基于DeepWalk算法的电力系统错误数据注入网络攻击分类方法

连祥龙，钱　瞳，张　银，唐文虎
（华南理工大学 电力学院，广东 广州 510641）

摘要：为了准确、有效地识别错误数据注入攻击（FDIA）对电网造成危害的严重程度，提出了基于DeepWalk算法的FDIA分类新方法。根据FDIA的特点，构建电力系统的响应模型；提出批量随机边删减策略，将响应模型生成的攻击数据构造为攻击场景图；采用DeepWalk算法将攻击场景图中的节点映射为低维向量，并将其作为机器学习算法的输入对FDIA进行分类。以遭受FDIA的IEEE 39节点系统为例进行仿真，结果表明所提方法可以根据FDIA对电网造成危害的严重程度准确、有效地对FDIA进行分类。

关键词：电力系统；网络攻击；错误数据注入攻击；DeepWalk算法；节点分类
中图分类号：TM761　　**文献标志码**：A　　DOI：10.16081/j.epae.202208037

0　引言

由于越来越多的嵌入式传感器、处理器及执行器被应用于电网中，电网的控制和运行方式正向智能化方向转变，这极大地提高了系统的态势感知能力[1]。但与此同时，来自网络攻击者的恶意网络攻击也给新型电力系统带来了新的挑战，如2015年因遭受网络攻击而导致的乌克兰大规模停电事件[2]。因此，为了确保电力系统的安全运行，研究网络攻击对电力系统造成威胁的机理和辨识对电网有重大威胁的攻击具有重要的现实意义。

错误数据注入攻击（false data injection attack，FDIA）是一种特殊的网络攻击，其通过在电网母线中注入功率或在支路潮流测量数据中注入虚假数据来恶意修改测量数据[3]。近年来，国内外学者已针对电网FDIA的构建机理和检测方法进行了广泛的探索和研究。文献[4]基于电力系统的状态估计模型，提出了电网在直流潮流和交流潮流模型下可躲避错误数据检测（bad data detection，BDD）系统检测的FDIA构造方法。文献[5]考虑信息物理系统高度融合的条件，提出了一种考虑FDIA的双层协同攻击模型，从攻击者视角为电网抵御此类攻击提供策略支持。此外，双层优化模型能够很好地描述FDIA下电力系统发电机出力的响应情况，并构造出攻击电网的错误数据向量[4,6]。

针对电网FDIA的检测，主要包括基于模型和基于数据驱动的检测方法[7]。基于模型的检测方法通过建立系统的响应模型并估计其参数的方式，实现对FDIA的检测，虽然不依赖于历史数据，但此类方法的可伸缩性差[8]。因此，为了摆脱对模型的依赖，研究人员提出了基于数据驱动的检测方法。文献[9]采用图论的方法辨识离群点中的邻接点，判断测量数据中的异常值，并将该类异常值作为FDIA。基于图神经网络，文献[10]结合电力网络的物理连接和测量数据的空间相关性，提出了一种可扩展的实时FDIA检测器。但上述检测方法只讨论了电力系统是否受到网络攻击，并不关心FDIA是否会对系统造成负荷损失等严重后果。

针对上述不足，本文根据FDIA对电力系统的威胁程度将网络攻击分为3种类别，并提出基于批量随机边删减策略和DeepWalk算法的FDIA严重程度分类方法。充分考虑电力系统在FDIA下的响应特性，以获得充足的FDIA样本；基于批量随机边删减策略构建描述样本关联关系的攻击场景图，并采用DeepWalk算法对图中的节点进行低维映射，实现严重网络攻击的分类任务。仿真结果验证了所提方法的有效性。

1　电力系统的FDIA响应模型

1.1　FDIA

随着智能传感元件在电力系统中的广泛应用，传统电网与信息系统的融合不断加深，信息物理系统一体化逐步成为一种新的系统发展趋势[3,11]。而电力系统向信息物理系统一体化方向的转化，为网络攻击者实施威胁电网安全运行的网络攻击提供了新途径。电力系统在FDIA下的响应模型如图1所示。图中：z为监控与数据采集（supervisory control and data acquisition，SCADA）系统的测量数据向量；

收稿日期：2022-02-14；**修回日期**：2022-06-19
在线出版日期：2022-08-25
基金项目：国家自然科学基金资助项目（51977082）；中国博士后科学基金资助项目（2021M701239）
Project supported by the National Natural Science Foundation of China（51977082） and China Postdoctoral Science Foundation（2021M701239）

$\boldsymbol{a}$为攻击向量；z_a为被篡改的测量数据向量，$z_a=z+\boldsymbol{a}$。

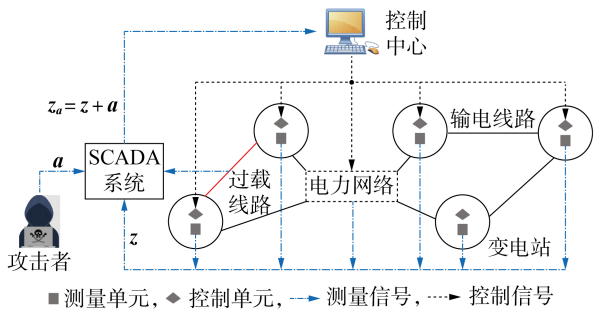


图1　电力系统在FDIA下的响应模型

Fig.1　Response model of power system under FDIA

电网一次侧的运行数据由测量单元采集后经过信息系统传输至控制中心，控制中心根据测量数据做出相应的决策后经信息系统向电网一次侧下达控制信号，确保电网的安全运行。网络攻击者可以利用通信网络的安全漏洞对测量装置发起FDIA，进而威胁整个电网的安全运行[4]。

SCADA系统可用于实现电力系统数据的采集、设备的控制及各种信号的报警功能。电网运行人员利用SCADA测量数据向量$\boldsymbol{z}=[z_1,\cdots,z_i,\cdots,z_m]$估计系统的实际状态向量$\boldsymbol{x}=[x_1,\cdots,x_i,\cdots,x_m]$，其中$z_i$、$x_i$($i=1,2,\cdots,m$)分别为第$i$个测量单元的测量量、状态量，$m$为测量单元的个数。研究表明，当攻击向量$\boldsymbol{a}$为雅可比矩阵$\boldsymbol{H}$的列向量的线性组合(即$\boldsymbol{a}=\boldsymbol{HC}$，$\boldsymbol{C}$为任意非零向量)时，被篡改的测量数据向量$z_a$将不会被BDD系统拦截[4]。本文重点关注负荷重分配攻击，即针对测量负荷数据的测量单元注入错误数据攻击向量。为了避免歧义，在后文中用$\Delta\boldsymbol{D}$代替$\boldsymbol{a}$。

1.2　FDIA向量的构建

本节从攻击者的视角出发，采用双层优化模型构建威胁电网安全运行的攻击向量$\Delta\boldsymbol{D}$[4]。如图1所示，当控制中心接收到来自SCADA系统的被篡改的测量数据向量z_a后，基于该错误数据进行的安全约束经济调度(security-constrained economic dispatch，SCED)会改变发电机的出力。该过程的双层优化模型可表示如下。

1)上层模型。

为了使所注入的攻击对电网造成严重危害，上层模型以最大化目标线路l的线路潮流$P_{\mathrm{f}}^{(l)}$为优化目标，如式(1)所示。

$$\begin{cases}\max\ P_{\mathrm{f}}^{(l)}\\ \text{s.t.}\ \ P_{\mathrm{f}}^{(l)}=\boldsymbol{\psi}_{\mathrm{PTDF}}^{(l)}(\boldsymbol{P}_{\mathrm{g}}-\boldsymbol{P}_{\mathrm{d}})\\ \quad\ \Delta\boldsymbol{D}=\boldsymbol{HC}\\ \quad\ -\alpha\boldsymbol{P}_{\mathrm{d}}\leqslant\Delta\boldsymbol{D}\leqslant\alpha\boldsymbol{P}_{\mathrm{d}}\\ \quad\ \sum_{i=1}^{N}d_i=0\end{cases}\tag{1}$$

式中：$\boldsymbol{\psi}_{\mathrm{PTDF}}^{(l)}$为功率传输分配因子矩阵的第$l$行；$\boldsymbol{P}_{\mathrm{g}}=[P_{\mathrm{g},1},P_{\mathrm{g},2},\cdots,P_{\mathrm{g},N}]$、$\boldsymbol{P}_{\mathrm{d}}=[P_{\mathrm{d},1},P_{\mathrm{d},2},\cdots,P_{\mathrm{d},N}]$分别为发电机的有功出力、负荷有功功率向量，$P_{\mathrm{g},i}$、$P_{\mathrm{d},i}$($i=1,2,\cdots,N$)分别为节点$i$处发电机的有功出力、负荷有功功率，$N$为电网节点数量；$\Delta\boldsymbol{D}=[\Delta d_1,\Delta d_2,\cdots,\Delta d_N]$，$\Delta d_i$为节点$i$处的注入功率；$\alpha$为强度因子，$\alpha<1$。式中的第2个约束条件用于确保所构造的攻击向量能够顺利通过BDD；第3个约束条件用于限制攻击向量的强度；第4个约束条件是为了确保电网功率平衡，即保持电网总功率不变。

2)下层模型。

当控制中心监测到系统负荷量发生变化时，应对电网下达基于SCED的控制指令，使系统发电成本最低，下层模型的优化目标如式(2)所示。

$$\begin{cases}\min\ \boldsymbol{c}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{g}}\\ \text{s.t.}\ \ \boldsymbol{P}_{\mathrm{f}}=\boldsymbol{\psi}_{\mathrm{PTDF}}(\boldsymbol{P}_{\mathrm{g}}-\boldsymbol{P}_{\mathrm{d}}-\Delta\boldsymbol{D})\\ \quad\ -\boldsymbol{r}\leqslant\boldsymbol{P}_{\mathrm{f}}\leqslant\boldsymbol{r}\\ \quad\ \boldsymbol{P}_{\mathrm{g}}^{\min}\leqslant\boldsymbol{P}_{\mathrm{g}}\leqslant\boldsymbol{P}_{\mathrm{g}}^{\max}\\ \quad\ \sum_{i=1}^{N}P_{\mathrm{g},i}=\sum_{i=1}^{N}P_{\mathrm{d},i}\end{cases}\tag{2}$$

式中：$\boldsymbol{c}$为系统的发电成本向量；$\boldsymbol{P}_{\mathrm{f}}$为所有线路的潮流向量；$\boldsymbol{\psi}_{\mathrm{PTDF}}$为功率传输分配因子矩阵；$\boldsymbol{r}$为线路潮流上限向量；$\boldsymbol{P}_{\mathrm{g}}^{\min}$、$\boldsymbol{P}_{\mathrm{g}}^{\max}$分别为发电机的最小、最大出力。式中的第1、2个约束条件为潮流约束，用于限制线路潮流；第3、4个约束条件分别为发电机的出力约束和系统功率平衡约束。

当网络攻击者向系统注入精心构造的攻击向量$\Delta\boldsymbol{D}$之后，控制中心会基于被篡改的测量数据发出错误的控制指令，调整发电机的出力。需要注意的是，此时一次侧系统均处于正常的安全运行状态，但是由于控制中心下发了错误的发电机出力分配指令，部分线路的潮流可能越限，造成部分负荷被削减，从而引发停电事件。

1.3　负荷削减模型

如图1所示，当部分线路因潮流越限而退出运行后，为了保证剩余线路的安全运行且不再引发连锁故障，控制中心会进行直流最优负荷削减(DC optimal power flow，DC-OPF)，以确保剩余线路的负荷运行在安全区域内。DC-OPF模型以最小化系统负荷削减总量(控制中心根据上述模型切除的负荷总功率)为优化目标，如式(3)所示。

$$\begin{cases}\min\ \sum_{i=1}^{N}\Delta P_{\mathrm{d},i}\\ \text{s.t.}\ \ \boldsymbol{P}'_{\mathrm{f}}=\boldsymbol{\psi}_{\mathrm{PTDF}}(\boldsymbol{P}_{\mathrm{g}}-\boldsymbol{P}'_{\mathrm{d}}+\Delta\boldsymbol{P}_{\mathrm{d}})\\ \quad\ -\boldsymbol{r}\leqslant\boldsymbol{P}'_{\mathrm{f}}\leqslant\boldsymbol{r}\\ \quad\ \sum_{i=1}^{N}\left(\boldsymbol{P}'_{\mathrm{d},i}-\Delta\boldsymbol{P}_{\mathrm{d},i}\right)=\sum_{i=1}^{N}P_{\mathrm{g},i}\\ \quad\ \boldsymbol{P}_{\mathrm{g}}^{\min}\leqslant\boldsymbol{P}_{\mathrm{g}}\leqslant\boldsymbol{P}_{\mathrm{g}}^{\max}\\ \quad\ 0\leqslant\Delta\boldsymbol{P}_{\mathrm{d}}\leqslant\boldsymbol{P}'_{\mathrm{d}}\end{cases}\tag{3}$$

式中：$\Delta \boldsymbol{P}_{\mathrm{d}}=[\Delta P_{\mathrm{d},1}, \Delta P_{\mathrm{d},2}, \cdots, \Delta P_{\mathrm{d},N}]$为负荷削减量向量，$\Delta P_{\mathrm{d},i}$为节点$i$处的负荷削减量；$\boldsymbol{P}'_{\mathrm{f}}$为负荷削减后的线路潮流；$\boldsymbol{P}'_{\mathrm{d}}=[P'_{\mathrm{d},1}, P'_{\mathrm{d},2}, \cdots, P'_{\mathrm{d},N}]$为被篡改后的负荷功率向量，$\boldsymbol{P}'_{\mathrm{d}}=\boldsymbol{P}_{\mathrm{d}}+\Delta \boldsymbol{D}$，$P'_{\mathrm{d},i}$为节点$i$处被篡改后的负荷功率。

2 攻击向量分类方法

根据网络攻击对电网威胁程度的不同，本文将网络攻击分为无损（non-destructive，ND）攻击、轻度（minor-destructive，MD）攻击、严重（severe-destructive，SD）攻击3种类别。当网络攻击者向电网注入ND攻击时，不会造成线路潮流越限和负荷削减；当向电网注入MD攻击时，会造成部分线路潮流越限，但不会造成负荷削减；当向电网注入SD攻击时，会在引发线路潮流越限的同时导致负荷削减，造成停电事故。为了检测系统所遭受的网络攻击程度，本文提出了一种基于DeepWalk算法的网络攻击分类方法。

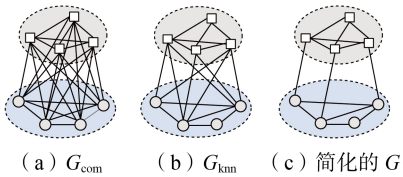
DeepWalk算法是一种基于随机游走的图嵌入算法，该算法能够将复杂网络中的节点表示为低维向量，而这些低维向量可作为机器学习算法的输入被广泛用于节点分类[12-13]。为了获得适用于DeepWalk算法处理的数据，可借鉴自然语言处理中文本分类的思路[14]，将网络攻击场景用一个无向无权的复杂图$G=(V, E)$表示，其中V为复杂图G中的节点集合，每个节点代表ND、MD、SD攻击场景（即控制中心接收到的系统状态量，本文中为注入母线的有功功率），E为节点之间的关联边集合。

2.1 批量边随机删减策略

为了描述复杂图G中节点之间的关联关系，本文提出了批量随机边删减策略，如图2所示。该策略主要包含以下3个步骤。

步骤1：构建描述网络攻击场景两两之间相关关系的全连接图G_{com}。在G_{com}中，每个节点代表1个网络攻击场景，两两节点之间均用1条权重值为节点之间相关系数的边连接。本文采用Kendall计算节点之间的相关系数[15]，相关分析见第4节。

步骤2：第一次边删减。考虑到G_{com}是一个全连接网络，过于冗余的图不仅会导致计算负担过重，还会因算法的过拟合而降低算法分类的准确性。因此，本文基于k-最邻近节点思路对G_{com}进行第一次边删减。在保证网络连通的前提下，只随机保留与每个节点关联程度最高的k个邻居节点的边，删除其他边，由保留的边和节点组成G_{knn}。



（a）G_{com}　（b）G_{knn}　（c）简化的G

图2 批量边随机删减策略

Fig.2 Batch random edge reduction strategy

步骤3：第二次边删减。虽然第一次边删减大幅降低了网络的冗余度，但并未对不同类型节点之间的边进行区分，需进行第二次边删减。针对G_{knn}中的每个节点，完全保留同类型节点之间的连接边，并以保证网络连通为前提，随机删除不属于同类型节点之间的边，将所有保留的边的权重值设置为1，最终获得简化的图G。

2.2 DeepWalk算法

DeepWalk算法的核心思想是通过随机游走算法对网络中的节点进行采样，并将采样序列当作语料送入SkipGram中进行学习，从而实现将连通图中节点映射至低维向量空间，且该空间能保证相似节点之间的距离尽可能接近[12]。本文采用DeepWalk算法将图G中的节点映射为低维映射矩阵$\boldsymbol{X}_V \in \mathbf{R}^{n\times d}$（$n$为节点数，$d$为低维向量的维度），并将$\boldsymbol{X}_V$作为机器学习算法如逻辑回归（logistic regression，LR）[16]的输入，完成节点的分类任务。

为了获得G中节点的低维映射矩阵$\boldsymbol{X}_V$，DeepWalk算法利用虚拟粒子在G中节点之间进行随机游走，获得大量的随机游走序列W_{v_1}。$W_{v_1}=\{v_1, v_2, \cdots, v_q\}$为以节点$v_1$为游走原点的随机游走序列，$q$为游走节点数。参考用于自然语言处理的Word2vec算法[17]，DeepWalk算法通过式（4）所示最大化观察到节点v_i的概率来训练获得$\boldsymbol{X}_V$的模型。

$$\max\left\{p_{\mathrm{r}}\left(v_i \middle| (v_1, v_2, \cdots, v_{i-1})\right)\right\} \tag{4}$$

式中：$p_{\mathrm{r}}\left(v_i \middle| (v_1, v_2, \cdots, v_{i-1})\right)$为游走粒子经过游走序列$(v_1, v_2, \cdots, v_{i-1})$后到达节点$v_i$的概率。

由于DeepWalk算法通过训练潜在的映射函数$\varphi: v\in V \mapsto \boldsymbol{X}_V$而非$v$，将$G$中的节点映射为低维向量，故式（4）可进一步表示为：

$$\max\left\{p_{\mathrm{r}}\left(v_i \middle| (\varphi(v_1), \varphi(v_2), \cdots, \varphi(v_{i-1}))\right)\right\} \tag{5}$$

为了改善生成的低维向量，借助SkipGram模型[17]，利用游走序列中的各节点来预测其左右节点。因此，式（4）可进一步转化为：

$$\min\left\{-\ln p_{\mathrm{r}}\left(\{v_{i-w}, v_{i-w+1}, \cdots, v_{i-1}, v_{i+1}, v_{i+2} \cdots, v_{i+w}\} \middle| \varphi(v_i)\right)\right\} \tag{6}$$

式中：w为单侧采样节点数。对所有游走序列中的节点进行如式（6）所示的训练后，即可得到由节点转化为低维向量的映射函数φ，如式（7）所示。

$$\varphi=\varphi+\eta\frac{\partial \ln p_{\mathrm{r}}\left(u_k \middle| \varphi(v_j)\right)}{\partial \varphi} \tag{7}$$

式中：$u_k \in W_{v_i}[j-w:j+w]$，$W_{v_i}[j-w:j+w]$为游走序列

W_{v_i}的第 $j-w$ 个至第 $j+w$ 个元素；$v_j \in W_{v_i}$，W_{v_i}为以节点v_i为游走原点的游走序列；η为学习率。在训练获得映射函数φ之后，便可获得节点的低维映射矩阵$\boldsymbol{X}_V$，并将其作为LR算法的输入对网络中的节点进行分类。

3　FDIA分类流程

本文所提基于DeepWalk算法的FDIA分类方法的流程图如图3所示。

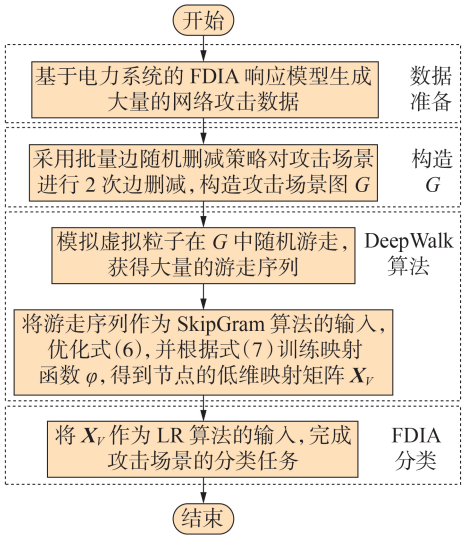


图3　基于DeepWalk算法的FDIA分类方法的流程图

Fig.3　Flowchart of FDIA classification method based on DeepWalk algorithm

4　算例分析

在MATLAB R2021a仿真环境下，对不同负荷水平下IEEE 39节点系统对FDIA的响应情况进行仿真分析；在Python 3.6环境中，将获得的攻击场景数据输入FDIA分类方法流程中，实现对FDIA严重程度的分类。仿真电脑配置为AMD Ruzen Core 52600-3.4 GHz处理器，16 GB RAM。

4.1　FDIA对电网运行的影响

首先仿真IEEE 39节点系统对FDIA的响应情况，分析FDIA对系统的危害。图4描述了测试系统在不同的负荷水平条件（负荷有功功率$P_d=\delta P_{d,0}$，其中$P_{d,0}$为系统的初始负荷，δ为负荷水平因子）下系统的负荷削减量，图中的每个数据点表示攻击者在相应负荷水平条件下造成系统失负荷量最大的攻击情况。由图可知：随着系统负荷水平的提高，系统在FDIA下的负荷削减量和负荷削减率都不断增大；当系统处于高负荷水平（$\delta=1.1$）时，系统负荷削减率达到8.46%，此时的负荷削减量是初始负荷水平条件下系统负荷削减量的8.29倍。分析结果表明：FDIA会对系统的安全运行造成严重威胁；当系统处于高负荷水平时，甚至有可能引发更严重的停电事故。因此，加强对FDIA等网络攻击的重视和防范，对电力系统的安全运行至关重要。

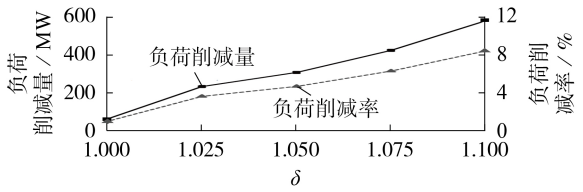


图4　系统在不同负荷水平下遭受FDIA时的负荷削减量

Fig.4　Load shedding of system under different load levels against FDIA

4.2　FDIA分类

根据所建电力系统的FDIA响应模型，仿真获得大量的网络攻击、系统响应样本，以便为分类算法提供足够多的攻击样本。本文共仿真获得4 397个样本数据，其中ND、MD、SD攻击的占比分别为35.8%（1 574个样本）、28.7%（1 262个样本）、35.5%（1 561个样本）。

根据样本点之间的相关系数确定节点之间的边权重值大小，进而构建G_{com}。节点对类别一致率与其相关系数大小之间的关系如图5所示。由图可知，只有采用Kendall相关系数时，节点对类别一致率的变化与相关系数呈正相关关系，故选用Kendall相关系数描述节点之间的相关系数。分别构建G_{knn}和G，G中边的条数比G_{knn}中边的条数减少了31.82%，这大幅降低了网络的冗余度，提高了DeepWalk算法的游走效率。

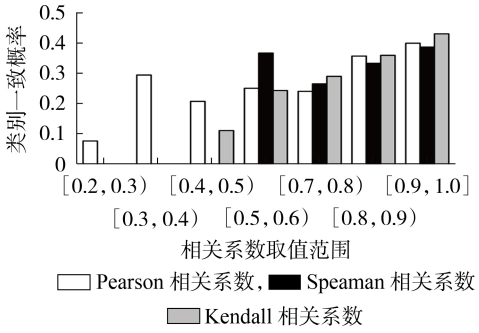


图5　节点对类别一致率与其相关系数大小之间的关系

Fig.5　Relationship between probability of sample pair with same label and its correlation coefficient

在上述工作的基础上，将G作为本文所提分类算法的输入用于实现样本点的分类。为了验证本文所提算法的有效性，将其与常用的分类算法（LR算法）和图嵌入算法（LINE算法、SDNE算法）进行比较。其中，LR算法是基于LR的机器学习算法[16]，LINE算法[18]和SDNE算法[19]是基于神经网络的图嵌入算法。对于LR算法，可直接将样本原始数据（控制中心接收的系统各节点注入有功功率）作为其

输入，获得分类结果；其他3种分类算法的输入为G。为了比较各算法的分类效果，本文采用准确率(ζ_{ACC})和F1值(ζ_{F1})来评价分类效果，ζ_{ACC}和ζ_{F1}的计算式分别为[16]：

$$\zeta_{ACC}=\frac{\lambda_{TP}+\lambda_{TN}}{\lambda_{TP}+\lambda_{TN}+\lambda_{FP}+\lambda_{FN}} \tag{8}$$

$$\zeta_{F1}=\frac{2\lambda_{TP}}{2\lambda_{TP}+\lambda_{FP}+\lambda_{FN}} \tag{9}$$

式中：λ_{TP}、λ_{FP}、λ_{FN}、λ_{TN}分别为对的正样本、错的正样本、错的负样本、对的负样本的个数。

4种分类算法对FDIA的分类结果如图6所示。由图可知：输入数据经过批量边随机删减策略的预处理后，3种图嵌入算法的分类效果明显优于LR算法，相较于LR算法，LINE、SDNE、DeepWalk算法的ζ_{ACC}分别提高了3.36%、12.90%、15.18%；本文所提批量边随机删减策略能有效地提升FDIA的分类效果，相比于LINE、SDNE算法，基于DeepWalk算法的FDIA分类方法的分类效果最优，其ζ_{ACC}和ζ_{F1}分别高达95.00%、95.02%，表明DeepWalk算法对G中节点的分类有明显的优势。上述对比结果很好地验证了本文所提基于DeepWalk算法的FDIA分类方法的有效性和优越性，这为电力系统运行人员辨识、分类、处理FDIA提供了很好的技术支持。

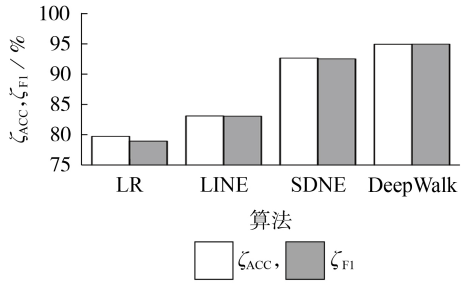


图6 4种分类算法的FDIA分类结果

Fig.6 FDIA classification results of four algorithms

4.3 FDIA分类结果可视化

为了更加直观地对比3种基于图嵌入算法的分类方法对FDIA的分类效果，对这3种算法的分类结果进行可视化处理，如附录A图A1所示。图A1(a)中有大量的蓝色节点被橙色节点和绿色节点遮挡，这表明LINE算法未能对3类节点进行很好的聚类；图A1(b)中节点之间的遮挡现象较少，但是聚类效果明显不如图A1(c)，即相较于SDNE算法，DeepWalk算法对节点聚类的可视化效果更优秀。上述结果表明，相较于其他2种降维算法，基于DeepWalk算法的FDIA分类方法的分类效果最佳。

5 结论

本文构建了电力系统对FDIA的响应模型，提出了基于DeepWalk算法的FDIA严重程度分类方法，所得结论如下：

1)对电力系统FDIA响应模型的数值仿真结果表明，电力系统的负载率越高，受到FDIA时的失负荷比例越高；

2)基于本文所提批量边随机删减策略的数据预处理方法能有效地提高FDIA分类方法的分类准确率；

3)本文所提基于DeepWalk算法的FDIA分类方法能很好地实现对FDIA严重程度的分类任务，其ζ_{ACC}、ζ_{F1}分别高达95.00%、95.02%，高于其他3种对比分类方法。

附录见本刊网络版(http://www.epae.cn)。

参考文献：

[1] LIU Y G, GAO S B, SHI J, et al. Pre-overload-graph-based vulnerable correlation identification under load redistribution attacks[J]. IEEE Transactions on Smart Grid, 2020, 11(6): 5216-5226.

[2] LIANG G Q, WELLER S R, ZHAO J H, et al. The 2015 Ukraine blackout: implications for false data injection attacks [J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317-3318.

[3] 阳育德，蓝水岚，覃智君，等. 电力信息物理融合系统的网络-物理协同攻击[J]. 电力自动化设备，2020，40(2)：97-103.
YANG Yude, LAN Shuilan, QIN Zhijun, et al. Coordinated cyber-physical attacks of cyber-physical power system[J]. Electric Power Automation Equipment, 2020, 40(2): 97-103.

[4] KAVIANI R, HEDMAN K W. A detection mechanism against load-redistribution attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2021, 12(1): 704-714.

[5] 阮振，吕林，刘友波，等. 考虑负荷数据虚假注入的电力信息物理系统协同攻击模型[J]. 电力自动化设备，2019，39(2)：181-187.
RUAN Zhen, LÜ Lin, LIU Youbo, et al. Coordinated attack model of cyber-physical power system considering false load data injection[J]. Electric Power Automation Equipment, 2019, 39(2): 181-187.

[6] WANG Q, TAI W, TANG Y, et al. A two-layer game theoretical attack-defense model for a false data injection attack against power systems[J]. International Journal of Electrical Power & Energy Systems, 2019, 104: 169-177.

[7] MUSLEH A S, CHEN G, DONG Z Y. A survey on the detection algorithms for false data injection attacks in smart grids [J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2218-2234.

[8] KHALAF M, YOUSSEF A, EL-SAADANY E. Joint detection and mitigation of false data injection attacks in AGC systems [J]. IEEE Transactions on Smart Grid, 2019, 10(5): 4985-4995.

[9] JORJANI M, SEIFI H, VARJANI A Y. A graph theory-based approach to detect false data injection attacks in power system AC state estimation[J]. IEEE Transactions on Industrial Informatics, 2021, 17(4): 2465-2475.

[10] BOYACI O, NARIMANI M R, DAVIS K R, et al. Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks[J]. IEEE Transactions on Smart Grid, 2022, 13(1): 807-819.

[11] 杨奕贤，郭力，王洪达，等. 基于数据驱动的直流微电网虚假数据注入攻击快速防御策略[J]. 电力自动化设备，2021，41(5)：

145-151.
YANG Yixian, GUO Li, WANG Hongda, et al. Fast defense strategy of false data injection attack in DC microgrid based on data-driven[J]. Electric Power Automation Equipment, 2021, 41(5): 145-151.
[12] PEROZZI B, AL-RFOU R, SKIENA S. DeepWalk: online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, USA: ACM, 2014: 701-710.
[13] CUI P, WANG X, PEI J, et al. A survey on network embedding[J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(5): 833-852.
[14] DEFFERRARD M, BRESSON X, VANDERGHEYNST P. Convolutional neural networks on graphs with fast localized spectral filtering[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems. New York, USA: ACM, 2016: 3844-3852.
[15] SCHOBER P, BOER C, SCHWARTE L A. Correlation coefficients: appropriate use and interpretation[J]. Anesthesia and Analgesia, 2018, 126(5): 1763-1768.
[16] SAYGHE A, HU Y, et al. Survey of machine learning methods for detecting false data injection attacks in power systems[J]. IET Smart Grid, 2020, 3(5): 581-595.
[17] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient estimation of word representations in vector space[EB/OL]. [2022-02-14]. https://arxiv.org/abs/1301.3781.
[18] TANG J, QU M, WANG M Z, et al. LINE: large-scale information network embedding[C]//2015 Proceedings of the 24th International Conference on World Wide Web. [S.l.]: Computing Machinery Inc., 2015: 1067-1077.
[19] WANG D X, CUI P, ZHU W W. Structural deep network embedding[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Francisco, California, USA: ACM, 2016: 1225-1234.

作者简介：


连祥龙

连祥龙（1995—），男，博士研究生，主要研究方向为图嵌入技术在电力信息物理系统中的应用（**E-mail**：msxianglonglian@mail.scut.edu.cn）；

唐文虎（1974—），男，教授，博士研究生导师，博士，通信作者，主要研究方向为电力设备智能化、电力系统状态评估和计算机智能及应用（**E-mail**：wenhutang@scut.edu.cn）。

（编辑　陆丹）

Cyber attack classification method of false data injection in power system based on DeepWalk algorithm

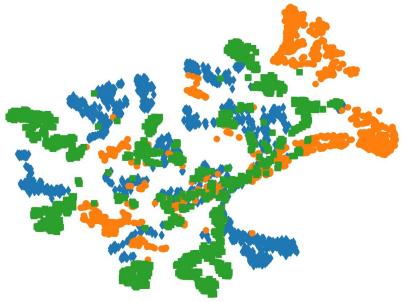
LIAN Xianglong, QIAN Tong, ZHANG Yin, TANG Wenhu
(School of Electric Power Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract: In order to accurately and effectively identify the severity of false data injection attacks (FDIAs) on power grid, a novel FDIA classification method based on DeepWalk algorithm is proposed. According to the characteristics of FDIAs, the response model of power system is constructed. The batch random edge reduction strategy is proposed to construct the attack data generated by the response model as the attack scenario graph. The DeepWalk algorithm is used to map the nodes in the attack scenario graph into low-dimensional vectors, which are used as the inputs of the machine learning algorithm to classify the FDIAs. The simulative results of the IEEE 39-bus system suffering from FDIAs show that the proposed method can accurately and effectively classify FDIAs according to the severity of the damage caused by FDIAs to the power grid.

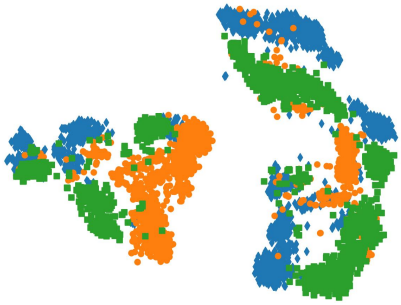
Key words: electric power systems; cyber attack; false data injection attack; DeepWalk algorithm; node classification

附录 A

（a）LINE 算法



（b）SDNE 算法



（c）DeepWalk 算法

绿色、橙色、蓝色节点分别表示 ND、MD、SD 攻击

图 A1　节点分类可视化结果

Fig.A1　Visualization results of node classification