IBNAD: 一种基于交互的 5G 核心网网络功能异常检测模型

张伟露[1], 吉立新[1,2], 刘树新[1,2], 李 星[1,2], 潘 菲[1,2], 胡鑫鑫[1]

[1]中国人民解放军战略支援部队信息工程大学 郑州 中国 450001
[2]国家数字交换系统工程技术研究中心 郑州 中国 450002

摘要 现有 5G(5th Generation Mobile Communication Technology)核心网异常检测主要基于信令流量深度解析, 但较少利用核心网网络功能交互关系的作用。针对上述问题, 提出一种基于交互的 5G 核心网网络功能异常检测模型。首先, 该模型以行为分析为驱动, 基于信令流量和网络功能注册数据提取多维属性, 通过行为画像来表征网络功能行为模式, 并采用集成学习算法 RFECV(Recursive Feature Elimination with Cross-Validation)进行属性特征选择, 降低特征维度的同时筛选出与区分网络功能行为模式高度相关的属性特征。然后, 模型基于网络功能交互关系对核心网进行图建模, 建模后的图数据融合了网络功能属性信息和交互信息。最后, 模型通过基于空间域的图卷积网络聚合邻域节点属性信息和结构信息来融合行为模式特征, 新生成的节点表示用于分类, 从而将核心网网络功能异常检测问题转化为图节点分类问题。通过在 free5GC 仿真平台上采集数据, 并在搭建的异常检测系统中的实验表明, 该模型的异常检测性能优于基于属性特征分析的传统机器学习模型、基于结构特征分析的图嵌入模型及部分 5G 核心网异常检测模型。10%数据集作为训练集时, 所提模型的准确率比支持向量机模型提高 6.6%, 比 Struc2vec 模型提高 13%, 比深度神经网络模型提高 8%。

关键词 5G 核心网; 异常检测; 行为画像; 网络建模; 图神经网络
中图法分类号 TN918; TP391 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2024.05.07

IBNAD: An Interaction-based Model for Anomaly Detection of Network Function in 5G Core Network

ZHANG Weilu[1], JI Lixin[1,2], LIU Shuxin[1,2], LI Xing[1,2], PAN Fei[1,2], HU Xinxin[1]

[1]PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
[2]National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002, China

Abstract The existing 5G (5th Generation Mobile Communication Technology) core network anomaly detection is mainly based on the deep analysis of signaling traffic. However, the existing researches seldom consider the interaction of core network functions. Aiming at the above problems, an interaction-based model for anomaly detection of network function in 5G core network is proposed. First of all, driven by behavior analysis, this model extracts multidimensional attributes based on signaling traffic and network function registration data, and characterizes the network function behavior mode through behavior portraits. In addition, the model also uses the integrated learning algorithm RFECV (Recursive Feature Elimination with Cross Validation) to select attribute features, so as to reduce the feature dimension and screen out the attribute features highly related to the differentiated network function behavior mode. Then, the core network is modeled as a graph based on the network function interaction relationship, and the graph structure data after modeling integrates the network function attribute information and interaction information. Finally, this model uses graph convolution network based on spatial domain to aggregate attribute information and structure information of neighborhood nodes to fuse behavior pattern features. The newly generated node representation is used for classification, thereby transforming the core network function anomaly detection problem into the graph node classification problem. Through the data collection on the free5GC simulation platform and the experiments in the built anomaly detection system, it is shown that the anomaly detection performance of this model is superior to the traditional machine learning model based on attribute feature analysis, graph embedding model based on structural feature analysis and some 5G core network anomaly detection models. When 10% of the data set is used as the training set, the accuracy of the proposed model is higher than that of support vector. The machine model is improved by 6.6%, 13% higher than the Struc2vec model, and 8% higher than the deep neural network model.

通讯作者: 李星, 博士, 助理研究员, Email: lixing_ndsc@163.com。
本课题得到河南省重大科技专项项目(No. 221100210100)资助。
收稿日期: 2022-07-08; 修改日期: 2022-10-13; 定稿日期: 2024-01-22

Key words 5G core network; anomaly detection; behavioral portraits; network modeling; graph neural network

1 引言

欧盟网络与信息安全局(European Network and Information Security Agency , ENISA)在年度报告[1]中指出 2020 年欧盟地区发生 170 起移动通信安全重大事故, 累计损失 8.41 亿用户小时, 一些有针对性的 DDoS(Distributed Denial of Service)攻击、信令攻击、SIM(Subscriber Identity Module)卡交换等较小规模事件还未统计在内。5G 系统采用基于服务的架构(Service Based Architecture), 使用互联网协议作为核心网信令协议, 引入软件定义网络(Software Defined Network, SDN)、网络功能虚拟化(Network Function Virtualization, NFV)、网络切片(Network Slice, NS)等技术, 实现 5G 愿景的同时也带来安全问题[2]。近年来标准组织、研究机构和学术界致力于 5G 安全研究, 取得大量成果。

标准组织和研究机构方面, 3GPP 将 5G 系统划分为网络接入域、网络域、用户域、应用程序域、SBA 域、安全的可见性和可配置性共 6 域安全[3], 并具体分析了 5GC 中关于 SBA 域的 20 个关键安全问题[4]。ENISA 更新发布《ENISA Threat Landscape for 5G Networks Report》[5], 总结了 17 类核心网漏洞及解决措施。中国信息通信研究院(China Academy of Information and Communications Technology, CAICT)发布了《5G Security Report》[6]和《5G 安全知识库》[7], 介绍了接入网、核心网、边缘计算等 8 大安全模块及 188 项安全措施, 从资源可用性保护、NEF (Network Exposure Function)安全、流量保护、内外边界隔离、网络功能(Network Function, NF)合法身份保障、虚拟机资源保护、用户标识符保护、漫游安全 8 个方面具体分析了核心网安全问题。

学术研究方面, Kim H[8]对 5G 核心网控制平面和用户平面攻击进行了分类, 指出 5G 核心网使用 HTTP/2 作为信令承载协议同时继承了传统 HTTP/2 安全漏洞, 成为 5G 核心网一个新安全问题。Park J H, Rathore S, Singh S K 等人[9]概述了 5G 引入新技术如 SDN、NFV、NS 等导致的新安全挑战。Khan R, Kumar P, Jayakody D N K 等人[10]回顾了已有 5G 安全威胁研究成果, 介绍了针对核心网的 DDoS(Distributed Denial of Service)攻击、TLS(Transport Layer Security)/SSL(Secure Sockets Layer)攻击、SDN 扫描等攻击行为。Zhang S, Wang Y, Zhou W 等人[11]从整体安全架构、云基础设施、物联网应用和核心网等方面详细讨论了 5G 安全和隐私的潜在解决方案。Park S, Kim D, Park Y 等人[12]将 5G NSA(Non-Stand Alone)安全威胁划分为无线接入网和核心网, 构建攻击树, 对开发的 15 个测试用例在 3 家移动运营商的实际网络上进行验证, 识别出 8 个漏洞。

标准组织、研究机构、学术界给予 5G 安全尤其是核心网安全足够重视, 研究主要聚焦两个方面: 一是完善上层机制以规避可预知的安全漏洞[3-7], 二是研究新关键技术漏洞以阻断可能的威胁行为[8-12]。但研究侧重于理论分析, 多样化的安全机制难以在工业界标准化, 实际硬件环境中实现难。

本文聚焦 5G 核心网安全, 通过研究 NF 异常检测达到及时发现网络存在的安全威胁。异常检测作为识别网络入侵的有效手段, 在 5G 核心网中研究应用的成果较少。已有的 5G 核心网异常检测主要基于信令流量和性能指标两类数据源进行异常检测, 本文主要研究基于信令流量的异常检测。辛冉等人[13]提出 5G 核心网 NF 服务安全需解决网络协议、网络架构、NF 交互 3 个基本安全问题, 设计了服务安全异常检测模型, 建立了序列基线、参数基线、API 操作基线, 模型在含异常场景的流量数据上可以有效检测出服务异常。Jordan Lam 等人[14]将软件定义安全性与机器学习相结合, 设计一种基于机器学习的 SDS(Software Defined Security)系统, 将接入网和核心网流量转换为图像供卷积神经网络分析, 实现了 5G 网络恶意流量检测。但基于基线的方法忽视了 5G 核心网使用 TLS(Transport Layer Security)加密现状, 基于加密信令的基线建立难度大; 基于卷积神经网络的方法对基于合法流量的恶意行为识别效果不好, 流量转图像加重了数据处理负担, 且上述方法均未考虑核心网 NF 交互关系对异常检测的作用。

针对上述问题, 本文提出一种基于交互的 5G 核心网 NF 异常检测模型(Interaction-based Network Function Anomaly Detection, IBNAD), 该模型是端到端的, 贯穿数据汇聚、特征提取、特征筛选、网络建模、异常识别整个异常检测流程, 在现有 5G 核心网异常检测研究型成果较少的情况下, 可供后续研究者参考和对比, 主要贡献如下:

(1) 针对现有 5G 核心网异常检测模型仅考虑信令流量本身, 较少考虑 NF 交互关系作用的问题, 提出一种基于交互关系的 5G 核心网图建模方法, 建模后的图融合了 NF 交互、信令流量、NF 注册多源信息。

(2) 鉴于加密场景下深度包解析(Deep Packet

Inspection, DPI)技术的局限性, 以行为分析为驱动, 提出一种 NF 行为画像方法。该方法基于信令流量和 NF 注册数据提取多维属性来表征 NF 行为模式, 通过同类 NF 行为模式比较来发现异常。此外, 采用递归特征消除与交叉验证结合(Recursive Feature Elimination with Cross-Validation, RFECV)的集成机器学习算法进行属性选择以筛选出与 NF 行为模式高度相关的属性, 提升检测性能。

(3) 考虑到现有 5G 核心网异常检测模型不能处理图结构数据, 采用基于空间域的两层 GCN 对 5G 核心网图结构数据进行学习并分类, 将 5G 核心网异常检测问题转化为图的节点分类问题。

(4) 基于开源 free5GC 平台进行实验仿真及验证, 结果表明 IBNAD 模型对 5G 核心网 NF 异常检测性能优于传统机器学习模型和经典图嵌入模型。

2 相关工作

异常检测, 又称离群点检测, 指检测明显偏离大多数数据实例的数据实例的过程[15]。本节既介绍了 5G 核心网异常检测研究现状, 又从传统机器学习和图表示学习方法两方面介绍当前异常检测研究现状。

2.1 5G 核心网异常检测

5G 核心网异常检测公开的研究成果较少, 文献[16]构建了一种基于多维特征融合的 5G 核心网故障预警模型, 通过关键绩效指标(Key Performance Indicator, KPI)、指标统计特征、历史告警信息构建多维特征矩阵, 采用 XGBoost(EXtreme Gradient Boosting)算法与深度神经网络(Deep Neural Networks, DNN)算法来训练模型而达到异常检测目的。文献[17]指出海量物联网设备接入扩大了核心网的攻击面, 但存在流量属性缺失导致异常分析难度加大的问题, 并针对性提出一种多核聚类(Multiple-kernel Clustering, MKC)算法的入侵检测方法。文献[18]提出基于流量特征分析、异常流量检测、监控诊断三个虚拟网络功能的异常流量检测方法, 其中异常流量检测以特征分析后的时间序列为输入, 采用 GRU(Gate Recurrent Unit)网络检测。文献[19]选取决策树、DBSCAN (Density-Based Spatial Clustering of Applications with Noise)、熵值法等数据统计方法进行异常检测。实验结果表明, 决策树方法效果最佳。文献[20]分析 5G 核心网存在访问流量基线异常、命令与控制通信异常、加密流量基线异常等, 通过建立通信业务访问矩阵, 形成预制访问关系, 将实际访问与预制访问关系进行对比以发现潜在威胁。文献[21]提出一种智能网络防御体系以保护 5G 系统端到端安全, 该防御体系由设备攻击检测、边缘攻击检测、核心攻击检测和监督攻击检测 4 个系统构成, 其中核心攻击检测系统采用深度学习神经网络来检测针对核心网网络功能的内部攻击。

上述研究虽针对 5G 核心网异常检测已取得一定效果, 但没有考虑 5G 核心网虚拟化、服务化的新特性, 忽略了 NF 交互关系对异常检测的作用, 亟需结合 5G 核心网新特性, 提出针对性异常检测模型。

2.2 基于传统机器学习的异常检测

一直以来, 传统机器学习在异常检测领域发挥着重要作用[22]。该类方法多以数据统计特征为模型输入, 根据特征进行分类、聚类从而达到异常检测的目的。支持向量机(Support Vector Machine, SVM) SVM[23-25]、决策树(Decision Tree, DT)[26-28]、随机森林(Random Forest, RF)[29-30]广泛应用于工业入侵检测系统, 是实现网络流量异常检测的重要模型。但支持向量机需要根据不同的数据样本选择合适的核函数, 且在面临大规模数据时效果不理想; 决策树易发生过拟合, 泛化性能差; 随机森林通过构建多个决策树降低了过拟合风险, 但同时也增加了计算复杂度。此外, 多层感知机(Multilayer Perceptron, MLP)、卷积神经网络(Convolutional Neural Network, CNN)、循环神经网络(Recurrent Neural Network, RNN)等神经网络模型也被应用于异常检测领域。文献[31]将序列特征选择与 MLP 相结合, 并设计一个反馈机制, 对分布式拒绝服务攻击的检测效果较好。文献[32]利用 MLP 来检测工业控制系统中的网络攻击, 实现结果优于孤立森林算法。文献[33]基于 CNN 开发了单包检测和序列检测两个模型用于解决有效载荷内容和包流转换攻击检测问题。但 CNN 大多用于图像识别, 因为图像中每个相邻的像素之间关系紧密, 可以通过池化操作获取图像的边缘信息和背景信息, 但相邻的流量特征之间并非都具有相关性, 池化操作反而会损失信息, 且 CNN 对内容合乎规范但行为模式异常的安全威胁检测效果不佳。文献[34]提出一种利用 INT(In-band Network Telemetry)和 RNN 的异常检测方法, 实现正常流量和异常流量分类。RNN 利用了时序信息, 常用于时间序列预测或异常检测, 但易存在梯度消失或梯度爆炸的问题。同样, 上述模型均没有考虑 NF 之间, NF 属性信息之间的相关性。

2.3 基于图的异常检测

传统异常检测通常通过识别特征空间中的离群点来解决, 这在本质上忽略了真实数据的关系信息, 图被广泛用于表示结构/关系信息, 因此引发基于图

的异常检测问题研究[35]。

为了从图结构中获取更多有价值的信息用于异常检测, 图嵌入方法得到广泛引用, 这些技术将图结构编码到嵌入的向量空间, 并通过与基于密度的技术或基于距离的技术相结合来识别异常节点。目前, 图嵌入方法如 Deepwalk[36]、LINE[37]、node2vec[38]和 struc2vec[39]已经显示出节点表示的有效性, 并被应用于异常检测[40-43]。图嵌入方法在捕捉网络结构方面存在明显优势, 对异常结构检测效果较好, 如越权访问。但由于没有利用节点特征和边的权重信息, 对通信结构正常但通信量异常, 如劫持合法用户的信令洪泛攻击, 检测效果差。

现实网络中除了结构信息外, 还包含丰富的与节点相关的属性信息, 节点属性信息与图结构信息结合可以检测到更多隐藏的异常[35]。图神经网络(Graph Neural Network, GNN)因其对图数据优异的非线性拟合性能受到广泛关注和深入探索[44]。

受上述讨论的两类异常检测方法或模型的启发, 结合 5G 核心网异常检测研究现状, 本文提出的模型基于信令流量、NF 注册信息提取特征, 基于 NF 交互关系对核心网建模, 从而同时拥有了节点属性信息和网络结构信息, 利用当前热门的图神经网络综合学习两类信息以构建分类器, 从而提高模型异常检测性能, 这在以往基于信令流量的核心网异常检测方法中较少涉及。

3 问题描述

为理解核心网 NF 异常检测问题及提出的 IBNAD 模型, 本节主要介绍 5G 核心网基础知识、图定义、符号定义、基于交互的 NF 安全威胁分析。

3.1 5G 核心网基础

核心网作为 5G 系统的“心脏”, 通过注册、注销、会话建立、会话释放等信令流程实现统一的策略控制、流量调度、连接管理和用户业务管理。

3GPP 组织将 5G 系统架构定义为基于服务的架构(Service Based Architecture, SBA), 由 AMF(Access and Mobility Management Function)、SMF(Session Management Function)、NRF(Network Repository Function)等虚拟化的 NF 构成, 非漫游场景下 5G 系统参考架构见图 1。NF 之间的交互有基于服务和基于参考点的两种方式, 而核心网控制平面内的 NF 只能使用基于服务的接口 (Service Based Interface, SBI)进行交互, 如图 2 所示。SBI 协议栈中 TLS 为传输层安全保护协议, HTTP/2 为应用层协议, JSON 为应用层序列化协议, 如图 3 所示。

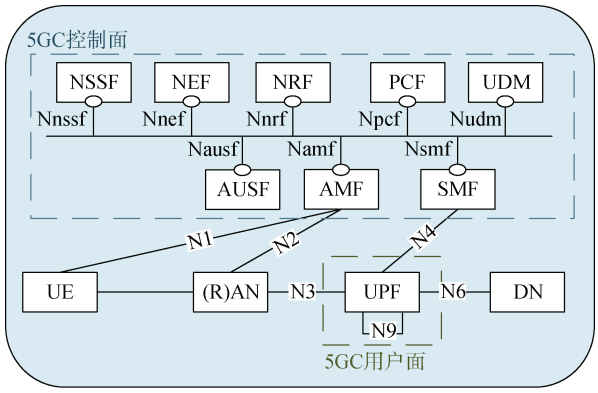


图 1 非漫游场景的 5G 系统参考架构

Figure 1 5G system reference architecture for non-roaming scenarios

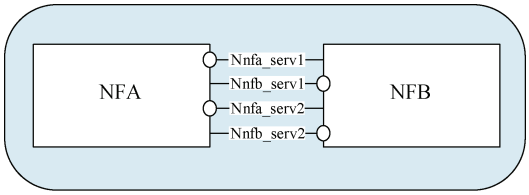


图 2 基于 SBI 的网络功能交互

Figure 2 SBI-based network function interaction

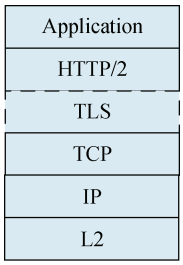


图 3 SBI 协议栈

Figure 3 SBI protocol stack

NF 服务是由 NF(NF 服务生产者)通过 SBI 向经授权的 NF (NF 服务消费者)公开的一种功能。一个 NF 可以公开多个服务。NF 服务由 NF 之间的一组交互组成。信令流程可以用一系列 NF 服务调用来描述。NF 服务框架功能包括服务注册/更新/注销、消费者授权、服务发现和服务间通信(包括选择和消息传递)[45]。为便于理解, 图 4 展示了交互、服务、信令流程、系统功能之间的关系, 服务由多个交互集合组成, 多个服务集合构成信令流程, 多个信令流程集合共同支撑 5G 系统功能。

3.2 图定义

图论中, 一个简单的图可定义为 $\mathcal{G}=(\mathcal{V},\mathcal{E},\Psi_{\mathcal{G}})$[46], 其中 $\mathcal{V}$ 是节点集合, 表示一组节点, $\mathcal{V}=\{v_1,v_2,v_3,\cdots,v_n\}$。$\mathcal{E}$ 是边集合, 表示一组连边, 即 $\mathcal{E}=\{e_1,e_2,e_3,\cdots,e_m\}$。$\Psi_{\mathcal{G}}$ 是关联集合, 表示边和节点的关联关系, $\Psi_{\mathcal{G}}=$

$\{\Psi_{\mathcal{G}}(e_i)|\Psi_{\mathcal{G}}(e_i)=v_s v_d, e_i\in\mathcal{E}, v_s\in\mathcal{V},\ \ v_d\in\mathcal{V}\}$。

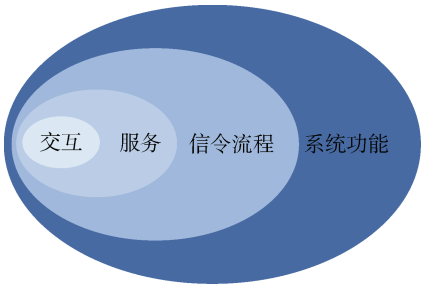


图 4　交互、服务、信令流程、系统功能关系

Figure 4　Relationship between interaction, service, signaling process, and system function

$\mathcal{G}$ 中每个节点有一个 d 维特征向量 $f_v\in R^d$，所有节点特征向量组成特征矩阵 $F\in R^{n\times d}$。邻接矩阵 $A\in R^{n\times n}$，表示节点间的相邻关系，即 $A=(a_{ij})_{n\times n}$，加权有向图上矩阵 A 第 i 行第 j 列上的元素 a_{ij} 定义如式(1)所示:

$$a_{ij}=\begin{cases} w_{ij}, \text{从节点 } i \text{ 指向节点 } j \text{ 的边权值为 } w_{ij} \\ 0\ , \text{没有从节点 } i \text{ 指向节点 } j \text{ 的边} \end{cases} \tag{1}$$

$\mathcal{Y}$ 代表节点的标签集合，y_v 代表节点 v_i 的标签值，表示节点是异常或正常节点。如何基于 NF 交互关系将 5G 核心网建模为图将在 4.4 节具体介绍。

3.3　符号定义

表 1　符号定义

Table 1　Definition of symbols

符号	含义
$\mathcal{D}$	源数据集
$\mathcal{G}$，$\mathcal{V}$，$\mathcal{E}$，$\mathcal{W}$	图，节点集，边集合，边权值集合
N，M	节点数，连边数
v_i，v_s，v_d	节点 i，源节点，目的节点
e_{ij}，w_{ij}	节点 i 指向 j 的有向边，边 e_{ij} 的权值
$\mathcal{Y}$，y_v，C	节点标签集，标签值，标签类别数
f_v，f_v^k	节点特征向量，节点第 k 维特征
F，A	特征矩阵，邻接矩阵
$\mathcal{A}$，a	基本属性提取函数集合，提取函数
$\mathcal{N}$，n	网络属性提取函数集合，提取函数
$\mathcal{B}$，b	行为属性提取函数集合，提取函数
$K_{\mathcal{A}}$，$K_{\mathcal{N}}$，$K_{\mathcal{B}}$	基本、网络、行为属性原始维度总数
$K'_{\mathcal{A}}$，$K'_{\mathcal{N}}$，$K'_{\mathcal{B}}$	基本、网络、行为属性降维后维度总数
K，k	特征维度总数，特征维度
$f_{v,STD}$，$f_{v,STD}^k$	节点标准化特征，第 k 维标准化特征
$f_{v,SEL}$，$f_{v,SEL}^k$	节点特征选择后的特征，第 k 维特征
L，l	GNN 总层数, GNN 层数
E，e	epoch 总数, epoch 数

3.4　基于交互的 NF 安全威胁分析

5G 核心网引入 NFV 技术[9]，攻击者利用虚拟化漏洞可劫持或者仿冒 NF[47]，主动发起偏离正常信令流程或通信模式以窃取、篡改、删除用户信息，干扰正常通信的异常行为。5G 核心网安全威胁包括越权攻击[48]、中间人攻击[49]、拒绝服务攻击[49-50]等。

如图 5 所示，以越权攻击、拒绝服务攻击、中间人攻击为例，安全威胁可以源于核心网域外，如恶意应用程序(Application Function, AF)、僵尸网络(Botnet)等，也可以源于核心网域内，如被劫持或仿冒的恶意 NF。上述恶意的 AF、NF、Botnet 通过发起异常交互行为(逻辑异常、频率异常、参数异常等)以达到其目的，这些异常在图中体现为节点或连边的某些属性异常，而图神经网络能够提取和发掘图结构数据中的特征和模式以达到分类、聚类、预测等任务需求，因此本文选择图神经网络作为 IBNAD 模型中执行分类任务的子模型。

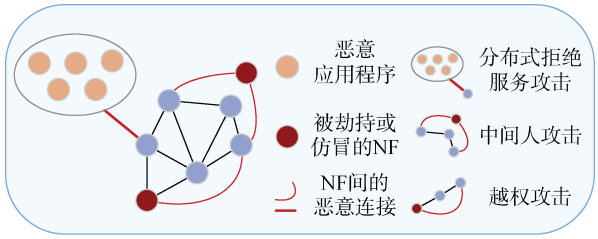


图 5　NF 安全威胁示意图

Figure 5　Schematic diagram of NF security threats

4　IBNAD 模型

4.1　模型概述

针对 5G 核心网 NF 异常检测问题，本文提出一个端到端的异常检测模型 IBNAD，涉及数据汇聚、特征提取、特征筛选、网络建模、异常识别等异常检测全流程，主要由核心网源数据汇聚、特征提取、网络建模、图神经网络 4 个模块构成。模型框架如图 6 所示，源数据汇聚模块主要功能是从 5G 核心网采集 NF 注册信息和信令流量。特征提取模块基于 NF 行为画像得到的多维属性，通过特征标准化和特征选择生成特征矩阵。网络建模模块结合邻接关系和节点特征构建图，便于图神经网络模块执行节点分类任务。本节剩余部分将对各模块作具体介绍。

4.2　核心网源数据汇聚

IBNAD 模型以行为分析为驱动，通过同类 NF 行为模式对比来分类 NF，因此建立相对完善的行为信息数据库是关键前提。

源数据汇聚模块主要功能是从 5G 核心网采集

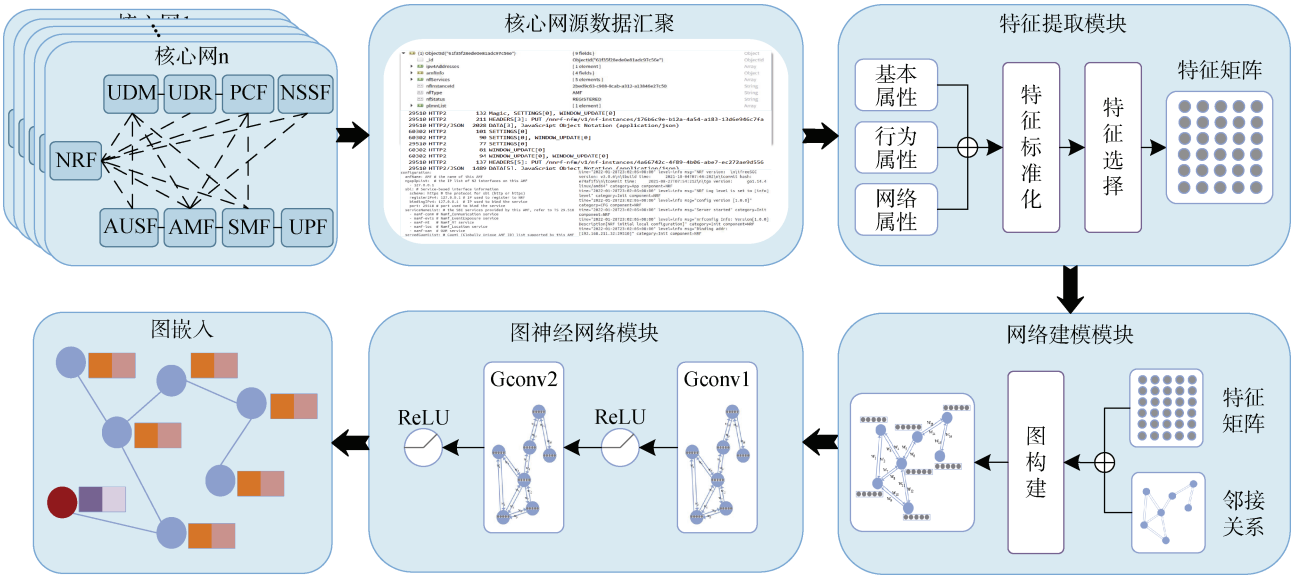


图 6　IBNAD 模型框架

Figure 6　Framework of the IBNAD model

NF 注册信息和信令流量。传统异常检测方法，特征来源单一，没有充分利用 NF 注册信息中丰富的身份信息和网络信息，因此本模型以注册信息和信令流量为源数据，通过特征提取模块提取多维属性信息，其中 NF 注册信息主要用于分析提取 NF 基本属性和网络属性，信令流量主要用于分析提取 NF 行为属性，从而为研究 NF 行为提供充足的信息。

4.3　特征提取

5G 开启万物互联时代，核心网信令流量规模也相应增大，给实时存储、测量与分析带来极大困难，因此需要通过引入特征提取来降低数据存储与处理的压力。IBNAD 模型区别以往仅基于流量特征和仅基于网络结构的异常检测模型，既利用了信令流量信息，又考虑了核心网 NF 间交互关系信息，特征提取模块设计的目的正是将不利于机器学习模型学习的流量序列映射到多维特征空间，映射后的特征空间保留了原始数据的主要信息，对异常具有良好的可分性，且特征存储的规模和特征处理的复杂度远远低于全流量存储与分析。本文所提出的特征提取模块主要由 NF 行为画像、特征标准化、特征选择三个子模块构成。

4.3.1　NF 行为画像

网络用户行为指网络空间内行为主体为实现特定目标，采用网络应用和协议作为手段及方法进行的有意识的活动。NF 作为 5G 核心网的行为实体，正常 NF 按照规范进行活动，而异常 NF 也会遵守部分规范以规避常见的检测，但更重要的是执行其背后隐藏的攻击者的意图，因此异常 NF 的行为模式与正常 NF 的行为模式存在可区分性。

交互设计之父 A.Cooper 最早提出并将用户画像定义为“基于用户真实数据的虚拟代表”，用户画像融合了用户基本属性、社会属性、行为属性、情境属性等多维信息，有助于分析用户不同阶段表现出来的行为特征、变化过程、动因要素等[51]。

本文受网络用户行为和用户画像两方面启发，提出一种 NF 行为画像方法，该方法基于信令流量和 NF 注册信息两类源数据，从基本属性、网络属性和行为属性三维视角利用多维属性特征对 NF 行为模式进行刻画，为构建分类器提供有效的数据输入。

基本属性指 NF 向 NRF 注册时使用或被分配的身份信息，其在 NF 生命周期内能够唯一标识一个 NF，对仿冒 NF 检测。基本属性按式(2)使用集合 $\mathcal{A}$ 中的函数从源数据中提取相关信息，如 nfInstanceId、nftype、nfip、nfervice_name 等，$\mathcal{A}$ 为预先定义好的基本属性提取函数集合，函数核心功能为关键信息匹配与识别。

$$f_{v,\mathcal{A}}^{k} = a_i(\mathcal{D}),\ a_i \in \mathcal{A} \tag{2}$$

网络属性又可称情境属性，是由 NF 所处的网络基本信息决定，如 network_id、taiList_mcc、taiList_mnc、taiList_tac、plmnList_mcc、plmnList_mnc 等，按式(3)使用网络属性提取函数集合 $\mathcal{N}$ 从源数据提取，$\mathcal{N}$ 中函数核心功能也为关键信息匹配与识别。

$$f_{v,\mathcal{N}}^{k} = n_i(\mathcal{D}),\ n_i \in \mathcal{N} \tag{3}$$

行为属性指 NF 参与核心网业务过程中的一系列动态特征。核心网信令流程一般由多个 NF 交互共同完成，从微观角度对某个信令流程或某两个 NF 的

具体交互进行检测存在加密背景下信令流程还原难度大, 单次 NF 交互合乎规范等问题。我们认为, 被劫持或仿冒的 NF 作为执行攻击者恶意意图的实体, 其微观行为在时间累积后呈现出异于正常 NF 的结果, 即以宏观行为作为 NF 行为画像的重要依据。因此, 提取阶段避免对信令流量包进行深度解析, 仅提取 NF 之间数据包数量和大小。以数据包数量和大小为基础, 按式(4)使用行为属性提取函数集合 $\mathcal{B}$ 中的多类函数扩展得到多维统计特征, 如总连接数、NF 数量、NF 类型数量、向各类 NF 发送流量总和, 从各类 NF 接受流量总和等, $\mathcal{B}$ 包括 sum、average、count 等。基于数据包浅层信息的统计特征适用于加密场景, 符合 5G 系统应用现状。

$$f_{v,\mathcal{B}}^{k}=b_i(\mathcal{D}),\ b_i\in\mathcal{B} \tag{4}$$

初步提取的特征中包含非数值型特征, 需要转换为数值型作为分类模型的输入, 因此需要对其进行数字编码, 本文选取基于字典的编码方法对非数值型特征进行重新编码。

最后, 行为特征、基本属性、网络属性特征如式(5)取并集共同构成 NF 的行为画像, 用式(6)所示向量表示。

$$f_v=f_{v,\mathcal{B}}\cup f_{v,\mathcal{A}}\cup f_{v,\mathcal{N}} \tag{5}$$

$$f_v=(f_{v,\mathcal{B}}^{1},...,f_{v,\mathcal{B}}^{K_{\mathcal{B}}},f_{v,\mathcal{A}}^{1},...,f_{v,\mathcal{A}}^{K_{\mathcal{A}}},f_{v,\mathcal{N}}^{1},...,f_{v,\mathcal{N}}^{K_{\mathcal{N}}}) \tag{6}$$

4.3.2 特征标准化

经特征提取得到的不同维度特征量级相差较大, 使用梯度下降法寻求最优解时, 不利于模型收敛, 因此需要对特征进行标准化以消除特征间量级差异影响, 加速模型收敛速度, 提升模型性能。z-score 标准化使用 z-score 值衡量特征值, 以此将不同维度的不同量级数据转化为统一量级, 保证数据之间的可比性, z-score 计算方式如(7)所示。

$$f_{v,STD}^{k}=\frac{f_v^{\,k}-\mu}{\sigma} \tag{7}$$

其中 $\mu=\frac{1}{N}\sum_{i=1}^{N}f_{v_i}^{\,k}$ 为样本平均值, $\sigma=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(f_{v_i}^{\,k}-\mu)^2}$ 为数据标准差。对数据进行标准化后, 数据的平均值变为 0, 方差变为 1。

4.3.3 特征选择

使用高维数据集训练过程中, 并非所有特征都与分类结果相关, 易引起时间复杂度高、准确率降低等问题, 特征选择作为解决方案, 可以减少特征数量以防止维度灾难, 缩短训练时间, 可以筛选出与区分 NF 行为正常与否高度相关的属性特征, 增强模型的泛化能力和可解释性。虽然我们提取的原始特征仅 84 维, 但实际应用中 NF 的数量、类型、注册信息较实验更加丰富, 特征维度也会随之大规模增加, 因此预先在 IBNAD 模型中研究并引入特征选择十分必要, 本文使用 RFECV 作为特征选择算法。

RFECV 是一种特征选择的包装方法, 通过删除对训练误差影响最小的冗余特征, 保持独立性强特征, 提高了模型的泛化性能[52]。RFECV 核心思想是递归特征消除和 K-fold 交叉验证, 递归特征消除是一种后向特征消除思想, 选择分类器遍历所有特征子集可获得每一维特征的排名、选择的最优特征数量及特征子集。K-fold 叉验证的基本思想是将原数据集分为 K 组, 其中 K-1 份用作训练, 1 份用作验证, K 次结果均值作为算法精确度值, 目的是提高模型的可靠性稳定性。

本文选择极端随机树(Extra Trees Classifier)作为分类器。极端随机树是一种集成学习技术, 通过聚集多个去相关决策树的结果输出分类结果, 相比随机森林算法的样本、特征、参数和模型随机, 增加了分叉随机, 比随机森林泛化性能更好。

经过特征标准化和特征选择后的所有 NF 特征向量共同构成特征矩阵 $\boldsymbol{F}$ 作为网络建模的基础之一, 特征矩阵如式(8)所示。

$$\boldsymbol{F}=\begin{pmatrix} f_{v_1,\mathcal{B}}^{1} & \cdots & f_{v_1,\mathcal{B}}^{K'_{\mathcal{B}}} & f_{v_1,\mathcal{A}}^{1} & \cdots & f_{v_1,\mathcal{A}}^{K'_{\mathcal{A}}} & f_{v_1,\mathcal{N}}^{1} & \cdots & f_{v_1,\mathcal{N}}^{K'_{\mathcal{N}}} \\ f_{v_2,\mathcal{B}}^{1} & \cdots & f_{v_2,\mathcal{B}}^{K'_{\mathcal{B}}} & f_{v_2,\mathcal{A}}^{1} & \cdots & f_{v_2,\mathcal{A}}^{K'_{\mathcal{A}}} & f_{v_2,\mathcal{N}}^{1} & \cdots & f_{v_2,\mathcal{N}}^{K'_{\mathcal{N}}} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ f_{v_N,\mathcal{B}}^{1} & \cdots & f_{v_N,\mathcal{B}}^{K'_{\mathcal{B}}} & f_{v_N,\mathcal{A}}^{1} & \cdots & f_{v_N,\mathcal{A}}^{K'_{\mathcal{A}}} & f_{v_N,\mathcal{N}}^{1} & \cdots & f_{v_N,\mathcal{N}}^{K'_{\mathcal{N}}} \end{pmatrix} \tag{8}$$

4.4 网络建模

网络分析与图论之间存在密切联系, 网络建模目的是将核心网建模为图。5G 核心网实现了虚拟化, NF 采用云化部署, 传统的物理网络拓扑在 5G 核心网中不复存在, 但物理解耦并没有减弱 NF 间的强业务逻辑关系, NF 间基于服务调用的方式, 即一组一组的交互建立连接。因此, 本文提出一种基于 NF 交互关系的 5G 核心网建模方法, 通过将核心网建模为图, 在现有仅考虑信令流量特征的基础上引入核心网行为实体 NF 间的交互关系信息, 从而充分利用多源信息提高模型异常检测性能。

建模过程中, NF 定义为图的节点, NF 间的交互关系定义为图的连边, NF 行为画像得到的多维属性为节点属性, NF 的交互频次为边的权值。通过建模, 将关系型特征数据转化为图结构数据, 便于利用图神经网络聚合传统特征与空间特征以达到更好的异

常检测效果。本文以节点集合、边集合、边权值集合、节点特征矩阵为输入构建了一个有向加权图作为图神经网络的输入, 如式(9)所示。

$$\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{W},F) \tag{9}$$

4.5 图神经网络设计

图神经网络(Graph Neural Networks, GNN)作为处理图数据的有效方法, 能够同时学习图的结构信息和特征信息, 近年来广受关注[53]。GCN 是 GNN 的经典代表之一, 通过图卷积对图的结构和特征信息进行学习以得到任务结果[54], 本文选用含 2 个隐藏层的 GCN 模型, 每一卷积层处理一阶邻域信息, 卷积层叠加可以实现多阶邻域信息传递, 其逐层传播规则[55]如式(10):

$$H^{(l+1)}=\sigma(\widetilde{D}^{-\frac{1}{2}}\widetilde{A}\widetilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}) \tag{10}$$

其中 $\widetilde{A}=A+\boldsymbol{I}_N$, $\boldsymbol{I}_N$ 为单位矩阵, $\widetilde{D}_{ii}=\sum_j\widetilde{A}_{ij}$, $\boldsymbol{W}^{(l)}$ 是 l 层的权值矩阵, σ 为激活函数, 本文选用 ReLU 函数作为激活函数。经过两层 GCN 获得节点的最终表示 Z [56], 公式化表示为式(11):

$$Z=f(F,A)=\mathrm{ReLU}(\hat{A}\,\mathrm{ReLU}(\hat{A}FW^{(0)})W^{(1)}) \tag{11}$$

其中 $\hat{A}=\widetilde{D}^{-\frac{1}{2}}\widetilde{A}\widetilde{D}^{-\frac{1}{2}}$。损失函数使用交叉熵损失, 如式(12)所示:

$$\mathcal{L}=-\sum_{i\in\mathcal{Y}_L}\sum_{j=1}^{C}Y_{ij}\log(softmax(Z_{ij})) \tag{12}$$

其中 $\mathcal{Y}_L$ 是含标签的训练集节点索引集合, C 是标签类别数。本文的损失函数优化算法采用梯度下降法。

算法:GAD(基于图的异常检测算法)

输入: 源数据: $\mathcal{D}$;
节点标签: $\mathcal{Y}$;
图卷积层数, 训练批次: L, E

输出: 节点表示向量: $\boldsymbol{z}_v$

```
// 初始化
// 特征提取
    // 行为画像
    For v in V Do
        For k = 1, 2,..., K_A Do
            f_{v,A}^k ← Eq.(2);
        End For
        For k = 1, 2,..., K_N Do
            f_{v,N}^k ← Eq.(3);
        End For
        For k = 1, 2,... K_B Do
            f_{v,B}^k ← Eq.(4);
        End For
        f_v ← Eq.(5);
    End For
    // 特征标准化
        f_{v,STD} ← Eq.(7);
    // 特征选择
        f_{v,SEL} ← RFECV Algorithm;
    F ← Eq.(8);
// 图构建
  G ← Eq.(9);
// 图神经网络
  For e =1, 2,..., E Do
    For l =1, 2,..., L Do
      h_v^(l) ← Eq.(10), h_v^(l) ∈ H^(l);
      z_v ← Eq.(11), z_v ∈ Z;
      L ← Eq.(12);
    End For
    Return z_v
  End For
// 结束
```

4.6 GAD 算法

IBNAD 模型的核心是基于图的异常检测(Graph-based Anomaly Detection)算法。在给定信令流量包和 NF 注册信息等源数据基础上, 首先根据属性提取函数集、提取 NF 行为属性、基本属性、网络属性特征以作为每个 NF 的初始特征向量。初始特征经过行 16 特征标准化和行 18 特征选择后得到最终特征向量, 所有 NF 特征向量构成特征矩阵 。然后基于式(9)进行网络建模, 将原始数据转化为图结构数据, 异常检测问题工程化为图节点分类问题。最后如行 23～30 所示, 采用 GCN 模型进行半监督学习训练, 利用训练后的模型进行节点表示学习与分类。

5 实验及分析

本节主要对所提出的 IBNAD 模型进行性能验证及结果分析, 实验使用 free5GC 开源平台生成的仿真数据集, 通过与异常检测领域常见的机器学习模型和图嵌入模型进行对比实验, 验证了 IBNAD 模型的有效性和优越性, 通过消融实验验证 NF 行为画像、特征标准化及特征选择 3 个子模块在提升 IBNAD 模型性能上的有效性和必要性。此外, 本节还对模型超参数敏感性进行了简要分析。

5.1 实验对比模型

5G 商用仅两年, 目前仅有的少数基于信令流量的核心网异常检测模型, 如基于基线还原[13], 基于卷积神经网络[14]的模型在海量加密信令的实际场景中实用性不强, 且现有的模型均没有考虑 NF 交互关系信息。本文提出的 IBNAD 模型, 既利用了基于行为画像得到的属性信息, 也利用了基于 NF 交互关系进行图建模得到的结构信息, 通过对比仅以属性信息为输入的传统机器学习模型和仅以结构信息为输入的图嵌入模型, 证明所提模型的有效性和优越性。

5.1.1 传统机器学习模型

传统机器学习模型因实现相对简单、结果易解释等原因广泛应用于异常检测、欺诈检测、文本分类、人像识别等领域[57], 本文选择支持向量机、随机森林、多层感知机作为 IBNAD 的对比模型。

(1) 支持向量机(Support Vector Machines, SVM)是一种基于最优边界的机器学习分类技术, 基本思想是求解能够正确划分训练数据集并且几何间隔最大的分离超平面[23]。

(2) 随机森林(Random Forest)是一种通用的分类和回归算法, 该算法结合几个随机决策树, 并通过平均聚合其预测[29]。

(3) 多层感知机(Multi-layer Perceptron, MLP)是一个分层的前馈神经网络, 由输入层、隐藏层和输出层组成, 每一层由功能相同的感知器组成, 可用于分类和回归任务[32]。

5.1.2 图嵌入模型

图嵌入是解决图分析问题的一种有效方法, 它将图数据转换为最大限度地保留图结构信息和图属性的低维空间, 可运用于节点分类、节点推荐、链路预测等[58]。本文选择 LINE、Node2vec、Struc2vec 作为 IBNAD 的对比模型。

(1) LINE(Large-scale Information Network Embedding, LINE)是一种基于邻域相似假设的算法, 考虑了节点一阶和二阶邻居的相似性, 且适用于加权图[37]。

(2) Node2vec 通过偏置随机游走采用平滑插值 BFS 和 DFS 搜索策略来生成节点的邻域, 目的是找到有向邻域和结构等价邻域[38]。

(3) Struc2vec 以空间相似性定义节点相似度, 能够发现两个节点在邻居域结构上的相似性[39]。

5.1.3 5G 核心网异常检测模型

如相关工作介绍, 支持向量机、决策树、XGBoost 等分类算法, MKC、DBSCAN 等聚类算法, GRU、DNN 等神经网络被用于构建 5G 核心网异常检测模型。本文选择 XGBoost[16]、MKC[17]、DNN[21]作为 IBNAD 的对比模型。

(1) XGBoost 的思想是将许多 CART (Classification and Regression Tree)树弱分类器集成在一起形成一个强分类器。

(2) MKC 为了降低异常检测精度对单个特征选择的敏感性, 通过不同特征属性构建多个基核, 并结合这些核来提高聚类性能。

(3) DNN 由输入层、若干隐藏层、输出层构成, 层与层之间是全连接的。输入的特征向量通过隐含层变换达到输出层, 在输出层得到分类结果。

5.2 实验数据集及评价指标

实验平台方面, 本文基于 free5GC 平台开展仿真实验, free5GC 是 5G 核心网的开源项目, 该项目目标是实施 3GPP Release 15 及更高版本的 5G 核心网[59]。仿真基于 free5GC(v3.0.6), 采用基于 NRF 重定向路由的直连组网方案[60], 在该方案中, NRF 只用于 NF 服务注册/注销/更新, 维护 NF 实例的状态、负载等信息, NF 之间采用点对点直连的方式进行组网, 采用 NRF 重定向的方式进行路由寻址。基于直连组网方案, 考虑到 5G 众多应用场景与演进, 虚拟化后的 NF 实例数量以 2 个乃至更多数量级(10 为底)增长[61], 实验仿真了 9 类(AMF、SMF、NRF、AUSF、PCF、UDM、UDR、UPF、NSSF)共 550 个 NF, 图 7 展示了按直连组网方案仿真, 结合 NF 交互关系得到的拓扑图。

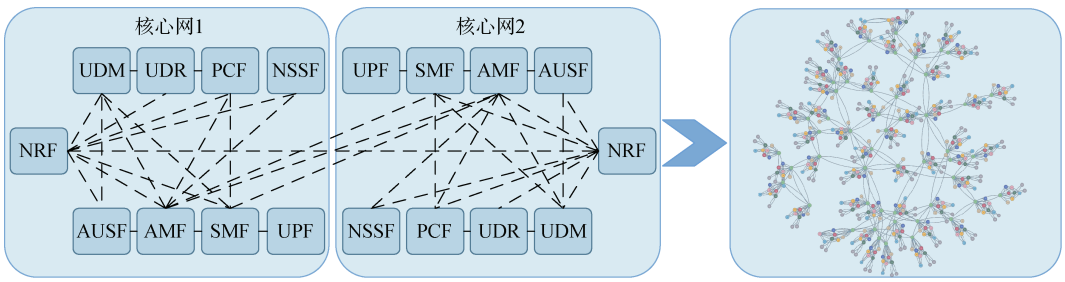


图 7 组网方案示示意与拓扑图

Figure 7 Schematic diagram and topology diagram of the networking scheme

实验仿真时, 各核心网随机运行 UE 注册、UE 注销、PDU 会话建立、PDU 会话释放、PDU 会话更新等核心网信令流程, 同时根据公开的安全威胁注入两个异常信令流程[13]: 1)被攻击者劫持的 AMF 在注册过程中不调用 AUSF, 直接调用 UDM 请求生成鉴权向量, 窃取用户鉴权信息; 2)被攻击者劫持的 UDM 批量访问 UDR 篡改用户数据, 干扰用户正常通信。数据采集时, 信令流量通过 wireshark 软件抓包获取, NF 注册信息通过访问 MongoDB 数据库(存储注册、会话等信息)获取, 根据 4.3.1 节描述的特征提取方法, 基于信令流量提取 NF 行为属性, 基于 NF 注册信息和信令流量提取 NF 基本属性和网络属性。数据标注时, 为便于异常溯源定位, 对触发异常流程的 NF 及其在异常流程中直接交互的 NF 均标记为异常, 标签值为 1, 只参与正常通信流程的 NF 标记为正常, 标签值设置为 0。数据集信息如表 2 所示。

表 2 数据集信息

Table 2 Dataset Information

类型	值
节点	550
连边	2046
异常比	25.45%
特征维度	84
行为属性维度	29
基本属性维度	36
网络属性维度	19

本文采用 Precision、Accuracy、Recall、F1-score 和 AUC 作为评价指标。

Precision 指模型预测为正的样本中实际为正的样本比例, Accuracy 指预测正确的样本占该类样本的比例, Recall 指实际为正的样本中预测为正的样本比例, $\mathrm{F1\_score}=\frac{2(\mathrm{Precision}*\mathrm{Recall})}{(\mathrm{Precision}+\mathrm{Recall})}$ 为 Precision 和 Recall 的调和平均值, AUC 指分类器判定正样本的值高于负样本的值的概率, 通常 F1_score 和 AUC 值越高, 分类器性能越好。

5.3 实验结果及分析

本文实验主要包括 2 部分。1) 有效性实验: 通过与基于属性特征的传统机器学习模型、基于结构信息的图嵌入模型、5G 核心网异常检测模型对比来证明 IBNAD 模型性能的有效性和优越性; 2) 消融实验: 通过与 IBNAD 模型的不同变体进行比较, 以验证 NF 行为画像、特征标准化模块和特征选择模块的必要性。实验软硬件环境配置如表 3 所示, GCN 参数设置参考文献[55]经微调优化后如表 4 所示, 优化器采用 Adam。

表 3 实验软硬件环境配置

Table 3 Configuration of software and hardware

名称	值(版本)
GPU 类型	NVIDIA GeForce RTX 3090
GPU 数量	1
内存(G)	36
处理器(核)	10
硬盘(G)	1000
free5GC	v3.0.6
Pytorch	v1.8.1
Python	v3.7.10

表 4 GCN 实验参数

Table 4 Parameters of GCN

参数名称	参数值
隐藏层	2
隐藏单元	16
训练批次	45
学习率	0.01
L2 损失权重	0.001

5.3.1 有效性实验

有效性实验有两个目的, 一是通过与传统机器学习模型和图嵌入模型对比, 突出 IBNAD 模型在处理 5G 核心网 NF 异常检测问题上的有效性和优越性; 二是分析不同百分比训练集对 IBNAD 模型性能的影响。对比模型的性能指标结果均基于核心网数据集实验得到, 且对比模型的参数量较少, 实验中通过网格搜索法来确定一组最优值, 如 DNN 模型隐藏层数、隐藏单元数等, 在原模型参数基础上结合经验给出参数范围, 训练时根据参数范围, 按步长依次调整, 遍历所有组合后返回最佳参数组合。

考虑到随机状态参数会影响实验结果, 特征选择时, 不同随机状态下特征选择数量与分类性能关系、特征排名结果存在差异, 图 8 列举了 3 种随机状态下特征选择数量与分类性能的关系, 多次实验观察发现当特征数量大于 10 时分类性能下降明显且特征数量大于 20 时分类性能基本稳定。图 9 显示了每次实验中 RFECV 算法给每维特征的排名, 排名越靠近 1, 说明该维特征对分类性能的贡献越大。因此实际选择最优特征组合时综合多种随机状态下特征选择数量与分类性能关系、特征排名两类因素, 选取排名前 10 中出现频率最高的 10 维特征作为特征选择的结果。模型评价时, 最终评价指标值由 50 次实验取算数平均值确定。

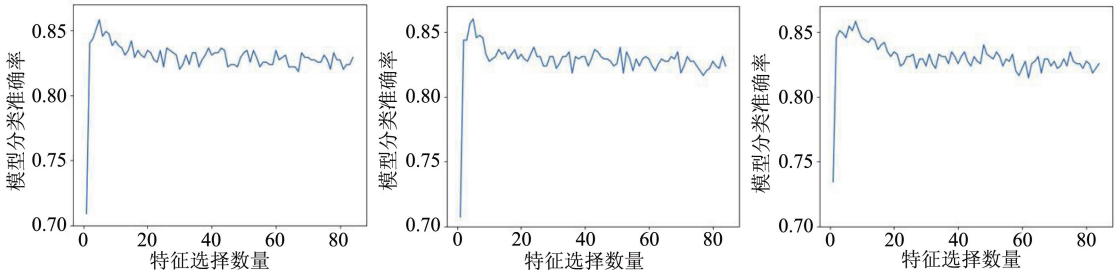


图 8　特征选择数量与分类性能关系

Figure 8　Relationship between number of feature selections and classification performance

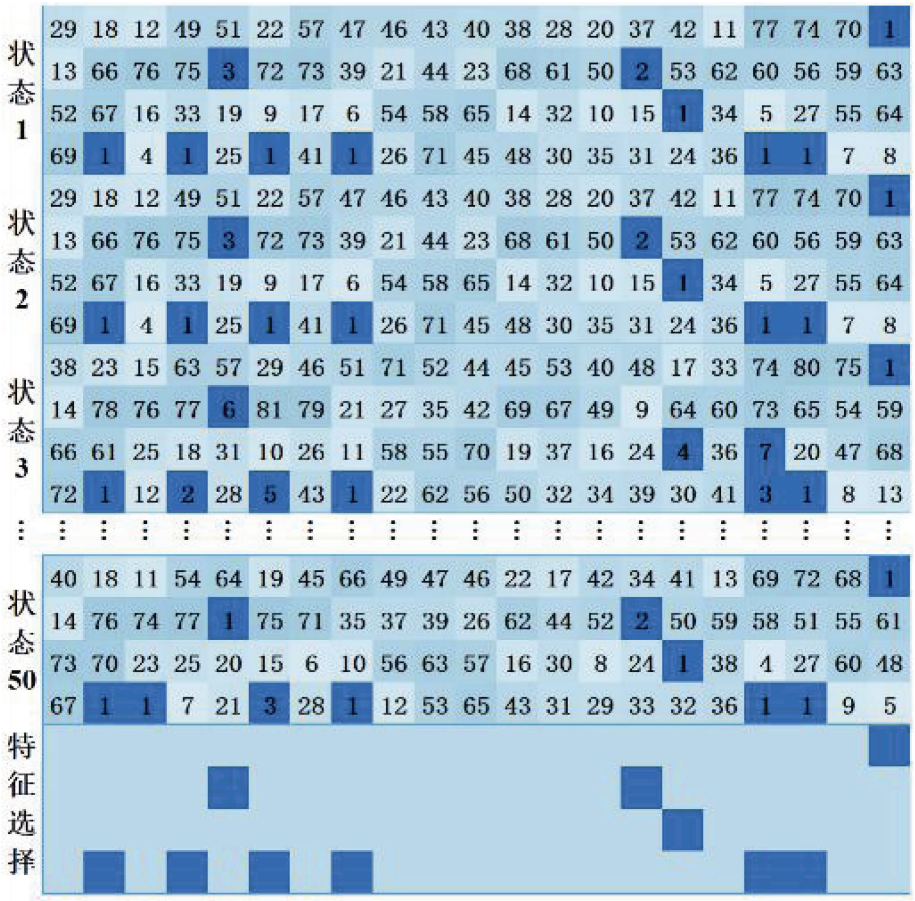


图 9　特征排名与特征选择

Figure 9　Feature ranking and feature selection

传统机器学习模型基于 NF 多维属性采取有监督学习方式训练模型, 实验中模型输入为 84 维 NF 属性特征。图嵌入方法基于图结构采取无监督方式训练模型, 实验中模型输入为 NF 交互关系信息, 即 2046 条边信息。有效性实验结果如表 5 所示, 各项评价指标结果表明 3 种传统机器学习模型的分类效果相当, 其中 SVM 模型分类性能最好, 10%比例训练集下 F1_score 和 AUC 值比 LINE、Node2vec 图嵌入模型高 0.25 以上, 导致模型相差较大的原因主要有: 一是 NF 异常信息主要体现在行为属性特征中, 而拓扑结构特征包含的区分正常异常的有效信息较少, 二是无监督学习方式, 缺少标签用于训练模型, 影响节点分类效果。

图嵌入模型中 Struc2vec 分类性能最佳, 评价指标远高于 LINE 和 Node2vec 模型, 究其原因主要为节点结构相似性定义不同。LINE 和 Node2vec 按照节点在网络中的位置关系定义节点结构相似性, 即共同邻居越多的节点结构越相似, 节点在嵌入空间学习到的表示就越相似。而 Struc2vec 按照节点局部拓扑结构定义节点结构相似性, 局部结构相似则节点结构相似, 即使两个节点在全局拓扑中相距很远。5G 核心网中, 同类 NF 服务功能和信令业务相同, 因

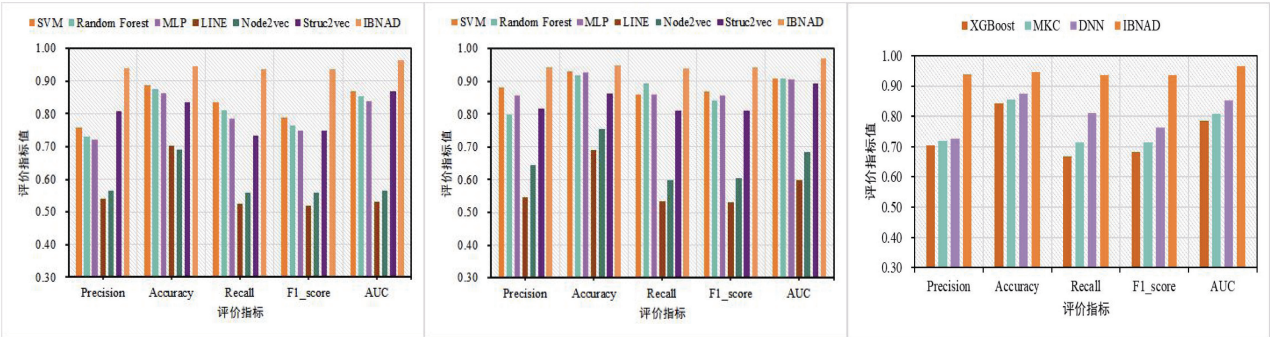
表 5 不同训练集比例下的各模型性能比较

Table 5 Performance comparison of each model under different training set proportions

Metrics	Train %	SVM	Random Forest	MLP	LINE	Node 2vec	Struc 2vec	XGB oost	MKC	DNN	IBNAD
Precision	10	0.7579	0.7319	0.7211	0.5415	0.5661	0.8066	0.7034	0.7196	0.7256	**0.9392**
	20	0.8152	0.7559	0.7473	0.5883	0.5732	0.8046	0.7123	0.7679	0.7664	**0.9432**
	40	0.8434	0.8096	0.7330	0.5583	0.6159	0.8096	0.7431	0.7741	0.8323	**0.9417**
	60	0.8791	0.7977	0.8567	0.5453	0.6448	0.8161	0.7214	0.7860	0.8421	**0.9433**
Accuracy	10	0.8858	0.8743	0.8632	0.7036	0.6897	0.8356	0.8413	0.8538	0.8739	**0.9445**
	20	0.8995	0.8902	0.8781	0.7101	0.6978	0.8432	0.8575	0.8750	0.8931	**0.9458**
	40	0.9177	0.9161	0.8800	0.7061	0.7315	0.8525	0.8767	0.8900	0.9138	**0.9480**
	60	0.9311	0.9168	0.9278	0.6909	0.7536	0.8606	0.8825	0.8967	0.9222	**0.9482**
Recall	10	0.8359	0.8089	0.7846	0.5246	0.5578	0.7349	0.6670	0.7137	0.8104	**0.9353**
	20	0.8333	0.8374	0.8102	0.5701	0.5598	0.7656	0.7581	0.7611	0.8247	**0.9362**
	40	0.8418	0.8780	0.8497	0.5372	0.5758	0.7889	0.8333	0.8360	0.8242	**0.9408**
	60	0.8601	0.8939	0.8601	0.5338	0.5979	0.8086	0.8485	0.8452	0.8421	**0.9403**
F1_score	10	0.7889	0.7649	0.7487	0.5182	0.5584	0.7494	0.6831	0.7135	0.7643	**0.9358**
	20	0.8209	0.7928	0.7716	0.5711	0.5629	0.7802	0.7309	0.7636	0.7916	**0.9372**
	40	0.8393	0.8409	0.7855	0.5340	0.5777	0.7963	0.7854	0.8029	0.8275	**0.9409**
	60	0.8672	0.8409	0.8565	0.5314	0.6037	0.8095	0.7797	0.8137	0.8387	**0.9416**
AUC	10	0.8698	0.8528	0.8382	0.5324	0.5655	0.8694	0.7847	0.8079	0.8529	**0.9644**
	20	0.8791	0.8728	0.8555	0.6366	0.5824	0.8788	0.8254	0.8387	0.8743	**0.9687**
	40	0.8931	0.9035	0.8704	0.6087	0.6588	0.8871	0.8630	0.8726	0.8844	**0.9690**
	60	0.9086	0.9092	0.9051	0.5992	0.6840	0.8923	0.8711	0.8801	0.8951	**0.9688**

此基于 NF 交互关系进行图建模后，同类 NF 的局部拓扑结构相似，而异常 NF 因偏离正常交互流程在局部拓扑特征上异于同类正常 NF，因此 Struc2vec 模型分类效果较好。

IBNAD 与现有 5G 核心网异常检测模型 XGBoost、MKC、DNN 的对比实验结果如表 5 及图 10(c)所示，上述 3 个模型仅以 NF 多维属性为输入，异常检测性能明显不及 IBNAD 模型，尤其在检测精确率上，IBNAD 相比表现较优的 DNN 模型提高 29.4%，表明引入 NF 交互关系可以进行特征聚合，可以增大正常和异常的可区分性，显著提升异常检测精确率。



（a）10%训练集（6 种模型）
(a) 10% training set（six models）

（b）60%训练集（6 种模型）
(b) 60% training set（six models）

（c）10%训练集（5G 核心网模型）
(c) 10% training set (5G core network models)

图 10 IBNAD 模型及 9 种对比模型性能

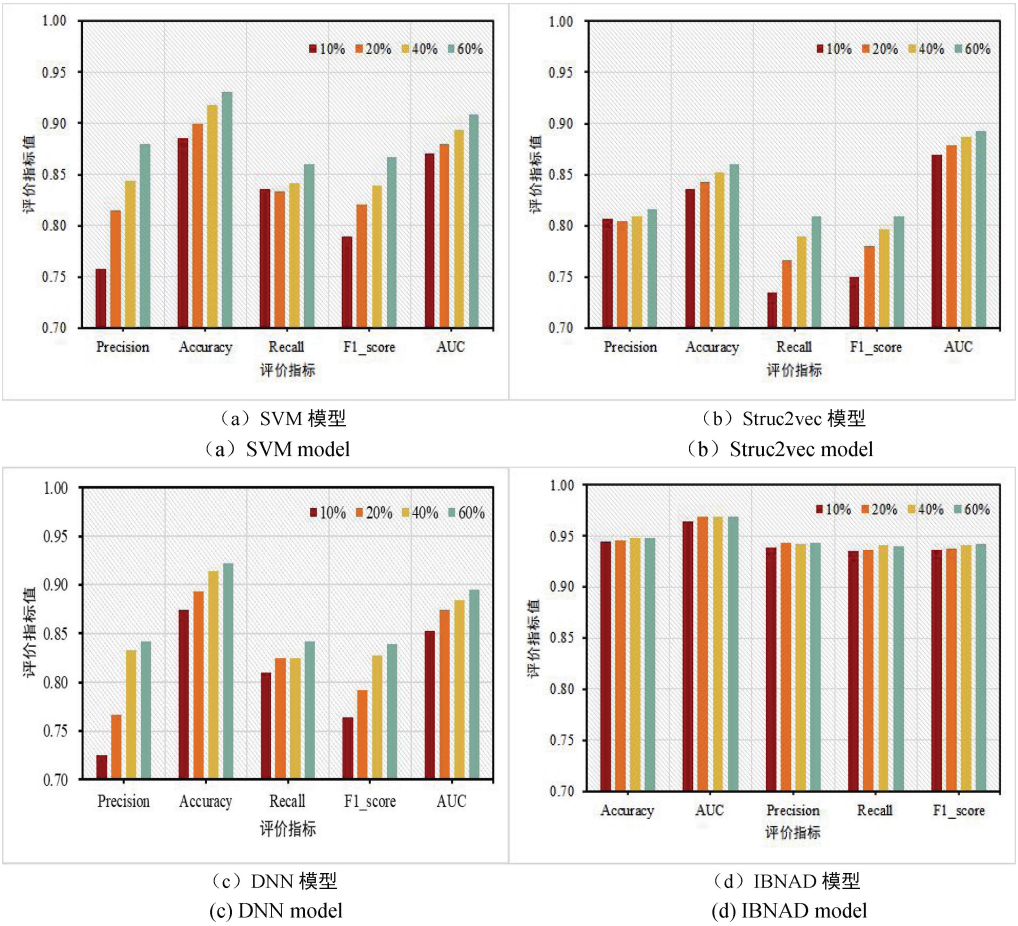
Figure 10 Performance of the IBNAD model and nine comparative models

传统机器学习、图嵌入模型以及现有 5G 核心网异常检测模型的实验结果说明 NF 多维属性和 NF 交互关系在异常检测中分别作出正贡献。因此，本文设计 IBNAD 模型，将核心网建模为图以融合利用 NF 属性和 NF 交互关系信息，采用可处理图结构数据的 GCN 模型采取有监督方式训练模型进行节点分类，

从而达到检测异常 NF 的目的。图 10 分别展示了 10%和 60%比例数据集作为训练集时, IBNAD 与 3 种传统机器学习模型, 3 种图嵌入模型, 3 种现有 5G 核心网异常检测模型的实验结果对比, 显而易见, IBNAD 模型在 5 个评价指标上均优于 9 种对比模型。10%比例数据集用于训练时, IBNAD 模型比传统机器学习对比模型中最优的 SVM 模型 F1_score 值提高 18.6%, AUC 值提高 10.8%; 比图嵌入对比模型中最优的 Struc2vec 模型 F1_score 值提高 24.8%, AUC 值提高 10.9%; 比 5G 核心网异常检测对比模型中最优的 DNN 模型 F1_score 值提高 22.4%, AUC 值提高 13%。

与传统机器学习、图嵌入模型以及现有 5G 核心网异常检测模型的对比实验, 一方面证明了所提出的 IBNAD 模型对解决 5G 核心网 NF 异常检测问题具有有效性; 另一方面表明同时利用 NF 属性信息和 NF 交互信息对提升异常检测性能作用明显, 证明了 IBNAD 模型所设计的网络建模模块和图神经网络模块对解决 5G 核心网异常检测问题并提升其效果具有有效性和必要性。

为探究训练集输入大小对模型性能的影响, 分别选择 10%、20%、40%、60%数据集作为训练集, 结果显示不同百分比训练集下 9 个对比模型各项评价指标抖动范围较大。图 11(a)～(d)分别展示了几类对比模型中性能最优的 SVM、Struc2vec、DNN 以及 IBNAD 模型结果, 现有 5G 核心网采用的 DNN 模型随训练集比例提高, 性能大幅提升, 对训练数据依赖性大, 而 IBNAD 模型在 10%比例训练集时即具有较好的检测性能, 且随着训练集比例提高, 各评价指标抖动保持在 0.006～0.026 内, 表明其对训练集比例敏感度低, 分类性能稳定。



（a）SVM 模型
（a）SVM model

（b）Struc2vec 模型
（b）Struc2vec model

（c）DNN 模型
(c) DNN model

（d）IBNAD 模型
(d) IBNAD model

图 11　不同比例训练集时模型性能

Figure 11　Model performance with different proportions of training sets

综上所述, 针对 5G 核心网 NF 异常检测问题, 融合 NF 属性信息和交互关系信息的 IBNAD 模型的分类性能优于基于单一类别信息的传统模型, 基于图论思想设计的网络建模和图神经网络模块对模型性能提升具有重要贡献度。此外, 实验还表明 IBNAD 模型对训练集敏感度低, 适用大量未标记数据和少量标记数据的现实应用场景[62]。

5.3.2　消融实验

与传统机器学习模型和图嵌入模型对比结果验证了 IBNAD 方法网络建模模块和图神经网络模块的

有效性, 本节主要进一步验证特征提取模块的有效性, 具体包括 NF 行为画像、特征标准化及特征选择子模块的有效性。消融实验考虑 IBNAD 模型的 6 种变体。

1) IBNAD(BA): NF 行为画像仅包含基本属性。

2) IBNAD(NA): NF 行为画像仅包含网络属性。

3) IBNAD(BxA): NF 行为画像仅包含行为属性。

4) IBNAD(STD): 特征提取模块去除特征选择子模块, 使用 NF 行为画像和特征标准化子模块。

5) IBNAD(SEL): 特征提取模块去除特征标准化子模块, 使用 NF 行为画像和特征选择子模块。

6) IBNAD(Feature): IBNAD 模型不引入 NF 交互关系, 仅基于 NF 属性信息进行分类。

表 6 为消融实验结果, 图 12 为 10%比例训练集时, IBNAD 及其 6 种变体的 5 项评价指标对比情况。如表 6 和图 12(a)所示, IBNAD(BA)、IBNAD(NA)模型效果较差, 各项评价指标值均在(0.5, 0.6)区间内, 而 IBNAD(BxA)模型各项指标约 0.8, 但相比 IBNAD 还存在差距。上述结果表明行为属性提供的可区分正常异常 NF 的信息较基本属性、网络属性多, 基于单一属性的 NF 行为画像不能很好地刻画正常 NF 的行为模式, 因此必须融合基本属性、网络属性、行为属性对 NF 行为画像, 验证了 NF 行为画像子模块的有效性。

如表 6 和图 12(b)所示, IBNAD 与 IBNAD(SEL)相比, 模型性能提升明显, 究其原因是经 NF 行为画像后得到的多维属性之间量纲差异较大, 导致模型训练时对数据拟合效果差, 分类性能不理想, 因此需通过特征标准化来统一属性特征量纲, 加快模型收敛, 提升模型性能。

如表 6 及图 12(c)所示, 以 10%比例训练集为例, 通过引入 NF 交互关系, IBNAD 模型各项性能评价指标均提升 10%以上, 表明通过引入 NF 交互关系进行网络建模以聚合邻居节点信息, 充分利用 5G 虚拟化核心网基于服务交互的新特性, 对提升异常检测性能具有重要意义。

表 6 模型不同变体性能对比

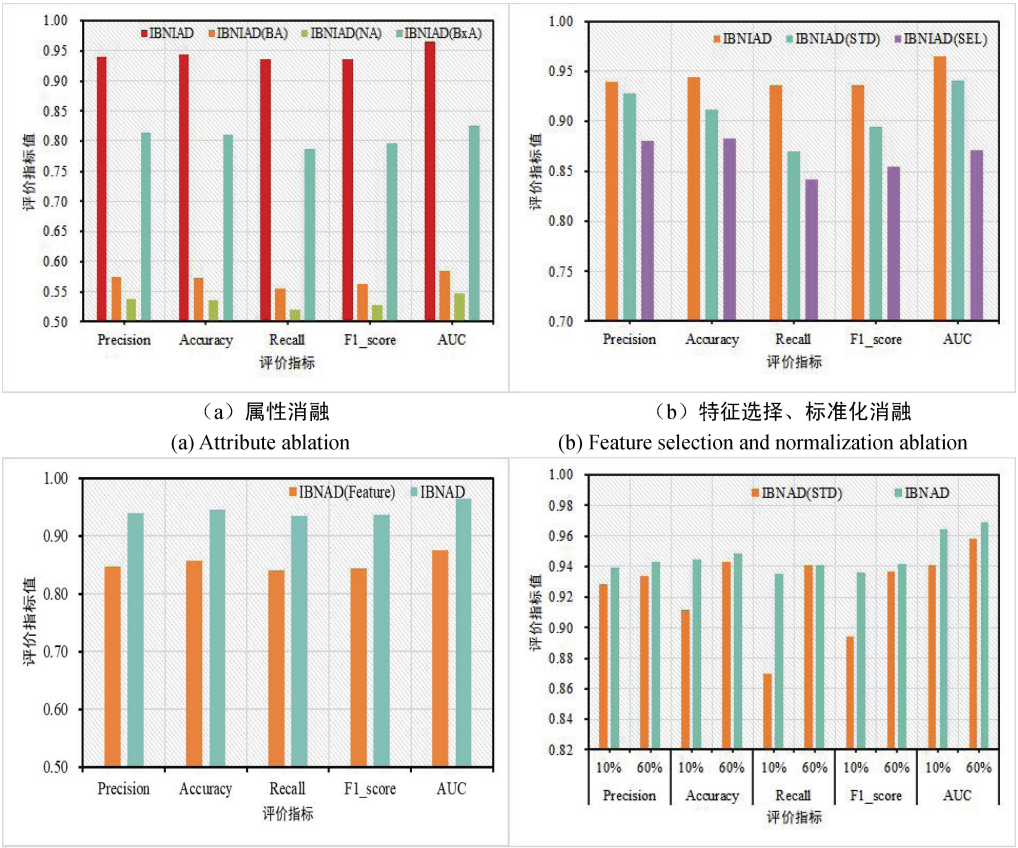
Table 6 Performance comparison of different variants of the model

Metrics	Train %	IBNAD	IBNAD (BA)	IBNAD (NA)	IBNAD (BxA)	IBNAD (STD)	IBNAD (SEL)	IBNAD (Feature)
Precision	10	**0.9392**	0.5742	0.5378	0.8129	0.9281	0.8797	0.8460
	20	**0.9432**	0.5784	0.5418	0.8188	0.9300	0.9044	0.8564
	40	**0.9417**	0.5773	0.5407	0.8172	0.9316	0.8941	0.8667
	60	**0.9433**	0.5779	0.5413	0.8181	0.9340	0.8904	0.8748
Accuracy	10	**0.9445**	0.5721	0.5359	0.8099	0.9120	0.8827	0.8572
	20	**0.9458**	0.5794	0.5427	0.8203	0.9300	0.9072	0.8707
	40	**0.9480**	0.5813	0.5444	0.8228	0.9344	0.9088	0.8744
	60	**0.9482**	0.5834	0.5464	0.8259	0.9427	0.9096	0.8797
Recall	10	**0.9353**	0.5552	0.5200	0.7859	0.8696	0.8425	0.8409
	20	**0.9362**	0.5689	0.5328	0.8053	0.9108	0.8760	0.8689
	40	**0.9408**	0.5746	0.5382	0.8135	0.9204	0.8967	0.8647
	60	**0.9403**	0.5796	0.5429	0.8206	0.9408	0.8991	0.8720
F1_score	10	**0.9358**	0.5625	0.5268	0.7962	0.8939	0.8551	0.8433
	20	**0.9372**	0.5727	0.5364	0.8107	0.9198	0.8888	0.8623
	40	**0.9409**	0.5756	0.5391	0.8148	0.9257	0.8932	0.8657
	60	**0.9416**	0.5786	0.5419	0.8190	0.9372	0.8937	0.8734
AUC	10	**0.9644**	0.5833	0.5463	0.8257	0.9410	0.8705	0.8756
	20	**0.9687**	0.5888	0.5515	0.8335	0.9568	0.8760	0.8780
	40	**0.9690**	0.5912	0.5537	0.8369	0.9572	0.8966	0.8787
	60	**0.9688**	0.5918	0.5543	0.8377	0.9585	0.8998	0.8788

如图 12(d)所示, 虽然模型 IBNAD 较 IBNAD(STD)性能提升幅度不大, 但仔细研究可以发现, 对比 10%比例训练集和 60%比例训练集时的结果, 10%时模型 IBNAD 较 IBNAD(STD)性能提升更明显, 表明当训练数据较少时, 通过特征选择可以显著提升模型性能, 适用实际工业环境中可用标记数据较少的场景。

综上所述, 通过 NF 行为画像、特征标准化、特

征选择、引入 NF 交互关系, IBNAD 模型性能分别得到提升, 验证了特征选择模块中 3 个子模块的有效性和必要性。同时, 实验也拓展了研究思路, 即如何通过特征选择改善基于小样本学习任务效果。



（a）属性消融
(a) Attribute ablation

（b）特征选择、标准化消融
(b) Feature selection and normalization ablation

（c）交互关系消融
(c) Interaction ablation

（d）IBNAD 与 IBNAD(STD)性能比较
(d) Comparison between IBNAD and IBNAD (STD)

图 12　消融实验对比

Figure 12　Comparison of ablation experiments

5.3.3　超参数敏感性分析

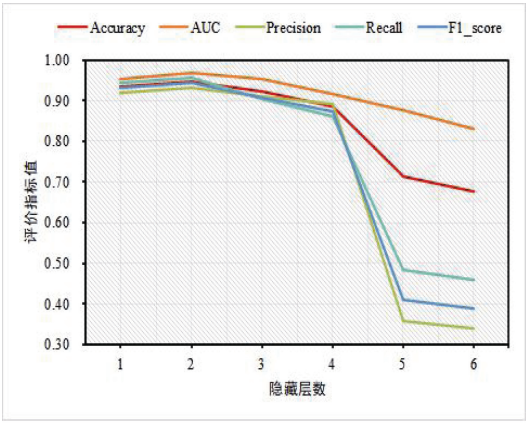
为研究所提的 IBNAD 模型中 GCN 超参数敏感性, 本节通过实验探究了不同隐藏层数、隐藏单元数、训练批次(epochs)数对模型异常检测性能的影响, 实验训练集比例为 10%。

图 13(a)显示了隐藏层数为(1, 6)时模型评价指标值, 当隐藏层数大于 2 时, 模型性能持续下降, 因此本文将隐藏层数设定为 2。图 13(b)描述了隐藏层单元为 16、32、64、128、256、512 时模型评价指标值, 结果表明模型对隐藏层单元大小不敏感, 本文设定为 16。图 13(c)刻画了 epochs 与训练损失、准确率的关系, 观察发现, 当 epochs=45 时, 模型大致收敛。

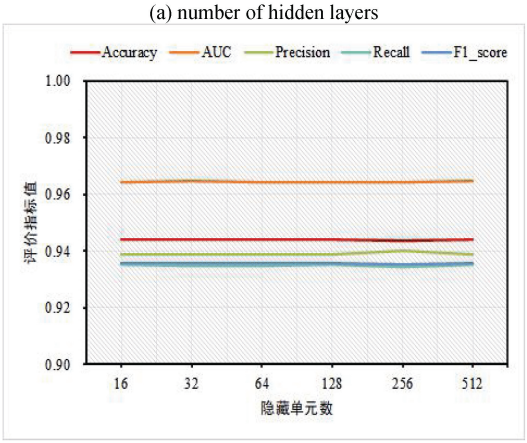
5.3.4　IBNAD 模型泛化能力分析

泛化能力, 指训练所得模型对未知数据的预测能力。5.2 节中提到在实验数据集中注入两类异常信令流程, 并实验验证 IBNAD 模型对两类异常具有较好的识别效果。为探究模型的泛化能力, 进一步开展实验仿真, 在原有异常基础上增加两类异常: 1)被攻击者劫持的恶意 NRF 向 UDM 请求大量资源, 但将 HTTP/2 信令帧 WINDOW_UPDATE 参数设置为非常小值, 导致 UDM 需长时间同时维护大量线程, 消耗 UDM 资源[50]; 2)被攻击者劫持的恶意 AMF 向 NRF 发送 Connection Preface 后, 不再继续发送服务请求, 导致 NRF 空等待, 消耗连接资源, 存在大量交互但流量极少的特点[63]。基于上述工作, 得到新的泛化能力分析数据集, 其中新增加的异常仅包含在测试集中, 特征维度不变, 数据集参数如表 7 所示。

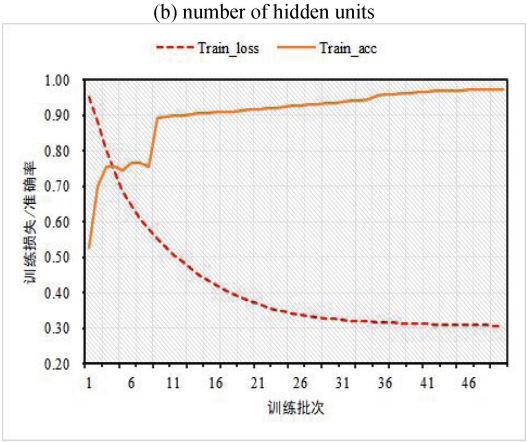
基于新构建数据集, 以不含新增异常的 10%比例数据集为训练集进行实验, 得到如表 8 所示结果, 在含未知异常的数据集上, IBNAD 模型各评价指标虽有所下降, 但下降幅度极小, 且对未知异常的检测准确率为 91.66%, 表明模型对未知异常也具有较好的检测性能, 具备一定的泛化能力, 分析原因主要为基于交互关系与多维属性的 NF 行为模式刻画使得模型在训练过程中充分学习了正常的 NF 行为模式特征, 从而达到区分正常与异常 NF 的目的。



（a）隐藏层数
(a) number of hidden layers



（b）隐藏单元数
(b) number of hidden units



（c）训练批次数
(c) number of training batches

图 13　超参数敏感性

Figure 13　Hyperparameter sensitivity

表 7　泛化能力分析数据集信息

Table 7　Dataset information for generalization analysis

类型	值
节点	623
连边	2385
异常比	28.89%
原有异常比	19.26%
新增异常比	9.63%

表 8　泛化能力分析数据集实验结果

Table 8　Experimental results of the dataset for generalization ability analysis

Metrics	原数据集	新数据集
Precision	0.9392	0.9342
Accuracy	0.9445	0.9390
Recall	0.9353	0.9305
F1_score	0.9358	0.9312
AUC	0.9644	0.9599
新增异常检测准确率		0.9166

5.3.5　IBNAD 模型应用可行性分析

IBNAD 模型面向 5G 核心网，以 GAD 算法为核心实现 NF 异常检测，本节将从网络规模、时间敏感性、模型部署三个方面对 IBNAD 模型应用的可行性进行分析。首先，模型的检测对象为 NF，虽然虚拟化后的 NF 实例数量较传统物理形态的 NF 以 2 个乃至更多的数量级增长[61]，但因其类别有限，总体数量仍然有限，且实验仿真的连边与节点比率仅为 3.72 和 3.82，表明网络建模所得到的图是稀疏图，因此网络规模决定模型的计算复杂度较小。其次，实验中以 1 min 为时间切片进行数据采集，数据预处理耗时约为 5 s，以 10%比例训练集为例，模型的训练时间约为 6 s，检测时间则为毫秒级，因为模型采取离线训练方式，所以实时检测的耗时主要为数据预处理时间，其相较于 1 min 的检测间隔可以忽略，在应用中也可根据实际情况调整时间切片间隔。最后，如何部署是模型应用落地的关键。网络数据分析网络功能(Network Data Analytics Function, NWDAF)是 5G 核心网新增的 NF，以机器学习为驱动向其他 NF 提供集中的数据收集与分析功能，且目前 3GPP 仅对 NWDAF 开放接口进行了规定，对其使用的人工智能算法并没有进行标准化[64]。IBNAD 模型及其 GAD 算法作为一种端到端的解决方案，可作为一个用例供厂商研究参考，以 NWDAF 作为模型与算法的载体，从而确保 5G 核心网的安全性。综上所述，IBNAD 模型因较小的计算复杂度、较低的耗时、可宿的制式载体而具有一定的应用可行性。

6　结论

本文提出一种基于交互的 5G 核心网 NF 异常检测模型 IBNAD，通过 NF 行为画像提取多维属性来刻画 NF 行为模式，利用 NF 交互关系将核心网建模为图结构，采用空间域的两层 GCN 聚合一阶和二阶邻域的节点属性信息和结构信息来学习 NF 的行为模式并分类，从而解决 5G 核心网 NF 异常检测问题。

实验结果表明, 相比基于属性信息的传统机器学习模型、基于结构信息的图嵌入模型及部分现有 5G 核心网异常检测模型, IBNAD 模型充分利用基于多源数据提取的属性信息和基于交互关系建模的结构信息, 能够更好的拟合正常 NF 的行为模式, 从而更好地检测异常, 且模型具有一定泛化能力, 能够检测出未知异常。实验还表明, IBNAD 模型对训练集比例敏感度低, 性能稳定, 适用仅有少量标记数据的现实应用场景。在模型中引入时间维度, 分析 NF 历史行为对异常检测的贡献, 以及考虑 NF 的动态部署是下一步研究的重点。

参考文献

[1] Vassiliki Gogou, Marnix Dekker. Telecom Security Incidents 2020-Annual Report. https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020.

[2] Tang Q, Ermis O, Nguyen C D, et al. A Systematic Analysis of 5G Networks with a Focus on 5G Core Security[J]. *IEEE Access*, 1000, 10: 18298-18319.

[3] ETSI TS 133 501-2021, 5G; Security architecture and procedures for 5G System (V16.5.0; 3GPP TS 33.501 version 16.5.0 Release 16).

[4] ETSI TR 133 855-2020, Study on security aspects of the 5G Service Based Architecture (SBA)(V16.1.0; 3GPP TR 33.855 version 16.1.0 Release 16).

[5] Marco Barros Lourenço, Louis Marinos, Lampros Patseas. ENISA Threat Landscape for 5G Networks Report. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[6] China Academy of Information and Communications Technology MT-2020(5G) Promotion Group. 5G Security Report[EB/OL]. http://www.caict.ac.cn/kxyj/qwfb/bps/202002/t20200204_274118.htm.

[7] China Academy of Information and Communications Technology MT-2020(5G) Promotion Group. 5G Security Knowledge Base [EB/OL].http://www.caict.ac.cn/kxyj/qwfb/ztbg/202112/t20211210_393875.htm.
中国信息通信研究院 IMT-2020(5G)推进组. 5G 安全知识库. http://www.caict.ac.cn/kxyj/qwfb/ztbg/202112/t20211210_393875.htm.

[8] Kim H. 5G Core Network Security Issues and Attack Classification from Network Protocol Perspective[J]. *J Internet Serv Inf Secur*, 2020, 10: 1-15.

[9] Park J H, Rathore S, Singh S K, et al. A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions[J]. *Hum.-Centric Comput. Inf. Sci*, 2021, 11(3).

[10] Khan R, Kumar P, Jayakody D N K, et al. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(1): 196-248.

[11] Zhang S L, Wang Y M, Zhou W H. Towards Secure 5G Networks: A Survey[J]. *Computer Networks*, 2019, 162: 106871.

[12] Park S, Kim D, Park Y, et al. 5G Security Threat Assessment in Real Networks[J]. *Sensors*, 2021, 21(16): 5524.

[13] Xin R, Gao S, Ruan B N. Abnormal Detection of 5G Core Netw Ork Function Services[J]. *Information and Communications Technology and Policy*, 2021(11): 89-96.
(辛冉, 高深, 阮博男. 5G 核心网网元服务异常检测[J]. *信息通信技术与政策*, 2021(11): 89-96.)

[14] Lam J, Abbas R. Machine Learning Based Anomaly Detection for 5G Networks[J]. *ArXiv e-Prints*, 2020: arXiv: 2003.03474.

[15] Pang G S, Shen C H, Cao L B, et al. Deep Learning for Anomaly Detection: A Review[J]. *ACM Computing Surveys*, 54(2): 38.

[16] Wei Q S, Song Y, Li H X, et al. Fault Warning Based on Feature Fusion with Multi-Dimension of Network Element in 5G Core Network[J]. *Communications Technology*, 2022, 55(3): 394-403.
(韦强申, 宋勇, 李红霞, 等. 5G 核心网网元多维特征融合故障预警[J]. *通信技术*, 2022, 55(3): 394-403.)

[17] Hu N, Tian Z H, Lu H, et al. A Multiple-Kernel Clustering Based Intrusion Detection Scheme for 5G and IoT Networks[J]. *International Journal of Machine Learning and Cybernetics*, 2021, 12(11): 3129-3144.

[18] Dong S Y. Research on 5G Authentication and Anomaly Traffic Detection Technology[D]. Nanjing: Southeast University.
(董士洋. 5G 接入认证和异常流量检测技术研究[D]. 南京: 东南大学.)

[19] Radivilova T, Kirichenko L, Lemeshko O, et al. Analysis of Anomaly Detection and Identification Methods in 5G Traffic[C]. *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications*, 2021: 1108-1113.

[20] Li Xuefang, Ji Xiangchuan, Ding Zhigang, et al. Research on 5G Network Security Risk Response Ideas [C]. *Promoting Network Evolution and Promoting Application Innovation. Proceedings of the 5G Network Innovation Seminar* (2021), 2021:35- 39.
(李雪芳, 吉翔川, 丁志刚, 等. 5G 网络安全风险应对思路研究[C]. *推动网络演进 促进应用创新. 5G 网络创新研讨会(2021)论文集*, 2021:35-39.)

[21] Sedjelmaci H. Cooperative Attacks Detection Based on Artificial Intelligence System for 5G Networks[J]. *Computers & Electrical Engineering*, 2021, 91: 107045.

[22] Bou Nassif A, Abu Talib M, Nasir Q, et al. Machine Learning for Anomaly Detection: A Systematic Review[J]. *IEEE Access*, 2021, 9: 78658-78700.

[23] Ma Q, Sun C, Cui B J, et al. A Novel Model for Anomaly Detection in Network Traffic Based on Kernel Support Vector Machine[J]. *Computers & Security*, 2021, 104: 102215.

[24] Ucci D, Sobrero F, Bisio F, et al. Near-Real-Time Anomaly Detection in Encrypted Traffic Using Machine Learning Techniques[C]. *2021 IEEE Symposium Series on Computational Intelligence*, 2021: 1-8.

[25] Mohammadi M, Rashid T A, Karim S H T, et al. A Comprehensive Survey and Taxonomy of the SVM-Based Intrusion Detection Systems[J]. *Journal of Network and Computer Applications*, 2021, 178: 102983.

[26] Charbuty B, Abdulazeez A. Classification Based on Decision Tree Algorithm for Machine Learning[J]. *Journal of Applied Science and Technology Trends*, 2021, 2(1): 20-28.

[27] Ramadhan I, Sukarno P, Nugroho M A. Comparative Analysis of K-Nearest Neighbor and Decision Tree in Detecting Distributed Denial of Service[C]. *2020 8th International Conference on Information and Communication Technology*, 2020: 1-4.

[28] Arowolo M O, Adebiyi M, Adebiyi A, et al. PCA Model for RNA-Seq Malaria Vector Data Classification Using KNN and Decision Tree Algorithm[C]. *2020 International Conference in Mathematics*, *Computer Engineering and Computer Science*, 2020: 1-8.

[29] Canavese D, Regano L, Basile C, et al. Encryption-Agnostic Classifiers of Traffic Originators and Their Application to Anomaly Detection[J]. *Computers & Electrical Engineering*, 2022, 97: 107621.

[30] Marteau P F. Random Partitioning Forest for Point-Wise and Collective Anomaly Detection—Application to Network Intrusion Detection[J]. *IEEE Transactions on Information Forensics and Security*, 2021, 16: 2157-2172.

[31] Wang M, Lu Y Q, Qin J C. A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback[J]. *Computers & Security*, 2020, 88: 101645.

[32] Alqurashi S, Shirazi H, Ray I. On the Performance of Isolation Forest and Multi Layer Perceptron for Anomaly Detection in Industrial Control Systems Networks[C]. *2021 8th International Conference on Internet of Things*: *Systems*, *Management and Security*, 2021: 1-6.

[33] Song J Y, Paul R, Yun J H, et al. CNN-Based Anomaly Detection for Packet Payloads of Industrial Control System[J]. *International Journal of Sensor Networks*, 2021, 36(1): 36-49.

[34] Nam S, Lim J, Yoo J H, et al. Network Anomaly Detection Based on In-Band Network Telemetry with RNN[C]. *2020 IEEE International Conference on Consumer Electronics - Asia*, 2020: 1-4.

[35] Ma X X, Wu J, Xue S, et al. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023, 35(12): 12012-12038.

[36] Perozzi B, Al-Rfou R, Skiena S. DeepWalk: Online Learning of Social Representations[C]. *The 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2014: 701-710.

[37] Tang J, Qu M, Wang M Z, et al. LINE: Large-Scale Information Network Embedding[C]. *The 24th International Conference on World Wide Web*, 2015: 1067-1077.

[38] Grover A, Leskovec J. Node2vec: Scalable Feature Learning for Networks[J]. *KDD*: *Proceedings International Conference on Knowledge Discovery & Data Mining*, 2016: 855-864.

[39] Ribeiro L F R, Saverese P H P, Figueiredo D R. *struc2vec*: Learning Node Representations from Structural Identity[C]. *The 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2017: 385-394.

[40] Bandyopadhyay S, Lokesh N, Murty M N. Outlier Aware Network Embedding for Attributed Networks[J]. *Proceedings of the AAAI Conference on Artificial Intelligence*, 2019, 33(1): 12-19.

[41] Cai L, Chen Z Z, Luo C, et al. Structural Temporal Graph Neural Networks for Anomaly Detection in Dynamic Graphs[C]. *The 30th ACM International Conference on Information & Knowledge Management*, 2021: 3747-3756.

[42] Yu W C, Cheng W, Aggarwal C C, et al. NetWalk: A Flexible Deep Embedding Approach for Anomaly Detection in Dynamic Networks[C]. *The 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2018: 2672-2681.

[43] Bandyopadhyay S, Lokesh N, Vivek S V, et al. Outlier Resistant Unsupervised Deep Architectures for Attributed Network Embedding[C]. *The 13th International Conference on Web Search and Data Mining*, 2020: 25-33.

[44] Wu B, Liang X, Zhang S S, et al. Advances and Applications in Graph Neural Network[J]. *Chinese Journal of Computers*, 2022, 45(1): 35-68.
(吴博, 梁循, 张树森, 等. 图神经网络前沿进展与应用[J]. *计算机学报*, 2022, 45(1): 35-68.)

[45] ETSI TS 123 501-2021, 5G; System architecture for the 5G System (5GS) (V16.7.0; 3GPP TS 23.501 version 16.7.0 Release 16).

[46] Bondy J A, Murty U S R. Graph theory with applications[M]. London: Macmillan, 1976.

[47] Bansal M K, Aswathy S V, Krishnaswami B. VNF Security in Telco Environment[J]. *Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020*, 2021, 694: 275.

[48] Rudolph H C, Kunz A, Iacono L L, et al. Security Challenges of the 3GPP 5G Service Based Architecture[J]. *IEEE Communications Standards Magazine*, 2019, 3(1): 60-65.

[49] Nyangaresi V O, Rodrigues A J, Abeka S O. Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications[C]. *2020 16th International Computer Engineering Conference*, 2020: 25-30.

[50] Hu X X, Liu C X, Liu S X, et al. Signaling Security Analysis: Is HTTP/2 Secure in 5G Core Network? [C]. *2018 10th International Conference on Wireless Communications and Signal Processing*, 2018: 1-6.

[51] Liu Haiou, Sun Jingjing, Su Yanyuan, et al. A review of user portrait research at home and abroad [J]. *Intelligence Theory and Practice*, 2018, 41(11): 155-160.
(刘海鸥, 孙晶晶, 苏妍嫄, 等. 国内外用户画像研究综述[J]. *情报理论与实践*, 2018, 41(11): 155-160.)

[52] Mustaqim A Z, Adi S, Pristyanto Y, et al. The Effect of Recursive Feature Elimination with Cross-Validation (RFECV) Feature Selection Algorithm Toward Classifier Performance on Credit Card Fraud Detection[C]. *2021 International Conference on Artificial Intelligence and Computer Science Technology*, 2021: 270-275.

[53] Wang M J, Zheng D, Ye Z H, et al. Deep Graph Library: A Graph-Centric, Highly-Performant Package for Graph Neural Networks[EB/OL]. 2019: arXiv: 1909.01315. http://arxiv.org/abs/1909. 01315.pdf.

[54] Wu Z H, Pan S R, Chen F W, et al. A Comprehensive Survey on Graph Neural Networks[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2021, 32(1): 4-24.

[55] Niepert M, Ahmed M, Kutzkov K. Learning Convolutional Neural

Networks for Graphs[C]. *The 33rd International Conference on International Conference on Machine Learning - Volume 48*, 2016: 2014-2023.

[56] Welling M, Kipf T N. Semi-supervised classification with graph convolutional networks[C]. *J. International Conference on Learning Representations*. 2016.

[57] Ilievski G, Latkoski P. Network Traffic Classification in an NFV Environment Using Supervised ML Algorithms[J]. *Journal of Telecommunictions and Information Technology*, 2021, 3(2021): 23-31.

[58] Cai H Y, Zheng V W, Chang K C C. A Comprehensive Survey of Graph Embedding: Problems, Techniques, and Applications[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2018, 30(9): 1616-1637.

[59] "Free5GC," https://www.free5gc.org/, 2021.

[60] Mu J, Ma R T. Research on Deployment and Evolution Strategies of 5G Signalling Network[J]. *Designing Techniques of Posts and Telecommunications*, 2020(9): 53-60.
(穆佳, 马瑞涛. 5G 信令网部署方案及演进策略研究[J]. *邮电设计技术*, 2020(9): 53-60.)

[61] Yun S. Practice of NFS Operation and Maintenance Support in 5G Core Network[J]. *Communications World*, 2021(5): 44-45.
(云杉网络. 5G核心网NFS运维保障实践[J]. *通信世界*, 2021(5): 44-45.)

[62] Wu H X, Han M, Chen Z Q, et al. Survey of Multi-Label Classification Based on Supervised and Semi-Supervised Learning[J/OL]. *Computer Science*, 2022: 1-21. (2022-04-13). https://kns.cnki.net/kcms/detail/50.1075.TP.20220412.1544.004.html.
(武红鑫, 韩萌, 陈志强, 等. 监督和半监督学习下的多标签分类综述[J/OL]. *计算机科学*, 2022: 1-21. (2022-04-13). https://kns.cnki.net/kcms/detail/50.1075.TP.20220412.1544.004.html.)

[63] Tripathi N, Hubballi N. Slow Rate Denial of Service Attacks Against HTTP/2 and Detection[J]. *Computers & Security*, 2018, 72: 255-272.

[64] Yuan Y C, Gehrmann C, Sternby J, et al. Insight of Anomaly Detection with NWDAF in 5G[C]. *2022 International Conference on Computer, Information and Telecommunication Systems*, 2022: 1-6.

张伟露 于 2016 年在解放军理工大学通信工程专业获得学士学位。现在战略支援部队信息工程大学电子信息专业攻读硕士学位。研究兴趣包括移动通信网络安全、数据挖掘。Email: zhangweilu2022@163.com

吉立新 于 1994 年在解放军信息工程学院获得硕士学位。现为国家数字交换系统工程技术研究中心副总工程师, 博士生导师。研究领域为数据挖掘、电信网安全。Email: jlxndsc@139.com

刘树新 于 2016 年在解放军信息工程大学专业获得博士学位。现为国家数字交换系统工程技术研究中心助理研究员。研究领域为复杂网络、链路预测、通信网络安全。Email: liushuxin11@126.com

李星 于 2020 年在战略支援部队信息工程大学获得博士学位。现为国家数字交换系统工程技术研究中心助理研究员。研究领域为链路预测、社团挖掘。Email: lixing_ndsc@163.com

潘菲 于 2017 年在解放军信息工程大学获得硕士学位。现为国家数字交换系统工程技术研究中心研究实习员。研究领域为通信网络安全。Email: roc_0@163.com

胡鑫鑫 于 2020 年在战略支援部队信息工程大学获得硕士学位。现在战略支援部队信息工程大学网络空间安全专业攻读博士学位。研究兴趣包括数据挖掘、机器学习、移动通信网络安全。Email: hxx@alumni.hust.edu.cn