

基于信息熵的电力通信网脆弱性评价方法

樊冰^① 曾瑛^② 唐良瑞^①

^①(新能源电力系统国家重点实验室(华北电力大学) 北京 102206)

^②(广东电网电力调度控制中心 广州 510600)

摘要: 电力通信网是智能电网的重要支撑网络, 针对如何对其脆弱性进行综合、有效评价的问题, 该文提出一种基于信息熵的电力通信网脆弱性跨层综合评价方法。首先给出了一种业务重要度计算方法, 并将业务重要度作为网络参数, 在业务层建立网络模型, 定义边业务重要度(EBI)作为边在业务层的重要性指标; 然后综合考虑网络的业务层、传输层和物理层, 定义了边跨层重要度(ECI), 进而将边跨层重要度的全网信息熵-边跨层信息熵(ECE)作为电力通信网脆弱性的评价指标; 最后, 以某实际电力通信网络为仿真背景, 在不同路由策略下, 通过对比网络脆弱性曲线和信息熵值的变化, 证明了该方法对电力通信网脆弱性评价的有效性。该方法不仅限于电力通信网, 还可推广至其它非一致性业务的承载网络。

关键词: 电力通信网; 网络脆弱性; 信息熵; 业务重要度; 边跨层重要度

中图分类号: TN915.85

文献标识码: A

文章编号: 1009-5896(2014)09-2138-07

DOI: 10.3724/SP.J.1146.2013.01481

Vulnerability Assessment of Power Communication Network Based on Information Entropy

Fan Bing^① Zeng Ying^② Tang Liang-ru^①

^①(State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources (North China Electric Power University), Beijing 102206, China)

^②(Electric Power Dispatching and Control Center of Guangdong Grid, Guangzhou 510600, China)

Abstract: In order to comprehensively and effectively assess the vulnerability of power communication network, which is an important supporting network of smart grid, a cross-layer assessment method based on the information entropy is proposed. Firstly, a calculation method of power business importance is presented and the business importance is taken as a parameter to model power communication network on the business layer. The importance of edges on the business layer is described by the Edge Business Importance (EBI). Secondly, taking into account the business layer, transport layer and physical layer, Edge Cross-layer Importance (ECI) is proposed and the information entropy of ECI on a network, which is called Edge Cross-layer Entropy (ECE), is defined as the assessment index of network vulnerability. Finally, taking a real communication network as the simulating background, the validity of the method is proved by comparing the change of network vulnerability curves and ECEs under different routing strategies. The proposed method is suitable for not only power communication networks but also all the networks which carry non-uniform businesses.

Key words: Power communication network; Network vulnerability; Information entropy; Business importance; Edge Cross-layer Importance (ECI)

1 引言

网络脆弱性作为网络可靠性的一种有效测度, 通过网络在遭受攻击时性能的下降程度, 反映了网络在拓扑、流量分布、路由等方面的合理性。已有的用来评价网络脆弱性的指标包括: 连通度^[1]、膨胀

系数^[2]、离散数^[3]、完整度^[4]、粘聚度^[5]、自然连通度^[6]和两两连通度^[7]等。传统的网络脆弱性分析大多基于物理层拓扑或传输层流量, 很少考虑网络中传输业务的类别和特征。电力通信网中传输的是对电力生产和运行影响程度不一的电力业务, 仅从物理层和传输层去分析电力通信网的脆弱性不能准确反映出电力通信网网络单元失效后对电网造成的损失, 因此, 有必要将网络的业务层考虑进来, 对电力通信网脆弱性进行跨层的综合性评价。目前, 已

2013-09-26 收到, 2014-02-28 改回

中央高校基本科研业务费专项资金(2014XS02)资助课题

*通信作者: 樊冰 fanbing@ncepu.edu.cn

有一些学者从电力业务角度对电力通信网性能进行了分析：文献[8,9]从单一业务角度对网络的脆弱性和有效性进行了分析；文献[10]利用模糊层次分析法计算业务重要度并从多业务角度对网络的可靠性进行了分析；文献[11,12]利用业务重要度建立网络的风险均衡模型，然后分别研究了网络的可靠性评价问题和路由分配机制问题。

从已有文献可以看出，电力业务重要度是电力通信网业务层性能分析的重要参数，因此本文首先给出了一种基于客观性能指标要求的电力业务重要度计算方法；然后以业务重要度作为参数，在业务层上建立电力通信网络模型，并与传输层网络模型综合考虑，以边攻击模型为例，提出边业务重要度(Edge Business Importance, EBI)、边流量重要度(Edge Traffic Importance, ETI)、边跨层重要度(Edge Cross-layer Importance, ECI)和边跨层信息熵(Edge Cross-layer information Entropy, ECE)一系列概念；最后通过仿真证明了ECE对电力通信网脆弱性评价的有效性。

2 电力业务重要度

传统电力业务重要度计算中专家评分环节具有较强的主观性，可能导致业务重要度的计算结果不一致，从而影响业务层网络性能分析的准确性。文献[12]将电力业务的性能指标与文献[13]中多属性决策问题属性权重的计算思想相结合，给出了仅基于客观指标的业务重要度计算方法。该方法对不在数域上且大于两种状态的性能指标，如安全区和保护方式等，无法映射到数域上参与业务重要度的计算，且数域上性能指标取值的差距也不能代表重要度上的差距。针对上述问题，本文提出了一种基于客观性能指标相对差异的业务重要度计算方法。

2.1 业务重要值矩阵

选取业务集 B 和性能指标集 K 。对每个性能指标 $k \in K$ ，将业务集按照其对指标要求的高低升序排列，对指标要求越高的业务越重要，其序号越大，相同要求的多个业务先后次序随机。令 $q(k, b)$ 表示业务 $b \in B$ 在指标 k 下排序后的序号， $b(k, q)$ 表示指标 k 下序号 q 对应的业务，则定义 $f: K \times B \rightarrow N^+$ ：

$$f(k, b, q) = \begin{cases} 1, & q(k, b) = 1 \\ f(k, b, q-1) + 1, & b(k, q) \succ b(k, q-1) \\ f(k, b, q-1), & b(k, q) \prec b(k, q-1) \end{cases} \quad (1)$$

其中，符号 \succ 表示其左侧的业务重要于右侧的业务，符号 \prec 表示两侧的业务同等重要。通过映射 f 可以将业务集 B 在指标集 K 下的重要性映射到正整数域上，该映射对指标集 K 没有数域的限制，且函数值与业务在指标下的数值差无关。根据映射 f ，可得到

业务重要值矩阵 $\mathbf{A} = [a_{ij}]_{I \times J}$ ，其中 $I = |B|$ 为选取的业务类数， $J = |K|$ 为选取的指标数， $|\cdot|$ 表示集合中元素的个数， a_{ij} 表示业务 b_i 在性能指标 k_j 下的相对重要值，即

$$a_{ij} = f(k_j, b_i, q(k_j, b_i)) \quad (2)$$

2.2 业务重要度计算

对业务重要值矩阵 \mathbf{A} 的行向量元素进行求和，得到业务 b_i 对业务集 B 中其他所有业务在性能指标集 K 下的综合相对重要值

$$a'_i = \sum_{j=1}^J a_{ij} \quad (3)$$

然后对其进行归一化处理，归一化公式为

$$a''_i = \frac{a'_i - a'_{i\min}}{a'_{i\max} - a'_{i\min}} \quad (4)$$

其中， $a'_{i\max}$ 和 $a'_{i\min}$ 分别表示 a'_i 的最大值和最小值。通过式(4)归一化后， a''_i 的最小值为 0，表示该类业务的重要度为 0，这显然不够合理，因此需要将 a''_i 通过式(5)映射到区间 $[X, 1]$ 上，

$$Q_i = Q(a''_i) = a''_i(1 - X) + X \quad (5)$$

其中 $0 < X < 1$ ，进而得到业务 b_i 的合理重要度评价价值 Q_i 。 X 取值过大会造成业务之间的重要度差别过小，业务之间的区分变得困难， X 取值过小会失去式(5)的意义。本文取 $X=0.1$ ，将重要度最大值与最小值的距离设定为 10 倍。

2.3 实例分析

本文选取的电力业务、性能指标、指标要求^[10,14]及通过 f 计算出的相对重要值如表 1 所示。其中“业务通道”指标下，“1 专”表示一路 E12 光纤专线通道，“1 调”表示一路调度数据网络通道，“1 综”表示一路综合数据网络通道。

将相对重要值代入式(3)，式(4)和式(5)，得到 13 种电力业务在区间 $[0.1, 1]$ 上的重要度值 Q_i 及排序， $i=1, 2, \dots, 13$ ，如表 2 所示。

表 2 中继电保护业务重要度最高，安稳系统、广域测量和调度自动化业务重要度仅次于继电保护，同时视频会议的重要程度应该高于一般的行政业务，其重要度在行政业务中排名最高。上述实例分析中典型电力业务的重要度计算结果与实际情况相符，验证了方法的正确性。

3 网络脆弱性多层次综合评价

3.1 业务层网络模型

定义网络模型为三元组 (G, R, W) 。 $G=(V, E)$ 为网络的拓扑结构， V 表示顶点集， E 表示无向边集； R 为网络的路由策略； W 为业务在网络中所有源宿节点之间的分布。在该网络模型中，所有节点是安

表1 电力业务指标要求及相对重要值

电力业务	性能指标要求/相对重要值 $f(k,b,q)$					
	时延	业务通道	误码率	实时性	可靠性	安全区
500 kV 继电保护	≤ 10 ms/8	每套主保护 1 专+1 专/7	$\leq 10^{-6}/3$	极高/3	极高/3	I 区/4
220 kV 继电保护	≤ 10 ms/8	两套主保护 1 专+1 专/6	$\leq 10^{-6}/3$	极高/3	极高/3	I 区/4
电能计量遥测	秒级/3	1 专+1 调/5	$\leq 10^{-6}/3$	低/1	极高/3	II 区/3
调度电话	≤ 150 ms/5	1 调+公网/4	$\leq 10^{-3}/1$	高/2	极高/3	I 区/4
调度自动化	≤ 100 ms/6	1 专+1 调/5	$\leq 10^{-6}/3$	高/2	高/2	I 区/4
安稳系统	≤ 30 ms/7	1 专+1 调/5	$\leq 10^{-7}/4$	极高/3	极高/3	I 区/4
保护信息管理(无远方设置)	≤ 15 min/2	1 调/3	$\leq 10^{-5}/2$	低/1	高/2	II 区/3
广域测量	≤ 30 ms/7	1 专+1 调/5	$\leq 10^{-9}/5$	高/2	高/2	I 区/4
雷电定位监测	≤ 250 ms/4	1 综/2	$\leq 10^{-5}/2$	低/1	高/2	III 区/2
变电站视频监控	≤ 150 ms/5	1 综/2	$\leq 10^{-3}/1$	高/2	高/2	III 区/2
办公自动化	无明确要求/1	1 综/2	$\leq 10^{-5}/2$	高/2	低/1	IV 区/1
行政电话	≤ 250 ms/4	无明确要求/1	$\leq 10^{-3}/1$	高/2	高/2	IV 区/1
视频会议	≤ 150 ms/5	1 综/2	$\leq 10^{-5}/2$	高/2	极高/3	IV 区/1

表2 电力业务重要度及排序

电力业务	Q_i /排序	电力业务	Q_i /排序	电力业务	Q_i /排序
500 kV 继电保护	1.00/01	220 kV 继电保护	0.95/02	安稳系统	0.91/03
广域测量	0.86/04	调度自动化	0.72/05	调度电话	0.57/06
电能计量遥测	0.53/07	视频会议	0.38/08	变电站视频监控	0.34/09
保护信息管理	0.29/10	雷电定位监测	0.29/11	行政电话	0.19/12
办公自动化	0.10/13				

全的, 仅考虑边的脆弱性对网络的影响。将网络边集与路径集之间的关系用矩阵 $\mathbf{D} = [d_{nm}]_{N \times M}$ 来表示, $N = |E|$, $M = C_{|V|}^2$, 矩阵的行向量对应网络中的边, 列向量对应网络中的源宿节点对, 当第 n 条边在第 m 个源宿节点对之间的路径上时, $d_{nm}=1$, 否则 $d_{nm}=0$ 。 w_m 表示第 m 个源宿节点对之间所有业务的业务重要度之和, 作为矩阵 \mathbf{D} 的列向量权重。边在业务层上的重要性用边业务重要度(EBI)来表示, 第 n 条边的 EBI 为

$$\text{EBI}_n = \sum_{m=1}^M w_m d_{nm} \quad (6)$$

3.2 传输层网络模型

定义网络模型为三元组 (G, R, T) 。 G , R 与 3.1 节中定义相同, T 为网络中所有源宿节点之间的流量分布。用 t_m 表示第 m 个源宿节点对之间所有业务的归一化流量之和。令 $t(b_i)$ 为业务 b_i 的单位流量, $t(b_i)_{\max}$ 为业务集 B 中的最大单位流量, 则业务 b_i 归一化流量为

$$t'(b_i) = \frac{t(b_i)}{t(b_i)_{\max}} \quad (7)$$

将 t_m 作为矩阵 \mathbf{D} 的列向量权重, 则边在传输层上的重要性用边流量重要度(ETI)来表示, 第 n 条边的

ETI 为

$$\text{ETI}_n = \sum_{m=1}^M t_m d_{nm} \quad (8)$$

3.3 攻击模型

已有的网络的攻击模型可分为蓄意攻击模型、随机攻击模型^[15]和区域攻击模型^[16,17]。蓄意攻击是网络攻击者最行之有效的攻击方式, 虽然根据业务分布情况对网络进行攻击的破坏性最大, 但攻击者一般对业务分布情况掌握较少, 而对网络的拓扑情况掌握较多, 因此会根据物理层信息对网络实施攻击。本文采用基于边介数^[18](Edge Betweenness, EB)的蓄意攻击模型(EB 值大的边优先被攻击)来分析电力通信网的脆弱性, 并以此证明边跨层信息熵(ECE)对电力通信网脆弱性评价的有效性。

设被攻击边集 E_x 由网络中 EB 值最大的前 x 条边组成, $x = 0, 1, \dots, N$ 。当 $x \geq 1$ 时, 令矩阵 \mathbf{D} 与 E_x 对应的行向量分别为 $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_x$, 则网络受到攻击后的损失为

$$\text{Loss}(E_x) = \frac{\sum_{m=1}^M ((1-\lambda)w_m + \lambda t_m) P_m}{\sum_{m=1}^M ((1-\lambda)w_m + \lambda t_m)} \quad (9)$$

其中 P_m 表示向量 P 的第 m 个元素, $P = e_1 \vee e_2 \vee \dots \vee e_x$, \vee 表示逻辑或运算, λ 为业务重要度与流量重要度的权重分配系数, 其定义为

$$\lambda = \exp\left(1 - \frac{a'_{i\max}}{a'_{i\min}}\right) \quad (10)$$

表示当网络中各类业务的重要度差别较小时, 网络的损失主要通过流量损失来描述, 反之, 则主要通过业务重要度损失来描述, $a'_{i\max}$ 和 $a'_{i\min}$ 的定义同式(4)。

3.4 边跨层信息熵

在网络受到攻击后, 网络真正的损失是其中传输的业务, 包括业务的重要度损失和业务的流量损失, 但攻击者大多基于物理层拓扑来进行破坏, 因此网络脆弱性的评价应该从攻击方式和网络损失两个方面来综合考虑。因此, 本文提出边跨层信息熵的概念。定义边的跨层重要度(ECI)为

$$ECI_n = EB_n \times EBTI_n \quad (11)$$

其中

$$EBTI_n = (1 - \lambda)EBI_n + \lambda ETI_n \quad (12)$$

式(11)综合考虑了边被攻击的概率和边被攻击后造成的损失: 当边的 EB 和 EBTI 值都很大时, 其 ECI 值很大, 说明该边容易受到攻击且被攻击后造成的损失很大; 当边的 EB 值很大, 但 EBTI 值很小时, 其 ECI 值较小, 说明该边虽然容易被攻击, 但造成的损失却较小; 当边的 EB 值很小, 但 EBTI 值很大时, 其 ECI 值也较小, 说明该边虽然被攻击后造成的损失很大, 但被攻击的概率很低, 其脆弱性也较小。

网络整体的脆弱性可通过 ECI 的分布情况来评价, 若 ECI 值过于集中在少数边上, 则这些边很容易被攻击, 且被攻击后的损失也非常大, 网络的脆弱性较高; 若 ECI 值在各边上的分布比较均衡, 则 EB 较大的边其 EBTI 值并不大, 受到攻击后的损失较小, 网络的脆弱性较低。本文利用 ECE 来描述

ECI 在网络中的分布情况, 并以此对电力通信网脆弱性做出评价。定义 ECE 为

$$ECE = \frac{\sum_{n=1}^N -ECI'_n \cdot \log_2(ECI'_n)}{\log_2(N)}, \quad ECE \in (0,1] \quad (13)$$

其中 ECI'_n 是 ECI_n 的归一化值, 即

$$ECI'_n = \frac{ECI_n}{\sum_{h=1}^N ECI_h} \quad (14)$$

网络的 ECE 值越大, 说明 ECI 值分布越均衡, 网络的脆弱性越低; 反之, 网络的脆弱性越高。

4 仿真分析

4.1 网络脆弱性分析

为简化计算, 将 2.3 节表 2 中的 13 种电力业务用其重要度序号来表示并将其分为 5 类: I = {1,2}, II = {3,4,5}, III = {6,7}, IV = {8,9,10,11}, V = {12,13}。每类业务中多种业务的重要度平均值和归一化流量平均值分别作为该类业务的重要度和单位流量, 得到 5 类业务的重要度向量(0.98, 0.83, 0.55, 0.33, 0.15)和流量向量(0.03, 0.08, 0.02, 0.52, 0.14), 13 种电力业务的单位流量可参见文献[19]。

网络的仿真配置如下: 拓扑结构 $G=(V,E)$ 如图 1 所示, 包含 14 个节点和 16 条链路。该网络拓扑源于广东电力通信传输骨干网, 其中 1 号节点为省级调度中心(中调), 13 号节点为地区调度中心(地调), 14 号节点为 220 kV 变电站, 其余节点均为 500 kV 变电站, 2 号、5 号和 7 号节点为汇聚节点, 链路权重为各站点之间实际距离; 网络的路由策略 R 为最短路径路由; 根据文献[20], 网络中的业务分布情况如表 3 所示, 各边的 EB, EBI, ETI 和 ECI 值如表 4 所示。

由表 1 和式(10)计算出 $\lambda = 0.1211$, 可知电力通信网中业务重要性差别较大, 网络的损失主要通过业务重要度的损失来刻画。由表 4 和式(13)计算出

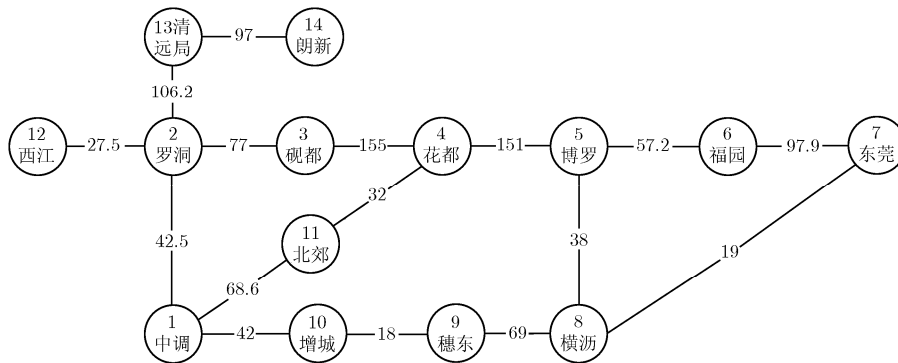


图 1 电力通信网拓扑结构

表 3 网络中的业务分布

节点对	类型×数量	节点对	类型×数量	节点对	类型×数量
(1,2)	II×15+III×10+IV×5+V×10	(1,10)	II×6+III×4+IV×2+V×4	(4,5)	I×1+V×2
(1,3)	II×9+III×6+IV×3+V×6	(1,11)	II×6+III×4+IV×2+V×4	(4,11)	I×1+V×2
(1,4)	II×6+III×4+IV×2+V×4	(1,12)	II×5+III×2+IV×1+V×2	(5,6)	I×1+V×2
(1,5)	II×15+III×10+IV×5+V×10	(1,13)	II×8+III×4+IV×6+V×5	(5,8)	I×1+V×2
(1,6)	II×6+III×4+IV×2+V×4	(13,14)	II×9+III×6+IV×12+V×6	(6,7)	I×1+V×2
(1,7)	II×18+III×12+IV×6+V×12	(2,3)	I×1+V×2	(7,8)	I×1+V×2
(1,8)	II×9+III×6+IV×3+V×6	(2,12)	I×1+V×2	(8,9)	I×1+V×2
(1,9)	II×6+III×4+IV×2+V×4	(3,4)	I×1+V×2	(9,10)	I×1+V×2

表 4 各边的 EB, EBI, ETI 和 ECI 值

边	EB	EBI	ETI	ECI	边	EB	EBI	ETI	ECI
1-2	43	50.94	14.50	2000.59	4-11	11	9.67	2.49	96.79
1-10	42	83.97	21.75	3210.40	5-6	12	9.67	2.49	105.59
1-11	16	16.80	4.35	244.60	5-8	21	30.66	7.93	586.08
2-3	11	13.87	3.58	138.83	6-7	1	1.27	0.31	1.15
2-12	13	7.12	1.57	83.84	7-8	12	26.46	6.84	289.04
2-13	24	11.50	4.55	255.73	8-9	34	68.45	17.71	2118.39
3-4	2	1.27	0.31	2.31	9-10	39	76.85	19.89	2728.02
4-5	6	1.27	0.31	6.93	13-14	13	15.52	7.90	189.78

该网络的 ECE 值为 0.6952, 此时网络在蓄意攻击下的脆弱性如图 2 所示。表 4 中, 网络的 ECI 值分布很不均匀, 最大值为 3210.40, 最小值仅为 1.15, 相差近 2792 倍, 说明该网络在遭受蓄意攻击下的脆弱性很高。从图 2 中可以看出, 仅 EB 值最大的两条边被攻击, 网络业务重要度损失就达到了 74.27%; 由于每个业务与多条边相关联, 被中断的业务不能在边失效过程中重复计算, 因此当 x 在区间[2,6]上时, 曲线的上升速度明显下降; 当 $x=8$ 时, 网络一半的边已经失效, 网络损失达到了 86.30%, 已基本瘫痪。曲线总的变化趋势是失效边较少的时候增长速度很快, 随着失效边数目的增加, 增长速度趋于平缓, 由此可见, EB 值较大的边是决定网络脆弱性的主要因素, 应该适当减少这些边上承载的业务重要度, 降低网络的脆弱性。

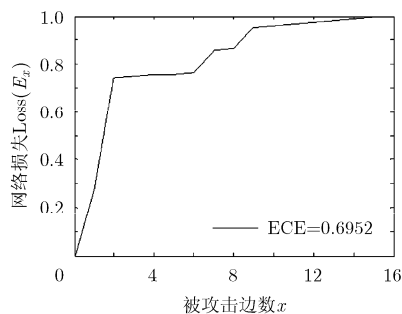


图 2 蓄意攻击下的网络脆弱性

4.2 基于 ECE 的脆弱性改进

通过上述分析, 发现提高 ECE 值必须使 ECI 在各边上的分布更加均匀, 而电力通信网中影响 ECI 值的主要因素是业务重要度。电力通信网源宿节点对之间的业务不能随便更改, 提高 ECE 值的有效途径只能是更改路由策略。

根据表 3 中的业务分布和表 4 中的 ECI 值, 本文对路由作了如下调整: 第 1 次调整, 将(1,5)之间的路由从 5-8-9-10-1 更改为 5-4-11-1; 第 2 次调整, 将(1,3)之间的路由从 3-2-1 更改为 3-4-11-1; 第 3 次调整, 将(1,7)之间 50% 的业务从 7-8-9-10-1 转移到路由 7-6-5-4-11-1 上。每次调整都以提高网络的 ECE 值为标准, 3 次调整后的 ECE 值分别为 0.7479, 0.7544 和 0.7901, 调整后各边最终 EB, EBI, ETI 和 ECI 值如表 5 所示。3 次调整对应的网络脆弱性曲线如图 3 所示。

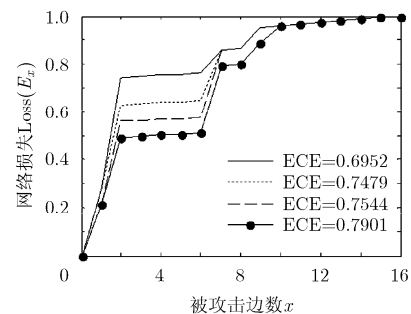


图 3 不同 ECE 下网络的脆弱性

表5 路由调整后各边的参数值

边	EB	EBI	ETI	ECI	边	EB	EBI	ETI	ECI
1-2	43	38.34	11.24	1507.56	4-11	11	54.20	14.07	542.71
1-10	42	48.73	12.67	1863.12	5-6	12	20.61	5.37	225.14
1-11	16	50.38	13.05	733.81	5-8	21	9.67	2.49	184.77
2-3	11	1.27	0.31	12.71	6-7	1	12.21	3.20	11.12
2-12	13	7.12	1.57	83.84	7-8	12	12.21	3.20	133.41
2-13	24	11.50	4.55	255.73	8-9	34	33.20	8.63	1027.73
3-4	2	13.87	3.58	25.24	9-10	39	41.60	10.81	1476.98
4-5	6	33.20	8.63	181.36	13-14	13	15.52	7.90	189.78

对比表4和表5,发现EBI的最大值从83.97下降至54.20,并且从EB值较大的边1-10,转移到了EB值较小的边4-11,这使得ECI的最大值从3210.40下降至1863.12,同时最小值从1.15上升至11.12,因此最大值最小值差距从2792倍下降至168倍,说明被攻击概率大的边上所承载的业务重要度转移到了相对安全的EB值较小的边上,降低了网络的脆弱性。图3中,3次调整使网络的ECE值不断提高,网络的脆弱性不断得到改进,对比ECE值为0.6952和0.7901两条脆弱性曲线: $x=1$ 时,业务损失从28.10%下降至21.57%; $x \in [2,6]$ 时,曲线比较平缓,业务损失平均下降了25.39%,网络的脆弱性得到了明显改善; $x \in [7,10]$ 时,虽然网络上业务损失的都已经很大,但后者还是优于前者。上述分析证明了用ECE对网络脆弱性进行评价是行之有效的办法,ECE值越高,网络的脆弱性越低,抵抗蓄意攻击的能力越强。

5 结论

将网络所承载的业务特性加入到脆弱性分析中,本文提出了一种基于信息熵的跨层脆弱性评价方法。为有效地将电力业务特性进行量化,给出了一种以电力业务性能指标相对差异为基础的业务重要度计算方法,并通过实例计算验证了方法的有效性。基于业务重要度,建立了电力通信网业务层模型,并将边所承载的业务重要度(EBI)作为边的业务层重要性指标。在蓄意攻击模型下,综合考虑被攻击概率和被攻击后的网络损失,将EBI与传输层重要性指标ETI,物理层重要性指标EB相结合提出了边跨层重要度(ECI)的概念。通过边跨层信息熵(ECE)来描述ECI在网络中的分布情况,ECE值越大,则ECI在网络中的分布越均衡,网络的脆弱性越低。结合电力通信网实例对不同路由策略下的网络脆弱性进行仿真,发现提高网络的ECE值可以使网络的脆弱性得到明显改善,也证明了用ECE值对网络脆弱性评价的有效性。

参考文献

- [1] Chvatal V. Tough graphs and Hamiltonian circuits[J]. *Discrete Mathematics*, 1973, 5(3): 215-228.
- [2] Bassalygo L A and Pinsker M S. The complexity of an optimal non-blocking communication scheme without reorganization[J]. *Problemy Peredai Informacii*, 1973, 9(1): 84-87.
- [3] Jung H A. Class of posets and corresponding comparability graphs[J]. *Journal of Combinatorial Theory Series B*, 1978, 24(2): 125-133.
- [4] Barefoot C A, Entringer R, and Swart H. Vulnerability in graphs — a comparative survey[J]. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1987, 1: 13-22.
- [5] Cozzens M, Moazzami D, and Stueckle S. The tenacity of a graph[C]. *Seventh International Conference on the Theory and Applications of Graphs*, New York, USA, 1995: 1111-1122.
- [6] Wu J, Barahona M, Tan Y J, et al. Natural connectivity of complex networks[J]. *Chinese Physics Letters*, 2010, 27(7): 295-298.
- [7] Dinh T N, Ying Xuan, Thai M T, et al. On new approaches of assessing network vulnerability: hardness and approximation[J]. *IEEE/ACM Transactions on Networking*, 2012, 20(2): 609-619.
- [8] 彭静, 卢继平, 汪洋, 等. 广域测量系统通信主干网的风险评估[J]. *中国电机工程学报*, 2010, 30(5): 84-90.
Peng Jing, Lu Ji-ping, Wang Yang, et al. Risk assessment of backbone communication network in WAMS[J]. *Proceedings of the CSEE*, 2010, 30(5): 84-90.
- [9] 刘文霞, 罗红, 张建华. WAMS通信业务的系统有效性建模与仿真[J]. *中国电机工程学报*, 2012, 32(16): 144-150.
Liu Wen-xia, Luo Hong, and Zhang Jian-hua. Modeling and simulation on effectiveness of communication services system in WAMS[J]. *Proceedings of the CSEE*, 2012, 32(16): 144-150.
- [10] 金鑫. 电力通信传输网业务可靠性分析方法研究[D]. [硕士论文], 华北电力大学(保定), 2010: 7-18.
Jin Xin. Research on service reliability analysis method of

- electric power communication transmission network[D]. [Master dissertation], North China Electric Power University (Baoding), 2010: 7-18.
- [11] 赵子岩, 刘建明. 基于业务风险均衡度的电力通信网可靠性评估算法[J]. 电网技术, 2011, 35(10): 209-213.
Zhao Zi-yan and Liu Jian-ming. A new service risk balancing based method to evaluate reliability of electric power communication network[J]. *Power System Technology*, 2011, 35(10): 209-213.
- [12] 曾庆涛, 邱雪松, 郭少勇, 等. 基于风险均衡的电力通信业务的路由分配机制[J]. 电子与信息学报, 2013, 35(6): 1318-1324.
Zeng Qing-tao, Qiu Xue-song, Guo Shao-yong, *et al.* Risk balancing based routing mechanism for power communication service[J]. *Journal of Electronics & Information Technology*, 2013, 35(6): 1318-1324.
- [13] 刘健, 刘思峰, 周献中, 等. 基于相似关系的多属性决策问题研究[J]. 系统工程与电子技术, 2011, 33(5): 1069-1072.
Liu Jian, Liu Si-feng, Zhou Xian-zhong, *et al.* Research on multiple-attribute decision making problems based on similarity relationship[J]. *Systems Engineering and Electronics*, 2011, 33(5): 1069-1072.
- [14] 中国南方电网系统运行部. Q/CSG1 10020-2011-南方电网通信网络生产应用接口技术规范[S]. 广东: 中国南方电网有限责任公司, 2012.
System Operation Department of CSG. Q/CSG1 10020-2011-Application of communication network interface technical specifications of CSG[S]. Guangdong: China Southern Power Grid, 2012.
- [15] Yehuda V and Zhang C H. Measures of network vulnerability [J]. *IEEE Signal Processing Letters*, 2007, 14(5): 313-316.
- [16] Peng W, Li Z, LiuxY, *et al.* Assessing the vulnerability of network topologies under large-scale regional failures[J]. *IEEE Journal of Communications and Networks*, 2012, 14(4): 451-460.
- [17] Wang X, Jiang X, and Pattavina A. Assessing network vulnerability under probabilistic region failure model[C]. IEEE 12th International Conference on High Performance Switching and Routing (HPSR), Cartagena, Spain, 2011: 164-170.
- [18] Igor M, Mario B, and Ljupco K. Vulnerability of complex networks[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2011, 16: 341-349.
- [19] 广东电网公司电力调度通信中心. 广东电网公司“十二五”二次系统规划[EB/DK]. 广东: 广东电网公司, 2010.
Power dispatch and control Center of Guangdong Power Grid Corporation. The power secondary system part of the 12th five-year plan of Guangdong Power Grid Corporation [EB/DK]. Guangdong: Guangdong Power Grid Corporation, 2010.
- [20] 中国南方电网计划发展部. 中国南方电网公司 220 千伏及以上电网规划技术原则系统二次部分[EB/DK]. 广东: 中国南方电网有限责任公司, 2009.
Planning and Development Department of CSG. The technical principles of instrumentation and control part for 220kV and above power grid planning of CSG[EB/DK]. Guangdong: China Southern Power Grid, 2009.
- 樊冰: 男, 1977年生, 博士生, 讲师, 研究方向为电力通信网规划、电力通信网可靠性和保密通信.
- 曾瑛: 女, 1972年生, 工程师, 研究方向为电力系统通信网络运维与管理.
- 唐良瑞: 男, 1966年生, 博士生导师, 教授, 研究方向为电力系统通信与信息处理、无线传感器网络及其在智能电网中的应用.