光电技术及应用

DOI：10.16818/j.issn1001－5868.2023080902

5G电力虚拟专网中基于联邦对抗学习的分布式异常检测算法

吴维农[1*]，王定国[1]，刘钰然[1]，邓雅文[1]，祖雪莹[1]，唐　伦[2]

（1. 国网重庆市电力公司信息通信分公司，重庆 400014；2. 重庆邮电大学 通信与信息工程学院，重庆 400065）

摘　要： 针对5G电力虚拟专网中高维、不均衡和分布式的数据特征，提出了一种基于联邦对抗学习的分布式异常检测算法。首先，鉴于生成对抗网络在获取高维复杂数据分布方面的优势，采用具有梯度惩罚的Wasserstien生成对抗网络（WGAN-GP）模型对网元中的多维运行数据进行分析和监控并获取其分布情况。其次，基于5G电力虚拟专网的管理架构，设计了一种基于联邦对抗学习的分布式异常检测框架，使分布式电力切片管理器能够协同训练全局异常检测模型，增强模型泛化能力。最后，通过数值仿真验证了基于联邦对抗学习的分布式异常检测算法的训练效率和检测性能。

关键词： 5G电力虚拟专网；电力网络切片；分布式异常检测；联邦对抗学习

中图分类号： TM711　**文章编号：** 1001－5868(2023)06－0955－10

Federated Adversarial Learning Based Distributed Anomaly Detection Algorithm for 5G Power Virtual Private Network

WU Weinong[1], WANG Dingguo[1], LIU Yuran[1], DENG Yawen[1], ZU Xueying[1], TANG Lun[2]

(1. Information and Telecommunication Branch of State Grid Chongqing Electric Power Com. Ltd, Chongqing 400014, CHN; 2. School of Communications and Information Engineering, Chongqing University of Posts and Telecomm., Chongqing 400065, CHN)

Abstract: A federated adversarial learning-based distributed anomaly detection algorithm for the high-dimensional, unbalanced, and locally collected data in 5G power virtual private network. Firstly, considering the powerful ability of generative adversarial network in capturing the distribution from high-dimensional complex data, a Wasserstein generative adversarial network with gradient penalty (WGAN-GP) model was adopted to monitor and analyze the multi-dimensional operational data in the network elements and to capture their data distributions. Secondly, based on the management framework of 5G power virtual private network, a federated adversarial learning-based distributed anomaly detection framework was designed to enable distributed power slice managers to collaboratively train a global anomaly detection model and improve the generalization ability. Finally, numerical simulation results validate the efficiency and effectiveness of the federated adversarial learning-based distributed anomaly detection algorithm.

Key words: 5G power virtual private network; power network slices; distributed anomaly detection; federated adversarial learning

收稿日期：2023－08－09.

基金项目：国家自然科学基金项目(62071078)；国家电网有限公司科技项目(2023渝电科技6#).

* **通信作者：**吴维农　**E-mail:** wuweinong2023@163.com

0 引言

当前常用的基于传统光纤的光传送网、以太网无源光网络、同步数字体系等通信手段难以满足新型电力系统中点多面广、海量设备接入、实时数据交互的通信需求[1]。5G电力虚拟专网的高效性、灵活性及定制化功能可以充分满足新型电力系统中控制类、采集类、应用类业务的差异化需求和隔离性要求。5G电力虚拟专网利用电力系统基础设施中提供定制网络功能的多个网元组成电力网络切片，电力网络切片可在新型电力系统全流程的生产和运营中发挥重要作用[2-3]。然而，随着电力网络切片中网元功能的软件化越来越广泛，保证其安全、稳定运行至关重要。电力切片通常由提供不同功能的网元按顺序连接而成，网元的运行异常会造成切片服务性能下降，违反电力业务的服务等级协议。因此，针对电力切片中网元的异常行为检测是保证5G电力虚拟专网服务性能的首要前提。

为实现对网元设备的异常检测，Yin等[4]通过建立正常流量行为表征模型并根据Grabs准则检测网元设备的流量异常值，形成具有深度防御能力的网元设备综合保护机制。Mishra等[5]提出了一种多级网元安全监控架构，针对不同类别的网元攻击，使用随机森林分类器建立攻击行为模型，作为异常检测基准。Zou等[6]使用优化孤立森林算法对网元设备的多维资源指标数据进行监控和分析，设计出一种在线异常检测方法。然而，5G电力虚拟专网中网元设备的异常检测仍面临三个方面的挑战：(1)5G电力虚拟专网中差异化的业务需求带来了数据类型多样化，数据结构较为复杂，数据分布获取难度高；(2)由于真实网络中异常情况发生的几率较低，且在拥有多样化业务类型的5G电力虚拟专网中，获取充足异常行为数据需要较高的成本，故可以得到的正常数据和异常数据极不均衡；(3)每个网元设备的运行数据在本地进行收集，学习全局异常检测模型需要一个逻辑中心将所有本地数据进行聚合，通信和计算开销较大，难以保证电力切片间的数据隔离。

最近，生成对抗网络(Generative Adversarial Network，GAN)因其在表征高维复杂数据分布方面的突出能力受到了学术界和产业界的广泛关注。考虑到5G电力虚拟专网中高维、不均衡和分布式的数据特征，本文提出了一种基于联邦学习的WGAN-GP模型来表征5G电力虚拟专网中网元设备正常运行数据的分布。作为一种分布式机器学习框架，联邦学习允许分布式智能体基于本地训练数据更新本地模型，且多个分布式智能体可通过周期性参数交互得到全局模型。鉴于联邦学习在隐私保护和通信成本方面的优势，其已被广泛应用到电力系统的入侵检测和负荷预测领域中[7-8]。WGAN-GP模型是GAN模型的一种改进形式，和经典GAN相比，主要存在两点差异：(1)引入Wasserstein-1距离代替GAN中的詹森-香农(JS)散度，从而避免GAN中常出现的梯度消失问题(WGAN[9])；(2)在WGAN模型中引入梯度惩罚用于强制满足其Lipschitz约束，目的是解决其权重剪裁中的优化难题(WGAN-GP[10])。生成对抗网络及其改进形式可用于电力系统中的设备运行状态检测和异常数据检测[11-12]。

基于5G电力虚拟专网的管理架构，本文提出了一种基于联邦对抗学习的分布式异常检测框架。在该框架中，使用WGAN-GP算法获取每个电力切片内网元数据的分布情况。此外，将网络控制器视为全局聚合节点，分布式电力切片管理器基于联邦学习进行协作训练，训练得到的全局检测模型可获取5G电力虚拟专网中所有网元设备的相关数据分布情况。与集中式检测模式相比，本文提出的异常检测框架可在保证电力切片间数据隔离的同时，降低系统通信和计算开销，准确检测出电力系统中存在的异常行为。

1 系统模型

图1给出了5G电力虚拟专网管理架构图，总共包括三层，每一层的具体功能描述如下：

新型电力系统基础设施层：由包括服务器、交换机和网关在内的多种类型的物理节点组成。物理节点可提供定制化网元创建和运行所需的计算、存储和网络资源。由基础设施管理器负责该层的管控和维护。

电力网络切片实例层：电力网络切片用以满足新型电力系统中控制类、采集类、应用类业务的差异化需求和隔离性要求，其中，分布式电力切片管理器负责每个电力切片的独立控制和管理。

业务实例层：该层的主要功能是接收各类电力业务请求，并将其转换为业务实现需要的网络功能。网络控制器通过对整个系统的可用资源和运行状况

的全面监控，统筹电力网络切片的编排和部署任务。

基于图 1 所示的 5G 电力虚拟专网管理架构，本文提出了一种分布式异常检测框架用于对 5G 电力虚拟专网下网元设备的异常行为进行检测。由于网元设备的异常行为通常伴随其运行数据的显著变化，因此，网元设备的异常检测可通过对相关运行数据的收集和分析来实现。本文采用 WGAN-GP 模型作为基本的异常检测方法，该模型由一个生成器和一个判别器组成。电力切片管理器将收集到的切片内网元设备的运行数据存储为本地训练数据集。为了训练全局异常检测模型，需要学习电力系统基础设施中所有网元设备的运行数据，从而构建出一个正常数据分布模型。为了避免集中式数据收集和分析带来的通信和计算成本，本文提出基于联邦对抗学习的分布式异常检测框架。在该框架中，分布式电力切片管理器负责本地 WGAN-GP 模型的训练，网络控制器可视为全局聚合节点，负责聚合在分布式电力切片管理器上训练的本地 WGAN-GP 模型，通过电力切片管理器和网络控制器的分层协作，训练全局异常检测模型。

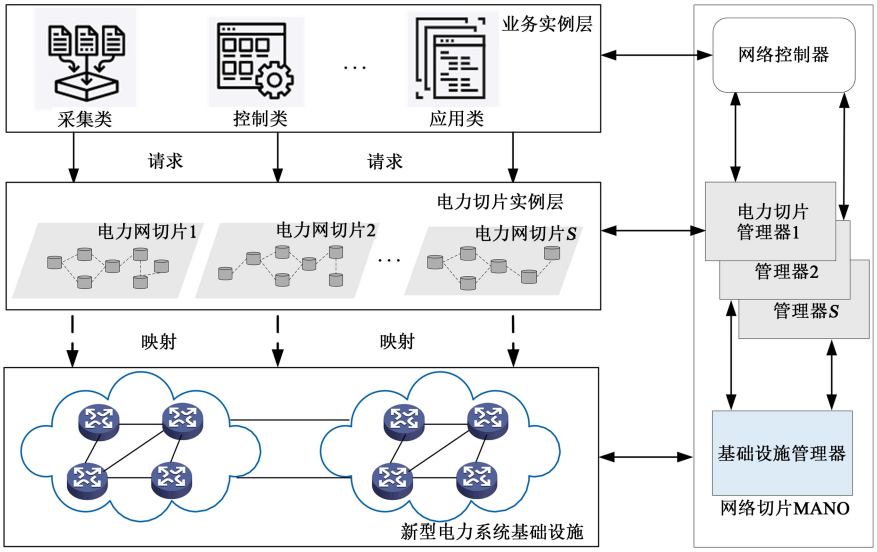


图 1　5G 电力虚拟专网管理架构图

2　基于 WGAN-GP 的异常检测

WGAN-GP 模型是 GAN 模型的一种改进形式，该模型基于分布式电力切片管理器中的本地数据集训练本地异常检测模型。WGAN-GP 模型旨在获取一个电力切片内所有网元设备正常运行数据的分布情况。

2.1　GAN 模型

GAN 包括生成器 G 和判别器 D 这两个基本模型[13]。给定由真实数据组成的训练数据集 $\{\boldsymbol{X}^{\mathrm{r}}\}_{r=1}^{N_{\mathrm{td}}}$，$G$ 将从先验分布 P_z 中提取的随机噪声 z 生成为虚假数据 $\bar{\boldsymbol{X}}$（即 $\bar{\boldsymbol{X}}=G(z)$），将从训练数据集中采样的真实数据 $\boldsymbol{X}$ 和虚假数据 D 同时输入 D 中，G 和 D 通过对抗学习使得 D 难以区分真实数据 $\boldsymbol{X}$ 和 G 生成的虚假数据 $\bar{\boldsymbol{X}}$。定义 P_X 和 $P_{\bar{X}}$ 分别为真实数据分布和虚假数据分布，$D(\boldsymbol{X})$ 表示 $\boldsymbol{X}$ 服从真实数据分布的概率，则 GAN 的优化目标如下式所示[13]：

$$\min_G \max_D V(G,D)=E_{\boldsymbol{X}\sim P_{\boldsymbol{X}}}[\log(D(\boldsymbol{X}))]+E_{z\sim P_z}\cdot[\log(1-D(G(z)))]=E_{\boldsymbol{X}\sim P_{\boldsymbol{X}}}[\log(D(\boldsymbol{X}))]+E_{\bar{\boldsymbol{X}}\sim P_{\bar{\boldsymbol{X}}}}[\log(1-D(G(\bar{\boldsymbol{X}})))] \tag{1}$$

GAN 模型的训练通过交替更新生成器 G 和判别器 D 完成。G 的训练过程是使虚假数据分布 $P_{\bar{\boldsymbol{X}}}$ 逐渐逼近真实数据分布 $P_{\boldsymbol{X}}$，直至 D 无法区分 $\boldsymbol{X}$ 和 $\bar{\boldsymbol{X}}$。在 GAN 中，逼近过程通过最小化 $P_{\boldsymbol{X}}$ 和 $P_{\bar{\boldsymbol{X}}}$ 之间的 JS 散度完成，即：

$$\min_G V(G)=2D_{\mathrm{JS}}(P_{\boldsymbol{X}}\,\|\,P_{\bar{\boldsymbol{X}}})-\log 4 \tag{2}$$

其中，$D_{\mathrm{JS}}(\cdot\,\|\,\cdot)$ 表示 JS 散度。当 GAN 模型收敛时，$P_{\boldsymbol{X}}=P_{\bar{\boldsymbol{X}}}$ 得到满足，此时生成器可得到真实数据分布情况。

2.2　WGAN-GP 模型

在 GAN 训练的初始阶段，分布 $P_{\boldsymbol{X}}$ 和 $P_{\bar{\boldsymbol{X}}}$ 之间很小的重叠都可能导致它们之间的 JS 散度成为常数，从而带来梯度消失的问题，训练过程被迫中止[9]。为了克服这个难题，WGAN 选择用

Wasserstein-1 距离取代 JS 散度，分布 $P_{\boldsymbol{X}}$ 和 $P_{\bar{\boldsymbol{X}}}$ 之间的 Wasserstein-1 距离如下式所示：

$$W_1(P_{\boldsymbol{X}} \| P_{\bar{\boldsymbol{X}}}) = \sup_{f \in L_1} \left\{ E_{\boldsymbol{X} \sim P_{\boldsymbol{X}}}[f(\boldsymbol{X})] - E_{\bar{\boldsymbol{X}} \sim P_{\bar{\boldsymbol{X}}}}[f(\bar{\boldsymbol{X}})] \right\} \tag{3}$$

其中，L_1 为 1-Lipschitz 函数集合。然而，WGAN 限制了判别器 D 必须为 1-Lipschitz 函数。通常情况下，WGAN 使用权重剪裁来满足判别器模型的 Lipschitz 约束[9]。但由于权重裁剪在优化过程中存在一定困难，文献[10]提出具有梯度惩罚的 WGAN-GP 模型强制满足 Lipschitz 约束，简化优化过程。在 WGAN-GP 模型中，将函数 $f \in L_1$ 近似为判别器 D 的梯度惩罚范数。此时，WGAN-GP 模型中判别器 D 的训练目标如下：

$$\max_D V(D) = E_{\boldsymbol{X} \sim P_{\boldsymbol{X}}}[D(\boldsymbol{X})] - E_{\bar{\boldsymbol{X}} \sim P_{\bar{\boldsymbol{X}}}}[D(\bar{\boldsymbol{X}})] + \eta E_{\hat{\boldsymbol{X}} \sim P_{\hat{\boldsymbol{X}}}}[(\| \nabla_{\hat{X}} D(\hat{\boldsymbol{X}}) \|_2 - 1)^2] \tag{4}$$

其中，η 是梯度惩罚的系数，$P_{\hat{\boldsymbol{X}}}$ 表示的含义为：从分布 $P_{\boldsymbol{X}}$ 和 $P_{\bar{\boldsymbol{X}}}$ 中随机各取一点连成一条线段，从这条线段上通过均匀采样得到数据 $\hat{X}$。因此，$\hat{X}$ 可表示成和的加权 $\boldsymbol{X}$ 和 $\bar{\boldsymbol{X}}$：即 $\hat{X} = \varepsilon \boldsymbol{X} + (1-\varepsilon)\bar{\boldsymbol{X}}$，其中权重 $\varepsilon \in U[0,1]$ 值。在 WGAN-GP 模型中，基于下式对生成器 G 进行训练：

$$\min_G V(G) = -E_{\bar{\boldsymbol{X}} \sim P_{\bar{\boldsymbol{X}}}}[D(\bar{\boldsymbol{X}})] = -E_{z \sim P_z}[D(G(\boldsymbol{z}))] \tag{5}$$

电力网络切片内本地 WGAN-GP 模型的基本工作原理如图 2 所示。

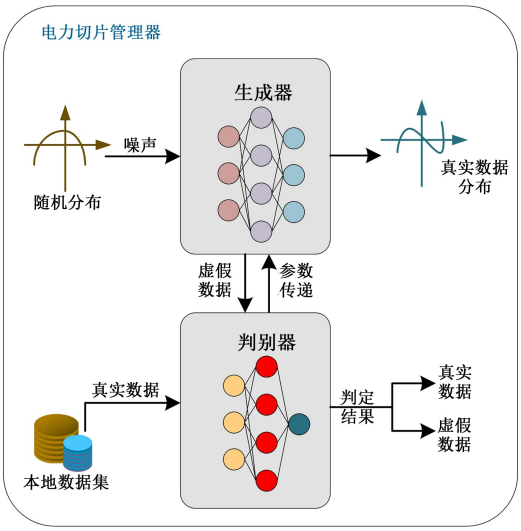


图 2 WGAN-GP 模型原理图

2.3 异常检测模型训练

因电力切片管理器内收集的网元设备运行数据通常是时间序列数据，因此本文利用长短期记忆网络(Long Short-Term Memory Network，LSTM)作为生成器的基本模型，LSTM 是循环神经网络的一种，在与时间相关的学习任务上具有突出表现[14]。假设$[\boldsymbol{y}_1, \cdots, \boldsymbol{y}_t]$是 LSTM 的输入数据，则在每个时间周期 $\tau = 1, \cdots, t$ 上，LSTM 模型包含的基本运算过程如下：

$$\begin{aligned}
\boldsymbol{i}_\tau &= \sigma(\boldsymbol{w}_i \cdot [\boldsymbol{y}_\tau, \boldsymbol{h}_{\tau-1}, \boldsymbol{c}_{\tau-1}] + \boldsymbol{b}_i) \\
\boldsymbol{f}_\tau &= \sigma(\boldsymbol{w}_f \cdot [\boldsymbol{y}_\tau, \boldsymbol{h}_{\tau-1}, \boldsymbol{c}_{\tau-1}] + \boldsymbol{b}_f) \\
\boldsymbol{c}_\tau &= \boldsymbol{f}_\tau \odot \boldsymbol{c}_{\tau-1} + \boldsymbol{i}_\tau \odot \tanh(\boldsymbol{w}_z \cdot [\boldsymbol{y}_\tau, \boldsymbol{h}_{\tau-1}] + \boldsymbol{b}_z) \\
\boldsymbol{o}_\tau &= \sigma(\boldsymbol{w}_o [\boldsymbol{y}_\tau, \boldsymbol{h}_{\tau-1}, \boldsymbol{c}_\tau] + \boldsymbol{b}_o) \\
\boldsymbol{h}_\tau &= \boldsymbol{o}_\tau \odot \tanh(\boldsymbol{c}_\tau)
\end{aligned} \tag{6}$$

其中，$\boldsymbol{i}_\tau$，$\boldsymbol{f}_\tau$ 和 $\boldsymbol{o}_\tau$ 分别为输入门，遗忘门和输出门。$\boldsymbol{c}_\tau$ 表示记忆单元，$\boldsymbol{h}_\tau$ 表示隐藏状态。$\boldsymbol{w}_*$ 和 $\boldsymbol{b}_*$ 分别为 LSTM 模型中包含的权重和偏置矢量。符号 $\sigma(\cdot)$表示 sigmoid 函数，$\odot$表示同位元素对应相乘运算。隐藏状态 $\boldsymbol{h}_\tau$ 可看作为输入$[\boldsymbol{y}_1, \cdots, \boldsymbol{y}_t]$的综合表征，即：

$$\boldsymbol{h}_t = \Gamma_r([\boldsymbol{y}_1, \cdots, \boldsymbol{y}_t]; [\boldsymbol{w}, \boldsymbol{b}]) \tag{7}$$

其中，$\Gamma_r(\cdot; [\boldsymbol{w}, \boldsymbol{b}])$ 表示由 LSTM 模型定义的映射函数。

构建生成器 G：将生成器 G 构建为由两个 LSTM 层和一个线性全连接层组成的三层模型。在电力切片管理器中，从先验分布 P_z 中提取随机噪声 z 后，通过 G 生成虚假数据 $\bar{\boldsymbol{X}}$：

$$\bar{\boldsymbol{X}} = G(z; [\boldsymbol{w}_G, \boldsymbol{b}_G]) \tag{8}$$

其中，$\boldsymbol{w}_G$ 和 $\boldsymbol{b}_G$ 分别是生成器 G 中模型参数 θ_G 的权重和偏置矢量。

构建判别器 D：将判别器 D 构建为由三个全连接层组成的神经网络模型，为了得到范围在(0,1)之间的概率值，D 的最后一层使用 sigmoid 激活函数。判别器 D 将其输入数据 $\boldsymbol{X}$ 和 $\bar{\boldsymbol{X}}$ 映射为一个标量 d：

$$d = D\{(\boldsymbol{X}, \bar{\boldsymbol{X}}); \boldsymbol{w}_D, \boldsymbol{b}_D\} \tag{9}$$

其中，$\boldsymbol{w}_{D_n}$ 和 $\boldsymbol{b}_{D_n}$ 分别是判别器 D 中模型参数 θ_D 的权重和偏置矢量。

WGAN-GP 模型的训练在电力切片管理器中执行，通过生成器 G 和判别器 D 之间的对抗学习完成，训练包括多个迭代周期，每个迭代周期中生成器 G 和判别器 D 的更新过程如下：

判别器 D 的更新：每次迭代中，基于从本地数据集中提取的一批次真实数据 $\boldsymbol{X}$ 和生成器生成的虚假数据 $\bar{\boldsymbol{X}}$，对判别器 D 进行 K 次训练，其中批数据大小为 M。在第 k 次训练过程中，对 $\boldsymbol{X}$ 和 $\bar{\boldsymbol{X}}$ 中

的每一条批数据 $\boldsymbol{X}^m$ 和 $\bar{\boldsymbol{X}}^m$ 来说，D 的损失函数可通过下式计算得到：

$$L_D^m = -\{D(\boldsymbol{X}^m) - D(\bar{\boldsymbol{X}}^m) + \eta[(\|\nabla_{\hat{\boldsymbol{X}}^m} D(\hat{\boldsymbol{X}}^m)\|_2 - 1]^2\} \tag{10}$$

因此，可得到 D 的参数梯度 $\nabla\theta_{\mathrm{D}}$ 为：

$$\nabla\theta_{\mathrm{D}} = \frac{1}{M}\sum_{m=1}^{M}\frac{\partial L_{\mathrm{D}}^m}{\partial\theta_{\mathrm{D}}} \tag{11}$$

之后，使用 Adam 优化器对判别器 D 的参数 θ_{D} 进行更新：

$$\theta_{\mathrm{D}} \leftarrow \mathrm{Adam}(\nabla_{\theta_{\mathrm{D}}}, \theta_{\mathrm{D}}, \alpha, \beta_1, \beta_2) \tag{12}$$

其中，α，β_1 和 β_2 是组成 Adam 优化器的超参数。

生成器 G 的更新：每次迭代中，生成器 G 将从先验分布 P_z 中采样的一批次随机噪声 z 生成为一批次虚假数据 $\bar{\boldsymbol{X}}$，对 $\bar{\boldsymbol{X}}$ 中的每一条批数据 $\bar{\boldsymbol{X}}^m$ 来说，G 的损失函数通过下式进行计算：

$$L_{\mathrm{G}}^m = -[D(\boldsymbol{X}^m)] \tag{13}$$

因此，可得到 G 的参数梯度 $\nabla\theta_{\mathrm{G}}$ 为：

$$\nabla\theta_{\mathrm{G}} = \frac{1}{M}\sum_{m=1}^{M}\frac{\partial L_{\mathrm{G}}^m}{\partial\theta_{\mathrm{G}}} \tag{14}$$

同样地，使用 Adam 优化器对生成器 G 的参数 θ_{G} 进行更新：

$$\theta_{\mathrm{G}} \leftarrow \mathrm{Adam}(\nabla_{\theta_{\mathrm{D}}}, \theta_{\mathrm{D}}, \alpha, \beta_1, \beta_2) \tag{15}$$

WGAN-GP 算法的伪代码如算法 1 所示。

算法 1　WGAN-GP 算法

超参数：批数据大小 M，两次生成器更新之间判别器的迭代次数 K，先验分布 P_z，加权系数 ε，Adam 超参数 α，β_1，β_2，惩罚系数 η，总训练迭代次数 I

输入：初始化模型参数 θ_{G}，θ_{D}；训练数据集 $\{\boldsymbol{X}^{\mathrm{r}}\}_{r=1}^{N_{\mathrm{td}}}$
输出：训练后的模型参数 θ_{G}，θ_{D}

1. for $i = 1 : I$ do
2. 从本地训练数据集 $\{\boldsymbol{X}^{\mathrm{r}}\}_{r=1}^{N_{\mathrm{td}}}$ 中采样一批次真实数据 $\boldsymbol{X}$
3. 从先验分布 P_z 中采样一批次随机噪声 z，并通过生成器得到一批次虚假数据 $\bar{\boldsymbol{X}}$
4. for $k = 1 : K$ for do
5. for $m = 1 : M$ for do
6. 计算 $\boldsymbol{X}$ 和 $\bar{\boldsymbol{X}}$ 的加权平均：$\hat{\boldsymbol{X}}^m = \varepsilon\boldsymbol{X}^m + (1-\varepsilon)\bar{\boldsymbol{X}}^m$
7. 根据公式(10)计算判别器的损失函数 $L_{\mathrm{D}}^{\mathrm{m}}$
8. end for
9. 基于公式(11)和(12)分别更新判别器的参数梯度 $\nabla\theta_{\mathrm{D}}$ 和模型参数 θ_{D}
10. end for
11. for $m = 1 : M$ do
12. 根据公式(13)计算生成器的损失函数 L_{G}^m
13. end for
14. 基于公式(14)和(15)分别更新生成器的参数梯度 $\nabla\theta_{\mathrm{G}}$ 和模型参数 θ_{G}
15. end for

3　基于联邦对抗学习的分布式异常检测框架

WGAN-GP 模型适用于单个电力网络切片内网元设备的监督和管理。为了将其扩展到整个 5G 电力虚拟专网中，本文引入联邦学习，让分布式电力切片管理器通过协同训练得到全局异常检测模型，在提高模型泛化能力的同时降低通信和计算成本。在如图 3 所示的基于联邦对抗学习的分布式异常检测框架中，网络控制器负责初始化 WGAN-GP 全局模型，并将全局模型下发到电力切片管理器中。在本地进行一定周期的训练后，电力切片管理器将本地 WGAN-GP 模型上传到网络控制器中进行全局模型平均，从而得到具有较强泛化能力的异常检测模型。

3.1　训练

基于联邦学习的 WGAN-GP 算法在电力切片管理器和网络控制器中的训练过程如下：

电力切片管理器：每个电力切片管理器内包含一个本地 WGAN-GP 模型，由本地生成器 $G_s(s\in S)$ 和判别器 $D_s(s\in S)$ 模型组成，其中 S 表示电力切片集合及其个数。电力切片管理器首先接收从网络控制器下发的初始化全局模型 G^{global} 和 D^{global}，并基于全局模型对本地模型进行初始化。在一个电力切片管理器 s 中，判别器和生成器每隔 K 个训练周期进行数据和参数交互。经过 L 次本地训练后，电力切片管理器将模型参数 θ_{G_s} 和 θ_{D_s} 上传到网络控制器中进行全局聚合。在网络控制器中进行模型平均后，电力切片管理器将接收新的全局模型 G^{global} 和 D^{global} 作为本地模型继续训练，同时基于全局模型参数 $\theta_G^{\mathrm{global}}$ 和 $\theta_D^{\mathrm{global}}$，利用 Adam 优化器对本地模型 $G_s(s\in S)$ 和 $D_s(s\in S)$ 进行更新：

$$\begin{aligned}\theta_{G_s} &\leftarrow \mathrm{Adam}(\nabla\theta_{G_s}, \theta_G^{\mathrm{global}}, \alpha, \beta_1, \beta_2), \forall s \in S\\ \theta_{D_s} &\leftarrow \mathrm{Adam}(\nabla\theta_{D_s}, \theta_D^{\mathrm{global}}, \alpha, \beta_1, \beta_2), \forall s \in S\end{aligned} \tag{16}$$

网络控制器：网络控制器负责本地 WGAN-GP 模型的全局聚合。网络控制器执行 2 个重要步骤：(1) 初始化全局模型并将其发送到电力切片管理器中；(2) 聚合电力切片管理器上传的所有模型参数，平均后将新的全局模型下发到电力切片管理器中。网络控制器基于 FedAVG[15] 算法进行模型平均，在接收到所有电力切片管理器上传的生成器模型参数 $\theta_{G_s}(s\in S)$ 和判别器模型参数 $\theta_{D_s}(s\in S)$ 后，网络控制器通过下式更新全局模型：

$$\theta_{\mathrm{G}}^{\mathrm{global}} = \frac{\sum_{s=1}^{S} Q_s\theta_{G_s}}{Q}, \theta_{\mathrm{D}}^{\mathrm{global}} = \frac{\sum_{s=1}^{S} Q_s\theta_{D_s}}{Q} \tag{17}$$

其中，Q_s 表示切片 s 中的训练数据量，$Q=\sum_{s=1}^{S}Q_s$ 为电力系统中的训练数据总量。全局模型 G^{global} 和 D^{global} 更新完成后，网络控制器会将 G^{global} 和 D^{global} 下发到电力切片管理器中。

反复执行以上步骤，直到全局模型收敛为止。

3.2 检测

训练完成后，将全局模型发送到每个电力切片管理器中用于网元设备的异常检测。为了衡量网元设备中新的运行数据 $\boldsymbol{X}$ 的异常与否，本文定义了异常分数 $A(\boldsymbol{X})$[16]，$A(\boldsymbol{X})$是重建误差 L_{G} 和判别误差 L_{D} 的加权和，具体通过下式计算得到：

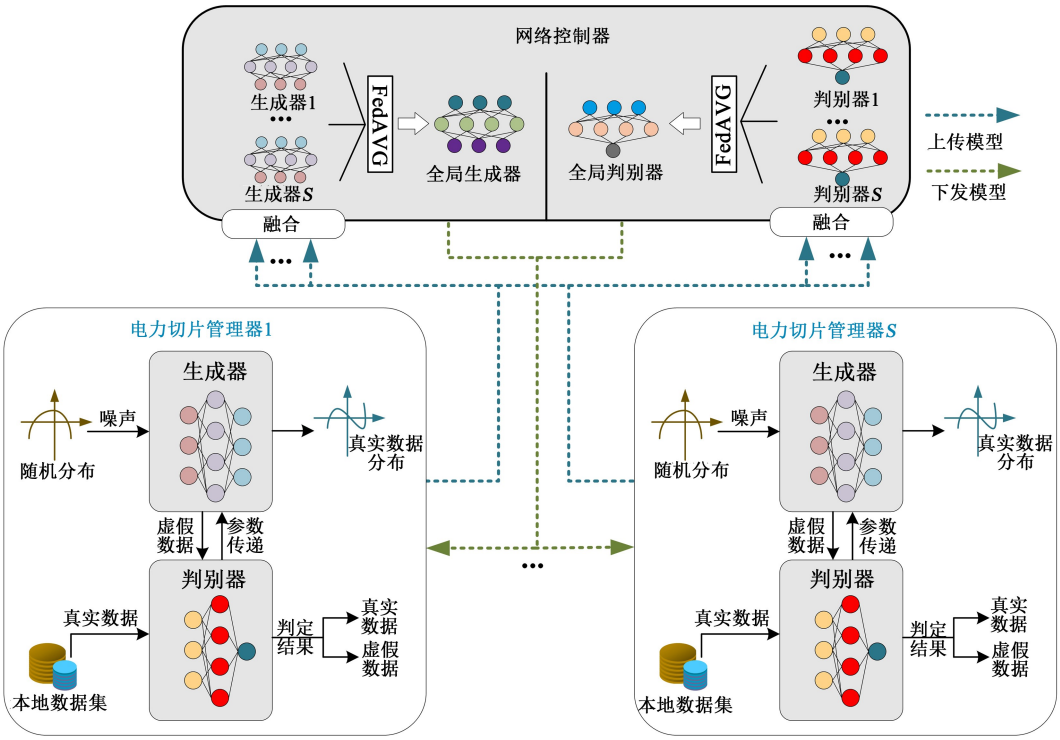


图 3 基于联邦对抗学习的分布式异常检测框架

$$A(\boldsymbol{X})=\alpha L_{\text{G}}(\boldsymbol{X})+(1-\alpha)L_{\text{D}}(\boldsymbol{X}) \tag{18}$$

其中，α 表示权重系数，$L_{\text{G}}(\boldsymbol{X})=\|\boldsymbol{X}-G(z)\|_1$ 是重建误差，$L_{\text{D}}(\boldsymbol{X})=\sigma(D(\boldsymbol{X}),1)$ 是判别器误差。在 $L_{\text{D}}(\boldsymbol{X})$中，$\sigma$ 是 sigmoid 交叉熵，$L_{\text{D}}(\boldsymbol{X})$表示新的运行数据 $\boldsymbol{X}$ 被判定为正常数据的判别误差，即 $\boldsymbol{X}$ 服从真实数据分布的置信度。对网元设备新的运行数据 $\boldsymbol{X}$ 来说，电力切片管理器基于接收到的全局生成器和判别器计算其异常分数 $A(\boldsymbol{X})$。若 $A(\boldsymbol{X})$大于异常判定门限值 threshold，$\boldsymbol{X}$ 会被认定为异常运行数据。

基于联邦对抗学习的分布式异常检测框架的伪代码如算法 2 所示。

4 数值仿真

在本节中，我们通过数值仿真对基于联邦学习的 WGAN-GP 算法在训练效率和检测效率方面的性能进行了广泛评估，同时将其和 GAN 算法[13]、WGAN 算法[9]、BiGAN 算法[17]、集中式 WGAN-GP 算法、独立式 WGAN-GP 算法进行了对比。

算法 2 基于联邦对抗学习的分布式异常检测框架

超参数：批数据大小 M，两次生成器更新之间判别器的迭代次数 K，先验分布 P_z，加权系数 ε，Adam 超参数 α,β_1,β_2，惩罚系数 η，训练迭代总次数 I，两次聚合间的迭代次数 L，异常分数门限值 threshold

输入：生成器和判别器的初始化模型参数 $\theta_{\text{G}}^{\text{global}}$ 和 $\theta_{\text{D}}^{\text{global}}$，所有电力切片下 $s\in S$ 的分布式训练数据集 $\cup_{s=1}^{S}\{\boldsymbol{X}_s^{\text{r}}\}_{r=1}^{N_{\text{td}}}$，新运行数据 $\boldsymbol{X}$

输出：训练后的模型参数 $\theta_{\text{G}}^{\text{global}}$ 和 $\theta_{\text{D}}^{\text{global}}$，新运行数据 $\boldsymbol{X}$ 的异常情况

1. for $i=1:I$ do
▷训练过程
2. ▷对于每个电力切片 $s\in S$，在电力切片管理器中更新本地 WGAN-GP 模型
3. 接收网络控制器下发的初始化全局参数 $\theta_{\text{G}}^{\text{global}}$ 和 $\theta_{\text{D}}^{\text{global}}$ 对本地参数 θ_{G_s} 和 θ_{D_s} 进行初始化
4. 执行算法 1 中的步骤(1)～(15)
5. if $i \bmod L == 0$ then
6. 将本地参数 θ_{G_s} 和 θ_{D_s} 上传到网络控制器中进行全局参数平均
7. end if
8. ▷在网络控制器中更新全局模型 G^{global} 和 D^{global}
9. 对全局模型参数 $\theta_{\text{G}}^{\text{global}}$ 和 $\theta_{\text{D}}^{\text{global}}$ 进行初始化，并下发到所有的电力切片管理器中

10. 每隔 L 个本地训练周期，接收从电力切片管理器 s 中上传的模型参数 θ_{G_s} 和 θ_{D_s}，并基于公式(17)更新全局模型参数 $\theta_{\mathrm{G}}^{\mathrm{global}}$ 和 $\theta_{\mathrm{D}}^{\mathrm{global}}$
11. end for
▷检测过程
12. 对网元设备的新运行数据 $\boldsymbol{X}$，基于相应的生成器 G 和判别器 D，基于公式(18)计算其异常分数 $A(\boldsymbol{X})$
13. if $A(\boldsymbol{X}) > threshold$ then
14. $\boldsymbol{X}$ 为异常数据，判定对应网元设备的运行出现异常
15. else
16. $\boldsymbol{X}$ 为正常数据，判定对应网元设备的运行一切正常
17. end if

4.1　实验建立

本文基于 Python3.6 语言和 Pytorch 工具包实现了集中式、独立式和分布式这三种异常检测框架。在具体实施过程中，我们模拟了 1 个网络控制器和 3 个电力切片管理器进程，并利用 socket 实现它们之间的信息交换[18]。

(1)数据集：本文利用虚拟 IP 多媒体系统[* VNFDataset: virtual IP Multimedia IP system, https://www.kaggle.com/imenbenyahia/clearwatervnf-virtual-ip-multimedia-ip-system] 的 VNFDataset 数据集对算法性能进行仿真评估。VNFDataset 数据集包含 6 个数据子集，每个数据子集对应一个网元设备的 17 万条运行数据记录，每条记录包含 26 个数据特征，主要由 CPU、磁盘、存储器和网络相关特征组成。在仿真评估中，每个子集被划分为三个不相交的数据集，包括训练数据集、验证数据集和测试数据集。

(2)评估指标：为了评估所提算法和对比算法的性能，本文选用以下评估指标作为衡量标准：1)训练效率：包括训练过程中电力切片管理器和网络控制器的通信、计算和内存成本；2)检测性能：包括最常用的三个异常检测指标，召回率(Recall)，精确率(Precision)和 F1-socre。这三种指标的计算基于几个基本定义：假阴率(False Negative，FN)，表示被错误识别为正常数据的异常数据量；假阳率(False Positive，FP)，表示被错误识别为异常数据的正常数据量；真阳率(True Positive，TP)，表示正确识别的异常数据量。Recall 表示正确预测的异常数据在总异常数据中所占比列，定义为：

$$Recall = \frac{TP}{TP + FN} \tag{19}$$

Precision 表示正确预测的异常数据在所有被判定为异常的数据中所占比例，定义为：

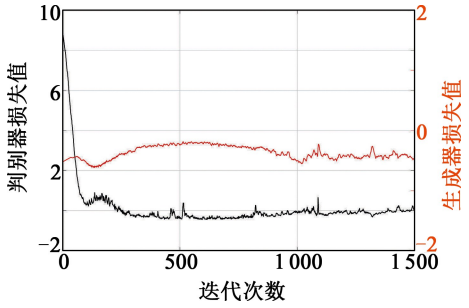
$$Precision = \frac{TP}{TP + FP} \tag{20}$$

F1-score 为 Recall 和 Precision 的加权平均，定义为：

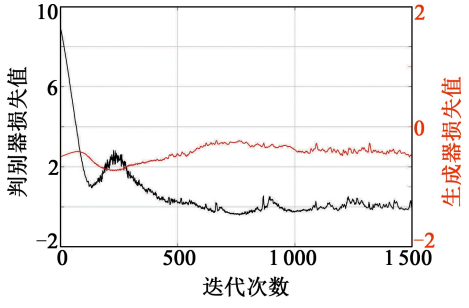
$$F1\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{21}$$

4.2　训练效率

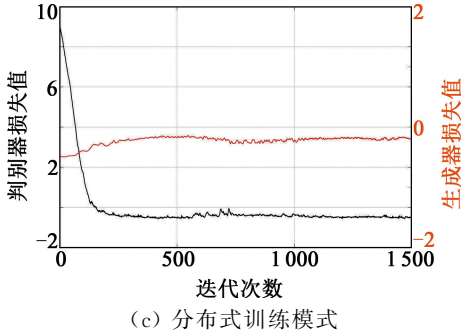
为了验证 WGAN-GP 算法在集中式、独立式和分布式训练模式下的收敛性，图 4 给出了每种模式训练过程中判别器损失和生成器损失值的收敛过程。在集中式训练模式下，网络控制器收集所有电力切片管理器中的网元设备运行数据，用于训练集中式 WGAN-GP 模型。在独立式训练模式下，WGAN-GP 模型在电力切片管理器中进行训练，独立式训练模式中不存在任何数据或参数交换过程。分布式训练模式使用算法 2 中给出的基于联邦学习的 WGAN-GP 算法，其中电力切片管理器负责本地 WGAN-GP 模型的训练，网络控制器负责本地模型的全局聚合。图 4(a)、(b)、(c)分别为集中式 WGAN-GP、独立式 WGAN-GP和分布式 WGAN-



(a) 集中式训练模式



(b) 独立式训练模式

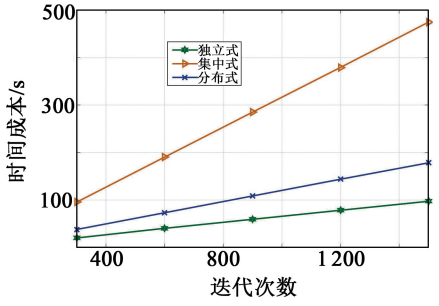


(c) 分布式训练模式

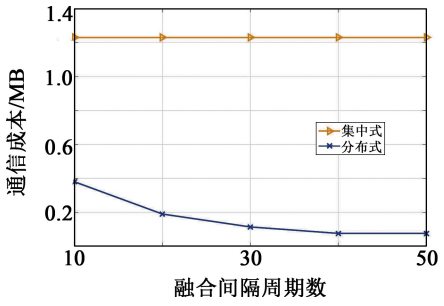
图 4　不同训练模式下判别器和生成器的收敛过程

GP 算法的训练过程。观察图 4 可知，经过多个训练周期后，三种训练模式下的判别器和生成器损失均可成功收敛至稳定值。对比三种训练模式的收敛曲线可知，由于本文提出的分布式训练模式的协作特性，其对应的 WGAN-GP 模型的收敛性能最佳。

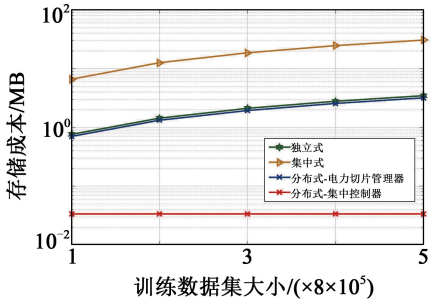
图 5(a)为上述三种训练模式所需的时间成本。因在集中式训练模式中，网络控制器需要收集所有电力切片管理器中的运行数据用于全局模型训练，所以集中式训练模式消耗的训练时间最长。因在独立式训练模式中，每个电力切片管理器仅基于本地数据训练独立的 WGAN-GP 模型，所以独立式训练模式所需的训练时间最短。此外，分布式训练模式的训练效率高于集中式训练模式，但消耗的训练时间略长于独立式训练模式。



(a) 计算成本



(b) 电力切片管理器和网络控制器间的通信成本



(c) 内存成本

图 5 不同训练模式的效率对比

在独立式训练模式下，电力切片管理器和网络控制器间不存在任何通信过程。图 5(b)为集中式和分布式训练模式下，电力切片管理器和网络控制器之间的通信成本对比结果。因本文提出的分布式训练模式将 WGAN-GP 模型的训练留在本地，故和集中训练模式相比，在本文提出的分布式训练模式下，电力切片管理器和网络控制器间的通信成本较低，且其值会随着全局聚合前本地训练次数的增加而降低。

图 5(c)比较了不同训练数据集规模下三种训练模式所需内存成本的变化情况。由图 5(c)可知，在基于联邦学习的分布式训练模式下，网络控制器所需的内存成本远小于集中式训练模式。此外，本文提出的分布式训练模式在电力切片管理器上的内存成本也略低于独立式训练模式。

由图 6 可知，不同 *threshold* 值对应不同的检测性能。因此，本文利用验证数据集计算有效的 *threshold* 值。首先，通过将四种故障类型随机插入验证数据集，包括 CPU 无限循环、内存溢出、磁盘 I/O 故障和网络拥塞，在验证数据集中模拟运行数据的异常情况[19]。然后，计算验证数据集中正常和异常运行数据的平均异常分数 A_{normal} 和 A_{abnormal}，从而定义 *threshold* 为$(A_{\text{normal}}+A_{\text{abnormal}})/2$。

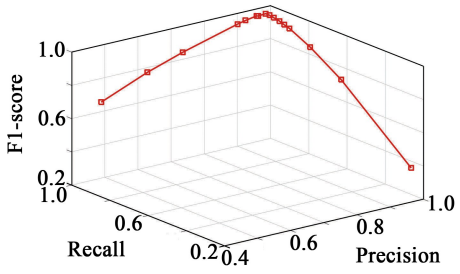


图 6 precision，recall 和 F1-score 关系图

WGAN-GP 算法是本文使用的基本异常检测算法。为了验证 WGAN-GP 算法的检测性能，将其和其他几种 GAN 算法进行了检测性能对比。为了模拟运行数据的异常情况，将上述四种故障类型随机插入测试数据集。图 7 呈现了 WGAN-GP，GAN，WGAN 和 BiGAN 四种算法的异常检测结果。为了便于比较，在这次仿真中，四种算法采用相同的独立式训练模式获取异常检测模型。由图 7 可知，WGAN-GP 算法的综合检测性能最优，与 GAN，WGAN 和 BiGAN 算法相比，WGAN-GP 算法的平均检测性能(F1-score)分别提高了 2.6%，0.5%和 0.2%。

图 8 为集中式 WGAN-GP 算法、独立式 WGAN-GP 算法和基于联邦学习的 WGAN-GP 算

法的检测性能对比结果。评价指标包括 Precision，Recall 和 F1-socre。由图可知，在经过大约 300 个训练周期后，三种算法的三项性能指标值均收敛到稳定值。这表明三种算法在经过大约 300 次训练后，可成功获取运行数据的分布情况，这和图 4 中判别器和生成器损失值的收敛过程基本一致。由图 8 可知，基于联邦学习的 WGAN-GP 算法取得的检测性能优于独立式 WGAN-GP 算法，而略逊于集中式 WGAN-GP 算法。此外，根据 Precision，Recall 和 F1-socre 的收敛曲线可知，由于基于联邦学习的 WGAN-GP 算法较强的泛化能力，其检测性能比独立式 WGAN-GP 算法更稳定。

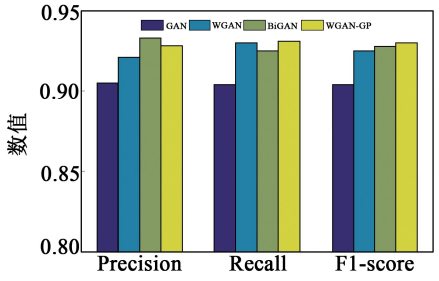
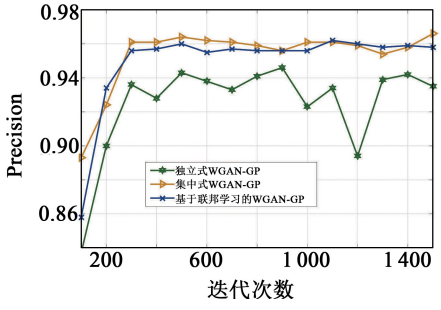
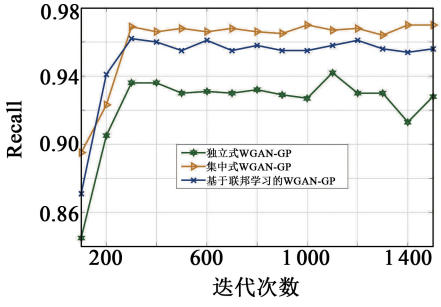


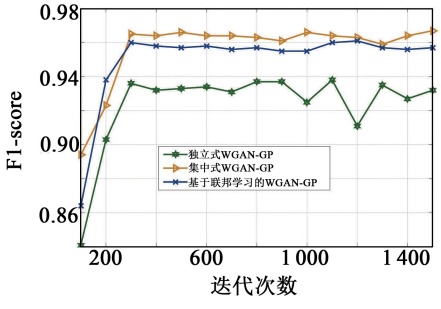
图 7　独立训练模式下四种 GAN 算法的检测性能比较



(a) Precision



(b) Recall



(c) F1-score

图 8　三种算法的检测性能对比图

5　结论

在 5G 电力虚拟专网中，有效检测和分析网元设备中的异常情况对电力网络切片的性能保证来说至关重要。基于 5G 电力虚拟专网的管理架构，本文利用 WGAN-GP 算法对网元设备的多维运行数据进行监控和分析，并基于该算法提出了一种基于联邦对抗学习的分布式异常检测框架。WGAN-GP 算法在电力切片管理器内使用本地数据集进行本地模型训练。此外，基于联邦学习框架，本地 WGAN-GP 模型会上传到网络控制器中进行全局聚合。本文使用 LSTM 作为生成器的基本模型以适应网元设备运行数据的时间序列特性。本文提出的基于联邦学习的 WGAN-GP 算法能够协同训练全局异常检测模型，且该模型具有较强的泛化能力。数值仿真结果表明，本文提出的基于联邦对抗学习的异常检测方法可以较低的通信和计算成本准确检测 5G 电力虚拟专网中存在的异常行为。

参考文献：

[1] 郁海彬，董　烨，翁锦德，等. 电力 5G 切片在城市配电网中的应用及经济效益研究[J/OL]. 综合智慧能源：1-9[2023-07-10]. http://kns.cnki.net/kcms/detail/41.1461.TK.20230504.1145.006.html.
Yu Haibin, Dong Ye, Weng Jinde, et al. Research on the application and economic benefits of 5G slice in the urban distribution network[J/OL]. Integrated Intelligent Energy, 2023: 1-9[2023-07-10]. http://kns.cnki.net/kcms/detail/41.1461.TK.20230504.1145.006.html.

[2] 王　荣，张剑寅，宋　月，等. 5G 电力虚拟专网架构及关键技术研究[J]. 电信科学，2022，38(S1)：240-249.
Wang Rong, Zhang Jianyin, Song Yue, et al. Architecture and key technologies of 5G power private network[J]. Telecommunications Science, 2022, 38(S1): 240-249.

[3] 瞿水华，郭钊杰，许乐飞. 5G 技术在智能电网中的实践和验证[J]. 供用电，2021，38(5)：1-9，34.
Qu Shuihua, Guo Zhaojie, Xu Lefei. Practice and verification of 5G technology in smart grid[J]. Distribution & Utilization, 2021, 38(5): 2-9, 34.

[4] Yin X, Chen X, Chen L, et al. Research of security as a service for VMs in IaaS platform[J]. IEEE Access, 2018, 6: 29158-29172.

[5] Mishra P, Varadharajan V, Pilli E, et al. VMGuard: A VMI-based security architecture for intrusion detection in cloud

environment[J]. IEEE Trans. on Cloud Computing, 2020, 8(3): 957-971.

[6] Zou Z, Xie Y, Huang K, et al. A docker container anomaly monitoring system based on optimized isolation forest[J]. IEEE Trans. on Cloud Computing, 2022, 10(1): 134-145.

[7] 刘长杰，石润华. 基于安全高效联邦学习的智能电网入侵检测模型[J]. 信息网络安全，2023，23(4)：90-101.
Liu Changjie, Shi Runhua. A smart grid intrusion delection model for secure and efficient federated leaving[J]. Netinfo Security, 2023, 23(4): 90-101.

[8] 车 亮，徐茂盛，崔秋实. 基于联邦学习的短期负荷预测模型协同训练方法[J]. 湖南大学学报(自然科学版)，2022，49(8)：117-127.
Che Liang, Xu Maosheng, Cui Qiushi. Federated learning based coordinated training method of a short-term load forecasting model[J]. J. of Hunan University (Natural Sciences), 2022, 49(8): 117-127.

[9] Arjovsky M, Chintala S, Bottou L. Wasserstein GAN[J/OL]. arXiv:1701.07875, 2017[2023-11-15]. https://arxiv.org/abs/1701.07875.

[10] Gulrajani I, Ahmed F, Arjovsky M, et al. Improved training of Wasserstein GANs[J/OL]. arXiv: 1704.00028, 2017[2023-11-15]. https://arxiv.org/abs/1704.00028.

[11] 陆 鹏，付 华，卢万杰. 基于长短时记忆网络和的生成对抗网络的VRB储能系统虚假数据注入攻击检测[J/OL]. 电网技术：1-11[2023-07-10]. https://doi.org/10.13335/j.1000-3673.pst.2022.2256.
Lu Peng, Fu Hua, Lu Wanjie. Detection method of false data injection attacks for VRB energy storage systems based on long short term memory and generative adversarial networks[J/OL]. 1-11[2023-07-10]. https://doi.org/10.13335/j.1000-3673.pst.2022.2256.

[12] 周远翔，林孟龙，陈健宁，等. 基于自注意力生成对抗网络的电力设备在线监测缺失数据填补[J]. 高电压技术，2023，49(5)：1795-1809.
Zhou Yuanxiang, Lin Menglong, Chen Jianning, et al. Missing data imputation for online monitoring of power equipment based on self-attention generative adversarial networks[J]. High Voltage Engineering, 2023, 49(5): 1795-1809.

[13] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]// NIPS'14: Proc. of the 27th Inter. Conf. on Neural Information Processing Systems, 2014: 2672-2680.

[14] Greff K, Srivastava R K, Koutník J, et al. LSTM: A search space odyssey[J]. IEEE Trans. on Neural Networks & Learning Systems, 2016, 28(10): 2222-2232.

[15] Konecný J, Mcmahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency[J/OL]. arXiv:1610.05492, 2016[2023-11-15]. https://arxiv.org/abs/1610.05492.

[16] Schlegl T, Seeböck P, Waldstein S M, et al. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery[C]// IPMI 2017: Information Processing in Medical Imaging, 2017: 146-157.

[17] Donahue J, Krähenbühl P, Darrell T. Adversarial feature learning[J/OL]. arXiv: 1605.09782, 2016[2023-11-15]. https://arxiv.org/abs/1605.09782.

[18] Shu J, Zhou L, Zhang W, et al. Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach[J]. IEEE Trans. on Intelligent Transportation Systems, 2021, 22(7): 4519-4530.

[19] Wang W, Liang C, Tang L, et al. Federated multi-discriminator BiWGAN-GP based collaborative anomaly detection for virtualized network slicing[J]. IEEE Trans. on Mobile Computing, 2022, 22(11): 6445-6459.

作者简介：

吴维农(1965—)，男，四川省人，正高级工程师，主要研究方向包括OPGW特种光缆、无线工业控制、北斗高精度监测等电力通信系统；

唐 伦(1973—)，男，重庆市人，博士，教授，研究方向为新一代无线网络基础理论和组网技术。