DOI: 10.7667/PSPC161974

基于业务的电力通信网络脆弱性分析评价方法

孙静月[1]，崔力民[2,3]，李珊君[1]

(1.四川大学电气信息学院，四川 成都 610065；2.华北电力大学经济与管理学院，北京 102206；
3.国网新疆电力公司信息通信公司，新疆 乌鲁木齐 830018)

摘要：为解决传统复杂网络理论脆弱性分析的局限性并改善网络性能，提出了一种基于业务的电力通信网络脆弱性分析方法。利用复杂网络理论构建网络模型，将业务重要度和业务流量作为网络参数，在蓄意攻击和随机攻击的策略下，以链路或节点失效所造成的业务量损失大小来描述网络的脆弱性，并找出网络中相应的脆弱部位。以电力 IEEE30 节点测试系统作为仿真实例，结果表明，网络业务分布越不均匀，网络脆弱性就会越高，进而网络抵御级联故障的能力就越差。而且在蓄意攻击的情况下，网络脆弱性极高。得出结论，网络业务分布越均匀，网络脆弱性就会越低。针对结论，提出了改进业务路由策略的方法以降低网络的脆弱性。仿真证明了该方法的有效性和可用性，并可为电力通信网络规划和维护提供参考，具有现实意义。

关键词：电力通信网；网络脆弱性；业务重要度；业务流量；业务损失

Vulnerability evaluation method of electric power communication network based on business

SUN Jingyue[1], CUI Limin[2,3], LI Shanjun[1]

(1. School of Electrical Engineering and Information, Sichuan University, Chengdu 610065, China; 2. College of Economics and Management, North China Electric Power University, Beijing 102206, China;
State Grid Xinjiang Information & Telecommunication Company, Urumqi 830018, China)

Abstract: In order to solve the limitation of the traditional complex network vulnerability analysis and improve the performance of the network, a vulnerability analysis method of power communication network based on the business is proposed. A power communication network model based on complex network theory is established. Business importance and business traffic are regarded as the network parameters, under the intentional and random attack strategy, the network vulnerability is measured by the loss of business when some nodes or links failed. And the corresponding vulnerable parts in the network is found. IEEE30-bus test system is used as a simulation example. The result shows that the more concentrated the distribution of business on network is, the higher the network vulnerability is and poorer the network is to withstand cascading failure. What's more, the network vulnerability is extremely high under intentional attacks. Based on the analysis, a method which can reduce the network vulnerability by changing routing strategy is given. The simulation results show that the method is effective and usable, can provide reference for the planning and maintenance of power communication network, and has practical significance.

Key words: electric power communication network; network vulnerability; business importance; business traffic; loss of business

0 引言

电力通信网作为电力系统的通信专网，承载着电力生产和管理的全部业务，其系统庞大、结构复杂，发生任何故障都可能对电网的安全稳定运行构成严重的威胁，所以安全可靠的电力通信网对电力系统的稳定运行起着举足轻重的作用[1-4]。有效地评估电力通信网运行状况，对于网络设计、规划与维护以及提高整个网络运行的质量等各个方面都有着现实意义。因此，有必要对电力通信系统进行安全性评估。

基金项目：四川省科技支撑计划项目(2017GZ0349)；国网新疆电力公司科技项目(SGXJXT00TJS1600206)

网络的可靠性、脆弱性等指标都是网络系统安全的一种评估方式[5-6]。为了有效地抵御各种危害事故的冲击，确保整个电力系统安全稳定运行，需要明确地找出电力通信系统的脆弱部位，网络的可靠性分析不能全面反映出系统的缺陷，故采用有效的方法进行网络系统脆弱性分析非常必要。针对电力通信网可靠性的研究已经很成熟[7-10]，然而对电力通信网脆弱性研究甚少。国内外针对计算机等复杂网络脆弱性研究方法颇多，如基于规则[11]、模型[12-13]、贝叶斯[14]网络的评估方法等。目前，电力通信网络的脆弱性研究主要是基于复杂网络理论，通过效能函数和最大子图连通度[15]来描述网络脆弱性。描述网络脆弱性指标还包括聚集系数、紧密度、介数、平均距离等。文献[16]应用复杂网络理论从连通性和网络效率两个角度分别对四川、重庆、河南、湖北、湖南和江西等六个网络进行了脆弱性评估。文献[17]从物理和结构两个方面对网络脆弱性进行量化评估。然而，电力通信网络具有明显的行业特点，单一地考虑网络拓扑不能完全地反映出电力通信网络的系统性能。已有学者考虑了通信业务因素对电力通信网络进行性能评估，文献[18-20]将电力通信网看作为信息物理融合系统，考虑了电力系统与通信系统的交互作用，通过业务通信中断、时延故障对电力系统的影响来分析网络的脆弱性。文献[21-22]融合了业务重要度对电力通信网进行性能评估。

针对复杂网络理论对电力通信网络脆弱性分析的局限性，本文融合了业务重要度和业务流量进行具有业务特征的网络脆弱性分析，更加准确地反映网络业务的损失情况，具有现实意义。本文首先基于复杂网络理论，建立电力通信网络模型，将业务重要度和业务流量作为网络参数，以业务量损失大小作为网络脆弱性评判标准；其次分析在不同的攻击策略下的网络脆弱性，通过分析结果提出调整路由政策的方法改善网络性能；最后将业务调整前和调整后的网络进行比对分析，仿真结果验证了该方法的有效性。

1　电力通信网络模型

利用图论的方法构建网络三元组模型，设为(G, D, P)。$G=(V, E)$为通信层网络拓扑结构，$V=\{1, 2, \cdots, N\}$为通信节点集，$E=\{1, 2, \cdots, M\}$为无向通信链路集。$D=\{(i, j)\}$为网络源宿节点对集，其中，$i, j \in V$。P为网络路由选择策略。

在构建网络拓扑时，将其 SDH 通信设备抽象描述为节点，光纤传输线抽象为链路。为了简化，需做如下几点处理：

(1) 只考虑 22 kV 以上的高压输电网，不考虑配电网通信系统；

(2) 网络拓扑节点主要包括调度中心和各厂站；

(3) 站点之间相连的光纤线路视为网络拓扑的链路，将 SDH 传输网络中的各种保护线路都合并为一条，消除重边和自环；

(4) 站点间通信视为双向通信，即所有链路设为无向的，链路的长度视为两站点间实际距离。

2　业务分析

2.1　业务

通信系统对电力系统的影响是通过业务实现的，业务故障则会影响电网的正常运行。电力通信业务的种类很多，对时延、带宽、误码率、丢包率等要求不同，每种业务的重要性就会不同。本文考虑部分电力业务，包括 500 kV 继电保护、220 kV 继电保护、电能计量遥测、调度电话、调度自动化、安稳系统、广域测量、雷电定位检测、变电站视频检测、保护信息管理、办公自动化、行政电话以及视频会议等 13 种业务，将业务重要度作为衡量业务在网络中相对重要性大小的指标。业务流量的分布情况体现了网络业务运行状态。

2.2　业务重要度矩阵

在已有的研究中，借助专家评分并通过模糊数学理论进行计算业务重要度的算法已经很成熟，不再陈述。业务重要度的求法见文献[23-24]。选取业务集 $\boldsymbol{Q}$，共含有 K 种业务，则可以将这 K 种业务的业务重要度 $\boldsymbol{W}$ 用 $K\times1$ 阶矩阵表示

$$\boldsymbol{W}=\begin{bmatrix} W_1 & W_2 & \cdots & W_K \end{bmatrix}^{\mathrm{T}} \tag{1}$$

2.3　源宿节点对业务重要度分布矩阵

设源宿节点对 (i, j) 所承载的业务矩阵 $\boldsymbol{S}^{(i,j)}=[S_1^{(i,j)} \quad S_2^{(i,j)} \quad \cdots \quad S_K^{(i,j)}]^{\mathrm{T}}$，其中 K 代表电力通信业务种类(如继电保护，安稳系统等)，而 $S_k^{(i,j)}$ 则表示(i, j)源宿节点对之间所承载的第 k 类业务的数量$(k=1, 2, \cdots, K)$。用 $\boldsymbol{I}^{(i,j)}$ 表示网络中源节点 i 和目的节点 j 之间所承载的各类业务重要度分布矩阵，则 $\boldsymbol{I}^{(i,j)}$ 公式为

$$\boldsymbol{I}^{(i,j)}=\begin{bmatrix} I_1^{(i,j)} & I_2^{(i,j)} & \cdots & I_K^{(i,j)} \end{bmatrix}^{\mathrm{T}} \tag{2}$$

式中，$I_k^{(i,j)}=S_k^{(i,j)}W_k$。

2.4　源宿节点对业务流量权重分布矩阵

设某一时间段内，F_k 为业务集 $\boldsymbol{Q}$ 中第 k 种业务的单位流量，$F_k^{\max}$ 为业务集 $\boldsymbol{Q}$ 中最大的业务单位流

量，$\frac{F_k}{F_k^{\max}}$ 则为第 k 类业务归一化流量。源宿节点对 (i,j) 之间的业务流量权重分布矩阵为

$$\boldsymbol{R}^{(i,j)}=[R_1^{(i,j)} \quad R_2^{(i,j)} \quad \cdots \quad R_K^{(i,j)}]^{\mathrm{T}} \tag{3}$$

式中，$R_k^{(i,j)}=S_k^{(i,j)}\frac{F_k}{F_k^{\max}}$，$(k=1,2,\cdots,K)$。

2.5 业务量和

网络业务量和(简称业务量)，包括业务重要度及业务流量权重两个方面，设信息路由经过第 m 条链路的源宿节点对集合为 $\boldsymbol{Y}(\boldsymbol{Y}\subseteq\boldsymbol{D})$，则第 m 条链路的业务量为

$$L_m=\sum_{(i,j)\in\boldsymbol{Y}}\sum_{k=1}^{K}\left(I_k^{(i,j)}R_k^{(i,j)}\right) \tag{4}$$

式中，$m=1,2,\cdots,M$。

类似地，第 n 节点的业务量为

$$L_n=\sum_{m\in\boldsymbol{C}}L_m \tag{5}$$

式中，$\boldsymbol{C}$ 为与节点 n 直接相连的链路集合。

3 电力通信网络脆弱性评估

3.1 脆弱性评估指标

因为对节点和链路的脆弱性分析方法相同，故以链路为例详细说明。

攻击脆弱性[25]的基本定义是从网络中有选择地删除某个节点或某条线路，以网络性能下降的程度来衡量此节点或线路的脆弱度。在网络受到攻击后，电力通信网络真正的损失是传输的业务。当网络链路受到攻击以后，网络业务流量进行重新分配，每条链路都有承受的容量阈值，当达到阈值以后，就会造成拥塞，引发级联故障。复杂网络中的级联行为[26]指网络中单个或少数链路发生的故障，通过链路间的耦合关系产生连锁反应引起其他链路发生故障，引发相当一部分链路甚至整个网络崩溃的动力学行为。级联故障会对网络造成毁灭性的伤害。级联故障模型如图 1 所示。

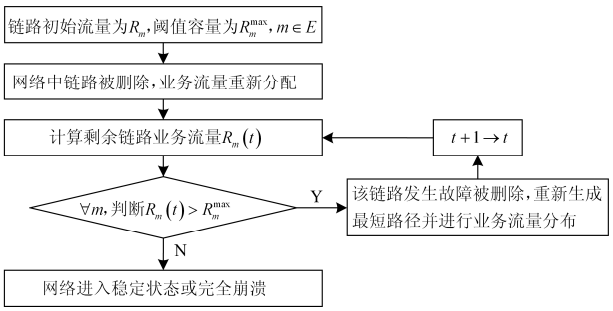

图 1 级联故障模型

Fig. 1 Cascading failure model

本文将业务量损失率作为评估指标对网络脆弱性进行描述。业务量损失率 η 为

$$\eta=\frac{\sum_{m\in\boldsymbol{Z}(t+1)}L_m(t+1)-\sum_{m\in\boldsymbol{Z}(t)}L_m(t)}{\sum_{m\in\boldsymbol{E}(t)}L_m(t)} \tag{6}$$

式中：$\boldsymbol{Z}(t+1)$表示下一个稳定状态时刻的失效链路集合；$\boldsymbol{Z}(t)$表示初始时间状态的失效链路集合；$\boldsymbol{E}(t)$表示初始链路总集合。

3.2 网络攻击策略

参考 Holme[13]在复杂网络中以网络拓扑结构参数作为指标，提出的模拟攻击策略(介数删除、重算介数删除、度删除以及重算度删除)，此处以链路业务量作为攻击指标，得到以下三种攻击策略。

(1) 业务量值降序删除

此攻击策略属于蓄意攻击类型，攻击链路集合为全网业务量损失最大的前 Z 条链路。

(2) 重算业务量值降序删除

此攻击策略属于蓄意攻击类型，攻击链路集合 $\boldsymbol{Z}$，每次攻击链路都是一个选择的过程，即在每次按最大业务量值进行攻击后，重算剩余链路业务量值，选择当前网络中业务量值最大的链路进行攻击。

(3) 随机删除

此攻击策略属于随机攻击类型，随机选取链路集合 $\boldsymbol{Z}$ 进行攻击。

3.3 脆弱性评估策略

(1) 分析三种攻击策略下网络脆弱性并进行比较。

攻击链路的集合为 $\boldsymbol{Z}$，由脆弱性指标得到在攻击策略下网络的脆弱性公式为

$$V=\frac{\sum_{m\in\boldsymbol{Z}(t+1)}L_m(t+1)-\sum_{m\in\boldsymbol{Z}(t)}L_m(t)}{\sum_{m\in\boldsymbol{E}(t)}L_m(t)} \tag{7}$$

在链路失效比率相同的情况下，业务量损失率越大，网络的脆弱性越高，以此来比较在三种攻击策略下的网络脆弱性。

(2) 量化分析链路脆弱性，找出网络中脆弱部位。

网络中删除某一链路，网络性能因此下降的程度定为该链路的脆弱性，则第 m 条链路的脆弱性公式为

$$V_m=\frac{\sum_{x\in\boldsymbol{E}(t)}L_x(t)-\sum_{x\in\boldsymbol{E}(t+1)}L_x(t+1)}{\sum_{x\in\boldsymbol{E}(t)}L_x(t)} \tag{8}$$

式中：$\boldsymbol{E}(t)$表示初始链路总集合；$\boldsymbol{E}(t+1)$表示删除链路 m 后下一个稳定状态时刻的链路集合。

4　仿真分析

4.1 构建网络拓扑

将 IEEE30 节点测试系统组网，组网模型参考文献[27]。电力通信网拓扑结构如图 2 所示，包含了 26 个节点，38 条链路。链路上的数值表示为两节点间实际距离。其中 25 号节点为省级调度中心，26 号为地区调度中心，4 号、15 号和 23 号为 500 kV 变电站，6 号为汇聚节点，其余节点为 220 kV 变电站。

为了简化计算，将业务按业务重要度大小分为 5 个等级。每种业务的业务重要度值和等级分类如表 1 所示。

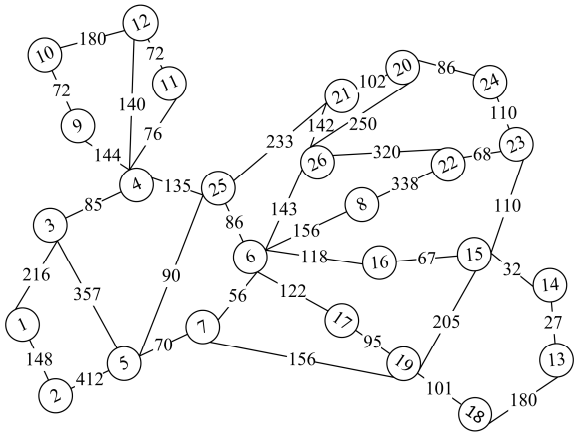

图 2 IEEE30 节点电力通信网拓扑结构

Fig. 2 Topology of communication network of the IEEE30-bus test system

表 1 业务等级及业务重要度

Table 1 Level of business and business importance

业务等级	业务	业务重要度值
5	500 kV 继电保护	1.00
5	220 kV 继电保护	0.98
4	安稳系统	0.96
3	广域测量	0.74
3	调度自动化	0.64
3	调度电话	0.57
3	电能计量遥测	0.52
2	视频会议	0.39
2	变电站视频检测	0.26
2	保护信息管理	0.22
1	办公自动化	0.12
1	雷电定位检测	0.18
1	行政电话	0.10

由表 1 可以看出，每种业务的重要度大小不同，以每个等级中各业务重要度平均值作为该等级业务的业务重要度值。由高到低的每个等级的业务重要度矩阵为 $\boldsymbol{W}=[0.99,0.96,0.62,0.29,0.13]^{\mathrm{T}}$，依次所对应的归一化单位业务流量为 0.03、0.08、0.02、0.52 和 0.14，通过 Matlab 编程，选择最短路径为路由方式。

4.2 链路脆弱性分析

由 3.2 节提到的网络攻击模型，分别对该网络进行攻击。(1) 链路业务量值降序删除；(2) 重算链路业务量值降序删除；(3) 随机链路删除。三种攻击模型下网络脆弱性曲线如图 3 所示。

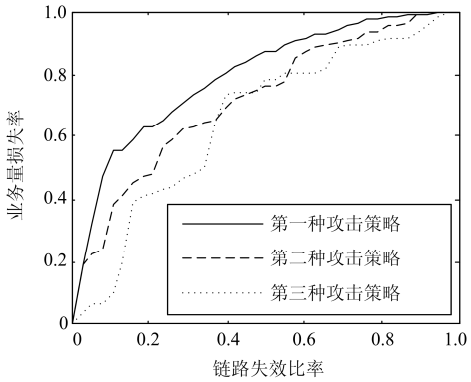

图 3 网络脆弱性曲线

Fig. 3 Network vulnerability curves

由图 3 可以看出：

(1) 随着网络中链路失效比例的增大，三种攻击方式下的业务量失效率都在大幅增加，发生了不同范围的级联故障。说明网络抵抗攻击的能力较差，级联故障给网络带来的损害巨大。

(2) 比较三种攻击方式，按业务量值降序依次删除链路的攻击方式对网络产生的影响最大，每次按业务量最大值依次降序删除链路攻击的方式次之，随机攻击对网络产生的影响最小。说明网络在随机攻击策略下，网络的脆弱性相对较好。

(3) 在第一种和第二种蓄意攻击的情况下，脆弱性曲线整体呈现对数增长趋势。原因在于网络业务分布极不均匀，有少部分链路(5、6、14)承载了很多业务，当这些链路失效时，网络业务损失率已经达到 50%。当链路失效越来越多时，网络中大部分业务已经丢失，脆弱性曲线则趋于平缓。当链路失效率为 60%时，业务量损失率已高达 90%，网络基本瘫痪，说明在蓄意攻击的情况下，网络抵抗级联故障的能力很差，脆弱性极高。

由攻击脆弱性的定义，求得各个链路脆弱性，结果如图 4 所示。

由图 4 可以看出，脆弱性相对比较高的链路有 5、6、14、15 和 29，在拓扑图中分别对应为 25-6、25-4、16-6、16-15 和 26-6 两节点间链路。可以看出这几条链路正处于中心位置，与省级调度中心相

连，正是关键性的几条链路，承载的业务是最多的，一旦失效，将会导致级联故障并给网络带来严重的危害。

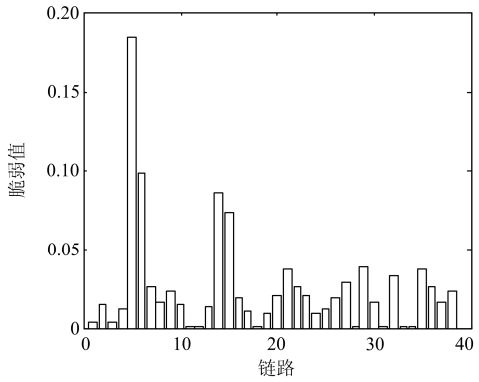

图 4 链路脆弱性

Fig. 4 Vulnerability value of links

4.3 节点脆弱性分析

参照链路脆弱性的分析，由 3.2 节提到的网络攻击模型，分别对该网络进行攻击。三种攻击模型下网络脆弱性曲线如图 5 所示。

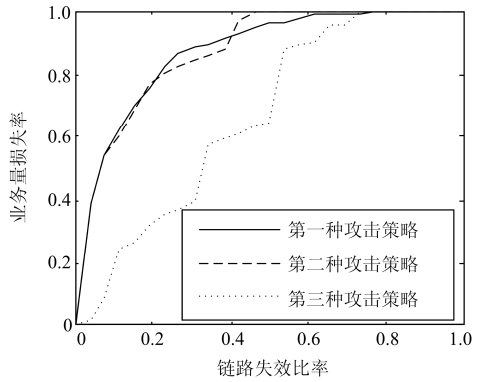

图 5 网络脆弱性曲线

Fig. 5 Network vulnerability curves

从图 5 可以看出：

(1) 随网络中节点失效比例的增大，三种攻击方式下的业务失效率急剧增加，网络发生了大范围的级联故障。说明网络抵抗攻击的能力很差，级联故障行为给网络带来的损害巨大。

(2) 比较三种攻击方式，两种蓄意攻击方式下的网络脆弱性曲线基本重合，网络抵御攻击的能力很差，网络脆弱性很高，这是因为与节点相连的链路业务分布不均匀，重要节点失效时业务就会损失惨重；随机攻击方式对网络产生的影响相对较小，说明在抵御随机攻击方式下的网络脆弱性相对良好。

(3) 对比图 3，图 5 曲线上升的趋势更为陡峭，说明节点失效给网络带来的危害更为严重。在蓄意攻击的方式下，当节点失效率为 10%(即 6 号、25 号两个节点)时，网络业务损失率已经达到 60%，说明网络已发生了级联故障。在网络拓扑图中，25 号节点为省级调度中心，6 号节点为中心汇聚节点，这两个节点正是网络中极为重要的通信节点。当两个通信节点失效时，网络中大部分业务将中断，网络基本瘫痪，说明在蓄意攻击的情况下，节点的脆弱性极高。

类似地，节点脆弱性如图 6 所示。

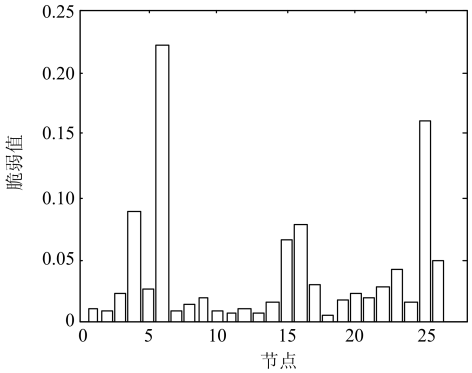

图 6 节点脆弱性

Fig. 6 Vulnerability value of nodes

从图 6 可以看出，6 号、25 号节点的脆弱性相对很高，25 号节点为省级调度中心节点，6 号节点为中心汇聚节点，两个节点为网络中为最重要的节点，承载的业务是最多的，一旦被攻击破坏，网络将面临级联崩溃，这正是图 5 中在蓄意攻击策略下脆弱曲线急剧上升的原因。

从仿真结果上综合分析，此网络业务分布不均匀，网络的脆弱性较高，抵抗外部攻击和预防级联故障能力较差。业务分布越多的节点或链路，其脆弱性相对越高，针对分析结果，可以通过调整业务路由的方法来降低网络的脆弱性。

4.4 改进策略

从上述网络脆弱性分析中可以得出，业务量分布不均匀，网络抵抗外部攻击和预防级联故障能力较差，网络的脆弱性较高。为了改善网络的性能，需调整业务路由使网络业务分布均匀。调整方法如下，在保持业务总量不变的情况下，选取此网络业务量较大的几条链路进行业务调整，将经过这些链路的源宿节点对之间业务的 50%分配到其他链路上。网络业务路径调整前和调整后的业务权重分布如图 7 所示。

从图 7 可以看出，链路调整以后，业务分布更加均匀。

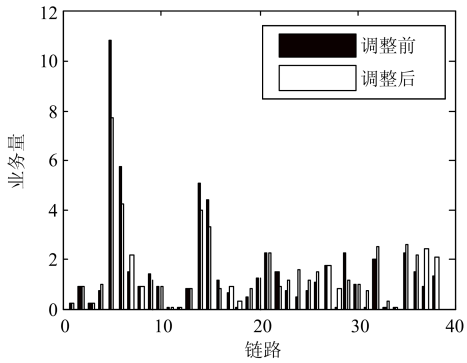

图 7 比较路径调整前后网络业务量分布情况

Fig. 7 Comparison of network business distribution between before and after adjusting path

考虑到第一种蓄意攻击方式对攻击者来说代价较小，因此，以第一种蓄意攻击方式为例，绘制网络链路在业务路径调整前和调整后的脆弱性变化曲线，如图 8 所示。

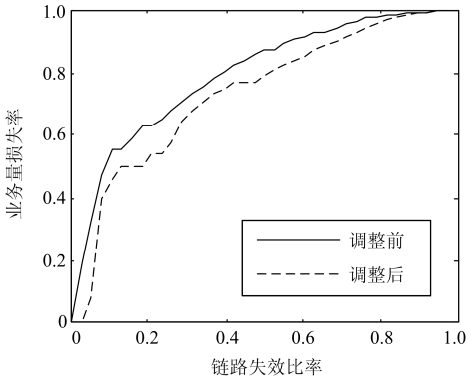

图 8 第一种攻击下路径调整前后网络脆弱性比较

Fig. 8 Network vulnerability comparison between before and after adjusting path under the first kind of attack

从曲线变化的情况来看，网络在蓄意攻击的策略下，网络链路的脆弱性有明显的下降；在相同链路失效比率的情况下，业务损失率相差 10%左右，说明此方法改善网络性能的效果较为明显。

网络业务调整前后链路脆弱值的变化如图9所示。

同样地，网络节点在业务调整前和调整后的脆弱性变化曲线如图 10 所示。

从曲线变化的情况来看，网络节点的脆弱性有明显的下降趋势。当节点失效率小于 30%时，业务损失率相差 10%左右，说明此方法改善网络性能的效果较为明显。当节点失效率大于 30%时，业务损失率已高达 70%，网络中重要的节点已经失效，网络面临瘫痪，再调整路由已经没有意义。

网络业务调整前后节点脆弱值的变化如图 11 所示。

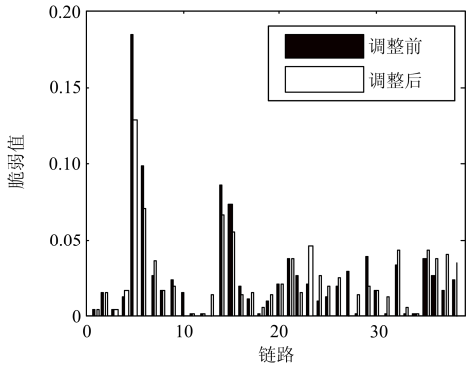

图 9 路径调整前后链路脆弱性比较

Fig. 9 Link vulnerability comparison between before and after adjusting path

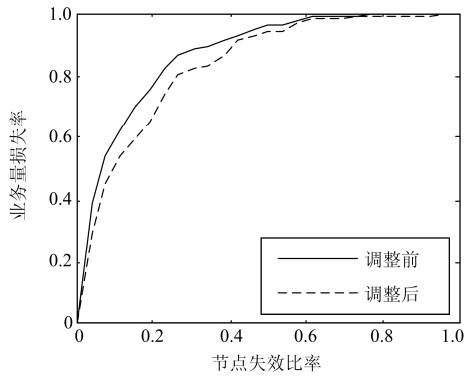

图 10 第一种攻击下路径调整前后网络脆弱性比较

Fig. 10 Network vulnerability comparison between before and after adjusting path under the first kind of attack

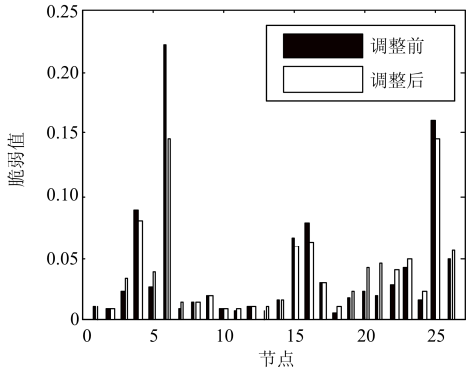

图 11 路径调整前后节点脆弱性比较

Fig. 11 Node vulnerability comparison between before and after adjusting path

对比业务调整前和调整后网络脆弱性的变化，得出：业务在网络中分布的越均匀，电力通信网络的脆弱性就越低，抵御级联故障的能力就越强。

6 结论

本文应用复杂网络理论，融合电力通信网具有

的业务特征，得到基于业务的电力通信网脆弱性分析方法。在三种攻击策略(业务量值降序删除、重算业务量值降序删除和随机删除)下，通过业务损失的大小来描述网络脆弱性。通过仿真结果的分析，验证该方法的有效性。得出网络业务分布的越不是均匀，网络受到攻击时，网络的脆弱性越高，网络抵御级联故障能力越小。提出了优化路由策略的方法改善网络性能，并验证了此方法的正确性。本文的不足之处则是没有给出有效的优化路由算法。

参考文献

[1] 曾瑛, 朱文红, 邓博仁, 等. 基于电网影响因子的电力通信网关键节点识别[J]. 电力系统保护与控制, 2016, 44(2): 102-108.
ZENG Ying, ZHU Wenhong, DENG Boren, et al. Crucial node decision algorithm based on power network impact factor in electric power communication network[J]. Power System Protection and Control, 2016, 44(2): 102-108.

[2] 姚致清. 通信规约实现与系统可靠性、安全性[J]. 继电器, 2008, 36(6): 68-70.
YAO Zhiqing. The relationship between communication protocol and system reliability and safety[J]. Relay, 2008, 36(6): 68-70.

[3] 蒋康明, 曾瑛, 邓博仁, 等. 基于业务的电力通信网风险评价方法[J]. 电力系统保护与控制, 2013, 41(24): 101-106.
JIANG Kangming, ZENG Ying, DENG Boren, et al. Risk evaluation method of electric power communication network based on services[J]. Power System Protection and Control, 2013, 41(24): 101-106.

[4] 丁明, 过羿, 张晶晶, 等. 基于效用风险熵权模糊综合评判的复杂电网节点脆弱性评估[J]. 电工技术学报, 2015, 30(3): 214-223.
DING Ming, GUO Yi, ZHANG Jingjing, et al. Node vulnerability assessment for complex power grids based on effect risk entropy-weighted fuzzy comprehensive evaluation[J]. Transactions of China Electrotechnical Society, 2015, 30(3): 214-223.

[5] 李俊刚, 张爱民, 张杭, 等. 广域保护系统数据网络可靠性评估[J]. 电工技术学报, 2015, 30(12): 344-350.
LI Jungang, ZHANG Aimin, ZHANG Hang, et al. Reliability evaluation of the wide area protect system[J]. Transactions of China Electrotechnical Society, 2015, 30(12): 344-350.

[6] 程晓荣, 张兰, 岳娇. 基于粗糙集属性约简的评估模型在电力通信网风险评估中的应用及实现[J]. 电力系统保护与控制, 2016, 44(8): 44-48.
CHENG Xiaorong, ZHANG Lan, YUE Jiao. Application and implementation of the assessment model based on rough set attribute reduction in power communication network risk assessment[J]. Power System Protection and Control, 2016, 44(8): 44-48.

[7] ANTONOPOULOS A, REILLY J J, LANE P. A framework for the availability assessment of SDH transport networks[J]. IEEE Symposium on Computers & Communications, 1997, 25(1): 666-670.

[8] WANG Y, LI W, LU J. Reliability analysis of wide-area measurement system[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1483-1491.

[9] 曾瑛. 电力通信网可靠性分析评估方法研究[J]. 电力系统通信, 2011, 32(226): 13-16.
ZENG Ying. Research on reliability analysis and evaluation method of electric power communication network[J]. Telecommunications for Electric Power System, 2011, 32(226): 13-16.

[10] 金鑫. 高压直流输电系统极控信号通信网络可靠性分析[J]. 电力系统保护与控制, 2015, 43(12): 110-116.
JIN Xin. Reliability analysis on HVDC pole control signal transmission network[J]. Power System Protection and Control, 2015, 43(12): 110-116.

[11] SWARUP V, JAJODIA S, PAMULA J. Rule-based topological vulnerability analysis[M]. Heidelberg, 2009.

[12] HOLME P, JUNKIM B J, YOON C N, et al. Attack vulnerability of complex networks[J]. Physical Review E, 2002, 65(2): 634-649.

[13] WANG L, NOEL S, JAJODIA S. Minimum-cost network hardening using attack graphs[J]. Computer Communications, 2006, 29(18): 3812-3824.

[14] FRIGAULT M, WANG L. Measuring network security using Bayesian network-based attack graphs[C] // 2008 32nd Annual IEEE International Computer Software and Applications Conference, Washington, United States of America, 2008: 698-703.

[15] DEKKER A H, COLBERT B D. Network robustness and graph topology[C] // 27th Australasian Conference on Computer Science, Dunedin, New Zealand, 2004: 359-368.

[16] 刘涤尘, 冀星沛, 王波, 等. 基于复杂网络理论的电力通信网拓扑脆弱性分析及对策[J]. 电网技术, 2015, 39(12): 3615-3621.
LIU Dichen, JI Xingpei, WANG Bo, et al. Topological vulnerability analysis and countermeasures of electrical communication network based on complex network theory[J]. Power System Technology, 2015, 39(12): 3615-3621.

[17] 郭静. 基于复杂网络理论的电力通信网脆弱性分析[D].

北京: 华北电力大学, 2010.
GUO Jing. Vulnerability analysis on power communication network based on complex network theory[D]. Beijing: North China Electric Power University, 2010.

[18] 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, 35(23): 6066-6074.
TANG Yi, HAN Xiao, WU Yingjun, et al. Electric power system vulnerability assessment considering the influence of communication system[J]. Proceedings of the CSEE, 2015, 35(23): 6066-6074.

[19] WANG Q, PIPATTANASOMPORN M, KUZLU M, et al. Framework for vulnerability assessment of communication systems for electric power grids[J]. IET Generation, Transmission & Distribution, 2016, 10(2): 477-486.

[20] 王中杰, 谢璐璐. 信息物理融合系统研究综述[J]. 自动化学报, 2011, 37(10): 1157-1166.
WANG Zhongjie, XIE Lulu. Cyber-physical systems: a survey[J]. Acta Automatica Sinica, 2011, 37(10): 1157-1166.

[21] 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(203): 6-10.
GUO Jing, WANG Dongrui. Vulnerability analysis on power communication network based on complex network theory[J]. Telecommunications for Electric Power System, 2009, 30(203): 6-10.

[22] 樊冰, 唐良瑞. 电力通信网脆弱性分析[J]. 中国电机工程学报, 2014, 34(7): 1191-1197.
FAN Bing, TANG Liangrui. Vulnerability analysis of power communication network[J]. Proceedings of the CSEE, 2014, 34(7): 1191-1197.

[23] 高红云, 王超, 哈明虎. 直觉模糊层次分析法[J]. 河北工程大学学报(自然科学版), 2011, 28(4): 101-105.
GAO Hongyun, WANG Chao, HA Minghu. Intuitionistic fuzzy analytic hierarchy process[J]. Journal of Hebei University of Engineering (Natural Science Edition), 2011, 28(4): 101-105.

[24] XU Z S, LIAO H C. Intuitionistic fuzzy analytic hierarchy process[J]. IEEE Transactions on Fuzzy Systems, 2014, 22(4): 749-761.

[25] HOLME P, JUNKIM B J, YOON C N, et al. Attack vulnerability of complex networks[J]. Physical Review E, 2002, 65(2): 634-649.

[26] 刘晓明. 复杂信息系统网络脆弱性分析与仿真验证技术研究[D]. 北京: 北京邮电大学, 2013.
LIU Xiaoming. Research on vulnerability analysis and simulation validation techniques of complex information system network[D]. Beijing: Beijing University of Posts and Telecommunications, 2013.

[27] WANG Y, LI W, LU J. Reliability analysis of wide-area measurement system[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1483-1491.

收稿日期：2016-11-27；　修回日期：2017-01-13

作者简介：

孙静月(1990—)，女，硕士研究生，研究方向为信号与信息处理；E-mail: ssjjyy1025@sina.com

崔力民(1973—)，男，博士研究生，高级工程师，研究方向为电力通信网评估；E-mail: clm2929639@163. com

李珊君(1967—)，女，通信作者，副教授，研究生导师，研究方向为光纤通信和数据通信。E-mail: lishanjun579@163.com

(编辑　姜新丽)