DOI: 10.7667/PSPC180226

基于边临毁度的电力通信网脆弱性分析

廖一名，李珊君

(四川大学电气信息学院，四川 成都 610065)

摘要：电力通信网脆弱性分析对确保电力系统安全运行和加强电网健壮性具有重要意义。首先建立了电力通信网络模型，从网络的业务层、网络传输层和物理层指标出发，建立了基于临毁度和网络损失度的电力通信网的脆弱性评估和分析模型。接着对边的业务传输时延指标、带宽占比指标和物理故障概率指标评估得出网络部件(节点、边)的临毁度。最后结合网络部件失效后的系统损失度，得出网络部件的脆弱度评估值。以 IEEE-30 节点系统为例进行仿真，完成了通信网络部件的脆弱性评估分析，结果表明通信链路的长度和业务分配方案与电力通信网的脆弱性密切相关。

关键词：电力通信网；脆弱性分析；临毁度；系统损失度

Vulnerability analysis of power communication network based on invalid proximity of edge

LIAO Yiming, LI Shanjun

(School of Electrical Engineering and Information, Sichuan University, Chengdu 610065, China)

Abstract: Vulnerability analysis of power communication network has important significance to ensure the safe operation of the power system and strengthen the network robustness. First, power communication network model is built. Based on the network business layer, network transmission layer and physical layer index, the vulnerability assessment and analysis model of power communication network based on the degree of destruction and network loss is established. Then invalid proximity of communication nodes and edges then can be got by analyzing the indicators such as proximity degree of services' invalid, bandwidth proportion and physical failure probability of communication side. Finally, the vulnerability value of nodes and edges can be got by combining with the loss degree of the system after the failure of network components. The vulnerability analysis of communication network is completed by taking the IEEE-30 node system as a simulation example. The results show that the length and service allocation scheme of communication links are closely related to the vulnerability of power communication network.

This work is supported by Science and Technology Support Plan Project of Sichuan Province (No. 2017GZ0349) and Science and Technology Project of State Grid Xinjiang Electric Power Company (No. SGXJXT00TJS1600206).

Key words: power communication network; vulnerability analysis; invalid proximity; loss degree of the system

0 引言

近年来，电网的信息化、自动化和互动化趋势愈发明显，对电力通信网的安全性、稳定性和自愈性提出了更高的要求[1-4]。脆弱性作为网络系统安全性的一种评估方式[5-7]，得到了越来越多的关注。网络的脆弱性指网络易于攻击威胁的程度和遭受攻击威胁的损失程度[8]。

电力通信网络的脆弱性主要表现在两个方面[9]：1) 电力通信业务普遍具有较高的实时性要求[10-13]，特别是继保业务和电力控制类业务，一旦满足不了实时性要求，业务就会失效，从而对电力通信网造成严重的影响。2) 电力通信网构建不具有规划性[14-17]，导致网络业务分配不均，个别网络区域业务较多。从而导致网络各局部运行状态不一，局部故障后造成的系统损失不一。电力通信网脆弱性分析过程是对网络系统中的隐患和漏洞因素进行评

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

估，以达到对网络脆弱环节的识别。脆弱性分析结果能为电力通信网络的维护检修、设备更新以及消除薄弱环节等提供依据，具有现实意义。

目前电力通信网脆弱性的研究主要有两种思路。基于复杂网络理论的脆弱性研究，主要研究复杂网络指标的统计特征，用到的复杂指标有连通度、介数、紧密度等。文献[18]通过效能函数和最大子图连通度来描述网络脆弱性。文献[19]从物理层面和拓扑结构对脆弱性进行评估。但仅考虑网络拓扑结构不能反映出电力通信业务的脆弱性。近年来，已有学者考虑电力通信业务进行脆弱性研究。文献[20]从单一业务角度出发，提出了融合多种风险影响要素的 WAMS(广域测量系统)通信主干网的风险评估模型和计算方法。文献[21]提出基于攻击模型，综合业务重要和业务流量重要度评价网络脆弱性。文献[22]用 OPNET 仿真软件模拟电力通信业，提取仿真中时延、网络利用率等指标，提出了考虑业务传输性能和网络性能的脆弱性评估方法。这些方法从业务角度评估分析了电力通信网的脆弱性，但都忽略了线路故障带来的脆弱性。对于远距离传输的电力通信网，线路故障应是考虑的重要因素。

在前人基础上，本文综合考虑业务层、网络传输层和物理层性能指标，结合网络部件故障后的网络损失，提出了基于边临毁度的电力通信网络的脆弱性分析方法。

1　电力通信网络模型

结合图论知识，对电力通信网进行简化。将电力通信站点等效为网络节点，通信链路等效为网络的边。忽略链路间差异，将链路长度作为边权值。由于业务数据在链路上双向传输，可将电力通信网简化成一个有权无向图。

定义电力通信网络模型为三元组 $G=(T,S,R)$。$T=(N,\boldsymbol{V},E)$ 表示网络拓扑结构，$N=\{1,2,\cdots,n\}$ 为节点序号集，n 为网络节点个数。$\boldsymbol{V}=\left[v_{ij}\right]_{n\times n}$ 为节点连接矩阵，v_{ij} 表示 i,j 号节点间连接状态，i,j 为网络中两个节点的序号，当 $i=j$ 或 i,j 节点间无链路连接时，$v_{ij}=0$，否则 $v_{ij}=1$。$E=(I,L,C)$ 表示网络的边，I 为边序号集。边序号按如下规则生成：用边链路两端节点对序号表示边，即 $(i,j),i<j$。将 i,j 作为十进制数的十位和个位，则每条边对应一个数。将这些数排序，令最小数对应边的序号为 1，次最小数对应边的序号为 2，依次升序编号。L 为边权值向量，向量元素表示边链路的长度。C 为边容量向量，向量元素表示边链路的带宽容量。

$S=(Th,In,B,Len,D)$ 表示网络中电力通信业务。为业务时延阈值向量，向量元素表示业务传输时延阈值，表示业务在路径上的传输时延必须在该时间阈值内。为业务重要度归一化向量，向量中元素数值和为 1。B 为业务带宽向量，向量元素表示业务占用带宽。为业务数据包长度，向量元素表示业务数据包的字节长度。$D=\{(S_{ki},s_{ki},d_{ki})\}$ 表示业务分合，S_{ki} 为第 i 个 k 类业务，s_{ki} 为该业务源节点，d_{ki} 为该业务宿节点。R 为业务路由选择策略。

2　电力通信网指标

2.1 业务分析

电力通信网承载了电力系统全部电力通信业务。不同业务对网络实时性、可靠性和安全性要求也不同，其对电力系统的重要程度也不同。本文考虑部分电力通信业务[22]，有广域继电保护(S1)、低频减载预测(S2)、广域阻尼功率振荡控制(S3)、闭环稳定控制服务(S4)、广域电压稳定性监测服务(S5)和基于 PMU 的状态估计服务(S6)等 6 种业务。

2.1.1 业务重要度

目前对于电力业务重要度评估方法已有多种，本文采取文献[23]的专家评分法，假设有 m 种业务，有业务重要度向量 In 为

$$In=\left[In_1\ In_2\cdots In_m\right] \tag{1}$$

2.1.2 业务传输时延

根据文献[24]，业务在边链路上的传输时延由发送时延、传播时延和排队时延三部分组成。i 类业务在 k 边上的传输时延为

$$t_{ki}=t_i+t_k+t_{qk} \tag{2}$$

式中：t_i 为 i 业务的发送时延；t_k 为业务在 k 边上的传播时延；t_{qk} 为业务在 k 边的排队时延。计算如式(3)。

$$\begin{cases} t_s=\dfrac{len_i}{B_i} \\ t_t=\dfrac{uL_k}{c} \end{cases} \tag{3}$$

式中：len_i 为业务的报文长度；B_i 为 i 业务带宽；u 为光纤链路长度修正系数，取 1.05；c 为光纤信号传输速度；L_k 为 k 边权值。排队时延在仿真中获取。

2.2 边介数

边介数为网络中所有最短路径中经过某边的数目占最短路径总数的比例，反映了相应的节点或边在整个网络中的重要度

$$w_i=\frac{2n_i}{n(n-1)} \tag{4}$$

式中：w_i 为 k 边的边介数；n_i 为网络中所有最短路

径中经过 k 边的数目； n 为网络节点数。

3 电力通信网脆弱性评价方法

3.1 电力通信网脆弱性

在研究电力通信网脆弱性时，考虑网络部件(节点、边)易于攻击威胁的程度和网络部件失效后系统损失程度两个方面的因素。

3.2 临毁度

评估网络易于攻击威胁的程度时，以业务层、网络传输层和物理层上易于攻击威胁的程度之和定义了临毁度指标。

3.2.1 通信边业务临近度

分析业务层实时指标，业务在边上传输时延越接近该业务的时延阈值，其承受攻击的能力越弱，就越容易引起攻击者注意并加以利用，故其临近失效的可能性就越大。本文定义业务在通信边上的传输时延接近业务时延阈值的程度为边的业务临近度，表示其易于攻击威胁的程度，计作 R 。

$$R_{ki}=\begin{cases}\dfrac{t_{ki}}{Th_i}, & t_{ki}<Th_i\\ 1, & t_{ki}\geq Th_i\end{cases} \tag{5}$$

式中：R_{ki} 表示 i 业务在 k 边上时延临近度；Th_i 为 i 类业务的时延阈值。考虑该边上最大的业务临近度值，综合各类业务临近度值，得到边链路的综合业务临近度为

$$R_k=\varepsilon_R\frac{\sum_k R_{kn}}{m}+(1-\varepsilon_R)R_{k\_\max} \tag{6}$$

式中： R_k 为 k 边综合业务临近度； $R_{k\_\max}$ 为 k 边各业务临近度值的最大值；ε_R 业务临近度最大值所占的权重因子，在[0,1]取值，本文仿真时取0.5。

以前面6个业务为例，假设各业务传输时延相等，可得到边的业务平均传输时延和临近度的趋势，如图1。当时延大于最小业务时延阈值5 ms，业务出现损失。故可用5 ms平均时延对应临近度值0.708 3为临界值，当临近度超过该临界值时，认为该边处于危险状态。

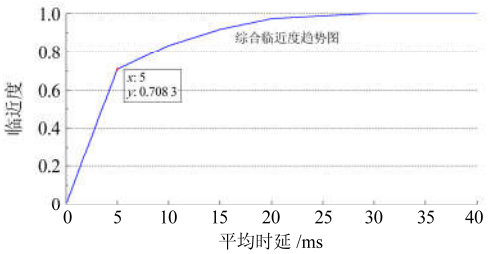

图 1 临近度趋势图

Fig. 1 Trend graph of comprehensive proximity

3.2.2 通信边临毁度

边链路的带宽占比间接反映了链路的链路利用率。带宽占比越大，运行中的边链路的利用率就可能越高，该边链路越易于攻击威胁。根据边链路传输的业务数量，可得边链路带宽占比

$$\eta_k=\frac{\sum_{i=1}^{m}n_{ki}B_i}{C_k} \tag{7}$$

式中： C_k 为 k 边的带宽容量； n_{ki} 为 k 边上 i 类业务的数量。

光纤线路故障会给链路带来根本性的损害，故障概率越大，物理链路就越易于攻击威胁。文献[8]指出光纤失效率主要与光纤长度有关，并给出了估算公式

$$P_k=L_k\cdot(MTTR\times FIT)/10^9 \tag{8}$$

式中： FIT 为光纤的失效率； $MTTR$ 为失效修复需要的时间； L_k 为 k 边对应光纤长度。

边的综合业务临近度、带宽占比和光纤故障概率分别反映了边在业务层、网络传输层和物理层上易于攻击威胁的程度。由于这三个指标量纲不同，对其进行如下归一化。

$$f_k'=\begin{cases}\dfrac{f_k}{f_m} & f_k<f_m\\ 1 & f_k\geq f_m\end{cases} \tag{9}$$

式中， f_m 为设定的指标门限值，当超过门限值时，该指标归一化值最大值为 1。根据临毁度定义，得到指标归一化值后，对其求均值可得边临毁度为

$$U_k=\frac{R_k'+\eta_k'+p_k'}{3} \tag{10}$$

式中， U_k 表示 k 边的临毁度。

3.3 节点临毁度

节点在网络结构中的复杂性，使其临毁度与以其为中心的局域网络分不开。假定节点物理故障概率为 0，只考虑节点和与该节点直接相连的边组成的星形网络，以周围各边的临毁度为指标，考虑最大的边临毁度，可求出节点临毁度为

$$U_n=\varepsilon_U\frac{\sum_{k\in E_n}U_k}{Q(E_n)}+(1-\varepsilon)U_{n\_\max} \tag{11}$$

式中： E_n 为与 n 节点直接相连的边集合； $U_{n\_\max}$ 为 E_n 中最大临毁度；$Q(E_n)$ 为集合 E_n 里元素个数；ε_U 为临毁度权重因子，在[0,1]间取值，本文取 0.5。

3.4 通信边、节点损失度

网络部件故障失效后，会造成所有流经该网络部件的业务源宿通路断开，引起网络资源重新分配。

前后两个网络状态的通信边传输时延和网络带宽占比也会产生相应变化，甚至是业务损失。因此在考虑网络部件故障带来的网络损失时应考虑以上两个因素。

首先是业务损失量，k 部件故障后，若某业务源宿节点间无通路，或源宿节点间传输时延不满足系统实时性要求时，视该业务损失。令 L_k 为 k 部件故障后业务损失量，则

$$L_k = \sum_{i=1}^{m} n_{ki} In_i \tag{12}$$

式中：In_i 为 i 类业务的重要度；n_{ki} 为 k 部件故障后 i 类业务损失数量。

本文用单元故障模型模拟网络遭受攻击的情形，一次去掉网络的一个部件，记录故障前后指标变化。用波动概念来描述故障前后业务传输时延和网络带宽占比指标的变化。故障前后业务临近度(带宽占比)的变化称为边的临近度(带宽占比)波动。若故障后的临近度(带宽占比)小于之前的业务临近度(带宽占比)，则称这个波动为正向波动。反之为反向波动。为突出网络部件故障带来的损失，只考虑指标反向波动。则指标的反向波动幅度如下。

$$\begin{cases} B_{Ri} = R_{i\_\text{new}} - R_{i\_\text{old}} \\ B_{\eta i} = \eta_{i\_\text{new}} - \eta_{i\_\text{old}} \end{cases} \tag{13}$$

式中：R_{i_old} 和 R_{i_new} 为故障前后 i 边综合业务临近度和带宽占比；η_{i_old} 和 η_{i_new} 为故障前后 i 边综合业务临近度和带宽占比。对结果按式(10)进行归一化。考虑部件 k 故障后所有出现两指标反向波动的边，可得总的网络性能损失。

$$N_k = \sum_{i \in E_k} \left(B'_{\eta i} + B'_{\mathrm{R}i} \right) w_i \tag{14}$$

式中：w_i 为 i 边的边介数；$B'_{\eta i}$ 和 $B'_{\mathrm{R}i}$ 为两指标波动归一化值；E_k 为 k 部件损失后两个指标产生反向波动的通信边集合。

综上，网络部件失效系统损失量为

$$C_k = L_k + N_k \tag{15}$$

3.5 通信边、节点脆弱度

根据脆弱性定义，综合部件临毁度和网络部件故障后网络损失度，得到网络部件的脆弱度为

$$V_k = U_k + C_k \tag{16}$$

式中：V_k 为通信部件 k 的脆弱度；U_k 为通信部件 k 的临毁度。

4　算例仿真

4.1 网络拓扑

仿真时采用 IEEE30 节点电力测试系统，其网络拓扑如图 2，共 26 个网络节点，38 条通信边，边上数值表示对应链路的长度。通信边的具体信息见表 1，其中序号为 4、5、9、10、12、16 的通信边为系统汇聚层通信边。电力通信业务相关参数见表 2，采用最短路由策略。网络中业务分布见表 3。 在计算临毁度时，设置指标门限值为：综合业务临近度 0.708 3，带宽占比 20%，边失效概率 0.005。

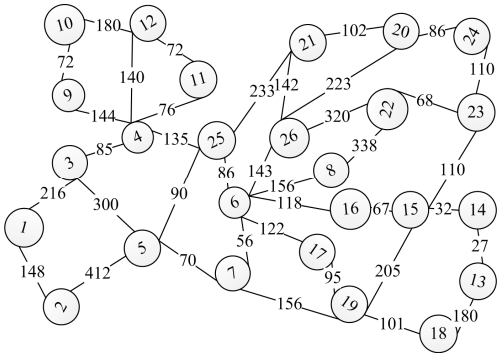

图 2 IEEE30 节点系统通信网拓扑图

Fig. 2 Topology graph of IEEE30 node system

表 1 通信边信息

Table 1 Communication edge information

边	长度/km	容量/Mbs	边	长度/km	容量/Mbs
1	148	155	20	72	1 250
2	216	155	21	180	1 250
3	412	155	22	72	1 250
4	85	155	23	27	1 250
5	300	155	24	180	1 250
6	144	155	25	32	1 250
7	76	256	26	32	1 250
8	140	256	27	205	1 250
9	135	256	28	110	1 250
10	70	1 250	29	95	1 250
11	90	1 250	30	101	1 250
12	56	1 250	31	102	1 250
13	156	1 250	32	86	1 250
14	118	1 250	33	223	1 250
15	122	1 250	34	233	1 250
16	86	1 250	35	142	1 250
17	143	1 250	36	68	1 250
18	156	1 250	37	320	1 250
19	338	1 250	38	110	1 250

表 2 业务信息

Table 2 Service information

业务	时延阈值/ms	重要度	数据长度/bit	带宽/kbs
S1	5	0.354 6	1 625	2 000
S2	20	0.185 9	1 500	1 000
S3	15	0.135 4	1 650	500
S4	20	0.163 2	1 700	2 000
S5	30	0.062 3	1 450	500
S6	10	0.098 6	1 550	2 000

表 3 业务分布

Table 3 Service distribution

业务	业务源宿节点集合
S1	(1,3)(1,2)(2,1)(2,5)(2,4)(2,6)(3,1)(3,4)(4,3)(4,2)(4,6)(4,9)(4,10)(4,11)(5,2)(5,7)(6,4)(6,7)(6,2)(6,8)(6,15)(6,12)(6,16)(6,17)(6,17)(6,22)(7,6)(7,5)(8,22)(8,6)(9,4)(9,10)(10,9)(10,4)(11,4)(11,12)(12,11)(12,6)(13,14)(14,13)(14,15)(15,14)(15,6)(16,6)(16,17)(17,16)(17,6)(17,6)(17,19)(18,19)(19,18)(19,17)(20,22)(20,21)(21,20)(22,20)(22,23)(22,24)(22,8)(22,6)(23,22)(23,24)(24,23)(24,22)
S2	(2,25)(3,25)(4,25)(5,25)(6,25)(7,25)(9,25)(10,25)(11,25)(12,25)(13,25)(14,25)(15,25)(16,25)(17,25)(18,25)(19,25)(26,25)(8,26)(21,26)(20,26)(24,26)(23,26)(22,26)
S3	(1,25)(2,25)(4,25)(5,25)(6,25)(8,25)(2,1)(1,2)(5,2)(2,5)(6,6)(6,8)(4,2)(2,4)(6,5)(5,6)
S4	(1,25)(2,25)(3,25)(4,25)(5,25)(6,25)(7,25)(9,25)(10,25)(11,25)(12,25)(13,25)(14,25)(15,25)(16,25)(17,25)(18,25)(19,25)(26,25)(8,25)(21,25)(20,25)(24,25)(23,25)(22,25)(8,26)(21,26)(20,26)(24,26)(23,26)(22,26)
S5	(1,1)(2,2)(3,3)(4,4)(5,5)(6,6)(7,7)(9,9)(10,10)(11,11)(12,12)(13,13)(14,14)(15,15)(16,16)(17,17)(18,18)(19,19)(8,8)(21,21)(20,20)(24,24)(23,23)(22,22)
S6	(1,1)(2,2)(3,3)(4,4)(5,5)(6,6)(7,7)(9,9)(10,10)(17,17)(18,18)(19,19)(26,26)(8,8)(21,21)(20,20)(22,22)

4.2 仿真分析

根据以上设置，通过 Matlab 编程仿真可得以下结果。

根据仿真结果，分析如下：

(1) 图 3 是通信边业务数量负载图，可以看到 1、4、9、12、14、16、20、26、36 边承载的业务数量超出其他边。其中 4、9、12、16 边位于汇聚层，1、14、20、26、36 边处于业务传输必经之路上。图 4 和图 5 分别为业务在通信边上传播时延和通信边综合业务临近度。对二者做相关分析得相关度为 0.987 9，可知边业务时延临近度主要反映了通信边传播时延的情况。这是因为一般情况下，网络状况良好，业务传输过程中的排队时延是微秒级的，占传输时延很小一部分。图 6 是通信边带宽占比，各边带宽占比均小于 10%。图中 1、14、20、26、36 边带宽占比较高，这与(1)中业务负载较大的通信边是一致的。其中位于汇聚层的 9、12、16 边由于带宽容量较大而带宽占比较小。图 7 是通信边链路失效概率，其中 3、5、19、37 边对应链路长度较大，其失效概率也较大。

(2) 图 8 和图 9 是通信边临毁度和节点临毁度。从图 8 可以看出，将通信边临毁度与通信边临近度、带宽占比和故障概率做相关分析，相关度分别为 0.891 0、0.097 0、0.887 8。该结果主要反映出通信边在传输时延和物理可靠性的脆弱程度。3、19、37 边业务临近度和故障概率值排序均相对较高，导致其边链路节点临毁度值较高。图 9 中，节点 1 和 2 直接相连边序号分别是 1、2 和 1、3，由于 3 边的临毁度高于 2 边，故节点 2 的临毁度大于节点 1。而节点 2 和 5 的相连边分别是 1、3 边和 3、5、10、11 边，其中 5、10、11 边脆弱性较低。1、3 边临毁度均值大于 3、5、10、11 边临毁度均值，故节点 2 临毁度大于节点 5。而节点 2、5、8、22、26 的节点相连边中均有临毁度值较高的 3、19、38 边，这些节点的临毁度值也相对较高。

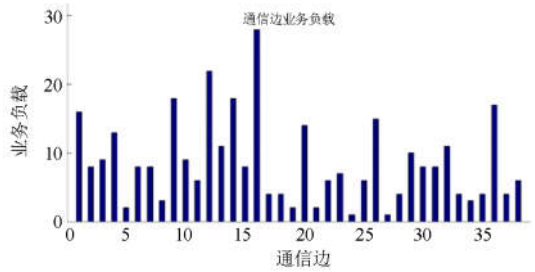

图 3 通信边业务负载

Fig. 3 Service load on the communication edges

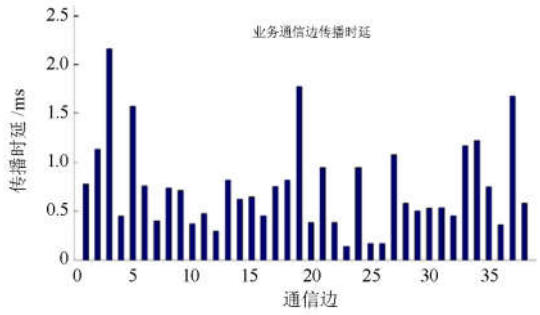

图 4 业务通信边传播时延

Fig. 4 Propagation delay of communication edges

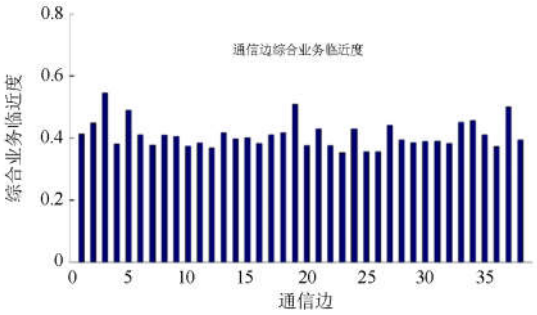

图 5 通信边综合业务临近度

Fig. 5 Integrated time delay of communication side services

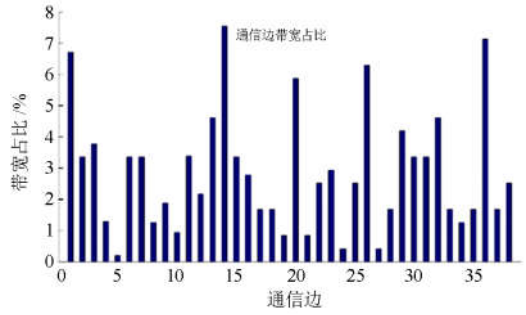

图 6 通信边带宽占比

Fig. 6 Bandwidth ratio of communication edges

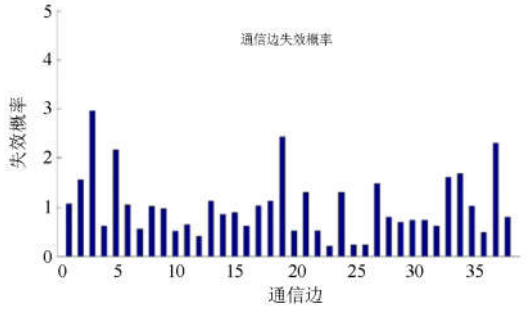

图 7 通信边失效概率

Fig. 7 Failure probability of communication edges

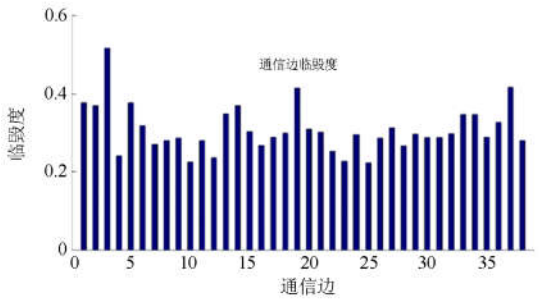

图 8 通信边临毁度

Fig. 8 Invalid proximity of communication edges

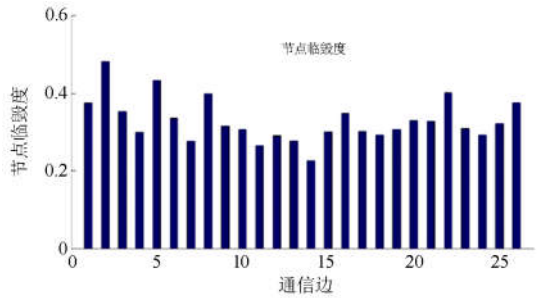

图 9 节点临毁度

Fig. 9 Invalid proximity of communication nodes

(3) 图 10 分别是通信边损失度和节点损失度。可以看到只有 1、2、13、36 边失效会产生业务损失，其他通信边失效只产生网络性能的下降。而节点失效后，都会产生业务损失，且业务损失占了很大比重，网络性能下降引起的损失则相对较小。从图中可见，节点损失度大于通信边损失度。因此在后期维护时应着重于节点的保护、业务分配和通信边的网络性能提升、保护。

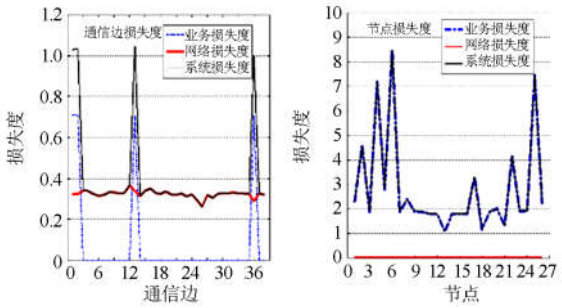

图 10 通信边、节点系统损失度

Fig. 10 System loss degree of communication edges and nodes

(4) 图 11 是通信边和节点的脆弱度。对比图 11，可发现通信边的脆弱性与边的业务损失度类似，1、2、13、36 边故障后的损失度较高，其脆弱值就被排在了前面。而 3、20、37 边则是由于临毁度较高，脆弱值得到了提升，脆弱值相对较高。因此需对这些边进行业务的重新分配甚至局部网络重新构建。对于节点的脆弱值情况，将节点脆弱值、临毁度和损失度一起分析，可见节点脆弱结果主要表现了节点故障后的损失度，而临毁度则对脆弱结果起到了修正作用。如节点 4 的损失度大于节点 2，但节点 2 的临毁度最高，加以修正后节点 2 的脆弱值超过节点 4。

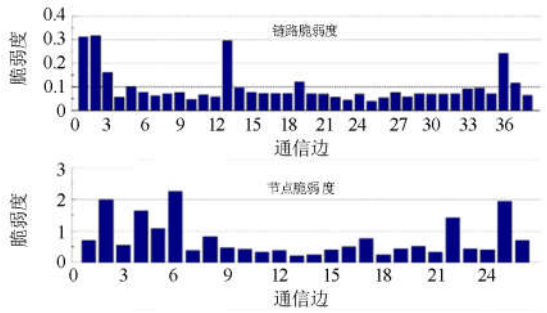

图 11 通信边、节点脆弱度

Fig. 11 Vulnerability of communication edges and nodes

5 结论

本文将业务传输时延、链路宽带占比和光纤故障率作为通信网业务层、网络层和物理侧脆弱性指标评估指标，提出了一种基于临毁度和业务损失度

的脆弱性评价方法。用 IEEE-30 电力节点测试系统进行通信系统仿真，结果表明网络部件的脆弱性与业务分布、链路长度和链路带宽容量有关，评估结果能够合理反映网络部件的脆弱性，验证了该方法的有效性。

参考文献

[1] 王汪兵, 王先培, 尤泽樟, 等. 电力通信网关键节点辨识方法研究[J]. 电力系统保护与控制, 2018, 46(1): 44-49.
WANG Wangbing, WANG Xianpei, YOU Zezhang, et al. Research on key node identification method in electric power communication network[J]. Power System Protection and Control, 2018, 46(1): 44-49.

[2] 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, 29(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.

[3] 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, 29(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.

[4] 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.

[5] 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.

[6] 苘大鹏. 网络系统安全性评估技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2009.
QING Dapeng. Research on security assessment technology of network system[D]. Harbin: Harbin Engineering University, 2009.

[7] 何玉钧, 刘毅, 周生平. 基于物元可拓模型的电力通信网风险评估[J]. 电力系统保护与控制, 2017, 45(14): 64-69.
HE Yujun, LIU Yi, ZHOU Shengping. Risk evaluation for electric power communication network based on matter-element extensible model[J]. Power System Protection and Control, 2017, 45(14): 64-69.

[8] 王明俊. 自愈电网与分布能源[J]. 电网技术, 2007, 31(6): 1-7.
WANG Mingjun. Self-healing grid and distributed energy resource[J]. Power System Technology, 2007, 31(6): 1-7.

[9] 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.

[10] 杨海健. 电力通信网的可靠性研究[D]. 西安: 西安电子科技大学, 2013.
YANG Haijian. Research on the reliability of power communication network[D]. Xi'an: Xi'an Electronic and Science University, 2013.

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

[12] 吴路明, 裘愉涛, 陈琦. 基于 SDN 的电力通信网络关键技术综述[J]. 电力工程技术, 2018, 37(3): 134-144.
WU Luming, QIU Yutao, CHEN Qi. The critical technology of the electric power telecommunication based on SDN[J]. Electric Power Engineering Technology, 2018, 37(3): 134-144.

[13] 丁力, 陈建松, 袁涛. 一种基于物理层的光纤通信断链快速监测方法[J]. 电力工程技术, 2017, 36(4): 103-107, 118.
DING Li, CHEN Jiansong, YUAN Tao. A fast monitoring method for optical fibre communication link based on physical layer[J]. Electric Power Engineering Technology, 2017, 36(4): 103-107, 118.

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

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

[16] 季知祥, 邓春宇. 面向电力大数据应用的专业化分析技术研究[J]. 供用电, 2017(6): 32-37.
JI Zhixiang, DENG Chunyu. Big data analytics technology research for power applications[J]. Distribution & Utilization, 2017(6): 32-37.

[17] 仝新宇, 孟凡杰, 孙志达, 等. 基于电力系统大数据平台的安全管控机制探讨[J]. 供用电, 2017(12): 48-52.
TONG Xinyu, MENG Fanjie, SUN Zhida, et al. Discussion on security management and control mechanism based on power system big data platform[J]. Distribution & Utilization, 2017(12): 48-52.

[18] DEKKER A H, COLBERT B D. Network robustness and graph topology[C] // Australasian Conference on Computer Science, Australian Computer Society, Inc., 2004: 359-368.

[19] 郭静. 基于复杂网络理论的电力通信网脆弱性分析[D]. 保定: 华北电力大学, 2010.
GUO Jing. Vulnerability analysis on power communication network based on complex network theory[D]. Baoding: North China Electric Power University, 2010.

[20] 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(4): 84-90.
PENG Jing, LU Jiping, WANG Yang, et al. Risk assessment of backbone communication networks in WAMS[J]. Proceedings of the CSEE, 2010, 30(4): 84-90.

[21] 孙静月, 崔力民, 李珊君. 基于业务的电力通信网络脆弱性分析评价方法[J]. 电力系统保护与控制, 2017, 45(24): 138-145.
SUN Jingyue, CUI Limin, LI Shanjun. Vulnerability evaluation method of electric power communication network based on business[J]. Power System Protection and Control, 2017, 45(24): 138-145.

[22] 刘焱滨. 计及通信网络影响的电力系统连锁故障分析[D]. 成都: 西南交通大学, 2017.
LIU Yanbin. Power system cascading failure analysis considering the effect of communication network[D]. Chengdu: Southwest Jiaotong University, 2017.

[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] 冯春燕, 李金岭. ATM 网络呼叫建立时延的估算[J]. 北京邮电大学学报, 2000, 23(1): 31-35.
FENG Chunyan, LI Jinling. An estimation of call setup delay in ATM network[J]. Journal of Beijing University of Posts and Telecommunications, 2000, 23(1): 31-35.

收稿日期：2018-03-05；　修回日期：2018-05-14

作者简介：

廖一名(1993—)，男，硕士研究生，研究方向为现代信号处理；E-mail: 727704323@qq.com

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

(编辑　姜新丽)