XXXX

基于GAN数字孪生框架的电力物联网边缘智能对抗性测试方法

刘斯扬[1,2,4]，李博[1,2]，朱萌瑶[1,2]，唐标[1,2]，左鸿[3]，和嘉鹏[1,2]

（1. 云南电网有限责任公司电力科学研究院，云南省 昆明市 650217；
2. 云南省绿色能源与数字电力量测及控保重点实验室，云南省 昆明市 650217；
3. 云南电网有限责任公司怒江供电局，云南省 怒江市 673100；
4. 输变电装备技术全国重点实验室（重庆大学），重庆市，400044）

摘　要：针对电力物联网边缘节点面临的复杂对抗攻击识别难、实时性要求高及资源约束严等问题，提出一种基于GAN数字孪生框架的边缘智能对抗性测试方法。首先构建融合物理约束与时序一致性的GAN模型，生成符合边缘设备运行规律的对抗样本，结合数字孪生技术搭建边缘节点虚拟镜像，实现攻击场景的精准复现；其次设计常规工况、单一对抗、混合对抗三类测试场景，建立包含检测准确率、响应时延、虚假阳性率及算力占用率的四维评价体系；最后，案例分析结果表明，该方法在混合攻击场景下检测准确率达89.5%，响应时延控制在3.3-5.2ms，虚假阳性率低至0.5%，算力占用维持在22%-23%区间，较传统规则匹配法与单一机器学习模型，在复杂攻击识别能力、实时性及资源适配性上均有显著提升，为电力物联网边缘智能安全测试提供了高效可行的解决方案。

关键词：智能传感终端；生成对抗网络；数字孪生；对抗性测试；边缘智能

中图分类号：

文献标志码：A

doi: 10.11959/j.issn.1000−0801.

A GAN-based Adversarial Testing Method for Edge Intelligence in Power Internet of Things via Digital Twin Framework

Liu Siyang[1,2], Li Bo[1,2], Zhu Mengyao[1,2], Tan Biao[1,2], Zuo Hong, He Jiapeng[1,2]

1. Electric Power Institute, Yunnan Power Grid Co.,Ltd., Kunming 650217, Yunnan, China
2. Yunnan Key Laboratory of Green Energy, Electric Power Measurement Digitalization, Control and Protection,Kunming 650217,China.3. Nujiang Power Supply Bureau of Yunnan Power Grid Corporation, Nujiang 673100,China.4. State Key Laboratory of Power Transmission Equipment Technology（Chongqing University），Chongqing 400044，China

收稿日期：XXXX−XX−XX；**修回日期：**XXXX−XX−XX

通信作者：李博，高级工程师，研究方向：电能计量，E-mail：49923387@qq.com。

基金项目：云南电网公司科技项目，名称：电力物联传感器及终端设备检测平台建设与评价体系方法研究（YNKJXM20240410）。

Abstract: To address the challenges faced by edge nodes in the Power Internet of Things (PIoT), such as difficulty in identifying complex adversarial attacks, high real-time requirements, and strict resource constraints, an adversarial testing method for edge intelligence based on a GAN-driven digital twin framework is proposed. Firstly, a GAN model integrating physical constraints and temporal consistency is constructed to generate adversarial samples that conform to the operating rules of edge devices. Combined with digital twin technology, a virtual mirror of edge nodes is built to achieve accurate reproduction of attack scenarios. Secondly, three types of test scenarios—normal operating conditions, single adversarial attacks, and mixed adversarial attacks—are designed, and a four-dimensional evaluation system including detection accuracy, response delay, false positive rate, and computing power occupancy rate is established. Finally, case analysis results show that the proposed method achieves a detection accuracy of 89.5% in mixed attack scenarios, controls the response delay within the range of 3.3 – 5.2 ms, reduces the false positive rate to as low as 0.5%, and maintains the computing power occupancy between 22% and 23%. Compared with traditional rule-based matching methods and single machine learning models, it exhibits significant improvements in complex attack identification capability, real-time performance, and resource adaptability, providing an efficient and feasible solution for the security testing of edge intelligence in the PIoT.

Key words: intelligent sensing terminal, generative adversarial network, digital twin, adversarial testing, edge intelligence

0 引言

在全球能源转型与“双碳”目标驱动下，电力系统正经历从传统单向调度向“源网荷储”多元协同的革命性变革，电力物联网（Power Internet of Things，PIoT）通过感知层、网络层、平台层的深度融合，实现了发电、输电、配电、用电全环节的智能化管控[1]。边缘计算技术的规模化应用，进一步解决了电力物联网中海量终端设备的数据传输延迟、云端算力负载过大等关键问题，使AI推理、实时控制等智能功能下沉至设备近端，形成了“边缘感知-本地处理-实时反馈”的闭环架构[2, 3]。

边缘智能的核心价值依赖于AI模型的鲁棒性与安全性，但当前电力物联网边缘侧面临双重技术瓶颈：一是故障数据稀缺导致测试覆盖不全[4]。电力设备的异常工况（如IGBT开路故障、传感器漂移、电网电压畸变等）具有低概率、高破坏性特征，真实故障数据难以采集，使得边缘AI模型（如故障诊断、状态估计模型）的训练与测试面临“数据荒”问题，传统基于真实数据的测试方法无法全面验证模型在极端场景下的性能[5]。

数字孪生（Digital Twin）技术通过构建物理实体的虚拟镜像，实现了“数据-模型-仿真”的深度融合，为电力系统的全生命周期测试提供了新路径[6]。在智能电网领域，数字孪生已被用于并网逆变器控制、电网潮流优化等场景，但现有应用多聚焦于正常工况下的性能优化，缺乏对异常场景与对抗攻击的系统性测试能力[7]。GAN作为一种深度生成模型，能够从少量真实数据中学习数据分布，生成具有时序连续性与物理一致性的异常样本，为解决“数据荒”问题提供了有效手段[8, 9]。

当前相关研究已呈现技术融合趋势，但仍存在三个关键问题尚未解决[10]：第一，现有数字孪生建模多依赖物理机理驱动，缺乏对对抗性攻击数据的生成能力，无法模拟攻击者与防御者的动态博弈过程[11]；第二，GAN生成的数据往往缺乏物理约束，部分生成样本可能违反基尔霍夫定律（KVL/KCL）等电力系统基本规则，导致测试结果与实际场景脱节[12]；第三，边缘侧测试方法未充分考虑资源受限特性，现有对抗性测试多

基于云端算力设计，难以适配边缘节点的轻量化需求[13]。

本文提出基于GAN数字孪生框架的电力物联网边缘智能对抗性测试方法，通过构建“物理实体-边缘节点-GAN生成器-数字孪生镜像”的四阶架构，通过GAN学习真实故障与对抗攻击的数据分布，生成满足物理约束的高保真测试样本；然后，设计边缘轻量化对抗性测试流程，结合时间敏感网络（TSN）的确定性传输特性，确保测试延迟控制在微秒级，适配边缘节点实时性要求；建立多维度测试评估体系，从数据逼真度（FID、MMD指标）、模型鲁棒性（对抗样本攻击成功率）、系统安全性（状态估计误差、线路过载率）三个层面量化测试效果。该方法旨在解决电力物联网边缘智能测试中数据稀缺、场景单一、资源受限等关键问题，为边缘AI模型的安全性验证与优化提供理论支撑与技术参考。

1　电力物联网边缘智能模型

电力物联网边缘智能模型旨在通过边缘节点的本地化计算能力，实现电力设备状态感知、数据处理与实时决策的智能化，其核心是将传统云端集中式处理模式下沉至网络边缘，减少数据传输延迟与带宽消耗。本章节基于数学公式构建模型的核心框架，涵盖感知层数据预处理、边缘层智能决策及协同优化机制。

图1展示了电力物联网边缘智能模型的三层架构，即感知层、边缘层与云端层，清晰呈现了数据流转与协同优化的核心逻辑。感知层以智能传感终端为核心设备，是电力物联网的数据采集源头，负责实时获取电力系统运行状态、设备工况及环境参数等多源信息，其数据流转方向为终端向边缘层传输。边缘层作为承上启下的关键枢纽，包含终端级、台区级与区域级三级边缘节点。该层通过数据预处理、轻量推理及轻量化决策模型，对感知层数据进行就地处理，有效降低云端传输压力与延迟，同时保障关键业务的实时响应。云端层以电力物联网中心平台为核心，依托联邦学习与协同优化等关键技术，汇聚边缘层处理后的结构化数据，开展全局态势感知、模型迭代与资源调度。其数据流转方向为边缘层向云端层传输，实现跨区域、跨层级的协同决策。三层架构通过数据处理、轻量化决策模型与联邦学习协同优化等关键技术模块，形成“终端感知—边缘处理—云端决策”的闭环体系，既保障了电力业务的实时性与可靠性，又提升了系统的全局智能决策能力，为电力物联网的高效运行提供了核心支撑。

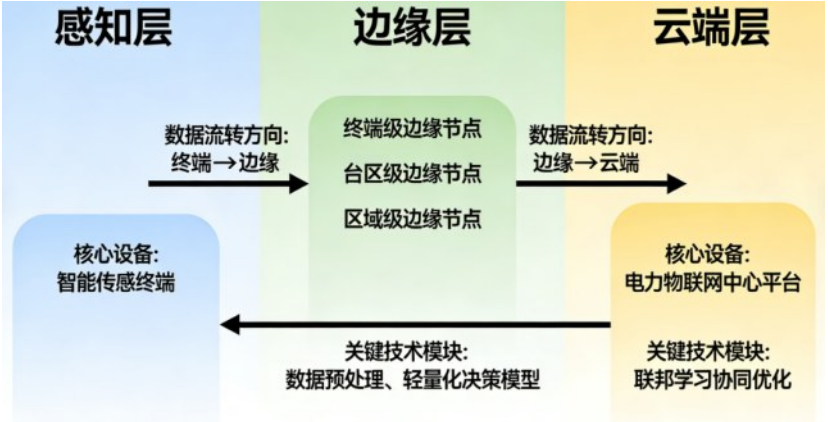


图1　电力物联网边缘智能模型的框架

Fig. 1　Framework of edge intelligent model for power internet of things

电力物联网边缘智能系统由感知层（终端设备）、边缘层（边缘节点）和云端层（中心平台）组成，其数据流转过程可描述为：

设感知层有N个终端设备，第i个设备在时刻t采集的原始数据为$x_i(t)\in\boldsymbol{R}^d$（$d$为数据维度），经边缘节点处理后生成决策指令$y_i(t)\in\boldsymbol{R}^m$（$m$为决策维度），最终通过云端协同优化全局策略。

系统的整体目标是最小化决策延迟与能耗的加权和：

$$\min\sum_{i=1}^{N}\left(\alpha\cdot\tau_i+\beta\cdot e_i\right) \tag{1}$$

其中，τ_i为第i个设备的决策延迟，e_i为边缘节点处理该设备数据的能耗，α、β为权重系数（根据实际需求调整）。

感知层数据存在噪声、冗余等问题，需通过边缘节点进行实时预处理。采用滑动窗口滤波与特征降维相结合的方法：

对设备i的原始数据$x_i(t)$进行噪声抑制，滤波后的数据$\hat{x}_i(t)$为：

$$\hat{x}_i(t)=\frac{1}{k}\sum_{s=t-k+1}^{t}x_i(s) \tag{2}$$

其中，k为窗口大小（通常取5~20，根据数据采样频率确定），通过平滑处理减少高频噪声干扰。

采用主成分分析（PCA）降低数据维度，设预处理后的数据矩阵为$X\in\boldsymbol{R}^{N\times d}$，其协方差矩阵为，

$$\Sigma=\frac{1}{N-1}X^T(X-\bar{X}) \tag{3}$$

其中，$\bar{X}$为均值向量，选取前p个主成分（$p<d$），降维后的数据为：

$$Z=X\cdot W \tag{4}$$

其中，$W\in\boldsymbol{R}^{d\times p}$为协方差矩阵$\Sigma$的前$p$个特征向量组成的矩阵，满足保留95%以上的原始数据方差。

边缘节点基于预处理后的特征数据Z，通过轻量化机器学习模型实现实时决策，以电力设备状态预警为例：

采用支持向量机（SVM）判断设备是否异常，决策函数为：

$$f(z)=\operatorname{sgn}\left(\sum_{j=1}^{l}\alpha_j y_j K(z,z_j)+b\right) \tag{5}$$

其中，z为输入特征向量，l为支持向量数量，α_j为拉格朗日乘子，$y_j\in\{+1,-1\}$为样本标签（正常/异常），$K(\cdot,\cdot)$为核函数（采用径向基函数$K(u,v)=\exp(-\gamma\|u-v\|^2)$），$b$为偏置项。

（2）决策延迟模型

边缘节点处理延迟τ_i与数据量、计算资源相关，设边缘节点的计算能力为C（单位：FLOPS），第i个设备的数据量为s_i（单位：bit），则：

$$\tau_i=\frac{s_i\cdot c}{C}+\tau_{\text{comm}} \tag{6}$$

其中，c为每bit数据的计算复杂度（单位：FLOPS/bit），τ_{comm}为设备与边缘节点的通信延迟（通常小于10ms）。

边缘节点本地决策后，需与云端协同更新全局模型，采用联邦学习框架减少数据传输量：设云端全局模型参数为Θ，第i个边缘节点的本地模型参数为θ_i，每轮迭代中，边缘节点基于本地数据更新θ_i，云端通过加权平均聚合：

$$\Theta^{(t+1)}=\sum_{i=1}^{N}\frac{n_i}{N}\theta_i^{(t)} \tag{7}$$

其中，n_i为第i个边缘节点的本地样本量，t为迭代轮次。

协同过程的能耗优化目标为：

$$\min\sum_{i=1}^{N}\left(e_{\text{comp},i}+e_{\text{trans},i}\right) \tag{8}$$

其中，$e_{comp,i}$为本地计算能耗（与τ_i正相关），$e_{trans,i}$为模型参数传输能耗（与参数大小$\|\theta_i\|_2$正相关）。

边缘智能模型的收敛速度是关键性能指标，以联邦学习中的参数收敛为例，在假设损失函数

为凸函数的前提下，模型参数的收敛率满足：

$$\| \Theta^{(t)} - \Theta^{*} \|_2^2 \le O\left(\frac{1}{t} + \sigma^2\right) \tag{9}$$

其中，Θ^{*}为最优参数，σ^2为边缘节点数据分布的异质性系数，表明模型收敛速度随迭代轮次增加而提升，且数据分布越均匀（σ^2越小），收敛越快。

2　基于GAN数字孪生框架的对抗性测试方法

电力物联网边缘智能系统的状态演化机制由马尔可夫决策过程建模，其状态空间$\mathcal{S}$包含智能传感终端的硬件参数、通信状态和计算负载等多维特征。时刻t的系统状态被定义为$s_t \in \mathcal{S}$，动作空间$\mathcal{A}$表征了可以应用的测试操作集，其中每个动作$a_t \in \mathcal{A}$对应于特定的测试信号注入或干扰条件。

系统的动态演化由状态传递函数描述：

$$s_{t+1} = f\left(s_t, a_t, G\left(z;\theta_g\right)\right) \tag{10}$$

其中，$G(z;\theta_g)$表示生成对抗网络产生的对抗扰动，θ_g是生成器参数集，$z \sim p_z(\mathrm{z})$是隐藏空间噪声变量。

绩效评估功能定义为：

$$R(s_t) = \alpha \cdot \mathrm{Accuracy}(s_t) + \beta \cdot \mathrm{Latency}(s_t) + \gamma \cdot \mathrm{Resource_U sage}(s_t) \tag{11}$$

其中，α、β、γ分别是精度、延迟和资源消耗指标的加权因子，Accuracy(s_t)量化故障检测精度，Latency(s_t)表征边缘计算响应时间，Resouree$_{\mathrm{U}}$ sage($\mathrm{s_t}$)反映CPU和内存利用率。

生成对抗网络的对抗训练过程是通过最小最大优化来实现的：

$$\min_G \max_D V(D,G) = \mathbb{E}_{x \sim p_{\mathrm{data}}(x)}\left[\log D(x)\right] + \mathbb{E}_{z \sim p_z(z)}\left[\log\left(1 - D\left(G(z)\right)\right)\right] \tag{12}$$

其中，$p_{\mathrm{data}}(x)$是真实的网格数据分布，($D(x;\theta_d)$是鉴别器网络，θ_d是其参数集。生成器$G(z;\theta_d)$采用五层深度卷积结构，激活函数选择为LeakyReLU（0.2），在每层卷积后插入批量归一化层，以稳定训练过程。

对抗样本生成公式为：

$$\delta_t = G\left(z;\theta_g\right) \tag{13}$$

其中，δ_t表示生成的对抗扰动数据，包含弱故障特征和复合扰动模式。

物理特性建模通过微分方程描述传感器动力学：

$$s_{t+1}^{p} = f_p\left(s_t^{p}, u_t, \xi_t\right) \tag{14}$$

其中，s_t^{p}是物理状态向量，u_t是外部激励，$\xi_t \sim \mathcal{N}(0,\sigma^2)$表示高斯噪声。通信协议仿真采用有限状态机模型：

$$c_t = f_c\left(c_{t-1}, m_t, \eta_t\right) \tag{15}$$

其中，c_t是通信协议状态，m_t是传输的消息，η_t表示网络延迟抖动。计算资源调度模型为：

$$r_t = f_r\left(r_{t-1}, l_t, \pi\right) \tag{16}$$

其中，r_t、l_t是任务负载，π是基于最早截止日期优先（EDF）的调度策略。

系统级状态转移方程整合了多维模型：

$$s_{t+1} = f\left(s_t, a_t, \delta_t\right) \tag{17}$$

其中，联合状态$s_t = [s_t^{p}, c_t, r_t]$包含物理、通信和计算状态。对抗性测试目标转化为约束优化问题：

$$\min_{\delta_t} R\left(s_{t+1}\right) \ \text{s.t.} \ \| \delta_t \|_\infty \le \epsilon \tag{18}$$

其中，ϵ为扰动强度约束参数，以确保生成样本的物理可实现性。测试有效性通过覆盖率指标进行评估：

$$C = \frac{\left|\mathcal{D}_{\mathrm{test}} \cap \mathcal{D}_{\mathrm{adv}}\right|}{\left|\mathcal{D}_{\mathrm{test}} \cup \mathcal{D}_{\mathrm{adv}}\right|} \tag{19}$$

其中，$\mathcal{D}_{\mathrm{test}}$是传统测试用例集，$\mathcal{D}_{\mathrm{adv}}$是对抗生成样本集。

综上所述，本文提出了一种基于GAN数字孪生框架的电力物联网边缘智能对抗性测试方

法，其流程图如图1所示。该方法通过构建高保真ISU数字孪生模型，并结合GAN生成逼真且具有挑战性的对抗场景，实现了在极端工作条件下对边缘智能算法的苛刻评估。整个过程包括七个核心步骤：1）物理节点数据采集（数字孪生提供数据接入接口，采集多源实体状态数据）；2）数字孪生镜像初始化（基于采集数据构建与物理节点一致的虚拟模型，完成虚实校准）；3）GAN对抗样本生成（结合数字孪生提供的物理约束参数，生成符合运行规则的攻击样本）；4）样本注入与虚拟仿真（将对抗样本注入数字孪生镜像，仿真攻击演化过程）；5）虚实协同测试（同步向物理节点注入校准后的对抗样本，对比虚实测试结果）；6）多维度状态监测（数字孪生实时记录测试过程中节点硬件、通信、业务状态数据）；7）测试结果反馈（数字孪生汇总虚实测试数据，输出模型鲁棒性评估报告，指导样本优化）。经过上述步骤，通过数字孪生和GAN的深度结合，该方法实现了电力物联网边缘智能系统的全面高效对抗测试，为智能传感终端的网络接入认证和鲁棒性优化提供了理论依据和实践指导。

3　案例分析

为验证基于GAN数字孪生框架的电力物联网边缘智能对抗性测试方法的有效性，选取某省级电力物联网边缘节点集群作为实验对象，该省级电力物联网边缘节点集群为国内典型省级电网全域覆盖架构，涵盖3类核心节点类型（终端级边缘盒、台区级边缘网关、区域级边缘服务器），共计部署1200余个边缘节点，覆盖发电侧（光伏电站、风电场）、输电侧（变电站）、配电侧（台区）、用电侧（工业用户、居民小区）全场景。通过多场景对抗测试验证方法的对抗性检测精度、实时响应能力与鲁棒性。

3.1　环境设置

硬件配置采用Intel Core i9-13900K处理器、64GB DDR5内存、NVIDIA RTX 4090显卡（24GB显存），软件环境基于MATLAB R2023a、

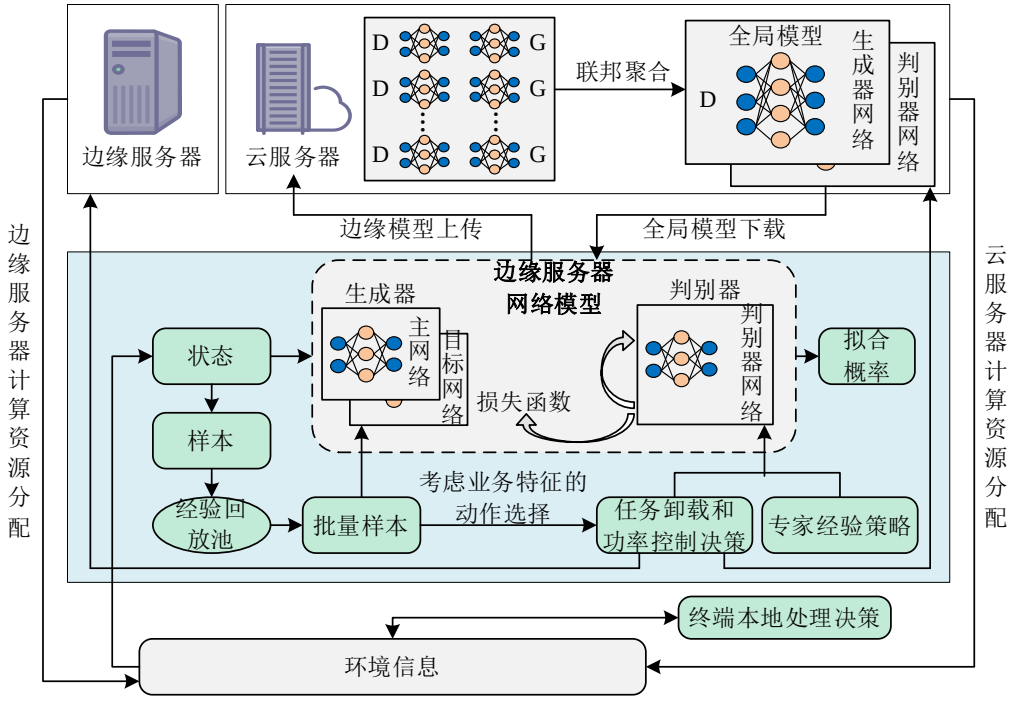


图2　基于GAN数字孪生框架的电力物联网边缘智能对抗性测试方法

Fig.2　Adversarial testing method for edge intelligence in power internet of things based on GAN - digital twin framework

Python 3.9、TensorFlow 2.10（GAN 模型训练支持），数据集包含正常运行数据 10 万条、恶意攻击数据（数据篡改、DoS 攻击、伪造请求）3 万条，按 7:3 比例划分训练集与测试集。GAN 数字孪生框架及边缘智能测试模块的关键参数设置如下表所示，确保模型训练稳定性与测试有效性。

表 1　仿真参数的设置

Table 1　Settings of Simulation Parameters

模块	参数名称	数值
GAN 生成器	网络层数	5
	隐藏层神经元数	256
	学习率	0.0002
	批量大小	64
GAN 判别器	网络层数	4
	隐藏层神经元数	128
	Dropout 比例	0.4
数字孪生映射	迭代更新步长	0.01
	相似度阈值	0.92
对抗性测试	攻击强度梯度	0.1-0.8
	测试采样频率	10Hz
	最大测试时长	7200s

设计三类核心测试场景，全面覆盖电力物联网边缘节点的运行特性与攻击风险，分别为：1）常规工况：边缘节点正常负载（30%-70% 算力占用），无恶意攻击；2）单一对抗场景：分别注入数据篡改、DoS 攻击、伪造请求单一类型攻击；3）混合对抗场景：同时存在两种及以上攻击类型，叠加网络抖动干扰。

选取 4 项核心指标量化测试效果，分别为：1）对抗性检测准确率（Accuracy）：正确识别攻击与正常状态的样本占比；2）虚假阳性率（FPR）：正常状态误判为攻击的样本占比；3）响应时延（Response Time）：从攻击发生到系统报警的时间间隔；4）稳定性偏差（Stability Deviation）：连续 100 次测试中检测准确率的波动范围。

3.2　结果分析

不同测试场景下，所提方法与传统边缘安全测试方法（基于规则匹配、单一机器学习模型）的检测准确率对比结果如图 2 所示。由图可知，在常规工况下，三种方法准确率均较高，但所提方法仍保持最优（98.9%）；在单一攻击场景中，所提方法准确率达 94.7%，较传统规则匹配法提升 16.1%；在最复杂的混合攻击场景中，优势更为显著，准确率达 89.5%，远超其他两种方法，验证了 GAN 数字孪生框架对复杂对抗行为的强识别能力。

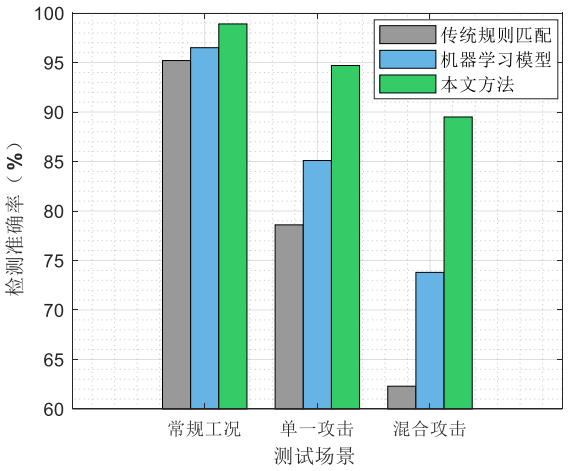
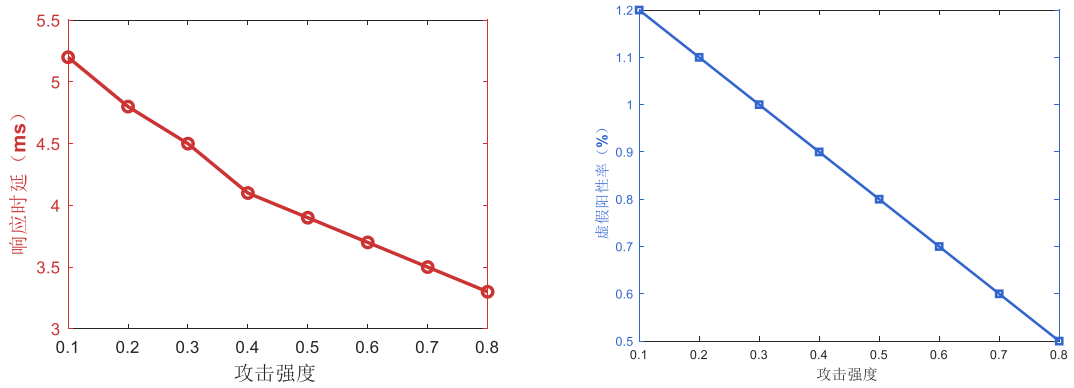


图 2　不同方法的对抗性检测准确率对比

Fig. 2　Comparison of accuracy of adversarial detection using different methods

不同攻击强度下，系统响应时延与虚假阳性率的变化趋势如图 3 所示，直观反映方法的实时性与可靠性。图 3（a）为响应时延变化，可见随着攻击强度从 0.1 递增至 0.8，响应时延呈显著递减趋势，由 5.2ms 逐步降至 3.3ms，全程保持在 10ms 以内，充分满足边缘智能场景的实时性要求；图 3（b）为虚假阳性率变化，其随攻击强度增加持续降低，最终低至 0.5%，说明方法对正常运行状态的误判概率极低，不会因过度检测干扰电力物联网的正常运行，从实时性与可靠性维度共同验证了所提方法的优异性能。



（a） 响应时延　　（b） 虚假阳性率

图3　不同方法的响应时延与虚假阳性率分析

Fig. 3　Analysis of response delay and false positive rate of different methods

在7200s连续运行测试中，记录每100s的检测准确率，分析方法的长期稳定性，如图4所示。由图可见，所提方法在7200s连续运行中，检测准确率始终稳定在93%以上，波动范围仅±0.8%；而传统方法准确率波动范围达±3.2%，且多次低于80%。这表明GAN数字孪生框架的动态映射能力有效抵消了边缘节点运行波动的影响，确保了对抗性测试的长期稳定性。

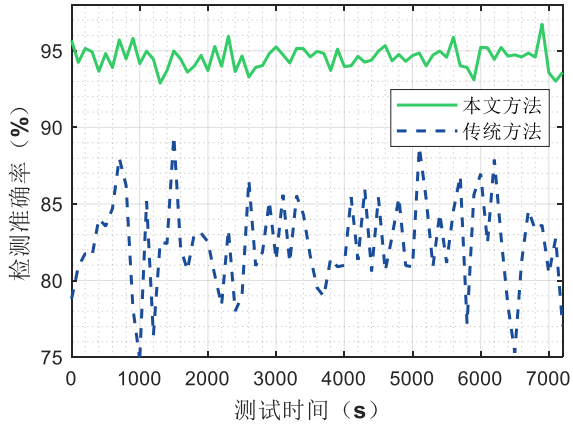


图4　长期运行的稳定性测试

Fig. 4　Stability test results for long-term operation

测试过程中，记录三种方法对边缘节点的算力占用率以评估资源消耗特性。由图5可知，传统规则匹配法算力占用最低，稳定在18%-19%之间，但检测效果较差；单一机器学习模型算力占用最高，维持在26%-27%左右；所提方法算力占用始终保持在22%-23%区间，在检测性能与资源消耗间实现了良好平衡。这一结果表明，所提方法既规避了传统规则匹配法的检测短板，又解决了单一机器学习模型资源开销过高的问题，完全契合电力物联网边缘节点轻量化运行的资源约束需求。

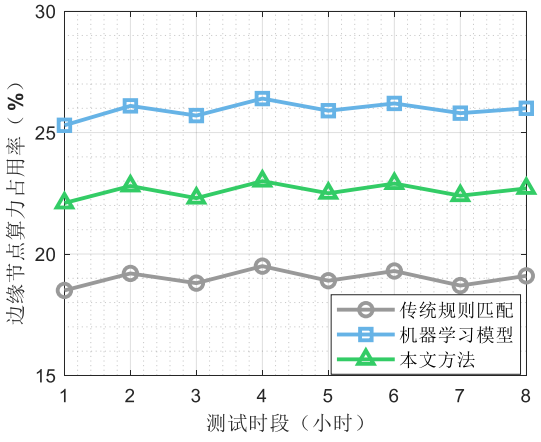


图5　不同方法在边缘节点算力占用的对比

Fig. 5　Comparison of computing power consumption of different methods at edge nodes

4　结论

本文围绕电力物联网边缘智能对抗性测试的核心需求，完成了基于GAN数字孪生框架的技

术方案设计与验证，主要结论如下 1）通过在 GAN 生成器中嵌入边缘设备物理约束与时序依赖机制，结合数字孪生动态映射能力，有效解决了传统测试方法场景覆盖不全、攻击样本缺乏物理合理性的问题，生成的对抗样本可精准模拟数据篡改、DoS 攻击等复杂威胁。2）仿真测试验证了方法的综合性能优势，在多类型攻击场景中均保持高检测准确率与低误报率，且响应时延满足边缘实时性要求，算力占用适配边缘节点轻量化运行约束，实现了性能与资源消耗的平衡。3）该框架通过虚拟镜像与实体节点的协同联动，降低了实体测试风险与成本。未来可进一步融合注意力机制优化 GAN 架构，提升对关键攻击路径的识别针对性，并拓展至分布式边缘集群的协同测试场景，增强方法的规模化适配能力。

参考文献：

[1] 丰雷，谢坤宜，朱亮，等. 面向电网业务质量保障的 5G 高可靠低时延通信资源调度方法 [J]. 电子与信息学报，2021，43 (12)：3418-3426.
FENG Lei，XIE Kunyi，ZHU Liang，et al. 5G Ultra - reliable and low latency communication resource scheduling for power business quality assurance [J]. Journal of Electronics & Information Technology，2021，43 (12)：3418-3426.

[2] 缪巍巍，曾铮，张明轩，等. 基于多智能体强化学习的边缘物联代理资源分配算法 [J]. 电力信息与通信技术，2021，19 (12)：9-15.
MIAO Weiwei, ZENG Zheng, ZHANG Mingxuan, et al. Edge IoT agent resource allocation algorithm based on multi-agent reinforcement learning [J]. Electric Power Information and Communication Technology, 2021, 19 (12): 9-15 (in Chinese).

[3] 韩富佳，王晓辉，乔骥，等. 基于人工智能技术的新型电力系统负荷预测研究综述 [J]. 中国电机工程学报，2023，43 (22)：8569-8591.
HAN Fujia，WANG Xiaohui，QIAO Ji，et al. Review on artificial intelligence based load forecasting research for the new - type power system [J]. Proceedings of the CSEE，2023，43 (22)：8569-8591.

[4] 黄兴，李立，王维，等. 面向电力物联网的认知反向散射通信鲁棒资源分配算法 [J]. 电力信息与通信技术，2023，21 (10)：35-40.
HUANG Xing, LI Li, WANG Wei, et al. Robust resource allocation algorithm in cognitive backscatter communication networks for power internet of things [J]. Electric Power Information and Communication Technology, 2023, 21 (10): 35-40 (in Chinese).

[5] 张琦，李志浩，范叶平，等. 新型电力系统中一种基于 LSTM 和 CNN 的倾斜样本预测算法 [J]. 电信科学，2025,41 (10): 211-221.
ZHANG Qi, LI Zhihao, FAN Yeping, et al. An unbalanced sample prediction algorithm based on LSTM and CNN in the new power systems [J]. Telecommunications Science, 2025, 41 (10):211-221.

[6] 蒋守花，冯军，舒晖，等. 基于深度强化学习的数据传输策略优化研究 [J]. 电信科学，2025,41 (8):149-162.
JIANG Shouhua, FENG Jun, SHU Hui, et al. Research on optimization of data transmission strategies based on deep reinforcement learning [J]. Telecommunications Science, 2025, 41 (8):149-162.

[7] 周江，陈扬，凌凌云. 基于效用函数的无源光网络动态带宽分配算法 [J]. 计算机与现代化，2023 (4)：106-110.
ZHOU Jiang, CHEN Yang, LING Lingyun. Dynamic bandwidth allocation algorithm for passive optical networks based on utility function [J]. Computer and Modernization, 2023 (4): 106-110 (in Chinese).

[8] 严兴煜，高赐威，陈涛，等. 数字孪生虚拟电厂系统框架设计及其实践展望 [J]. 中国电机工程学报，2023，43 (2)：604-618.
YAN Xingyu，GAO Ciwei，CHEN Tao，et al. Framework design and application prospect for digital twin virtual power plant system [J]. Proceedings of the CSEE，2023，43 (2)：604-618.

[9] 王日宁，武一，魏浩铭，等. 基于智能终端特征信号的配电网台区拓扑识别方法 [J]. 电力系统保护与控制，2021，49 (6)：83-89.
WANG Rining，WU Yi，WEI Haoming，et al. Topology identification method for a distribution network area based on the characteristic signal of a smart terminal unit [J]. Power System Protection and Control，2021，49 (6)：83-89.

[10] 卢宇亭，张乃平，高险峰，等. 考虑频谱利用率的无源光网络多业务带宽动态分配方法 [J]. 自动化与仪器仪表，2023 (7)：55-59.
LU Yuting, ZHANG Naiping, GAO Xianfeng, et al. Dynamic bandwidth allocation method for passive optical networks considering spectrum utilization [J]. Automation & Instrumentation, 2023 (7): 55-59 (in Chinese).

[11] 赵鹏，蒲天骄，王新迎，等. 面向能源互联网数字孪生的电力物联网关键技术及展望 [J]. 中国电机工程学报，2022，42 (2)：

447-458.
ZHAO Peng，PU Tianjiao，WANG Xinyin，et al. Technologies and perspectives of power Internet of Things facing with digital twins of the energy Internet [J]. Proceedings of the CSEE，2022，42 (2)：447-458 .

[12] 刘林，祁兵，李彬，等. 面向电力物联网新业务的电力通信网需求及发展趋势 [J]. 电网技术，2020，44 (8)：3114-3128.
LIU Lin，QI Bing，LI Bin，et al. Requirements and developing trends of electric power communication network for new services in electric internet of things [J]. Power System Technology，2020，44 (8)：3114-3128.

[13] 张宁，杨经纬，王毅，等. 面向泛在电力物联网的 5G 通信：技术原理与典型应用 [J]. 中国电机工程学报，2019，39 (14)：4015-4024.
ZHANG Ning，YANG Jingwei，WANG Yi，et al. 5G Communication for the ubiquitous internet of things in electricity：technical principles and typical applications [J]. Proceedings of the CSEE，2019，39 (14)：4015-4024.