分布式电源接入场景下的电网振荡攻击建模与检测

刘 杨, 桂宇虹, 安 豆, 管晓宏, 刘 烃

西安交通大学 智能网络与网络安全教育部重点实验室 西安 中国 710049

摘要 随着分布式电源在电网中所占比重的不断提升, 针对分布式电源的攻击将给电网带来更严重的安全威胁。攻击者可以通过网络入侵手段协同控制电网中防御较弱的配网侧分布式电源功率输出, 最终影响发电侧发电机等关键设备的安全运行。为保障电网安全稳定运行, 亟需研究针对分布式电源接入场景下的安全威胁及其防御措施。首先, 本文在电力系统动态模型基础之上建立了电网振荡攻击的最小代价攻击模型, 通过协同控制多个分布式电源的功率, 在牺牲最少被控节点的前提下导致电网发生振荡。其次, 针对现有振荡检测算法的不足, 本文提出一种启发式的攻击源检测算法, 通过分析系统内各节点的势能变化, 可有效辅助定位攻击源。算例仿真分析结果验证了通过最小代价攻击影响电网稳定运行的可行性, 以及攻击检测方法的有效性。

关键词 智能电网; 分布式电源; 信息-物理攻击; 振荡攻击; 攻击检测
中图法分类号 TM727 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2019.05.05

Oscillation Attack Modelling and Detection with Penetration of Distributed Energy Resources in Smart Grid

LIU Yang, GUI Yuhong, AN Dou, GUAN Xiaohong, LIU Ting

Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China

Abstract The increasing distributed renewable resources (DERs) will introduce more vulnerabilities to smart grids. In this scenario, attackers can change the power output of DERs in the distribution network, and finally disturb the secure operation of crucial devices such as generators in the transmission network. To secure the operation safety and stability in smart grids, it is necessary to study the threats and relevant defense strategies under the scenario with high penetration of DERs. First, a novel attack model is proposed based on power system dynamics model, which could can cause power system oscillation with minimal attack costs via coordinated control of DERs maliciously. Second, in consideration of current oscillation detection algorithms' limitations, a heuristic attack detection method is proposed. The simulation-based case studies demonstrate that the proposed attack could threat power system operational safety with minimal costs, and the detection method can effectively locate the real attack sources.

Key words smart grid; distributed energy resources (DERs); cyber-physical attack; oscillation attack; attack detection

1 引言

随着新能源技术的不断发展, 包括风电、光伏电源等在内的分布式可再生能源通过逆变器大量接入智能电网[1]。由于可再生能源具有不确定性、波动性以及低惯性的特点, 其渗透率的逐渐增加导致系统朝“低惯量、欠阻尼”的状态演变, 给电网的稳定性带来了巨大挑战[2]。为此, 国内外学者提出了虚拟同步发电机技术[3-5], 通过结合储能设备、合理调控并网逆变器等方式来弥补系统惯量的不足。目前虚拟同步发电机技术被已经被应用到诸如风电[6]、光伏[7]、储能[8-9]等多种分布式电源并网的场景中。

此外, 根据国家电网公司企业标准《分布式电源接入电网技术规定》(Q/GDW480—2010), 分布式电源接入电网时一般需要满足以下原则:

(1) 总容量不超过上一级变压器供电区域内最

通讯作者: 刘烃, 博士, 西安交通大学教授, Email: tingliu@mail.xjtu.edu.cn。
本课题得到国家重点研发计划资助项目(No.2016YFB0800202); 国家自然科学基金(No.61772408, No.U1766215, No.U1736205, No.61721002, No.61632015, No.61833015); 霍英东基金(No.151067)和中央高校基本科研业务费专项资金资助。
收稿日期: 2019-01-28; 修改日期: 2019-04-18; 定稿日期: 2019-05-13

大负荷的 25%, 同时并网点的短路电流与分布式电源额定电流之比不低于 10。

(2) 并网点的电压不平衡度、直流电流分量、电压波动和闪变、电磁兼容等电能质量指标要满足相关规定。

(3) 分布式电源应满足规定的有功/无功功率供给要求, 或具有有功功率控制和电压/无功调节的能力, 以确保电网故障或特殊运行方式时电力系统的稳定。

以上技术和规定试图保障分布式电源接入后电网的稳定性。然而, 作为典型的物理信息系统, 电力电子设备的高度信息化和自动化使电网面临信息-物理攻击[10, 11]的安全威胁。攻击者可利用设备漏洞, 通过网络入侵等方式获取设备控制权限, 读取数据并控制逆变器等关键设备的运行状态, 进而控制风电、光储能等系统的功率输出。例如, 文献[12]分析了采用 Windshark 等软件对风电场实施攻击。文献[13]验证了采用 IEC61850 通信规约的光伏逆变器存在中间人攻击风险, 对逆变器数据的篡改会影响实际电力系统运行。同时, 安全公司 ITsec 在德国艾思玛(System Mess Anlagentechnik, SMA)光伏逆变器中找出了 14 个已知 CVE 安全漏洞(Common Vulnerabilities and Exposures, CVE), 说明了当前基础设施存在被攻击的风险 [14]。

由于分布式电源在电网中分布广泛, 目前的安全防护措施难以覆盖到所有设备, 实现对攻击行为的全面阻断和隔离。此外, 在大量分布式能源接入后, 电网的供电模式从原来的“源-网-荷”单向供电向多区域分布式双向供电演变; 控制策略由原来的“分层集中管理”模式逐渐向“分层集中控制+分布式控制”的混合策略转变, 以应对大量分布式设备的管控需求。电网结构的复杂化和高度异构, 也给攻击行为识别和定位带来了新的挑战。

因此, 在大量分布式能源接入电网的场景下, 虽然传统发电机节点受到了严格的保护, 难以直接入侵和破坏, 但攻击者可通过对电网中配网侧脆弱节点的分布式电源发起大规模的信息-物理攻击, 改变配电侧的功率供需, 最终可导致发电机频率失稳。此外, 信息网络和电力网络的高度耦合也使得系统更易发生连锁崩溃[15]。即该攻击可通过对防护弱的设备的网络攻击最终影响到严格保护区域设备的安全可靠运行, 降低系统的安全可靠性。

为研究在分布式能源大量接入的场景下信息-物理攻击对电网的安全威胁, 本文在电力系统动态模型基础之上, 基于输出反馈控制的思想, 设计了一种最小攻击代价的攻击方案, 验证了攻击导致目标电力系统发生振荡的可能性。同时, 针对攻击行为, 为从所有受攻击影响的节点中尽快找出真实攻击源, 本文基于能量函数的思想, 通过分析攻击后系统的势能变化特征, 提出了一种启发式的攻击源检测和定位方法。

本文组织结构如下: 第 2 节在电力系统动态模型基础之上建立了电网振荡攻击的最小代价攻击模型, 并简要分析了具体实施方式; 第 3 节分析了现有振荡检测算法的不足, 并基于能量函数的思想, 通过分析攻击后系统的势能变化特征, 提出了一种启发式的攻击源检测和定位方法; 第 4 节基于 IEEE 14-节点测试系统进行了算例仿真分析, 验证攻击方案的可行性以及攻击检测算法的有效性; 最后, 在第 5 节进行了总结和展望。

2 电网振荡攻击

2.1 攻击模型概述

如图 1 所示是一个多节点电力系统输电网拓扑示意图, 其中包括输电网传输线、发电机节点与负荷节点; 在负荷节点以下, 大量分布式电源和普通用电负载通过配电网接入输电网。下面结合图 1 阐述本文所提出的电网振荡攻击模型。

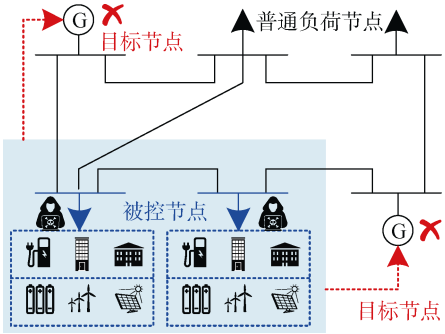

图 1 电力系统信息-物理攻击模型

Figure 1 Power system cyber-physical attack model

本文的攻击模型基于如下假设: (1)攻击者已通过信息窃取、系统辨识等手段掌握了电力系统输电网的拓扑和部分负荷节点的关键运行信息; (2)攻击者可通过对大量分布式电源并网逆变设备的入侵, 实现对部分负荷节点的功率控制。针对假设(1), 输电网的拓扑可以通过卫星图等获得地理信息系统(Geographic Information System, GIS)数据, 结合实地勘探等手段获取得到, 再结合线路的长度和输电线规格参数可以估计得到线路的阻抗信息。节点的运行状态可通过入侵部分量测设备或布置额外的隐

蔽探测设备实现。针对假设(2), 逆变器采用的Modbus,IEC61850 规约, 缺乏安全认证机制和数包隐藏机制, 导致在通信过程中存在数据篡改的风险[12-14]。

在此假设基础上, 攻击者通过入侵大量的分布式能源系统(如风电、光伏、储能等系统)和可控负载(如智能楼宇等系统)进而控制负荷节点。同时, 攻击者通过恶意控制被控负荷节点和电网的功率交换, 破坏系统频率稳定性, 最终导致系统中的目标发电机振荡, 并最终离网运行。

传统的基于负荷的攻击方式主要通过动态调节负荷构造正反馈导致系统频率失稳。例如, 文献[16,17]中, 利用频率测量信号动态调整部分被控节点的负荷, 当频率偏高时减小负荷, 当频率偏低时增大负荷, 最终导致系统的频率失稳, 使目标发电机频率偏离过大而离网。这种攻击方式虽然实现了攻击目标, 但是振荡影响了系统内的所有节点, 即也牺牲了攻击者所掌握的所有节点稳定性。

基于上述考虑, 本文从攻击者角度出发, 提出一种攻击方式, 使得攻击者能以最小的攻击代价实现攻击目标。即通过牺牲尽可能少的被控节点的稳定性, 导致目标发电机频率失稳, 而其余被控节点频率保持稳定。

下面先构建电力系统的动态模型; 然后通过分析影响系统稳定性的因素, 设计出可行的攻击方案; 最后讨论攻击的具体实施。

2.2 电力系统动态模型

目前针对电力系统低频振荡模态的研究方法主要是在运行点附近进行局部线性化, 得到系统的动态模型后再进一步分析[18]。类似地, 为了研究电力系统的动态特性, 本文对图 1 系统中的同步发电机 i 采用 2 阶经典模型, 其转子运动状态方程可表述为:

$$\begin{cases} \dfrac{\mathrm{d}\delta_i}{\mathrm{d}t} = \omega_0(\omega_i - 1) \\ T_{J_i}\dfrac{\mathrm{d}\omega_i}{\mathrm{d}t} = (P_{m,i} - P_{e,i}) - D_i(\omega_i - 1) \end{cases} \tag{1}$$

式中: δ_i 是电机转角, ω_i 是电机的旋转频率, ω_0 是基准频率, $P_{m,i}$ 是发电机的原动机功率, $P_{e,i}$ 是发电机电磁功率(发电机输出的功率), T_{J_i} 是发电机惯性时间常数, D_i 是阻尼系数。

借助虚拟同步发电机的概念, 图 1 中负荷节点自身具有的惯量等效于和同步发电机类似的虚拟惯量[19]。因此, 可将图 1 中被控的负荷节点看成虚拟发电机进行控制, 其动态特性同样可用式(1)模型表述。其中 $P_{m,i}$ 是虚拟发电机的原动机功率, 代表了配网侧向该负荷节点子系统注入的总功率, 即节点处新能源发电总功率减去负荷消耗总功率; $P_{e,i}$ 是虚拟发电机电磁功率, 代表了负荷节点向输电网其他所有节点传递的总功率。其他参数和虚拟同步发电机概念类似, 不再赘述。对于不包含新能源接入的负荷节点, 可继续按照传统的负荷建模方式进行建模。

综上, 系统的各节点动态特性都可由式(1)的模型进行表述。在实际分析中可利用 Kron Reduction[20] 对系统的拓扑进行约减, 只保留待分析的 L 个(虚拟)发电机节点。之后, 结合节点的代数方程以及相应的坐标变换和适当简化, 并在稳定点附近线性化, 可得到相应的多机系统的动态模型[21]:

$$\begin{bmatrix} \Delta\dot{\boldsymbol{\omega}} \\ \Delta\dot{\boldsymbol{\delta}} \end{bmatrix} = \begin{bmatrix} -\boldsymbol{T}_J^{-1}\boldsymbol{D} & -\boldsymbol{T}_J^{-1}\boldsymbol{K}_1 \\ \boldsymbol{\omega}_0 & \boldsymbol{0} \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{\omega} \\ \Delta\boldsymbol{\delta} \end{bmatrix} \tag{2}$$

其中:

$$\begin{cases} \boldsymbol{T}_J^{-1} = diag(T_{J_1}^{-1}, T_{J_2}^{-1}, \cdots, T_{J_L}^{-1}) \\ \boldsymbol{D} = diag(D_1, D_2, \cdots, D_L) \\ \boldsymbol{\omega}_0 = diag(w_0, \cdots, w_L) \\ \Delta\boldsymbol{\omega} = [\Delta\omega_1, \Delta\omega_2, \cdots, \Delta\omega_L]^T \\ \Delta\boldsymbol{\delta} = [\Delta\delta_1, \Delta\delta_2, \cdots, \Delta\delta_L]^T \end{cases} \tag{3}$$

式(3)中, $\Delta\omega_i = \omega_i - 1$ 和 $\Delta\delta_i = \delta_i - \delta_0$ 分别代表发电机频率偏移和发电机转角偏移, $diag(*)$ 表示将各矩阵块按对角排列的操作, 其他的变量含义参见文献[21], 不再赘述。

因此, 在分析电力系统稳定性时, 可在稳定点附近将其描述成线性时不变系统, 相应的状态空间模型可表述为:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} \tag{4}$$

其中:

$$\begin{cases} \boldsymbol{x} = \begin{bmatrix} \Delta\boldsymbol{\omega} \\ \Delta\boldsymbol{\delta} \end{bmatrix} \\ \boldsymbol{A} = \begin{bmatrix} -\boldsymbol{T}_J^{-1}\boldsymbol{D} & -\boldsymbol{T}_J^{-1}\boldsymbol{K}_1 \\ \boldsymbol{\omega}_0 & \boldsymbol{0} \end{bmatrix} \end{cases}$$

式(4)中, $\boldsymbol{A} \in \Re^{n\times n}(n = 2L)$ 为线性化后的系统状态转移矩阵, $\boldsymbol{x} \in \Re^n$ 为线性化后的系统状态量, 其时域解形式如下:

$$\boldsymbol{x}(t) = \sum_{i=1}^{n} \boldsymbol{u}_i^T \boldsymbol{x}(0) e^{\lambda_i t} \boldsymbol{v}_i \tag{5}$$

式中: λ_i, $\boldsymbol{u}_i$, $\boldsymbol{v}_i$ 分别为第 i 个模态对应的特征值和左右特征向量。对于特征值 λ_i, 实部为负对应衰减模态, 实部为正对应不稳定模态, 复特征值对应振荡

模态。模态 i 的右特征向量 $\boldsymbol{v}_i$ 的第 k 行元素代表了第 k 个系统状态量在模态 i 中的活跃度。

2.3 振荡攻击模型

2.3.1 攻击模型构建

已知电力系统动态模型中有 L 个节点, $n=2L$ 个系统状态量。假定其中 m 个节点为被攻击者控制的负荷节点所表征的虚拟同步发电机, 且系统内节点位置已经过调整保证前 m 个状态量对应的节点集合 $X_{at}=[x_1,x_2,\cdots,x_m]^T$ 对应于攻击者可控设备集合。由此, 结合式(4)可得到系统被攻击后的状态空间表达式为:

$$\begin{cases}\dot{\boldsymbol{x}}=A\boldsymbol{x}+B\boldsymbol{u}\\ \boldsymbol{y}=C\boldsymbol{x}\end{cases} \tag{6}$$

其中:

$$\begin{cases}B_{L\times m}=\left[diag(T_{J_1}^{-1},T_{J_2}^{-1},\cdots,T_{J_n}^{-1})_{m\times m}\quad \boldsymbol{0}_{m\times(n-m)}\right]^T\\ \boldsymbol{u}_{m\times 1}=\left[P_{a,1}\quad\cdots\quad P_{a,m}\right]^T\\ \boldsymbol{y}_{r\times 1}=[\Delta\omega_1,\Delta\omega_2,\cdots,\Delta\omega_m,\ \Delta\delta_1,\Delta\delta_2,\cdots,\Delta\delta_m]^T\end{cases}$$

式(6)中, $\boldsymbol{u}\in\Re^m$ 代表系统的攻击扰动输入量, 分别对应于节点 $i\,(i=1,\cdots,m)$ 的扰动功率输入量 $P_{a,i}$, $\boldsymbol{y}\in\Re^r$ $(r=2m)$ 代表系统的观测量, 分别对应于节点 $i\,(i=1,\cdots,m)$ 的频率偏移 $\Delta\omega_i$ 和转角偏移 $\Delta\delta_i$, 且原系统能控能观。

针对式(6)所述系统, 攻击者需要构造特定的攻击向量输入 $\boldsymbol{u}$, 使得系统产生至少一个振荡不稳定模态。攻击构造问题等价于系统特征根和特征向量的配置问题, 一般可采用状态反馈或输出反馈的方式实现。状态反馈[22]虽然选择范围大, 但是需要全维状态观测器来估计系统的状态量, 成本高且技术复杂, 实现难度大。而被攻击者控制的节点所在位置的输出量容易测得, 故笔者考虑采用输出反馈来实现攻击。

针对式(6)描述的动态系统构造基于输出反馈的攻击向量 $\boldsymbol{u}=K\boldsymbol{y}$, 对应的闭环系统的表达式:

$$\dot{\boldsymbol{x}}=(A+BKC)\boldsymbol{x} \tag{7}$$

攻击后的系统状态转移矩阵 $A+BKC$ 有至少一个振荡不稳定模态。为了简化分析, 本文仅讨论通过构造一个振荡不稳定模态实现攻击目标, 对应一对实部为正的共轭特征值 $(\hat{\lambda}_{at},\hat{\lambda}_{at}^{*})$。特征值 $\hat{\lambda}_{at}$ 对应右特征向量为 $\hat{\boldsymbol{v}}_{at}\in\Re^n$, $\hat{\boldsymbol{v}}_{at}$ 中前 m 行对应可控节点的元素构成子向量为 $\tilde{\boldsymbol{v}}_{at}\in\Re^m$。

为了实现最小代价攻击, 需要构造攻击向量 $\boldsymbol{u}$, 使得攻击后系统有一个模态满足条件:

(Condition 1)

1. 不稳定模态: $\mathrm{Re}(\hat{\boldsymbol{\lambda}}_{at})>0$;
2. 最小代价: $\min\left\|\tilde{\boldsymbol{v}}_{at}\right\|_0$。

其中(Condition 1-1)保证攻击能引入不稳定模态, 导致系统不稳定; (Condition 1-2)保证了尽量少的被控节点参与到该不稳定模态中, 即牺牲尽可能少的被控节点, 实现攻击成本最小化。由于攻击者至少需要牺牲一个被控节点参与到不稳定模态中才能引导系统振荡, 因此如果通过牺牲单个节点可实现攻击目标, 则(Condition 1-2)可等价于 $\left\|\tilde{\boldsymbol{v}}_{at}\right\|_0=1$。

2.3.2 攻击向量求解

下面根据文献[23]提供的思路, 分析如何构造最小代价攻击向量。对 $A+BKC$ 的一组特征值 $\hat{\lambda}_c$ 和特征向量 $\hat{\boldsymbol{v}}_c\,(c=1,2,\cdots,n)$, 有:

$$(A+BKC)\hat{\boldsymbol{v}}_c=\hat{\lambda}_c\hat{\boldsymbol{v}}_c \tag{8}$$

对式(8)进行矩阵拆分, 令 $A_{11},B_1\in\Re^{m\times m}$, $\hat{v}_c^{\,T}=[\hat{p}_c^{\,T}\ \ \hat{q}_c^{\,T}]$, $\hat{p}_c\in\Re^m$, 可得:

$$\left(\begin{bmatrix}A_{11}&A_{12}\\A_{21}&A_{22}\end{bmatrix}+\begin{bmatrix}B_1\\B_2\end{bmatrix}KC\right)\begin{bmatrix}\hat{p}_c\\\hat{q}_c\end{bmatrix}=\hat{\lambda}_c\begin{bmatrix}\hat{p}_c\\\hat{q}_c\end{bmatrix} \tag{9}$$

由式(9)可得(详细推导过程见附录 A):

$$\begin{aligned}\hat{q}_c=&\left[\hat{\lambda}_cI_{n-m}-(A_{22}-B_2B_1^{-1}A_{12})\right]^{-1}\times\\&\left[(A_{21}-B_2B_1^{-1}A_{11})+\hat{\lambda}_cB_2B_1^{-1}\right]\hat{p}_c\end{aligned} \tag{10}$$

另外, 若攻击者事先给定 r 组特征值 $\hat{\lambda}_1,\cdots,\hat{\lambda}_r$ 和右特征向量子向量 $\hat{p}_1,\cdots,\hat{p}_r$, 由式(8)按类似拆分可知:

$$\left(\begin{bmatrix}A_1\\A_2\end{bmatrix}+\begin{bmatrix}B_1\\B_2\end{bmatrix}KC\right)V=\underbrace{\begin{bmatrix}P\\Q\end{bmatrix}}_{\tilde{V}}\Lambda \tag{11}$$

式中: $\Lambda=diag(\hat{\lambda}_1,\cdots,\hat{\lambda}_r)$, $V=\left[\hat{v}_1,\cdots,\hat{v}_r\right]$, $P=\left[\hat{p}_1,\cdots,\hat{p}_r\right]$, $Q=\left[\hat{q}_1,\cdots,\hat{q}_r\right]$, $A_1=[A_{11}\ \ A_{12}]\in\Re^{m\times n}$, $A_2=[A_{21}\ \ A_{22}]\in\Re^{(n-m)\times n}$。由式(11)可得(推导过程见附录 A):

$$K=B_1^{-1}[P\Lambda-A_1V][CV]^{-1} \tag{12}$$

因此, 攻击者可在事先给定 r 组特征值和特征向量 Λ 和 P 的前提下, 根据式(10)和式(12)求得输出反馈矩阵 K。这里需要注意的是, 在配置指定 Λ 和 P 时, 要满足以下条件:

(Condition 2)

1. $[CV]$ 必须非奇异, 即 r 个右特征向量之间需满足线性无关;

2. 除配置的 r 个特征值之外, 剩余的 n-r 个特征值必须对应稳定的模态, 即实部必须为负。

其中(Condition 2-1)保证了式(7)中 $[CV]^{-1}$ 可求解; (Condition 2-2)保证了攻击后的不稳定模态可控。

2.3.3 攻击流程实现

综上, 构造最小代价攻击向量 $\boldsymbol{u}$ 实现系统部分振荡的详细流程如表 1 所示。首先给定 r 组特征值和右特征向量子向量, 其中包含一组预期的不稳定振荡模态(步骤 1), 然后根据式(10)和式(12)求得输出反馈矩阵 $\boldsymbol{K}$ (步骤 2-步骤 4)。实际实现过程中, 由于输出反馈的方式能够配置的特征值个数有限, 配置结果中剩余的 n-r 个特征值中可能会出现实部为正的特征值, 如果结果不满足预期条件可反复尝试修改 Λ 和 P, 直到达到预期攻击目标(步骤 5)。最后, 由输出反馈矩阵 $\boldsymbol{K}$ 构造攻击向量 $\boldsymbol{u}$, 并发起振荡攻击。

表 1 最小代价电网振荡攻击流程

Table 1 Procedure of oscillation attack with minimal cost in power grid

算法 1: 最小代价振荡攻击构造算法

输入: 线性系统参数 $A_{n\times n}$, $B_{n\times m}$, $C_{r\times n}$; 可控的节点(设备)集合 M

输出: 输出反馈矩阵 $\boldsymbol{K}$, 攻击向量 $\boldsymbol{u}$

步骤:

1. 初始化, 给定特征值 $\Lambda=diag(\hat{\lambda}_1,\cdots,\hat{\lambda}_r)$ 和右特征向量子向量 $\boldsymbol{P}=[\hat{p}_1,\cdots\hat{p}_r]$, 其中一对特征值 $\hat{\lambda}_{at}$ 和右特征向量子向量 $\tilde{\boldsymbol{v}}_{at}$ 符合(Condition 1);
2. 根据式(5), 计算 $\hat{q}_c(c=1,2,\cdots,r)$, 得到 Q;
3. 验证 $[CV]$ 是否符合(Condition 2-1)。是则继续; 否则, 在 $\hat{\lambda}_{at}$ 和 $\tilde{v}_{at}$ 遵循(Condition 1)的前提下适当的调整 Λ 和 $\boldsymbol{P}$, 返回步骤 2;
4. 根据式(7), 计算 $\boldsymbol{K}$;
5. 验证 $(A+BKC)$ 的所有特征值和特征向量是否符合(Condition 2-2)。是则继续; 否则, 在 $\hat{\lambda}_{at}$ 和 $\tilde{v}_{at}$ 遵循(Condition 1)的前提下适当的调整 Λ 和 $\boldsymbol{P}$, 返回步骤 2;
6. 计算攻击向量 $\boldsymbol{u}=\boldsymbol{K}\boldsymbol{y}$。

2.4 振荡攻击实施

在完成攻击向量 $\boldsymbol{u}$ 的构建后, 可得到分别对应于节点 $i\,(i=1,\cdots,m)$ 的扰动功率输入量 $P_{a,i}$。为了实施攻击, 需要将计算得到的扰动功率输入转换为实际被控分布式电源或负荷节点的功率。这里以节点 i 为例进行分析, 假设在节点 i 处下有 s 个可控电源/负荷, 其最大可增加发电功率(通过削减可控负荷用电、储能电池放电或者增加新能源发电量实现)分别为 $\overline{P}_{L,1}$,$\overline{P}_{L,2}$,$\cdots$,$\overline{P}_{L,s}$, 最大可削减发电功率分别为 $\underline{P}_{L,1}$,$\underline{P}_{L,2}$,$\cdots$,$\underline{P}_{L,s}$ (通过增加负荷用电、储能电池充电或削减新能源发电量实现)。当 $P_{a,i}>0$ (需要增加功率输出)时, 各可控电源/负荷实际的功率增量按比例分配为:

$$P_{a,i,z}=P_{a,i}\bullet\overline{P}_{L,z}/\sum_{j=1}^{s}\overline{P}_{L,j},z=1,2,\cdots,s \tag{13}$$

类似地, 当 $P_{a,i}<0$ (需要减少功率输出)时, 各可控电源/负荷实际的功率增量按比例分配为:

$$P_{a,i,z}=P_{a,i}\bullet\underline{P}_{L,z}/\sum_{j=1}^{s}\underline{P}_{L,j},z=1,2,\cdots,s \tag{14}$$

3 振荡攻击源检测

由上节分析可知, 攻击者可利用被控节点注入扰动能量, 导致其他发电机组振荡。下面首先建立攻击后系统振荡的能量变化模型, 分析基于传统能量函数的强迫功率振荡检测方法的不足, 并在此基础上提出一种启发式的攻击源检测方法。

3.1 暂态能量函数建模

借鉴暂态能量函数建立的方法, 通过对式(2)进行首次积分, 可构造出多机系统下各节点的暂态能量函数[18, 24]。在只考虑有功情况下, 发电机 i 的暂态动能 W_{ki} 和暂态势能 W_{ei} 分别为:

$$W_{ki}=\int_0^t T_{J_i}\Delta\dot{\omega}_i\Delta\omega_i\omega_0\mathrm{d}\tau=T_{J_i}\omega_0\Delta\omega_i^2/2\big|_0^t \tag{15}$$

$$W_{ei}=\int_0^t\Delta P_{e,i}\Delta\omega_i\omega_0\mathrm{d}\tau=\int_{\Delta\delta_0}^{\Delta\delta_t}\Delta P_{e,i}\mathrm{d}\Delta\delta_i \tag{16}$$

式(16)中: $\Delta P_{e,i}$ 表示电磁功率变化量。下面通过推导 W_{ki} 和 W_{ei} 的具体数学表达, 分析攻击后系统的暂态能量变化特征。

假设受到攻击的系统后只有一个不稳定模态 $\eta\pm\gamma i$, 令 $a\pm bi$ 表示状态量 $\boldsymbol{x}$ 在该模态右特征向量中对应的元素, 则根据式(5), 得到其他模态衰减后的时域表达:

$$\begin{aligned}\boldsymbol{x}(t)&=(a+bi)e^{(\eta+\gamma i)t}+(a-bi)e^{(\eta-\gamma i)t}\\&=2\|a+bi\|e^{\eta t}\sin(\gamma t+\varphi)\end{aligned} \tag{17}$$

式中: $\varphi=\tan^{-1}(\frac{a}{b})$。其中, 由于式(5)中的 $u_i^T\boldsymbol{x}(0)$ 是常数项, 不影响分析结论, 为表述方便, 故忽略。此结果可以作为 $\Delta\omega_i$ 和 $\Delta\delta_i$ 的一般表达参考。

由于 $\Delta P_{e,i}$ 可由各发电机的功角偏差 $\Delta\delta_i$ 线性表示(对于式(2)所述系统, 有 $\Delta \boldsymbol{P}_e = \boldsymbol{K}_1\Delta\boldsymbol{\delta} = -\boldsymbol{T}_J\boldsymbol{M}\Delta\boldsymbol{\delta}$, 其中 $\boldsymbol{M} = -\boldsymbol{T}_J^{-1}\boldsymbol{K}_1$ 是系统状态矩阵的子矩阵), 故将 $\Delta\delta_i$ 采用式(12)中的结果进行表示, 求解(11), 可得到暂态势能 W_{ei} 的一般表达形式:

$$W_{ei} = \pi_i \bullet e^{\mu t}\sin^2(\gamma t + \varphi) \tag{18}$$

式中: π_i 为常数, 可由 $\boldsymbol{M}$ 中参数和不稳定模态的右特征向量中对应 $\Delta\delta_i$ 的元素模值求出。

根据式(15), 又 $\dfrac{\mathrm{d}\Delta\delta_i}{\mathrm{d}t} = \omega_0\Delta\omega_i$, 即 $\Delta\omega_i$ 和 $\Delta\delta_i$ 的相位相差 $\pi/2$, 易得到暂态动能 W_{ki} 的一般表达形式为:

$$W_{ki} = \kappa_i \bullet e^{\mu t}\cos^2(\gamma t + \varphi) \tag{19}$$

式中: κ_i 为常数, 可由不稳定模态的右特征向量中对应 $\Delta\omega_i$ 的元素模值求出。

3.2 现有检测算法局限性分析

传统的振荡检测方法, 如 Prony[25]等算法可通过实测数据直接提取出振荡模态的幅值、初始相角、衰减因子和频率, 虽然可以检测和分析振荡模态, 但是无法定位振荡源。基于能量函数的分析方法可用于振荡源的定位, 其主要思想为: 采用式(18)所述 W_{ei} 上升或下降趋势来表示势能的增加或减少(振荡能量的注入和吸收), 向系统中注入振荡能量的节点被认为是问题机组[26]。然而, 由式(18)和式(19)可知, 在本文所述攻击发生且不稳定模态分量占主导后, 系统内受影响机组的动能和势能都呈现增幅振荡趋势。即, 在攻击影响下, 非攻击者所在机组也会被动地向系统注入或吸收部分振荡能量。如单纯采用传统大电网中的振荡检测方法, 会将攻击者的攻击目标机组都判定为振荡节点, 而无法区分出本文所述攻击的发起节点。因此, 这里无法通过 W_{ei} 的上升或下降趋势来直接判定节点 i 是否是真正的攻击源。

然而, 按照能量守恒原理, 在一个节点处, 外施扰动的注入能量减去阻尼耗散, 应该等于势能加动能之和。在攻击源所在节点, 必定存在大量的外施扰动注入的振荡能量, 这些能量除了部分被阻尼消耗和转化为动能外, 多余部分将通过网络以势能的形式传递出去, 影响系统内的其他节点发生振荡; 而对于正常节点, 其外部注入的能量主要是为了维持自身平衡, 受攻击影响后注入的能量也有限。因此, 攻击源所在节点向系统注入的振荡能量必然在振荡能量中占主导地位。据此, 本文拟通过综合分析各节点暂态势能的变化趋势大小来辅助定位真实的攻击源。

3.3 启发式检测算法

为了在攻击实施后能够快速检测和定位攻击源, 以及时采取应对措施减少攻击对电力系统的危害, 本文提出了一种启发式的在线检测方法。如表 2 所示, 首先通过检测时间窗内的最大频率偏差判断系统是否发生振荡(步骤 2), 在判断出系统发生了明显振荡的情况下, 通过各节点势能占总体比重来评判在该节点存在振荡源的可能性(步骤 6)。最终得到的节点可疑度向量 Θ 表征了每一节点存在攻击源的可疑程度, 其中可疑度最大的节点即最可能的潜在被攻击节点。在实际应用中, 各节点的 W_{ei} 可由相位测量单元(Phasor Measurement Unit, PMU)监测 $\Delta P_{e,i}$ 和 $\Delta\omega_i$ 而求得。

表 2 振荡攻击源检测算法流程

Table 2 Procedure of attack source detection algorithm

算法 2: 攻击源检测算法

输入: 所有待分析节点的频率偏差 $\Delta\omega_i(j)$ 和暂态势能 $W_{ei}(j)$ 样本点, $j=[1,2,\cdots,J]$; 滑动窗口采样点数 win, 步长 $step$

输出: 节点可疑度向量 Θ

步骤:

1. 初始化, 采样起始时刻 $h=0$, $\Theta=[0,\cdots,0]_n$;
2. 求取系统当前最大频率偏差 $\Delta\omega_m = \max_{i,j\in[h,h+win]}\left|\Delta\omega_i(j)\right|$, 判断是否符合条件 $\Delta\omega_m > \eta_1$, 是则表明系统存在明显振荡现象, 继续检测; 否则跳至步骤 7;
3. 按窗口截取部分势能样本数据: $\Psi_{ei} = [W_{ei}(h), W_{ei}(h),\cdots,W_{ei}(h+win)], i=1.2,\cdots,n$;
4. 求取各节点势能平均值 $\bar{W}_{ei} = ave(\Psi_{ei}), i=1.2,\cdots,n$;
5. 求取系统势能平均值 $\bar{W}_e = ave(\bar{W}_{e1},\bar{W}_{e2},\cdots,\bar{W}_{en})$;
6. 计算各对节点势能占总体的比重 $\alpha_i = \bar{W}_{ei}/\bar{W}_e, i=1.2,\cdots,n$, 判定是否符合条件 $\alpha_i > \eta_2$, 是则列为可疑节点, 更新可疑度向量 $\Theta(i) = \Theta(i)+1$;
7. 采样起始时刻前移 $h = h + step$;
8. 判定是否符合条件 $h + win \leqslant J$, 是则返回步骤 2, 否则继续;
9. 等待新数据样本, 更新 J, 返回步骤 8。

4 算例仿真分析

4.1 仿真系统设定

在 IEEE 的标准输电测试系统中, 发电机节点数量太少的系统无法说明本文提出的协同攻击构造过程, 例如 IEEE 9-节点系统中仅有三个发电机节点; 而发电机数量较多的系统的状态空间矩阵较难表述,

例如 IEEE 24-节点系统中有 11 个发电机节点。因此, 本文选取 IEEE14-节点标准测试系统为研究对象, 构建攻击案例并验证检测方法。如图 2 所示, IEEE 14-节点系统是一个简单的 5 机系统, 本文假定节点 1、2、3 连接着有大量可再生能源接入的可控负荷节点, 用虚拟同步发电机模型表述, 节点 6、8 连接着传统的同步发电机, 其他节点连接着非可控的普通负荷。为叙述方便, 后文将上述系统中的 5 台发电机按照节点顺序用 1-5 依次编号。

由式(1)模型表征系统中的 5 个(虚拟)同步发电机节点, 可得式(2)所示的系统动态模型, 并用式(1)以状态空间模型的形式表述系统, 其中系统状态量 $\boldsymbol{x}=[\Delta\omega_1,\cdots,\Delta\omega_5,\Delta\delta_1,\cdots,\Delta\delta_5]^T$。攻击实施前, 假定系统中 1、2、3 号节点(对应虚拟同步发电机 G1、G2、G3)下的大量分布式能源已被攻击者入侵和控制。特别地, 攻击者可以通过控制节点 i 处向电网注入的功率进而影响节点状态 $\Delta\omega_i$ $(i=1,2,3)$, 并可通过本地量测设备观测到 $\Delta\omega_i$ $(i=1,2,3)$ 以及 $\Delta\delta_i$ $(i=1,2,3)$。对应式(6)所述状态空间模型中, L=5, n=10, m=3, r=6, 模型具体参数如附录 B 所示[22]。

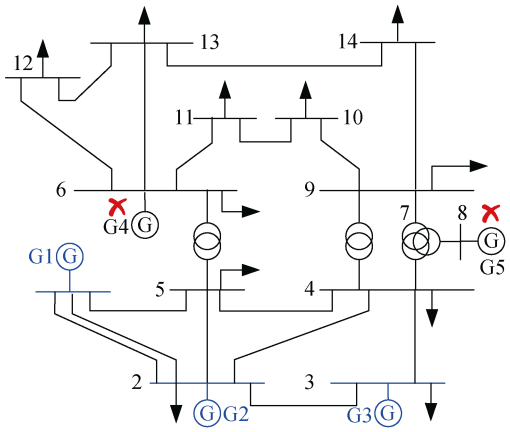

图 2 IEEE 14-节点标准测试系统单线图

Figure 2 IEEE 14-bus system one-line diagram

4.2 典型攻击案例构建与振荡分析

本文构造了两个典型的攻击案例, 分别对应了低频振荡中的区域振荡模式和局部振荡模式。通过协同控制被控节点 1、2、3 处的虚拟同步发电机(G1、G2、G3)的功率输入, 在保护 G1、G3 不受振荡影响的情况下, 牺牲 G2 引导发电机 G4、G5 发生振荡。据此, 按照表 1 步骤 1 所述, 分别给定案例一和案例二的目标特征值和特征向量子向量 Λ_1 和 $\boldsymbol{P}_1$, Λ_2 和 $\boldsymbol{P}_2$。其中, Λ_1 和 Λ_2 中各有一个不稳定振荡模态(一对实部为正的共轭特征根), 并在对应特征向量子向量 $\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 中保证 G1 和 G3 没有参与该模态的振荡。

针对以上两个案例, 分别按照表 1 流程构造输出反馈矩阵并将结果代入 $A+BKC$。检验攻击后系统的全部特征值, 其中除了目标特征值外, 其余构造出的特征值实部均为负, 即该系统的不稳定模态只有一个, 满足构造目标。

此外, 本文按照输出反馈的方法构造了不符合最小攻击代价要求的攻击案例三, 用以说明本文提出攻击构造方式和普通的攻击方式在电网振荡节点数量和影响上的区别。三个案例对应的目标特征值、特征向量子向量以及相应的构造结果(构造后的反馈矩阵 $\boldsymbol{K}$、系统全部特征值和不稳定模态对应的特性向量)详见附录 C。下面对系统进行时域仿真, 根据结果分析攻击后系统的振荡特性。其中, 各结果曲线纵坐标数值都为标幺值。

4.2.1 案例一攻击(区域振荡)

在 10s 时通过牺牲虚拟发电机 G2 对系统发起案例一所述攻击, 图 3 反映了攻击开始后各发电机运行状态变化。从图 3 和附录表 C2 可知, G1、G3 在不稳定模态中的活跃程度是 0, 即可以保持自身的稳定运行, 而 G2 作为被牺牲的发电机, 会和系统中发电机 G4、G5 一起振荡。以上攻击成功保证了 G1、G3 的稳定, 实现了攻击成本最低的预期目标。

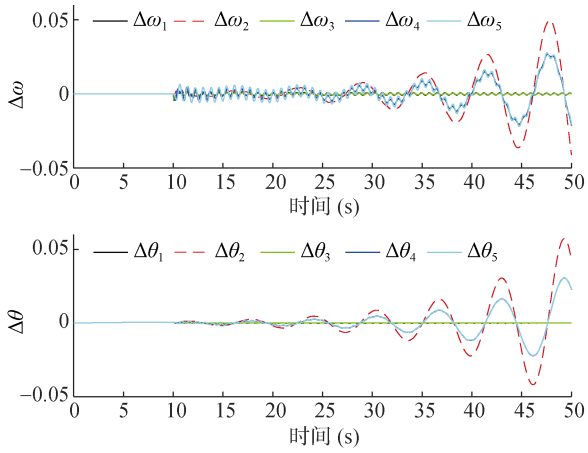

图 3 系统状态量的振荡变化(案例一)

Figure 3 Oscillation of system states (case 1)

由于其他稳定模态衰减较快, 故图中清晰的表现出发散振荡的周期约 1/0.16≈6.25s, 与式(12)中结论相符(不稳定模态 $\eta\pm\gamma i=0.1\pm 1i$, 对应振荡频率 $\gamma/(2\pi)=1/(2\pi)\approx 0.16\text{Hz}$)。同时, G2 和 G4、G5 的振荡趋势是同向变化的(对应附录表 C2 中 G2、G4、G5 的辐角差接近 0°), 符合区域振荡的特性。

4.2.2 案例二攻击(局部振荡)

在 10s 时通过牺牲虚拟发电机 G2 对系统发起案例二的攻击, 图 4 反映了攻击开始后各发电机运行状态变化。由于振荡频率较高, 且系统内的其他稳定模态衰减比较慢, 为便于分析, 图 5 和图 6 展示了系统频率偏差在部分时间段内的变化曲线。图 5 反映了攻击开始 10s 内其他稳定模态的缓慢衰减过程。图 6 反映了其他稳定模态衰减后, 不稳定模态起主导作用的系统频率偏差变化曲线。

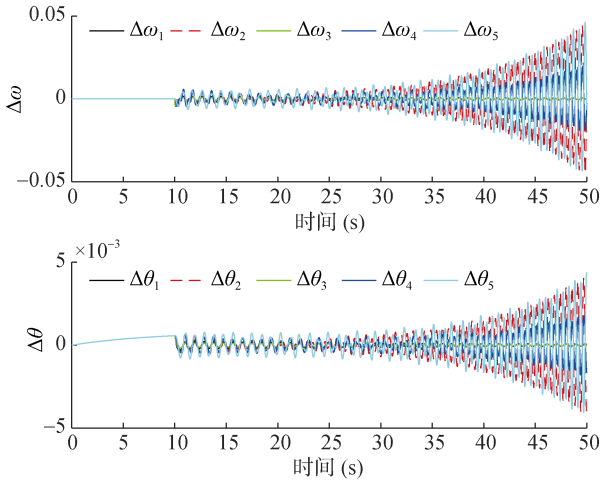

图 4 系统状态量的振荡变化(案例二)

Figure 4 Oscillation of system states (case 2)

从图 4 到图 6 以及附录表 C3 可知, 除虚拟发电机 1、3 外, 其他发电机都在发散振荡。以上攻击在牺牲 G2 的前提下成功保护了 G1、G3, 实现了攻击成本最低的目标。由于主导的不稳定模态是 $0.1\pm11i$, 故图 6 中一个振荡周期约为 0.57s, 同时, 发电机 G2、G4 与发电机 G5 的振荡趋势相反(对应附录表 C3 中发电机 G2、G4 与发电机 G5 的辐角差接近 180°), 符合局部振荡的特性。

4.2.3 案例三攻击(失控振荡)

在 10s 时, 与前面的两个案例类似, 通过协同控制 G1、G2、G3 的功率输入对系统发起案例三的攻击, 图 7 反映了攻击开始后各发电机运行状态变化。从图 7 和附录表 C4 可知, 构造的攻击中有两组不稳定模态 $0.1\pm10i$ 和 $0.1\pm1i$。虽然 G1 和 G3 不参与模态 $0.1\pm10i$, 却参与了模态 $0.1\pm1i$。因此, 在该攻击场景下, 攻击者并不能保护 G1、G2、G3 中任何机组的稳定性, 最终所有的发电机组都会受到攻击的影响而发生振荡。

以上结果表明, 如果攻击者不精心构造攻击以控制振荡过程, 则攻击结果将会影响到攻击者控制的所有发电机组, 大大增加了攻击的成本。

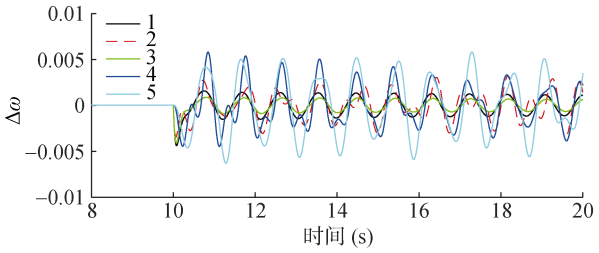

图 5 频率偏差局部曲线 1(案例二)

Figure 5 Part 1 of the frequency deviation curves (case 2)

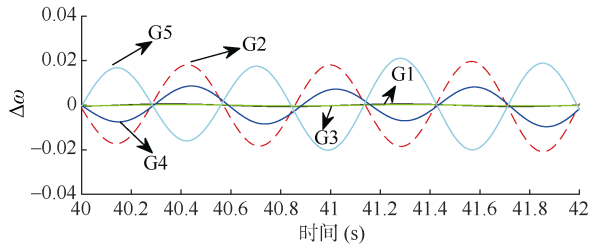

图 6 频率偏差局部曲线 2(案例二)

Figure 6 Part 2 of the frequency deviation curves (case 2)

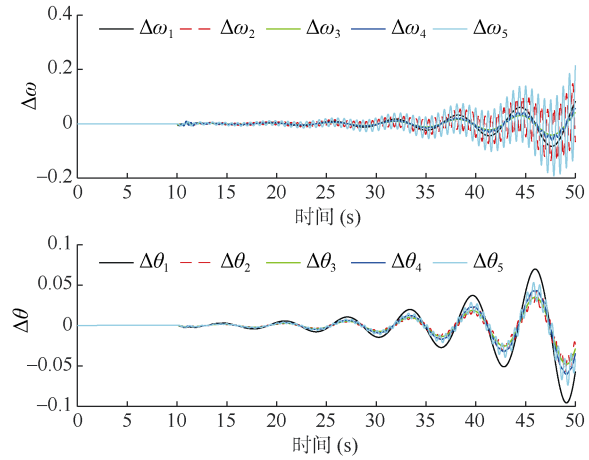

图 7 系统状态量的振荡变化(案例三)

Figure 7 Oscillation of system states (case 3)

4.3 攻击案例检测

本文首先由式(11)计算得到仿真实验中各机组的暂态势能, 然后利用势能数据验证表 2 所述攻击源检测算法有效性。实验中, 滑动窗口采样点数 *win* 设置为 2s 内的采样数据量, 步长 *step* 设置为 1s。

4.3.1 案例一检测(区域振荡)

图 8 展示了攻击案例一发生后从仿真数据中计算得到系统的势能曲线。由图 8 可知, 攻击发生后, 虚拟发电机 G2 所在节点的势能明显占主导地位。

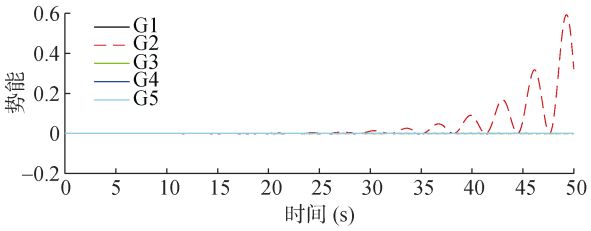

图 8　机组势能变化曲线(案例一)

Figure 8　Potential energy curves of units (case 1)

采用振荡源检测算法分析各节点势能占总体的比重 α_i 进行分析, 其在检测过程中的变化如图 9 所示, 横坐标代表了检测发生的时刻。

由图 8 可知, 攻击发生前(10s 前)系统未检测出明显振荡, 其势能总体量很小, 因此对应这段时间内的图 9 所示势能比重结果对检测没有实际意义, 会在检测算法步骤 5(判断频率偏差的大小)中被过滤掉。同时, 由图 9 可知, 在攻击发生后(10s 以后), 由于其他稳定模态衰减很快, G2 在振荡过程中很快占据主导地位, 因此很容易辨识出 G2 为真正的攻击源。

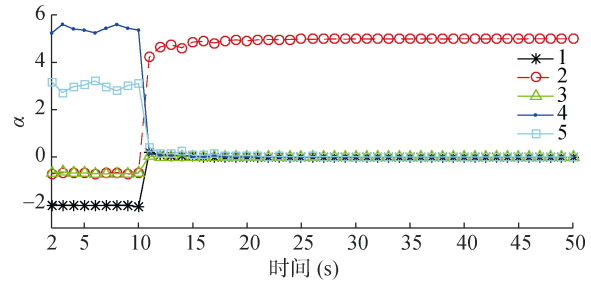

图 9　机组势能比重 α_i 变化曲线(案例一)

Figure 9　Potential energy percentage curves of units (case 1)

4.3.2　案例二检测(局部振荡)

图 10 展示了攻击案例二发生后系统的势能曲线。由于发电机 G2、G4 共同与发电机 G5 发生局部振荡, 故发电机 G5 的振荡势能比重较大。但由于虚拟发电机 G2 主导攻击的发生, 其势能依旧明显占据主导地位。

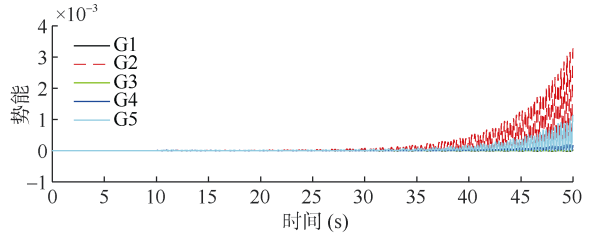

图 10　机组势能变化曲线(案例二)

Figure 10　Potential energy curves of units (case 2)

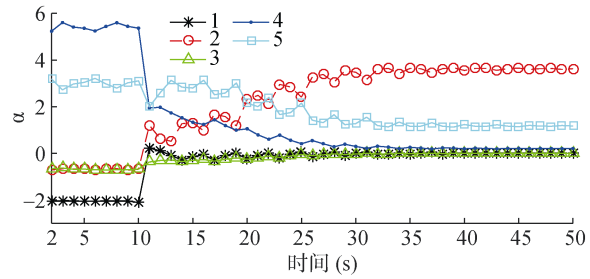

图 11　机组势能比重 α_i 变化曲线(案例二)

Figure 11　Potential energy percentage curves of units (case 2)

类似地, 各节点势能占总体的比重 α_i 在检测过程中的变化如图 11 所示。由图 11 可知, 由于其他模态衰减较慢, 且不稳定模态的增幅相对较缓, 故在攻击发生后机组势能比重曲线变化较平缓, 20s 以后虚拟发电机 2 的势能比重才将持续占据主要地位。因此, 在攻击刚发生 10s 内(10s 到 20s)的过渡过程中, 容易产生误判而将发电机 5 认为是受攻击的节点。然而, 从图 10 可知, 由于该攻击过程较缓, 20s 之前的系统振荡并不显著。通过合理设置表 2 中的参数 η_1 和 η_2, 可利用检测算法步骤 5 过滤掉大部分的干扰数据。同时, 通过结合 20s 后的大量检测数据, 可最终确定真正攻击源在虚拟发电机 G2 所对应节点。

4.3.3　现有检测算法分析

为了说明本文所提出检测算法的必要性, 现对 3.2 小节所述的两大类振荡检测算法进行分析。

Prony 算法可以把时域信号分解成衰减的正弦信号组合形式, 通过线性拟合等处理, 最终可以估算出采样信号的频率、衰减、幅值和初相角等, 并通过检测机组的主导振荡模态确定机组是否异常。在理想情况下, Prony 算法可以完美估计出原始信号的振荡模态信息。然而, 由于本文采取的协同攻击方式引导其他发电机组振荡, 因此检测的结果中无法仅根据主导振荡模态确定出真实的攻击源。例如, 案例一中, 从图 3 易知, G2、G4 和 G5 是三个主要的振荡模态(G2 振幅最大); 案例二中, 从图 6 易知, G2、G4 和 G5 是三个主要的振荡模态(G5 振幅最大)。因此, 采用 Prony 算法的检测结果会将这几个振荡的机组都列为可疑振荡源, 或者产生误判。

基于能量函数的分析方法认为向系统中注入振荡能量(势能增加)的节点是问题机组。然而, 系统内受振荡攻击影响机组的势能都呈现增幅振荡趋势, 因此同样会被认为是振荡源。在案例一种, 由图 8 可知, G2 的势能增长明显占主导地位, 因此该方法可

以大概率判断出 G2 为真实的攻击源。然而, 在案例二中, 由图 10 可知, G2、G4 和 G5 都呈现明显的增幅振荡趋势, 因此该方法会将这三个机组都判断为问题机组。因此, 在本文的协同攻击场景下, 有必要借助机组势能所占比重判定所有振荡机组中真正的攻击源。

5 结论

在大量分布式能源接入智能电网的场景下, 本文提出一种通过控制大量分布式能源使电网发生振荡的最小代价攻击模型, 验证信息-物理攻击对电网安全可靠运行的潜在威胁。本攻击基于输出反馈构建了攻击策略, 保证在牺牲最少被控节点前提下, 使系统内其它发电机节点进入振荡状态。在此基础上, 本文基于振荡能量函数提出了一种启发式的振荡攻击源检测方法, 在攻击实施后可快速评估定位可疑攻击源, 以减轻攻击的危害。后续工作将进一步研究通过牺牲多个节点和构造多个不稳定模态的复杂攻击案例, 以及研究针对该攻击行为的主动式防御方法, 以阻断攻击的实施过程。

参考文献

[1] H. Jiayi, J. Chuanwen, X. Rong, "A review on distributed energy resources and MicroGrid," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 9, pp. 2472-2483, 2008.

[2] J.A.P. Lopes, N. Hatziargyriou, J. Mutale, et al, "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," *Electric Power Systems Research*, vol. 77, no. 9, pp. 1189-1203, 2007.

[3] Z. Lyu, W. Sheng, Q. Zhong, et al, "Virtual synchronous generator and its applications in micro-grid," *Proceedings of the CSEE*, no. 16, pp. 2591-2603, 2014.(In Chinese)
(吕志鹏, 盛万兴, 钟庆昌, 等, "虚拟同步发电机及其在微电网中的应用", *中国电机工程学报*, 2014(16):2591-2603。)

[4] Q. Zhong, G. Weiss, "Synchronverters: inverters that mimic synchronous generators," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 4, pp. 1259-1267, 2011.

[5] J. Alipoor, Y. Miura, T. Ise, "Power system stabilization using virtual synchronous generator with alternating moment of inertia," *IEEE Journal of Emerging & Selected Topics in Power Electronics*, vol. 3, no. 2, pp. 451-458, 2015.

[6] Y. Ma, W. Cao, L. Yang, et al, "Virtual synchronous generator control of full converter wind turbines with short-term energy storage," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 11, pp. 8821-8831, 2017.

[7] Y. Guo, L. Chen, K. Li, et al, "A novel control strategy for stand-alone photovoltaic system based on virtual synchronous generator," in *IEEE Power and Energy Society General Meeting*, pp. 1-5, 2016.

[8] A.T.L. Miguel, L.A.C. Lopes, A.M.T. Luis, et al, "Self-tuning virtual synchronous machine: a control strategy for energy storage systems to support dynamic frequency control," *IEEE Transactions on Energy Conversion*, vol. 29, no. 4, pp. 833-840, 2014.

[9] Z. Zeng, W. Shao, L. Ran, et al, "Mathematical model and strategic energy storage selection of virtual synchronous generators," *Automation of Electric Power Systems*, no. 13, pp. 22-31, 2015. (In Chinese)
(曾正, 邵伟华, 冉立, 等, "虚拟同步发电机的模型及储能单元优化配置", *电力系统自动化*, 2015(13): 22-31。)

[10] Y. Mo, T.H. Kim, K. Brancik, et al, "Cyber--physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-209, 2012.

[11] S. Liu, X. Feng, D. Kundur, et al, "Switched system models for coordinated cyber-physical attack construction and simulation," in *IEEE First International Workshop on Smart Grid Modeling and Simulation*, pp. 49-54, 2011.

[12] J. Staggs, D. Ferlemann, S. Shenoi, "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3-14, 2017.

[13] B. Kang, P. Maynard, K. Mclaughlin, et al, "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *IEEE 20th Conference on Emerging Technologies & Factory Automation*, pp. 1-8, 2015.

[14] "Practical proof-Horus Scenario," W. Westerhof, https:// horusscenario.com/practical-proof/, 2017.

[15] S.V. Buldyrev, R. Parshani, G. Paul, et al, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, p. 1025, 2010.

[16] S. Amini, F. Pasqualetti, H. Mohsenian-Rad, "Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2262-2872, 2016.

[17] S. Amini, H. Mohsenian-Rad, F. Pasqualetti, "Dynamic load altering attacks in smart grid," in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*, pp. 1-5, 2015.

[18] Yi Ping Yu, Yong Min, Lei Chen, et al, "Disturbance source location of forced power oscillation using energy functions," *Automation of Electric Power Systems*, vol. 34, no. 05, pp. 1-6, 2010.(In Chinese)
(余一平, 闵勇, 陈磊, 等, "基于能量函数的强迫功率振荡扰动源定位", *电力系统自动化*, 2010, 34(05): 1-6。)

[19] D. Pudjianto, C. Ramsay, G. Strbac, "Virtual power plant and system integration of distributed energy resources," *IET Renewable Power Generation*, vol. 1, no. 1, pp. 10-16, 2007.

[20] F. Dorfler, F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Transactions on Circuits & Systems I Regular Papers*, vol. 60, no. 1, pp. 150-163, 2013.

[21] Q. Liu, "Power system stability and generator excitation control". China Electric Power Press, 2007. (In Chinese)
(刘取, "电力系统稳定性及发电机励磁控制", 中国电力出版社, 2007。)

[22] C.L. Demarco, J.V. Sariashkar, F. Alvarado, "The potential for malicious control in a competitive power systems environment," in *Proceeding of the 1996 IEEE International Conference on Control Applications*, pp. 462-467, 1996.

[23] S. Srinathkumar, "Eigenvalue/eigenvector assignment using output feedback," *IEEE Transactions on Automatic Control*, vol. 23, no. 1, pp. 79-81, 1978.

[24] M.A. Pai, "Energy function analysis for power system stability". Kluwer Academic Publishers, 1989.

[25] J.F. Hauer, "Application of Prony analysis to the determination of modal content and equivalent models for measured power system response," *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 1062-1068, 1991.

[26] L. Chen, Y. Chen, Y. Min, et al, "Equivalent model of doubly-fed wind turbine generator systems based on auto mutation particle swarm optimization algorithm," *Automation of Electric Power Systems*, vol. 36, no. 04, pp. 1-5, 2012.(In Chinese)
(陈磊, 陈亦平, 闵勇, 等, "基于振荡能量的低频振荡分析与振荡源定位(二)振荡源定位方法与算例", *电力系统自动化*, 2012, 36(04): 1-5。)

附录 A

由式(9)计算得到式(10)的推导过程表述如下:

首先将式(9)拆分可得两个子方程组:

$$\begin{bmatrix} A_{11} & A_{12} \end{bmatrix}\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} + B_1 KC\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} = \hat{\lambda}_c \hat{p}_c \tag{A-1}$$

$$\begin{bmatrix} A_{21} & A_{22} \end{bmatrix}\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} + B_2 KC\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} = \hat{\lambda}_c \hat{q}_c \tag{A-2}$$

将式(A-1)两边左乘矩阵 $B_2 B_1^{-1}$, 可得:

$$\begin{aligned} &B_2 B_1^{-1}\begin{bmatrix} A_{11} & A_{12} \end{bmatrix}\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} + B_2 KC\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} \\ &= B_2 B_1^{-1}\hat{\lambda}_c \hat{p}_c \end{aligned} \tag{A-3}$$

式(A-2)减去式(A-3), 可得:

$$\begin{aligned} &\begin{bmatrix} A_{21} & A_{22} \end{bmatrix}\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} - B_2 B_1^{-1}\begin{bmatrix} A_{11} & A_{12} \end{bmatrix}\begin{bmatrix} \hat{p}_c \\ \hat{q}_c \end{bmatrix} \\ &= \hat{\lambda}_c \hat{q}_c - B_2 B_1^{-1}\hat{\lambda}_c \hat{p}_c \end{aligned}$$

进一步整理可得:

$$\begin{aligned} &[(A_{21} - B_2 B_1^{-1} A_{11}) + \hat{\lambda}_c B_2 B_1^{-1}]\hat{p}_c = \\ &[\hat{\lambda}_c I_{n-m} - (A_{22} - B_2 B_1^{-1} A_{12})]\hat{q}_c \end{aligned}$$

两边左乘$[(A_{21} - B_2 B_1^{-1} A_{11}) + \hat{\lambda}_c B_2 B_1^{-1}]^{-1}$, 即可得式(10)。

由式(11)计算得到式(12)的推导过程表述如下:

由式(11)拆分其上半部分可得方程: $(A_1 + B_1 KC)V = P\Lambda$, 即 $B_1 KCV = P\Lambda - A_1 V$。两边左乘 B_1^{-1}, 右乘$[CV]^{-1}$, 即可得式(12)。

附录 B

IEEE-14bus 系统状态空间方程参数如下:

$\boldsymbol{A} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, 其中:

$A_{11} = diag(-0.0754, -0.1077, -0.1077, -0.2513, -0.1946)$,

$$A_{12} = \begin{bmatrix} -199.4235 & 180.4162 & 6.3879 & 9.5592 & 3.0602 \\ 243.509 & -386.0927 & 97.6856 & 30.4570 & 14.4410 \\ 7.6282 & 90.0311 & -119.1232 & 12.6939 & 8.77 \\ 30.9971 & 67.2109 & 28.9808 & -171.9813 & 44.7925 \\ 7.9334 & 25.4575 & 15.4448 & 33.5227 & -82.3584 \end{bmatrix},$$

$A_{21} = \mathbf{I}_{5\times 5}$(单位矩阵), $A_{22} = [\mathbf{0}]_{5\times 5}$(零矩阵);

$$B^T = \begin{bmatrix} 13.46 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 13.46 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 13.46 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix};$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}。$$

附录 C

案例一和案例二的目标特征值和特征向量子向量 Λ_1 和 $\boldsymbol{P}_1$, Λ_2 和 $\boldsymbol{P}_2$ 分别表述如下:

$$\begin{aligned} &\Lambda_1 = diag(-10+12i, -10-12i, 0.1+1i, 0.1-1i, -3+1i, -3-1i) \\ &\Lambda_2 = diag(-10+12i, -10-12i, 0.1+11i, 0.1-11i, -3+1i, -3-1i) \end{aligned},$$

$$\boldsymbol{P}_1 = \boldsymbol{P}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}。$$

攻击案例一对应的反馈矩阵 $\boldsymbol{K}_1$ 为:

$$\boldsymbol{K}_1 = \begin{bmatrix} 0.5675 & 0.0025 & -2.0804 & 30.6453 & -13.9032 & -34.3596 \\ 0.9121 & 0.0319 & -2.5247 & -3.6976 & 26.8331 & -39.3484 \\ 0.9723 & 0.0045 & -2.5016 & 15.3357 & -7.5380 & -24.9580 \end{bmatrix}$$

攻击案例二对应的反馈矩阵 $\boldsymbol{K}_2$ 为:

$$\boldsymbol{K}_2 = \begin{bmatrix} 0.5675 & 0.0061 & -2.0840 & 30.6453 & -13.4697 & -34.7931 \\ 0.9121 & 0.0437 & -2.5365 & -3.6976 & 19.8386 & -32.3539 \\ 0.9723 & 0.0095 & -2.5066 & 15.3357 & -6.4209 & -26.0751 \end{bmatrix}$$

表 C1 攻击案例一和二前后特征值结果对比

Table C1 Eigenvalues before and after attack case 1 & 2

初始特征值	配置后特征值(案例一)	配置后特征值(案例二)
–0.0500 +23.1912i	**–10.0000 – 12.0000i**	**–10.0000 – 12.0000i**
–0.0500 –23.1912i	**–10.0000 + 12.0000i**	**–10.0000 + 12.0000i**
–0.0002	–0.2495 – 13.7472i	–0.1913 – 14.0106i
–0.1234	–0.2495 + 13.7472i	**0.1000 – 11.0000i**
–0.0884 + 9.1444i	–0.0203 – 8.0157i	–0.0332 – 6.7902i
–0.0884 – 9.1444i	–0.0203 + 8.0157i	**–3.0000 – 1.0000i**
–0.1187 +13.9015i	**–3.0000 – 1.0000i**	**–3.0000 + 1.0000i**
–0.1187 –13.9015i	**–3.0000 + 1.0000i**	–0.1913 + 14.0106i
–0.0494 +12.0101i	**0.1000 – 1.0000i**	–0.0332 + 6.7902i
–0.0494 –12.0101i	**0.1000 + 1.0000i**	**0.1000 + 11.0000i**

表 C2 攻击案例一不稳定模态对应特征向量

Table C2 Eigenvector for unstable mode in attack case 1

状态量	特征向量	
	$\hat{\lambda}_1$=0.1+1i	$\hat{\lambda}_2$=0.1−1i
$\Delta\omega_1$	**0.0000 – 0.0000i**	**0.0000 + 0.0000i**
$\Delta\omega_2$	0.5664	0.5664
$\Delta\omega_3$	**0.0000 – 0.0000i**	**0.0000 + 0.0000i**
$\Delta\omega_4$	0.3015 – 0.0013i	0.3015 + 0.0013i
$\Delta\omega_5$	0.3013 – 0.0020i	0.3013 + 0.0020i
$\Delta\delta_1$	**–0.0000 – 0.0000i**	**–0.0000 + 0.0000i**
$\Delta\delta_2$	0.0561 – 0.5608i	0.0561 + 0.5608i
$\Delta\delta_3$	**–0.0000 – 0.0000i**	**–0.0000 + 0.0000i**
$\Delta\delta_4$	0.0285 – 0.2987i	0.0285 + 0.2987i
$\Delta\delta_5$	0.0278 – 0.2985i	0.0278 + 0.2985i

攻击案例三的目标特征值和特征向量子向量 Λ_3 和 $\boldsymbol{P}_3$ 分别表述如下:

$$\Lambda_3 = \mathrm{diag}(-10+12i,-10-12i,0.1+10i,0.1-10i,0.1+1i,0.1-1i),$$

$$\boldsymbol{P}_3 = \begin{bmatrix} 1 & 1 & 0 & 0 & 2 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}。$$

攻击案例三对应的反馈矩阵 $\boldsymbol{K}_3$ 为:

$$\boldsymbol{K}_3 = \begin{bmatrix} 0.2476 & 0.0100 & -0.4586 & 24.9328 & -13.0900 & -22.3294 \\ 0.3693 & 0.0599 & -0.7548 & -9.9600 & 22.7608 & -21.7799 \\ 0.2510 & 0.0185 & -0.4873 & 8.5012 & -5.7638 & -12.2453 \end{bmatrix}$$

表 C3 攻击案例二不稳定模态对应特征向量

Table C3 Eigenvector for unstable mode in attack case 2

状态量	特征向量	
	$\hat{\lambda}_1$=0.1−1i	$\hat{\lambda}_2$=0.1+1i
$\Delta\omega_1$	**–0.0000 – 0.0000i**	**–0.0000 + 0.0000i**
$\Delta\omega_2$	–0.6684 – 0.0295i	–0.6684 + 0.0295i
$\Delta\omega_3$	**–0.0000 – 0.0000i**	**–0.0000 + 0.0000i**
$\Delta\omega_4$	–0.2765 – 0.0658i	–0.2765 + 0.0658i
$\Delta\omega_5$	0.6807 + 0.0000i	0.6807 + 0.0000i
$\Delta\delta_1$	**0.0000 – 0.0000i**	**0.0000 + 0.0000i**
$\Delta\delta_2$	0.0021 – 0.0608i	0.0021 + 0.0608i
$\Delta\delta_3$	**0.0000 – 0.0000i**	**0.0000 + 0.0000i**
$\Delta\delta_4$	0.0057 – 0.0252i	0.0057 + 0.0252i
$\Delta\delta_5$	0.0006 + 0.0619i	0.0006 – 0.0619i

表 C4 攻击案例三不稳定模态对应特征向量

Table C4 Eigenvector for unstable mode in attack case 3

状态量	特征向量	
	$\hat{\lambda}_1$=0.1±10i	$\hat{\lambda}_2$=0.1±i
$\Delta\omega_1$	**–0.0000 ∓ 0.0000i**	**0.4725 ± 0.0000i**
$\Delta\omega_2$	–0.5579 ± 0.0568i	0.2362 ± 0.0000i
$\Delta\omega_3$	**0.0000 ∓ 0.0000i**	**0.2362 ± 0.0000i**
$\Delta\omega_4$	–0.0072 ± 0.0534i	0.2933 ∓ 0.0013i
$\Delta\omega_5$	0.8202 ± 0.0000i	0.2856 ∓ 0.0019i
$\Delta\delta_1$	**–0.0000 ∓ 0.0000i**	**0.0468 ∓ 0.4678i**
$\Delta\delta_2$	0.0051 ± 0.0558i	0.0234 ∓ 0.2339i
$\Delta\delta_3$	**–0.0000 ∓ 0.0000i**	**0.0234 ∓ 0.2339i**
$\Delta\delta_4$	0.0053 ± 0.0008i	0.0278 ∓ 0.2905i
$\Delta\delta_5$	0.0008 ∓ 0.0820i	0.0264 ∓ 0.2830i

刘杨 于 2012 年在西安交通大学自动化专业获得学士学位。现在西安交通大学控制科学与工程专业攻读博士学位。研究领域为智能电网安全。研究兴趣包括：基础量测设施安全、通信安全。Email: yliu@seil.xjtu.edu.cn

桂宇虹 于 2015 年在西安交通大学自动化专业获得硕士学位。研究领域为智能电网安全与优化。研究兴趣包括: 电力系统状态估计、电力系统稳定性分析。Email: yhgui@sei.xjtu.edu.cn

安豆 于 2017 年在西安交通大学自动化专业获得博士学位。现任西安交通大学讲师。研究领域为: 信息物理融合系统。研究兴趣包括：智能电网信息安全、智能电网需求侧能源管理。Email: douan2017@xjtu.edu.cn

管晓宏 于 1993 年获美国康涅狄格大学博士学位。现任中国科学院院士, 西安交通大学和清华大学双聘教授。研究领域为: 复杂网络系统、能源电力系统优化与安全。研究兴趣包括: 智能电网、网络安全、生产制造系统以及电力市场的规划和调度。E-mail: xhguan@mail.xjtu.edu.cn

刘烃 于 2010 年在西安交通大学自动化专业获得博士学位。现任西安交通大学教授, 网络空间安全学院副院长。研究领域为信息物理融合系统、软件系统。研究兴趣包括: 智能电网漏洞与入侵检测、楼宇综合安全节能优化、软件行为建模与遗传检测、软件测试和验证。Email: tingliu@mail.xjtu.edu.cn