计及 EV 源荷双向性的配电网 CPS 攻防策略

王义贺[1,2]，张明理[2]，程孟增[2]，刘 凯[2]，满林坤[2]
(1.东北大学 信息科学与工程学院，辽宁 沈阳 110819；2.国网辽宁省电力有限公司经济技术研究院，辽宁 沈阳 110015)

摘 要：随着电动汽车的大规模并网，配电网对新能源的消纳能力大幅提升，但同时充电桩的低安全性、高可及性也进一步降低了配电网网络安全。文章首先提出一种基于一致性算法的分布式能量管理策略，将电动汽车集群视为具有源-荷双向特性的储能设备，以实现完全分布式经济调度。考虑到通信延时下，拒绝服务攻击以及面向电动汽车的新型数据完整性攻击的存在，提出了一种结合隐私保护协议和隔离机制的抗扰控制策略，以实现网络攻击下系统的能量有效管理及经济运行。最后通过算例仿真对比，验证了该加密机制的有效性及控制策略的可行性。

关键词：电动汽车；分布式能量管理；一致性算法；源-荷双向
中图分类号：TK81 **文献标志码**：A **文章编号**：1671-5292(2024)07-0955-09

0 引言

随着分布式电源，包括分布式发电机(DG)和分布式储能(DES)的广泛接入和智能电网建设的不断发展，配电网逐渐成为一种活跃的、可控制、灵活的主动配电网信息物理系统(CPS)。CPS 的发展不仅提高了电网系统的控制能力，也为电力基础设施建设提供了条件。然而，智能设备构建的感知和控制层受到网络攻击的风险较高，用于经济调度和能源管理的分布式电源和储能设备也会受到影响。

可移动式储能设备电动汽车(Electric Vehicle，EV）的用电行为导致电力系统负荷发生一定变化，如负荷波动性增大，随机性增加，负荷峰谷差增大等。上述变化给电网的运行带来了一定的影响，因此国内外学者对 EV 并网进行了相关研究。文献[1]提出了一种分层分布式的优化控制框架，使电动汽车管理系统(EVMS)成为配电网管理系统的一部分，与控制配电网馈线电动汽车充电负荷的电动汽车聚合器通信，使电网负荷变化最小。文献[2-5]利用电动汽车作为集合器[6]，参与电网调峰、时变延迟调频、充电规划和基于分布式位置边际定价的最优调度[7-15]。然而，目前鲜有针对电力信息物理系统中 EV 并网控制的研究。

目前，一致性算法已被用于解决智能电网的负荷损失[16]、经济调度和插电式电动汽车充电规划[17]等问题。然而，现有的基于一致性算法的分布式控制假设邻居间通信是可信的，该假设与实际应用并不完全一致。基于上述内容，本文提出一种基于一致性算法的实时分布式能量管理策略，在配电网中的微网接口设置一个虚拟的领导者智能体，用于实现大量电动汽车并网的能量最优调度。针对可能出现的网络攻击(拒绝服务攻击、数据完整性攻击)，设计一种隐私保护协议和隔离机制，通过更新声望值权重，将受到攻击的分布式电源从通信网络中逐渐边缘化甚至隔离，实现网络攻击下的稳定运行。

1 考虑通信延时的一致性算法

一致性算法的本质为通过本地节点与邻居节点相互通信，更新本地节点的状态量，使网络拓扑中的所有节点状态量收敛至相同的稳态值。考虑系统中各节点间通信存在可变延时的情况时，一致性算法可表示为

$$\dot{x}_n(t)=-\boldsymbol{L}\{\delta(t)x(t-\tau)+[1-\delta(t)x(t-\tau)]\} \quad (1)$$

式中：$\dot{x}_n(t)$为第 n 个智能体的系统动态特性；$\boldsymbol{L}$ 为多智能体网络拓扑结构连通图的拉普拉斯矩阵；$\delta(t)$为随机变量。

其中定义随机变量：

收稿日期：2023-07-19。
基金项目：国网辽宁省电力有限公司科技项目(2020YF-19)。
通信作者：程孟增(1987-)，男，博士，高级工程师，研究方向为电力系统。E-mail：tuda_t@163.com

$$\delta(t)=\begin{cases}0 & \tau=0\\ 1 & \tau\neq 0\end{cases} \tag{2}$$

2 分布式能量管理

2.1 基于一致性算法的能量管理策略

能量管理问题为电力系统最基本的问题之一,决定了电网的稳定运行点,使得某一条件(发电成本或能量损耗)最小。本文考虑电动汽车的源荷双向性,将其视为分布式储能设备[18,19]。能源管理问题被表述为一个离线优化问题,以尽量减少在一定时间范围内的发电成本,即:

$$\begin{aligned}\min C=\min &\sum_{t=1}^{T}\left\{\sum_{i\in N_g}\left[\alpha_i p_{g,i}^{2}(t)+\beta_i p_{g,i}(t)+\gamma_i\right]\right\}+\\ &\sum_{t=1}^{T}\left\{\sum_{i\in N_b} a_i\left[p_{b,i}(t)+b_i\right]^2\right\}+\\ &\sum_{t=1}^{T}\left\{\begin{aligned}&\sum_{i\in N_e} a_{e,i}\left[\sum_i \eta_{e,i}p_{e,i}(t)\right]^2+\\ &b_{e,i}\left[\sum_i \eta_{e,i}p_{e,i}(t)\right]+c_{e,i}\end{aligned}\right.\end{aligned} \tag{3}$$

式中:C 为系统运行总成本;第一项为 DGs 的运行总成本;第二项为融合电动汽车集群的储能设备的运行总成本;第三项为 t 时刻电动汽车集群发电成本;N_g 为 DG 所在节点的集合;$p_{g,i}(t)$ 为第 i 个 DG 在 t 时刻的电出力;$\alpha_i,\beta_i,\gamma_i$ 为第 i 个DG 的费用系数;N_b 为储能设备所在节点的集合;$p_{b,i}(t)$ 为第 i 个储能设备在 t 时刻的功率需求;a_i,b_i 为第 i 个储能设备功率交换成本参数;$p_{e,i}(t)$ 为第 i 个电动汽车集群在 t 时刻向微网放电功率;$a_{e,i},b_{e,i},c_{e,i}$ 为第 i 个电动汽车集群的发电成本系数;$\eta_{e,i}$ 为第 i 个电动汽车集群的能量反转效率。

目标函数的约束条件为

$$\forall t\in T,\ \sum_{g\in G}p_g(t)+\sum_{b\in B}p_b(t)+\sum_{e\in E}p_e(t)=P_L \tag{4}$$

$$P_L=P_d+P_{loss} \tag{5}$$

$$p_{g,i}^{t,\mathrm{down}}\le p_{g,i}^{t}\le p_{g,i}^{t,\mathrm{up}} \tag{6}$$

$$p_{b,i}^{t,\mathrm{down}}\le p_{b,i}^{t}\le p_{b,i}^{t,\mathrm{up}} \tag{7}$$

$$p_{e,i}^{t,\mathrm{down}}\le p_{e,i}^{t}\le p_{e,i}^{t,\mathrm{up}} \tag{8}$$

$$p_{l,line}^{\mathrm{down}}\le p_{l,line}\le p_{l,line}^{\mathrm{up}} \tag{9}$$

式中:P_L 为微网系统内的总负荷需求;P_d,P_{loss} 分别为负荷需求与对应的电网网损功率。

式(4),(5)为在每个时间步长,系统内发电功率与负荷需求相平衡;式(6)~(8)为各机组出力约束式;式(9)为第 l 条物理传输线可传输的电功率下界和上界。DGs、储能设备及 EV Aggregator 的出力值/充放电值受其物理容量限制。

为了解决分布式能源管理策略(3)~(9)的问题,本文采用一种典型的分布式双一致性算法[20],实现了分布式能源连接管理和最优控制。核心思想是设计两套一致性协议,其中一个用于更新局部功率的估计值平衡供需,另一个用于更新系统增量成本调整能源设备的出力,算法迭代过程可参考文献[21],这里不再赘述。通过使用特征值扰动方法,已有工作证明[20]基于一致性的分布式算法将会收敛到最优值。

$$\begin{aligned}\forall t\in T:&\lim_{k\to\infty}\lambda_i^k(t)==\lambda^*(t),\lim_{k\to\infty}\Delta P_i^k(t)=0,\\ &\lim_{k\to\infty}\Delta P_i^k(t)=P_i^*(t)\end{aligned} \tag{10}$$

2.2 事件触发机制

将事件触发机制引入一致性算法中,可合理地解决通信消耗问题。不同于理论模型研究,本部分采用的局部节点事件触发机制并不需要掌握 Laplace 矩阵的特征值相关信息,通信拓扑的连通性要求不高,前文提出的分布式一致性算法可以保证在各机组出力阈值范围内系统稳定运行,实现经济调度。本文设计的局部节点事件触发机制如下:①设置系统参数,并根据系统拓扑设定邻接矩阵;②设定误差函数 $e_i(t)$ 及局部节点的事件触发函数 $l_i(t)$,定义 $e_i(t)=[e_1(t),e_2(t),\cdots,e_n(t)]^{\mathrm{T}}$,误差函数为

$$e(t)=\tilde{\boldsymbol{\lambda}}(t)-\boldsymbol{\lambda}(t),t\in[t_k,t_{k+1}] \tag{11}$$

其中 $\tilde{\boldsymbol{\lambda}}(t)=[\tilde{\lambda}_1(t),\tilde{\lambda}_2(t),\cdots,\tilde{\lambda}_n(t)]^{\mathrm{T}}$,表示在前一次触发时刻增量成本的状态向量与实时状态量的误差,定义误差向量为 $\boldsymbol{\varepsilon}_0=\boldsymbol{\lambda}(t)-\lambda^*1^{\mathrm{T}}$ 事件触发函数为

$$l_i(t)=\|e(t)\|-\frac{\varpi(1-\tilde{\varpi})\|\boldsymbol{\varepsilon}_0\|}{N_i^+\|W\|} \tag{12}$$

式中:ϖ,$\tilde{\varpi}$ 为 $(0,1/N_i^+)$ 的常数,此时系统间通信通过判定该触发函数的正负判定误差是否在阈值内,当 $l_i(t)>0$ 时更新智能体信息。

③依据①,②提供的系统参数和触发函数系统内各节点进行网络通信,此时各智能体间的增量成本、发电量及功率偏差按式(7)~(9)的规则

进行迭代。

3　网络攻击

3.1　拒绝服务攻击

拒绝服务攻击(Denial of Service,DoS)主要通过以下两种方式同时影响多智能体系统[22]:①局部传感器无法传递状态量测值;②智能体之间的通信被切断。与周期性DoS建模相比,本文提出了一种更一般的DoS类型,其中并没有针对DoS的性质考虑特定的攻击模式,且不单独限制每次攻击发起时刻。

3.2　数据完整性攻击

本文考虑可控分布式储能设备$U(U\in B)$受到网络攻击,攻击者的攻击目标为在满足系统物理约束的前提下,实现攻击者自身利益的最大化。由于经济调度问题一般与实时电价相关,因此本文假设所有设备均可获得电价信息,在衡量攻击效果时,加入不同电价情景的考虑。

攻击者只需要从目标的邻居获取局部信息,就可以实现攻击,如局部容量和局部功率等。将一致性算法[23,24]重新定义为

$$\lambda_i^{k+1}(t)=\boldsymbol{M}\{\delta(t)\lambda_i^{k}(t-\tau_i)+[1-\delta(t)]\lambda_i^{k}(t)\}+\eta\Delta P_i^{k}(t)+\mu_i^{\lambda}(t) \tag{13}$$

$$P_i^{k+1}(t)=\delta(t)\mu_i^{x}(t-\tau_i)+[1-\delta(t)\mu_i^{x}(t)] \tag{14}$$

$$\Delta P_i^{k+1}(t)=\boldsymbol{N}\Delta P_i^{k}(t)-[P_i^{k+1}(t)-P_i^{k}(t)]+\mu_i^{y}(t) \tag{15}$$

式中:$\mu_i^{x}(t),\mu_i^{y}(t)\in\boldsymbol{N}$;$\boldsymbol{M},\boldsymbol{N}$均为系统参数矩阵。

当储能设备i受攻击时,$\mu_i^{x}(t)\equiv0$。对式(13)~(15)重新整理得到:

$$\begin{bmatrix}\lambda(k+1)\\ \Delta P(k+1)\end{bmatrix}=\begin{bmatrix}\boldsymbol{M} & \eta I\\ Z(I-\boldsymbol{M}) & \boldsymbol{N}-\eta Z\end{bmatrix}\cdot\left\{\delta\begin{bmatrix}\lambda(k-\tau)\\ \Delta P(k)\end{bmatrix}+(1-\delta)\begin{bmatrix}\lambda(k)\\ \Delta P(k)\end{bmatrix}\right\}-\begin{bmatrix}0\\ \Delta B(k)\end{bmatrix}+\begin{bmatrix}\boldsymbol{\mu}^{\lambda}(k)\\ \boldsymbol{\mu}^{p}(k)\end{bmatrix} \tag{16}$$

式中:$\boldsymbol{\mu}^{\lambda}$为攻击者注入到每个节点的增量成本中的虚假数据向量;$\boldsymbol{\mu}^{p}$为攻击者注入到每个节点的局部功率偏差估计中的虚假数据向量。

假设在迭代过程中,第S1与S2次存在网络攻击,且$s_2>s_1$,攻击者分别发送虚假信息$\Delta P_{U,u}^{s_1}$,$\Delta P_{U,u}^{s_2}$,则两次攻击所造成的功率偏差值为简单的加和形式。因此,攻击者可以将攻击效果分为多次迭代来限制攻击幅度,降低被发现概率。

当注入攻击成功时,增量成本估计收敛到一个稳定点,但此时并不是最优的[25]。收敛结果为

$$\forall t\in T:\lim_{k\to\infty}\lambda_i^{k}(t)==\vec{\lambda}(t),\lim_{k\to\infty}\Delta P_i^{k}(t)=0,\lim_{k\to\infty}\Delta P_i^{k}(t)=\vec{P}_i(t) \tag{17}$$

式中:$\lambda^{*}\neq\vec{\lambda}$,$P^{*}\neq\vec{P}$,在这种情况下,能量管理问题的解决方案并不符合系统的最低运行成本。

4　基于加密机制的控制策略

4.1　加密机制

为了解决信息安全问题,本文提出了一种加密机制作为抵御攻击的第一道防线。在分布式经济调度中引入噪声项来掩盖智能体之间传递的迭代信息,使攻击者无法直接获得影响经济调度的关键信息的真实值。设置时变噪声项向量$\boldsymbol{r}^{\lambda}(k)$和$\boldsymbol{r}^{p}(k)$,并将其嵌入到分布式能量管理算法中,即:

$$\begin{bmatrix}\lambda(k+1)\\ \Delta P(k+1)\end{bmatrix}=\begin{bmatrix}\boldsymbol{M} & \eta I\\ Z(I-\boldsymbol{M}) & \boldsymbol{N}-\eta Z\end{bmatrix}\cdot\left\{\delta\begin{bmatrix}\lambda(k-\tau)\\ \Delta P(k)\end{bmatrix}+(1-\delta)\begin{bmatrix}\lambda(k)\\ \Delta P(k)\end{bmatrix}\right\}-\begin{bmatrix}0\\ \Delta B(k)\end{bmatrix}+\begin{bmatrix}\boldsymbol{r}^{\lambda}(k)\\ \boldsymbol{r}^{p}(k)\end{bmatrix} \tag{18}$$

本文提出的嵌入式加密机制本质上是一种特殊的网络攻击;不同之处在于,本文提出的噪声项来自于系统内部,它主动增加了对传输的迭代信息的干扰。本文干扰向量也需要满足以下条件:

$$\sum_{k=0}^{\infty}\left|r_i^{\lambda}(k)\right|\le\upsilon,\sum_{k=0}^{\infty}\left|r_i^{p}(k)\right|\le\upsilon,\sum_{j=0}^{k}\sum_{i\in V}r_i^{p}(j)=0 \tag{19}$$

为了防止加密机制被攻击者窃取,系统会定期重新分配噪声项。通过结合下面的防御策略,在任何通信条件下,系统的所有单元噪声项之和均为0。

考虑到引入时滞后算法的稳定性,对式(17)进行重定义:

$$\Gamma=\begin{bmatrix}\boldsymbol{M} & 0\\ Z(I-\boldsymbol{M}) & \boldsymbol{N}\end{bmatrix},\Lambda=\begin{bmatrix}0 & I\\ 0 & -\boldsymbol{N}\end{bmatrix},\Psi=\begin{bmatrix}\boldsymbol{r}^{\lambda}(k)\\ \boldsymbol{r}^{p}(k)\end{bmatrix} \tag{20}$$

此时系统可视作受 Γ,$\eta\Lambda$ 与 Ψ 的扰动,由文献[26]可得,当 η 特别小时,表征系统受时延影响部分的两个特征值与其扰动量 $\eta\Lambda$ 可由 K 来量化,且:

$$K=\begin{bmatrix} 0 & 0 \\ -\dfrac{\lambda_1}{\eta^*} & \lambda_1 \end{bmatrix} \tag{21}$$

式中:$\lambda_1(\lambda_1<0)$和 0 分别为 K 的两个特征值。

因此,矩阵 Γ 的两个特征值分别关于 η 的导数为零和导数为负,即当 η 增大时,其中一特征值不变,另一特征值逐渐减小。而 $\Gamma+\eta\Lambda$ 的其他特征值则受 $\eta\Lambda$ 的影响,因此当选定 η 取值为某一闭区间时,会始终存在一个值为 1 的特征值,其余特征值均在单位圆内,也就是说在式(17)中,当 $k\to\infty$ 时,$\Delta P\to 0$。

4.2 网络攻击下的防御策略

本文针对不同网络攻击设置了相应的检测算法和基于邻居监视子网络的防御策略。监视子网络本质上是通信网络的一个衍生子网,来自子网络的观测结果仅用于传输网络攻击的检测结果和监控相邻单元的行为。本文提出的数据完整性攻击,被攻击的智能体向其邻居智能体发送错误请求,二者构成共谋智能体。此时,即使被邻居智能体检测到异常,也不会激活相应的隔离过程,异常智能体始终与共谋智能体连接,错误的更新信息会传播到整个网络,扰乱系统的正常运行。基于上述情况,本文提出了一种针对上述攻击的隔离算法,即:

$$Num_{ij}(k)=\begin{cases} Num_{ij}(k-1)+1, o_j(k)=1 \\ Num_{ij}(k-1), o_j(k)=0 \end{cases} \tag{22}$$

式(22)为定义的计数规则,以记录在通信链路上正常通信的次数,初始值设置为 0。

声望值辅助变量以适应分布式经济调度算法,即:

$$rep_{ij}(k)=\frac{\omega_k Num_{ij}(k)+1}{\omega_k k+1} \tag{23}$$

式中:ω_k 为时变声望参数,用于动态调整适应率,声望值在[0,1]。正常状态下,智能体的声望值为 1。

一致性算法中的权重更新矩阵 $\boldsymbol{M}$,$\boldsymbol{N}$ 与通信网络拓扑中的连接信息有关,即与智能体的声望值有关,矩阵各元素的变化规律服从:

$$m_{ij}(k)=\frac{[rep_{ij}(k)]^+_{rep_{ij}'}}{\sum_{l\in N_i^+}[rep_{il}(k)]^+_{rep_{ij}'}} \tag{24}$$

$$n_{ij}(k)=\frac{[rep_{ij}(k)]^+_{rep_{ij}'}}{\sum_{l\in N_j^-}[rep_{lj}(k)]^-_{rep_{lj}'}} \tag{25}$$

定义的拓扑矩阵 $\boldsymbol{F}(k)=[f_{ij}(k)]^{n\times n}$ 的更新规则,用于记录观测子网中的拓扑连接信息,即:

$$f_{ij}=\begin{cases} 1, & (j,i)\in E' \\ 0, & (j,i)\notin E' \end{cases} \tag{26}$$

式中:E'为通信网络中所有边的集合。

5 仿真及结果分析

本文使用 IEEE-39 节点进行案例仿真,在 Matlab2014b 环境中构建仿真测试平台。39 节点分布式微电网的配置和通信拓扑结构如图 1 所示。通信模式为点对点模式。

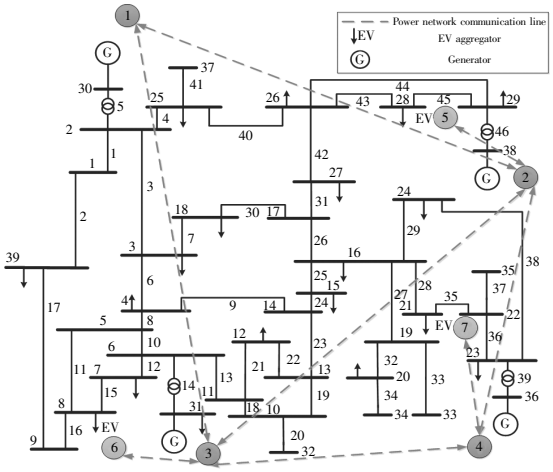


图 1 39 节点测试系统通信拓扑图

Fig.1 The communication topology diagram corresponding to the 39-node test system

测试系统包括 4 个分布式发电机组(1,3 为风电机组)和 3 个电动汽车集群,通过分布式通信网络进行通信,相关数据如表 1,2 所示。学习增益设定为 0.005。

表 1 风电机组的电气参数

Table 1 Electrical parameters of wind turbines

参数	数值	参数	数值
型号	GW82/1500	切出风速/m·s^{-1}	10.3
额定功率/kW	1 500	最大安全风速/m·s^{-1}	52.5
切入风速/m·s^{-1}	3	运行温度/℃	-30~+40
额定风速/m·s^{-1}	10.3	超低温后再启/℃	≥28

表 2　EV 的电气参数

Table 2 Electrical parameters of EV

参数	数值
充电时间/h	0.5~9
最大功率/kW	100
最大扭矩/N·m	180
百公里耗电/kW·h	12.8
电池容量/kW·h	53.6

为了验证延时的随机性,在系统每个采样时间生成随机变量,以保证每次采样时调用随机矩阵中对应的元素,如图 2 所示。其中,$\delta(t)=0$ 的概率设定为 0.8,通信延时 $\tau\in[0,1.5]$。

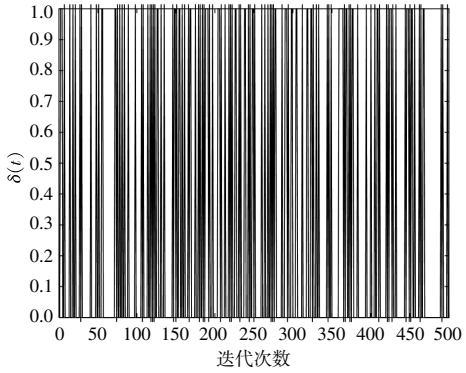
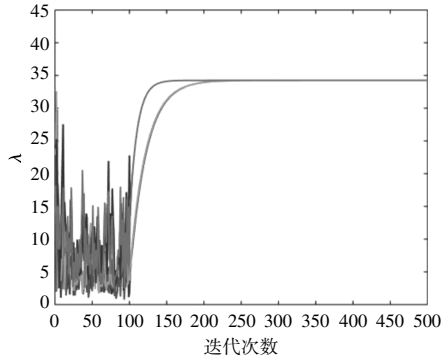


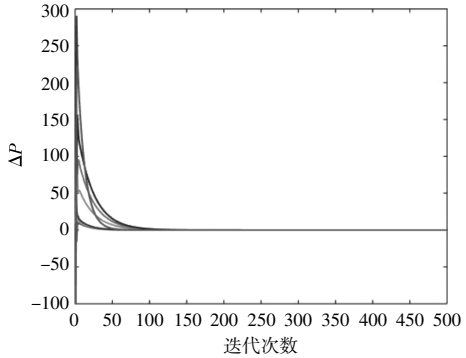
图 2　随机矩阵

Fig.2 Random matrix

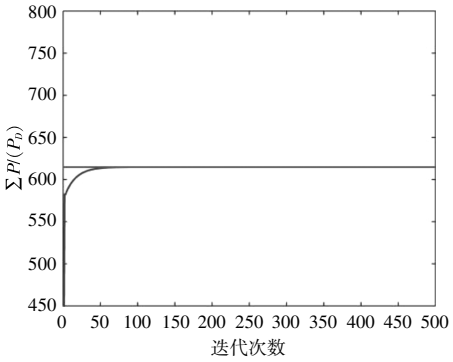
图 3 为系统在没有网络攻击的干扰下,微电网中各能源机组的功率输出、增量成本、系统总功率输出的演变机理。



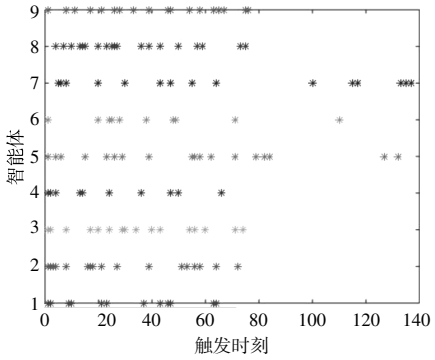
(a)增量成本



(b)局部功率偏差估计值



(c)系统总功率输出



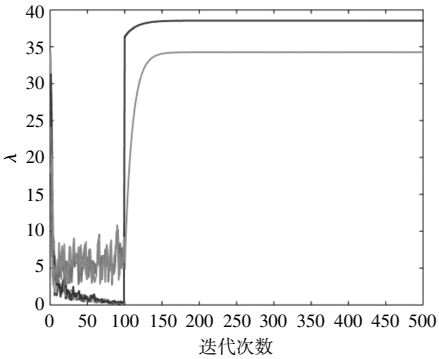
(d)各智能体事件触发时刻

图 3　正常情况下系统投切状态

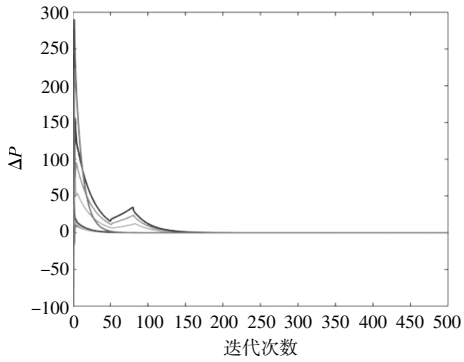
Fig.3 System switching status under normal circumstances

由图 3 可知，各机组在稳定状态下出力值均在其出力范围内，各智能体的局部功率偏差均收敛到 0。DG,EV Aggregator 以及储能设备的发电增量成本最终均收敛到一致,λ^*=2.47 元/(kW·h)。此时系统处于成本最低的最优运行点,并且满足系统的供需平衡,使系统运行在稳定状态,由事件触发机制可知，此过程节约了通信资源并且在迭代一定次数后,状态量便收敛到一致。

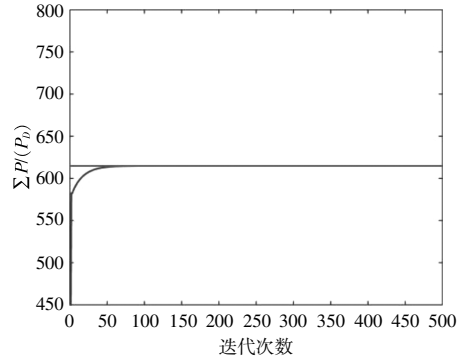
图 4 为 Dos 攻击系统状态。



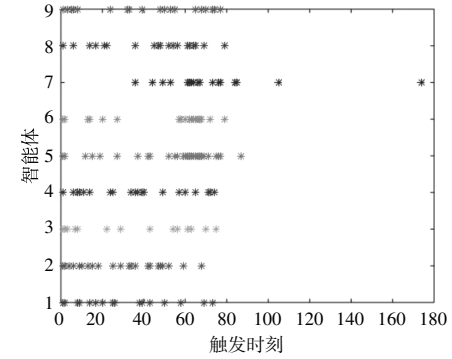
(a)增量成本



(b)局部功率偏差估计值



(c)系统总功率输出



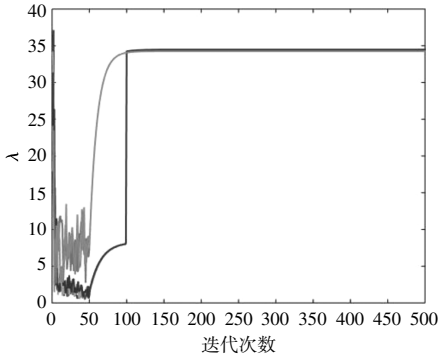
(d)各智能体事件触发时刻

图 4 DoS 攻击下系统状态

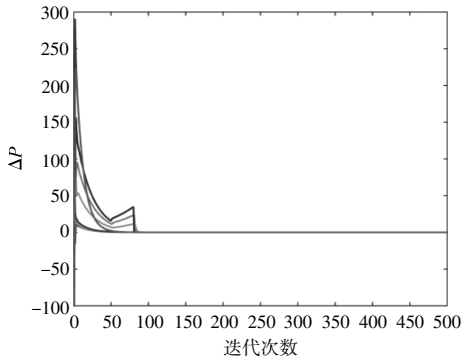
Fig.4 System status under DoS attack

由图 4 可知,由于 DoS 攻击的存在,表现正常的机组增量成本最终会收敛到 $\lambda^{*'}$=2.47 元/(kW·h),而受攻击的机组及其通信网络相连的机组增量成本收敛至 λ'=2.83 元/(kW·h)。此时受攻击的机组及其通信邻居机组的增量成本收敛值与正常机组的增量成本收敛值相比明显增大,具体受攻击所造成的增量成本增加量为 0.37 元/(kW·h),不再对应微电网的成本最低运行点,这也从侧面证明了前文的结论。根据上述分析可得,DoS 攻击会破坏系统运行经济性,与此同时由于系统供需平衡被满足,也表明此类攻击具备一定的隐蔽性,为攻击者提供了一定的便利。

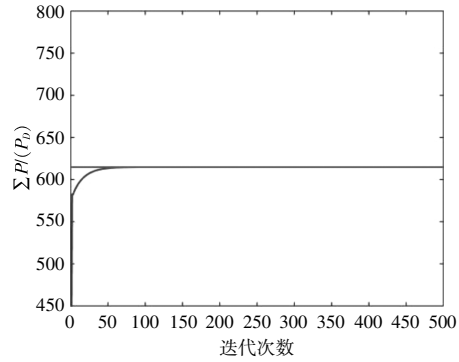
图 5 为采用本文提出的抵御网络攻击控制策



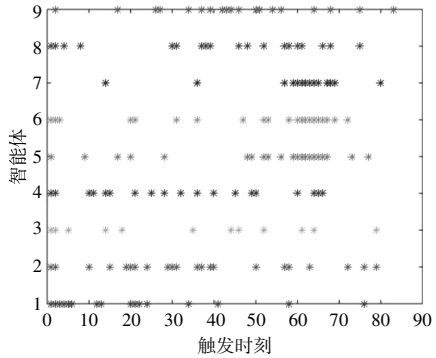
(a)增量成本



(b)局部功率偏差估计值



(c)系统总功率输出



(d)各智能体事件触发时刻

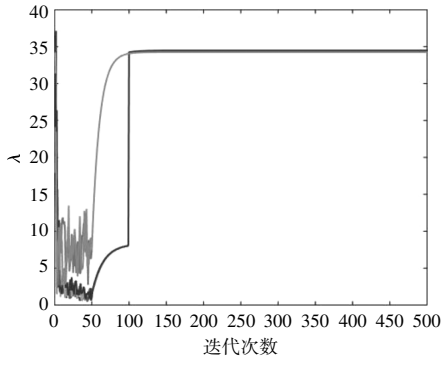
图 5 施加防御策略后的系统状态

Fig.5 System status after applying a defense strategy

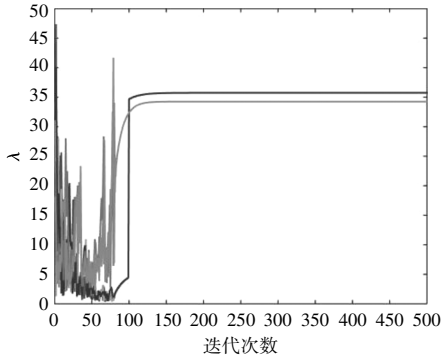
略后系统的状态。

由图 5 可知,受攻击的智能体 7 在 k=100 的迭代时刻被隔离,设定其局部功率偏差量为 0,而其他正常智能体依据现有的通信网络重新计算其局部功率偏差量进行迭代。所有剩余智能体在受攻击的智能体 7 被隔离后,其增量成本收敛至次优值 λ^*=2.49 元/(kW·h),相对于正常运行状态下增量成本仅增加了 0.017 元/(kW·h)。同时,相较于受攻击后系统增量成本趋于稳定的迭代次数 100,本文所提出的抗扰控制策略在迭代 50 次后使系统趋于稳定,大大缩短了调控时长,表明本文提出的抗扰控制策略的有效性。

为进一步体现本文所提算法的高效性,将本文抗干扰算法与传统仅将受攻击节点进行简单隔离的典型抗干扰算法进行对比,结果如图 6 所示。



(a)本文抗干扰算法



(b)典型隔离算法

图 6　典型抗攻击算法与本文算法对比

Fig.6 Comparison between typical anti-attack algorithm and this algorithm

由图 6 可知,相较于受攻击后系统的稳定周期 100 次迭代,无论是典型隔离算法的 80 次迭代,还是本文抗干扰算法的 50 次迭代,均增加了系统的收敛速度。本文抗干扰算法受通信延时的影响更小,系统收敛速度更快,系统增量成本收敛值更加接近最优值,运行成本更小。

6　结论

本文将电动汽车集群作为一种变容量分布式储能装置,并入电网参与经济调度。考虑到通信资源的有限性,设计了一种事件触发机制,能够减轻微网 CPS 的通信负担;引入 Dos 攻击和数据完整性攻击,提出攻击者可以通过与邻居共享虚假数据来操纵调度结果,从而实现攻击目标。从系统防御的角度,提出了一种分布式的经济调度策略,嵌入加密机制,隐藏各代理之间重要更新信息的真实值,并在此基础上,将基于条件识别机制的检测算法与基于声望值的隔离算法相结合,实现对 Dos 攻击及所提出的新型数据完整性攻击的有效防御,并在 Matlab R2014b 上进行仿真验证,证实所提方法的有效性。

参考文献:

[1] Khaki B,Chu C,Gadh R. A hierarchical ADMM based framework for EV charging scheduling [A].2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)[C].Denver:IEEE,2018.1-9.

[2] Patnam B S K,Pindoriya N M. DLMP calculationand congestion minimization with EV aggregator loading in a distribution network using bilevel program [J].IEEE Systems Journal,2020,99:1-12.

[3] Wei W,Liu F,Mei S. Charging strategies of EV aggregator under renewable generation and congestion: A normalized nash equilibrium approach [J]. IEEE Trans. Smart Grid,2017(7):1630-1641.

[4] Seo M,Kim C,Han S. Peak shaving of an EV aggregator using quadratic programming [A]. In Proceedings of the 2019 IEEE Innovative Smart Grid Technologies—Asia (ISGT Asia)[C].Chengdu:IEEE,2019.2794-2798.

[5] Ko K S,Sung D K. The effect of EV aggregators with time-varying delays on the stability of a load frequency control system[J].IEEE Transactions on Power Systems,2018,33:669-680.

[6] Wang R,Sun Q, Tu P,et al. Reduced-order aggregate model for large-scale converters with inhomogeneous initial conditions in DC microgrids[J].IEEE Transactions on Energy Conversion,2021,36(3):2473-2484.

[7] Bonan Huang,Yushuai Li,Fengnan Zhan,et al. A distributed robust economic dispatch strategy for integrated energy system consideringcyber-attacks [J]. IEEE Transactions on Industrial Informatics,2022,18

(2):880-890.

[8] Fu C Y,Wang L Z,Qi D L,et al. Design method and example implementation of hybrid simulation platform for active distribution network information physical system[J]. Chin. J. Electr. Eng.,2019,39:7118-7125.

[9] 李培恺,刘云,辛焕海,等.分布式协同控制模式下配电网信息物理系统脆弱性评估[J].电力系统自动化,2018,42(10):22-29,59.

[10] Zhang L,Ji S,Gu S,et al. Design considerations for high-voltage-insulated gate driver power supply for 10 kV SiC MOSFET applied in medium-voltage converter [J]. IEEE Transactions on Industrial Electronics,2021,68(7):5712-5724.

[11] Zhang L,Ruan X. Control schemes for reducing the second harmonic current in two-stage single-phase converter:An overview from DC-bus port-impedance characteristic[J].IEEE Trans. Power Electron,2019,34:10341-10358.

[12] 张宇航,倪明,孙永辉,等.针对网络攻击的配电网信息物理系统风险量化评估 [J]. 电力系统自动化,2019,43(21):12-22,33.

[13] 汤奕,陈倩,李梦雅,等.电力信息物理融合系统环境中的网络攻击研究综述[J].电力系统自动化,2016,40(17):59-69.

[14] 王琦,李梦雅,汤奕,等.电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J].电力系统自动化,2019,43(9):9-21.

[15] Zeng W,Zhang Y,Chow M Y. Resilient distributed energy management subject to unexpected misbehaving generation units [J]. IEEE Transactions on Industrial Informatics,2017,13(1):208-216.

[16] Zhao C,He J,Cheng P.Analysis of consensus-based distributed economic dispatch under stealthy attacks[J]. IEEE Transactions on Industrial Electronics,2017,64(6):5107-5117.

[17] Sharifi Arman,Pourgholi Mahdi. Adaptive controller design for fixed-time leader-following consensus of multi-agent systems with discontinuous dynamics [J]. International Journal of Control,2022,95(3):830-839.

[18] 陈啸.层次化信息物理系统中的无领导一致性问题研究[D].杭州:浙江大学,2021.

[19] L Guan, H Chen,L Lin.A multi-agent-based self-healing framework considering fault tolerance and automatic restoration for distribution networks [J].IEEE Access,2021,9:21522-21531.

[20] Xu Y,Liu W,Gong J.Stable multi-agent-based load s heddingalgorithm for power systems [J].IEEE Transactions on Power Systems,2011,26 (4):2006-2014.

[21] Claudio De Persis,Pietro Tesi.Input-to-state stabilizing control under denial-of-service [J].IEEE Transactions on Automatic Control,2015,60(11):2930-2944.

[22] RahbariAsr N,Zhang Y,Chow M Y. Consensus-based distributedscheduling for cooperative operation of distributed energy resources andstorage devices in smart grids [J].IET Generation Transmission & Distribution,2016,10(5):1268-1277.

[23] 韩子媛,王莉.5G 移动通信与物联网技术在电力系统中的应用[J].数字技术与应用,2022,40(2):51-53.

[24] D Zou, S Li, X Kong,et al. Solving the combined heat and power economic dispatch problems by an improved genetic algorithm and a new constraint handling strategy [J]. Applied Energy,2019,237:646-670.

[25] Huang B,Li Y,Zhan F,et al. A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks [J].IEEE Transactions on Industrial Informatics,2022,18(2):880-890.

[26] 黄景光,郑钦杰,林湘宁,等.电动汽车与风电协同入网的双层优化策略[J].可再生能源,2021,39(4):514-520.

Cyber-physical system attack and defense strategy of distribution network considering source load bidirectional of electric vehicle

Wang Yihe[1,2], Zhang Mingli[2], Cheng Mengzeng[2], Liu Kai[2], Man Linkun[2]
(1.Northeastern University, School of Information Science and Engineering, Shenyang 110819, China; 2.Institute of Economic Technology, State Grid LiaoNing Electric Power Supply Co.,LTD., Shenyang 110015, China)

Abstract: Modern power system has developed into cyber-physical system (CPS),which is highly integrated between power network and information network. However, advanced information technology not only improves system performance, but also introduces new security risks. With the large-scale grid-connection of Electric Vehicle (EV) with mobile energy storage equipment, the absorption capacity of distribution network for new energy has been greatly improved. However, the low security and high accessibility of charging piles have further reduced the network security of distribution network. On this basis, a distributed energy management strategy based on consistency algorithm is firstly proposed in this paper,which considers the EV cluster as an energy storage device with source-charge bidirectional characteristics to achieve fully distributed economic scheduling. Considering denial of service attacks and new data integrity attacks for electric vehicles, a disturbance rejection control strategy combining privacy protection protocol and isolation mechanism is proposed to achieve effective energy management and economic operation of systems under network attacks. Finally, the effectiveness of the encryption mechanism and the feasibility of the control strategy are verified by simulation.

Keywords: electric vehicle; distributed algorithm; consistency algorithm; source-charge bidirectional characteristics