5G 网络环境下电子信息系统的安全传输机制研究

庄 姗[1] 鹿 璐[1] 刘 洋[1]
ZHUANG Shan LU Lu LIU Yang

摘 要 针对 5G 网络边缘计算环境资源受限及数据孤岛带来的安全挑战，文章构建了一个集终端安全代理、边缘安全网关与云端编排中心于一体的纵深防御架构。在边缘侧部署轻量级孤立森林模型对加密流量特征进行提取与推理，实现威胁近源阻断；在云端提出基于检测贡献度感知的自适应联邦聚合算法，通过动态调整节点权重优化全局模型更新策略。同时引入正则化约束机制，解决网络切片场景下数据非独立同分布导致的模型偏差与灾难性遗忘问题。实验结果表明，该机制在保护数据隐私的前提下综合 F_1 分数达到 95.8%，实现云边协同的毫秒级响应与模型持续迭代，为异构网络环境下的电子信息系统安全传输提供兼顾效能与隐私的高效解决方案。

关键词 5G 网络；边缘计算；联邦学习；异常检测；自适应聚合

doi：10.3969/j.issn.1672-9528.2026.04.019

0 引言

随着 5G 技术在工业互联网及物联网领域的广泛应用，电子信息系统的连接边界急剧扩张，面临着传统集中式防御失效与边缘侧计算资源受限的双重困境。海量异构终端接入导致的网络攻击面扩大，使得基于全流量分析的传统安全手段难以满足低时延与隐私保护的严苛需求 [1]。针对网络切片场景下数据分布差异显著及未知威胁演进快速的特性，建立一套融合轻量级身份认证、边缘实时检测与云端协同智能的传输机制显得尤为迫切。研究旨在突破传统单点防御局限，利用云边协同架构实现对加密流量特征的深度挖掘与模型自动化迭代，形成感知、分析至响应的安全闭环，对于构建具备自适应能力的内生安全体系具有重要理论意义与实际应用价值。

1. 中电装备山东电子有限公司 山东济南 250109

time image processing,2024[2026-04-10].https://link.springer.com/article/10.1007/s11554-023-01401-9.

[6] 周飞，郭杜杜，王洋，等 . 基于改进 YOLOv8 的交通监控车辆检测算法 [J]. 计算机工程与应用 ,2024,60(6):110-120.

[7] 裴少通，张行远，胡晨龙，等 . 基于 ER-YOLO 算法的跨环境输电线路缺陷识别方法 [J]. 电工技术学报 , 2024, 39(9): 2825-2840.

[8] 王大阜，王静，石宇凯，等 . 基于深度迁移学习的图像隐私目标检测研究 [J]. 图学学报 ,2023,44(6):1112-1120.

[9]SUNKARA R, LUO T. No more strided convolutions or pooling: a new CNN building block for low-resolution images and small objects[C]//Machine Learning and Knowledge Discovery in Databases. Berlin: Springer, 2022: 443-459.

[10]LI H L, LI J, WEI H B, et al. Slim-neck by GSConv: A lightweight-design for real-time detector architectures[J/OL]. Journal of real-time image processing,2024[2026-04-10].https://link.springer.com/article/10.1007/s11554-024-01436-6.

[11]CHEN J R, KAO S, HE H, et al. Run, don't walk: chasing higher FLOPS for faster neural networks[C]// 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). Piscataway: IEEE, 2023: 12021-12031.

[12] 秦伦明，梅温泉，崔昊杨，等 . 改进 YOLOv8s 的遥感图像目标检测算法 [J]. 激光与光电子学进展 ,2025,62(10):317-325.

[13]LIU Y, LIU D C, HUANG X B, et al. Insulator defect detection with deep learning: a survey[J].IET generation, transmission & distribution,2023,17(16):3541-3558.

[14] 赵朗月，吴一全 . 基于机器视觉的表面缺陷检测方法研究进展 [J]. 仪器仪表学报 ,2022,43(1):198-219.

【作者简介】

樊计兰（2002—），女，山东临沂人，硕士研究生，研究方向：目标检测。

赵飞燕（1981—），通信作者（email: zfynd@163.com），女，宁夏固原人，硕士，副教授，研究方向：计算机视觉与图像处理。

（收稿日期：2025-09-11 修回日期：2026-04-15）

1 总体架构与工作流程

针对前述安全挑战，本研究构建安全功能下沉与集中智能管控相结合的纵深防御架构，如图 1 所示。架构纵向划分为终端安全代理（TSA）、边缘安全网关功能（SGF）及云端安全编排与分析中心（SOAC）三个核心层级。部署于终端设备的 TSA 负责发起基于物理特征的初始认证，建立至网络边缘的轻量级加密隧道，从源头保障接入可信。位于 MEC 边缘节点的 SGF 作为核心策略执行点，承载虚拟化网关逻辑，负责终结终端加密隧道，执行深度包检测与本地威胁清洗；其内部集成轻量级孤立森林算法，对流经的业务数据进行实时异常特征提取与推理，实现威胁的近源阻断 [2]。部署在云端的 SOAC 汇聚全网 SGF 上传的模型参数差量，利用联邦平均算法聚合生成全局威胁模型，并负责全网安全策略的动态编排与下发。该架构通过云边协同机制，在边缘侧实现毫秒级威胁响应，在云端实现跨域攻击溯源与模型迭代，形成感知、分析至响应的自动化安全闭环体系。

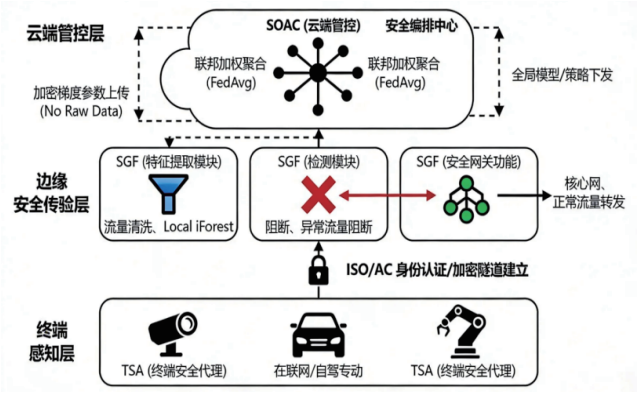

图 1 架构设计

该机制在实际业务场景中的运行流程划分为接入认证、数据传输监控与协同模型更新三个阶段：

阶段一：安全接入与密钥协商。终端启动业务时，TSA 与最近的 SGF 触发双向身份认证流程，双方基于椭圆曲线算法生成临时会话密钥，建立独立加密通道，SGF 根据终端能力与网络状态自适应匹配加密策略，完成安全上下文建立。

阶段二：边缘实时检测与阻断。业务数据经加密通道传输至 SGF，网关解密并提取流量特征向量，输入本地孤立森林模型进行推理。若计算出的异常得分超过预设阈值，SGF 立即触发阻断指令并隔离可疑终端；若判定为正常流量，则转发至核心网 [3]。

阶段三：联邦协同与模型迭代。SGF 在本地利用新采集的流量特征持续微调检测模型，周期性提取模型参数梯度并加密上传至 SOAC。SOAC 对来自多节点的参数进行联邦聚合，生成包含全局威胁特征的新版模型，随即下发至全网 SGF。各 SGF 加载新参数完成热更新，从而具备识别全网未知威胁的能力，全程无需上传原始业务数据。

2 5G 边缘计算环境下的智能安全传输机制设计

2.1 边缘侧轻量级异常特征提取与本地检测模型

2.1.1 5G 流量特征工程

为适应 5G 网络边缘受限的计算资源并保障毫秒级检测时延，SGF 节点需对高速吞吐的业务流量进行多维特征降维与重构，构建适用于轻量级模型的特征向量空间。针对 5G 业务普遍采用加密传输的特性，特征提取不再依赖对载荷内容的深度解析，转而聚焦于侧信道统计特征及流行为模式 [4]。SGF 通过滑动窗口机制实时捕获数据包序列，提取包括五元组信息、流量方向、分组长度分布及时间间隔等关键维度，将离散的原始数据包流转化为定长的特征向量。设 t 时刻捕获的第 i 条业务流特征向量为 x_i，包含 d 个维度的统计特征，则该向量用公式表示为：

$$\boldsymbol{x}_i = \{f_{i,1}, f_{i,2}, \ldots, f_{i,d}\} \tag{1}$$

式中：$f_{i,k}$ 为该业务流在第 k 个维度上的统计特征值；d 为特征总维度数，涵盖平均包长、字节速率、流持续时间等指标。

为捕捉 DDoS 攻击或低频慢速扫描在时间域上的异常波动，引入到达时间间隔（IAT）的统计矩作为关键特征，第 i 条流的平均到达时间间隔计算为：

$$\mu_{\mathrm{IAT},i} = \frac{1}{N_i - 1}\sum_{j=1}^{N_i-1}(T_{i,j+1} - T_{i,j}) \tag{2}$$

式中：N_i 为滑动窗口内该流的数据包总数；$T_{i,j}$ 为第 j 个数据包到达 SGF 的时间戳。

考虑到不同维度的特征值量纲差异巨大，直接输入模型会导致梯度更新不稳定或距离计算偏差，因此需对特征向量进行归一化处理 [5]。采用最大最小标准化方法将所有特征值映射至 [0,1] 区间，消除数值尺度影响，归一化后的特征值 $x'_{i,k}$ 计算公式为：

$$x'_{i,k} = \frac{x_{i,k} - \min(F_k)}{\max(F_k) - \min(F_k)} \tag{3}$$

式中：$x_{i,k}$ 为原始特征值；$\max(F_k)$ 和 $\min(F_k)$ 分别为历史观测窗口内第 k 维特征的最大值与最小值。经此预处理，SGF 能够输出标准化的特征张量，为后续孤立森林模型的快速推理提供高质量输入数据。

2.1.2 SGF 本地孤立森林模型构建

SGF 基于标准化特征集构建孤立森林检测模型，利用异常流量在特征空间分布稀疏的特性实现快速筛选。系统初始化 M 棵二叉隔离树（iTree），每棵树从特征维度中随机选择属性 q 及切割点 p 进行递归分裂，直至节点不可分。对于实时流量样本 x，其异常程度量化为在所有树中的平均路径长度 $E(h(x))$，计算公式为：

$$E(h(x)) = \frac{1}{M}\sum_{m=1}^{M} h_m(x) \tag{4}$$

式中：$h_m(x)$ 为样本 x 在第 m 棵树中从根至叶的遍历边数。DDoS 等攻击流量因特征极端，极易被早期切分，导致路径显著短于正常流量。为消除样本规模差异，引入归一化因子 $c(n)$，SGF 解算最终异常得分 $s(x,n)$：

$$s(x,n)=2^{-\frac{E(h(x))}{c(n)}} \tag{5}$$

式中：$s(x,n)$ 取值区间为 [0,1]。指数部分的负号确保路径长度越短（即特征越异常），得分越接近 1。当 $s(x,n)$ 逼近 1 时，表明该流量具备显著的攻击特征（如极高的包速率或异常的载荷分布），SGF 随即判定为恶意入侵并执行本地阻断；反之，若得分远小于 0.5，则视为正常业务放行 [6]。

此机制将前述提取的高维特征映射为单一量化的安全指标，实现从特征空间到决策空间的快速转换。

2.2 云端侧基于联邦平均的全局模型协同更新

2.2.1 模型参数上传与安全通信

边缘节点 SGF 在本地完成多轮次孤立森林模型训练后，并不直接传输包含敏感隐私的原始流量数据，而是仅提取能够表征数据分布特征的模型梯度参数。为进一步增强传输过程中的抗窃听与抗推断攻击能力，系统设计了一种轻量级掩码加密机制。设第 k 个 SGF 节点在第 t 轮训练得到的本地模型参数为 W_k^t，节点生成一个随机掩码矩阵 $\boldsymbol{R}_k$，将参数混淆为 $\boldsymbol{P}_k^t=W_k^t+\boldsymbol{R}_k$，仅将混淆后的 $\boldsymbol{P}_k^t$ 经由 SSL/TLS 加密隧道上传至云端 SOAC。同时，为量化各节点对全局检测能力的实际贡献，SGF 需同步上传本地模型在本地验证集上的精确率（Precision）与召回率（Recall）指标向量 $\boldsymbol{V}_k^t$。此机制确保云端仅获取模型更新方向与性能元数据，彻底阻断通过参数反演原始 5G 业务流量的可能性，实现数据所有权与使用权的严格分离。

2.2.2 SOAC 全局聚合策略设计

云端 SOAC 在接收到各 SGF 节点的参数更新后，需解决 5G 网络切片场景下严重的数据非独立同分布（Non-IID）问题。传统联邦平均算法仅依据数据量进行加权，极易导致拥有海量正常流量的节点稀释掉包含关键小样本攻击特征的节点权重。为此，本文提出一种基于检测贡献度感知的自适应聚合算法。SOAC 首先评估各节点上传的性能指标 V_k^t，结合节点数据量 n_k，计算综合贡献度因子 β_k^t。该因子倾向于奖励那些在保持高准确率同时能识别更多异常类别的节点，计算公式为：

$$\beta_k^t=\frac{n_k}{n}\cdot\exp(F_{1_k}^t-\overline{F_1}^t) \tag{6}$$

式中：$F_{1k}{}^t$ 为第 k 个节点本地检测的 F_1 分数；$\overline{F_1}^t$ 为全网平均 F_1 分数；随后，基于归一化的贡献度因子 β_k^t，SOAC 对去掩码后的参数进行加权聚合，生成第 t+1 轮全局模型 W_{global}^{t+1}：

$$W_{\text{global}}^{t+1}=\sum_{k=1}^{K}\hat{\beta}_k^t W_k^t \tag{7}$$

式中：$\hat{\beta}_k^t=\dfrac{\beta_k^t}{\sum_j\beta_j^t}$。

该策略动态能够有效提升那些捕获了新型攻击特征的 SGF 节点在全局模型中的话语权，抑制低质量或被投毒节点的负面影响，确保全局模型能快速收敛至全网最优的威胁识别状态。

2.2.3 基于正则化约束的个性化本地更新

SOAC 下发全局模型 W_{global}^{t+1} 后，各 SGF 节点需利用该通用模型提升本地检测能力，但直接覆盖本地模型会导致“灾难性遗忘”，即丧失对本地特定业务场景（如特定的工业控制协议模式）的识别精度。为此，本机制设计了基于正则化约束的个性化更新策略。SGF 在更新本地模型时，不再简单地做线性加权，而是将其建模为一个带有近端项的优化问题。节点在最小化本地损失函数 $L_k(W)$ 的同时，约束更新后的参数不能偏离全局模型 W_{global}^{t+1} 太远，其优化目标函数为：

$$\min_W\left(L_k(W)+\frac{\mu}{2}\|W-W_{\text{global}}^{t+1}\|^2\right) \tag{8}$$

式中：$L_k(W)$ 为孤立森林在本地数据上的拟合损失；μ 为正则化系数，用于调节全局通用知识与本地个性化特征之间的平衡。

在实际部署中，SGF 通过梯度下降求解该目标函数，使得更新后的模型既吸收全网的共性威胁特征（由 W_{global}^{t+1} 引导），又能保留本地特定的流量行为模式（由 $L_k(W)$ 保持）。这种机制使得同一套系统能同时适应车联网的高速移动场景和工业互联网的周期性通信场景，实现“千网千面”的精准防御。

3 仿真实验与结果分析

3.1 仿真环境搭建与数据集预处理

为全面评估所提机制在 5G 边缘计算环境下的有效性，实验基于 Mininet 网络仿真平台构建由 1 个云端 SOAC 节点、10 个边缘 SGF 节点及数十个异构终端组成的仿真拓扑。硬件环境采用 IntelXeonGold6248CPU 与 NVIDIATeslaT4GPU 加速

表 1 五种不同运行模式下的攻击检测性能对比

单位：%

方案类型	DDoS 检测 F_1	Botnet 检测 F_1	平均精确率 P	平均召回率 R	综合 F_1-score
单机孤立森林 (Local)	84.5	72.1	79.2	75.4	78.6
传统联邦平均 (FedAvg)	89.2	81.4	86.5	84.2	87.5
近端联邦学习 (FedProx)	92.4	86.8	90.1	88.5	91.1
集中式深度学习 (Centralized)	97.2	94.1	97.5	96.2	96.8
本文协同机制 (Proposed)	96.5	93.2	96.1	94.8	95.8

计算，软件栈基于 Ubuntu20.04LTS 操作系统及 PyTorch1.9.0 联邦学习框架。实验选用 CIC-IDS2017 作为基准数据集，该数据集涵盖了 DDoS、PortScan、Botnet 等典型网络攻击流量及正常背景流量。为真实模拟 5G 网络切片的异构性与数据非独立同分布特征，实验对数据集进行 Dirichlet 分布划分，使不同 SGF 节点持有的数据类别分布存在显著差异，例如部分节点仅包含工业控制协议流量，而另一部分节点集中了高频 Web 访问流量。数据预处理阶段，提取 82 维统计特征，并进行最大最小归一化处理，将数据集按 7:3 比例划分为本地训练集与测试集，评价指标采用精确率（Precision）、召回率（Recall）及 F_1 分数（F_1-score）。

3.2 协同检测性能与鲁棒性验证

为全面验证所提机制在 5G 异构切片场景下的防御效能，实验构建了包含特征提取、加密上传及全局聚合的完整闭环验证流程。为了确保对比的科学性与先进性，实验设置五组对照方案：

（1）单机孤立森林（Local），代表无协同的基准线；

（2）集中式深度学习（Centralized），代表理想状态下的性能上限；

（3）传统联邦平均（FedAvg），代表基础协同方案；

（4）近端联邦学习（FedProx），代表针对 Non-IID 数据的优化方案；

（5）本文自适应协同机制（Proposed）。

实验在各 SGF 节点注入非独立同分布的 DDoS 与 Botnet 攻击流量，量化评估各方案在精确率、召回率及 F_1 分数上的表现。

实验统计各方案在最终稳定状态下的各项性能指标，具体数值对比如表 1 所示。单机模式因缺乏全局视野，综合 F_1 分数仅为 78.6%。FedProx 虽然针对异构数据进行了优化，F_1 分数提升至 91.1%，但仍略逊于本文机制。本文所提机制通过贡献度感知聚合，综合 F_1 分数达到 95.8%，不仅显著优于 FedAvg（提升 8.3%）和 FedProx（提升 4.7%），且在保护隐私的前提下，性能极其逼近集中式全量训练的理论上限（96.8%），证明其在数据可用性与安全性之间的卓越平衡。

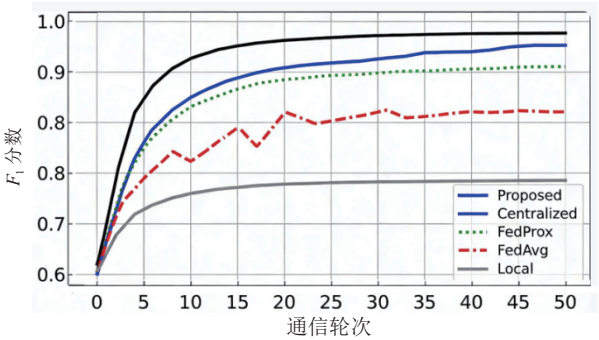

图 2 收敛曲线

从图 2 的收敛曲线可以直观观察到，FedAvg 受数据分布差异影响，曲线震荡明显且收敛较慢。FedProx 虽然稳定性有所提升，但收敛速率较为平缓。相比之下，本文机制在初始阶段表现出极高的学习效率，收敛轨迹最接近集中式方案，约在第 25 轮通信时即达到稳定高分状态。这表明本文设计的自适应聚合策略能有效利用高质量节点的贡献，显著缩短了系统防御能力的构建窗口，能够满足 5G 网络对快速响应的严苛要求。

4 结语

研究提出的基于云边协同的智能安全传输机制，通过终端物理特征认证、边缘孤立森林检测及云端贡献度感知联邦聚合的有机结合，有效解决了 5G 异构切片场景下的安全防御难题。该机制利用检测质量加权策略，在保障数据隐私的同时克服非独立同分布数据带来的模型训练偏差，以逼近集中式全量训练的性能实现了对未知威胁的精准识别。方案成功在数据可用性与安全性之间取得平衡，实现适应不同业务场景的个性化防御。未来研究可进一步探索在更复杂动态网络环境下的模型压缩与轻量化部署技术，以适应超大规模终端接入条件下的实时安全防护需求，推动内生安全技术的持续演进。

参考文献：

[1] 张建岳 . 电子信息工程的现代化技术探讨 [J]. 信息与电脑 , 2025, 37(18):110-112.

[2] 黄卓莹 , 范木杰 .5G 技术对电子信息专业实验教学的影响 [J]. 电脑知识与技术 , 2025,21(23):129-131.

[3] 毕飞 , 王乃尧 , 王恒强 . 电子信息技术在高效通信系统优化中的应用 [J]. 中国宽带 ,2025,21(7):13-15.

[4] 牛宬 . 工业智能化时代电子信息技术的发展及应用 [J]. 中国产经 , 2025(11):149-151.

[5] 齐泽荣 , 胡明征 . 物联网时代电子信息工程中网络技术运用 [J]. 中国宽带 ,2025,21(1):154-156.

[6] 董会祥 .5G 与工业物联网融合中的电子信息技术应用 [J]. 中国宽带 , 2024,20(11):153-155.

【作者简介】

庄姗（1985—），女，山东临沂人，硕士研究生，中级经济师，研究方向：电子工程。

鹿璐（1988—），女，山东莱芜人，本科，助理工程师，研究方向：电子工程。

刘洋（1989—），女，山东泰安人，本科，助理工程师，研究方向：电子工程。

（收稿日期：2026-01-08 修回日期：2026-04-01）