电力系统自动化
Automation of Electric Power Systems
ISSN 1000-1026,CN 32-1180/TP

《电力系统自动化》网络首发论文

题目：面向互动需求响应的虚假数据注入攻击及其检测方法

作者：陈刘东，刘念

收稿日期：2020-05-05
网络首发日期：2020-08-14
引用格式：陈刘东，刘念. 面向互动需求响应的虚假数据注入攻击及其检测方法[J/OL]. 电力系统自动化.
https://kns.cnki.net/kcms/detail/32.1180.TP.20200813.1500.006.html

第XX卷 第XX期 XXXX年XX月XX日
DOI：10.7500/AEPS20200505006
电力系统自动化
Automation of Electric Power Systems
Vol. XX No. XX XX XX, XXXX

面向互动需求响应的虚假数据注入攻击及其检测方法

陈刘东，刘　念
（新能源电力系统国家重点实验室（华北电力大学），北京市 102206）

摘要： 对互动需求响应（IDR）框架下，需求侧虚假数据注入（FDI）攻击的脆弱性进行分析，凝练了对用户能量管理系统（UEMS）的攻击过程。在此基础上，采用主从博弈建立了针对IDR的FDI攻击模型，并证明其斯塔克伯格均衡存在且唯一。选取电价成本函数参数为攻击者的攻击向量，攻击目标为造成负荷的反向调节。提出了一种基于分布式事件触发机制与机器学习的攻击检测方法，事件触发机制在UEMS中执行，系统检测在能量零售商（ER）中基于长短期记忆网络（LSTM）进行。最后，通过实例分析了攻击者的攻击结果以及攻击参数的灵敏度，比较了分布式事件触发机制和时间触发机制在不同负荷阈值和攻击率下的准确性及检测时间。

关键词： 虚假数据注入攻击；攻击检测；互动需求响应；博弈论；机器学习

0　引言

随着电网中光伏用户群的大比例渗透以及产销者数量不断增加[1-2]，源荷时间分配的差异逐渐增大。由于负荷峰值通常在夜晚出现，而光伏发电的峰值在日间时刻，因此，净负荷将形成“鸭型曲线”[3]，使得峰谷差异增加，为电力系统的调控带来困难。此外，光伏信息的实时性及不确定性，容易被攻击者利用，危害系统运行安全。

互动需求响应（interactive demand response，IDR）作为重要的负荷调控措施，通过在产销者侧引入用户能量管理系统（user energy management system，UEMS），进行产销者与电网之间的互动，对负荷分布以及交易电价进行调整，达到削峰填谷和增加经济性的效果[4-5]。在IDR中，博弈论作为一种重要的技术手段得到广泛应用[6]，模型主要包括古诺博弈[7]和斯塔克伯格博弈[8]这2类。

由于UEMS的运行处理能力有限，其安全防御通常远低于电网侧设备，加之需求侧的开放接入环境，导致在电网侧更容易发生网络攻击[9]。随着信息物理系统的发展以及需求侧对信息通信的依赖，针对需求侧进行的虚假数据注入（false data injection，FDI）攻击将对系统造成更加严重的影响[10]。①攻击者可以通过植入病毒或恶意软件修改系统的关键参数，例如由木马病毒植入造成的2015年乌克兰电网大停电事故[11]；②鉴于其强大的传播能力，可以在短时间内对系统造成大范围影响，例如由勒索蠕虫病毒的大量传播导致的2017年“永恒之蓝”事件[12]。

在分布式光伏大量渗透的区域，由于产销者与电网管理者对光伏发电信息的掌握程度不同，更有利于实施FDI攻击。FDI攻击通过生成攻击向量并发送给攻击目标来伪造交互信息[13-15]，从电网发、输、配、用的关键层面出发，现有研究可分为以下4类。①针对自动发电控制装置以及发电机节点数据的发电侧攻击[16]。②针对数据采集与监控系统、能量管理系统等输电侧主体的攻击，实现对数据控制单元以及状态估计结果的篡改[17]。③针对智能量测终端注入病毒进行数据篡改，通过影响公共数据中心造成能量管理及预测系统混乱的配电侧攻击[18]。④针对用户侧需求响应的攻击，包括单独攻击电价[19]以及针对用户行为的差异性进行参数的篡改[20]。

为了减轻FDI攻击对系统造成的负面影响，学术界提出了防御措施，例如：密钥管理机制[21]、混合量测技术[22]和攻击检测[23-24]等。其中攻击检测方法主要包括状态估计[23]和机器学习技术[24]这2类。

然而，在“鸭型曲线”背景下，针对IDR中产销者UEMS的FDI攻击还未受到足够的重视，相关的检测系统仍然是有待研究的问题。本文基于博弈论研究了针对UEMS的FDI攻击，采用文献[6]中的IDR框架，选择成本函数参数作为攻击者篡改的目标，意在造成负荷的反向调节，并构建分布式事件触

收稿日期：2020-05-05；修回日期：2020-07-27。
国家自然科学基金资助项目（51877076）。

发机制与机器学习结合的攻击检测系统。

1 系统框架

1.1 IDR过程

IDR框架基于文献[6]中提出的博弈模型建立，框架中包括作为管理者的能量零售商(energy retailer，ER)以及带有UEMS的用户，其中ER具有一定的计算能力并管理用户与公用电网间的交互过程，将向用户传递成本函数参数以及系统总负荷；UEMS也带有部分计算能力，处理产销者的计算任务，管理产销者运行，并将产销者的负荷需求传递给ER。

在需求侧采用电力成本函数来确定ER的动态电价，该函数受到产销者净负荷以及ER收益的影响[25]，产销者i在时刻h的净负荷$L_{i,h}$由可平移负荷$l_{s,i,h}$与固定负荷$l_{f,i,h}$的和，再减去光伏发电量$E_{PV,i,h}$进行计算，$l_{s,i,h}\in[l_{s,i,h,\min},l_{s,i,h,\max}]$，且$\sum_{h=1}^{H}l_{s,i,h}=q_{t,i}$，其中$l_{s,i,h,\max}$和$l_{s,i,h,\min}$分别为$l_{s,i,h}$的上、下限，$H$为时刻总数，$q_{t,i}$为产销者$i$在全时刻的可平移负荷总和。根据文献[26]，采用二次多项式模型表征时刻h的成本函数$C_{g,h}(L_{i,h})$为：

$$C_{g,h}(L_{i,h})=a_{ini,h}L_{i,h}^2+b_{ini,h}L_{i,h} \tag{1}$$

式中：$a_{ini,h}$和$b_{ini,h}$为时刻h的成本函数参数。

式(1)中的成本函数参数由ER基于电价成本的相关影响因素决定，例如：发电机类型、燃料价格、ER的利润空间和其他发电商提供的信息。在ER确定成本函数参数以后，将会传递给产销者，用以协助UEMS计算动态电价。

当产销者的光伏发电量大于负荷消耗时，产销者将向电网输送电能，相当于负成本，因此，整体在时刻h的成本函数$C_{0,h}(L_{i,h})$可以表示为：

$$C_{0,h}(L_{i,h})=\begin{cases}C_{g,h}(L_{i,h}) & L_{i,h}\geqslant 0\\ \zeta L_{i,h} & L_{i,h}<0\end{cases} \tag{2}$$

式中：ζ为产销者向电网输送电能的单位收益。

式(2)中的分段函数可以用严格凹的二次函数近似替代，因此，产销者在时刻h的成本函数可以修正为函数$C_h(L_{i,h})$，表达式为：

$$C_h(L_{i,h})=a_hL_{i,h}^2+b_hL_{i,h} \tag{3}$$

式中：a_h和b_h为时刻h的修正成本函数参数。

基于式(1)，动态电价的计算方法为：

$$P_h=\frac{C_h(L_h)}{L_h}=a_hL_h+b_h \tag{4}$$

式中：P_h为时刻h的动态电价；L_h为时刻h的所有用户负荷总量，且$L_h=\sum_{i=1}^{N}L_{i,h}$，其中$N$为产销者总数。

1.2 IDR中的信息安全问题

在信息物理系统中，需求侧和电网侧之间存在大量的数据交互，奠定了数据注入攻击发生的基础。攻击者通过在交互过程中操纵数据对系统造成运行威胁，通常针对大系统，可以对系统的运行造成更大的负面影响。然而，由于需求侧的设备安全保护措施远低于电网侧，并且IDR过程中存在大量数据交互，针对需求侧的数据注入攻击将给系统带来信息安全问题。

数据注入攻击的目的是妨碍系统中各主体之间的信息交互过程，具体信息包括负荷消耗、动态电价和电价函数的参数。由于负荷消耗和动态电价是相对明显的信息，并且已有相关研究[27]，为了更好地隐藏攻击性，本文选择发送到UEMS的成本函数参数作为FDI的攻击目标，用户负荷消耗和ER的动态电价也将根据该参数的变化进行修改，进而达到影响系统调控的目的。实施FDI需要获取系统总负荷消耗量和成本函数参数，通过发动中间人攻击和注入恶意软件寻找关键配置文件的方式获取信息并对UEMS实施攻击，如图1所示。由于UEMS采用计算机操作系统，存在与计算机相似的安全漏洞，UEMS更容易受到网络攻击的威胁。

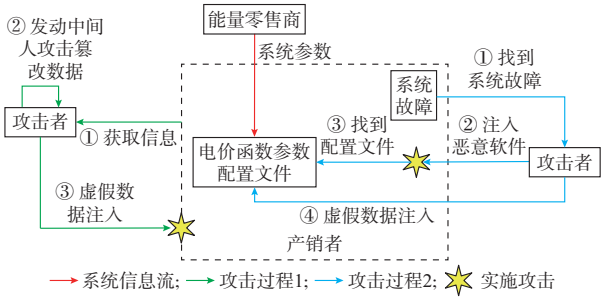


图1 网络攻击原理图

Fig. 1 Schematic diagram of cyber-attacks

本文选取攻击方式1作为研究对象，攻击者利用需求响应，恶意增加某个时刻的负荷，造成馈线过载甚至停电，以削弱系统运行的稳定性。此外，由于系统运营商很难完全掌握所有产销者的光伏发电情况，通过FDI篡改负荷数据将具有一定的隐蔽性。更为严重的是，对同一变电站的多条中压线路进行协同攻击可能会导致更严重的后果，例如：整个变电站的服务中断或是向变电站供电的高压输电线路出现故障。

2　基于博弈论的数据注入攻击模型

2.1　基于非合作博弈的IDR

IDR可以通过非合作博弈实现[6]，每个博弈者都将在博弈中调整自己的策略以获得最优收益。不同博弈者在博弈过程中存在着相互影响[28]，IDR博弈的本质在于每个产销者基于动态电价调整负荷分布以最大化自身收益，然而动态电价又取决于系统负荷的总量。该非合作博弈G_{C}可以表示为：

$$G_{\mathrm{C}}=\left\{S_1,S_2,\cdots,S_N,E_1,E_2,\cdots,E_N\right\} \tag{5}$$

式中：S_i和$E_{i,h}$分别为第i个博弈参与者（即产销者）及其在全时段的收益，且$E_i=-\sum_{h=1}^{H}C_h(L_{i,h})$，$i\in N$，$N$为产消者总数。

定义1：在博弈G_{C}中，如果任意产销者i在时刻h的策略$l^*_{\mathrm{s},i,h}$是响应其他产销者同一时刻策略$(l^*_{\mathrm{s},1,h},\cdots,l^*_{\mathrm{s},i-1,h},l^*_{\mathrm{s},i+1,h},\cdots,l^*_{\mathrm{s},N,h})$的最优策略，其收益$E_i^*$满足：

$$E_i^*\geqslant E_i \tag{6}$$

那么各产销者在各时刻的最优策略$l^*_{\mathrm{s},i,h}$组成纳什均衡。

如果所有参与者改变策略的动机都可以用一个称为势函数的全局函数来表示，那么该博弈为势博弈[29]，其势函数$f(L_{i,h},L_{j,h})$为：

$$f(L_{i,h},L_{j,h})=\sum_{h=1}^{H}a_h\sum_{i=1}^{N-1}L_{i,h}\sum_{j=i+1}^{N}L_{j,h}+\sum_{h=1}^{H}a_h\sum_{i=1}^{N}L_{i,h}^2+\sum_{h=1}^{H}b_h\sum_{i=1}^{N}L_{i,h} \tag{7}$$

式中：$ij\in[1,N]$；j为产销者序数。

通过对该势函数求取最优解，可以得到博弈G_{C}的纳什均衡。当势函数不存在的时候，仍然可以基于非合作博弈的迭代求解方法，求得该博弈的纳什均衡，只是在计算时间上存在劣势，不影响文中所提攻击模型的实现。

定理1：非合作博弈G_{C}中存在唯一的纳什均衡。证明过程如附录A所示。

2.2　基于主从博弈的数据注入攻击模型

攻击模型可以通过一主多从的主从博弈表示，在本文的IDR中，攻击者作为主导者，通过调整公式(7)中参数a_h的变化量来篡改参数a_h，影响UEMS设置动态电价。产销者作为跟随者，基于UEMS所计算出的动态电价调整自己的负荷分布。攻击者与产销者之间的主从博弈K定义为：

$$K=\left\{(S\cup A),l_{\mathrm{s},i,h},\Delta a_h,E_i,f_{\mathrm{vir}}\right\} \tag{8}$$

式中：S和A分别表示产销者和攻击者的集合；Δa_h为成本函数参数a_h的变化量，由攻击者基于用户的负荷分布产生；f_{vir}为攻击者在全时段的虚拟收益，攻击者通过最大化该虚拟收益造成负荷高峰。

在产销者i的全时段收益函数E_i中，参数a_h受到攻击量Δa_h的影响，攻击者在全时段的虚拟收益可以表示为：

$$f_{\mathrm{vir}}=\sum_{h=1}^{H}(a_h-\Delta a_h)L_h^2+\sum_{h=1}^{H}b_hL_h \tag{9}$$

式中：Δa_h为在时刻h，攻击者对成本函数参数为a_h的攻击量，且$0\leqslant\Delta a_h\leqslant ua_h$，$\sum_{h=1}^{H}\Delta a_h=va_h$，其中$u$和$v$分别为攻击量的幅值约束及求和约束参数。

需要注意的是，攻击者的收益函数为虚拟收益函数，其设计目的是利用用户对错误电价的需求响应，诱发更高的负荷高峰。虽然它在形式上与产销者的成本函数相似，但其实际意义却与产销者的成本函数不同。

主从博弈的均衡解是斯塔克伯格均衡（Stackelberg equilibrium，SE），它是所有参与者在博弈中的最优解。下面给出博弈K中SE的定义。

定义2：主从博弈K中的SE定义为$(l^*_{\mathrm{s},i,h},\Delta a_h^*)$，其中$h\in[1,H]$，$\Delta a_h^*$为……，且在SE时，产销者$i$的收益满足式(6)，攻击者收益$f_{\mathrm{vir}}^*$满足式(10)。

$$f_{\mathrm{vir}}^*\leqslant f_{\mathrm{vir}} \tag{10}$$

当博弈K到达SE，没有参与者能仅通过调整自己的策略$l_{\mathrm{s},i,h}$和Δa_h来增加自身收益。

定理2：在主从博弈K中，消费者和攻击者存在唯一的SE。证明过程如附录B所示。

主从博弈框架是数学描述所提出网络攻击模型的一种形式，鉴于攻击者与产销者之间决策参数的相互影响以及双方具有的利益冲突，通过主从博弈框架体现攻击的过程及机理，保证完备的数学理论。无论采用何种框架，需求响应的逻辑都相同，攻击的过程也具有普适性。

2.3　模型实现流程及方法

为了解决主从博弈K，首先，应对产销者之间的非合作博弈进行求解，由于采用迭代算法求解非合作博弈将耗费大量计算资源，因此，通过最优化其等价势函数的方法获取纳什均衡。启发式算法可以用来解决主从博弈的问题，例如遗传算法[31]，但其数学机制不明确，且计算效率低。因此采用库恩-塔克（Karush-Kuhn-Tucker，KKT）条件求解主从博弈K，将跟随者侧的非合作博弈模型转化为KKT最优条件，使得主、从两侧分别的优化问题转化为主侧单独的优化问题，采用互补松弛条件进行线性化

后[32],使式(9)最小化的KKT约束条件为:

$$\begin{cases} -(a_h-\Delta a_h)\left(\sum\limits_{j=1,j\neq i}^{N}(L_j+2L_i)\right)-b_h- \\ \quad \underline{\beta}_i+\overline{\beta}_i-\lambda_i=0 \\ \overline{\beta}_i\leqslant M\overline{\gamma}_i \\ l_{\mathrm{s},i,h,\max}-l_{\mathrm{s},i}\leqslant M(1-\overline{\gamma}_i) \\ \underline{\beta}_i\leqslant M\underline{\gamma}_i \\ l_{\mathrm{s},i}-l_{\mathrm{s},i,h,\min}\leqslant M(1-\underline{\gamma}_i) \end{cases} \tag{11}$$

式中:$\overline{\beta}_i$,$\underline{\beta}_i$和λ_i为产销者i的拉格朗日乘子,且$\overline{\beta}_i\geqslant 0$,$\underline{\beta}_i\geqslant 0$,$\lambda_i\geqslant 0$;$M$为足够大的正数;$\overline{\gamma}_i$和$\underline{\gamma}_i$为产销者$i$的互补松弛条件的二元变量。

KKT条件的引入,使得主从博弈斯塔克均衡的分析和求解更加简便,省去了大量的迭代过程。而在实际系统中,攻击者通过植入病毒或恶意软件获取系统信息,生成攻击向量,植入到产销者获取的电价函数中,二者随着博弈进程的推进逐渐进行信息的交互。

3 基于长短期记忆网络的攻击检测方法

由于数据量大、参与者的多样性和攻击的隐蔽性等特点,如何在交互过程中检测网络攻击是具有挑战性的问题。简单的用户反馈由于用户信息的局限性以及反馈的真实性,无法准确检测系统的攻击,需要系统级别的攻击检测方法。由于不同攻击方式具有不同的特点,例如:数据注入攻击将着重于修改数据交互过程中的数据值;而对于物理设备的攻击以损害系统中终端设备为目标,故通过数学方法分析其数学模型具有一定的局限性,很难在各种攻击方式中广泛应用。在本文的框架中,攻击者的目标是造成更高的负荷高峰,导致馈线过载或运行中断,因此,检测的重点为负荷特性。

采用机器学习技术对系统攻击进行检测,应对多变的攻击形式。由于负荷在1天内具有很强的相关性,并且可平移负荷需要满足总和约束,因此,对负荷特性的研究属于时间序列问题,鉴于长短期记忆(long short-term memory,LSTM)网络的遗忘门机制,在处理时间序列问题方面具有很大的优势[33],因此,本文采用LSTM技术进行攻击检测。对于攻击成功的历史数据缺失的问题,可以通过仿真手段构造攻击成功的例子,在保证不对电网运行产生影响的前提下,获取大量的仿真数据,并基于这些数据对检测系统进行训练。

3.1 事件触发机制

本文提出一种基于UEMS对攻击进行初步检测的事件触发机制,其中ER与UEMS构成闭环系统,并带有反馈控制器,当UEMS检测到以下事件时,ER中的系统攻击检测将被激活。

事件1:$L_{i,h}$超过负荷上限L_{Thre},定义为$\boldsymbol{\varphi}_{\mathrm{a},h}=[\varphi_{\mathrm{a},1,h},\varphi_{\mathrm{a},2,h},\cdots,\varphi_{\mathrm{a},N,h}]$。

事件2:$l_{\mathrm{s},i,h}$超过下限约束$l_{\mathrm{s},i,h,\min}$,定义为$\boldsymbol{\varphi}_{\mathrm{b},h}$。

事件3:$l_{\mathrm{s},i,h}$超过上限约束$l_{\mathrm{s},i,h,\max}$,定义为$\boldsymbol{\varphi}_{\mathrm{c},h}$。

$$\boldsymbol{\varphi}_h=\{\boldsymbol{\varphi}_{\mathrm{a},h}\|\boldsymbol{\varphi}_{\mathrm{b},h}\|\boldsymbol{\varphi}_{\mathrm{c},h}\} \tag{12}$$

在正常情况下,$\boldsymbol{\varphi}_{\mathrm{a},h}$,$\boldsymbol{\varphi}_{\mathrm{b},h}$,$\boldsymbol{\varphi}_{\mathrm{c},h}$为仅含有0元素的向量,当UEMS中发生上述任意事件时,对应事件将置1,该过程的状态机模型如图2所示。

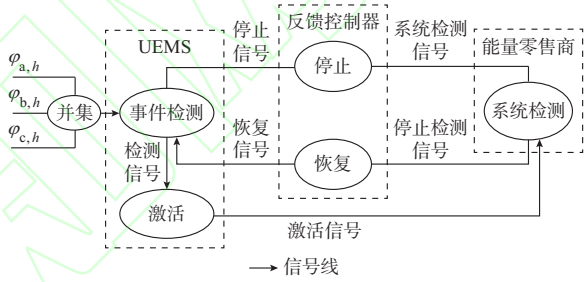


图2 分布式事件触发机制状态机模型

Fig. 2 State machine model of distributed event trigger mechanism

UEMS中的“事件检测”状态将对这3个事件进行检测。某个事件发生后,将触发进入“激活”状态,向ER发送激活信号,使ER执行“系统检测”状态,同时反馈控制器执行“停止”状态,并向UEMS发送停止信号,停止UEMS中的检测过程。当ER中的检测完成后,ER触发“恢复”状态,反馈控制器向UEMS发送一个恢复信号恢复检测。

3.2 LSTM网络模型及其分布式实现方法

LSTM模型的结构包括输入层、隐含层和输出层。具有时间序列特征的多维输入数据$\boldsymbol{X}=\{\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_h,\cdots,\boldsymbol{X}_H\}$是供LSTM网络学习的基础信息,在隐含层中,信息将从某时刻传到其他时刻。LSTM中的长期记忆来源于一种特殊的遗忘门机制,在时间序列问题的预测和分类中具有优势[34]。

LSTM模型通过所提出的博弈模型来检测和区分正常情况及攻击情况。由于可平移负荷在不同时刻随着动态电价(被成本函数参数影响)的变化而变化,选择可平移负荷相关的物理量作为LSTM网络的特征,包括初始可平移负荷、可平移负荷上限和最优可平移负荷。为了确定系统的总负荷,将固定

负荷也选为特征，因此，时刻 h 输入到LSTM中的数据可以表示为：

$$\boldsymbol{X}_h=[l_{\mathrm{f},h},l_{\mathrm{s},h},l_{\mathrm{s},h,\max},l^*_{\mathrm{s},h}] \tag{13}$$

式中，$\boldsymbol{X}_h$ 为LSTM网络在时刻 h 的输入。

由图3可知，隐含层的遗忘门机制由输入门、输出门和遗忘门组成。控制过程中的关键因素为记忆细胞，承载着过去时刻中的信息，并根据遗忘门决定是否将其传输给该时刻的记忆细胞或者遗忘。在这个过程中，存在被输入门控制的替代记忆细胞。输出门则控制是否将记忆细胞输出。最后，该时刻的输出信息和记忆细胞将会被传输到下个时刻的隐含层中，用于未来的学习。整个过程中，门和节点的定义如下。

$$\boldsymbol{I}_h=\sigma(\boldsymbol{X}_h\boldsymbol{W}_{\mathrm{inx},h}+\boldsymbol{D}_{h-1}\boldsymbol{W}_{\mathrm{inh},h}+b_{\mathrm{in},h}) \tag{14}$$

$$\boldsymbol{F}_h=\sigma(\boldsymbol{X}_h\boldsymbol{W}_{\mathrm{fx},h}+\boldsymbol{D}_{h-1}\boldsymbol{W}_{\mathrm{fh},h}+b_{\mathrm{f},h}) \tag{15}$$

$$\boldsymbol{O}_h=\sigma(\boldsymbol{X}_h\boldsymbol{W}_{\mathrm{ox},h}+\boldsymbol{D}_{h-1}\boldsymbol{W}_{\mathrm{oh},h}+b_{\mathrm{o},h}) \tag{16}$$

$$G^*_h=\tanh(\boldsymbol{X}_h\boldsymbol{W}_{\mathrm{cx},h}+\boldsymbol{D}_{h-1}\boldsymbol{W}_{\mathrm{ch},h}+b_{\mathrm{c},h}) \tag{17}$$

$$\boldsymbol{G}_h=\boldsymbol{F}_h\boldsymbol{G}_{h-1}+\boldsymbol{I}_hG^*_h \tag{18}$$

$$\boldsymbol{D}_h=\boldsymbol{O}_h\tanh(\boldsymbol{G}_h) \tag{19}$$

式中：$\boldsymbol{X}_h$ 和 $\boldsymbol{D}_{h-1}$ 为分别为时刻 h 的输入向量和时刻 $h-1$ 的输出向量；$\boldsymbol{I}_h$，$\boldsymbol{F}_h$，$\boldsymbol{O}_h$，$\boldsymbol{G}_h$，G^*_h 和 $\boldsymbol{D}_h$ 分别为时刻 h 的输入门向量、遗忘门向量、输出门向量、记忆细胞状态向量、替代记忆细胞状态向量和输出向量；$\boldsymbol{W}_{\mathrm{inx},h}$，$\boldsymbol{W}_{\mathrm{inh},h}$，$\boldsymbol{W}_{\mathrm{fx},h}$，$\boldsymbol{W}_{\mathrm{fh},h}$，$\boldsymbol{W}_{\mathrm{ox},h}$，$\boldsymbol{W}_{\mathrm{oh},h}$，$\boldsymbol{W}_{\mathrm{cx},h}$ 和 $\boldsymbol{W}_{\mathrm{ch},h}$ 分别为时刻 h 输入门、遗忘门、输出门、记忆细胞的权重矩阵；$b_{\mathrm{in},h}$，$b_{\mathrm{f},h}$，$b_{\mathrm{o},h}$ 和 $b_{\mathrm{c},h}$ 分别为 h 时刻输入门、遗忘门、输出门、记忆细胞的偏执；$\sigma(\cdot)$ 及 $\tanh(\cdot)$ 分别为Sigmoid函数和双曲正切函数，可以分别将数值映射到[0，1]及[−1，1]。

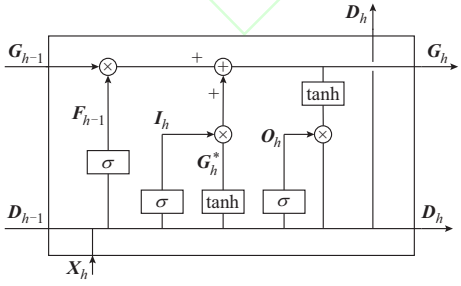


图3　LSTM网络隐含层结构

Fig. 3　Network hidden layer structure of LSTM

LSTM的整个学习过程可以分为2步：①基于式(14)至式(19)的正向传播，得到初始的权重与偏执；②基于时间的反向传播，从输出层到输入层进行计算，利用损耗函数最小化①中积累的误差，从而更新各个权重及偏执[34]。

$$J=\sum_{t=1}^{T}(D(x_{t,h})-y_{t,h})^2 \tag{20}$$

式中：J 为反向传播过程中的损耗；$D(x_{t,h})$ 为输出单元 t 在时刻 h 的实际输出；$y_{t,h}$ 为输出单元 t 在时刻 h 的理论输出；T 为输出单元总数。

LSTM模型在UEMS的辅助下在ER中执行，UEMS凭借自身计算能力对数据进行预处理，如筛除坏数据和生成模拟数据等，具有强大计算能力的ER基于UEMS的样本数据执行LSTM模型的学习过程。ER也通过与UEMS合作，在事件触发机制中负责系统级别的检测。

4　算例

4.1　基础数据

以广东某工业园区为例，对模型性能进行验证。该系统由8个与中压馈线相连的产销者组成，负荷类型包括商业建筑和工厂，由20%可平移负荷和80%固定负荷组成，其中可平移负荷包括电动汽车和洗衣机等。系统中产销者与发电企业之间通过ER协调，系统中馈线的正常传输限制为8 MW，最大限制为8.3 MW，负荷峰值为7.966 MW，出现在22:00。各产销者的可移负荷的下限为0，上限分别为0.58，0.58，0.58，0.55，0.55，0.50，0.52和0.52 MW。正常情况下，成本函数中的参数 a_h 和 b_h 分别为0.000 59和0.302，假设它们在指定的时间段内不随时间变化。8个产销者的初始负荷分布如图4所示，可以看出净负荷曲线呈现出“鸭型曲线”的形态，曲线中间的下沉是由于光伏发电量引起的。由于ER对光伏发电信息的非完全掌握，在光伏发电时间段内展开FDI攻击不易被发现。

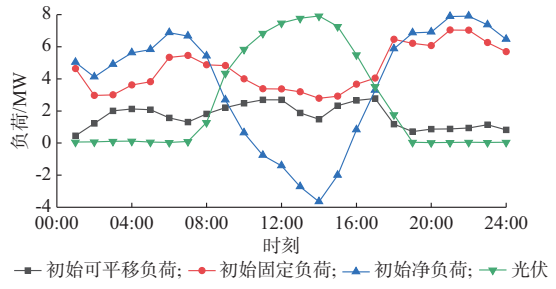


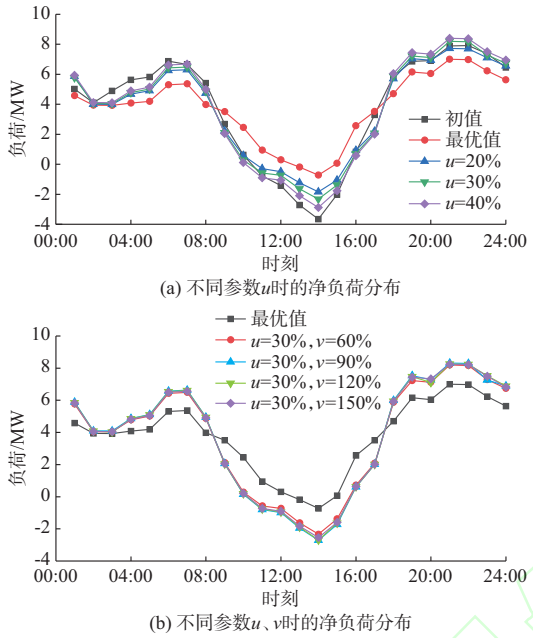
图4　初始负荷分布

Fig. 4　Initial load distributions

4.2　攻击博弈模型的结果及灵敏度分析

产销者的最优可平移负荷分布很大程度上受到动态电价的影响，而动态电价又受到成本函数参数 a_h 的影响。因此，对攻击参数 Δa_h 进行2种灵敏度分析。①u 设置为20%，30%和40%；v 分别相应设置为40%，60%和80%；②u 设置为30%，v 分别设置

为60%,90%,120%和150%。图5(a)和(b)分别表示了2种灵敏度分析的结果,每个场景中最优的Δa_h结果如表1所示。



(a) 不同参数u时的净负荷分布

(b) 不同参数u、v时的净负荷分布

图5 攻击参数灵敏度分析

Fig. 5 Sensitive analysis of attack parameters

表1 各个攻击场景的Δa_h值

Table 1 Each attack case value of Δa_h

u/%	v/%	Δa_h				
		18:00	19:00	21:00	22:00	23:00
20	40			0.000 12	0.000 12	
30	60			0.000 18	0.000 18	
40	80			0.000 24	0.000 24	
30	90	0.000 18		0.000 18	0.000 18	
30	120	0.000 18		0.000 18	0.000 18	0.000 18
30	150	0.000 18	0.000 18	0.000 18	0.000 18	0.000 18

最优负荷分布为没有攻击时,非合作博弈的结果,如图5(a)所示,与净负荷初值相比,优化后的净负荷峰值明显下降,并且由光伏发电造成的负荷低谷得到补充,使得负荷分布更加平缓,有利于系统的稳定运行。对于各个攻击场景,负荷峰值在04:00—08:00以及18:00—24:00升高,并且这些升高的负荷来自低谷时段09:00—17:00的可平移负荷,容易被误认为是光伏发电变化产生的改变。负荷的最高峰值仍然在21:00—22:00,与成本函数参数Δa_h的变化时刻相同(如表1所示)。虽然只对2个时刻进行攻击,但为了满足可平移负荷的时间耦合约束,其他时刻的可平移负荷也会进行相应的变化,从而使得系统负荷分布发生变化。

负荷高峰随着参数u逐渐增加。当$u=20\%$时,攻击造成的峰值负荷与初始负荷峰值相近,对系统并未造成严重的影响。然而,根据式(4),负荷峰值的增长将导致动态电价升高,对产销者的经济效益产生影响。当u为30%和40%时,负荷峰值分别为8.2 MW和8.4 MW,分别超过了传输线额定容量8.0 MW和最大限度8.3 MW,导致线路过载和停电事故。

对于第2个灵敏度分析场景,从表1可以看出,随着v的增大,参数Δa_h的变化分布在更多的时段内。如图5(b)所示,当v分别设置为90%,120%和150%时,负荷峰值的增大体现在不止1个时刻上。例如,当$v=90\%$时,19:00的负荷开始增大;当$v=120\%$时,23:00的负荷开始增大。因此,不同的u和v的比值将会影响攻击效果,但从图5(a)和(b)可以看出,攻击时刻多少的影响明显小于攻击程度,因为针对1个时刻的攻击会导致全时段可平移负荷分布发生变化。

根据这些结果,攻击者可以选择不同的攻击策略造成不同的攻击效果,例如输电线过载威胁系统的稳定性,或者停电事故给系统带来直接破坏。

4.3 LSTM网络训练及网络攻击的检测

网络攻击检测由ER在UEMS的帮助下实现,UEMS通过检测产销者的负荷分布执行事件触发机制,ER通过LSTM模型进行系统检测,并执行LSTM模型的训练。在本节的检测分析中,u和v分别设置为30%和60%

4.3.1 LSTM网络训练过程

采用MATLAB软件中的LSTM工具箱执行LSTM模型,采用CPU型号为酷睿i5-8250,主频为1.6 GHz,内存为16 GB的计算机作为执行环境。模型的输入数据为正常情况及攻击情况下具有4维特征的24 h负荷值,输出层具有1维特征,反映对应输入数据处于正常或是攻击情况。隐含层设置为80个节点,学习速率设置为0.01,梯度阈值设为1,最大种群代数设为60。从MATLAB的学习过程可知,当接近600代时,检验准确度趋于100%;并且随着迭代进行,损失函数的值趋近于0。通过8个用户在正常情况及攻击情况的仿真各生成300组样本数据,并在样本生成过程中加入不同的固定负荷偏移量,以增加样本的多样性,采用这600组样本数据训练LSTM网络,并选取80%的数据作为训练组,20%作为检验组,随着样本数从100按步长100增加至600,检验准确度也从75%逐步增加至99.5%。

4.3.2 基于事件触发机制的网络攻击检测

UEMS通过检测用户的负荷分布执行事件触发机制,并在任意事件发生时向ER发送出发信号,

触发系统检测。然而，对于时间触发机制，需要在每个特定的时间间隔中进行。以第2个触发事件为例，将L_{Thre}设为1.41 MW，在攻击情况下，产销者4在21:00的负荷为1.411 MW，UEMS将进入“激活”状态，并向ER发送信号使其进入“系统检测”状态，使用LSTM进行系统检测。系统的检测结果显示系统存在攻击。

本节采用400个样本数据进行分析，图6显示了事件触发机制在不同L_{Thre}及攻击率时检测时间及准确率的变化规律，其中攻击率为受到攻击的样本占总样本的百分比，且LSTM执行每次检测的时间约为0.1 s。根据图6的结果，检测时间及准确率随着UEMS的L_{Thre}的增大而减少，最大的检测时间为340 s。ER在时间触发机制下采用LSTM模型进行攻击检测的时间为400 s，准确率为99.5%（适用于所有攻击率）。因此，在事件触发机制下选取合适的L_{Thre}（例如1.36 MW），可以在相近准确率的前提下，较时间触发机制减少15%的检测时间。

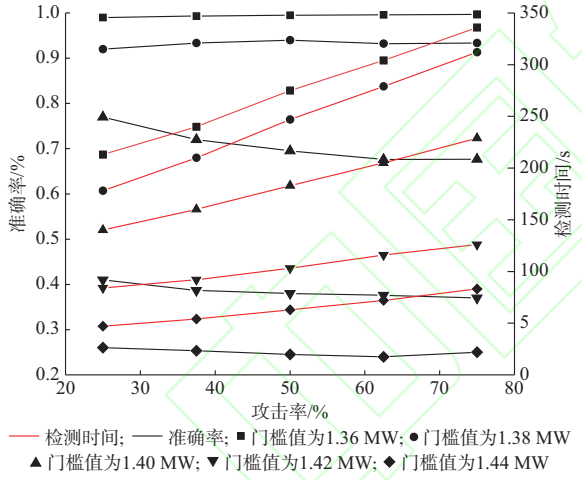


图6　不同负荷阈值下的检测准确率与时间

Fig. 6　Detection accuracy and times with different load thresholds

5　结语

本文采用基于非合作博弈的IDR框架，研究了针对于用户侧UEMS的FDI攻击，并利用主从博弈构建攻击模型。基于所构建的UEMS侧事件触发机制以及ER侧机器学习模型，提出了分布式的攻击检测体系，其中事件触发机制通过UEMS侧的状态机模型执行，ER侧则基于LSTM模型进行系统检测。算例部分的结果表示了在光伏发电时刻的可平移负荷将会向着原始的负荷高峰移动，以造成更高的负荷高峰，对攻击参数的灵敏度分析则表现出攻击效果很大程度上受到单时刻攻击幅度的影响，而对攻击时刻的影响不大，这是由于可平移负荷的时间约束使得可平移负荷在各个时段存在关联。通过事件触发机制与时间触发机制的比较，看出通过选择适当的阈值负荷，可以在保证检验准确率的情况下减少15%的时间消耗。

附录见本刊网络版（http://www.aeps-info.com/aeps/ch/index.aspx），扫英文摘要后二维码可以阅读网络全文。

参 考 文 献

[1] FACCHINI A. Distributed energy resources: planning for the future[J]. Nature Energy, 2017, 2(8): 1-2.

[2] PARAG Y, SOVACOOL B. Electricity market design for the prosumer era[J]. Nature Energy, 2016, 1(4): 1-6.

[3] DENHOLM P, O' CONNELL M, BRINKMAN G, et al. Overgeneration from solar energy in California: a field guide to the duck chart[EB/OL]. [2020-05-02]. https://www.doc88.com/p-0738673936901.html.

[4] LIU Nian, YU Xinghuo, WANG Cheng. et al. Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers[J]. IEEE Transactions on Power Systems, 2017, 32(5): 3569-3583.

[5] 刘念，余星火，王剑辉，等.泛在物联的配用电优化运行：信息物理社会系统的视角[J].电力系统自动化，2020，44(1)：1-12.
LIU Nian, YU Xinghuo, WANG Jianhui, et al. Optimal operation of ubiquitous IoT-based power distribution and consumption system: cyber physical social system perspective [J]. Automation of Electric Power Systems, 2020, 44(1): 1-12.

[6] MOHSENIAN-RAD A, WONG V W S, JATSKEVICH J, et al. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid [J]. IEEE Transactions on Smart Grid, 2010, 1(3): 320-331.

[7] 刘念，王程，雷金勇.市场模式下光伏用户群的电能共享与需求响应模型[J].电力系统自动化，2016，40(16)：49-55.
LIU Nian, WANG Cheng, LEI Jinyong. Power energy sharing and demand response model for photovoltaic prosumer cluster under market environment [J]. Automation of Electric Power Systems, 2016, 40(16): 49-55.

[8] MA L, LIU N, ZHANG J, et al. Energy management for joint operation of CHP and PV prosumers inside a grid-connected microgrid: a game theoretic approach[J]. IEEE Transactions on Industrial Informatics, 2016, 12(5): 1930-1942.

[9] 刘念，张建华.互动用电方式下的信息安全风险与安全需求分析[J].电力系统自动化，2011，35(2)：79-83.
LIU Nian, ZHANG Jianhua. Cyber security risks and requirements for customer interaction of smart grid [J]. Automation of Electric Power Systems, 2011, 35(2): 79-83.

[10] 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.
TANG Yi, CHEN Qian, LI Mengya, et al. Overview on cyber-attack against cyber physical power system [J]. Automation of Electric Power Systems, 2016, 40(17): 59-69.

[11] 刘念，余星火，张建华.网络协同攻击：乌克兰停电事件的推演

与启示[J].电力系统自动化,2016,40(6):144-147.
LIU Nian, YU Xinghuo, ZHANG Jianhua. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147.

[12] 陈兴跃.勒索蠕虫病毒事件反思:网络安全能力急需协同[J].中国信息化,2017(6):8-11.
CHEN Xingyue. Reflection on the ransomware incident: synergy in cyber security capabilities is urgently needed [J]. China Informatization, 2017(6): 8-11.

[13] 舒隽,郭志锋,韩冰.电网虚假数据注入攻击的双层优化模型[J].电力系统自动化,2019,43(10):95-100.
SHU Jun, GUO Zhifeng, HAN Bing. Bi-level optimization model of false data injection attack for power grid [J]. Automation of Electric Power Systems, 2019, 43(10): 95-100.

[14] ZHAO J, ZHANG G, DONG Z, et al. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation [J]. IEEE Transactions on Smart Grid, 2016, 7(1): 6-8.

[15] CHE L, LIU X, LI Z, et al. False data injection attacks induced sequential outages in power systems [J]. IEEE Transactions on Power Systems, 2019, 34(2): 1513-1523.

[16] TAN R, NGUYEN H H, FOO E Y S, et al. Modeling and mitigating impact of false data injection attacks on automatic generation control [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(7): 1609-1624.

[17] ANWAR A, MAHMOOD A N. Stealthy and blind false injection attacks on SCADA EMS in the presence of gross errors [C]// 2016 IEEE Power and Energy Society General Meeting (PESGM), July 17-21, 2016, Boston, USA.

[18] LIU X, ZHU P, ZHANG Y, et al. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure [J]. IEEE Transactions on Smart Grid, 2015, 6(5): 2435-2443.

[19] DAYARATNE T, RUDOLPH C, LIEBMAN A, et al. High impact false data injection attack against real-time pricing in smart grids [C]// 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), September 29- October 2, 2019, Bucharest, Romania.

[20] RAMAN G, PENG J C, RAHWAN T. Manipulating residents' behavior to attack the urban power distribution system [J]. IEEE Transactions on Industrial Informatics, 2019. 15 (10): 5575-5587.

[21] LIU N, CHEN J, ZHU L, et al. A key management scheme for secure communications of advanced metering infrastructure in smart grid[J]. IEEE Transactions on Industrial Electronics, 2013, 60(10): 4746-4756.

[22] 刘鑫蕊,吴泽群.面向智能电网的空间隐蔽型恶性数据注入攻击在线防御研究[J/OL].中国电机工程学报:1-13[2020-04-27].https://doi.org/10.13334/j.0258-8013.pcsee.190089.
LIU Xinrui, WU Zequn. Online defense research of spatial-hidden malicious data injection attack in smart grid [J/OL]. Proceedings of the CSEE: 1-13 [2020-04-27]. https://doi.org/10.13334/j.0258-8013.pcsee.190089.

[23] ZHAO J, ZHANG G, SCALA M L, et al. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks [J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1580-1590.

[24] 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.

[25] 马丽,刘念,张建华,等.自动需求响应模式下光伏用户群的优化运行模型[J].中国电机工程学报,2016,36(13):3422-3432.
MA Li, LIU Nian, ZHANG Jianhua, et al. Optimal operation model of user group with photovoltaic in the mode of automatic demand response [J]. Proceedings of the CSEE, 2016, 36(13): 3422-3432.

[26] WOOD A J, WOLLENBERG B F. Power generation, operation, and control [M]. Hoboken, USA: Wiley-Interscience, 1996.

[27] JHALA K, NATARAJAN B, PAHWA A, et al. Stability of transactive energy market-based power distribution system under data integrity attack[J]. IEEE Transactions on Industrial Informatics, 2019, 15(10): 5541-5550.

[28] NASH J. Noncooperative games[J]. Annals of Mathematics, 1951, 54(2): 289-295.

[29] MONDERER D, SHAPLEY L S. Potential games [J]. Games and Economic Behavior, 1996, 14(1): 124-143.

[30] DAVID G L. Linear and nonlinear programming [M]. New York, USA: Springer, 2008.

[31] WANG J, SHAHIDEHPOUR M, LI Z, et al. Strategic generation capacity expansion planning with incomplete information[J]. IEEE Transactions on Power System, 2009, 24(2): 1002-1010.

[32] DING T, BO R, GU W, et al. Absolute value constraint based method for interval optimization to SCED model [J]. IEEE Transactions on Power System, 2014, 29(2): 980-981.

[33] LIU F, CAI M, WANG L, et al. An ensemble model based on adaptive noise reducer and over-fitting prevention LSTM for multivariate time series forecasting [J]. IEEE Access, 2019, 7: 26102-26115.

[34] GOODFELLOW I, BENGIO Y, COURVILLE A. Deep learning[M]. Cambridge, MA, USA: MIT Press, 2016.

陈刘东(1997—),男,硕士研究生,主要研究方向:信息物理系统、配电网优化。E-mail:liudong@ncepu.edu.cn

刘　念(1981—),男,通信作者,博士,教授,博士生导师,主要研究方向:智能配用电、综合能源系统、信息物理系统。E-mail:nianliu@ncepu.edu.cn

(编辑　杨松迎)

False Data Injection Attack and Detection Method for Interactive Demand Response

CHEN Liudong, *LIU Nian*

(State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources (North China Electrical Power University), Beijing 102206, China)

Abstract: It is analyzed that the vulnerability to the false data injection (FDI) attack on the demand side of interactive demand response (IDR). The attack process to user energy management system (UEMS) is also summarized. Based on this, an attack model for the IDR is established by the leader-follower game framework. The existence and uniqueness of Stackelberg equilibrium are proved. The parameter of the cost function is selected as the attacker′s attack vector, and the attack goal is to cause the reverse peak-load regulation. An attack detection method based on a distributed event trigger mechanism and machine learning is proposed. The event trigger mechanism is implemented in the UEMS. The system detection is carried out in the energy retailer (ER) based on the long short-term memory (LSTM) network. Finally, it is concluded that the results of attack model and sensitivity of attack parameters in the case study. It is also compared that the accuracy and detection time of distributed event trigger mechanism and time trigger mechanism under different load thresholds and attack rates.

This work is supported by National Natural Science Foundation of China (No. 51877076).

Key words: false data injection attack (FDI); attack detection; interactive demand response (IDR); game theory; machine learning

附录A

为了证明博弈G_C中纳什均衡的唯一性，需要证明存在唯一的最优负荷策略$L_{i,h}^*$。由于式(7)为3项的加和，并且产销者数量的多少并不改变函数的凹凸性，因此，采用$n=2$分析式(7)海森矩阵的凹凸性，针对$L_{1,h}$及$L_{2,h}$的海森矩阵表示为：

$$H_M=\begin{bmatrix}2a_h & a_h\\ a_h & 2a_h\end{bmatrix} \tag{A1}$$

该海森矩阵的1阶主子式为$2a_h$，2阶主子式为$3(a_h)^2$，由于$a_h>0$，所以H_M为正定矩阵，$f(\cdot)$关于$L_{i,h}$，$i\in[1,N]$，$h\in[1,H]$为凹函数，纳什均衡在下述区域中存在且唯一：

$$L_{i,h}^*=\arg\max_{L_{i,h}}\left(f(\cdot)\right) \tag{A2}$$

产销者可以通过设定负荷策略最大化势函数，因此纳什均衡存在且唯一，定理1得证。

附录B

根据正文中文献[23]的定理1，从3个方面证明主从博弈中SE的唯一性，首先，每个博弈者的策略集是凸集、紧凑集和非空集，这些特征可通过式(3,9)直接看出。其次，每个产销者相对于攻击者的策略都有唯一的最优策略，这在定理1中已经证实。最后，攻击者对于所有产销者的策略具有唯一的最优策略。采用线性规划的单纯形法对其进行证明[30]。将式(9)表示的线性规划问题转化为标准形式：

$$\max_{\Delta a_h} f_{vir}(\Delta\boldsymbol{a})=\sum_{h=1}^{H}\Delta a_h L_h^2+0\Delta a_h'-a_h L_h^2-b_h L_h \tag{B1}$$

$$\text{s.t.}\begin{cases}\Delta a_h+\Delta a_h'=ua_h\\ \sum_{h=1}^{H}\Delta a_h=va_h\\ \Delta a_h\geqslant 0\end{cases} \tag{B2}$$

式中：$\Delta a_h'$为松弛变量，将不等式约束变为等式约束，式(B2)对$\forall h\in[1,H]$成立。

该线性规划问题包含$2H$个变量，其中H个实际变量以及H个松弛变量，约束的数量为$H+1$个，因此，基变量数量为$H+1$。方便起见，选取H个实际变量以及1个松弛变量作为基变量Δa_m，m为基变量序数，非基变量Δa_n个数则为$H-1$，n为非基变量序数，且由松弛变量构成。为了证明最优解的唯一性，需要证明所有检验数σ_n，$n\in[H+2,2H]$为负数[30]。由于$a_h L_h^2$以及$b_h L_h$在L_h确定以后为常数，故将这2项忽略，第1次单纯型迭代的结果为：

$$\begin{aligned}f_{vir}^{(0)}\left(\{\Delta a_m\}_{m\in[1,H+1]}\right)&=\sum_{m=1}^{H+1}L_m^2\Delta a_m^{(0)}\\ f_{vir,n}^{(1)}\left(\{\Delta a_m\}_{m\in[1,H+1]}\right)&=f_{vir}^{(0)}+\theta(0-\sum_{m=1}^{H+1}L_m^2\boldsymbol{\omega}_{m,n})\end{aligned} \tag{B3}$$

式中：$\sigma_n=0-\sum_{m=1}^{H+1}L_m^2\boldsymbol{\omega}_{m,n}$，$\forall n\in[H+2,2H]$；$\{\Delta a_m\}_{m\in[1,H+1]}$表示初始基变量；$f_{vir}^{(0)}$为初始基变量$\Delta a_m^{(0)}$的解；$f_{vir,n}^{(1)}$为第1次单纯型迭代的解；$\boldsymbol{\omega}_{m,n}$为约束系数矩阵；$m$和$n$分别表示矩阵的行列序数；$\theta$为正数乘子。

根据式(B2)，所有的$\boldsymbol{\omega}_{m,n}=1$，并且$L_m^2$为正数，所以所有的$\sigma_n$都为负数。因此定理2得证，即存在唯一的SE。