Journal of Electric Power Science and Technology

Volume 37 | Issue 4 Article 14

9-23-2022

Research on vulnerability analysis of cyber-physical distribution system based on interdependent network theory

Xianghui XIAO
School of Mechatronic Engineering and Automation, Foshan University, Foshan 528500 , China

Zhenshan ZHANG
School of Mechatronic Engineering and Automation, Foshan University, Foshan 528500 , China

Haishu TAN
School of Mechatronic Engineering and Automation, Foshan University, Foshan 528500 , China

Recommended Citation

XIAO, Xianghui; ZHANG, Zhenshan; and TAN, Haishu (2022) "Research on vulnerability analysis of cyber-physical distribution system based on interdependent network theory," *Journal of Electric Power Science and Technology*: Vol. 37: Iss. 4, Article 14.
DOI: 10.19781/j.issn.1673-9140.2022.04.014
Available at: https://jepst.researchcommons.org/journal/vol37/iss4/14

基于相依网络理论的配电信息物理系统脆弱性

肖祥慧，张振山，谭海曙

（佛山科学技术学院机电工程与自动化学院，佛山 528500）

摘　要：配电信息物理系统（CPDS）利用配电网与信息系统的互通与深度耦合，实现超越传统配电网系统的运行效果和性能水平的同时，也给配电系统运行的可靠性和安全性带来了潜在的负面影响。因此，考虑信息物理交互研究配电信息耦合网络的脆弱性具有重要的意义。借鉴相依网络理论的思想与方法，考虑孤岛电网运行，分析不同攻击策略下信息网络拓扑和耦合模式对 CPDS 的影响，探索具有强鲁棒性的 CPDS 网络架构。仿真结果表明：高介数节点攻击对 CPDS 网络模型具有最强的破坏性，并且具有小世界特性信息网络的 CPDS 具有最强的鲁棒性；不同的网络耦合模式面对不同的攻击方式具有不同的脆弱性，相对于随机耦合模式，同配性耦合模式面对随机攻击具有更强的鲁棒性，但对于蓄意攻击方式，同配性耦合具有更差的鲁棒性。

关　键　词：配电网；信息物理系统；脆弱性；相依网络

DOI：10.19781/j.issn.1673-9140.2022.04.014　　**中图分类号**：TM72　　**文章编号**：1673-9140(2022)04-0125-09

Research on vulnerability analysis of cyber-physical distribution system based on interdependent network theory

XIAO Xianghui, ZHANG Zhenshan, TAN Haishu

(School of Mechatronic Engineering and Automation, Foshan University, Foshan 528500, China)

Abstract: The cyber physical distribution system (CPDS) is designed to realize the interoperability and deep integration of physical and cyber systems, so that it can obtain better operating effects beyond the traditional distribution system. At the same time, it also brings potential negative impact on the reliability and security of distribution systems' operation. Therefore, it is of great significance to study the vulnerability of the CPDS considering cyber-physical interactions. Considering the islanded operation of power grids, this paper analyzes the influence of network topology and coupling mode under different attack strategies on CPDS, and explores the strong robustness of the CPDS network topology based on the theory of interdependent networks. The simulation results show that: high-betweenness node attack is the most destructive to CPDS network model, and the CPDS with small-world characteristic cyber network has the strongest robustness. Different network coupling modes have different vulnerabilities to different attack modes. Compared with random coupling mode, assortative coupling mode has stronger robustness to random attack, but assortative coupling mode has worse robustness to target attack mode.

Key words: distribution network; cyber-physical system; vulnerability; interdependent network

收稿日期：2020-05-01；**修回日期**：2021-04-30

基金项目：国家自然科学基金(52177132)；国家重点研发计划(2018YFB1308200；2018YFB1308203)

通信作者：肖祥慧(1983-)，男，博士，副教授，主要从事电力系统故障诊断、电机智能控制以及人工智能算法等研究；E-mail：xiaoen3@126.com

能源与环境问题事关人类社会的生存和可持续发展,电网作为承载能源革命的基础性平台,对能源革命具有重大的推动作用[1]。未来电网将逐渐转变为大规模可再生能源的电能输送与分配的智能电网[1],变成集数字化与信息化为一体的综合体系平台。在电力系统“发、输、变、配、用”五大环节中,配电网和人们的日常用电密切相关。在经济社会不断发展的过程中[2-3],人们对供电服务质量的要求也日益严格,因此,城市配电网既是提高城市电能服务质量的关键环节,也是构建智能电网的关键环节,同时还是实现能源互联网这一重大目标的关键环节[4]。随着国家智能电网发展战略的逐步深入和能源互联网发展战略的逐步深入,大量大规模电气设备、数据采集设备和计算机设备接入了城市配电网络中,以各种电力设备为核心的传统城市配电网络,正逐步发展为信息物理高度耦合的配电网信息—物理系统(cyber physical distribution system,CPDS)[5]。

信息物理系统之间的相互作用和相互依赖关系是一把双刃剑,能让系统呈现出更复杂的性质并具备实现单个系统无法实现的功能,同时也能降低系统的鲁棒性,导致系统大规模失效的灾难发生[6]。自 2010 年 Buldyrev 教授在文献[7]中提出相依网络的概念及其脆弱性分析框架以来,已有很多学者尝试从相依网络的角度对电力 CPS 的脆弱性进行研究;文献[8]建立了考虑电力网和信息网传输容量的相互依存网络模型,并考虑网络节点的特征参数,利用数据分析的方法识别关键节点,文献[9]在此基础上得出了不同耦合方式与耦合率对网络鲁棒性的影响;文献[10]通过分析网间异质节点之间的依存关系,建立相依网络模型,并考虑网络的拓扑参数,利用数据驱动的方法建立回归模型预测级联故障结果;文献[11]在直流潮流模型的基础上,考虑电力网与信息网深度耦合,构建了一种电力—信息耦合网络故障模型,研究了信息网元件失效对电力网连锁故障的影响。但这些研究基本集中在高压输电系统,对配电网的研究还处于萌芽阶段。分布式能源(distributed energy resources, DER)的引入,如太阳能/风电以及电动汽车(electric vehicle,EV),改变了配电网的拓扑结构及运行情况,且中低压配电网在地理上覆盖范围更小,而且多覆盖在城镇及城市等人口密集的地区。因此,考虑配电网的特性,输电网领域中得出的结论并不完全适用于配电网。

配电网是电力系统输送电能的最后一个环节,直接与用户的用电网络相连接,其稳定性与可靠性如何,用户会有最直接的体验。但是,目前对于 CPDS 脆弱性的研究还处于探索阶段,文献[12]建立了中压配电网相互依存网络模型,从静态角度分析了模型的统计特性,提出具有小世界特性信息网络系统的 CPDS 鲁棒性最好;文献[13]从拓扑角度对中低压配电网络进行了分析,并利用拓扑与能量参数之间的关系分析了产消者之间的相互作用。因此,对于 CPDS 的研究还需更大量的创新性工作。

本文借鉴相互依存网络理论及其在输电网信息物理系统脆弱性分析中的研究,构建 CPDS 的相依网络模型;在传统网络模型节点理想的无向依存的基础上,考虑 CPDS 节点的异质性,通过分析网络异质节点之间的有向依存,建立 CPDS 相依网络模型。CPDS 随着通信技术的发展也在逐渐演变,采用具有不同特征的网络拓扑模型作为配电网的通信网,并采用不同的耦合模式,分析通信网络结构和网络耦合模式对 CPDS 整体鲁棒性的影响。

1 CPDS 相依网络模型

分布式电源(distributed generation,DG)与配电网网供电源并网协同运行后,联合向负载提供电能;DG 故障时断开开关使 DG 脱离并网,让配电网单独供电,不会对整个配电网造成任何影响。当检测到配电网出现故障后,操作开关让 DG 与故障电网脱离,就可使得 DG 就近向没有发生故障的用电区域单独供电,形成一种孤岛运行方式。孤岛大小随着 DG 输出的电能不同而发生变化,负荷功率的平衡情况也会使其改变大小。但是,当处于孤岛运行并如潮汐、光伏发电等可再生能源作为 DG 时,因自身受环境影响较大的缺陷,其输出的功率可能会及不稳定,有较强的间歇性与波动性,并不能保证让孤岛内的用电负荷正常运行。为此,区分配电网和信息网中节点的异质性,并根据节点之间的依存关系建立 CPDS 相依网络模型,如图 1 所示。

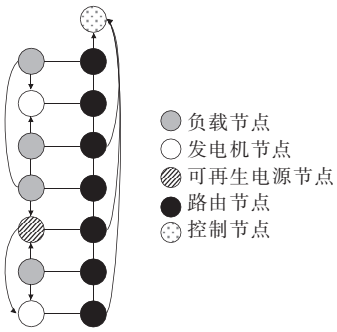

图 1　CPDS 异质依存网络模型

Figure 1　CPDS heterogeneous dependency network model

CPDS 异质相依网络模型中包含配电和信息网络，配电网络可表示为 $G_p=(V_p,E_p;\varphi,\psi;A,R)$，其中，$V_p=\{v_{p1},v_{p2},\cdots,v_{pn}\}$ 为节点集合，$E_p=\{e_{p1},e_{p2},\cdots,e_{pm}\}$ 为边集合。信息网络可表示为 $G_c=(V_c,E_c;\varphi,\psi;A,R)$，其中，$V_c=\{v_{c1},v_{c2},\cdots,v_{cn}\}$ 为节点集合，$E_c=\{e_{c1},e_{c2},\cdots,e_{cm}\}$ 为边集合。在 V_p、V_c 中，φ 表示节点类型映射函数：$V\to A$，满足 $\varphi(v)\in A(v\in V)$；ψ 表示边类型映射函数：$E\to R$，满足 $\psi(e)\in R(e\in E)$，且节点类型数量 $A>0$，边类型数量 $R>0$。CPDS 异质相依网络模型可以描述为 $G=(G_p,G_c,E_{p\text{-}c})$，其中 $E_{p\text{-}c}$ 表示配电网和信息网之间的依存关系。本文中配电网络由 3 种类型的节点组成：负载、发电机、可再生节点；信息网络由 2 种类型的节点组成：控制、路由节点。路由节点向对应的电力节点发送状态信息和接收控制命令，与此同时，电力节点则给路由节点提供其需要的电力支持。并且将配电网中的电力线路和信息网络中的光纤线路视为网络的连接边，可区分为单向和双向边。因此，配电网和信息网形成相互依存的网络系统。

1.1　配电网模型

区别于传统的配电网络，本文研究对象是含多种分布式电源的智能配电网。智能配电网中拥有不同种类的节点，这些节点按照功能特性的差别分为 2 种：等值电源、等值负荷节点。等值电源节点因不同的供电特性分为发电机、可再生电源节点。此外，为保证联络开关在配电网中的作用，将其视作等值负荷节点，闭合时其所在支路视作边，电力传输线路和变压器所在支路同样视作边。因可再生能源节点提供的电能具有很强的间歇性与不稳定性，仅依靠其并不能保证用电负荷运行，故可再生能源节点在逻辑上和另一个电源节点即发电机节点存在依存关系。建模过程中假设存在一条单向边连接 2 种电源节点，系统的依存关系可以概述：可再生电源节点依存于发电机节点，等值负荷节点依存于异质的等值电源节点[14]。

1.2　通信网络模型

根据通信网中节点的功能差异，本文将信息网中节点分为路由、控制中心节点。路由节点负责信息采集及调度命令下达，信息网络控制中心具有远程监测和控制电力网络的功能，负责整个电网的安全运行及经济调度。控制中心通过路由节点与电力网络连接，由于控制中心节点的重要作用，一般都设有备用电源，可视为自治节点而与电力网络解耦，即控制中心节点与电力网络之间不存在直接的连接关系，将通信线路视为边。在通信网络中，路由节点依存于控制中心节点。

1.3　依存关系

CPDS 异质依存网络中电力节点负责给信息节点提供能源，当电力节点失去作用后，依存于其上的信息节点也会当即失效。信息节点中的路由节点会对电力节点进行监视控制，信息节点的故障也会导致电力节点失去控制导致故障，电力网与信息网之间的依存是双向依存。为了不失一般性，本文假设路由节点数与电力节点数一一对应，能够非常明显的体现其相互依存的关系。

2　CPDS 级联故障模型

2.1　异质依存网络衰退过程

根据异质依存网络不同节点的相互联系以及逻辑关系，可知节点间的关系分为双向和单向依存。电力网络内部同质性节点间的依存关系和不同网络中异质性节点之间的依存关系都可以是双向依存关系。而单向依存关系就只能出现在同一网络内的异质性节点之中，如：负载与电源节点、可再生电源与发电机节点。本文从 2 个不同的方面进行 CPDS 相依网络的脆弱性评价研究，包含各单侧网络的脆弱

性评估,也包含单侧网络对其依存网络的影响。因此,网络故障传播呈现出交互影响的特点,如图 2 所示。

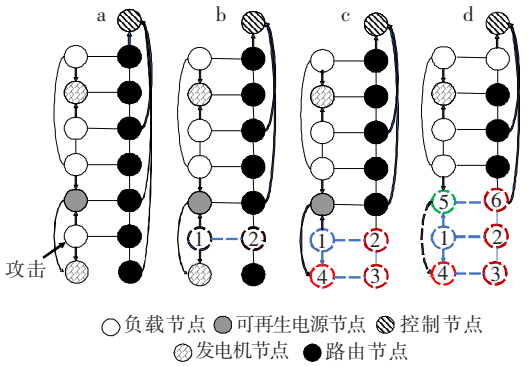

图 2 异质依存网络衰退过程

Figure 2 Heterogeneous dependent network decay process

1)电力网中的节点 1 被攻击(图 2a)。

2)依存于电力节点 1 的信息网络路由节点 2 被删除(图 2b)。

3)路由节点 2 的失效导致路由节点 3 失去与控制节点的连通而失效,同时使依存于路由节点 3 的发电机节点 4 失效(图 2c)。

4)发电机节点 4 的失效使其依存的可再生电源节点 5 以及可再生电源节点对应的路由节点 6 失效,(图 2d),并得到最终网络。

2.2 电网潮流计算

配电系统通过电力网络将电力从电源节点输送到用户节点。实际电力系统是一个高阶复杂的非线性网络,网络结构的任何突变都会改变潮流分布,同时引起大的暂态振荡[15]。假设发生跳闸时系统总是能够达到稳定状态,并且系统达到稳定状态的时间足够短。本文主要研究配电网中故障传播的影响,仅考虑由于过载引起的停电,忽略电路元件的非线性特性和可能的振荡行为。采用文献[16]中提出的线性潮流模型,该模型考虑了电力过载引起的故障,并结合基尔霍夫定律得到了电力系统中稳定的潮流分布。

本文考虑等值电源、等值负荷节点这 2 种类型的电力节点。

1)等值电源节点。等值电源节点是配电网络中的发电节点,包含可再生能源、发电机节点,电源节点 i 的等式可表示为

$$(0 \quad \cdots \quad y_i \quad \cdots \quad 0) \cdot \boldsymbol{U} = u_i \tag{1}$$

式中 $y_i = 1$;u_i 为节点 i 的电压;$\boldsymbol{U} = (\cdots \quad u_i \quad u_j \quad u_k \quad \cdots)^{\mathrm{T}}$ 为电压向量。

2)等值负荷节点。等值负荷节点是在电路中吸收电流的消耗节点。等值负荷节点 j 的基尔霍夫定律方程为

$$(Y_{j1} \quad \cdots \quad Y_{jj} \quad \cdots \quad Y_{jn}) \cdot \boldsymbol{U} = I_j \tag{2}$$

式中 I_j 为注入节点 j 的外部注入电流;Y_{ji} 为节点 j、i 间的线路导纳,且 $Y_{jj} = -\sum_{j \neq i} Y_{ji}$,若节点 j、i 间没有电力线路,则 $Y_{ji} = 0$。由此可得:

$$\boldsymbol{Y} \cdot \boldsymbol{U} = \boldsymbol{I} \tag{3}$$

其中

$$\boldsymbol{Y} = \begin{bmatrix} \ddots & & & & & \cdots & \\ 0 & \cdots & y_i & 0 & 0 & \cdots & 0 \\ Y_{j1} & \cdots & Y_{ji} & Y_{jj} & Y_{jk} & \cdots & Y_{jn} \\ & & & & & \cdots & \ddots \end{bmatrix}$$

$$\boldsymbol{I} = (\cdots \quad u_i \quad I_j \quad I_k \quad \cdots)^{\mathrm{T}}$$

在给定吸收电流、发电信息和拓扑结构的情况下,利用式(3)求出每个节点的电压,然后计算出输电线路中的电流:

$$I_{ij} = (u_i - u_j) \cdot Y_{ij} \tag{4}$$

方程式(3)是根据电路定律推导出来的,因此实际描述了电网的行为。此外,该模型还借助于计算软件,为从复杂网络的角度研究电网提供了一种方便的手段,产生了传统电路分析无法得到的结果。需要注意的是,连接系统中发电机提供的功率应始终等于所消耗的功率,电力系统发生变化时负荷应手动或自动平衡。

2.3 信息网络数据传输

本文采用目前广泛应用的数据传输模型对信息网络进行建模,在该模型中数据包以离散的时间步进行发送,在每一时间步都会随机产生新的数据包,然后沿着最短路径传输[17]。可以采用介数表征节点的传输负载[18-19],则节点 i 的传输负载 $L_i(t)$ 为

$$L_i(t) = \sum_{\substack{j,k \in V \\ j \neq k \neq i}} \frac{n_{jk}^i}{n_{jk}}$$

式中 V 为网络中的节点集;n_{jk}^i 为从节点 j 到 k 经过节点 i 的最短路径数;n_{jk} 为从节点 j 到 k 的最短

路径数。

节点 i 的传输容量表示节点能够处理的最大传输负荷，设置为与其初始传输负荷成比例[18]，即 $C_i(t)=(1+\alpha)L_i(t)$，其中 $\alpha(\alpha\geqslant 0)$ 是网络的容限系数。

2.4　级联故障流程

异质和同质节点有很大的区别，同质性节点间的依存关系大多是双向的，但异质性节点间的相互依存关系却完全可以不依赖于实际的连接边，如：可再生能源与发电机节点之间就不存在直接的物理连接边。因可再生能源节点提供的电能具有很强的间歇性与不稳定性，仅依靠它并不能让用电负荷运行，故可再生能源节点必须依存于发电机节点，当发电机节点失去作用后，与之有关的可再生能源节点也立即失去作用。

考虑相依网络节点之间的依存关系，级联故障过程如图 3 所示，具体流程如下。

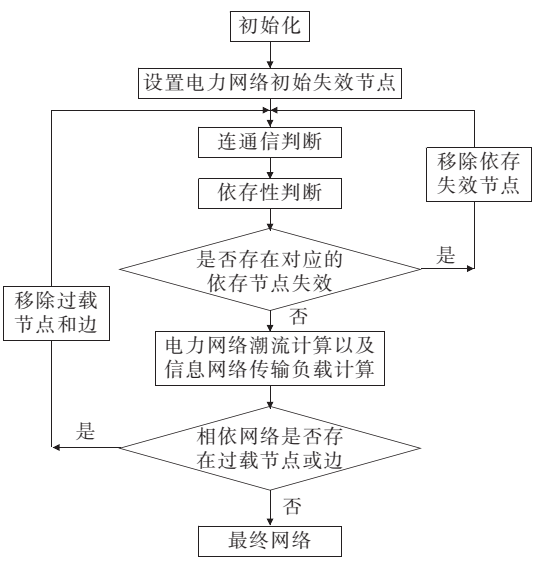

图 3　CPDS 相互依存网络级联故障流程

Figure 3　CPDS interdependent network cascading fault flowchart

1）初始化。信息网络和电力网络初始化，并设置初始失效节点，本文假设耦合系统初始故障是由物理攻击负载节点而导致其在电力网络中失去作用而引起的。

2）连通性判断。耦合系统网络是一个相互关联的整体，若网络中的某一个节点失效，则与之相连接的边和存在依存关系的节点也失效，相依网络演化为相连或者不相连的几个连通域。

3）依存性判断。在通信网中，判断各路由节点连通域是否与控制中心节点相连，若不相连则路由节点失效并移除；在电力网中，判断各等值负荷节点连通域是否与等值电源节点相连，若不相连则等值负荷节点连通域失效并移除，若相连则进一步判断等值电源节点中是否包含发电机节点，若不包含则移除该连通域。返回步骤 2，若不存在节点移除则执行步骤 4。

4）过载故障探测。计算剩余配电网络中的潮流分布以及信息网络中的传输负载。如果配电网或者信息网络存在一些负载超过其容量的节点或链路，则移除它们和它们的对应节点，然后转到步骤 2；否则，输出最终的网络。

3　脆弱性分析

区别于一般网络，分析中采用最大连通子集作为网络脆弱性指标，本文考虑网络异质节点之间的依存关系，采用网络中一定比例的节点被攻击后，网络剩余有效工作节点占整个网络的百分比作为网络的脆弱性指标。

3.1　攻击方式

网络脆弱性表现为网络遭受攻击或故障时的性能下降。本文假设网络攻击是对电力网络节点的物理攻击，利用网络节点删除方式使这些节点失去作用，模拟网络系统中某些元件发生故障的现象。实际系统中出现故障的形式多种多样，本文只研究其中的 2 种故障形式：随即失效和恶意攻击。

1）随机元件攻击。包括由设备故障、自然灾害（如地震、海啸等）或简单的人为事故（如错误配置）引起的故障，发生的位置通常不确定，可通过随机移除一定比例的节点来模拟这种故障。本文采用连续攻击模式，具体攻击策略：依次随机删除节点，每次删除都会引发级联故障，重复此过程，直至删除规定节点比例。

2）恶意目标攻击。通过攻击系统的脆弱部分来最大限度地破坏相互依存网络系统。要进行这样

的攻击，攻击者必须拥有关于目标系统的一些先验知识，例如拓扑及其相互依存关系的信息。从逻辑上讲，攻击者会攻击被认为对系统运行最重要的节点，目的是造成最大的破坏。假设攻击者根据节点的重要性按降序对节点进行排序，然后按降序攻击系统，具体描述如下：

①高度数节点攻击，即将节点按度数降序排列，依次删除高度数节点，每次删除都会引发级联故障，重复此过程，直至删除规定节点比例；

②高介数节点攻击，即将节点按介数降序排列，依次删除高介数节点，每次删除都会引发级联故障，重复此过程，直至删除规定节点比例。

3.2 信息网络结构及耦合模式

随着智能电网的发展，配电网网络拓扑也由传统配电网辐射状结构向新的网络拓扑进化。分析新一代配电网的网络拓扑结构，探索不同信息网络拓扑和网络耦合方式在不同攻击策略下的网络脆弱性，选择与新一代配电网结构相匹配的具有强鲁棒性的信息网络拓扑结构，具有重要的现实意义。本文讨论信息网络结构及耦合模式对相互依存系统脆弱性的影响，采用无标度网络（barabási-albert scale-free，BA）[20]、小世界网络（watts-strogatz small-world，WS）[21]这 2 种经典类型网络，信息网络与配电网之间的耦合模式也分为随机和同配性耦合。

4 仿真分析

区别于传统配电网，本文主要研究具有新一代智能配电网特性的 CPDS 系统，在经典配电系统案例 PG&E69 节点系统的基础上进行改进，改进后的拓扑如图 4 所示，其中方块节点表示等值电源节点，蓝圆圈节点表示等值负荷节点，支路和节点的潮流限值设置为初始潮流的 1.5 倍。信息网络容限系数设置为 $\alpha = 0.5$。本文以存活节点比率作为耦合网络的脆弱性指标，在不同信息网络耦合模式下，分析不同的攻击方式对同一模式结构、同一种攻击方式对不同模式结构的脆弱性结果。为了结果的普遍性，本文生成 20 个不同耦合模式的信息网，统计展示 20 个 CPDS 网络的平均脆弱性结果。

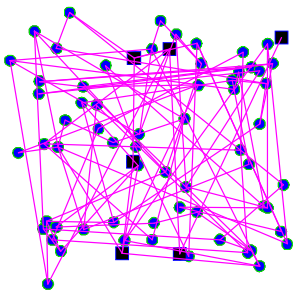

图 4 改进的 PG&E69 节点系统拓扑网络模型

Figure 4 Improved PG&E69 node system topology network model

4.1 攻击模式分析

现有的模型存在一定的不足，实际电网中的孤岛运行情况并没有被考虑，最大连通子集网络规模无法反映相依网络脆弱性的变化。不同攻击策略时的网络脆弱性分析如图 5 所示。

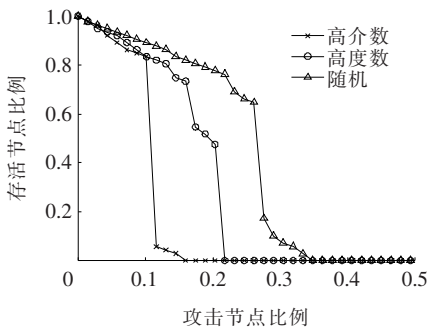

图 5 不同攻击策略时的网络脆弱性

Figure 5 Network vulnerability when different attack strategies

由图 5 可知，随着攻击节点比例的增加，存活节点数逐渐降低，并且当攻击节点数达到一定比例时，存活节点比例迅速减小，即随着攻击节点比例的增加，网络逐渐裂解为互不连通的子图，当电源节点全部受到攻击或者所有子图均失去与电源节点的连接时，整个网络陷入瘫痪状态。对比 3 种攻击模式，蓄意攻击相比于随机攻击模式，后果更严重，这是因为蓄意攻击一般是攻击网络重要的节点，相比于随机攻击更有目标性，破坏性更加严重。其中，蓄意攻击中的高介数节点攻击比高度数节点攻击更严重，即高介数节点攻击对 CPDS 相依网络系统有最严重的破坏性。

不同攻击模式下网络完全解列时的平均攻击节点比例如表 1 所示，可知高介数节点攻击使网络完

全解列时的攻击节点比例仅为 0.159，攻击比例最低，随机节点攻击使网络完全解列的攻击节点比例最高，可达 0.348。为抵抗外界的攻击，应着重保护高介数电力节点，其次是保护高度数电力节点。

表 1　网络解列时的攻击节点比例

Table 1　The proportion of attack nodes when the network is delisted

不同攻击模式下的攻击节点比例		
随机节点	高度数节点	高介数节点
0.348	0.217	0.159

4.2　信息网络结构分析

信息网络结构影响系统的脆弱性，分析不同信息网络面对各种攻击模式时的脆弱性，选择最优的信息网络结构特性，对于改善耦合系统的脆弱性有重要的意义。不同信息网络面对各种攻击模式时的脆弱性结果如图 6 所示，可知在 3 种攻击模式下，具有 WS 小世界特性的信息网络的耦合系统的鲁棒性强于具有 BA 无标度特性的信息网络的耦合系统。从图 6 也可以得出，高介数节点攻击具有最强的破坏性。

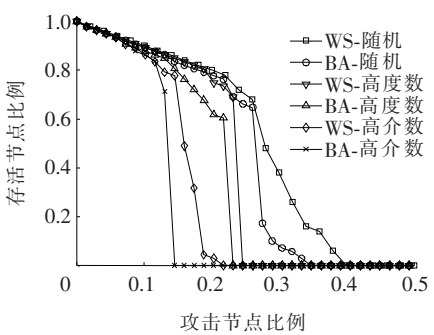

图 6　不同信息网络在不同攻击模式下的脆弱性

Figure 6　Vulnerability of different information networks in different attack modes

不同信息网络结构时的 CPDS 系统在不同攻击模式下，网络完全解列时的平均攻击节点比例如表 2 所示，可知对于 2 种不同的信息结构，高介数节点攻击使网络完全解列时的攻击节点比例最低，随机攻击使网络完全解列的攻击节电比例最高，与前面的分析结果一致，对比 2 种信息网络结构可知，当信息网络具有 WS 小世界特性时，CPDS 系统鲁棒性优于 BA 无标度特性的信息网络。

表 2　不同信息网络网络解列时的攻击节点比例

Table 2　The proportion of attack nodes when different information network networks are de-listed

节点攻击模式	WS-攻击比例	BA-攻击比例
随机	0.400	0.348
高度数	0.246	0.232
高介数	0.217	0.145

4.3　耦合模式分析

不同的耦合模式导致耦合系统的鲁棒性不同。随机耦合模式(random coupling mode，RC)和同配性耦合模式(degree coupling mode，DC)在 3 种不同攻击模式下的系统脆弱性如图 7 所示。

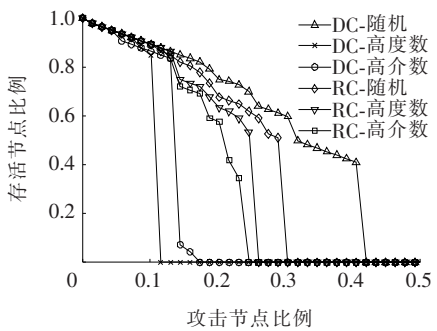

图 7　不同耦合模式下 3 种攻击模式下的系统脆弱性

Figure 7　System vulnerability in three attack modes in different coupling modes

由图 7 可知，不同的系统耦合模式对不同的攻击方式表现出来的鲁棒性不同，同配性耦合模式对随机攻击的鲁棒性最强，但对高度数攻击和高介数攻击的鲁棒性很弱，这是因为目标攻击首先攻击重要节点，而同配性耦合是将重要的节点耦合到一起，所以目标攻击会对系统造成严重的影响。对于随机耦合，高介数节点攻击对系统造成的危害最严重，这与前面的分析一致，值得注意的是，高度数节点攻击和高介数攻击对系统造成的影响差别不大，这说明高度数节点与高介数节点有一定的相关性，即高度数节点是高介数节点的可能性很大，从高度数耦合系统的高度数节点攻击和高介数节点攻击结果也可以验证这一点。

不同耦合方式在不同攻击模式下，网络完全解列时的平均攻击节点比例如表 3 所示，可知在 2 种耦合模式下，高介数节点攻击使网络完全解列时的攻击节点比例最低，随机攻击使网络完全解列的攻

击节电比例最高,与前面的分析结果一致。对比 2 种耦合模式可知,同配性耦合模式对于随机攻击具有最强的鲁棒性,攻击节点比例可达 0.420;随机耦合模式对于蓄意攻击相比于同配性耦合具有更高的鲁棒性。

表 3 不同耦合模式下网络解列时的攻击节点比例

Table 3 The proportion of attack nodes when the network is delegated in different coupling modes

节点攻击模式	DC-攻击比例	RC-攻击比例
随机	0.420	0.304
高度数	0.116	0.261
高介数	0.174	0.246

5 结语

当今智能电网的发展越发受到世界关注,随着电力与信息通信系统相互融合的逐步加深,对电力通信耦合网的组成特性研究和脆弱性的分析也就变得特别关键。本文通过研究实际 CPDS 耦合系统网络元件的功能特性和工作特点,解决了以往在运用较复杂网络建立参考模型时出现的缺陷,并基于电网拓扑,建立出更符合实际情况的 CPDS 耦合网络模型。考虑各种元件的失效规律、各种元件之间的相互作用以及电力网及信息网络中的动态运行特性,建立 CPDS 耦合网络的连锁故障模型。通过分析不同攻击模式下网络的脆弱性结果,可知蓄意攻击中的高介数节点攻击具有最强的破坏性。本文通过分析信息网络结构和耦合模式对 CPDS 相依网络系统脆弱性的影响,得出具有小世界特性的信息网络可以使 CPDS 相依网络系统具有最强的鲁棒性,并且同配性耦合模式对随机攻击模式具有很好的鲁棒性,但对于蓄意攻击则鲁棒性降低。

参考文献:

[1] 张显,史连军. 中国电力市场未来研究方向及关键技术[J]. 电力系统自动化,2020,44(16):1-11.
ZHANG Xian, SHI Lianjun. Future research areas and key technologies of electricity market in China[J]. Automation of Electric Power Systems, 2020, 44(16): 1-11.

[2] KÄMPFER S, MATOS P G, KÖRNER C, et al. The Ries Ling (Germany) and Inov Grid (Portugal) projects-Pilot projects for innovative hardware and software solutions for Smart Grid requirements[C]//CIGRE 2014, Paris, France, 2014.

[3] 刘世涛,杨凯,伍弘,等. 基于多维信息特征映射的电网风险区段路径匹配模型研究[J]. 高压电器,2020,56(9):87-93.
LIU Shitao, YANG Kai, WU Hong, et al. Research on path matching model of power grid risk section based on multidimensional information feature mapping[J]. High Voltage Apparatus, 2020, 56(9): 87-93.

[4] 邓科,张丽红,蔡昂,等. 基于分级调度算法的交换机路由信息处理技术[J]. 电网与清洁能源,2020,36(1):8-13.
DENG Ke, ZHANG Lihong, CAI Ang, et al. Routing information processing technology of switch based on hierarchical scheduling algorithm[J]. Power System and Clean Energy, 2020, 36(1): 8-13.

[5] 王云,刘东,陆一鸣. 电网信息物理系统的混合系统建模方法研究[J]. 中国电机工程学报,2016,36(6):1464-1470.
WANG Yun, LIU Dong, LU Yimin. Research on hybrid system modeling method of cyber physical system for power grid[J]. Proceedings of the CSEE, 2016, 36(6): 1464-1470.

[6] 刘文霞,徐慧婷,陈晔,等. 计及多维不确定性影响的配电信息物理系统优化规划方法[J]. 中国电机工程学报,2017,37(24):7205-7215.
LIU Wenxia, XU Huiting, CHEN Hua, et al. Cyber physical distribution system optimal planning considering the influence of multi-dimensional uncertainties[J]. Proceedings of the CSEE, 2017, 37(24): 7205-7215.

[7] 吴英俊,范婷婷,徐昊,等. 考虑天气影响的配电信息物理系统可靠性评估[J]. 中国电力,2020,53(4):59-68.
WU Yingjun, FAN Tingting, XU Hao, et al. Reliability evaluation of cyber-physical distribution network considering the impact of weather conditions[J]. Electric Power, 2020, 53(4): 59-68.

[8] SHAI S, DOBSON S. Effect of resource constraints on intersimilar coupled networks[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2012, 86

(2)：066120.

[9] CHEN Z H，WU J J. Robustness of interdependent power grids and communication networks：a complex network perspective[J]. IEEE Transactions on Circuit and System，2018，65(6)：115-119.

[10] STURARO A，SILVESTRI S，CONTI M，et al. A realistic model for failure propagation in interdependent cyber-physical systems[J]. IEEE Transactions on Network Science and Engineering，2020，7(2)：817-831.

[11] 李秋燕，王利利，张艺涵，等. 能源互联网多能流的耦合模型及动态优化方法综述[J]. 电力系统保护与控制，2020，48(19)：180-186.
LI Qiuyan，WANG Lili，ZHANG Yihan，et al. A review of coupling models and dynamic optimization methods for energy internet multi-energy flow[J]. Power System Protection and Control，2020，48(19)：180-186.

[12] CHAI W K，KYRITSIS V，KATSAROS K V，et al. Resilience of Interdependent communication and power distribution networks against cascading failures[C]// IEEE IFIP Networking Conference (IFIP Networking) and Workshops，Vienna，Austria，2016.

[13] PAGANI G A，AIELLO M. Towards decentralization：a topological investigation of the medium and low voltage grids[J]. IEEE Transactions on Smart Grid，2011，2(3)：538-547.

[14] 陈家璘，周正，李磊. 配电网信息物理系统异常检测研究[J]. 电测与仪表，2021，58(8)：185-189.
CHEN Jialin，ZHOU Zheng，LI Lei，et al. Research on anomaly detection of information physical system in distribution network[J]. Electrical Measurement & Instrumentation，2021，58(8)：185-189.

[15] MILANO F，VANFRETTI L，MORATAYA J C. An open source power system virtual laboratory：the PSAT case and experience[J]. IEEE Transactions on Education，2008，51(1)：17-23.

[16] ZHANG X，TSE C K. Assessment of robustness of power systems from a network perspective[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems，2015，5(3)：456-464.

[17] WU J，TSE C K，LAU F C M，et al. Analysis of communication network performance from a complex network perspective[J]. IEEE Transactions on Circuits and Systems I：Regular Papers，2013，60(12)：3303-3316.

[18] CHEN Z，WU J，XIA Y，et al. Robustness of interdependent power grids and communication networks：a complex network perspective[J]. IEEE Transactions on Circuits and Systems II：Express Briefs，2018，65(1)：115-119.

[19] 计丽妍，李存斌，贾雪枫，等. 多证据融合下电力信息物理系统风险评估研究[J]. 智慧电力，2021，49(10)：23-29.
JI Liyan，LI Cunbin，JIA Xuefeng，et al. Risk assessment of cyber-physical power system based on multi-evidence fusion[J]. Smart Power，2021，49(10)：23-29.

[20] BARABASI A L，ALBERT R. Emergence of scaling in random networks[J]. The Structure and Dynamics of Networks，2011，9781400841356：349-352.

[21] WATTS D J，STROGATZ S H. Collective dynamics of small-world networks[J]. The Structure and Dynamics of Networks，2011，9781400841356：301-303.