FedSTGCN：一种基于联邦时空图学习的物联网网络入侵检测新方法

王亚鲁[1]，李捷[2]，韩志杰[3]，程普[3]，Roshan Kumar[4]
[1]河南大学计算机与信息工程学院，中国开封市，475004
[2]郑州航空工业管理学院计算机学院，中国郑州市，450046
[3]河南大学软件学院，中国开封市，475004
[4]河南大学迈阿密学院，中国开封市，475004

摘要：物联网（IoT）设备的快速增长和其复杂性的增加使得网络入侵检测成为一个关键挑战，尤其是在以数据隐私为主要关注点的边缘计算环境中。基于机器学习的入侵检测技术可以增强物联网网络的安全性，但通常需要集中式的网络数据，这带来数据隐私和安全方面的重大风险。近年来，尽管出现了基于联邦学习的网络入侵检测方法以应对隐私问题，但这些方法尚未充分利用图神经网络（GNN）在入侵检测中的优势。为解决这一问题，提出一种联邦时空图卷积网络框架（FedSTGCN），该框架结合了时空图神经网络（STGNN）和联邦学习的能力。该框架支持在分布式物联网设备间协同训练模型，无需共享原始数据，从而在保护数据隐私的同时提高网络入侵检测的准确性。在两个广泛使用的物联网入侵检测数据集上进行了大量实验，以评估所提方法的有效性。实验结果表明，FedSTGCN在二分类和多分类任务中均优于其他方法，在二分类任务中准确率超过97%，在多分类任务中加权 F1 分数超过92%。

关键词：物联网；网络入侵检测；时空图神经网络；联邦学习；数据隐私
https://doi.org/10.1631/FITEE.2400932