基于双马尔科夫链的新型能源互联网虚假数据注入攻击检测

杨 杉,谭 博,郭静波
(清华大学 电机工程与应用电子技术系,北京 100084)

摘要:新型能源互联网中各环节信息的高度融合和开放削弱了其防御外界攻击的能力。针对具有隐蔽性特征的虚假数据注入攻击(FDIA),提出了适用于新型能源互联网的基于双马尔科夫链的FDIA检测方法。考虑到新型能源互联网的FDIA原理、特征以及新型能源互联网包含大量的测量数据和多变的运行状态,将待检测的数据映射到2个不同的状态空间,并生成2个不同的马尔科夫链模型;根据该模型估计所得的能源互联网运行状态的精确度,生成FDIA的检测器。通过实验案例验证所提检测方法的正确性和有效性。实验结果表明:所提FDIA检测方法具有优秀的检测概率和较少的检测计算量,检测概率可达98.60%,虚警概率仅为1.35%,计算量相比于支持向量机方法降低了1个数量级,能满足新型能源互联网的应用要求。

关键词:新型能源互联网;信息安全;攻击检测;虚假数据注入攻击;马尔科夫链
中图分类号:TM 761 **文献标志码**:A DOI:10.16081/j.epae.202101001

0 引言

以信息系统和能量系统深度融合为特征的新型能源互联网是电力信息物理系统发展过程中的一次重大进展[1-3]。新型能源互联网能更加充分有效地发挥信息融合带来的优势,但如何保证信息的安全是实现能源互联网安全运行的首要问题。然而,数据驱动的新型能源互联网依赖于海量数据的开放共享,这样带来了更多的信息安全隐患,导致新型能源互联网更容易受到网络攻击。其中,虚假数据注入攻击(FDIA)[4-5]基于状态估计中不良数据检测方法的漏洞而生成,具有隐蔽性特征,能对能源互联网的监测数据进行篡改,破坏其信息的完整性和正确性,实现误导控制系统和调度人员做出错误决策的目的。若不能及时准确地检测FDIA,会严重影响能源互联网的正常运行。因此,研究适用于新型能源互联网的FDIA检测方法具有重要的现实意义。

目前,已有一些从不同角度实现的FDIA检测方法。文献[6-7]利用矩阵分解方法检测FDIA,根据攻击者的攻击能力有限所导致的虚假数据趋向于稀疏而正常情况下测量数据是连续平稳的这一特点,将虚假数据检测问题视为一个矩阵分解问题,从而实现检测。文献[8-9]利用相关性分析方法检测FDIA。其中,文献[8]将控制变量、量测量分别定义为因变量、主变量,然后计算主变量发生变化时因变量与主变量间的关联度,以此作为判断是否存在FDIA的依据;文献[9]计算量测变化序列间的关联度范围,根据关联度差异判别系统量测是否受到FDIA。文献[10-11]利用支持向量机(SVM)原理研究了FDIA的检测方法,根据SVM的分类学习能力,生成区分有攻击和无攻击的数据训练样本的分类超平面,并构建了基于该分类模型的FDIA检测方法。文献[12-13]利用神经网络模型建立FDIA检测模型。其中,文献[12]引入离散小波变换用于提取给定时间周期内系统状态的特征,采用深度神经网络建立特征中时空信息的学习模型,根据该模型提出了识别FDIA的检测方法;文献[13]将门控循环单元结构加入卷积神经网络的全连接层之前,建立了一种混合神经网络对电网历史量测数据进行训练,同样提取数据的空间和时间特征以实现对FDIA的检测。

然而,目前电力系统的FDIA检测方法并不能直接应用于新型能源互联网,主要存在以下问题:①新型能源互联网的信息感知更广、更深,输电网以及配电网皆可得到信息的全面感知;②大部分关于FDIA检测方法的研究基于数据的学习训练模型,不仅计算量大,而且检测精度也容易受到训练数据的影响;③新型能源互联网先进的测量、传感、通信技术要求数据之间的交互速度更快以及系统的调度周期更短。因此,为了保障新型能源互联网的安全运行,需要研究兼具检测精度和检测速度的FDIA检测方法。

新型能源互联网含有高比例的随机性电源(光伏发电、风力发电)和随机性用电负荷(电动汽车、智能电器)。因此,本文从随机过程的角度研究新型能

收稿日期:2020-08-22;**修回日期**:2020-11-04
基金项目:国家自然科学基金资助项目(51677094);国家电网有限公司总部科技项目(面向5G的信息能源融合技术与装备研制)
Project supported by the National Natural Science Foundation of China(51677094) and the Science and Technology Program of State Grid Corporation of China(Research and Development of 5G Cyber-energy Fusion Technology and Equipment)

源互联网的FDIA检测方法。其中，马尔科夫链[14]的本质是“时间状态转移”，其可以从概率的角度描述能源互联网运行状态之间的关联性和差异性，非常适用于分析FDIA对能源互联网运行状态的影响。利用马尔科夫链计算量少的优势，满足新型能源互联网对FDIA检测速度的要求，通过设计双马尔科夫链以满足新型能源互联网对FDIA检测精度的要求。

本文首先分析了FDIA的原理与特征，明确了FDIA的构建方法；然后，提出基于双马尔科夫链的新型能源互联网的FDIA检测方法，该方法将每个采样时刻生成的庞大测量向量映射到2个距离空间，并生成2个马尔科夫链模型，以适应能源互联网运行状态的多变，同时根据每一个模型估计所得的能源互联网运行状态的精确度生成FDIA检测器；最后，通过一个典型案例对所提检测方法进行验证，进一步说明所提FDIA检测方法能够满足新型能源互联网对检测速度与检测精度的要求。

1 FDIA的原理与特征

新型能源互联网是一个大型的电力信息物理系统[15-16]，信息系统的错误与物理系统的事故密不可分。因此，通过分析FDIA作用于新型能源互联网的原理，结合电力系统固有的不良数据检测方法，得到FDIA的隐蔽性特征，并通过实际情况获得FDIA的多样性特征，保证研究所用的攻击实例满足实际应用要求。

FDIA作用于新型能源互联网的原理如图1所示。当虚假数据向量$\boldsymbol{a}$攻击于新型能源互联网的信息系统时，量测向量$\boldsymbol{Z}$变为$\boldsymbol{Z}+\boldsymbol{a}$，引起状态估计结果$\hat{\boldsymbol{x}}$产生一个状态误差向量$\boldsymbol{c}$，进而引起调度模型生成错误的调度策略控制变量$\boldsymbol{u}'$，最终导致物理系统运行于不正常的状态$\boldsymbol{x}'$。

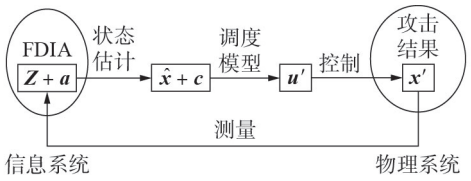


图1 FDIA作用于新型能源互联网的原理图

Fig.1 Schematic diagram of FDIA on new-type energy internet

在实际情况中，测量或者远动系统的随机性扰动会导致量测向量$\boldsymbol{Z}$产生具有随机误差特性的不良数据。不良数据不是攻击，且现有电力系统的状态估计方法已通过$\boldsymbol{r}_{\mathrm{W}}$检测和$\boldsymbol{r}_{\mathrm{N}}$检测，实现了不良数据的检测。具体的不良数据检测方法如下。

计算第i个量测的残差r_i、加权残差$r_{\mathrm{W}i}$和正则化残差$r_{\mathrm{N}i}$，计算表达式分别如式(1)—(3)所示[17]。

$$r_i = z_i - h_i(\hat{\boldsymbol{x}}) \tag{1}$$

$$r_{\mathrm{W}i} = r_i/\sigma_i \tag{2}$$

$$r_{\mathrm{N}i} = r_i/\sigma_{\mathrm{N}i} \tag{3}$$

其中，z_i为第i个量测的值；σ_i为第i个量测的量测误差的标准差；$\sigma_{\mathrm{N}i}$为r_i的标准差；$h_i(\hat{\boldsymbol{x}})$为第$i$个量测的估计值，通过将$\hat{\boldsymbol{x}}$(电压幅值$\boldsymbol{U}$和相位$\boldsymbol{\theta}$的估计值)代入量测函数$\boldsymbol{h}(\boldsymbol{\theta},\boldsymbol{U})$获得。具体的量测函数$\boldsymbol{h}(\boldsymbol{\theta},\boldsymbol{U})$包括支路有功功率量测函数$\boldsymbol{P}_{ij}(\boldsymbol{\theta},\boldsymbol{U})$、支路无功功率量测函数$\boldsymbol{Q}_{ij}(\boldsymbol{\theta},\boldsymbol{U})$、节点注入有功功率量测函数$\boldsymbol{P}_i(\boldsymbol{\theta},\boldsymbol{U})$、节点注入无功功率量测函数$\boldsymbol{Q}_i(\boldsymbol{\theta},\boldsymbol{U})$及节点电压幅值量测函数$\boldsymbol{U}_i$，如式(4)所示。

$$\boldsymbol{h}(\boldsymbol{\theta},\boldsymbol{U}) = \begin{bmatrix} \boldsymbol{P}_{ij}(\boldsymbol{\theta},\boldsymbol{U}) \\ \boldsymbol{Q}_{ij}(\boldsymbol{\theta},\boldsymbol{U}) \\ \boldsymbol{P}_i(\boldsymbol{\theta},\boldsymbol{U}) \\ \boldsymbol{Q}_i(\boldsymbol{\theta},\boldsymbol{U}) \\ \boldsymbol{U}_i \end{bmatrix} \tag{4}$$

式(4)是非线性方程组，在输电网中可忽略方程中的电阻分量，将其近似处理为线性方程组。然而对于电压等级较低的配电网而言，其电阻分量不应忽略。因此，考虑到新型能源互联网的应用需求，本文不忽略电阻分量。

若残差计算结果满足式(5)，则说明量测向量中存在不良数据。

$$\max\left\{\left|r_{\mathrm{W}i}\right|\right\} > \delta_{\mathrm{tr1}} \text{ 或 } \max\left\{\left|r_{\mathrm{N}i}\right|\right\} > \delta_{\mathrm{tr2}} \tag{5}$$

其中，δ_{tr1}和δ_{tr2}分别为$\boldsymbol{r}_{\mathrm{W}}$检测和$\boldsymbol{r}_{\mathrm{N}}$检测的阈值。

隐蔽性是FDIA的重要特征，其来源于不良数据检测方法的漏洞。当不含虚假数据$\boldsymbol{a}$和含有虚假数据$\boldsymbol{a}$时，残差的计算表达式分别见式(6)和式(7)。

$$\boldsymbol{r}_1 = \boldsymbol{Z} - \boldsymbol{h}(\hat{\boldsymbol{x}}) \tag{6}$$

$$\boldsymbol{r}_2 = \boldsymbol{Z} + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) \tag{7}$$

其中，$\boldsymbol{r}_1$、$\boldsymbol{r}_2$分别为不含、含有虚假数据时的残差向量。

若构造理想攻击向量$\boldsymbol{a}$使其满足式(8)，此时$\boldsymbol{r}_1 = \boldsymbol{r}_2$，导致电力系统的基于残差计算的不良数据检测方法对虚假数据的检测失效。换言之，现有的不良数据检测方法并不适用于FDIA检测。

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}} + \boldsymbol{c}) - \boldsymbol{h}(\hat{\boldsymbol{x}}) \tag{8}$$

同时，具有隐蔽性特征的FDIA表现出多样性的特征。①不完备的攻击能力导致不同的虚假数据具有不同的稀疏程度。将这样的攻击向量设为$\boldsymbol{a}'$，其是一个含有零元素的向量，只能实现对特定量测的攻击。且注入了$\boldsymbol{a}'$的状态估计的残差不能触发不良数据检测，即残差满足式(9)。②不同的FDIA对量测向量$\boldsymbol{Z}$的影响程度不同，导致不同FDIA的攻击强度不同。强度越小的攻击向量所引起的量测向量$\boldsymbol{Z}$的变化量越小，攻击很难被发现。本文所采用的攻击强度P_{a}(单位为dB)的计算表达式如式(10)所示。

$$\max\left\{\left|r_{\mathrm{W}i}\right|\right\} \leqslant \delta_{\mathrm{tr1}} \text{ 且 } \max\left\{\left|r_{\mathrm{N}i}\right|\right\} \leqslant \delta_{\mathrm{tr2}} \tag{9}$$

$$P_{\mathrm{a}}=20\lg\frac{\sum_{i=1}^{m}\left|a_i'\right|/z_i}{m} \tag{10}$$

其中，a_i'为$\boldsymbol{a}'$的元素；m为测量单元的数量。

综上可见，FDIA表现出了固有的隐蔽性特征和多样性特征。为了满足实际应用要求，FDIA的检测方法应能实现对各种FDIA的检测。

2　适用于新型能源互联网的FDIA检测方法

根据马尔科夫链建立能源互联网的运行状态变化模型，分析FDIA所导致的状态变化与正常状态变化规律间的差别，可实现能源互联网FDIA的检测。

为了提高检测的全面性，使FDIA的检测范围能够覆盖具有不同稀疏程度和攻击强度的FDIA，并保证对其中的微弱攻击足够敏感，本文采用2个互补的马尔科夫链对新型能源互联网的运行状态进行建模，解决单一的马尔科夫链模型无法有效区分部分FDIA的问题。因此，为了避免单一马尔科夫链出现检测盲区而导致的误检测问题，应基于新型能源互联网的双马尔科夫链模型生成FDIA检测方法。

2.1　新型能源互联网运行状态的马尔科夫链模型

新型能源互联网中含有很多具有随机变化特征的量测值，分别研究每一个量测的状态变化过程会大幅降低计算效率。能源互联网作为一个整体，其中的各量测值之间是相互影响的。因此，本文将每一采样时刻的量测向量$\boldsymbol{Z}$作为一个整体进行研究。

由式(4)和式(8)可以看出，只要存在攻击向量，量测子向量(支路有功功率量测$\boldsymbol{P}_{ij}$、支路无功功率量测$\boldsymbol{Q}_{ij}$、节点注入有功功率量测$\boldsymbol{P}_i$、节点注入无功功率量测$\boldsymbol{Q}_i$、节点电压幅值量测$\boldsymbol{U}_i$)均会发生变化。因此，为了减少用于检测的数据量，本文选择量测子向量$\boldsymbol{P}_{ij}$、$\boldsymbol{P}_i$构建向量$\boldsymbol{Z}_{\mathrm{D}}$，并用马尔科夫链对$\boldsymbol{Z}_{\mathrm{D}}$的状态变化过程进行建模，分析$\boldsymbol{Z}_{\mathrm{D}}$的状态及其转移规律。

状态空间、一步转移矩阵和初始概率分布向量是建立能源互联网马尔科夫链模型的3个关键要素，它们共同决定了马尔科夫链的性质。

对于状态空间而言，通过计算$\boldsymbol{Z}_{\mathrm{D}}$与规定的基准向量$\boldsymbol{Z}_{\mathrm{B}}$间的欧氏距离$d$表征两者间的相似程度，统一$\boldsymbol{Z}_{\mathrm{D}}$的评价标准；同时考虑到能源互联网具有大量历史量测数据，将距离值接近的量测向量处理为相同的状态，进一步对距离值进行分类，生成状态空间。

根据式(11)计算状态空间中状态S_i所对应距离值的范围。

$$[d_{\min}+(i-1)l,d_{\min}+il]\quad i=1,2,\cdots,N_{\mathrm{S}} \tag{11}$$

其中，N_{S}为状态空间中的状态数量；l为间隔量；$d_{\min}$为所有历史量测数据距离值d的最小值，d的计算表达式如式(12)所示。

$$d=\sqrt{\sum_{n=1}^{N_{\mathrm{Z}}}(Z_{\mathrm{D},n}-Z_{\mathrm{B},n})^2} \tag{12}$$

其中，$Z_{\mathrm{D},n}$、$Z_{\mathrm{B},n}$分别为$\boldsymbol{Z}_{\mathrm{D}}$、$\boldsymbol{Z}_{\mathrm{B}}$中的第$n$个元素；$N_{\mathrm{Z}}$为$\boldsymbol{Z}_{\mathrm{D}}$中的元素数量。

对于一步转移矩阵而言，根据式(11)和式(12)计算得到每个历史量测数据的距离及其对应的状态，求得由状态S_i一步转移到状态S_j的一步转移矩阵$\boldsymbol{P}$，如式(13)所示。

$$\boldsymbol{P}=\left[p_{S_i,S_j}\right] \tag{13}$$

$$p_{S_i,S_j}=N_{ij}/N_i \tag{14}$$

其中，N_{ij}为状态S_i一步转移到状态S_j的样本数量；N_i为处于状态S_i的样本数量。

对于初始概率分布向量而言，将待检测时刻的前一采样时刻作为初始时刻且此时的状态变量为X_0，在历史数据已知的情况下，其初始概率分布向量$\boldsymbol{\pi}(0)$是已知的。$\boldsymbol{\pi}(0)$中元素$\pi_{S_i}(0)$的取值见式(15)。

$$\pi_{S_i}(0)=\begin{cases}1 & X_0=S_i\\ 0 & \text{其他}\end{cases} \tag{15}$$

2.2　基于双马尔科夫链的FDIA检测方法

新型能源互联网FDIA检测的关键在于如何将攻击向量引起的量测变化处理为状态值的明显变化。然而，新型能源互联网的状态变化过程具有随机性、复杂性，导致根据式(11)—(15)建立的单一马尔科夫链对具有不同稀疏程度、攻击强度的攻击向量不敏感，即无法保证检测的全面性，以致检测概率不足。

为了使运行状态变化对FDIA的多样性足够敏感，本文选择了近似互补的2个场景，将其作为基准场景，生成双马尔科夫链。由此，构建基于双马尔科夫链的FDIA检测方法，结构如图2所示。2个基准向量$\boldsymbol{Z}_{\mathrm{B1}}$和$\boldsymbol{Z}_{\mathrm{B2}}$的具体选择流程如图3所示。图3中，$\boldsymbol{P}_{\mathrm{Lh}}$、$\boldsymbol{Q}_{\mathrm{Lh}}$分别为节点负荷的历史有功功率、无功功率；$\boldsymbol{P}_{\mathrm{Lh,max}}$、$\boldsymbol{Q}_{\mathrm{Lh,max}}$分别为节点负荷历史有功功率、无功功率的最大值；$\boldsymbol{P}_{\mathrm{DG}}$为分布式电源的容量；$\boldsymbol{P}_{ij,1}$、$\boldsymbol{P}_{ij,2}$分别为场景1、场景2的支路有功功率；$\boldsymbol{P}_{i,1}$和$\boldsymbol{P}_{i,2}$分别为场景1、场景2的节点注入有功功率。

场景1为电网满负荷且分布式电源输出功率为0的运行工况，反映了重负荷但分布式电源无输出的情况；场景2为电网接入一半负荷且分布式电源满功率输出的运行工况，反映了轻负荷但分布式电源满输出的情况。通过双场景选择基准向量，可以保证各种虚假数据对马尔科夫链模型表征的运行状态产生明显变化，减少误检测的概率。

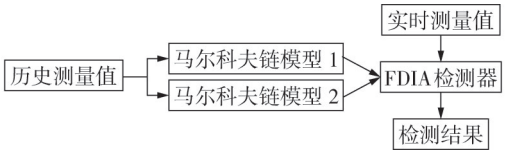


图2　基于双马尔科夫链的FDIA检测方法的结构

Fig.2　Structure diagram of FDIA detection method based on double Markov chains

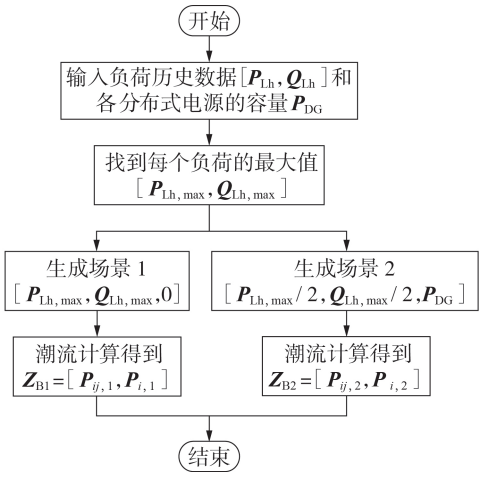


图3 基准向量的选择流程图

Fig.3 Flowchart of selecting reference vectors

对于双模型中的每一个马尔科夫链模型而言，可根据式(11)—(15)、历史数据和不同的基准值分别获得其结果。

根据生成的双马尔科夫链模型，可以求得待检测时刻能源互联网运行状态的概率分布向量$\boldsymbol{\pi}_1$和$\boldsymbol{\pi}_2$，进而对待检测时刻的运行状态求取期望，估计得到待检测时刻的运行状态S_1^E和S_2^E。具体的计算表达式如式(16)—(19)所示。

$$\boldsymbol{\pi}_1 = \boldsymbol{\pi}_1(0)\boldsymbol{P}_1 \tag{16}$$

$$\boldsymbol{\pi}_2 = \boldsymbol{\pi}_2(0)\boldsymbol{P}_2 \tag{17}$$

$$S_1^E = \sum_{n=1}^{N_{S1}} \pi_{1,n} S_{1,n} \tag{18}$$

$$S_2^E = \sum_{n=1}^{N_{S2}} \pi_{2,n} S_{2,n} \tag{19}$$

其中，$\boldsymbol{P}_1$、$\boldsymbol{P}_2$分别为2个马尔科夫链的一步转移矩阵；$\boldsymbol{\pi}_1(0)$、$\boldsymbol{\pi}_2(0)$分别为2个马尔科夫链的初始概率分布向量；N_{S1}、N_{S2}分别为2个马尔科夫链的状态个数；$S_{1,n}$、$S_{2,n}$分别为2个马尔科夫链状态空间中的第n个状态值；$\pi_{1,n}$、$\pi_{2,n}$分别为$\boldsymbol{\pi}_1$、$\boldsymbol{\pi}_2$中的第n个元素。

分别利用2个马尔科夫链模型对历史数据样本进行估计，得到历史状态的估计值分别为$\boldsymbol{S}_{ZB1}^E$和$\boldsymbol{S}_{ZB2}^E$。按照2个不同的基准向量计算得到历史状态的实际值分别为$\boldsymbol{S}_{ZB1}$和$\boldsymbol{S}_{ZB2}$，分别按照式(20)和式(21)计算实际状态与估计状态间的误差值$\boldsymbol{D}_1$和$\boldsymbol{D}_2$。

$$\boldsymbol{D}_1 = \boldsymbol{S}_{ZB1} - \boldsymbol{S}_{ZB1}^E \tag{20}$$

$$\boldsymbol{D}_2 = \boldsymbol{S}_{ZB2} - \boldsymbol{S}_{ZB2}^E \tag{21}$$

$\boldsymbol{D}_1$和$\boldsymbol{D}_2$反映了利用2个不同的马尔科夫链模型估计已知的历史状态的精确度。选取置信区间的范围为95%~99%，在$\boldsymbol{D}_1$和$\boldsymbol{D}_2$中分别找到D_1^*和D_2^*使其分别满足式(22)和式(23)，即$\boldsymbol{D}_1$和$\boldsymbol{D}_2$中有95%~99%元素的绝对值分别不大于D_1^*和D_2^*。这样可以认为能源互联网运行状态的2个马尔科夫链的估计误差区间分别为$[-D_1^*, D_1^*]$和$[-D_2^*, D_2^*]$。

$$95\% \leqslant p\left\{\left|D_{1,n}\right| \leqslant D_1^*, n=1,2,\cdots,N_h\right\} \leqslant 99\% \tag{22}$$

$$95\% \leqslant p\left\{\left|D_{2,n}\right| \leqslant D_2^*, n=1,2,\cdots,N_h\right\} \leqslant 99\% \tag{23}$$

其中，$p\{\cdot\}$表示求事件$\{\cdot\}$发生的概率；N_h为历史数据的采样个数。

利用马尔科夫链模型估计待检测数据状态的精确度与估计历史数据状态的精确度相同，且为了保证检测器对FDIA的多样性足够敏感，生成一个基于估计误差区间$[-D_1^*, D_1^*]$和$[-D_2^*, D_2^*]$的双马尔科夫链能源互联网FDIA检测器，如式(24)所示。

$$\begin{cases} H_0: S_1^E - D_1^* < S_1^T < S_1^E + D_1^* \text{ 且} \\ \quad S_2^E - D_2^* < S_2^T < S_2^E + D_2^* \\ H_1: S_1^T \leqslant S_1^E - D_1^* \text{ 或 } S_1^T \geqslant S_1^E + D_1^* \text{ 或} \\ \quad S_2^T \leqslant S_2^E - D_2^* \text{ 或 } S_2^T \geqslant S_2^E + D_2^* \end{cases} \tag{24}$$

其中，H_0为检测数据正常的假设；H_1为检测数据是虚假数据的假设；S_1^T、S_2^T分别为根据式(11)、(12)计算所得待检测时刻$\boldsymbol{Z}_D$的2个不同基准值条件下的实际状态值。若实际状态值满足假设H_1，说明存在FDIA，即任意一个马尔科夫链判断待检测向量的实际状态(S_1^T, S_2^T)与估计状态(S_1^E, S_2^E)间的误差不满足马尔科夫链模型的正常估计误差区间，则认为存在FDIA。

2.3 基于双马尔科夫链的FDIA检测流程

本文所提基于双马尔科夫链的新型能源互联网FDIA检测方法的具体检测流程如图4所示。

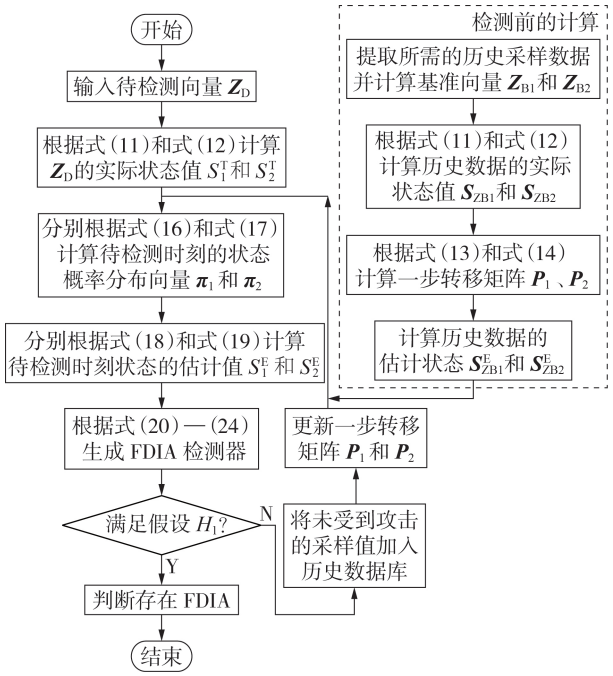


图4 基于双马尔科夫链的FDIA检测流程

Fig.4 Flowchart of detecting FDIA based on double Markov chains

根据检测流程及其自身的特点可知，基于双马尔科夫链的FDIA检测方法非常适用于新型能源互

联网，主要原因有以下三方面：①虽然马尔科夫链利用一定量的历史数据完成能源互联网运行状态的建模，但是在相同历史数据量的情况下，与基于历史数据训练的机器学习方法相比，其计算量明显减少，性能更加优异；②马尔科夫链建模过程中的一步转移矩阵只需在检测前生成一次，并在每一次检测后将新的未受到攻击的采样值加入历史数据库，实时更新一步转移矩阵即可，该过程的计算量明显小于机器学习方法的训练模型更新；③双马尔科夫链模型在实际应用时可以采用并行计算的方法，双链的应用对整体检测时间的影响不大。

3　算例分析

本文采用一个标准的33节点配电网模型（线路和负荷参数参见文献[18]），并在原始网络的基础上加入典型的随机性电源和负荷，改造后的算例结构如图5所示。图中，节点1为系统电源，节点9接入1座电动汽车充电站，节点17和节点32分别接入1台容量为0.5 MW的光伏电源。本文算例基于电网采集的测量数据以及构建的大量虚假数据，验证所提FDIA检测方法的正确性和有效性。

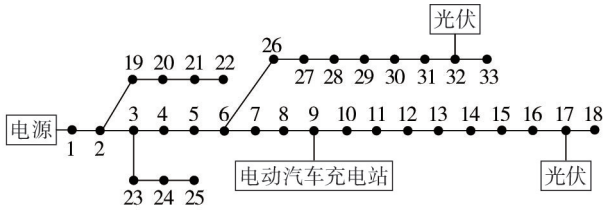


图5　改造后的33节点配电网的拓扑结构

Fig.5　Topology structure of modified 33-bus distribution network

3.1　电网测量数据的生成

电网的测量数据根据负荷、光伏电源、电动汽车充电站的测量数据获得。其中，负荷、光伏电源的测量数据基于美国PJM公司网站给出的WESTERN地区在2019年8月22日到9月20日（共30 d）有功功率量测数据的变化趋势构造而成，有功功率（标幺值，后同）变化曲线见附录中图A1。假设各节点负荷、光伏电源的变化规律与图A1相同，将原始负荷功率、光伏电源功率乘以每个时刻的功率标幺值，构造每5 min一次采样的各节点负荷、光伏电源的测量数据。

电动汽车充电站的测量数据根据电动汽车的负荷特征生成。在已知电动汽车数量、充电功率、续航里程、充电起始时间概率分布函数、日行驶里程概率分布函数等[19]信息的情况下，生成每5 min一次采样的电动汽车充电站的负荷变化曲线，见附录中图A2。其中，模拟的电动汽车的数量为100辆，充电功率为3.5 kW，续航里程为300 km。

根据每5 min一次采样的负荷功率、光伏发电功率、电动汽车充电站负荷功率，使用潮流计算工具计算电网潮流值作为电表记录的测量数据，并在其中加入满足正常数据要求的随机误差，构成163个测量单元（32条支路有功和无功测量、33个节点有功和无功测量、33个节点电压幅值测量）30 d的测量数据。

3.2　电网攻击数据的生成

新型能源互联网中的负荷和电源具有随机性，导致其一天中存在多种状态变化。为了验证所提检测方法在不同时刻的检测性能，本节算例将9月20日的03:00、06:00、09:00、12:00、15:00、18:00、21:00、24:00这8个时刻作为FDIA的注入时刻。

根据FDIA的特征，随机构造一系列虚假数据。为尽量覆盖具有不同攻击强度、稀疏程度的FDIA，分别针对以上8个时刻随机生成8×6 000个隐蔽性攻击向量组$\boldsymbol{a}_1$—$\boldsymbol{a}_8$，攻击强度范围为[−30,5] dB，且每个攻击向量的零元素满足均匀分布，具体零元素在不同时刻的分布情况如图6所示。

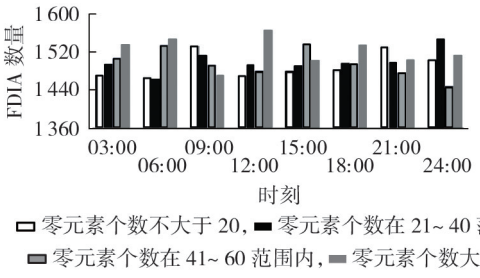


图6　攻击向量零元素的分布情况

Fig.6　Distribution of zero elements in attack vectors

3.3　FDIA检测

利用本文所提检测方法对3.2节生成的大量虚假数据$\boldsymbol{a}_1$—$\boldsymbol{a}_8$进行检测。为了验证本文所提检测方法的检测性能优势，同时采用性能优异的高斯核函数SVM[20]对相同的虚假数据样本$\boldsymbol{a}_1$—$\boldsymbol{a}_8$进行检测。其中，SVM采用相同的历史测量样本，分别针对上述8个时刻生成29个正常数据样本和29个典型的虚假数据样本作为训练样本。

本文所提检测方法的检测关键信息以及2种检测方法的检测概率p_D如表1所示。

表1　检测概率以及检测关键信息

Table 1　Detection probability and detection key information

检测时刻	D_1^*	D_2^*	S_1^E	S_2^E	p_D / %	
					本文方法	SVM方法
03:00	3	2	78	62	99.73	75.32
06:00	3	2	74	66	98.90	74.47
09:00	3	2	94	41	99.88	43.52
12:00	3	2	105	30	98.60	24.78
15:00	3	2	77	58	99.93	43.07
18:00	3	2	28	108	99.98	69.70
21:00	3	2	34	103	99.83	66.18
24:00	3	2	61	78	99.25	76.92

由表1可以看出，本文所提FDIA检测方法在每一个检测时刻的检测概率都优于SVM方法，且最低检测概率可达98.60%（12:00），明显优于SVM方法的最高检测概率76.92%（24:00）。这是因为SVM方法需要同时将正常数据和虚假数据作为训练样本，而虚假数据样本很难尽量覆盖具有不同攻击强度和稀疏程度的虚假数据，导致检测特征提取困难；而本文所提检测方法只需对正常数据样本随时间的状态变化规律进行建模并分析，无需考虑虚假数据样本，减少了虚假数据对检测模型精度的影响。

为了验证使用双马尔科夫链的必要性和正确性，分别计算单马尔科夫链1和单马尔科夫链2对攻击向量组$\boldsymbol{a}_1$—$\boldsymbol{a}_8$（检测关键信息与表1相同）的检测概率，其计算结果均约为90%，小于双链模型的最低检测概率98.60%（12:00），说明双链模型会显著提高检测概率，验证了使用双链的必要性和正确性。

为了验证本文所提检测方法的虚警性能，分别在9月20日的03:00、06:00、09:00、12:00、15:00、18:00、21:00、24:00时刻构造500个满足正常测量误差要求的正常数据，并采用本文所提检测方法进行检测，其中只有1.35%的数据被误判为虚假数据，说明本文所提检测方法有非常优越的虚警性能。

为了验证本文所提检测方法随攻击强度变化的检测性能，计算攻击向量组$\boldsymbol{a}_1$—$\boldsymbol{a}_8$随攻击强度变化的检测概率，结果如图7所示。

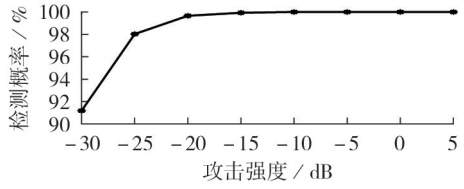


图7 检测概率随攻击强度的变化曲线

Fig.7 Change curve of detection probability vs. attack power

由图7可看出，当FDIA的攻击强度大于−20 dB时，检测概率已达99.66%（接近100%），且在攻击强度非常微弱（−30 dB）时，检测概率也大于90%。说明本文所提FDIA检测方法具有全面性，同时也进一步说明所提检测方法具有非常优越的检测性能。

为了验证本文所提检测方法的计算量优势，分别计算本文所提检测方法和SVM检测方法单次检测过程的计算量，结果对比如表2所示。

表2 2种检测方法的计算量对比

Table 2 Comparison of calculation amount between two detection methods

检测方法	乘法计算量	加法计算量
本文方法	≥398	≥524
SVM方法	≥3944	≥7482

由表2可知，本文所提检测方法的检测计算量较SVM方法减少了1个量级。这是因为SVM方法增加的虚假数据训练样本会增加检测计算量，很难同时满足检测速度、精度的要求；而本文所提检测方法无需考虑虚假数据样本，有效减少了检测计算量。

上述算例结果验证了本文所提FDIA检测方法的正确性、有效性，其优越的检测概率、虚警概率和检测计算量完全满足新型能源互联网的应用要求。

4 结论

对基于双马尔科夫链的新型能源互联网FDIA检测方法进行了研究，基于算例仿真可得如下结论：

（1）利用马尔科夫链对新型能源互联网的运行状态进行建模，以测量向量与基准向量间的欧氏距离生成状态空间，可以很好地描述测量向量间的关联性和差异性，避免了对大量随机性测量数据进行单独分析，提高了检测性能的同时，降低了计算量；

（2）双马尔科夫链模型选择2个不同的运行场景作为基准向量，可保证隐蔽及多样的攻击向量能引起新型能源互联网马尔科夫链模型状态值的明显变化，减少误检测的概率；

（3）算例结果表明，所提检测方法具有优越的检测性能和较少的计算量，检测概率可达98.60%，虚警概率仅为1.35%，计算量相比于SVM降低了1个数量级，完全满足新型能源互联网对FDIA检测准确性和实时性的应用要求。

附录见本刊网络版（http://www.epae.cn）。

参考文献：

[1] 张勇军，陈泽兴，蔡泽祥，等. 新一代信息能源系统：能源互联网[J]. 电力自动化设备，2016，36(9)：1-7，16.
ZHANG Yongjun，CHEN Zexing，CAI Zexiang，et al. New generation of cyber-energy system：energy internet[J]. Electric Power Automation Equipment，2016，36(9)：1-7，16.

[2] 吴克河，王继业，李为，等. 面向能源互联网的新一代电力系统运行模式研究[J]. 中国电机工程学报，2019，39(4)：966-979.
WU Kehe，WANG Jiye，LI Wei，et al. Research on the operation mode of new generation electric power system for the future energy internet[J]. Proceedings of the CSEE，2019，39(4)：966-979.

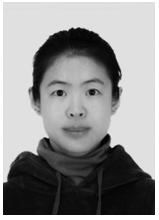
[3] 江秀臣，刘亚东，傅晓飞，等. 输配电设备泛在电力物联网建设思路与发展趋势[J]. 高电压技术，2019，45(5)：1345-1351.
JIANG Xiuchen，LIU Yadong，FU Xiaofei，et al. Construction ideas and development trends of transmission and distribution equipment of the ubiquitous power Internet of Things[J]. High Voltage Engineering，2019，45(5)：1345-1351.

[4] LIU Y，NING P，REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security，2011，14(1)：1-33.

[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] LIU L C,ESMALIFALAK M,DING Q F,et al. Detecting false data injection attacks on power grid by sparse optimization [J]. IEEE Transactions on Smart Grid,2014,5(2):612-621.
[7] HAO J P,PIECHOCKI R J,KALESHI D,et al. Sparse malicious false data injection attacks and defense mechanisms in smart grids[J]. IEEE Transactions on Industrial Informatics,2015,11(5):1-12.
[8] ZHANG Z D,WANG Y F,XIE L B. A novel data integrity attack detection algorithm based on improved grey relational analysis[J]. IEEE Access,2018,6:73423-73433.
[9] 苑开波,罗萍萍,王高猛,等. 基于灰色关联分析法的电力系统隐蔽性数据攻击检测新方法[J]. 电工电能新技术,2019,38(1):17-23.
YUAN Kaibo,LUO Pingping,WANG Gaomeng,et al. A new method of power system false data attack detection based on grey relational analysis[J]. Advanced Technology of Electrical Engineering and Energy,2019,38(1):17-23.
[10] ESMALIFALAK M,LIU L C,NGUYEN N,et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal,2017,11(3):1644-1652.
[11] OZAY M,ESNAOLA I,YARMAN VURAL F T,et al. Machine learning methods for attack detection in the smart grid [J]. IEEE Transactions on Neural Networks and Learning Systems,2016,27(8):1773-1786.
[12] YU J J Q,HOU Y H,LI V O K. Online false data injection attack detection with wavelet transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics,2018,14(7):3271-3280.
[13] 李元诚,曾婧. 基于改进卷积神经网络的电网假数据注入攻击检测方法[J]. 电力系统自动化,2019,43(20):97-104.
LI Yuancheng,ZENG Jing. Detection method of false data injection attack on power grid based on improved convolutional neural network[J]. Automation of Electric Power Systems,2019,43(20):97-104.
[14] COGBURN R. Markov chains in random environments: the case of Markovian environments[J]. The Annals of Probability,1980,8(5):908-916.
[15] 王东芳,刘水源,张勇军,等. “互联网+”形势下电力信息物理融合发展研究综述与展望[J]. 电力自动化设备,2020,40(6):90-99.
WANG Dongfang,LIU Shuiyuan,ZHANG Yongjun,et al. Review and prospect of cyber-physical development of power system under background of “Internet+” technology[J]. Electric Power Automation Equipment,2020,40(6):90-99.
[16] 陈柯任,文福拴,赵俊华,等. 考虑物理-信息虚拟连接的电力信息物理融合系统的脆弱性评估[J]. 电力自动化设备,2017,37(12):67-72,79.
CHEN Keren,WEN Fushuan,ZHAO Junhua,et al. Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections[J]. Electric Power Automation Equipment,2017,37(12):67-72,79.
[17] 吴文传,张伯明,孙宏斌. 电力系统调度自动化[M]. 北京:清华大学出版社,2011:117-123.
[18] 王守相,王成山. 现代配电系统分析[M]. 2版. 北京:高等教育出版社,2014:245-247.
[19] 田立亭,史双龙,贾卓. 电动汽车充电功率需求的统计学建模方法[J]. 电网技术,2010,34(11):126-130.
TIAN Liting,SHI Shuanglong,JIA Zhuo. A statistical model for charging power demand of electric vehicles[J]. Power System Technology,2010,34(11):126-130.
[20] 李航. 统计学习方法[M]. 北京:清华大学出版社,2012:115-124.

作者简介:


杨　杉

杨　杉(1986—),女,四川成都人,助理研究员,博士,研究方向为新一代电力系统信息的分析和处理(**E-mail**:yangshan@mail.tsinghua.edu.cn);

谭　博(1988—),男,湖南湘潭人,助理研究员,博士,研究方向为微弱信号检测与估计(**E-mail**:tanbo2019@mail.tsinghua.edu.cn);

郭静波(1960—),男,吉林长春人,教授,博士研究生导师,博士,主要研究方向为智能电网信息安全、信号检测与估计、混沌理论、压缩感知等(**E-mail**:guojb@tsinghua.edu.cn)。

(编辑　陆丹)

Detection of false data injection attack for new-type energy internet based on double Markov chains

YANG Shan,TAN Bo,GUO Jingbo

(Department of Electrical Engineering,Tsinghua University,Beijing 100084,China)

Abstract: The highly integrated and open information in each link of new-type energy internet weakens its ability to defend against external attacks. Aiming at the FDIA(False Data Injection Attack) with the characteristics of concealability,a FDIA detection method available for new-type energy internet is proposed based on double Markov chains. Considering the principle and characteristics of FDIA and a large number of measurement data and changeable operation states in the new-type energy internet,the data to be detected is mapped into two different state spaces and two different Markov chain models are generated. Based on the accuracy of energy internet's operation state estimated by the model,FDIA detector is generated. The correctness and effectiveness of the proposed detection method are verified by experimental cases. The experimental results show that the proposed FDIA detection method has excellent detection probability and less detection computation amount,the detection probability is up to 98.60%,and the false alarm probability is only 1.35%. The calculation amount is reduced by one order of magnitude compared with the support vector machine method,which can meet the application requirements of new-type energy internet.

Key words: new-type energy internet; information security; attack detection; false data injection attack; Markov chain

附　录

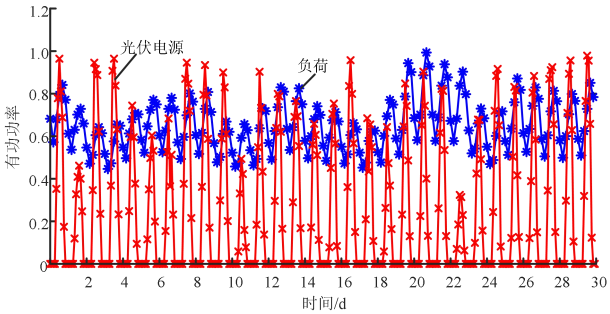


图 A1 WESTERN 地区 2019 年 8 月 22 日至 9 月 20 日有功测量数据的变化趋势

Fig.A1 Change trend of active power measurement data of WESTERN region from August 22 to September 20 in 2019

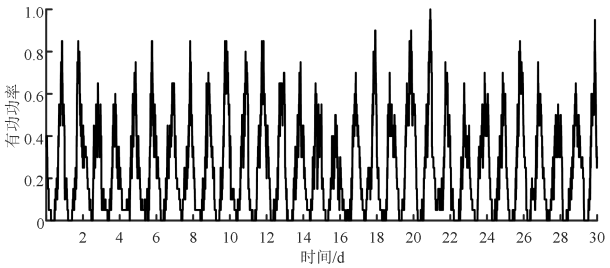


图 A2 电动汽车充电站的负荷曲线

Fig.A2 Load curve of electric vehicle charging station