

基于多视角异构图的上下文感知 加密恶意流量检测

王翔宇, 芦 斌, 杨青洲, 杨煜吉, 李 玎

(信息工程大学, 河南 郑州 450001)

摘要: 针对现有加密恶意流量检测方法存在的依赖单视角特征、多视角特征融合方法低效等问题, 提出基于多视角异构图学习的加密恶意流量检测方法(MHC-GNN)。首先, MHC-GNN 引入 TLS 证书特征和 IP 特征, 与流量统计特征进行异构图建模。其次, MHC-GNN 利用基于元路径的特征信息聚合机制, 动态融合多视角上下文信息, 生成具有高判别力的流嵌入向量, 从而实现加密恶意流量的精准检测。实验结果表明, 该方法在 CIC-IDS2017 数据集上的 $F1$ 分数为 99.7%, 在 CIC-DDoS2019 数据集上的 $F1$ 分数为 95.7%, 整体优于多种基于图的基线方法, 说明了该方法在加密恶意流量检测任务中的有效性。

关键词: 加密流量分析; 恶意流量检测; 异构图; 上下文感知; 图注意力网络

中图分类号: TP393.08

文献标识码: A

文章编号: 1671-0673(2026)02-0208-08

Context-Aware Encrypted Malicious Traffic Detection Based on Multi-Perspective Heterogeneous Graphs

WANG Xiangyu, LU Bin, YANG Qingzhou, YANG Yuji, LI Ding

(Information Engineering University, Zhengzhou 450001, China)

Abstract: To address the limitations of existing encrypted malicious traffic detection method such as reliance on single-view features and inefficient multi-view feature fusion techniques, the multi-view heterogeneous context graph neural network (MHC-GNN) is proposed for encrypted traffic threat detection. First, in MHC-GNN TLS certificate features and IP features are incorporated into heterogeneous graph modeling alongside traffic statistical features. Second, a multi-path feature fusion mechanism based on meta-paths is employed to dynamically integrate multi-view contextual information and generate highly discriminative flow embedding vectors that enables precise detection of encrypted malicious traffic. Experiments demonstrate that the proposed method achieves an $F1$ score of 99.7% on CIC-IDS2017 dataset and 95.7% on CIC-DDoS2019 dataset, outperforming multiple baseline graph-based methods overall. This verifies the framework's effectiveness for detecting encrypted malicious traffic.

Key words: encrypted traffic analysis; malicious traffic detection; heterogeneous graphs; context-aware; graph attention networks

近年来,随着全球范围的对隐私和数据安全的日益关注,流量加密已成为互联网通信的常态。据谷歌数据统计,如今超过 94% 的网络流量使用

加密协议来进行通信^[1]。越来越多的攻击利用加密信道进行恶意活动,而传统的基于深度包检测的技术无法有效解析加密载荷,导致这些隐藏在

加密信道中的潜在威胁很难被检测出来^[2]。在诸多加密协议中,TLS协议因其能够很好地保护传输数据的安全性和完整性,在实际网络中得到了广泛的部署。根据MITRE的报告^[3],过去几年的许多网络攻击都与TLS协议有关。因此,目前迫切需要研究针对TLS协议的加密恶意流量检测方法。

近年来,许多研究选择机器学习算法和深度学习算法进行加密恶意流量检测。然而这类加密恶意流量检测方法存在两方面的不足。首先,这些方法^[4-8]大多仅仅提取与流相关的统计特征,而忽略了从其他视角提取的可以作为补充信息的辅助特征。目前有研究^[9]从TLS特征、数据元统计特征和上下文数据3个方面提取特征进行分析,证明TLS特征和上下文数据对于检测模型性能的提升有重要贡献。其次,这些方法还存在多视角特征融合方法不合理的问题。现有方法大多没有充分融合和利用流量中的TLS证书与IP的信息,未能将这些实体及其特征进行统一建模,限制了模型对加密恶意流量的多维度感知能力。

为解决上述不足,构建MHC-GNN(Multi-view Heterogeneous Context Graph Neural Network)方法。该方法先将目标流量构建为一个由TLS证书、IP端点和流构成的三元异构图。在此基础上,再基于元路径的特征信息聚合机制,使得流节点能动态聚合邻居节点的上下文信息。最后,再提取流节点的嵌入向量输入到下游分类器中,进而实现加密恶意流量的高精度检测。

1 相关工作

恶意流量检测对于构建安全稳定的网络环境意义重大,正因为此,研究人员目前越来越关注加密恶意流量的检测。现有的加密恶意流量检测方法主要可分为两大类:基于统计特征的方法、基于图学习的方法。

1.1 基于统计特征的方法

这类方法依赖大量先验知识提取所需要的流级特征,并利用传统机器学习模型或深度学习模型进行分类。文献[10-12]针对依赖手工特征的机器学习方法,提出不同的流量数据处理的方法,在无需专家知识特征的前提下,实现对加密流量的分类。

1.2 基于图学习的方法

由于图方法具有强大的建模节点间复杂依赖关系和结构性信息的能力,学者们正深入研究基

于图的方法在加密流量分类领域的应用。

GraphDApp^[13]方法首次将图神经网络(Graph Neural Network, GNN)引入加密流量识别领域。ST-Graph^[14]框架通过图表示学习算法探索网络行为的空间和时间特征并集成所有可用信息,以实现加密恶意流量的检测。文献[15-16]从基于流构图转向基于数据包构图,将数据包中的数据对应图中的节点,构建出规模受控的图,提升了模型的检测效率。文献[17]通过分析流的统计特征和基于流量构建出的通信图的特征,得出相应的分数,再基于得分投票得到最终的流量检测结果。文献[18]将每个加密会话作为一个节点,基于会话的图像特征相似度构建K-NN(K-Nearest Neighbors)图,并将向量化特征作为节点属性,再利用GraphSAGE模型进行学习。文献[19]提出的上下文感知网络入侵检测方法,将网络流量在流级别和包级别分别建模为有向无环图,以数据包为节点、包间余弦相似度为边属性,通过图神经网络和FEATHER算法提取图嵌入向量,并与传统流特征拼接后用于二分类。文献[20]将流量区分为短流和长流,对短流进行聚合以减小图的规模,对长流进行特征分布拟合以保留高保真度的交互信息,再通过连通分量分析、边预聚类、关键顶点求解和交互模式聚类步骤实现无监督的异常检测。文献[21]针对传统方法对包头和有效载荷的关注度相同以及未能挖掘字节间的潜在相关性,提出基于图神经网络进行细粒度加密流量分类方法。文献[22]将IP地址作为节点,流作为边构建图,再通过GNN模型学习节点间的关系和节点与边之间的关系,最后将融合了节点间关系和节点与边之间关系的嵌入向量送入到下游的随机森林分类器中,实现高精度的恶意流检测。文献[23]构建流量关系多图,通过图注意力网络选择性地融合上下文信息,并通过迭代优化校正误导性关系,以提升在对抗条件下的检测鲁棒性。文献[24]使用流量图抽象表示流内部的包关系结构,并针对环境迁移场景设计了自适应分类方法。

以上方法尽管一定程度上能实现加密流量的分类,但仍存在以下不足:首先,大多数方法仅考虑流这一单视角的特征,没有考虑TLS证书和IP地址这两类实体的信息;其次,利用多视角特征的方法对于这些多视角特征的融合方式较为简单。虽然有诸如SnifferDog^[22]的方法将IP节点与流一同构建为图,考虑了利用不同视角的特征信息,但这

些方法仅通过简单拼接的方式融合节点和边的嵌入,未考虑在不同攻击类型下的IP特征信息提供的贡献是可能存在显著差异的。

2 MHC-GNN设计

如图1所示,MHC-GNN由4个紧密耦合的模块构成:数据预处理、异构图建模、图表示学习以及恶意性判别。

首先,数据预处理阶段将原始网络数据转换

为训练需要的流量数据。其次,异构图建模阶段将流量数据映射为结构化的异构图。然后,图表示学习阶段利用预定义的元路径捕获多源上下文信息以更新流嵌入向量。最后,恶意性判别阶段将流嵌入向量输入至多层感知机(Multilayer Perceptron, MLP)分类器,实现对加密流量的恶意性判别。需要注意的是,图中的 m, n, q 分别为异构图中的Flow、IP、TLS节点的数量, f_1, f_2, f_3 分别代表Flow、IP、TLS节点的原始特征维度。

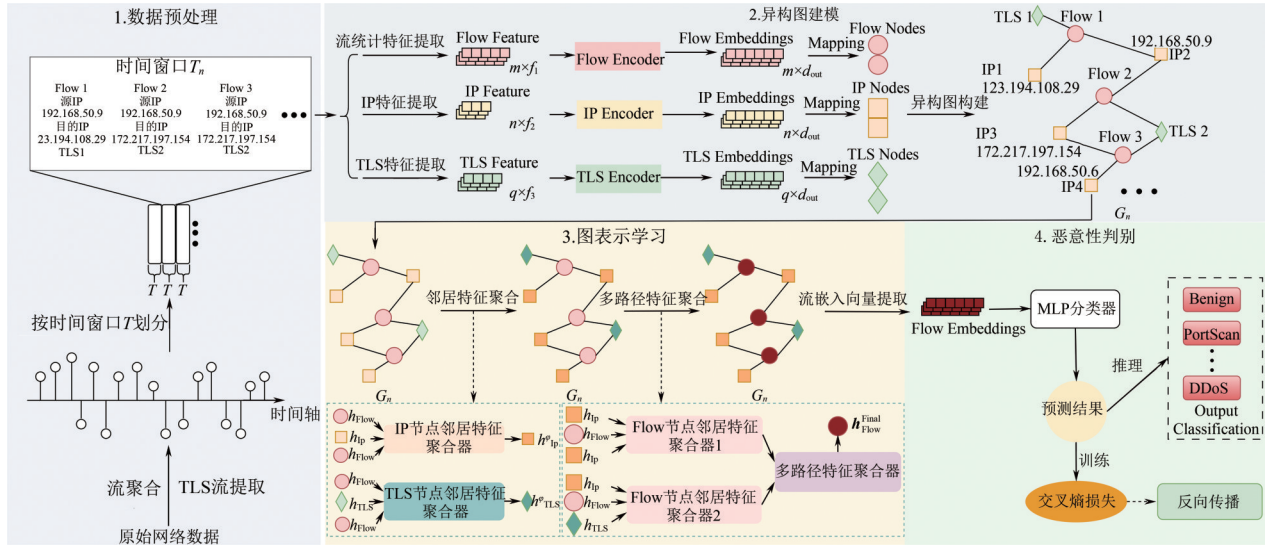


图1 MHC-GNN总体流程

2.1 数据预处理

该阶段先按照传统的五元组形式将原始网络流量pcap包进行流聚合。随后,系统过滤掉所有非TLS流量,仅保留TLS流量进行后续分析。为能够在动态网络环境中进行有效分析并控制图的规模,采用基于时间窗口的切片策略,以大小为 T 的时间窗口将流量数据切分至一系列独立非重复的时间窗口 T_n 中。

2.2 异构图建模

针对每一个时间窗口内的所有流,该阶段根据这些流构建一个异构图。异构图形式化定义为 $G=(V,E)$ 。集合 V 包含3类异构节点,分别对应网络通信中不同的实体。

1) 流节点(Flow Node, h_{Flow})

作为图的核心分类目标,代表一条独立的加密会话。该节点属性包括流持续时长、包长统计、包间隔时间等在内的流统计特征。

2) IP节点(IP Node, h_{IP})

该节点代表网络通信中的端点。由于IP地址本身属于难以泛化的高基数类别特征,因此在该方法中不直接使用IP地址作为特征,而是构建了

IP端点的行为特征,包括内网标识、流吞吐量、唯一目的IP数等,以量化该IP的网络角色与活跃度。

3) TLS节点(TLS Node, h_{TLS})

该节点代表TLS握手过程中使用的证书。从TLS握手的明文字段中解析证书信息,提取包括证书是否自签名、证书有效期、证书issuer和subject字段间的欧式距离等在内的证书特征,以捕获加密身份蕴含的信息。

由于不同类型节点的原始特征的维度和分布存在显著差异,为每种节点类型分别设计了特定的特征编码器。通过类型特定的变换网络,将各节点的原始特征映射至维度一致的向量空间。定义 $\Gamma = \{h_{IP}, h_{TLS}, h_{Flow}\}$ 表示节点类型的集合,类型映射函数 $\tau: V \rightarrow \Gamma$ 表示某个节点 i 的类型 $\tau(i)$ 。具体而言,采用由两个全连接层组成的MLP将异构的原始特征统一映射至统一向量空间。对于类型为 τ 的任意节点 i ,其初始嵌入向量 h_i 的计算过程如下:

$$h_i = W_{\tau}^{(2)} \cdot \sigma(W_{\tau}^{(1)} \cdot X_i + b_{\tau}^{(1)}) + b_{\tau}^{(2)} \quad (1)$$

式中: $X_i \in \mathbb{R}^{d_n}$ 是节点 i 的原始特征向量; $W_{\tau}^{(1)} \in \mathbb{R}^{d_{hidden} \times d_n}$

和 $\mathbf{W}_\tau^{(2)} \in \mathbf{R}^{d_{\text{hidden}} \times d_{\text{out}}}$ 分别是第1层和第2层的权重矩阵; $\mathbf{b}_\tau^{(1)}$ 和 $\mathbf{b}_\tau^{(2)}$ 为偏置项; d_{hidden} 为隐藏层维度; d_{in} 为输入层维度; d_{out} 为输出层维度; σ 表示激活函数 Leaky-ReLU, 用于增强模型对非线性特征关系的捕获能力。

边集合 E 定义了3种实体间的直接交互关系:

- 1) E_1 (Flow-SrcIP): 连接 Flow 与其源 IP。
- 2) E_2 (Flow-DstIP): 连接 Flow 与其目的 IP。
- 3) E_3 (Flow-TLS): 连接 Flow 与其使用的 TLS 证书。

基于上述的边集合 E , 将各异构节点连接为完整的异构图结构。在该图中, 将该阶段经过特征映射得到的向量作为图中各节点的属性, 也作为各节点初始向量嵌入。

2.3 图表示学习

针对上一阶段构建的异构图, 图表示学习阶段的目标是让图中的各节点充分学习邻居节点的特征信息。特别是, 让流节点能充分聚合不同来源的特征信息, 以便后续输入到分类器中进行高精度的加密流量识别。

为捕获实体间的高阶关系, 通过边关系设计一组元路径 $P = \{P_1, P_2, P_3, P_4\}$, 用于指导邻居信息的融合。具体的元路径设计如下。

1) P_1 : Flow-IP-Flow, 关联同一 IP 发出的所有流, 旨在捕获主机级别的集体行为异常。

2) P_2 : Flow-TLS-Flow, 关联使用相同 TLS 证书的所有流, 旨在通过 TLS 证书追踪同一恶意软件家族或攻击工具的活动踪迹。

3) P_3 : SrcIP-Flow-DstIP, 刻画通信端点间的交互拓扑, 旨在帮助模型能够识别到通信中经常表现出异常行为特征的 IP。

4) P_4 : DstIP-Flow-TLS, 建立流和通信端点与加密身份之间的关联, 旨在让流节点学习其他实体的特征信息。

图表示学习阶段设计了一个特征信息聚合机制, 该机制包含两个关键步骤: 邻居特征聚合和多路径特征聚合。邻居特征聚合步骤利用图注意力机制, 在单个元路径视角下自适应地聚合邻居节点信息。多路径特征聚合步骤则通过融合不同元路径下的节点表示, 最终生成融合多源上下文的节点嵌入向量。

考虑到异构图中节点和边的多样性, 传统的 GNN 无法有效地处理和利用异构图信息。因此, 该阶段引入异构图注意力网络模型 HAN^[25] (Het-

erogeneous Graph Attention Network) 聚合特定元路径下的邻居节点的特征信息。各步骤的具体流程如下。

1) 邻居特征聚合

首先, 为处理不同类型节点特征的异质性, 使用特定节点类型的转换矩阵对节点嵌入进行投影。对于任意节点 i , $\mathbf{h}_i$ 表示节点 i 当前的节点嵌入, 则其投影为:

$$\mathbf{h}'_i = \mathbf{W}_{\tau(i)} \cdot \mathbf{h}_i \quad (2)$$

式中: $\mathbf{W}_{\tau(i)}$ 是节点类型 $\tau(i)$ 对应的可训练转换矩阵。 $\phi \in P = \{P_1, P_2, P_3, P_4\}$ 指代任意一条元路径。对于给定的元路径 ϕ , 用 N_i^ϕ 表示节点 i 基于元路径 ϕ 的邻居节点的集合 (包括节点 i 自身)。基于此, 计算目标节点 i 与邻居节点 $j \in N_i^\phi$ 之间的重要性系数 e_{ij}^ϕ 和相应的权重 ε_{ij}^ϕ :

$$\varepsilon_{ij}^\phi = \text{Softmax}(e_{ij}^\phi) = \text{Softmax}\left\{\sigma(\alpha_\phi^T \cdot [\mathbf{h}_i \parallel \mathbf{h}'_j])\right\} \quad (3)$$

式中: α_ϕ 是每个元路径 ϕ 对应的矩阵; $\parallel$ 表示向量拼接操作; σ 代表激活函数 LeakyReLU。通过使用 Softmax 函数对元路径 ϕ 下各邻居节点的重要性系数 e_{ij}^ϕ 进行归一化, 可以得到最终的权重 ε_{ij}^ϕ 。节点 i 会根据各邻居节点的权重聚合其邻居信息和多头注意力拼接操作, 得到聚合元路径 ϕ 下各邻居节点信息的特定嵌入 $\mathbf{h}_i^\phi$ 。

$$\mathbf{h}_i^\phi = \sigma\left(\mathbf{W}_{\text{node}} \cdot \left\|_{k=1}^K \left(\sum_{j \in N_i^\phi} (\varepsilon_{ij}^\phi \cdot \mathbf{h}'_j)\right) + \mathbf{b}_{\text{node}}\right.\right) \quad (4)$$

式中: $\left\|_{k=1}^K$ 表示 φ 多头注意力拼接操作; K 代表注意力头数; $\mathbf{W}_{\text{node}}$ 和 $\mathbf{b}_{\text{node}}$ 是线性层中的可训练权重矩阵和偏置向量; σ 代表激活函数 LeakyReLU。

2) 多路径特征聚合

考虑到不同元路径对特定攻击类型的判别贡献度不同, 引入多路径特征聚合机制以自适应融合不同视角的嵌入向量。在通过邻居特征聚合机制分别计算得到聚合各个元路径 ϕ 下各邻居节点信息的特定嵌入 $\{\mathbf{h}_i^\phi\}_{\phi \in P}$ 后, 再使用多路径特征聚合机制来融合这些嵌入。

首先, 计算每条元路径 ϕ 的重要性系数 β_ϕ :

$$\beta_\phi = \frac{1}{|h_{\text{Flow}}|} \sum_{i \in h_{\text{Flow}}} \mathbf{q}_{\text{sem}}^T \cdot \tanh(\mathbf{W}_{\text{sem}} \cdot \mathbf{h}_i^\phi + \mathbf{b}_{\text{sem}}) \quad (5)$$

式中: h_{Flow} 代表图中所有 Flow 节点的集合; $|h_{\text{Flow}}|$ 代表图中所有 Flow 节点的总数; $\mathbf{q}_{\text{sem}}$ 是全局共享的向量; $\mathbf{W}_{\text{sem}}$ 和 $\mathbf{b}_{\text{sem}}$ 是可训练的权重矩阵和偏置向量。

然后, 对元路径的重要性系数用 Softmax 函数归一化处理, 得到每条元路径的权重 θ_ϕ :

$$\theta_\phi = \text{Softmax}(\beta_\phi) = \frac{\exp(\beta_\phi)}{\sum_{\phi \in P} \exp(\beta_\phi)} \quad (6)$$

最后,通过加权融合不同元路径的嵌入向量,得到了节点 i 在经过图神经网络处理之后的最终嵌入 h_i^{final} :

$$h_i^{\text{final}} = \sum_{\phi \in P} \theta_\phi \cdot h_i^\phi \quad (7)$$

2.4 恶意性判别

为了将学习到的节点嵌入向量映射到具体的恶意流量类别空间,设计一个两层MLP作为下游分类器。分类过程主要分为两个步骤。

首先,为增强模型的非线性表达能力并压缩特征维度,将 h_i^{final} 投影到低维的隐藏空间。然后,再应用激活函数引入非线性因子,并引入Dropout抑制过拟合以提高模型对未知流量的泛化能力。随后,通过输出层将隐藏层特征映射到目标类别的概率分布空间。计算过程如下:

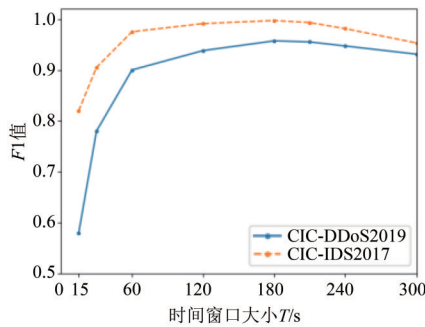
$$h_i^{\text{hidden}} = \text{Dropout}(\sigma(W_1 \cdot h_i^{\text{final}} + b_1)) \quad (8)$$

$$\bar{y}_i = \text{Softmax}(W_2 \cdot h_i^{\text{hidden}} + b_2) \quad (9)$$

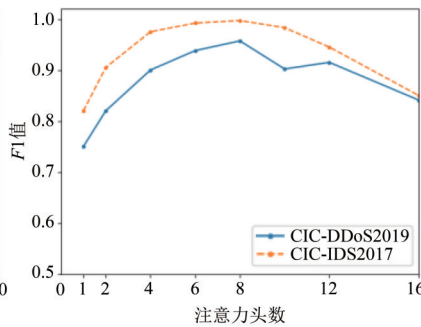
式中: $W_1 \in \mathbf{R}^{d_{\text{hidden}} \times d_{\text{out}}}$ 和 $W_2 \in \mathbf{R}^{|Y| \times d_{\text{hidden}}}$ 分别是第1层和第2层的权重矩阵; b_1 和 b_2 是偏置向量; $|Y|$ 代表流量类别总数。

在模型训练过程中,采用交叉熵损失函数作为优化目标,以衡量预测标签的概率分布与真实标签之间的差异。设 y_{Label} 是所有带标签的Flow节点的集合,对于任意节点 i ,将流节点 i 真实标签视为向量 $Y^i \in \mathbf{R}$,则有:

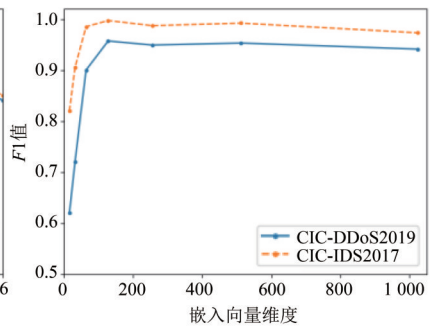
$$L = - \sum_{i \in y_{\text{Label}}} Y^i \cdot [\ln \bar{y}_i]^T \quad (10)$$



(a) 时间窗口



(b) 注意力头数



(c) 嵌入向量维度

图2 超参数实验

通过分析超参数实验的结果,可以得到如下3点结论。

1)图2(a)表明,模型性能随时间窗口增大呈现先快速上升后趋于平稳最后略有下降的趋势。当 $T=180$ s时, $F1$ 分数达到峰值,随后性能保持稳定,直到210 s左右开始下降。这表明过小的时间

窗口无法覆盖完整的攻击行为,导致上下文信息不足;而过大的时间窗口则会引入过多的无关噪声,稀释当前攻击行为的显著性,同时还会增加图的构建和推理开销。

3 实验及结果分析

3.1 数据集

为验证MHC-GNN在加密环境下的有效性,选用在加密恶意流量检测领域被广泛使用和认可的公开数据集CIC-IDS2017和CIC-DDoS2019进行综合评估^[26-27]。

CIC-IDS2017数据集中包含了DoS、端口扫描、DDoS、暴力破解、僵尸网络、内部渗透和Heartbleed等多种复杂攻击流量,其中良性流量约210万条,攻击流量约55万条。CIC-DDoS2019数据集中包含NTP、DNS、LDAP、MSSQL、NetBIOS、SNMP、SSDP、UDP、UDP-Lag、WebDDoS、SYN和TFTP等在内的12种DDoS变体攻击。这些公开数据集的流量分布情况见表1。

表1 公开数据集流量分布情况

数据集	攻击类别数量	流总数
CIC-IDS2017	8	2 660 377
CIC-DDoS2019	13	12 794 627

3.2 超参数实验

为了在计算效率与特征捕获能力之间寻求最佳平衡,针对时间窗口大小、注意力头数和嵌入向量维度等3个超参数进行了系统实验,实验结果如图2所示。

窗口无法覆盖完整的攻击行为,导致上下文信息不足;而过大的时间窗口则会引入过多的无关噪声,稀释当前攻击行为的显著性,同时还会增加图的构建和推理开销。

2)图2(b)表明,模型的性能总体随着注意力头数的增加呈现先升后降的趋势。在注意力头数

为8时,模型在两个数据集的 $F1$ 分数均到达峰值。这表明,多头注意力机制相较于单头注意力,增强了模型的特征信息捕获能力。但是,过多的注意力头反而会导致参数冗余和优化困难,进而削弱模型的泛化能力。

3)图2(c)表明,模型性能随嵌入维度的增加呈现边际收益递减的规律。当维度从16增加到64维时,性能均出现大幅提升,这是因为较低维度的表示空间不足以捕获异构图中复杂的多源特征。当维度达到128维时,模型的性能最高。随后,嵌入维度一直增加到256维、512维和1 024维,性能没有出现大的波动,而计算成本显著增加。由于

嵌入维度的增加会较大增加计算量,因此本实验优先考虑使用128维作为嵌入向量的维度。

基于上述实验分析,后续所有实验均固定时间窗口大小为180 s,注意力头数为8,嵌入维度 d_{out} 为128。

3.3 对比实验

为验证MHC-GNN方法的有效性,将MHC-GNN与现有主要方法在两个公开数据集上进行测试。将每个数据集均按照8:2划分为训练集和测试集。本文使用准确率、精确率、召回率、 $F1$ 值评估各模型在数据集上的性能。对比实验的具体结果如表2所示。

表2 对比实验结果

单位:%

模型	CIC-IDS2017				CIC-DDoS2019			
	准确率	精确率	召回率	$F1$ 值	准确率	精确率	召回率	$F1$ 值
DNN	94.6	95.1	96.3	95.7	75.2	76.5	78.1	77.3
CNN+RNN	94.9	95.5	93.3	94.4	73.8	78.2	61.0	68.5
GraphDApp ^[13]	87.6	86.5	80.3	83.3	69.3	72.0	42.5	53.5
HyperVision ^[20]	96.4	96.2	97.2	96.7	88.1	88.0	88.6	88.3
SnifferDog ^[22]	99.7	99.7	99.7	99.7	79.3	82.1	74.1	77.9
TFE-GNN ^[21]	99.7	99.5	99.3	99.4	94.5	95.2	92.1	93.6
MHC-GNN	99.8	99.7	99.6	99.7	96.2	96.5	94.9	95.7

通过对比分析实验结果,可以得到以下结论:MHC-GNN在两个数据集的所有核心指标上实现了最优或次优表现,证明了在常规攻击场景下,本文方法具备优秀的检测精度。值得注意的是,在CIC-DDoS2019数据集上,其他方法出现明显的性能下降,而MHC-GNN仍能达到95.7%的 $F1$ 分数,这表明在DDoS攻击的高并发场景下,MHC-GNN凭借引入的IP、TLS节点和相应的元路径设计,能够有效捕捉DDoS攻击中多源拓扑特征。

表3记录了MHC-GNN在CIC-IDS2017和CIC-DDoS2019数据集上的运行时间。在验证推理阶段,MHC-GNN对CIC-IDS2017和CIC-DDoS2019单条流的平均推理耗时分别约为4.2 μs 和4.9 μs ,表明该方法具备较高的推理效率。与非图方法相比,MHC-GNN确实引入了图构建与图推理的额外开销。但从检测性能来看,DNN和CNN+RNN在CIC-DDoS2019上的 $F1$ 分数分别仅为77.3%和68.5%,而MHC-GNN达到了95.7%,分别高出18.4和27.2个百分点。因此,以合理的计算开销换取大幅度的检测精度提升是值得的。此外,在实际部署中,可结合GPU并行推理和流水线处理进一步降低延迟。

表3 MHC-GNN运行效率

数据集	平均训练时间/s	平均推理时间/s	单条流平均推理耗时/ μs
CIC-IDS2017	275.5	9.3	4.2
CIC-DDoS2019	1 123.6	46.1	4.9

3.4 消融实验

为探究MHC-GNN方法中各个关键组件对检测性能的贡献,也为了验证TLS-IP-Flow三元异构图建模与基于元路径的上下文感知融合机制的必要性,设计了一系列变体模型。各变体模型具体如下3种。

1)w/o IP Context 移除图中的所有IP节点及相关边,验证拓扑上下文的贡献。

2)w/o TLS Context 移除图中的所有TLS节点及相关边,验证加密身份上下文的贡献。

3)w/o Heterogeneity 移除图的异构属性,将IP、TLS、Flow节点视为同构节点,使用标准的GCN模型代替MHC-GNN使用的HAN模型,验证异构建模的贡献。

在CIC-DDoS2019数据集上进行消融实验,实验结果如表4所示,表中 $\Delta F1$ 为变体模型与完整模型 $F1$ 值的对比差值。

表4 消融实验结果

单位: %

变体模型	准确率	精确率	召回率	F1 值	$\Delta F1$
w/o IP Context	85.2	86.0	82.3	84.1	-11.6
w/o TLS Context	91.3	91.5	89.5	90.5	-5.2
w/o Heterogeneity	90.4	90.8	87.5	89.1	-6.6

由表4分析可得以下两点:

1) w/o IP Context 变体模型出现了最大的性能下滑, $F1$ 分数下降了 11.6 个百分点。这一结果与 DDoS 攻击的本质高度吻合。CIC-DDoS 数据集包含大量分布式拒绝服务攻击, 这类攻击特征主要体现为特定源 IP 或目的 IP 的高频交互模式。而移除 IP 节点意味着模型无法聚合 IP 相关的特征, 导致模型在检测 DDoS 攻击时性能大幅下降。w/o TLS Context 变体模型的 $F1$ 分数下降了 5.2 个百分点, 这说明 TLS 证书信息能够帮助模型识别特定攻击工具或僵尸网络家族生成的流量。这两种变体证明了仅依靠流的时空特征无法有效识别复杂的攻击模式, 引入 IP 端点和 TLS 证书的上下文信息是提升检测性能的关键。

2) w/o Heterogeneity 变体模型的 $F1$ 分数下降了 6.6 个百分点。这表明, 简单的同构图神经网络将 IP、TLS 和 Flow 视为同质节点会导致无法有效区分高相似度的流行为。而 MHC-GNN 通过特征信息融合机制, 实现了不同视角信息的有效融合。

4 结束语

本文提出一种基于多视角异构图的上下文感知检测方法(MHC-GNN), 将传统的恶意流与良性流分类问题重塑为异构图中的上下文感知的节点分类问题。通过构建 TLS-IP-Flow 三元异构图, 将 TLS 证书的加密身份、通信端点的交互行为与流自身的统计模式进行了统一的结构化建模。在此基础上, 利用异构图注意力网络的信息传递能力和元路径机制, 实现了多视角特征信息的聚合, 从而生成了具有强判别力的流嵌入表示, 进而实现精准的加密恶意流量检测。后续工作可从以下几个方面进行: 1) 少标签或者噪声标签条件下的鲁棒性增强; 2) 图的计算效率优化, 包括图采样、模型蒸馏及增量推理等; 3) 基于证书主体的数据划分与泛化性验证; 4) QUIC 等其他加密协议上的应用。

参考文献:

[1] ZANG X D, WANG T L, ZHANG X C, et al. Encrypted

malicious traffic detection based on natural language processing and deep learning[J]. Computer Networks, 2024, 250: No.110598.

- [2] GU G F, ZHANG J J, LEE W K. Botsniffer: detecting botnet command and control channels in network traffic [C] // Proceedings of the 2008 Network and Distributed System Security Symposium. San Diego, USA: Internet Society, 2008: 269-286.
- [3] The MITRE Corporation. Non-standard port [EB/OL]. (2020-03-14) [2025-10-25]. <https://attack.mitre.org/techniques/T1571/>.
- [4] SHEN M, WEI M W, ZHU L H, et al. Classification of encrypted traffic with second-order markov chains and application attribute bigrams [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1830-1843.
- [5] 李慧慧, 张士庚, 宋虹, 等. 结合多特征识别的恶意加密流量检测方法[J]. 信息安全学报, 2021, 6(2): 129-142.
- [6] FU C P, LI Q, SHEN M, et al. Realtime robust malicious traffic detection via frequency domain analysis [C] // Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2021: 3431-3446.
- [7] 孙相宇, 刘永杰, 郑永辉. DETB: 一种针对 IPsec 产品识别的流量分类方法[J]. 信息工程大学学报, 2025, 26(6): 723-730.
- [8] 骆子铭, 许书彬, 刘晓东. 基于机器学习的 TLS 恶意加密流量检测方案[J]. 网络与信息安全学报, 2020, 6(1): 77-83.
- [9] SHEN M, LIU Y T, ZHU L H, et al. Fine-grained web-page fingerprinting using only packet length information of encrypted traffic [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2046-2059.
- [10] SHAO G L, CHEN X S, ZENG X M, et al. Deep learning hierarchical representation from heterogeneous flow-level communication data [J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1525-1540.
- [11] LIN K D, XU X L, GAO H H. TSCRNN: a novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT [J]. Computer Networks, 2021, 190: No.107974.
- [12] 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.
- [13] 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.
- [14] FU Z Q, LIU M X, QIN Y, et al. Encrypted malware traf-

- fic detection via graph-based network analysis [C]//Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses. New York, USA: ACM, 2022:495-509.
- [15] HUOH T L, LUO Y, LI P L, et al. Flow-based encrypted network traffic classification with graph neural networks [J]. IEEE Transactions on Network and Service Management, 2023, 20(2):1224-1237.
- [16] GHADERMAZI J, HORE S, SHAH A, et al. GTAE-IDS: graph transformer-based autoencoder framework for real-time network intrusion detection [J]. IEEE Transactions on Information Forensics and Security, 2025, 20:4026-4041.
- [17] WANG W, SHANG Y Y, HE Y Z, et al. Botmark: automated botnet detection with hybrid analysis of flow-based and graph-based traffic behaviors [J]. Information Sciences, 2020, 511:284-296.
- [18] HONG Y P, LI Q, YANG Y Q, et al. Graph based encrypted malicious traffic detection with hybrid analysis of multi-view features [J]. Information Sciences, 2023, 644: No.119229.
- [19] PREMKUMAR A, SCHNEIDER M, SPIVEY C, et al. Graph representation learning for context-aware network intrusion detection [C]//Proceedings of SPIE 12538, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V. Orlando, USA: SPIE, 2023:No.125380H.
- [20] FU C P, LI Q, XU K. Detecting unknown encrypted malicious traffic in real time via flow interaction graph analysis [DB/OL]. (2023-01-31) [2026-03-03]. <https://doi.org/10.48550/arxiv.2301.13686>.
- [21] 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, USA: ACM, 2023:2066-2075.
- [22] LUO X, YIN L H, YANG H Y, et al. SnifferDog: comprehensively learning heterogeneous features of network traffic to identify malicious flows [J]. IEEE Transactions on Information Forensics and Security, 2025, 20:11684-11699.
- [23] ZHAO J, LI Q, HAN Z, et al. ReTrial: robust encrypted malicious traffic detection via discriminative relation incorporation and misleading relation correction [J]. IEEE Transactions on Information Forensics and Security, 2025, 20:677-692.
- [24] CUI S S, HAN X Y, HAN D Q, et al. FG-SAT: efficient flow graph for encrypted traffic classification under environment shifts [J]. IEEE Transactions on Information Forensics and Security, 2025, 20:5326-5339.
- [25] WANG X, JI H Y, SHI C, et al. Heterogeneous graph attention network [DB/OL]. (2021-01-20) [2026-03-03]. <https://doi.org/10.48550/arxiv.1903.07293>.
- [26] SHARAFALDIN I, HABIBI LASHKARI A, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization [C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Setúbal, Portugal: SCITEPRESS, 2018:108-116.
- [27] 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. Piscataway, USA: IEEE, 2019:1-8.

(编辑:邵 华)