基于联邦学习的电力通信网络异常检测与安全防御机制

刘　妍[1]　杨世博[2]
1.哈尔滨石油学院　黑龙江哈尔滨　150028
2.国网哈尔滨供电公司　黑龙江哈尔滨　150028

摘　要：本文聚焦于电力通信网络的安全问题，提出基于联邦学习的异常检测与安全防御机制。传统集中式机器学习方法在电力通信网络中面临数据隐私泄露、通信开销大等挑战。联邦学习通过分布式训练模式，在不共享原始数据的前提下实现模型协同训练。本文详细阐述了联邦学习在电力通信网络异常检测中的应用，包括模型架构设计、数据预处理、训练算法优化等关键环节。同时，针对联邦学习可能遭受的投毒攻击、推理攻击等安全威胁，提出了基于差分隐私、安全多方计算和模型鲁棒性提升的防御策略。实验结果表明，所提机制在检测准确率和安全性方面均有显著提升，为电力通信网络的安全运行提供了有效保障。

关键词：联邦学习；电力通信网络；异常检测；安全防御；差分隐私

随着智能电网和能源互联网的快速发展，电力通信网络作为电力系统的“神经中枢”，其安全性与可靠性直接关系到整个电力系统的稳定运行。电力通信网络不仅承载着电力调度、控制指令等关键业务，还涉及大量用户隐私和敏感信息。然而，随着网络攻击手段的不断升级，电力通信网络面临着日益严峻的安全挑战，如数据泄露、恶意攻击、异常行为等，这些威胁可能导致电力系统中断、设备损坏甚至大面积停电等严重后果。机器学习作为一种强大的数据分析工具，在网络安全领域展现出巨大的潜力。传统的集中式机器学习方法需要将所有数据集中到中心服务器进行训练，这在电力通信网络中存在诸多问题：一方面，数据传输过程中存在隐私泄露风险；另一方面，海量数据的集中处理对服务器性能要求极高，且通信开销巨大。联邦学习作为一种新兴的分布式机器学习技术，为解决这些问题提供了新思路。它允许参与方在本地训练模型，仅共享模型参数而非原始数据，从而在保护数据隐私的同时实现模型协同训练。本文将深入探讨基于联邦学习的电力通信网络异常检测与安全防御机制，旨在构建一个高效、安全、可靠的电力通信网络安全防护体系，为电力系统的稳定运行提供坚实保障。

一、联邦学习在电力通信网络异常检测中的应用

（一）联邦学习模型架构设计

联邦学习在电力通信网络异常检测中的模型架构主要包括参与方、参数服务器和全局模型三个部分。参与方为电力通信网络中的各个节点，如变电站、配电终端等，每个参与方拥有本地的数据集，并在本地进行模型训练。参数服务器负责协调参与方的训练过程，收集并聚合参与方上传的模型参数，更新全局模型。全局模型是所有参与方协同训练的结果，用于对电力通信网络中的异常行为进行检测。

在模型架构设计中，需要考虑参与方的异构性，即不同参与方的数据分布、计算能力和通信条件可能存在差异。因此，采用异步联邦学习算法，允许参与方根据自己的情况选择合适的时机上传模型参数，提高训练效率和灵活性。

（二）数据预处理

电力通信网络中的数据具有多样性和复杂性，包括网络流量数据、设备状态数据、用户行为数据等。为了提高异常检测的准确性，需要对这些数据进行预处理。首先，进行数据清洗，去除噪声数据和异常值，确保数据的质量。其次，进行特征提取，从原始数据中提取出与异常检测相关的特征，如网络流量的统计特征、设备状态的变化特征等。最后，对数据进行标准化处理，将不同特征的数据缩放到相同的范围，避免某些特征对模型训练产生过大影响。

（三）训练算法优化

联邦学习的训练过程是一个迭代优化的过程，为了提高训练效率和模型性能，需要对训练算法进行优化。采用联邦平均算法作为基础训练算法，该算法通过加权

平均的方式聚合参与方上传的模型参数，更新全局模型。为了进一步提高算法的收敛速度和稳定性，引入动量梯度下降算法，在更新模型参数时考虑历史梯度信息，加速模型的收敛。同时，采用学习率衰减策略，随着训练的进行逐渐减小学习率，避免模型在训练后期出现震荡。

二、电力通信网络联邦学习的安全威胁与防御策略

（一）安全威胁分析

联邦学习在电力通信网络中的应用宛如一把双刃剑，尽管为数据隐私保护和协同训练带来了显著优势，但也使系统暴露于多种复杂的安全威胁之下。其中，投毒攻击和推理攻击犹如两颗隐藏在暗处的“定时炸弹”，对电力通信网络联邦学习的安全性和可靠性构成了严重挑战。

1.投毒攻击

投毒攻击是一种极具破坏性的安全威胁，攻击者通过精心策划和巧妙手段，篡改参与方的本地数据或模型参数，如同在全局模型的“营养液”中注入毒素，向其注入恶意信息，进而破坏模型的性能和准确性。在电力通信网络的复杂环境中，攻击者有多种途径实施投毒攻击。

一方面，攻击者可以利用系统漏洞或社会工程学手段，获取参与方的本地数据访问权限，故意在本地数据中添加异常样本。这些异常样本就像隐藏在正常数据中的“陷阱”，在模型训练过程中，会使模型学习到错误的模式和特征。例如，在电力通信网络的流量数据中，攻击者添加大量异常的高流量数据样本，导致模型误认为这种高流量是正常现象。当实际网络中出现真正的异常高流量攻击时，模型却无法准确检测，从而使检测准确率大幅下降，严重影响电力通信网络的安全运行。另一方面，攻击者还可以直接篡改参与方上传的模型参数。在联邦学习的分布式训练过程中，参与方将本地训练得到的模型参数上传至参数服务器进行聚合。攻击者可以在这个传输过程中截获模型参数，并对其进行恶意修改。被篡改的模型参数会干扰全局模型的更新方向，使模型逐渐偏离正确的训练轨迹，最终导致模型性能恶化，无法有效完成异常检测等任务。

2.推理攻击

推理攻击则是一种更为隐蔽的安全威胁，它如同一个“隐形的窃听者”，攻击者通过分析参与方上传的模型参数或全局模型的输出，试图推断出参与方的本地数据信息，从而泄露用户隐私。在电力通信网络中，用户隐私涉及多个方面，包括网络流量模式、设备状态信息、用户用电习惯等，这些信息的泄露可能会给用户带来严重的经济损失和安全风险。例如，攻击者可以通过观察参与方上传的模型参数的变化，运用先进的机器学习算法和数据分析技术，逆向推断出参与方的网络流量模式。如果攻击者得知某个变电站的网络流量在特定时间段内出现异常增加，就可以推测该变电站可能正在进行设备维护或遭受攻击，从而有针对性地进行进一步的网络攻击或破坏活动。又如，攻击者可以通过分析全局模型的输出，结合已知的背景知识，推断出参与方的设备状态信息。如果模型输出显示某个配电终端的某些参数异常，攻击者可以推断该终端可能存在故障或被恶意控制，进而实施更精准的攻击。

（二）防御策略

1.差分隐私保护

差分隐私保护是一种在数据发布过程中添加精心设计的噪声，以保护个人隐私的先进技术。在电力通信网络联邦学习中，将差分隐私保护应用于参与方上传模型参数的环节，就像为模型参数披上了一层“神秘的面纱”，使得攻击者无法从模型参数中准确推断出单个参与方的本地数据信息。具体实现时，通常采用拉普拉斯机制或高斯机制添加噪声。拉普拉斯机制通过在模型参数中添加服从拉普拉斯分布的噪声，使得相邻数据集（即仅有一个数据点不同的数据集）的输出概率分布相似，从而保护了单个数据点的隐私。高斯机制则是添加服从高斯分布的噪声，在满足一定隐私条件的情况下，也能有效保护数据隐私。在实际应用中，需要根据具体场景和隐私需求，合理控制隐私预算。隐私预算决定了添加噪声的大小，隐私预算越小，添加的噪声越大，对隐私的保护越强，但同时也会对模型性能产生一定的影响。因此，需要在保护隐私和保证模型性能之间找到一个平衡点，在保护用户隐私的同时，尽量减少对模型准确性和效率的影响。例如，在电力通信网络的异常检测任务中，可以通过实验和调整，确定一个合适的隐私预算，使得添加噪声后的模型仍然能够保持较高的检测准确率，同时有效防止用户隐私泄露。

2.安全多方计算

安全多方计算是一种在多个参与方之间进行协同计算，而无需泄露任何一方原始数据的强大技术。在电力通信网络联邦学习中，利用安全多方计算实现模型参数的安全聚合，就像为模型参数的传输和计算打造了一个“安全的密室”，确保参与方的本地数据在传输和计算过

程中始终保持加密状态，有效保护了数据隐私。例如，采用基于同态加密的安全多方计算协议。同态加密是一种特殊的加密技术，它允许在加密数据上进行计算，而无需先解密数据。参与方在本地对模型参数进行加密后上传到参数服务器，参数服务器在加密状态下对模型参数进行聚合操作，如加法、乘法等。由于同态加密的性质，加密状态下的聚合结果与解密后的聚合结果是一致的。最后，参数服务器将聚合结果解密后返回给参与方，参与方根据解密后的结果更新本地模型。通过这种方式，即使攻击者截获了加密的模型参数，也无法获取其中的原始信息，因为解密需要特定的密钥，而密钥只有合法的参与方拥有。安全多方计算为电力通信网络联邦学习中的数据隐私保护提供了一种可靠的解决方案，使得不同参与方能够在不泄露本地数据的前提下，共同完成模型训练任务，提高了系统的安全性和可靠性。

3.模型鲁棒性提升

为了提高联邦学习模型对投毒攻击的鲁棒性，需要采用先进的鲁棒性聚合算法。传统的加权平均聚合算法在面对投毒攻击时较为脆弱，因为异常的模型参数会通过加权平均的方式影响全局模型的更新。而基于中位数的聚合算法则具有更好的鲁棒性，它就像一个“稳健的裁判”，在聚合参与方上传的模型参数时，选择中位数作为全局模型的参数更新值，而不是采用加权平均的方式。中位数对异常值具有较好的鲁棒性，即使有部分参与方的模型参数被攻击者篡改，中位数也能够忽略这些异常值的影响，选择一个相对稳定的值作为全局模型的更新参数。例如，在一个包含多个参与方的联邦学习系统中，假设大部分参与方的模型参数是正常训练得到的，而少数参与方的模型参数被攻击者篡改，变得异常大或异常小。采用基于中位数的聚合算法时，这些异常的模型参数不会对中位数的计算产生显著影响，全局模型仍然能够基于正常的模型参数进行更新，从而有效抵抗投毒攻击对模型参数的影响。

三、实验与结果分析

（一）实验设置

为了验证基于联邦学习的电力通信网络异常检测与安全防御机制的有效性，搭建了实验平台。实验采用真实的电力通信网络数据集，包括网络流量数据和设备状态数据。将数据集划分为训练集和测试集，训练集用于训练联邦学习模型，测试集用于评估模型的性能。实验中设置多个参与方，模拟电力通信网络中的不同节点。采用不同的安全防御策略进行对比实验，包括无防御策略、差分隐私保护、安全多方计算和模型鲁棒性提升。

（二）实验结果

实验结果表明，基于联邦学习的异常检测模型在检测准确率上明显优于传统的集中式机器学习方法。在无防御策略的情况下，模型容易受到投毒攻击和推理攻击的影响，检测准确率下降明显。而采用差分隐私保护、安全多方计算和模型鲁棒性提升等防御策略后，模型的检测准确率得到显著提高，同时有效保护了用户隐私。具体来说，差分隐私保护策略在一定程度上降低了模型的检测准确率，但能够有效防止推理攻击；安全多方计算策略对模型性能影响较小，同时保证了数据的安全传输和计算；模型鲁棒性提升策略能够有效抵抗投毒攻击，提高模型的稳定性和可靠性。

结语

本文提出了一种基于联邦学习的电力通信网络异常检测与安全防御机制，通过分布式训练模式保护数据隐私，采用差分隐私、安全多方计算和模型鲁棒性提升等防御策略应对安全威胁。实验结果表明，该机制在检测准确率和安全性方面均有显著提升，为电力通信网络的安全运行提供了有效保障。未来，将进一步优化联邦学习算法，提高模型的训练效率和性能，探索更多的安全防御策略，以应对不断升级的网络攻击手段。同时，将加强与其他领域的交叉融合，如区块链技术，进一步提升电力通信网络的安全性和可靠性。

参考文献

[1]李义.基于人工智能的电力通信传输网络异常检测算法[J].通信电源技术，2025，42（2）：242-245.

[2]魏晶平，杜梦迪，王阔.基于深度学习的电力通信网络异常数据流入侵自动检测方法[J].自动化应用，2025，66（4）：247-248，252.

[3]张楠，李涛涛.基于模糊神经网络的电力通信信号异常检测研究[J].通信电源技术，2024，41（3）：191-193.

[4]孙祥刚.基于加权SVM的电力通信网络异常流量入侵检测方法[J].通信电源技术，2024，41（10）：91-93.