基于改进自注意力机制生成对抗网络的智能电网GPS欺骗攻击防御方法

李元诚，杨珊珊
（华北电力大学 控制与计算机工程学院，北京 102206）

摘要：为了避免全球定位系统欺骗攻击（GSA）对相量测量装置造成的危害，提出了一种基于改进自注意力机制生成对抗网络（SAGAN）的智能电网GSA防御方法。首先，通过引入深度学习参数，构建了改进网络-物理模型，利用历史数据计算得到当前时刻的量测值。然后，在SAGAN的生成器和判别器网络中分别融入一个时间注意力模块，提出了一种用于实现网络-物理模型的改进SAGAN防御方法。通过训练改进SAGAN，得到一对判别器和生成器，利用判别器检测采集的量测值是否遭受GSA，当检测到攻击时，利用生成器生成的数据替换欺骗数据，从而实现智能电网对GSA的主动防御。最后，基于IEEE 14节点和IEEE 118节点系统进行仿真测试，结果验证了所提方法的可行性和有效性。

关键词：智能电网；全球定位系统；欺骗攻击；相量测量装置；生成对抗网络；防御方法
中图分类号：TM 761　　**文献标志码**：A　　DOI：10.16081/j.epae.202107014

0 引言

现代电力系统的规模不断扩大，互联程度不断加强，结构和运行方式日趋复杂，对状态估计[1]提出了更高的要求，传统的数据采集与监视控制SCADA（Supervisory Control And Data Acquisition）系统所采集量测值的精度已不能满足状态估计的要求。相量测量装置PMU（Phasor Measurement Unit）[2]能够对节点电压相量和支路电流相量等状态量进行高精度的同步量测，有效提高智能电网状态估计的精度[3]。但PMU成本高，经常采用基于PMU和SCADA系统混合量测的电力系统状态估计方法[4]。

PMU在提高智能电网状态估计精度的同时，也带来了一系列的安全问题。PMU的全球定位系统（GPS）接收机以射频方式接收来自不同卫星的GPS信号。GPS信号包括未加密的C/A码和加密的P（Y）码。PMU接收到的GPS信号为未加密的C/A码[5]。C/A码的码结构是公开的，很容易被攻击者利用，通过伪造GPS信号欺骗接收机，所以未加密的GPS信号容易受到欺骗攻击。研究人员已经对GPS欺骗攻击GSA（GPS Spoofing Attack）进行了现场测试，验证了其可行性[6]。此外，欺骗者可以成功地修改PMU量测值的时间戳。当GPS信号受到欺骗时，相应的PMU量测值会变得不可靠，因此必须在检测到欺骗后立即通过删除或校正等方式对量测值进行修正，否则，基于欺骗数据的状态估计结果将是错误的，并可能误导控制中心发起不必要的、可能破坏稳定的补救控制措施。例如，基于欺骗数据的状态估计可能导致墨西哥当前运行系统的控制方案自动使发电机跳闸，这会导致整个电网发生级联故障，甚至崩溃[7]。因此，如何高效地对GSA进行防御，减轻其带来的危害，对于保障智能电网的安全运行具有重要意义。

针对GSA的防御机制主要分为2类：一类是在GPS接收器接收GPS信号阶段进行防御；另一类是在PMU测量数据之后及进行状态估计之前的阶段进行防御。第一类防御机制通过检测导航数据，区分真实的GPS信号和伪GPS信号，通过恢复伪GPS信号对GSA进行防御。该类方法可以分为信号处理方法、天线防御方法、基于与其他时间源相关性的防御方法、加密策略四大类。信号处理方法需要从接收信号中监测导航信息的功率、质量，提取出导航信息的具体特征用于识别不相关数据，利用信号中的数学关系能够区分真实的GPS信号和伪GPS信号[8]。天线防御方法大多采用到达角分辨技术[9]，但通常需要高电平的附加硬件。基于与其他卫星系统权威机构的相关性的防御方法仅对特定的GPS信号[10]有用。加密策略较昂贵，且需要修改GPS信号结构，主要用于军事版本的GPS信号[11]。第二类防御机制是在PMU测量数据之后，通过各种算法提取出量测数据的具体特征用于识别异常数据，对被攻击的PMU量测值进行校正。文献[5]提出了一种基于探测技术的GSA识别算法，文献[12]提出了一种基于广义似然比检验的校正算法，但都只适用于单一GSA的情况。文献[9]从物理角度提出了一种针对多GSA的检测机制，需在PMU的现有接收器附近

收稿日期：2020-12-24；**修回日期**：2021-05-17
基金项目：中央高校基本科研业务费专项资金资助项目（2020YJ003）
Project supported by the Fundamental Research Funds for the Central Universities（2020YJ003）

安装另一台商用GPS接收器。文献[13]考虑多GSA的情况，将状态估计、攻击重构问题转化为双线性最小二乘问题，并利用交替最小化算法进行求解，但所提方法仅适用于系统可观测的环境，并不适用基于PMU和SCADA系统混合量测的电力系统环境。文献[14]提出了一种可以同时估计线参数和修正量测值的方法，但系统需具备一个预先校准的PMU。文献[15]提出了一种多层的多接收机结构，可以增强GPS的定时性能，以抵抗干扰、欺骗和接收机误差，但会增加额外的硬件成本。

生成对抗网络(GAN)[16]已被应用于网络攻击的防御策略研究中，但大多GAN方法在某些设定条件下仍存在样本生成质量低或者不能收敛等问题。文献[17]将自注意力机制引入GAN的框架，提出了自注意力机制生成对抗网络SAGAN(Self-Attention Generative Adversarial Network)。自注意力机制模块在建模长期依赖方面很有效，有利于提高生成样本的质量。另外，SAGAN将谱归一化应用于生成器，解决了GAN训练稳定性的问题，且生成器和判别器更新规则TTUR(Two-Timescale Update Rule)加速了正则化判别器的训练。

本文首先在SAGAN结构[17]中引入基于门控循环单元GRU(Gated Recurrent Unit)的时间注意力模块，提出了一种改进SAGAN模型；然后，基于改进SAGAN，实现对引入深度学习参数的新网络-物理模型的训练。改进SAGAN通过学习历史量测值，提取数据的时空特征，利用判别器对欺骗攻击进行检测，利用生成器实现对欺骗数据的恢复，最终得到一个基于改进SAGAN的主动防御模型。与现有研究相比，本文所提方法无需任何变电站级别的硬件增强，极易应用于实时场景或现场研究。此外，本文所提方法不仅能实现对GSA的检测，还能对欺骗数据进行校正。随着现代化电网的数据量越来越大，电网拓扑结构越来越复杂，现有研究提出的大多数据校正算法可能无法保证实时性，但算例仿真结果证明本文所提防御方法能很好地保证防御算法的实时性。

1　问题描述

1.1　GSA过程

GSA的原理为：攻击者的信号发射器发射与卫星信号结构相同/相似而功率更强的信号，使PMU中的GPS接收机误以为其是真实信号而进行搜索捕获。卫星导航系统的基本原理是无线电测距定位，近地面用户通过接收4颗以上卫星的信号，计算伪距后通过球面交汇完成定位。所以GSA的本质是通过发射信号误导目标用户得到错误的传播时延、伪距，致使目标用户定位到欺骗点上。若欺骗干扰源能灵活控制伪距的变化，则可实现任意位置欺骗。

为了欺骗GPS接收机，需要误导GPS接收机获取伪GPS信号。由于捕获阶段是通过在载波频率-码相二维空间中搜索最高相关峰值(直观而言，具有较高信噪比(SNR)的信号将具有较高的相关峰值)实现的，故存在一种两步法欺骗策略：在第一步中，欺骗者发射某些干扰，导致GPS接收机失去跟踪；在第二步中，当GPS接收机进行捕获时，欺骗者启动伪GPS信号。由于伪GPS信号具有更高的SNR，GPS接收机将因搜索到较高的相关峰值而跟踪伪GPS信号。

GSA的过程如下：攻击者通过学习真实的GPS信号，判断给定时间区域内攻击目标附近的轨道卫星，然后利用公开数据库中的公式，伪造不同卫星的C/A码，在攻击目标附近广播与真实信号相同的C/A码值信息；当攻击目标在捕获阶段的载波频率-码相二维空间中进行粗略扫描以搜索功率较大的GPS信号时，攻击者逐渐增加虚假信号的功率，致使GPS接收机锁定伪GPS信号，之后攻击者可以慢慢改变伪GPS信号的码相，接收机会调整其信号发生器与伪信号对齐，使码相偏离真实信号，最终将真实信号当作噪声处理。码相是计算传播时间和时间偏置的关键，因此GSA会通过随机移动GPS信号中的相角来破坏接收机与系统时间之间的时间同步，最终使接收机估计得到错误的卫星位置和时钟偏置量，使PMU计算得到错误的相角，之后能量管理系统(EMS)中的状态估计器利用被篡改的量测值估计得到不正确的系统状态，从而给电网带来严重威胁[18]。

1.2　受GSA影响的PMU量测值

假设在有N条母线的电力系统中安装了p台PMU，PMU_k提供的同步数据表示如下：

$$\boldsymbol{m}_k=\boldsymbol{A}_k\boldsymbol{s}+\boldsymbol{e}_k \tag{1}$$

$$\boldsymbol{m}_k=[m_{k_1},m_{k_2},\cdots,m_{k_n}]^{\mathrm{T}} \tag{2}$$

$$\boldsymbol{s}=[S_1,S_2,\cdots,S_N]^{\mathrm{T}} \tag{3}$$

式中：$\boldsymbol{m}_k$为PMU_k提供的量测值向量，其元素m_{k_i}($i=1,2,\cdots,n$；n为量测值数量)为PMU_k提供的序号为k_i的量测值；$\boldsymbol{s}$为电网状态向量；S_j($j=1,2,\cdots,N$)为母线j的电压相角；$\boldsymbol{A}_k$由系统状态和PMU_k提供的量测值决定，可以基于PMU的位置、网络拓扑和传输线参数获得；$\boldsymbol{e}_k$为PMU_k的测量噪声向量，不失一般性，假设$\boldsymbol{e}_k$服从相同的独立分布(方差为σ^2的复高斯分布)。

将p台PMU提供的量测值进行叠加，可得：

$$\begin{bmatrix}\boldsymbol{m}_1\\ \boldsymbol{m}_2\\ \vdots\\ \boldsymbol{m}_p\end{bmatrix}=\boldsymbol{m}=\begin{bmatrix}\boldsymbol{A}_1\\ \boldsymbol{A}_2\\ \vdots\\ \boldsymbol{A}_p\end{bmatrix}\boldsymbol{s}+\begin{bmatrix}\boldsymbol{e}_1\\ \boldsymbol{e}_2\\ \vdots\\ \boldsymbol{e}_p\end{bmatrix}=\boldsymbol{A}\boldsymbol{s}+\boldsymbol{e} \tag{4}$$

式中：$\boldsymbol{m}$、$\boldsymbol{A}$、$\boldsymbol{e}$可以分别由对应于不同PMU的子块$\boldsymbol{m}_k$、$\boldsymbol{A}_k$、$\boldsymbol{e}_k$适当地构造得到，在不失一般性的前提下，

假设所有PMU的测量噪声服从相同的分布。

假设一个GSA出现在PMU_k上，且相量偏移量为θ_{spf}，根据GSA对同步相量数据的影响特征，被欺骗的同步相量数据可表示为：

$$\boldsymbol{m}_{spf}=\boldsymbol{G}\boldsymbol{m}=\begin{bmatrix}\boldsymbol{m}_1\\ \vdots\\ \boldsymbol{m}_k e^{j\theta_{spf}}\\ \vdots\\ \boldsymbol{m}_p\end{bmatrix}=\begin{bmatrix}\boldsymbol{I}_1 & \cdots & 0 & \cdots & 0\\ 0 & \cdots & 0 & \cdots & 0\\ 0 & \cdots & \boldsymbol{I}_k e^{j\theta_{spf}} & \cdots & 0\\ \vdots & & \vdots & & \vdots\\ 0 & \cdots & 0 & \cdots & \boldsymbol{I}_p\end{bmatrix}\begin{bmatrix}\boldsymbol{m}_1\\ \vdots\\ \boldsymbol{m}_k\\ \vdots\\ \boldsymbol{m}_p\end{bmatrix} \tag{5}$$

式中：$\boldsymbol{m}_{spf}$为被欺骗的同步相量数据；$\boldsymbol{G}$为攻击矩阵；$\boldsymbol{I}_k(k=1,2,\cdots,p)$为单位矩阵，其大小由$PMU_k$提供的量测值数量决定（即与$\boldsymbol{m}_k$同维度）。

2 GSA防御机制

为了防御GSA，本文提出了一种改进网络-物理模型，该模型根据历史量测数据计算当前的量测值，并基于改进SAGAN实现模型训练。

2.1 改进网络-物理模型

首先通过回归算法对量测值向量进行预处理。量测值的非线性回归模型如式(6)所示。

$$\begin{aligned}\boldsymbol{M}_t=&\alpha_t\boldsymbol{V}_i^2+\beta_t\boldsymbol{V}_j^2+\eta_t\boldsymbol{V}_i\boldsymbol{V}_j+\gamma_t l(\boldsymbol{P}_{ij};\boldsymbol{Q}_{ij})+\\&\delta_t f(\boldsymbol{g}_{ij};\boldsymbol{b}_{ij};\boldsymbol{\theta}_{ij})+\boldsymbol{e}_t\end{aligned} \tag{6}$$

式中：$\boldsymbol{M}_t$为t时刻的量测值向量；$\boldsymbol{V}_i$、$\boldsymbol{V}_j$分别为母线i、母线j的电压幅值向量；$\boldsymbol{P}_{ij}$、$\boldsymbol{Q}_{ij}$分别为线路ij的有功潮流、无功潮流向量；$\boldsymbol{\theta}_{ij}$为母线i、母线j间的电压相角差向量；$\boldsymbol{g}_{ij}$、$\boldsymbol{b}_{ij}$分别为线路ij的电导、电纳向量；α_t、β_t、η_t、γ_t、δ_t为t时刻的测量系数；$l(\boldsymbol{P}_{ij};\boldsymbol{Q}_{ij})$为有功潮流与无功潮流间的非线性关系函数；$f(\boldsymbol{g}_{ij};\boldsymbol{b}_{ij};\boldsymbol{\theta}_{ij})$为电导、电纳、电压相角差之间的非线性关系函数；$\boldsymbol{e}_t$为$t$时刻的测量噪声向量。

基于式(6)，可以得到计算t时刻量测值的改进网络-物理模型如式(7)所示。

$$\begin{aligned}\boldsymbol{M}_c(t)=&\alpha\boldsymbol{V}_i^2(t-1)+\beta\boldsymbol{V}_j^2(t-1)+\eta\boldsymbol{V}_i(t-1)\boldsymbol{V}_j(t-1)+\\&\gamma l(\boldsymbol{P}_{ij}(t-1);\boldsymbol{Q}_{ij}(t-1))+\\&\delta f(\boldsymbol{g}_{ij}(t-1);\boldsymbol{b}_{ij}(t-1);\boldsymbol{\theta}_{ij}(t-1))+\boldsymbol{e}_t+\boldsymbol{u}_t\end{aligned} \tag{7}$$

式中：$\boldsymbol{M}_c(t)$为改进网络-物理模型计算所得t时刻的量测值向量；$\boldsymbol{V}_i(t-1)$、$\boldsymbol{V}_j(t-1)$、$\boldsymbol{P}_{ij}(t-1)$、$\boldsymbol{Q}_{ij}(t-1)$、$\boldsymbol{g}_{ij}(t-1)$、$\boldsymbol{b}_{ij}(t-1)$、$\boldsymbol{\theta}_{ij}(t-1)$为历史量测值向量；$\alpha$、$\beta$、$\eta$、$\gamma$、$\delta$为可以通过深度神经网络模型学习得到的模型参数值；$\boldsymbol{u}_t$为$t$时刻深度神经网络模型预测所得量测值与实际量测值之间的偏差向量。

结合所提改进网络-物理模型，利用$t-1$时刻采集的量测值对神经网络模型进行训练，可以计算得到t时刻的量测值。

2.2 改进SAGAN模型

SAGAN中的生成器和判别器网络采用卷积结构，结合自注意力机制可以有效提取输入数据的空间特征，但并不擅长提取数据中的周期性变化规律。在现代化电网中，拓扑信息越来越复杂，数据量也越来越大，量测值不仅具有空间相关性，也具有时间相关性，而GSA会篡改量测值，导致被篡改后的量测值具有与正常数据不同的时空特征。所以同时提取量测值的时空特征，学习正常数据和被欺骗数据的不同之处，可以有效提高修正数据的精度。

循环神经网络(RNN)可以有效地对动态时间序列数据进行建模，学习序列的周期性变化规律。而GRU是RNN的一种变体，其训练时间短，收敛速度快，可以避免梯度消失或梯度爆炸问题。

将SAGAN生成器和判别器中的空间自注意力模块提取所得的特征图输入GRU中进行动态时间建模，同时提取数据的时间和空间特征，可以有效提高判别器的判别准确率和生成器生成样本的质量，所以本文在SAGAN的生成器和判别器网络的最后一层卷积层之后分别融入基于GRU的时间注意力模块，提出了一种改进SAGAN模型，通过结合多种结构有效学习输入数据中丰富的特征和规律。

本文所提改进SAGAN中空间自注意力模块和时间注意力模块的具体叙述如下。

1)空间自注意力模块。

将前一隐藏层输出的数据特征$\boldsymbol{x}\in\mathbf{R}^{C\times M}$($C$为通道数，$M$为前一隐藏层特征的位置数量)变换为2个特征空间$f$、$g$来计算注意力，其中$f(\boldsymbol{x})=\boldsymbol{W}_f\boldsymbol{x}$，$g(\boldsymbol{x})=\boldsymbol{W}_g\boldsymbol{x}$，$\boldsymbol{W}_f\in\mathbf{R}^{\bar{C}\times C}$、$\boldsymbol{W}_g\in\mathbf{R}^{\bar{C}\times C}$($\bar{C}$为通道数，且有$\bar{C}=C/K$，$K=1,2,4,8$)为学习权重矩阵，则模型在合成第$j$个区域时对第$i$个区域的关注程度$\beta_{j,i}$可表示为：

$$\beta_{j,i}=\frac{e^{s_{ij}}}{\sum_{l=1}^{M}e^{s_{lj}}} \tag{8}$$

式中：$s_{ij}=f^{\mathrm{T}}(\boldsymbol{x}_i)g(\boldsymbol{x}_j)$，$\boldsymbol{x}_i$、$\boldsymbol{x}_j$分别为第$i$、$j$个区域的数据特征。自注意力层的输出为$\boldsymbol{o}=[\boldsymbol{o}_1,\boldsymbol{o}_2,\cdots,\boldsymbol{o}_j,\cdots,\boldsymbol{o}_M]\in\mathbf{R}^{C\times M}$，其第$j$列元素$\boldsymbol{o}_j$如式(9)所示。

$$\boldsymbol{o}_j=v\left(\sum_{i=1}^{M}\beta_{j,i}h(\boldsymbol{x}_i)\right) \tag{9}$$

$$h(\boldsymbol{x}_i)=\boldsymbol{W}_h\boldsymbol{x}_i \tag{10}$$

$$v(\boldsymbol{x}_i)=\boldsymbol{W}_v\boldsymbol{x}_i \tag{11}$$

式中：$\boldsymbol{W}_h\in\mathbf{R}^{\bar{C}\times C}$、$\boldsymbol{W}_v\in\mathbf{R}^{\bar{C}\times C}$为学习权重矩阵。为了提高内存效率，本文选取$K=8$进行测试。

此外，将自注意力层的输出与比例参数相乘，并重新添加输入的特征图，得到最终空间自注意力模块的输出为：

$$\boldsymbol{y}_i=\gamma_s\boldsymbol{o}_i+\boldsymbol{x}_i \tag{12}$$

式中：γ_s为可学习的标量，初始值为0。

2)时间注意力模块。

将空间自注意力模块输出的特征图构造为时间序列形式输入GRU进行动态时间建模，并引入注意

力机制通过映射加权和学习参数矩阵赋予GRU隐含状态不同的权重，减少历史信息的丢失并加强重要信息的影响。其中单个GRU结构由更新门和重置门组成，具体公式如下：

$$\boldsymbol{z}_t=\sigma(\boldsymbol{W}_z\boldsymbol{x}_t+\boldsymbol{U}_z\boldsymbol{h}_{t-1}) \tag{13}$$

$$\boldsymbol{r}_t=\sigma(\boldsymbol{W}_t\boldsymbol{x}_t+\boldsymbol{U}_t\boldsymbol{h}_{t-1}) \tag{14}$$

$$\tilde{\boldsymbol{h}}_t=\tanh(\boldsymbol{W}\boldsymbol{x}_t+\boldsymbol{U}(\boldsymbol{r}_t\circ\boldsymbol{h}_{t-1})) \tag{15}$$

$$\boldsymbol{h}_t=(1-\boldsymbol{z}_t)\circ\boldsymbol{h}_{t-1}+\boldsymbol{z}_t\circ\tilde{\boldsymbol{h}}_t \tag{16}$$

式中：$\boldsymbol{z}_t$为更新门，用于更新行为时的逻辑门；$\boldsymbol{r}_t$为重置门，用于决定候选行为时是否要放弃之前的行为$\boldsymbol{h}_t$；$\boldsymbol{x}_t$为t时刻GRU的输入；$\tilde{\boldsymbol{h}}_t$为t时刻的候选行为，接收$\{\boldsymbol{x}_t,\boldsymbol{h}_{t-1}\}$；$\boldsymbol{h}_t$为$t$时刻GRU的隐藏层输出，接收$\{\boldsymbol{h}_{t-1},\tilde{\boldsymbol{h}}_t\}$；$\boldsymbol{W}_z$、$\boldsymbol{U}_z$、$\boldsymbol{W}_t$、$\boldsymbol{U}_t$、$\boldsymbol{W}$、$\boldsymbol{U}$为权重矩阵；“$\circ$”为哈达码积；$\sigma(\cdot)$、$\tanh(\cdot)$为激活函数。

将GRU层的输出记为$\boldsymbol{H}$。注意力机制层的输入为经过GRU层激活处理的输出向量$\boldsymbol{H}$，根据权重分配原则计算不同特征向量对应的概率，不断更新迭代得到的较优权重参数矩阵。注意力机制层的权重系数计算公式为：

$$\boldsymbol{G}_t=u\tanh(w\boldsymbol{h}_t+\boldsymbol{B}) \tag{17}$$

$$\boldsymbol{a}_t=\sum_{i=1}^{t}\boldsymbol{G}_i'\boldsymbol{h}_i \tag{18}$$

$$\boldsymbol{G}_t'=\frac{\mathrm{e}^{\boldsymbol{G}_t}}{\sum_{i=1}^{t}\boldsymbol{G}_i} \tag{19}$$

式中：$\boldsymbol{G}_t$为t时刻由GRU层输出向量$\boldsymbol{h}_t$所决定的注意力概率分布值；u、w为权重系数；$\boldsymbol{B}$为偏置系数；$\boldsymbol{a}_t$为注意力机制层在t时刻的输出。

在改进SAGAN模型中，通过最小化铰链式的对抗性损失函数对模型交替训练，判别器的损失函数L_{D}、生成器的损失函数L_{G}分别见式(20)和式(21)。

$$L_{\mathrm{D}}=-E_{\boldsymbol{x}\sim p_{\mathrm{data}}}[\min\{0,-1+D(\boldsymbol{x})\}]-E_{z\sim p_z}[\min\{0,-1-D(G(z))\}] \tag{20}$$

$$L_{\mathrm{G}}=-E_{z\sim p_z}[D(G(z))] \tag{21}$$

式中：$E[\cdot]$为求期望值；$\boldsymbol{x}\sim p_{\mathrm{data}}$表示量测值向量数据$\boldsymbol{x}$服从真实数据分布；$D(\boldsymbol{x})$为判别器正确判断的概率；$G(z)$为生成器生成的数据；$D(G(z))$为判别器对生成器生成数据的判别结果；$z$为噪声向量。

2.3　GSA防御模型

将改进SAGAN模型应用到GSA防御中，设计GSA防御模型。防御模型分为数据采集与控制、数据检测与防御2个模块，其中，数据采集与控制模块进行数据采集、状态估计、初步检测坏数据等操作，并将含有欺骗数据的量测数据输入数据检测与防御模块；数据检测与防御模块包括训练好的生成器和判别器2个组件，主要采用的防御机制见2.4节。本文所提GSA防御模型如图1所示。

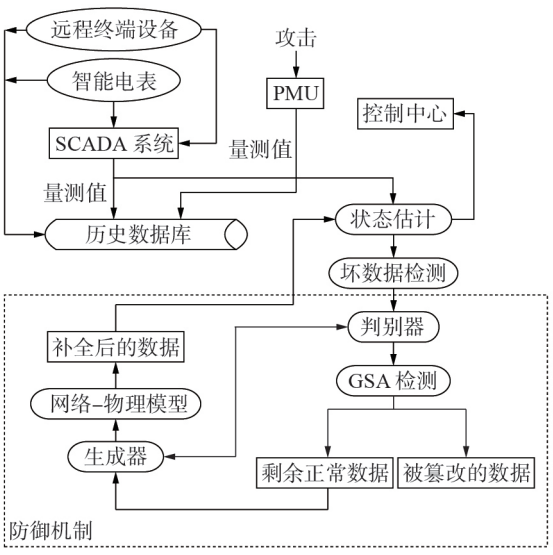

图1　GSA防御模型

Fig.1　Defense model of GSA

GSA防御模型的主要工作原理可以概括如下：攻击者对PMU的GPS接收机进行欺骗，引入错误的时间戳，从而篡改同步相量数据；PMU和SCADA系统将采集的数据传送到状态估计器进行状态估计和坏数据检测；经过坏数据检测后，将量测数据输入所提算法中；利用所提算法对量测数据进行检测，并对检测所得欺骗数据进行校正。数据检测与防御模块的实现过程如下：

1)进行GSA检测，检测数据是否为欺骗数据；

2)分离欺骗数据和正常数据；

3)删除欺骗数据并将剩余正常数据输入生成器；

4)利用生成器从正常数据中提取特征；

5)生成器结合网络–物理模型，根据提取的特征计算得到与损失数据特征尽可能一样的数据；

6)将计算得到的数据加入剩余正常数据中，合成补全后的数据，将其发送给状态估计器。

2.4　防御机制

根据所提改进SAGAN模型设计GSA防御机制，如图2所示。图中，$\boldsymbol{M}$为原始量测值数据；$\boldsymbol{M}_{\mathrm{r}}$为正常量测值数据；$\boldsymbol{M}_{\mathrm{c}}$为生成器计算得到的数据；$G(\boldsymbol{M}_{\mathrm{c}})$表示将一个向量$\boldsymbol{M}_{\mathrm{r}}$输入生成器G并输出量测值$\boldsymbol{M}_{\mathrm{c}}$的构造过程。

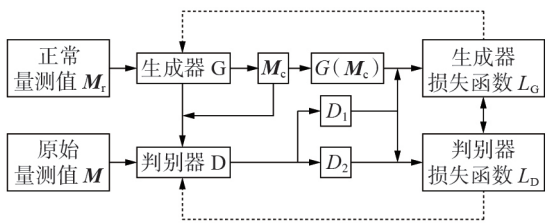

图2　GSA防御机制

Fig.2　Defense mechanism of GSA

本文所提防御机制的基本思想如下：①将原始量测值数据$\boldsymbol{M}$输入判别器D，判别器D的输出为概率值D_1和D_2，其中D_1为生成器G计算得到的数据属于正常数据的概率，D_2为该原始量测值数据属于正常数据的概率；②分离被欺骗的量测数据$\boldsymbol{m}_{spf}$与正常量测值数据$\boldsymbol{M}_r$；③将$\boldsymbol{M}_r$输入生成器G，生成器G计算并输出$\boldsymbol{M}_c$，将$\boldsymbol{M}_c$作为输入发送给判别器D。改进SAGAN中的判别器D和生成器G被交替训练，如果D_1很大，则说明生成器G生成样本的质量已经符合要求；否则，说明质量未达到要求，需要继续训练。谱归一化可以防止参数幅度增大，避免异常梯度。使用谱归一化的生成器和判别器使模型在每次生成器更新时进行较少的判别器更新次数，从而大幅缩短了训练时间，同时也提高了训练的稳定性。

判别器D的训练目的是为了使$E_{\boldsymbol{M}}[D(\boldsymbol{M})]$最大化，以此实现从量测值数据$\boldsymbol{M}$中提取更好的特征进行建模，增大正确判断的概率$D(\boldsymbol{M})$，即最大化甄别哪些向量值属于真实数据分布的概率。生成器G的训练的目的是为了使$E_{\boldsymbol{M}_c}[D(\boldsymbol{M}_c)]$最大化，从而使生成器计算得到的数据$\boldsymbol{M}_c$能接近真实的未被欺骗的量测数据，即最大化生成器输出的向量值被判别器判断为来自真实数据分布的概率。

本文所提改进SAGAN的具体训练过程见附录A。在改进SAGAN中，生成器和判别器以不同的学习率同时进行训练，具体步骤如下。

1）对原始量测数据集$\{\boldsymbol{m}_i\}$进行预处理，将n个量测值向量处理为$a\times b$阶矩阵$\boldsymbol{M}$，如式（22）所示。将矩阵$\boldsymbol{M}$作为改进SAGAN的输入。

$$\boldsymbol{M}=\begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1b} \\ m_{21} & m_{22} & \cdots & m_{2b} \\ \vdots & \vdots & & \vdots \\ m_{a1} & m_{a2} & \cdots & m_{ab} \end{bmatrix} \tag{22}$$

2）将经过预处理的矩阵$\boldsymbol{M}$和生成器生成的数据输入判别器的空间自注意力模块，利用其卷积层和自注意力层对输入数据进行高维特征提取，输出特征图。

3）将空间自注意力模块输出的特征图构造为时间序列形式，作为时间注意力模块的输入。

4）将步骤2）和步骤3）所得结果输入全连接层，分离正常数据和被欺骗数据，删除欺骗数据。

5）将正常量测数据作为先验的输入噪声变量输入生成器，经过一个全连接层，将其重塑为2维矩阵，然后将2维矩阵输入生成器的空间自注意力模块对输入数据进行高维特征提取，输出正常数据的特征图。

6）将空间自注意力模块输出的特征图构造为时间序列形式，作为时间注意力模块的输入，并提取数据的时间特征，得到生成数据。同时，将生成的数据输入判别器，利用判别器进行判别。

7）经过生成器和判别器不断地进行博弈，最终输出最接近于正常数据特征的数据。

3 算例分析

3.1 参数设置

为了验证所提防御方法的有效性，以IEEE 14节点、IEEE 118节点测试系统为例，采用文献[19]中的系统拓扑结构、参数进行仿真设置。每个系统对应不同的PMU位置配置文件，具体见附录B表B1。

在每个系统中，随机选择1台或多台PMU，对每台PMU随机选择相量偏移量θ_{spf}进行GSA，并在传输到状态估计器之前修改其量测值。本文考虑对1台PMU进行攻击的情况，采取文献[20]中的欺骗干扰策略，被欺骗者修改的PMU量测值以0.8（°）/s的速度偏离真实值，在2 min内突破PMU的IEEE C37.118标准[9]。本文所提方法通过学习量测值来恢复被欺骗的量测值数据，所以同样适用于针对多台PMU进行攻击的情况。设改进SAGAN判别器、生成器的学习速率分别为0.0004、0.0001。

3.2 GSA下PMU量测值变化测试

为了验证所提防御机制的性能，在进行防御机制性能测试之前，首先对受GSA的PMU量测值变化情况进行研究。由于GSA只会对电压相角值造成影响，而对电压幅值的影响不大，本节只研究电压相角值的变化情况。实验分别在2个测试系统中进行。设IEEE 14节点系统中的PMU_1（即母线2处的PMU）遭受相量偏移量为θ_{spf}的GSA（将其记为GSA$(1,\theta_{spf})$），具体实验结果如图3所示。针对IEEE 118节点系统的GSA结果见附录B图B1。

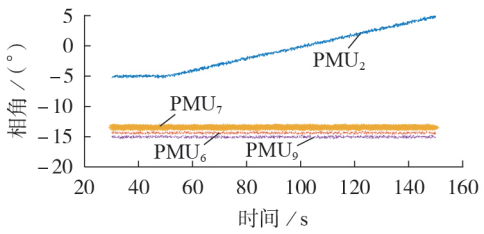

图3 IEEE 14节点系统遭受GSA时PMU量测值的变化曲线

Fig.3 Change curves of PMU measurement values when IEEE 14-bus system suffers GSA

由图3和附录B图B1可以看出，在2个测试系统中，攻击者在50 s后开始攻击，50 s之前的数据为正常数据，50 s后的数据为受欺骗的数据，IEEE 14节点系统中的PMU_2受到欺骗，IEEE 118节点系统中的PMU_9受到欺骗，欺骗在2 min内使相角偏离真值10°。因此，GSA的相量偏移量会对系统母线的电压相角值产生一定的影响。

3.3 防御机制性能测试

3.2节的测试结果表明，GSA会对系统的电压相

角值造成一定的影响。在防御机制中，生成器需要从正常数据中提取数据特征，计算得到与正常数据特征尽可能一样的数据。生成器在生成数据之前需要进行迭代训练，迭代的次数不同，则训练的效果不同。测试中设置不同的迭代次数，比较生成数据与未受攻击的正常数据之间的差别。在IEEE 14节点、IEEE 118节点系统中进行防御测试，验证所提防御机制的性能，结果分别见图4和附录B图B2。

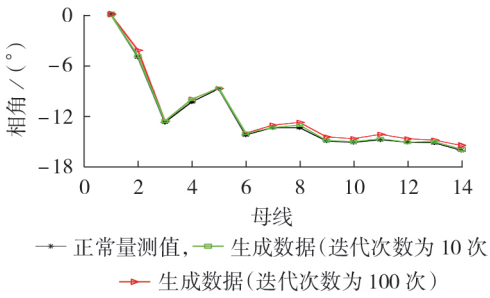

图4　迭代次数不同时的电压相角值（IEEE 14节点系统）

Fig.4　Voltage phase angle values with different iteration times (IEEE 14-bus system)

由图4可看出，在IEEE 14节点系统中，当训练迭代次数为10次时，生成器生成的数据略高于未受攻击的正常量测值；当迭代次数增加到100次时，生成器生成的数据几乎接近正常量测值。由图B2可看出，在IEEE 118节点系统中，当训练迭代次数超过100次后，生成器生成的数据与正常量测值接近。上述结果证明了本文所提防御机制在不同测试系统中的可行性。

关于测试算法的计算时间，IEEE 14节点系统和IEEE 118节点系统的计算时间分别为0.047、1.092 s，可见本文所提防御机制具有较短的延迟，从而保证了实时性防御。

为了进一步验证本文所提防御机制的有效性，设置生成器的迭代次数为100次，在IEEE 14节点系统和IEEE 118节点系统中进行不同算法的对比测试，结果分别如图5和附录B图B3所示。由图可知，相比于交替最小化算法、GAN算法和SAGAN算法，改进SAGAN算法生成的数据更接近于正常量测值，从而证明了所提改进SAGAN算法的有效性。

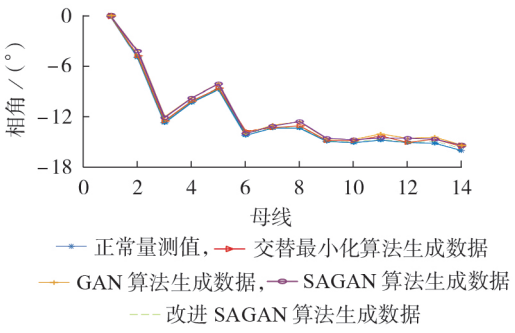

图5　不同算法所得电压相角值对比（IEEE 14节点系统）

Fig.5　Comparison of voltage phase angle values obtained by different algorithms (IEEE 14-bus system)

不同算法的计算时间对比如表1所示。由表可知，相较于其他防御算法，本文所提算法的计算时间最短，能更好地保证实时防御。

表1　不同算法的计算时间对比

Table 1　Comparison of computation time among different algorithms

算法	计算时间/s	
	IEEE 14节点系统	IEEE 118节点系统
交替最小化算法	0.732	2.527
GAN	0.249	1.703
SAGAN	0.093	1.357
改进SAGAN	0.047	1.092

4　结论

为了检测和防御GSA，本文提出了一种新的网络-物理模型，该模型在原模型的基础上引入了一个深度学习参数，具有更高的计算准确率。基于此网络-物理模型，提出了基于改进SAGAN的GSA检测和防御机制。在该机制中，利用改进SAGAN的空间自注意力模块对历史量测数据进行特征提取，基于GRU的时间注意力模块对所提特征进行动态时序建模，不断地通过生成器、判别器对量测数据进行学习，通过数据生成、对比和替换实现对GSA的检测和防御。将本文所提防御算法与交替最小化算法、GAN算法进行对比，测试结果表明本文所提防御方法生成得到的数据更接近正常数据，防御效果更好。

附录见本刊网络版（http://www.epae.cn）。

参考文献：

[1] 乐健，李星锐，周谦，等. 电力系统多区域分布式状态估计方法[J]. 电力自动化设备，2020，40(5)：165-172.
LE Jian，LI Xingrui，ZHOU Qian，et al. Multi-area distributed state estimation method for power system[J]. Electric Power Automation Equipment，2020，40(5)：165-172.

[2] 徐艳春，刘晓明，李振华，等. PMU准实时数据对主动配电网抗差估计的影响[J]. 电力自动化设备，2020，40(10)：15-22.
XU Yanchun，LIU Xiaoming，LI Zhenhua，et al. Influence of PMU quasi-real-time data on robust estimation of active distribution network[J]. Electric Power Automation Equipment，2020，40(10)：15-22.

[3] 孔祥玉，王玉婷，袁枭枭，等. 基于定制遗传算法考虑配电网多种拓扑可观性的PMU优化配置[J]. 电力自动化设备，2020，40(1)：66-72.
KONG Xiangyu，WANG Yuting，YUAN Xiaoxiao，et al. Optimal configuration of PMU based on customized genetic algorithm and considering observability of multiple topologies of distribution network[J]. Electric Power Automation Equipment，2020，40(1)：66-72.

[4] 朱鹏程，柳劲松，范士雄，等. 考虑混合量测的配电网二次约束二次估计方法[J]. 电网技术，2019，43(3)：841-847.
ZHU Pengcheng，LIU Jinsong，FAN Shixiong，et al. A quadratic constraint quadratic estimation method based on hybrid mea-

surements for distribution networks[J]. Power System Technology,2019,43(3):841-847.
[5] ZHANG Y,WANG J H,LIU J Z. Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems[J]. IEEE Transactions on Smart Grid,2020,11(1):762-773.
[6] SIAMAK S,DEHGHANI M,MOHAMMADI M. Dynamic GPS spoofing attack detection,localization,and measurement correction exploiting PMU and SCADA[J]. IEEE Systems Journal,2020,PP(99):1-10.
[7] SHEPARD D P,HUMPHREYS T E,FANSLER A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[J]. International Journal of Critical Infrastructure Protection,2012,5(3/4):146-153.
[8] KHALAJMEHRABADI A,GATSIS N,AKOPIAN D,et al. Real-time rejection and mitigation of time synchronization attacks on the global positioning system[J]. IEEE Transactions on Industrial Electronics,2018,65(8):6425-6435.
[9] FAN Y W,ZHANG Z H,TRINKLE M,et al. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids[J]. IEEE Transactions on Smart Grid,2015,6(6):2659-2668.
[10] JAFARNIA-JAHROMI A,LIN T,BROUMANDAN A,et al. Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver[C]//Proceedings of the 2012 International Technical Meeting of the Institute of Navigation. Newport Beach,CA,USA:ION ITM,2012:790-800.
[11] JAFARNIA-JAHROMI A,BROUMANDAN A,NIELSEN J,et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques[J]. International Journal of Navigation and Observation,2012(9):127072.1-127072.16.
[12] FAN X Y,DU L,DUAN D L. Synchrophasor data correction under GPS spoofing attack:a state estimation-based approach[J]. IEEE Transactions on Smart Grid,2018,9(5):4538-4546.
[13] RISBUD P,GATSIS N,TAHA A. Vulnerability analysis of smart grids to GPS spoofing[J]. IEEE Transactions on Smart Grid,2019,10(4):3535-3548.
[14] WU Z Y,ZORA L T,PHADKE A G. Simultaneous transmission line parameter and PMU measurement calibration[C]// 2015 IEEE Power & Energy Society General Meeting. Denver,CO,USA:IEEE,2015:1-5.
[15] HENG L,MAKELA J J,DOMINGUEZ-GARCIA A D,et al. Reliable GPS-based timing for power systems:a multi-layered multi-receiver architecture[C]//2014 Power and Energy Conference at Illinois(PECI). Champaign,IL,USA:IEEE,2014:1-7.
[16] GOODFELLOW I,POUGET-ABADIE J,MIRZA M,et al. Generative adversarial networks[J]. Communications of the ACM,2020,63(11):139-144.
[17] ZHANG H,GOODFELLOW I,METAXAS D,et al. Self-attention generative adversarial networks[EB/OL]. [2020-12-24]. https://arxiv.org/pdf/1805.08318.pdf.
[18] RISBUD P,GATSIS N,TAHA A. Multi-period power system state estimation with PMUs under GPS spoofing attacks[J]. Journal of Modern Power Systems and Clean Energy,2020,8(4):597-606.
[19] JAFARNIA JAHROMI A,BROUMANDAN A,NIELSEN J,et al. GPS spoofer countermeasure effectiveness based on signal strength,noise power,and C/N0 measurements[J]. International Journal of Satellite Communications and Networking,2012,30(4):181-191.
[20] XUE Ancheng,XU Feiyang,XU Jingsong,et al. Correction of phasor measurements independent of transmission line parameters[J]. IEEE Transactions on Smart Grid,2020,11(1):346-356.

作者简介:


李元诚

李元诚(1970—),男,山东烟台人,教授,博士研究生导师,博士,主要研究方向为电网安全、信息安全(**E-mail**:yuancheng@ncepu.cn);

杨珊珊(1995—),女,河北保定人,硕士研究生,主要研究方向为电网安全、深度学习算法(**E-mail**:1219605795@qq.com)。

(**编辑** 陆丹)

Defense method of smart grid GPS spoofing attack based on improved self-attention generative adversarial network

LI Yuancheng,YANG Shanshan

(School of Control and Computer Engineering,North China Electric Power University,Beijing 102206,China)

Abstract: In order to avoid the damage caused by GSA(Global positioning system Spoofing Attack) on PMU(Phasor Measurement Unit),a defense method of smart grid GSA based on improved SAGAN(Self-Attention Generative Adversarial Network) is proposed. Firstly,by introducing deep learning parameters,the improved cyber-physical model is built,and the measurement value at the current moment is calculated by using historical data. Then,a time attention module is incorporated into SAGAN's generator and discriminator respectively,and an improved SAGAN defense method is proposed to implement the cyber-physical model. By training the improved SAGAN,a pair of discriminator and generator is obtained. The discriminator is used to detect whether the collected measurement values are subject to GSA. When the attack is detected,the data generated by the generator is used to replace the spoofing data,so as to realize the active defense of smart grid GSA. Finally,simulation tests are carried out based on IEEE 14-bus system and IEEE 118-bus system,and the results verify the feasibility and effectiveness of the proposed method.

Key words: smart grid; global positioning system; spoofing attack; phasor measurement unit; generative adversarial network; defense method

附录 A

改进 SAGAN 的训练过程如下。

（1）首先对模型进行初始化设置：采用参数 $\beta_1=0$ 和 $\beta_2=0.9$ 的 Adam optimizer 进行训练；超参数 $k=1$；批大小为 n。

（2）输入原始量测值数据 $\boldsymbol{M}$。

（3）判别器检测量测值是否遭受 GSA，并分离被欺骗数据 $\boldsymbol{M}_{\text{spf}}$。

（4）根据 $p_{\boldsymbol{M}_{\text{c}}}$ 取样 n 个再生数据 $\{\boldsymbol{M}_{\text{c}}^{(1)},\boldsymbol{M}_{\text{c}}^{(2)},\cdots,\boldsymbol{M}_{\text{c}}^{(n)}\}$。

（5）根据 $p_{\boldsymbol{M}}$ 取样 n 个数据 $\{\boldsymbol{M}^{(1)},\boldsymbol{M}^{(2)},\cdots,\boldsymbol{M}^{(n)}\}$。

（6）计算鉴别器的代价函数 $L_{\text{D}}=\dfrac{\sum_{i=1}^{n}[-\min\{0,-1+D(\boldsymbol{M}^{(i)})\}-\min\{0,-1-D(\boldsymbol{M}_{\text{c}}^{(i)})\}]}{n}$。

（7）通过 Adam 梯度下降算法更新鉴别器的参数 $\theta_d=\text{Adam}(\nabla\theta_d(L_{\text{D}}),\theta_d)$。

（8）从步骤（4）到步骤（7）进行 k 次迭代。

（9）根据 $p_{\boldsymbol{M}_{\text{c}}}$ 取样 n 个再生数据 $\{\boldsymbol{M}_{\text{c}}^{(1)},\boldsymbol{M}_{\text{c}}^{(2)},\cdots,\boldsymbol{M}_{\text{c}}^{(n)}\}$。

（10）计算生成器的代价函数：$L_{\text{G}}=\dfrac{1}{n}\sum_{i=1}^{n}[-D(\boldsymbol{M}_{\text{c}}^{(i)})]$。

（11）通过 Adam 梯度下降算法更新生成器的参数 $\theta_g=\text{Adam}(\nabla\theta_g(L_{\text{G}}),\theta_g)$。

（12）从步骤（4）到步骤（11）不断进行训练迭代，生成器和判别器不断地进行博弈，输出最接近于正常数据特征的数据时，停止训练。

（13）输出测量值向量受到攻击的概率 $D(\boldsymbol{M})$ 和再生数据 $\boldsymbol{M}_{\text{c}}$。

附录 B

表 B1 不同测试场景下 PMU 位置配置文件

Table B1 PMU location profiles for different test scenarios

母线	PMU 数量/台	安装 PMU 的母线
14	4	2，6，7，9
118	20	5，9，12，15，21，25，29，37，42，49，56，62，70，75，80，85，91，94，102，105，114

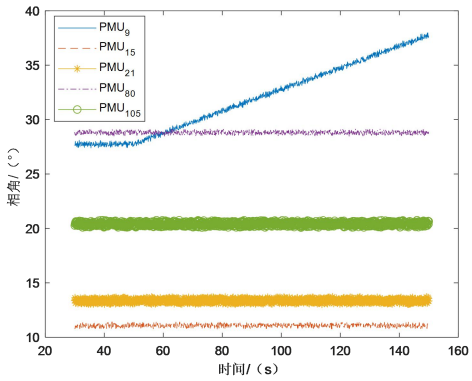

图 B1 IEEE 118 节点系统遭受 GSA 时 PMU 量测值的变化曲线

Fig.B1 Change curves of PMU measurement values when IEEE 118-bus system suffers GSA

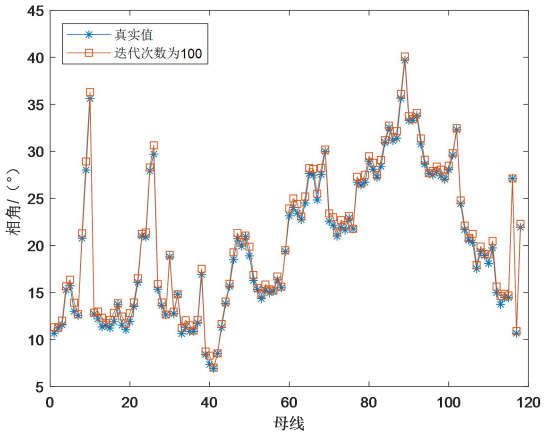

图 B2 IEEE 118 节点系统生成器补全后的电压相角值

Fig.B2 Voltage phase angle values of generator after completion for IEEE 118-bus system

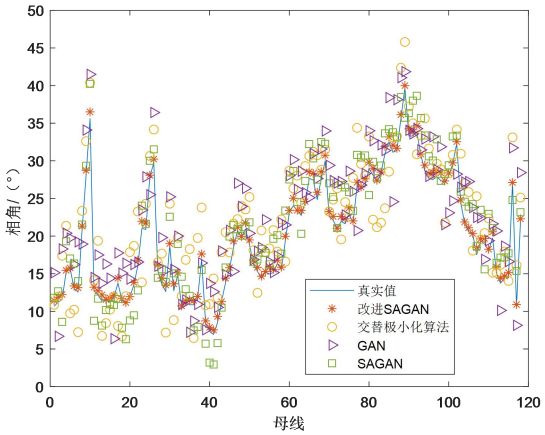

图 B3 IEEE 118 节点系统不同算法所得电压相角值对比

Fig.B3 Comparison of voltage phase angle values obtained by different algorithms for IEEE 118-bus system