文章编号：2095-4980(2024)07-0752-06

用频装备电磁频谱参数泄露风险评估方法

颜　军，刘　青*，张江明

(中国电波传播研究所，山东 青岛 266107)

摘　要：针对通信、雷达等用频装备日益突出的电磁频谱使用安全，以及电磁频谱参数泄露风险量化评估难等问题，本文采用数值、解析等方法对敌我用频装备发射特征、接收敏感特征及天线辐射特性等进行电磁特征参数建模；结合电磁频谱参数泄露完整的通信链路结构，从用频装备效能与电波环境影响角度进行分析，运用网格剖分思想，量化分析用频装备电磁频谱参数泄露概率，提出一种电磁频谱参数泄露概率计算方法，并通过仿真验证了该计算方法。计算得到地面固定雷达L1和1 000跳发射电台M1分别在300~450 km和350~450 km范围内的泄露概率值，实现了电磁频谱参数泄露风险量化评估，解决了电磁频谱参数泄露风险量化评估难问题。

关键词：电磁频谱；电波传播；泄露概率；量化评估

中图分类号：TN911　　**文献标志码：**A　　**doi：**10.11805/TKYDA2023004

Risk assessment method for electromagnetic spectrum parameter leakage of frequency equipment

YAN Jun，LIU Qing*，ZHANG Jiangming

(China Research Institute of Radiowave Propagation，Qingdao Shandong 266107，China)

Abstract：In response to the increasingly prominent issues of electromagnetic spectrum usage safety for communication and radar equipment, as well as the difficulty in quantifying the risk assessment of electromagnetic spectrum parameter leakage, this paper employs numerical and analytical methods to model the electromagnetic characteristic parameters of emission features, reception sensitivity, and antenna radiation characteristics for both friendly and adversary frequency-dependent equipments. By integrating the complete communication link structure of electromagnetic spectrum parameter leakage, the analysis is conducted from the perspectives of equipment effectiveness and the impact on the radio wave environment. Utilizing the concept of grid division, a method for calculating the probability of electromagnetic spectrum parameter leakage is proposed, and the calculation method is verified through simulation. The leakage probabilities for a ground-based fixed radar L1 and a 1 000-hop transmission station M1 within the ranges of 300~450 km and 350~450 km, respectively, are calculated. This achieves a quantified assessment of the risk of electromagnetic spectrum parameter leakage, solving the problem of difficult risk quantification in electromagnetic spectrum parameter leakage assessment.

Keywords：electromagnetic spectrum；radio wave propagation；leakage probability；quantitative evaluation

通信、雷达等用频装备在正常工作时，会有意向外发射电磁信号，但可能会无意辐射一些电磁信号，这些电磁信号如被接收分析，极可能被还原相关信息，导致电磁频谱参数泄露[1]。这种由于电磁发射而造成的电磁频谱使用安全问题即为电磁频谱参数泄漏。

随着军队信息化装备不断演进，用频装备逐渐从保障装备转化为主战装备，涉及到通信、雷达、导航、制导、电磁攻击、战场感知等领域，几乎涵盖了现代化战争的所有功能域[2]，频率范围覆盖了短波、超短波、微波等各个频段。超短波、微波信号为视距传播，辐射距离通常可达几公里至十几公里，微波接力装备通过单跳接

收稿日期：2023-01-05；**修回日期：**2023-02-16

***通信作者：**刘　青　email:15029956267@163.com

力可达数十公里。近年来，敌对势力进一步加大了对我军情报信息的侦收力度，利用高灵敏度的接收设备侦收我军用频装备向外辐射的电磁信号，并将其复现和利用；尤其是敌对势力在我周边地区建立起立体化的电磁频谱参数侦收网的大环境下[2]，用频系统能正常使用电磁频谱，但不能保证电磁频谱信息不被窃取和利用[3]，用频装备电磁参数面临巨大的安全威胁。随着技术的不断发展，电磁频谱参数泄露给用频装备使用带来的安全隐患日益突出[4]。

目前，针对用频装备参数泄露问题，西方发达国家关于装备电磁频谱参数安全领域的研究已涉及陆基、海基和天基等领域，但未见具体成果的公开报道。国内各研究机构做了大量的研究，但都仅限于用频装备电磁频谱参数泄露原理、泄露途径、泄露模式等防护措施理论的分析研究[3,5−6]，没有考虑装备在实际作战环境中，尤其是敌我攻防条件下的组织运用，对泄露风险情况摸不清，无法针对性采取相应防护措施。如何精确计算出电磁频谱参数泄露概率，确保用频装备安全用频成为目前亟待解决的问题。

本文首先分析了用频装备电磁频谱参数泄露原理，考虑辐射泄露为电磁频谱参数泄露的主要途径，参考完整的通信链路结构，建立用频装备电磁辐射特性模型、接收敏感性模型、天线辐射特性模型及电波传播模型；基于此模型，从电磁信号功率与侦收系统灵敏度关系着手，综合考虑装备辐射能力、电磁信号传输损耗等因素，结合侦收设备接收敏感特性进行分析，引入网格分析方法，进行用频装备电磁频谱参数量化分析。最后采用数值仿真计算方法，验证了评估方法的合理性。

1　电磁频谱参数泄露原理

电磁泄露实际上是从“泄露源”向“窃收系统”有意或无意地传输信息，因此从泄露源产生电磁发射到窃收系统还原信息各环节可视为一个“无意发送、蓄意接收”的等效通信链路[1]，敌方通过分析处理截获的电磁信号，从中获取用频装备的地理位置、工作方式、频率特征、使用规律等频谱参数，并加以利用[2]。电磁参数泄露等效通信链路结构如图 1 所示，按照传输链路，泄露途径可分为辐射泄露和传导泄露 2 种[2,6−7]。其中辐射泄露为主要模式，本文针对辐射泄露模式的风险情况进行分析评估。

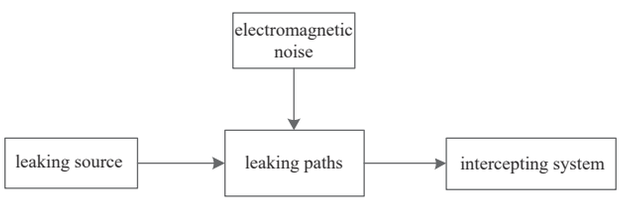

Fig.1 Communication link structure of electromagnetic parameter leakage

图 1 电磁参数泄露等效通信链路结构

电磁频谱泄露过程涉及发信机正常信号发射，同时承载电磁频谱参数信息的发射，经过无线信道传输后被侦收系统接收。电磁信号在传输中受地理环境、气象环境以及噪声干扰的影响，会发生信号衰减、方向以及相位改变，侦收系统一般具备高灵敏接收能力与信号处理能力，能够从接收信号中提取泄露的电磁频谱参数。

电磁频谱参数泄露必须满足 3 个条件：a) 己方存在主动(有意或无意)向外辐射电磁信号的电磁频谱参数泄露源；b) 电磁频谱参数泄露源向外辐射的电磁信号可被敌方接收；c) 敌方能够从接收的电磁信号中提取电磁频谱参数信息。

2　电磁频谱参数泄露风险评估方法

基于电磁频谱参数泄露机理分析，从能量角度出发，电磁频谱参数泄露造成电磁频谱安全风险程度都可以归结为泄露电磁信号功率与侦收系统灵敏度之间的关系。电磁信号发射功率大小与装备电磁辐射能力、电波传播环境等相关，因此，从电磁信号功率与侦收系统灵敏度关系着手，综合考虑装备辐射能力、电磁信号传输损耗等因素，结合侦收设备接收敏感特性进行分析。电磁频谱参数泄露风险评估方法包括用频装备效能建模、电波传播环境分析、用频装备电磁频谱参数风险评估等方面。

2.1 用频装备电磁频谱参数建模

首先对敌我用频装备进行数字化建模，如图 2 所示，确定其电磁频谱基本参数模型，包括空间位置、频率、功率、信号调制方式等参数；之后根据电磁理论，利用数值、解析等方法建立相应数学模型，考虑通信链路收发特性，基于调制特征参数(调制方式、扩展参数及辅助分析参数等)，建立发射设备辐射特性模型，输出不同调

制样式电磁信号时域特征和频域特征参数；最后根据典型设备接收性能分析结果，建立接收设备选频特性模型，包括模拟滤波模型、数字滤波模型和设备灵敏度特性模型。其中数字滤波器分为无限冲击响应(Infinite Impulse Response，IIR)和有限冲击响应(Finite Impulse Response，FIR)两类；设备灵敏度特性模型根据设备最小信噪比要求、噪声系数和带宽分析设备灵敏度。此外，还需建立不同类型天线辐射特性模型，实现不同类型天线辐射方向图。

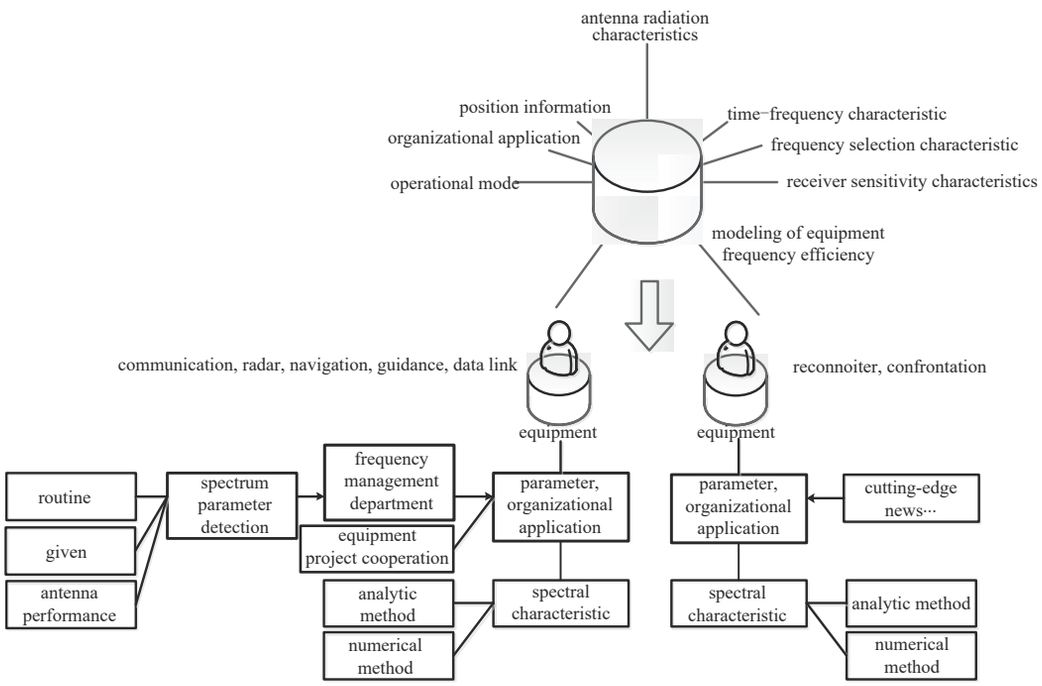

Fig.2 Modeling approach for electromagnetic characteristics of friendly and hostile frequency–dependent equipments

图2 敌我用频装备电磁特性建模思路

2.2 电波传播环境分析

电波环境与传播预测技术是研究装备电磁频谱参数泄露分析的技术基础，电磁信号的发送、传播、接收均依赖电波环境实现，复杂的电波传播环境特性将直接影响装备被侦测感知的概率。本文针对地面固定雷达和通信电台电磁频谱泄露风险进行评估，选取典型的超短波、微波波段地空链路传播模型。典型的超短波、微波波段无线电波在空间传播时会遭受许多外界因素的影响，如：地形、建筑物、植被对电波的阻挡和遮蔽，大气气体对电波能量的吸收，降雨对电波的散射等，使超短波和微波波段无线电波传播存在多种传播机理。对于传播机理的选择，具体流程图如图3所示。

考虑通信链路地理位置及电波传播环境条件，对于一个典型超短波微波地空链路，主要通过视距模型、双径模型、峰刃绕射3种近似模型确定其近传播损耗。

对于定向传输信号的截获，采用视距传播模型，收发2个增益天线之间的典型链路损耗为：

$$L = 32.44 + 20\log R + 20\log f + A_{\mathrm{g}} \tag{1}$$

式中：R为传播距离；f为信号发射频率；A_{g}为大气吸收衰减。

对于非定向传输信号，根据菲涅尔距离，可采用视距或双径传播模型。当链路距离大于菲涅尔距离，采用双径传播模型。该模型主要来自直达波和地面/水面的反射波的相位对消，链路损耗取决于链路距离和收发天线相对水面/地面的高度，链路损耗为：

$$L = 120.4 + 40\log R - 20\log H_{\mathrm{t}} - 20\log H_{\mathrm{r}} \tag{2}$$

式中：H_{t}为发射天线高度；H_{r}为接收天线高度。

当链路中出现遮挡物，计算非视距传播损耗时，可在计算出对应的视距传播损耗基础上，加上峰刃绕射衰减因子。

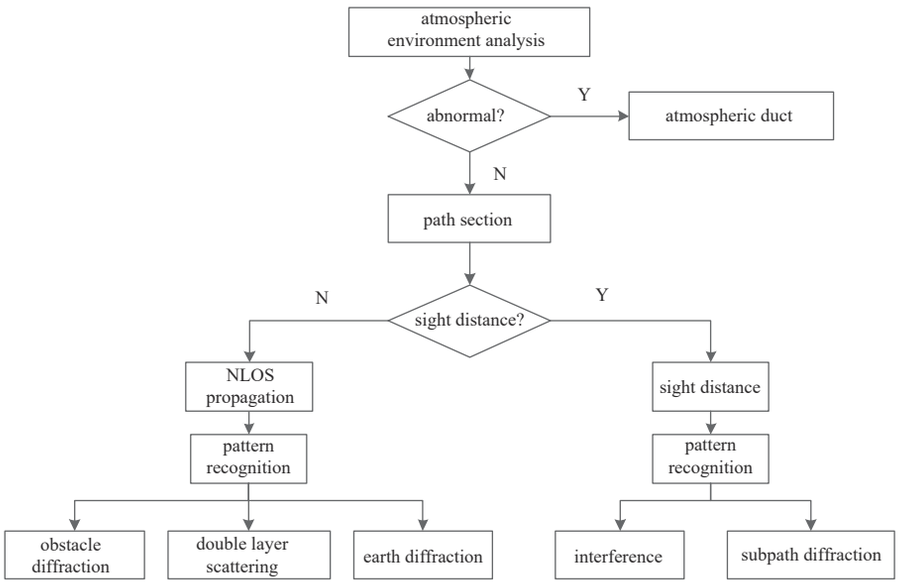

Fig.3 Analysis of radio wave propagation environment
图3 电波传播环境分析

2.3 用频装备电磁频谱参数泄露风险评估

从能量角度出发，考虑接收功率与敌侦收设备灵敏度的相互关系，采用网格剖分思想，对我方用频装备电磁参数泄露概率进行计算。

假设装备发射天线方位角为 θ_1，俯仰角为 θ_2，敌侦收装备与我军装备距离为 D，如图 4 所示。利用网格剖分思想，将我军重点关注区域按照天线方位角度 θ_1 每隔 ϑ_1 等分为 n_1 份，俯仰角 θ_2 每隔 ϑ_2 等分为 n_2 份，区域宽度 l 每隔 1 km(l 为一固定值，并不随敌我距离的改变而改变)等分为 m 份。

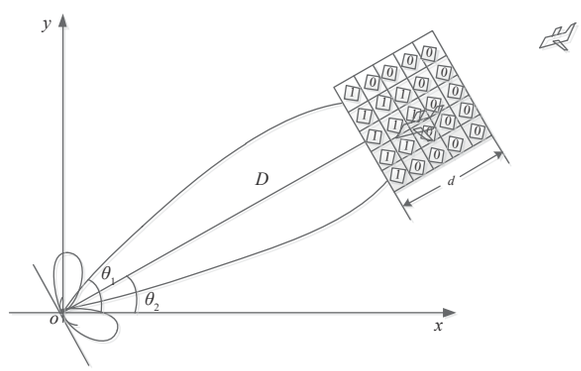

Fig.4 Leakage probability analysis of electromagnetic spectrum parameters with grid subdivision
图4 网格剖分电磁频谱参数泄露概率分析

我军装备发射功率 P_T 经过传播环境之后，由侦收设备截获的功率大小为 P_R，针对单向链路：

$$P_R = P_T + G_T - L + G_R \tag{3}$$

式中：G_T 为发射天线增益(在接收方向上)；G_R 为接收天线增益(在发射方向上)。

为确定信号是否成功被截获，需要利用侦收设备的接收机灵敏度。假设敌侦收设备的接收机灵敏度为 S，当接收到的信号功率 P_R 大于 S 时，则存在信号泄露的可能。

$$S = P_0 + N_0 + R_{SN} \tag{4}$$

$$P_0 = -114 + 10\log(B/1) \tag{5}$$

式中：$P_0=kTB$ 为带宽范围内的热噪声功率，k 为玻尔兹曼常数，T 为电阻的热力学温度，B 为信号带宽；N_0 为接收机噪声系数；R_{SN} 为检测前最小信噪比。

当 P_R 大于 S 时，将网格中该点值置为 1，否则置为 0，我军装备泄露概率为：

$$\eta = \frac{A}{n_1 \times n_2 \times m} \times 100\% \tag{6}$$

式中：A 为满足 P_R 大于 S 的点个数；$n_1 \times n_2 \times m$ 为划分网格的数量。

3　仿真结果计算

根据以上理论，进行参数设置。我军用频装备为地面固定雷达 L1 和 1 000 跳发射电台 M1，其中地面固定雷

达L1的发射功率为2 000 W，增益为28 dBi，频率为9 370 MHz；方位角以正北为基准，起始值为0°，终止值为360°；俯仰角以水平为基准，起始值为−1°，终止值为10°。1 000跳发射电台M1的发射功率为1 000 W，增益为8 dBi，频率为312.5 MHz；方位角以正北为基准，起始值为0°，终止值为360°；俯仰角以水平为基准，起始值为−1°，终止值为10°。敌电子侦察装备为EP−3，EP−3设备包括AN/ALR−60型通信侦察分析系统、AN/ALQ−76机鼻电子干扰吊舱、AN/ALQ型自动电子支援系统、AN/ALQ−108型敌我识别干扰器、AN/ALQ−132型红外干扰系统、MRD−7便携式侦察设备等。其中MRD−7便携式侦察设备的灵敏度为−107 dBm。

分别仿真地面固定雷达L1和1 000跳电台M1传播损耗随距离的变化，结果如图5~图6所示。图5为雷达L1的传播损耗随距离的变化，从图中可以看出，随着传播距离的增大，剩余功率越来越小。传播距离为379 km时，雷达L1发射功率经过环境传播衰减后的功率恰好为107 dBm，达到MRD−7便携式侦察设备的灵敏度，即地面固定雷达L1的安全距离为379 km。即379 km以内，电磁泄露概率为100%；379 km以外，电磁泄露概率为0。

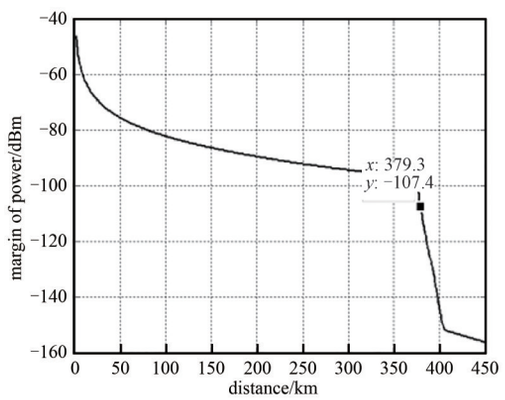

Fig.5 Variation of radar L1 propagation loss with distance
图5雷达L1传播损耗随距离的变化

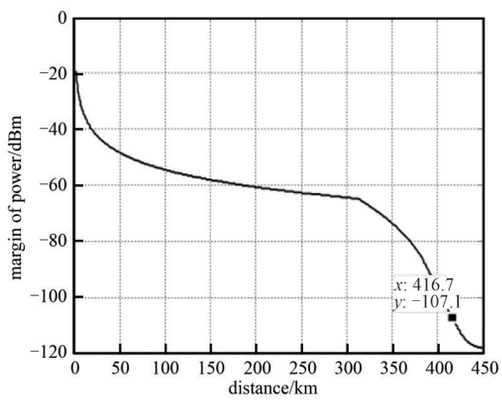

Fig.6 Variation of M1 transmission loss with distance for 1 000−hop radio
图6 1 000跳电台M1传播损耗随距离的变化

图6为1 000跳电台M1的传播损耗随距离的变化，从图中可以看出，随着传播距离的增大，剩余功率越来越小。当传播距离为416 km时，1 000跳发射电台M1的发射功率经过环境传播衰减后的功率恰好为107 dBm，达到MRD−7便携式侦察设备的灵敏度。即1 000跳发射电台M1的安全距离为416 km，416 km以内，电磁泄露概率为100%；416 km以外，电磁泄露概率为0。

根据以上仿真结果，利用电磁参数泄露理论，计算出300~450 km、350~450 km范围内，地面固定雷达L1和1 000跳发射电台M1的泄露概率，结果如表1~2所示。

表1 300~450 km范围内的泄露概率

Table1 Leakage probability within 300~450 km

parameter	ground fixed radar L1	1 000−hop transmitter M1
azimuth angle of transmitting antenna/(°)	360	360
azimuth bisection	360	360
elevation angle of transmitting antenna/(°)	11	11
elevation bisection	11	11
scope of attention/km	300~450	300~450
distance bisection/m	150	150
number of grids	594 000	594 000
number meeting	312 840	459 162
leakage probability/%	52.7	77.3

从表1和表2中可以看出，在同一区域内，相同的侦察装备、不同的发射装备，传播的距离越远，泄露概率越大。对比表1和表2可知，相同的发射装备、相同的侦察装备，关注区域的起始点越靠近侦察装备，泄露概率越大。

4 结论

本文基于敌我用频装备效能建模、电波传播环境分析和用频装备电磁频谱参数泄露风险评估理论，从能量角度出发，利用网格剖分思想，提出了一种用频装备电磁频谱参数泄露风险评估的方法。通过理论和仿真验证，

能准确评估出不同用频装备在不同距离处的电磁频谱参数泄露概率。该方法为作战人员提供了精确的参考标准，为开展核心要害区域电磁环境的管控与安全防护等工作提供技术支撑。

表2 350~450 km范围内的泄露概率

Table2 Leakage probability within 350~450 km

parameter	ground fixed radar L1	1 000-hop transmitter M1
azimuth angle of transmitting antenna/(°)	360	360
azimuth bisection	360	360
elevation angle of transmitting antenna/(°)	11	11
elevation bisection	11	11
scope of attention/km	350~450	350~450
distance bisection/m	100	100
number of grids	396 000	396 000
number meeting	114 840	216 360
leakage probability/%	29	66

参考文献：

[1] 王利涛,郁滨. 信息技术设备电磁泄漏建模与防护[J]. 计算机工程与设计, 2013,34(1):49-54. (WANG Litao, YU Bin. Modeling and security protection on electromagnetic compromising emanations of information technology equipment[J]. Computer Engineering and Design, 2013,34(1):49-54.) doi:10.3969/j.issn.1000-7024.2013.01.010.

[2] 张余,陈勇,柳永祥,等. 用频装备电磁频谱参数泄露机理及防护方法[J]. 太赫兹科学与电子信息学报, 2018,16(6):1066-1071, 1079. (ZHANG Yu, CHEN Yong, LIU Yongxiang, et al. Research on the electromagnetic spectrum parameters leaking mechanism and defense approach for the spectrum-dependent equipment[J]. Journal of Terahertz Science and Electronic Information Technology, 2018,16(6):1066-1071,1079.) doi:10.11805/TKYDA201806.1066.

[3] 姚富强,张余,柳永祥. 电磁频谱安全与控制[J]. 指挥与控制学报, 2015,1(3):278-283. (YAO Fuqiang,ZHANG Yu,LIU Yongxiang. Security and control of the electromagnetic spectrum[J]. Journal of Command and Control, 2015,1(3):278-283.) doi: JCC.CN.2015.00278.

[4] 吴昊,柳永祥,赵杭生. 用频装备电磁频谱参数安全风险若干问题探讨[J]. 现代军事通信, 2012,20(1):54-58. (WU Hao,LIU Yongxiang,ZHAO Hangsheng. Research on some problem of the electromagnetic spectrum parameters security for spectrum-dependent equipment[J]. Journal of Modern Military Communications, 2012,20(1):54-58.)

[5] 唐朝京,刘培国. 电磁频谱安全问题探讨[J]. 国防科技, 2011, 32(4): 18-20, 69. (TANG Chaojing, LIU Peiguo. On electromagnetic spectrum security[J]. Defence Technology, 2011,32(4):18-20,69.) doi:10.3969/j.issn.1671-4547 2011.04.002.

[6] 张余,李连宝,柳永祥,等. 一种基于视意图式的用频系统电磁频谱参数泄露检测与识别方法[J]. 通信对抗, 2015,34(1):11-14. (ZHANG Yu,LI Lianbao,LIU Yongxiang,et al. An electromagnetic spectrum parameters leaking detection and identification approach for spectrum-dependent systems based on view and sense marking schema[J]. Communications Counter-Measures, 2015,34(1):11-14.)

[7] 徐平,万海军,张勇,等. 舰船信息技术设备电磁泄露研究[J]. 微波学报, 2012,28(S3):390-392. (XU Ping,WAN Haijun,ZHANG Yong, et al. Research on electromagnetic information leakage in information technology equipment of navalship[J]. Journal of Microwaves, 2012,28(S3):390-392.) doi:10.14183/j.cnki.1005-6122.2012.(s3.063.)

作者简介：

颜　军(1973-)，男，硕士，高级工程师，主要研究方向为电磁频谱管理、复杂电磁环境效应建模等.email: joyjiang2002@sina.com.

刘　青(1989-)，女，硕士，工程师，主要研究方向为电磁频谱管理、电磁频谱资源筹划与调度等.

张江明(1991-)，男，硕士，工程师，主要研究方向为电磁频谱管理、电磁干扰计算等.