文章编号:1671-4598(2025)12-0246-08 DOI:10.16526/j.cnki.11-4762/tp.2025.12.032 中图分类号:TP274 文献标识码:A

# 拒绝服务攻击下基于自注意力机制的数据恢复

杨晓芬[1,2]，陈晓婷[2]，李沁雪[2]，闫桂林[3]，钟杰宇[1]
(1. 广州大学 机械与电气工程学院，广州 510006；
2. 广州航海学院 低空装备与智能控制学院，广州 510725；
3. 广东能源集团公司 调度运营中心，广州 510630)

**摘要**：针对信息物理系统（CPSs）在遭受拒绝服务（DoS）攻击后的测量数据缺失，提出了基于数据插补的缺失数据恢复策略；构建了非周期性、资源受限的DoS攻击模型，同时引入随机数据丢包以模拟实际CPSs中网络攻击的复杂性；针对系统测量数据恢复问题，引入了一种基于对角线遮蔽自注意力机制的数据插补算法；为了提升插补的准确性和训练速度，该算法通过对角线遮蔽机制减少模型对自身值的依赖，再对对角线遮蔽自注意力模块进行加权组合；电力CPSs的实验结果表明，与几种深度学习算法相比，该数据恢复方法在复杂通信环境下可提高系统测量数据的恢复精度和效率，增强了系统的抗攻击能力和稳定性。

**关键词**：拒绝服务攻击；信息物理系统；丢包；测量数据恢复；数据插补；自注意力机制

# Data Recovery Based on Self-Attention Mechanism under Denial of Service Attacks

YANG Xiaofen[1,2]，CHENXiaoting[2]，LI Qinxue[2]，YAN Guilin[3]，ZHONG Jieyu[1]
(1. School of Mechanical and Electrical Engineering，Guangzhou University，Guangzhou 510006，China；
2. School of Low Altitude Equipment and Intelligent Control，Guangzhou Maritime University，Guangzhou 510725，China；
3. Dispatching Operation Center of Guangdong Energy Group Co.，Guangzhou 510630，China)

**Abstract**：In order to solve the missing measurement data in cyber physical systems (CPSs) after being attacked by denial of service (DoS)，a missing data recovery strategy based on data imputation is proposed. Firstly，an aperiodic，resource constrained DoS attack model is built，which introduce a random packet loss to simulate the complexity of cyber-attacks in actual CPSs. For the system measurement data recovery，a novel data imputation algorithm that leverages a diagonal masking self-attention mechanism is presented. To enhance the accuracy of data imputation and expedite the training process，the algorithm reduces the model's reliance on its own values by a diagonal masking self-attention mechanism，then conducts a weighted combination of the diagonal masking self-attention module. Experimental results of power CPSs show that，compared with several deep learning algorithms，the proposed data recovery method can improve the accuracy and efficiency of the system measurement data recovery in complex communication environments，and enhances the anti-attack ability and stability of the system.

**Keywords**：DoS attacks；cyber physical systems；packet loss；recovery of measurement data；data imputation；self-attention mechanism

## 0 引言

随着信息技术和通信技术的快速发展，智能技术的大量融入，诸如智慧交通、智慧建筑及智能电网等各种与国民经济、生活密切相关的信息物理系统（CPSs，cyber physical systems）的自动化和智能化水平不断提

**收稿日期**:2024-11-19； **修回日期**:2024-12-31。
**基金项目**:国家自然科学基金项目(62006052)；广东省基础与应用基础研究基金(2023A1515012468，2022A1515110148)；广州市教育局高校科研项目(2024311991)。
**作者简介**:杨晓芬(1998-)，女，硕士研究生。
**通讯作者**:李沁雪(1983-)，女，博士，副教授，硕士生导师。
**引用格式**:杨晓芬，陈晓婷，李沁雪，等. 拒绝服务攻击下基于自注意力机制的数据恢复[J]. 计算机测量与控制，2025，33(12)：246-253.

高。同时，这些 CPSs 的网络攻击风险也大为增加[1-2]。作为典型的网络攻击，拒绝服务（DoS，denial of service）攻击通过耗尽系统资源，可导致 CPSs 中传输数据的大量缺失，从而影响系统的正常运行和决策支持[2-4]。比如，DoS 攻击可导致系统中测量数据的大量缺失，若不及时恢复，将严重影响系统后续的控制决策、故障分析和处理，进而导致更为严重的物理故障。因此，研究有效的数据恢复方法，不仅能增强 CPSs 应对 DoS 攻击的能力，而且对丢包、虚假数据的丢弃造成的数据缺失等同样有效，具有长远的研究意义[5-8]。

目前，CPSs 抗攻击防御策略主要分为攻击前、攻击中和攻击后防御。在攻击前，多采用身份认证和数据加密技术以提前阻断潜在攻击；在攻击中，依靠多道防线、备用路由切换、先进的控制策略等措施来减轻攻击影响；在攻击后，主要通过取证分析及数据恢复[9-15]来维护系统的数据安全或采用先进的弹性控制策略[16-19]来维持系统的稳定运行。值得注意的是，对于控制器而言，若能通过取证分析及数据恢复的方式确保数据安全，则无需研究弹性控制策略，一样可维持攻击后系统的稳定运行。

在数据恢复方面，研究者提出了多种深度学习算法，如基于循环神经网络（RNN，recurrent neural networks）的时序双向循环插补（BRITS，bidirectional recurrent imputation for time series）、依靠注意力机制的 Transformer 模型、多向递归神经网络（M-RNN，multi-directional recurrent neural network）等，这些方法在提升数据恢复精度和效率方面表现突出[20-26]。然而，BRITS 通过 RNN 建模时间序列的双向动态性，无需对数据生成过程做特定假设[5]。BRITS 使用双向 RNN，需要对每个时间步长进行两次推理（前向和后向），这增加了计算量和内存占用，尤其在处理大规模数据集时，计算成本较高。Transformer 则通过注意力机制实现了高效的并行处理[7]，但 Transformer 不具备像 RNN 那样的序列内在顺序感知能力，因此需要引入额外的位置编码（Positional Encoding）来弥补这一点。而位置编码的设计仍然存在一些局限性，特别是在处理非常长的序列时。M-RNN 通过多向循环插补算法有效利用了时间序列中的跨数据流相关性[8]。类似于传统 RNN，M-RNN 也面临着梯度消失和梯度爆炸的问题，且其优化非常复杂。显然，以上问题限制了深度学习算法在 CPSs 数据恢复中的应用效果[24-26]。

本文针对 DoS 攻击导致的 CPSs 数据缺失问题，提出了一种基于插补算法的缺失数据恢复策略，旨在提升恢复精度和效率。通过优化算法结构和训练机制，本文的方法在复杂攻击场景下展现了更好的鲁棒性和收敛性，为 CPSs 抗攻击防御提供了新的技术支持。

## 1　拒绝服务攻击模型及衍生

### 1.1　拒绝服务攻击模型

现有研究多采用特定概率分布或周期性的 DoS 攻击模型，但由于实际攻击行为具有资源受限和隐蔽性，更具随机性，因此本研究采用非周期性的 DoS 攻击模型，随机设定活跃时长和休眠时长，以更真实地模拟间歇性、非周期的 DoS 攻击行为。CPSs 中的多变量时间序列在网络传播时容易受到 DoS 攻击，导致数据缺失，进而影响系统稳定性。

非周期性 DoS 攻击的数学模型如下：

$$z_{\mathrm{DoS}}(t)=\begin{cases}0, t\in[g_n, g_n+l_n)\\ 1, t\in[g_n+l_n, g_{n+1})\end{cases} \tag{1}$$

式中，$n$ 为周期编号；$g_n$ 为第 $n$ 个时间区间中 DoS 攻击的开始时刻；$z_{\mathrm{DoS}}(t)$ 为攻击状态，$z_{\mathrm{DoS}}(t)=0$ 时，代表 DoS 攻击处于休眠状态，$z_{\mathrm{DoS}}(t)=1$ 时，代表 DoS 攻击处于活跃状态；$[g_n, g_n+l_n)$ 为第 $n$ 个周期的休眠区间；$[g_n+l_n, g_{n+1})$ 为第 $n$ 个周期的活跃区间；$l_n$ 为第 $n$ 个周期的休眠长度；$c_n=g_{n+1}-g_n-l_n$ 为第 $n$ 个周期的活跃长度。

为了更逼近实际情况，在构建非周期性 DoS 攻击模型时，还需考虑测量数据过程噪声的存在，这里，过程噪声用高斯白噪声来模拟。DoS 攻击的休眠时长和活跃时长在程序中设定为随机值，每次攻击的时长为 3～10 s，以模拟间歇性和非周期性攻击行为。

### 1.2　随机数据丢包模型

随机数据丢包在网络通信中常见且无法预测。本研究基于文献［27］构建了随机数据丢包模型，将其建模为时变马尔可夫链：

$$P[l_R(0)=v]=p_v^{in} \tag{2}$$

$$P[l_R(k+1)=r \mid l_R(k)=v]=p_{v,r}(k) \tag{3}$$

式中，$v, r\in\{0,1\}$，$P[l_R(0)=v]$ 即马尔可夫链初始状态为 $v$ 的概率，$p_v^{in}\in[0,1]$ 为马尔可夫链的初始分布，$p_{v,r}(k)\in[0,1]$ 为时变的状态转移概率，$l_R(k)=1$ 表示发生数据丢包，$l_R(k)=0$ 表示通信成功，数据成功被接收。

程序中创建了 prob 向量，用以存储每个时刻是否丢包的状态，并通过 $\boldsymbol{p}_{\mathrm{loss}}$ 向量索引保存丢包位置。通过循环读取数据，判断每个数据点的丢包状态。

### 1.3　拒绝服务攻击下的混合数据缺失

DoS 攻击导致连续数据缺失，而丢包导致离散数据缺失。为模拟复杂情况，本研究结合了这两种模型，构建了混合数据缺失模型。混合数据缺失的公式可以表示为：

$$X'=X\cdot\boldsymbol{M}_{\mathrm{DoS}}\cdot\boldsymbol{M}_{\mathrm{Loss}} \tag{4}$$

式中，$X$ 是原始的多变量时间序列数据。$\boldsymbol{M}_{\mathrm{DoS}}$是一个矩

阵，表示 DoS 攻击导致的数据缺失情况。它的元素取值为 0 或 1，当元素为 1 时，表示该数据点未受到 DoS 攻击；当元素为 0 时，表示该数据点因 DoS 攻击而缺失。$\boldsymbol{M}_{\text{Loss}}$是一个矩阵，表示随机数据丢包导致的数据缺失情况。它的元素同样取值为 0 或 1，当元素为 1 时，表示该数据点未发生丢包；当元素为 0 时，表示该数据点因丢包而缺失。

在 DoS 攻击模型中，最终数据存储在 data _ do 中，将其输入到随机数据丢包模型中，生成 DoS 攻击下的混合数据缺失数据。

## 2 基于数据插补算法的数据恢复策略

通过构建非周期性 DoS 攻击模型及随机数据丢包模型，模拟了实际网络环境中对 CPSs 数据完整性的攻击。本文重点探讨如何利用数据插补算法恢复受损的 CPSs 测量数据，引入一种基于对角线遮蔽自注意力（DMSA，diagonally-masked self-attention）[28-29] 机制的数据插补算法（DMSAdi，DMSA-based data imputation）来提升数据插补的精度和效率。其算法核心在于两个对角线遮蔽自注意力模块和一个加权组合模块的协同工作。

### 2.1 缺失值插补和重构的联合优化训练方法

为了更有效地在具有缺失值的多变量时间序列上训练自注意力插补模型，基于 DMSA 机制的数据插补算法提出了一种插补和重构的联合优化训练方法。该训练方法包括两个学习任务：遮蔽插补任务（MIT，masked imputation task）和观测重构任务（ORT，observed reconstruction task），相应的训练损失由插补损失和重构损失组成[28]。

传统的 RNN 插补模型（如 BRITS）通常通过以下步骤进行训练：输入时间序列特征和缺失掩码，模型重构观测部分并计算误差，最后根据误差更新参数。这种训练方法在 RNN 模型中表现良好，称为观测重构任务（ORT）[23]。然而，对于基于自注意力机制的 Transformer 模型，仅使用 ORT 进行训练可能导致插补误差（MAE，mean absolute error）增加。换言之，由于 ORT 未对插补值进行惩罚，Transformer 可能忽略这些缺失值，无法准确预测。因此，引入了遮蔽插补任务 MIT，通过遮蔽观测值，要求模型准确预测缺失值。这种 MIT 与 ORT 结合的训练方法，被称为联合优化训练方法。

联合优化训练方法的总体如图 1 所示。

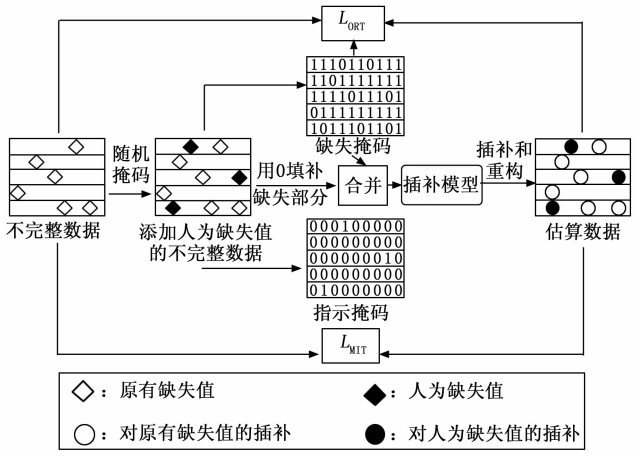


图 1 联合优化训练方法的总体结构

### 2.2 基于加权组合 DMSA 模块的算法模型

DMSAdi 由两个 DMSA 模块和一个加权模块组合而成，如图 2 所示。

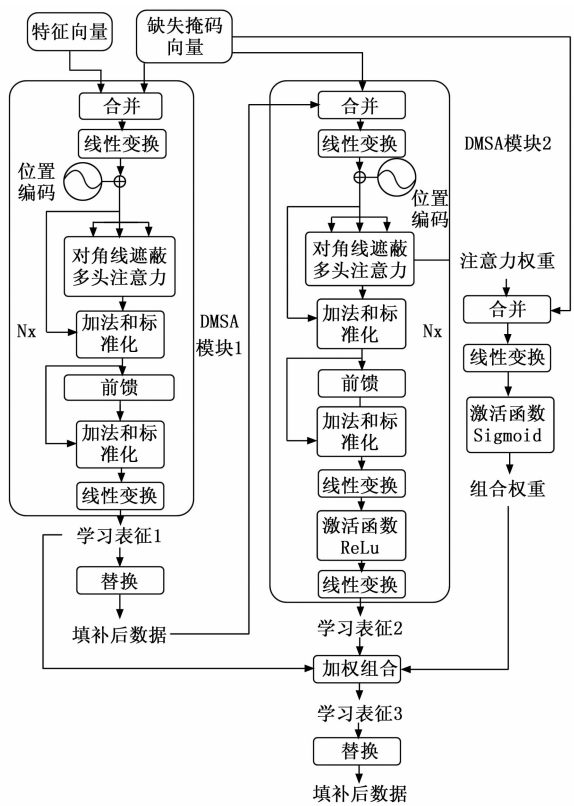


图 2 DMSAdi 的总体结构

具体原理如下：

1）对角线遮蔽自注意力：将给定序列映射为维度为 $d_k$ 的查询（Queries）向量和键（Keys）向量，以及维度为 $d_v$ 的值向量，通过缩放点积计算 $\boldsymbol{Q}$ 和 $\boldsymbol{K}$ 的注意力分数（或注意力图），然后，应用归一化指数函数获得注意力权重，最终的输出结果就是经过注意力加权的 $\boldsymbol{V}$，过程如下[29]：

$$\text{SelfAttention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \text{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^T}{\sqrt{d_k}}\right)\boldsymbol{V} \quad (5)$$

为了增强 DMSAdi 的插补能力，自注意力内部应用了对角线遮蔽。如式（6）和式（7），将注意力图（$\in \mathbb{R}^{T\times T}$）的对角线项设置为 $-\infty$（实际中设置为 $-1\times 10^9$），因此对角线的注意力权重在归一化指数函数后趋近于 0：

$$[\mathrm{DiagMask}(x)](i,j)=\begin{cases}-\infty, i=j\\ x(i,j), i\neq j\end{cases} \tag{6}$$

$$\mathrm{DiagMaskedSelfAttention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=$$
$$\mathrm{Softmax}\left[\mathrm{DiagMask}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^T}{\sqrt{d_k}}\right)\right]\boldsymbol{V}=\boldsymbol{A}\boldsymbol{V} \tag{7}$$

式中，$\boldsymbol{A}$ 为注意力权重。DMSA 机制如图 3 所示。

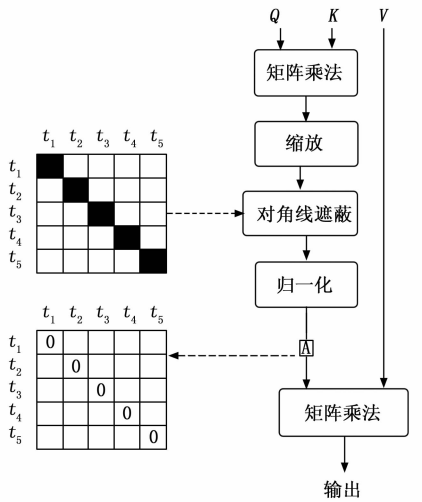


图 3　对角线遮蔽自注意力

通过这些对角线遮蔽，第 $t$ 步的输入值不会看到自己，并且无法对自身的估算做出贡献。因此，它们的估算仅取决于其他（$T$-1）个时间步的输入值。这种机制使得 DMSA 能够在高维空间中只通过一次注意力操作捕捉时间步之间的时序依赖关系和特征相关性。据此，对角线遮蔽多头注意力的数学表达如下：

$$\mathrm{DiagMaskedMHA}(x)=$$
$$\mathrm{Concat}(h_1^d,h_2^d,\cdots,h_i^d,\cdots,h_h^d)\boldsymbol{W}^O \tag{8}$$

$$h_i^d=\mathrm{DiagMaskedSelfAttention}(x\boldsymbol{W}_i^Q,x\boldsymbol{W}_i^K,x\boldsymbol{W}_i^V) \tag{9}$$

其中：$\boldsymbol{W}_i^Q\in\mathbb{R}^{d_{\mathrm{model}}\times d_k}$、$\boldsymbol{W}_i^K\in\mathbb{R}^{d_{\mathrm{model}}\times d_k}$ 和 $\boldsymbol{W}_i^V\in\mathbb{R}^{d_{\mathrm{model}}\times d_v}$ 是将输入 $x$ 映射到 $\boldsymbol{Q}$、$\boldsymbol{K}$ 和 $\boldsymbol{V}$ 的线性层的参数矩阵，$\boldsymbol{W}^O\in\mathbb{R}^{hd_v\times d_{\mathrm{model}}}$ 是将多个注意力头的输出拼接起来并映射到最终输出的线性变换矩阵，$h$ 是多头注意力的头部个数。

2）位置编码和前馈网络：在 DMSAdi 中，保留了 Transformer 中的位置编码和前馈网络。其中，位置编码由正弦和余弦函数组成；前馈网络有两个线性变换，它们之间有一个 ReLu 激活函数，具体见文献［24］和［28］。

3）第一个 DMSA 模块：

在第一个 DMSA 模块中，实际输入特征向量 $\hat{\boldsymbol{X}}$ 和缺失掩码向量 $\hat{\boldsymbol{M}}$ 被合并起来作为输入。式（10）将输入投影到 $d_{\mathrm{model}}$ 维度，并与位置编码 $p$ 相加生成 $e$。$\boldsymbol{W}_e$ 和 $b_e$ 是参数（$\boldsymbol{W}_e\in\mathbb{R}^{2D\times d_{\mathrm{model}}}$，$b_e\in\mathbb{R}^{d_{\mathrm{model}}}$）。式（11）中的操作 $\{\}^N$ 表示堆叠 $N$ 层。式（11）通过 $N$ 层堆叠的对角线遮蔽多头注意力和前馈网络将 $e$ 转化为 $z$。式（12）将 $z$ 从 $d_{\mathrm{model}}$ 个维度缩减为 $D$ 个维度，并生成 $\tilde{\boldsymbol{X}}_1$（学习表征 1）。参数 $\boldsymbol{W}_z\in\mathbb{R}^{d_{\mathrm{model}}\times D}$ 和 $b_z\in\mathbb{R}^D$。在式（13）中，$\hat{\boldsymbol{X}}$ 中的缺失值由 $\tilde{\boldsymbol{X}}_1$ 中的相应值代替，从而得到完整的特征向量 $\hat{\boldsymbol{X}}'$，并保持 $\hat{\boldsymbol{X}}$ 中的观测部分不变。数学表示如下：

$$e=[\mathrm{Concat}(\hat{\boldsymbol{X}}\hat{\boldsymbol{M}})\boldsymbol{W}_e+b_e+p \tag{10}$$

$$z=\{\mathrm{FFN}[\mathrm{DiagMaskedMHA}(e)]\}^N \tag{11}$$

$$\tilde{\boldsymbol{X}}_1=z\boldsymbol{W}_z+b_z \tag{12}$$

$$\hat{\boldsymbol{X}}'=\hat{\boldsymbol{M}}\odot\hat{\boldsymbol{X}}+(1-\hat{\boldsymbol{M}})\odot\tilde{\boldsymbol{X}}_1 \tag{13}$$

4）第二个 DMSA 模块：

第二个 DMSA 模块接收第一个 DMSA 模块的输出 $\hat{X}'$ 并继续学习。与式（10）类似，式（14）将合并后的 $\hat{\boldsymbol{X}}'$ 和 $\hat{\boldsymbol{M}}$ 从 $D$ 个维度投影到 $d_{\mathrm{model}}$ 个维度，然后将结果与 $p$ 相加生成 $\alpha$，参数 $\boldsymbol{W}_\alpha\in\mathbb{R}^{2D\times d_{\mathrm{model}}}$、$b_\alpha\in\mathbb{R}^{d_{\mathrm{model}}}$。在式（15）中，对 $\alpha$ 执行 $N$ 次嵌套注意函数和前馈网络，并输出 $\beta$。在式（16）中，为了得到 $\tilde{\boldsymbol{X}}_2$（学习表征 2），对 $\beta$ 应用了两个线性投影，中间有一个 ReLU 激活函数，其中参数 $\boldsymbol{W}_\beta\in\mathbb{R}^{d_{\mathrm{model}}\times D}$，$b_\beta\in\mathbb{R}^D$，$\boldsymbol{W}_\gamma\in\mathbb{R}^{D\times D}$，$b_\gamma\in\mathbb{R}^D$。根据经验，更深层次的结构可以更好地捕捉时间序列中更复杂的相关性。在式（16）中，比式（12）额外应用了一个非线性层，以构建一个更深的区块。在实践中，这样的操作确实有助于实现比应用单一线性投影更好的插补性能。这里，没有采用在第一个 DMSA 模块中取得 $\tilde{\boldsymbol{X}}_1$ 的相同的变换，因为下面加权组合中的可学习参数可以动态调整 $\tilde{\boldsymbol{X}}_1$ 和 $\tilde{\boldsymbol{X}}_2$ 的权重，从而取得更好的 $\tilde{\boldsymbol{X}}_3$（学习表征 3）。此外，通过实验可发现，即使在这里应用取得 $\tilde{\boldsymbol{X}}_1$ 的相同的变换也无助于取得比当前设计更好的结果，这验证了加权组合的有效性。数学表示如下：

$$a=[\mathrm{Concat}(\hat{\boldsymbol{X}}',\hat{\boldsymbol{M}})\boldsymbol{W}_a+b_a]+p \tag{14}$$

$$\beta=\{\mathrm{FFN}[\mathrm{DiagMaskedMHA}(\alpha)]\}^N \tag{15}$$

$$\tilde{\boldsymbol{X}}_2=\mathrm{ReLu}(\beta\boldsymbol{W}_\beta+b_\beta)\boldsymbol{W}_\gamma+b_\gamma \tag{16}$$

5）加权组合模块：

$$\hat{\boldsymbol{A}}=\frac{1}{h}\sum_{i=1}^{h}\boldsymbol{A}_i \tag{17}$$

$$\eta=\mathrm{sigmoid}[\mathrm{Concat}(\hat{A},\hat{\boldsymbol{M}})\boldsymbol{W}_\eta+b_\eta] \tag{18}$$

$$\tilde{\boldsymbol{X}}_3=(1-\eta)\odot\tilde{\boldsymbol{X}}_1+\eta\odot\tilde{\boldsymbol{X}}_2 \tag{19}$$

$$\hat{\boldsymbol{X}}_c=\hat{\boldsymbol{M}}\odot\hat{\boldsymbol{X}}+(1-\hat{\boldsymbol{M}})\odot\tilde{\boldsymbol{X}}_3 \tag{20}$$

为了取得更好的学习表征 $\tilde{\boldsymbol{X}}_3$，设计了加权组合模块，以根据时间依赖性和缺失信息动态权衡 $\tilde{\boldsymbol{X}}_1$ 和 $\tilde{\boldsymbol{X}}_2$。式（17）中的 $\hat{\boldsymbol{A}}(\in\mathbb{R}^{T\times T})$ 是由第二个 DMSA 模块最后一层多头输出的注意力权重 $\boldsymbol{A}$ 平均后得出的。式（18）以平均注意力权重 $\hat{\boldsymbol{A}}$ 和缺失掩码 $\hat{\boldsymbol{M}}$ 为参考，生成带有可学习参数 $\boldsymbol{W}_\eta(\in\mathbb{R}^{(T+D)\times D})$ 和 $b_\eta(\in\mathbb{R}^D)$ 的组合权重 $\eta[\in(0,1)^{T\times D}]$。等式（19）通过权重 $\eta$ 将 $\tilde{\boldsymbol{X}}_1$ 和 $\tilde{\boldsymbol{X}}_2$ 合并成 $\tilde{\boldsymbol{X}}_3$。最

后，在式（20）中，$\hat{\boldsymbol{X}}$ 中的缺失值由 $\tilde{\boldsymbol{X}}_3$ 中的相应值替换，以产生补充向量 $\hat{\boldsymbol{X}}_c$，即插补数据。

6）学习目标的损失函数：

$$L_{\mathrm{ORT}} = \frac{1}{3}[l_{\mathrm{MAE}}(\tilde{\boldsymbol{X}}_1, \boldsymbol{X}, \hat{\boldsymbol{M}}) + l_{\mathrm{MAE}}(\tilde{\boldsymbol{X}}_2, \boldsymbol{X}, \hat{\boldsymbol{M}}) + l_{\mathrm{MAE}}(\tilde{\boldsymbol{X}}_3, \boldsymbol{X}, \hat{\boldsymbol{M}})] \tag{21}$$

$$L_{\mathrm{MIT}} = l_{\mathrm{MAE}}(\tilde{\boldsymbol{X}}_c, \boldsymbol{X}, \boldsymbol{I}) \tag{22}$$

$$L = L_{\mathrm{ORT}} + \lambda L_{\mathrm{MIT}} \tag{23}$$

模型训练中有两个学习任务：MIT 和 ORT。MIT 的插补损失（$L_{\mathrm{MIT}}$）和 ORT 的重构损失（$L_{\mathrm{ORT}}$）都是通过 MAE 损失函数计算的，该函数有 3 个输入：估算值、目标值和掩码（它们都 $\in \mathbb{R}^{T\times D}$），它计算由掩码表示的估算值和目标值之间的 *MAE*。式（21）中 $L_{\mathrm{ORT}}$ 的目标和掩码是输入特征向量 $\hat{\boldsymbol{X}}$ 及其缺失掩码向量 $\hat{\boldsymbol{M}}$。让 $\tilde{\boldsymbol{X}}_1$ 和 $\tilde{\boldsymbol{X}}_2$ 直接参与 $\tilde{\boldsymbol{X}}_3$ 的构成。因此，这里的 $L_{\mathrm{ORT}}$ 是由 3 个学习到的表征累积而成的：$\tilde{\boldsymbol{X}}_1$、$\tilde{\boldsymbol{X}}_2$ 和 $\tilde{\boldsymbol{X}}_3$。这种累积损失可以加快收敛速度。为了确保 $L_{\mathrm{ORT}}$ 不会过大而主导梯度方向，将其缩小为三分之一，即平均值。式（22）中，$L_{\mathrm{MIT}}$ 的输入估算值、目标值和掩码分别是补充特征向量 $\hat{\boldsymbol{X}}_c$、不含人工遮蔽的原始特征向量 $\boldsymbol{X}$ 和指示掩码向量 $\boldsymbol{I}$。最后，式（23）将 $L_{\mathrm{ORT}}$ 和 $L_{\mathrm{MIT}}$ 加权组合，其中 $\lambda$ 是可以调整的加权系数，可通过 NNI（Neural Network Intelligence）工具进行超参调优。为了简化分析，参考文献［28］，将插补损失和重构损失的影响五五分，将 $\lambda$ 固定为 1。DMSAdi 模型是通过最小化最终损失 $L$ 来更新的。

## 3 电力 CPSs 仿真实验验证

### 3.1 数据预处理及评估指标

基于 Matpower 对 IEEE 57 节点电力系统进行潮流运算，得到系统支路有功测量数据。确保数据格式适合算法，需进行无量纲化处理。常用方法包括标准化和归一化。本文采用 *z*-score 标准化，消除数据量级影响，确保训练结果不受单位干扰。

此外，为了评估缺失数据插补算法的预测精度，本文采用均方根误差（*RMSE*）作为指标。*RMSE* 衡量插补结果与真实值之间的差异，其公式如下：

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2} \tag{24}$$

式中，$N$ 为样本数量，$y_i$ 为无量纲化后的真实值，$\hat{y}_i$ 为插补算法得到的预测值。*RMSE* 值越低，表示预测精度越高。此外，本文还记录了各算法的训练时间和测试时间，并结合预测精度综合评估算法的效率。

### 3.2 实验设计

在实验中，首先对 IEEE 57 节点电力系统进行潮流运算，生成 57 节点电力系统支路有功测量数据，并输入到第 1 节的 DoS 攻击模型或混合数据缺失模型中，生成缺失的测量数据作为攻击数据集。然后，应用数据插补算法，输出各算法的 RMSE 值、训练时间和测试时间，以评估其性能。

为测试算法在不同缺失度下的表现，实验中设置了不同数量的数据攻击点，模拟不同数量支路被攻击的情况。随着攻击点数量的增加，DoS 攻击数据集的缺失度也增加，从而生成不同缺失度的数据集。通过对这些数据集进行插补，评估算法在不同缺失度下的性能。缺失度 =（缺失值的数量/总数据量）×100%，它表示在整个数据集中，有多少比例的数据是缺失的。

此外，实验还在 DoS 攻击数据集基础上添加了随机数据丢包，生成混合缺失数据集，并使用相同算法进行插补，以评估它们在混合数据缺失情况下的性能。

### 3.3 实验结果分析

第 1 节中式（1）中的关键参数被设置为：$l_n = 5$、$c_n = 5$；选择不同数量的传感器测量数据（即攻击点）发动非周期性的 DoS 攻击，生成不同数量数据攻击点 DoS 攻击下的缺失数据集，数据集的缺失度情况见表 1。

表 1 DoS 数据攻击点数量与数据集的缺失度关系

| DoS 攻击数据攻击点数 | 缺失度/% |
|---|---|
| 5 数据攻击点 DoS 攻击 | 3.196 |
| 10 数据攻击点 DoS 攻击 | 6.387 |
| 15 数据攻击点 DoS 攻击 | 9.666 |
| 20 数据攻击点 DoS 攻击 | 12.843 |
| 30 数据攻击点 DoS 攻击 | 19.407 |
| 40 数据攻击点 DoS 攻击 | 25.003 |
| 50 数据攻击点 DoS 攻击 | 31.754 |
| 60 数据攻击点 DoS 攻击 | 38.689 |
| 70 数据攻击点 DoS 攻击 | 45.302 |
| 80 数据攻击点 DoS 攻击 | 51.863 |

通过设置模拟了不同数量的数据攻击点，以映射不同数量支路被攻击的情况，DoS 攻击数据集的缺失度也随之改变，可见当数据攻击点数越多时，数据集的缺失度也越高。

不同算法针对缺失数据集（DoS 攻击下）插补后的 *RMSE* 情况见表 2。由表 2 加粗部分数据看出，DMSAdi 算法在所有缺失度下的 *RMSE* 值均为最小，表现出优于其他算法的插补效果，尤其是在较低的缺失度和较高的缺失度时，DMSAdi 依然能够保持较低的 *RMSE*，说明该算法对数据缺失的鲁棒性较强，无论缺失度高低，都能提供相对准确的插补结果。

不同算法针对缺失数据集（DoS 攻击下）插补后的 *RMSE* 值如图 4 所示。

由表 2 和图 4 看出，无论缺失度如何，BRITS 算法的 *RMSE* 值均明显低于 M-RNN 算法，差值在 0.293 8～0.326 5 之间，表明在缺失数据集（DoS 攻击下）的恢

表 2　缺失数据集(DoS 攻击下)插补后的 *RMSE* 情况表

| 缺失度/% | 不同算法进行插补的 *RMSE* | | | |
|---|---|---|---|---|
| | BRITS | Transformer | M-RNN | DMSAdi |
| 3.196 | 0.070 2 | 0.414 9 | 0.366 2 | **0.011 8** |
| 6.387 | 0.061 3 | 0.396 1 | 0.371 0 | **0.014 1** |
| 9.666 | 0.063 8 | 0.387 6 | 0.374 0 | **0.016 4** |
| 12.843 | 0.070 0 | 0.380 2 | 0.396 5 | **0.013 7** |
| 19.407 | 0.062 2 | 0.388 9 | 0.383 0 | **0.012 4** |
| 25.003 | 0.075 7 | 0.397 9 | 0.383 2 | **0.034 6** |
| 31.754 | 0.091 2 | 0.384 5 | 0.374 6 | **0.039 4** |
| 38.689 | 0.094 3 | 0.381 8 | 0.376 8 | **0.037 7** |
| 45.302 | 0.082 7 | 0.386 5 | 0.398 4 | **0.034 0** |
| 51.863 | 0.115 4 | 0.392 2 | 0.409 2 | **0.046 9** |

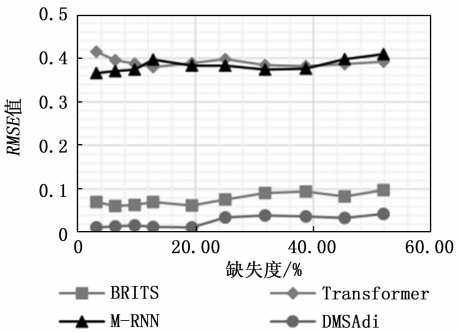


图 4　缺失数据集（DoS 攻击下）插补后的 *RMSE* 值曲线图

复中，BRITS 算法通过加权组合历史和特征估算，插补精度远高于 M-RNN 算法。无论缺失度如何，DMSAdi 算法的 *RMSE* 值也明显低于 Transformer 算法，差值在 0.344 1～0.403 1 之间，表明在缺失数据集（DoS 攻击下）的恢复中，DMSAdi 算法通过对角线遮蔽自注意力（DMSA）更好地捕捉时序依赖性和特征相关性，插补精度优于 Transformer 算法。此外，对比 *RMSE* 值最低的两种算法 DMSAdi 和 BRITS，DMSAdi 的 *RMSE* 值均低于 BRITS 算法的 *RMSE* 值，差值在 0.041 1～0.068 5 之间。综上可见，在缺失数据集（DoS 攻击下）恢复方面，基于对角线遮蔽自注意力机制的缺失值插补算法 DMSAdi 在 4 种算法中插补精度最高。

不同数量数据攻击点的 DoS 攻击和随机数据丢包混合数据缺失场景下，数据集的缺失度情况见表 3。

由表 3 可见，随机数据丢包使数据集缺失度略有增加。与 DoS 攻击相比，缺失度未增加固定值，因为随机丢包位置可能与 DoS 攻击位置重叠，导致缺失度增加呈反比关系。

不同算法针对缺失数据集（混合数据缺失下）插补后的 *RMSE* 情况见表 4。由表 4 加粗部分数据看出，即使在非常高的缺失度（如 52.030％和 57.229％）情况下，DMSAdi 的 *RMSE* 也仅稍微增加，表明该算法具有很好的鲁棒性，在处理数据缺失比例较大的场景时仍能提供准确的插补。

表 3　DoS 数据攻击点数量与混合数据缺失数据集的缺失度关系

| DoS 攻击数据攻击点数 | 缺失度/% |
|---|---|
| 5 数据攻击点 DoS 攻击 | 14.594 |
| 10 数据攻击点 DoS 攻击 | 17.259 |
| 15 数据攻击点 DoS 攻击 | 20.803 |
| 20 数据攻击点 DoS 攻击 | 22.654 |
| 30 数据攻击点 DoS 攻击 | 28.487 |
| 40 数据攻击点 DoS 攻击 | 33.654 |
| 50 数据攻击点 DoS 攻击 | 39.474 |
| 60 数据攻击点 DoS 攻击 | 46.341 |
| 70 数据攻击点 DoS 攻击 | 52.030 |
| 80 数据攻击点 DoS 攻击 | 57.229 |

表 4　缺失数据集(混合数据缺失下)插补后的 *RMSE* 情况表

| 缺失度/% | 不同算法进行插补的 *RMSE* | | | |
|---|---|---|---|---|
| | BRITS | Transformer | M-RNN | DMSAdi |
| 14.594 | 0.059 0 | 0.416 9 | 0.402 2 | **0.041 2** |
| 17.259 | 0.063 7 | 0.403 1 | 0.403 3 | **0.039 1** |
| 20.803 | 0.065 9 | 0.400 5 | 0.377 5 | **0.036 4** |
| 22.654 | 0.077 8 | 0.388 0 | 0.375 2 | **0.033 2** |
| 28.487 | 0.070 7 | 0.388 8 | 0.375 9 | **0.029 8** |
| 33.654 | 0.072 8 | 0.394 4 | 0.379 0 | **0.039 3** |
| 39.474 | 0.087 0 | 0.385 6 | 0.373 2 | **0.041 8** |
| 46.341 | 0.079 9 | 0.384 0 | 0.373 5 | **0.039 2** |
| 52.030 | 0.114 6 | 0.382 6 | 0.401 0 | **0.038 5** |
| 57.229 | 0.105 5 | 0.407 2 | 0.404 3 | **0.042 5** |

不同算法针对缺失数据集（混合数据缺失下）插补后的 *RMSE* 值如图 5 所示。

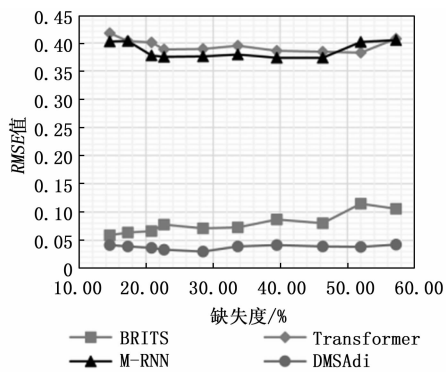


图 5　缺失数据集（混合数据缺失下）插补后的 *RMSE* 值曲线图

由表 4 和图 5 可知，无论缺失度如何，BRITS 的 *RMSE* 值均明显低于 M-RNN 的 *RMSE* 值，差值在 0.286 2～0.343 2 之间，表明在混合数据缺失下，BRITS 的插补精度远高于 M-RNN。DMSAdi 的 *RMSE* 值也明显低于 Transformer，差值在 0.343 8～0.375 7 之间，证明其插补精度更高。此外，DMSAdi 的 *RMSE* 值略低于 BRITS 的 *RMSE* 值，差值在 0.017 8～

0.076 1之间，说明基于对角线遮蔽自注意力的 DMSAdi 算法在精度上仍略优于 BRITS。

对比图 4 和图 5、表 2 和表 4 可知，尽管加入随机丢包后，各算法的插补精度有所下降，但整体波动不大；且推荐的 DMSAdi 算法的 *RMSE* 值仅从 0.011 8～0.046 9 变化为 0.029 8～0.042 5 区间，即，低缺失率时，其 *RMSE* 值略有增大，而高缺失率时 DMSAdi 的 *RMSE* 值不增反略降，表明 DMSAdi 在应对复杂攻击时具有一定的鲁棒性。

DMSAdi 算法针对两种情况进行插补的 *RMSE* 值如图 6 所示。

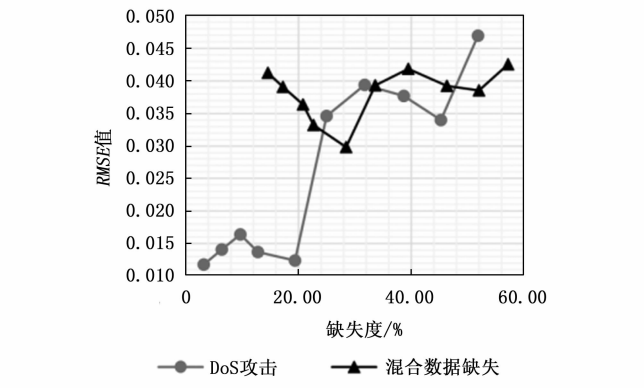


图 6 DMSAdi 针对两种情况进行插补的 *RMSE* 值

由图 6 看出，在更复杂的混合数据攻击下，DMSAdi 的 *RMSE* 值高于单 DoS 攻击，说明其在复杂环境下的适用性较低，后续改进应侧重于提升适用性。为了评估数据恢复算法在实时性方面的性能，除了基于数据插补的数据恢复精度方面的性能比较，本节还对各算法针对单个训练集进行插补的平均训练时间和测试时间做了统计，统计数据见表 5。

表 5 各算法平均训练时间和平均测试时间

| 算法类型 | 平均训练时间/s | 平均测试时间/s |
|---|---|---|
| BRITS | 7 372.652 | 109.841 91 |
| Transformer | **79.002 01** | **0.444 1** |
| M-RNN | 576.949 26 | 46.050 59 |
| DMSAdi | **125.582 91** | **0.691 22** |

由表 5 加粗部分数据看出，Transformer 和 DMSAdi 这两个算法在模型训练和测试时间上都表现出较高的效率，特别是在测试时间方面，显示了它们在预测或推理任务中的快速响应能力。且能看出基于自注意力的算法在单个训练集上的平均训练和测试时间明显低于基于 RNN 的算法。这证明了自注意力机制在处理电力系统测量数据时的高并行度，显著缩短了计算时间，加快了整体训练和测试过程。

综上所述，自注意力算法，特别是其中的 DMSAdi，以其在插补精度和处理效率方面的显著优势，在应对庞大数据集和需快速响应的电力系统中展现出比基于 RNN 的算法更加出色的性能。

## 4 结束语

CPSs 的自动化和智能化水平不断提高，遭受网络攻击的风险也随之提高。为了提高 CPSs 信息安全防护水平，本文提出了基于缺失数据插补算法的抗攻击防御策略，通过对含有缺失值的测量数据进行缺失数据插补，尽可能精确地恢复原有测量值，增强 CPSs 抗攻击能力和稳定性。本文主要做了以下工作：

1）构建了非周期性的 DoS 攻击模型，并加入了随机数据丢包的机制，使这种混合数据缺失模型更加接近真实攻击环境的复杂性和隐蔽性。

2）引入了一种基于对角线遮蔽自注意力机制的数据插补算法来完成 CPSs 攻击后残缺数据的恢复。该算法通过优化自注意力机制，减少了模型对自身数据的依赖，从而提高了插补的准确性和训练速度。

3）通过电力 CPSs 的对比实验，验证了本文引入的插补算法即使在非常高的数据缺失度（如 52.030% 和 57.229%）下，也具有更为稳定而优秀的数据恢复效果。

本文对 DoS 攻击下的 CPSs 数据恢复策略进行了探索，今后还可在以下两个方面做进一步工作：

1）当前的插补算法虽然在插补精度和处理效率上有显著提升，但算法复杂性依然较高，恢复过程的实时性不高。可能存在更加高效的算法结构，以适应实时或近实时的数据恢复需求。

2）提出的缺失数据插补算法仅适配了 DoS 攻击或者简单的混合数据缺失情况，针对其他复杂网络攻击的防御，还需要结合精确的攻击检测和故障定位技术，以形成普适性更好的数据恢复策略。

**参考文献：**

[1] 陈彦峰，邓庆绪，张天宇，等. 面向传感器攻击的概率时间窗感知融合算法研究 [J]. 计算机学报，2023，46 (6)：1227－1245.

[2] XING W，ZHAO X，LI Y，et al. Denial-of-service attacks on cyber-physical systems against linear quadratic control：a stackelberg-game analysis [J]. IEEE Transactions on Automatic Control，2024：1－8.

[3] LI J，ZHANG W，ZHANG Z，et al. Predictive control based on event-triggering mechanism of cyber-physical systems under denial-of-service attacks [J]. Information Sciences，2022，586：294－309.

[4] 高 兵，步 兵. 列车控制系统的抗拒绝服务攻击弹性控制策略 [J]. 控制理论与应用，2024，41 (2)：311－320.

[5] LI Q，LI S，XU B，et al. Data-driven attacks and data recovery with noise on state estimation of smart grid [J]. Journal of the Franklin Institute，2021，358 (1)：35－55.

[6] WANG S，LI H，CHEN J，et al. DAG blockchain-based lightweight authentication and authorization scheme for IoT devices [J]. Journal of Information Security and Applications，2022，66：103134.

[7] AZAD M A，BAG S，PERERA C，et al. Authentic caller：Self-enforcing authentication in a next-generation network [J]. IEEE Transactions on Industrial Informatics，2019，16 (5)：3606－3615.

[8] 于洁潇，于丽莹，杨　挺. 基于区块链的电力物联终端信任共识方法 [J]. 电力系统自动化，2021，45 (17)：1－10.

[9] YAN B，JIANG Z，YAO P，et al. Game theory based optimal defensive resources allocation with incomplete information in cyber-physical power systems against false data injection attacks [J]. Protection and Control of Modern Power Systems，2024，9 (2)：115－127.

[10] SMITH M D，PATé-CORNELL M E. Cyber risk analysis for a smart grid：how smart is smart enough? a multiarmed bandit approach to cyber security investment [J]. IEEE Transactions on Engineering Management，2018，65 (3)：434－447.

[11] 伏　帅. 考虑信息物理协同攻击的气—电混联系统的优化调度策略研究 [D]. 南京：南京邮电大学，2022.

[12] BADAR H M S，QADRI S，SHAMSHAD S，et al. An identity based authentication protocol for smart grid environment using physical uncloneable function [J]. IEEE Transactions on Smart Grid，2021，12 (5)：4426－4434.

[13] LIN H，CHEN C，WANG J，et al. Self-healing attack-resilient PMU network for power system operation [J]. IEEE Transactions on Smart Grid，2018，9 (3)：1551－1565.

[14] GHASEMI S，MOSHTAGH J. Distribution system restoration after extreme events considering distributed generators and static energy storage systems with mobile energy storage systems dispatch in transportation systems [J]. Applied Energy，2022，310：118507.

[15] 万　里. 拒绝服务攻击下的多区域电力系统负荷频率控制研究 [D]. 重庆：西南大学，2023.

[16] XIE X，LIU Y，LI Q. Neural network-based adaptive event-triggered control for cyber-physical systems under resource constraints and hybrid cyberattacks [J]. Automatica，2023，152：110977.

[17] GUO J，LI L，WANG J，et al. Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks [J]. IEEE Transactions on Industrial Informatics，2022，19 (5)：6624－6635.

[18] ZHAO Y，DU X，ZHOU C，et al. Anti-saturation resilient control of cyber-physical systems under actuator attacks [J]. Information Sciences，2022，608：1245－1260.

[19] YAO Y，KANG Y，ZHAO Y，et al. Prescribed-time output feedback control for cyber-physical systems under output constraints and malicious attacks [J]. IEEE Transactions on Cybernetics，2024，54 (11)：6518－6530.

[20] 刘雪花，丁丽萍，郑　涛，等. 面向网络取证的网络攻击追踪溯源技术分析 [J]. 软件学报，2021，32 (1)：194－217.

[21] WANG Y，ZHANG Z，MA J，et al. KFRNN：An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network [J]. IEEE Internet of Things Journal，2021，9 (9)：6893－6904.

[22] LIANG W，LI Y，XIE K，et al. Spatial-temporal aware inductive graph neural network for C-ITS data recovery [J]. IEEE Transactions on Intelligent Transportation Systems，2022，24 (8)：8431－8442.

[23] CAO W，WANG D，LI J，et al. Brits：Bidirectional recurrent imputation for time series [J]. Advances in Neural Information Processing Systems，2018：31.

[24] VASWANI A，SHAZEER N，PARMAR N，et al. Attention is all you need [J]. Advances in Neural Information Processing Systems，2017：30.

[25] YOON J，ZAME W R，VAN DER SCHAAR M. Estimating missing data in temporal data streams using multi-directional recurrent neural networks [J]. IEEE Transactions on Biomedical Engineering，2018，66 (5)：1477－1490.

[26] DU W. PyPOTS：A Python toolbox for data mining on partially-observed time series [J]. ArXiv Preprint ArXiv：2305.18811，2023.

[27] LIAN J，HUANG X，HAN Y. Observer-based stability of switched system under jamming attack and random packet loss [J]. IET Control Theory & Applications，2020，14 (9)：1183－1192.

[28] DU W，DAVID C，LIU Y. Saits：self-attention-based imputation for time series [J]. Expert Systems with Applications，2023，219：119619.

[29] YANG K，WANG J，YANG L，et al. A diagonal masking self-attention-based multi-scale network for motor imagery classification [J]. Journal of Neural Engineering，2024，21：036040.