中国科技期刊卓越行动计划项目入选期刊

控制与决策

CONTROL AND DECISION

基于博弈组合赋权的有源相控阵雷达收发组件脆弱性评估

张倩, 黄大荣, 王晶, 周萌, 赵宁, 张宇

引用本文:
张倩,黄大荣,王晶,周萌,赵宁,张宇. 基于博弈组合赋权的有源相控阵雷达收发组件脆弱性评估[J]. 控制与决策, 2024, 39(6): 1995−2004.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2022.1741

基于博弈组合赋权的有源相控阵雷达收发组件脆弱性评估

张 倩[1], 黄大荣[1], 王 晶[2†], 周 萌[2], 赵 宁[3], 张 宇[3]

(1. 重庆交通大学 信息科学与工程学院，重庆 400074；2. 北方工业大学 电气与控制工程学院，北京 100043；
3. 中国船舶集团有限公司 第八研究院，南京 211153)

摘 要: 面向有源相控阵雷达的核心部件——T/R 组件(transmit/receive module),提出综合脆弱性评估概念及其数学模型表达,给出定量评估的博弈组合赋权-优劣解距离方法. 首先,从元件和系统两个层次出发分别构建脆弱性评估标准:利用元件自身物理特性建立故障树,基于蒙特卡洛仿真计算得到运行状态的物理脆弱性指标(即可靠性指标);根据系统的电路结构,建立其拓扑网络,计算结构脆弱性指标. 然后,提出融合物理和结构的综合脆弱性评估数学模型,建立博弈组合赋权问题优化组合权重,结合优劣解距离法实现对T/R组件综合脆弱性的定量评估. 实验结果表明,T/R组件的综合脆弱性不仅与各元件固有的可靠性水平相关,更与其系统的电路网络拓扑结构密不可分,所建立的综合脆弱性评估模型能够有效合理地辨识其薄弱环节.

关键词: 收发(T/R)组件；故障树分析；复杂网络理论；脆弱性评估；博弈法；优劣解距离法

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2022.1741

引用格式: 张倩, 黄大荣, 王晶, 等. 基于博弈组合赋权的有源相控阵雷达收发组件脆弱性评估 [J]. 控制与决策, 2024, 39(6): 1995-2004.

Vulnerability assessment of active phased array radar transceiver based on game combination weighting

ZHANG Qian[1], *HUANG Da-rong*[1], *WANG Jing*[2†], *ZHOU Meng*[2], *ZHAO Ning*[3], *ZHANG Yu*[3]

(1. School of Information Science and Engineering，Chongqing Jiaotong University，Chongqing 400074，China；
2. School of Electrical and Control Engineering，North China University of Technology，Beijing 100043，China；
3. The Eighth Research Institute of China Shipbuilding Corporation，Nanjing 211153，China)

Abstract: For T/R (transmit/receive) module, the core component of active phased array radar, the concept of comprehensive vulnerability assessment and its mathematical model expression are proposed, and a quantitative evaluation method of game combination weighting-good and bad distance solution is presented. Firstly, the vulnerability assessment criteria are constructed respectively from two levels of components and systems. The fault tree is established by using the physical characteristics of components, and the physical vulnerability index (i.e., reliability index) of operating state is obtained based on Monte Carlo simulation calculation. According to the circuit structure of the system, the topological network is established and the structural vulnerability index is calculated. Then, a mathematical model of comprehensive vulnerability assessment integrating physics and structure is proposed, and the game combination weighting problem is established to optimize the combination weight. The quantitative assessment of comprehensive vulnerability of T/R components is realized by combining the superior and inferior solution distance method. The experimental results show that the comprehensive vulnerability of T/R components is not only related to the inherent reliability level of each component, but also closely related to the circuit network topology of the system. The established comprehensive vulnerability assessment model can identify the weak links effectively and reasonably.

Keywords: transmit/receive module；fault tree analysis；complex network theory；vulnerability assessment；game theory；TOPSIS

0 引 言

现代相控阵雷达技术在多目标检测、跟踪和多波束形成等方面应用广泛[1],其核心部件发射-接收(T/R)组件成为学者们的重点研究对象[2]. 随着雷达技术的蓬勃发展,T/R组件的规模、复杂程度以及重要性得到了提高,同时由于运行环境恶劣,对维持系统安全稳定可靠运行提出了更高的要求.

T/R组件的良好作战性能是决定雷达系统稳定

收稿日期: 2022-10-06；**录用日期:** 2023-03-12.

基金项目: “十三五”国防技术基础科研项目(JSZL2019207B008)；国家自然科学基金项目(61973023)；重庆市技术创新与应用发展专项重点项目(cstc2019jscx-mbdxX0015).

†通讯作者. E-mail: jwang@ncut.edu.cn.

运行的重要前提. 针对相控阵雷达系统的现有研究, 包含T/R组件的评估主要集中于作战效能[3]、维修策略和保障能力[4]、安全性[5]、可靠性[6]等方面. 作为安全性概念进一步深化和延拓, 脆弱性表示系统在正常运行条件下承受干扰或故障的能力[7], 它从全局的角度表达系统的安全稳定性, 是对系统性能的衡量; 脆弱性评估往往是为了找到故障后对系统稳定运行影响最大的关键元件. 因此, 本文将脆弱性的概念引入T/R组件的性能研究, 实现T/R组件脆弱性的科学合理测度, 准确识别系统薄弱环节, 以更好地提升雷达系统的安全性和可靠性.

目前, 关于脆弱性的理论研究主要集中于对运行状态或系统结构的脆弱性评价: 1) 基于运行状态的脆弱性评估, 包括风险分析理论、能量函数方法. Li等[8]以基于图的模型揭示级联故障的传播, 提出了表示电力系统运行状态多变、发电不确定性的脆弱性综合评价指标; Yan等[9]和Sun等[10]基于流量、电气阶数、节点约束、线路限制等电气特性研究了系统脆弱性. 2) 基于结构重要性的脆弱性评估方案主要基于复杂网络理论, 从电路拓扑特性出发, 挖掘系统的脆弱单元. Wu等[11]、Dai等[12]、Beyza等[13]以及Yang等[14]基于图论的方法, 建立了系统拓扑的图模型进行脆弱性评估; Liu等[15]以攻击场景中网络连通性作为脆弱性衡量指标, 识别出导致网络连通性降级的最小关键元件集合. 然而, 当以电路拓扑结构特性参数建立脆弱性模型时, 电路的简化会忽略节点的运行特性. 后来有研究结合拓扑特性与潮流、流量等电气特性来提高评估的准确性. Liu等[16]研究了电力系统网络脆弱性, 使用复杂网络理论确定电网的关键节点, 并建立了基于交流潮流模型和网络拓扑加权的级联故障模型; Cetinay等[17]和Wei等[18]基于复杂网络理论建立了系统的网络拓扑模型, 分析不同攻击场景中电力网络的脆弱性; Rocchetta等[19]和Wang等[20]根据基于系统拓扑的度量, 与不确定性、最大流量等其他算法, 从不同角度对脆弱性进行了评估, 评估结果表明这种结合可有效识别系统薄弱环节, 但是, 这些环节往往处于电气联络的关键节点, 可靠性较高, 不易发生故障.

可靠性是衡量系统优劣的重要指标, 表示规定条件下、规定时间内实现规定功能的概率[21]. 可靠性分析和评估在系统模型的基础上, 通过概率方法得到反映运行状态的可靠性指标以及易造成系统故障的环节, 其结果能够表征脆弱性. 因此, 如何结合可靠性建立综合脆弱性模型, 解决复杂系统脆弱性研究忽略节点运行特性以及元件可靠性的问题, 将有效提升系统薄弱环节识别的效率和准确性.

由于T/R组件涉及因素众多, 基于状态的脆弱性虽然在一定程度上揭示了系统运行的物理特性、运行特性, 但是, 其依托于系统电路结构. 本文在可靠性分析的基础上融合拓扑特性, 提出一种同时考虑运行状态和电路结构的T/R组件综合脆弱性数学模型, 定量评估T/R组件各节点的脆弱程度, 进而识别系统的薄弱环节. 本文主要内容如下: 1) 结合可靠性, 提出一种基于元件运行状态的物理脆弱性与基于电路拓扑的结构脆弱性相融合的综合脆弱性评估概念; 2) 从元件层面出发, 分析元件可靠性获得物理脆弱性表达, 从系统层面出发通过系统拓扑特性获得结构脆弱性, 进而建立综合脆弱性加权评价指标的数学模型; 3) 提出博弈组合赋权-优劣解距离(TOPSIS)方法, 优化求解综合指标的组合权重, 实现综合脆弱性的定量评价.

1 T/R组件综合脆弱性

T/R组件系统3大基本功能如下: 放大接收信号、产生发射信号和逻辑控制. 执行接收功能时, 小信号从天线至环形器进入接收通道, 经过滤波器、限幅低噪放大器、数控衰减器后再经过收发切换开关到移相器后送至后续处理系统; 执行发射功能时, 组件发射的激励信号依次通过收发开关、移相器, 在功放链路内完成信号功率放大, 然后通过耦合器、环形器输出至天线辐射; 同时通过移相和衰减器的控制实现雷达系统对波束的有序调配和控制.

T/R组件良好的可靠性和连通性是雷达安全稳定运行的基础保障. 本文结合物理脆弱性和结构脆弱性提出综合脆弱性概念, 并对其进行定量评估. 物理脆弱性研究基础元件对系统运行造成的伤害, 以可靠性作为评价指标, 可通过故障树-蒙特卡洛仿真计算得到; 结构脆弱性考察T/R组件电路系统的网络拓扑结构稳定、网络边界连接安全等属性, 基于复杂网络理论构建相关统计特征作为评价指标. 将物理

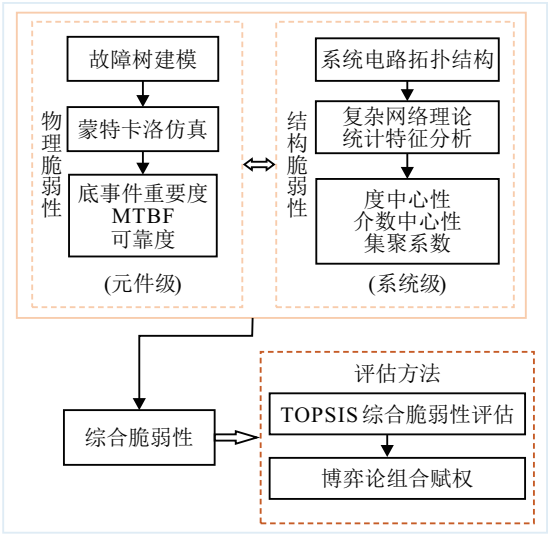

图 1 T/R组件综合脆弱性评估基本架构

脆弱性指标与结构脆弱性指标加权相融合,给出综合脆弱性评价的数学模型. 本文提出了博弈组合赋权-TOPSIS方法优化组合权重,评估其脆弱性. 综上,T/R组件综合脆弱性评估体系如图1所示. 下面分别给出物理脆弱性和结构脆弱性的获取.

1.1　基于故障树-蒙特卡洛的元件物理脆弱性

基于运行状态的元件物理脆弱性主要研究系统故障时的内在演化机理,即各元件的可靠性水平. 首先采用故障树分析(FTA)方法[22],对T/R组件故障传播由上至下按逻辑关系构建故障树模型. 以T/R组件故障为顶事件T,有TR数字板故障M_1等共5个中间事件,导致顶事件发生;继续分析找到引起中间事件发生的共25个底事件,分别为FPGA短路X_1等,T/R组件故障树如图2所示.

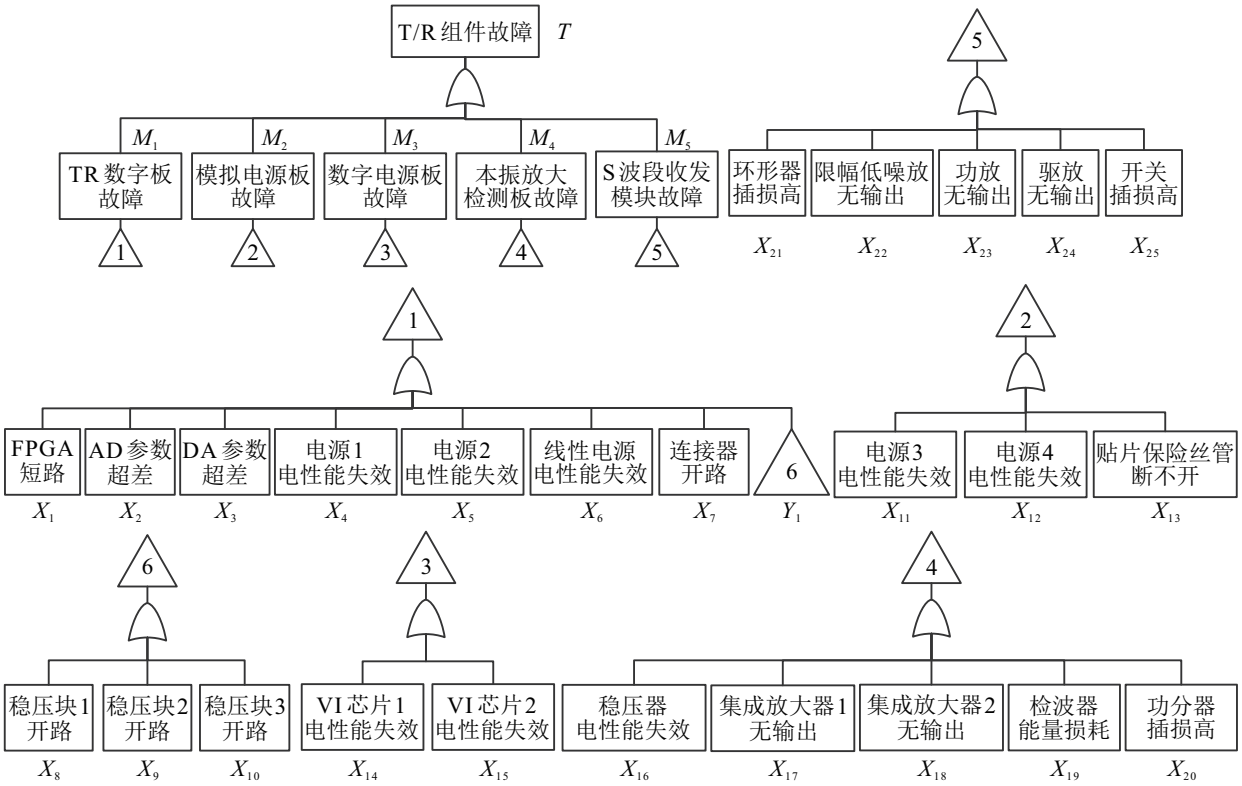

图 2　T/R组件故障树

如图2所示的FPGA短路X_1等底事件$X_i\,(i=1,2,\ldots,25)$为T/R组件故障树的25个最小割集[23]. 故障服从指数分布的故障密度函数为

$$f_i(t)=\lambda_i \mathrm{e}^{-\lambda_i t},\ t>0, \tag{1}$$

则可靠度函数定义[24]如下式所示:

$$R_i(t)=\int_t^{\infty} f_i(t)\mathrm{d}t=\mathrm{e}^{-\lambda_i t}. \tag{2}$$

元件的平均寿命等于失效率的倒数,即

$$\mathrm{MTBF}_i=\frac{1}{\lambda_i}. \tag{3}$$

为了更好地得到上述可靠性指标,本文运用蒙特卡洛(Monte Carlo method)方法建立T/R组件故障树仿真模型并进行计算,仿真流程如图3所示.

设T/R组件故障树T为n个基本事件的集合,$T=\{X_i|i=1,2,\ldots,n\}$,用$x_i(t)$、$\Phi(t)$分别表示基本事件X_i、顶事件的状态变量,即

$$x_i(t)=\begin{cases}1,\ t\text{时刻}X_i\text{发生};\\ 0,\ t\text{时刻}X_i\text{不发生}.\end{cases} \tag{4}$$

$$\Phi(t)=\begin{cases}1,\ t\text{时刻顶事件发生};\\ 0,\ t\text{时刻顶事件不发生}.\end{cases} \tag{5}$$

故障树的结构函数为$\Phi[X(t)]$,其中$X(t)=\{x_i(t)|i=1,2,\ldots,n\}$. 显然,$\Phi(t)$由$X(t)$决定,即$\Phi(t)=\Phi[X(t)]$.

第i个基本事件的失效时间t_i为其失效分布函数$F_i(t)$取反,即$t_i=F_i^{-1}(t)(i=1,2,\ldots,n)$. 由此得到包含$b$个基本事件的最小割集$m\,(m=1,2,\ldots,k)$的失效时间为$T_m=\max\{t_1,t_2,\ldots,t_b\}$,则故障树中$k$个最小割集的失效时间$T_1,T_2,\ldots,T_k$从小到大进行排序后为$T_{f_1},T_{f_2},\ldots,T_{f_k}$,进而判断出基本事件以及顶事件的状态,得到系统的失效时间TF(取$\min\{T_{f_i}|i=1,2,\ldots,k\}$).

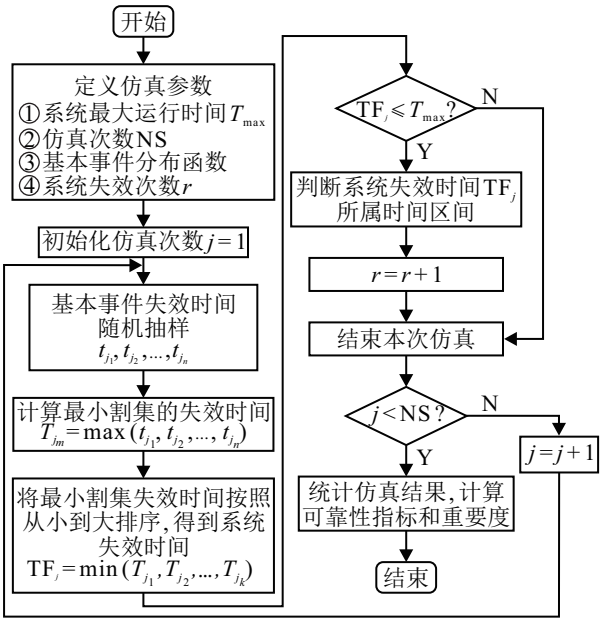

图 3 T/R 组件的故障树仿真流程

设定系统在 $(0,T_{\max}]$ 仿真 NS 次,仿真次数 $j=1,2,\ldots,$ NS,并以固定步长 $\Delta T=T_{\max}/M$ 划分为 M 个均等时间间隔区间. Δm_x 为在时间区间 $(t_{x-1},t_x]$ 内系统失效次数,即

$$\Delta m_x=\sum_{j=1}^{\mathrm{NS}}\Phi_j(\mathrm{TF}_j),\ t_{x-1}<\mathrm{TF}_j\leqslant t_x. \tag{6}$$

其中: $t_{x-1}=(x-1)\Delta T, t_x=x\Delta T$. 则时刻 t_x 前的累计故障数 $m_x=\sum_{i=1}^{x}\Delta m_i$, 系统总失效次数 $r=\sum_{i=1}^{M}\Delta m_i$.

根据仿真抽样结果计算可靠性相关指标[25],具体如下.

1) 可靠度为

$$R(t)=1-\frac{m_x}{\mathrm{NS}}. \tag{7}$$

2) 故障概率分布为

$$f(t)=\Delta m_x/\mathrm{NS}. \tag{8}$$

3) 平均无故障时间 MTBF 为

$$\mathrm{MTBF}=\int_0^{\mathrm{T}}t\cdot f(t)\mathrm{d}t\approx 1\Big/\sum_{j=1}^{\mathrm{NS}}\mathrm{TF}_j. \tag{9}$$

4) 基本部件单元重要度为

$$w(X_i)=s_i/s_0. \tag{10}$$

其中: s_i 为基本部件 X_i 故障引起系统失效的次数, s_0 为基本部件 X_i 故障的次数.

5) 基本部件模式重要度为

$$w_N(X_i)=s_i/r. \tag{11}$$

其中: s_i 为基本部件 X_i 故障引起系统失效的次数, r 为系统总失效次数.

1.2 基于复杂网络理论的系统结构脆弱性

基于电路拓扑的系统结构脆弱性主要研究某一元件节点退出电路网络后,系统保持其拓扑结构完整并正常运行的能力,可采用复杂网络理论计算系统统计特征量构建结构脆弱性指标[26]. T/R 组件规模庞大,元件数量众多,关系复杂;任意一个元件的故障,均会影响系统的稳定性;同时作战环境具有随机性. 因此, T/R 组件具备复杂网络的一般特性.

在故障树中, FPGA 短路等 25 个底事件为组成 T/R 组件的 25 个元件对应的故障模式. 基于 T/R 组件的结构和运行特点,由 FPGA 等 25 个元件作为节点,将元件间的连接关系等效为边,建立 T/R 组件电路网络的等效拓扑模型如图 4 所示. 根据复杂网络理论,选取表现局域特征的度中心性、集聚系数以及表现全局特征的介数中心性的 3 个统计特征来描述 T/R 组件电路网络的结构脆弱性[27].

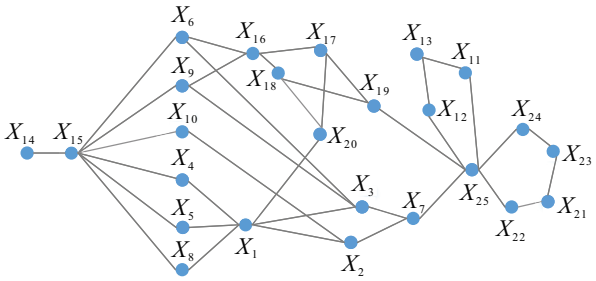

图 4 T/R 组件电路网络拓扑图

度中心性用于衡量节点邻接边数的多少,值越大,该节点越重要,有

$$\mathrm{DC}_i=k_i/(N-1). \tag{12}$$

其中: k_i 为节点 i 的度, N 为网络的节点个数.

集聚系数为在局部网络中,节点失效对其连通性的影响程度,有

$$C_i=\frac{2E_i}{k_i(k_i-1)}, \tag{13}$$

其中 E_i 为有 k_i 个邻节点的节点 i 实际存在的邻边数.

介数中心性为节点间相互独立的程度,有

$$\mathrm{BC}_i=\sum_{s\neq i\neq t}\frac{\sigma_{st}^i}{\sigma_{st}}. \tag{14}$$

其中: σ_{st} 为从节点 s 到节点 t 所有的最短路径数量, σ_{st}^i 为经过节点 σ_{st}^i 的最短路径数量.

2 基于博弈组合赋权-TOPSIS 脆弱性评估

2.1 综合脆弱性评估指标模型

第 1 节分别讨论了元件物理脆弱性和系统结构脆弱性,由此建立综合脆弱性评估层次体系,如图 5 所示. 综合脆弱性 O 定义为物理脆弱性 S_1 与结构脆弱性 S_2 两个一级指标的集合,即 $O=(S_1,S_2)$. S_1、S_2

分别定义为其对应的二级指标集合,表示为$S_i=(I_j^i|j=1,2,\dots,q^i)(i=1,2)$,其中二级指标个数$q=\sum_{i=1}^{2}q^i$. 值得指出的是,所提出方法不仅局限于上述两类一级指标,当存在多个一级指标及其对应的二级指标时,只需将i从2直接拓展为一级指标个数即可.

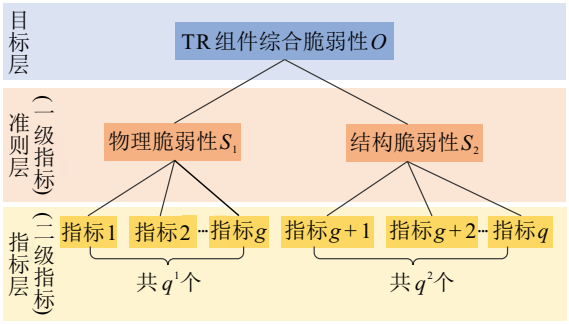

图 5　综合脆弱性评估层次体系

综合脆弱评估体系的指标权重由多种不同的赋权方法确定. 通过a种赋权方法得到最底指标层对目标层的权重向量为$\omega_m=(\omega_{m_n}|m=1,2,\dots,a,\ n=1,2,\dots,q)$,其中$q$为二级指标个数. 组合权重为$\omega^*=(\omega_j^*|j=1,2,\dots,q)$. 其中:$\omega_j^*=\sum_{m=1}^{a}\beta_j^*\cdot\omega_{m_n}$,$\beta_j^*$和$\omega_{m_n}$分别为不同赋权方法的线性组合系数和指标权重.

为了求得最合理的权重组合ω^*,引入博弈理论,提出了博弈组合赋权-TOPSIS的综合脆弱性指标权重优化方法. 该方法将多种权重视为博弈中的决策主体,在不断冲突中寻找利益平衡点,有效避免了单一权重确定方法的局限性,提升指标赋权的科学合理性. 同时,博弈理论广泛应用于脆弱性模型构建等相关研究,电路的攻击与防御构成竞争关系,攻防博弈理论已应用于攻防行为模型[28]、制定攻防策略[29]和负荷计算损失[30]等方面.

2.2　博弈组合赋权优化问题和求解

博弈组合赋权的思想为在不同赋权方法所求权重间寻找一致或妥协,使得可能的组合权重与各基本权重间的偏差达到最小,即纳什均衡点[31]. 由a种不同赋权方法得到q个指标的权重向量为ω_m,进而构造一个基本权重集$\{\omega_1,\omega_2,\dots,\omega_a\}$.

基本权重的任意线性组合构成可能的组合权重为

$$\omega=\sum_{m=1}^{a}\beta_m\cdot\omega_m^{\mathrm{T}}. \tag{15}$$

其中:β_m为线性组合系数,$\sum_{m=1}^{a}\beta_m=1$,且$\beta_m>0$.

寻找最合理的组合权重ω^*,即以ω与ω_m的偏差最小化为目标,优化式(15)的线性组合系数β_m. 由此构造博弈对策模型为

$$\min\left\|\sum_{m=1}^{a}\beta_i\cdot\omega_j^{\mathrm{T}}-\omega_i^{\mathrm{T}}\right\|_2,\ i=1,2,\dots,a. \tag{16}$$

由矩阵微分原理得到式(16)最优化一阶导数条件[32]为

$$\sum_{j=1}^{a}\beta_j\cdot\omega_i\cdot\omega_j^{\mathrm{T}}=\omega_i\cdot\omega_i^{\mathrm{T}}. \tag{17}$$

对应的线性方程组记为

$$\begin{bmatrix}\omega_1\omega_1^{\mathrm{T}} & \omega_1\omega_2^{\mathrm{T}} & \dots & \omega_1\omega_a^{\mathrm{T}}\\ \omega_2\omega_1^{\mathrm{T}} & \omega_2\omega_2^{\mathrm{T}} & \dots & \omega_2\omega_a^{\mathrm{T}}\\ \vdots & \vdots & \ddots & \vdots\\ \omega_a\omega_1^{\mathrm{T}} & \omega_a\omega_2^{\mathrm{T}} & \dots & \omega_a\omega_a^{\mathrm{T}}\end{bmatrix}\begin{bmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_a\end{bmatrix}=\begin{bmatrix}\omega_1\omega_1^{\mathrm{T}}\\ \omega_2\omega_2^{\mathrm{T}}\\ \vdots\\ \omega_a\omega_a^{\mathrm{T}}\end{bmatrix}. \tag{18}$$

由式(18)计算β_m值,并归一化处理,则最终的组合权重为

$$\omega^*=\sum_{m=1}^{a}\beta_i^*\cdot\omega_m^{\mathrm{T}}. \tag{19}$$

其中:$\beta_i^*=\beta_m\Big/\sum_{m=1}^{a}\beta_m$,$\omega^*=(\omega_1^*,\omega_2^*,\dots,\omega_q^*)^{\mathrm{T}}$,$\omega_q^*=\sum_{m=1}^{a}\omega_m^*\cdot\omega_{m_n}$.

值得指出的是,本文中综合评价权重包括客观和主观,分别采用反熵法和层次分析法(analytic hierarchy process, AHP)确定,具体如下.

1) 基于反熵法的客观权重计算.

设有p个待评估对象集合为$A=(A_1,A_2,\dots,A_p)$,q个评价指标组成的指标层集合为$I=(I_1,I_2,\dots,I_q)$,则A_i对I_i的决策样本r_{ij}构成了决策矩阵$R=(r_{ij})_{p\times q}$,R标准化处理后得到标准化决策矩阵$R'=(r'_{ij})_{p\times q}$,即

$$r'_{ij}=\begin{cases}\dfrac{r_{ij}-r_{\min j}}{r_{\max j}-r_{\min j}}, & \text{正向指标;}\\ \dfrac{r_{\max j}-r_{ij}}{r_{\max j}-r_{\min j}}, & \text{负向指标.}\end{cases} \tag{20}$$

其中:r_{ij}为评估对象i的指标j的数值,r'_{ij}为标准化决策矩阵$R'=(r'_{ij})_{p\times q}$中的第i行第j列的元素,$r_{\min j}$为决策矩阵R第j列数值最小的元素,$r_{\max j}$为第j列数值最大的元素,$1\leqslant i\leqslant p$,$1\leqslant j\leqslant q$.

指标的比重为$v_{ij}=r'_{ij}\Big/\sum_{i=1}^{p}r'_{ij}$,由此得到指标的熵值为

$$E_j=-k\cdot\sum_{i=1}^{p}v_{ij}\times\ln v_{ij}, \tag{21}$$

其中$k=1/\ln p$.

改进反熵1为$E'_j=-k\cdot\sum_{i=1}^{p}(1-v_{ij})\times\ln v_{ij}$;改

进反熵2为$E'_j=-k\cdot\sum_{i=1}^{p}v_{ij}\times\ln(1-v_{ij})$. 若$v_{ij}=1$, 则定义$\lim\limits_{p_{ij}\to 1}v_{ij}\times\ln(1-v_{ij})=0\,(1\leqslant i\leqslant p,1\leqslant j\leqslant q)$. 计算反熵1、反熵2的客观权重为

$$\omega'_j=\frac{e'_j}{\sum\limits_{j=1}^{p}e'_j},\ \omega''_j=\frac{e''_j}{\sum\limits_{j=1}^{p}e''_j}. \tag{22}$$

其中: $e'_j=1-E'_j, e''_j=1-E''_j$, 分别为反熵1、反熵2的差异系数. 通过上述计算得到两类反熵, 确定各评估指标权重分别为$\omega'_1=\{\omega'_{11},\omega'_{12},\dots,\omega'_{1q}\}$、$\omega''_1=\{\omega''_{11},\omega''_{12},\dots,\omega''_{1q}\}$.

2) 基于AHP的主观权重计算.

以系统综合脆弱性作为目标层, 以物理脆弱性和结构脆弱性作为准则层, 对应指标作为指标层. 根据表1构造判断矩阵, 有

$$H=\begin{bmatrix}h_{11}&h_{12}&\dots&h_{1q}\\h_{21}&h_{22}&\dots&h_{2q}\\\vdots&\vdots&\ddots&\vdots\\h_{q1}&h_{q2}&\dots&h_{qq}\end{bmatrix}. \tag{23}$$

表 1 判断矩阵标度值

等级	1	3	5	7	9	2,4,6,8
相对重要程度	同等重要	稍微重要	明显重要	强烈重要	极端重要	中间重要状态
标度方法	9/9	9/7	9/5	9/3	9/1	9/2,9/4,9/6,9/8

计算判断矩阵的几何平均值$\bar{w}_i$, 得到指标的权重系数ω_2以及判断矩阵的最大特征根$\lambda_{\max}$, 即

$$\begin{cases}\bar{w}_i=\sqrt[q]{\prod\limits_{j=1}^{q}h_{ij}},\ i=1,2,\dots,q;\\ \omega_{2i}=\dfrac{\bar{w}_i}{\sum\limits_{i=1}^{q}\bar{w}_i};\\ \omega_2=\{\omega_{21},\omega_{22},\dots,\omega_{2q}\}.\end{cases} \tag{24}$$

$$\lambda_{\max}=\frac{1}{q}\sum_{i=1}^{q}\frac{\sum\limits_{j=1}^{q}h_{ij}\omega_{2j}}{\omega_{2i}}. \tag{25}$$

判断矩阵一致性的检验标准为

$$\mathrm{CI}=\frac{\lambda_{\max}-q}{q-1},\ q>1. \tag{26}$$

$$\mathrm{CR}=\frac{\mathrm{CI}}{\mathrm{RI}}. \tag{27}$$

其中: CR为随机一致性比率, $\mathrm{CR}<0.1$时通过检验, $\mathrm{CR}\geqslant 0.1$时不通过检验; CI为一般一致性指标; RI为平均随机一致性指标.

2.3 基于TOPSIS的综合脆弱性评价

利用博弈组合赋权方法得到主、客观的最优权重组合, 进而采用优劣解距离法(technique for order preference by similarity to ideal solution, TOPSIS)根据被评对象与理想目标的接近程度确定优劣[33], 实现系统综合脆弱性评估, 流程如图6所示.

根据标准化决策矩阵$R'=(r'_{ij})_{p\times q}$和组合赋权方法确定组合权重集合为ω_j^*, 求得加权标准决策矩阵Z, 即

$$Z=(z_{ij})_{p\times q}=(\omega_j^*\cdot r'_{ij})_{p\times q}. \tag{28}$$

其中: $i=1,2,\dots,p, j=1,2,\dots,q$.

确定所有被评对象集合的正、负理想解为

$$\begin{cases}z_j^+=\{(\max\limits_j z_{ij}|i\in J_1),(\min\limits_j z_{ij}|i\in J_2)\},\\ z_j^-=\{(\min\limits_j z_{ij}|i\in J_1),(\max\limits_j z_{ij}|i\in J_2)\}.\end{cases} \tag{29}$$

式中: 正、负理想解分别为z_j^+、z_j^-, 正、负向指标分别为J_1、J_2. 计算被评对象与理想目标的接近程度, 即

$$d_i^+=\sqrt{\sum_{j=1}^{q}(z_j^+-z_{ij})^2},\ d_i^-=\sqrt{\sum_{j=1}^{q}(z_j^--z_{ij})^2}. \tag{30}$$

得到节点的相对贴近度, 即

$$c_i=d_i^-/(d_i^++d_i^-). \tag{31}$$

根据c_i的大小排序结果给出关键元件脆弱性评价.

3 实例分析

3.1 综合脆弱性评估模型

以物理脆弱性S_1、结构脆弱性S_2作为一级指标及其对应指标$I_i\,(i=1,2,\dots,q)$作为二级指标构建T/R组件的综合脆弱性体系O. 物理脆弱性指标$I_i\,(i=1,2,3)$由故障树仿真确定, 依次为元件的模式重要度、平均故障间隔时间(MTBF)、可靠度. 本文基于T/R组件的25个元件为电路网络拓扑节点、元件间的连接关系为边, 构建T/R组件电路拓扑模型, 如图4所示; 将电路拓扑的统计特性确定为结构脆弱性指标$I_j\,(j=4,5,6)$, 依次为度中心性、介数中心性、集聚系数.

3.2 故障树仿真

查询资料确定T/R组件故障树FPGA短路X_1等25个底事件的故障率以及故障分布类型. 由式(3)计算得到理论平均寿命MTBF为62 527 h. 设定仿真参数$T_{\max}=500\,000$ h, $M=1\,000$ h. 当NS设定为

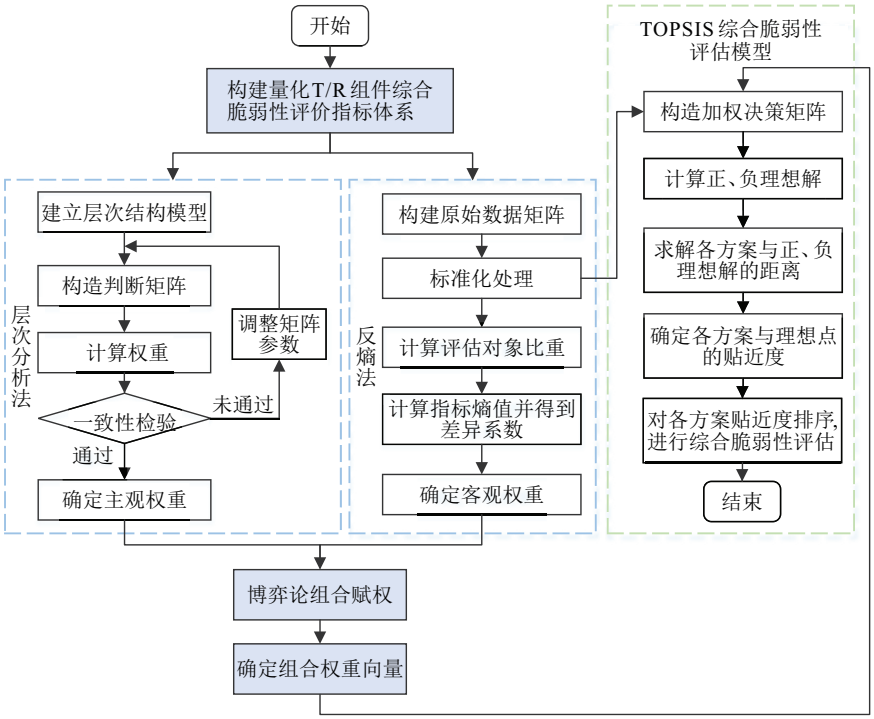

图 6　系统综合脆弱性评估流程

20 000次时,仿真结果趋于稳定且仿真MTBF与理论MTBF的相对误差为0.01 %,因此NS取20 000次. 重复以上实验10次,求得10次仿真的MTBF均值为62 532 h,方差为238.488,波动幅度较小,表明仿真结果有效;计算仿真MTBF与理论MTBF的相对误差为0.007 9 %,验证了仿真的正确性. T/R组件可靠性仿真曲线、基本元件的可靠性仿真指标以及拓扑统计特征分别如图7和表2所示.

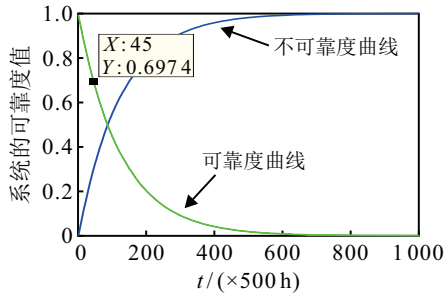

图 7　T/R组件失效的可靠度/不可靠度曲线

图7为可靠度/不可靠变化曲线. 由图7可见,当系统运行时间$t \in (0, 22\,500\ \text{h}]$时,T/R组件的可靠度大于0.7. 运行至250 000 h后,可靠度接近0. 随着工作时间增加,系统可靠度呈现明显下降趋势,不可靠度反之,与实际情况相符. 曲线反映了T/R组件失效随时间变化的动态响应关系,在描述故障问题时比传统故障树的定量计算结果更加形象. 表2给出了基本部件的单元重要度$w(X_i)$、模式重要度$w_N(X_i)$、MTBF和可靠度. 其中:$w(X_i)$均为1,表明系统必然会因底事件X_i故障而发生崩溃. 该结果与故障树分析的最小割集计算结果保持一致. 若$w_N(X_i)$越大,则基本部件X_i失效对系统影响程度越大,X_i为系统的薄弱环节.

3.3　结构脆弱性和物理脆弱性评价

1) 反熵法确定客观权重.

3种熵值赋权方法求出综合脆弱性的各项指标权重如图8所示. 由图8可见,不同赋权方法得到的权重变化趋势比较一致,但是波动大小不同. 相较于熵权法,反熵权对指标的敏感度更小,避免了指标权重过小的极端情况;相比于反熵权1,反熵权2使得少数指标权重较高,多数指标权重相对落后,提高了系统评价的合理科学性. 因此,本文采用反熵权2确定指标的客观权重为$\omega_1 = (0.162\,0, 0.169\,0, 0.162\,3, 0.169\,4, 0.167\,8, 0.169\,2)$.

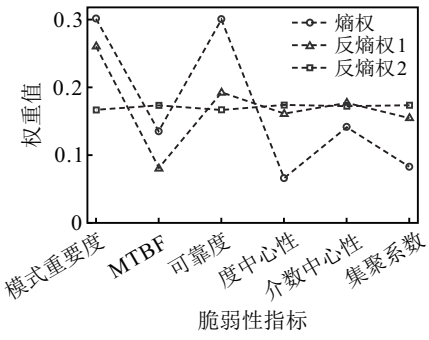

图 8　基于不同熵值赋权法的指标客观权重

2) AHP确定主观权重.

针对T/R组件的脆弱性,基于AHP的权重确定方案需要考虑以下因素. 单一从物理脆弱性或结构脆

表2 T/R组件基本元件可靠性仿真指标以及拓扑统计特征

基本元件序号	可靠性仿真指标				拓扑统计特征		
	单元重要度	模式重要度	MTBF/(10^7h)	可靠度	度中心性	介数中心性	集聚系数
X_1	1	0.001 68	3.333 3	0.999 2	0.250 0	43.000	0.210 0
X_2	1	0.001 52	3.333 3	0.999 2	0.125 0	26.500	0.201 1
X_3	1	0.001 84	3.333 3	0.999 2	0.166 6	36.500	0.230 7
X_4	1	0.001 60	3.333 3	0.999 2	0.083 3	0.666 6	0.055 5
X_5	1	0.001 96	3.333 3	0.999 2	0.083 3	0.666 6	0.055 5
X_6	1	0.001 92	3.333 3	0.999 2	0.125 0	10.000	0.055 5
X_7	1	0.002 24	3.333 3	0.999 2	0.125 0	60.000	0.223 2
X_8	1	0.002 28	3.333 3	0.999 2	0.083 3	0.666 6	0.055 5
X_9	1	0.001 68	3.333 3	0.999 2	0.125 0	10.000	0.055 5
X_{10}	1	0.002 00	3.333 3	0.999 2	0.083 3	6.000 0	0.055 5
X_{11}	1	0.083 48	0.075 7	0.967 5	0.083 3	2.500 0	0.041 6
X_{12}	1	0.084 52	0.075 7	0.967 5	0.083 3	2.500 0	0.041 6
X_{13}	1	0.009 12	0.657 8	0.996 2	0.083 3	0	0
X_{14}	1	0.077 08	0.079 4	0.969 0	0.0416	0	0
X_{15}	1	0.078 36	0.079 4	0.969 0	0.291 6	20.000	0.041 6
X_{16}	1	0.077 28	0.079 4	0.969 0	0.166 6	20.000	0.095 2
X_{17}	1	0.266 44	0.023 8	0.900 3	0.125 0	11.500	0.086 8
X_{18}	1	0.260 40	0.023 8	0.900 3	0.125 0	11.500	0.086 8
X_{19}	1	0.004 48	1.492 5	0.998 3	0.125 0	16.000	0.107 4
X_{20}	1	0.036 48	0.166 6	0.985 1	0.125 0	15.000	0.107 4
X_{21}	1	0.000 52	8.333 3	0.999 7	0.083 3	26.000	0.193 5
X_{22}	1	0.000 80	8.333 3	0.999 7	0.083 3	6.000 0	0.166 6
X_{23}	1	0.000 76	8.333 3	0.999 7	0.083 3	46.000	0.230 7
X_{24}	1	0.000 60	8.333 3	0.999 7	0.083 3	66.000	0.285 7
X_{25}	1	0.000 96	8.333 3	0.999 7	0.250 0	86.000	0.375 0

弱性均不能揭示系统整体的脆弱性,因此,认为两个准则同样重要. 在结构脆弱性中,节点度中心性和集聚系数表现局部特征,介数中心性体现全局特征,因此,介数中心性比前两者更重要;在物理脆弱性中,基本部件模式重要度表征系统的薄弱环节,因此,比其他两个指标更重要. 根据评估体系中不同脆弱性的不同指标组合的贡献程度,构造判断矩阵,并进行一致性检验,确定主观权重为$\omega_2 = (0.250\,0, 0.125\,0, 0.125\,0, 0.084\,5, 0.221\,7, 0.193\,6)$.

3.4 综合脆弱性评估和分析

根据求得的脆弱性指标的主、客观权重,基于博弈组合赋权求得综合脆弱性指标的最优组合权重;选取主观偏好系数为0.4、0.5、0.6的加权组合赋权法求得综合权重,将两种方法进行对比,如表3所示. 将TR组件综合脆弱性评估体系的各指标数据构造的加权标准化评价矩阵代入式(28)～(31),得到T/R组件各节点的综合脆弱性水平,结果如表4和图9所示.

由表3可见,选取不同的主观偏好系数对某些指标的权重造成较大影响,加权赋权方法以固定系数笼统地表示指标的重要度,人为地削弱了某些指标的权重对系统综合脆弱性的贡献程度,该方法稳定性较差. AHP可灵活地反映主观者的意图,但是没有考虑数据的内部规律;反熵法可显示出内部规律和有用的信息,但是忽略了实际情况. 结果表明,博弈组合权重与AHP的结果非常相似,源于达到纳什均衡的权重系数决定了AHP与反熵法的比例. 博弈赋权法通过降低AHP中模式重要度的比例,提高反熵法中介数中心性的比例,使得一些异常值更加合理,克服了单一算法的片面性问题,因此,能够更加合理有效地确定不同脆弱性指标的重要程度.

表3 不同赋权法的指标权重

指标	单一赋权法		加权组合赋权法			博弈组合赋权法
	层次分析法	反熵权法	0.4	0.5	0.6	
模式重要度	0.250 0	0.162 0	0.197 2	0.206 0	0.214 8	0.247 9
MTBF	0.125 0	0.169 0	0.151 4	0.147 0	0.142 6	0.126 0
可靠度	0.125 0	0.162 3	0.147 3	0.143 6	0.139 9	0.125 8
度中心性	0.084 5	0.169 4	0.135 4	0.126 9	0.118 4	0.086 4
介数中心性	0.221 7	0.167 8	0.189 3	0.194 7	0.200 1	0.220 4
集聚系数	0.193 6	0.169 2	0.178 9	0.181 4	0.183 8	0.193 0

表 4　脆弱性排序

节点编号	节点脆弱性排序		
	物理	结构	综合
X_1	6	5	4
X_2	9	7	9
X_3	7	6	5
X_4	12	21	2
X_5	11	20	19
X_6	4	17	12
X_7	8	3	2
X_8	10	19	18
X_9	5	16	13
X_{10}	3	18	17
X_{11}	25	23	23
X_{12}	17	22	22
X_{13}	20	24	24
X_{14}	21	25	25
X_{15}	24	9	11
X_{16}	22	10	14
X_{17}	1	15	17
X_{18}	2	14	8
X_{19}	13	13	15
X_{20}	23	12	21
X_{21}	15	8	10
X_{22}	19	11	16
X_{23}	14	4	6
X_{24}	18	2	3
X_{25}	16	1	1

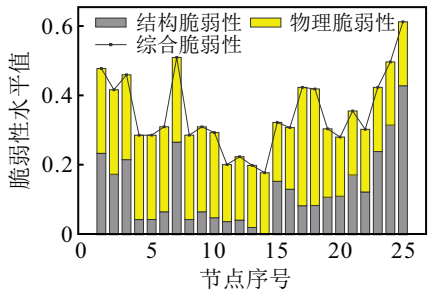

图 9　节点脆弱性水平值

由表4可见,在考虑单一脆弱性以及综合脆弱性筛选出的脆弱节点大致排序趋同,亦存在一定差异. 以物理脆弱性为评价指标,脆弱性最大的为节点X_{17},这是因为该节点元件故障率较高,易发生故障,在运行时故障将对系统的安全造成重大影响,是影响系统可靠性的关键因素;以结构脆弱性为评价指标时,节点X_{25}脆弱性最高,该节点位于电路结构的关键位置,其节点度、介数中心性等较大,即结构重要度较大,发生故障将影响整体的连通性.

如图9所示,综合脆弱性是融合物理与结构脆弱性的共同结果. 根据综合脆弱性评估结果,节点X_{25}、节点X_7的脆弱性较大. 节点X_7临界节点$X25$,其结构脆弱性相对较高,是电路的重要枢纽,且该节点物理脆弱性也位于前列. 评估结果表明,综合脆弱性不仅考量节点的电路结构重要性,且反映出节点失效对系统的影响. 同样如节点X_{21} ～ X_{24},其失效会对整个电路安全性造成很大影响,进一步表明了同时考虑节点状态脆弱性指标和结构脆弱性指标的必要性,同时表明了综合评价指标具有应用的可行性.

4　结　论

随着雷达技术的不断发展,研究T/R组件可靠性并分析其脆弱性具有重要的现实意义. 制定系统薄弱环节的防护策略,以有效降低系统的脆弱性. 本文基于融合元件可靠性和复杂网络脆弱性,构建了T/R组件的综合脆弱性评估体系. 与传统可靠性评估方法相比,所提出综合脆弱性评估融合多种指标,克服了单一评价指标的缺陷,有较高的参考价值,但是,本文的研究并未考虑实际情况中数据误差等不确定因素的影响,这也将是下一步的研究思路.

参考文献(References)

[1] Wang F, Zhang Z K, Sellathurai M, et al. Adaptive Markov transition matrix based multiple targets tracking for phased array radar[J]. Journal of the Chinese Institute of Engineers, 2014, 37(7): 955-963.

[2] Chen X Q. Investigation and design of high power T/R module[J]. Electronics & Packaging, 2012, 12(8): 19-22.

[3] Gai M Q, Yan S Q, Ma L, et al. Operational effectiveness evaluation of anti-ballistic-missile EWR based on improved ADC model[J]. Modern Radar, 2020, 42(3): 20-24.

[4] Song R Y, Liu S H, Yu J, et al. Evaluation of the effectiveness of the configuration of new phased array radar spare parts[C]. IEEE the 6th Information Technology and Mechatronics Engineering Conference. Chongqing, 2022: 969-972.

[5] Xia L, Xiang J, Yang J, et al. Safety evaluation of radar software system based on improved AHP and cloud model[J]. Journal of Ordnance Equipment Engineering, 2019, 40(8): 145-150.

[6] Deng R, Deng C J, Wang R L, et al. Research on reliability life evaluation method based on airborne T/R components[C]. The 22nd International Conference on Electronic Packaging Technology. Xiamen, 2021: 1-4.

[7] Fouad A A, Zhou Q, Vittal V. System vulnerability as a concept to assess power system dynamic security[J]. IEEE Transactions on Power Systems, 1994, 9(2): 1009-1015.

[8] Li X G, Hu X Y, Zhou C J, et al. Multi-dimensional collaborative analysis of vulnerability for full-lifecycle of industrial control systems[J]. Control and Decision, 2022, 37(11): 2827-2838.

[9] Yan J, He H B, Zhong X N, et al. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(1): 200-210.

[10] Sun Y, Xie B L, Wang S, et al. Dynamic assessment of road network vulnerability based on cell transmission model[J]. Journal of Advanced Transportation, 2021,

2021: 1-14.

[11] Wu D, Ma F, Javadi M, et al. A study of the impacts of flow direction and electrical constraints on vulnerability assessment of power grid using electrical betweenness measures[J]. Physica A: Statistical Mechanics and Its Applications, 2017, 466: 295-309.

[12] Dai Y Y, Chen G, Dong Z Y, et al. An improved framework for power grid vulnerability analysis considering critical system features[J]. Physica A: Statistical Mechanics and Its Applications, 2014, 395: 405-415.

[13] Beyza J, Ruiz-Paredes H F, Garcia-Paricio E, et al. Assessing the criticality of interdependent power and gas systems using complex networks and load flow techniques[J]. Physica A: Statistical Mechanics and Its Applications, 2020, 540: 123169.

[14] Yang S H, Chen W R, Zhang X X, et al. A graph-based method for vulnerability analysis of renewable energy integrated power systems to cascading failures[J]. Reliability Engineering & System Safety, 2021, 207: 107354.

[15] Liu S M, Yu Y, Guo L. A vulnerability analysis method for critical elements based on network connectivity[J]. Control and Decision, 2020, 35(6): 1421-1426.

[16] Liu B, Li Z, Chen X, et al. Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 65(3): 346-350.

[17] Cetinay H, Devriendt K, Van Mieghem P. Nodal vulnerability to targeted attacks in power grids[J]. Applied Network Science, 2018, 3(1): 34.

[18] Wei X G, Gao S B, Huang T, et al. Identification of two vulnerability features: A new framework for electrical networks based on the load redistribution mechanism of complex networks[J]. Complexity, 2019, 2019: 1-14.

[19] Rocchetta R, Patelli E. Assessment of power grid vulnerabilities accounting for stochastic loads and model imprecision[J]. International Journal of Electrical Power & Energy Systems, 2018, 98: 219-232.

[20] Wang W C, Zhang Y, Li Y X, et al. Vulnerability analysis of a natural gas pipeline network based on network flow[J]. International Journal of Pressure Vessels and Piping, 2020, 188: 104236.

[21] Kou S K, Kou Z M. Fault analysis and reliability simulation of deep mine hoisting wire rope[J]. Coal Engineering, 2018, 50(3): 112-115.

[22] Boryczko K, Szpak D, Żywiec J, et al. The use of a fault tree analysis in the operator reliability assessment of the critical infrastructure on the example of water supply system[J]. Energies, 2022, 15(12): 4416.

[23] Cheliyan A S, Bhattacharyya S K. Fuzzy fault tree analysis of oil and gas leakage in subsea production systems[J]. Journal of Ocean Engineering and Science, 2018, 3(1): 38-48.

[24] Zeng S K. Reliability design and analysis[M]. Beijing: National Defense Industry Press, 2011: 14-15.

[25] Shi F Y, Gao X D, Xing Z Y, et al. Reliability analysis of the subway door system based on Monte Carlo[J]. Modular Machine Tool & Automatic Manufacturing Technique, 2015(8): 104-106.

[26] Xie B H, Tian X G, Kong L L, et al. The vulnerability of the power grid structure: A system analysis based on complex network theory[J]. Sensors, 2021, 21(21): 7097.

[27] Chen C Y, Zhou Y, Chi M, et al. Review of large power grid vulnerability based on complex network theory[J]. Control and Decision, 2022, 37(4): 782-798.

[28] Huang J H, Feng D Q, Wang H. A method for quantifying vulnerability of industrial control system based on attack graph[J]. Acta Automatica Sinica, 2016, 42(5): 792-798.

[29] Sanjab A, Saad W. Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.

[30] Wang C, Hou Y H, Ten C W. Determination of Nash equilibrium based on plausible attack-defense dynamics[J]. IEEE Transactions on Power Systems, 2017, 32(5): 3670-3680.

[31] Lai C G, Chen X H, Chen X Y, et al. A fuzzy comprehensive evaluation model for flood risk based on the combination weight of game theory[J]. Natural Hazards, 2015, 77(2): 1243-1259.

[32] Dong M T, Cheng J H, Zhao L. A combination weighting model based on iMOEA/D-DE[J]. Frontiers of Information Technology & Electronic Engineering, 2022, 23(4): 604-616.

[33] Yang W C, Xu K, Lian J J, et al. Integrated flood vulnerability assessment approach based on TOPSIS and Shannon entropy methods[J]. Ecological Indicators, 2018, 89: 269-280.

作者简介

张倩 (1999−), 女, 硕士生, 从事故障诊断与容错控制等研究, E-mail: zhang_qian_email@163.com;

黄大荣 (1978−), 男, 教授, 博士, 从事故障诊断与预测、可靠性与容错控制等研究, E-mail: drhuang@cqjtu.edu.cn;

王晶 (1972−), 女, 教授, 博士, 从事数据驱动的复杂过程建模、优化、控制以及故障诊断等研究, E-mail: jwang@ncut.edu.cn;

周萌 (1988−), 女, 副教授, 博士, 从事故障诊断与容错控制等研究, E-mail: zhoumeng@ncut.edu.cn;

赵宁 (1972−), 男, 高级工程师, 从事舰船电子系统六性设计技术的研究, E-mail: zxt616@163.com;

张宇 (1983−), 男, 高级工程师, 从事舰船电子系统六性设计技术的研究, E-mail: 15305180040@163.com.