文章编号：2096-5125 (2020) 06-0560-09 中图分类号：TM73 文献标志码：A
DOI：10.19705/j.cnki.issn2096-5125.2020.06.003

电力系统网络攻击信息物理双层协同紧急控制方法

蔡星浦[1]，王琦[1*]，黄建业[2]，李周[1]
（1. 东南大学电气工程学院，江苏省 南京市 210096；
2. 国网福建省电力有限公司电力科学研究院，福建省 福州市 350000）

Double-layered Cyber-physical Cooperative Emergency Control-strategy-adjustment Method to Prevent Power-system Cyber Attacks

CAI Xingpu[1], WANG Qi[1*], HUANG Jianye[2], LI Zhou[1]
(1. School of Electrical Engineering, Southeast University, Jiangsu, Nanjing 210096, China;
2. Electric Power Research Institute of State Grid Fujian Electric Power Co., Ltd, Fujian, Fuzhou 350000, China)

Abstract: Owing to significant developments in information communication technology (ICT), power systems have evolved to become typical examples of cyber-physical systems (CPSs). Despite the development of intelligent power-system control functions, cyber-physical power systems (CPPSs) remain susceptible to potential cyber attacks. This study analyzes the impacts of CPPS cyber-attacks based on the correlation matrix model. A double-layered cyber-physical cooperative control-strategy-adjustment method is proposed considering the status of cyber modules and physical devices affected by cyber attacks. The feasibility and effectiveness of the proposed method are verified using the standard IEEE system.

Keywords: cyber-physical power system; cyber attacks; correlation matrix; double-layer control strategy

摘 要：信息通信技术的快速发展使得电力系统成为典型的信息物理系统（cyber physical systems, CPS）。在电网侧控制日趋智能化的同时，也引入了网络攻击的风险。本文基于关联矩阵模型分析了网络攻击对电力CPS的影响，然后针对攻击后的信息组件、物理设备状态对后续控制策略的影响，提出了信息物理协同的双层控制策略调整方法，通过IEEE标准系统验证所提方法的可行性和有效性。

关键词：电力信息物理系统；网络攻击；关联矩阵；双层控制策略

0 引言

电力信息物理系统（cyber physical system, CPS）信息业务、通信网络和物理实体逐渐深度融合，一方面使得电力侧的感知和控制更加准确高效，另一方面也引入了潜在的网络攻击风险[1-3]。近年来世界各地已发生（或疑似）多起网络攻击引起电力系统瘫痪的大型事故，2015年乌克兰电网遭受网络攻击引发停电事件被确认为第一起由网络攻击导致大规模停电的实例[3]，其后以色列、美国、委内瑞拉等国陆续发生了多起由网络攻击引发的电网安全威胁乃至大停电的事件，造成的社会、经济影响难以估量。针对电力CPS的网络攻击根据其攻击目标的不同，对电力系统可能造成多方面影响，主要可以分为两类[4-5]。

1）针对电力信息系统的攻击。这类攻击主要通过传统网络攻击技术（例如恶意代码、网络窃听等）渗透进入信息业务，进而非法获取用户的隐私数据或电力市场相关数据，意图获取一定的经济利益，此类攻击通常不会威胁电力系统运行的工程安全。传统的网络安全技术可以被应用于针对此类攻击的防御。鉴于电力系统相对隔离的运行环境且多采用专用信道通信，此类攻击者的攻击难度相对较大。

2）针对电力物理系统的攻击。这类攻击利用了现代电力系统信息物理高度耦合的特性，将网络攻击

基金项目：国家重点研发计划（基础研究类2017YFB0903000）；国家电网公司科技项目（电网信息物理系统分析与控制的基础理论与方法（配套项目））。
National Key Research and Development Program of China (2017YFB0903000); Science and Technology Foundation of SGCC (Basic Theory and Method of Analysis and Control of Power Grid Information Physics System (Supporting Project)).

技术与社会工程学方法（例如钓鱼邮件、身份盗用）相结合，突破CPS网络边界进入内部网络，进而恶意改变工程运行状态，造成重大安全事故。这类CPS攻击过程一般由两部分组成：①利用网络技术对信息网络进行探测、入侵、提权和控制，探知目标系统的各项参数（拓扑、运行状态等），为后续攻击提供基础。②针对CPS设计和业务流程实施攻击，包括诸如安全状态下注入虚假数据诱导系统异常运行，紧急状态下阻断控制系统安全响应扩大故障后果等。此类攻击一旦实现，对经济生产造成的后果不可估量，对工程安全的威胁更大。

为了应对造成工程故障的网络攻击，需要在工作流程、权限制度设计方面广泛讨论，挖掘漏洞，减小电力CPS系统网络边界被突破的风险。但是面对难以预料的攻击手段，由网络攻击造成工程故障的风险始终存在。因此，有必要研究如何快速有效地应对网络攻击造成的工程故障。

目前电力系统应对工程故障主要采取事前预设故障、制定策略、实时故障诊断和策略匹配的安全措施，保证系统的安全可靠运行。常规的电力系统实时故障诊断系统已经有很长的发展历史，通常首先提取故障特征进行学习，形成专家系统，在工程应用中，实时处理电压、电流和二次设备状态等数据诊断故障类型[6-8]。在电力系统新兴网络攻击的诊断方面，近期也开展了大量研究。为应对针对工程的蓄意攻击，许多研究在传统IDS的基础上提出协同应用信息侧的记录和物理侧的数据，并结合最新的模式挖掘方法和机器学习算法，实现网络攻击的快速准确辨识。文献[9]提出在不同电力CPS层级部署智能分析模块实现针对通信网络的攻击检测。文献[10]提出了基于广域监控系统的电力系统暂态紧急控制方案，但是没有考虑通信扰动对电力系统的影响。文献[11]提出基于双侧信息提取事件特征辨识攻击类型的序列挖掘方法。在紧急状态下的控制措施方面，当前的预想故障及相应的策略集合还是依赖传统的三道防线，通过物理侧的切机、切负荷以及严重情况下的系统主动解列等措施保证电力系统的安全稳定运行。文献[12]考虑并定量评估了通信系统事件（延时、误码）对电力系统控制的影响，但没有考虑人为蓄意攻击的情况。文献[13]提出了电力系统在信息物理融合环境下的紧急负荷控制理论和方法，但没有提出考虑攻击对系统后续的影响修正控制策略的方法。由于电力CPS信息物理紧密耦合的特性，执行提前制定的紧急控制策略需要相关通信路径、设备均正常可靠运行才能实现预想效果[14]。对于自然因素（天气、偶发事故）导致的常见故障，通信环境通常不会受到影响，二次执行设备的可靠性也可以保证。但在网络攻击环境下，由于人为参与的特殊性，攻击者为了扩大攻击影响，往往有意选择与电力系统后续防御措施关联的线路、设备配合攻击，由于CPS系统信息物理紧密耦合的特性，应综合考虑攻击在信息和物理双侧的影响，在常规措施的基础上延伸。因此，应对网络攻击造成的电力系统工程故障，有必要实时根据攻击影响，考虑策略相关通信路径的实时性和物理设备的可靠性。

基于上述分析，本文提出一种信息物理协同应对网络攻击造成工程故障的双层自适应调整方法。首先，根据基于关联矩阵的电力CPS通用化建模方法分析网络攻击的影响并提出策略判断函数分析既定策略的可行性。然后，提出一种包含信息物理双层优化的策略调整方法，上层物理侧优化考虑攻击对物理控制目标的影响，下层信息侧优化考虑攻击对信息侧控制路径的影响，实现紧急状态下电力CPS应对网络攻击威胁的快速策略调整。

1 基于关联矩阵的网络攻击影响分析

1.1 电力CPS结构

随着信息通信与智能控制技术的广泛应用，电力CPS中信息系统与电力物理系统的耦合和交互的过程日益复杂[15]。电力系统发电控制、优化调度、本地保护、安全稳定控制等系统都可以归纳为不同层级的CPS系统，包括状态感知、实时分析、科学决策、精准执行的闭环过程。

一般的，电力CPS单元可以抽象为物理实体层、信息物理耦合层和信息系统层，分别对应物理网络、二次设备/通信网络和控制决策单元。物理实体层主要指通过电气连接紧密耦合的电力一次设备，包括发电机、变压器、线路、负荷等。信息物理耦合层主要指二次设备（例如量测装置和控制装置）和通信设备，通过二次设备采集和执行物理层的状态信息，随后通过通信设备间既定的通信规约，实现数据和指令的上/下行传输。通过此过程，物理实体层和信息物理耦合层实现交互。信息系统层则是指不同电力控制业务的抽象集合，信息系统具体应用的功能单元将经由通信网络上传的信息作为输入，根据事前制定的规则、流程，通过控制决策单元得到控制指令结果作为输出。

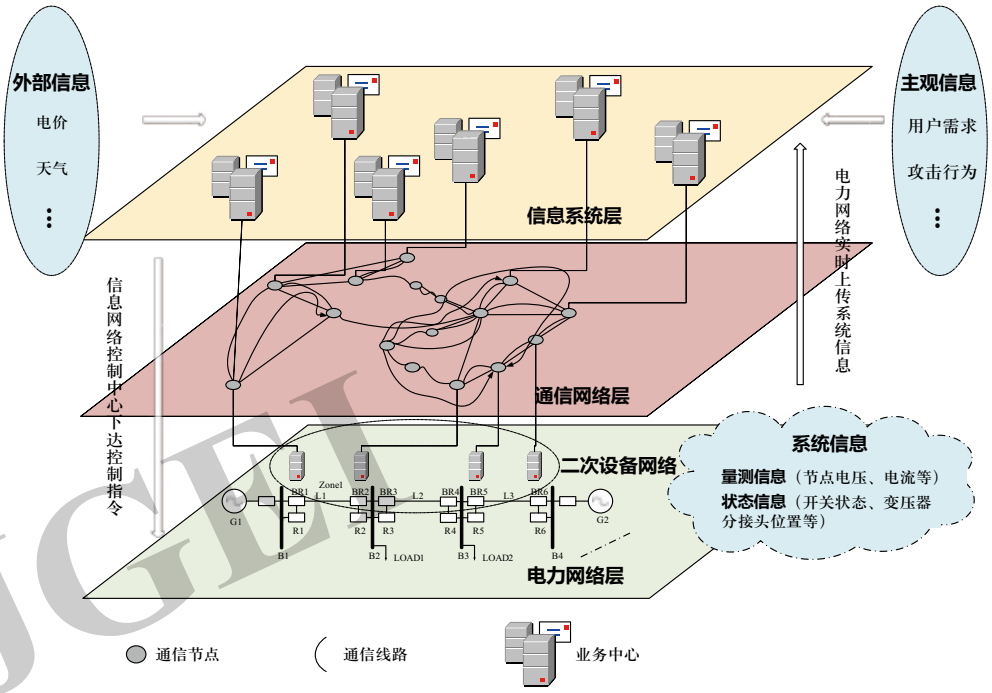

图 1 电力CPS单元结构

Fig. 1 Structure of CPPS

在电力CPS中，物理实体层和通讯网络层通过二次设备网络紧密耦合、相互影响，电力CPS中任意节点故障，都可能给电力系统的安全稳定运行带来不利影响。

1.2 基于关联矩阵的电力CPS建模方法

本文基于关联特性矩阵对电力CPS进行耦合建模[16]，描述各层之间的拓扑关联关系和逻辑关联关系，对包含n个物理节点、m个通信节点、k个二次设备节点和l个信息应用节点的电力CPS网络的建模过程如下。

1.2.1 通信网络建模

采用多元组C_{ij}描述通信节点和通信支路的通信性能，多元组中元素可以根据电力CPS应用需求进行拓展，例如电力CPS通信可能存在的单播、组播和冗余通信等不同通信方式，但本文目前仅考虑传统的有线通信，所提模型亦未考虑无线通信特点。

$$C_{ij}=\left(T_{ij},P_{Bij},P_{Mij},\cdots\right) \tag{1}$$

式中：T_{ij}、P_{Bij}、P_{Mij}分别表示i节点与j节点之间的通信延时、中断概率和传输错误概率。

基于通信节点和支路模型，采用$m\times m$阶通信网邻接矩阵C来描述通信网拓扑及特性，描述信息在通信网中的传输过程，定义如下：

$$C=\begin{array}{c} \\ 1\\ \vdots\\ i\\ \vdots\\ m\end{array}\begin{array}{c}\begin{array}{cccccc}1 & \cdots & j & \cdots & m\end{array}\\ \begin{bmatrix} C_{11} & \cdots & C_{1j} & \cdots & C_{1m}\\ \vdots & \ddots & \vdots & \iddots & \vdots\\ C_{i1} & \cdots & C_{ij} & \cdots & C_{im}\\ \vdots & \iddots & \vdots & \ddots & \vdots\\ C_{m1} & \cdots & C_{mj} & \cdots & C_{mm}\end{bmatrix}\end{array} \tag{2}$$

$$C_{ij}=\left(T_{ij},P_{Bij},P_{Mij}\right),\begin{cases} i=j,\text{表示通信节点}\\ i\neq j,\text{表示通信支路}\end{cases} \tag{3}$$

通信节点i与节点j之间有直接连接时，C_{ij}表示支路的通信性能。通信节点i与节点j之间无直接连接时，C_{ij}=(+∞,0,0)。

对于组播情况，所涉及的计算元素与计算逻辑在单播通信网络模型中均已包含，只需根据具体通信逻辑重新定义计算流程；对于冗余通信，可通过将通信节点多元组C_{ij}中的T_{ij}扩展为T_{ij1}, T_{ij2}，……，同时按照实际冗余通信的通信逻辑重新定义混成计算内涵即可实现通用建模方法的灵活拓展。

1.2.2 二次设备节点建模

二次设备同时具备信息处理和通信的功能，服务于电网的测量、控制、分析和初步分析计算。二次设备节点的建模需要能反映出其对电力CPS的影响，即能够反映出两个方面的特性：一是信息侧和物理侧逻

辑对应关系（信息处理功能）；二是信息处理和传输过程中产生的延时、中断和信号传输错误等。本文对二次设备的节点建模方法如图2所示。

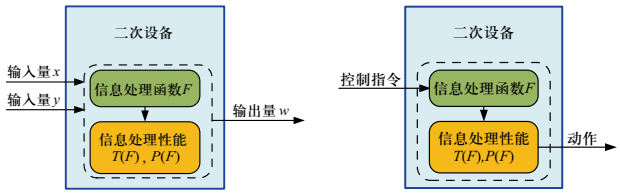

图 2　二次设备功能模型

Fig. 2　Function model of secondary equipment

采用多元组来描述二次设备节点的功能特性，如式（4）所示。

$$S_{ii}=\left(F_{ii}\left(input\right),T_{ii}\left(F_{ii}\right),P_{ii}\left(F_{ii}\right),E_{ii}\left(F_{ii}\right),\cdots\right) \tag{4}$$

式中：$F_{ii}(input)$为信息处理算法，可能由多个部分组成。信息处理产生的延时$T_{ii}(F_{ii})$和信息处理错误概率$P_{ii}(F_{ii})$等取决于二次设备内置的算法逻辑，$E_{ii}(F_{ii})$取决于装置的机械状态。与通信网络邻接矩阵C类似，对每个二次设备进行建模，构成二次设备网络的对角矩阵（二次设备之间无直接通信）。

1.2.3　二次设备–通信网络关联建模

二次设备层网络是基于通信网络的控制网络，二次设备网络和通信网络之间的关联关系主要包含两个方面：通过物理链路直连产生的物理关联；通过通信网络产生的逻辑关联。在实际CPS中，逻辑关联关系取决于具体业务需求，包括具体的静态配置、路由搜索等，并且可能根据系统状态发生改变。以C-S关联特性矩阵描述命令通过通信网络的下发过程为例，S-C矩阵描述信息上传过程的建模思路类似：

$$S\text{-}C=\begin{array}{c} \\ 1\\ \vdots\\ i\\ \vdots\\ k\end{array}\begin{array}{c}\begin{array}{cccccc}1 & \cdots & j & \cdots & m\end{array}\\ \begin{bmatrix} SC_{11} & \cdots & SC_{1j} & \cdots & SC_{1m}\\ \vdots & \ddots & \vdots & \iddots & \vdots\\ SC_{i1} & \cdots & SC_{ij} & \cdots & SC_{im}\\ \vdots & \iddots & \vdots & \ddots & \vdots\\ SC_{k1} & \cdots & SC_{kj} & \cdots & SC_{km}\end{bmatrix}\end{array} \tag{5}$$

采用可扩展多元组SC_{ij}=(S_{ii}, $SC_{\mathrm{TP}ii}$, $SC_{\mathrm{T}ij}$, $SC_{\mathrm{PB}ij}$, …)来描述通信节点和二次设备层节点之间的关联关系，S_{ii}、$SC_{\mathrm{TP}ii}$、$SC_{\mathrm{T}ij}$和$SC_{\mathrm{PB}ij}$分别表示二次设备节点i的性能、二次设备节点i和通信节点j是否可达、延时和中断概率。应用层为业务运算，在求解特定业务时仅需考虑计算时间和计算结果，以I表示该多元组，并输入关联矩阵模型即可。基于上述方法，可以得到电力CPS关联建模示意图如图3所示。

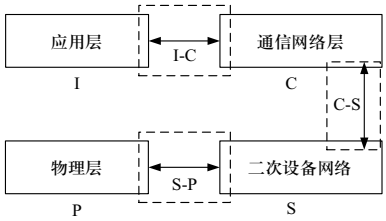

图 3　电力CPS关联建模

Fig. 3　Correlation modeling of CPPS

基于关联矩阵方法对电力信息物理系统各部分建模可以得到完整的电力CPS模型。在应用该模型分析具体业务时，由于不同元素间的融合计算方式不同，因此采用混成计算方法[16]，运算规则可根据元素内容改变，用“⊗”表示，如图4所示。例如在延时元素计算时，混成计算采用直接相加，而涉及逻辑判断时，则通过“与”或“非”的逻辑运算得到结果。

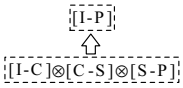

图 4　电力CPS关联模型混成计算

Fig. 4　Model calculation process of CPPS

1.3　基于关联矩阵的网络攻击影响分析

网络攻击对策略执行过程的影响，常见包括针对通信设备的攻击造成某通信节点失去路由功能或某条通信链路不可用；针对二次设备功能模块的破坏攻击或通信模块的攻击导致该设备不可观、不可控或功能不可用。常见的拒绝服务攻击（denial of service, DoS）、中间人攻击（man in the middle, MITM）、蠕虫病毒等均有可能通过技术手段结合社会工程学方法达到上述目的。在电力系统信息物理高度耦合的背景下，局部的攻击在特殊场景下可能影响到整个系统。

基于本章提出的电力CPS关联矩阵建模方法，通过对应矩阵元素的改变，可以实现局部网络攻击对系统整体功能的影响分析。例如若某通信节点i被攻击导致该节点失去了通信功能，则所有与该节点相关的支路$C_{ij}'=C_{ij}\otimes\Delta CA_1=(+\infty,0,0)$，其中$\Delta CA_1$为攻击向量；若通信网络中某通信链路$i$-$j$被DoS攻击导致延时异常或中间人攻击修改报文导致误码，则$C_{ij}'=C_{ij}\otimes\Delta CA_2$，其中$\Delta CA_2$为攻击向量，$\Delta CA_2=(\Delta T_{ij}, \Delta PB_{ij}, \Delta PM_{ij}, \cdots)$；若二次设备因攻击导致不可观，不可控或功能破坏，则$S_{ii}'=S_{ii}\otimes\Delta S_{ii}$，其中$\Delta S_{ii}$为攻击向量，$\Delta S_{ii}=(\Delta F_{ii}, \Delta T_{ii},$

ΔP_{ii},…)，其他因攻击或其他因素导致的元素改变也可参照该模式。

2 信息物理协同双层策略修正架构

电力CPS技术将信息、通信技术以及先进的计算平台、控制设备等引入电力系统领域中，推进了智能电网实时感知、实时决策的能力。在已经分析的网络攻击威胁下，有必要根据攻击对系统的影响，实时判断现阶段既定策略的可行性，并根据判断结果自适应调整策略。基于上述背景，本文提出了基于关联矩阵影响分析的信息物理协同双层自适应替代控制策略，为网络攻击下电力系统快速可靠响应提供支撑。

传统的电力系统稳定控制体系（被动安全）三道防线包括快速切除故障元件、稳定控制措施和系统失稳时的紧急措施。快速切除故障元件要求就地精准操作，后续控制措施和紧急措施则由信息侧通过策略匹配和指令下发完成。在网络攻击威胁下，策略匹配和指令下发过程在物理侧和信息侧都存在无法达到预期目标的隐患。以信息系统安全稳定控制业务优化切负荷过程为例，详述双层自适应替代控制策略。

2.1 双层策略整体架构

本文所提的信息物理协同双层自适应替代控制策略如图5所示。首先，基于关联矩阵方法对CPS初始状态进行关联建模，在网络攻击发生后对受到攻击影响的元素和突发事件对电力CPS的影响进行修正，形成攻击后新的CPS模型；基于新的模型，本文提出策略判断函数通过模型混成计算分析既定切负荷策略的可用性，若可行，则执行原策略；若不可行，则执行自适应替代控制策略模块中的信息物理双层优化方法，得到新的策略并执行，保证一次系统的安全稳定运行。

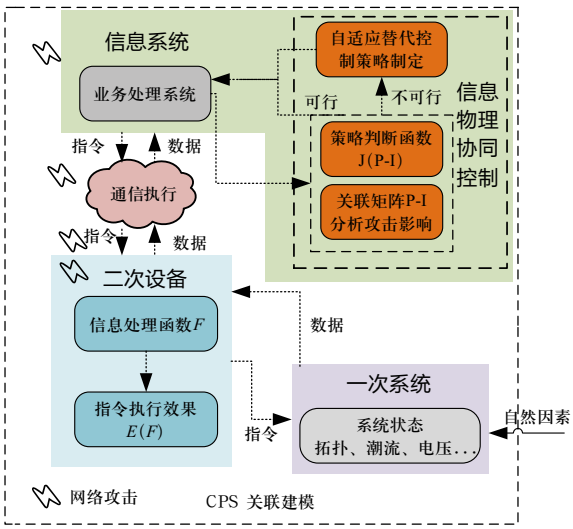

图 5 基于关联矩阵的信息物理自适应控制架构

Fig. 5 Cyber physical cooperative control structure based on CPPS confusion matrix

2.2 既定策略判断

由于网络攻击对电力CPS的影响可能在暂态过程中持续，若既定策略涉及的元件无法在可接受的状态下执行指令，电力故障的暂态恢复过程无法达到预期效果，因此有必要基于攻击的影响范围判断既定策略的可行性。基于前面提出的关联矩阵分析方法，攻击的影响可以叠加到电力CPS关联模型P–I中，得到攻击后的模型$(P–I)'$。在本方法中，通过可拓展的判断函数$J((P–I)')$实现，在实际应用中，判断函数可随工程要求进行拓展或改变。其中：

$$J((P-I)')=r((P-I)')\otimes T((P-I)')\otimes F((P-I)')\cdots$$

式中，判断函数的内容包括：

$r(P–I)$：通过矩阵是否满秩，判断涉及的信息路径，元件是否正常相连，判断原业务指令能否正常下达。

$T(P–I)$：通过业务路径涉及矩阵元素的延时参数总和与业务阈值要求相比，判断原业务指令延时是否满足预设要求。

$F(P–I)$：判断信息处理、指令处理元件是否能正常工作，判断原业务指令能否执行。

2.3 双层信息物理策略自适应调整

对于上层物理侧策略调整，以电力系统安全稳定控制优化切负荷过程为例，优化切负荷策略需要考虑受攻击导致指令无法到达的设备节点、受攻击导致功能受到破坏的控制设备、自然故障下已经脱网导致无法调用的控制设备以及因攻击导致设备处于不可观区域而不可信、不可控的设备和受攻击影响无法正常使用的发电机等因素。基于以上分析，提出基于直流潮流模型并考虑攻击影响的物理侧最优负荷削减算法。优化目标为电网因攻击或偶然因素共同导致的拓扑改变后，损失的负荷最少：

$$\begin{aligned}&\min y=\sum\nolimits_{n\in N'}L_n\\&N'=N-\Delta N\end{aligned}\tag{6}$$

式中：y为系统负荷减载量之和；N为系统节点集合；ΔN为受攻击导致不可控的节点集合；N'为当前状态下

可切负荷节点集合；n为节点编号。

线路功率受到两端节点相角约束，因此线路潮流应满足：

$$F_l = \frac{Z_l}{x_l}\sum_{t\in T} H_t\delta_t \quad l\in W \tag{7}$$

式中：W为系统线路集合；l为线路序号；F_l为线路上的潮流；Z_l为线路的状态；x_l为线路的阻抗；H_t为节点关联矩阵；δ_l为节点相角矩阵。

系统中流入各个节点的功率和节点的负荷应满足基本的平衡约束：

$$\sum_{m\in M} B_m G_m - \sum_{l\in W} H_t F_l = Q_t - L_t \quad t\in T \tag{8}$$

式中：M为系统可用发电机集合；m为发电机序号；B_m为发电机的状态；G_m为发电机的发电功率；Q_t为节点t上所带负载。

线路上流过的功率和发电机的出力应处于各自的承受范围内，并限制发电机爬坡率限制为装机容量的0.5%：

$$-F_l^{\max} \leqslant F_l \leqslant F_l^{\max} \quad l\in W \tag{9}$$

$$G_m^{\min} \leqslant G_m \leqslant G_m^{\max} \quad m\in M \tag{10}$$

式中：$F_l^{\max}$为线路l的传输极限；$G_m^{\max}$和$G_m^{\min}$分别为发电机m的最大和最小出力。

在MATLAB simulink中基于三阶转子运动方程搭建模型，限制发电机爬坡率限制为装机容量的0.5%验证得到的结果，保证系统稳定可靠恢复。

将上层物理侧优化得到的切负荷节点直接相连的二次通信节点集合记为C_e，指令下发设备集合记为C_s。对于下层信息侧通信路径调整，指令的下发过程需要考虑受攻击导致不可用的通信链路和通信节点。考虑到此类紧急控制业务主要承载于电力通信网的传输层，若上层优化后得到的通信节点之间已经提前规划了通信路径并建立了电路连接且连接正常，则按照既定通信路径传输。若提前建立的连接收到攻击影响无法正常通信，则调用提前制定的备用通信链路。若无现有的备用通信策略，可将路径上的延时作为路径权重，转化为图论中的路径寻优问题。信息侧的优化目标为指令下发过程的延时最短：

$$\min R = \sum r_{ij}' \quad i\in C_s, j\in C_e \tag{11}$$

$$r_{ij}' = r_{ij} + \Delta r_{ij} \tag{12}$$

式中：R为指令下发过程的总延时；r_{ij}为所有通信节点延时集合；Δr_{ij}为受攻击导致不可用的通信节点延时集合；r_{ij}'为当前状态下可用通信节点延时集合。该层优化可采用常见的路径寻优方法例如经典Dijkstra算法或基于遗传算法等智能算法。

得到双层的策略优化方案后，需要再次由策略判断函数J判断新策略的可行性。新的策略仍然可能会出现延时不符合业务延时阈值情况，此时剔除不符合的指令路径对应的物理节点，重新进入双层策略优化架构，直到策略可行。

3　算例分析

以某14节点电网对应的安全稳定控制系统作为研究对象，在Simulink中搭建物理模型，在OPNET中对应的搭建通信网络。控制信息从负控中心站（MS）经不同切负荷子站（SS）到达执行站（ES）的总体通信时延。比如，主站向子站SS1下达切负荷指令，该指令通过2 M光纤传输到子站，再通过就近变电站中的光纤/E1转换器转成分路信号，传输给子站下面管理的执行站ES2、ES3等。攻击场景为DoS攻击导致通信链路不可用，验证在攻击状况下本文所提信息物理协同自适应策略调整方法的有效性。系统对应的二次设备层和通信层简化网络如图6所示，包含1个主站（MS）、4个子站（SS）、11个执行站（ES）和14个通信节点。

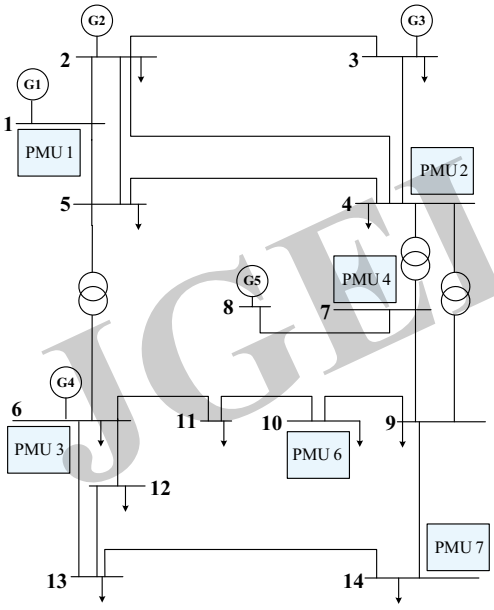

图 6　IEEE 14节点系统图

Fig. 6　IEEE 14 bus system

由系统初步仿真可以得到，当线路6~13断线时，为保证电网稳定运行，需要切除4节点4.5 MW负荷。

信息传输过程通常为二次设备采集并处理物理节点信息，再通过通信节点向信息你上传，信息节点根据故障情况进行决策，并向相关执行单元（二次设备）下达指令。在理想场景下，安全稳定防御系统（SSDS）动作顺序是：

1）节点13传输信息给SS3，SS3给MS发送故障信息；

2）MS识别故障，进行控制决策。MS的决策过程为；首先根据检测到的故障，匹配离线策略；针对此故障，切除节点4所带部分负荷4.5 MW；

3）MS根据控制决策结果通过SS3向节点4的执行站ES4下发控制指令。

由于DoS攻击主要涉及延时，因此本文关联矩阵的多元组中仅展示延时。根据NERC的标准，故障发生，策略匹配到动作指令到达整个过程需要在300 ms以内完成[17]；国家电网规定故障匹配和策略制定环节需要在50 ms以内完成[18]。对CPS模型建立基于关联特性矩阵的通信延时模型，线路传输的正常通信延时按5 s/km计算，攻击后的通信延时无穷大。在本算例中二次设备到物理侧的动作时间不受通信延时影响，暂不在计算中给出。对攻击前的过程应用关联矩阵方法建立I、C、S、C-S、S-I矩阵如下所示：

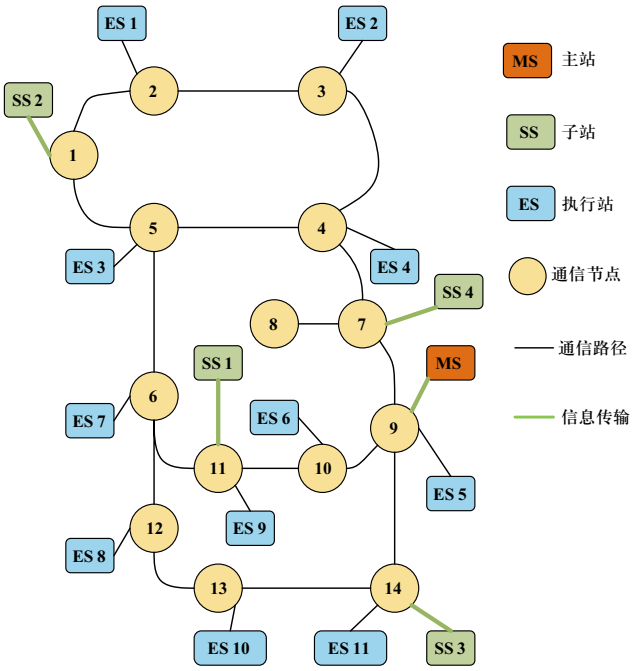

图 7 通信网络拓扑和安全稳定控制系统各站的位置

Fig. 7 Topology of the communication network and the location of control stations

I=diag(54.31, 39.22, 65.55, 17.12, 40.61);

S=diag(54.72, 63.86, 44.93, 75.75, 84.07, 25.43, 41.43, 24.35, 92.93, 35.00, 29.66);

$$C=\begin{bmatrix}
0 & 1.970 & 0 & 0 & 2.745 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 2.345 & 2.905 & 2.845 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0.335 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 1.665 & 0 & 1.587 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2.745 & 0.610 & 0.330 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.374 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.590 & 0 & 0 & 0 & 0.635\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.410 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.100 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1.085\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

同理，建立I-C和C-S矩阵分别可以建立5×14维和14×11维的稀疏矩阵，并且I-C=(C-I)^{T},C-S=(S-C)^{T}，本算例中矩阵数据的单位为ms。

基于关联矩阵采用混成计算方法，建立CPS系统信息上传过程P-I和指令下发过程I-P矩阵。上述矩阵中的元素可根据具体场景和攻击影响进行修正。

场景1：无网络攻击，信息上传的路径为ES10-SS3-MS，指令下发的路径为MS-SS4-ES4。

场景2：DoS攻击导致通信链路7-9堵塞，系统无策略调整能力，攻击的影响为$C'(7,9)=C(7,9)+\Delta C_{7\text{-}9}=+\infty$。频率继续下降到49.90 Hz后触发后续动作，切除节点9负荷10 MW，指令下发路径为MS-ES5。

场景3：DoS攻击导致通信链路7-9堵塞，触发系统策略调整模块。第一次优化，物理目标不变，指令通过通信路径9-10-11-6-5-4-7到达SS4，经校核，延时不符合业务要求。第二次优化，切除目标改为节点6负荷6 MW，指令下发路径为MS-SS1-ES7，策略优化过程耗时约20 ms，重新规划的信息下发路径耗时比既定策略耗时多24 ms。各场景根据关联特性矩阵计算得到的动作延时情况如表1所示。

表 1　各场景动作延时情况

Table 1　Delay of the instructions in all scenarios

ms

场景	故障上传	策略选择	指令下发
场景1	91.550	16.863	47.490
场景2	91.550	48.690	159.308
场景3	91.550	41.546	66.554

分析得到各场景动作延时，负荷损失情况和系统频率变化如表2所示。

表 2　各场景指令控制效果对比

Table 2　Comparison of the system recovery process in all scenarios

场景	最终后果/MW	动作时间/ms	频率最低点/Hz
场景1	4.5	155.883	49.941
场景2	10	299.548	49.851
场景3	6.2	199.650	49.907

在MATLAB Simulink分别仿真三种场景，结果如图8所示。

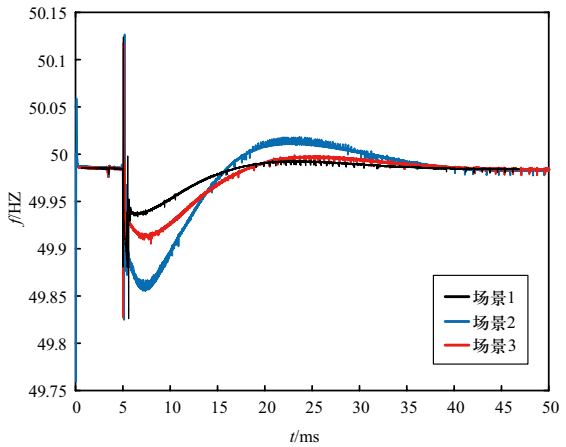

图 8　各场景下系统频率变化图

Fig. 8　Frequency recovery process in 3 scenarios

在理想情况下，通常不考虑信息系统的延时或考虑其在一个可接受的范围内。在常规故障时，电力系统的三道防线可以较好的使系统的频率在跌落之后快速恢复到正常状态。当有DoS攻击造成控制指令延时，继电保护装置作用之后，二道防线的切负荷指令没有快速执行，导致系统频率没有按照预想情况开始恢复，反而不断跌落，触发了后续的切负荷指令执行，不仅导致负荷减载量变大，同时频率跌落情况更加严重。在本算例中，假设后续的切负荷指令没有经过被DoS攻击堵塞的链路，若后续的攻击仍被堵塞，可预见造成的后果将更加严重。若在传统电力系统三道防线保护与控制措施的基础上，考虑到网络攻击造成的可能性，在网络攻击造成故障时，对既定策略可行性进行判断，并双侧协同进行策略调整。尽管优化过程会延长策略制定时间，但仿真验证证明快速的优化仍可以满足工程要求，且控制效果明显好于既定策略。

4　结论

电力系统信息物理紧密耦合的特性使得通过信息技术手段造成工程故障成为可能。目前广泛应用的事前策略制定，在线匹配执行的紧急控制方法可能会由于网络攻击的影响使得既定效果无法达到。本文通过对电力CPS关联建模，通过关联矩阵定量分析攻击影响。基于影响分析提出信息物理协同的双层策略自适应调整方法，快速判断既定策略的可行性并自适应调整策略，保证电力系统在网络攻击风险下的可靠紧急控制。但该方法需建立在电力系统对网络攻击的快速、准确辨识基础上，因此有必要继续深入研究电力系统网络攻击的快速辨识和三道防线在网络攻击背景下的对应修正方法。

参考文献

[1] 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(in Chinese).

[2] 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(in Chinese).

[3] 汤奕，王琦，倪明，等. 电力信息物理融合系统中的网络攻击分析[J]. 电力系统自动化，2016，40(6)：148-151.
TANG Yi, WANG Qi, NI Ming, et al. Analysis of cyber attacks in cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(6): 148-151(in Chinese).

[4] 刘烃，田决，王稼舟，等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报，2019，45(1)：5-24.
LIU Ting, TIAN Jue, WANG Jiazhou, et al. Integrated security threats and defense of cyber-physical systems[J]. Acta Automatica Sinica, 2019, 45(1): 5-24(in Chinese).

[5] 赵俊华，梁高琪，文福拴，等. 乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J]. 电力系统自动化，2016，40(7)：149-151.
ZHAO Junhua, LIANG Gaoqi, WEN Fushuan, et al. Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems, 2016, 40(7): 149-151(in Chinese).

[6] 张文浩，钱瞳，连祥龙，等. 基于集中式与分布式的信息物理融合微电网电压频率二次恢复控制仿真研究[J]. 全球能源互联网，2019，2(5)：476-483.
ZHANG Wenhao, QIAN Tong, LIAN Xianglong, et al. Simulation of centralized and distributed control of voltage and frequency secondary restoration in cyber-physical microgrid[J]. Journal of Global Energy Interconnection, 2019, 2(5): 476-483(in Chinese).

[7] LEE H J, PARK D Y, AHN B S, et al. A fuzzy expert system for the integrated fault diagnosis[J]. IEEE Transactions on Power Delivery, 2000, 15(2): 833-838.

[8] 边莉，边晨源. 电网故障诊断的智能方法综述[J]. 电力系统保护与控制，2014，42(3)：146-153.
BIAN Li, BIAN Chenyuan. Review on intelligence fault diagnosis in power networks[J]. Power System Protection and Control, 2014, 42(3): 146-153(in Chinese).

[9] ZHANG Y C, WANG L F, SUN W Q, et al. Distributed intrusion detection system in a multi-layer network architecture of smart grids[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 796-808.

[10] 谢欢，张保会，沈宇，等. 基于WAMS的电力系统暂态紧急控制启动方案[J]. 电网技术，2009，33(20)：59-64.
XIE Huan, ZHANG Baohui, SHEN Yu, et al. Designing a start-up scheme for power system transient emergency control based on WAMS[J]. Power System Technology, 2009, 33(20): 59-64(in Chinese).

[11] PAN S Y, MORRIS T, ADHIKARI U. Developing a hybrid intrusion detection system using data mining for power systems[J]. IEEE Transactions on Smart Grid, 2015, 6(6): 3104-3113.

[12] 余文杰. 通信系统对电力系统稳定控制的影响研究[D]. 南京：东南大学，2016.

[13] 王琦. 电力信息物理融合系统的负荷紧急控制理论与方法[D]. 南京：东南大学，2017.

[14] 连祥龙，张文浩，钱瞳，等. 考虑信息节点失效的电力信息物理系统脆弱性评估方法[J]. 全球能源互联网，2019，2(6)：523-529.
LIAN Xianglong, ZHANG Wenhao, QIAN Tong, et al. Vulnerability assessment of cyber physical power system considering cyber nodes failure[J]. Journal of Global Energy Interconnection, 2019, 2(6): 523-529(in Chinese).

[15] 赵俊华，文福拴，薛禹胜，等. 电力CPS的架构及其实现技术与挑战[J]. 电力系统自动化，2010，34(16)：1-7.
ZHAO Junhua, WEN Fushuan, XUE Yusheng, et al. Cyber physical power systems: architecture, implementation techniques and challenges[J]. Automation of Electric Power Systems, 2010, 34(16): 1-7(in Chinese).

[16] 薛禹胜，李满礼，罗剑波，等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化，2018，42(2)：11-19.
XUE Yusheng, LI Manli, LUO Jianbo, et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems, 2018, 42(2): 11-19(in Chinese).

[17] System preformance criterion, WECC standard TPL-001-WECC-CRT-2, 2011.

[18] 电力系统安全稳定导则，国家电网标准 DL 755-2001，2001.

收稿日期：2020–05–11；修回日期：2020–09–14。

作者简介：

蔡星浦

蔡星浦（1996），男，硕士研究生，研究方向为电力信息物理系统安全，E-mail：caixingpu@seu.edu.cn。

王琦（1989），男，副教授，研究方向为电力系统稳定与控制，电力信息物理系统。通信作者，E-mail：wangqi@seu.edu.cn。

黄建业（1986），男，硕士，研究方向为配电网信息物理系统，E-mail：cxpseuee@163.com。

李周（1985），男，副教授，研究方向为电力系统稳定控制、交直流混合输电等，E-mail：lizhou@seu.edu.cn。

（责任编辑　张鹏）