计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(8):55−63 [doi: 10.15888/j.cnki.csa.008628]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于云模型和改进证据理论的电力监控系统风险评估①

曾　颖[1,2], 武　斌[1,2], 田宁姗[1,2]

[1](北京邮电大学 信息安全中心, 北京 100876)
[2](北京邮电大学 网络空间安全学院, 北京 100876)
通信作者: 武　斌, E-mail: binwu@bupt.edu.cn

摘　要: 针对电力监控系统风险评估中存在的系统建模不完整、专家评价意见的模糊性和缺乏对系统整体风险的考虑的问题, 提出了基于云模型和改进证据理论的电力监控系统风险评估方法. 首先根据电力监控系统的结构和安全需求, 对电力监控系统的设备、安全目标和威胁进行分析, 建立系统整体风险评估模型; 然后结合 FAHP 和修正的熵权法, 使用最优化组合赋权的方法得到各元素的权重; 最后利用云模型和改进证据理论完成对电力监控系统的综合风险评估, 得到系统的风险等级. 仿真实验证明了该方法的适用性和有效性, 为电力监控系统的安全管理工作提供了新的思路.

关键词: 最优化组合赋权; 云模型; 证据理论; 电力监控系统; 风险评估; 故障诊断

引用格式: 曾颖,武斌,田宁姗.基于云模型和改进证据理论的电力监控系统风险评估.计算机系统应用,2022,31(8):55–63. http://www.c-s-a.org.cn/1003-3254/8628.html

Risk Assessment of Power Monitoring System Based on Cloud Model and Improved Evidence Theory

ZENG Ying[1,2], WU Bin[1,2], TIAN Ning-Shan[1,2]

[1](Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)
[2](School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In view of the problems existing in the risk assessment of power monitoring systems, such as incomplete system modeling, fuzzy evaluation opinions of experts, and lack of consideration of the overall risk of systems, a risk assessment method for power monitoring systems is proposed, which is based on the cloud model and improved evidence theory. Firstly, according to the structure and security requirements of a power monitoring system, the equipment, security objectives, and threats of the system are analyzed, and the overall risk assessment model of the system is built. Then, in combination with the FAHP and modified entropy weight method, the weight of each element is obtained by using the optimal combination weighting method. Finally, the comprehensive risk assessment of the power monitoring system is completed by the cloud model and improved evidence theory, and the risk level of the system is obtained. The simulations show that the method is feasible and effective, which provides a new idea for the security management of the power monitoring system.

Key words: optimal combination weighting method; cloud model; evidence theory; power monitoring system; risk assessment; fault diagnosis

① 收稿时间: 2021-11-03; 修改时间: 2021-12-02; 采用时间: 2021-12-21; csa 在线出版时间: 2022-05-31

计算机和网络技术的发展使得信息技术在各个行业都得到了广泛的应用, 电力系统的信息化水平在不断提高, 但同时也带来了更多的安全威胁. 据 ICS-CERT 报告, 近年来类似于“震网”、HaveX、Black Engery 等针对电力行业的网络安全事件在呈现稳步增长的趋势. 电力监控系统具有监控现场设备和故障处理的能力, 一旦遭受攻击, 会极大影响电力系统的正常运行. 因此保障电力监控系统的安全已经成为各级安全责任单位的重中之重. 风险评估作为检测系统安全状态的有力手段, 能够评估系统的安全风险, 利于及时制定相应的风险控制策略. 对电力监控系统进行合理的安全风险评估, 可以帮助提高电力监控系统的安全性, 有效避免灾害的发生.

从目前的研究来看, 电力系统的风险评估主要集中在对电力设备和输电网络上[1–4], 对电力监控系统的研究较少. 梁宁波[5] 通过漏洞排查对电力监控系统进行风险管理, 但对于漏洞结果未给出明确风险评估标准; 杨鹏[6] 针对电力监控系统中的两个子系统进行安全风险分析, 但缺乏对系统整体的考虑; 梁智强等人[7] 使用 AHP 方法, 并结合模糊数学的原理对关键资产风险进行了评估, 但没有给出电力系统的整体风险; 曹波等人[8] 结合状态攻击图对电力监控系统的脆弱性进行评估, 但在大规模场景下攻击图易产生状态爆炸问题. 总体来看, 目前电力监控系统风险评估主要存在着系统建模不完整以及缺乏对系统整体风险的考虑的问题.

风险评估中在定性指标的评价上会表现为专家评价意见的模糊性, 影响评估结果的准确性. 因此, 云模型[9] 自提出以来, 由于其能够刻画自然语言中概念的不确定性和模糊性[10], 已广泛应用于评估领域. 张仕斌等人[11] 引入云模型对复杂网络环境中的用户信息进行信任评估; 徐岩等人[12] 利用云模型得到定量指标对变压器各状态的隶属等级对变压器状态进行评估; 胡文平等人[13] 将正态云模型用于输变电设备故障的不确定性推理预测, 完成对电网的综合风险评估; 龙赛琴等人[14] 设计了基于云模型的多指标融合评估策略对数据中心的能效进行评估. 云模型在评估领域的应用中取得了不错的效果, 能够在一定程度上减小评价中模糊性和不确定性的影响.

云模型解决了定性指标的量化问题, 然而在综合评估时, 由于多位专家侧重点不同, 还存在着评估信息不一致的问题. 在多源信息的融合方面, 证据理论是一种有效的尝试. 证据理论能够将多源信息视为证据, 解决证据间的冲突并进行融合, 形成相对完整和一致的表达. 因而在质量评估[15]、故障诊断[16]、多属性决策[17] 等领域应用广泛, 能有效提高结果的准确性.

为此, 本文提出基于云模型和改进证据理论的电力监控系统综合风险评估方法. 在建立风险评估模型时充分考虑系统的特点, 使得对系统的建模更加完整; 使用云模型实现专家语言评价的有效转换, 同时使用基于冲突系数和概率距离函数的证据修正方法和基于矩阵分析的证据合成算法, 可减小证据冲突的影响和提高评估的效率.

1 构建电力监控系统风险评估模型

1.1 电力监控系统的安全性分析

典型电力监控系统的组网结构如图 1 所示, 3 个层次的主要功能如下: 主站层能够人机交互, 可从整体上对系统的工作进行维护和管理; 网络通讯层是层次间数据交换的桥梁, 使得主站层能够快速得到现场设备层的监测信息和下发控制指令; 现场设备层主要用于监测设备的运行, 并根据上层指令对设备进行控制.

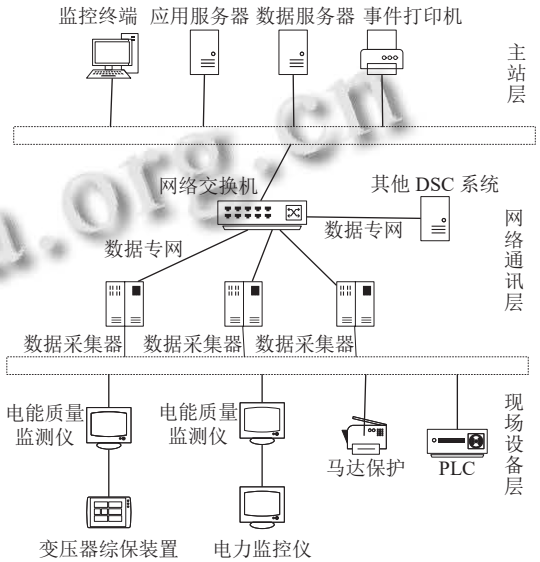

图 1 电力监控系统组网结构图

相比于传统网络系统, 电力监控系统具有节点多样性、网络异构性、应用实时性和业务连续性的特点, 因而在电力监控系统中, 可用性是其首要保障, 其次是完整性和机密性. 针对电力监控系统的特点, 本文另提出了可见性和可控性的安全属性. 可见性是指可观察

过程的当前状态以便做出决策以及监视过程的当前状态并对异常事件做出警报; 可控性是防止对电力系统控制功能的影响.

威胁是系统风险产生的关键因素, 根据《工业控制网络安全风险评估规范》[18] 和电力监控系统的实际情况, 分析得到电力监控系统常见的威胁主要有非法设备的物理接入、访问权限非法获取、控制信息被篡改、未授权的网络连接、数据包重放攻击、拒绝提供服务、病毒感染、被植入木马、控制信息非法获取等[19].

1.2 电力监控系统风险评估模型的建立

根据《信息安全风险评估规范》[20] 的定义, 信息安全风险评估是通过资产、威胁和脆弱性对信息的安全属性进行评价的过程. 本文参照该原理, 通过对系统及其安全属性进行评价以实现电力监控系统的综合风险评估. 针对电力监控系统, 将系统关键设备类比“资产”, 系统攻击方式类比于“威胁”[21], 通过威胁对系统安全属性的影响以及系统关键设备对安全属性的依赖来对系统总体安全风险进行评估. 结合第 1.1 节对电力监控系统的安全性分析, 建立图 2 所示的电力监控系统风险评估模型.

由电力监控系统组网结构图可知, 现场设备层主要由电力一次设备组成, 对攻击者来说, 攻击成本大且收益小. 因此本文的风险评估主要针对主站层和网络通讯层, 选取的关键设备有监控终端、应用服务器、数据服务器、网络交换机、数据采集器和 PLC.

各关键设备功能的不同导致与其相关的安全属性的重要程度的差异, 本文在建立关键设备层与安全属性层的联系时, 根据关键设备的功能选择其最为重要的 3 个安全属性建立联系, 这样既可以突出各设备的功能特性, 也便于后文各元素权重的确定.

最后根据威胁对系统的影响建立评价层与安全属性层间的联系.

1.3 电力监控系统风险评估原理

本文的电力监控系统风险评估流程如图 3 所示. 具体步骤如下.

(1) 收集数据: 根据建立的风险评估模型, 收集专家评价信息和系统的运行数据;

(2) 计算指标的主客观权重: 根据收集的专家意见基于 FAHP 方法对指标进行主观赋权, 根据系统运行数据基于修正的熵权法对指标进行客观赋权;

(3) 计算综合权重: 使用最优化模型确定主客观权重的组合系数, 对指标进行组合赋权;

(4) 综合评估: 使用云模型和改进的证据理论进行综合评估, 得到系统的风险评估结果.

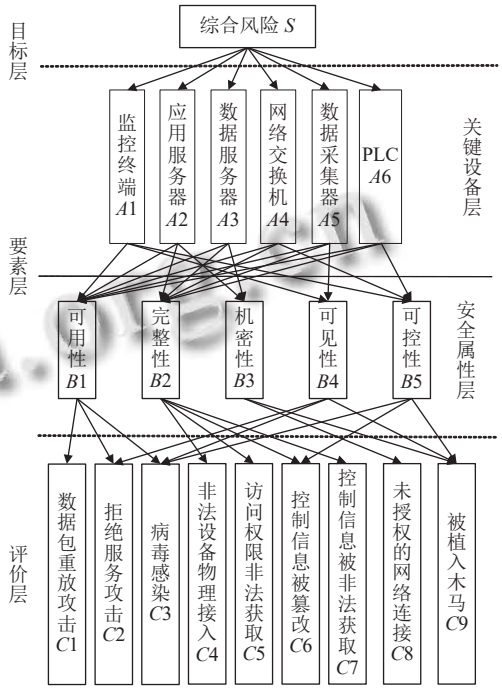

图 2 电力监控系统风险评估模型

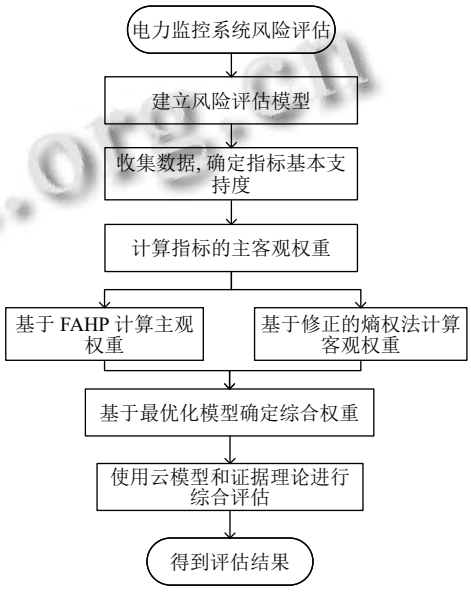

图 3 电力监控系统风险评估流程图

2 基于组合赋权的指标权重的确定

为提高权重的准确性和评估的合理性, 以更好地反映电力监控系统的运行状态, 本文采用组合赋权的

方法. 该方法能够减小专家意见的主观性影响, 又能兼顾客观数据信息, 可避免单一权重赋值方法的主导性.

2.1 基于 FAHP 的主观权重赋值方法

由于本文评估模型中元素多样且层次间的关联复杂, 若使用传统的 AHP 方法, 构造的判断矩阵维度较大, 查验矩阵一致性以及调整元素使其一致非常困难. 因此, 为避免上述问题, 本文引入了模糊 AHP 方法[22]. 步骤如下.

(1) 根据表 1, 专家评判构造模糊判断矩阵$A=(r_{ij})_{n\times n}$, r_{ij} 含义为: 对于上层某个元素, 本层与之相关的元素 x_i 和 x_j 的相对重要程度.

表 1 模糊互补判断矩阵重要性标度

标度	说明
0.5	x_i与x_j同等重要
0.6	x_i比x_j稍微重要
0.7	x_i比x_j明显重要
0.8	x_i比x_j重要得多
0.9	x_i比x_j极端重要
0.1, 0.2, 0.3, 0.4	x_i与x_j的反比较

(2) 将矩阵$A=(r_{ij})_{n\times n}$按$f_{ij}=\dfrac{r_i-r_j}{2n}+0.5$进行转换使其一致, 其中$r_i$和$r_j$表示对应行元素的和, 即$r_x=\sum_{k=1}^{n}r_{xk}$.

(3) 按照式 (1) 进行计算各要素的权重值:

$$w_i=\frac{1}{n}-\frac{1}{2\alpha}+\frac{1}{n\alpha}\sum_{k=1}^{n}r_{ik},\ i=1,2,\cdots,n \tag{1}$$

其中, w_i即本层第 i 个要素的权重值, n 为总个数, r_{ik}模糊一致矩阵 A 的元素值, 参数α需满足$\alpha\geqslant\dfrac{n-1}{2}$, α越小权重差异度越大, 本文取为$\alpha=\dfrac{n-1}{2}$, 此时得到的各要素权重差异度最大, 即区分度最高.

2.2 基于改进熵权法的客观权重赋值方法

熵权法利用信息熵表征指标集的不确定度, 熵值大小表示各指标的变异程度. 若某个指标的信息熵越小, 表示该指标所包含的信息量越大, 则相应赋予的权重应较大. 传统的熵权法确定客观权重的步骤如下:

(1) 根据原始客观数据, 确定指标集的评价矩阵$R=\left[r_{ij}\right]_{m\times n}$, 其中 r_{ij} 表示第 i 个评估对象对第 j 个评价指标的评价结果.

(2) 根据式 (2) 对评价矩阵 R 进行归一化处理得到归一化后的评价矩阵$X=\left[x_{ij}\right]_{m\times n}$:

$$x_{ij}=\frac{r_{ij}}{\sum_{j=0}^{n}r_{ij}} \tag{2}$$

(3) 根据式 (3) 计算得到第 j 个指标的熵值:

$$e_j=-\frac{1}{Inn}\sum_{i=1}^{m}(x_{ij}Inx_{ij}),\ (j=1,2,\cdots,n) \tag{3}$$

(4) 由式 (4) 计算第 j 个指标的客观权重:

$$v_j=\frac{1-e_j}{n-\sum_{j=1}^{n}e_j},\ (j=1,2,\cdots,n) \tag{4}$$

由于电力监控系统的数据不稳定, 不确定性较大, 导致指标的信息熵易接近于 1. 在这种情况下, 若采用上述传统的熵权法, 结果易与现实相悖[23]. 因此本文对该方法进行修正, 在传统计算方法中加入起修正作用的正数 z, 修正的熵权法计算第 j 个指标的权重公式为:

$$v_j=\frac{1-e_j+z}{\sum_{j=1}^{n}\left(1-e_j+z\right)},\ (j=1,2,\cdots,n,\ z>0) \tag{5}$$

研究表明[23], 使用该公式进行权重计算能够成功解决传统熵权法存在的上述问题. 其中, z 的值越大时修正作用越好, 本文令$z=\frac{1}{n}\sum_{j=1}^{n}\left(1-e_j\right)$.

2.3 组合权重赋值方法

组合权重赋值公式如下:

$$\sigma_j=\alpha w_j+\beta v_j,\ (j=1,2,\cdots,n) \tag{6}$$

其中, w_j 和 v_j 分别为主观权重和客观权重, α和β为权重系数, 取值范围为 [0, 1], 并且$\alpha+\beta=1$. 本文使用基于最小方差原理的最优化模型确定权重系数, 该模型可使主客观权重的比例达到最佳, 使得评估结果更加准确. 建立的最优化模型如下:

$$\min B=\sum_{j=1}^{n}\left(\sigma_j-w_j\right)^2+\left(\sigma_j-v_j\right)^2 \tag{7}$$

其中, B 为主客观权重与组合权重的方差值, 上述模型表示求取使得式 B 最小的权重系数α和β. 根据微分的性质, 上式存在的唯一解, 因此根据主客观权重可唯一确定组合权重值.

3 基于云模型和证据理论的风险评估方法

3.1 证据理论

3.1.1 传统证据理论

证据理论能够有效处理问题的模糊性, 符合人类

推理的决策过程, 用于风险评估可充分利用评估过程中的不确定性, 得到更为合理的评估结果, 其关键是 Dempster 证据合成规则[24]:

$$m(A)=\begin{cases}0, A=\varphi\\ \dfrac{\sum_{A_i\cap B_j\cap C_k\cdots=A} m_1(A_i)\cdot m_2\left(B_j\right)\cdot m_3(C_k)\cdots}{K}, A\neq\varphi\end{cases}$$

$$K=\sum_{A_i\cap B_j\cap C_k\cdots\neq\varphi} m_1(A_i)\cdot m_2\left(B_j\right)\cdot m_3(C_k)\cdots \tag{8}$$

其中, $m_1, m_2, \cdots, m_n$ 表示 n 个独立证据, K 为冲突系数, 代表证据的冲突程度.

然而, 传统证据理论在电力监控系统中应用时存在着以下问题: 由于各层元素间关系复杂, 专家评判时受主观因素的影响易出现证据冲突, 直接使用上述合成规则的计算结果可能与实际情况不符; 另外, 直接使用上述合成规则进行证据融合效率较低. 因此有必要对证据理论进行改进.

3.1.2 证据冲突修正方法

为解决证据冲突的问题, 本文引入了基于冲突系数和概率函数的证据冲突修正方法, 具体运算过程参考文献 [25], 流程如图 4 所示.

该方法的基本原理是: 在获取原始证据体后, 根据冲突系数、Jousselme 概率距离和 Pignistic 概率距离定义一种新的证据冲突量, 通过计算各专家的证据可信度, 结合专家权重得到各专家的证据修正系数, 对原始证据体进行修正.

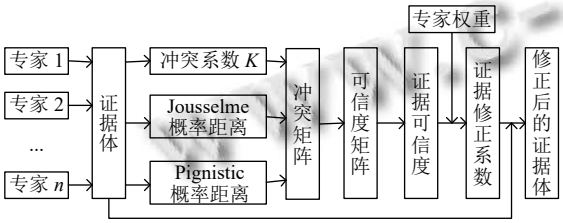

图 4 证据冲突修正流程图

3.1.3 基于矩阵分析的证据合成方法

为解决证据融合的效率问题, 本文引入了基于矩阵分析[26] 的方法, 该方法通过递推计算的方式融合专家意见, 可提高证据融合的效率.

假设有 n 位专家, 5 个隶属等级, 根据评判得到 *mass* 矩阵为:

$$M=\begin{bmatrix}M_1\\M_2\\\vdots\\M_n\end{bmatrix}=\begin{bmatrix}m_{11}&m_{12}&m_{13}&m_{14}&m_{15}\\m_{21}&m_{22}&m_{23}&m_{24}&m_{25}\\\vdots&\vdots&\vdots&\vdots&\vdots\\m_{n1}&m_{n2}&m_{n3}&m_{n4}&m_{n5}\end{bmatrix}$$

m_{ij} 表示第 i 位专家的评判中目标风险等级 j 的隶属度, 基于矩阵分析的证据融合流程如图 5 所示.

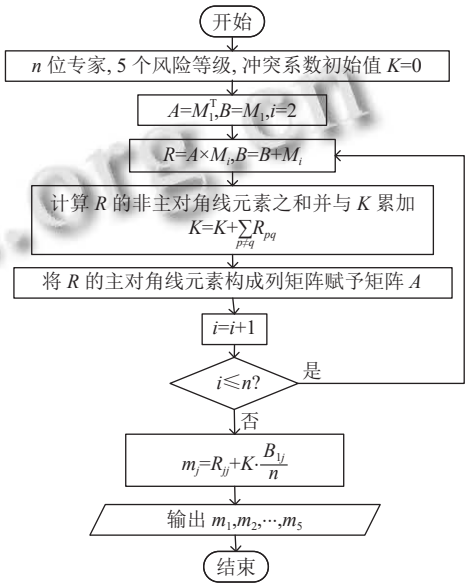

图 5 基于矩阵分析的 D-S 合成算法流程图

3.2 利用云模型实现 *mass* 函数的构造

在证据理论的应用中, 原始证据大都是用定性语言进行描述的, 具有较大的不确定性, 难以进行直接融合, 因此构造有效的 *mass* 函数是难点之一. 云模型刻化了定性语言值和精确数值之间随机和模糊的性质, 具有定性与定量信息转换上的优势. 因此, 本文将云模型用于构造证据理论的 *mass* 函数, 以实现专家评价从定性向定量的有效转化, 具体方法如下:

(1) 设专家的自然语言评价有 r 个等级, 评价值的有效论域为$[X_{\min}, X_{\max}]$, 使用黄金分割法[27] 将评价等级转化为标准云$C_h(Ex_h, En_h, He_h)$, 其中, $h=1,\cdots, r$, 表示第 n 个评语等级. 再利用标准云将 m 位专家相对于上层元素 X_i 对应的第 j 个元素的语言评价值转化为评价云决策矩阵$\left[C_{gij}\left(Ex_{gij}, En_{gij}, He_{gij}\right)\right]_{m\times r}$.

(2) 结合标准云模型, 将云决策矩阵的元素转换为隶属度, 公式如下:

$$\mu_g\left(x_{ij}\right)_h=\mathrm{e}^{-\frac{\left(Ex_{gij}-Ex_h\right)}{2\left(En_h\right)^2}} \tag{9}$$

得到的隶属度矩阵为:

$$U_{ij}=\begin{bmatrix} \mu_1(x_{ij})_1 & \mu_1(x_{ij})_2 & \cdots & \mu_1(x_{ij})_r \\ \mu_2(x_{ij})_1 & \mu_2(x_{ij})_2 & \cdots & \mu_2(x_{ij})_r \\ \vdots & \vdots & \ddots & \vdots \\ \mu_m(x_{ij})_1 & \mu_m(x_{ij})_2 & \cdots & \mu_m(x_{ij})_r \end{bmatrix} \tag{10}$$

然后按照式 (11) 进行归一化处理:

$$m_g(x_{ij})_h=\frac{\mu_g(x_{ij})_h}{\sum_{h=1}^{n}\mu_g(x_{ij})_h} \tag{11}$$

3.3 基于云模型-证据理论的风险评估步骤

(1) 以问卷的方式收集专家关于评价层元素对上层元素影响等级的定性评价信息.

(2) 利用第 3.2 节的方法将专家定性评价信息转换为隶属度矩阵也即证据理论的原始证据体.

(3) 证据冲突修正.

根据图 4 所示的方法计算各位专家的证据修正系数, 并对原始证据体按照式 (12) 进行修正:

$$m_g(x_{ij})_h{}'=\rho_g\cdot\mu_g(x_{ij})_h \tag{12}$$

其中, ρ_g为第 g 个专家的证据修正系数.

(4) 综合评估

得到评价层元素相对于上层元素的 *mass* 矩阵后, 利用图 5 所示的基于矩阵分析的证据合成方法进行证据合成. 然后根据各属性的权重值$\bar{\omega}=\{\omega_j|j=1,2,\cdots,l\}$, 得到上层第 i 个元素的 *mass* 函数值为:

$$m(X_i)_h=\sum_{j=1}^{l}\omega_j\cdot m(x_{ij})_h \tag{13}$$

根据上式自底向上进行合成, 最终得到综合风险 S 的 *mass* 函数值, 最大隶属等级即为系统的风险等级.

4 算例仿真

4.1 实例计算

本次仿真使用的数据来源于国网河北省电力有限公司实验网络, 该网络的拓扑图如图 1 所示. 该实验网络与真实网络以同样的方式运行, 将实际网络约 1/20 的运行流量镜像到该实验网络, 并通过人工干预的方式对其定时实施攻击.

为验证本文方法的适用性, 实验收集实验网络中监控终端、应用服务器、数据服务器、网络交换机、数据采集器和 PLC 的运行数据, 并邀请 4 位电网的工程技术人员进行专家评判, 其中, 1 位正高级工程师, 2 位副高级工程师, 1 位中级工程师.

4.1.1 最优化组合赋权确定元素权重

计算各层元素的主客观权重并运用最优化模型进行组合, 得到各元素的权重如图 6 所示.

S																
*A*1 0.21			*A*2 0.18			*A*3 0.07			*A*4 0.20			*A*5 0.09			*A*6 0.25		
*B*1 0.23	*B*4 0.30	*B*5 0.47	*B*1 0.39	*B*2 0.33	*B*3 0.28	*B*1 0.35	*B*2 0.29	*B*3 0.36	*B*1 0.41	*B*2 0.24	*B*5 0.25	*B*1 0.36	*B*5 0.32	*B*4 0.22	*B*1 0.31	*B*2 0.34	*B*5 0.35

*B*1			*B*2				*B*3		*B*4			*B*5		
*C*1 0.38	*C*2 0.29	*C*3 0.35	*C*4 0.37	*C*5 0.24	*C*6 0.19	*C*7 0.20	*C*8 0.72	*C*9 0.28	*C*2 0.49	*C*3 0.23	*C*9 0.28	*C*3 0.32	*C*6 0.36	*C*9 0.32

图 6 各元素权重值

图 6 中, *S*, *A*1,⋯, *A*6, *B*1,⋯, *B*5, *C*1,⋯, *C*9 代表图 2 中的各层元素.

4.1.2 专家语言评价信息转换

设专家评估有效论域为 [0, 100], 分数越高表示评价指标对上层元素的影响越大, 利用黄金分割法确定的 5 朵标准云为: C_{-2}(0, 10.31, 0.26), C_{-1}(30.9, 6.37, 0.16), C_0(50, 3.93, 0.1), C_{+1}(69.1, 6.37, 0.16), C_{+2}(100, 10.31, 0.26).

由决策专家组成员{*G*1, *G*2, *G*3, *G*4}确定指标对上层元素的评价值, 假设隶属等级分为 5 级, 描述为{V_{-2}=很低, V_{-1}=低, V_0=中, V_1=高, V_2=很高}. 以可用性 *B*1 为例, 评价下层威胁对其的影响程度, 专家评价信息如表 2 所示.

表 2 专家评价结果

专家	*C*1	*C*2	*C*3
*G*1	V_0	V_2	V_1
*G*2	V_{-1}	V_1	V_0
*G*3	V_0	V_0	V_0
*G*4	V_2	V_1	V_{-1}

根据标准云转化得到的云决策矩阵为:

$$V=\begin{bmatrix} (50,3.93,0.1) & (100,10.31,0.26) & (69.1,6.37,0.16) \\ (50,3.93,0.1) & (69.1,6.37,0.16) & (50,3.93,0.1) \\ (50,3.93,0.1) & (50,3.93,0.1) & (50,3.93,0.1) \\ (100,10.31,0.26) & (69.1,6.37,0.16) & (30.9,6.37,0.16) \end{bmatrix}$$

根据式 (9)–式 (11), 以 $C1$ 为例, 计算各等级的隶属度并归一化处理得初始 *mass* 矩阵为:

$$M_{C1}=\begin{bmatrix} 0.154 & 0.154 & 0.196 & 0.248 & 0.248 \\ 0.129 & 0.149 & 0.277 & 0.239 & 0.206 \\ 0.154 & 0.154 & 0.196 & 0.248 & 0.248 \\ 0.213 & 0.145 & 0.068 & 0.233 & 0.341 \end{bmatrix}$$

4.1.3 证据冲突修正

以M_{C1}为例, 证据冲突修正步骤如下:

计算两两专家间的冲突系数 K、Jousselme 概率距离和 Pignistic 概率距离, 如表 3 所示.

表 3 冲突系数 K 和概率距离

指标	$G1$–$G2$	$G1$–$G3$	$G1$–$G4$	$G2$–$G3$	$G2$-$G4$	$G3$–$G4$
K	0.2077	0.2095	0.2113	0.2077	0.1940	0.2113
Jousselme	0.0623	0	0.1170	0.0623	0.1778	0.1170
Pignistic	0.0810	0	0.1280	0.0810	0.2090	0.1280

根据表 3, 利用文献 [25] 中的方法, 得各专家的证据可信度分别为:

$Rel(G1)=1$, $Rel(G2)=0.9636$, $Rel(G3)=1$, $Rel(G4)=0.9395$.

根据专家的经验和行业认可度确定专家权重向量 $\lambda=\{0.3,0.2,0.4,0.1\}$, 则相对权重为:

$$\lambda_{G1}=0.75,\lambda_{G2}=0.50,\lambda_{G3}=1,\lambda_{G4}=0.25$$

令证据可信度分配系数β=0.6, 则专家 $G1$ 的证据修正系数为:

$$\rho_{G1}=\beta\times Rel(G1)+(1-\beta)\times\lambda_{G1}=0.9$$

同理得$\rho_{G2}=0.78$, $\rho_{G3}=1$, $\rho_{G4}=0.66$.

根据式 (12) 得修正后的 *mass* 矩阵为:

$$M'_{C1}=\begin{bmatrix} 0.140 & 0.140 & 0.176 & 0.223 & 0.223 & 0.098 \\ 0.101 & 0.116 & 0.216 & 0.186 & 0.161 & 0.220 \\ 0.154 & 0.154 & 0.196 & 0.248 & 0.248 & 0 \\ 0.141 & 0.096 & 0.045 & 0.154 & 0.225 & 0.339 \end{bmatrix}$$

4.1.4 综合评估

使用图 5 所示方法对M'_{C1}进行合成得:

mass($C1$)=(0.1336, 0.1260, 0.1577, 0.2038, 0.2158, 0.1631)

同理可得 *mass*($C2$) 和 *mass*($C3$). 然后结合表 2 的权重值, 根据式 (13) 求取 *mass*($B1$). 以此类推进行逐层合成, 最终得 S 的隶属度向量:

mass(S)=(0.0156, 0.2124, 0.3460, 0.1819, 0.2056, 0.0385)

得系统的风险等级为 V_0 即“中”, 该结果与系统的实际安全状态一致, 证明了所提方法的适用性.

根据各元素的 *mass* 函数值, 得各元素的风险等级评价结果如图 7 所示.

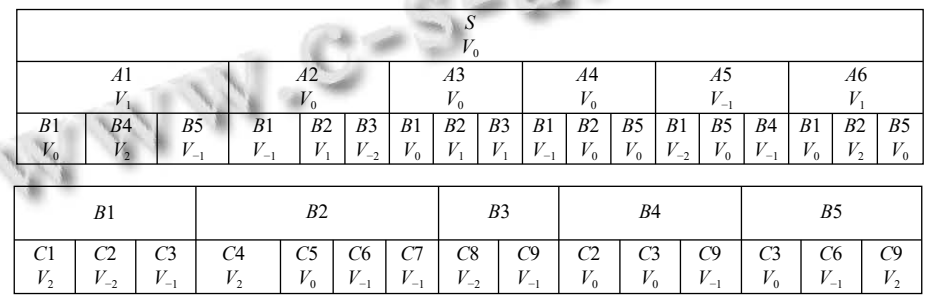

图 7 各元素风险等级

根据以上评价结果, 系统管理人员可明确当前系统的薄弱环节以进行针对性的防护, 防护建议如下.

(1) 系统整体的风险等级为“中”, 有提高安全性的必要, 需要对其进行安全管理. 根据系统关键设备的评估结果, 监控终端和 PLC 的风险评估等级为“高”, 可知系统的薄弱点集中于监控终端和 PLC, 需要对两者进行针对性的管理;

(2) 对于监控终端, 评估结果表明其可见性的威胁程度较高, 且主要风险来源于拒绝服务攻击和病毒感染, 因此需要尽可能对系统加载最新的补丁, 采取有效

的合规性配置, 对安全域划分的合理性进行检验, 并检查防火墙和入侵检测系统的配置安全性;

(3) 对于 PLC 来说, 评估结果表明其完整性的威胁程度较高, 且主要风险来源于非法设备的物理接入, 因此需加强对设备的安全边界管理和设备接入的管控措施, 同时应该严格控制机房区域的人员进出.

4.2 有效性分析

根据元素 $C1$ 的原始 *mass* 矩阵 M_{C1} 和修正后的 *mass* 矩阵 M'_{C1}, 得证据修正前后专家间的证据冲突系数如表 4 所示. 对比如图 8 所示.

表 4 专家间冲突系数

修正状态	*G*1–*G*2	*G*1–*G*3	*G*1–*G*4	*G*2–*G*3	*G*2–*G*4	*G*3–*G*4
修正前	0.2077	0.2095	0.2113	0.2077	0.1940	0.2113
修正后	0.1692	0.1882	0.1588	0.1618	0.1745	0.1393

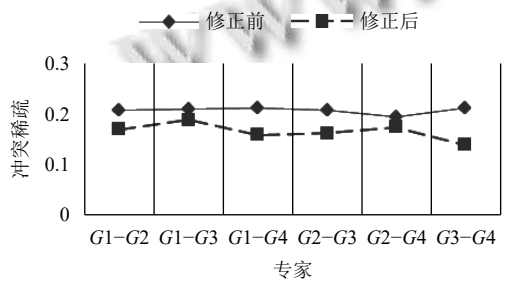

图 8 冲突系数对比图

由图 8 可知, 本文使用的证据修正方法使得专家间的证据冲突程度明显降低, 整体证据冲突系数由 0.0096 降低为 0.0077, 证明了本文证据冲突修正方法的有效性.

同样以 $C1$ 的 *mass* 矩阵 M'_{C1} 为例, 分别使用传统方法和本文的方法进行证据合成, 得到的结果以及运行时间如表 5 所示.

表 5 结果对比

方法	很低	低	中等	高	很高	执行时间 (s)
传统方法	0.0687	0.0537	0.0750	0.3544	0.4482	0.0041
本文方法	0.1336	0.1260	0.1577	0.2038	0.2158	0.0005

结果表明, 传统方法和本文方法得系统可用性的风险等级结果均为“很高”, 然而对比发现, 采用本文方法的执行时间仅为传统方法的 1/8, 能够大大提高数据融合的效率.

上述分析证明了本文电力监控系统风险评估方法的有效性.

5 结语

在电力监控系统的风险评估过程中, 构建评估模型时结合系统的特点进行了详细的安全性分析, 并提出了可见性和可控性的安全目标, 层次间关联和层次元素的细化使得对系统的建模更加完整; 将云模型引入证据理论, 能够充分考虑到专家评价意见的模糊性; 使用基于冲突系数和概率函数的证据冲突修正方法和矩阵分析的证据合成算法, 可在一定程度上解决证据冲突的问题和提高风险评估的效率. 本文的工作为电力监控系统的安全管理工作提供了新的思路.

参考文献

1 Yao JM, Wu P, Wang Y, *et al*. Research on power wireless network quality evaluation method based on multi-dimensional index. Proceedings of 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). Chongqing: IEEE, 2020. 376–381. [doi: 10.1109/ICIBA50161.2020.9277019]

2 杨至元, 张仕鹏, 孙浩, 等. 基于 Cyber-Net 与学习算法的变电站网络威胁风险评估. 电力系统自动化, 2020, 44(24): 19–27. [doi: 10.7500/AEPS20191230009]

3 金文俊. 基于社团结构的电力通信网可靠性评估方法 [硕士学位论文]. 北京: 北京邮电大学, 2019.

4 王俊芳. 面向状态检修的继电保护系统可靠性评估 [硕士学位论文]. 北京: 北京交通大学, 2018.

5 梁宁波. 电力监控系统漏洞隐患排查及风险管理技术研究. 自动化博览, 2019, 36(S2): 41–45.

6 杨鹏. 电力监控系统中 KVM 系统和动力环境监控系统的安全风险分析研究. 电工技术, 2017, (8): 10–11. [doi: 10.3969/j.issn.1002-1388.2017.08.005]

7 梁智强, 林丹生. 基于电力系统的信息安全风险评估机制研究. 信息网络安全, 2017, (4): 86–90. [doi: 10.3969/j.issn.1671-1122.2017.04.012]

8 曹波, 吴峥, 杨杉, 等. 电力监控系统脆弱性评估模型研究. 计算机与数字工程, 2014, 42(1): 107–111. [doi: 10.3969/j.issn.1672-9722.2014.01.029]

9 李德毅, 孟海军, 史雪梅. 隶属云和隶属云发生器. 计算机研究与发展, 1995, 32(6): 15–20.

10 付斌, 李道国, 王慕快. 云模型研究的回顾与展望. 计算机应用研究, 2011, 28(2): 420–426. [doi: 10.3969/j.issn.1001-3695.2011.02.004]

11 张仕斌, 许春香. 基于云模型的信任评估方法研究. 计算机学报, 2013, 36(2): 422–431.

12 徐岩, 陈昕. 基于合作博弈和云模型的变压器状态评估方法. 电力自动化设备, 2015, 35(3): 88–93. [doi: 10.16081/

j.issn.1006-6047.2015.03.014]
13 胡文平, 于腾凯, 巫伟南. 一种基于云预测模型的电网综合风险评估方法. 电力系统保护与控制, 2015, 43(5): 35–42. [doi: 10.7667/j.issn.1674-3415.2015.05.006]
14 龙赛琴, 黄金娜, 李哲涛, 等. 面向云网融合的数据中心能效评估方法. 计算机研究与发展, 2021, 58(6): 1248–1260. [doi: 10.7544/issn1000-1239.2021.20201069]
15 李玲玲, 刘敬杰, 凌跃胜, 等. 物元理论和证据理论相结合的电能质量综合评估. 电工技术学报, 2015, 30(12): 383–391. [doi: 10.3969/j.issn.1000-6753.2015.12.048]
16 张文元, 赵卫国, 晋涛, 等. 多神经网络与证据理论的变压器故障诊断方法. 高压电器, 2018, 54(8): 207–211. [doi: 10.13296/j.1001-1609.hva.2018.08.032]
17 Li P, Wei CP. An emergency decision-making method based on D-S evidence theory for probabilistic linguistic term sets. International Journal of Disaster Risk Reduction, 2019, 37: 101178. [doi: 10.1016/j.ijdrr.2019.101178]
18 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. GB/T 26333-2010 工业控制网络安全风险评估规范. 北京: 中国标准出版社, 2011.
19 林云威, 陈冬青, 彭勇, 等. 基于 D-S 证据理论的电厂工业控制系统信息安全风险评估. 华东理工大学学报 (自然科学版), 2014, 40(4): 500–505. [doi: 10.3969/j.issn.1006-3080.2014.04.016]
20 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. GB/T 20984-2007 信息安全技术 信息安全风险评估规范. 北京: 中国标准出版社, 2007.
21 贾驰千, 冯冬芹. 基于模糊层次分析法的工控系统安全评估. 浙江大学学报 (工学版), 2016, 50(4): 759–765. [doi: 10.3785/j.issn.1008-973X.2016.04.022]
22 张吉军. 模糊层次分析法 (FAHP). 模糊系统与数学, 2000, 14(2): 80–88. [doi: 10.3969/j.issn.1001-7402.2000.02.016]
23 Zhi H, Zhang GD, Liu YQ, *et al*. A novel risk assessment model on software system combining modified fuzzy entropy-weight and AHP. Proceedings of the 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). Beijing: IEEE, 2017. 451–454. [doi: 10.1109/icsess.2017.8342953]
24 Firth S. Combination of evidence in Dempster-Shafer theory. Contemporary Pacific, 2002, 11(2): 416–426.
25 狄鹏, 倪子纯, 尹东亮. 基于云模型和证据理论的多属性决策优化算法. 系统工程理论与实践, 2021, 41(4): 1061–1070.
26 奚婷婷. 多传感器数据融合中 DS 证据理论算法的改进与应用 [硕士学位论文]. 无锡: 江南大学, 2009.
27 徐选华, 吴慧迪. 基于改进云模型的语言偏好信息多属性大群体决策方法. 管理工程学报, 2018, 32(1): 117–125. [doi: 10.13587/j.cnki.jieem.2018.01.01]

(校对责编: 牛欣悦)