基于安全博弈的综合能源系统安全性分析及防御策略

王 丹[1,2],赵 平[1],臧宁宁[2],闫 英[3]
(1. 西安建筑科技大学 土木工程学院,陕西 西安 710055;2. 中国大唐集团科学技术研究院有限公司,北京 100040;
3. 中国能源建设集团陕西省电力设计院,陕西 西安 710054)

摘要:基于安全博弈理论,分析辨识综合能源系统安全运行的关键影响因素,将其作为安全防御的薄弱环节,制定防御策略并重点防护。构建综合能源系统防御者-攻击者-防御者3层零和主从博弈模型,攻击者以攻击系统的薄弱环节为策略期望最大化系统损失,防御者制定防护策略以增强系统的安全性;求解博弈模型的均衡解,得到的最小系统损失即为最佳防御策略;以某综合能源系统为例进行仿真分析,结果表明优先防护系统的薄弱环节可提升系统的安全可靠性,为分析综合能源系统的安全性提供参考。

关键词:安全博弈;综合能源系统;防御策略;攻击策略;薄弱环节
中图分类号:TM 73 **文献标志码**:A DOI:10.16081/j.epae.201908028

0 引言

综合能源系统与互联网技术深度融合,产生了新的供能、用能、消费模式[1]。多种能源生产、配送、转换、交易和消费复杂多变,不同环节的时空关联度增强,受外部因素影响加剧,任何薄弱环节都会导致事故,尤其是物联网接入终端数量发生裂变,从终端侵入系统网络或云,系统运行将面临巨大安全风险,同时社会对能源供应的安全可靠性也提出了更高的安全要求[2-4],如何保证其安全运行是极具挑战的课题。

目前,综合能源控制系统多以系统功能作为第一要素,在设计、研发和集成阶段都没有过多考虑数据、网络、信息等安全问题,综合能源系统组件多、信息-物理融合程度高,对信息系统的攻击将影响到系统整体的安全稳定。部分学者针对综合能源系统安全性分析、规划与优化运行技术等方面开展了相关研究。文献[5]针对区域多能源枢纽单元互联的热电耦合综合能源系统,在多能流计算及静态安全性分析的基础上提出了一种综合考虑热电最优潮流与静态安全因素的综合能源系统双层优化模型。文献[6]阐述状态估计层面下恶性数据的定义,从状态估计、闭环控制、安全稳定分析及电力市场4个方面分别探讨恶性数据对电力系统的影响,综述了国内外学者应对恶性数据所提的各种防御方法。文献[7]考虑电网的安全约束,建立虚拟电厂优化调度的下层安全调度模型。文献[8]建立电热水负荷模型分析其对供能可靠性指标的影响。文献[9]构建的机会约束规划模型有助于提高电-气互联综合能源系统运行的安全性。文献[10-11]分析了多区域综合能源系统热网以及热电联产系统运行优化问题。文献[12-18]分析研究了虚拟电厂、电网等系统的投资收益风险和安全可靠等问题。相较于传统的能源系统,综合能源系统更具有复杂性、互联性、开放性和共享性,其安全运行面临的不确定因素范围更广,系统运行过程中的信息透明度增强,任何随机或蓄意的破坏行为都可能造成极大的经济损失和社会危害。在有限的安全防御资源下,识别系统中薄弱环节和脆弱元件,优先对其进行重点防护,对提升系统的安全可靠性至关重要[19-20]。目前,安全博弈理论可以较好地模拟攻防过程,识别最关键的安全威胁并制定最恰当的防护策略,为综合能源系统安全分析提供了新的研究思路[21-25]。安全博弈不能够对现有的系统进行安全评估,虽然其在传统计算机网络和信息安全方向应用得非常广泛,但是将其引入综合能源系统中解决安全相关的问题尚处于初步研究阶段。

鉴于此,本文运用安全博弈理论构建综合能源系统防御者-攻击者-防御者3层零和主从博弈的模型,分析防御者和攻击者双方策略,攻击者攻击系统的薄弱环节,以造成系统的最大损失;防御者采取适当的防御措施并进行策略调整,最小化攻击造成的损失。求得博弈模型的均衡解,既可用于预测攻击行为,识别系统薄弱环节,又可为系统部署防御决策提供指导性意见,提高系统安全性与可靠性水平。

1 综合能源系统安全博弈分析

综合能源系统是一种多种能源网络协调耦合形成的复杂多网流系统,网络系统中大数据与实体设备互联互通,各种设备、元件、控制装置、输送系统、

收稿日期:2019-04-01;**修回日期**:2019-06-20
基金项目:陕西省重点研发计划项目(2018SF-385);中国大唐集团科技项目(KYJ2017-6000)
Project supported by the Key Research and Development Program of Shaanxi Province(2018SF-385) and the Science and Technology Program of China Datang Corporation Ltd (KYJ2017-6000)

耦合系统从独立封闭走向互联互通，分析系统安全面临的威胁需要从系统防御和修复2个维度进行，将态势感知系统发现的威胁自动转化成网络设备的策略进行处理，搭建威胁检测发现到应急处理的桥梁，实现一体化协同安全体系。

安全博弈[26]是指防御者与攻击者为参与者，并能够描述二者相互作用过程的博弈格局，为分析综合能源系统安全问题提供了合适的研究手段，防御方和攻击方在复杂互联的系统中展开博弈，攻击方蓄意破坏系统中薄弱环节以最大化系统的损失，防御方合理预测采取防护策略以增强系统的安全稳定运行。

1.1　组成要素

参与者为防御者F和攻击者G。综合能源系统可能受到病毒、黑客、信息泄露、自然灾害和资金断裂等破坏，引发系统运行风险，虽然各种不确定因素攻击的对象不同，但其造成的结果是系统停运、瘫痪等故障，此种情况下，可将这些不确定威胁因素统一描述为博弈的攻击者。系统管理者以及安全维护人员具有相同的目标行为和信息，可以抽象概括为防御者[20]。

策略空间为防御者和攻击者的行动方案。攻击者的策略P_G是利用有限的资源攻击系统的关键点或薄弱环节，每个具体的攻击目标都有具体的攻击行为，攻击策略在应用安全方面可以攻击系统中的各类资源、设备和数据的接口、数据平台、集成调控装置等；在数据安全方面，破坏系统权限和窃取数据采集、存储、运输、发布、用户挖掘等环节信息；在设备安全方面，设备老化，基础设施薄弱，维护不足，系统中的元件、设备等可成为攻击点，遭到人为破坏或自然灾害，损失巨大；在网络安全方面，利用病毒大规模的复制、传输或采用黑客技术攻击操作系统、应用程序、传输通道端口等，造成网络瘫痪；在物理安全方面，攻击机房和计算机通信网络传输媒体等设备，造成系统失控等。防御者的策略P_F是合理配置资源，预估攻击者的攻击策略，考虑在最坏的干扰下系统能够实现最佳性能。针对应用安全攻击，可设置身份认证、权限控制、访问监控，解决控制系统中智能终端之间信息交换安全等防御措施；针对数据安全防御，有数据加密、隐私保护、备份和恢复设置、安全审计、对历史数据进行扰动分析等策略；针对设备安全防御，采用设备监控保护、更换升级等；针对网络安全的防御策略包括安全区域划分、资源隔离、系统加密、安装补丁弥补漏洞、提升网闸网关技术、隐藏IP地址、终端入侵检测、安装防火墙、解决公网信息安全交换等；针对物理安全采取的防御措施有门禁管控、云监控、机房及环境监控、应急管理等。上述攻击者和防御者决策可采用单次纯策略或者混合策略。

支付可用参与者行为造成的系统损失值进行量化表达，对不同的参与者可用系数矩阵进行表示，矩阵中的行和列分别表示攻击者和防御者，矩阵中的每一个元素表示双方各自选择策略下的支付。本文中防御者的支付值与攻击者造成的损失值之和为0，可由一个矩阵进行表示。

本文假设防御者可根据攻击者的攻击行为进行策略预测部署，博弈双方对系统的最坏情况都可以完全知悉，参与者双方都具有完全理性，信息结构为完全信息状态，其均衡为Stackelberg均衡。

系统的脆弱程度是指攻击者为达到某一特定目的，针对系统脆弱性在明确的攻击下完成的，而非系统自身不稳定导致的故障，脆弱程度反映了系统抵御攻击的能力。脆弱状态是介于安全和失败2个稳态中的暂态，系统脆弱程度的评估指标包括系统环境、受保护对象和安全需求、系统输入信息和数据、系统状态、系统规则触发、系统威胁等[27]。

1.2　博弈过程

防御者和攻击者安全博弈形成Stackelberg均衡的过程可以分为以下3个阶段。

第一阶段是防御者制定防御策略，投入资源对系统元件进行保护，以降低故障带来的损失。此防御是极小化攻击所造成的损失。本文重点分析关键环节的防护以及故障维修时间等，具体的措施有加强培训和提升运维人员的安全应急能力、对数据进行监控分析、分析历史数据扰动预判故障、定期杀毒、安全隔离关键元件等。

第二阶段是攻击者对目标发起攻击，试图极大化攻击造成的损失。攻击策略是造成损失大于最低停运损失。

第三阶段是系统受到攻击恢复运行的策略调整，防御者根据攻击方的策略进行投入资源调整，可利用大数据技术和威胁情报提升检测和响应为核心的积极防御能力，保护关键环节，极小化防御成本，一般以系统最小失负荷量作为调整目标。

2　安全博弈模型

2.1　模型构建

（1）防御者策略及表达。

防御者根据可投入的资源数对系统进行保护、修复。防御者可配置投入的资源总量为：

$$C_{\text{total}}=(c_1,c_2,\cdots,c_p,c_r) \tag{1}$$

其中，c_1、c_2、…、c_p为防御者对元件的防护成本；c_r为修复成本。

令p_k表示元件k受到防护的程度，假设攻击元件k遭到攻击的概率仅与受到保护的程度有关，则攻击元件k成功的概率为$1-p_k$。系统中各元件受到

的保护程度用向量$\boldsymbol{p}=[p_1,p_2,\cdots,p_p]$表示，将元件$k$受到的保护程度$p_k$定义为投入受保护元件的资源量$c_k$的函数，则：

$$\begin{cases}p_k=p_k(c_k)\\ \sum_{k=1}^{n}c_k\leqslant c_p\end{cases}\tag{2}$$

其中，$0\leqslant p_k\leqslant 1$；$n$为防御方选择受保护元件的数量。

令T表示不增加额外资源投入时系统的修复时间，若防御方投入额外资源进行系统元件修复，则修复时间减少，可表示为：

$$t_k=Tf_k(c_r)\tag{3}$$

易得$p_k(c_k)$为连续增函数，$f_k(c_r)$为连续减函数。防御者的策略可以表示为：

$$P_F=\left\{C_{total}=(c_1,c_2,\cdots,c_p,c_r)\ \middle|\ \sum_{k=1}^{n}c_k\leqslant c_p,\ C_{total}=C_P+c_r\right\}\tag{4}$$

(2)攻击者策略及表达。

攻击者可能攻击系统的一个元件或者其组合，令N为攻击策略数量，系统中有m个攻击元件，同时攻击的元件为$l(l>1)$，则攻击的策略数量为：

$$N=C_m^l=\frac{m!}{l!(m-l)!}\tag{5}$$

设定一个攻击策略为一个概率分布，q_i表示目标i被击中的概率，则有：

$$\sum_{i=1}^{N}q_i=1\tag{6}$$

其中，$q_i\geqslant 0$。

令μ_k表示元件k受到攻击后的单位时间损失，t_k表示修复时间，则元件k受到攻击后的损失为：

$$x_k=\mu_k t_k\tag{7}$$

攻击者的混合策略可描述为：

$$P_C^*=\left\{S_C=(q_1,q_2,\cdots,q_N)\ \middle|\ q_i\geqslant 0,i=1,2,\cdots,N;\sum_{i=1}^{N}q_i=1\right\}\tag{8}$$

(3)支付。

防御者目标是对抗外来攻击的同时最小化防御成本[20]，即：

$$\min_{\boldsymbol{y}\in Y}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{y}\tag{9}$$

其中，$\boldsymbol{C}$为防御成本列向量；$\boldsymbol{y}$为防御策略列向量；Y为系统安全运行的约束条件集合。

攻击者目标是极大化防御成本，设$\boldsymbol{x}$为攻击决策的列向量，X为攻击者G攻击行为策略集合，则攻击者-防御者模型为：

$$\max_{\boldsymbol{x}\in X}\min_{\boldsymbol{y}\in Y(\boldsymbol{x})}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{y}\tag{10}$$

将攻击者-防御者模型作为内层模型，则可将攻击者-防御者-攻击者表示为：

$$\min_{\boldsymbol{\omega}\in W}\max_{\boldsymbol{x}\in X(\boldsymbol{\omega})}\min_{\boldsymbol{y}\in Y(\boldsymbol{x})}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{y}\tag{11}$$

其中，$\boldsymbol{\omega}$为防御策略列向量；W为可行的防御策略构成的集合；$\boldsymbol{x}\in X(\boldsymbol{\omega})$表示攻击者的攻击策略受到防御策略的制约。式(11)描述了攻击者G给系统造成的最严重损失被极小化。

综上所述，博弈模型可描述为：

$$\min_{\boldsymbol{\omega}\in W}\max_{\boldsymbol{x}\in X(\boldsymbol{\omega})}\min_{\boldsymbol{y}\in Y(\boldsymbol{x})}\boldsymbol{C}^{\mathrm{T}}\boldsymbol{y}\tag{12}$$

$$\text{s.t.}\quad \boldsymbol{A}\boldsymbol{y}=\boldsymbol{b}$$

$$\boldsymbol{F}\boldsymbol{y}\leqslant\boldsymbol{x}(1-p_k)$$

约束条件中的等式表示系统正常运行的约束，不等式表示系统有安全防御资源投入时受到攻击不可能完全失效，只是系统安全性能降低。

基于1.2节的分析，为保证第一阶段的防御措施的鲁棒性，即该防御措施足以应对最严重的并发系统元件故障情况，必须在制定第一阶段防御策略时考虑第二、三阶段的影响。上述3个阶段可描述为上-中-下3层博弈模型。

(1)下层模型。

下层模型决策目标是最小化系统损失，综合能源系统负荷P包含电负荷、热负荷、冷负荷等，在模型中，以电负荷损失量Δp_d、热负荷损失量Δp_h、冷负荷损失量Δp_c、其他负荷损失量Δp_g为系统调整手段，引入单位负荷损失成本系数m_{dk}、m_{hi}、m_{cj}、m_{gt}将目标函数表示为损失成本，考虑系统正常运行的经济性和系统受到攻击不会完全失效的情形为约束条件，下层模型表达式为：

$$\min_{\Delta p_d,\Delta p_h,\Delta p_c,\Delta p_g}\sum_{k\in\Omega^d}m_{dk}\Delta p_{dk}+\sum_{i\in\Omega^h}m_{hi}\Delta p_{hi}+\sum_{j\in\Omega^c}m_{cj}\Delta p_{cj}+\sum_{t\in\Omega^g}m_{gt}\Delta p_{gt}\tag{13}$$

$$\text{s.t.}\quad p_{dk}^{(0)}+p_{hi}^{(0)}+p_{cj}^{(0)}+p_{gt}^{(0)}=P$$

$$0\leqslant\Delta p_{dk}\leqslant p_{dk}^{(0)},\ 0\leqslant p_{dk}^{(0)}+\Delta p_{dk}\leqslant p_{dk}^{\max},\ p_{dk}^{(0)}-\Delta p_{dk}\geqslant p_{dk}^{\min}$$

$$0\leqslant\Delta p_{hi}\leqslant p_{hi}^{(0)},\ 0\leqslant p_{hi}^{(0)}+\Delta p_{hi}\leqslant p_{hi}^{\max},\ p_{hi}^{(0)}-\Delta p_{hi}\geqslant p_{hi}^{\min}$$

$$0\leqslant\Delta p_{cj}\leqslant p_{cj}^{(0)},\ 0\leqslant p_{cj}^{(0)}+\Delta p_{cj}\leqslant p_{cj}^{\max},\ p_{cj}^{(0)}-\Delta p_{cj}\geqslant p_{cj}^{\min}$$

$$0\leqslant\Delta p_{gt}\leqslant p_{gt}^{(0)},\ 0\leqslant p_{gt}^{(0)}+\Delta p_{gt}\leqslant p_{gt}^{\max},\ p_{gt}^{(0)}-\Delta p_{gt}\geqslant p_{gt}^{\min}$$

其中，Ω^d、Ω^h、Ω^c、Ω^g分别为电力系统、热力系统、制冷系统和其他系统负荷集合；$p_{dk}^{(0)}$、$p_{hi}^{(0)}$、$p_{cj}^{(0)}$、$p_{gt}^{(0)}$为各系统的初始需求负荷，即经济负荷；$p_{dk}^{\max}$、$p_{dk}^{\min}$分别为电力系统正常运行负荷的上、下限；$p_{di}^{\max}$、$p_{hi}^{\min}$分别为热力系统正常运行负荷的上、下限；$p_{cj}^{\max}$、$p_{cj}^{\min}$分别为制冷系统正常运行负荷的上、下限；$p_{gt}^{\max}$、$p_{gt}^{\min}$分别为其他系统正常运行负荷的上、下限。

(2)中层模型。

中层模型决策目标是极大化系统损失，约束条件为确定造成系统同时停运元件集合y，中层模型表达式为：

$$\max_{y}\sum_{k\in\Omega^{\mathrm{d}}}m_{\mathrm{d}k}\Delta p_{\mathrm{d}k}+\sum_{i\in\Omega^{\mathrm{h}}}m_{\mathrm{h}i}\Delta p_{\mathrm{h}i}+\sum_{j\in\Omega^{\mathrm{c}}}m_{cj}\Delta p_{cj}+\sum_{t\in\Omega^{\mathrm{g}}}m_{gt}\Delta p_{gt}\tag{14}$$

$$\text{s.t.}\quad\sum_{k\in\Omega^{\mathrm{d}}}y_k+\sum_{i\in\Omega^{\mathrm{h}}}y_i+\sum_{j\in\Omega^{\mathrm{c}}}y_j+\sum_{t\in\Omega^{\mathrm{g}}}y_t=K$$

$$y_k,y_i,y_j,y_t\in\{0,1\},\ k\in\Omega^{\mathrm{d}},\ i\in\Omega^{\mathrm{h}},\ j\in\Omega^{\mathrm{c}},\ t\in\Omega^{\mathrm{g}}$$

其中，K为系统故障时停运的元件总数；y_k、y_i、y_j、y_t为各系统中元件停运策略，取值为1时表示停运，取值为0时表示未停运。

（3）上层模型。

防御者利用有限资源Q投入安全防御，上层模型的表达式为：

$$\min_{x}\sum_{k\in\Omega^{\mathrm{d}}}m_{\mathrm{d}k}\Delta p_{\mathrm{d}k}+\sum_{i\in\Omega^{\mathrm{h}}}m_{\mathrm{h}i}\Delta p_{\mathrm{h}i}+\sum_{j\in\Omega^{\mathrm{c}}}m_{cj}\Delta p_{cj}+\sum_{t\in\Omega^{\mathrm{g}}}m_{gt}\Delta p_{gt}\tag{15}$$

$$\text{s.t.}\quad y_k\leqslant 1-x_k,\ y_i\leqslant 1-x_i,\ y_j\leqslant 1-x_j,\ y_t\leqslant 1-x_t$$

$$\sum_{k\in\Omega^{\mathrm{d}}}c_kx_k+\sum_{i\in\Omega^{\mathrm{h}}}c_ix_i+\sum_{j\in\Omega^{\mathrm{c}}}c_jx_j+\sum_{t\in\Omega^{\mathrm{g}}}c_tx_t\leqslant Q$$

$$x_k,x_i,x_j,x_t\in\{0,1\},\ k\in\Omega^{\mathrm{d}},\ i\in\Omega^{\mathrm{h}},\ j\in\Omega^{\mathrm{c}},\ t\in\Omega^{\mathrm{g}}$$

其中，x_k、x_i、x_j、x_t为各系统防御策略，取值为1时表示防御，取值为0时表示未防御；c_k、c_i、c_j、c_t分别为保护各系统元件k、i、j、t投入的资源数。

2.2　模型求解

博弈模型求解过程分为2个过程，首先针对中层与下层模型利用强对偶模型进行转换求解，将max-min问题转化为单层的max问题进行求解，经过转化消去了防御者-攻击者-防御者模型中的下层问题，得到双层规划问题，然后采用枚举树方法对模型进行求解。

（1）强对偶定理。

将式（13）和式（14）转化为：

$$\max_{y}\sum_{k\in\Omega^{\mathrm{d}}}p_{\mathrm{d}k}^{(0)}y_k+\sum_{i\in\Omega^{\mathrm{h}}}p_{\mathrm{h}i}^{(0)}y_i+\sum_{j\in\Omega^{\mathrm{c}}}p_{cj}^{(0)}y_j+\sum_{t\in\Omega^{\mathrm{g}}}p_{gt}^{(0)}y_t\tag{16}$$

$$\text{s.t.}\quad\sum_{k\in\Omega^{\mathrm{d}}}y_k+\sum_{i\in\Omega^{\mathrm{h}}}y_i+\sum_{j\in\Omega^{\mathrm{c}}}y_j+\sum_{t\in\Omega^{\mathrm{g}}}y_t=K$$

$$y_k,y_i,y_j,y_t\in\{0,1\},\ k\in\Omega^{\mathrm{d}},\ i\in\Omega^{\mathrm{h}},\ j\in\Omega^{\mathrm{c}},\ t\in\Omega^{\mathrm{g}}$$

$$p_{\mathrm{d}k}^{(0)}y_k\leqslant p_{\mathrm{d}k}^{\max},\ p_{\mathrm{h}i}^{(0)}y_i\leqslant p_{\mathrm{h}i}^{\max},\ p_{cj}^{(0)}y_j\leqslant p_{cj}^{\max},\ p_{gt}^{(0)}y_t\leqslant p_{gt}^{\max}$$

$$\sum_{k\in\Omega^{\mathrm{d}}}y_k\leqslant m_{\mathrm{d}k},\ \sum_{i\in\Omega^{\mathrm{h}}}y_i\leqslant m_{\mathrm{h}i},\ \sum_{j\in\Omega^{\mathrm{c}}}y_j\leqslant m_{cj},\ \sum_{t\in\Omega^{\mathrm{g}}}y_t\leqslant m_{gt}$$

（2）枚举树算法。

经过上述转化消去了模型的下层问题，得到式（16），采用枚举方法[20]求解式（15）和式（16）所示两层规划模型。枚举法的效率取决于枚举状态的数量以及单个状态，研究者可通过减少状态总数，降低单个状态的考察代价来缩短计算时间，满足工程应用要求，步骤如下。

a. 生根策略。令x_k、x_i、x_j、x_t都等于0，求解无防御状态下的故障元件集y^*，该集合为当前无防御状态下可使系统损失最大的故障元件集合，对应于攻击者的最优攻击策略集，则$\{0,y^*\}$即为枚举树的根节点。

b. 生长节点。在父节点$\{x(k),y^*(k)\}$的故障元件集合y^*中，依次选择一个元件进行防御，求解一系列新的故障元件集合$y^*(k+1)$，降低系统的最大损失，进而得到若干新的子节点，新生子节点与父节点的树枝长度取决于相应选择元件所需的防御资源数。

c. 终止策略。若当前节点距离根节点长度等于限定防御资源总数，或剩余防御资源不足以展开进一步防御，则认为该节点为叶节点，不再另生新枝。否则转至步骤**b**，直至所有节点均为叶节点为止。

d. 确定最优防御策略。分析求得的所有叶节点，其中具有最小系统损失者对应系统最优防御策略，表明该节点应当优先被防御。

3　算例分析

基于上述讨论，以某综合能源系统为例进行系统安全性分析，该综合能源系统包括光伏发电、太阳能热水、冰蓄冷等系统。综合能源安全稳定运行需要考虑应用安全、数据安全、设备安全、网络安全、物理安全5个关键环节受到单一或组合攻击。目前该系统运行稳定，系统的脆弱程度评估级是一般，根据该系统中各分系统供能需求、系统脆弱程度及常规的安全投入经验数值设置发电、太阳能热水、冰蓄冷系统投入资源数c_k、c_i、c_j分别为3、2、1，成本系数$m_{\mathrm{d}k}$、$m_{\mathrm{h}i}$、m_{cj}分别为5、2、4，负荷损失值Δp_{d}、Δp_{h}、Δp_{c}分别为30、20、15 p.u.，负荷初设需求值$p_{\mathrm{d}k}^{(0)}$、$p_{\mathrm{h}i}^{(0)}$、$p_{cj}^{(0)}$分别为50、30、20 p.u.。安全防御的5个关键环节策略权重如表1所示。根据表1所示结果对算例进行综合能源系统安全性分析，如图1所示。

根据式（15）和式（16）求解综合能源系统在K=3时投入不同防御资源情形下最优防御策略，结果如表2所示。需要说明的是，仿真为数值模拟，计算结果没有单位，后同。

表1　安全防御指标权重

Table 1　Safety and defense index weights

关键环节	指标权重		
	光伏发电	太阳能热水	冰蓄冷系统
应用安全	0.23	0.215	0.23
数据安全	0.17	0.230	0.18
设备安全	0.20	0.185	0.19
网络安全	0.24	0.200	0.21
物理安全	0.16	0.170	0.19

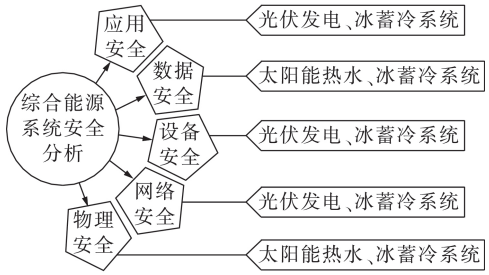

图1 综合系统安全性分析

Fig.1 Safety analysis of integrated energy system

表2 K=3时不同防御资源下的最优防御策略

Table 2 Optimal defense strategy under different defense resources when K=3

Q	最优防御策略	被攻击对象	损失
3	光伏系统网络安全、应用安全、设备安全	太阳能热水系统数据安全,冰蓄冷系统应用安全	47.60
4	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全	太阳能热水系统数据安全,冰蓄冷系统应用安全、设备安全	46.82
5	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全、应用安全	太阳能热水系统数据安全,冰蓄冷系统应用安全、物理安全	45.50
6	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全、应用安全、网络安全	冰蓄冷系统网络安全、应用安全、物理安全	44.50

K=5时投入不同防御资源情形下最优防御策略,结果如表3所示。

表3 K=5时不同防御资源下的最优防御策略

Table 3 Optimal defense strategy under different defense resources when K=5

Q	最优防御策略	被攻击对象	损失
3	光伏系统网络安全、应用安全、设备安全	太阳能热水系统数据、应用、设备安全,冰蓄冷系统应用、网络安全	70.44
4	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全	太阳能热水系统数据、应用安全,冰蓄冷系统应用、设备、网络安全	68.81
5	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全、应用安全	太阳能热水系统数据、应用、设备安全,冰蓄冷系统应用、物理安全	65.74
6	光伏系统网络安全、应用安全、设备安全,太阳能热水系统数据安全、应用安全、网络安全	太阳能热水系统数据、应用、设备安全,冰蓄冷系统应用、物理安全	63.14

由表2、3可知,相较于无防御状态,随着防护资源的增加,系统失负荷逐渐减少,系统损失不断降低,系统的安全可靠性逐渐提升;系统投入防护资源较少时,防御策略是优先光伏系统的网络安全、应用安全、设备安全等,随着防御资源投入增多,增加对太阳能热水系统数据安全和应用安全进行防御保护;在同样的防御资源下,停运对象增加导致系统损失上升,防御者根据安全指标的策略权重进行防御策略调整,系统损失减少。

由上述计算结果分析可得防御资源、系统同时停运元件数量以及系统损失三者变化的通用结果。在防御资源相对多、系统同时停运元件少的情况下,系统损失较低;在防御资源相对少、系统同时停运元件多的情况下,系统损失较高。

由此可绘制系统损失随防御资源变化的趋势,如图2所示。可见K=3时,Q值由3增到6,系统损失由47.6降低到44.5;K=5时,Q值由3增到6,系统损失由70.44降低到63.14;$K>5$时,系统损失增大,随着Q值增大损失降低;Q为3、4、5、6时,K值增大,系统损失不断增大。

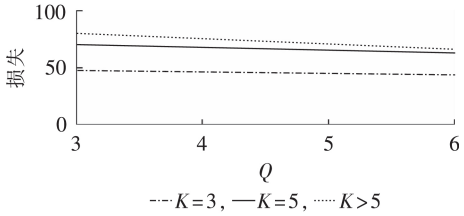

图2 系统损失随防御资源变化趋势

Fig.2 Variation tendency of system loss vs. defense resource

根据表2、3中攻防防御策略分析,制定各系统在不同防御策略下的防御措施如表4所示。

表4 各系统在不同防御策略下的防御措施

Table 4 Defense measures of each system under different defense strategies

系统	防御策略	防御措施
光伏	网络安全	在系统内部不同子系统或区域部署防火墙实现边界保护和访问控制,在系统内部核心流量节点布置监测和审计系统,在系统内部关键区域的边界部署入侵检测系统等
	应用安全	设置服务器报警策略并产生报警日志,用户设置账户密码,设置用户身份权限,设置访问权限和时间期限,定期备份日志信息备份
	设备安全	部署工控主机和服务设备卫士,实现外设管理、病毒防护、基线管理和系统完整性保护
太阳能热水	数据安全	系统中应用的数据确保完整、可用,并对数据加密,数据传输防止窃听、泄露、篡改和破坏,数据库进行加密及监控,保护数据分析结果,数据处理注意备份和保密等
	应用安全	拒绝未经过认证签名的应用软件的安装和执行,采用口令或解锁图案等强制进行用户身份鉴别
	网络安全	能够提供安全域隔离运行环境,保证应用的输入、输出以及存储信息不被非法获取
冰蓄冷	安全防御	进行系统的高风险排名,识别高风险漏洞进行针对性的解决,提升风险的识别和分析能力

4 结论

本文对综合能源系统安全性进行了初步的分析和探讨。综合能源系统应用安全、数据安全、设备安全、网络安全、物理安全五方面的安全问题值得关注,需要重点防护。利用安全博弈的理论方法分析系统的攻防策略,系统的薄弱环节和最佳防御策略即为安全博弈的均衡解,该均衡解可为系统的防御

决策提供指导性意见，可用于预测攻击行为，亦可分析遭受攻击后的防御资源配置，提高薄弱环节或元件的防护程度，使系统能够在真实发生攻击故障的情形下仍具有较高的防御能力。最后以某综合能源系统为例进行攻防模拟分析，计算结果表明，防御成本投入增多，系统的防护程度高，修复时间短，系统的安全可靠性提高；防御成本一定时，调整防御策略，优先保护最薄弱环节或元件，可以降低系统的损失；应用安全和网络安全比其他安全问题更脆弱，需要进行优先防御；系统的薄弱环节或元件保护程度越高，系统损失越小。

参考文献：

[1] 彭克，张聪，徐丙垠，等. 多能协同综合能源系统示范工程现状与展望[J]. 电力自动化设备，2017，37(6)：3-10.
PENG Ke，ZHANG Cong，XU Bingyin，et al. Status and prospect of pilot projects of integrated energy system with multi-energy collaboration[J]. Electric Power Automation Equipment，2017，37(6)：3-10.

[2] 侯恺. 电力系统可靠性评估方法改进与应用研究[D]. 天津：天津大学，2016.
HOU Kai. Power system reliability assessment methodology improvement and its application[D]. Tianjin：Tianjin University，2016.

[3] 刘吉臻，王玮，胡阳，等. 新能源电力系统控制与优化[J]. 控制理论与应用，2016，33(12)：1555-1561.
LIU Jizhen，WANG Wei，HU Yang，et al. Control and optimization of alternate electrical power system reliability[J]. Control Theory & Applications，2016，33(12)：1555-1561.

[4] 王伟亮，王丹，贾宏杰，等. 能源互联网背景下的典型区域综合能源系统稳态分析研究综述[J]. 中国电机工程学报，2016，36(12)：3292-3305.
WANG Weiliang，WANG Dan，JIA Hongjie，et al. Review of steady-state analysis of typical regional integrated energy system under the background of energy internet[J]. Proceedings of the CSEE，2016，36(12)：3292-3305.

[5] 潘益，梅飞，郑建勇，等. 计及静态安全因素与热电最优潮流的综合能源系统联合运行优化模型[J]. 电网技术，2019，43(1)：50-57.
PAN Yi，MEI Fei，ZHENG Jianyong，et al. Operation optimization model for multi-integrated energy systems considering static security and optimal energy flow[J]. Power System Technology，2019，43(1)：50-57.

[6] 卫志农，陈和升，倪明，等. 电力信息物理系统中恶性数据定义、构建与防御挑战[J]. 电力系统自动化，2016，40(17)：70-78.
WEI Zhinong，CHEN Hesheng，NI Ming，et al. Definition construction and defense of false data in cyber physical system[J]. Automation of Electric Power Systems，2016，40(17)：70-78.

[7] 臧海祥，余爽，卫志农，等. 计及安全约束的虚拟电厂两层优化调度[J]. 电力自动化设备，2016，36(8)：96-102.
ZANG Haixiang，YU Shuang，WEI Zhinong，et al. Safety-constrained two-layer optimal dispatch of virtual power plant[J]. Electric Power Automation Equipment，2016，36(8)：96-102.

[8] 黄玉雄，李更丰，别朝红，等. 分布式能源可靠性评估[J]. 智慧电力，2017，45(7)：43-50.
HUANG Yuxiong，LI Gengfeng，BIE Zhaohong，et al. Reliability evaluation of distributed integrated energy systems[J]. Smart Power，2017，45(7)：43-50.

[9] 张思德，胡伟，卫志农，等. 基于机会约束规划的电-气互联综合能源系统随机最优潮流[J]. 电力自动化设备，2018，38(9)：121-128.
ZHANG Side，HU Wei，WEI Zhinong，et al. Stochastic optimal power flow of integrated power and gas energy system based on chance-constrained programming[J]. Electric Power Automation Equipment，2018，38(9)：121-128.

[10] 刘涤尘，马恒瑞，王波，等. 含冷热电联供及储能的区域综合能源系统运行优化[J]. 电力系统自动化，2018，42(4)：113-120.
LIU Dichen，MA Hengrui，WANG Bo，et al. Operation optimization of regional integrated energy system with CCHP and energy storage system[J]. Automation of Electric Power Systems，2018，42(4)：113-120.

[11] 顾伟，陆帅，王珺，等. 多区域综合能源系统热网建模及系统运行优化[J]. 中国电机工程学报，2017，37(5)：1305-1315.
GU Wei，LU Shuai，WANG Jun，et al. Modeling of the heating network for multi-district integrated energy system and its operation optimization[J]. Proceedings of the CSEE，2017，37(5)：1305-1315.

[12] 卫志农，梅建春，孙国强，等. 电-气互联综合能源系统多时段暂态能量流仿真[J]. 电力自动化设备，2017，37(6)：41-47.
WEI Zhinong，MEI Jianchun，SUN Guoqiang，et al. Multi-period transient energy-flow simulation of integrated power and gas energy system[J]. Electric Power Automation Equipment，2017，37(6)：41-47.

[13] 李升，卫志农，孙国强，等. 大规模光伏发电并网系统电压稳定分岔研究[J]. 电力自动化设备，2016，36(1)：17-23.
LI Sheng，WEI Zhinong，SUN Guoqiang，et al. Voltage stability bifurcation of large-scale grid-connected PV system[J]. Electric Power Automation Equipment，2016，36(1)：17-23.

[14] 李宁. 北京市3E-S(能源-经济-环境、安全)系统MARKAL模型研究开发[D]. 北京：清华大学，2010.
LI Ning. Research on MARKAL model for Beijing 3E-S (Energy-Economy-Environment，Security) system[D]. Beijing：Tsinghua University，2010.

[15] 曾鸣，刘英新，周鹏程. 综合能源系统建模及效益评价体系综述与展望[J]. 电网技术，2018，42(6)：1697-1708.
ZENG Ming，LIU Yingxin，ZHOU Pengcheng. Review and prospects of integrated energy system modeling and benefit evaluation[J]. Power System Technology，2018，42(6)：1697-1708.

[16] 卫志农，陈妤，黄文进，等. 考虑条件风险价值的虚拟电厂多电源容量优化配置模型[J]. 电力系统自动化，2018，42(4)：39-46.
WEI Zhinong，CHEN Yu，HUANG Wenjin，et al. Optimal allocation model for multi-energy capacity of virtual power plant considering conditional value-at-risk[J]. Automation of Electric Power Systems，2018，42(4)：39-46.

[17] 陈凡，卫志农，黄正，等. 大电网可靠性评估状态分析实现方法的比较[J]. 电力系统及其自动化学报，2016，28(11)：82-87.
CHEN Fan，WEI Zhinong，HUANG Zheng，et al. Comparison of implementation methods for state analysis of bulk power system reliability[J]. Proceedings of the CSU-EPSA，2016，28(11)：82-87.

[18] 卫志农，张清松，赵静波，等. 电力系统线性化模型研究综述与改进[J]. 电网技术，2017，41(9)：2919-2927.
WEI Zhinong，ZHANG Qingsong，ZHAO Jingbo，et al. Review and improvement of power system linearization models[J]. Power System Technology，2017，41(9)：2919-2927.

[19] 王莹莹,梅生伟,刘锋. 混合电力系统合作博弈规划的分配策略研究[J]. 系统科学与数学,2012,32(4):418-428.
WANG Yingying,MEI Shengwei,LIU Feng. Imputation schemes for the cooper active game in the hybrid power system planning [J]. Journal of System Science and Mathematical Science Chinese Series,2012,32(4):418-428.
[20] 梅生伟,刘锋,魏韡. 工程博弈论基础及电力系统应用[M]. 北京:科学出版社,2016:235-467.
[21] 王元卓,林闯,程学旗,等. 基于随机博弈模型的网络攻防量化分析方法[J]. 计算机学报,2010,33(9):1748-1762.
WANG Yuanzhuo, LIN Chuang, CHENG Xueqi, et al. Quantitative analysis method of network attack and defense based on stochastic game model[J]. Chinese Journal of Computers, 2010, 33(9):1748-1762.
[22] 樊磊. 网络攻击威胁下电力系统脆弱性分析模型与方法[D]. 北京:华北电力大学,2015.
FAN Lei. Analysis of power system vulnerability under cyber attack threat[D]. Beijing:North China Electric Power University,2015.
[23] 程杉. 含分布式电源的配电网多目标优化问题研究[D]. 重庆:重庆大学,2013.
CHENG Shan. Study on multi-objective optimization of distribution network with distributed generation [D]. Chongqing: Chongqing University,2013.
[24] 赵轩才. 基于网络安全与服务质量的多目标模型优化研究[D]. 深圳:深圳大学,2015.
ZHAO Xuancai. Optimization research in a muti-objective model for integrating network security and quality of service[D]. Shenzhen:Shenzhen University,2015.
[25] YUAN W,ZHAO L,ZENG B. Optimal power grid protection through a defender-attacker-defender model[J]. Reliability Engineering & System Safety,2014,121:83-89.
[26] ZHAO L,ZENG B. Vulnerability analysis of power grids with line switching[J]. IEEE Transactions on Power Systems,2013, 28(3):2727-2736.
[27] 王玉龙. 一种新型的脆弱性评估方法及其在IMS中应用的研究[D]. 北京:北京邮电大学,2009.
WANG Yulong. A new vulnerability assessment method and its application in IMS[D]. Beijing:Beijing University of Post and Telecommunications,2009.

作者简介:


王 丹

王 丹(1982—),女,河北张家口人,高级工程师,博士研究生,主要研究方向为电力工程建造与管理(**E-mail**: 5591533@qq.com);

赵 平(1968—),女,陕西西安人,教授,博士研究生导师,主要研究方向为土木工程施工与管理、工程经济、建筑仿真与优化技术(**E-mail**:zhao_ping163@163.com);

臧宁宁(1985—),男,山东济宁人,高级工程师,博士,主要研究方向为综合能源系统优化运行、煤基分布式(**E-mail**: 125669144@qq.com)。

Security analysis and defense strategy of integrated energy system based on security game

WANG Dan[1,2],ZHAO Ping[1],ZANG Ningning[2],YAN Ying[3]

(1. School of Civil Engineering,Xi'an University of Architecture and Technology,Xi'an 710055,China;
2. China Datang Corporation Science and Technology Research Institute,Beijing 100040,China;
3. China Energy Engineering Group Shaanxi Electric Power Design Institute Co.,Ltd.,Xi'an 710054,China)

Abstract: Based on the security game theory, the critical factors that impact the safe operation of an integrated energy system are analyzed and identified. These critical factors, which represent the weak link of security defense, are employed to produce defense strategies and are given priority to be protected. A three-layer zero-sum master-slave game model, i.e. the defender-attacker-defender model is formulated for the integrated energy system. The attacker utilizes the weak link of the attack system as strategies to maximize system loss, while the defender develops protection strategies to enhance system security. An equilibrium solution of the game model that represents the best defense strategy is obtained to minimize the system loss. Numerical results on an integrated energy system indicate that the proposed strategy improves the system safety and reliability by giving priority of the protection system to the weak links. The present work, hence, contributes to analyzing the safety of integrated energy systems.

Key words: security game; integrated energy system; defense strategy; attack strategy; weak link