引用格式:栗会峰,李铁成,李均强,等.FDIA-蠕虫混合攻击下的配电网信息物理系统弹性拓扑优化配置[J].电力科学与技术学报,2024,39(4):20-32.
Citation: LI Huifeng,LI Tiecheng,LI Junqiang,et al.Resilient topology optimization on cyber-physical system of distribution networks under FDIA-Worm hybrid attacks[J]. Journal of Electric Power Science and Technology,2024,39(4):20-32.

FDIA-蠕虫混合攻击下的配电网信息物理系统弹性拓扑优化配置

栗会峰[1],李铁成[1],李均强[1],刘千贺[2],孔祥兴[2],卢志刚[2]
(1.国网河北省电力有限公司电力科学研究院,河北 石家庄 050021;2.燕山大学电气工程学院河北省电力电子节能与传动控制重点实验室,河北 秦皇岛 066004)

摘 要:电力安全是现代社会持续发展的重要保障。随着信息技术逐步发展,网络攻击手段的日渐增多和变强会对新型电力系统造成严重破坏,而合理的网络拓扑结构和有效的网络防御资源的是电力系统遭受网络攻击后负荷恢复的关键。为此,提出一种虚假数据注入(false data injection attack,FDIA)-蠕虫混合攻击下的配电网信息物理系统(cyber-physical systems,CPS)弹性拓扑优化和防御资源配置策略,用于提高配电系统网络攻击下的弹性。该模型采用上、中、下3层的框架对拓扑结构和防御资源进行优化:上层建立以规划成本和失负荷风险为目标的多目标帕累托规划模型,结合中层计及攻击与恢复的网络攻击传播模型,采用非支配排序遗传算法-II(non-dominated sorting genetic algorithm II,NSGA-II)进行规划方案求解;下层考虑信息层与物理层的多种耦合方案,基于配电网CPS弹性度量指标对拓扑优化配置进行评估。与传统的一对一串联模式方案相比,通过模型求解的3种耦合关系下的网络拓扑结构与防御资源优化方案,在提高系统弹性方面能够发挥重要作用。

关 键 词:弹性;配电网信息物理系统;网络拓扑优化;多目标帕累托规划;多阶段弹性度量指标
DOI:10.19781/j.issn.1673-9140.2024.04.003 **中图分类号**:TM863 **文章编号**:1673-9140(2024)04-0020-13

Resilient topology optimization on cyber-physical system of distribution networks under FDIA-Worm hybrid attacks

LI Huifeng[1], LI Tiecheng[1], LI Junqiang[1], LIU Qianhe[2], KONG Xiangxing[2], LU Zhigang[2]
(1.Electric Power Research Institute, Shijiazhuang, State Grid Hebei Electric Power Co., Ltd., Shijiazhuang 050021, China; 2. Key Lab of Power Electronics for Energy Conservation and Motor Drive of Hebei Province, Yanshan University, Qinhuangdao 066004, China)

Abstract: Power security is a crucial guarantee for the sustainable development of modern society. With the gradual development of information technology, the increasing number and strength of cyber attack methods can cause severe damage to new power systems. Reasonable network topology and effective network defense resources are key to load recovery after a power system suffers a cyber attack. Therefore, a strategy for resilient topology optimization and defense resource allocation of the cyber-physical system (CPS) of distribution networks under FDIA-Worm hybrid attacks is proposed to enhance the resilience of distribution systems against cyber attacks. This model adopts a three-tier framework of upper, middle, and lower levels to optimize the topology and defense resources: the upper level establishes a multi-objective Pareto planning model with planning costs and load loss risks as objectives, combines it with the middle-level network attack propagation model that considers attacks and recovery, and uses the non-dominated sorting genetic algorithm II (NSGA-II) to solve the planning scheme; the lower level considers various coupling schemes between the information layer and the physical layer, and evaluates the optimal topology

收稿日期:2022-11-25;**修回日期**:2023-12-29
基金项目:国网河北省电力有限公司科技项目(TSS2021-09)
通信作者:卢志刚(1963—),男,博士,教授,主要从事电力系统优化运行与控制的研究;E-mail:zhglu@ysu.edu.cn

configuration based on resilience metrics of the CPS of distribution networks. Compared with traditional one-to-one series mode schemes, the optimized network topology and defense resource schemes under the three coupling relationships obtained through model solution can play a significant role in enhancing system resilience.

Key words: resilience; cyber-physical system for distribution networks; network topology optimization; multi-objective Pareto programming; multi-stage resilience metrics

随着现代信息通信技术的深度发展与应用，在传统的电力系统理论基础上形成了电网信息物理系统（cyber-physical systems，CPS）[1]。先进的信息技术优化能源利用效率、提高可靠性和安全性的同时也带来了负面影响[2-3]。电力系统的运行将越来越依赖于信息系统，这种依赖会使电力系统在网络安全方面更加脆弱。当信息系统发生故障或遭受信息攻击时，会对信息物理系统的安全稳定运行造成极大的影响[4-5]。

近年来，CPS遭受网络攻击的事件频发，例如，2015年BlackEnergy恶意软件入侵电网数据采集与监视控制（supervisory control and data acquisition，SCADA）系统，致系统无法重启，乌克兰国家电网突发停电事故，致140万人口失去供电3～6 h[6]；2019年攻击方通过对委内瑞拉古里水电站和首都控制中心发动信息攻击，导致水电站机组和送出线设备跳闸，委内瑞拉发生全国18个州的电力大停电事故[7]。以上大停电事故表明，攻击者可以通过信息—物理跨空间风险传播机制对电力系统构成严重安全威胁。因此，为保障配电网CPS的安全稳定运行，研究以弹性最大化为目标的网络攻击下的电网CPS网络拓扑和防御资源优化，对保障电网CPS的安全运行具有重要意义。

对于弹性的研究，国内外学者在极端自然灾害背景下的研究较多。文献[8]首次对弹性电网及其恢复力的基本概念进行阐述；文献[9-11]对弹性电网的概念及关键特征进行了扩充；文献[12-14]针对电力系统弹性评估问题，分别提出了弹性三角形、弹性梯形和多维度弹性模型。国内外鲜有在FDIA-蠕虫混合攻击背景下进行电力通信网络弹性拓扑优化配置的研究。文献[15]给出了配电网CPS协同规划框架，详细地阐述了配电网规划、信息系统规划和配电自动化之间的协调关系。传统的电力通信网络规划方法主要关注经济投资、网络可靠性和安全要求[16-19]，却都没有考虑网络攻击的威胁。文献[20]提出将节点的拓扑均势差异缩小，以达到减少单个重要节点遭受攻击时带来的影响；文献[21]从信息传输可达性的角度研究兼顾正常运行水平和抵御网络攻击能力的电力通信网络拓扑规划问题。但都没有考虑到特定的网络攻击类型和电力通信网络与电网之间的耦合关系。

综上所述，相较CPS信息层随机故障，FDIA-蠕虫混合攻击模型造成信息层与物理层间的耦合故障更为严重，在此基础上的链路拓扑规划防御力更强。为避免信息层链路冗余，计及攻击与恢复的网络攻击传播模型将信息节点恢复过程纳入进来，保证了方案经济性。

在以往文献的基础上，本文开展FDIA-蠕虫混合攻击下的配电网CPS弹性拓扑优化配置的研究。首先对配电网信息物理系统建模；然后建立以规划成本和失负荷风险为目标的多目标帕累托规划模型，采用非支配排序遗传算法-II（non-dominated sorting genetic algorithm II，NSGA-II）进行求解；最后，采用改进的IEEE 33节点算例对3种耦合关系下的拓扑与防御资源优化方案的弹性进行计算对比，验证本文规划模型的弹性提升效果。

1　配电网信息物理系统建模

1.1　配电网信息物理系统的定义

配电网CPS是在传统的配电网基础上融入先进的信息与通信技术后发展而来的。在各种信息设备和终端设备间，配电网CPS可以进行实时高效的数据传输，弥补了传统配电网在信息侧决策分析、应对网络攻击、防护自愈和故障预警方面的不足。

1.2　配电网信息物理系统的建模

如图1所示，配电网CPS模型主要由信息层（决策分析、通信网络和二次设备层）、物理层组成，表示为$G=(V,E)$，其中$V=\{V_c,V_p\}$表示信息层和物理层中所有节点的集合，$E=\{E_c,E_p\}$表示为信息层和物理层中各个节点间的通信链路与电网线路的集合。由复杂网络理论可知，G中的各条边为无向边，可由邻接矩阵A表示配电网CPS中各节点的连接关系：

$$A=\begin{bmatrix} C_{m\times m} & I_{m\times n} \\ D_{n\times m} & P_{n\times n} \end{bmatrix} \tag{1}$$

式中，A为$m+n$阶的矩阵，m、n分别为信息层、物理层的节点数目；$C_{m\times m}$、$P_{n\times n}$分别为信息层和物理层的连接矩阵，表示各层内部的连接关系；$I_{m\times n}$、$D_{n\times m}$为信息层和物理层间的耦合连接矩阵，$I_{m\times n}$主要表示数据采集和指令下达链路，$D_{n\times m}$主要表示信息节点的供能路径。$A(i,j)=1$表示节点(i,j)存在连接边；$A(i,j)=0$表示节点(i,j)不存在连接边。

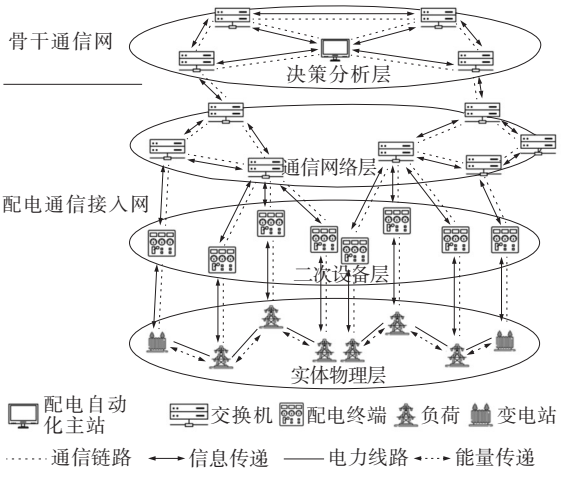


图1 配电网CPS架构

Figure 1 CPS architecture of distribution network

2 基于NSGA-II算法的多目标帕累托规划模型

首先，建立考虑信息节点入侵和恢复的网络病毒传播模型，对配电网CPS遭受网络攻击后的病毒传播及恢复进行模拟，得出不同配电网CPS网络拓扑下的物理节点失负荷风险；然后，建立以规划成本（拓扑和防御资源成本）和失负荷风险为目标的帕累托规划模型，使用NSGA-Ⅱ算法生成配电网CPS网络拓扑与防御资源分配优化方案。

2.1 考虑信息节点入侵和恢复的网络病毒传播模型

本文将网络攻击考虑为蠕虫病毒传播与虚假数据注入攻击组合的形式，如图2所示。

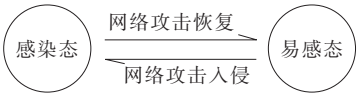


图2 信息节点状态转换

Figure 2 State transitions for information nodes

信息节点的运行状态分为2类：

$$S(i,t)=\begin{cases}0, \text{第}i\text{个节点处于易感态}\\1, \text{第}i\text{个节点处于感染态}\end{cases} \tag{2}$$

前一时刻被蠕虫病毒成功入侵的信息节点（感染态信息节点）会通过节点间的通信链路以一定的传播概率入侵相邻的其他信息节点（易感态信息节点），造成下一时刻相邻节点被蠕虫病毒入侵，进而引发节点的运行状态发生变化。考虑各个信息节点部署的防御资源影响，感染态的信息节点会经过一段时间的打补丁修复操作后，恢复为易感态的运行状态。

2.1.1 信息节点的入侵概率

令X_i为第i个信息节点的网络攻击难度，其值不仅与第i个信息节点的漏洞固有特性相关，还与其相邻已被成功入侵的节点数目有关。第i个信息节点的网络攻击难度为

$$X_i=X_i^1\cdot X_i^2 \tag{3}$$

其中，X_i^1为与漏洞特性相关的攻击难度。参考国家漏洞数据库（national vulnerability database，NVD）提供的通用漏洞评分系统（common vulnerability scoring system，CVSS），对X_i^1进行评估，计算公式为

$$X_i^1=\omega_1V_i+\omega_2C_i+\omega_3U_i \tag{4}$$

其中，V_i、C_i、U_i分别为第i个信息节点的漏洞固有特性，分别为攻击途径、攻击复杂度和认证次数，表征了漏洞评分的静态分数值。使用熵权法计算得到$\omega_1\sim\omega_3$，$\omega=[0.402\,1\quad 0.301\,5\quad 0.296\,4]$。

考虑蠕虫病毒的传播方式为被感染的信息节点通过端口扫描的方式向邻近的信息节点设备渗透。设置参数X_i^2为与第i个信息节点相邻已被成功入侵的节点数目相关的攻击难度，计算公式为

$$X_i^2=\frac{3}{1+\exp\{-1.5-\log_2[0.4(M_{i,t}+1)]\}} \tag{5}$$

式中，$M_{i,t}$为t时刻第i个信息节点的临近节点中被成功入侵的数目。

令$\mu_{i,j}$为第i个信息节点向第j个信息节点发起网络攻击的概率，前提条件是i、j之间存在通信链路。相应的计算公式为

$$\mu_{i,j}=X_j\Big/\sum_{k\in N_i}X_k \tag{6}$$

式中，N_i表示与第i个信息节点相连的信息节点集。

$t+1$时刻第i个信息节点攻击第j个信息节点的概率为

$$\chi_{i,j}(t+1)=S(i,t)\cdot\mu_{i,j} \tag{7}$$

$t+1$时刻第j个信息节点被选为攻击目标的概率为

$$\chi_j(t+1)=1-\prod_{i\in N_j}\big(1-\chi_{i,j}(t+1)\big) \tag{8}$$

t时刻第j个信息节点若已被入侵，则无法在$t+$

1时刻再次被入侵。因此，第j个信息节点在$t+1$时刻被入侵成功的概率为

$$\mathrm{Pr}_j(t+1)=X_j\cdot\chi_j(t+1)\cdot\big(1-S(j,t)\big) \quad (9)$$

2.1.2　信息节点网络攻击修复时间模型

为了刻画防御资源的作用效果（剔除信息节点中的网络病毒），本文提出信息节点网络攻击修复时间模型。令λ_i为信息节点i的攻击修复时间参数，其值与第i个信息节点部署的防御资源特性相关。具体计算公式为

$$\lambda_i(j)=W_1L_j+W_2E_j+W_3R_j \quad (10)$$

式中，$\lambda_i(j)$为第i个信息节点部署防御资源R_j后产生的攻击修复时间参数；L_j、E_j、R_j为防御资源R_j的固有特性，分别为漏洞补丁修复等级、漏洞渗透代码可利用性、漏洞报告可信度。使用熵权法计算得到$W_1\sim W_3$，$W=[0.3172\quad 0.3172\quad 0.3656]$。

在配电网CPS的信息节点遭受网络攻击后，考虑各个信息节点配置的防御资源不同和临近入侵节点数的不同，则各个信息节点的修复时间也为非确定值。

文献[22]采用指数Weibull分布作为修复时间模型，具体定义为

$$F(\Omega,k_\mathrm{r},\lambda_\mathrm{r},\alpha_\mathrm{r})=\{1-\exp[-(\Omega/\lambda_\mathrm{r})^{k_\mathrm{r}}]\}^{\alpha_\mathrm{r}},\ t>0 \quad (11)$$

式中，k_r、λ_r、α_r为修复过程中使用的参数。

为简化计算，网络攻击情况下的修复时间看作与网络攻击强度k_w相关的值，具体计算公式为

$$\begin{cases} T_{i,t}=k_\mathrm{w}[1-F(\Omega_i,k_\mathrm{r},\lambda_\mathrm{r},\alpha_\mathrm{r})]\cdot f_\mathrm{kw}(M_{i,t})\cdot S(i,t),\ t=1 \\ T_{i,t}=k_\mathrm{w}[1-F(\Omega_i,k_\mathrm{r},\lambda_\mathrm{r},\alpha_\mathrm{r})]\cdot f_\mathrm{kw}(M_{i,t})\cdot[S(i,t)-S(i,t-1)],\ t>1 \\ f_\mathrm{kw}(M_{i,t})=1.5+\dfrac{1}{1+\exp\{2-\log_2[0.4(M_{i,t}+1)]\}} \\ \Omega_i=\dfrac{1}{k_\mathrm{w}}\cdot\sum_{j=1}^{3}k_i(j)\cdot\lambda_i(j) \\ T_{i,t}\geqslant 0 \end{cases} \quad (12)$$

式中，$T_{i,t}$为第i个节点t时刻被入侵后计算得到的修复时间；$f_\mathrm{kw}(M_{i,t})$为t时刻受相邻被入侵节点数$M_{i,t}$影响的修复时间加成函数；网络攻击强度k_w取值为3；Ω_i为第i个节点部署的全部防御资源量总和；$k_i(j)$为0-1变量，表示在第i个节点是否部署防御资源R_j，为1时表示部署。

本文仅考虑对配电通信接入网进行网络拓扑和防御资源的优化，并且防御资源仅对已被病毒入侵的信息节点起到攻击修复的作用，与病毒入侵概率无关。

2.1.3　蠕虫病毒攻击传播模型框架

蠕虫病毒攻击传播模型框架如图3所示，具体步骤如下：

1）初始化，即①生成信息层连接矩阵；②输入各信息节点漏洞信息与防御资源部署信息；③确定初始被入侵节点；

2）初始时刻$t=t_0$，令$S(i,t_0)=1$，计算$M_{i,t}$；

3）输出被入侵的节点，确定各节点的邻近节点状态；

4）计算下一时刻各个信息节点成功入侵概率，计算已被入侵节点的修复时间；

5）$t=t+1$，判断t是否大于24，若判断为否则进入步骤6），否则进入步骤8）；

6）判断被入侵的信息节点中是否有被修复的节点，若存在则更新对应信息节点状态，否则不发生变化；

7）将各个信息节点的成功入侵概率与攻击成本概率相比，得出被入侵节点，更新信息节点状态，返回步骤3）；

8）输出各时刻信息节点状态。

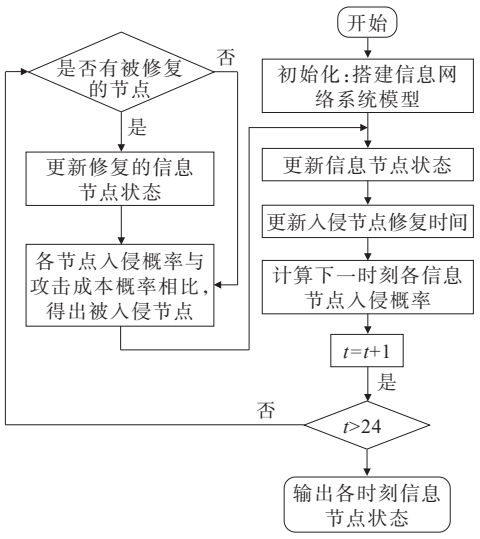


图3　配电网CPS蠕虫病毒传播模型框架

Figure 3　Framework of CPS worm propagation model

2.2　多目标帕累托规划模型目标函数

建立以规划成本（拓扑成本、防御资源成本）和失负荷风险最小化为目标的帕累托规划模型。

2.2.1 最小化拓扑成本

以太网可以采用多种连接介质，包括同轴缆、双绞线和光纤等，其中双绞线多用于从主机到集线器或交换机的连接，而光纤则主要用于交换机间的级联和交换机到配电子站交换机间的点到点链路上；同轴缆作为早期的主要连接介质已经逐渐趋于淘汰。

$$\min f_1(x)=\sum_{i,j\in V_c,i\neq j} C_{\text{line}}^{k}\cdot l_{ij} \tag{13}$$

式中，C_{line}^{1}、C_{line}^{2}分别为双绞线、光纤价格（如表1所示）；l_{ij}为第i、j个信息节点之间的通信链路长度，由各信息节点的地理位置所决定。

表1 不同通信链路介质价格

Table 1 Price of different communication link media

介质	价格/(元·m^{-1})	介质	价格/(元·m^{-1})
C_{line}^{1}	4.5	C_{line}^{2}	6.0

假设各个相邻的物理节点间距离为100 m。配电终端地理位置为物理层的各个节点位置，配电子站交换机节点位于物理层的变电站节点，而交换机节点的位置由其供能节点（文献[23]表A2～A4中的第1个节点）位置决定。因此，相邻第i、j个信息节点之间的通信链路长度为与其相连的物理节点间的最短路径，数值由Dijkstra算法求得。

2.2.2 最小化防御资源成本

最小化防御资源成本为

$$\begin{cases}\min f_2(x)=\sum\limits_{i\in V_c,j\in\{1,2,3\}} C_{\text{def}}^{j}\cdot k_i(j)\\ C_{\text{def}}^{j}=C_{\text{def\_con}}^{j}+24C_{\text{def}}^{j}\end{cases} \tag{14}$$

式中，C_{def}^{j}为防御资源R_j的总成本；$C_{\text{def\_con}}^{j}$、$C_{\text{def_run}}^{j}$分别为防御资源R_j的建造成本（造价价格）和运行成本。各种防御资源价格[24]如表2所示。

表2 各种防御资源价格

Table 2 Price of various defense resources

R_j	造价价格/元	运行成本/(元·h^{-1})
1	479.04	134.13
2	239.52	143.71
3	958.08	86.23

考虑各种防御资源的运行成本较为固定且基本不受外界因素干扰，本文选取防御资源的单位日运行成本（1 d即24 h运行成本之和）作为防御资源总运行成本的代表。

2.2.3 最小化失负荷风险

考虑受网络攻击影响的信息节点会遭受虚假数据注入攻击的影响，采集错误的数据，进而影响信息层的正确指令下达，引发物理层的节点为维持系统的安全进行紧急切负荷控制。因此，结合信息节点网络病毒传播模型，对于各个时刻受到网络攻击影响的配电终端，将其所控制的物理层负荷按照等级进行加权求和，作为失负荷风险目标函数进行优化。

$$\min f_3(x)=\sum_{i\in V_p,t=\{1,2,\cdots,24\}} \omega_i\cdot P(i,t)\cdot S(i,t) \tag{15}$$

式中，ω_i为各节点负荷权重值；$P(i,t)$为第i个节点t时刻的有功负荷。

2.3 多目标帕累托规划模型约束条件

多目标帕累托规划模型是对配电网CPS的信息层网络拓扑结构和防御资源分配进行优化。因此，需要考虑配电通信接入网中各种信息设备的连接关系，即配电网CPS信息层连接矩阵的连通性、成本和分组约束等。配电网CPS信息层连接矩阵如图4所示。

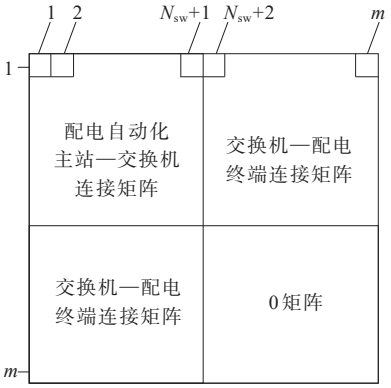


图4 配电网CPS信息层连接矩阵

Figure 4 Connection matrix of CPS information layers

2.3.1 连通性约束

配电子站交换机与交换机的通信链路呈星型，保证了配电监测子站与各交换机之间的通信连接。

$$H(i)\geqslant 1,i\in V_c \tag{16}$$

式中，$H(i)$为各交换机节点的通信连接标志位，其大小由深度优先搜索算法得出。

2.3.2 成本约束

成本约束条件为

$$0\leqslant \sum_{\substack{i,j\in V_c,i\neq j\\ A(i,j)=1,k\in\{1,2\}}} C_{\text{line}}^{k}\cdot l_{ij}+\sum_{i\in V_c,j\in\{1,2,3\}} C_{\text{def}}^{j}\cdot k_i(j)\leqslant C_{\text{T}} \tag{17}$$

式中，C_{T}为成本约束的上限。

2.3.3　分组约束

交换机与配电终端呈一对多的关系，即一台交换机可连接多台配电终端且一台配电终端仅与一台交换机相连，分组约束条件为

$$0\leqslant\sum_{i=2}^{m}A(i,j)\leqslant 1,j=N_{\mathrm{sw}}+2,\cdots,m \quad (18)$$

2.3.4　防御资源约束

每个信息节点至少部署一种防御资源，防御资源约束条件为

$$\sum_{i\in V_c,j\in\{1,2,3\}}k_i(j)\geqslant 1 \quad (19)$$

2.4　基于 NSGA-II 的多目标帕累托规划模型求解

2.4.1　基于帕累托最优的多目标规划

帕累托最优体现了各个子目标问题解不能够再继续同时优化的状态。达到帕累托最优的解称为问题的非劣解，所有非劣解可构成问题解的帕累托前沿，帕累托前沿中的解均是多目标规划的可行解，但还需根据一定的偏好和原则对这些可行解进行筛选排序，进而确定最优方案。

2.4.2　非支配排序遗传算法

本文采用文献[25-27]中的 NSGA-II 对多目标优化问题进行求解。NSGA-Ⅱ算法流程如图 5 所示。

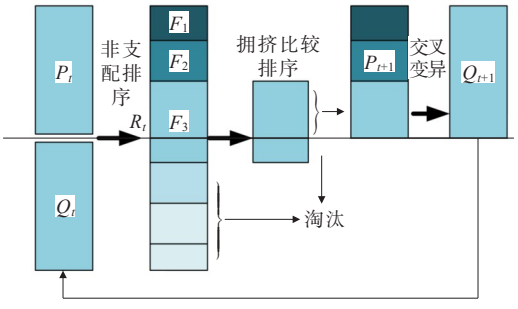


图 5　NSGA-Ⅱ算法流程

Figure 5　Flow chart of NSGA－Ⅱ algorithm

两段式自交叉变异指的是，分别对配电自动化主站—交换机连接矩阵、各信息节点防御资源分配矩阵进行自交叉变异操作。自适应指的是，在迭代过程中对交叉变异概率进行调整，使得交叉变异过程满足在前期扩大全局搜索的能力，后期专注局部搜索的能力，最终达到快速收敛的目的。拓扑矩阵的结构存在对称的特性，所以与传统的遗传算法不同，在自适应两段式自交叉变异遗传算法中，种群中的每个个体会与自身进行交叉变异。

3　弹性度量模型

弹性电力系统可以有效地应对人为极端外力破坏或通过信息攻击手段引发电网大面积停电事故，在无法避免的故障时，强调保证关键负荷的供给，并能迅速、高效恢复系统性能。

3.1　多阶段耦合弹性度量指标

为了对规划方案的弹性进行更加全面准确的度量，提出并使用多阶段耦合弹性度量指标。信息侧的弹性指标主要体现网络攻击（蠕虫病毒攻击）的入侵和恢复，物理侧的弹性指标体现网络攻击（虚假数据注入攻击）引发的负荷切除和恢复。

3.1.1　物理侧弹性度量指标

电力系统的基本要求之一是保证持续可靠的供电，因此，采用负荷类指标作为评估电力系统物理侧弹性水平的主要依据。物理侧选取的弹性度量指标有失负荷速率、系统适应率及负荷恢复速率，分别为

$$R_{\text{p-los}}=\frac{\sum_{i=1}^{N_{\mathrm{p}}}P_0(i,T_2)-\sum_{i=1}^{N_{\mathrm{p}}}P_1(i,T_2)}{\sum_{i=1}^{N_{\mathrm{p}}}P_0(i,T_2)\cdot(T_2-T_1)} \quad (20)$$

$$R_{\text{p-fit}}=\frac{\sum_{t=T_2}^{T_3}\sum_{i=1}^{N_{\mathrm{p}}}P_1(i,t)}{\sum_{t=T_2}^{T_3}\sum_{i=1}^{N_{\mathrm{p}}}P_0(i,t)} \quad (21)$$

$$R_{\text{p-rec}}=\frac{\sum_{i=1}^{N_{\mathrm{p}}}P_1(i,T_4)-\sum_{i=1}^{N_{\mathrm{p}}}P_1(i,T_2)}{\sum_{i=1}^{N_{\mathrm{p}}}P_0(i,T_4)\cdot(T_4-T_2)} \quad (22)$$

式(20)～(22)中，N_{p}为物理层节点总数；$P_0(i,t)$、$P_1(i,t)$分别为t时刻正常、网络攻击状态下系统向物理层第i个节点提供的有功值；T_1为网络攻击入侵开始时刻；T_2为网络攻击入侵影响最严重时刻；T_3为网络攻击结束时刻；T_4为弹性恢复结束时刻。

3.1.2　信息侧弹性度量指标

本文从网络弹性的定义出发，将信息节点正确处理业务的能力作为评估电力系统信息侧弹性水平的主要依据。类比物理侧弹性度量指标，得出信息侧弹性度量指标有信息失准速率、信息适应率及信息恢复速率，分别为

$$R_{\text{c-los}}=\frac{1-\dfrac{N_1(T_2)}{N_0(T_2)}}{T_2-T_1} \quad (23)$$

$$R_{\text{c-fit}}=\frac{\sum_{t=T_2}^{T_3}N_1(t)}{\sum_{t=T_2}^{T_3}N_0(t)} \tag{24}$$

$$R_{\text{c-rec}}=\frac{\dfrac{N_1(T_4)}{N_0(T_4)}-\dfrac{N_1(T_2)}{N_0(T_2)}}{T_4-T_2} \tag{25}$$

式(23)～(25)中,$N_0(t)$、$N_1(t)$分别为t时刻正常、网络攻击状态下信息层未被入侵节点数。

3.1.3 综合弹性度量指标

综合弹性度量指标综合了物理侧负荷弹性和信息侧信息准确率弹性指标,对系统弹性的刻画更为准确,其计算式为

$$R=\alpha_1R_{\text{p-los}}R_{\text{c-los}}+\alpha_2R_{\text{p-fit}}R_{\text{c-fit}}+\alpha_3R_{\text{p-rec}}R_{\text{c-rec}} \tag{26}$$

其中,α_i为各阶段指标权重值。为平均考虑各阶段的影响,本文中各阶段指标权重值分别取1/3、1/3、1/3,后续可结合实际需要修改其所占权重比例。

3.2 考虑信息节点失效的规划方案评价

3.2.1 信息节点供能约束

文献[28]中定义了耦合程度系数,其具体的供能关系为

$$S_{\text{sup}}(i,t)=\begin{cases}0, D_i<\alpha D_i'\\ 1, D_i\geqslant\alpha D_i'\end{cases} \tag{27}$$

其中,$S_{\text{sup}}(i,t)$为t时刻第i个节点的供能状况,1表示正常供能;D_i、D_i'分别为第i个节点当前时刻的实际和正常负荷功率;$\alpha(0\leqslant\alpha\leqslant1)$为供能系数,体现了信息层与物理层之间的耦合关系。

3.2.2 失效信息节点信息采集与控制约束

当第i个信息节点因供能不足而失效时,将退出运行并无法接受调度中心下达的指令和传递信息。具体调度中心的控制指令生成模型和紧急切负荷控制模型均采用传统二阶锥规划[29]模型。失效信息节点信息采集与控制约束为

$$P_{\text{inj}}(i,t)\in\begin{cases}\left[P_{\text{inj}}^{\min}(i),P_{\text{inj}}^{\max}(i)\right], & S_{\text{sup}}(i,t)=1\\ P_{\text{inj}}(i,t'), & S_{\text{sup}}(i,t')=0\\ t'\leqslant t\end{cases} \tag{28}$$

$$Q_{\text{inj}}(i,t)\in\begin{cases}\left[Q_{\text{inj}}^{\min}(i),Q_{\text{inj}}^{\max}(i)\right], & S_{\text{sup}}(i,t)=1\\ Q_{\text{inj}}(i,t'), & S_{\text{sup}}(i,t')=0\\ t'\leqslant t\end{cases} \tag{29}$$

式中,P_{inj}、Q_{inj}分别为信息节点采集到的有功、无功量测值;t'为信息节点失效时刻。

3.2.3 连通性约束

连通性约束条件为

$$S_{\text{con}}(i,t)=\begin{cases}0, H(i)\geqslant1\\ 1, H(i)=0\end{cases} \tag{30}$$

其中,$S_{\text{con}}(i,t)$为t时刻第i个节点的连通状况,当t时刻第i个节点的通信连接标志位$H(i)=0$时,代表第i个信息节点与调度中心失去连接。失去连接的信息节点都归为失效节点,其影响效果与失去供能的失效节点相同。

3.2.4 考虑信息节点失效的规划方案评价流程

考虑信息节点失效的规划方案评价流程如图6所示,其基本步骤如下:

1)搭建电力信息物理系统模型,输入多目标帕累托规划模型的解,设置初始网络攻击时刻;

2)确定节点入侵状态,对入侵的信息节点当前时刻量测值进行虚假数据注入攻击;

3)各节点量测值通过信息链路输入配电自动化主站信息节点,通过二阶锥规划模型得出各节点控制指令(有载调压器挡位、储能装置输入输出功率和燃气轮机输出值);

4)控制指令通过信息链路下达给电力系统的各节点,为保证潮流约束和系统的安全运行,进行负荷削减的系统紧急控制;

5)对于因供能不足或与配电自动化主站失去联系的信息节点,更新整体的信息连接拓扑;

6)根据改进的网络病毒传播模型得出下一时刻各节点入侵状态;

7)重复步骤2)～6),直至网络攻击结束;

8)使用多阶段弹性度量指标对规划方案进行弹性计算。

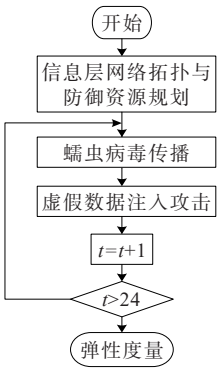


图6 规划方案评价流程

Figure 6 Evaluation flow chart of planning scheme

4 算例分析

4.1 算例参数

配电网CPS的物理侧采用IEEE 33节点标准

模型考虑多微网接入的形式，节点电压限制为电压等级的0.95～1.05倍。假设所有微电网拓扑结构相同，包括1台微型燃气轮机、1个光伏电站和1个能量储存系统(energy storage system，ESS)，其功率分别为250、50、5 kW，ESS的容量设置为250 kW·h。所有设备均简化为连接在1条母线上，负荷重要程度划分如图7所示。

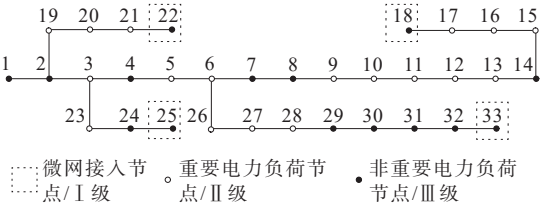


图7　负荷重要程度划分

Figure 7　Load importance division

按照负荷的类型和大小分为3类节点，如表3所示，第Ⅲ类节点所连负荷较大，权重较小。在遭受网络攻击时，系统为保证安全运行会优先切除所连负荷较大的节点，保证所连负荷较小的节点不会因供能不足而过快地造成信息节点失效。考虑各时刻各节点的负荷需求不同，各节点的有功、无功负荷变化曲线及详细物理侧参数详见文献[23]。

表3　节点重要程度划分

Table 3　Node importance division

重要程度	节点负荷权重值	节点序号
Ⅰ	1.5	18、22、25、33
Ⅱ	1.0	3、5、6、9、10、11、12、13、15、16、17、19、20、21、23、26、27、28
Ⅲ	0.5	2、4、7、8、14、24、29、30、31、32

4.2　算例分析

本文主要工作是对配电通信接入网进行网络拓扑和防御资源的优化。考虑信息层与物理层之间的耦合关系并非为简单的一对一关系，而是一对多的关系，因此，首先给出3种耦合关系下的拓扑与防御资源优化方案，即①4/5个配电终端为一组的网络拓扑和防御资源的优化；②3/4个配电终端为一组的网络拓扑和防御资源的优化；③2/3个配电终端为一组的网络拓扑和防御资源的优化。然后与传统的一对一串联模式下的方案进行弹性度量比较，选取弹性最好的方案作为最优方案，同时验证本文规划模型的解在弹性度量指标上的优势。

4.2.1　3种耦合关系下的拓扑与防御资源优化方案

为简化算法的计算，本文未考虑对配电终端的分组进行求解，采用就近分组的形式进行固定分组，各方案的固定分组详见文献[23]。3种方案最优解集多目标函数值分布如图8所示。

对于多目标规划模型帕累托前沿中的解，采用文献[30-32]中熵加权优劣解距离法(technique for order preference by similarity to ideal solution，TOPSIS)，得出前沿中的最优解。各方案中最优方案的防御资源分配如表4所示；各方案中最优方案的拓扑连接分别如图9所示，其中，D为配电子站交换机节点；C为交换机节点；P为配电终端节点。

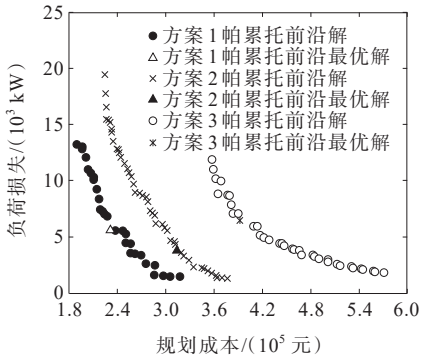


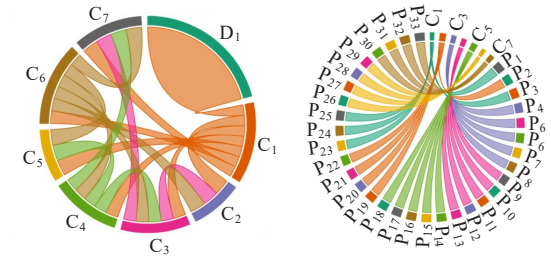
图8　3种方案最优解集多目标函数值分布

Figure 8　Multi-objective function value distribution of optimal solution set under three schemes

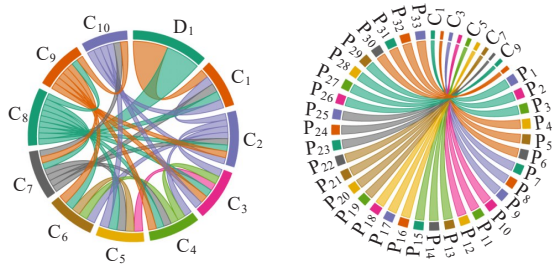
表4　各方案最优方案的防御资源分配

Table 4　Defense resource allocation of each optimal scheme

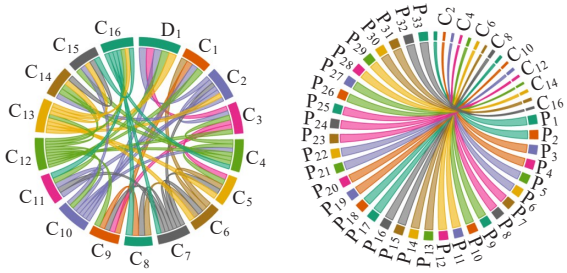
方案	防御资源	信息节点序号
1	1	D_1、C_1、C_7、P_2、P_{14}、P_{18}、P_{22}、P_{24}、P_{30}、P_{31}、P_{33}
	2	C_3、P_1、P_2、P_3、P_5、P_7、P_9、P_{15}、P_{19}、P_{20}、P_{27}、P_{28}、P_{29}
	3	C_2、C_4、C_5、C_6、C_7、P_4、P_6、P_8、P_{10}、P_{11}、P_{12}、P_{13}、P_{16}、P_{17}、P_{21}、P_{23}、P_{25}、P_{26}、P_{32}
2	1	D_1、C_1、C_2、C_4、C_6、C_9、P_5、P_7、P_8、P_{10}、P_{12}、P_{17}、P_{25}、P_{27}、P_{28}、P_{30}、P_{32}、P_{33}
	2	D_1、C_5、C_8、C_{10}、P_1、P_3、P_9、P_{11}、P_{14}、P_{18}、P_{19}、P_{21}、P_{24}
	3	C_3、C_7、P_1、P_2、P_4、P_5、P_6、P_8、P_{12}、P_{13}、P_{15}、P_{16}、P_{17}、P_{20}、P_{22}、P_{23}、P_{25}、P_{26}、P_{29}、P_{31}、P_{32}
3	1	D_1、C_3、C_4、C_6、C_{10}、C_{14}、C_{15}、P_4、P_7、P_8、P_{12}、P_{13}、P_{17}、P_{19}、P_{20}、P_{21}、P_{22}、P_{23}、P_{24}、P_{26}、P_{30}、P_{31}
	2	C_2、C_{11}、C_{13}、C_{16}、P_1、P_3、P_{11}、P_{14}、P_{15}、P_{16}、P_{18}、P_{25}、P_{27}、P_{28}、P_{29}、P_{30}、P_{32}
	3	C_1、C_4、C_5、C_7、C_8、C_9、C_{12}、C_{13}、P_2、P_3、P_5、P_6、P_8、P_9、P_{10}、P_{12}、P_{19}、P_{21}、P_{25}、P_{27}、P_{28}、P_{33}



(a) 方案1



(b) 方案2



(c) 方案3

图9 各方案下最优方案的拓扑连接

Figure 9 Topological connection of the optimal scheme under each scheme

4.2.2 与传统拓扑方案对比

工业以太网常用的拓扑结构为单环拓扑结构，如图10所示。各个交换机之间依此相连，各条支路的头尾交换机接入上级交换机并形成环状结构。环上各节点的工业以太网交换机位于各个终端上，并通过以太网接口和配电终端连接。上级节点的工业以太网交换机(配电子站交换机)一般配置在变电站内，负责收集环上所有通信终端的业务数据，并接入骨干层通信网络。

考虑配电终端与外界接触的概率最大，初始入侵节点选取为多个配电终端节点；同时，为了对网络攻击时各规划方案进行准确的弹性度量，选取方案1各个配电终端分组中的第1个节点作为入侵节点，即配电终端节点P_1、P_2、P_4、P_9、P_{14}、P_{26}、P_{30}。网络攻击下各方案的总负荷曲线(百分值)如图11所示。

网络攻击具有蓄意性且网络攻击资源有限，因此在有限的时间和资源的限制下，造成更多的失负荷是网络攻击的首要目标。选取10:00为网络攻击

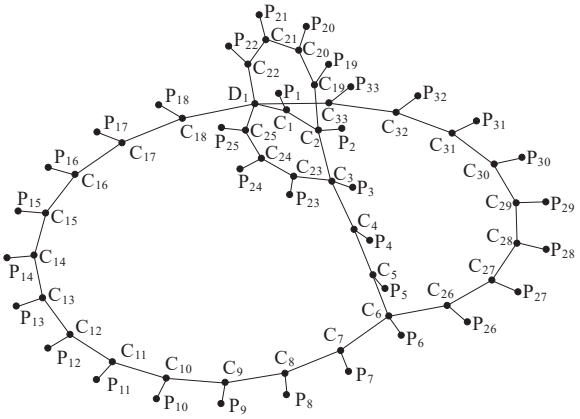


图10 传统拓扑方案的拓扑连接

Figure 10 Topological connection diagram of traditional topology scheme

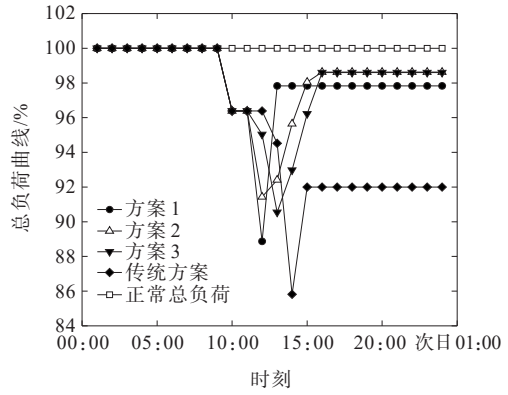


图11 网络攻击下各方案的总负荷曲线(百分值)

Figure 11 Total load curve of each scheme under network attack (percentage value)

初始时刻，各规划方案相关参数如表5～8所示。

表5 各规划方案目标函数

Table 5 Objective function of each planning scheme

方案	拓扑成本/元	防御资源成本/元	失负荷风险/kW
1	85 500.0	146 155.4	5 598.0
2	136 350.0	178 097.8	3 791.3
3	182 100.0	210 672.2	6 507.8
传统	43 200.0	376 199.0	710 24.9

表6 各规划方案物理侧弹性度量指标

Table 6 Physical side elasticity measurement index of each planning scheme

方案	$R_{\text{p-los}}$	$R_{\text{p-fit}}$	$R_{\text{p-rec}}$
1	0.055 6	0.971 4	0.089 6
2	0.042 9	0.973 2	0.017 9
3	0.031 5	0.972 6	0.026 9
传统	0.035 4	0.914 4	0.061 8

表 7　各规划方案信息侧弹性度量指标

Table 7　Measurement index of elasticity on the information side of each planning scheme

方案	$R_{\text{c-los}}$	$R_{\text{c-fit}}$	$R_{\text{c-rec}}$
1	0.414 6	0.609 8	0.048 8
2	0.250 0	0.649 6	0.090 9
3	0.215 0	0.538 2	0.120 0
传统	0.197 0	0.137 3	0.031 9

表 8　各规划方案综合弹性度量指标

Table 8　Comprehensive elasticity measurement index of each planning scheme

方案	R	方案	R
1	0.191	3	0.173
2	0.208	传统	0.040

由表 5～8 的数据可知，各方案在弹性性能方面的排序为方案 2、1、3、传统方案。因此，方案 2 中使用的 3/4 个配电终端为一组的网络拓扑结构在网络攻击下表现得最为优异。在前期的投资建设（拓扑与防御资源成本之和）中方案 2 比传统方案少 104 951.2 元。在失负荷风险的表现上传统方案是方案 2 的 18.73 倍。对于 10 kV 等级的配电接入网而言，所带负荷多为工厂用电，大范围的失负荷会对国民经济和安全造成严重影响，所以方案 2 的拓扑和防御资源优化方案相比于传统方案更好。各规划方案信息节点失效情况如表 9 所示。

表 9　各规划方案信息节点失效情况

Table 9　Failure of information nodes in each planning scheme

方案	信息节点失效数目/个	失效节点
1	3	P_7、P_8、P_{24}
2	1	P_{24}
3	1	P_{24}
传统	28	C_1、C_2、C_3、C_4、C_5、C_6、C_7、C_8、C_9、C_{10}、C_{11}、C_{12}、C_{13}、C_{23}、P_1、P_2、P_3、P_4、P_5、P_6、P_7、P_8、P_9、P_{10}、P_{11}、P_{12}、P_{13}、P_{23}

对比 4 种方案的拓扑连接图可知，在网络攻击背景下，网状的拓扑结构相比于传统的单环拓扑结构，在弹性性能上的表现更好。主要原因是，在传统的单环拓扑结构中，网络攻击会导致很多上游交换机信息节点由于供能不足而失效，下游交换机因此失去与调度中心之间的信息传输，使得调度中心的控制指令无法下达，进而扩大了网络攻击的影响范围。虽然网状的拓扑结构会很大程度上改善下游交换机失去与调度中心联系的情况，但各方案的拓扑平均度会随着信息节点数目的增多而变大，即各节点的关联程度逐渐加强。网络节点数目与弹性的 3 种指标间有不同的关联关系。各方案网络拓扑平均度如图 12 所示。

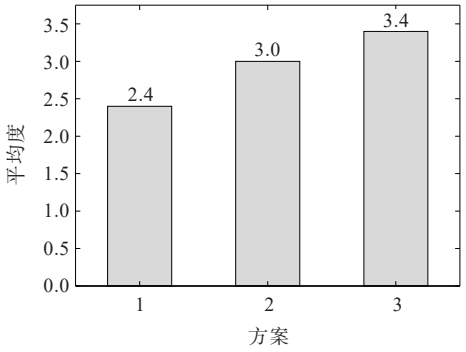


图 12　各方案网络拓扑平均度

Figure 12　Average degree of network topology for each scheme

对于失负荷失准速率（$R_{\text{p-los}}$）和信息失准速率（$R_{\text{c-los}}$），此类弹性指标数值越小弹性性能越好。数值上方案 1、2、3 依次呈下降趋势，体现出不同的分组情况和该 2 组指标间呈现较强的相关性。当单个交换机所连配电终端数量越多时，在网络攻击初期的传播速度也是最快的；相反，所连配电终端数量越少时，传播速度也相对较慢。

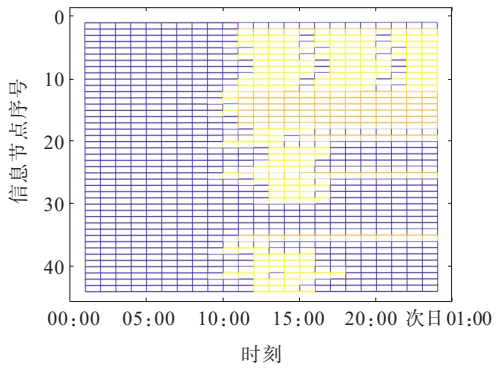
对于系统适应率（$R_{\text{p-fit}}$）和信息适应率（$R_{\text{c-fit}}$），此类弹性指标数值越大弹性性能越好，该指标体现的是配电网 CPS 在遭受网络攻击这种极端事件后维持关键负荷供给的能力。由表 6、7 的数据可知，在 $R_{\text{p-fit}}$ 指标上，3 种方案的表现相差不大，都具有较好的维持负荷能力。但对于 $R_{\text{c-fit}}$ 指标来讲，方案 2 优于方案 3。主要原因是，方案 3 的网络拓扑平均度较大，受临近节点入侵数目的影响，在网络攻击中后期，信息节点的入侵概率会更大。

对于负荷恢复速率（$R_{\text{p-rec}}$）和信息恢复速率（$R_{\text{c-rec}}$），此类弹性指标数值越大弹性性能越好，该指标体现极端事件后快速恢复关键负荷供给和信息设备正常运作的能力，数值上分别与切负荷时间和最终失效节点数目相关。因此，即使在 $R_{\text{p-rec}}$ 指标中方案 1 的表现最好，但在其他指标的表现上却不尽如人意。

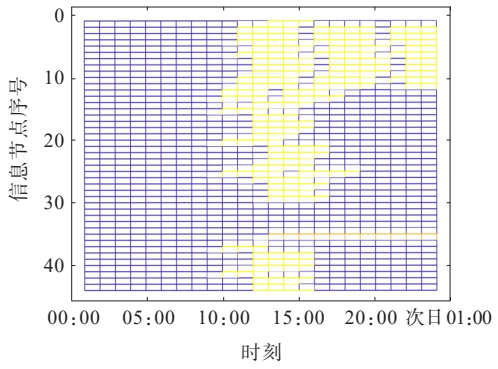
4.2.3　耦合系数变化对比

供能系数体现了信息层与物理层之间的耦合

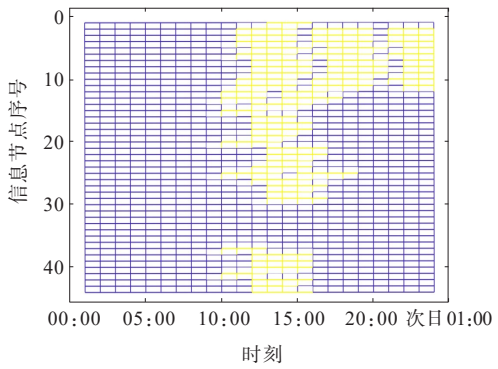
关系。以方案2为例，耦合系数α为0.9、0.8和0.7时信息节点的网络病毒传播如图13所示，黄色网格代表相应的信息节点在该时刻被网络攻击控制，正遭受虚假数据注入攻击；橙色网格代表相应的信息节点在该时刻失效，退出运行并无法接受调度中心下达的指令和传递信息。由图13可知，当信息层与物理层之间的耦合关系越强时，物理节点的失负荷情况对信息节点带来的影响越为严重。



(a) α=0.9



(b) α=0.8



(c) α=0.7

图13 耦合系数变化对比

Figure 13 Comparison of coupling coefficient variation

4.2.4 虚假数据注入攻击程度变化对比

考虑虚假数据注入攻击对配电网CPS造成的影响。以方案2为例，不同攻击程度下的总负荷曲线变化如图14所示，其中，β为攻击程度系数，表示系统采集到的有功、无功量测值与真实值之间的比值，其值越小攻击程度越大。由图14可知，当$\beta \geqslant 0.85$时，虚假数据注入攻击不会造成信息节点失效的情况，系统可恢复到初始状态。

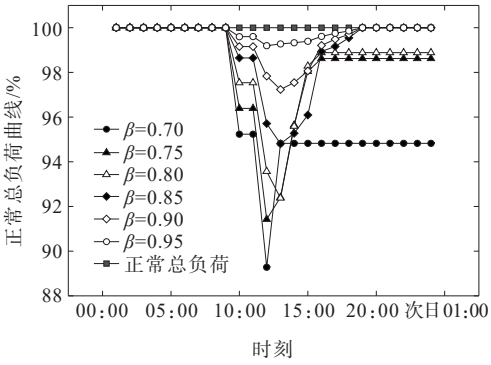


图14 虚假数据注入攻击程度变化

Figure 14 Change of attack degree of false data injection

综上所述，由式(26)计算得出的表8中各方案的综合弹性度量指标可知，方案2的弹性性能最好，为最优方案。该规划方案是以IEEE 33节点改进模型为基准，而规划决策者也可根据配电网的实际情况和自身规划预算选择最为经济有效的规划方案。

5 结语

本文提出了一种FDIA-蠕虫混合攻击下的配电网CPS弹性拓扑优化和防御资源配置策略，用于提高配电系统网络攻击下的弹性。

1) 相较CPS信息层随机故障，FDIA-蠕虫混合攻击模型造成信息层与物理层间的耦合故障更为严重，在此基础上的链路拓扑规划防御力更强；

2) 为避免信息层链路冗余，计及攻击与恢复的网络攻击传播模型将信息节点恢复过程纳入进来，保证了方案经济性；

3) 使用多阶段信息侧与物理侧结合的弹性度量指标对3种耦合关系下的拓扑与防御资源优化方案的弹性进行计算，并与传统的一对一串联模式方案进行比较，验证了本文规划模型的结果能够起到弹性提升的作用。

本文提出的以弹性最大化为目标的电网信息物理系统网络拓扑优化模型，在提高系统弹性能力的基础上对有限的资源进行了合理的分配，研究成果可以为网络攻击下的配电网CPS网络拓扑优化和防御资源分配提供合理的方案指导，提高配电网

应对网络攻击的弹性性能,保证配电网的安全稳定运行。

参考文献:

[1] 秦博雅,刘东.电网信息物理系统分析与控制的研究进展与展望[J].中国电机工程学报,2020,40(18): 5816-5827.
QIN Boya,LIU Dong.Research progresses and prospects on analysis and control of cyber-physical system for power grid[J]. Proceedings of the CSEE, 2020, 40(18): 5816-5826.

[2] FALAHATI B, FU Y, WU L. Reliability assessment of smart grid considering direct cyber-power interdependencies[J]. IEEE Transactions on Smart Grid, 2012,3(3):1515-1524.

[3] 吕华辉,杨航,林志达,等.交直流混联电网信息多协议安全认证集成技术研究[J].电网与清洁能源,2023,39(1):64-69.
LÜ Huahui, YANG Hang, LIN Zhida, et al. Research on information multi-protocol security authentication integration technology of the AC/DC hybrid power grid [J].Power System and Clean Energy, 2023, 39(1): 64-69.

[4] TANG Y,CHEN Q,LI M,et al.Challenge and evolution of cyber attacks in cyber physical power system[C]//IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC),Xi'an,China,2016.

[5] KARNOUSKOS S. Stuxnet worm impact on industrial cyber-physical system security[C]//37th Annual Conference of the IEEE Industrial Electronics Society (IECON),Melbourne,VIC,Australia,2011.

[6] 郭庆来,辛蜀骏,王剑辉,等.由乌克兰停电事件看信息能源系统综合安全评估[J].电力系统自动化,2016,40(5): 145-147.
GUO Qinglai, XIN Shujun, WANG Jianhui, et al. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016, 40(5): 145-147.

[7] ZHOU X,YANG Z,NI M,et al.Analysis of the impact of combined information-physical-failure on distribution network CPS[J].IEEE Access,2020,8: 44140-44152.

[8] 别朝红,林雁翎,邱爱慈.弹性电网及其恢复力的基本概念与研究展望[J].电力系统自动化,2015,39(22):1-9.
BIE Zhaohong, LIN Yanling, QIU Aici. Concept and research prospects of power system resilience[J]. Automation of Electric Power Systems,2015,39(22):1-9.

[9] 别朝红,林超凡,李更丰,等.能源转型下弹性电力系统的发展与展望[J].中国电机工程学报,2020,40(9): 2735-2745.
BIE Zhaohong, LIN Chaofan, LI Gengfeng, et al. Development and prospect of resilient power system in the context of energy transition[J]. Proceedings of the CSEE,2020,40(9): 2735-2745.

[10] 阮前途,谢伟,许寅,等.韧性电网的概念与关键特征[J].中国电机工程学报,2020,40(21):6773-6784.
RUAN Qiantu, XIE Wei, XU Yin, et al. Concept and key features of resilient power grids[J]. Proceedings of the CSEE,2020,40(21):6773-6784.

[11] 陈玥,李力,孙少华,等.弹性电力系统灾害防御及快速恢复智能调度平台设计与实现[J].智慧电力,2023,51(8):38-45.
CHEN Yue, LI Li, SUN Shaohua, et al. Design and implementation of intelligent dispatching platform for disaster prevention and rapid recovery in resilient power system[J].Smart Power,2023,51(8):38-45.

[12] BRUNEAU M,REINHORN A.Exploring the concept of seismic resilience for acute care facilities[J]. Earthquake Spectra,2007,23(1):41-62.

[13] PANTELI M, MANCARELLA P, TRAKAS D, et al. Metrics and quantification of operational and infrastructure resilience in power systems[J]. IEEE Transactions on Power Systems,2017,32(6):4732-4742.

[14] OUYANG M, DUEÑAS-OSORIO L. Multi-dimensional hurricane resilience assessment of electric power systems [J].Structural Safety,2014,48:15-24.

[15] LUO F,ZHANG T,WEI W,et al.A coordinative planning framework for cyber-power distribution system[C]// IEEE Power and Energy Society General Meeting (PESGM),Boston,MA,USA,2016.

[16] LIU W,CHEN Y,WANG L,et al.An integrated planning approach for distributed generation interconnection in cyber physical active distribution systems[J]. IEEE Transactions on Smart Grid,2020,11(1):541-554.

[17] 张博,唐巍,蔡永翔,等.面向高比例户用光伏消纳的储能系统与通信网络协同规划[J].电网技术,2018,42(10): 3161-3169.
ZHANG Bo, TANG Wei, CAI Yongxiang, et al. Collaborative configuration of energy storage systems and communication networks for accommodation of high-penetration residential PVs[J]. Power System Technology, 2018,42(10): 3161-3169.

[18] 朱晓荣,司羽.考虑物理—信息—交通网耦合的配电网多时段动态供电恢复策略[J].电工技术学报,2023,38(12):3306-3320.
ZHU Xiaorong, SI Yu. Multi-period dynamic power supply restoration strategy considering physical-cyber-traffic network coupling[J]. Transactions of China Electrotechnical Society,2023,38(12):3306-3320.

[19] 张艺伟,刘文霞,张帅,等.考虑极端场景的输电-通信网络协同鲁棒扩展规划方法[J].电力建设, 2022,43(10): 121-135.

ZHANG Yiwei, LIU Wenxia, ZHANG Shuai, et al. Joint robust expansion planning of transmission network and communication network considering extreme scenarios [J]. Electric Power Construction, 2022,43(10):121-135.

[20] 杨挺,黄志勇,盆海波,等.基于拓扑势均衡的配电网信息物理系统规划算法[J].电网技术,2017,41(12): 3988-3995.
YANG Ting, HUANG Zhiyong, PEN Haibo, et al. Planning algorithm of cyber physical system for distribution networks based on topological potential equilibrium[J]. Power System Technology, 2017, 41(12): 3988-3995.

[21] WU Y, CHEN J, RU Y, et al. Research on power communication network planning based on information transmission reachability against cyber-attacks[J]. IEEE Systems Journal,2021,15(2): 2883-2894.

[22] BESSANI M, FANUCCHI R Z, ACHCAR J A, et al. A statistical analysis and modeling of repair data from a Brazilian power distribution system[C]//17th International Conference on Harmonics and Quality of Power (ICHQP),Belo Horizonte,Brazil,2016.

[23] 栗会峰.论文附录[EB/OL]. https://pan. baidu. com/s/1BCseJ0AivJUiBf7prtdoIg(提取码:asdf),2024-07-15.
LI Huifeng. Appendix to the paper[EB/OL]. https://pan. baidu.com/s/1BCseJ0AivJUiBf7prtdoIg(extraction code: asdf),2024-07-15.

[24] LINS I D,RÊGO L C,MOURA M D C,et al.Selection of security system design via games of imperfect information and multi-objective genetic algorithm[J]. Reliability Engineering & System Safety, 2013, 112: 59-66.

[25] DEB K,PRATAP A,AGARWAL S,et al.A fast and elitist multiobjective genetic algorithm: NSGA-II[J]. IEEE Transactions on Evolutionary Computation, 2002, 6(2): 182-197.

[26] 张育颖,谢品杰.基于NSGA-Ⅱ算法的互补能源接入方案优化配置[J].电力科学与技术学报,2021,36(5): 153-160.
ZHANG Yuying, XIE Pinjie. Research on multi-energy supplement system optimization method based on NSGA-II[J]. Journal of Electric Power Science and Technology,2021,36(5): 153-160.

[27] 蔡晔,汤丽,唐夏菲,等.基于NSGA-II的电力信息物理系统骨干网络辨识[J].电力系统自动化,2023,47(12):38-46.
CAI Ye, TANG Li, TANG Xiafei, et al. Backbone network identification of cyber-physical power system based on non-dominated sorting genetic algorithm-II[J]. Automation of Electric Power Systems, 2023, 47(12): 38-46.

[28] 曹一家,张宇栋,包哲静.电力系统和通信网络交互影响下的连锁故障分析[J]. 电力自动化设备,2013,33(1):7-11.
CAO Yijia, ZHANG Yudong, BAO Zhejing. Analysis of cascading failures under interactions between power grid and communication network[J]. Electric Power Automation Equipment,2013,33(1):7-11.

[29] 陈倩,王维庆,王海云.基于需求侧响应的主动配电网双层优化方法[J].电力系统保护与控制,2022,50(16):1-13.
CHEN Qian, WANG Weiqing, WANG Haiyun. Bi-level optimization model of an active distribution network based on demand response[J]. Power System Protection and Control,2022,50(16):1-13.

[30] JIANG R, CI S, LIU D, et al. A hybrid multi-objective optimization method based on NSGA-II algorithm and entropy weighted TOPSIS for lightweight design of dump truck carriage[J].Machines,2021,9(8): 156.

[31] 沈国辉,陈光,赵宇,等.基于双目标分层优化和TOPSIS排序的电动汽车有序充电策略[J].电力系统保护与控制,2021,49(11):115-123.
SHEN Guohui, CHEN Guang, ZHAO Yu, et al. Orderly charging optimization strategy of an electric vehicle based on double objective hierarchical optimization and TOPSIS ranking[J]. Power System Protection and Control,2021,49(11):115-123.

[32] 肖丽,谢尧平,胡华锋,等.基于V2G的电动汽车充放电双层优化调度策略[J].高压电器,2022,58(5):164-171.
XIAO Li, XIE Yaoping, HU Huafeng, et al. Two-level optimization scheduling strategy for EV's charging and discharging based on V2G[J]. High Voltage Apparatus, 2022,58(5):164-171.