{tM}-\chi_K^t\right| \end{pmatrix} \chi^t = \begin{pmatrix} X_1^t & \cdots & X_n^t \\ \vdots & & \vdots \\ X_1^t & \cdots & X_n^t \end{pmatrix} \mathbf{MEr}^{(X^r)} \approx \begin{pmatrix} \left|X_1^{rM}-\chi_1^r\right| \\ \vdots \\ \mathbf{0} \\ \vdots \\ \left|X_j^{rM}-\chi_j^r\right| \\ \vdots \\ \left|X_K^{rM}-\chi_K^r\right| \end{pmatrix} \chi^r = \begin{pmatrix} X_1^r & \cdots & X_n^r \\ \vdots & & \vdots \\ X_1^r & \cdots & X_n^r \end{pmatrix} \tag{17}$$

$\mathbf{MEr}^{X_t}$ 矩阵和 $\mathbf{MEr}^{X_r}$ 矩阵的相似性仅在第 i 个行向量上有所体现，导致同一类别数据 X^t，X^r 的多维重构误差特征相似度低，因此需要选取合适的函数将多维重构误差特征映射为新的数值，提高同一类别数据在新数值表示下的相似度。

（2）映射函数

双曲正切函数（hyperbolic tangent function，Tanh）常被用作神经网络的激活函数，在实数域内是连续可导函数，将其导函数记为 $f'(x)$，双曲正切函数的导函数图像如图 5 所示。

由图 5 可见，$f'(x)$的特点为：将接近 0 的数映射到数字 1 附近，将较大的数映射为数字 0。X^t、X^r 的多维重构误差矩阵的第 i 个行向量近似为零向量，虽然其他行向量均不近似于零向量，但这一特点是两个矩阵之间可以被量化的共性，可通过 $f'(x)$函数进行统一度量。

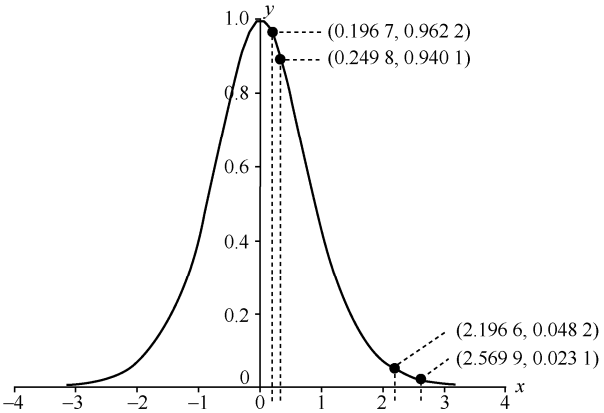

图 5　双曲正切函数的导函数图像

考虑多维重构误差的特点，$f'(x)$能够将不同程度的“不近似零向量”属性映射为相似的“近似零向量”属性，因此选取 $f'(x)$作为映射函数。

将多维重构误差经过 $f'(x)$函数映射后的数据称为“双曲正切多维重构误差”，记为 TMEr，同一类型数据 X^t，X^r 的 TMEr 分别近似表示为式（18）。其中，**0** 代表零向量，**1**=[1,1,⋯,1]。

$$\mathbf{TMEr}^{(X^t)} \approx \begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{1} \\ \vdots \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}_{K\times n} \quad \mathbf{TMEr}^{(X^r)} \approx \begin{pmatrix} \mathbf{0} \\ \vdots \\ \mathbf{1} \\ \vdots \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}_{K\times n} \tag{18}$$

5　DDoS 攻击检测

如前文所述，由队列提取到的定量和定性特征矩阵，经过自编码器、多维重构编码器和函数映射的处理，定量特征矩阵中每一行向量均为矩阵 **TMEr** 展平后的向量，定性特征矩阵未改变。

在检测 DDoS 攻击时，将频率信息作为补充特征可以提升检测效果[7]，文本卷积网络可以提取定量特征矩阵蕴涵的频率信息，信息熵计算可以统计定性特征值在矩阵中出现的概率，由此得到定量和定性特征贡献的频率信息，均为一维向量。队列信息编码负责拼接两个一维向量，拼接后的向量是待检测流量最终的特征表示，使用机器学习分类器检测出流量是正常流量或某种类型的 DDoS 攻击流量。

5.1　文本卷积网络和信息熵计算

通过文本卷积网络和信息熵计算分别提取定量和定性特征矩阵的频率信息。使用大小分别为 3、4、5 的卷积核在定量特征矩阵上执行卷积操作，卷积层最大池化后得到单个数值，拼接所有卷积层池化后的数值得到一维卷积向量，卷积、池化过程如图 6 所示。

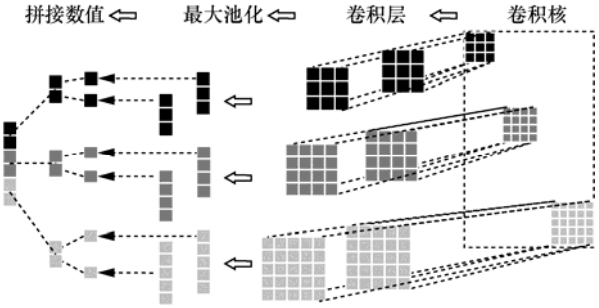

图 6　卷积、池化过程

将定性特征矩阵记为 $\boldsymbol{W}$：

$$\boldsymbol{W} = \begin{pmatrix} F_{11} & F_{21} & \cdots & F_{m1} \\ \vdots & \vdots & & \vdots \\ F_{1n} & F_{2n} & \cdots & F_{mn} \end{pmatrix} \tag{19}$$

对于任一定性特征，计算其信息熵值，信息熵计算方法如下。

$$\text{entropy}_{F_i} = -\sum_{j\in\{1,\cdots,n\}} p(F_{ij})\lg p(F_{ij}) \tag{20}$$

其中，$p(F_{ij})$表示特征 F_i 的特征值 F_{ij} 在矩阵中出现的概率，计算各定性特征的信息熵值，得到信息熵向量[entropy_{F_1}, entropy_{F_2},⋯,entropy_{F_m}]。

5.2　队列信息编码和 DDoS 攻击检测

如前文所述，通过文本卷积网络和信息熵计算得到卷积定量特征的一维卷积向量和定性特征的一维信息熵向量，分别表示为[Conv_1,Conv_2,⋯, Conv_i] 和 [entropy_{F_1}, entropy_{F_2},⋯,entropy_{F_m}]。队列信息编码负责横向拼接两个向量，得到流量队列的一维编码，用向量表示为 FinalVec=[Conv_1, Conv_2,⋯,Conv_i,entropy_{F_1}, entropy_{F_2},⋯,entropy_{F_m}]。

使用机器学习分类器计算向量 FinalVec 的预测标签值 label，label∈{0,1,⋯,K−1}，0 标签值代表检测结果为正常流量，其余标签值代表不同类型的 DDoS 攻击流量。

6　实验及结果分析

为验证本文方法的可行性和有效性，开展以下 3 个实验：空间开销对比实验、队列长度的影响评估实验和 DDoS 检测对比实验。

6.1 实验环境及数据集

实验硬件配置为：Intel Core i5 处理器，Intel(R) Iris(R) Xe Graphics 集成显卡。实验中训练和测试均在 Windows 11 操作系统上进行，使用 Python3.9 编程语言及 PyTorch1.9 开源深度学习框架。

为评估本文方法对物联网 DDoS 攻击流量的检测能力，本文选择 Bot-IoT 数据集[27]。Bot-IoT 数据集由澳大利亚新南威尔士大学堪培拉分校的网络空间实验室通过设计仿真网络环境创建，网络环境模拟正常流量和物联网僵尸网络流量，僵尸网络流量包括 3 种类型的 DDoS 攻击流量。加拿大网络安全研究所在 2019 年发表的一篇论文中给出 CICDDoS2019 数据集[28]，其中包括正常流量和最新的 12 种 DDoS 攻击流量，近年来有多篇物联网 DDoS 攻击检测领域的文献在实验中采用 CICDDoS2019 数据集[12-13,24-26]。综上所述，本文采用 CICDDoS2019 数据集进行实验能够更客观地评估 SFDTFRM 的检测性能。

6.2 评价指标

为充分评估 SFDTFRM 的有效性，使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 F1 分数（F1-score）作为评价指标。准确率表示正确分类的样本占总样本的比例，精确率表示预测结果为正例的样本中实际正样本的比例，召回率表示预测结果为正例的样本中实际正样本占所有正样本的比例，F1 分数是精确率和召回率的加权平均，F1 分数越高，模型越稳健。4 个评价指标的计算式如下。

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{TN}+\text{FN}} \tag{21}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{22}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{23}$$

$$\text{F1-score}=\frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{24}$$

其中，精确率、召回率和 F1 分数方法的计算取不同类别评估指标的平均值，给予所有类别相同权重。

6.3 空间开销对比实验

为评估 SFDTFRM 与基准模型[23]相比之下的空间开销优势以及 SFDTFRM 适用于物联网环境的轻量级优势，开展空间开销对比试验。

在评估实验中，分别使用 CICDDoS2019 数据集的正常流量、12 种 DDoS 攻击流量、BoT-IoT 数据集的正常流量及 2 种物联网 DDoS 攻击流量训练 SFDTFRM 中的多维重构编码器和 Method[23] 中的基准模型。通过比较两种预训练模型所占用的内存大小来评估两种方法的空间开销，空间开销对比结果如图 7 所示。

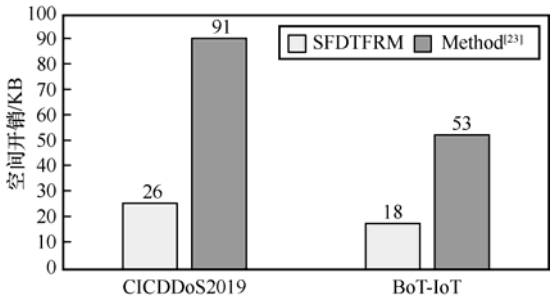

图 7 空间开销对比结果

由图 7 可知，SFDTFRM 中的多维重构编码器模型所占用的内存开销更小。假设流量数据有 n 类，为了检测出 n 类流量，在文献[23]的方法中，堆叠了 n 个自编码器。在训练阶段，分别使用一类流量数据训练一个自编码器；在检测阶段，将待检测流量作为训练好的 n 个自编码器的输入，可得到 n 个向量重构误差，分别与设定好的阈值比较，确定待检测流量的类别。如前文所述，本文提出的多维重构编码器通过共享参数，仅在解码器的最后一个全连接层保留不同类型数据的特殊参数，只需要训练一个模型便可得到相似的输出结果，因此 SFDTFRM 具有更小的空间开销。

实验结果表明，将检测方法部署在主机端来检测主机与目标通信流量是否异常时，更加轻量化的多维重构编码器更适用于资源受限的物联网设备。

6.4　队列长度的影响评估

为确定 SFDTFRM 中队列长度参数 k，在 CICDDoS2019 数据集上进行队列长度的影响评估实验，评估不同 k 值对检测效果的影响。在 SFDTFRM 中，长度为 k 的队列用于存储流量，将队列视为一个长度为 k 的滑动窗口，滑动窗口示意图如图 8 所示，滑动窗口的长度对应时间跨度。

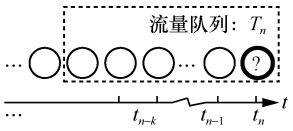

图 8　滑动窗口示意图

在评估实验中，选取 5 个时间跨度，分别为 5 ms、10 ms、15 ms、25 ms 和 35 ms。在 CICDDoS2019 数据集中，首日流量状态可描述为 9 min 内生成了约 70 万条流量，则 5 个时间跨度内存储的流量数量约为 4、8、12、20 和 27，即 k 的 5 个候选值。

分别将 k 值设置为 4、8、12、20 和 27，得到 SFDTFRM 的检测准确率和内存开销，不同 k 值对准确率和内存开销的影响如图 9 所示。

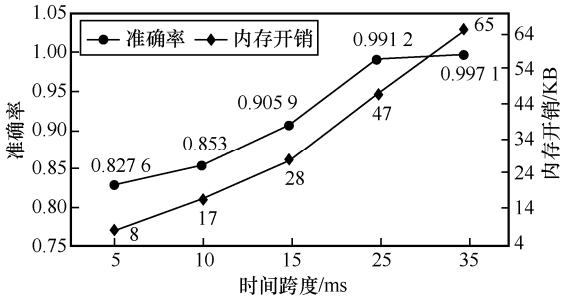

图 9　不同 k 值对准确率和内存开销的影响

由图 9 可见，随着时间跨度变长，检测准确率上升。这是因为存储的流量增多带来了包括频率信息在内更丰富的特征，但准确率的上升趋势会随着时间跨度的延长而变缓直到停滞，存在边际效应，SFDTFRM 的内存开销也随之增大。

因此，k 值的选取需要综合考虑准确率上升的边际效应和物联网设备资源受限的情况。最终选取 25 ms 时间窗口，对应的 k 值为 20。

6.5　DDoS 检测对比实验

为评估 SFDTFRM 对物联网 DDoS 攻击的检测性能，在两个数据集上分别进行 DDoS 攻击检测实验。在实验中，将本文的 SFDTFRM 与 DDoS 攻击检测领域最新的 7 种方法进行对比。

SFDTFRM 与 CIOT[6]、RMSD[7]、LSTM[24]、NDL[25]、SDELM[17]、ODIT[10] 和 RAD[26] 在 CICDDoS2019 和 Bot-IoT 数据集上的 DDoS 检测实验对比结果见表 2。

表 2　CICDDoS2019 和 Bot-IoT 数据集上的 DDOS 检测实验对比结果

方法	CICDDoS2019 数据集				Bot-IoT 数据集			
	准确率	精确率	召回率	F1 分数	准确率	精确率	召回率	F1 分数
CIOT[6]	0.919 5	0.920 5	0.920 6	0.920 4	0.966 3	0.966 9	0.966 6	0.966 3
RMSD[7]	0.897 0	0.866 2	0.897 2	0.879 4	0.970 9	0.927 9	0.952 7	0.940 3
LSTM[24]	0.934 7	0.918 4	0.934 6	0.926 5	0.948 0	0.926 5	0.947 9	0.937 2
NDL[25]	0.983 4	0.943 4	0.970 2	0.956 8	0.983 7	0.983 8	0.983 6	0.983 7
SDELM[17]	0.949 0	0.953 1	0.948 9	0.951 0	0.959 8	0.963 0	0.959 0	0.961 0
ODIT[10]	0.973 9	0.973 9	0.973 7	0.973 7	0.961 5	0.962 7	0.961 4	0.961 7
RAD[26]	0.999 9	0.801 0	0.999 9	0.889 5	0.999 9	0.810 9	0.999 9	0.895 5
SFDTFRM	0.991 2	0.991 2	0.991 3	0.991 2	0.998 3	0.998 3	0.998 4	0.998 4

由表2可知，SFDTFRM不仅在CICDDoS2019数据集上具有良好的检测性能，还能够以较高准确率与F1分数检测出物联网DDoS攻击流量，除此之外，SFDTFRM的4个性能指标值均优于上述7种方法中的6种，平均性能指标值优于所有方法。

与RAD[26]相比，SFDTFRM的准确率、召回率偏低，精确率、F1分数更高。其原因如下。

（1）RAD[26]是基于用户的三阶段检测方法。在RAD[26]中，如果将合法用户检测为攻击者，则合法用户产生的所有流量将被识别为恶意流量，导致DDoS攻击流量检测的误报率（false positive，FP）较高，因此RAD的准确率较高但精确率较低。

（2）SFDTFRM是基于单条流量的，且多维重构与函数映射部分可以增强相同类型流量的相似性和不同类型流量的区分度，有助于检测出DDoS攻击流量，FP和漏报率（false negative，FN）低，检测效果更好。

7 结束语

针对当前物联网DDoS攻击检测方法未充分进行物联网DDoS攻击流量特征衍生导致的特征差异性低、对单条流量的检测性能差等问题，提出一种基于流量特征重构与映射的单流检测方法。通过队列按照先入先出规则存储流量来捕获数值和频率信息，使用队列的整体特征表示待检测流量，丰富单条流量特征信息的同时检测单条流量。通过改进损失函数搭建多维重构编码器，依据流量对应的索引从相应位置重构流量。基于多维重构编码器的输出和输入数据计算多维重构误差，提高不同类型流量的区分度。基于多维重构误差特点，选择双曲正切函数的导函数作为映射函数，增强同一类型流量的相似性同时保留不同类型流量的区分度。通过文本卷积网络、信息熵提取频率信息，通过机器学习分类器执行检测。

在CICDDoS2019数据集和Bot-IoT数据集的实验结果表明，SFDTFRM能有效检测不同类型的DDoS攻击流量。在未来的研究工作中，将探索如何使用无监督学习方法训练并提升DDoS攻击检测性能。

参考文献：

[1] YANG H Y, ZHANG L, ZHANG X G, et al. An adaptive IoT network security situation prediction model[J]. Mobile Networks and Applications, 2022, 27(1): 371-381.

[2] YANG H Y, YUAN H H, ZHANG L. Risk assessment method of IoT host based on attack graph[J]. Mobile Networks and Applications, 2023: 1-10.

[3] 一个藏在我们身边的巨型僵尸网络：Pink[EB]. 2023.
A giant zombie network hidden around us: Pink[EB]. 2023.

[4] YANG H Y, ZHANG Z X, XIE L X, et al. Network security situation assessment with network attack behavior classification[J]. International Journal of Intelligent Systems, 2022, 37(10): 6909-6927.

[5] DDoS attack report for Q3 2022[EB]. 2023.

[6] DOSHI R, APTHORPE N, FEAMSTER N. Machine learning DDoS detection for consumer Internet of things devices[C]//Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW). Piscataway: IEEE Press, 2018: 29-35.

[7] LIU Z, HU C Z, SHAN C. Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method[J]. Computers & Security, 2021(109): 102392.

[8] AHMED M E, ULLAH S, KIM H. Statistical application fingerprinting for DDoS attack mitigation[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(6): 1471-1484.

[9] DAS S, VENUGOPAL D, SHIVA S, et al. Empirical evaluation of the ensemble framework for feature selection in DDoS attack[C]//Proceedings of the 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). Piscataway: IEEE Press, 2020: 56-61.

[10] DOSHI K, YILMAZ Y, ULUDAG S. Timely detection and mitigation of stealthy DDoS attacks via IoT networks[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2164-2176.

[11] ZHU T, QIU X K, RAO Y, et al. HiAtGang: how to mine the gangs hidden behind DDoS attacks[J]. Chinese Journal of Electronics, 2022, 31(2): 293-303.

[12] SALAHUDDIN M A, POURAHMADI V, ALAMEDDINE H A, et al. Chronos: DDoS attack detection using time-based autoencoder[J]. IEEE Transactions on Network and Service Management, 2022, 19(1): 627-641.

[13] LIU X Q, REN J D, HE H T, et al. Low-rate DDoS attacks detection method using data compression and behavior divergence measurement[J]. Computers & Security, 2021(100): 102107.

[14] JIA Y Z, ZHONG F T, ALRAWAIS A, et al. FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks[J]. IEEE Internet of Things Journal, 2020, 7(10): 9552-9562.
[15] BHAYO J, JAFAQ R, AHMED A, et al. A time-efficient approach toward DDoS attack detection in IoT network using SDN[J]. IEEE Internet of Things Journal, 2022, 9(5): 3612-3630.
[16] DING D M, SAVI M, SIRACUSA D. Tracking normalized network traffic entropy to detect DDoS attacks in P4[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(6): 4019-4031.
[17] RAVI N, SHALINIE S M. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture[J]. IEEE Internet of Things Journal, 2020, 7(4): 3559-3570.
[18] KUSHWAH G S, RANGA V. Optimized extreme learning machine for detecting DDoS attacks in cloud computing[J]. Computers & Security, 2021(105): 102260.
[19] DORIGUZZI-CORIN R, MILLAR S, SCOTT-HAYWARD S, et al. Lucid: a practical, lightweight deep learning solution for DDoS attack detection[J]. IEEE Transactions on Network and Service Management, 2020, 17(2): 876-889.
[20] CVITIĆ I, PERAKOVIC D, GUPTA B B, et al. Boosting-based DDoS detection in Internet of things systems[J]. IEEE Internet of Things Journal, 2022, 9(3): 2109-2123.
[21] 张龙, 王劲松. SDN 中基于信息熵与 DNN 的 DDoS 攻击检测模型[J]. 计算机研究与发展, 2019, 56(5): 909-918.
ZHANG L, WANG J S. DDoS attack detection model based on information entropy and DNN in SDN[J]. Journal of Computer Research and Development, 2019, 56(5): 909-918.
[22] ZHOU L, ZHU Y, ZONG T R, et al. A feature selection-based method for DDoS attack flow classification[J]. Future Generation Computer Systems, 2022, 132: 67-79.
[23] TORABI H, MIRTAHERI S L, GRECO S. Practical autoencoder based anomaly detection by using vector reconstruction error[J]. Cybersecurity, 2023, 6(1): 1-13.
[24] AYDIN H, ORMAN Z, ALI AYDIN M. A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment[J]. Computers & Security, 2022(118): 102725.
[25] AKGUN D, HIZAL S, CAVUSOGLU U. A new DDoS attacks intrusion detection model based on deep learning for cybersecurity[J]. Computers & Security, 2022(118): 102748.
[26] HAJIMAGHSOODI M, JALILI R. RAD: a statistical mechanism based on behavioral analysis for DDoS attack countermeasure[J]. IEEE Transactions on Information Forensics and Security, 2022(17): 2732-2745.
[27] The Bot-IoT dataset[EB]. 2023.
[28] SHARAFALDIN I, LASHKARI A H, HAKAK S, et al. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy[C]//Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST). Piscataway: IEEE Press, 2019: 1-8.

[作者简介]

谢丽霞（1974− ）,女，中国民航大学教授、硕士生导师，主要研究方向为网络与系统安全、网络安全态势感知。

袁冰迪（2000−），女，中国民航大学硕士生，主要研究方向为网络信息安全和 DDoS 攻击检测。

杨宏宇（1969− ），男，博士，中国民航大学教授、博士生导师，CCF 专业会员，主要研究方向为网络与系统安全、软件安全检测和网络安全态势感知。

胡泽（1989− ），男，博士，中国民航大学讲师、硕士生导师，主要研究方向为人工智能、自然语言处理和网络信息安全。

成翔（1988− ），男，博士，扬州大学实验师、硕士生导师，主要研究方向为网络与系统安全、网络安全态势感知和 APT 攻击检测。

张良（1987−），男，博士，亚利桑那大学博士后研究员，主要研究方向为强化学习、基于深度学习的信号处理和网络与系统安全。