

基于改进联邦学习的无线通信网络入侵安全检测方法

熊磊[†]

(汉中职业技术学院, 陕西 汉中 723002)

摘要:针对目前无线通信网络领域存在的安全问题,提出了一种基于改进联邦学习的无线通信网络入侵安全检测方法。改进联邦学习框架包含本地训练和服务器聚合两部分。本地训练基于注意力-门控循环单元(Attention-gated Recurrent Unit, AGRU)训练本地数据,并上传服务器。服务器基于注意力机制(Attention Mechanism, AM)为每个客户端赋予不同的权重,并对加权后的模型参数进行聚合。通过消融实验验证了所提改进联邦学习框架的有效性。与 FedAvg 和 FedNovaka 联邦学习框架相比,所提方法综合性能最优。所提方法为无线通信网络入侵检测的发展提供了一定借鉴,具有广泛的应用前景。

关键词:无线通信网络;联邦学习;深度学习;卷积神经网络;注意力机制

中图分类号:TP393

文献标识码:A

A Wireless Communication Network Intrusion Security Detection Method Based on Improved Federated Learning

XIONG Lei[†]

(Hanzhong Vocational and Technical College, Hanzhong, Shaanxi 723002, China)

Abstract: A wireless communication network intrusion security detection method based on improved federated learning is proposed to address the current security issues in the field of wireless communication networks. Improving the federated learning framework also includes two parts: local training and server aggregation. Local training is based on attention gated recurrent unit (AGRU) to train local data and upload it to the server. The server assigns different weights to each client based on the attention mechanism (AM) and aggregates the weighted model parameters. In the experimental stage, the effectiveness of the proposed improved federated learning framework was verified through ablation experiments. Compared with FedAvg and FedNovaka federated learning frameworks, the proposed method has the best overall performance. The proposed method provides a certain reference for the development of intrusion detection in wireless communication networks and has broad application prospects.

Key words: wireless communication network; federated learning; deep learning; convolutional neural networks; attention mechanism

随着无线通信网络流量和用户数量的急剧增加^[1-3],无线通信网络正承受着网络安全和性能方面面临的若干挑战^[4]。无线通信网络的无线信道

特性使得连接不稳定,容易受到恶意入侵。因此,需要高效的入侵检测^[5]算法确保数据安全和网络性能。

收稿日期:2024-01-08

基金项目:陕西省中华职业教育社2023年职业教育研究课题(ZJS202367);汉中中院2021年院级教学研究与教学改革项目(HZZYJY2021006)

作者简介:熊磊(1985—),男,陕西汉中,人,硕士研究生,讲师,研究方向:计算机应用技术。

[†]通信联系人, E-mail: xuelei20061@163.com

目前,许多学者针对入侵检测进行了研究。文献[6]提出一种新型生成对抗网络的无线传感器网络异常检测方法。文献[7]构建了一个基于卷积神经网络和双向长短时记忆(Bidirectional Long Short-term Memory, Bi-LSTM)网络的检测模型,并将其应用于各类入侵检测系统。然而上述入侵检测方法大多是集中式学习方法,需要将大量数据上传到服务器。该过程中,模型性能很容易受到不稳定和低速传输信道的影响。此外,常见的机器学习算法通常遵循数据是独立同分布(Independent and Identically Distributed, IID)的假设。然而,在实际网络(尤其是边缘网络)中,设备生成的数据通常是非独立同分布(Non-independent and Uniformly Distributed, NIID)数据。使用现有的机器学习方法对 NIID 数据进行训练会导致模型精度低和模型收敛失败。

有学者提出基于联邦学习框架的网络入侵检测模型,从而以分布式训练的方法提高局部参与者模型的准确性。与传统的集中式学习方法相比,联邦学习不需要将原始数据传输到中央服务器。因此,在确保模型准确性的同时,可有效降低数据泄露的风险。文献[8]提出了一种联盟链下基于联邦学习聚合算法的入侵检测方法。文献[9]提出了一种基于深度神经网络和联邦学习的网络入侵检测方法。尽管联邦学习已成为入侵检测领域的主流方案,然而在联邦学习框架中,通信成本和分类精度仍是一个重难点问题。

本研究提出了一种改进联邦学习的无线通信网络入侵安全检测方法,旨在建立一种联邦学习框架提高学习效率及入侵检测精度。

1 问题陈述

近年来,深度学习越来越多地应用于无线网络入侵检测。然而,随着入侵检测数据量不断增多,传统基于集中式的训练方法存在资源限制、高传输延迟、数据和隐私安全等问题。为此,可充分利用边缘计算的特点和优势,利用网络边缘的计算资源进行联邦学习以实现协同入侵检测。边缘网络的联邦学习框架中,云中心需要与多个边缘节点进行交互。一方面,由于客户端和服务端之间的无线连接通常较慢或不可靠,因此客户端和服务端间的通信循环次数将尽可能小;另一方面,任何单个客户

端的数据集都小于总数据集,边缘客户端的处理器相对较快。因此,与通信成本相比,计算成本通常可以忽略不计,并且通信延迟成为学习框架的性能瓶颈。

传统联邦学习框架图如图 1 所示。其主要有两个实体:客户端和联邦学习服务器。客户端使用私有数据集训练本地入侵检测模型,并且只向服务器(通常位于云中心)发送本地模型参数;然后,所有收集到的本地模型通过聚合以生成全局模型。需注意,客户端包括边缘设备、路由器和传感器等网络实体;联邦学习服务器包括数据库、云等。同时,客户端和联邦学习服务器之间通常以互联网进行通信。

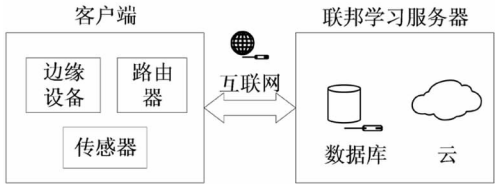


图 1 传统联邦学习框架图

假设客户端 k 存储的本地数据集为 D_k , 联邦学习框架下的入侵检测的主要过程总结如下:首先,服务器确定入侵检测的训练任务,并指定训练过程的全局模型和超参数。其次,服务器向选择的客户端广播初始化的全局模型参数 w'_G 。然后,基于全局模型 w'_G , 每个客户端使用本地私有数据更新本地模型参数 w_k^{t+1} 。客户端 k 在迭代 t 时的目标为找到使损失函数最小化的最优参数为:

$$w_k^{t+1} = \arg \min L(w'_k, D_k) \tag{1}$$

式中: L 为损失函数。

接下来,所有 K 个客户端协同训练全局预测模型,并将本地训练模型参数发送给服务器。传统联邦学习框架下,服务器聚合所有客户端模型参数,通过平均操作获得新的全局模型:

$$w_G^{t+1} = w'_G + \sum_{k=1}^K \frac{1}{N} w_k^{t+1} \tag{2}$$

式中: w_G^{t+1} 为迭代 $t+1$ 时的全局模型参数; w'_G 为迭代 t 时的全局模型参数; N 为客户端总数; w_k^{t+1} 为迭代 $t+1$ 时客户端 k 的模型参数。

考虑到某些客户端的本地优化更新与服务端上的全局聚合更新不密切相关,为了避免不相关的本地更新过多浪费通信传输资源,每个客户端都应该预先了解全局聚合优化更新趋势。本研究的目

标是在确保学习算法收敛的同时,最大限度地减少与服务器通信回合的累积次数:

$$\begin{cases} o_{\text{total}} = \min \sum_{t=1}^T C_t \\ \text{s. t. } \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{t=1}^T |f(x_t) - f(x^*)| = 0 \end{cases} \quad (3)$$

式中: C_t 为第 t 次迭代时向服务器上传本地更新的客户端的数量; T 为迭代总次数; $f(x_t)$ 为本地客户端预测函数; $f(x^*)$ 为全局更新函数; x_t 为第 t 次迭代时客户端本地数据; x^* 为服务器全局数据。

2 入侵检测模型

为加快模型收敛速度,降低通信开销,减少本地坏权重参数干扰全局参数更新的影响,本文提出了一种改进联邦学习的无线网络入侵检测方法。参考传统联邦学习框架,改进联邦学习框架也包含两部分:本地训练和服务器聚合。客户端通过注意力-门控循环单元(Attention-gated Recurrent Unit, AGRU)训练本地数据,并上传服务器。服务器基于注意力机制(Attention Mechanism, AM)为每个客户端赋予不同的权重,并对加权后的模型参数进行聚合,从而提升模型训练性能。

2.1 本地训练

传统联邦学习算法通常采用深度神经网络(Deep Neural Network, DNN)和随机梯度下降(Stochastic Gradient Descent, SGD)训练本地数据。网络流量数据本质上是一种时间序列数据,传统 DNN 无法有效学习时间序列中的隐含关系。为此,可采样递归神经网络(Recurrent Neural Networks, RNN)或其变种(LSTM、GRU)处理序列数据。GRU 在时间序列中具有强大的记忆能力,其可以学习较长上下文序列的依赖性,而不局限于局部特征。与 LSTM 相比,GRU 简化了网络结构,减少了模型参数。为进一步提升模型训练性能,本研究提出了一种 AGRU 执行本地训练。所提 AGRU 包含 4 层结构:输入层、GRU 层、注意力层、输出层。AGRU 结构图如图 2 所示。

输入层:输入层首先基于滑动窗口提取本地网络数据,以确保数据每小时连续性。提取的数据用作特征向量,并输入到 GRU 网络的一个时间步长中。窗口以一个步长在滞后数据上连续滑动,以确

保 GRU 的相邻时间步长处的矢量的连续性。

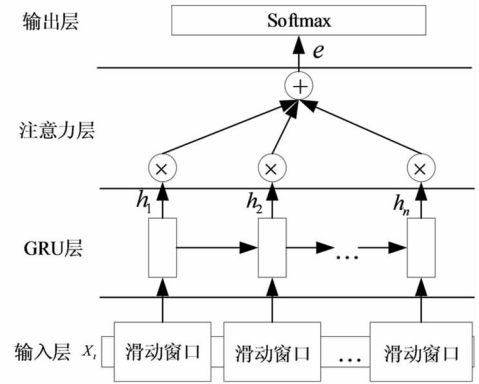


图 2 AGRU 结构图

GRU 层:令时间 t 时输入的序列为 X_t 。隐藏层 t 时的输出状态 h_t 可通过更新 GRU 的 $(t-1)$ 时的状态 h_{t-1} 获得。接着,将 h_t 作为特征值输入到网络的下一层。GRU 层特征提取过程可表示为:

$$r_t = \sigma(w_r \cdot [h_{t-1}, X_t]) \quad (4)$$

$$z_t = \sigma(w_z \cdot [h_{t-1}, X_t]) \quad (5)$$

$$\tilde{h}_t = \tanh(w_h \cdot [r_t h_{t-1}, X_t]) \quad (6)$$

$$h_t = (1 - z_t)h_{t-1} + z_t \tilde{h}_t \quad (7)$$

$$g_t = \sigma(w_o h_t) \quad (8)$$

式中: X_t 为输入序列; σ 为激活函数; h 输出特征; $\tilde{h}$ 为候选输出; 下标 t 为第 t 时的时间步长; $t-1$ 为第 $t-1$ 时的时间步长; w 为需要确定的参数; 下标 r 为确定如何将新输入信息与先前存储器组合的重置门; 下标 z 为定义需要将多少先前信息保存到当前时间步长的更新门; g 为最终输出。

注意力层:本研究引入注意力机制用于捕捉数据中的关键信息,并将每一时刻提取的特征组合成一个融合特征,该过程可以表示为:

$$e = \tanh(w^T G) \quad (9)$$

式中: e 为通过注意力机制形成的融合特征; H 为由 GRU 层的输出特征 $[h_1, h_2, \dots, h_n]$ 组成的特征向量; w 为训练的权重参数; T 为转置操作。

输出层:传统深度学习分类模型经常使用 Softmax 激活函数作为其最后一个神经网络层来获得分类结果,并最大限度地减少交叉熵损失。为提升训练性能,本研究使用铰链损失函数(Hinge Loss, HL)作为目标函数:

$$L = \min \frac{1}{2} \|w\|_2^2 +$$

$$C \sum_{i=1}^n \max(0, 1 - y_i(\omega x_i + b_i))^2 \quad (10)$$

式中: y_i 为真实标签; x_i 为 GRU 模型的输出; ω 为训练权重, C 为容错的惩罚参数。惩罚系数过大会导致过拟合和模型泛化能力差; 较小的惩罚系数会导致拟合不足, 并增加分类错误的数量。决策函数为每个类别生成一个得分向量, 并返回最大值作为预测类别:

$$L_C = \arg \max (\text{sign}(\omega x_i + b_i)) \quad (11)$$

2.2 服务器聚合

当本地模型训练完数据后将权重参数上传至服务器。本研究基于注意力机制计算上传的模型参数的重要性, 以便根据不同的客户端的重要性对其进行排序。当带宽资源稀缺时, 可以优先允许具有高重要性(上传参数的权重高)的客户端上传, 这减少了对模型整体性能的影响。如果局部模型的重要性低于某个阈值并超过设定次数, 则不再计算该模型, 并且只接受全局模型参数进行更新。这种机制降低了计算成本, 并在确保模型收敛的同时大大降低了通信成本。

假设在第 t 次迭代中, k 个客户端输出的模型参数向量集表示为 $\mathbf{W} = [\omega_1, \omega_2, \dots, \omega_k]$, 基于注意力机制生成加权输出表示:

$$\begin{cases} M = \tanh(\mathbf{W}) \\ A = f_{\text{sm}}(\mathbf{W}_m^T M) \\ \mathbf{W}^* = H A^T \end{cases} \quad (12)$$

式中: $\mathbf{W}_m^T$ 为要学习的参数矩阵; $\mathbf{A} = [a_1, a_2, \dots, a_k]$ 为不同客户端的参数的重要性权重。此外, 本研究还结合了权重归一化降低计算成本。权重越大, 客户端对整体入侵检测性能就越重要。如果最终获得的客户端的参数权重小于设置的阈值 μ , 则该参数不参与服务器的参数聚合。假设所获得的参数权重大于阈值 μ 的模型参数集为 $\mathbf{W} = [\omega_1, \omega_2, \dots, \omega_s]$, 则最终收敛的模型参数 $\mathbf{W}_G$ 为:

$$\mathbf{W}_G = \sum_{i=1}^s \frac{|D_i|}{\bar{N}} a_i \omega_i \quad (13)$$

式中: $\bar{N}$ 为最终选定客户的数据样本总数; $|D_i|$ 为第 i 个样本的数量。

3 实验与分析

3.1 实验设置

为了验证本文提出的改进联邦学习的性能, 本

节以 python + pytorch + PySyft 搭建联邦学习框架, 运行在 Pycharm 2021 社区版。训练时采用 Adam 优化器对本地 AGRU 网络参数进行更新。搭建的联邦学习框架包括 1 个服务器和 2 个客户端(台式机和笔记本)。服务器配置如下: 操作系统为 win10 64 位的工作站, 处理器为 Inter(R)Core(TM)i7-8700k CPU@3.70 GHz, 内存为 32 GB, 固态 256 G, 显卡为 NVIDIA GeForce RTX 3080 1 块。台式机客户端配置如下: 操作系统为 win 10 64 位台式电脑, 处理器为 Intel(R) Core(TM) i5-1135G7 CPU@ 2.40 GHz, 内存为 16 G, 显卡为 NVIDIA Quadro P5000。笔记本配置如下: 操作系统为 win10 64 位的联系笔记本, 显卡为酷睿 i7 7500U @2.7 GHz, 内存为 8 G, 显卡为 NVIDIA Geforce 940MX。

实验时使用的数据集为 KDD CUP 99 数据集和 CIC-IDS-2017 数据集。KDD CUP 99 数据集中训练数据包含约 500 万条网络连接, 测试数据包含约 200 万条网络连接。数据集中每个网络连接被标记为正常(Normal)或异常(Attack), 异常类型包含 4 大类: 拒绝服务攻击(DOS)、监视和其他探测活动(Probing)、远程非法访问(R2L)、普通用户非法访问本地超级用户(U2R)。CIC-IDS-2017 数据集包含良性连接和常见的攻击, 包括源数据和基于时间戳、源和目标 IP、源和目标端口、协议和攻击令牌流的网络流量分析结果, 并以 CSV 格式进行存储。该数据集包含的暴力破解攻击包括暴力 FTP、暴力 SSH、DoS、Heartbleed、Web 攻击、渗透、僵尸网络和 DDoS 等。将每个数据集按 8:1:1.5 分为训练和测试集。训练集平均分为 10 个客户端, 每个客户端学习自己的模型, 并将模型参数上传到服务器进行聚合。此外, 实验时随机抽取 KDD CUP 99 测试集中部分数据生成 IID 数据集, 抽取 CIC-IDS-2017 测试集中部分数据构成 NIID 数据集。

实验时超参数设置如下: 容错惩罚参数设置为 0.5, 初始学习率设置为 1×10^{-4} , 最大迭代次数为 30000, Dropout 设置为 0.5, 学习率衰减周期设置为 800, 衰减率设置为 0.1。

3.2 结果与分析

3.2.1 消融实验

为了验证所提方法在网络入侵安全检测中的性能, 实验时采用均方根误差(Root Mean Squared

Error, RMSE) 为指标对不同方法进行评估。RMSE 可评估不同方法的训练能力, RMSE 越低表明模型训练性能越高。对比的基准联邦学习方法包括 FedAvg(Federated Averaging)和 FedNova

(Federated Learning via Normalized Averaging)。对比的基准本地训练模型包括 Bi-LSTM、GRU-SVM 等主流深度神经网络模型。对比的损失函数包括交叉熵和 HL。

表 1 不同策略下消融实验 RMSE 对比结果

联邦学习	本地训练		损失函数		CIC-IDS-2017	KDD CUP 99
	Bi-LSTM	GRU-SVM	AGRU	交叉熵		
FedAvg	✓			✓	0.0898	0.0830
		✓		✓	0.0873	0.0792
			✓	✓	0.0871	0.0787
	✓				0.0891	0.0788
		✓			0.0878	0.0789
			✓		0.0863	0.0784
FedNova	✓			✓	0.0853	0.0778
		✓		✓	0.0848	0.0763
			✓	✓	0.0833	0.0749
	✓				0.0863	0.0778
		✓			0.0847	0.0763
			✓		0.0831	0.0742
所提方法	✓			✓	0.0843	0.0759
		✓		✓	0.0830	0.0745
			✓	✓	0.0801	0.0711
	✓				0.0832	0.0758
		✓			0.0831	0.0757
			✓		0.0781	0.0663

不同策略下消融实验 RMSE 对比结果如表 1 所示。可以观察到,所提改进联邦学习框架(AGRU+HL)在 2 个数据集上实现了比其他方法更好的 RMSE 性能。在 KDD CUP 99 数据集上,本地训练模型采用 AGRU+ HL,与 FedAvg、FedNovaka 联邦学习框架相比,所提改进联邦学习框架(AGRU+HL)的 RMSE 值分别减少了 1.21%和 0.79%。结果表明,在所提改进联邦学习框架下,使用 AGRU 和 HL 有效地提高了模型的性能。此外,在 CIC-IDS-2017 数据,本地训练模型采用 AGRU+ HL,与 FedAvg、FedNovaka 联邦学习框架相比,所提改进联邦学习框架(AGRU+HL)的 RMSE 值分别减少了 0.82%和 0.5%,表明了改进联邦学习框架(AGRU+HL)能够有效地对 NIID 数据进行训练。此外,AGRU、GRU-SVM 的性能都优于 Bi-LSTM 模型,表明改进的循环神经网络能够有效提取上下文信息的深层特征,尤其是关于时间尺度的特征信息。反之,Bi-LSTM 模型时间尺度特征提取能力较弱,因此性能较低。同时,损失函数表明 HL 略优于交叉熵。实验结果验证了所提改进联邦学习方法的有效性和优越训练性能。

3.2.2 通信效率对比实验

本节进行了不同联邦学习框架通信效率对比实验。该实验以通信次数为指标,使用 AGRU+HL 本地训练模型比较了 FedAvg 和 FedNovaka 联邦学习框架在典型通信次数下的分类精度性能。为保证测试的公平性,所有方法实验硬件环境均相同。不同联邦学习框架通信效率对比结果如图 3 所示。可以看出,所提联邦学习框架在相同的通信次数下实现了最佳的分类精度和最快的学习速度。换言之,所提框架需要更少的通信次数即可实现模型收敛。在 KDD CUP 99 测试集上,FedAvg 20 多次通信达到 80%精度,FedNovaka 将近 20 次通信达到 80%精度,与之对比所提框架不到 10 次通信即可达到超过 90%精度。同理,CIC-IDS-2017 数据集下,FedAvg 经过 30 次通信达超过 88%精度,FedNovaka 经过 30 次通信达超过 90%精度,与之对比所提框架 30 次通信时模型已收敛。实验结果证明了所提框架可有效应对多种入侵检测分类,同时通信效果最高。

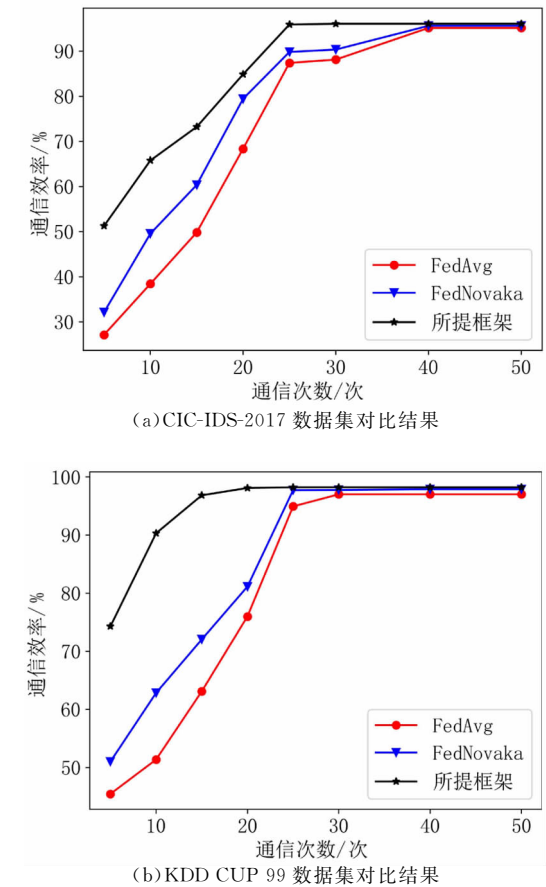


图 3 不同联邦学习框架通信效率对比结果

4 结 论

提出了一种改进的联邦学习框架以应对无线通信网络中的入侵检测。所提框架可基于本地 AGRU+ HL 学习网络数据,基于注意力机制提升模型学习性能并有效减少通信开销。与其他方法相比,所提框架具有更好的精度和效率。所提方法可为无线通信网络入侵检测技术的发展提供一定借鉴作用。

参考文献

[1] 刘晓峻. 自组织远距离无线通信网络虫洞攻击检测方法研究[J]. 数字通信世界, 2023(12): 54—56.

[2] 唐忠杰. 5G 无线通信技术与网络安全研究[J]. 长江信息通信, 2023, 36(12): 197—199.

[3] 刘闯. 5G 无线通信技术与网络安全探析[J]. 中国设备工程, 2023(23): 217—219.

[4] 付仅华, 容有略. 无线通信技术智能化发展研究[J]. 网络安全和信息化, 2023(12): 7—9.

[5] 左娟娟, 陈宇民, 朱红杰, 等. 基于深度置信网络的电力系统网络入侵检测方法[J]. 电子设计工程, 2023, 31(24): 85—89.

[6] 刘拥民, 张钱全, 杨钰津, 等. 新型 GAN 的 WSN 异常检测方法[J]. 计算机工程与设计, 2023, 44(12): 3554—3562.

[7] 张明明, 刘凯, 李贤慧, 等. 基于深度学习的恶意行为检测与识别模型研究[J]. 信息安全研究, 2023, 9(12): 1152—1158.

[8] 彭翰中, 张珠君, 闫理跃, 等. 联盟链下基于联邦学习聚合算法的入侵检测机制优化研究[J]. 信息网络安全, 2023, 23(8): 76—85.

[9] 刘金硕, 詹岱依, 邓娟, 等. 基于深度神经网络和联邦学习的网络入侵检测[J]. 计算机工程, 2023, 49(1): 15—21+30.