基于数据驱动的稀疏虚假数据注入攻击

田继伟,王布宏,尚福特,刘帅琦
(空军工程大学 信息与导航学院,陕西 西安 710077)

摘要:提出了一种基于数据驱动的稀疏虚假数据注入攻击策略。攻击策略分为3个阶段:第一阶段,基于稀疏优化技术对窃听的数据进行预处理以剔除异常值;第二阶段,基于平行因子分解算法推断不完整的系统信息矩阵;第三阶段,根据推断的系统矩阵,使用凸优化的方法求解稀疏攻击向量。仿真实验结果表明,当存在异常值时,传统的攻击策略无法成功实施,而所提攻击策略仍能成功地实施稀疏虚假数据注入攻击。

关键词:虚假数据注入;数据驱动;稀疏优化;平行因子分析;凸优化;状态估计
中图分类号:TM 761 **文献标识码**:A DOI:10.16081/j.issn.1006-6047.2017.12.007

0 引言

电力系统是极其关键的基础设施,其安全稳定运行对整个国家和社会的安全稳定发展发挥着至关重要的作用。随着智能电网的建设和发展,越来越多的信息通信技术和设备应用到了电力系统中,这使得现代电力系统越来越"智能化",但同时也使得电力系统面临的网络攻击威胁越来越突出。

状态估计是智能电网能源管理系统EMS(Energy Management System)中的一个关键模块,其通过采集的测量信息对电力系统的运行状态进行估计,状态估计的结果用来完成最优潮流计算、负荷预测和暂态稳定分析等相关分析控制功能。然而,最近的研究表明,状态估计很容易受到一种新型网络攻击——虚假数据注入攻击FDIA(False Data Injection Attack)的威胁。2009年,Liu等[1]首次提出了虚假数据注入攻击的概念,其通过研究表明攻击者在掌握系统信息的情况下可以通过篡改测量信息任意操纵状态估计的结果,而不被状态估计的坏数据检测BDD(Bad Data Detection)模块所发现。虚假数据注入攻击的隐蔽性和攻击后果的严重性,使得其一经提出就受到了大量关注,很多研究者在此基础上对虚假数据注入攻击进行了深入的研究。

由于Liu等提出的虚假数据注入攻击需要2个条件:第一个是攻击者要掌握系统拓扑信息矩阵,第二个是攻击者要控制所有的测量单元,满足这2个条件的攻击者才能达到任意篡改状态估计结果的目的。但上述2个条件在实际情况下都很难达到:系统拓扑信息属于电力系统核心信息,攻击者很难掌握;由于资源和能力限制,攻击者很难控制所有的测量单元。

因此,关于切实可行的虚假数据攻击向量的构造,目前有2条研究的主线。一条主线是研究如何在控制较少测量单元的情况下实施攻击,即低稀疏度的虚假数据注入攻击,该条主线的研究均需要攻击者准确地获取电力系统的测量雅可比矩阵。其中,文献[2]首先提出了用于衡量攻击难度的安全指标,即攻击某一测量单元时需要同时控制并篡改的测量单元的数目,并采用凸优化的方法给出了求得近似解的方法;文献[3]在文献[2]的基础上,进一步研究了部分量测值受到保护时最小攻击向量的构建问题;文献[4]提供了一个在实际电力系统中寻找所有稀疏攻击的有效算法,其根据系统拓扑得到的稀疏攻击仅需要控制2个节点测量单元和极少的线路测量单元;文献[5]对稀疏攻击向量构建问题的研究不仅局限于集中式状态估计模型,还对分布式状态估计模型的情况进行了分析;文献[6]对前人的工作做了进一步改进,使得攻击在保持较高成功率(不被系统检测)的同时,攻击向量的稀疏度更低(控制并篡改的测量单元更少)。另一条主线试图解决如何在不掌握系统拓扑信息矩阵的情况下实施攻击的问题。在攻击者可以获取整个系统量测值的条件下,文献[7]提出采用独立成分分析ICA(Independent Component Analysis)的方法估计测量矩阵,其基本思想是通过寻找一个分离矩阵使得测量数据分解成统计独立的成分。由于上述等效矩阵关联的状态变量为相互独立的负荷,故此时虚假数据注入的攻击对象仅局限于负荷。为了克服该缺点,文献[8]采用主成分分析PCA(Principle Component Analysis)法将传统状态变量映射到低维空间下,削弱传统状态变量之间的相关性,求解低维空间下的等效测量矩阵。由于上述2种方法需要获得系统的所有量测值,导致攻击者的成本过高。文献[9]指出攻击者在获取部分量

收稿日期:2017-05-15;**修回日期**:2017-10-25
基金项目:国家自然科学基金资助项目(61272486);信息安全国家重点实验室开放课题基金资助项目(2014-02)
Project supported by the National Natural Science Foundation of China(61272486) and the Open Project Fund of State Key Laboratory of Information Security(2014-02)

测的情况下,采用子空间方法仍然可以构建攻击向量。虽然以上各种方法可以用来估计系统信息矩阵以实施攻击,但由于大量的测量数据中总会由于各种原因(设备故障、通信故障、数据丢失)出现部分异常值,因此基于测量数据矩阵估计系统信息并实施攻击的方法很可能无法成功地进行。文献[10]对上述情况进行了分析研究,并提出了新的攻击策略以解决上述问题。

上述 2 条主线的研究有着相对独立的发展,本文试图将这 2 条主线的研究相结合,即本文试图解决在不具备系统信息矩阵的情况下,如何通过估计系统信息矩阵进而实施稀疏攻击的问题。虽然文献[11]研究了通过估计系统信息矩阵进而实施稀疏攻击的问题,但是该文献并没有考虑测量数据含有异常值的情况,这将使得该文献提供的攻击策略的成功概率大幅降低。本文将在异常值存在的情况下,解决当不具备系统信息矩阵时,如何通过估计系统信息矩阵进而实施稀疏攻击的问题,以提供更加切实可行的攻击策略。

1　问题描述

1.1　系统模型

电力系统的线性状态估计模型为:

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e} \tag{1}$$

其中,$\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}$ 为量测值;$\boldsymbol{H}$ 为测量雅可比矩阵;$\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$ 为需要估计的状态变量;$\boldsymbol{e}=[e_1,e_2,\cdots,e_m]^{\mathrm{T}}$ 为测量误差。

电力系统状态估计问题以冗余的测量值为基础($\mathrm{rank}(\boldsymbol{H})=n$),可以通过加权最小二乘 WLS(Weighted Least-Squares)获得状态变量的估计值:

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{z} \tag{2}$$

其中,$\boldsymbol{W}$ 为加权矩阵,通常有 $\boldsymbol{W}=\boldsymbol{R}^{-1}$,$\boldsymbol{R}$ 为测量误差 $\boldsymbol{e}$ 的协方差矩阵,即 $\boldsymbol{R}=\mathrm{cov}(\boldsymbol{e})$。

由于状态估计以冗余的测量值为基础,其中的测量值可能含有坏数据或者恶意数据,这就需要检测坏数据并加以剔除,以确保状态估计结果的可靠性。为了消除不良数据对状态估计的影响,以残差方程为基础的不良数据检测方法得到了广泛应用。残差的表达式为:

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{H}(\hat{\boldsymbol{x}}) \tag{3}$$

检测坏数据的判据是:$\|\boldsymbol{r}\|<\tau$,τ 为判断的阈值。如果 $\|\boldsymbol{r}\|<\tau$ 成立,则认为没有坏数据;否则就要剔除相应的坏数据并重新进行状态估计,直到通过坏数据检测为止。

1.2　不可检测攻击

虚假数据注入攻击就是利用了上述检测方法的缺陷,若用 $\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$ 表示攻击者在量测值中注入的虚假数据向量,则实际的测量数据为 $\boldsymbol{z}_{\mathrm{bad}}=\boldsymbol{z}+\boldsymbol{a}$,此时估计的状态变量为 $\boldsymbol{x}_{\mathrm{bad}}=\boldsymbol{x}+\boldsymbol{c}$,其中 $\boldsymbol{c}=[c_1,c_2,\cdots,c_n]^{\mathrm{T}}$ 为由于虚假数据的注入在状态变量中引入的误差向量。此时残差表达式为:

$$\|\boldsymbol{r}\|=\|\boldsymbol{z}_{\mathrm{bad}}-\boldsymbol{H}\boldsymbol{x}_{\mathrm{bad}}\|=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\| \tag{4}$$

显然,当 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$ 时,有下式成立:

$$\|\boldsymbol{r}\|=\|\boldsymbol{z}_{\mathrm{bad}}-\boldsymbol{H}\boldsymbol{x}_{\mathrm{bad}}\|=\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\| \tag{5}$$

此时,采用基于残差的不良数据检测方法无法发现测量数据中的虚假数据,攻击者可以将量测值和状态变量修改为任意值,这将危害电力系统的安全稳定运行。

1.3　低稀疏度不可检测攻击

文献[4]提供了稀疏虚假数据注入攻击的数学定义和相关的推论。

定义 $A=(\Omega,\boldsymbol{a})$ 表示攻击,其中 Ω 为攻击的测量单元集,$\boldsymbol{a}$ 为对应的攻击向量,$a_i\neq0(i\in\Omega)$,即 $\boldsymbol{a}$ 中的非零元素对应 Ω 中的测量单元。Ω 中测量单元的个数为 $|\Omega|=s$,s 即为该攻击的稀疏度,$\|\boldsymbol{a}\|_0=\delta$。用 M 表示所有的测量单元集,$\Theta=M\backslash\Omega$ 表示 Ω 的补集。当攻击向量 $\boldsymbol{a}$ 满足式(6)所示的条件时,则攻击 A 属于稀疏攻击。

$$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}=\begin{bmatrix}\boldsymbol{C}\\ \boldsymbol{U}\end{bmatrix}\boldsymbol{c}=\begin{bmatrix}\boldsymbol{\gamma}\\ 0\end{bmatrix} \tag{6}$$

其中,$\boldsymbol{C}=\boldsymbol{H}(\Omega,:)$;$\boldsymbol{U}=\boldsymbol{H}(\Theta,:)$。

推论 1　当满足下述条件时,攻击 $A=(\Omega,\boldsymbol{a})$ 属于稀疏攻击:

a. $\mathrm{rank}(\boldsymbol{C})\leqslant n-1$;

b. 攻击向量 $\boldsymbol{a}$ 属于子空间,即 $\Psi=\{\boldsymbol{a}\in\mathbf{R}^m:\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c},0=\boldsymbol{U}\boldsymbol{c}\}(\boldsymbol{c}\neq0)$。

上述定义中展示了稀疏攻击中的 2 个关键组成部分:攻击测量单元集合和稀疏攻击向量。推论 1 提供了确定稀疏攻击向量的数学条件。由该数学条件可以看出,该稀疏攻击向量的求解依赖于准确的系统测量雅可比矩阵。可实际情况中,该信息矩阵属于核心信息,将会被系统严加防护,攻击者很难掌握。因此,为了解决该问题,需要研究更加切实可行的稀疏攻击策略。

2　不完整系统矩阵信息下的攻击情况分析

首先,攻击者需要确定攻击的测量单元集合。分别用 $B=\{B_1,B_2,\cdots,B_{n+1}\}$ 和 $F=\{F_{n+2},F_{n+3},\cdots,F_m\}$ 表示系统中所有节点测量单元和线路测量单元的集合。显然,$M=\{B,F\}$。每一个攻击测量集为 $S_i=\{B_l,F_j\}$ $(l\in\{1,2,\cdots,n+1\},j\in\{n+2,n+3,\cdots,m\})$,其中,$B_l$ 为节点 l 的邻近节点测量单元的集合(也包括节点 l 的测量单元);F_j 为节点 j 和邻近节点间线路测量单

元的集合。由于电力系统的稀疏特性,攻击测量单元集合 S_i 满足:$|S_i| \ll m$。尤其值得注意的是,攻击测量单元集合 S_i 仅仅依赖于本地的局部拓扑结构。图1展示了5-稀疏度的攻击测量单元集示意图。

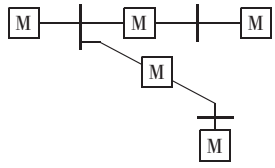


图1 5-稀疏度的攻击测量单元集

Fig.1 Attack meter set with 5-sparseness

然后,攻击者需要构建与攻击测量单元集合 S_i 对应的稀疏攻击向量。将攻击者试图篡改的状态变量值表示为:

$$\boldsymbol{c}_i=[0 \ \cdots \ 0 \ \delta_i \ 0 \ \cdots \ 0]^{\mathrm{T}} \tag{7}$$

其中,δ_i 为非零元素。相应的攻击向量为:

$$\boldsymbol{a}_i=\boldsymbol{H}\boldsymbol{c}_i \tag{8}$$

文献[11]表明,式(8)中攻击向量的稀疏度满足:$\| \boldsymbol{a}_i \|_0=|S_i|=\delta$。而且,$\boldsymbol{a}_i$ 中的非零元素并不需要得知系统的完整矩阵,而仅仅依赖于子矩阵 $\boldsymbol{H}(S_i,:)$。

推论2 每个攻击 $A_i=(S_i,\boldsymbol{a}_i)(i \in \{1,2,\cdots,n+1\})$ 都属于不可检测的稀疏攻击。而且,$A_i=(S_i,\boldsymbol{a}_i)$ 属于不可简化的攻击,即不存在攻击 $\hat{A}_i=(\hat{S}_i,\hat{\boldsymbol{a}}_i)$,$\hat{S}_i \subset S_i$。攻击向量 $\boldsymbol{a}_i$ 可由攻击测量单元集合和相应子矩阵 $\boldsymbol{H}(S_i,:)$ 确定。推论的证明见文献[4]。

上述推论2确保了攻击向量的稀疏性,而且该攻击是不可简化的,即上述攻击中的攻击测量单元集合是最小的攻击测量单元集合。更为关键的是,推论也表明稀疏的攻击向量可以由攻击测量单元集合和不完整系统子矩阵 $\boldsymbol{H}(S_i,:)$ 求得。然而,在实际情况下,不完整系统子矩阵 $\boldsymbol{H}(S_i,:)$ 通常会受到系统的保护,对于攻击者而言仍是未知的。在第3节中,笔者将提供一个全面的攻击策略,基于数据驱动的方式估计系统子矩阵,进而在未知系统子矩阵 $\boldsymbol{H}(S_i,:)$ 的情况下仍能成功地实施稀疏攻击。

3 基于数据驱动的稀疏虚假数据注入攻击

由文献[12]可知,对电力系统中传输的测量数据进行窃听是较为切实可行的攻击手段。本文中,窃听得到的测量数据将用来实施下一步的稀疏虚假数据注入攻击。本文提出的基于数据驱动的稀疏虚假数据注入攻击策略共包括以下3个阶段。

a. 第一阶段:对窃听得到的大量测量数据进行数据预处理。由于设备故障、通信故障、数据丢失等常见的原因,窃听得到的大量数据中难免会含有一些严重的错误,这里将这些严重的错误视为异常值。该阶段将基于稀疏优化技术对数据进行预处理,以剔除异常值,恢复真实准确的测量数据。

b. 第二阶段:根据测量数据识别不完整的系统矩阵。该阶段将采用平行因子分解算法推断不完整的系统矩阵。

c. 第三阶段:根据识别的系统矩阵,建立稀疏攻击优化模型。该阶段将采用凸优化的方法求得稀疏攻击向量。

3.1 攻击第一阶段

含异常值的矩阵可以表示为:

$$\boldsymbol{Z}_{\mathrm{outlier}}=\boldsymbol{Z}+\boldsymbol{E} \tag{9}$$

其中,$\boldsymbol{Z}$ 为原始的低秩矩阵;$\boldsymbol{E}$ 为代表异常值的稀疏矩阵;$\boldsymbol{Z}_{\mathrm{outlier}}$ 为攻击者真实观测到的含有异常值的测量矩阵。攻击者首先需要在测量矩阵 $\boldsymbol{Z}_{\mathrm{outlier}}$ 中对 $\boldsymbol{Z}$ 和 $\boldsymbol{E}$ 进行分离,以便恢复低秩矩阵 $\boldsymbol{Z}$。这可以看成一个典型的低秩矩阵恢复问题。

从数学上而言,将矩阵 $\boldsymbol{Z}_{\mathrm{outlier}}$ 分解为一个低秩矩阵 $\boldsymbol{Z}$ 和一个稀疏矩阵 $\boldsymbol{E}$ 的问题可以由下述优化问题来描述:

$$\begin{cases}\min\limits_{\boldsymbol{Z},\boldsymbol{E}} \ \mathrm{rank}(\boldsymbol{Z})+\lambda \| \boldsymbol{E} \|_0 \\ \text{s.t.} \ \boldsymbol{Z}_{\mathrm{outlier}}=\boldsymbol{Z}+\boldsymbol{E}\end{cases} \tag{10}$$

然而,由于目标函数中 $\mathrm{rank}(\boldsymbol{Z})$ 和 $\| \boldsymbol{E} \|_0$ 都是非线性非凸的组合优化函数,对上述问题的求解是十分困难的。

借鉴压缩感知和矩阵秩最小化方面的研究成果,上述问题可转化为求解下述凸优化问题:

$$\begin{cases}\min \| \boldsymbol{Z} \|_*+\lambda \| \boldsymbol{E} \|_1 \\ \text{s.t.} \ \boldsymbol{Z}_{\mathrm{outlier}}=\boldsymbol{Z}+\boldsymbol{E}\end{cases} \tag{11}$$

在该凸优化问题中,$\| \cdot \|_*$ 和 $\| \cdot \|_1$ 分别表示矩阵的核范数和 L_1 范数,λ 为值大于0的加权参数。本文使用增广拉格朗日乘子法[13]ALM(Augmented Lagrange Multiplier)对该问题进行求解。

增广拉格朗日乘子法可用于求解一般的约束优化问题,函数表达式为:

$$\begin{cases}\min \ f(\boldsymbol{X}) \\ \text{s.t.} \ \boldsymbol{h}(\boldsymbol{X})=0\end{cases} \tag{12}$$

上述问题的目标函数可以表示为一个拉格朗日函数:

$$L(\boldsymbol{X},\boldsymbol{Y},\mu)=f(\boldsymbol{X})+\langle \boldsymbol{Y},\boldsymbol{h}(\boldsymbol{X}) \rangle+\frac{\mu}{2} \| \boldsymbol{h}(\boldsymbol{X}) \|_{\mathrm{F}}^2 \tag{13}$$

其中,μ 为拉格朗日乘子,是一个正的标量。考虑到 $\boldsymbol{X}=(\boldsymbol{Z},\boldsymbol{E})$,$f(\boldsymbol{X})=\| \boldsymbol{Z} \|_*+\lambda \| \boldsymbol{E} \|_1$ 以及 $\boldsymbol{h}(\boldsymbol{X})=\boldsymbol{Z}_{\mathrm{outlier}}-\boldsymbol{Z}-\boldsymbol{E}$,拉格朗日函数可以表示为:

$$L(\boldsymbol{Z},\boldsymbol{E},\boldsymbol{Y},\mu)=\| \boldsymbol{Z} \|_*+\lambda \| \boldsymbol{E} \|_1+\langle \boldsymbol{Y},\boldsymbol{Z}_{\mathrm{outlier}}-\boldsymbol{Z}-\boldsymbol{E} \rangle+\frac{\mu}{2} \| \boldsymbol{Z}_{\mathrm{outlier}}-\boldsymbol{Z}-\boldsymbol{E} \|_{\mathrm{F}}^2 \tag{14}$$

优化过程通过以下2个更新步骤解决:

$$\boldsymbol{Z}_{k+1}=\mathrm{argmin} \ L(\boldsymbol{Z},\boldsymbol{E}_k,\boldsymbol{Y}_k,\mu_k) \tag{15}$$

$$\boldsymbol{E}_{k+1}=\mathrm{argmin} \ L(\boldsymbol{Z}_{k+1},\boldsymbol{E},\boldsymbol{Y}_k,\mu_k) \tag{16}$$

式(15)可以用矩阵 $\boldsymbol{Z}_{\mathrm{outlier}}-\boldsymbol{E}_k+\mu_k^{-1}\boldsymbol{Y}_k$ 的奇异值分

解进行迭代求解。在获得酉矩阵 $\boldsymbol{U}$、$\boldsymbol{V}$ 和矩形对角矩阵 $\boldsymbol{S}$ 后,对 $\boldsymbol{Z}$ 进行更新:

$$\boldsymbol{Z}_{k+1}=\boldsymbol{U}\xi_{\mu_k^{-1}}[\boldsymbol{S}]\boldsymbol{V}^{\mathrm{T}} \tag{17}$$

然后,对 $\boldsymbol{E}$ 进行更新:

$$\boldsymbol{E}_{k+1}=\xi_{\lambda\mu_k^{-1}}[\boldsymbol{Z}_{\text{outlier}}-\boldsymbol{Z}_{k+1}+\boldsymbol{\mu}_k^{-1}\boldsymbol{Y}_k] \tag{18}$$

其中,ξ 为可变阈值函数,其定义如式(19)所示。

$$\xi_\varepsilon[x]=\begin{cases}x-\varepsilon & x>\varepsilon\\ x+\varepsilon & x<-\varepsilon\\ 0 & \text{其他}\end{cases} \tag{19}$$

在每次迭代中同样对 $\boldsymbol{Y}$ 和 μ 进行更新:

$$\boldsymbol{Y}_{k+1}=\boldsymbol{Y}_k+\mu_k(\boldsymbol{Z}_{\text{outlier}}-\boldsymbol{Z}_{k+1}-\boldsymbol{E}_{k+1}) \tag{20}$$

$$\mu_{k+1}=\Psi\mu_k \tag{21}$$

其中,Ψ 为一个正的常量。优化过程将一直持续进行,直到式(22)满足给定的误差限 τ。

$$c_k^{\text{ite}}=\frac{\|\boldsymbol{Z}_{\text{outlier}}-\boldsymbol{Z}_{k+1}-\boldsymbol{E}_{k+1}\|}{\|\boldsymbol{Z}_{\text{outlier}}\|_{\mathrm{F}}}<\tau \tag{22}$$

一旦上述算法收敛,就可成功地恢复原始的测量矩阵 $\boldsymbol{Z}$。

3.2　攻击第二阶段

由于状态变量 $\boldsymbol{x}$ 内在的数据相关性,使得系统模型式(1)并不是一个线性独立的系统。因此,直接基于系统模型式(1)识别系统矩阵的方法并不可取。在文献[7]中,系统模型式(1)首先基于负荷转化为一个线性独立的系统。用 $\boldsymbol{L}=[l_1,l_2,\cdots,l_{l_{\mathrm{d}}}]^{\mathrm{T}}$ 表示系统的负荷变量,其中 l_{d} 为负荷的数量($l_{\mathrm{d}}<n$)。因为系统状态变量 $\boldsymbol{x}$ 与系统负荷变量 $\boldsymbol{L}$ 相关,因此,可用 $\boldsymbol{x}=f(\boldsymbol{L})$ 表示两者之间的非线性关系。不失一般性,$\boldsymbol{L}$ 中的元素是相互独立的,且 $f(0)=0$。对 $\boldsymbol{x}$ 进行泰勒展开:

$$\begin{aligned}\boldsymbol{x}&=f(0)+\boldsymbol{\Gamma}(\boldsymbol{L}-0)+\boldsymbol{o}(\|\boldsymbol{L}-0\|_{\mathrm{F}}^2)=\\ &\boldsymbol{\Gamma}\boldsymbol{L}+\boldsymbol{o}(\|\boldsymbol{L}\|_{\mathrm{F}}^2)\end{aligned} \tag{23}$$

其中,矩阵 $\boldsymbol{\Gamma}$ 为 $f(\boldsymbol{L})$ 在 0 处进行泰勒展开的一阶系数矩阵;$\boldsymbol{o}(\|\boldsymbol{L}\|_{\mathrm{F}}^2)$ 为余项。一般情况下,如果负荷的变化足够小,余项可以忽略不计。因此,系统模型式(1)可转化为:

$$\boldsymbol{z}=\boldsymbol{N}\boldsymbol{L}+\boldsymbol{e} \tag{24}$$

其中,$\boldsymbol{N}=[n_1\ \ n_2\ \ \cdots\ \ n_{l_{\mathrm{d}}}]=\boldsymbol{H}\boldsymbol{\Gamma}\in\mathbf{R}^{m\times l_{\mathrm{d}}}$ 为一个新的系统矩阵。由于负荷 $\boldsymbol{L}$ 是相互独立的,因此式(24)是一个线性独立的系统模型。

系统子矩阵 $\boldsymbol{H}(S_i,:)$ 需要根据收集的测量数据进行识别和推断。基于新的系统模型式(24)估计系统子矩阵 $\boldsymbol{H}(S_i,:)$ 等价于估计新的系统子矩阵 $\boldsymbol{N}(S_i,:)=\boldsymbol{H}(S_i,:)\boldsymbol{\Gamma}$。为了方便表示,在下文的描述中用 $\boldsymbol{N}$ 代替 $\boldsymbol{N}(S_i,:)$,后续将对两者的关系进行补充说明。由于平行因子(Parafac)分解算法可以根据原始变量的信息进行重新组合,找出影响变量的共同因子,化简数据。因此,本文采用平行因子分解算法推断潜在的系统矩阵。平行因子分解算法是一种多维数据的分解方法[14]。首先,假设攻击者收集了 T 个采样时刻的测量数据序列。计算采集数据的高阶累积量(如四阶张量):

$$\hat{\boldsymbol{\Phi}}_{\sigma_1,\sigma_2,\sigma_3,\sigma_4}=\boldsymbol{c}_{\text{um}}(\boldsymbol{z}_{\sigma_1},\boldsymbol{z}_{\sigma_2},\boldsymbol{z}_{\sigma_3},\boldsymbol{z}_{\sigma_4}) \tag{25}$$

其中,σ_1—$\sigma_4=1,2,\cdots,m$;$\boldsymbol{c}_{\text{um}}(\cdot)$ 为分布的矩;$\boldsymbol{z}_{\sigma_1}$、$\boldsymbol{z}_{\sigma_2}$、$\boldsymbol{z}_{\sigma_3}$、$\boldsymbol{z}_{\sigma_4}$ 为 $\hat{\boldsymbol{\Phi}}$ 的 4 个相迎轮廓矩阵。在没有噪声的情况下,式(25)中的四阶张量可以分解为一系列有限个对称的 rank-one 张量的线性组合:

$$\boldsymbol{\Phi}=\sum_{k=1}^{l_{\mathrm{d}}}\boldsymbol{\kappa}_k\times(\boldsymbol{n}_j\circ\boldsymbol{n}_j\circ\boldsymbol{n}_j\circ\boldsymbol{n}_j) \tag{26}$$

其中,$\boldsymbol{\kappa}_k$ 为第 k 个负荷变量的峰度,即 $\boldsymbol{\kappa}_k=\boldsymbol{c}_{\text{um}}(l_j,l_j,l_j,l_j)$;$\boldsymbol{n}_j$ 为分解的张量;"∘"表示张量的外积运算。文献[15]表明,如果 $(m+1)(m+2)(m+3)/4!\geqslant l_{\mathrm{d}}$,式(26)中的分解是唯一的。基于该结论,当负荷数 l_{d} 确定时,可以求得所需窃听测量单元的最少数目 $f_{\min}$(实际选择时,通常要大一些),如表 1 所示。

表 1　l_{d} 与 $f_{\min}$ 的关系

Tabel 1　Relationship between l_{d} and $f_{\min}$

l_{d}	$f_{\min}$	l_{d}	$f_{\min}$	l_{d}	$f_{\min}$
5	3	14	5	30	7
8	4	21	6	41	8

通常,式(26)的分解可以表示为一个约束最小化问题,即:

$$\begin{cases}\min\limits_{\boldsymbol{\Phi}}\ \|\hat{\boldsymbol{\Phi}}-\boldsymbol{\Phi}\|_{\mathrm{F}}^2\\ \text{s.t.}\quad \boldsymbol{\Phi}=\sum\limits_{k=1}^{l_{\mathrm{d}}}\boldsymbol{\kappa}_k\times(\boldsymbol{n}_j\circ\boldsymbol{n}_j\circ\boldsymbol{n}_j\circ\boldsymbol{n}_j)\end{cases} \tag{27}$$

上述问题可以通过交替最小二乘 ALS(Alternating Least Squares)[16]法计算求解。用 $\hat{\boldsymbol{N}}$ 表示从式(27)中求得的对系统矩阵 $\boldsymbol{N}$ 的估计值,则:

$$\hat{\boldsymbol{N}}=\boldsymbol{N}\boldsymbol{\Pi}\boldsymbol{\Lambda} \tag{28}$$

其中,$\boldsymbol{\Pi}$ 为置换矩阵;$\boldsymbol{\Lambda}$ 为对角矩阵。文献[7]中指出,这些微小的不确定性对系统矩阵识别没有影响。

3.3　攻击第三阶段

攻击的最终目标是根据估计的系统矩阵 $\hat{\boldsymbol{N}}$ 求得与攻击测量单元集 S_i 对应的攻击向量。基于式(24)的新模型,与式(8)对应的攻击向量为:

$$\boldsymbol{a}_i=\hat{\boldsymbol{N}}\boldsymbol{l} \tag{29}$$

其中,$\boldsymbol{l}\in\mathbf{R}^{l_{\mathrm{d}}}$ 为负荷的变化量。$\boldsymbol{l}$ 需要精心选择,以得到稀疏的攻击向量。

上述稀疏攻击向量的求解问题实际上可转化为一个约束最小化问题。令 $\boldsymbol{u}=(\hat{\boldsymbol{N}}(i,:))^{\mathrm{T}}$,$\boldsymbol{V}_i=[\boldsymbol{v}_1^{\mathrm{T}},\boldsymbol{v}_2^{\mathrm{T}},\cdots,\boldsymbol{v}_m^{\mathrm{T}}]^{\mathrm{T}}=\hat{\boldsymbol{N}}(I_i,:)$,其中 $I_i=M\backslash\{i\}$。经过行变换,$\boldsymbol{a}_i$ 可以表示为:

$$\boldsymbol{a}_i=\begin{bmatrix}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{l}\\ \boldsymbol{V}_i\boldsymbol{l}\end{bmatrix} \tag{30}$$

在式(30)中,限制 $\boldsymbol{u}^{\mathrm{T}}\boldsymbol{l}=1$。该限制条件意味着固

定了第 i 个节点测量单元，也即攻击测量单元集为 S_i。基于式(29)和(30)，攻击向量的构建可以表示为一个约束基最小化问题：

$$\begin{cases}\min\limits_{\boldsymbol{l}} \|\boldsymbol{a}_i\|_0=\|\hat{\boldsymbol{N}}\boldsymbol{l}\|_0 \\ \text{s.t.} \quad \boldsymbol{u}^{\mathrm{T}}\boldsymbol{l}=1\end{cases} \Leftrightarrow \begin{cases}\min\limits_{\boldsymbol{l}} \|\boldsymbol{a}_i\|_0=\|\boldsymbol{V}_i\boldsymbol{l}\|_0 \\ \text{s.t.} \quad \boldsymbol{u}^{\mathrm{T}}\boldsymbol{l}=1\end{cases} \tag{31}$$

由于式(31)是一个非确定性多项式难(NP-hard)问题，故通过凸松弛技术[17]转化为凸优化问题，可以直接采用已有的凸优化问题的求解方法，以减少算法的复杂度。L_1 范数是 L_0 范数的最优凸近似，因此将式(31)直接转化为 L_1 范数的最优问题，如式(32)所示。

$$\begin{cases}\min\limits_{\boldsymbol{l}} \|\boldsymbol{a}_i\|_1=\|\boldsymbol{V}_i\boldsymbol{l}\|_1 \\ \text{s.t.} \quad \boldsymbol{u}^{\mathrm{T}}\boldsymbol{l}=1\end{cases} \tag{32}$$

为了得到稀疏的攻击向量，没有必要获得完整的系统信息矩阵。实际上，只需要获得系统的子矩阵 $\boldsymbol{N}(E_i,:)$ 即可，其中 E_i 为攻击者窃听的测量单元集合，满足 $S_i \subset E_i$、$|E_i|<m$。窃听的测量单元数量相对大于负荷的数量即可，相应地只需要收集测量数据 $\boldsymbol{Z}(E_i,:)$。因此，稀疏攻击向量的构建可以表示为：

$$\boldsymbol{a}_i^*=\begin{bmatrix}\boldsymbol{a}_i^*(E_i) \\ 0\end{bmatrix} \tag{33}$$

其中，$\boldsymbol{a}_i^*(E_i)=\boldsymbol{N}(E_i,:)\boldsymbol{l}^*$，$\boldsymbol{l}^*$ 为由上述凸优化方法得到最优结果时对应的 $\boldsymbol{l}$。

4 实验分析

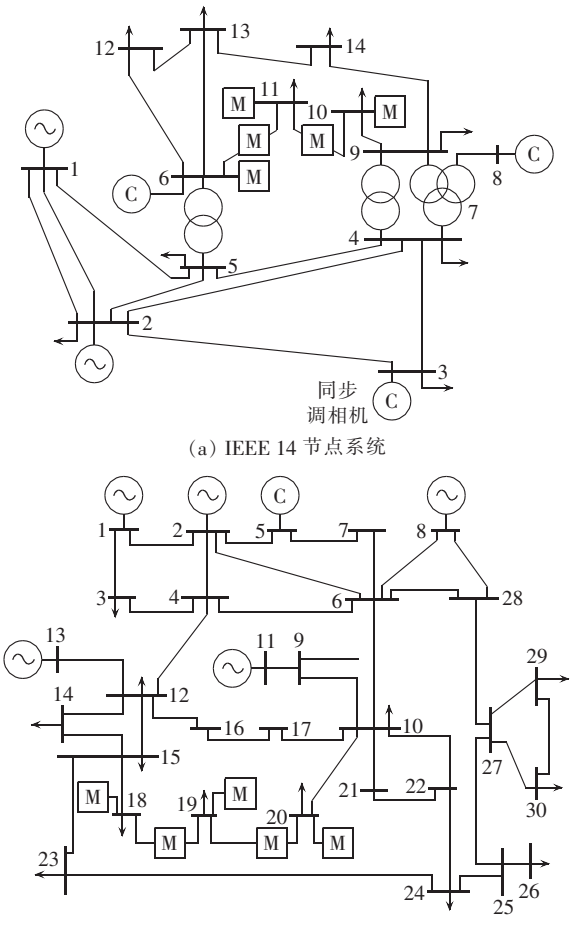
4.1 实验设定

分别在 IEEE 14 节点和 IEEE 30 节点系统进行实验。图 2 为测试系统的拓扑示意图。相关系统的参数可从 Matpower 工具箱[18]中获得，假设所有母线及线路均设置测量单元。负荷变量符合均匀分布，在基准负荷的 50%~150% 之间随机变化，以产生实验所需的测量数据。设定实验采集 5 000 个时刻的测量样本，信噪比变化范围为 5~40 dB。

4.2 结果分析

如图 2 所示，本文所提攻击策略针对文献[4]中的稀疏攻击案例进行时，2 个系统中选定的攻击稀疏度皆为 5(即所需攻击测量单元的数量为 5)。在 IEEE 14 节点系统中，攻击测量单元集为 $S_{11}=\{B_{11},F_{11}\}$。在 IEEE 30 节点系统中，攻击测量单元集为 $S_{19}=\{B_{19},F_{19}\}$。攻击的第一阶段，使用增广拉格朗日乘子法对数据进行预处理以剔除异常值，恢复真实准确的测量数据；攻击的第二阶段，采用平行因子分解算法推断不完整的系统矩阵；攻击的第三阶段，采用凸优化的方法求得稀疏攻击向量。

图 3 为 IEEE 14 节点系统下只含有一个异常值时的效果图，由图 3 可以看出，经过数据预处理后，



(a) IEEE 14 节点系统

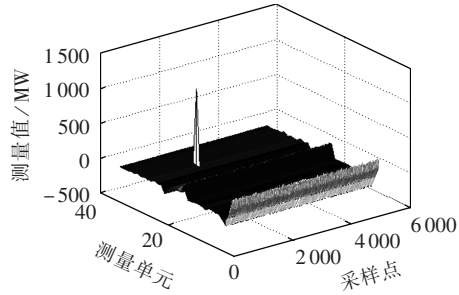
(b) IEEE 30 节点系统

图 2 测试系统示意图

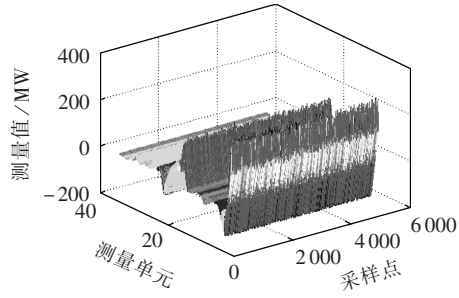
Fig.2 Schematic diagram of test systems

含有异常值的测量数据 $\boldsymbol{Z}_{\text{outlier}}$ 可以恢复真实测量数据 $\boldsymbol{Z}$ 和异常值 $\boldsymbol{E}$。

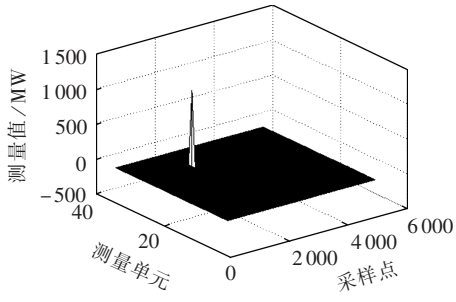
为了分析平行因子分解算法推断系统矩阵的可



(a) $\mathbf{Z}_{\text{outlier}}$



(b) $\boldsymbol{Z}$



(c) $\boldsymbol{E}$

图 3 IEEE 14 节点系统只含有一个异常值时的数据恢复效果图

Fig.3 Data recovery effect of IEEE 14-bus system with only one outlier

行性,这里对系统矩阵识别的均方误差进行评估,并与独立成立分析算法进行对比。需要估计的系统矩阵为 $\boldsymbol{N}(E_i,:)$,在 IEEE 14 节点系统中,i=11;在 IEEE 30 节点系统中,i=19。为了确保攻击向量的稀疏度,测量单元集合 E_i 的数量要比负荷的数量大,这里选择 $|E_i|=2l_d$。均方误差定义为测量值与估计值之间的残差。2 种算法下 2 个系统的系统矩阵识别均方保差如图 4 所示。由图 4(a)可以看出,随着信噪比的增加,均方误差关于对数呈线性下降。当信噪比很高(40 dB)时,均方误差很低,大约为 10^{-4}。这意味着将系统转化为线性独立的模型是可行的,基于平行因子分解算法对系统信息矩阵进行推断是可行

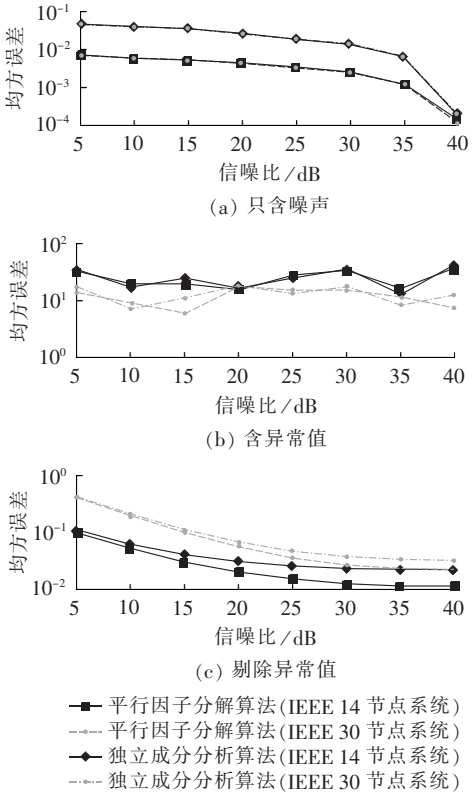


图 4 估计系统矩阵的性能对比

Fig.4 Performance comparison of estimating system matrix

的。而且,不论是 IEEE 14 节点系统还是 IEEE 30 节点系统,平行因子分解算法都比独立成分分析算法表现出更好的性能。但是,在测量数据存在异常值时,平行因子分解算法将会出现较大的均方误差,如图 4(b)所示,此时推断出的系统信息矩阵将严重偏离系统真实状态(此时,由于异常值的影响,无论是独立成分分析算法还是平行因子分解算法,均表现出较大的误差和不确定性)。采用第一阶段的策略进行数据预处理以剔除异常值后,再使用平行因子分解算法进行系统信息矩阵的推断,此时均方误差将大幅降低,而且此时平行因子分解算法仍然比独立成分分析算法表现出更好的性能,如图 4(c)所示。

攻击的第三阶段,使用估计出的系统信息矩阵,采用凸优化的方法求得稀疏攻击向量。本节对攻击向量的求解情况进行分析。图 5 展示了 IEEE 14 节点系统和 IEEE 30 节点系统的情况(纵轴为标幺值),实验在 30 dB 的信噪比下进行。IEEE 14 节点系统的实验结果如图 5(a)所示,可见系统信息已知情况下求得的攻击向量和只含有噪声的测量数据下求得的攻击向量完全相同,这就意味着基于平行因子分解算法的攻击策略是有效的。但是,当存在异常值时,上述方法求得的攻击向量不仅与系统信息已知情况下求得的攻击向量不同,还出现了新的需要控制的测量单元,即此时需要控制的测量单元更多(这实际上是由估计的系统矩阵误差较大导致的,此时求出的攻击向量已经与实际系统脱离了关系)。当采用本文的攻击策略进行数据预处理以剔除异常值后(图 3 为 IEEE 14 节点系统只含有一个异常值时的效果图),再采用上述的方法进行攻击向量的求解,得到的攻击向量与系统信息已知情况下求得的攻击向量完全相同。由于大量的测量数据中总会由于各种原因(设备故障、通信故障、数据丢失)[19-20]出现部

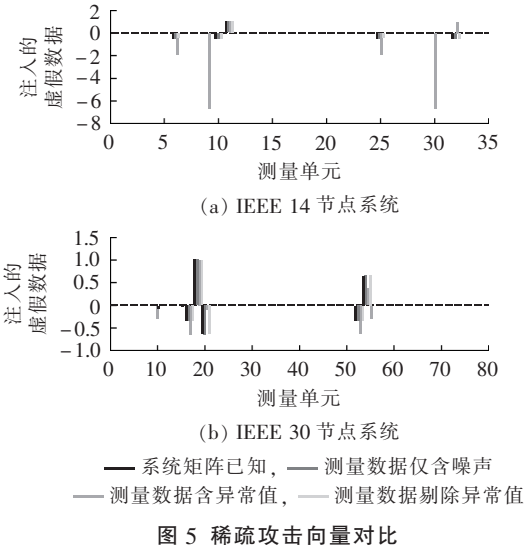


图 5 稀疏攻击向量对比

Fig.5 Comparison of sparse attack vector

分异常值,因此如果不对数据进行预处理以剔除异常值,基于平行因子分解算法的攻击策略很难成功,而本文提出的攻击策略通过增广拉格朗日乘子法剔除异常数据,保证了在异常值存在的情况下,仍然能够成功地实施攻击。IEEE 30节点系统的实验结果和IEEE 14节点系统相似,如图5(b)所示。

最后,采用文献[7]中的错误检测概率MDP(Missed Detection Probably),本文指系统检测不到攻击的概率,对本文所提攻击策略的攻击效果进行评估。进行 M_m 次蒙特卡洛实验,取 $M_m=10000$,用 M_{missed} 表示系统未检测到攻击的次数,则系统检测不到攻击的概率表示为 M_{missed}/M_m。对于每一次蒙特卡洛实验,使用坏数据检测算法对系统进行检测。基于式(3),如果 $\max\limits_j(|r_j|/\sqrt{\mathrm{cov}(r_j)})\leqslant v$,则系统检测不到攻击的存在,其中 v 为设定的检测阈值,本文取 $v\in[0.1,0.8]$。图6展示了4种情况下错误检测概率随阈值的变化示意图。以图6(a)所示IEEE 14节点系统为例,在测量数据仅含噪声时,其错误检测概率与系统矩阵已知情况下攻击的检测概率差别很小,但是当测量数据含有异常值时,其错误检测概率大幅降低,这意味着此时攻击的隐蔽性大幅降低。然而,此时若使用本文的方法对测量数据进行预处理以剔除异常值,得到的错误检测概率依然能够得到较为满意的效果。这意味着当存在异常值时,使用本文的攻击策略依然能够对系统实施隐蔽攻击。IEEE 30节点系统实验也得出了相似的结果,如图6(b)所示。

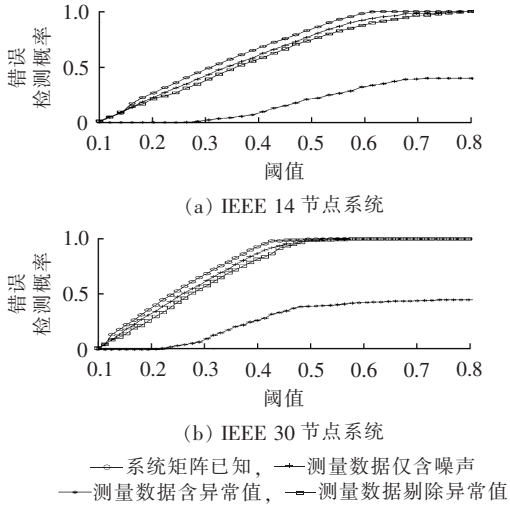


图6 错误检测概率随阈值的变化示意图

Fig.6 Curves of error detection probability vs. threshold value

5 结论

本文提出了一种基于数据驱动的稀疏虚假数据注入攻击策略,以解决在不具备系统信息矩阵的情况下,如何通过估计系统信息矩阵进而实施稀疏攻击的问题。实验结果证明了所提策略即使在异常值存在的情况下依然能够成功地实施稀疏攻击。下一步,笔者将针对该类攻击研究防御策略以应对稀疏虚假数据注入攻击的威胁,提高电力系统的安全性。

参考文献:

[1] LIU Y,NING P,REITER M K. False data injection attacks against state estimation in electric power grids[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago,Illinois,USA:ACM,2009:21-32.

[2] SANDBERG H,TEIXEIRA A,JOHANSSON K H. On security indices for state estimators in power networks[C]//Preprints of the First Workshop on Secure Control Systems. Stockholm,Sweden:[s.n.],2010:1-6.

[3] SOU K C,SANDBERG H,JOHANSSON K H. Electric power network security analysis via minimum cut relaxation[C]//Decision and Control and European Control Conference. [S.l.]:IEEE,2011:4054-4059.

[4] GIANI A,BITAR E,GARCIA M,et al. Smart grid data integrity attacks[J]. IEEE Transactions on Smart Grid,2013,4(3):1244-1253.

[5] OZAY M,ESNAPLA I,VURAL F T Y,et al. Sparse attack construction and state estimation in the smart grid:centralized and distributed models[J]. IEEE Journal on Selected Areas in Communications,2013,31(7):1306-1318.

[6] HAO J,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.

[7] ESMALIFALAK M,NGUYEN H,ZHENG R,et al. Stealth false data injection using independent component analysis in smart grid[C]//IEEE International Conference on Smart Grid Communications. [S.l.]:IEEE,2011:244-248.

[8] YU Z H,CHIN W L. Blind false data injection attack using PCA approximation method in smart grid[J]. IEEE Transactions on Smart Grid,2015,6(3):1219-1226.

[9] KIM J,TONG L,THOMAS R J. Subspace methods for data attack on state estimation:a data driven approach[J]. IEEE Transactions on Signal Processing,2015,63(5):1102-1114.

[10] ANWAR A,MAHMOOD A,PICKERING M. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements[J]. Journal of Computer and System Sciences,2017,83(1):58-72.

[11] YANG J,YU R,LIU Y,et al. A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid[C]//2015 IEEE International Conference on Communications(ICC). [S.l.]:IEEE,2015:7210-7215.

[12] LI H,LAI L,ZHANG W. Communication requirement for reliable and secure state estimation and control in smart grid[J]. IEEE Transactions on Smart Grid,2011,2(3):476-486.

[13] LIN Z,CHEN M,MA Y. The augmented Lagrange multiplier method for exact recovery of corrupted low-rank matrices[R]. [S.l.]:UIUC,2009.

[14] 丁小焕,彭甫镕,王琼,等. 基于平行因子分解的协同聚类推荐算法[J]. 计算机应用,2016,36(6):1594-1598.
DING Xiaohuan,PENG Furong,WANG Qiong,et al. Co-cluste-

ring recommendation algorithm based on parallel factorization decomposition[J]. Journal of Computer Applications,2016,36(6):1594-1598.
[15] DE LATHAUWER L,CASTAING J,CARDOSO J. Fourth order cumulant-based blind identification of under-determined mixtures[J]. IEEE Transactions on Signal Processing,2007,55(6):2965-2973.
[16] KOLDA T G,BADER B W. Tensor dcompositions and aplications[J]. Siam Review,2009,51(3):455-500.
[17] CANDÈS E J,TAO T. The power of convex relaxation:near-optimal matrix completion[J]. IEEE Transactions on Information Theory,2010,56(5):2053-2080.
[18] ZIMMERMAN R D,MURILLO-SÁNCHEZ C E,THOMAS R J. Matpower:steady-state operations,planning,and analysis tools for power systems research and education[J]. IEEE Transactions on Power Systems,2011,26(1):12-19.
[19] ANWAR A,MAHMOOD A N,PICKERING M. Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements[J]. Journal of Computer and System Sciences,2017,83(1):58-72.
[20] ANWAR A,MAHMOOD A N. Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors[C]// Power and Energy Society General Meeting (PESGM). Boston,MA,USA:IEEE,2016:1-5.

作者简介:


田继伟

田继伟(1993—),男,河南驻马店人,硕士研究生,主要研究方向为智能电网、信息安全(**E-mail**:tianjiwei2016@163.com);

王布宏(1975—),男,山西太原人,教授,博士研究生导师,博士,主要研究方向为信号处理、信息安全(**E-mail**:adhd2016@163.com);

尚福特(1992—),男,山东泰安人,博士研究生,主要研究方向为信息安全、智能电网安全(**E-mail**:2417162923@qq.com);

刘帅琦(1992—),女,陕西咸阳人,硕士研究生,主要研究方向为智能电网、信息安全(**E-mail**:3459700751@qq.com)。

Sparse false data injection attacks based on data driven

TIAN Jiwei,WANG Buhong,SHANG Fute,LIU Shuaiqi
(Information and Navigation College,Air Force Engineering University,Xi'an 710077,China)

Abstract: A sparse false data injection attack strategy based on data driven is proposed. The attack strategy is divided into three stages:in the first stage,intercepted data are preprocessed based on sparsity optimization techniques to eliminate the outliers;in the second stage,the incomplete system information matrix is deduced by parallel factor decomposition algorithm;in the third stage,the sparse attack vectors are solved by convex optimization method based on the system matrix. Results of simulation tests verify that traditional attack strategy can't be implemented successfully with outliers,while the proposed strategy can still implement the sparse false data injection attack successfully.

Key words: false data injection; data driven; sparsity optimization; parallel factor analysis; convex optimization; state estimation