网络异常检测中的流量表示研究

孙剑文，张斌，常禾雨
（信息工程大学密码工程学院，河南 郑州 450001）

摘　要：针对网络异常检测中流量表示存在的信息丢失问题，从数据采集粒度入手分析不同流量表示的特征信息维度对异常检测性能的影响。首先，介绍了恶意异常检测中流量表示粒度间的协同与耦合关系，以及异常检测中的流量表示、特征学习和检测三环节间的耦合关系。然后，系统审视流量表示在网络异常检测中的发展轨迹，深入分析了流量表示形式、流量特征学习与流量表示在异常检测中的应用3个方面的国内外研究现状。最后，围绕流量表示在网络异常检测应用中协同耦合的发展趋势对未来研究进行展望。

关键词：异常检测；网络流量；流量表示形式；特征类型；多模态流量表示
中图分类号：TP393.08
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025003

Research on traffic representation in network anomaly detection

SUN Jianwen, ZHANG Bin, CHANG Heyu
Cryptography Engineering Institute, Information Engineering University, Zhengzhou 450001, China

Abstract: Aiming to address the problem of information loss in traffic representation for network anomaly detection, the impact of feature information dimension of different traffic representation on anomaly detection performance was analyzed from the perspective of data collection granularity. Firstly, the integrated collaboration between traffic representation granularity and the coupling among traffic representation, feature learning, and detection in malicious anomaly detection was introduced. Subsequently, the evolution of traffic representation in network anomaly detection was systematically reviewed, providing a comprehensive analysis of its forms, feature learning, and application in anomaly detection both globally and domestically. Finally, the future research directions revolving around the collaborative development trend of traffic representation in network anomaly detection were outlined.

Keywords: anomaly detection, network traffic, traffic representation form, feature type, multimodal traffic representation

0　引言

伴随网络空间攻防对抗的日益加剧，不断演进、多样和隐蔽的网络攻击手段，对网络安全研究人员和数据网络管理人员提出了新的挑战。网络异常检测是网络安全防护的重要环节，从系统工程角度来看，不难发现网络异常检测是一个多维度、多层次和多因素相互作用的复杂过程，如图1所示。通过梳理总结，可以将网络异常检测的逻辑关系划分为3个层面：在数据层面，系统通常依据专家经验采集所需数据源、数据粒度以及提取相应特征信息；在控制层面，通过建立和优化机器学习模型，学习相关特征在不同抽象层次的信息，并迭代特征表示、特征抽象和预处理过程以适应模型训练，在此过程中专家可以依据验证性能结果进行分析和调整；在应用部署层面，检测模块被用于识别异常，最终由专家决策并采取适当措施，同时检测结果反

收稿日期：2024–09–25；**修回日期：**2024–11–19
通信作者：常禾雨，okaychy@163.com
基金项目：国家自然科学基金资助项目（No.62276091）
Foundation Item：The National Natural Science Foundation of China (No.62276091)

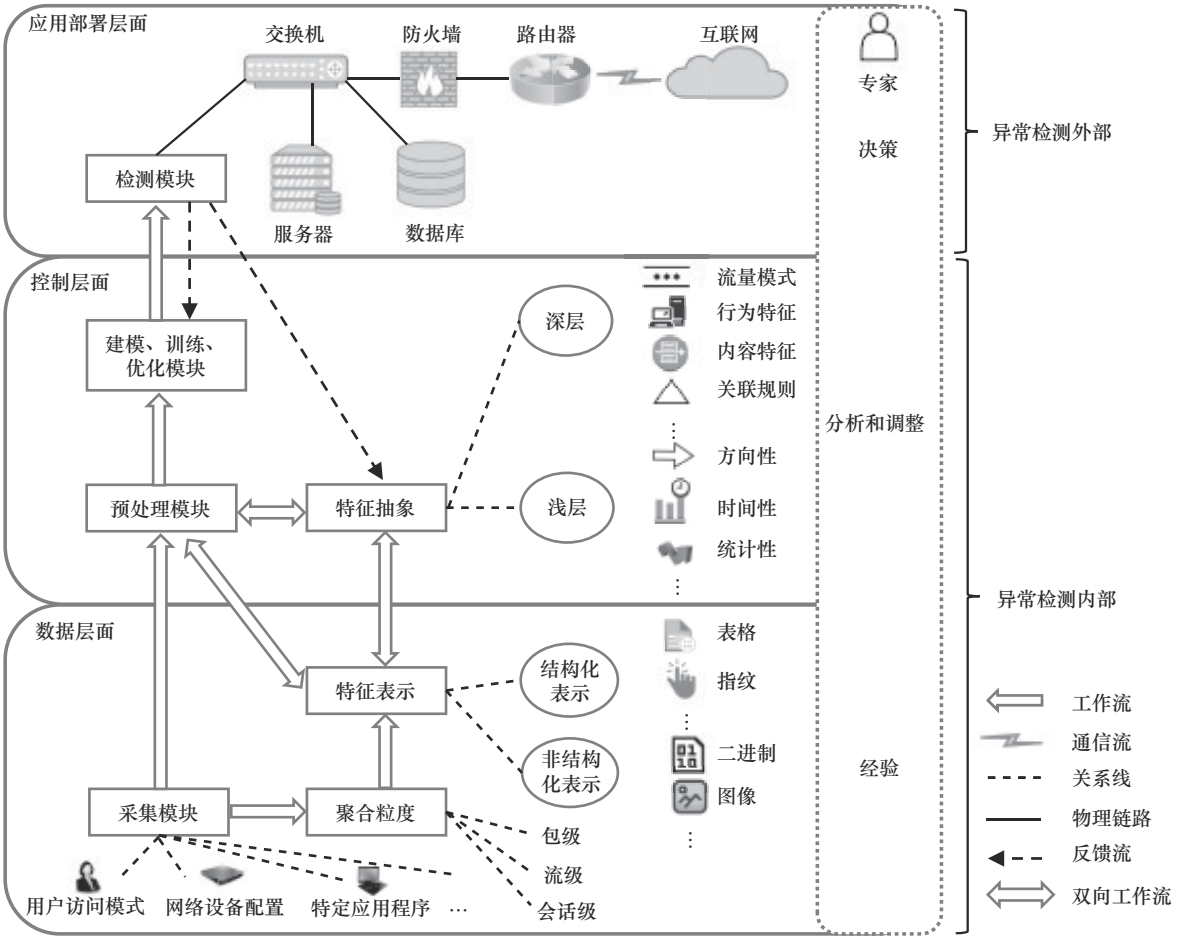

图1　网络流量异常检测

馈可以用于不断优化训练模型。

随着机器学习算法的不断发展，异常检测技术在精确检测已知攻击以及检测出未知攻击上已取得了显著进展[1-2]。然而，当前异常检测技术仍面临着一系列挑战，如模型训练受限于训练数据规模和特定数据分布。这些挑战的核心问题在于训练模型的流量数据。数据集的扩展为深入分析流量和提高异常检测的准确性奠定了坚实基础。随着攻击者策略的演变，单一特征已不足以有效区分正常网络行为和恶意网络行为，而在数据集构造中通过引入统计特征和时序特征，进一步丰富了场景和网络流量的表示形式，如UGR’16、CIC-IDS2017以及持续更新的LUflow’20[3]数据集等。由此可以看出，当前主流的网络流量入侵检测重点关注网络攻击技术演进对研究数据的需求，尤其是在网络流量的多样性特征和复杂性行为模式的表示方面。

网络流量的表示是理解和解释网络行为的关键步骤，通过抽象化过程（数据采集-特征提取-特征选择-特征转换-特征抽象-模型构建）突出了网络行为最重要的特征。然而，网络流量数据的复杂性和动态性给流量表示带来了挑战。在将网络行为流量映射到流量特征表示过程中，标准化处理或形式转换导致信息丢失的问题难以避免。因此，设计鲁棒的流量特征表示，提升流量表示的泛化性进而提升异常检测性能，成为该技术领域的一个严峻挑战。为此，本文从流量表示的视角出发，采用以网络异常检测流程驱动的方式，从流量数据采集粒度入手，探讨不同粒度级别对流量表示的影响。在此基础上，系统分析了特征表示形式，并进一步探讨特征学习过程中流量表示对特征空间的影响，以及对异常检测产生的作用，如表1所示。其中，○表示未明确涉及，√表示涉及，×表示未涉及。

在网络流量异常检测领域，国内外学者进行了系统且深入的研究，涉及广泛的议题和视角。例如，重点关注检测技术或算法的进展[5-7]、侧重不同检测场景下的应用和挑战[2,8-10]、偏向数据分析

表 1 与相似工作的对比

分析框架	特征表示形式分类		文献[1]	文献[4]	本文方法
数据粒度		包级别	√	√	√
		流级别	√	√	√
		会话级别	○	√	√
特征表示形式类别	统计时序层面	统计信息	√	√	√
		时序信息	○	√	√
	结构层面	图结构信息	√	×	√
	内容层面	语义信息	○	×	√
		指纹信息	×	×	√
	数据层面	原始信息（字节/二进制）	○	×	√
		图像信息	×	×	√
特征学习方法		传统机器学习	√	√	√
		深度学习	√	√	√
检测方法		传统机器学习	√	√	√
		深度学习	√	√	√
		混合方法	○	√	√

或特征选择技术在检测中的关键作用[4,11-12]等。文献[1]围绕网络安全威胁检测的数据采集和分析进行介绍，涵盖了结构化的流量表示方法，并系统性地讨论了特征类型和特征学习的不同形式。文献[4]围绕高维度大数据环境下的异常检测问题，讨论了高维度数据集中的流量表示问题，并通过降维和子空间等分析策略和技术改善特征表示。本文在前人工作的基础上进行了更为全面的探索讨论与梳理总结，涵盖了特征信息等更多层面的内容，不仅系统性地回顾了目前已知的网络流量表示形式，还详细讨论了不同阶段网络流量表示形式的研究进展和相互之间的关系。本文主要贡献总结如下。

1) 提出了一种新的分类方法，将流量特征表示形式分为 4 个主要层面，并进一步细分为 7 个信息维度，为网络流量特征提取和分析提供了结构化框架，进而理解不同网络流量特征表示方法之间的关联性和适用性，同时也为后续任务中机器学习模型的设计和应用提供了新的思路和依据。

2) 围绕网络流量特征表示和特征学习与异常检测性能的关联性，分析不同特征表示形式在结合机器学习技术时的具体影响，尤其是在采用不同网络结构和学习策略提升模型对网络流量的学习和检测效果方面。同时，指出这些方法在实际应用中的优势与局限性，进而深入剖析现有研究在处理流量特征多样性和行为模式复杂性等方面所面临的问题和挑战，为理解和改进流量表示提供了依据。

3) 分别从设计多维度、跨层次、自适应、可解释和对抗性攻击下的鲁棒性流量表示方面，对适应网络环境变化的协同模式、协同模式的标准化和兼容性，以及流量表示、学习、检测耦合技术深度整合的必要性等开放性研究问题进行了讨论与展望。

1 流量表示与异常检测的耦合关系

在异常检测中，一个任务的完成依赖于流量在数据表示转换、特征学习和检测等环节的高效、有序协同运作。从本质上讲，这 3 个过程是通过网络流量在数据层、控制层和应用部署层上耦合在一起的。具体来说，这包括不同粒度（包、流、会话）级别的数据进行协同处理与耦合，以及 3 个关键环节（表示、学习、检测）的耦合，这些协同与耦合关系共同构成异常检测流程的核心，如图 2 所示。

1.1 包、流和会话三级别间的协同与数据耦合关系

网络流量在数据层进行转换处理之前，需要先经历数据采集，确定其在粒度级别上的流量表示，包括从原始网络流量中提取出包、流或会话级别的数据。网络流量的连接单元决定了数据粒度的划分与数据表示的详细程度。数据粒度的选择将影响分析深度和计算复杂性。

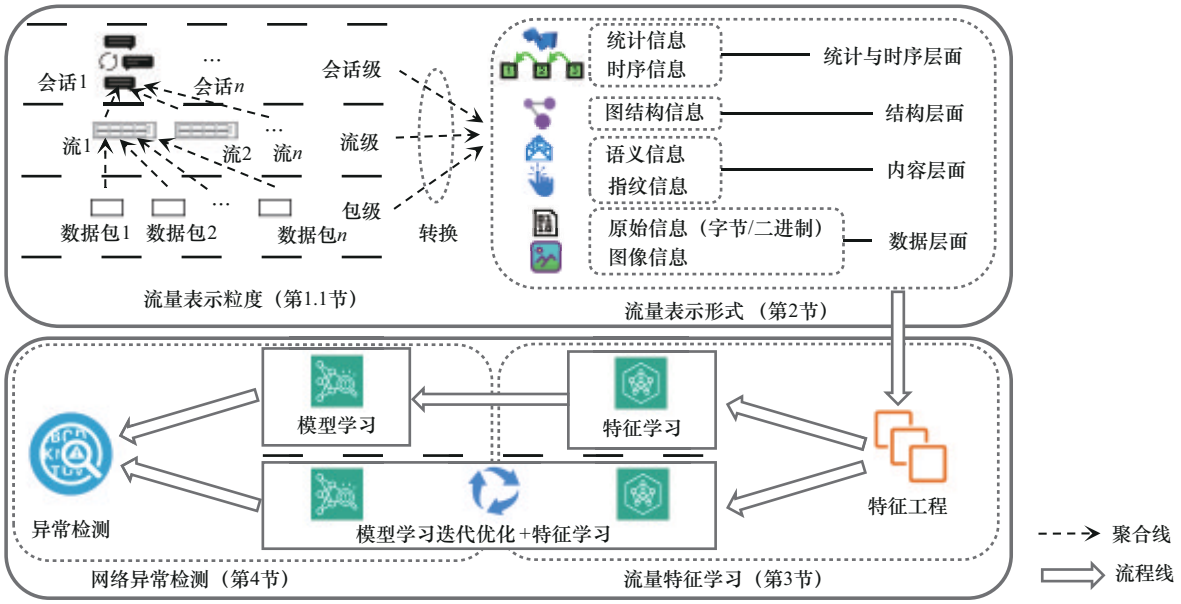

图2　流量表示与异常检测的耦合关系

1) 数据包级别的流量分析能够识别出特定攻击行为，但对于行为关联度高的复杂网络攻击和加密流量存在检测局限性。分析数据包级别的流量主要分为两部分。首先，数据包头部包含了引导数据包在网络中传输的必要信息，对理解数据包传输延迟与否、通信信息完整与否和识别潜在的恶意行为方面至关重要。分析数据包头部信息可以提升资源受限环境下识别欺骗攻击的效率[13]。然而，数据包头部信息的特征与恶意行为之间的关系是非线性的，仅依赖数据包头部信息不足以准确判断流量的性质和攻击类别。

其次，数据包有效载荷直接反映了数据传输实质信息的内容，与控制数据传输的数据包头部信息相区分。研究表明，攻击行为流量常在有效载荷中携带恶意代码或内容，包括恶意软件签名、恶意脚本、加密通信中的特定模式等[14-15]。通过N-gram方法能够检测攻击行为在有效载荷中的异常状态[16]，但也受限于加密算法的强度和复杂性[17]。然而，由于缺乏解密密钥，加密的有效载荷在技术上难以直接分析。因此，在没有额外上下文信息的情况下，恶意活动数据包可能因其与正常流量相似的流量特征而难以被区分。上述研究表明，在包级别下更准确的流量表示需要结合数据包头部信息和有效载荷的上下文信息，且在异常检测角度看包级别的流量表示时，需要面临高速流量背景下处理和分析每个数据包的计算密集性问题和扩展性问题，以避免成为系统瓶颈。

2) 流级别的流量分析具备行为关联性，能够识别单个数据包流量看似无害而整体流量行为存在恶意的情况，并且能够分析加密流量和非加密流量。依据此应用场景，通过预定义的流量键将数据包分成不同流以实现流级别聚合[3,18-19]。一些研究采用超越N元组的聚合方式进行自定义，如Gupta等[20]选择从特定应用程序中生成数据包子集来定义流。

流级别分析捕捉数据包之间的关联性信息和时间序列信息[21]。通过分析行为上下文信息可以揭示整体流量表示中的有组织行为模式，有助于推断攻击者的潜在意图。尽管单个恶意请求与正常请求相似而难以被直接区分，但通过检查多个流之间的相关性可以发现整体上高度协调的分布式拒绝服务（DDoS, distributed denial of service）攻击行为。通过减少数据量降低了计算需求和存储需求，在快速检测流量型攻击和中央服务器监控大量流量的场景中均适用。然而，流级别流量表示会丢失数据包级别的细节，如有效载荷信息，从而削弱了检测更高层次威胁的能力。基于有效载荷传输的攻击（如蠕虫、勒索软件和特洛伊木马等）难以被基于流级别的检测方法发现。从异常检测角度看流级别流量表示，决策速度可能因处理历史数据或计算统计特征等延迟。

3) 会话级别的流量分析能够揭示应用部署层的复杂攻击模式，但受限于流量解析方法的技术复

杂性和分析过程的非实时性。会话级别分析聚焦于客户端与服务器之间的连续交互，通过关联一系列数据包来记录完整的通信过程。与流级别分析关注数据包传输特征不同，会话级别分析更侧重应用部署层逻辑和用户交互，适用于检测那些在数据包层面表现不显著但在会话层面表现异常的攻击模式。会话级别的流量分析不仅能够揭示完整网站访问过程中的数据包行为[22]，还可以将会话保存为独立文件以进行详细取证分析和攻击检测[23]。会话中请求的完整性和传输速率等特征，能够识别特定的拒绝服务（DoS, denial of service）攻击模式，如 Slowloris DoS 攻击。还能够通过会话持续时间、频率和流量模式，识别出渗透攻击的异常特征。这一点在涉及非标准服务端口或观察到异常行为时尤为明显。从异常检测角度看，通过分析流计数、平均持续时间等单个会话级细节，可以揭示网络通信行为模式和可能存在的异常检测情况，能够检测隐蔽性通信行为和恶意加密流量[24-25]。然而，会话级别分析需要等待、处理和理解完整会话的上下文信息，在计算资源和存储空间方面需求较大，影响了会话级别分析的实时性。

综上所述，从系统工程视角审视网络流量，可以认识到数据包、流、会话这 3 个级别的数据是相互关联的。通过整合数据包级别的细致审查、流级别的行为趋势分析以及会话级别的交互过程追踪，可以构建一个多维度的网络行为视图，进而揭示攻击模式、理解攻击策略和意图。突发（burst，即短时间内传输的连续数据包数据量）可以被视为一种特殊的流，既能够描述数据包级别的现象，又能够描述一定的网络行为。流量表示粒度是一个多因素决策过程，基于应用场景、检测精度要求、可用计算资源与检测目标等多个维度综合权衡，以达到整体性能最优。然而，采集参数设定对于流量聚合与分割、识别与理解具有决定性作用。超时时间戳等参数设定不恰当可能导致连续性攻击行为被错误地划分为独立的流量单元，从而扭曲流量行为的结构表示[26]。

1.2 表示、学习和检测三环节间的耦合关系

网络流量的表示、学习和检测三者之间的紧密关联是理解和提升网络异常检测性能的关键。流量表示在异常检测全流程中至关重要，通过流量的特征表示可以提取出对后续研究有用的信息。在异常检测中，直接使用流量原始字节或二进制数据，虽然简化了对网络协议和数据包结构的理解，但由于数据包头部字段和长度不一致，数据呈现出异构性、模式可变性和特征高维性。这些因素迫使模型适应不同维度输入，而这反过来又对模型性能构成了限制。然而，固定输入维度能使模型在学习过程中将流量表示中的每个位置与其他数据对应进行特定的特征信息学习，避免引入噪声。因此，将流量数据转换为模型可处理的适当形式是提升异常检测性能的前提。

依据使用的流量特征学习方法，可以将网络流量的抽象分为浅层和深层 2 种。在浅层抽象中，信息输入检测模型通过进一步学习后执行检测任务。而在深层抽象中，信息的处理和抽象过程通常与检测模型的迭代学习过程紧密相连。随着各领域技术不断发展，特别是传统机器学习方法的持续改进，神经网络、图表示学习（GRL, graph representation learning）以及多模态数据融合技术的进步等，现在能够将流量数据转换至不同的分析领域，为检测模型提供新视角，进而识别数据中的不同结构和模式。有效的流量表示策略有助于提升异常检测的准确率，优化模型训练和推理时间，降低计算资源消耗。然而，过于简化的流量表示可能忽略关键攻击特征，过于复杂的流量表示可能导致模型过拟合，影响模型的泛化能力和检测精度。

2 流量表示形式

由流量表示与异常检测的耦合关系可以看出，流量表示应考虑到不同检测场景需求，需要平衡信息量的充分性和对扰动的鲁棒性，以实现高效异常检测。本节着重分析流量表示形式中的特征表示方法，特征表示方法的选择与所使用模型的类别紧密相关，并且可以增强模型学习数据中模式和关系的能力。特征表示可以概括为以下 3 种方法。

1) 数值特征表示。通过将流量数据映射到数值空间，允许进行数学运算和统计分析。具体地，通过提取描述性统计量[27]以及滑动窗口平均和自相关系数等时间序列特征，量化网络流量分布和动态变化。然而，这种方法在捕捉数据中的复杂非线性结构和模式方面存在局限性。

2) 可视化特征表示。通过将流量数据转换为图像形式，利用视觉直观性揭示关键趋势和异常检测模式。例如，灰度图像[28-29]、彩色图像[30-31]、

图像矩阵[32]等，这种方法便于在时间和空间上进行分析，但在精确量化数据细节方面存在局限性。

3) 结构化特征表示。通过构造结构来保留流量数据的原始结构和关系。例如，使用图结构[33-35]、指纹结构[36]和语义结构[37]，该方法从多方面捕获数据之间的关系和模式，但可能带来较高的计算成本和存储成本，并且在数据分析上需要特定的技术支持。

网络流量的特征表示直接影响检测器输入。为此，需要从4个层面审视当前研究中的特征表示和应用场景。图3说明了流量数据转换为特征表示之前的通用步骤和关键要素。

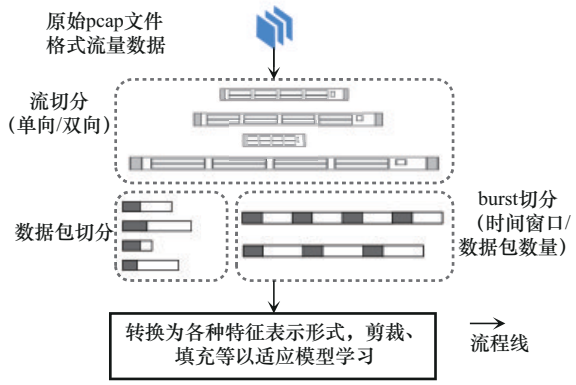

图3　流量表示方法处理流程

2.1　统计与时序层面表示

2.1.1　基于统计信息量化的网络流量模式

传统异常检测方法通常基于预定义规则，如果待检测流量样本包含已知攻击签名，则分类为相应攻击，而在面对新型和未知攻击时无法有效识别。为了实现在异常检测中识别未知流量，一部分研究转向了基于统计信息的方法[36,38-43]，量化分析整体流量行为模式而非单个数据包中的具体内容，即使在数据包有效载荷被加密的情况下，也能够从数据包头部信息中提取出统计特征以进行粗粒度表征。Ahmed等[36]通过数据包级别统计分析，使用加权均值方法计算窗口内流量特征的直方图，实现正常流量特征的紧凑高效表达。Zhao等[43]关注单向流连接的统计特征，从原始流量中提取包括窗口大小、持续时间、速率等关键信息。而Zolotukhin等[38]提取了会话持续时间、每秒发送数据包数量、每秒发送字节数等8种类型的统计特征。Xu等[39]利用信息熵、包大小、包频率和连接时间来描述攻击特征。另外，基于互信息和广义熵的特征选择技术被用于选择与异常类别高度相关且非冗余的特征子集[40]。例如，Hamamoto等[41]通过遗传算法（GA, genetic algorithm）从单向流中提取6个特征，其中包括源和目的IP熵、源和目的端口熵，以构建数字签名从而识别网络流量。

信息熵及其衍生指标被广泛应用于数据集特征的解释和异常检测。通过比较网络流量中IP地址的实际分布与预先定义的正常分布，可以使用信息熵等度量量化分布的随机性或不确定性。如果实际分布的熵值显著高于正常分布的熵值，则表明IP地址的选择具有高度随机性，可以作为一个辅助指标识别潜在的攻击行为，如DDoS攻击行为。基于统计信息的异常检测方法假设与特定程序或服务相关的流量会展现出可区分的统计特征，进而在不依赖具体攻击手段或特征等预先知识的情况下检测到新出现的攻击。然而，如果这些统计特征的流量表示过于粗略或抽象，会被攻击者利用以模拟正常流量的统计特征，从而欺骗检测模型。此外，设定合适阈值以平衡误报或漏报是一个多因素驱动任务，需要在不同应用场景中进行调整。

2.1.2　基于时序信息捕捉网络活动的时态特性

传统异常检测方法往往依赖于静态特征集，使其在面对时间上关联的攻击行为时存在特征捕捉上的局限性。为了解决这一问题，时序信息的提取侧重于通信事件的时间顺序和时间间隔，通常通过计算时间序列数据统计量来量化这些时序特征，揭示一系列如周期性、平稳性等关键行为模式和特征[22,44-47]。David等[46]通过计算时间间隔内的流计数熵并设定动态阈值检测DDoS攻击。Roosmalen等[47]从每个流的前320个数据包头部信息中提取IP头部字段、有效载荷大小等13个特征，以区分P2P-botnet流量和HTTP/HTTPS流量。

此外，Sirinam等[22]通过数据包方向和相对时间序列向量来识别访问的网站，而不依赖于对流量内容的明文解码。Mirsky等[45]利用双向流的统计特征和时序特征，提取每5个时间窗口的统计数据作为输入特征，并通过构建分布式特征提取框架以提升特征表示的实时性和可扩展性。Msadek等[44]采用滑动窗口方法自动分割流量数据，并结合基于统计分布的衍生特征生成用于识别流量模式的指纹特征。Ma等[27]提出了序列概要表示方法，提取了

包括基于IP头部信息的数据包向量、基于一定时间间隔内的数据包突发信息和基于2个包突发之间的最长公共子序列轮廓信息，以构建空间和时间特征，进一步丰富了时序信息应用场景。

虽然，时序信息的核心在于捕捉时间维度上的动态变化和依赖性，但发展中的时序信息已不局限于传统时序分析的定义。Radford等[48]将网络流量转换为“单词”序列组成句子，并将其作为特定网络语言模型的输入学习新生成的语义和语法。基于时间顺序的事件特征表示结合协议、字节和端口，揭示了网络通信中的模式和异常行为。

尽管时序信息能够揭示网络活动的时态特性，但在处理高速率网络流量时仍存在诸多挑战，这包括处理多通道数据的复杂性，尤其是在不同通信流中数据包可能以不同的速率和模式交错到达。对于这些复杂数据流的分析技术还需要进一步研究和优化。

2.2 结构层面表示

采用图结构信息表示网络行为的关联关系。由于缺乏对网络复杂性在交互结构上的流量表示，传统异常检测方法往往难以准确区分恶意活动和正常活动。图表示学习技术为检测网络流量中的潜在威胁提供了新维度[17]。确定图结构中节点与边的表示，引入传输方向和关系权重，对行为特征的上下文信息进行多维度考量，增强了机器学习模型对流量分析和异常检测的准确性[33,49]。

在网络流量分析中，可以通过识别和计算图中频繁出现的小型子图模式（即图基）的出现频率，提取出能够反映图中局部连接模式的特征。在区分目标流量与背景流量方面，Mongkolluksamee等[34]融合基于图基的特征向量（35维）、基于传输控制协议（TCP, transmission control protocol）和用户数据报协议（UDP, user datagram protocol）与数据包大小相关的特征向量（各12维），构成图结构的流量表示，通过流持续时间约束过滤短时流，进而去除背景噪声。

在加密流量方面，Shen等[33]提出了流量交互图（TIG, traffic interaction graph），将数据包作为节点，节点之间的边表示数据包之间的特定关系，结合数据包长度、上/下行方向、突发现象以及顺序等特征，有效地表示了加密应用流量的行为特征。TIG在处理加密流量时显示出了较高适用性，但计算密集型的特点限制了其实时处理能力。此外，当出现新加密协议或流量模式等网络环境变化时，TIG需要重新训练。

在协同流量粒度层级的表示方面，Premkumar等[35]通过GRL增强网络入侵检测系统（NIDS, network intrusion detection system）的数据上下文信息感知能力。具体包括2种图表示方法：一是基于网络流信息的位图表示，以数据包作为节点形成简单有向无环图；二是基于连续数据包的线性排列，通过余弦相似度计算连续数据包之间的相似性，在提高检测准确性的同时，实现快速处理连续数据包的目的。

上述基于图的方法利用局部和全局信息交流，加深对网络行为依赖的上下文信息感知方面的深入理解。为了有效利用图卷积网络（GCN, graph convolutional network）等技术，需要仔细考虑如何定义流量图、初始化节点和边，并通过学习后的图嵌入技术优化特征表示。同时，实时处理能力和模型适应性问题也需要进一步研究。

2.3 内容层面表示

2.3.1 采用语义信息分析流量的高层结构和内容

传统异常检测方法虽然考虑了完整语义字段中的数据包高层次头部信息，但忽略了选项字段顺序和内容在指纹识别等应用中的重要影响[46]。一方面，解析应用层协议可以为网络元数据赋予类似自然语言的语法结构，从而提供IP选项等网络通信技术细节及其语义层面信息。然而，利用上述信息表示时，即使是像IP选项存在与否的微小差异，也可能导致数据包表示中的位出现不匹配，这种不匹配会在模型中引入噪声，导致模型难以识别关键特征，进而降低模型性能，影响分析结果。另一方面，如果结果表示无法解释，那么表示中的位就无法映射到具体语义含义。

为了克服这些局限性，Holland等[37]设计的nPrint流量表征格式结合了语义和二进制数据包表示，有效对齐了数据包的二进制数据和特定语义结构，从而能够识别数据包的语义特征。Diallo等[50]将数据包转换为结构化向量，除了头部信息和统计特征，还通过词嵌入技术提取有效载荷内容的语义表示。这些特征向量表示为后续聚类和分类任务提供了信息基础。

流量中的语义信息包括数据意图、上下文信

息、用户行为等深层次信息，可能因标准化表示的截断而无法完全捕捉，如何更全面地表示和利用语义信息仍需进一步研究。

2.3.2　采用指纹信息识别流量结构和特定模式

传统异常检测中基于内容的检测方法受加密流量限制，而指纹技术通过匹配已知模式或行为，为物联网设备[27,51-53]、网页[54]、应用指纹[34,55]识别以及入侵检测[45]等提供了有效解决方案。单一层面信息不足以实现高效的指纹识别[53]。Wang 等[42]通过综合分析数据包尺寸、传输顺序以及在短时间内的连续传输模式构建网站指纹特征。Shen 等[54]利用交互过程中前几个数据包，特别是上行主导阶段与数据包长度相关的特征来识别网页。该研究综合了块特征、序列特征和统计特征，为实现高精度的网页识别奠定了基础，同时保持了较低的时间开销。此外，还有基于时序表示[27]、位图表示[37]等的指纹。上述研究的共同特点是构造指纹不依赖于流量内容的明文解码，从而在保护隐私安全的前提下实现了有效识别和检测。

异构流量的复杂性与同质输入的定制化之间存在矛盾，可能导致数据失真或丢失重要的上下文信息。为了解决这些问题，Qu 等[56]设计了与输入无关的指纹层次框架，将不同层面的异构流量特征抽象为具有相同特征表示的向量，从而分析数据包之间以及流之间的时空相关性。而 Shen 等[33]通过构建信息丰富的图结构，提升了指纹识别方法的准确率。

尽管如此，随着攻击手段演变和加密技术加强，攻击者可能会采用措施来隐藏或伪装其流量特征，对指纹识别技术的有效性构成了挑战。同时，为提升检测的准确性和适应性而开发的精细指纹框架和信息丰富的图结构表示，可能因增加计算和存储需求成为性能瓶颈。

2.4　数据层面表示

2.4.1　流量原始数据底层结构和内容格式

在处理流量原始数据时，理想的做法是将数据包转换为一致且预归一化的格式，并保留它们的顺序信息。然而，在转换过程中可能会忽略数据包大小、协议类型等关键的基础属性信息，导致特征向量在特定位置表示的语义不一致，进而影响机器学习模型的训练和检测效果。

在二进制表示方面，Holland 等[37]提出了包级别的位图表示方法，通过标准化和空间有效编码，自动发现数据包中语义上的重要信息。Premkumar 等[35]基于完整网络流信息的位图表示增强了检测的准确性和上下文信息感知能力。Hosseini 等[14]基于压缩位图索引表表示有效载荷部分，结合流量采样技术有效降低了检测中的误报率。Sohi 等[57]挖掘了流级别二进制表示中的内容特征，以相对较小的特征维度映射特定蠕虫类型的流量，有效地检测了互联网上的智能攻击。

在原始字节表示方面，Lucia 等[15]简化了特征提取过程，组合 TCP 和 UDP 头部字段以及有效载荷字节值构建特征向量，降低了特征向量的维度和计算复杂度。Lotfollahi 团队和 Marin 团队采用“深度包”方法，通过固定长度的有效载荷字节向量捕捉网络流量的本质特征[58-59]。后者额外考虑了流级别的表示以增强检测和分类恶意流量的能力。通过直接使用原始字节数据，可以减少对专家设计特征的依赖，从而允许机器学习模型从数据中学习到更丰富的信息。

尽管上述研究取得了进展，但仍需继续探索和优化自动信息提取技术以及高效的数据压缩和降维技术，使在保留足够信息用于准确分析流量的同时，降低表示所需的存储资源和计算资源。

2.4.2　基于图像信息的网络流量视觉模式转化

传统异常检测面临处理复杂和高维度数据的挑战。一种有效的方法是将流量数据映射到图像像素值，使流量的空间分布和变化趋势通过像素提供直观视觉表示。计算机视觉领域技术，尤其是卷积神经网络（CNN, convolutional neural network）被广泛应用于由流量转化的图像以进行特征提取。较早期，Wang 等[28]将加密流量 TCP 会话的有效载荷转换为灰度图像。从原始流量中自动提取和学习特征，减少了人工干预并为学习内在结构和模式引入了新视角。王勇等[60]将流量数据截取后映射为灰度图像，以解决数据包长度可变的流量分类问题。

为了捕捉时间相关信息，一类典型工作，如 Aneja 等[29]利用数据包之间的到达时间间隔，将序列重塑为二维图像。进一步，Xu 等[30]以时间序列将数据流的前 n 个数据包转换为灰度图像后，又取相邻的 3 个灰度图像组合成 RGB 图像。而 Garg 等[31]从 tcpdump 日志中提取 TCP 和 UDP 数据包的相关特征集，并将其转换为 RGB 图像。这些方法

结合了时间和空间信息，证明了转换后的图像在网络入侵检测领域的应用前景，其中不同类别的图像仍然有不同视觉表示。

另一类典型工作，如Wang等[28]将数据包大小和到达时间转换为一系列对应关系来创建二维直方图，通过归一化将时间轴映射到一个固定范围内，并将其转换为图像矩阵。图像信息通过视觉化的方式提供直观数据表示，增强了流量在空间分布和变化趋势的特征表达，但转换过程中需要额外的处理时间，如果转换过程设计不当或执行不精确，容易导致关键信息丢失。因此，选择合适的图像表示尺寸和颜色通道以及设计有效网络模型来处理这些图像，都值得进一步研究。

基于上述4个层面讨论可以得出，有效特征编码和表示是构建高性能异常检测模型的关键步骤。特征表示形式作为连接原始数据与模型之间的桥梁，通常界定了模型能够捕获的信息范围及其对高维相互作用、时间序列、空间结构、长期依赖性、非线性关系等复杂模式的识别能力。设计特征表示策略，包括有效特征编码、数据预处理和特征向量构建，其中涉及数据的代表性，特征相关性、独立性、尺寸和动态性、模型反馈、领域知识应用以及交叉验证实施等多因素的影响。这些策略有助于提高特征向量质量，从而直接影响模型检测的准确性和鲁棒性。特征表示、学习策略、任务模型的选择过程与反馈关系之间存在密切的相互作用，共同决定了模型的检测性能和适用性。

3 流量特征学习方法

特征抽象将提炼出的信息转换为易于分析的高级形式以识别潜在威胁和异常行为。这一过程通过特征选择、提取、构造、变换等技术，去除冗余细节，优化特征在转换和学习时的表示（包括隐层表示），提高模型的检测性能和效率。

特征学习方法主要分为2种，分别为人工特征工程和自动特征学习。2种方法在实际应用中具有互补性，可以根据特定任务的需求和流量特性进行选择。本节通过趋势分析评估这些方法的有效性，旨在为选择合适的方法提供依据。

3.1 基于传统机器学习方法的流量特征学习

人工特征工程作为特征学习的初步阶段，侧重于从原始网络数据中提取、构造和选择能够揭示网络行为和模式的特征，其效果具有情境依赖性[61]，该领域专家的知识和经验被用于识别检测网络异常行为最可能的关键特征。

1) 在特征选择方面，Bhuyan等[40]通过基于树的聚类算法构建树形结构形成层次化聚类来识别数据模式，进而生成特征摘要，有效地将数据在特定维度上的分布转换为模型可以利用的特征向量。Hamamoto等[41]采用GA自动优化特征选择，以生成描述网络正常行为的数字签名，通过迭代进化找到适应度最高的特征组合，用于构建最佳的网络行为预测模型。

2) 在特征提取方面，Wang等[42]在开放世界实验场景中，使用K-最近邻分类器并基于数据包特征集构建高精度指纹识别模型，有效识别了加密流量中的网站访问行为。在Maiti等[53]的研究中，采用随机森林（RF, random forest）、决策树和支持向量机（SVM, support vector machine）算法提取对分类任务最有贡献的特征以优化特征集。

3) 在特征降维方面，Fernandes等[62]利用主成分分析（PCA, principal components analysis）算法对流量特征化，通过降维来提取描述性的流量特征并滤除噪声。

特征学习方法是机器学习方法中连接特征工程与模型优化的桥梁。通过精心设计的特征集和恰当的学习方法，可以显著提升模型在各种场景下的检测准确性和泛化能力。尽管低层次特征学习面临着处理复杂数据的挑战，但它在提高模型性能方面发挥着不可或缺的作用。

3.2 基于深度学习方法的流量特征学习

自动特征学习方法，尤其是深度学习算法，能够有效解决传统机器学习方法中无法自动提取深层次特征表示的限制，提高了特征提取效率和准确性。对于网络流量的自动特征学习，其发展经历可以概括为以下4个阶段。

1) 基础模型发展阶段。例如，CNN在处理图像数据以及词嵌入技术处理文本数据方面得到了广泛应用[31,50]。而递归神经网络（RNN, recurrent neural network）及其变体长短期记忆（LSTM, long short-term memory）网络或门控循环单元能够有效地处理时间序列数据，解析流量表示数据分布、关系、模式及关联性等。Lucia等[15]使用一维CNN和前馈神经网络从原始网络流量字节中学习特征表示。

Sirinam 等[22]利用 CNN 学习数据包方向序列表示。Ma 等[27]选择具有高时间频率和空间泛化性的序列概要作为物联网（IoT, Internet of things）设备空闲状态流量的特征表示，通过 CNN 学习包级别的空间上下文信息。Garg 等[31]利用改进的 CNN 从转换为 RGB 图像的流量中抽象关键特征。随着技术跨领域应用，无监督语言模型能够推断网络元数据生成过程的自然选择。Sohi 等[57]利用 RNN 学习和提取未知语法规则，并生成属于相应语法规则的新序列。这些研究表明，时序特征学习对于识别周期性模式和预测未来流量趋势至关重要，空间特征分析为理解网络流量的静态结构提供了重要视角。上述基础模型分别针对不同类型的数据提供了有效的特征提取方法。

2) 模型融合与增强阶段。探索融合不同模型优势的方法以提升其在特定任务上的性能。Ahmed 等[36]利用基于 Dirichlet 过程的混合模型对流级别特征进行聚类分析，生成多模态概率分布以精确描述正常应用流量特征。该方法为网络流量的特征表示提供了新的视角。Roosmalen 等[47]利用深度神经网络和梯度下降自编码器，通过编解码过程学习数据的压缩表示并滤除噪声。Marín 等[59]设计了 DeepMAL 框架，利用 CNN 结合 LSTM 网络对有效载荷的固定位数字节进行自动特征抽象，CNN 学习数据包中的局部特征和流中的统计特征，然后通过 LSTM 网络处理序列数据，以理解数据包之间的时间顺序关系和数据流的动态变化行为。这些方法不仅提高了特征表示的质量，而且增强了模型对网络流量的理解能力和分类能力。

3) 图结构数据处理崛起阶段。随着图神经网络（GNN, graph neural network）和 GCN 的出现，自动特征学习能够高效处理复杂图结构数据，如 GNN 通过聚合邻居节点信息来更新每个节点特征表示，并捕捉复杂关系。Shen 等[33]基于 GNN 技术自动提取输入流量交互图的特征，将多层次流量模式映射到一个高维空间以区分不同的去中心化应用（DApp, decentralized application）流量。Premkumar 等[35]使用 GNN 和图嵌入算法创建每个图的低维向量表示，从而增强特征表示。

4) 综合应用与创新阶段。模型设计重点逐渐由基础模型的集成融合转向策略性的创新融合，以兼顾学习流量数据结构和模式的同时提升模型处理性能。Mirsky 等[45]开发的 kitsune 特征提取器能够从到达数据包中自动提取特征，创建描述性向量并通过自编码器集成的方式映射到神经网络。每个自编码器专注于捕捉特定子空间内的正常行为模式，降低了处理高维数据的复杂性，并易于随着网络流量的变化动态更新统计数据。Diallo 等[50]设计了自适应聚类模块，通过多核神经网络自动学习网络流量特征的低维嵌入表示。这种学习方法能够识别数据中的复杂结构和模式，在处理新数据时实现快速适应，以应对网络流量动态变化和新出现的攻击模式。为了解决实际流量与输入模型流量之间的差距，Qu 等[56]设计了一个与输入无关的层次深度学习框架，通过 5 种神经网络结构实现基于压缩的包向量序列到流映射。

基于上述分析可以得出，自动特征学习方法从学习流量的单一特征到能够兼容复杂行为模式并提升处理效率的演变，虽然与标准分类器相比，神经网络因参数数量、非线性激活、深度架构等原因导致训练时间更长，但考虑到人工设计特征时选择、构造、处理非线性和交互性等复杂性，额外的时间投入是可接受的。此外，特征提取框架需要将不同长度的输入序列转换为固定长度的向量，使设计的框架能够适应网络流量的动态特性，涉及时间窗口划分、序列填充或截断等技术。然而，此类框架的设计受限于协议模型，可能在处理并发的逻辑流时会因同步问题、上下文切换开销、资源竞争等原因导致效果降低。

流量表示的研究不仅要关注如何从原始数据中提取和学习有意义的特征向量，还需要考虑这些特征向量如何影响检测模型的学习过程。特征向量作为特征抽象的产物或特征学习的结果，其维度、噪声水平、可解释性等是影响检测模型学习的关键因素。首先，特征向量的维度和组成特征向量的相关性直接影响了模型的表示空间、学习与泛化能力。高维特征向量可能导致“维度灾难”[63]，而维度太低无法充分捕捉数据的复杂性。另外，组成特征之间的高相关性可能导致特征冗余，增加了模型训练的难度和计算成本。因此，亟须平衡表达能力和计算效率之间的关系，确保模型在有效学习的同时保持合理计算开销。此外，高维特征向量也需要与模型的复杂度相匹配，通过合适的模型选择和足够的训练数据避免过拟合，使其在实际应用中可能面

临数据采集和资源限制等挑战。

其次，特征向量的噪声水平会影响模型的鲁棒性和泛化能力，导致模型容易关注错误数据模式或不重要的变化。数值特征通常与量化指标有直接关联，但这些特征向量的噪声水平不一定低。相比之下，将数据转换为图像或处理为具有复杂结构的形式时，也可能会在特征提取中引入额外噪声，特别是提取了不相关或冗余的信息，需要进一步处理数据以净化特征向量并去除噪声。因此，在选择特征表示时，需要考虑特征向量的噪声水平及必要的预处理需求，以确保最终模型在实际应用中的检测性能和可靠性。

最后，特征向量的可解释性对于理解模型决策过程至关重要。数值特征向量的直观性在某些情况下更容易解释，但并不能总保证较高可解释性。图像数据通常由大量像素组成，每个像素点包含的颜色信息在原始形式下很难直接关联到模型的决策过程，但如果通过可视化技术，如映射图或者显著性分析图，则能够解释模型是如何关注图像的特定部分并做出决策的。类似地，图结构信息也需要理解边和节点是如何共同影响模型的输出，而不同类型的特征向量需要不同的解释性技术以确保结果的透明度和可信度。因此，需要在模型的可解释性和预测性能之间做出权衡，满足特定任务需求。

4 流量表示在异常检测中的应用

本节专注于探讨以网络流量特征表示为核心的异常检测算法，这些算法通过模式识别预测和识别潜在网络异常行为，主要从3个方面介绍网络流量表示在异常检测领域的研究现状，即传统机器学习方法、深度学习方法和混合方法应用，探讨它们与特征表示的关系。

4.1 基于传统机器学习方法的低层次流量特征的应用

首先，基于异常行为的检测主要依赖于无监督技术，侧重于使用历史正常流量数据建立用户行为模型，并通过检测与该模型的显著偏离来识别潜在的异常行为或威胁。Bhuyan等[40]提出了快速分布式特征提取和数据准备框架，侧重于结合多步离群值分析提升异常检测的效率，但受限于特征阈值和聚类参数的设置以及对训练数据量的依赖。Hamamoto等[41]结合GA和模糊逻辑提出了一种网络异常检测系统，该系统侧重于通过GA最优化网络行为预测模型并使用模糊逻辑评估网络行为，通过计算时间间隔的异常分数发出警报，提高检测的准确性并降低误报率。

其次，基于分类的检测主要依赖于监督学习技术，结合正常和异常的流量数据来训练分类器以区分正常行为和异常行为。Xu等[39]通过分析信息熵、包大小、包频率等特征，使用RF算法有效检测加密流量中的Eclipse攻击。RF算法作为一种集成学习方法，通过构建多个决策树并结合预测结果来提升分类的准确性，在面对复杂多变的网络攻击时，依然能够有效识别加密流量中的异常行为。

最后，基于分类与异常混合的检测方法结合了两者的优势，提供了复合检测过程，通常能够获得更高的检测准确性，并适应更广泛的应用范围。例如，Yang等[64]通过无监督聚类技术对良性流量进行聚类，再基于深度学习的框架进行未知攻击检测。这种与深度学习模型相结合的方法能够让传统机器学习方法的优势获得进一步发展。

4.2 基于深度学习方法的高层次流量特征的应用

传统机器学习方法在处理高维复杂特征方面存在一定局限性，特别是在检测的泛化能力方面。而深度学习方法可以解决这些限制，并且可以实现从原始数据到最终决策的直接映射[15,47,58-59]。通过训练神经网络识别加密流量的行为模式和元数据特征，可以实现对加密流量的识别和分类。同时，对于非加密流量，神经网络能够学习数据包的内容特征，从而进行有效检测和分类。

Radford等[48]通过LSTM网络学习流序列转换的单词序列，为正常行为建模，以有效识别恶意行为，结果表明该方法能够有效检测未知攻击，并减少对特征工程和阈值设定的依赖。Shen等[33]探索了基于GNN的分类器以识别加密流量，其在封闭和开放场景下的性能评估显示出优越的分类准确性，尤其是在处理背景噪声方面。尽管该模型训练时间可能较长，但检测执行效率较高。

应用端到端的检测方法简化了从数据到结果的流程，减少了人为干预，从而降低了任务中间步骤导致的误差积累。Lucia等[15]使用一维CNN自动提取网络流量中的原始字节特征，并通过多层全连接迭代学习来识别恶意流量。Marín等[59]的DeepMAL模型使用CNN直接从原始字节流数据中学习

恶意软件的表示，减少了额外的预处理或特征工程，在恶意软件流量检测和分类任务上优于传统的浅层模型。

4.3　基于混合方法的应用

当前研究中，一些高精确度检测方法在部署时面临诸多问题，包括资源和数据的可用性限制、专家经验及人工标注的限制、对未知攻击或零日漏洞的检测效果不佳，以及需要适应对抗技术不断发展[8]的挑战。为此，当前研究致力于开发轻量级、鲁棒性和泛化性强的异常检测模型，流量表示对于网络异常检测的性能优化至关重要，本节将介绍流量表示在4个具有代表性检测场景中的应用。

1) 端到端异常检测场景。Psathas 等[65]采用一种多模型融合方法，通过结合二维 CNN、RNN、LSTM 网络层以及多层感知器，形成了一个从数据捕获到分类的完整解决方案。这种自动化的流量表示及特征学习方法极大地提高了检测效率和准确性，并且拥有良好的可扩展性。

2) 边缘网络自适应场景。Diallo 等[50]提出了基于自适应聚类的入侵检测方法，将聚类中心作为额外的特征输入分类器，使系统能够适应网络的动态变化。该方法结合统计特征和语义特征的低维嵌入表示来区分不同流量类别，解决了流量特征对微小变化的敏感性问题，具有良好的鲁棒性和泛化能力。此外，在边缘网络环境中的自适应能力，使系统在资源受限情况下拥有快速响应并适应不断变化的网络威胁。

3) 上下文感知场景。Premkumar 等[35]基于 GNN 和图嵌入算法构建了对抗性入侵检测系统。将网络流量的每个数据包和它们之间的关系转换为图结构，利用节点和边表示网络实体间极其复杂的交互关系，从而对网络流量间的依赖和模式检测提供了丰富的上下文信息表示，这对检测的可解释性十分重要。

4) 实时流量监控与响应场景。Fu 等[66]将网络流量的统计性时序信息通过离散傅里叶变化转换到频域，利用频域特征表示流量的连续信息，使系统能够鲁棒地处理高吞吐量的网络数据，以快速应对包括复杂和隐蔽的各种攻击并保持较高的检测准确率。Wang 等[67]对流中数据包提取头部信息和有效载荷原始字节，并通过步幅切割转换为时间序列，使用线性投影和位置嵌入将步幅序列转换为模型可以处理的嵌入表示，进一步利用单向 Mamba 架构的状态空间模型有效处理序列数据，通过自监督预训练学习流量数据的通用表示。这种方法在预训练阶段使用大量无标记学习样本，但在微调阶段可以通过少量标记学习样本快速适应具体的下游任务，从而达到快速推理的目的。

4.4　不同流量表示方法在数据集上的表现

为了更清楚地说明基于不同信息维度的流量表示方法的检测性能，对比分析了 NetMamba[67]、MTC-MAE[68]等 12 种方法在 USTC-TFC2016、ISCXTor2016 等 9 个公开数据集上的表现。数据集涵盖了加密流量场景（包括常规加密流量和协议封装流量）和非加密流量场景，对比研究中的特征学习和检测方法包含传统机器学习方法、深度学习方法和混合方法。为避免不同研究在指标计算时因采用方法（如宏平均、加权平均等）不同而带来偏差，选用准确率作为评估指标（其中文献[37]中未计算准确率，用其精确度代替）。不同流量表示方法在数据集上的实验结果对比如表 2 所示。其中，√表示涉及该信息维度，空白表示未涉及该信息维度，—表示未对该数据集进行测试。

从表 2 中信息维度融合的趋势来看，时序信息和二进制/原始字节信息的流量表示与其他信息维度结合率最高。融合了这 2 种维度信息流量表示的检测方法在 ISCXTor2016 数据集上获得了最佳准确率，这表明对加密封装混合流量场景的检测有效。而且包含这 2 种信息维度流量表示的检测方法在其他数据集上也具有较高的检测准确率和稳定性。文献[37]对数据包级别的流量表示采用对齐策略，具体为每个比特都包含在表示中，表示中的每个位置具有相同含义且表示大小相同。文献[72]基于 burst 进行流量表示，然后使用 bi-gram 模型将十六进制数据包转换为 token 嵌入。文献[67]将原始流量分层信息基于步长（stride）表示，嵌入的流量步长对编码器可见。这些研究表明，鲁棒的流量表示应包含原始流量的头部信息和有效载荷信息，采用预处理技术（包括但不限于对齐、转换等）使流量特征表示在嵌入模型之前能够以一种有意义的方式被处理和表示。

综上所述，本节讨论了网络流量异常检测中不同方法的应用和挑战。传统机器学习方法在处理高维特征学习和检测泛化性方面存在局限性。相比之

表 2 不同流量表示方法在数据集上的实验结果对比

文献	信息维度							学习模型		数据集准确率									备注
	统计信息	时序信息	图结构信息	语义信息	指纹信息	二进制/原始字节信息	图像/矩阵信息	传统机器学习	深度学习	KDD 99	NSL-KDD	ISCX-IDS 2012	UNSW-NB15	CIC-IDS 2017	CSE-CIC-IDS 2018	ISCX Tor 2016	ISCX VPN 2016	USTC-TFC 2016	
文献[58]						√			√	—	—	—	—	—	—	—	—	87.7%	
文献[69]						√	√		√	—	—	—	—	98.67%	—	—	—	—	
文献[37]		√			√	√	√	√	√	—	—	—	—	100%	—	—	—	—	
文献[50]	√	√		√					√	100%	—	100%	—	—	100%	—	—	—	
文献[70]	√	√					√		√	—	90.67%	95.333%	96.344%	—	—	—	—	—	
文献[71]	√	√	√					√	√	—	98.67%	97.003%	98.667%	—	98.25%	—	—	—	
文献[72]		√				√			√	—	—	—	—	—	—	83.11%	97.29%	99.29%	流
										—	—	—	—	—	—	99.21%	98.9%	99.15%	包
文献[73]			√			√			√	—	—	—	—	—	—	—	98.86%	95.91%	
文献[74]						√	√	√	√	—	—	—	—	—	—	99.72%	98.07%	97.86%	
文献[35]	√	√	√					√	√	—	—	—	—	99.95%	—	—	—	—	流
										—	—	—	—	98.92%	—	—	—	—	包
文献[67]		√		√		√			√	—	—	—	—	—	—	99.93%	98.99%	99.9%	
文献[68]							√		√	—	—	—	—	—	—	—	77.33%	98.43%	

下，深度学习方法虽然在特征学习和泛化能力上优势显著，但同时也面临着数据需求大、模型复杂度高、决策过程缺乏可解释性等挑战。鉴于深度学习方法的高计算成本和对硬件资源的依赖性，在实际部署中需要进一步优化。

5　未来研究展望

结合前文所述网络异常检测中的流量表示、学习、检测技术发展趋势及研究进展，未来研究需要在数据采集技术、异常识别智能算法、适应网络环境变化的协同模式、推动协同模式的标准化和兼容性以及表示、学习、检测耦合技术的深度整合等方面进行深入探索。

5.1　多维度跨层次的流量表示

未来的流量表示方法设计要能够适应正常的网络演进、网络策略的调整或用户行为模式的变化等，最小化信息损失的同时，最大化对信息内容的理解。

首先，可以开发层次化的流量表示框架，该框架将时间依赖、空间关联和语义结构信息作为独立的分析维度，同时保持这些维度之间的内在联系。通过这种解耦但相互关联的方法，构建一种在流量表示上的“多模态”视角，并通过对各类信息有偏好的学习方法进一步抽象高层次特征表示。例如，网络层侧重于表示数据包的传输顺序、生存时间限制以及路由变化的响应时间等，这些特征与时间依赖性紧密联系，因此可以探索如何利用时间卷积网络等基于时间序列分析的算法，深入理解和预测这些动态的时间依赖性关系。传输层侧重于表示不同服务或应用程序通过 IP 地址和端口区分的数据包以及业务传输状态，可以集中开发和优化如 SVM、CNN 等算法，提高对不同数据包分类的准确性和效率。应用层侧重于表示对特定应用程序的请求和响应格式，以及解读网络流量背后的实际意图，可以采用自然语言处理技术，如利用 Bert 模型分析和理解应用层数据的语义内容，从而更准确地捕捉和解释网络行为的意图和模式。

其次，可以开发信息融合算法，如卡尔曼滤波的非线性和非高斯噪声模型的改进方案，以联邦卡尔曼滤波（FKF, federated Kalman filter）的应用为例[75]，若干子系统执行局部卡尔曼滤波，而后子系统之间通过某种协议，如事件驱动的信息交换或周期性协议，共享必要的信息以进行联合估计，从而整合网络层、传输层和应用层的流量信息。此外，构建分布式系统架构，使在不同计算节点上能够进行并行处理，利用各层次在数据采集、特征提取和行为分析方面的优势来平衡流量表示效率，从而高效地开展分布式检测任务。例如，利用包级别头部特征快速筛选算法，如哈希匹配算法，分类流量应用类别。流级别特征应用异常检测算法，如孤立森林算法，及时发现并过滤掉快速攻击。会话级别特征利用深度学习技术，如 RNN 算法，感知流量意图和模式。被滤出的流量再尝试高级载荷分析技术，如协议状态机和行为分析，进一步识别潜在攻击。

最后，设计多模态学习框架，它能够处理结构化数据和非结构化数据以形成全面的流量视图。以 2 种流量特征表示为例，可以采用基于张量低秩分解的方法[76-77]来融合不同层次的流量特征。具体地，将原始数据表示为一个三维张量，其中 2 个维度对应不同的流量特征，第 3 个维度对应时间序列。应用张量低秩分解方法，通过求解优化问题来最小化原始张量与分解后张量之间的差异，从而找到最佳的因子矩阵和核心张量，以提取出关键特征，并利用正则化方法将张量低秩分解后的低维表示进行特征融合，使其具有多模态数据的互补性并采用时间序列和空间分析算法捕捉时间和空间的依赖关系，以保证数据在时间和空间上的一致性。

5.2　自适应可解释的流量表示

从提升适应性和灵活性的角度出发，实施基于流量波动和异常检测算法反馈的自适应数据采集机制，以动态调整采集频率和粒度从而减少冗余数据采集。设计自动化的特征选择和提取策略，根据实时流量模式动态选择最相关的特征，优化处理流程采用流式计算框架实现实时性分析。同时利用高效的数据结构和算法，如哈希索引，减少计算资源和存储成本消耗。例如，使用自适应哈希索引能够在内存中基于 B-Tree 索引的基础上创建哈希索引，进一步提升查询效率[78]。在流量分析中，可以采用这种哈希索引快速定位和处理数据包，从而提高整体系统的响应速度和处理能力，其动态调整特性能够适应流量模式实时变化。

此外，也可从提高可解释性和可扩展性的角度出发，设计模块化的流量表示框架，使系统关键组

件支持独立更新，从而使流量表示能够灵活适应新的研究进展。同时兼容增量学习机制，如采用在线随机梯度下降，可以通过一次仅训练一个样本的方式，根据样本标注的反馈更新参数[79]。使模型有效更新以适应流量的持续动态变化，提高模型对新数据的适应性和响应速度。并通过设计策略来平衡新旧数据对模型训练的影响，以避免模型对新数据的过度拟合，确保模型的泛化能力和长期稳定性。

应用流量表示与模型决策的可解释技术，如利用局部可解释的模型无关解释（LIME, local interpretable model-agnostic explanation）[80]揭示决策过程与特征重要度分析，设计反馈机制将检测和分析结果用于前端策略的制定和调整。同时遵循标准化的数据格式和协议，如NetFlow可与其他网络监控工具进行集成。

具体案例可采用基于Bert的大语言模型（LLM, large language model）方法。以TF-LLM为例，该方法通过将多模态数据转换为文本提示，然后微调LLM以生成解释性输出[81]。在网络流量分析中，可以采用类似策略，将流量数据转换为描述性的语义信息，并利用预训练的LLM预测和解释流量变化。通过指令微调学习不同流量分析指令的可区分性表示，为不同类别流量学习恰当的嵌入，进而在特征空间中形成清晰边界，有助于提高流量检测任务的准确性。

5.3 对抗性攻击下的鲁棒性流量表示

扰动可能源自攻击者的策略[82]，针对攻击者可能利用算法生成在视觉上或统计上与正常流量相似的对抗性样本来欺骗机器学习模型的问题，流量表示的鲁棒性设计不仅要提高对故意扰动的识别能力，还需要深入理解攻击模式。研究表明，通过提供上下文信息可以显著提高LLM对抗视觉对抗性输入的鲁棒性[83]。例如，在模型中集成一个反馈机制，当检测到对抗性样本时，该机制可以触发参数调整，从而优化模型的决策边界以减少未来的误报。

在设计鲁棒性流量表示时，通过限制输入特征空间或简化模型结构，减少模型的潜在攻击面，从而降低被对抗性样本欺骗的风险。研究表明，在图像分类任务中可以预先处理图像，移除异常像素或使用图像增强技术减少对抗性扰动的影响[83]。类似地，在流量检测任务中，可以在流量表示过程中滤除噪声并进行特征增强，从而增强模型在对抗攻击下的鲁棒性。

最后，提高模型的可解释性和透明度对于分析和理解模型在面对对抗性样本时的行为至关重要，这可以通过理论分析鲁棒性的数学定义和界限来实现，从而指导如何设计与改进流量表示。与通用的异常检测技术相比，对抗性鲁棒性表示还需要结合多模态和多任务学习，以提高模型对于复杂攻击场景的泛化能力。这与多维度跨层次流量表示中对数据深度分析的需求，以及自适应可解释流量表示中对模型透明度和可解释性的需求是一致的。这些方法共同强化了流量分析的多级别粒度协同，以及异常检测中流量表示、学习和检测3个环节间的紧密耦合，从而提升流量分析的整体性能。

6 结束语

本文立足于网络异常检测中的流量表示技术，首先，以检测流程为引线，介绍了异常检测中流量分析的多级别粒度的协同与耦合关系，以及异常检测中的流量表示、学习、检测3个环节间的耦合关系。随后，系统地审视了流量表示在异常检测领域的发展轨迹，从流量表示形式、流量特征学习、流量表示在异常检测中的应用3个方面回顾了国内外研究现状，并分析了现有研究面临的问题。最后，对流量表示未来的发展趋势进行了展望，期望能够为研究人员提供一个全面深入的视角来理解和改进网络异常检测领域的流量表示。

参考文献：

[1] JING X Y, YAN Z, PEDRYCZ W. Security data collection and data analytics in the Internet: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 586-618.

[2] 冯光升, 蒋舜鹏, 胡先浪, 等. 面向物联网的入侵检测技术研究新进展[J]. 信息网络安全, 2024, 24(2): 167-178.
FENG G S, JIANG S P, HU X L, et al. New research progress on intrusion detection techniques for the Internet of things[J]. Netinfo Security, 2024, 24(2): 167-178.

[3] MILLS R, MARNERIDES A K, BROADBENT M, et al. Practical intrusion detection of emerging threats[J]. IEEE Transactions on Network and Service Management, 2022, 19(1): 582-600.

[4] THUDUMU S, BRANCH P, JIN J, et al. A comprehensive survey of anomaly detection techniques for high dimensional big data[J]. Journal of Big Data, 2020, 7(1): 42.

[5] HOJJATI H, HO T K K, ARMANFARD N. Self-supervised anomaly detection in computer vision and beyond: a survey and outlook[J]. Neural Networks, 2024, 172: 106106.

[6] ALEESA A M, ZAIDAN B B, ZAIDAN A A, et al. Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions[J]. Neural Computing and Applications, 2020, 32(14): 9827-9858.

[7] TU B T, ZHAO Y, YIN G X, et al. Research on intelligent calculation method of intelligent traffic flow index based on big data mining[J]. International Journal of Intelligent Systems, 2022, 37(2): 1186-1203.

[8] 侯剑, 鲁辉, 刘方爱, 等. 加密恶意流量检测及对抗综述[J]. 软件学报, 2024, 35(1): 333-355.
HOU J, LU H, LIU F A, et al. Detection and countermeasure of encrypted malicious traffic: a survey[J]. Journal of Software, 2024, 35(1): 333-355.

[9] 付钰, 王坤, 段雪源, 等. 面向软件定义网络的异常流量检测研究综述[J]. 通信学报, 2024, 45(3): 208-226.
FU Y, WANG K, DUAN X Y, et al. Survey of research on abnormal traffic detection for software defined networks[J]. Journal on Communications, 2024, 45(3): 208-226.

[10] UMER M A, JUNEJO K N, JILANI M T, et al. Machine learning for intrusion detection in industrial control systems: applications, challenges, and recommendations[J]. International Journal of Critical Infrastructure Protection, 2022, 38: 100516.

[11] MALDONADO J, RIFF M C, NEVEU B. A review of recent approaches on wrapper feature selection for intrusion detection[J]. Expert Systems with Applications, 2022, 198: 116822.

[12] SARHAN M, LAYEGHY S, PORTMANN M. Evaluating standard feature sets towards increased generalisability and explainability of ML-based network intrusion detection[J]. Big Data Research, 2022, 30: 100359.

[13] RUDMAN L, IRWIN B. Characterization and analysis of NTP amplification based DDoS attacks[C]//Proceedings of the 2015 Information Security for South Africa (ISSA). Piscataway: IEEE Press, 2015: 1-5.

[14] HOSSEINI S M, JAHANGIR A H. An effective payload attribution scheme for cybercriminal detection using compressed bitmap index tables and traffic downsampling[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(4): 850-860.

[15] LUCIA M J D, MAXWELL P E, BASTIAN N D, et al. Machine learning raw network traffic detection[C]//Proceedings of the Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III. SPIE, 2021, 11746: 185-194.

[16] STABILI D, FERRETTI L, ANDREOLINI M, et al. DAGA: detecting attacks to in-vehicle networks via N-gram analysis[J]. IEEE Transactions on Vehicular Technology, 2022, 71(11): 11540-11554.

[17] FU Z Q, LIU M X, QIN Y, et al. Encrypted malware traffic detection via graph-based network analysis[C]//Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses. New York: ACM Press, 2022: 495-509.

[18] WU H, WU Q Y, CHENG G, et al. SFIM: identify user behavior based on stable features[J]. Peer-to-Peer Networking and Applications, 2021, 14(6): 3674-3687.

[19] 郝唯杰. 工业网络流量异常智能分析与动态安全策略[D]. 杭州: 浙江大学, 2022.
HAO W J. Intelligent analysis and dynamic security strategy of industrial network traffic anomaly[D]. Hangzhou: Zhejiang University, 2022.

[20] GUPTA A, GUPTA H P, DUTTA T. A deep learning based traffic flow classification with just a few packets[C]//Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2021: 1-2.

[21] ZHOU J T, ZHANG H, JIN D, et al. Dual adversarial transfer for sequence labeling[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 43(2): 434-446.

[22] SIRINAM P, IMANI M, JUAREZ M, et al. Deep fingerprinting: undermining website fingerprinting defenses with deep learning[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1928-1943.

[23] KIM J, MONACO J V. User identification in dynamic web traffic via deep temporal features[C]//Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW). Piscataway: IEEE Press, 2021: 282-290.

[24] 陈兴蜀, 陈敬涵, 邵国林, 等. 基于会话流聚合的隐蔽性通信行为检测方法[J]. 电子科技大学学报, 2019, 48(3): 388-396.
CHEN X S, CHEN J H, SHAO G L, et al. A covert communication behavior detection method based on session flow aggregation[J]. Journal of University of Electronic Science and Technology of China, 2019, 48(3): 388-396.

[25] 巩思越, 刘辉, 王宝会. 基于会话统计编码器的恶意加密流量检测方法研究[J]. 计算机科学, 2024, 51(11): 340-346.
GONG S Y, LIU H, WANG B H. Malicious encrypted traffic detection method based on conversation statistical encoder model[J]. Computer Science, 2024, 51(11): 340-346.

[26] ENGELEN G, RIMMER V, JOOSEN W. Troubleshooting an intrusion detection dataset: the CICIDS2017 case study[C]//Proceedings of the 2021 IEEE Security and Privacy Workshops (SPW). Piscataway: IEEE Press, 2021: 7-12.

[27] MA X B, QU J, LI J F, et al. Pinpointing hidden IoT devices via spatial-temporal traffic fingerprinting[C]//Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 894-903.

[28] WANG W, ZHU M, WANG J L, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Piscataway: IEEE Press, 2017: 43-48.

[29] ANEJA S, ANEJA N, ISLAM M S. IoT device fingerprint using deep learning[C]//Proceedings of the 2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS). Piscataway: IEEE Press, 2018: 174-179.

[30] XU C Y, SHEN J Z, DU X. A method of few-shot network intrusion detection based on meta-learning framework[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3540-3552.

[31] GARG S, KAUR K, KUMAR N, et al. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks[J]. IEEE Transactions on Network and Service Management, 2019, 16(3): 924-935.

[32] SHAPIRA T, SHAVITT Y. FlowPic: a generic representation for encrypted traffic classification and applications identification[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1218-1232.

[33] SHEN M, ZHANG J P, ZHU L H, et al. Accurate decentralized application identification via encrypted traffic analysis using graph neural networks[J]. IEEE Transactions on Information Forensics and Security,

2021, 16: 2367-2380.

[34] MONGKOLLUKSAMEE S, VISOOTTIVISETH V, FUKUDA K. Combining communication patterns & traffic patterns to enhance mobile traffic identification performance[J]. Journal of Information Processing, 2016, 24(2): 247-254.

[35] PREMKUMAR A, SCHNEIDER M, SPIVEY C, et al. Graph representation learning for context-aware network intrusion detection[C]//Proceedings of the Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V. SPIE, 2023, 12538: 82-92.

[36] 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.

[37] HOLLAND J, SCHMITT P, FEAMSTER N, et al. New directions in automated traffic analysis[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2021: 3366-3383.

[38] ZOLOTUKHIN M, HÄMÄLÄINEN T, KOKKONEN T, et al. Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic[C]//Proceedings of the 2016 23rd International Conference on Telecommunications (ICT). Piscataway: IEEE Press, 2016: 1-6.

[39] XU G Q, GUO B J, SU C H, et al. Am I eclipsed? A smart detector of eclipse attacks for Ethereum[J]. Computers & Security, 2020, 88: 101604.

[40] BHUYAN M H, BHATTACHARYYA D K, KALITA J K. A multi-step outlier-based anomaly detection approach to network-wide traffic[J]. Information Sciences, 2016, 348: 243-271.

[41] HAMAMOTO A H, CARVALHO L F, SAMPAIO L D H, et al. Network anomaly detection system using genetic algorithm and fuzzy logic[J]. Expert Systems with Applications, 2018, 92: 390-402.

[42] WANG T, CAI X, NITHYANAND R, et al. Effective attacks and provable defenses for website fingerprinting[C]//Proceedings of the 23rd USENIX Conference on Security Symposium. Berkeley: USENIX Association, 2014: 143-157.

[43] ZHAO S C, LI W, ZIA T, et al. A dimension reduction model and classifier for anomaly-based intrusion detection in Internet of things[C]//Proceedings of the 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). Piscataway: IEEE Press, 2017: 836-843.

[44] MSADEK N, SOUA R, ENGEL T. IoT device fingerprinting: machine learning based encrypted traffic analysis[C]//Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2019: 1-8.

[45] MIRSKY Y, DOITSHMAN T, ELOVICI Y, et al. Kitsune: an ensemble of autoencoders for online network intrusion detection[C]//Proceedings 2018 Network and Distributed System Security Symposium. Reston: Internet Society, 2018.

[46] DAVID J, THOMAS C. DDoS attack detection using fast entropy approach on flow-based network traffic[J]. Procedia Computer Science, 2015, 50: 30-36.

[47] ROOSMALEN J V, VRANKEN H, EEKELEN M V. Applying deep learning on packet flows for botnet detection[C]//Proceedings of the 33rd Annual ACM Symposium on Applied Computing. New York: ACM Press, 2018: 1629-1636.

[48] RADFORD B J, APOLONIO L M, TRIAS A J, et al. Network traffic anomaly detection using recurrent neural networks[J]. arXiv Preprint, arXiv: 1803.10769, 2018.

[49] LIU Y X, LI Z, PAN S R, et al. Anomaly detection on attributed networks via contrastive self-supervised learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(6): 2378-2392.

[50] DIALLO A F, PATRAS P. Adaptive clustering-based malicious traffic classification at the network edge[C]//Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[51] MA X B, QU J, LI J F, et al. Inferring hidden IoT devices and user interactions via spatial-temporal traffic fingerprinting[J]. IEEE/ACM Transactions on Networking, 2022, 30(1): 394-408.

[52] PERDISCI R, PAPASTERGIOU T, ALRAWI O, et al. IoTFinder: efficient large-scale identification of IoT devices via passive DNS traffic analysis[C]//Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2020: 474-489.

[53] MAITI R R, SIBY S, SRIDHARAN R, et al. Link-layer device type classification on encrypted wireless traffic with COTS radios[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2017: 247-264.

[54] SHEN M, LIU Y T, ZHU L H, et al. Fine-grained webpage fingerprinting using only packet length information of encrypted traffic[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2046-2059.

[55] LI J F, ZHOU H, WU S H, et al. FOAP: fine-grained open-world android app fingerprinting[C]//31st USENIX Security Symposium (USENIX Security 22). Berkeley: USENIX Association, 2022: 1579-1596.

[56] QU J, MA X B, LI J F, et al. An input-agnostic hierarchical deep learning framework for traffic fingerprinting[C]//32nd USENIX Security Symposium. Berkeley: USENIX Association, 2023: 589-606.

[57] SOHI S M, SEIFERT J P, GANJI F. RNNIDS: enhancing network intrusion detection systems through deep learning[J]. Computers & Security, 2021, 102: 102151.

[58] LOTFOLLAHI M, JAFARI SIAVOSHANI M, SHIRALI HOSSEIN ZADE R, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.

[59] MARÍN G, CAASAS P, CAPDEHOURAT G. DeepMAL-deep learning models for malware traffic detection and classification[C]//Data Science-Analytics and Applications: Proceedings of the 3rd International Data Science Conference-iDSC2020. Berlin: Springer, 2021: 105-112.

[60] 王勇, 周慧怡, 俸皓, 等. 基于深度卷积神经网络的网络流量分类方法[J]. 通信学报, 2018, 39(1): 14-23.
WANG Y, ZHOU H Y, FENG H, et al. Network traffic classification method basing on CNN[J]. Journal on Communications, 2018, 39(1): 14-23.

[61] MAXWELL P, ALHAJJAR E, BASTIAN N D. Intelligent feature engineering for cybersecurity[C]//Proceedings of the 2019 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2019: 5005-5011.

[62] FERNANDES G, CARVALHO L F, RODRIGUES J J P C, et al. Net-

work anomaly detection using IP flows with principal component analysis and ant colony optimization[J]. Journal of Network and Computer Applications, 2016, 64: 1-11.

[63] BERISHA V, KRANTSEVICH C, HAHN P R, et al. Digital medicine and the curse of dimensionality[J]. NPJ Digital Medicine, 2021, 4(1): 153.

[64] YANG J, CHEN X, CHEN S W, et al. Conditional variational autoencoder and extreme value theory aided two-stage learning approach for intelligent fine-grained known/unknown intrusion detection[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3538-3553.

[65] PSATHAS A P, ILIADIS L, PAPALEONIDAS A, et al. COREM2 project: a beginning to end approach for cyber intrusion detection[J]. Neural Computing and Applications, 2022, 34(22): 19565-19584.

[66] FU C P, LI Q, SHEN M, et al. Frequency domain feature based robust malicious traffic detection[J]. IEEE/ACM Transactions on Networking, 2023, 31(1): 452-467.

[67] WANG T Z, XIE X H, WANG W D, et al. NetMamba: efficient network traffic classification via pre-training unidirectional mamba[J]. arXiv Preprint, arXiv: 2405.11449, 2024.

[68] XU K, ZHANG X X, WANG Y, et al. Self-supervised learning malware traffic classification based on masked autoencoder[J]. IEEE Internet of Things Journal, 2024, 11(10): 17330-17340.

[69] SUN P F, LIU P J, LI Q, et al. DL-IDS: extracting features using CNN-LSTM hybrid network for intrusion detection system[J]. Security and Communication Networks, 2020, 2020: 8890306.

[70] 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.

[71] KANNA P R, SANTHI P. Hybrid intrusion detection using MapReduce based black widow optimized convolutional long short-term memory neural networks[J]. Expert Systems with Applications, 2022, 194: 116545.

[72] LIN X J, XIONG G, GOU G P, et al. ET-BERT: a contextualized datagram representation with pre-training transformers for encrypted traffic classification[C]//Proceedings of the ACM Web Conference. New York: ACM Press, 2022: 633-642.

[73] ZHANG H Z, YU L, XIAO X, et al. TFE-GNN: a temporal fusion encoder using graph neural networks for fine-grained encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2023. New York: ACM Press, 2023: 2066-2075.

[74] ZHAO R J, ZHAN M W, DENG X W, et al. Yet another traffic classifier: a masked autoencoder based traffic transformer with multi-level flow representation[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2023, 37(4): 5420-5427.

[75] XU X B, PANG F L, RAN Y Y, et al. An indoor mobile robot positioning algorithm based on adaptive federated Kalman filter[J]. IEEE Sensors Journal, 2021, 21(20): 23098-23107.

[76] JANG J G, KANG U. D-tucker: fast and memory-efficient tucker decomposition for dense tensors[C]//Proceedings of the 2020 IEEE 36th International Conference on Data Engineering (ICDE). Piscataway: IEEE Press, 2020: 1850-1853.

[77] ZHOU S, ERFANI S, BAILEY J. Online CP decomposition for sparse tensors[C]//Proceedings of the 2018 IEEE International Conference on Data Mining (ICDM). Piscataway: IEEE Press, 2018: 1458-1463.

[78] LIU Z X, CHEN S M. Pea hash: a performant extendible adaptive hashing index[J]. Proceedings of the ACM on Management of Data, 2023, 1(1): 1-25.

[79] 史加荣, 王丹, 尚凡华, 等. 随机梯度下降算法研究进展[J]. 自动化学报, 2021, 47(9): 2103-2119.
SHI J R, WANG D, SHANG F H, et al. Research advances on stochastic gradient descent algorithms[J]. Acta Automatica Sinica, 2021, 47(9): 2103-2119.

[80] RIBEIRO M T, SINGH S, GUESTRIN C."Why should I trust you?": explaining the predictions of any classifier[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2016: 1135-1144.

[81] GUO X S, ZHANG Q M, JIANG J Y, et al. Towards explainable traffic flow prediction with large language models[J]. arXiv Preprint, arXiv: 2404.02937, 2024.

[82] HAN D Q, WANG Z L, ZHONG Y, et al. Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors[J]. IEEE Journal on Selected Areas in Communications, 2021, 39(8): 2632-2647.

[83] CUI X M, APARCEDO A, JANG Y K, et al. On the robustness of large multimodal models against image adversarial attacks[C]//Proceedings of the 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE Press, 2024: 24625-24634.

[作者简介]

孙剑文（1988– ），女，北京人，信息工程大学博士生、工程师，主要研究方向为网络流量异常检测、机器学习等。

张斌（1969– ），男，河南南阳人，博士，信息工程大学教授、博士生导师，主要研究方向为信息系统安全等。

常禾雨（1993– ），女，河南郑州人，博士，信息工程大学助理研究员，主要研究方向为人工智能安全、网络信息防御。