doi:10.11835/j.issn.1000-582X.2022.05.004

基于 CML 的智能变电站设备节点网络连锁失效模型

王 胜[1],张 颉[1],唐 超[1],张凌浩[1],王 海[1],唐 勇[1],
柴继文[1],郑永康[1],邓 平[2],曹亮[3],柯亚文[4]
(1. 国网四川省电力科学研究院,四川成都 610072;2. 国网自贡供电公司,四川自贡 643000;
3. 国网甘孜供电公司,四川甘孜 626700; 4. 重庆大学大数据与软件学院,重庆 400044)

摘要:为了确保智能变电站的安全,规避信息安全风险,对变电站存在的漏洞进行评估和管理是必要的。通用的信息安全风险评估流程是将资产重要性、威胁等级和脆弱性等级作为量化指标,通过这 3 个指标得出安全事件的影响和可能性值,再以此为基础计算出对象的风险值。研究提出一种基于 CML 的智能变电站设备节点网络失效连锁的模型,通过对智能变电站设备节点以及节点间的设备连接建立网络,评估不同设备节点在发生故障时对智能变电站整体设备网络的影响,从而对智能变电站信息安全风险进行有效分析。基于该模型的智能变电站信息安全风险分析管理子系统可以实现数据可视化协助管理者对智能变电站的信息安全风险数据进行管理。结果表明,对智能变电站的信息安全风险分析管理有改善作用。

关键词:智能变电站;风险分析;漏洞;IEC61850
中图分类号:TN914 **文献标志码**:A **文章编号**:1000-582X(2022)05-033-010

An intelligent substation logic mode metwork failure chain model based on CML

Wang Sheng[1], *Zhang Jie*[1], *Tang Chao*[1], *Zhang Linghao*[1], *Wang Hai*[1], *Tang Yong*[1], *Chai Jiwen*[1], *Zheng Yongkang*[1], *Deng Ping*[2], *Cao Liang*[3], *Ke Yawen*[4]
(1.Electric Power Research Institute of State Grid Sichuan Electric Power Company, Chengdu, 610072, P. R. China;2.State Grid Zigong Power Supply Company, Zigong, 643000,P.R.China;3.State Grid Ganzi Power Supply Company, Ganzi, 626700,P. R. China;4.School of Bigdata and Software Engineering, Chongqing University, Chongqing, 400044,P. R. China)

Abstract: In order to ensure the safety of intelligent substation and avoid information security risks, it is necessary to evaluate and manage the vulnerability in the substation. The mainstream risk assessment methods use asset importance, threat level and vulnerability level as quantitative indicators. Through these three indicators, the value of the impact and possibility of security events is obtained, and then the risk of

收稿日期:2021-04-12
基金项目:国家十三五密码发展基金项目(MMJJ20180211);国网四川省电力公司电力科学研究院项目(SGSCDK00XTJS1800093)。
Supported by Key special projects of the National 13th Five Year Code Development Fund (MMJJ20180211) and Project of Electric Power Research Institute of State Grid Sichuan Electric Power Company (SGSCDK00XTJS1800093).
作者简介:作者简介:王胜(1983—),男,工程师,主要从事信息安全方向研究,(Tel)18908203892;(E-mail) 240517810@qq.com.

the object is calculated. This paper proposes a CML-based intelligent substation logic node network failure chain model, Through the establishment of a network of intelligent substation logical nodes and logical connections between nodes, the impact of different logical nodes on the overall logical network of intelligent substation in the event of a fault is evaluated, so that the intelligent substation information security risk can be effectively analyzed. The intelligent substation information security risk analysis and management subsystem based on this model can help managers manage information security risk data of intelligent substation and realize data visualization. The results show that the information security risk analysis and management of intelligent substation can be improved.

Keywords: intelligent substation; risk assessment; vulnerability; IEC61850

随着计算机科学和通信技术的发展,传统变电站的运营形式已无法满足需求,国家电网提出了发展建设智能电网的目标,国内大量智能变电站的新建和改造工程也正在进行中。相比于传统的变电站,智能电网中的智能变电站采用了安全、集成度高、环保的设备,站内信息一体化、数字化,通过中国 DL/T 860(IEC 61850)标准进行信息共享,建设智能电网已经成为了国家新能源战略的重要环节[1]。

智能变电站,作为智能电网的核心节点,其安全的重要性自然不言而喻,一旦出现问题,后果可能是灾难性的。一些不法分子也可能利用黑客技术窃取智能变电站的相关信息,使国家资产蒙受损失。因此,分析变电站存在的风险,确保智能电网信息安全是重要目标[2]。

智能变电站可能面临的信息安全风险来自多个方面,包括信息和控制系统的信息安全风险、通信协议方面的信息安全风险、运维信息安全风险和人员信息安全风险,其中信息和控制系统的信息安全风险是关注的主要内容,即由站控层、间隔层操作系统漏洞和部分主流工业控制系统漏洞导致的信息安全风险。

研究详细阐述了一些关于智能变电站信息安全风险分析的方法和智能变电站信息安全风险分析管理子系统从设计到实现的思路和过程,有助于提高对智能变电站信息安全风险的分析、管理和预警能力。

1 智能变电站信息安全风险

1.1 传统的信息安全风险概念

信息安全风险是指在信息化建设进程中,各种类型的系统网络及其中存储和传输的数据信息,由于可能存在的软硬件、系统集成等各种缺陷,以及信息安全管理流程中潜在的薄弱环节,导致的不同程度的安全风险。

1.2 面向智能变电站的信息安全风险概念

1.2.1 智能变电站基本概念

智能变电站是使用智能设备,能实现信息采集自动化、按标准进行信息共享,同时具备基本的测控、采集、保护等功能的新一代变电站。

智能变电站的总体结构从上而下依次为站控层、站控层网络、间隔层、过程层网络和过程层。站控层主要包括远动站、数据和应用服务器、对时服务器、通信网关等。间隔层主要包括继电保护装置、录波装置、测控装置等。过程层主要包括合并单元、智能终端和组件等。两网:站控层网络主要实现站控层内部设备间以及站控层和间隔层设备之间的通信。过程层网络主要实现间隔层设备和过程层设备之间的数据传输。

1.2.2 智能变电站的信息安全风险

随着计算机通信和网络技术的发展,智能变电站逐渐替代了传统变电站,成为了变电站未来的发展方向。但在广阔发展前景的同时,智能变电站的安全问题也逐渐引起关注,来自传统网络空间的安全威胁以及有针对性的工控系统攻击手段已经日益严峻地影响到电力系统的信息安全。如何监测、评估、管理智能变电站中存在的漏洞和风险,保证智能变电站的可靠性成为了重要研究内容[3]。研究选择并改进了基于 CML 的连锁故障模型,结合采用 CVSS 评分标准基于机器学习方法的漏洞评估模型,对智能变电站整体安全风险进行分析评估并给出相应的改进意见。

2　相关工作

2.1　智能变电站信息安全风险分析的传统方法

随着电力需求的逐步增长以及国家电网提出建设智能电网的发展目标,几批国家变电站试点工程的成功使得智能变电站建设中不仅强调技术创新和经济效益,智能变电站本身的安全和可靠性更是被纳入了重要目标。为此,如何利用智能变电站的漏洞信息对其存在的安全风险进行评估也成为重要研究内容。

在实际的智能变电站信息安全风险分析过程中,大多还是利用传统的信息安全风险评估流程(如图 1 所示),首先识别资产,然后评估威胁和脆弱性,以此得出影响和可能性,最后利用影响和可能性计算风险值[4]。

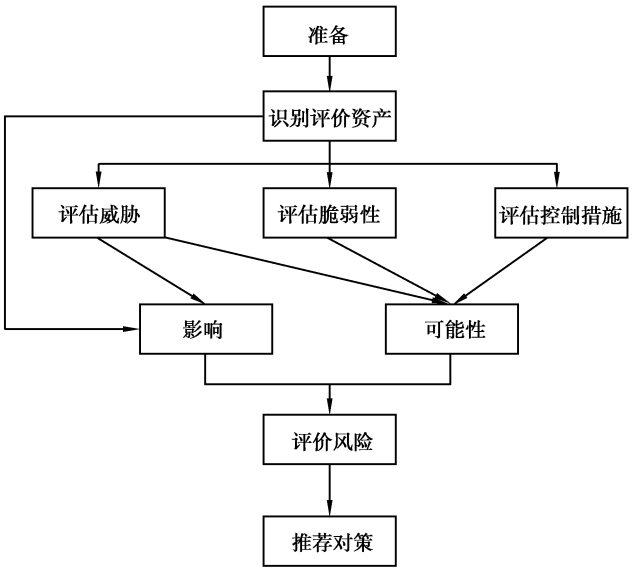

图 1　传统风险评估流程

Fig 1　Traditional Risk Evaluation Process

2.2　引入机器学习后的风险模型选择

常用的风险及威胁分析方法包括:微软 STRIDE 模型、基于风险传递网络的风险评估模型、基于机器学习的安全风险评估,基于 CML 的连锁故障评估模型。其中基于机器学习的安全风险评估又包括基于支持向量机(SVM, support vector machine)的评估模型、基于 C4.5 决策树评估模型、基于 BP 神经网络评估模型、基于朴素贝叶斯的评估模型、基于 K 近邻(KNN, k-nearest neighbor)算法的评估模型(如表 1 所示)。

表 1　模型分析

Table 1　Models analysis

评估模型	优点	缺点
微软 STRIDE 模型	评估范围广泛	对威胁的分类是一维的
基于风险传递网络的风险评估模型	评估范围广泛 思想简单,理论成熟	权重设定具有一定主观性
支持向量机	主观性小 对小样本适应性强 可用于线性/非线性分类	计算次数多 对参数和核函数的选择比较敏感

续表1

评估模型	优点	缺点
C4.5 决策树	计算简单,易于理解 对数据类别无要求 准确率较高	构造树时需对数据集多次扫描和排序,算法效率低 数据量较大时,不易求解
BP 神经网络	避免主观性、简单性 结果更有效客观	选取样本数据量有限
朴素贝叶斯	对小规模的数据表现很好 适合多分类任务	对输入数据的表达形式很敏感
K 近邻	思想简单,理论成熟 可用于非线性分类 对数据类别无要求	计算量大 样本不平衡问题 需要大量的内存
基于 CML 的连锁故障评估模型	评估范围广泛 性能较好	权重设定具有一定主观性

分析以上模型方法的优缺点之后,决定采用基于 CML 的连锁故障评估模型应用于智能变电站信息安全风险分析。

3 智能变电站信息安全风险分析方法

在 IEC61850 标准中,设备节点(LN, logical node)是实现功能的基本单位,同时也是数据对象的容器,变电站的自动化系统功能的实现依赖于不同的设备节点之间的信息交互,而在智能变电站的信息网络中,设备中的漏洞被利用很容易导致设备节点功能失效,如何分析一个或多个设备节点故障对整个智能变电站网络带来的影响,进一步评估对应设备节点乃至其所在设备上存在的信息安全风险正是所要研究的内容[5](如图 2、图 3 所示)。

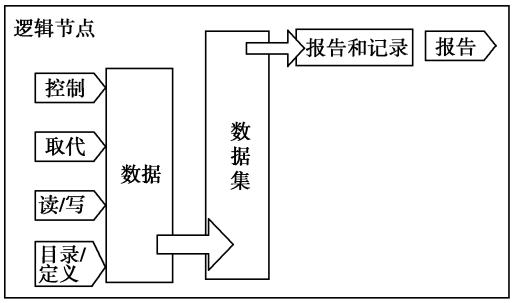

图 2 设备节点

Fig. 2 Logical Node

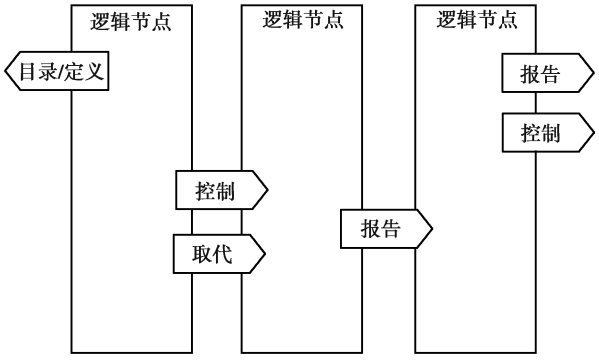

图 3 设备节点连接

Fig. 3 Logical Node Connection

3.1 复杂网络

3.1.1 概念介绍

复杂网络,是呈现高度复杂性的网络,严格定义是指具有自组织、自相似、吸引子、小世界、无标度中部分或全部性质的网络,常被应用于研究现实世界中各种复杂系统的模型建立。目前复杂网络的研究内容包括以下几个方向:几何性质、形成机制、网络演化、结构稳定性、网络动力学机制以及多重复杂性融合等问题[6]。

复杂网络一般具有如下几种重要性质[6]（如图 4 所示）。

1）小世界：该性质表现了一些复杂网络虽然具有很大规模，但任意 2 个节点之间总能找到一条较短连通路径，正如六度空间理论所描述的，地球上任意 2 个陌生人之间所间隔的人不会超过 6 个；

2）集群/集聚程度：集聚程度表现了一个网络的集群化程度，即复杂网络系统中小网络的内聚程度以及小网络之间的联系；

3）无标度：无标度网络是指分布严重不均匀，较少的节点具有较高的介数，而其余大部分节点介数较低，度分布符合幂律分布，即 $P(k)\sim k-\gamma$ 的网络称为无标度网络（如图 5 所示）。

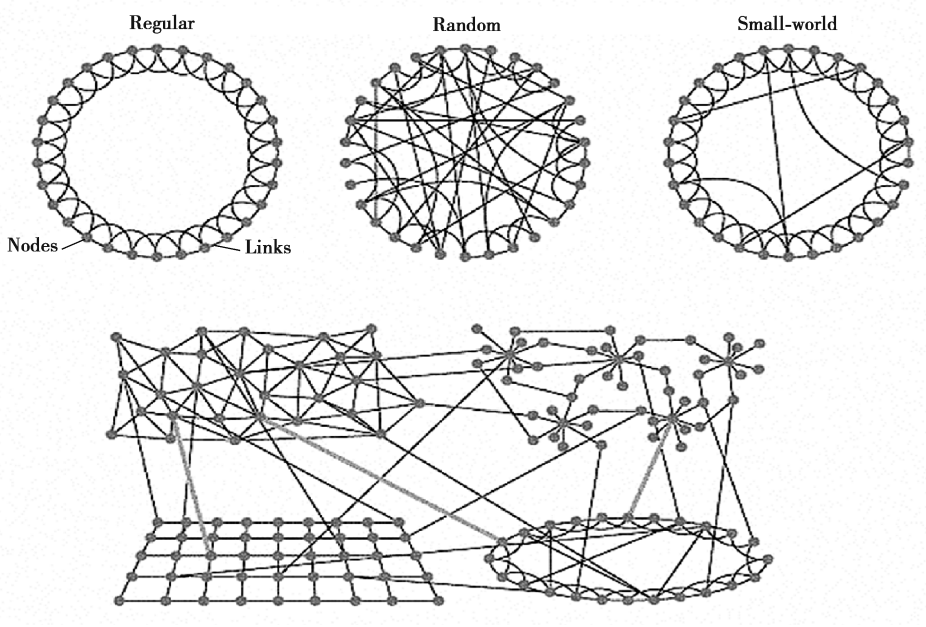

图 4　复杂网络

Fig. 4　Complex Network

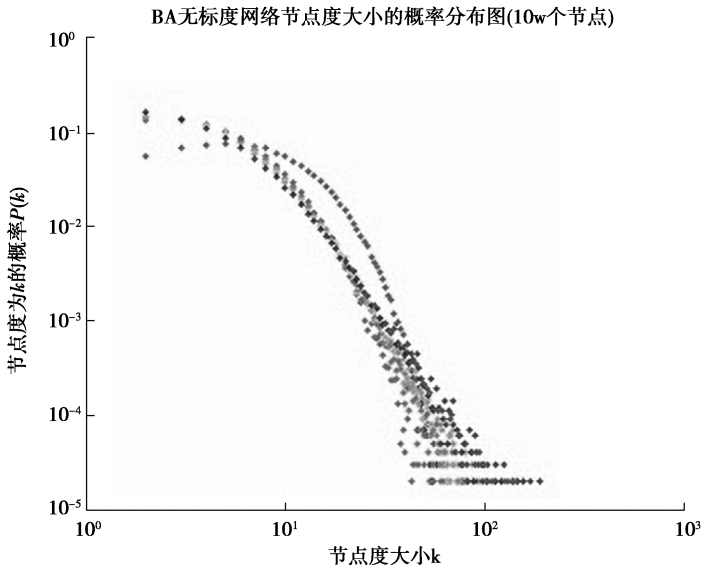

图 5　复杂网络的度分布

Fig. 5　Degree distribution of Complex Network

3.1.2 相关知识

复杂网络可以用一个由点集 V 和边集 E 构成的图 $G=(V,E)$ 来抽象表示。图中的节点为复杂网络系统中实体的映射，边则为复杂网络系统中实体间关系的映射，边可以有权重和方向，权重表征节点间联系的紧密程度，方向表征节点间联系的单向或者多向。

1)度分布：网络中所有节点 v 的度；k 的平均值称为网络的平均值

$$\overline{k}=\frac{1}{N}\sum_{i=1}^{N}k_i。\tag{1}$$

2)平均路径长度：网络的平均路径长度 L，定义为任意 2 个节点之间距离的平均值

$$L=\frac{1}{C_N^2}\sum_{1\leqslant i<j\leqslant N}d_{ij}。\tag{2}$$

3)聚类系数：节点v_i的k_i个邻居节点之间实际存在的边数E_i和总的边数 $C_{k_i}^2$ 之比就定义为节点v_i的聚类系数C_i

$$C_i=\frac{E_i}{C_{k_i}^2}。\tag{3}$$

整个网络的聚类系数 C 为C_i的平均值。

4)度相关性：度相关性用于描述网络中节点之间的连接关系，若度较大的节点倾向于连接度大的节点，则称此网络是正相关的；否则称之为负相关的。只需计算顶点度的 Pearson 相关系数 r 即可描述网络的度相关性。

$$r=\frac{M^{-1}\sum_i j_i k_i-\left[M^{-1}\sum_i\frac{1}{2}(j_i+k_i)\right]^2}{M^{-1}\sum_i\frac{1}{2}(j_i^2+k_i^2)-\left[M^{-1}\sum_i\frac{1}{2}(j_i+k_i)\right]^2},\tag{4}$$

其中：j_i，k_i分别表示连接第 i 条边的 2 个顶点 j，k 的度；M 表示网络的总边数。

3.2 智能变电站设备节点网络的性质分析

将智能变电站中设备节点映射为网络中的节点，设备节点间的数据交互映射为网络中的边。经考察，智能变电站设备节点网络中的平均路径长度较小，整个网络的集聚系数较高，符合小世界网络的特征。同时网络中设备节点的度分布服从幂律分布，也符合无标度网络的特征[7]。

可以看出智能变电站的设备节点网络同时具有小世界和无标度网络的特征，即网络中小网络的内聚程度高，少量的节点具有较高的出入度，大量的节点凝聚在少量的 HUB 节点周围。上述对智能变电站设备节点网络性质的分析为信息安全风险分析模型的选择建立了基础。

3.3 基于 CML 的智能变电站设备节点网络的连锁失效模型

CML(coupled map lattice)即耦合映像格子，是日本东京大学纯应用科学系 Kunihiko Kaneko 博士于 1984 年提出的理论，它是一个将时间、空间进行离散化，状态保持连续的非线性动力学模型，是近年来一种广泛应用于研究复杂网络中的时空动力学行为模型，该理论常用于一些有规则拓扑结构的复杂网络中，如今在一些具有小世界或无标度网络的动力学研究中也得到广泛应用[8-9]。

含有 N 个节点的有向 CML 模型如下

$$x_i(t+1)=\left|(1-\varepsilon_1-\varepsilon_2)f(x_i(t))+\varepsilon_1\sum_{j=1,j\neq i}^{N_1}a_{ij}\frac{f(x_j(t))}{\deg^+(i)}+\varepsilon_2\sum_{j=1,j\neq i}^{N_2}a_{ij}\frac{f(x_j(t))}{\deg^-(i)}\right|,\tag{5}$$

其中：$x_i(t)$表示节点 i 在 t 时刻的状态，如果节点 i 的状态一直维持在(0,1)内，则该节点状态正常；如果节点 i 在 m 时的状态$x_i(m)\geqslant 1$，则节点 i 在 m 时刻失效，m 时刻后该节点状态均为 0。节点间的连接信息可表示为连接矩阵：$\boldsymbol{A}=(a_{i,j})_{N\times N}$，若有向边从 i 到 j 连接，则$a_{i,j}=1$，反之亦然，若 2 节点之间无连接，则$a_{i,j}=a_{j,i}=0$。N_1为含有入度的节点个数，N_2为含有出度的节点个数；$\deg^+(i)$为 i 节点的入度，$\deg^-(i)$为 i 节点的出度；ε_1为 i 节点的入边耦合强度，ε_2为 i 节点的出边耦合强度，$\varepsilon_1,\varepsilon_2\in(0,1)$。$f$ 为混沌 Logistic 映射 $f(x)=4x(1-x)x\in[0,1]f(x)\in[0,1]$。

在 CML 模型下，网络中所有节点都按该公式进行演化，若开始时网络中所有节点都处于正常状态，且无

外部影响因素，那么演化过程中所有节点均将保持正常状态。

为了模拟设备在遭受攻击等设备节点失效情况下智能电网的变化情况，考虑对节点 i 的状态于时刻 m 施加一个扰动 $R\geqslant 1$，使得该节点在 m 时刻发生了故障，节点 i 的状态变化由下式描述

$$x'_i(t+1)=\left|(1-\varepsilon_1-\varepsilon_2)f(x_i(t))+\varepsilon_1\sum_{j=1,j\neq i}^{N_1}a_{ij}\frac{f(x_j(t))}{\deg^+(i)}+\varepsilon_2\sum_{j=1,j\neq i}^{N_2}a_{ij}\frac{f(x_j(t))}{\deg^-(i)}\right|+R。\tag{6}$$

施加扰动后，即从下一个时间片 $m+1$ 开始节点 i 的状态持续为 0，同时 m 时刻节点 i 的状态 $x_i(m)$ 将会影响其所有的邻节点，并使其邻节点依照式(4)所描述的方式进行状态值刷新，而这可能导致邻节点同样失效，继续影响其邻节点，从而在整个网络中产生设备节点失效的连锁反应[10-12]（如图 6 所示）。

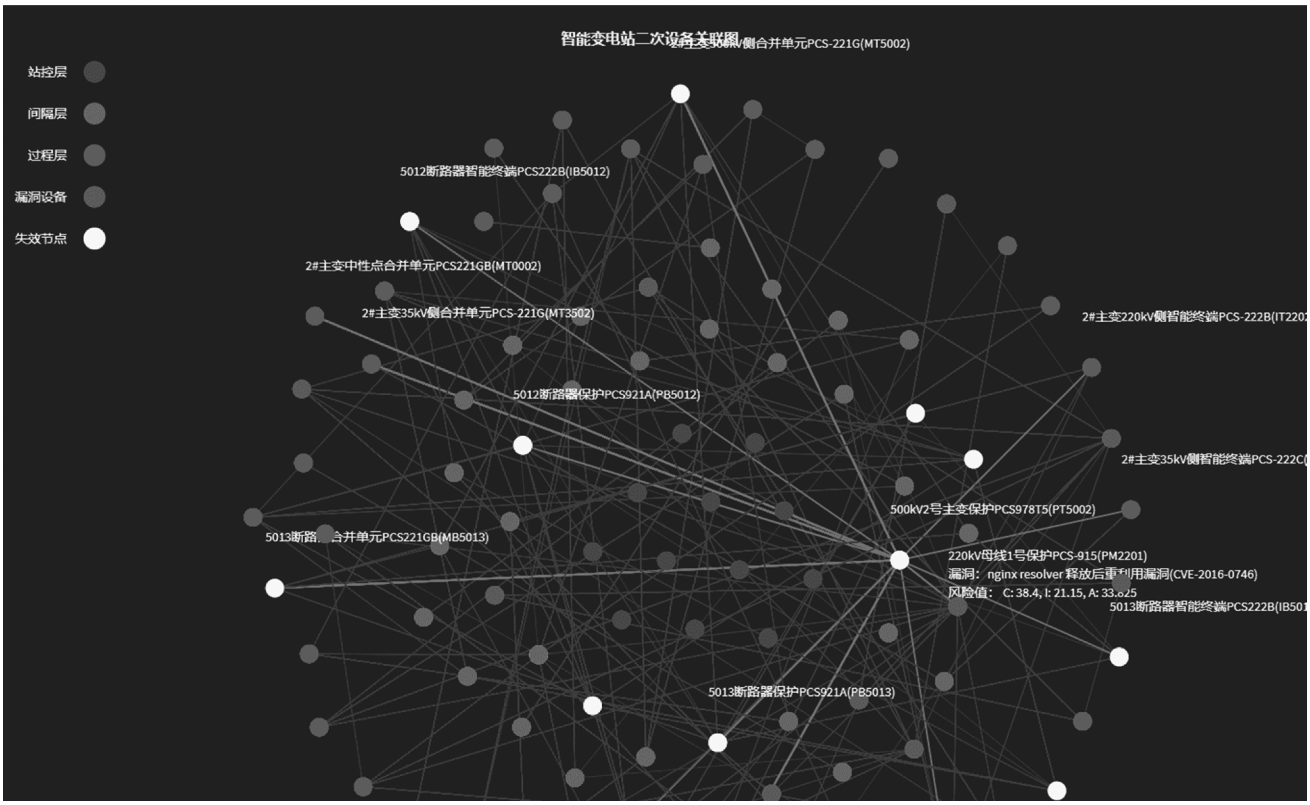

图 6　设备节点连锁失效模拟

Fig. 6　Device Nodes Chain Failure Simulation

3.4　其他智能变电站信息安全风险分析方法介绍

3.4.1　基于贝叶斯网络的风险关联模型

1986 年，美国加州大学教授珀尔(J.F.Pearl)针对不确定性知识提出贝叶斯网络(Bayesian network)模型。贝叶斯网络也称为因果网络(causal networks)，它是由图论和概率论结合描述多元统计关系的模型，是可以用贝叶斯概率理论与图形模式结合起来由有向无环图(DAG，directed acyclic graph)来表示的模型。

基于贝叶斯网络的风险关联模型将贝叶斯网络与粗糙理论集相结合，基于专家群决策方法来确定智能变电站的风险诱发因素及设备风险，建立决策表，利用粗糙集提取最佳属性约简组合；利用贝叶斯网络技术构建风险关联关系图，采用专家知识与伽玛分布函数联合确定贝叶斯图的条件概率分布，并通过融入监测数据的方式对模型进行更新[13-14]。

相比 CML 智能变电站设备节点连锁失效模型以设备为基本节点构建网络，基于贝叶斯网络的风险关联模型针对具体变电站设备约简了相关的风险因素，生成了基于贝叶斯网络的风险关联图，最后逆向分析出风险诱发因素的可能性次序。CML 模型主要研究了智能变电站中风险在设备节点之间的传播，贝叶斯网络风险模型则是通过概率分布反向分析出风险诱发因素（如图 7 所示）。

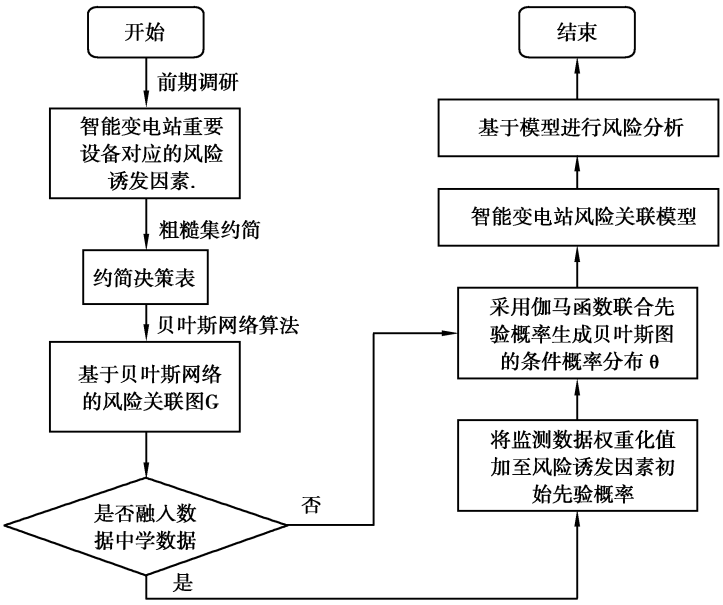

图7 贝叶斯网络方法流程

Fig. 7 Bayesian network method model

3.4.2 基于风险传递网络的智能变电站风险评估模型

该方法是结合复杂网络理论和风险传递理论,鉴于二次系统中设备和功能的连接关系,定义网络风险元素,并考虑网络元素间的相互影响,构建二次系统风险传递网络并建立了一套评估二次系统风险的指标体系。具体流程如图8所示:通过建立待评估二次设备的风险网络,构建网络功能关联矩阵,求出节点度、主体度等相关网络参数,对基本主体集失效概率和损失进行分析,得到基本主体集风险,最后根据基本主体集风险求出系统级和设备级的其他风险指标[15]。

与基于CML的智能变电站设备节点网络连锁失效模型中的设备节点网络相似,基于风险传递网络的智能变电站风险评估模型也构建了二次设备的风险传递网络,2个网络均涵盖了智能变电站"三层两网"结构中的所有设备,不同之处在于CML的设备节点网络选用了耦合映像格子作为风险传递模型,而基于风险传递网络的二次设备网络则是选用了常用于金融行业的风险传递模型并制定了风险体系指标用于评估智能变电站系统和设备的风险[16-17]。

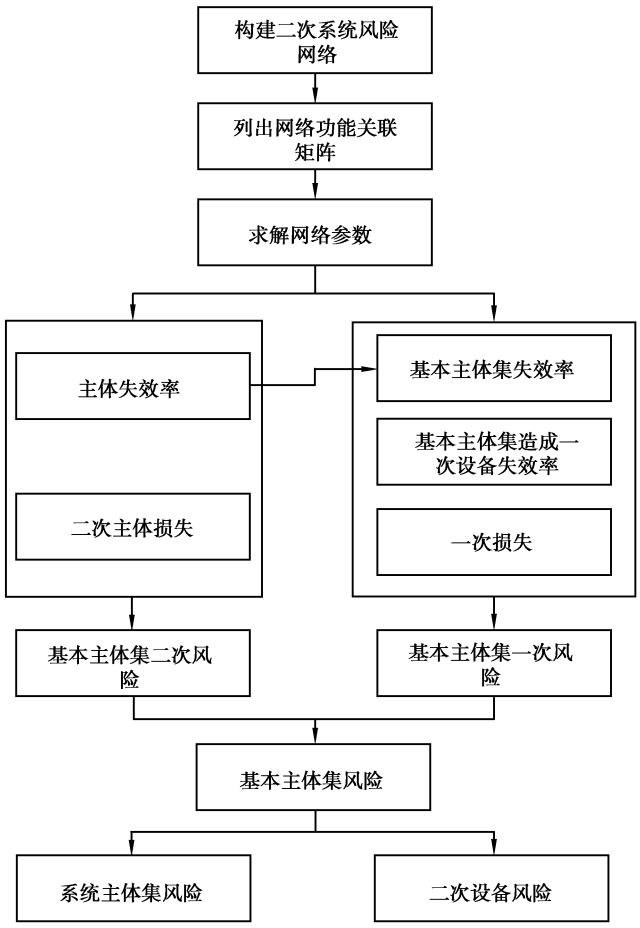

图8 风险评估流程图

Fig. 8 Flowchart of Risk Assesment

4　结　论

传统的变电站漏洞扫描信息以分散的报告形式组成，不方便用户从中读取整体风险信息，而且没有以数据库形式装载数据，不方便进行管理。

利用 web 技术实现的基于 CML 的设备节点网络连锁失效风险模型的智能变电站信息安全风险分析管理系统是为了方便变电站工作和管理人员对变电站信息安全风险信息管理而开发的一款原型系统，通过此系统可以对站内设备信息安全风险信息进行分析和管理，得出基于 CML 设备节点网络连锁失效风险模型计算出的各个变电站的风险评分，使用户更直观查看变电站漏洞数据，使管理人员在处理变电站漏洞时更有针对性。

参考文献：

[1] 黄雅宣. 智能变电站的涵义及发展探讨[J]. 通讯世界，2017(7)：131-132.
Huang Y X. Discussion on the meaning and development of intelligent substation[J]. Telecom World，2017(7)：131-132. (in Chinese)

[2] 江南，纪陵，杨小凡. 智能变电站信息安全技术[J]. 电气自动化，2018，40(6)：48-51.
Jiang N，Ji L，Yang X F. Information security technology of smart substation[J]. Electrical Automation，2018，40(6)：48-51. (in Chinese)

[3] 胡斌，郭亚飞，杨彬，等. 智能变电站技术的现状与发展趋势研究[J]. 智慧电力，2018，46(3)：87-90.
Hu B，Guo Y F，Yang B，et al. Research on status and development trend of smart substation technology[J]. Smart Power，2018，46(3)：87-90. (in Chinese)

[4] 中国国家标准化管理委员会.信息安全技术-信息安全风险评估规范[EB/OL].[2019.05.31].https：// max.book118.com/html/2018/1224/7120025034001166.shtm.
Standardization Administration of the People's Republic of China. Information Security Technology- Risk Assessment Specification for Information Security [EB/OL]. [2019. 05. 31]. https：// max. book118. com/html/2018/1224/7120025034001166.shtm.

[5] 韩宇奇，郭嘉，郭创新，等. 考虑软件失效的信息物理融合电力系统智能变电站安全风险评估[J]. 中国电机工程学报，2016，36(6)：1500-1508.
Han Y Q，Guo J，Guo C X，et al. Intelligent substation security risk assessment of cyber physical power systems incorporating software failures[J]. Proceedings of the CSEE，2016，36(6)：1500-1508. (in Chinese)

[6] Newman M E J. The structure and function of complex networks[J]. SIAM Review，2003，45(2)：167-256.

[7] 李孟超，王允平，李献伟，等. 智能变电站及技术特点分析[J]. 电力系统保护与控制，2010，38(18)：59-62.
Li M C，Wang Y P，Li X W，et al. Smart substation and technical characteristics analysis[J]. Power System Protection and Control，2010，38(18)：59-62. (in Chinese)

[8] Radziwill N M. Countdown to zero day：stuxnet and the launch of the world's first digital weapon[J]. Quality Management Journal，2018，25(2)：109-110.

[9] Greene T. Indegy finds out when industrial controls go bad (think Stuxnet)[J]. Network World (Online)，2016.

[10] 张其林，王先培，赵宇. 基于 IEC 61850 的变电站自动化系统连锁故障分析[J]. 电力系统自动化，2013，37(2)：61-66.
Zhang Q L，Wang X P，Zhao Y. Analysis on cascading failures of substation automation system based on IEC 6185[J]. Automation of Electric Power Systems，2013，37(2)：61-66. (in Chinese)

[11] Zongxiang L，Zhongwei M，Shuangxi Z. Cascading failure analysis of bulk power system using small-world network model[C]// 2004 International Conference on Probabilistic Methods Applied to Power Systems. Ames，IA，USA：IEEE，2004：635-640.

[12] 丁明，韩平平. 小世界电网的连锁故障传播机理分析[J]. 电力系统自动化，2007，31(18)：6-10.
Ding M，Han P P. Study of failure spreading mechanism in the small-world power grid[J]. Automation of Electric Power

Systems，2007，31(18)：6-10.(in Chinese)

[13] 马秀娟，马福祥，赵海兴. 基于耦合映像格子的有向网络相继故障[J]. 计算机应用，2011，31(7)：1952-1955.
Ma X J，Ma F X，Zhao H X. Cascading failure in coupled map lattices with directed network[J]. Journal of Computer Applications，2011，31(7)：1952-1955.(in Chinese)

[14] 曲朝阳，杨琴，杨杰明，等. 基于贝叶斯网络的智能变电站风险关联模型[J]. 电力系统自动化，2016，40(2)：95-99.
Qu Z Y，Yang Q，Yang J M，et al. Risk associated model of smart substations based on Bayesian network[J]. Automation of Electric Power Systems，2016，40(2)：95-99.(in Chinese)

[15] 王力军，周凯，吴迪，等. 基于风险传递网络的智能变电站二次系统风险评估[J]. 电力系统保护与控制，2018，46(6)：97-105.
Wang L J，Zhou K，Wu D，et al. Risk assessment for smart substation secondary system using risk transfer network model[J]. Power System Protection and Control，2018，46(6)：97-105.(in Chinese)

[16] Holovaty A，Kaplan-Moss J. The definitive guide to django[M]. Berkeley，CA：Apress，2008.

[17] Bennett J. Practical django projects[M]. Berkeley，CA：Apress，2009.

（编辑 侯 湘）

(上接第 32 页)

[26] Hong B，Chen J，Zhang K，et al. Multi-authority non-monotonic KP-ABE with cryptographic reverse firewall[J]. IEEE Access，2019，7：159002-159012.

[27] Zhou Y，Guan Y，Zhang Z，et al. Cryptographic reverse firewalls for identity-based encryption[C]// Frontiers in Cyber Security，FCS 2019. Singapore：Springer 2019：36-52.

[28] Zhou Y Y，Guo J，Li F G. Certificateless public key encryption with cryptographic reverse firewalls[J]. Journal of Systems Architecture，2020，109：101754.

[29] Kumar M，Saxena P. PF-AID-2KAP：Pairing-free authenticated identity-based two-party key agreement protocol for resource-constrained devices [C] // Futuristic Trends in Network and Communication Technologies. Singapore：Springer. 2018：425-440.

[30] Tseng Y M，Huang S S，You M L. Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments[J]. International Journal of Communication Systems，2017，30(11)：e3251.

[31] Islam S H，Biswas G P. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication[J]. Journal of King Saud University-Computer and Information Sciences，2017，29(1)：63-73.

[32] Barker E B，Barker W C，Burr W E，et al. Recommendation for key management，part 1：[R]. National Institute of Standards and Technology，2005.

[33] Barker E，Mouha N. Recommendation for the triple data encryption Algorithm（TDEA）block cipher[R]. National Institute of Standards and Technology，2017.

（编辑 侯 湘）