考虑自恢复能力的电力-通信网可靠性与经济性分析

罗紫航，关翔友，魏震波
（四川大学电气工程学院，四川 成都 610041）

摘 要： 随着泛在电力物联网的建设，电力网与通信网耦合程度加深，对新型发展趋势下的电力物理信息系统可靠性与经济性的研究具有十分重要的理论价值和实际意义。首先，系统性阐述了泛在电力物联网中感知层与网络层的运行特点及其对电力网与通信网耦合关系的影响；然后，运用相互依存网络理论建立了完全一一对应的电力CPS相依网络模型，并介绍了网络攻击方式以及通信节点的自恢复能力；最后，通过电力通信系统的网络攻击算例仿真，分析并对比4种攻击方式和恢复方式组合下的电力网可靠性和通信网经济性，由此为泛在电力物联网初期建设提出合理性建议。

关键词： 泛在电力物联网；网络攻击；自恢复能力；可靠性；经济性
中图分类号： TM73 **文献标志码：** A **文章编号：** 1003-6954(2019)05-0010-07
DOI:10.16527/j.cnki.cn51-1315/tm.2019.05.003

Reliability and Economy Analysis of Cyber Physical Power Systems Considering Self-recovery Ability

Luo Zihang, Guan Xiangyou, Wei Zhenbo
(College of Electrical Engineering, Sichuan University, Chengdu 610041, Sichuan, China)

Abstract: With the development of ubiquitous power internet of things (UPIoT), the power network and communication network are deeply coupled, and it is of great theoretical value and practical significance to study the reliability and economy of cyber physical power systems (CPPS) in new growing trend. Firstly, the running characteristics of perception layer and network layer of UPIoT and its influence on the coupling between power network and communication network are systematically described. Secondly, a completely one-to-one model of CPPS interdependent network is established based on the theory of interdependent networks, and the cyber-attack mode and self-recovery ability of communication nodes are introduced. Finally, the reliability of power network and the economy of communication network under the combination of four attack-recovery modes are analyzed and compared by cyber-attack simulation in CPPS. Therefore, some reasonable suggestions on the preliminary development of UPIoT are put forward.

Key words: ubiquitous power internet of things (UPIoT); cyber-attack; self-recovery ability; reliability; economy

0 引 言

近年来，国外和国内发生的多次大规模的电力供应中断事故，不少与电力-通信网发生的意外故障和网络攻击等相关。如2003年美国和加拿大“8·14”大停电中，电网自动风险扫描报警系统被意外闭锁，继而其主系统和后备系统服务器停机[1]；2015年乌克兰停电事件中黑客采用多种网络手段攻击了乌克兰国家电网[2]等国外停电事故。又如2008年湖南冰灾事件中架空光纤大量损毁，严重影响电网调度控制决策[3]等国内停电事故。现阶段中国致力于建设泛在电力物联网，旨在促进电力网络与通信网络的深度融合。因此，对电力-通信网络可靠性深入分析，同时考虑其经济性，对电力-通信网络的安全稳定运行有积极意义。

当前，电力系统安全稳定分析方法主要分为两类。一是基于传统还原论，通过事故仿真与暂态稳定性分析等手段，试图推演出事故的发展趋势；然而在当今电网大规模互联发展趋势下，其计算量过大，

且方法本身存在重视模型忽略结构的缺陷，因而不适用。二是以复杂网络理论[4-5]为核心，不但在一定程度上弥补了基于还原论方法的不足，且也可实现电力-通信系统可靠性分析。

作为复杂网络理论的延伸之一，相互依存网络[6]的研究在诸多领域得到应用，如生态系统[7]、硬件软件系统[8]等，同时在电力信息物理系统(cyber physical systems，CPS)[9]的脆弱性分析中也得到广泛应用。例如，文献[10]研究了低度数节点加边和分配策略对电力CPS相互依存网络的脆弱性的影响并仿真证明了其有效性。文献[11]在脆弱性分析中设定了3种攻击模式：随机节点攻击模式、高度数节点攻击模式和高介数节点攻击模式。文献[12]介绍了复杂网络抗毁性评价指标、级联失效模型和攻击方式，并扩展至相互依存网络，然后以电力系统为例介绍了相互依存网络的具体应用。

综上所述，考虑以电力网和通信网连接边的拓扑结构为出发点，采用完全一一对应的相依网络模型，建立两网耦合关系，研究通信网的多个节点在一次性遭受不同形式的网络攻击时(如随机节点攻击和高度数节点攻击)，其与电力网的耦合关系对电力网的可靠性的影响；同时考虑在多个节点具有不同形式的自恢复能力(如随机节点恢复和高度数节点恢复)的情况下，对电力网的可靠性和通信网的经济性进行分析。

1 泛在电力物联网的建设

从技术视角看，泛在电力物联网包含了感知层、网络层、平台层和应用层。其中感知层用于感知和采集物理世界中的事件和数据；网络层作为感知层和平台层的枢纽，起数据传输的作用；平台层实现采集数据的“一次采集，处处使用”；应用层接收并处理信息，做出业务决策。

电力物联网发展初期的重心在基础设施的建设上，即采用自下而上的发展思路，其主要任务是电力网络状态信息的采集、传输过程的加强和完善。所以感知层和网络层的建设显得尤为重要。现以感知层和网络层为例，分析泛在电力物联网在建设初期的2个特点。

1.1 传感器的两极效应

在电力系统各个环节，如输电网、配电网等层面，各种传感设备实现了电力系统的物物相联，同时采集大量的信息。一方面，传感器提高了所采集信息的丰富性和冗余性，为调度自动化系统提供更详细和更可靠的信息支持；另一方面，传感器难以保证信息的安全性，网络攻击者可借助传感器等泛在电力物联网的底层设备，对通信网络进行破坏性网络攻击。该类故障会通过两网耦合边界渗透到电力网中，导致调度系统失去对电力网的可观性和可控性，若此时电网发生大规模级联事故，会造成系统难以估量的损失。

1.2 5G通讯技术的应用

先进通信技术的应用提高了通信网对电力网的可观性和可控性。5G技术因其高带宽、低延迟的特性得以快速发展，也将成为泛在电力物联网的主要通信形式。同时5G技术可能在无线通信技术中出现类似于不停电电源(uninterrupted power supply，UPS)相似功能的不停传递信源[13]，即在一种形式下的通信网络(如光纤通信)中断，可以短时间内建设另一条无线通信网络(如5G通信)，以保证数据传输的实时性和可靠性，这种特性可以称为自适应通信技术或者自恢复通信技术[14]。自恢复通信技术的使用虽然能够提高电力系统的可靠性，但是受到通信网络的经济性制约。

2 电力CPS相依网络模型及分析

相互依存网络起源于复杂网络理论，也被称为网络的网络(networks of networks，NON)[15]、耦合网络(coupled networks)[16]或多层网络(multiplex/multilayer networks)[17]。

基于电力网和通信网的拓扑结构，将其分别表示为一个无权无向图G_P和G_C，每个网络可以表示为边和节点的集合$G=(V,E)$，$V=\{1,2,\cdots,N\}$表示网络的节点集合，$E=\{e_{ij}\}$表示网络的边集合；$\boldsymbol{A}=(a_{ij})\subset\boldsymbol{R}^{N\times N}$，为网络的邻接矩阵，且$a_{ij}=1\Leftrightarrow e_{ij}=(i,j)\subset E$，否则，$a_{ij}=0$。

与复杂网络相比，相互依存网络存在2种边[18]：1)连接边(connectivity link)，表示通信线路或者电力线路；2)依存边(dependency link)，表示电力网和通信网耦合节点间的信息和能量交互。依存边包括以下2种：1)单向依存边，用“→”表示；2)双向依存边，用“↔”表示。网络间的依存边集合$\boldsymbol{E}_D$

包括了电力网和通信网之间的能量依存和信息依存。$\boldsymbol{E}_{\mathrm{D}}=\{\boldsymbol{E}_{\mathrm{C-P}},\boldsymbol{E}_{\mathrm{P-C}}\}$，式中 $\boldsymbol{E}_{\mathrm{C-P}}$ 为通信网依存于电力网的依存边矩阵。$\boldsymbol{E}_{\mathrm{C-P}}(u,v)=1\Leftrightarrow V_{\mathrm{P}}(v)\rightarrow V_{\mathrm{C}}(u)$，表示通信节点 u 的正常运行需要电力节点 v 的支持，否则 $\boldsymbol{E}_{\mathrm{C-P}}(u,v)=0$，$\boldsymbol{E}_{\mathrm{P-C}}$ 同理。

将会使用的复杂网络基本概念如下：

1) 节点数 N：电力网或者通信网中站点数。

2) 边数 M：输电线路或者通信线路的数目。

3) 度数 k：站点连接的连接边的边数。

4) 平均度数 $<k>$：每个站点连接边数的平均值。

$$<k>=\frac{2M}{N} \tag{1}$$

作为电力 CPS 领域研究方法的分支之一，电力 CPS 的节点和边的保护策略，对电力网和通信网的耦合关系下的电网可靠性有一定的改善。

2.1 建立电力网和通信网模型

在输电系统中，通过光纤线路连接的通信网包括采集设备和计算设备等；通过输电线路连接的电力网包括发电机组、变压器、综合负荷等。对于通信网来说，网络攻击者发动的网络攻击导致与发电厂或者变电站远程终端设备（remote terminal unit，RTU）（通信节点）相连接的所有光纤线路（通信连接边）失效；同时定义其为通信网失联节点，失联节点的度为 0，由于调度中心的遥控和遥调命令无法下达给该通信节点，从而失去对对应的电力节点的可观性和可控性。对于电力网来说，如果发电厂和变电站（电力节点）无法调节发电机出力或者切除部分综合负荷，那么变电站相连的输电线路（电力连接边）可能会出现过负荷情况，结果导致继电保护装置动作，使输电线路断开，潮流可能发生大规模转移。

按照现行的规程规章，光纤通信网络常常随输电线路铺设，在变电站就地安装 RTU 等装置，因此电力网和通信网在地理位置上具有高度的拓扑相似性。同时，电力网和通信网在拓扑结构上具有网状网络结构，且都具有无标度特性，即节点的度服从幂律分布特性[19]。

$$P(k)=ck^{-\lambda} \tag{2}$$

式中：$P(k)$ 表示网络中节点度数为 k 的节点所占的比例；c 为系数；λ 为幂律值。

2.2 建立电力 CPS 相依网络模型

电力 CPS 是电力网和通信网两网耦合而成的相互依存网络。两网耦合中的 RTU 的遥控、遥调、遥测和遥信等实现电力网依存于通信网，为调度系统完成监视控制和数据采集（supervisory control and data acquisition，SCADA）以及高级应用功能奠定基础，同时 RTU 等设备接收来自电力网的电力支持，实现通信网依存于电力网，即通过网间节点的耦合关系实现信息和能量的传递。

但是考虑到通信节点装有备用柴油发电机组或者不停电电源（UPS）等应急供电设备，因此通信节点足以应付数小时的短期停电，所以在相互依存关系中不考虑能量的传递，即依存边考虑为单向依边，电力网依存于通信网。

对电力网和通信网采用完全一一对应的相依网络模型：电力网和通信网的节点数分别设为 N_{P}、N_{C}，且 $N_{\mathrm{P}}=N_{\mathrm{C}}$，并且一个电力节点只与地理位置重合的一个通信节点通过单向依存边连接。

在通信线路中，传输信息误码率极低的前提下，只要通信节点不发生故障，对应的电力节点在理论上也不会发生故障，所以电力 CPS 只考虑监测控制，不考虑数据采集，即采集和传输的信息正确率为 100%。

电力节点对应的通信节点发生网络攻击时，该通信节点的所有连接边将会断开，而与电力节点连接的单向依存边不会失效。如果该通信节点处于未失联状态，那么则可以认为该电力节点具有可观性和可控性，不会发生过负荷等故障；如果该通信节点处于失联状态，那么则可以认为该电力节点不具有可观性和可控性，有一定概率会出现一条连接边断开的情况，从而导致电力网的大停电事故概率增加。图 1 为电力信息 – 物理相互依存网络。

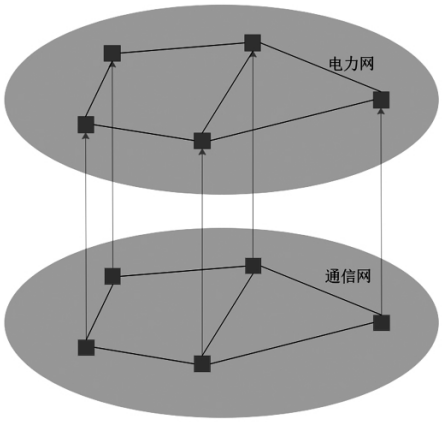

图 1 电力信息 – 物理相互依存网络

如图 1 所示，电力 CPS 相依网络模型考虑如下：

1) 在输电网层面，将电力系统变电站及其通信系统分别认为是电力节点和通信节点，电力节点注入功率，通信节点注入信息；

2) 电力系统的输电网络认为是电力网的连接边，通信系统的传输网络认为是通信网的连接边；

3) 不考虑电力网和通信网的连接边的自环和重边；

4) 不考虑通信网设备和线路的容量，认为电力网设备和线路的容量有限；

5) 相互依存关系考虑为单向依存，即使用单向边“→”表示，由通信节点指向对应的电力节点。

2.3 建立攻击方式和自恢复方式

网络攻击(cyberattack)是指任何一种破坏网络“保密性”“完整性”和“可用性”安全目标的恶意攻击行为[20]。在电力 CPS 中的网络攻击是以破坏或降低电力 CPS 功能为目的，在未经许可情况下对通信系统和控制系统行为进行追踪，利用电力信息通信网络存在的漏洞和安全缺陷对系统本身或资源进行攻击[21]。

泛在电力物联网的建设，如果通过无线网络(如 5G 通信技术实现)使部分通信节点具有自恢复能力，即如果通信节点转变为失联节点，通过自恢复能力使其与另一些具有自恢复能力的通信节点之间建立新的连接边。其本质上是一种通过实时的加边策略改变通信网自身的拓扑结构，使之处于一种动态的过程，从而改变电力网的可靠性，即具有自恢复能力的通信节点数量与受网络攻击通信节点数量的平衡。下面主要讨论各种攻击方式和自恢复方式的形式。

2.3.1 攻击方式

来自感知层外的网络攻击者一次攻击 n_A 个通信节点($n_A \leqslant N_C$)，n_A 由通信节点个数 N_C 及攻击百分比 $a\%$ 决定，即

$$n_A = N_C \times a\% \tag{3}$$

攻击方式主要有 2 种：1) 随机节点攻击，每一个通信节点被攻击的概率是均匀的；2) 高度数节点攻击，度数较高的通信节点会被优先攻击，即按照度数从大到小排列，优先选择度数较大的通信节点攻击。同时认为网络攻击具有明确性和破坏性，即不可能两次或多次攻击同一个通信节点，且网络攻击成功率为 100%。定义电力节点 i 与相邻度数最大节点 j(若存在两个及以上，也只选择其中的一个)之间的连接边失效概率为 P，失效概率由该电力节点相连的节点的度作为衡量指标，其值越大，则失效概率越大。

$$P = \frac{D_{ij}}{D_{i\Sigma}} \tag{4}$$

式中：D_{ij} 为与节点 i 相连的节点 j 的度；$D_{i\Sigma}$ 为与节点 i 相连的所有节点的度之和。

以攻击通信节点触发电力－通信网故障开始，考虑事件发生顺序如下：

1) 来自互联网的网络攻击者一次攻击 n_A 个通信节点，导致 n_A 个通信节点的所有连接边失效；

2) 网络攻击导致所有失联通信节点通过单向依存边使对应的电力网的电力节点的一条连接边可能失效；

3) 网络攻击结束。

2.3.2 自恢复方式

通信节点中的自恢复节点为 n_R 个，$n_R \leqslant N_C$，n_R 由通信节点个数 N_C 及恢复百分比 $r\%$ 决定，即

$$n_R = N_C \times r\% \tag{5}$$

自恢复节点具有性质如下：在网络攻击发生后，自恢复节点识别出通信网络遭受网络攻击，通过自恢复能力使其与具有自恢复能力的其他通信节点建立新的连接边，在一定程度上，改善了通信网遭受网络攻击后的拓扑结构。自恢复方式有随机节点恢复和高度数节点恢复两种恢复方式。随机节点恢复是指随机选择 n_R 个通信节点作为自恢复节点，自恢复节点之间建立连接边。高度数节点恢复是指优先选定攻击前度数较高的 n_R 个通信节点作为自恢复节点，自恢复节点之间建立连接边，即按照攻击前度数从大到小排列，优先选择度数较大的通信节点恢复。

以攻击通信节点触发电力－通信网故障开始，考虑事件发生顺序如下：

1) 来自互联网的网络攻击者一次攻击 n_A 个通信节点，导致 n_A 个通信节点的所有连接边失效；

2) 选择 n_R 个通信节点作为自恢复节点，使自恢复节点间建立连接边；

3) 网络攻击导致所有失联通信节点通过单向依存边使对应的电力网的电力节点的一条连接边可能失效；

4) 网络攻击结束。

同时，考虑以下 4 种攻击方式和恢复方式的组合：1) 随机节点攻击，随机节点恢复；2) 随机节点攻

击,高度数节点恢复;3) 高度数节点攻击,随机节点恢复;4) 高度数节点攻击,高度数节点恢复。

2.4 可靠性和经济性分析

电力网的可靠性在这里定义为通信网遭受攻击后的电力网的潮流交换能力。定义 P_R 为通信网遭受网络攻击结束后的电力网连接边占攻击开始前的电力网连接边的百分数。

$$P_R = \frac{E_{P2}}{E_{P1}} \times 100\% \tag{6}$$

式中: E_{P1} 为网络攻击开始前电力网连接边条数; E_{P2} 为网络攻击结束后电力网连接边条数。

通信网的经济性在这里定义为保证电力网的可靠性不小于 95% 时,通信网的恢复百分比 $r\%$ 的大小,其值越小则其经济性就越好。

3 算例仿真

生成一个初始节点数为 5 的随机网络,经过网络演化,生成节点数为 200 的无标度网络,其系数 c 为 0.698 8、幂律值 λ 为 2.267,如图 2 所示,节点的度 k 服从幂律分布特性,$P(k)$ 表示网络中节点度数为 k 的节点所占的比例。

$$P(k) = 0.6988k^{-2.267} \tag{7}$$

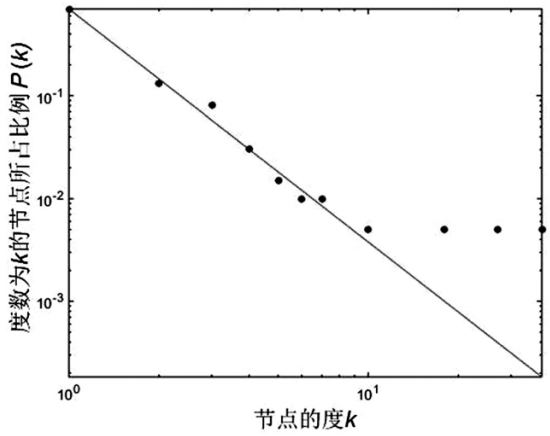

图 2 无标度网络的幂律分布特性

将该无标度网络同时作为电力网和通信网,并建立完全一一对应关系的相互依存网络模型。

3.1 随机节点和高度数节点攻击

图 3 为随机节点和高度数节点攻击下的电力网可靠性图。

如图 3 所示,随着网络攻击者对通信网的网络攻击范围扩大,通信网中失联节点数目也会增加,电力网中的连接边的断开数量呈现增加的状况,因此,电力网的可靠性指标 P_R 呈现下降的趋势。在攻击百分比 $a\% = 0$ 的情况下,电力网可靠性指标 $P_R = 1$; 在攻击百分比 $a\% = 100\%$ 的情况下,随机节点攻击和高度数节点攻击基本上不存在区别,电力网可靠性指标 P_R 介于 0.89 ~ 0.9。在攻击百分比 $a\%$ 超过 30% 以后,电力网中的连接边断开数量增加的趋势下降,电力网可靠性指标 P_R 趋于收敛。

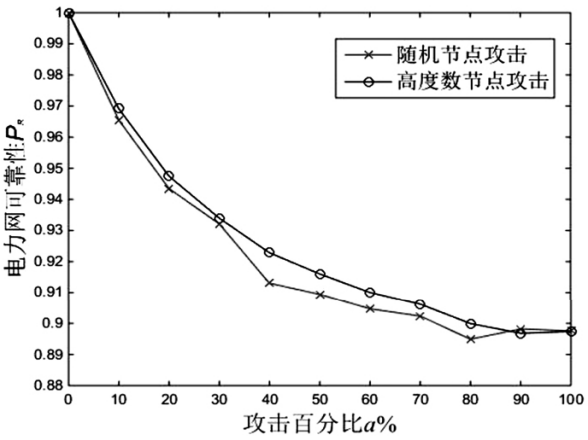

图 3 随机节点和高度数节点攻击下的电力网可靠性

同时由图 3 可知,在攻击百分比 $a\%$ 较小或较大时,通信网节点攻击类型对电力网的可靠性的影响基本相同,而在攻击百分比 $a\%$ 在 50% 左右时对电力网的可靠性的影响有较明显的区别。随机节点攻击相比于高度数节点攻击对电力网可靠性威胁更大,即从通信网的网络边缘发起的网络攻击对电力网的线路故障具有更明显的作用,因为高度数节点在通信网中得到有效的保护,在发生网络攻击时,该电力节点的输电线路因过负荷断开而失效的概率较其他边缘节点低。

总之,在通信网高度数节点得到有效保护的情况下,也要注重对通信网中的边缘节点的保护,采取有效措施如加边策略、节点保护策略等,可以有效地提高电力网的可靠性。

3.2 随机节点恢复

随机节点恢复是指随机选择 n_R 个通信节点作为自恢复节点,自恢复节点之间建立连接边。对于随机节点攻击和高度数节点攻击分别使用随机节点恢复,以攻击百分比 $a\%$ 为参变量,恢复百分比 $r\%$ 为自变量,分析电力网的可靠性和通信网的经济性,其仿真结果如图 4 和图 5 所示。

如图 4 和图 5 所示,随着自恢复节点数目增加,

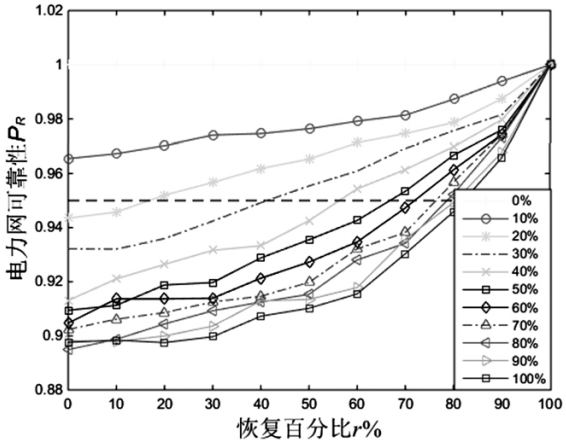

图 4　随机节点攻击后随机节点恢复的电力网可靠性

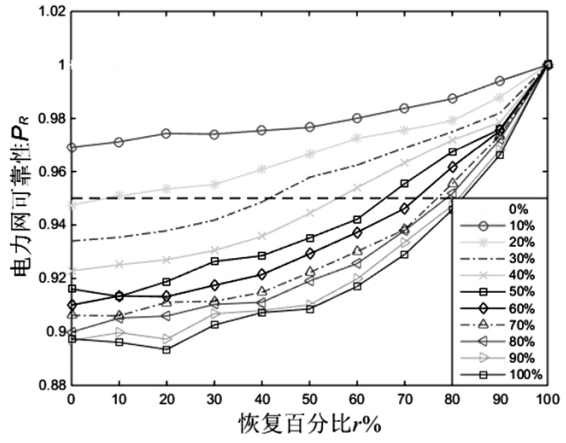

图 5　高度数节点攻击后随机节点恢复的电力网可靠性

通信网的网络攻击范围不变的情况下，通信网中失联节点数目将可能会减少，电力网中的连接边的断开数量呈现下降的状况，因此，电力网的可靠性指标 P_R 呈现增加的趋势。

在恢复百分比 $r\% = 0$ 的情况下，电力网可靠性指标与图 3 中随机节点攻击和高度数节点攻击下的电力网可靠性相一致；在恢复百分比 $r\% = 100\%$ 的情况下，任何类型和任何程度的网络攻击都对电力网的可靠性无影响，因此，电力网可靠性指标 P_R 趋于收敛于 1。在受到随机节点攻击和高度数节点攻击后采取随机节点恢复的大体趋势相一致。

由图 4 和图 5 可以获得关于经济性的指标，图中虚线为 $P_R = 0.95$。在受到网络攻击，攻击百分比 $a\% \geqslant 20\%$ 时，电力网络的可靠性指标 P_R 下降至 95% 以下。为保证电力网在受到网络攻击后的可靠性，现讨论自恢复设备投入量，即自恢复节点比例 $r\%$。

在保证电力网的可靠性的前提下，最小 $r\%$ 如表 1 所示。对于小规模的网络攻击（$a\% < 30\%$），随机节点恢复对高度数节点攻击较随机节点攻击更为经济；对于中等规模和大规模的网络攻击（$a\% \geqslant 30\%$）时，随机节点恢复对两种攻击方式的经济性较为一致。

表 1　随机节点恢复下 $P_R \geqslant 95\%$ 的最小 $r\%$

攻击百分比/%	最小恢复百分比/%	
	随机节点攻击	高度数节点攻击
0	0	0
10	0	0
20	16.8	7.3
30	41.2	41.5
40	56.2	55.9
50	66.8	65.8
60	71.9	72.4
70	76.3	76.8
80	78.6	78.8
90	80.5	81.2
100	82.1	82.0

总之，在保证电力网可靠性的前提下，为了经济性上的考虑，可以采用在通信网的边缘节点安装自恢复设备，以防御高度数节点的网络攻击。

3.3　高度数节点恢复

高度数节点恢复是指优先选定度数较高的 n_R 个通信节点作为自恢复节点，自恢复节点之间建立连接边。对于随机节点攻击和高度数节点攻击分别使用高度数节点恢复，以攻击百分比 $a\%$ 为参变量，恢复百分比 $r\%$ 为自变量，分析电力网的可靠性和通信网的经济性，仿真结果如图 6、图 7 所示。

如图 6 和图 7 所示，随着自恢复节点数目增加，通信网的网络攻击范围不变的情况下，通信网中失联节点数目将可能会减少，电力网中的连接边的断开数量呈现下降的状况，因此，电力网的可靠性指标 P_R 呈现增加的趋势，直到稳定在 $P_R = 1$。

在恢复百分比 $r\% = 0$ 的情况下，电力网可靠性指标与图 3 中随机节点攻击和高度数节点攻击下的电力网可靠性相一致；在恢复百分比 $r\% = 100\%$ 的情况下，任何类型和任何程度的网络攻击都对电力网的可靠性无影响，因此，电力网可靠性指标 P_R 趋于收敛于 1。特别是在高度数节点攻击后，采取高

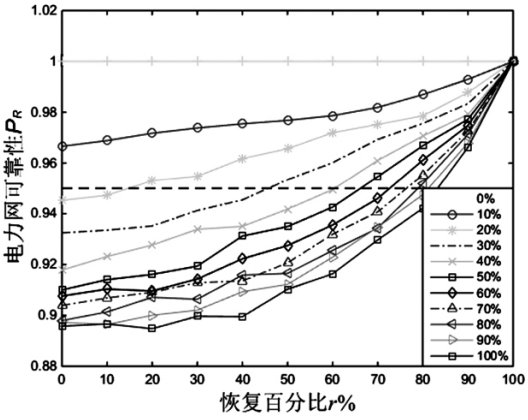

图 6　随机节点攻击后高度数节点恢复的电力网可靠性

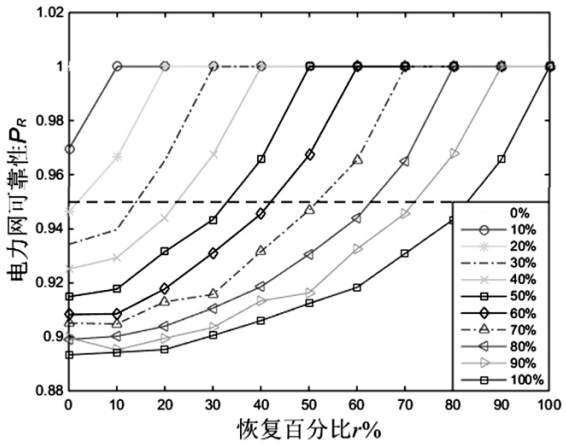

图 7　高度数节点攻击后高度数节点恢复的电力网可靠性

度数节点恢复具有明显的效果，在恢复百分比 $r\%<100\%$ 的情况下也能保证电力网的可靠性 $P_R=1$；在随机节点攻击后，采取高度数节点恢复的效果与随机恢复相近。

由图 6 和图 7 也可以获得关于经济性的指标，图中虚线为 $P_R=0.95$，在受到网络攻击时，攻击百分比 $a\%\geqslant 20\%$ 时，电力网络的可靠性指标 P_R 下降至 95% 以下，为保证电力网在受到网络攻击后的可靠性，现讨论自恢复设备投入量，即自恢复节点比例 $r\%$。

在保证电力网的可靠性的前提下，最小 $r\%$ 如表 2 所示，对于所有规模的网络攻击，高度数节点恢复对高度数节点攻击较随机节点攻击更为经济，特别是对于小规模和中等规模的网络攻击（$a\%\leqslant 70\%$）时，高度数节点恢复对高度数节点攻击的经济性显而易见。

总之，在保证电力网可靠性的前提下，为了经济性上的考虑，可以采用在通信网的高度数节点优先安装自恢复设备，以防御高度数节点的网络攻击。

表 2　高度数节点恢复下 $P_R\geqslant 95\%$ 的最小 $r\%$

攻击百分比/%	最小恢复百分比/%	
	随机节点攻击	高度数节点攻击
0	0	0
10	0	0
20	14.7	1.8
30	45.6	14.0
40	60.5	22.5
50	66.2	32.9
60	72.6	42.0
70	76.4	51.6
80	78.9	62.8
90	81.2	71.9
100	83.2	82.9

综上所述，P_R 是受网络攻击通信节点数目 n_A、攻击方式（随机节点攻击、高度数节点攻击）、恢复方式（随机节点恢复、高度数节点恢复）、自恢复节点数目 n_R 的影响。如果网络攻击通信节点数目 n_A 越多，P_R 越小，电力网越不可靠。如果自恢复节点数目越多，P_R 越大，电力网越可靠。被攻击通信节点 n_A 越多，那么自恢复节点 n_R 的需求也就越多，找到网络攻击通信节点 n_A 与自恢复节点 n_R 的平衡，使 P_R 满足一定的要求。

4　结　语

通过相依网络下的电力网和通信网的两网耦合模型，分析了两种网络攻击方式和两种恢复方式下的通信网通过耦合作用对电力网的可靠性的影响，并分析了电力网的可靠性与通信网的经济性。在面对随机节点攻击和高度数节点攻击时，随机节点攻击的威胁显得稍大。在电力系统通信网的安全防护中，除了注意高度数节点，如枢纽变电站、大型发电厂等，还需注意处于网络边缘的低度数节点，即在泛在电力物联网建设时期，边缘节点的保护显出一定的必要性。同时，高度数节点恢复在面临高度数节点攻击时，具有较好的经济性，即使面对随机攻击，在攻击范围很小时，也具有经济上的优越性。

（下转第 55 页）

供用电,2013(1):1-5.
[2] 李景禄,吴维宁,杨廷方,等. 配电网防雷保护的分析与研究[J]. 高电压技术,2004,30(4):58-59.
[3] 段绪金,齐飞,叶会生,等. 配网防雷现状与治理措施研究[J]. 电气应用,2015(S1):17-20.
[4] 黄清社,徐奔,彭利强,等. 10 kV 架空绝缘导线防雷保护的措施研究[J]. 高压电器,2010,46(12):32-35.
[5] 帅玲,毕涛,李荣兵. 有机材料在 10KV 绝缘横担上的应用与发展[J]. 山东工业技术,2014(14):93-93.
[6] 戴波涛,方向,田维. 10 kV 配电线路绝缘横担防雷实践研究[J]. 湖南电力,2017,37(S2):102-105.
[7] 何金良,曾嵘. 配电线路雷电防护[M]. 北京:清华大学出版社,2013:160-161.
[8] 韩晋平,王晓丰,马心良,等. 10 kV 架空绝缘导线雷电过电压与防雷综合措施研究[J]. 高电压技术,2008,34(11):2395-2399.

作者简介:

林礼健(1971),硕士研究生,高级工程师,硕究方向为电力与新能源。

(收稿日期:2019-06-10)

(上接第 16 页)

参考文献

[1] 苏盛,吴长江,马钧,等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术:2014,38(11):3115-3120.
[2] 童晓阳,王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化:2016,40(7):144-148.
[3] 陆佳政,张红先,方针,等. 湖南电力系统冰灾监测结果及其分析[J]. 电力系统保护与控制,2009,37(12):99-105.
[4] Watts D J,Strogatz S H. Collective Dynamics of Small-world Networks[J]. Nature,1998,393(6684):440-442.
[5] Barabasi A L,Albert R. Emergence of Scaling in Random Networks[J]. Science,1999,286(5439):509-512.
[6] Buldyrev S V,Parshani R,Paul G,et al. Catastrophic Cascade of Failures in Interdependent Networks[J]. Nature,2010,464(7291):1025-1028.
[7] Albrecht J, Berens D G, Jaroszewicz B, et al. Correlated Loss of Ecosystem Services in Coupled Mutualistic Networks[J]. Nature Communications, 2014,5:3810.
[8] 孟令中,陆民燕,黄百乔,等. 网络控制系统的连锁失效影响分析[J]. 合肥工业大学学报(自然科学版),2012,35(3):353-356.
[9] Sridhar S,Hahn A,Govindarasu M. Cyber-Physical System Security for the Electric Power Grid[J]. Proceedings of the IEEE,2012,100(1):210-224.
[10] 冀星沛,王波,董朝阳,等. 电力信息-物理相互依存网络脆弱性评估及加边保护策略[J]. 电网技术,2016,40(6): 1867-1873.
[11] 冀星沛. 基于相互依存网络理论的电力信息-物理系统结构脆弱性研究[D]. 武汉:武汉大学,2016.
[12] 董政呈,方彦军,田猛. 相互依存网络抗毁性研究综述[J]. 复杂系统与复杂性科学,2017,14(3): 30-44.
[13] 王亚非,胡四全,马力. 基于 GPRS 网络的调度备用通道[J]. 电力系统保护与控制,2009,37(16):80-83.
[14] 郭伟. 抗干扰、自适应、自组织、自恢复通信网技术[J]. 电子科技大学学报,1996,25(S3):304-308.
[15] Gao J,Li D,Havlin S. From A Single Network to A Network of Networks[J]. National Science Review,2014,1(3):346-356.
[16] Parshani R,Rozenblat C,Ietri D,et al. Inter-similarity between Coupled Networks[J]. EPL,2010,92(6):68002.
[17] Boccaletti S,Bianconi G,Criado R,et al. The Structure and Dynamics of Multilayer Networks[J]. Physical Reports,2014,544(1):1-122.
[18] Bashan A,Parshani R,Havlin S. Percolation in Networks Composed of Connectivity and Dependency Links[J]. Physical Review E,2011,83(5):05112.
[19] 胡海波,王林. 幂律分布研究简史[J]. 物理,2005(12):889-896.
[20] National Institute for Standards and Technology(NIST). Guidelines for Smart Grid Cyber Security: Vol. 3,Supporitive Analyses and References: NISTIR 7628[S],2010.
[21] 汤奕,陈倩,李梦雅,等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化,2016,40(17):59-69.

作者简介:

罗紫航(1997),本科生,研究方向为复杂系统及其理论、电力系统安全稳定分析;

关翔友(1994),硕士研究生,研究方向为复杂系统及其理论、电力系统安全稳定分析;

魏震波(1978),博士,副教授,研究方向为复杂系统及其理论、电力系统安全稳定分析与控制及电力市场。

(收稿日期:2019-07-09)