文章编号: 1001-0920(2017)03-0411-08 DOI: 10.13195/j.kzyjc.2016.0311

DoS攻击下电力网络控制系统脆弱性分析及防御

王轶楠[1†], 林彦君[1], 李 焕[2], 林志赟[1], 徐文渊[1], 杨 强[1], 颜钢锋[1]

(1. 浙江大学 电气工程学院, 杭州 310007; 2. 国家电网 智能电网研究院, 北京 102209)

摘 要: 考虑DoS攻击对电力信息物理系统的影响,提出一种电力网络控制系统脆弱节点的检测方法和防御策略,采用分布式控制架构设计传感器和RTU的传输路径.通过求解最稀疏矩阵优化问题,提出一种识别并保护电力通信网脆弱节点和边的方法,保证系统实现安全稳定运行.进一步提出一种可以抵御DoS攻击的电力网络控制系统拓扑设计方法,研究系统遭受DoS攻击时能恢复稳定的电力网络控制系统拓扑连接方式. IEEE 9节点系统用于仿真验证,充分验证了算法的可行性和可靠性,并针对该9节点电力网络控制系统,给出了具体的网络攻击防御策略.

关键词: DoS攻击; 电力网络控制系统; 脆弱性; 防御策略

中图分类号: TP273 **文献标志码:** A

Vulnerability analysis and countermeasures of electrical network control systems under DoS attacks

WANG Yi-nan[1†], *LIN Yan-jun*[1], *LI Huan*[2], *LIN Zhi-yun*[1], *XU Wen-yuan*[1], *YANG Qiang*[1], *YAN Gang-feng*[1]

(1. College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China; 2. Smart Grid Research Institute, State Grid, Beijing 102209, China)

Abstract: Considering the influence of denial-of-service(DoS) attacks on electrical cyber physical systems(ECPSs), this paper studies the problem of vulnerability analysis and countermeasure synthesis for electrical network control systems under DoS attacks. Distributed control and its features are considered for the design of transmission paths of sensors and remote terminal units(RTUs) based on automatic voltage regulators(AVR) of synchronous generators. An algorithm is proposed for identifying and protecting vulnerable nodes and lines in electrical network control systems by solving a problem of optimum sparse matrix. Countermeasures of electrical communication networks under DoS attacks are further studied. The proposed algorithms are validated on the IEEE 9-node system. Spectific advice and defending strategies against cyber attacks are given according to the algorithms.

Keywords: DoS attack; electrical network control systems; vulnerability; countermeasure

0 引 言

智能电网是将现代先进的通信技术、信息技术、传感测量技术、计算机技术和控制技术与电力物理网高度集成而形成的电力信息物理系统[1].智能电网的发展使得电力系统更加依赖于电力通信网的可靠运行[2-3].近年来,世界范围内频繁发生针对信息物理系统的重大信息安全事件,如2003年美国的蓝宝石(SQL Slammer)蠕虫病毒、2008年的波兰地铁系统入侵事故、2010年的“震网”病毒(StuxNet)、2011年美国伊利诺伊州城市供水系统入侵事故、2012年的“火焰”病毒(Flame)[4]以及最近乌克兰发生的恶意代码导致的大停电事故,都是由于信息网、通信系统受到网络攻击而引起的.因此,研究信息攻击下,电力网络控制系统的脆弱性和防御策略具有重要意义[5-6].

现有文献中提到的对电网实施网络攻击的类型主要包括:拒绝服务式(DoS)攻击[7]、重放攻击[8]和虚假数据注入攻击[9]等.文献[10]指出,网络攻击者可以隐蔽地通过篡改电网中的传感器或相量测量单元(PMU)等数据采集设备的数据,影响调度中心的决策,并由此提出电力网络控制系统的脆弱性.针对

收稿日期: 2016-03-17; **修回日期:** 2016-07-31.

基金项目: 国家自然科学基金面上项目(61471328); 国家电网公司科技项目(XXB17201400056); 国家863计划项目(2015AA05002).

作者简介: 王轶楠(1992–), 男, 博士, 从事智能电网信息物理系统的研究; 林志赟(1976–), 男, 教授, 博士生导师, 从事多智能体系统协调控制等研究.

†通讯作者. E-mail: 11410065@zju.edu.cn

信息攻击,有关电力网络控制系统的脆弱性和防御策略研究主要分为以下3类:

第1类研究基于复杂网络理论,从网络拓扑和模型的角度评估通信网的结构脆弱性.通过改变通信网的拓扑结构,文献[11-15]研究了随机网络、无标度网络和小世界网络结构下的电力网络控制系统脆弱性;文献[16]从网络效率的角度评估了电力网络控制系统的脆弱性.

第2类研究通过分析具体信息攻击的产生机理和对电网的影响方式,研究故障检测和防御方法.文献[17-18]针对虚假数据注入攻击,改进了传统的基于残差的电网状态检测算法,使得新算法可以在一定程度上检测到信息攻击并进行防御;文献[19]通过隔离技术,研究一种针对电网的非线性攻击类型.

第3类研究从信息攻击作用后果角度,研究大规模电网受到通信网络攻击后的脆弱性和防御策略[20].由于信息攻击的作用点为传感器节点或传输信道,作用效果为阻塞传输信道或篡改传输数据,因此文献[8]从信息攻击者的角度研究对电网成功实施网络攻击所应具备的条件,进而对网络施加物理保护;文献[17]提出增加节点传感器和PMU数量的方法,可以提高电网系统对信息攻击的识别能力,进而能够及时作出保护.

由于电力网络控制系统的结构特点及电力系统与电网二次设备的紧密联系,利用复杂网络的方法存在局限性.本文的研究属于第2类和第3类的研究范畴,结合同步发电机的自动电压控制方法,通过求解带约束条件的最稀疏矩阵优化问题,规划电力网络控制系统中传感器和RTU的数据和控制策略及传输路径,提高系统在信息攻击下的稳定性.基于电力系统广域分布式控制框架,识别并保护电力网络控制系统中脆弱节点和边,增强系统的自恢复性能.最后,根据优化问题得到最稀疏矩阵,提出一种可以抵御DoS攻击的电力网络控制系统拓扑设计方法.通过分析当前控制方式下控制系统节点和连接边的脆弱性,研究系统遭受DoS攻击时,能够使ECPS恢复稳定的电力控制网拓扑连接方式.最后将IEEE 9节点系统用于实验仿真,验证了所提出算法的可行性和可靠性.

1 ECPS建模

1.1 ECPS动力学模型

本文采用同步发电机的三阶动态方程[21],结合电网的潮流功率方程,建立电网物理系统模型.考虑发电机自动电压控制(AVR)策略[22],建立电网信息系统的控制模型.为了分析系统受到扰动情况下的稳定性,取电网运行的频率、相角、励磁电势的变化值作为系统状态变量,得到如下状态方程组:

$$\Delta\dot{\delta} = \Delta\omega, \tag{1}$$

$$M\Delta\dot{\omega} = -D\Delta\omega - \Delta P_e, \tag{2}$$

$$T_{do}^{'}\Delta\dot{E}_q^{'} = -\Delta E_q^{'} + (X_d - X_d^{'})\Delta I_d + \Delta E_f. \tag{3}$$

其中:δ和ω分别为发电机转子相角和频率,M为惯性系数,D为阻尼系数,P_e为电磁功率,$E_q^{'}$为发电机的q轴暂态电势,X_d为发电机的d轴等效电抗,$X_d^{'}$为发电机d轴等效暂态电抗,$T_{do}^{'}$为励磁绕组d轴暂态时间常数,E_f为励磁电动势.

考虑发电机电压控制和发电机励磁系统

$$\dot{z}_2 = -c_1 z_2 - c_0 z_1 + \Delta u, \tag{4}$$

$$\dot{z}_1 = z_2, \tag{5}$$

$$\Delta E_f = b_1 z_2 + b_0 z_1. \tag{6}$$

其中:b_0、b_1、c_0和c_1为电压控制和励磁系统传递函数变量,z_1和z_2为二阶控制器状态量,Δu为系统的控制输入.

综上,同步发电机的状态变量为

$$x_i = [\Delta\delta_i \ \ \Delta\omega_i \ \ \Delta E_{qi}^{'} \ \ z_{2i} \ \ z_{1i}]^{\mathrm{T}}.$$

对于系统输电线路建模,根据文献[23]提出的系统等效策略,等效后的电网系统的总线(i,j)特性可以用线端发电机i的d轴等效电枢电流I_{di}和电磁功率P_{ei}表示为

$$I_{di} = \sum_{j=1}^{N} E_{qi}^{'}[B_{ij}\cos(\delta_i - \delta_j) - G_{ij}\sin(\delta_i - \delta_j)], \tag{7}$$

$$P_{ei} = E_{qi}^{'}\sum_{j=1}^{N} E_{qj}^{'}[B_{ij}\sin(\delta_i - \delta_j) + G_{ij}\cos(\delta_i - \delta_j)]. \tag{8}$$

其中:N为系统中发电机总节点数,$i,j \in \{1,2,\cdots,N\}$,G_{ij}和B_{ij}分别为线路电导和电纳,$E_{qi}^{'}$为发电机暂态电势,δ为发电机转子相角.

1.2 ECPS分布式架构

本文建立的ECPS分布式控制框架模型为双层网络框架,如图1所示.将发电机、变压器和负载设备分类为电力物理网的节点,节点间无向实线为输电线,如图1中下层P平面A-E节点所示;与A-E节点一一对应虚线连接的上层C平面节点1-5为通信节点,通信节点属于电网二次设备节点,对所控制的物理节点起到“遥测、遥信、遥控”的作用.在通信网层面,

为了提高控制效率,减轻调度中心的调配压力,本文采用分布式控制框架,各通信网节点之间通过电压、电流互感器等数据采集装置收集电网运行数据,数据站间采用RTU设备实现无线通讯,如图1中双向虚线所示.

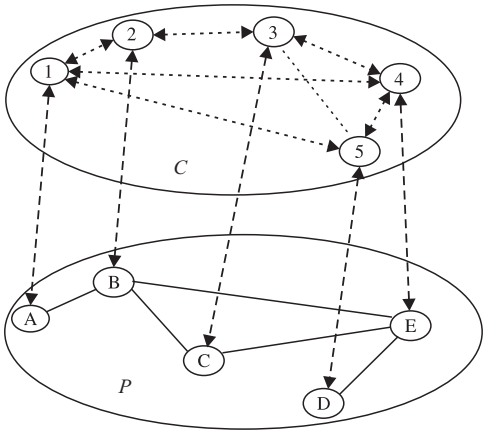

图 1　ECPS分布式框架

根据文献[24]提出方法线性化式(7)和(8),联立式(1)～(5)可得ECPS线性动态方程. 假设系统由N个物理节点构成,物理系统表述如下:

$$\dot{x}_i = A_{ii}x_i + B_{ii}u_i + \sum_{j\in N_i} A_{ij}x_j. \tag{9}$$

其中:x_i为节点i的状态变量;u_i为节点i的控制输入;N_i为节点i的邻居集,反映物理拓扑连接关系;矩阵A_{ij}反映节点i与j之间的物理耦合关系,即节点j的状态对节点i的影响.

设计分布式控制器

$$u_i = K_{ii}x_i + \sum_{j\in L_i} K_{ij}x_j. \tag{10}$$

本文假设系统的状态变量状态x_i可以直接由RTU、PMU装置测量获得. L_i反映了通信网拓扑,即节点i的通信邻居集. 因此,由N个发电机组成的ECPS的线性非时变模型可以表示为

$$\dot{x} = Ax + Bu, \tag{11}$$

$$u = -Kx. \tag{12}$$

其中:$x = [x_1, x_2, \cdots, x_N]^{\mathrm{T}}$, $u = [u_1, u_2, \cdots, u_N]^{\mathrm{T}}$, $A \in \boldsymbol{R}^{5N\times 5N}$, $B \in \boldsymbol{R}^{5N\times N}$.

2　电力网络控制系统的脆弱性研究

基于分布式控制框架,设计恰当的反馈控制器增益矩阵K,可以提高系统受到扰动下的稳定性和自恢复性,同时保证发电机处在能够承受的暂态过程变化范围内. 将矩阵K分块表示为方阵,用来识别电力通信网的脆弱节点和边. 在分块后的方阵K中,对角元素表示对发电机节点的控制;非对角元素反映通信网节点之间的信息交互. 因此,设计控制器增益矩阵K,通过分析对角元素,可以得到电力网络控制系统节点的脆弱性;分析非对角元素,可以得到电力网络控制系统边的脆弱性.

本章主要根据1.2节建立的ECPS线性微分方程,研究电力网络控制系统分布式控制器的通信方式,并设计算法识别电力网络控制系统的脆弱性.

2.1　分布式控制器设计

在电力系统中,通过传感器等二次设备采集到的物理节点的测量数据通常经过智能变电站节点汇总后传输到调度中心,调度中心通过决策将控制指令下达到发电机、变电站和断路器. 这样的信息传输过程存在传输数据量大、同步性差的特点.

为此,基于电网的运行方式,设计分布式电力通信网,考虑能够实现系统稳定的通信网最少RTU设备信息交互情形,即设计最稀疏的控制器矩阵K实现系统稳定. 通过分析该最稀疏控制器矩阵K,分析电力网络控制系统节点和边的脆弱性.

反馈控制器K可以表述为

$$K = \begin{bmatrix} K_{11} & K_{12} & \cdots & K_{1N} \\ K_{21} & K_{22} & \cdots & K_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ K_{N1} & K_{N2} & \cdots & K_{NN} \end{bmatrix} = K_{\mathrm{loc}} + K_{\mathrm{dist}}. \tag{13}$$

其中:K_{loc}表示对发电机节点的本地控制,K_{dist}表示对节点间信息交互边的控制. 控制器K_{loc}仅根据单个物理点的状态量进行控制,如图1中的虚实线所示. 控制器K_{dist}的设计反映在图1中为C平面,信息交互为虚点线所示.

求解最稀疏控制矩阵K,即要求分块矩阵K中有尽可能多的块为0,可通过对矩阵求解l_0范数实现,具体分为2步. 第1步计算矩阵K中每个分块矩阵的2范数,记$k'_{ij} = ||K_{ij}||_2, 1 \leqslant i,j \leqslant N$,得到控制邻接矩阵$K^*$;第2步计算$||K^*||_{l_0}$,此时得到的邻接矩阵即为要求的最稀疏控制邻接矩阵. 由于求解矩阵l_0范数在数学上是一个NP难问题,不能直接求解l_0范数,因此采用求解邻接矩阵K^*的l_1范数,得到近似优化解[25].

由上述分析, 得到优化控制问题

$$\min\ ||K^*||_{l_1};$$

$$\text{s.t. } \max\ \mathrm{Re}\{\lambda_i(A+BK)\} < 0,\ i = 1, 2, \cdots, N.$$

其中:w_0和p分别为同步发电机额定转速和极对数,Δf为电力系统正常运行情况下供电频率的允许

偏差.

注1 这里仅考虑电力控制网拓扑的最少连接数,并未考虑由于节点间距离不同而导致的通信信号衰减问题.

注2 限制条件保证的是电网系统的稳定性,即闭环系统全部特征根的实部都处在左半平面内.

注3 本文考虑的是通过设计控制拓扑实现系统的稳定性,而系统的瞬态响应问题可以通过设计控制器增益K实现,因此本文假设系统的瞬态过程都在合理的范围内.

解此优化问题,得到最稀疏控制邻接矩阵 K^* 的集合

$$S = \{K_l | l = 1, 2, \cdots, r\}, \tag{14}$$

其中r为集合S中元素的数量.

2.2 电力网络控制系统的脆弱性

基于2.1节得到的集合S,认为S中的每一个矩阵K_l所对应的电力通信网拓扑为稀疏拓扑关系,表示在该控制方式下,能够保持系统稳定的电力网络控制系统最少的信息交互方式. 在此拓扑关系下,每条连接都是必要的通信连接. 而对实际的电力控制网络设计时,需要以S中邻接矩阵K_l为基础,通过增加节点间的信息交互实现通信冗余,从而达到稳定控制,且具有一定的防御攻击效果.

本文定义电力网络控制系统的脆弱性是基于通信冗余和最稀疏拓扑的. 若一个节点控制信号或一条边的信息交互信号被阻断,控制系统不能通过修改K^*中其他不为零参数值保持必要的通信,使得系统稳定,则认为在这种控制方式下,该点或边的脆弱性较高;与之相反,若阻断一个节点控制信号或一条边的信息交互信号,系统通过修改控制器中其他不为零参数值,仍可以保持稳定,则认为该点或边的脆弱性较低.

具体从集合S中的K_l矩阵来说,K_l中出现非零元素位置的概率大小决定了系统的脆弱性程度. 当K_l中某一元素出现非零的概率较大,那么说明在该控制方式下,该点或边的通信被阻断,系统通过设计K^*中其他参数,系统能够再次实现稳定的概率较小. 因此基于本文的分析,电力网络控制系统的脆弱性可以通过统计S中矩阵K_l出现非零元素的概率衡量. 由前文假设可知,与电力物理网一一对应的电力通信网节点数量也为 N.

算法1 电力通信网脆弱性节点排序. 通过轮询的方式统计集合S中每个矩阵K_l非零元素出现位置的概率,排序电力网络控制系统节点和边的脆弱性. 具体步骤如下.

初始化: $G = \text{zeros}(N, N)$, $k = 0$
for $i = 1, 2, \cdots, N$
  for $j = 1, 2, \cdots, N$
    for $l = 1, 2, \cdots, r$
      if 构建的通信网拓扑在(i, j)间有通信连接
        then $k = k + 1$
        else $k = k$
      end if
    end for
    $G(i, j) = kk/r$, $kk = 0$
  end for
end for

注4 本文采用$K_l(i, j) \neq 0$的数学表达为判断“构建的控制网拓扑在(i, j)间有通信连接”的依据. 在实际数值计算中,由于计算误差的影响,不能保证$K_l(i, j)$严格等于0, 在实际的应用中,通常采用$K_l(i, j) \geqslant e$代替$K_l(i, j) \neq 0$的判别条件,其中e为误差量,可根据工程需求取$e = 0.001$.

注5 对角元素$K_l(i, i) \neq 0$,表示控制网对发电机节点的本地控制;非对角元素$K_l(i, j) \neq 0$,表示控制网节点间存在信息传递. 根据上述分析,G 中数值较大的元素表示该点或边较为脆弱.

由算法1得到的矩阵G,可以得出电力网络控制系统不同节点和边的脆弱性. 参照此结果,在设计控制器或实施安全保护时,应该给予足够重视. 对于通信节点的软件保护可包括防火墙保护、数据加密,物理保护包括隔离保护,降低这些节点的故障率和事故率,对于提高系统的稳定性和可恢复性有重要作用.

3 DoS攻击与防御

3.1 DoS攻击

本节主要研究拒绝服务(DoS)攻击[7]对电力网络控制系统所造成的影响. DoS拒绝服务攻击的作用对象是电力网络控制系统的通信信道,如馈线终端设备(FTU)、开闭所、环网柜智能终端(DTU)或远程终端单元(RTU)的遥测、遥信、遥控信道,其作用的效果都是阻断信道中的信息传输,进而影响式(11)中控制指令$u(t)$对动态系统的调控作用,以此造成电网的故障.

在本文提出的ECPS分布式架构下,对信息网通信造成的影响主要为:通信网(i, j)节点信道间发生

DoS攻击,通信传输被阻断,使得$K_l(i,j)=0$.

3.2 防御策略

算法2 防御DoS攻击下的控制网拓扑设计. 基于算法1中求得的矩阵G,通过增加信息交互边的方式(增加邻接矩阵K^*中不为零的元素数量),设计电力控制网拓扑,实现DoS攻击下的电力网络控制系统防御策略. 具体步骤如下.

Step 1: 初始化S, K_0, $k=0$;

Step 2: 生成矩阵集合$S'=\{K'_l|l=1,\cdots,r\}$,使得S中元素K_l与S'中元素K'_l对应,对应关系为

for $l=1,\cdots,r$
  for $i=1,\cdots,N$
    for $j=1,\cdots,N$
      if $K_l(i,j)\neq 0$
      then $K'_l(i,j)=1$
      else $K'_l(i,j)=0$
      end if
    end for
  end for
end for
for $l=1,\cdots,r$
  if K'_l中非零元素包含K_0全部非零元素位置
    then 将K'_l存入集合$S_{(K_0)}$中
  end if
end for;

Step 3: 计算集合$S_{(K_0)}$中元素个数为n_0;

Step 4: 对$S_{(K_0)}$中的元素依次作$C_{n_0}^2$、$C_{n_0}^3$、$\cdots$、$C_{n_0}^{n_0}$分组,并按照算法1分别计算G,则该组控制邻接矩阵$K_{t0}^*(t=1,2,\cdots)$中非零元素的位置与G中非零元素的位置相同;

Step 5: 生成有效的防御拓扑集合$K^{\rm def}$.

依照本文分析,对通信节点和边实施物理隔离保护或增加冗余信息传递边,都可以有效地抵御网络攻击,依据算法1中矩阵G的数值,给定物理隔离保护节点的位置,算法2可以求解能够抵御一定程度DoS攻击的最少信息交互通信拓扑连接关系.

算法2的设计思路为:

1) 依据给定的需要物理隔离的节点或边的位置关系邻接矩阵K_0,搜索最稀疏控制邻接矩阵集合S中元素,得到子集$S_{(K_0)}$,则$S_{(K_0)}$中每个邻接矩阵非零元素位置都包含K_0中全部非零元素的位置;

2) 假设集合$S_{(K_0)}$中元素个数为$n_0(n_0\geqslant 1)$,对$S_{(K_0)}$中的元素依次作$C_{n_0}^2$、$C_{n_0}^3$、$\cdots$、$C_{n_0}^{n_0}$分组,并按照算法1分别计算G,则该组控制邻接矩阵$K_{t0}^*(t=1,2,\cdots)$中非零元素的位置与G中非零元素的位置相同;

3) 该控制方式下,判断该通信连接拓扑K_{t0}^*是否可以抵御n_c点网络DoS攻击($n_c=1$时为单点网络攻击).

注6 本文定义邻接矩阵中的元素只有'0'和'1'两种. 如果电力网络控制系统中,信息网节点(i,j)间存在信息传递通道,那么$k_{ij}=1$,反之为0.

注7 本算法假设K_0中受物理隔离保护的通信网节点和边能够抵御DoS攻击.

注8 判断一个控制邻接矩阵$K_{t0}^*(t=1,2,\cdots)$是否可以抵御一定程度的攻击,是判断在此拓扑中,将K_{t0}^*中的任意不受物理保护的非零元素变为0,新的邻接矩阵$K_{t0}^{*'}$包含至少一种最稀疏控制邻接矩阵拓扑关系时,通过调整$K_{t0}^{*'}$对应的控制增益K的参数值可以实现系统的稳定.

注9 对于防御n_c点网络攻击($n_c>1$),在算法2中的Step 5,需要任意去掉n_c个非零元素,得到$K_{t0}^{*'}$,存在$K^{\rm test}=K_{t0}^{*'}-K'_l(1\leqslant l\leqslant r)$,其中$K^{\rm test}$的元素全为非负,则该$K_{t0}^*(t=1,2,\cdots)$为有效的防御拓扑. 因此,要抵御多点攻击时,需要设计连接更多的通信网信道,这将对信道带宽和传输速度提出更高要求.

4 仿真实验

本文以3机电力系统模型[26]为例(如图2所示),分析DoS攻击下的电力网络控制系统的脆弱性和相应的防御策略. 该系统包括发电机模型、电压自动控制的激励模型. 具体参数见文献[26]. 根据《供电营业规则》,本文考虑大范围系统情况,取$|\Delta f|\leqslant 0.2$ Hz,即$|\Delta w|\leqslant 0.6$ rad/s.

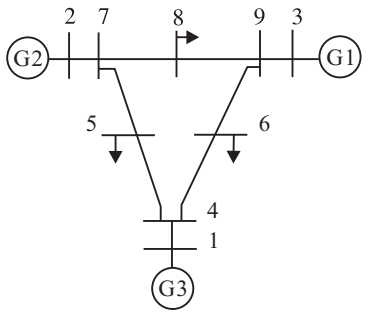

图2 电力系统3机模型

由系统方程(1)~(3),在电压自动控制方式下,有

$$B_{ii}=[0\ \ 0\ \ 0\ \ 1\ \ 0]^{\rm T},$$

$$B=\begin{bmatrix}B_{11}&0&0\\0&B_{22}&0\\0&0&B_{33}\end{bmatrix}^{\mathrm{T}}.$$

因此$B\in\boldsymbol{R}^{15\times3}$,设计$K\in\boldsymbol{R}^{3\times15}$,分块$K_{ij}=[k_{ij1}\ k_{ij2}\ k_{ij3}\ k_{ij4}\ k_{ij5}]$,则反馈控制邻接矩阵$K^*$可以表示为

$$K^*=\begin{bmatrix}K_{11}&K_{12}&K_{13}\\K_{21}&K_{22}&K_{23}\\K_{31}&K_{32}&K_{33}\end{bmatrix}=$$

$$\begin{bmatrix}K_{11}&0&0\\0&K_{22}&0\\0&0&K_{33}\end{bmatrix}+\begin{bmatrix}0&K_{12}&K_{13}\\K_{21}&0&K_{23}\\K_{31}&K_{32}&0\end{bmatrix}=$$

$$K_{\mathrm{loc}}+K_{\mathrm{dist}}.$$

由Matlab仿真结果, 得到能够使系统稳定的近似最稀疏控制邻接矩阵的集合

$$S=\left\{\begin{bmatrix}*&*&\\*&*&\\&&*\end{bmatrix},\begin{bmatrix}*&*&\\&*&\\&*&*\end{bmatrix},\begin{bmatrix}*&*&\\&*&\\*&&*\end{bmatrix},\begin{bmatrix}*&&*\\&*&*\\&&*\end{bmatrix},\right.$$
$$\left.\begin{bmatrix}*&&*\\&*&\\*&&*\end{bmatrix},\begin{bmatrix}*&&*\\&*&\\&*&*\end{bmatrix},\begin{bmatrix}*&&\\&*&*\\&*&*\end{bmatrix}\right\}.$$

本文重点考虑控制器的设计和拓扑连接方式,因此$*$表示矩阵中元素非零.

由算法1得到

$$G=\begin{bmatrix}1&0.43&0.43\\0.14&1&0.29\\0.29&0.43&1\end{bmatrix}.$$

据此得到,该系统在电压自动控制(AVR)下,发电机1、2、3节点最为重要. 因此在对系统的安全保护中,需要物理隔离保护3个发电机节点.

由算法2,考虑发电机AVR控制下,通信过程中可能遭受的单一信道DoS攻击而导致某条通信信道受到$*\to0$攻击情况,分别保护3、4、5个物理节点时,得到可用于防御单一DoS攻击的电力控制网拓扑构建方式集合如下:

1) 由计算得到的S和G的结果可知,对3个通信节点施加物理保护时

$$K_0=\left\{\begin{bmatrix}\otimes&&\\&\otimes&\\&&\otimes\end{bmatrix},\right.$$

由此得到

$$K^{\mathrm{def}-1}=$$
$$\left\{\begin{bmatrix}\otimes&&*\\&\otimes&*\\*&*&\otimes\end{bmatrix},\begin{bmatrix}\otimes&*&*\\&\otimes&*\\*&&\otimes\end{bmatrix},\begin{bmatrix}\otimes&*&*\\&\otimes&\\*&*&\otimes\end{bmatrix}\right\}.$$

2) 由计算得到的和的结果可知,对4个通信节点施加物理保护时

$$K^{\mathrm{def}-1}=$$
$$\{K_1^{\mathrm{def}-1},K_2^{\mathrm{def}-1},K_3^{\mathrm{def}-1},K_4^{\mathrm{def}-1},K_5^{\mathrm{def}-1}\}.\quad(15)$$

其中

$$K_1^{\mathrm{def}-1}=$$
$$\left\{\begin{bmatrix}\otimes&\otimes&\\*&\otimes&\\*&&\otimes\end{bmatrix},\begin{bmatrix}\otimes&\otimes&\\*&\otimes&\\&*&\otimes\end{bmatrix},\begin{bmatrix}\otimes&\otimes&\\&\otimes&\\*&*&\otimes\end{bmatrix}\right\},$$

$$K_2^{\mathrm{def}-1}=$$
$$\left\{\begin{bmatrix}\otimes&&\otimes\\&\otimes&\\*&*&\otimes\end{bmatrix},\begin{bmatrix}\otimes&&\otimes\\&\otimes&*\\&*&\otimes\end{bmatrix},\begin{bmatrix}\otimes&&\otimes\\&\otimes&*\\*&&\otimes\end{bmatrix}\right\},$$

$$K_3^{\mathrm{def}-1}=\left\{\begin{bmatrix}\otimes&&*\\&\otimes&\otimes\\&*&\otimes\end{bmatrix}\right\},$$

$$K_4^{\mathrm{def}-1}=\left\{\begin{bmatrix}\otimes&*&*\\&\otimes&\\\otimes&&\otimes\end{bmatrix}\right\},$$

$$K_5^{\mathrm{def}-1}=$$
$$\left\{\begin{bmatrix}\otimes&*&*\\&\otimes&\\&\otimes&\otimes\end{bmatrix},\begin{bmatrix}\otimes&*&\\&\otimes&*\\&\otimes&\otimes\end{bmatrix},\begin{bmatrix}\otimes&&*\\&\otimes&*\\&\otimes&\otimes\end{bmatrix}\right\}.$$

3) 由计算得到的和的结果可知,对5个通信节点施加物理保护时

$$K^{\mathrm{def}-1}=$$
$$\left\{\begin{bmatrix}\otimes&\otimes&\\\otimes&\otimes&\\&&\otimes\end{bmatrix},\begin{bmatrix}\otimes&\otimes&\\&\otimes&\\&\otimes&\otimes\end{bmatrix},\right.$$
$$\left.\begin{bmatrix}\otimes&\otimes&\\&\otimes&\\\otimes&&\otimes\end{bmatrix},\begin{bmatrix}\otimes&&\otimes\\&\otimes&\otimes\\&&\otimes\end{bmatrix},\begin{bmatrix}\otimes&&\otimes\\&\otimes&\\\otimes&&\otimes\end{bmatrix},\right.$$

$$\left\{\begin{bmatrix}\otimes & & \otimes\\ & \otimes & \\ & \otimes & \otimes\end{bmatrix},\begin{bmatrix}\otimes & & \\ & \otimes & \otimes\\ & \otimes & \otimes\end{bmatrix}\right\}.$$

注10　‘$\otimes$’表示受到物理保护的节点和线路,不可被攻击;‘$*$’表示未受到物理保护的线路.

图3 ~ 图5分别为系统中发电机1、发电机2和发电机3的状态图. 横坐标表示时间轴,纵坐标表示发电机机端频率的变化量. 图中虚线用于区分不同的控制阶段.

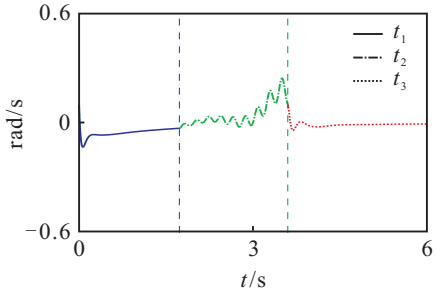

图 3　发电机1的频率变化

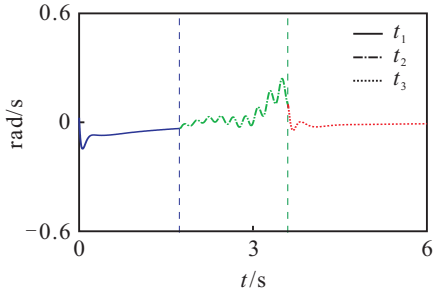

图 4　发电机2的频率变化

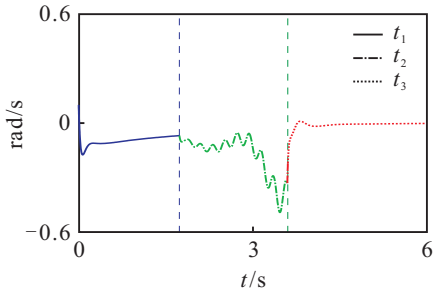

图 5　发电机3的频率变化

当前电力网络控制系统拓扑设计为

$$K_1^{*}=\begin{bmatrix}\otimes & \otimes & \\ * & \otimes & \\ * & & \otimes\end{bmatrix}.$$

$t_1 \in (0, 1.73)$ s时,系统在控制增益K_1^{*}的控制下,经过微小的波动达到稳定,如图中实线所示;$t_2 = 1.73$ s时,系统受到DoS网络攻击,通信网$(3, 1)$间通信受阻,此时控制增益的数值还未调整,因此$t_2 \in (1.73, 3.6)$ s时间范围内,系统不稳定故障运行,如图中虚线所示;当$t_3 = 3.6$ s时,系统调整K_1^{**}的参数,则在此控制邻接矩阵形式的控制网拓扑下,系统在$t_3 \in (3.6, 5)$ s时间范围内,重新达到稳定,其中

$$K_1^{**}=\begin{bmatrix}\otimes & \otimes & \\ * & \otimes & \\ & & \otimes\end{bmatrix}.$$

5　结　论

智能电网的发展对电力网络控制系统的安全性提出了更高的要求. 本文基于信息攻击下的电力网络控制系统可能受到的影响,结合发电机的同步电压控制方式,提出了一种寻找电力通信网脆弱节点和边的算法,并在此基础上,提出了抵御DoS攻击的分布式控制器设计方法. 所提出方法的优点是: 1) 降低了通信冗余度和设备间数据传输量,有效抵御了DoS攻击对电力网络控制系统的影响; 2) 对于单点或多点DoS攻击都适用. 今后的工作将结合更多的电网控制方式,考虑多种控制方式下的电力网络控制系统防御网络攻击的拓扑设计,并进一步考虑发电成本、经济成本约束下的最优问题.

参考文献(References)

[1] Gungor V C, Sahin D, Kocak T, et al. Smart grid technologies: Communication technologies and standards[J]. IEEE Trans on Industrial Informatics, 2011, 7(4): 529-539.

[2] 刘东,盛万兴,王云,等. 电网信息物理系统的关键技术及其进展[J]. 中国电机工程学报, 2015, 14: 7.
(Liu D, Sheng W X, Wang Y, et al. Key technologies and trends of cyber physical system for power grid[J]. Proc of the CSEE, 2015, 14: 7.)

[3] 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 J H, Wen F S, Xue Y S, et al. Cyber physical power systems: Architecture, implementation techniques and challenges[J]. Automation of Electric Power Systems, 2010, 34(16): 1-7.)

[4] 赵俊华,文福拴,薛禹胜,等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化, 2011, 35(16): 1-8.
(Zhao J H, Wen F S, Xue Y S, et al. Modeling analysis and control research framework of cyber physical power systems[J]. Automation of Electric Power Systems, 2011, 35(16): 1-8.)

[5] 叶夏明,文福拴,尚金成,等. 电力系统中信息物理安全风险传播机制[J]. 电网技术, 2015, 11: 12.
(Ye X M, Wen F S, Shang J C, et al. Propagation mechanism of cyber physical security risks in power systems[J]. Power System Technology, 2015, 11: 12.)

[6] 汤奕,韩啸,吴英俊,等. 考虑通信系统影响的电力系统综合脆弱性评估[J]. 中国电机工程学报, 2015, 23: 15.

(Tang Y, Han X, Wu Y J, et al. Electric power system vulnerability assessment considering the influence of communication system [J]. Proc of the CSEE, 2015, 23: 15.)

[7] Teixeira A, Sou K C, Sandberg H, et al. Secure control systems: A quantitative risk management approach[J]. IEEE Control Systems, 2015, 35(1): 24–45.

[8] Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51: 135–148.

[9] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Trans on Information and System Security(TISSEC), 2011, 14(1): 1-33.

[10] Rahman M A, Mohsenian-Rad H. False data injection attacks with incomplete information against smart power grids[C]. IEEE Global Communications Conf. IEEE, 2012: 3153–3158.

[11] Buldyrev S V, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464(7291): 1025-1028.

[12] Huang X, Gao J, Buldyrev S V, et al. Robustness of interdependent networks under targeted attack[J]. Physical Review E, 2011, 83(6): 065101.

[13] Shin D H, Qian D, Zhang J. Cascading effects in interdependent networks[J]. IEEE Network, 2014, 28(4): 82-87.

[14] Shao J, Buldyrev S V, Havlin S, et al. Cascade of failures in coupled network systems with multiple support-dependence relations[J]. Physical Review E, 2011, 83(036116): 036116.

[15] 李稳国,邓曙光,李加升,等. 智能电网中信息网与电力物理网间连锁故障的防御策略[J]. 高电压技术, 2013, 39(11): 2714-2720.
(Li W G, Deng S G, Li J S, et al. Defense strategy of cascading failures between information network and physical power grid[J]. High Voltage Engineering, 2013, 39(11): 2714-2720.)

[16] 郭静,王东蕊. 基于复杂网络理论的电力通信网脆弱性分析[J]. 电力系统通信, 2009, 30(9): 6-10.
(Guo J, Wang D R. Vulnerability analysis on power communication network based on complex network theory[J]. Telecommunications for Electric Power System, 2009, 30(9): 6-10.)

[17] Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation[C]. Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[18] Teixeira A, Amin S H, Sandberg H, et al. Cyber security analysis of state estimators in electric power systems[C]. IEEE Conf on Decision and Control. Xuzhou: IEEE, 2010: 5991–5998.

[19] Esfahani P, Vrakopoulou M, Andersson G, et al. A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems[C]. IEEE Conf on Decision and Control. Taiyuan: IEEE, 2012: 3433–3438.

[20] Wang Y, Lin Z, Liang X, et al. On modeling of electrical cyber-physical systems considering cyber security[J]. Frontiers of Information Technology and Electronic Engineering, 2016, 17(5): 465-478.

[21] 韩祯祥. 电力系统分析[M]. 第5版: 杭州: 浙江大学出版社, 2011: 3-36.
(Han Z X. Power system analysis[M]. 5th ed. Hangzhou: Zhejiang University Press, 2011: 3-36.)

[22] 韩英铎, 谢小荣, 崔文进. 同步发电机励磁控制研究的现状与走向[J]. 清华大学学报: 自然科学版, 2001, 41(4/5): 142-146.
(Han Y D, Xie X R, Cui W J. Status quo and future trend in research on synchronous generator excitation contro[J]. J of Tsinghua University: Science and Technology, 2001, 41(4/5): 142-146.)

[23] Machowski J, Bialek J, Bumby J. Power system dynamics: Stability and control[M]. New York: John Wiley and Sons, 2011.

[24] Liu J, Gusrialdi A, Hirche S, et al. Joint controller communication topology design for distributed wide-area damping control of power systems[C]. Proc of the 18th IFAC. Milan, 2011: 519-525.

[25] Donoho D L, Elad M. Optimally sparse representation in general(nonorthogonal) dictionaries via L1 minimization[J]. Proc of the National Academy of Sciences, 2003, 100(5): 2197-2202.

[26] IEEE test system data[ED/OL]. (1993-08-01)[2016-06-17]. http://www.ee.washington.edu/research/pstca/.

（责任编辑：齐 霁）