中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 270–286
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

面向 6G 流量监控: 基于图神经网络的加密恶意流量检测方法

赵键锦[1,2], 李祺[1,2*], 刘胜利[3], 杨彦青[1,2], 洪岳平[1,2]

1. 北京邮电大学网络空间安全学院, 北京 100876
2. 移动互联网安全技术国家工程实验室, 北京 100876
3. 数学工程与先进计算国家重点实验室, 郑州 450001
* 通信作者. E-mail: liqi2001@bupt.edu.cn

收稿日期: 2021–08–14; 修回日期: 2021–09–27; 接受日期: 2021–10–29; 网络出版日期: 2022–02–07

国家自然科学基金 (批准号: 62172055, U20B2045, U1836103)、北京邮电大学提升科技创新能力行动计划项目 (批准号: 2021XD-A09) 和国家协同创新专项课题 (批准号: 2019QY1404) 资助

摘要 6G 作为下一代移动通信技术演进的重要方向, 将全面推动经济社会数字化浪潮. 6G 网络承载的众多业务将依赖于实体间共享和协同处理海量的数据, 数据安全显得尤为重要. 当前多数网络应用都会使用 SSL/TLS 加密协议来保障网络通信的机密性与安全性. 然而, 加密机制在保障数据安全的同时也给网络安全监管带来了巨大的挑战. 尽管针对传统网络的加密恶意流量检测已成为研究热点, 但现有技术无法直接应用于 6G 网络. 在海量异构终端即时、无限制通信的 6G 网络中, 网络通信行为模式更加多样化, 这使得正常流量与恶意流量的边界相较于传统网络更加模糊, 深入分析并利用网络服务相关性与通信行为相关性对加密恶意流量检测有着重要的价值. 然而, 现有研究不管是对加密流量进行孤立分析还是聚合分析, 都忽略了加密流量间丰富的相关关系. 为此, 我们面向未来 6G 网络的网络安全问题提出了基于图神经网络的加密恶意流量检测方法 ET-RSGAT. 首先, 针对 6G 网络超高速率、超大连接的特点, 我们设计了便捷的加密流量特征提取方法: 为单条加密会话提取其 TLS 握手原始字节、TLS 记录长度序列等特征表示; 其次, 考虑到 6G 网络中海量异构终端互联、多源异质数据共存, 我们从网络服务相关性和通信行为相关性这两个方面分析加密会话之间的相关关系, 并构建加密流量图 ETG. 在 ETG 的基础上, 我们引入图注意力网络, 充分利用相关关系来丰富节点的特征表示. 在更加丰富的节点特征表示的基础上, 我们基于多层感知器构建检测模型来识别威胁. 考虑到当前 6G 网络的仿真环境不成熟, 我们针对 6G 网络海量异构终端互联的特点, 部署多种异构终端节点并运行各类网络服务来模拟 6G 通信场景并设计了相关实验对本方法进行了评价. 实验结果表明, 本方法能够同时在传统网络与模拟环境数据集中取得令人满意的检测结果.

关键词 6G, 恶意流量检测, 加密流量, 图神经网络, 注意力机制

引用格式: 赵键锦, 李祺, 刘胜利, 等. 面向 6G 流量监控: 基于图神经网络的加密恶意流量检测方法. 中国科学: 信息科学, 2022, 52: 270–286, doi: 10.1360/SSI-2021-0280
Zhao J J, Li Q, Liu S L, et al. Towards traffic supervision in 6G: a graph neural network-based encrypted malicious traffic detection method (in Chinese). Sci Sin Inform, 2022, 52: 270–286, doi: 10.1360/SSI-2021-0280

1 引言

随着 5G 商用的落地, 云端计算、万物互联、智慧城市等多种应用场景从幻想走进了现实[1~3]. 与此同时, 新的需求也在酝酿, 人们开始展望通信技术未来的发展. 第六代移动通信技术 (6G) 将呈现出覆盖区域更加全面、网络架构更加异构、通信技术更加多样、设备连接更加密集的特征. 6G 网络将实现即时、无限的无线连接, 以更高的宽容度支持多类型的海量异构终端接入, 可以说, 6G 移动通信技术的发展将全面推动经济社会数字化浪潮[4~7].

6G 网络当前虽然还没有投入应用, 但人们已开始展望 6G 网络的美好愿景以及可能的安全挑战. 更高的数据传输速率、更低的传输时延, 以及更高的连接密度等特性使得 6G 网络可以提供更加全面的智能化、自动化服务. 此外, 6G 网络还将融入新的网络架构[8], 如软件定义网络/网络功能虚拟化 (software-defined network/network functions virtualization, SDN/NFV)、动态网络切片、基于服务的架构 (service-based architecture, SBA)、认知服务架构 (cognitive service architecture, CSA) 和 cell free(CF) 架构等. 可以预见, 6G 网络将是一个多种异构网络架构协同工作、海量异构终端无限制连接、各类型网络应用多样化存在的网络. 然而, 海量异构终端的广泛互联以及网络应用的多样化发展将会给恶意流量检测带来巨大挑战. 首先, 6G 终端高度异构化, 这导致应用在不同终端上发起相同网络通信时产生的流量通信模式差异明显. 其次, 6G 网络应用的类型更加丰富, 流量的多样化与个性化也更加凸显. 上述两种情况必然导致 6G 网络中的正常流量与异常流量边界更加模糊.

当前, 为了保障网络通信安全, 安全套接字协议 (secure socket layer, SSL) 及其改进协议传输层安全协议 (transport layer security, TLS) 被广泛用来加密通信数据[9,10]. 在以数据为中心的 6G 通信网络中, SSL 和 TLS 必将遍布终端与终端、终端与服务器、服务器与服务器通信的各个环节, 加密协议的引入给攻击者提供了更多的可乘之机. 一方面, 攻击者可以利用加密流量隐藏其恶意行为, 例如恶意负载传递、命令和控制通道, 以及数据回传等[11~13]. 另一方面, 在正常与异常流量边界模糊的 6G 网络中, 加密机制使得攻击者更易将威胁活动伪装成正常的网络通信, 这给网络安全带来了严重威胁. 因此, 对于 6G 网络的加密恶意流量检测进行预研具有重要的意义.

近年来, 研究者提出了许多加密恶意流量检测方法, 由于加密流量的载荷不可见, 这些研究工作主要集中在未加密的 TLS 握手消息分析和元数据分析两方面[14,15]. 在这些研究中, 传统的机器学习方法与新兴的深度学习模型相继被引入到加密恶意流量检测的工作中来, 并取得了较好的效果. 但是, 现有针对传统网络的检测技术不能直接应用于通信节点高度异构化的 6G 网络中.

首先, 现有方法大多对单条加密会话进行单独分析. Anderson 等[16,17] 最早关注加密恶意流量检测研究, 并定义检测粒度为单条加密会话, 主要关注握手信息 (版本、加密套件、扩展、证书等) 以及会话的元数据 (数据包长度序列、数据包时间间隔序列等) 两类统计特征. 虽然后续研究提出了利用上下文背景数据如 HTTP, DNS 流量扩充可用信息, 但其目的是对单条加密会话缺失的特征进行补全. 虽然检测效果得到了提升, 但并没有对具有相关关系的加密会话进行关联聚合分析. 这种方法在复杂的 6G 网络中存在严重的问题. 一方面, 6G 网络中海量的网络应用对应的通信行为模式复杂且攻击技术不断升级, 恶意软件可以轻易改变通信行为把恶意流量伪装成正常的 6G 通信数据. 另一方面, 终端设备异构化的特点在 6G 网络中将更加明显, 标准化是一大难题. 终端设备加密通信时使用的各种参数, 如加密套件, 更加复杂且标准化不足, 因此在通信过程中很容易由于握手信息非标准化而被误认为恶意流量.

其次, 现有的多条加密会话关联分析方法仅考虑了简单的统计特征聚合. Strasak[18] 最早提出基于多元组连接聚合加密会话, 对单条加密会话的特征进行了更高级的统计, 在传统网络中取得了不错

的检测效果, 但这种做法忽略了加密会话之间丰富的关系. 在 6G 网络中, 海量异构终端节点紧密、无缝地协同工作, 相应产生的加密会话之间也蕴含着丰富的相关关系, 可以充分反映终端节点的服务类型与通信行为模式, 是加密恶意流量检测任务中必须深入分析的内容. 而现有的关联分析方法, 虽然将统计分析单元从单条加密会话转为多元组连接, 如四元组 (源 IP、目的 IP、目的端口、协议) 连接, 突破了单流检测的局限性. 然而, 此类关联分析方法在对流量聚合时只考虑了简单特征的聚合. 随着攻击手段的不断升级, 简单特征容易被伪造, 因此亟需从业务相关性等方面对加密流之间的关联关系进行深入分析.

综上, 6G 网络中海量的异构终端为攻击者提供了巨大的攻击入口, 加密协议的使用和通信行为模式多样性对 6G 网络安全提出了更大挑战. 但同时, 终端设备和通信数据之间的强相关性也为检测提供了新思路. 虽然异构终端的通信行为模式五花八门, 同一恶意软件由于系统类型、固件版本、网络情况等区别, 在不同终端设备上的通信行为也存在差异, 但与正常流量的复杂、多样性相比, 恶意软件通常会遵循固定的模式建立加密会话, 即加密恶意流量的通信模式相对稳定. 对应到具体的检测任务中, 未加密的 SSL/TLS (后文仅用 TLS 表示) 握手信息可以体现业务的可信度, 而加密会话元数据中的数据包长度序列不仅可以表征网络行为、反映 6G 网络应用或威胁活动的类型, 还可以通过关联分析刻画相关加密会话的通信模式平稳性, 并进一步识别自动化行为.

本文面向 6G 网络提出了一种基于图神经网络的加密恶意流量检测方法. 首先, 我们为每条单独的加密会话定义两类特征表示及两组关系建模方法. 两类特征表示分别用于刻画该加密会话的握手信息和与通信行为模式. 两组关系分别用于表示加密会话间访问网络服务的相关性和共享相似通信行为模式的相关性. 在此基础上, 我们构建了一种有向图, 加密流量图 (encryped traffic graph, ETG) 来建模加密会话之间的复杂关系. 通过 ETG, 可以将加密恶意流量检测问题转化为节点分类任务. 根据不同的流量特征表示, 利用改进的图注意力网络 (graph attention network, GAT) 来表征加密会话的两类不同特性、可信度和平稳性, 并综合这两类特性自动识别隐藏在加密流量中的威胁活动.

本文的主要工作包括:

(1) 针对 6G 网络加密恶意流量检测中的单条加密会话判定困境, 使用有向图结构来表征加密会话间复杂丰富的关联关系. 在 ETG 中, 每个节点表示一条加密会话, 每条边表示两个节点 (加密会话) 之间存在相关关系. 当两条加密会话之间有边相连时, 则表示它们访问相同的网络服务或是共享相似的通信行为模式.

(2) 在多条加密会话关联分析的基础上, 提出一种改进的面向可信度 (reliability) 和平稳性 (stationary) 的基于图注意网络 (GAT) 的加密恶意流量检测框架 (RS-GAT), 来进一步学习加密会话之间的相关关系, 并在此基础上将加密恶意流量检测问题有效转化为节点分类问题, 实现了加密恶意流量的高效检测.

论文其余部分章节组织安排如下: 在第 2 节, 回顾了加密恶意流量检测的相关工作. 在第 3 节中, 介绍了本文提出的面向 6G 网络的基于图神经网络的加密恶意流量检测框架 (encrypted traffic-reliability and stationary-oriented graph attention network, ET-RSGAT). 在第 4 节, 介绍了 ET-RSGAT 方法的具体工作流程, 包括加密流量表示提取、加密流量图构建与加密恶意流量检测模块. 在第 5 节, 进行了充分的实验来评估本文所提出的方法在公共数据集和模拟网络环境中的性能. 最后, 对本文的工作进行了总结和展望.

2 相关工作

加密恶意流量的检测是当前网络安全研究的重点, 引发了学术界与工业界的广泛关注. 研究者们就此展开了大量的研究工作. Velan 等 [19] 研究了现有各种加密流量协议的分类和分析方法. 他们讨论了加密协议 (如 IPSec, TLS, SSH 等) 结构和工作原理, 并探索了基于应用程序的协议 (如 Bit-Torrent 和 Skype 等). 通过研究, 作者揭示了大多数检测方法使用的是用于监控、检查和加密流量分类的初始阶段的信息, 对握手协议进行深入分析可以有效提高加密恶意流量检测的准确率. Rezaei 等 [20] 利用深度学习算法对加密流量进行精细化分类工作, 并证明了可以在这一工作的基础上进行用户行为检测. 总之, 当前的研究大多从 3 个方面展开: 基于有效载荷的研究、基于特征工程的研究和基于原始数据的研究.

基于有效载荷的研究方法侧重于网络流量的具体内容, 包括基于深度包检测 (deep packet inspection, DPI) 的检测方法和通过中间代理的解密方法等. 由于加密过程将原始流数据转换为伪随机无意义的字符序列, 因此传统的 DPI 检测方法 [21,22] 不再适用. Sourabh 等 [23] 使用 SSL Split 等透明 SSL 代理工具作为客户端和服务器之间的中介, 通过解密获得纯文本, 然后应用模式匹配方法进行检测. 但是这种方法严重侵犯了用户的隐私, 影响了网络性能且对解密能力的依赖性很大.

在基于特征工程的研究中, 研究者们充分利用了 TLS 加密协议在握手阶段所引入的可见数据特征. Roesch 等 [24] 提出了一种详细描述 TLS 连接构建过程的方法, 从 TLS 加密协议的可见字段中提取流特征, 然后将特征量化为二值向量来训练 Logistic 回归模型. 这一方法所提取的特征不具备平台鲁棒性, 很多应用软件在不同操作系统 (如 Windows XP 与 Windows 10) 上运行的流量特征有明显差异, 当平台类型多样时, 这一方法的准确率会受到较大影响. Anderson 等 [16] 在研究中利用相关的背景流量信息, 比如 DNS 请求应答数据来优化检测结果. 在后续研究中, Anderson 等 [17] 又解决了加密恶意流量检测中存在的噪声标签与非平稳问题, 他们通过对比 6 种机器学习发现 random forest 模型在加密恶意流量检测这一问题中是最鲁棒的. 然而, 这些方法存在以下两个缺点: 一方面, 它们忽略了证书的特征, 也没有考虑流量的原始数据信息. 另一方面, 这些方法收集的流量数据仅局限于企业内网, 不代表通用网络流量. Dai 等 [25] 提出了一种基于多维特征的加密恶意流量检测方法, 其中的多视图表示包括流量统计特征、TLS 握手字段和证书, 并应用多种机器学习模型进行分类, 其中 XGBoost 模型取得了最高的准确率. 检测器在判别过程中会依赖更多层次的特征信息, 进而提升检测效果. 然而在实现过程中, 该方法会对多视图特征进行提取, 检测过程相对复杂. Liu 等 [26] 提出了 MalDetect, 针对加密恶意软件流量的检测架构, 采用在线随机森林的模型在恶意软件造成危害前检出恶意流量, 此类方法具有较好的泛化能力. 但是上述方法的检测效果很大程度上依赖于专家先验知识. 如果流量报文发生变化或被人为混淆, 则检测效果将大大降低. 在 6G 网络中, 新的应用类型和新的节点设备海量涌现, 先验知识很难准确而完备, 因而该方法难以直接应用.

在基于流量原始数据的研究中, Bazuhair 等 [27] 提出了一种基于图像的加密流量表示方法, 使用柏林噪声编码给定的连接特征到图像, 并训练一个深度学习的二分类模型. Yang 等 [28] 使用自编码器和卷积神经网络两种深度学习模型对流量特征进行学习和分类. 然而, 这些方法一方面没有充分结合流量的向量化特征, 不能充分考虑加密流量的不同特征. 另一方面, 忽略了数据样本与结构信息之间的关系.

有研究者使用图神经网络方法 [29] 对僵尸网络进行分析, 虽然作者仅单单对一种网络攻击类型进行了调研, 但是实验充分表明, 图分析方法可以在加密流量检测过程中充分利用通信数据之间的相关性, 这非常符合 6G 通信网络广域互联的应用背景.

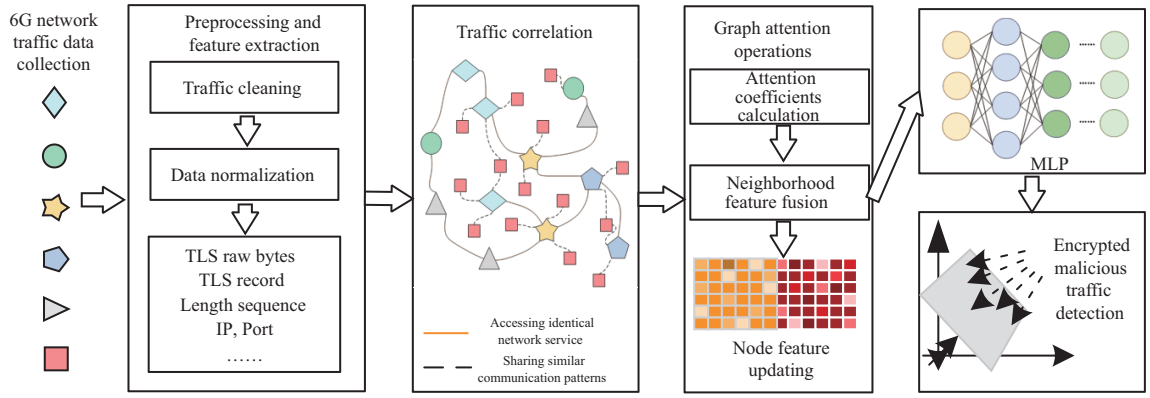

图 1　(网络版彩图) 面向 6G 网络的加密恶意流量检测框架

Figure 1　(Color online) Architecture of encrypted malicious traffic detection framework towards 6G network

3　加密恶意流量检测架构

考虑到未来 6G 通信网络中异构节点共存、应用种类复杂、正常流量与异常流量的边缘相较于传统网络更加模糊. 本文针对这些特点提出了一种基于图神经网络的加密恶意流量检测方法, ET-RSGAT. 该方法不仅考虑到共享四元组的网络流量之间的相关性, 还充分考虑了同类网络业务间网络流量的关联关系, 利用加密会话的业务可信度和通信模式平稳性, 提出基于可信度 (reliability) 与平稳性 (stationarity) 的图注意力网络 (GAT) 来检测加密恶意流量. 这种方法可以在通信终端高度异构化的 6G 网络中取得良好的检测效果.

如图 1 所示, 在进行加密恶意流量检测的过程中, 首先采集异构终端访问多种类型网络应用的流量数据. 在进行流量清洗和格式归一化等预处理工作后, 提取 TLS 握手原始字节、TLS 记录长度序列, 以及 IP 地址、端口等特征表示. 之后, 基于网络服务相关性和通信模式相关性两种关联规则构建加密流量图 (ETG). 该关系图以单条加密会话为节点, 并在共享相同目的 IP 与目的端口, 或共享相同或相似通信模式的加密会话 (节点) 之间连边, 存在边相连的节点称为邻居节点. 考虑到能从加密流量中获取的消息非常有限, 将邻居节点的特征通过图注意力机制有权重地聚合到目标节点, 将更加丰富的节点特征输入到多层感知器, 从而实现了加密恶意流量检测模型.

通过这一方法, 一方面, 我们建立了加密会话之间的关联关系, 突破了以往研究中对单条加密会话孤立分析的局限性; 另一方面, 我们利用邻居节点的特征来丰富每一条加密会话节点的特征表示, 弥补了现有加密流量研究中相关关系分析缺失的不足.

4　基于图注意力机制的加密恶意流量检测方法

4.1　加密流量预处理模块

未来 6G 通信网络中将存在海量异构终端节点, 且运行着多种多样的网络服务. 在对加密恶意流量进行检测之前, 需要对采集到的原始流量数据进行数据清洗、检测单元划分、归一化表示等预处理操作. 在现有工作中, 研究者提出了多种适用于不同具体任务的流量划分粒度, 如基于相同源 IP 的划分方式可以识别受感染的主机, 而基于相同目的 IP 的划分方式可发现恶意域名服务等.

本文选择在会话粒度层级上处理加密流量数据, 即每一个分析单元都是一条共享相同五元组 (srcIP,

表 1 本文中的符号含义表示

Table 1 The list of notations

Notation	Meaning
srcIP	Source IP of single encrypted session
srcPort	Source port of single encrypted session
dstIP	Destination IP of single encrypted session
dstPort	Destination port of single encrypted session
protocol	Communication protocol
b_n^i	The nth byte in TLS records of encrypted session i
l_m^i	The mth TLS record length of encrypted session i
v, e	The vertex and edge in the graph
V, E	The vertex set and edge set in the graph
H_i	Feature representation based on TLS handshake raw bytes of encrypted session i
S_i	Feature representation based on TLS record length sequence of encrypted session i
$E_{i,j}$	Edge representation between vertex i and vertex j
$\boldsymbol{h}$	Feature representation set of encrypted sessions
$\boldsymbol{h}_i$	Feature representaion of encrypted session i
$\boldsymbol{W}$	Linear transformation weight matrix
$\boldsymbol{W}^H$	Linear transformation weight matrix in TLS handshake message operation
$\boldsymbol{W}^S$	Linear transformation weight matrix in TLS record length sequence operation
a	Self-attention mechanism
$\boldsymbol{a}$	Parametric weight vector in self-attention mechanism
$e_{i,j}$	The attention coefficient that indicates the importance of vertex j's features to vertex i
N_i	The first-order neighborhood vertex set of encrypted session i

srcPort, dstIP, dstPort, protocol) 的加密会话, 其中源和目的 IP 与 Port 可互换. 会话 (双向流) 表示方法在流量刻画上具有如下优势:

(1) 可以描述客户端和服务器之间的细粒度交互行为;

(2) 可以灵活地将流量信息进行融合且在融合过程中不造成信息损失;

(3) 可以为后续加密流量间的相关性分析工作提供便利;

(4) 在分析过程中可以灵活地选择时间窗口.

具体来说, 预处理模块包括拆分、重组和过滤 3 个步骤. 首先, 将捕获到的原始流量拆分成独立的分析单元. 其次, 在单条会话的基础上进行重组操作. 考虑到网络流量 MTU (maximum transmission) 的限制和 TLS 记录的多样性, 单个 TCP (transmission control protocol) 段中可能包含多条 TLS 记录, 单条 TLS 记录也可能分布在多个 TCP 段中. 在重组过程中, TCP 会话和 TLS 记录从离散的 TCP 段中被还原, 同时重传、乱序和丢包等问题也在这一过程中被解决. 最后, 本文重点关注加密恶意流量检测任务, 所有未加密会话都被丢弃. 此外, 不完整的加密会话除了占用网络带宽以外, 对网络服务没有任何实质性的影响, 因此没有成功建立的加密会话也会被过滤以减少内存和计算开销. 本文使用的符号含义表示如表 1 所示.

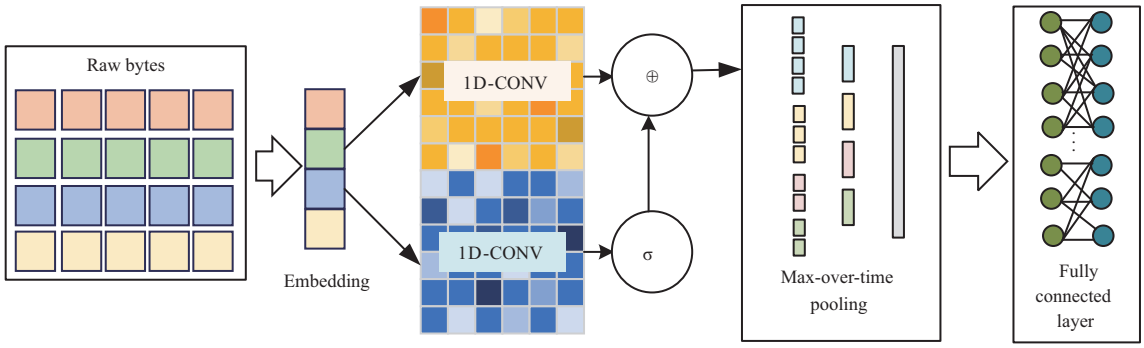

图 2 (网络版彩图) 基于 TLS 握手信息原始字节的流量表示

Figure 2 (Color online) Traffic representation based on TLS handshake raw bytes

4.2 加密流量表示提取模块

由于加密流量的有效载荷不可见, 只能基于明文传输的握手消息和流量的元数据统计特征 (如数据包长度序列) 进行检测. 在基于浅层机器学习的研究中, 特征提取工作需要专家知识, 这导致检测结果对专家知识的依赖性过强. 基于深度学习的研究虽然可以自动地学习加密会话的表示, 但仍然缺少对加密会话间相关关系的考虑. 基于上述考虑, 本文从两个方面对加密会话进行表征和定义.

(1) 基于 TLS 握手信息原始字节的流量表示. TLS (安全传输层协议) 作为 SSL (安全套接字协议) 的改进版本为网络应用通信提供数据保密性与完整性保证. 由于应用数据 (application data) 不可见, 我们可以利用加密连接建立前协商的明文信息, 即握手阶段的 TLS 记录数据来刻画访问服务的可信度. 在这一阶段的原始字节包含了加密通信时使用的版本、扩展、加密套件、证书等信息. 由于恶意软件缺乏安全性与正规性保证, 其 TLS 握手阶段协商的各种信息与正常通信有所区别, 因而可以用于加密恶意流量检测. 此外, 由于会话层以下的数据本身, 如网络层的 IP 地址和传输层的各种 TCP 控制字段, 不能有效反映加密会话的性质. 因此, 在本文中, 我们只保留握手阶段的 TLS 记录的前 N 个字节, 不对会话层以下 (网络层和传输层) 的数据进行处理. 其中, N 的选择对检测结果至关重要, 一方面, N 必须足够长, 保证前 N 个字节中包含 ClientHello, ServerHello 和部分 Certificate 消息; 另一方面, 选取的数据中尽量不要融入过多无关数据而导致检测效率的降低. 在 5.4 小节中, 我们经过了充分的分析和实验, 最终确定 $N = 1800$. 单条加密会话的握手信息原始字节可以表示如下:

$$\text{RawBytes}(i) = \left(b_1^i, b_2^i, \ldots, b_n^i, \ldots, b_N^i\right), \tag{1}$$

其中, b_n^i 为表示第 i 条加密会话 TLS 握手记录的第 n 个字节, $b_n^i \in [0, 255]$.

如图 2 所示, 在后续的处理中, 我们首先利用 embedding 操作将原始字节映射到固定长度的特征向量, 然后使用一维卷积网络架构对该向量进行处理, 获取每个字节的上下文关联以及在握手信息中的映射关系, 通过这一操作, 可以获取 TLS 握手过程中更加丰富的语义表示信息 H, 即加密会话 i 的基于 TLS 握手信息原始字节的流量表示 H_i:

$$H_i = \text{1DCNN}(\text{embedding}(\text{RawBytes}(i))). \tag{2}$$

(2) 基于 TLS 记录长度序列的流量表示. 在以往的研究中, 研究者发现加密会话的数据包长度序列不仅可以刻画加密会话的通信模式, 也可以反映其承载的应用程序类型. 如图 3(a)~(c) 所示, 可以看到不同网络应用的 TLS 记录长度序列有很大差异.

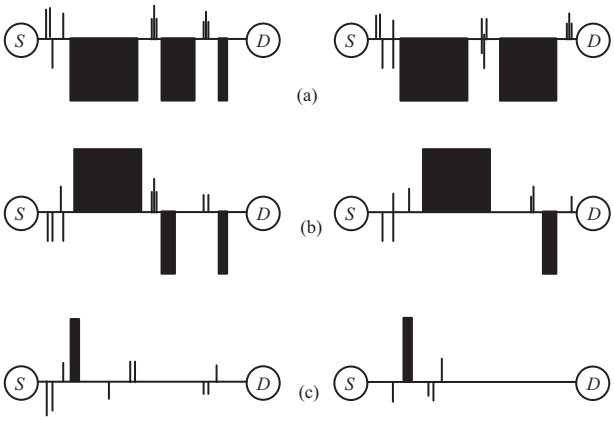

图 3 (a) 某浏览器运行时生成的 TLS 记录长度序列图表示; (b) 某游戏软件运行时生成的 TLS 记录长度序列图表示; (c) 某远程控制恶意软件运行时生成的 TLS 记录长度序列图表示

Figure 3 The TLS record length sequence diagram generated by a browser(a), a computer game(b), and a remote control malware(c), respectively

如 4.1 小节所述, 在预处理过程中, TCP 重组技术不仅解决了网络问题导致的数据包重传和乱序问题, 也消除了 MTU (1500) 的限制还原了 TLS 记录, 进而恢复了加密会话的原貌. 因此, 我们利用 TLS 记录长度序列来代替数据包长度序列, 这更适用于加密恶意流量检测的任务.

基于上述分析, 本文选取加密会话的前 M 条 TLS 记录. M 的选值必须满足包含 TLS 记录中的 ClientHello, ServerHello, Certificate 和部分 application data, 从而有效地反映加密会话的通信模式. 在 5.4 小节中, 通过充分的对比实验, 我们确定 M 取值为 10. TLS 记录长度序列如下:

$$\text{Sequence}(i) = (l_1^i, l_2^i, \ldots, l_m^i, \ldots, l_M^i), \tag{3}$$

其中, l_m^i 表示第 i 条加密会话的第 m 个 TLS 记录长度. 数据流向信息用 l_m^i 的符号表示: 上行流量 (客户端到服务器) 为正, 下行流量 (服务器到客户端) 为负.

此外, 在建模加密会话关系时, 由于 TLS 记录的长度序列可以帮助我们识别更多具有相似通信模式的相关加密会话, 因此可以被应用于加密流量图的构建. 在检测过程中, 也可以通过考虑相关加密会话的 TLS 记录长度序列差异来反映加密会话通信模式的平稳性.

为了消除不同类型的 TLS 记录长度差异的影响, TLS 记录的长度序列通过 ZScore 进行标准化, 如式 (4) 所示.

$$l'_n = \frac{(l_n - \text{mean}(l_n))}{\text{std}(l_n)}, \tag{4}$$

其中, $\text{mean}(l_n)$ 与 $\text{std}(l_n)$ 分别为实验集上所有加密会话第 n 个 TLS 记录长度的均值与标准差. 经过标准化后, 得到加密会话 i 的基于 TLS 记录长度序列的流量表示 S_i:

$$S_i = \text{ZScore}(\text{Sequence}(i)). \tag{5}$$

需要声明的是, 这里的标准化操作需在整个实验数据集上进行. 在模型训练完成后部署到真实网络环境中时, 我们只使用训练数据的标准差与均值进行预处理, 这样可以保证所有数据的 TLS 记录长度被缩放到同样的尺度, 数据分布不会偏移, 保证了模型的检测效果.

4.3 加密流量图构建模块

与非加密流量相比, 从加密流量中可以获取的信息更为有限. 加密会话之间的相关关系对于网络威胁识别具有重要价值, 在判定加密会话是否为恶意时, 应当充分考虑流量之间的相关性而非孤立分析. 网络中的各种资源与服务都托管在特定的 IP 与端口上向外界开放, 很多研究者开始研究通过 IP 和端口将流量进行聚合分析, 然而这种方法存在严重的缺陷.

在此, 我们以僵尸网络为例. 僵尸网络是由被控主机组成的网络, 被控主机会被远端的攻击者通过命令控制通道 (C&C channel) 远程控制以进行威胁活动. 随着攻击技术的升级, 传统的中心化僵尸网络逐渐演变为去中心化的 P2P 架构, 变得更加健壮与难以防御, 此外 fast flux 技术也被部署到僵尸网络中, 通过快速切换 IP 地址来逃避检测. 上述两种情形, 都不能简单地依靠 IP 与端口去关联分析.

而在 6G 通信网络中, 广泛互联的海量异构终端与多种攻击技术的演进都使得加密流量的相关关系变得十分复杂, 这给加密恶意流量检测带来了更加严峻的挑战.

为了有效地对加密流量进行关联分析, 本文通过构建加密流量图 ETG 来建模加密会话间丰富的相关关系. ETG= (V, E) 是一个有向图, $V = \{V_1, V_2, \ldots, V_N\}$ 是所有待检测加密会话也即节点的集合, V_i 表示图中的节点 i, N 为图中节点的总数. 边的集合为 $E = \{E_{i,j}\}$, $i, j \in [1, N]$. 在确定两个节点间是否有关联关系的过程中, 我们从两个步骤进行计算.

首先, 将共享相同目的 IP 地址和目的端口号的两条加密会话之间建立关联关系, 即: 若 $\mathrm{dstIP}_i = \mathrm{dstIP}_j$ 且 $\mathrm{dstPort}_i = \mathrm{dstPort}_j$, 则 $E_{i,j} = 1$; 否则, $E_{i,j} = 0$.

考虑到在实际通信过程中, 一些恶意软件会基于 P2P 架构或 fast flux 机制来干扰第 1 类关联关系分析, 我们基于 TLS 记录长度序列的距离刻画通信模式的相似性来对加密流量图进行补充.

两条加密会话之间的距离计算方法如下:

$$\mathrm{Distance}_{i,j} = \sqrt{(S_i - S_j)(S_i - S_j)^{\mathrm{T}}} = \sqrt{\sum_{n=1}^{M} (l_n^{i\prime} - l_n^{j\prime})^2}. \tag{6}$$

若存在 $x \in N_i$ 使得 $\mathrm{Distance}_{i,j} < \mathrm{Distance}_{i,x}$, 则 $E_{i,j} = 1$; 否则, $E_{i,j} = 0$.

可以看出, 在分析加密会话相关关系的过程中, 我们既考虑了通信过程中的服务一致性, 也考虑了通信行为模式的相似性.

4.4 加密恶意流量检测模块

针对 6G 网络中超高速数据流的加密和完整性保护需求以及超大连接场景的海量设备安全接入需求, 本文将图注意网络 (GAT) 引入到加密恶意流量的检测任务中. 图注意力网络通过注意力机制聚合邻居节点, 对不同的邻居自适应地分配权重, 有效地提高了图神经网络模型的表达能力.

在本检测框架中, 首先收集预设时间窗内的所有加密会话, 之后根据相关关系构建 ETG 来作为模型输入. 图中的单个节点表示单条加密会话, 连边表示两条加密会话之间存在着相关关系. 加密会话节点的特征表示集合为 $\boldsymbol{h} = \{\boldsymbol{h}_1, \boldsymbol{h}_2, \ldots, \boldsymbol{h}_N\}, \boldsymbol{h}_i \in \mathbb{R}^F$. 其中 N 为图中节点 (即加密会话) 的数量, F 表示加密会话的特征维数. 可学习的共享线性变换权重矩阵 $\boldsymbol{W} \in \mathbb{R}^{F' \times F}$ 被应用于每个节点, 来学习更高级的特征表示以取得更好的表达能力. 在最开始随机化初值, 并在后续的训练过程中通过计算损失函数梯度反向传播更新. 该变换可以用如式 (7) 中的权重矩阵线性变换表示:

$$\boldsymbol{h}_i' = \boldsymbol{W}\boldsymbol{h}_i. \tag{7}$$

经过线性变换后, 获得了加密会话节点更新后的特征表示集合 $\boldsymbol{h}' = \{\boldsymbol{h}'_1, \boldsymbol{h}'_2, \ldots, \boldsymbol{h}'_N\}$, $\boldsymbol{h}'_i \in \mathbb{R}^{F'}$, 其中 F' 是变换后的加密会话特征维数. 之后我们基于一个共享的自注意力机制 $a : \mathbb{R}^{F'} \times \mathbb{R}^{F'} \to \mathbb{R}$ 计算节点之间的注意力互相关系数, 如下所示:

$$e_{i,j} = a(\boldsymbol{h}'_i || \boldsymbol{h}'_j). \tag{8}$$

仿照原始图注意力网络的设定, 自注意力机制 a 基于单层前馈神经网络实现. 首先将目标节点与邻居节点线性变换后的特征表示拼接, 然后由权重向量 $\boldsymbol{a} \in \mathbb{R}^{2F'}$ 进行参数化, 并输入非线性激活函数 LeakyReLU 得到未归一化的注意力互相关系数:

$$e_{i,j} = \text{LeakyReLU}(\boldsymbol{a}(\boldsymbol{W}\boldsymbol{h}_i || \boldsymbol{W}\boldsymbol{h}_j)). \tag{9}$$

我们对每个加密会话节点 i 与其一阶邻居节点 $k \in N_i$ 分别计算注意力互相关系数, 其中 N_i 为加密会话节点 i 的一阶邻居节点集合. 同时基于 softmax 函数对该系数进行归一化操作. 具体来说, 节点 i 和 j 之间的注意力互相关系数 $\alpha_{i,j}$ 可以通过式 (10) 计算得到:

$$\alpha_{i,j} = \text{softmax}(e_{i,j}) = \frac{\exp(e_{i,j})}{\sum_{k \in N_i} \exp(e_{ik})} = \frac{\exp(\text{LeakyReLU}(\boldsymbol{a}(\boldsymbol{W}\boldsymbol{h}_i || \boldsymbol{W}\boldsymbol{h}_j)))}{\sum_{k \in N_i} \exp(\text{LeakyReLU}(\boldsymbol{a}(\boldsymbol{W}\boldsymbol{h}_i || \boldsymbol{W}\boldsymbol{h}_k)))}. \tag{10}$$

$\alpha_{i,j}$ 反映了邻居节点 j 对目标节点 i 的重要程度. 在图神经网络的学习过程中, 每个节点的表示由自身及其邻居来共同表示. 基于注意力互相关系数 $\alpha_{i,j}$ 对邻居节点进行加权线性组合从而得到新的节点表示:

$$\boldsymbol{h}_i^{l+1} = \sigma\left(\sum_{j \in N_i} \alpha_{i,j} \boldsymbol{W}\boldsymbol{h}_j^l\right). \tag{11}$$

如 4.2 小节所述, 本文分别提取了 TLS 握手信息与 TLS 记录长度序列的特征表示. 由于 TLS 握手信息表示包含了握手阶段协商的各种参数, 其安全性反映了访问网络服务的可信度. 在基于 TLS 握手信息进行分析时, 应考虑所有相关加密会话的访问服务可信度. 因此对于 TLS 握手信息的聚合计算采用原始的图注意力机制, 代入式 (12) 可得:

$$\boldsymbol{H}_i^{l+1} = \sigma\left(\sum_{j \in N_i} \alpha_{i,j}^H \boldsymbol{W}^H \boldsymbol{H}_j^l\right). \tag{12}$$

考虑到恶意软件通常遵循严格的代码逻辑来建立加密会话, 即其产生的加密会话在 TLS 记录长度序列这一特征维度具有较好的平稳性. 在考虑 TLS 记录长度序列特征聚合时, 我们在式 (11) 的基础上进行改进, 通过求解每个节点与其对应的一阶邻居节点之间的差异来得到通信模式平稳性的特征表示, 具体计算方法如下:

$$\boldsymbol{S}_i^{l+1} = \sigma\left(\sum_{j \in N_i} \alpha_{i,j}^S \boldsymbol{W}^S |\boldsymbol{S}_i^l - \boldsymbol{S}_j^l|\right). \tag{13}$$

6G 网络应用海量涌现, 其通信行为模式也是多种多样, 因此我们在通信模式平稳性的特征表示上叠加高斯 (Gauss) 噪声来增强检测模型的鲁棒性. 最后, 将服务可信度与通信模式平稳性两类特征表示拼接起来作为每条加密会话的最终特征表示, 输入前馈神经网络以进行最终的二分类任务.

$$\bar{y} = \text{softmax}(\boldsymbol{W}(\boldsymbol{H} || \boldsymbol{S}) + b), \tag{14}$$

其中 $\bar{y}$ 为模型的预测值, 表示加密会话是恶意的概率. 我们利用交叉熵损失函数来优化模型, 该函数被广泛应用于分类问题来计算预测标签和真实标签之间的差异, 如下所示:

$$L = -(y \log \bar{y} + (1-y)\log(1-\bar{y})), \tag{15}$$

其中 $y \in \{0,1\}$ 为真实标签, 0 表示当前加密会话属于正常流量, 1 表示当前加密会话属于恶意流量. 在检测过程中, 我们只需要将固定时间窗口的加密流量按照规则构图, 输入 ET-RSGAT 框架, 即可以实现加密恶意流量检测.

5 实验

5.1 数据集描述和设置

由于当前的 6G 网络还缺少仿真环境, 所以如何设计合理的应用场景、验证 ET-RSGAT 算法的有效性是我们面临的一大挑战.

首先, 为了证明 ET-RSGAT 在加密恶意流量检测本身的先进性, 我们需要在传统网络的通用数据集上与现有方法进行比较. 其次, 由于本文所提方法主要是为了应对 6G 网络中海量异构终端、多源异质数据带来的挑战, 所以我们需要在模拟环境中部署大量的异构网络节点并在其上运行多种加密通信的应用程序, 进而证实 ET-RSGAT 在未来 6G 网络中的应用潜力.

基于上述考虑, 选取了 3 个数据源来构建我们的实验样本集, 这 3 个数据源分别是 CTU 数据集、MTA 数据集, 以及从北京邮电大学真实的校园网环境中收集的 BUPT-ETC 数据集.

CTU 数据集. 该数据集是捷克理工大学 (Czech Technical University) 于 2015 年公开的一类完备的僵尸网络流量数据集, 常常被用作加密恶意流量检测任务中的基准数据集, 数据集中包含了在各种场景中捕获的正常流量样本和恶意软件流量样本 (例如, Curdix, Geodo, Zeus, Virut, Tinba 等). 本实验从 CTU 数据集中随机选择 50000 条恶意软件的加密会话与 50000 条正常的加密会话, 构成实验数据集 1.

MTA 数据集. 当前有一个专门关注恶意软件流量研究的博客站点 (malware-traffic-analysis), 该站点重点关注与恶意软件相关的网络流量. 2013 年 6 月至今, 该站点累计发布了 2700 多个恶意软件产生的流量及相关分析. 在本实验中, 我们从该站点收集恶意流量数据, 并随机选取了 50000 条完整的加密会话作为实验数据集 2 的第 1 部分正样本集组成.

BUPT-ETC 数据集. 现有的公开数据集普遍存在着平台类型单一、网络应用类型较少的问题. 为此, 我们构建了 BUPT-ETC 数据集, 针对 6G 网络通信环境中异构节点大量共存、网络应用类型多样这一特点而进行模拟. 在数据集的构造过程中, 首先要保证网络内节点类型多样异构. 在北京邮电大学的校园网络环境中, 我们部署了大量异构通信节点, 包括各类型物联网节点 (摄像头、传感器、气味传感器等)、ad hoc 节点等. 此外, 对于有运算能力的设备, 我们在其上部署多版本的操作系统. 例如 Windows XP/7/10, Ubuntu 16/18/20, CentOS 6/7/8 等. 之后, 我们运行了大量的正常应用, 并收集了各种正常网络应用的加密流量. 我们随机选择 100000 条完整的加密会话作为负样本集来补充实验数据集 2. 相应地, 为了模拟恶意代码在异构网络节点大量共存的网络环境中的行为, 在 100 余个异构节点 (物联网节点) 上部署了 50 种恶意代码监测其运行, 并采集 50000 条完整的加密会话作为实验数据集 2 的第 2 部分正样本集组成.

需要注意的是, 现实世界数据收集中的噪声标签是网络安全领域的一个重大问题. 以上 3 个数据集都只在流量捕获的粒度级别 (packet capture) 进行了标记. 然而, 即使在恶意软件的流量捕获中, 正

常的网络通信行为仍然存在. 恶意软件的非核心行为 (如访问 Google 以验证网络连通性) 发起的加密会话会被标记为恶意的. 相应地, 加密恶意会话也可能存在于正常流量捕获而被标记为正常. 因此, 我们过滤了所有域名为已知合法站点 (如 Google, Twitter, Youtube, Reddit) 的加密会话. 在过滤过程中, Alexa Top-100 万热门站点列表被用作白名单, 以最大程度地减少噪声标签的影响进而取得更好的性能.

实验数据集 1 和 2 首先被按照 6:2:2 的比例随机分成训练、验证和测试集. 可以看出, 实验数据集 1 主要用于验证 ET-RSGAT 在加密恶意流量检测工作中的有效性. 而实验数据集 2 可以验证 ET-RSGAT 是否能够应对 6G 通信网络中大量异构终端即时、无限制通信的挑战.

本实验中, 模型的运行环境为 24 核 Intel(R) Xeon(R) Gold 6240R CPU @2.40 GHz, 64 GB RAM 和 2×NVIDIA Quadro RTX 5000 GPU. 基于 python 3.8.5 开发实验代码并在 Ubuntu 18.04.5 操作系统支持的 Pytorch-GPU 框架上执行. 我们利用精度、召回率和 Micro-F1 这 3 种指标来评估算法的性能.

5.2 用于比较的基准模型

为了验证所提出模型的有效性, 我们选择了多种恶意流量检测领域的基准方法进行了比较, 具体包括:

ET-LR. 逻辑回归是在许多加密恶意流量检测研究中流行的模型. 给定精心设计的特征, 它可以有效地识别加密恶意流量, 并具有理想的鲁棒性和可解释性.

ET-RF. 随机森林是一种由决策树集合组成的监督学习算法, 使用 bootstrap 聚合 (即 bagging 方法) 进行训练. 在加密恶意流量检测中, 该方法可以解释数据包长度和 TLS 握手元数据等特征的重要性, 有助于早期检测并提高检测性能.

ET-MLP. 多层感知器是一类前馈人工神经网络, 已被证明在许多任务中是非常先进的, 尤其是在网络安全领域. 作为一般的神经网络, 它通用于加密恶意流量检测, 以进行性能比较和评估.

ET-CNN. 卷积神经网络 (CNN) 是目前最流行的表示学习方法之一, 它可以帮助研究人员从原始数据中自动学习最佳表示, 而无需专家知识和精心设计的特征. 在这里, 我们从 TLS 握手的原始字节中学习每条加密会话的表示以检测恶意活动.

ET-GCN. 图卷积网络将经典的卷积神经网络推广到图结构数据. GCN 直接对整张图进行图卷积操作. 在本文中, 我们实现了 ET-GCN, 这种基于 GCN 的加密恶意流量检测方法以加密双向流的特征和相关性作为输入.

ET-RSGAT. 本文提出的加密恶意流量检测框架, 可以全面地处理握手消息与所有相关流的通信模式. 基于 2 类图注意力操作, 从访问服务的可信度和通信模式的平稳性的角度识别加密的恶意会话. 我们还测试了 ET-RSGAT 的 3 个变体来综合评估每个组件的性能. 分别是:

ET-RSGAT without noise. ET-RSGAT 的简化版本, 去除了面向平稳性的图注意力层之后的高斯噪声添加操作.

ET-RGAT. ET-RSGAT 的简化版本, 去除了面向平稳性的图注意力操作, 只关注访问网络服务的可信度.

ET-SGAT. ET-RSGAT 的简化版本, 去除了面向可信度的图注意力操作, 只关注通信模式的平稳性.

表 2　加密恶意流量检测中不同方法的性能比较

Table 2　Performance comparison of different encrypted malicious traffic detection approaches

	CTU			BUPT-ETC		
	Precision	Recall	Micro-F1	Precision	Recall	Micro-F1
ET-LR	93.29	91.63	92.45	96.62	96.93	96.77
ET-RF	98.59	98.27	98.43	98.51	98.81	98.66
ET-MLP	96.94	96.63	96.79	97.33	96.58	96.96
ET-CNN	99.22	98.54	98.88	99.21	99.25	99.23
ET-GCN	99.54	98.93	99.24	99.55	99.28	99.41
ET-RGAT	99.42	98.91	99.16	99.50	99.45	99.47
ET-SGAT	74.56	75.16	74.86	81.76	85.01	83.36
ET-RSGAT without noise	99.51	99.22	99.36	99.66	99.24	99.45
ET-RSGAT	99.69	99.55	99.62	99.91	99.88	99.90

5.3　性能评估与结果分析

在 CTU 与 BUPT-ETC 数据集上, 我们进行了大量实验, 以评估 ET-RSGAT 与上述基准模型的性能. 对于每个实验, 我们重复 10 次, 并取精度、召回率和 Micro-F1 的平均值作为最终结果. 表 2 表明本文提出的 ET-RSGAT 模型在传统网络与模拟环境数据集上所有评估指标的表现都优于其他基准模型. 图 4 显示了 ET-RAGAT 模型与其他基准模型在 3 个评价指标上的性能对比情况.

本文方法的优越性可以归因于以下几个方面:

首先, 现有的加密恶意流量检测研究, 不管是基于经典机器学习还是新兴深度学习 (例如, ET-LR, ET-RF, ET-MLP, ET-CNN) 的研究, 只单独关注孤立的分析单元 (网络流、会话或多元组连接) 而不考虑它们之间的相关性. 为了弥补这一差距, 我们构建了加密流量图 ETG 来整合加密会话间的复杂关系, 它可以更精细地描述通信行为并更好地建模加密会话的全局和局部结构关系. 与基于单流的孤立分析相比, 基于图的协同分析更能够从全局角度同时处理所有相关的加密会话, 从而识别高度隐蔽的威胁活动. 在基于独立单元分析的基准模型中, ET-RF 和 ET-CNN 在两个数据集的所有评估指标上都取得了比 ET-LR 和 ET-MLP 更好的性能. 值得注意的是, 即使与表现最好的 ET-CNN 相比, ET-RSGAT 在两个数据集上的 Micro-F1 指标方面也实现了大约 0.7% 的提升.

其次, 虽然在 ETG 中建立了加密会话之间的连接来模拟它们的复杂关系, 但在确定加密会话是否恶意时, 不同相关加密会话的影响显然是不同的. 与 ET-GCN 利用多个传播层来简单地聚合整个图上的邻域信息相比, ET-RSGAT 利用图注意力机制自适应地为相同邻域的节点分配不同的重要性, 并以 inductive 的方式工作. 这样可以更准确地描述不同的关系并推广到完全未知的加密会话. 在 CTU-13 数据集和 BUPT-ETC 数据集上, ET-RSGAT 相对于 ET-GCN 在 Micro-F1 分数提高了 0.38% 和 0.49%. 虽然看上去提升不大, 但需要注意的是, ET-GCN 只能被应用于图结构固定的设定, 即以 transductive 的方式工作, 而不能被推广到全新的流量数据. 尽管实验数据集被分为训练、验证和测试集, 但它们仍被构建成一张固定的图, 在所有阶段 (即训练、验证和测试) 中, 使用不同的掩码作为输入. 全局拓扑结构和测试集的信息在训练阶段不可避免地被利用, 因此, 尽管 ET-GCN 取得了令人满意的性能, 但它不能推广到未知的流量数据, 因此是不实用的. 我们在 inductive 设定中提出的 ET-RSGAT 在具有可扩展大小的未知加密流量图上效果很好, 性能上也优于 ET-GCN.

第三, 我们为每条加密会话定义了两类表示 (即握手消息和通信模式), 并提出了面向可信度与平

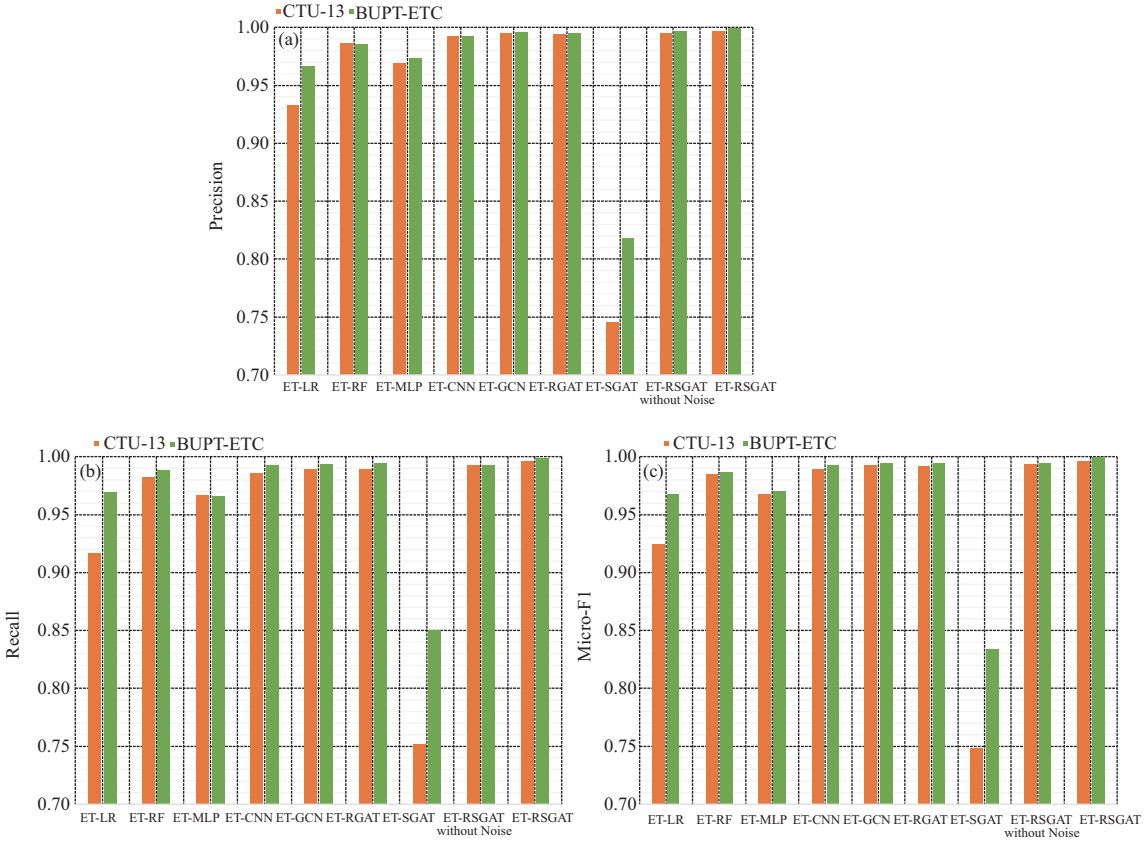

图 4 (网络版彩图) ET-RSGAT 与其他基准模型在精确率 (a), 召回率 (b), Micro-F1 (c) 上的比较

Figure 4 (Color online) Comparison of precision (a), recall (b) and Micro-F1 (c) between ET-RSGAT and other baseline models

稳性的图注意力机制来分别处理这些表示. 此外, 在平稳性表示中添加了高斯噪声以增强鲁棒性. 为了验证本文提出的图注意力机制和高斯噪声添加设定在加密恶意流量检测中的有效性, 我们实现了 ET-RSGAT 的 3 种变体, 即 ET-RGAT, ET-SGAT 和 ET-RSGAT without noise. 单独来看, ET-RGAT 只使用了面向可信度的图注意力机制, 而去除了面向平稳性的图注意力机制, 而 ET-SGAT 则相反. 相应地, ET-RSGAT without noise 去除了高斯噪声. 综上所述, ET-RSGAT 在精度和 Micro-F1 方面优于 ET-RGAT, ET-SGAT 和 ET-RSGAT without noise, 这说明同时从可信度和平稳性两方面去检测隐藏在加密流量中的威胁活动是合理有效的.

5.4 参数敏感性实验

本小节对 ET-RSGAT 中参数选择的敏感性进行了广泛的对比实验和分析, 包括 TLS 握手原始字节长度和 TLS 记录数量的选择.

在现有基于传统特征分析的工作中, ClientHello, ServerHello 和 Certificate 这 3 类 TLS 握手记录是最常用的信息. 我们这里不人工设定需要提取的特征, 而是应用一维卷积神经网络从 TLS 握手信息原始字节中自动学习最佳的特征表示. 具体来说, TLS 握手原始字节包含了握手阶段为后续加密通信使用的各种安全参数, 这是加密恶意流量检测任务中最有价值的信息. 而原始字节大小决定了要利用的握手信息多少, 在选择原始字节长度时应包括 ClientHello, ServerHello 与 Certificate 握手记录. 如图 5(a)

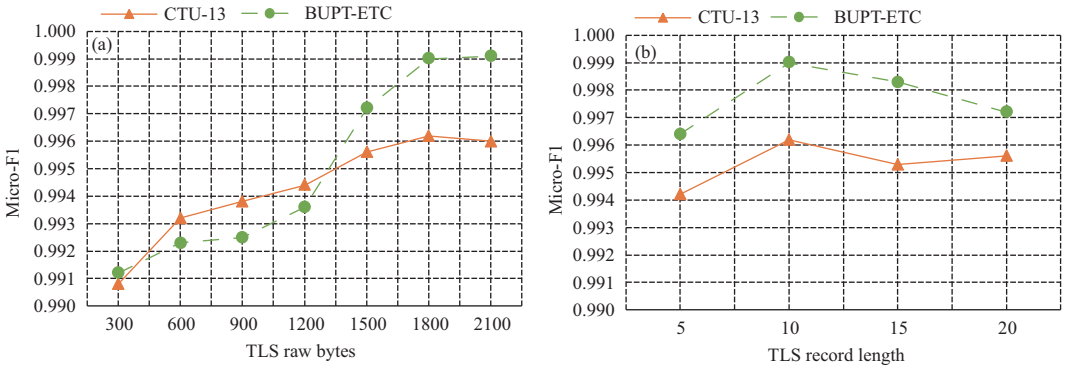

图 5 (网络版彩图) ET-RSGAT 在 (a) 不同原始字节长度和 (b) 不同 TLS 记录数量选择下的 Micro-F1 的比较

Figure 5 (Color online) Comparison of Micro-F1 among ET-RSGAT under the different raw byte lengths and TLS record counts

所示, 我们测试了 ET-RSGAT 在 TLS 握手原始字节长度取值为 300, 600, 900, 1200, 1500, 1800, 2100 时的表现, 在不同原始字节长度选择上检测模型取得了不同的效果, 当原始字节长度设置为 1800 时效果最佳. 虽然大多数 Certificate 记录中会包含由多个证书构成的证书链, 数据长度远远超过 1800. 但取前 1800 个字节可以有效包含证书链中的第一条证书也即用户证书, 该证书为加密会话访问的服务器所有, 反映了业务的可信度.

TLS 记录长度序列则更好地反映了加密流量承载的应用程序类型和 TLS 会话的通信模式. TLS 记录数量的影响如图 5(b) 所示, 我们测试了 ET-RSGAT 在 TLS 记录数量取值为 5, 10, 15, 20 时的表现, 发现 TLS 记录数量选择对检测模型性能的影响小于 TLS 握手信息原始字节长度选择的影响. 当我们将 TLS 记录数量设置为 10 时, ET-RSGAT 取得了最优性能, 前 10 个 TLS 记录包括了握手记录与部分应用数据记录, 即只需要少部分加密传输数据的统计信息就可以实现通信模式的刻画, 以帮助识别加密恶意流量.

6 结论

网络通信技术不断发展, 6G 通信时代将会有更大规模、更多类型的异构设备加入网络通信. 流量加密技术在保证 6G 网络通信安全的同时也给恶意流量的检测带来了巨大挑战. 面向未来 6G 网络中必然存在异构终端设备大规模互联、恶意软件及其网络行为不断发展的特点, 本文提出了一种基于图神经网络的加密恶意流量检测方法, ET-RSGAT. 该检测方法首先将加密会话间的复杂关系建模为一个有向图, 之后在有向图的基础上将加密恶意流量检测问题转化为图上的节点分类问题. 具体来说, 我们从握手信息和通信模式这两个维度来表示单条加密会话, 并构建加密流量关系图 (ETG) 来建模它们的关系, 综合考虑通信的可信度与平稳性来自动化地识别加密恶意流量. 实验结果表明, ET-RSGAT 在传统网络与模拟环境数据集上的表现都优于现有的各种基准模型.

参考文献

1 Chettri L, Bera R. A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Int Things J, 2020, 7: 16–32

2 Li S, Xu L D, Zhao S. 5G Internet of Things: a survey. J Indust Inf Integr, 2018, 10: 1–9

3 Wang D, Chen D, Song B, et al. From IoT to 5G I-IoT: the next generation IoT-based intelligent algorithms and 5G technologies. IEEE Commun Mag, 2018, 56: 114–120
4 Saad W, Bennis M, Chen M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems. IEEE Network, 2020, 34: 134–142
5 Li Q B, Xiao R. The use of data mining technology in agricultural e-commerce under the background of 6G Internet of Things communication. Int J Syst Assur Eng Manag, 2021, 12: 813–823
6 Letaief K B, Chen W, Shi Y M, et al. The roadmap to 6G: AI empowered wireless networks. IEEE Commun Mag, 2019, 57: 84–90
7 Gui G, Liu M, Tang F X, et al. 6G: opening new horizons for integration of comfort, security, and intelligence. IEEE Wirel Commun, 2020, 27: 126–132
8 You X H, Wang C X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301
9 Faisal A, Zulkernine M. A secure architecture for TCP/UDP-based cloud communications. Int J Inf Secur, 2021, 20: 161–179
10 Hu Q W, Asghar M R, Brownlee N. A large-scale analysis of HTTPS deployments: challenges, solutions, and recommendations. J Comput Secur, 2021, 29: 25–50
11 Durumeric Z, Ma Z, Springall D, et al. The security impact of HTTPS interception. In: Proceedings of the 24th Network and Distributed System Security Symposium (NDSS), San Diego, 2017. 1–14
12 Yaacoubi O. The rise of encrypted malware. Netw Secur, 2019, 2019: 6–9
13 Roccia T. Malware packers use tricks to avoid analysis, detection. McAfee Blogs. 2017. https://www.mcafee.com/blogs/enterprise/malware-packers-use-tricks-avoid-analysis-detection/
14 Shekhawat A S, Troia F D, Stamp M. Feature analysis of encrypted malicious traffic. Expert Syst Appl, 2019, 125: 130–141
15 Wang W, Zhu M, Wang J L, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks. In: Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, 2017. 43–48
16 Anderson B, Paul S, McGrew D. Deciphering malware's use of TLS (without decryption). J Comput Virol Hack Tech, 2018, 14: 195–211
17 Anderson B, McGrew D. Machine learning for encrypted malware traffic classification: accounting for noisy labels and non-stationarity. In: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, 2017. 1723–1732
18 Strasak F. Detection of https malware traffic. Dissertation for Bachelor Degree. Prague: Czech Technical University, 2017
19 Velan P, Čermák M, Čeleda P, et al. A survey of methods for encrypted traffic classification and analysis. Int J Netw Mgmt, 2015, 25: 355–374
20 Rezaei S, Liu X. Deep learning for encrypted traffic classification: an overview. IEEE Commun Mag, 2019, 57: 76–81
21 Creech G, Hu J K. A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. IEEE Trans Comput, 2014, 63: 807–819
22 Zhang H, Papadopoulos C, Massey D. Detecting encrypted botnet traffic. In: Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM), Turin, 2013. 1–6
23 Sourabh S. Demystifying Malware Traffic. Global Information Assurance Certification Paper. 2016. https://www.sans.org/white-papers/37222/
24 Roesch M. Snort: lightweight intrusion detection for networks. In: Proceedings of the 13th USENIX Conference on System Administration, Washington, 1999. 229–238
25 Dai R, Gao C, Lang B, et al. SSL malicious traffic detection based on multi-view features. In: Proceedings of the 9th International Conference on Communication and Network Security, Chongqing, 2019. 40–46
26 Liu J Y, Zeng Y Z, Shi J Y, et al. MalDetect: a structure of encrypted malware traffic detection. Comput Mater Continua, 2019, 60: 721–739
27 Bazuhair W, Lee W. Detecting malign encrypted network traffic using Perlin noise and convolutional neural network. In: Proceedings of the 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas.

2020: 200–206
28 Yang Y, Kang C C, Gou G P, et al. TLS/SSL encrypted traffic classification with autoencoder and convolutional neural network. In: Proceedings of the 20th International Conference on High Performance Computing and Communications, Exeter, 2018. 362–369
29 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. Inf Sci, 2020, 511: 284–296

Towards traffic supervision in 6G: a graph neural network-based encrypted malicious traffic detection method

Jianjin ZHAO[1,2], Qi LI[1,2*], Shengli LIU[3], Yanqing YANG[1,2] & Yueping HONG[1,2]

1. *School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*;
2. *National Engineering Laboratory of Mobile Internet Security Technology, Beijing* 100876*, China*;
3. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450001*, China*
* Corresponding author. E-mail: liqi2001@bupt.edu.cn

Abstract As an important direction for the evolution of next-generation wireless communication technology, 6G will comprehensively promote the wave of economic and social digitization. Services carried by 6G network will rely heavily on the sharing and processing of massive amounts of data between entities, data security is therefore of great importance. Currently, most network applications utilize SSL/TLS protocols to ensure the confidentiality and security of network communications, while encryption mechanism also brings huge challenges to network security supervision. Though encrypted malicious traffic detection in traditional networks has become a research hotspot, existing technologies cannot be directly applied in 6G networks. In a 6G network with massive, instant and unlimited communications between heterogeneous terminals, network communication behavior patterns are much more diversified, which makes the boundary between normal traffic and malicious traffic more blurred in 6G networks than in traditional networks. Existing studies either analyze encrypted traffic in isolation or aggregation, while they all ignore the rich correlations among encrypted traffic. To this end, we propose an encrypted malicious traffic detection framework based on the graph neural network towards the network security problem of future 6G networks, ET-RSGAT. First, considering the characteristics of super high speed and super large connection of 6G network, we design a simple feature extraction method of encrypted traffic: extracting the TLS handshake raw bytes and TLS record length sequence for one single encrypted session. Second, in view of the correlations of large numbers of heterogeneous terminals and the coexistence of multi-source heterogeneous data communication in 6G networks, we analyze the correlations between encrypted sessions from 2 aspects, which are service correlations and communication behavior correlations. Then we construct an encrypted traffic graph, named ETG. On the basis of ETG, we introduce a graph attention network to utilize the correlations between encrypted sessions to enrich the feature representation of nodes. With rich representation, we build the detection model based on a multi-layer perceptron to identify threats. Considering that the simulation environment of 6G networks is immature, we deploy a variety of heterogeneous terminal nodes and run various network services to simulate the 6G communication scenario, and design related experiments for the interconnection of many heterogeneous terminals in 6G networks. The evaluation and experimental results show that our method can obtain satisfactory detection results in both traditional network and simulated environment datasets.

Keywords 6G, malicious traffic detection, encrypted traffic, graph neural network, attention mechanism