计算机科学
COMPUTER SCIENCE

基于联邦学习的智能电网AMI入侵检测方法研究

刘东奇，张琼，梁皓澜，张孜栋，曾祥君

引用本文

刘东奇，张琼，梁皓澜，张孜栋，曾祥君．基于联邦学习的智能电网AMI入侵检测方法研究[J]．计算机科学，2024，51(6A)：230700077-8.

LIU Dongqi，ZHANG Qiong，LIANG Haolan，ZHANG Zidong，ZENG Xiangjun. Study on Smart Grid AMI Intrusion Detection Method Based on Federated Learning [J]. Computer Science，2024，51(6A)：230700077-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700077

基于联邦学习的智能电网 AMI 入侵检测方法研究

刘东奇[1]　张　琼[1]　梁皓澜[1,2]　张孜栋[1]　曾祥君[1]
1 长沙理工大学电气与信息工程学院　长沙 410114
2 湖南工程学院电气与信息工程学院　湖南 湘潭 411104
(liudongqi@csust.edu.cn)

摘　要　高级量测体系(Advanced Metering Infrastructure,AMI)是建设智能电网及泛在电力物联网的关键一环。随着海量终端接入和异构通信网络组件的应用,AMI 遭受网络攻击的风险大大增加。针对传统 AMI 网络攻击入侵检测方法存在主站计算压力过大、抗灾能力弱以及识别精度不足的问题,提出一种基于联邦学习的 AMI 入侵检测方法。首先,构建面向 AMI 的联邦学习入侵检测模型,在模型中集成联邦学习框架;然后,设计一种边缘侧的融合决策树的轻量级入侵检测算法,并提出跨台区云边协同的联合训练方法,实现跨台区经验的共享,提升入侵检测性能;最后,基于 NSL-KDD 数据集进行仿真验证,结果表明,与集中式、联邦学习与神经网络的入侵检测模型相比,所提方法准确率可达 99.76%,误报率仅为 0.17%。同时减少了检测时间,提高了通信效率,并且保证数据不离开本地,降低了数据隐私泄露的风险。

关键词:AMI;联邦学习;入侵检测;云边协同;决策树
中图分类号　TP399

Study on Smart Grid AMI Intrusion Detection Method Based on Federated Learning

LIU Dongqi[1],ZHANG Qiong[1],LIANG Haolan[1,2],ZHANG Zidong[1] and ZENG Xiangjun[1]
1 College of Electrical and Information Engineering,Changsha University of Science & Technology,Changsha 410114,China
2 College of Electrical and Information Engineering,Hunan Institute of Engineering,Xiangtan,Hunan 411104,China

Abstract　Advanced metering infrastructure(AMI) is a key link in building smart grid and ubiquitous electric IoT. With the application of mass terminal access and heterogeneous communication network components,the risk of network attacks on AMI is greatly increased. For the problems of traditional AMI network attack intrusion detection methods,such as excessive computing pressure of the main station,weak disaster resistance ability and insufficient recognition accuracy,an AMI intrusion detection method based on federated learning is proposed. Firstly,the federated learning intrusion detection model for AMI is constructed,and the federated learning framework is integrated into the model. Then,a lightweight intrusion detection algorithm that integrates decision tree on the edge side is designed,and a cross-platform cloud-edge collaborative joint training method is proposed to realize cross-platform experience sharing and improve intrusion detection performance. Finally,based on the NSL-KDD dataset,simulation results show that compared with the centralized and federated learning fusion neural network intrusion detection models,the accuracy of the proposed method can reach 99.76%,and the false positive rate is only 0.17%. At the same time,the detection time is reduced,the communication efficiency is improved. It also ensures that data does not leave the local area,reducing the risk of data privacy disclosure.

Keywords　AMI,Federated learning,Intrusion detection,Cloud edge collaboration,Decision tree

1　引言

随着国家双碳目标的推动,以新能源为主体的新型电力系统的建设迅速发展,多层级微电网、分布式电源、电力交易、碳足迹追溯等需求快速呈现,物联化、智能化、数字化成为电网下一步发展的主要趋势。作为多元用户供需互动的关键环节,配电网将逐渐发展为泛在的电力物联网,支撑海量电力用户接入并开展灵活电力市场交易。高级量测体系(AMI)作为泛在电力物联网的重要组成部分,为实时双向交互、用户用电计量、需求响应管理、分布式能源发电和存储等高级应用提供信息平台和技术支持[1]。然而,AMI 靠近用户侧,在其开放的互联网环境下,一旦网络攻击威胁侵入,突破边界安全防护便可畅通无阻,从而引发大范围停电事故。因此,对 AMI 网络攻击入侵检测方法开展

基金项目:国家自然科学基金(52177068);国家重点研发计划(2018YFB0904900);湖南省教育厅科研项目(21C0577);长沙理工大学科研创新项目(CXCLY2022076)
This work was supported by the National Natural Science Foundation of China (52177068), National Key R&D Program of China (2018YFB0904900),Research Project of Hunan Provincial Department of Education(21C0577) and Scientific Research and Innovation Project of Changsha University of Science and Technology(CXCLY2022076).
通信作者:梁皓澜(2631650704@qq.com)

研究具有重要的理论意义和实际应用价值。

目前，入侵检测系统(Intrusion Detection System，IDS)在AMI的网络安全领域中得到了广泛的应用，它可以通过监控和分析网络流量、系统审核记录等来检测和识别入侵行为，从而发出警报或采取有效安全措施。国内外学者就此开展了深入研究，主流方法有集中式和分布式入侵检测方法。文献[2]基于采集到的流量数据来检测AMI网络的状态，但所使用的方法为多分类支持向量机(Support Vector Machine，SVM)，它在处理复杂的高维非线性数据时效果并不理想。文献[3-4]基于不同的深度学习方法来提高AMI场景下对网络攻击行为的检测能力，但二者入侵检测模型的误报率较高，训练时间较长。文献[5]提出了一种基于改进的在线序列简化极端核心学习机(DBNOS-RKELM)的AMI入侵检测算法，不仅缩短了检测时间，而且提高了OS-ELM算法的泛化能力和入侵检测精度。此外，还有一些文献提出更复杂的算法，如半监督[6]、无监督[7]、强化学习[8]和深度学习[9]，以在检测模型上实现更高的准确性。上述集中式入侵检测方法要求将网络中每个节点的所有数据传输到数据中心进行检测，虽然保证了检测精度却存在以下问题：

1)依赖具有强大计算和存储能力的主站；

2)越来越大的数据吞吐量以及有限的通信资源使得AMI数据中心实时处理数据的能力降低，这可能导致电网的一些关键操作(如负荷需求响应)无法及时执行；

3)抗灾能力弱，数据存储在主站的方式很容易导致数据泄露和网络攻击。

进而，相关学者陆续开展了网络攻击下AMI分布式入侵检测方法研究。文献[10]采用分布式入侵检测技术，将基于机器学习的入侵检测方法嵌入每个智能电表、数据集中器和数据处理中心。文献[11]提出了一种基于无监督数据挖掘和滑动窗口方法的实时分布式入侵检测系统，用于监控流经分布式AMI组件的数据流量。该方法虽然能分担主站的计算压力，但检测模型为独立的模型，存在“数据孤岛”问题，使系统难以获得检测性能较好的模型。同时，该方法的部署成本相对较高。

近年来，联邦学习(Federated Learning，FL)作为一种新型分布式训练框架，受到了国内外学者的广泛关注与应用，它以“数据不动模型动”的方式打破了数据源之间的壁垒，同时可合作建模，提升模型性能。因此有学者提出将联邦学习应用于入侵检测研究中以弥补集中式和分布式入侵检测方法的不足，并保证本地数据的安全性[12-14]。然而，目前大多数研究是将联邦学习与神经网络相结合，而将联邦学习与决策树结合进行入侵检测的相关研究较少，且未见在电网领域的应用。与被称为“黑盒子”的神经网络相比，决策树的可解释强，符合人类直观思维，被视为准确性和可解释性的“黄金标准”，适合将电网运维技术人员的经验提取为规则进行预测性分析。因此，本文面向AMI场景提出一种联邦学习框架融合决策树的入侵检测方法，同时结合边缘计算技术，解决大量终端数据上传导致的主站计算压力大以及模型检测性能不足等问题。本文的主要贡献如下：

1)构建了一种面向AMI的联邦学习框架。通过分析AMI通信架构存在的网络攻击安全威胁来设计入侵检测模型。在联邦学习机制下，智能融合终端作为参与方与数据处理中心的中心服务器进行合作建模，可提高入侵检测性能以及AMI系统运行的可靠性。

2)提出了一种联邦学习框架下融合决策树的入侵检测方法。将基于决策树的入侵检测模型部署在具有边缘计算能力的各节点处，并与数据处理中心进行云边协同训练，实现各配电台区业务的高效合作及经验共享，且海量数据能够就近处理，降低了网络负载和数据泄露风险。

3)采用NSL-KDD数据集进行大量的实验来验证所提出的基于联邦学习框架的AMI入侵检测方法的有效性和优越性。

2 AMI体系架构

AMI是智能电网及泛在电力物联网的核心子系统，被广泛认为是实现智能电网的第一步。AMI通过数据处理中心和智能电表(Smart Meter，SM)实现了供电方与用户之间的双向数据交换。为了提升数据传输与计量效率，以及缓解通信网络的压力，在主站与智能电表之间引入边缘计算装置——智能融合终端，如图1所示。

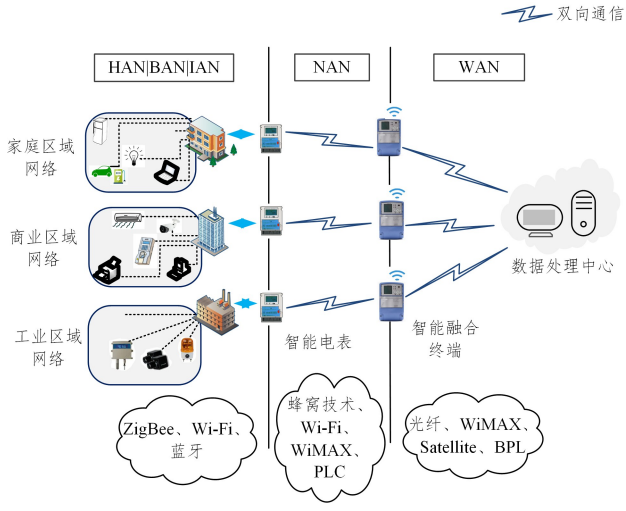


图1 AMI体系架构

Fig. 1 AMI architecture

AMI体系架构分为三层，第一层由智能电表及与之相连的可控设备构成。智能电表作为一种具备双向通信能力的智能计量终端，负责采集和计量各区域的用电信息(包括家庭区域网络(HAN)、商业区域网络(BAN)和工业区域网络(IAN))，同时还可对用户端设备进行远程控制。该层网络可用的通信技术为ZigBee、Wi-Fi、蓝牙等[15]。

第二层的关键组件是智能融合终端，大部分都部署在配电台区。智能融合终端定期收集、存储和传输来自SM的大量数据包，优先进行本地化处理，并将处理后的结果或者超出计算能力的数据传输到数据处理中心[16]。SM与智能融合终端之间通过邻域网(NAN)进行通信，多采用蜂窝、Wi-Fi、WiMAX及PLC等技术。

第三层的组件是AMI头端设备——数据处理中心(也称为主站)，部署在广域网(WAN)中，负责存储、分析和管理用户的计量计费信息，为智能电网的决策运行提供基础数据支持。通过光纤(Fiber Optic)、WiMAX、Satellite和BPL(Broadband over Power Lines)等长距离高带宽通信技术与智能融合终端进行双向通信[17]。

由于大量包含能耗信息以及 AMI 组件状态的数据通过互联网实现双向通信传输，因此通信网络是 AMI 系统中最容易受到威胁和攻击的部分，需采用入侵检测技术进行实时监控。数据中心的防御资源一般比较充足，攻击成本较高，因此主要对第一、二层的网络流量数据进行监测。

3 基于联邦学习框架的 AMI 入侵检测方法

AMI 系统结构复杂且设备数量庞大，若将终端产生的数据全部集中到云端处理，将会给云端服务器带来严重的计算压力和通信压力，且远距离传输数据增加了隐私泄露的风险，因此提出一种 AMI 场景下基于联邦学习的入侵检测方法。在该方法中，将模型训练任务分配给各边缘节点，而数据处理中心作为全局模型训练的聚合器。利用智能融合终端的计算存储资源与数据处理中心进行云边协同训练学习，从而提高入侵检测性能以及 AMI 系统运行的可靠性。所提方法的总体架构如图 2 所示。

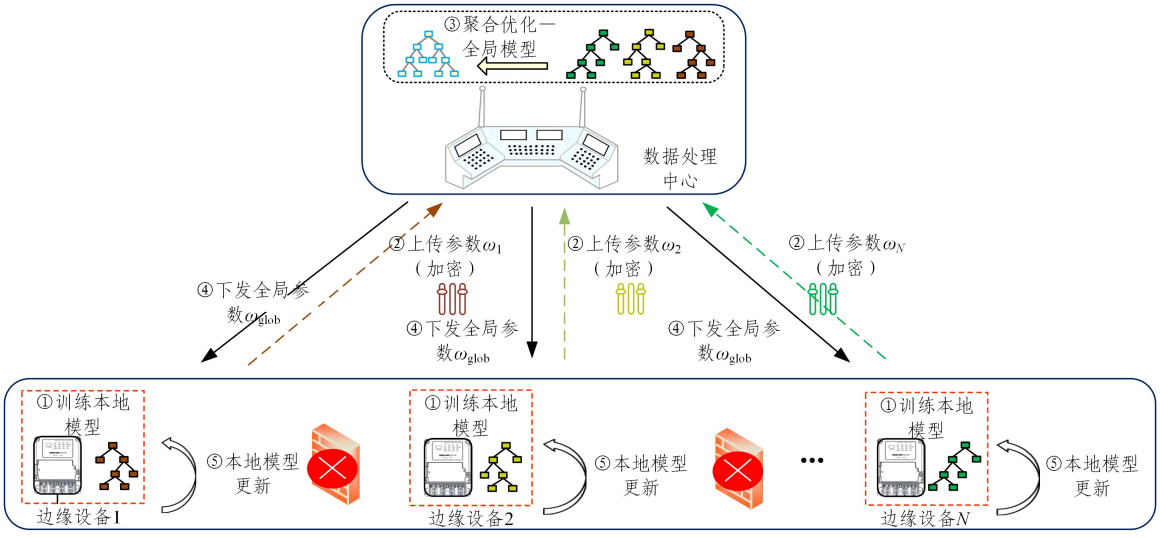


图 2 联邦学习框架下的 AMI 入侵检测架构

Fig. 2 AMI intrusion detection architecture with federated learning framework

3.1 基于决策树的入侵检测模型

通过决策树(Decision Tree)，可以构建一个高效的 AMI 入侵检测模型，它比 DNN 等更复杂的模型训练速度更快，特别是在小数据集多特征的情况下。决策树算法可解释性强、计算复杂度较低并且可处理缺失数据，它不需要复杂的数据处理工作，如归一化或标准化[18]。

构造决策树的算法有 ID3，C4.5 和 CART，相比前两种方法，CART 通过基尼指数(Gini)选择最佳决策属性，它的计算不涉及对数，因此采用该方法可更快构造出决策树模型。如式(1)所示：

$$Gini(D)=1-\sum_{u=1}^{c}p_u^2 \tag{1}$$

其中，D 表示训练数据集，c 表示数据类别数，p_u 表示类别 u 在 D 中出现的概率。

在对 AMI 系统的网络流量数据进行监测时，智能融合终端作为边缘设备需要识别每一条数据的类别，从中检测出异常数据，即攻击数据。因此可将其看作一个二分类问题，检测结果有遭到攻击与未遭到攻击两种情况。每个数据样本由特征向量和类别结果组成，将特征向量定义为一个多维矩阵 $\boldsymbol{x}$，每一列代表不同的特征属性，而每一行则代表不同的样本数据；将数据集样本的结果集合定义为一个列向量 $\boldsymbol{Y}$。因此可将每个设备所拥有的数据集合看作一个多维矩阵 $\boldsymbol{D}$，如式(2)－式(4)所示。

$$\boldsymbol{x}=\begin{bmatrix} x_{11} & x_{21} & \cdots & x_{n1} \\ x_{12} & x_{22} & \cdots & x_{n2} \\ \vdots & \vdots & \vdots & \vdots \\ x_{1s} & x_{2s} & \cdots & x_{ns} \end{bmatrix} \tag{2}$$

$$\boldsymbol{Y}=\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_s \end{bmatrix} \tag{3}$$

$$\boldsymbol{D}=\begin{bmatrix} x_{11} & x_{21} & \cdots & x_{n1} & y_1 \\ x_{12} & x_{22} & \cdots & x_{n2} & y_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{1s} & x_{2s} & \cdots & x_{ns} & y_s \end{bmatrix} \tag{4}$$

其中，n 表示特征属性个数，s 表示数据样本个数。

将第 φ 列属性命名为 L_φ，该列属性值为 $(x_{\varphi 1}\ x_{\varphi 2}\ \cdots\ x_{\varphi s})^{\mathrm{T}}$，因此将每个数据样本在该列的属性值定义为一个函数：

$$L_\varphi(x_\tau)=x_{\varphi\tau}(\varphi=1,\cdots,n;\tau=1,\cdots,s) \tag{5}$$

当选择某一属性 A 进行分支时，根据属性 A 中属性值是否满足不等式而将样本集合 D 分割为 D_1 和 D_2 两个子集：

$$\begin{cases} D_1=\{(x,y)\in D\,|\,L_A(x)\leqslant a\} \\ D_2=\bar{D_1}\cap D \end{cases} \tag{6}$$

其中，a 为特征属性 A 中某一属性值。

分别根据式(7)计算两个子集的 Gini 值：

$$Gini=2p(1-p) \tag{7}$$

其中，p 为子集 D_1 中的类别结果，y 为攻击的概率。

则此次划分的 Gini 指数为：

$$Gini(D,L_a)=\frac{|s_1|}{|s|}Gini(D_1)+\frac{|s_2|}{|s|}Gini(D_2) \tag{8}$$

其中，$s1$，$s2$ 分别是为 D_1，D_2 中的样本个数。

以最小化基尼指数值来选择特征属性作为树的节点，即：

$$\min\ Gini(D,L_k)(k=1,\cdots,n) \tag{9}$$

根据式(6)－式(9)进行特征属性的遍历，每次选择一个

节点进行分叉，在下次进行属性选择时将其从候选属性中去除。从根节点到叶节点，自上而下逐步迭代形成一棵二叉决策树。从整体来看，该二叉决策树分支过多，过于复杂，会产生严重的过拟合，且每次的特征选择考虑的是局部最优。因此，为了防止过拟合并且得到一棵更优的树，需要控制决策树的广度与深度，即对决策树进行剪枝。剪枝过程是一个全局优化的过程，正确的剪枝策略是优化决策树算法的核心[19]。

决策树的深度是由特征属性的个数决定的，用 h 表示。而决策树的广度用节点样本大小来衡量，用 r 表示，根据节点是否至少包含 $r_{\min}$ 个样本来确定是否发生分枝。寻找最佳剪枝策略的过程就是找到使模型得分最高的解(h,r)。采用随机搜索算法(Randomized Search CV，RSCV)得到的最优解是全局最优解，因此用 RSCV 进行决策树模型优化。基本原理如式(10)－式(12)所示：

$$\begin{matrix} h_{i\_\max} \\ h_{i\_\min} \end{matrix}\Big] h_i^1 \cdots h_i^j \cdots h_i^J \tag{10}$$

$$\begin{matrix} r_{i\_\max} \\ r_{i\_\min} \end{matrix}\Big] r_i^1 \cdots r_i^j \cdots r_i^J \tag{11}$$

$$f(X)=Score(h_i^j, r_i^j) \tag{12}$$

其中，f 为衡量决策树模型得分的函数，X 为函数的解，即决策树的剪枝参数值。

每个参数都有一个预先确定的参数范围，用最小值到最大值的区间表示；当进行第一次搜索时，每个参数都先在其取值范围内随机生成一个值 h_i^1(i 表示设备序号)，r_i^1，即初始解为 $X_1:(h_i^1, r_i^1)$，并计算其目标函数值 $f(X_1)$为当前的决策树模型得分，如式(11)所示；进行下一次搜索后会生成一个新解 $X_{new}:(h_i^j, r_i^j)$(j 表示某次随机搜索计算的编号)，如果 $f(X_{new})\geqslant f(X_1)$，接受当前解作为新解[20]。经过不断的迭代，当算法满足迭代上限 J 时，便可获得最终的优化结果，此时入侵检测模型的优化完成。具体流程如算法 1 所示。

算法 1 决策树优化算法

输入：分布在各边缘节点 $F_1,\cdots,F_N$ 的数据 $D_1,\cdots,D_N$，h，r 剪枝参数范围

输出：决策树优化模型

1. DT_i^0 = BuildDecisionTree()
   /* 各参与方构建初始决策树模型 */
2. FOR each $DT_1^0,\cdots,DT_N^0$ DO
3. For h_i, r_i in range
4. While using h_i^j, r_i^j, h_i^{j+1}, r_i^{j+1} by RSCV
   /* 采用随机搜索算法进行剪枝优化 */
5. $X_j:(h_i^j, r_i^j)$; $X_{j+1}:(h_i^{j+1}, r_i^{j+1})$
   /* 随机搜索生成两个不同的剪枝策略 */
6. DTacc[j] = Score(DT_i^j, (h_i^j, r_i^j))
   /* 第 j 次剪枝后决策树模型得分(即准确率) */
7. DTacc[j+1] = Score(DT_i^{j+1}, (h_i^{j+1}, r_i^{j+1}))
8. IF DTacc[j+1]≥DTacc[j] THEN /* 下一次搜索模型得分优于上一次 */
9. Select the j+1 random search result: X_{j+1}
10. ELSE:
11. return X_j /* 迭代 */
12. END IF
13. OptTree = BuildDecisionTree(DT_i^0, X)
    /* 选择最终的剪枝策略构建最优决策树模型 */
14. END FOR

3.2 基于联邦学习和决策树的入侵检测算法

与集中式和分布式入侵检测模型相比，基于联邦学习的 AMI 入侵检测方法通过只上传模型参数来降低网络传输负载与主站计算压力，同时云边协同的训练方式使各台区智能融合终端共享经验，可提升入侵检测系统在复杂网络情况下的性能，增加了攻击者的攻击成本。本文提出的基于联邦学习和决策树的入侵检测算法框架如图 3 所示。

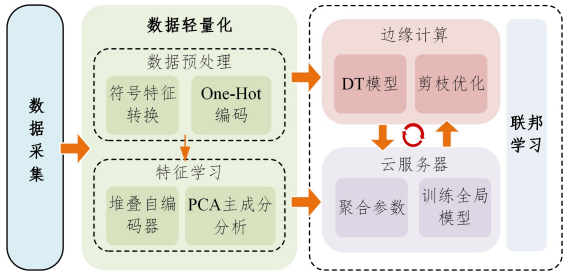


图 3 算法框架图

Fig. 3 Algorithm framework diagram

3.2.1 数据预处理

AMI 入侵检测系统采集的原始数据不能直接送入模型中，因此需要对数据集进行数字化处理。其中，Object 类型特征有 protocol_type，flag，service，将这 3 类非数值型特征编码转化为数值型，如：将 protocol_type 中“tcp”“udp”和“icmp”分别转换为“1”“2”“3”。其他非数字特征都用这种方法进行转换。

数字化处理后将其进行独热编码。独热编码又称为 One-Hot 编码，主要是采用 N 个状态寄存器来对 N 个状态进行编码，每个状态都有它独立的寄存器位，并且在任意时候只有一位有效。如：对于某个样本的 protocol_type 特征为 udp，则表示为 010。

3.2.2 特征学习

真实的 AMI 流量数据中，攻击样本数量一般少于数据集的 10%，若在这样一个不平衡的数据集上直接训练分类模型，得到的是一个主要学习多数类模式而忽略少数类特征的 DNN 模型。因此本文在不改变、生成或删除样本的情况下采用两个无监督的堆叠自动编码器来处理不平衡数据集[21]。每个自动编码器都负责从一个类中寻找模式，由于每个模型都尝试提取一个类的抽象模式而不考虑另一个类，因此该模型的输出可以很好地表示其输入。

式(13)、式(14)分别为堆叠自编码器的编码器函数和解码器函数，中间层的输出即是对原始高维数据的最新表示，如式(15)所示。

$$m_i = g(\lambda_i x_i + \phi_i) \tag{13}$$

$$x_i^* = g^*(\lambda_i^* m_i + \phi_i^*) \tag{14}$$

其中，g 和 g^* 分别是是编码器与解码器的激活函数，$\boldsymbol{\lambda}$ 和 $\boldsymbol{\lambda}^*$ 是编码器与解码器的权值矩阵，$\boldsymbol{x}$ 为样本特征的向量，ϕ 和 ϕ^* 是编码器与解码器的偏置，m 为输入经过编码器降维后的最新表示，x^* 是对输入 x 的重建，$i\in\{Normal, Attack\}$。

$$X_{new} = (M_{normal}, M_{attack}) \tag{15}$$

其中，X_{new} 是一个新的数据集，由每一个正常和攻击样本经过自编码器学习表示的超向量组成；M_{normal} 为一个 m_{normal} 矩阵，它是样本 x 为正常的特征属性的一部分，M_{attack} 为一个 m_{attack} 矩阵，表示样本 x 如何表示一个攻击样本。

再将超向量通过 PCA 主成分分析进行降维，如式(16)

所示：

$$X_{\text{new}}^{*}=X_{\text{new}}P^{*} \tag{16}$$

其中，P^{*} 为根据特征值对特征向量进行排序的第一个 K（提取的特征数）向量，X_{new}^{*} 为 PCA 降维后的结果。

数据降维后，不仅减少了数据集自身的冗余，降低了无效、错误的数据对实验的影响，有效加快入侵检测系统的检测速度，且降低了存储数据的成本，进一步优化了实验效率。

3.2.3 联邦学习框架下的云边协同训练

AMI 系统不同层级网络中的设备进行跨域交互时，智能融合终端作为下层网络边缘设备，构建本地检测模型的训练数据往往需要采集该层网络流量数据，各边缘节点因为隐私和成本方面的考虑，不愿进行数据共享，数据以“孤岛”的形式存在。数据“孤岛”的存在迫使各节点无法突破本地数据的局限，导致其入侵检测模型无法自动更新，检测性能不高。因此本节讲述了联邦学习框架下入侵检测模型的云边协同训练模式，提高各台区入侵检测精度。

将 N 个智能融合终端设备即边缘节点集合记为 $F=\{F_1,\cdots,F_N\}$。首先各边缘节点根据 2.1 节介绍构建本地决策树模型并采用随机搜索算法进行剪枝优化训练，每次随机搜索看作一次本地迭代，当达到本地训练次数时，将所求出的最优剪枝策略作为模型参数上传至云中心，如式(17)所示，本地模型参数 ω_i^t 中包含决策树的广度与深度信息。

$$\omega_i^t=X_i^t(h_i^t,r_i^t) \tag{17}$$

其中，t 表示第 t 轮通信。

云中心对各节点的本地模型参数进行聚合，合并为一个集合形式$\{\omega_1^t,\omega_2^t,\cdots,\omega_i^t\}$，将其作为全局模型随机搜索优化的范围来进行最优参数的选择，从而计算出全局模型参数 $w^{t+1}(H_{\text{opt}}^{t+1},R_{\text{opt}}^{t+1})$，如图 4 所示。

$$\begin{bmatrix}h_1^t\\ \vdots\\ h_n^t\end{bmatrix}H_{\text{opt}}^{t+1}$$

$$\begin{bmatrix}r_1^t\\ \vdots\\ r_n^t\end{bmatrix}R_{\text{opt}}^{t+1}$$

图 4 全局聚合原理图

Fig. 4 Schematic diagram of global aggregation

将全局模型的剪枝参数 w^{t+1}，也即$(H_{\text{opt}}^{t+1},R_{\text{opt}}^{t+1})$下发给各边缘节点，为了缩小最优节点的数据集与其他节点数据集之间的差异，各节点将全局模型参数 w^{t+1} 并入本地剪枝参数范围中，根据 RSCV 在更新的参数范围内训练最优的本地决策树模型剪枝参数，如式(20)、式(21)所示，至此本地模型的更新完成。再将模型参数上传，以此进行迭代，直至各子模型的精度达到平衡状态。利用更新后的本地模型对本地网络流量进行异常检测，若检测出攻击流量，则发出警报通知系统管理员主动采取相应措施。

$$(h_{i\_\min},h_{i\_\max})\rightarrow(h_{i\_\min},\cdots,H_{\text{opt}}^{t+1},h_{i\_\max}) \tag{18}$$

$$(r_{i\_\min},r_{i\_\max})\rightarrow(r_{i\_\min},\cdots,R_{\text{opt}}^{t+1},r_{i\_\max}) \tag{19}$$

云边协同训练流程如图 5 所示。

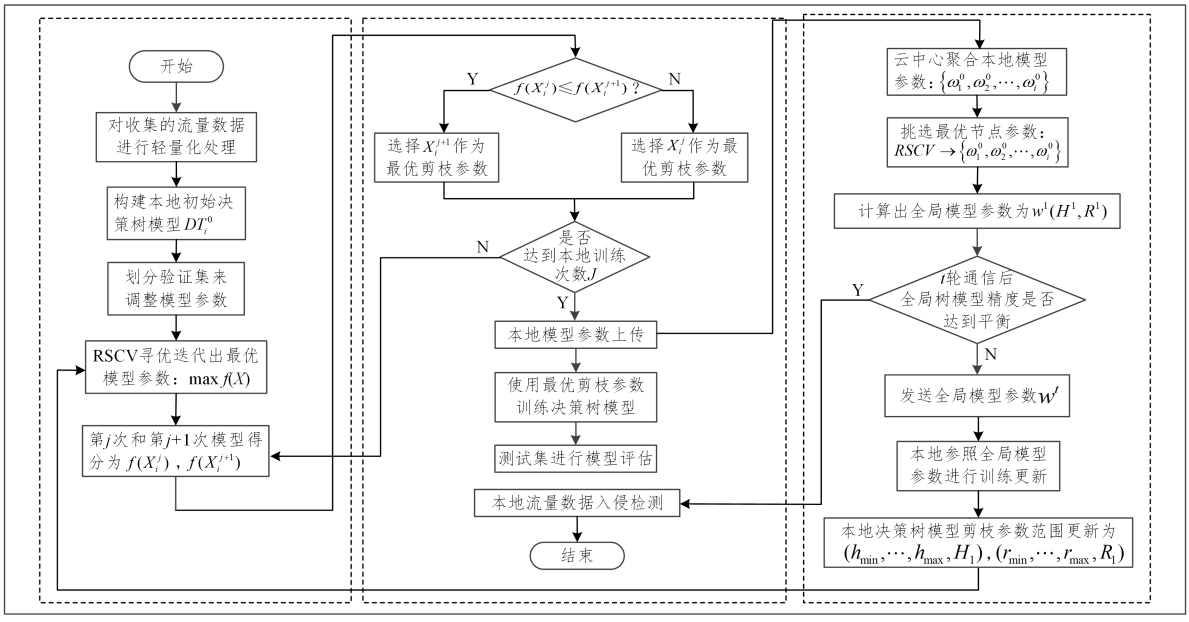


图 5 云边协同训练流程图

Fig. 5 Flow chart of cloud edge collaborative training

具体步骤为：

1）各边缘节点基于本地训练数据集构建初始决策树模型 DT_i^0，在预定的本地训练次数内采用随机搜索算法选择使决策树模型得分最高的剪枝参数；

2）将模型参数发送至云处理中心；

3）云中心聚合本地模型参数并挑选出最优节点，根据 RSCV 算法计算全局模型参数并下发；

4）各节点接收到全局参数后，更新本地剪枝参数范围，并训练出最新的模型参数；

5）重复上述步骤，直至模型精度达到平衡，结束训练。

4 实验与结果分析

4.1 数据集

本文基于 NSL-KDD 数据集进行 AMI 系统网络攻击检测模型训练和验证。其中，数据集中的每条记录都包含 41 个特征和 1 个标签的向量，41 个特征可分为基本特征、内容特征和流量特征 3 类，包括两个较小的组（同一主机功能和相同服务功能）。标签标记的攻击类型包括 DoS，Probe，U2R 和

R2L 4 类[22]，与 AMI 系统遭受的网络攻击特征相似，符合 AMI 的入侵检测实验，因此基于 NSL-KDD 数据集进行 AMI 入侵检测研究具有可行性。

NSL-KDD 数据集包含 KDDTrain＋，KDDTrain_20%，KDDTest＋和 KDDTest_20% 4 个数据集，本文分别使用 NSL-KDD 数据集的两个子集（KDDTrain＋和 KDDTest＋）进行模型训练和评估。虽然 KDDTrain＋和 KDDTest＋都包含多个类标签，但本文将它们重新分为两类，即这些数据集中包含的流量样本是正常还是异常，以关注主要评估指标的影响。

4.2 评价指标

评价分类模型的指标是基于混淆矩阵（Confusion Matrix）进行计算的，如表 1 所列。具体来说，使用真正类（TP）、真负类（TN）、假正类（FP）和假负类（FN）分别表示正确分类为攻击、正确分类为正常、错误分类为攻击和错误分类为正常的样本数量。根据这些度量，可以定义准确率（Acc）、精确度（Pre）、F1-measure（F1）和误报率（FPR），以量化模型在入侵检测中的性能，如式（20）－式（24）所示：

$$Acc=\frac{TP+TN}{TP+FP+TN+FN} \tag{20}$$

$$Pre=\frac{TP}{TP+FP} \tag{21}$$

$$Rec=\frac{TP}{TP+FN} \tag{22}$$

$$F_1=\frac{2\cdot Pre\cdot Rec}{Pre+Rec} \tag{23}$$

$$FPR=\frac{FP}{FP+TN} \tag{24}$$

其中，Acc 表示在整个数据集中被正确分类的样本的比例，在入侵检测中是一个较常用的评价指标；F_1 是 Pre 和 Rec 的加权调和平均；FPR 为误报率，表示被错分到正样本类别的负样本在全部负样本中所占比例，是入侵检测模型的重要评估指标之一[23]。

表 1 混淆矩阵

Table 1 Confusion matrix

True Label	Predict 0	Predict 1
0	TN	FP
1	FN	TP

4.3 结果分析

本文将 NSL-KDD 数据集随机划分至多个训练节点中，并设置本地迭代次数为 15，同时设定 $cv=3$，采用 3 折交叉验证来评估模型在数据集上的预测效果；调用 best_params_属性可查看优化后 DT 的最佳参数。为验证本文所提出的联邦学习框架下融合决策树的入侵检测方法的有效性，与基于联邦学习和神经网络的入侵检测方法（FL-DNN）、集中式检测方法（Concentrate）进行性能比较分析。

4.3.1 模型性能

如表 2 所列，对比本文方法、FL-DNN、集中式 3 种入侵检测方法的检测精度可知，本文方法明显优于基于联邦学习和神经网络的入侵检测方法；同时如表 3 所列，在 Pre，Rec 和 F1 等评价指标上本文方法比 FL-DNN 模型的入侵检测性能更好，与集中式模型的性能差别不大。

表 2 不同入侵检测模型的精度对比

Table 2 Accuracy comparison of different intrusion detection models

（%）

模型	准确率（Acc）
本文方法	99.76
FL-DNN	98.99
集中式	99.81

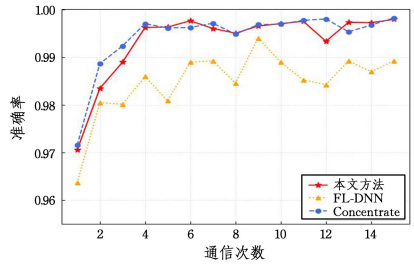
表 3 不同入侵检测模型的性能对比

Table 3 Performance comparison of different intrusion detection models

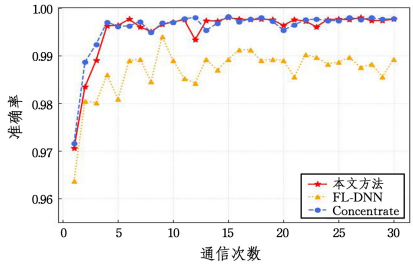
（%）

模型	Normal			Attack		
	Pre	*Rec*	F_1	*Pre*	*Rec*	F_1
本文方法	99.83	99.71	99.77	99.69	99.82	99.75
FL-DNN	99.34	99.45	99.38	93.73	96.36	95.55
集中式	99.80	99.83	99.82	99.82	99.79	99.81

图 6 给出了随着通信轮数的增加 3 种方法各模型准确率的变化情况。结果表明，与基于联邦学习和神经网络的入侵检测模型相比，本文提出的模型检测性能更优；与集中式模型相比，二者的模型检测性能几乎相当，但基于联邦学习和决策树的入侵检测模型不需要本地数据输出，只需上传模型参数即可产生和它相近的检测效果，因此在数据安全性方面有一定的优势。在 AMI 场景下，这种优势能有效分担电力通信网络传输压力，减少通信时延，满足业务的实时响应需求。



(a)15 轮通信

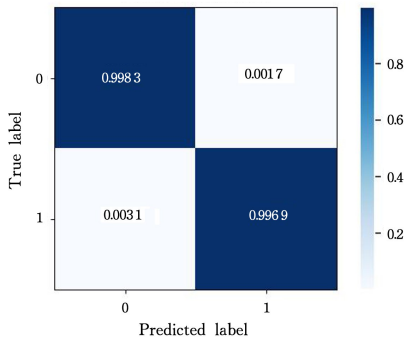


(b)30 轮通信

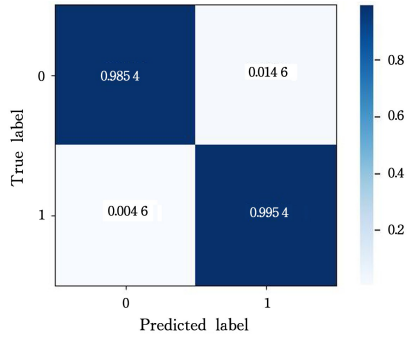
图 6 各模型准确率变化

Fig. 6 Changes of accuracy of each model

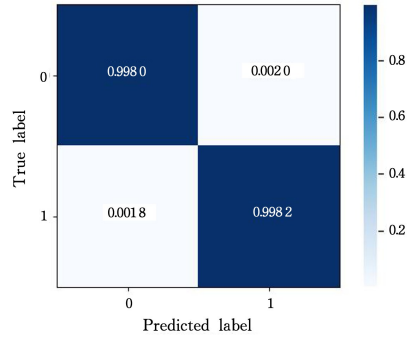
FPR 为误报率，又称虚警率，是正常样本被预测为攻击样本在所有正常样本中所占的比例。，在入侵检测中，误报率带来的损失较大，因此研究人员都期望在保证提升准确率的情况下误报率尽可能低，这样更符合实际应用的要求。图 7 分别给出了 FL-DT 模型，FL-DNN 模型和集中式 DT 模型的混淆矩阵，其中 1 表示正例，为攻击样本；0 表示反例，为正常样本。由此可得到它们的 FPR 分别为 0.17%，1.46%，0.20%。本文方法的误报率（FPR）较低，FL-DNN 模型的误报率较高，这可能是因为神经网络存在梯度消失、爆炸、计算效率低等问题，对模型的准确性有一定的影响，并会导致更高的误报率。



(a)本文方法的混淆矩阵



(b)基于联邦学习和神经网络入侵检测方法的混淆矩阵



(c)集中式检测方法的混淆矩阵

图 7　FL-DT，FL-MLP 和 Concentrate 模型的混淆矩阵

Fig. 7　Confusion matrixes of FL-DT，FL-MLP and Concentrate models

4.3.2　训练时间

我们分别计算 3 种方法的训练时间，其中传统集中学习方法的时间成本为所有训练样本训练出一个 DT 分类器所需要的时间；而基于联邦学习和神经网络方法与基于联邦学习和决策树方法的训练时间采用以下方法进行计算：包括各智能融合终端设备 D_i 分别训练本地模型所需的最大时间与上传参数后全局聚合参数训练模型所需的时间，如式(25)所示：

$$T_{\mathrm{FL}}=\max\{t_1,\cdots,t_i\}+t_{\mathrm{global}} \tag{25}$$

其中，t_i 为第 i 个智能融合终端设备训练本地模型所需时间，t_{global} 为全局训练模型所需时间。

本文实验仿真使用的软硬件平台配置为 Intel(R)Core(TM)i5-8250U 1.60 GHz 处理器，8 GB 内存，操作系统为 Windows11，主要实验工具有 Python 和 Sklearn。集中式检测的参与者只有主站，且训练数据样本为 $D=D_1\cup\cdots\cup D_N$，联邦学习框架下的入侵检测方法设定参与者数量为 5，训练数据样本为各本地训练数据集 D_i。

将本文方法的时间成本与集中式检测方法(Concentrate)、基于联邦学习和神经网络(FL-DNN)的入侵监测方法进行比较，如表 4 所列。结果表明，本文方法的时间成本低于基于联邦学习和神经网络模型，且基于联邦学习的方法的训练时间明显少于集中学习。

表 4　各模型的训练时间

Table 4　Training time of each model

(s)

模型	训练时间
本文方法	114.648 0
集中式方法	157.175 0
FL-DNN	131.496 0

结束语　针对传统入侵检测方法的局限性，本文提出了一种基于联邦学习的高级量测体系入侵检测方法，通过算例分析，验证了方法的可行性和有效性，主要结论如下：

1)提出的 AMI 场景下基于联邦学习框架的入侵检测模型实现了跨台区训练经验的共享，提高了 AMI 入侵检测模型的识别精度；同时，边缘计算技术有效减轻了主站的计算压力，降低了通信时延，而且增强了 AMI 系统的抗灾能力。

2)提出的基于联邦学习框架的入侵检测方法使整个系统更有效率且轻量，其准确率达 99.76%，误报率仅为 0.17%。

3)相较于集中式检测方法，本文方法解决了前者通信负担大的问题，所花费的时间成本降低了约 37%，更能满足业务的实时响应需求，且在一定程度上保证了数据安全。相较于结合神经网络的分布式入侵检测方法，所提方法在各性能指标上均优于前者。

在未来的工作中，我们将研究识别恶意用户上传的本地模型参数的问题，以进一步提高 AMI 系统入侵检测模型的可靠性和安全性。

参 考 文 献

[1] PANAGIOTIS I R G，PANAGIOTIS G S. Securing the Smart Grid：A Comprehensive Compilation of Intrusion Detection and Prevention Systems[J]. IEEE Access，2019，7：46595-46620.

[2] ZHANG L P，LU W，XIAO Y，et al. Anomaly Detection method of Smart Meters data based on GMM-LDAclustering feature Learning and PSO Support Vector Machine[C]// IEEE Sustainable Power and Energy Conference. Beijing，China，2019.

[3] WANG X. Multi-domain Network Intrusion Detection Based on Attention-based Bidirectional LSTM[C]// 2023 IEEE 6th Information Technology，Networking，Electronic and Automation Control Conference. Chongqing，China，2023：805-810.

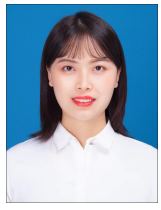
[4] YU Y，HENG Y H，LIANG Z Y，et al. AdaBoost-CNN：a hybrid method for electricity theft detection[C]// Asia Conference on Power and ElectricalEngineering(ACPEE). Chongqing，China，2021.

[5] LIU F F. Research on Application of Intrusion Detection Algorithm Based on Deep Learning in AMI[D]. Lanzhou：Lanzhou Jiaotong University，2020.

[6] OZAY M，ESNAOLA I，VURAL F，et al. Machine Learning Methods for Attack Detection in the Smart Grid[J]. IEEE Transactions on Neural Networks and Learning Systems，2016，27(8)：1773-1786.

[7] AHMED S，LEE Y D，SEUNG H H，et al. Unsupervised Machine Learning-based Detection of Covert Data Integrity Assault in Smart Grid Networks Utilizing Isolation Forest[J]. IEEE

Transactions on Information Forensics and Security, 2019, 14(10): 2765-2777.
[8] KURT M N, OGUNDIJO O, LI C, et al. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach [J]. IEEE Transactions on Smart Grid, 2018, 10(5): 5174-5185.
[9] AN D, YANG Q, LIU W, et al. Defending Against Data Integrity Attacks in Smart Grid: A Deep Reinforcement Learning-Based Approach[J]. IEEE Access, 2019, 7: 110835-110845.
[10] ZHANG Y C, WANG L F, SUN W Q, et al. Distributed IDS in a multi-layer network architecture of smart grids[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 796-808.
[11] ALSEIARI F, AUNG Z. Real-time anomaly-based distributed intrusion detection systems for advanced Metering Infrastructure utilizing stream data mining[C]// International Conference on Smart Grid and Clean Energy Technologies. Offenburg, Germany, 2016: 148-153.
[12] ZHAO R J, YIN Y, SHI Y, et al. Intelligent intrusion detection based on federated learning aided long short-term memory[J]. Physical Communication, 2020, 42: 1874-4907.
[13] RAHMAN S, TOUT H, TALHI C, et al. Internet of things intrusion detection: Centralized, on-device, or federated learning? [J]. IEEE Network, 2020, 34(6): 310-317.
[14] WANG R, MA C G, WU P. Intrusion detection method based on federated learning and convolutional neural network[J]. Information Network Security, 2020(4): 47-54.
[15] TANG Z, MIN Q Q. Line Fault Monitoring System of Distribution Network Based on Power Line Carrier and ZigBee Technology[J]. Journal of Electric Power Science and Technology, 2012, 27(1): 70-74.
[16] LUO H X, JIN X, QIAN B, et al. Security protection method of intelligent terminal and smart electricity meter based on block chain[J]. China Southern Power Grid Technology, 2021, 15(4): 50-58.
[17] ROBERTO M C. Modular Advanced Metering Infrastructure to Reduce Electricity Theft and a Cluster-Based Illegal Loads Detection[J]. IEEE Latin America Transactions, 2023, 21(4): 579-587.
[18] ZHANG Y. Research on decision tree classification and pruning algorithm[D]. Harbin: Harbin University of Technology, 2009.
[19] SHI W C. Research on industrial internet intrusion detection method based on integrated learning[D]. Changchun: Jilin University, 2022.
[20] JIANG H B, LIU B, YUAN W H. Research on Adaptive Random Search Algorithm Based on Metropolis Criterion[J]. Science and Technology in Western China, 2015, 14(3): 17-19.
[21] JAHROMI A, KARIMIPOUR H, DEHGHANTANHA A, et al. Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber-Physical Systems [J]. IEEE Internet of Things Journal, 2021, 8(17): 13712-13722.
[22] ZHANG S C, XIE X Y, XU Y. Intrusion Detection Method Based on DCNN[J]. Journal of Tsinghua University (Natural Science Edition), 2019, 59(1): 46-54.
[23] MA Q, HU J H, YU Y J. Research on intrusion detection based on decision tree algorithm[J]. Telecommunication Engineering Technology and Standardization, 2022, 35(5): 33-39.



LIU Dongqi, born in 1986, Ph.D, associate professor. His main research interests include intelligent grid information processing and distributed collaborative control.

LIANG Haolan, born in 1993, Ph.D candidate. Her main research interest is power system information security.