

基于功率谱熵的隐蔽通信信号检测技术研究

洪泽坤^{1,2}, 徐艳云^{1,2}, 黄伟庆^{1,2}, 李婷婷^{1,2}, 于超^{1,2}

¹中国科学院信息工程研究所 北京 中国 100093

²中国科学院大学网络空间安全学院 北京 中国 100049

摘要 作为国家的战略资源,对电磁频谱进行有效的监测是保障电磁空间安全的重要环节。在复杂电磁环境下,低功率隐蔽通信信号的检测率低,存在潜在的电磁空间安全风险。针对这一问题,本文提出了一种基于频域功率谱熵的双门限隐蔽通信信号检测算法。在信息熵检测模型的理论基础上,该算法利用信号功率谱的信息熵作为检验统计量,针对传统单一门限检测方法在低信噪比下性能下降这一问题,设计了改进后的双判决门限,实现了在强干扰和低信噪比下对隐蔽的低功率微弱信号的盲检测。仿真和实测结果表明,在接收信噪比 SNR=-10dB 时,信号的检测率大于 90%,优于其他传统算法,显著提升了隐蔽通信信号的检测率,同时该算法也具有抗噪声不确定性的鲁棒性。针对复杂电磁环境下的非合作频谱检测场景,基于该算法,本文提出了基于频谱迹线的分阶段功率谱熵检测方法,实现对大带宽内隐蔽通信信号个数和占用频段的估计。利用矢量信号源和 USRP 软件无线电平台产生若干不同调制类型的宽带信号和窄带信号,作为信息传输的隐蔽通信信号,以模拟实际环境下的宽带频谱感知场景。实测实验结果表明,该方法能在宽带范围内准确估计信号个数和占用频段,在 SNR=-5dB 时,准确率大于 80%。

关键词 电磁空间安全;微弱信号检测;隐蔽通信;信息熵;频谱感知;频谱监测

中图分类号 TN911.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2026.05.18

Research on Covert Communication Signal Detection Technology Based on Power Spectrum Entropy

HONG Zekun^{1,2}, XU Yanyun^{1,2}, HUANG Weiqing^{1,2}, LI Tingting^{1,2}, YU Chao^{1,2}

¹ Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

² School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract As a strategic resource of the country, effective monitoring of the electromagnetic spectrum is an important part of ensuring the security of electromagnetic space. In a complex electromagnetic environment, the detection rate of covert communication signals is low, which creates potential electromagnetic space security risks. Aiming at this problem, this paper proposes a double-threshold covert communication signal detection algorithm based on frequency domain power spectrum information entropy. Based on the theoretical derivation of the information entropy detection model, this algorithm uses the information entropy of the signal power spectrum as the test statistic. In order to solve the problem of the performance degradation of the traditional single-threshold detection method, an improved dual-decision threshold is designed to achieve blind detection of hidden low-power weak signals under the background of strong interference and low signal-to-noise ratio. The simulation and experimental results show that the detection rate is greater than 90% when SNR=-10dB, which is superior to other traditional algorithms, and greatly improves the detection rate of low-power covert signals. At the same time, the algorithm also has robustness to noise uncertainty. Based on this algorithm, for non-cooperative spectrum detection scenarios in complex electromagnetic environments, this paper proposes a phased frequency domain information entropy detection method based on spectrum traces to realize the estimation of the number of covert communication signals and occupied frequency bands in a large bandwidth. The vector signal source and the USRP software radio platform are used to generate several wideband signals and narrowband signals of different modulation types, which are used as covert communication signals for information transmission to simulate the wideband spectrum sensing scenario in the actual environment. Actual experimental results show that this method can accurately estimate the number of signals and occupied frequency bands within a wideband range. When SNR=-5dB, the detection accuracy is greater than 80%.

Key words electromagnetic space security; weak signal detection; covert communication; information entropy; spectrum sensing; spectrum monitoring

通讯作者: 徐艳云, 博士, 高级工程师, Email: xuyanyun@iie.ac.cn。

本课题得到中国科学院战略性先导科技专项(No. XDC02040300)资助。

收稿日期: 2021-03-15; 修改日期: 2021-04-23; 定稿日期: 2023-08-29

1 引言

电磁频谱是国家有效的战略资源,对电磁频谱进行有效的监测是保障电磁空间安全的重要一环。在实际的监测环境中,受信道衰弱、电磁干扰、接收系统多样性等因素的影响,某些信号容易淹没在背景噪声中,在非合作的频谱检测环境中,往往难以判断其存在。尤其是以扩频通信、超宽带通信、跳频通信等为代表的低检测概率(隐蔽)通信方式,功率谱密度低,作为电磁频谱的监测方,在缺乏先验信息的低信噪比条件下,往往难以感知其正在进行的隐蔽信息传输,是电磁空间安全监管的重要威胁。

隐蔽通信技术基于信号检测理论,利用一定的策略或系统参数优化来降低通信双方被第三方监听者检测到的概率,进而构建一定的隐蔽通信网络。在非合作的第三方频谱监测中,使用最多的方法就是能量检测法^[1],该方法计算简单,无须任何先验信息,属于信号的非相干检测,但在低信噪比和存在噪声不确定度的情况下,该算法性能损失严重。匹配滤波器^[2]利用了输出信噪比最大时的最佳线性滤波器进行检测,在信噪比达到一定门限时,能取得较好的处理增益。但是该方法通常需要先验信息,在非合作环境下难以使用。循环平稳检测^[3]利用了通信信号在调制后表现的循环平稳特性,该方法抗噪声不确定度的鲁棒性好,但是计算量大,需要较长的观察时间。此外,对于低信噪比下频谱检测(感知)问题,结合机器学习^[4]、小波变换^[5]、随机共振^[6]、经验模态分解^[7]等理论的方法也各有优劣。

为了更有效地对电磁频谱进行安全监管,针对现实中可能的隐蔽通信信号往往淹没在噪声中,难以有效检测的问题,本文提出了一种改进的基于频域功率谱信息熵的双门限低信噪比微弱信号检测算法。其基本思想是,通过计算接收信号的功率谱信息熵,利用与噪声熵的差异作为检验统计量,构造相应的检测门限,进行信号存在性判决。仿真和实验结果表明,该算法在低信噪比下具有较好的检测性能。最后,在此算法的基础上,设计了一种基于频谱迹线的分阶段频谱检测方法,实现在大带宽范围内,对低功率隐蔽信号个数和占用频段的准确感知。

本文的主要贡献如下:

(1) 提出了一种基于功率谱信息熵的双门限低信噪比微弱信号检测算法,对算法的模型和相关参数进行了理论推导,并进行了数值仿真和实测实验。结果表明,该算法在低信噪比下,对隐蔽通信信号的检测性能优于其他传统算法,且算法复杂度低,

抗噪声不确定度的鲁棒性较好。

(2) 设计了一种基于频谱迹线的分阶段宽带频谱检测方法,用于对大带宽范围内低功率、低信噪比隐蔽通信信号个数和占用频段的估计,实测实验表明,该方法可实现宽带范围内隐蔽通信信号个数和频段的有效估计,更好地感知电磁空间安全风险。

本文的章节安排为:第2节介绍算法的理论模型和时频域信息熵的相关概念,第3节介绍基于功率谱信息熵的改进双门限检测算法,第4节基于功率谱熵检测算法,介绍基于频谱迹线的分阶段宽带频谱感知方法,第5节是仿真和实测实验,以及结果分析,第6节为全文总结。

2 相关背景

2.1 系统模型

对于一个待检频段,当存在信号占用时,在接收机端,一般的离散时间信号模型可表示为

$$x(n) = s(n) + w(n), n = 0, 1, \dots, N-1 \quad (1)$$

其中, $x(n)$ 为接收信号; $s(n)$ 为待测信号,对于随机信号,可假设其服从均值为 μ_1 , 方差为 σ_s^2 的高斯分布; $w(n)$ 表示背景噪声,服从均值为 0, 方差为 σ_0^2 的高斯分布, N 为样本大小, $s(n)$ 和 $w(n)$ 相互独立。

对于频谱检测(感知),可表述为以下二元假设模型:

$$\begin{cases} H_0 : x(n) = w(n), & n = 0, 1, \dots, N-1 \\ H_1 : x(n) = s(n) + w(n), & n = 0, 1, \dots, N-1 \end{cases} \quad (2)$$

式中, H_0 、 H_1 分别表示不存在和存在信号占用,接收信号 $x(n)$ 服从以下的高斯分布:

$$\begin{cases} H_0 : x(n) \sim N(0, \sigma_0^2) \\ H_1 : x(n) \sim N(\mu_1, \sigma_0^2 + \sigma_s^2) \end{cases} \quad (3)$$

2.2 基于信息熵的检测方法

2.2.1 基本概念

在信息论中,熵用来衡量一串离散随机变量的不确定性。该术语通常指香农(信息)熵,以量化包含在消息中的信息^[8],表示为

$$H(Y) = -\sum_{i=1}^L p_i \log_b p_i \quad (4)$$

式中, p_i 表示随机变量 Y 的概率质量函数, L 表示概率空间的维数, b 表示对数的底数,通常取 2 或 e 。

差分熵(连续熵)是香农熵定义的扩展。在实际应用中,常利用其与香农熵的关系计算香农熵。对于一

个连续随机变量, 其差分熵^[9]定义为

$$b(y) = -\int f(y) \log_{\alpha} f(y) \quad (5)$$

式中, $f(y)$ 表示随机变量 y 的概率密度函数(PDF), α 为对数底数。不失一般性, 假设将 y 均分为长度 Δ 的区间, 若概率密度函数 $f(y)$ 满足黎曼可积条件, 则差分熵和香农熵将建立如下的关系^[10]:

$$b(y) \approx H(y^{\Delta}) + \log_{\alpha} \Delta \quad (6)$$

当 $\Delta \rightarrow 0$, 差分熵可以近似为上述香农熵加上区间长度 Δ 对数的形式。

在基于差分熵的随机信号检测过程中^[11], 由 m 阶 AR 过程构建的检验统计量 $T(x)$ 表示为

$$T(x) = N \ln \left[\prod_{i=1}^m \left(\frac{\sigma_0^2}{\sigma_i^2} \right)^{\beta_i} \right] \quad (7)$$

式中, m 表示 AR 过程的阶数, β_i 表示 AR 过程第 i 阶的概率, σ_i^2 表示第 i 阶线性预测误差的方差, σ_0^2 表示加性高斯白噪声的方差, N 是样本大小。从式(7)可见, 检验统计量是一个关于噪声功率的单调递增函数, 与噪声相关, 会受到噪声不确定度较大的影响。与差分熵相比, 基于频域信息熵构造的检验统计量更好地反映了信号的复杂程度和非线性特征, 是一种盲检测方法。后续小节将对此作详细的理论推导和证明。

2.2.2 基于时域熵的检测算子

令 σ_x^2 表示为接收信号 $x(n)$ 的方差, 则接收信号的差分熵^[12]可表示为

$$b(X) = \ln(\sqrt{\sigma_x^2 2\pi\gamma}) = \frac{1}{2} \ln 2\pi\gamma\sigma_x^2 \quad (8)$$

则由式(6), 当 $\Delta \rightarrow 0$ 时, 时域的香农熵 $H(X)$ 可由差分熵 $b(X)$ 近似表示为

$$H(X) \approx b(X) - \log_{\alpha} \Delta = \frac{1}{2} \ln 2\pi\gamma\sigma_x^2 - \ln \Delta \quad (9)$$

式中, 底数取 $\alpha = e$, γ 表示欧拉常数。

对每一个随机变量 X_m , 其累计分布函数(CDF)表示为 $\rho = P(X < X_m)$, 则可得到:

$$Q(X_m - \mu_x) / \sigma_x = 1 - \rho \quad (10)$$

式中, μ_x 为接收信号均值, $Q(x)$ 是标准正态分布的尾函数, 表示为

$$Q(x) = \int_x^{\infty} (1/\sqrt{2\pi}) \exp((-1/2)t^2) dt \quad (11)$$

则由式(10), 随机变量 X_m 可表示为

$$X_m = \mu_x + \sigma_x Q^{-1}(1 - \rho) \quad (12)$$

设 L 为所划分的概率空间维数(区间数), 则可得区间宽度为

$$\Delta = X_m / L = (\mu_x + \sigma_x Q^{-1}(1 - \rho)) / L \quad (13)$$

将式(13)代入式(9), 可得时域香农熵表达式为

$$\begin{aligned} H(X) &\approx \frac{1}{2} \ln 2\pi\gamma\sigma_x^2 - \ln \frac{\mu_x + \sigma_x Q^{-1}(1 - \rho)}{L} \\ &= \ln \frac{\sigma_x L \sqrt{2\pi\gamma}}{\mu_x + \sigma_x Q^{-1}(1 - \rho)} \end{aligned} \quad (14)$$

为简化分析, 假设信号均值 $\mu_x = 0$, 则时域熵的表达式简化为

$$H(X) \approx \ln(L\sqrt{2\pi\gamma}) / (Q^{-1}(1 - \rho)) \quad (15)$$

从上式可见, 二元假设下, 在给定概率空间维数 L 和置信水平的条件下, 时域的香农熵是一个常数。图 1 为在不同信噪比下, 基于信号二元假设所得的时域熵数值仿真。参数设置为: 实验信号二进制相移键控(BPSK), 样本点数目 $N = 6000$, 概率空间维数为 $L = 15$, 基于式(14)计算时域信息熵, 每个实验结果进行 2000 次蒙特卡罗模拟。

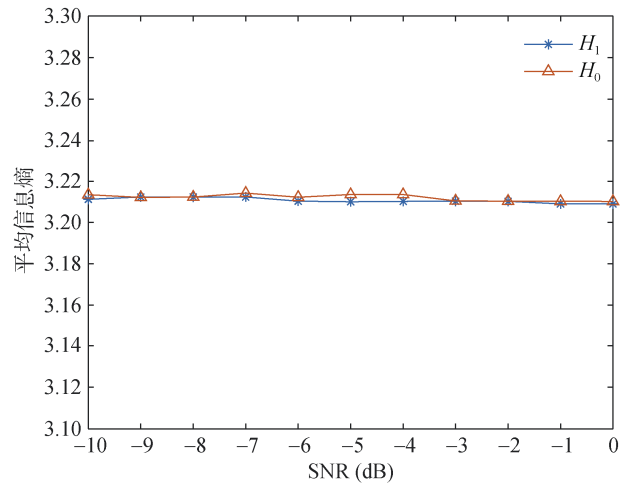


图 1 不同信噪比下的时域熵数值比较

Figure 1 Comparison of time-domain entropy value under different signal-to-noise ratios

由图 1 的结果可见, H_0 和 H_1 假设下的熵值存在重叠, 不同信噪比下, H_1 假设下含噪信号的熵值近似为一个常数。可见, 基于所估计的时域信息熵难以将噪声与信号区分, 因此不适用于检测。为此, 本文从频域信息熵角度, 比较噪声和信号复杂程度差异, 构建相应的检验统计量, 实现低信噪比下的信号检测。

2.2.3 基于频域熵的检测算子

本文利用接收信号功率谱计算频域信息熵, 构造检验统计量和判决门限, 用于对淹没在噪声下的隐蔽

通信信号的盲检测。本节首先介绍功率谱信息熵的计算方法, 然后证明其对噪声不确定度的鲁棒性。

(1) 功率谱信息熵

对式(2)进行离散傅里叶变换(DFT), 可得

$$\begin{cases} H_0: \bar{X}(k) = \bar{W}(k), & k = 0, 1, \dots, K-1 \\ H_1: \bar{X}(k) = \bar{S}(k) + \bar{W}(k) & k = 0, 1, \dots, K-1 \end{cases} \quad (16)$$

式中, K 为信号 DFT 长度, $\bar{X}(k)$, $\bar{S}(k)$ 和 $\bar{W}(k)$ 分别表示接收信号, 待测信号和噪声的复频谱。

接收信号的傅里叶变换, 可表示为

$$\begin{aligned} \bar{X}(k) &= X_r(k) + jX_i(k) \\ &= \frac{1}{N} \sum_{n=0}^{N-1} x(n) \exp\left(-j\frac{2\pi}{N}kn\right) \end{aligned} \quad (17)$$

式中, $X_r(k)$ 和 $X_i(k)$ 分别为 $\bar{X}(k)$ 的实部和虚部, 本文利用接收信号的功率谱计算信息熵, 基于直方图法^[13]构造的检验统计量表示为

$$H(X^2) = -\sum_{i=1}^L \frac{k_i}{N} \log \frac{k_i}{N} \quad (18)$$

式中, $H(X^2)$ 表示为接收信号功率谱的信息熵, N 为功率谱点数, L 为概率空间维数(分段数), k_i 表示第 i 个区间的频数, 对应第 i 个区间的概率为 $p_i = k_i / N$, 则区间宽度表示为

$$\Delta = \frac{X_{\max} - X_{\min}}{L} \quad (19)$$

式中, $X_{\max}$ 和 $X_{\min}$ 分别为接收信号功率谱的最大值与最小值。

图 2 为不同信噪比下, 基于二元假设所得的功率谱信息熵数值仿真。参数设置为: 实验信号直接序列扩频二进制相移键控(DS-BPSK), 样本点数 $N = 6000$, 概率空间维数 $L = 15$, 基于式(18)计算频域信息熵, 每个实验结果进行 2000 次蒙特卡罗模拟。由图 2 的结果可见, H_0 假设下高斯白噪声的功率谱熵数值近似为一个常数, 与 H_1 假设下信号的功率谱熵存在明显差异。由此, 可构造相应的判决门限, 区分信号和噪声。

(2) 抗噪声不确定度的鲁棒性

首先在 H_0 假设下, 证明功率谱信息熵的估计方法对噪声不确定度的鲁棒性问题。对于 H_0 假设下的接收信号, 可表示为均值为 0, 方差为 σ_0^2 的高斯白噪声, 其离散傅里叶变换表示为

$$\begin{aligned} \bar{W}(k) &= W_r(k) + jW_i(k) \\ &= \frac{1}{N} \sum_{n=0}^{N-1} w(n) \exp\left(-j\frac{2\pi}{N}kn\right) \end{aligned} \quad (20)$$

上式中复频谱 $\bar{W}(k)$ 的实部和虚部都满足方差为 $\sigma_0^2 / 2N$ 的高斯分布, 其功率谱密度可表示为

$$W^2(k) = W_r^2(k) + W_i^2(k) \quad (21)$$

上式满足方差为 $\sigma_1^2 = \sigma_0^2 / 2N$ 的指数分布。记 $Y(k) = W^2(k)$, 则其概率密度函数(PDF)、累计分布函数(CDF)和差分熵可分别表示为^[14]

$$f(Y) = \begin{cases} \frac{1}{2\sigma_1^2} e^{-\frac{Y}{2\sigma_1^2}}, & Y \geq 0 \\ 0, & Y < 0 \end{cases} \quad (22)$$

$$F(Y) = \begin{cases} 1 - e^{-\frac{Y}{2\sigma_1^2}}, & Y \geq 0 \\ 0, & Y < 0 \end{cases} \quad (23)$$

$$\begin{aligned} h(Y) &= -\int_{-\infty}^{+\infty} f(Y) \log_{\alpha}(f(Y)) dY \\ &= 1 + \log_{\alpha}(2\sigma_1^2) \end{aligned} \quad (24)$$

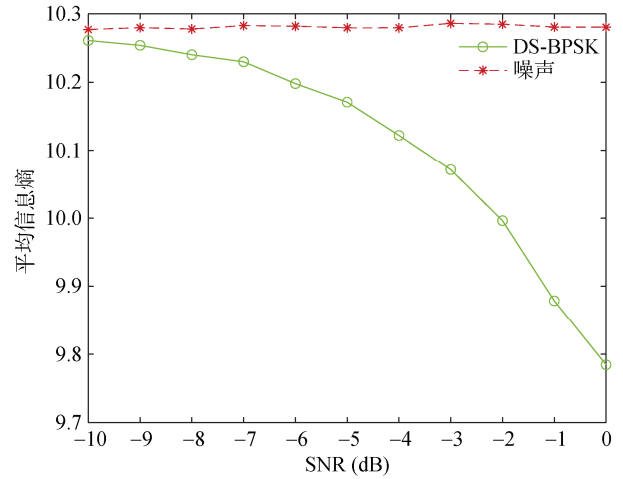


图 2 不同信噪比下, 信号和噪声的功率谱熵数值比较
Figure 2 Comparison of the power spectrum entropy value of signal and noise under different SNR

接收信号的功率谱信息熵, 可由式(18), 基于直方图法计算得出。当固定区间宽度 Δ 时, 概率空间维数 L 会随噪声功率而变化; 当固定概率空间维数 L 时, 区间宽度 Δ 会随功率谱幅度而变化。本文利用固定概率空间维数的方法计算信息熵, 并证明其对噪声不确定度的鲁棒性。

推论: 概率空间维数 L 一定时, 高斯白噪声的频域功率谱信息熵是常数, 因此具有抗噪声不确定度的内在鲁棒性。

证明: 对于一系列的随机变量样本 Y ($Y(k) = W^2(k)$), 假设范围在 $[0, Y_{\max}]$, 当累计分布函数

(CDF) 概率 $\rho \rightarrow 1$ (e.g., $0.99 < \rho < 1$) 时, 根据式(23), $Y_{\max}$ 可表示为

$$Y_{\max} = -2\sigma_1^2 \ln(1 - \rho) = C\sigma_1^2 \quad (25)$$

其中 $C = -2\ln(1 - \rho)$, 在给定累积分布函数概率 ρ 的条件下为常数, 则在概率空间维数 L 一定时, 间隔宽度 Δ 可表示为

$$\Delta = \frac{Y_{\max}}{L} = \frac{C\sigma_1^2}{L} \quad (26)$$

根据均值定理, 在每个间隔宽度 Δ 内, 总存在某个值 Y_i , 使得在每个分段区间的概率 p_i 可被表示为

$$p_i = \int_{i\Delta}^{(i+1)\Delta} f(Y) dY = f(Y_i) \Delta \quad (27)$$

结合式(24)、式(26), 则频域功率谱的信息熵可被量化为(底数取 $\alpha = e$):

$$\begin{aligned} H_L(Y) &\approx -\sum_{i=1}^L p_i \log_{\alpha} p_i \\ &= -\sum_{i=1}^L f(Y_i) \Delta \log_{\alpha} (f(Y_i) \Delta) \\ &= -\sum_{i=1}^L f(Y_i) \Delta \ln(f(Y_i)) - \ln \Delta \\ &= h(Y) - \ln \Delta \\ &= 1 + \ln(2\sigma_1^2) - \ln \frac{C\sigma_1^2}{L} \\ &= 1 + \ln\left(\frac{2L}{C}\right) \end{aligned} \quad (28)$$

由上式可知, 在给定概率空间维数 L 的条件下, 高斯白噪声的功率谱信息熵近似为一个常数, 与噪声的方差无关, 因此对噪声不确定度具有鲁棒性。

3 基于功率谱熵的双门限检测算法

当信噪比降低时, 基于 H_0 和 H_1 假设下的功率谱熵差异减小, 传统的构造单一门限的检测方法性能下降。为提高基于功率谱熵算法在低信噪比下的检测性能, 提出了一种改进的双门限功率谱熵检测算法。

算法流程如图 3 所示, 首先对接收信号进行功率谱估计, 计算功率谱信息熵作为检验统计量, 与设定的两个高低门限值 λ_H , λ_L 进行比较, 当落在 $(\lambda_L - \varepsilon, \lambda_H + \varepsilon)$ 判决区间内时, 进入二次判决, 继续取样本点, 计算功率谱熵的均值, 与二次判决门限进行比较, 得出检测结果。

3.1 功率谱估计

在基于功率谱熵的检测中, 对接收信号良好的功率谱估计是影响算法检测性能的重要因素。本文利用改进周期图的 Welch 法进行谱估计^[15], 有效降

低方差和偏差, 更接近于真实的功率谱。

计算流程如图 4 所示, 其详细步骤如下。

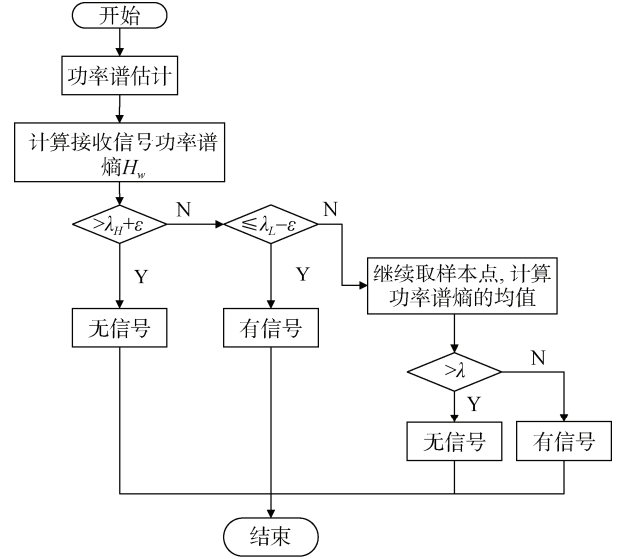


图 3 双门限功率谱熵算法流程图

Figure 3 Flow chart of double-threshold power spectrum entropy algorithm

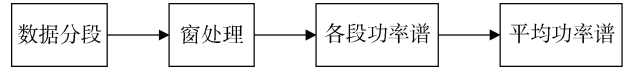


图 4 Welch 谱估计法流程图

Figure 4 Flow chart of Welch method

(1) 对于接收信号 $x(n)$, 将其分成 L 段, 每段有 M 个数据点, 则第 i 段数据表示为

$$x_i(n) = x(n + iM - M), 0 \leq n \leq M, 1 \leq i \leq L \quad (29)$$

(2) 把窗函数 $w(n)$ 加到每个数据段上, 求出每一段的周期图, 第 i 段的周期图表示为

$$I_i(k) = \frac{1}{U} \left| \sum_{n=0}^{M-1} x_i(n) w(n) e^{-jkn} \right|^2, i = 1, 2, \dots, M-1 \quad (30)$$

上式中的 U 作为归一化因子, 表示为

$$U = \frac{1}{M} \sum_{n=0}^{M-1} w^2(n) \quad (31)$$

(3) 对于每一段周期图, 相互间互不相干, 则最后的功率谱可表示为

$$S(k) = \frac{1}{L} \sum_{i=1}^L I_i(k) \quad (32)$$

文献[16]证明, 当分段数 L 和分段数据点数 M 相等或近似相等时, 基于频域熵的检测性能最佳。

3.2 检验统计量

由式(32), 对谱估计后的接收信号功率谱 $S(k)$, $k = 0, 1, 2, \dots, N-1$, 进行归一化处理, 计算功率谱熵, 表示为

$$p(k) = S(k) / \sum_{k=0}^{N-1} S(k) \quad (33)$$

式中, $p(k)$ 表示在总的功率谱中, 第 k 个功率谱值的占比。则接收信号功率谱熵表示为

$$H_\omega = - \sum_{k=0}^{N-1} p(k) \log_2 p(k) \quad (34)$$

式中, 概率空间维数 $L = N$, 基于功率谱熵构造的检验统计量表示为

$$T = H_w = - \sum_{k=0}^{N-1} p(k) \log_2 p(k) \begin{cases} \leq \lambda, \text{判决} H_1 \\ > \lambda, \text{判决} H_0 \end{cases} \quad (35)$$

当存在信号占用时, H_1 情况下的概率密度函数分布会比 H_0 时更密集, 由于信息熵的凸性质^[17], 此时的熵值降低。即当检验统计量小于门限值 λ 时, 判决为 H_1 , 有信号存在。

3.3 检测门限及检测概率

首先, 对该算法的检测门限进行推导。基于信号功率谱熵构造的检验统计量 T 服从如下分布:

$$T \sim \begin{cases} N(\mu_0, \sigma_0^2) & H_0 \\ N(\mu_1, \sigma_1^2) & H_1 \end{cases} \quad (36)$$

式中, H_0 假设下的功率谱熵, 为服从均值 μ_0 , 方差 σ_0^2 的高斯分布, H_1 假设下的功率谱熵, 为服从均值 μ_1 , 方差 σ_1^2 的高斯分布。采用纽曼皮尔逊(N-P)准则^[18]实现假设检验。设虚警概率 P_{fa} , 判决门限 λ 。

则虚警概率可表示为

$$\begin{aligned} P_{fa} &= P(T < \lambda | H_0) \\ &= Q\left(\frac{\lambda - \mu_0}{\sigma_0}\right) \end{aligned} \quad (37)$$

式中, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp(-\frac{t^2}{2}) dt$, 为标准正态分布的尾概率函数, 则由式(37)可得检测门限 λ :

$$\lambda = \sigma_0 Q^{-1}(P_{fa}) + \mu_0 \quad (38)$$

设理论检测概率为 P_d , 由 N-P 准则, 可得

$$\begin{aligned} P_d &= P(T < \lambda | H_1) \\ &= Q\left(\frac{\lambda - \mu_1}{\sigma_1}\right) \end{aligned} \quad (39)$$

将计算所得的门限值 λ 代入式(39), 可得给定虚警率下, 算法的理论检测概率。

3.4 检测判决方法

为进一步提高算法在低信噪比下的检测性能, 降低噪声不确定度的影响, 本文利用双门限进行检测判决。通过设置高低门限值, 划分为三个判决区

域。对双门限外的区域进行单步判决, 双门限内的区域采用两步判决, 其判决流程如下。

(1) 基于给定的虚警率, 设置高低门限值, 由式(38)计算可得

$$\begin{cases} \lambda_H = \sigma_0 Q^{-1}(P_{faH}) + \mu_0 \\ \lambda_L = \sigma_0 Q^{-1}(P_{faL}) + \mu_0 \end{cases} \quad (40)$$

式中, P_{faH} , P_{faL} 表示为设置的高低虚警率 $P_{faH} \geq (P_{faL})$ 。

(2) 引入调节系数: 当信噪比降低时, 基于 H_0 假设下的噪声功率谱熵估计会有较大偏差, 对门限值的构建造成影响。为了弥补估计的偏差, 在算法中引入一个调节系数 ε , 则对接收信号功率谱熵的检测判决表示为

$$H_\omega \begin{cases} \leq \lambda_L - \varepsilon: \text{判决} H_1 \\ > \lambda_H + \varepsilon: \text{判决} H_0 \\ \text{其他, 进行二次判决} \end{cases} \quad (41)$$

(3) 二次判决: 当功率谱熵(检验统计量)落在双门限区间内时, 进入二次判决, 继续取 m 帧的样本点, 每帧样本点计算 N 点功率谱估计, 求功率谱熵, 记为 $H_n, n=1, 2, \dots, m$ 。将每帧样本点的功率谱熵与第一步判决计算的样本点功率谱熵求和取均值, 作为检验统计量, 判决过程表示为

$$T_2 = \frac{\sum_{n=1}^m H_n + H_\omega}{m+1} \begin{cases} \leq \lambda: H_1 \\ > \lambda: H_0 \end{cases} \quad (42)$$

式中, 取虚警率 P_{faH} 计算得到的 λ 作为判决门限。当检验统计量 T_2 小于门限值时, 判决为有信号占用, 大于门限值时, 判决为无信号。

上述所提方法, 由本文 2.2.3 小节对噪声的鲁棒性证明可知, 所构建的判决门限与噪声的方差不相关, 在复杂的电磁环境下, 对噪声不确定度的鲁棒性更好, 可利用功率谱熵这一特征量, 较好地反映信号与噪声的差异。相反, 传统的能量检测法, 所构造的门限值与噪声的方差相关, 在信噪比降低, 存在噪声不确定度的情况下, 门限值不能很好确定, 大大影响了检测性能。此外, 本文方法通过设计双门限值, 考虑到了实际的隐蔽通信信号侦测过程中, 信噪比降低时, 接收信号功率谱熵值较大, 单一门限值容易造成信号漏检的情况, 所以设计了双门限和两步判决过程, 同时引入调节系数, 弥补了强噪声干扰下功率谱熵估计偏差对门限值确定的影响。若第一阶段判决中的检验统计量 H_ω 落在 $(\lambda_L - \varepsilon, \lambda_H + \varepsilon)$ 区间外, 可基于二元假设做出相应判

决。该过程基于 N 点功率谱的功率谱熵估计。如果 H_ω 在 $(\lambda_L - \varepsilon, \lambda_H + \varepsilon)$ 区间内, 则进行二次判决, 判决结果基于 $(m+1) \times N$ 个样本点功率谱, 接近于使用 $(m+1) \times N$ 点功率谱进行功率谱熵单门限检测的性能, 从而使最终判决更加可靠, 提高了在低信噪比下对隐蔽通信信号的检测率。后续的仿真与实验验证将进一步证明其有效性。

4 分阶段宽带频谱感知

在实际电磁频谱监测过程中, 分辨带宽(RBW)较小时, 采集的频谱迹线点数足够多, 可更精确地估计功率谱熵, 但对于宽带频谱检测而言, 小的分辨带宽, 频段扫描时间长, 算法检测时间长, 检测复杂度高。为了既保证算法检测率, 又提高算法的检测速度, 提升检测性能, 本文针对复杂电磁环境下的非合作频谱检测场景, 在所提出的双门限功率谱熵检测算法基础上, 设计了一种基于频谱迹线的分阶段宽带隐蔽信号频谱检测方法, 实现大带宽范围内对可能的隐蔽通信信号个数和占用频段的有效估计, 以预知可能的电磁空间安全风险。

方法所用频谱监测设备为实验室自研频谱监测系统。设备主要参数如表 1 所示。

表 1 设备主要参数

Table 1 Main parameters of the equipment

参数	数值
频率范围	9kHz~30GHz
分辨率带宽	1Hz~10MHz
实时带宽	0.1 / 10 / 80 / 160 MHz
平均噪声电平	-160~-148dBm/Hz(0.1~27GHz)
电平测量不确定度	0.4dB

4.1 基本流程

该方法的基本思想是: 将频谱检测过程分为两阶段。第一阶段为粗感知阶段, 针对大带宽频谱, 设置大分辨带宽(频谱范围 500MHz~1GHz, 通常取 500kHz~1MHz), 采集频谱迹线, 利用双门限功率谱熵算法进行检测, 判断是否有信号占用。如果有信号占用, 则进入第二阶段。

第二阶段为降低分辨带宽对信号进行重获取的细感知阶段。将第一阶段采集的频谱迹线划分为若干子带, 针对每一个子带所在的频段范围, 降低分辨带宽(频谱范围 10~20MHz, 通常取 1~30kHz), 重新采集该子带范围的频谱迹线。利用本文所提功率谱熵算法进行检测, 以确定每个子带信号的占用

情况。

本方案流程图如图 5 所示, 详细的检测步骤如下:

(1) 设置分辨带宽为 RBW_1 , 待测频段带宽表示为 B_w , 采集待测宽带的频谱迹线, 记为 $X(k), k = 0, 1, \dots, N-1$ 。

(2) 粗感知: 利用采集的迹线, 计算归一化后的信息熵作为检验统计量:

$$H_y = -\sum_{k=0}^{N-1} y(k) \log_2 y(k) \quad (43)$$

式中, $y(k) = X(k) / \sum_{k=0}^{N-1} X(k)$ 。利用本文所提功率谱熵检测算法, 对该检验统计量进行判决。若判决为信号存在, 则进入细感知阶段。

(3) 细感知: 将待测频段划分为 M 个子带, 则每个子带带宽记为

$$B_s = B_w / M \quad (44)$$

对各个子带, 设置分辨带宽为 RBW_2 , 采集待测子带的频谱迹线, 计算检验统计量, 利用双门限功率谱熵检测算法进行判决。依次对各个子带进行检测判决, 判断各子带是否有信号占用。

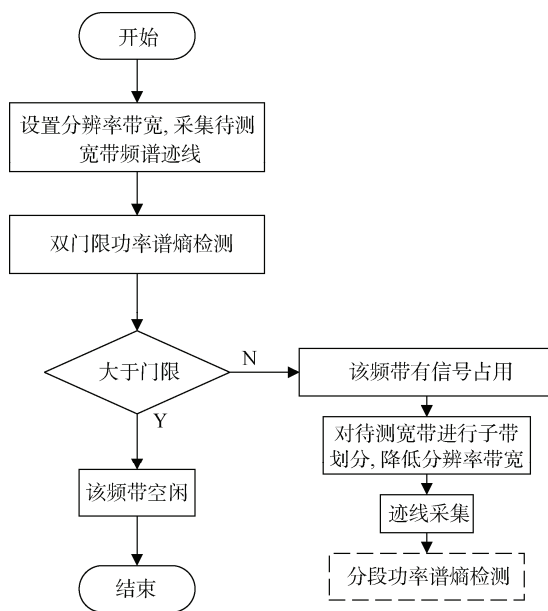


图 5 分阶段宽带频谱感知方案流程图

Figure 5 Flow chart of two-stage wideband spectrum sensing method

基于上述步骤, 可得待测宽带内信号的个数和占用的频段。

4.2 信号切分修正

在上述检测过程中, 在细感知阶段对子带进行频谱检测时, 可能存在信号被切分的现象。如图 6 所示,

信号被划入两个子带中, 造成错判。为了进一步提升算法的鲁棒性和信号个数的检测成功率, 本文在细感知阶段, 增加信号切分修正单元, 利用两相邻子带的迹线构造检验统计量, 判断信号的切分现象。

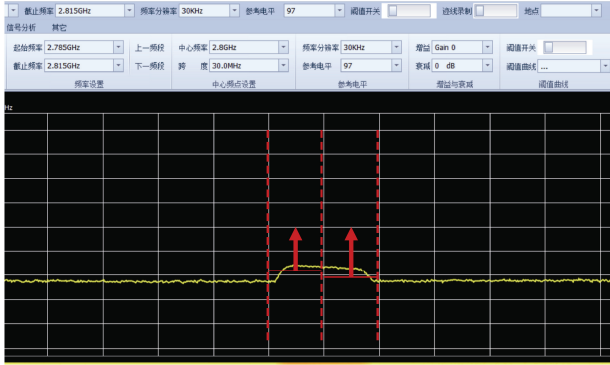


图 6 信号的切分现象
Figure 6 Signal segmentation

完整的切分调整流程如图 7 所示。记第 k 个已检子带中心频点为 f_k , 第 $k+1$ 个已检子带中心频点为 f_{k+1} (如图 6 所示), 则中间部分带宽为

$$B_k = f_{k+1} - f_k \quad (45)$$

采集这部分带宽内的迹线, 由式(43)计算功率谱熵 H_k , 则判决过程可表示为

$$H_k \begin{cases} \leq \lambda_k, \text{切分} \\ > \lambda_k, \text{未切分} \end{cases} \quad (46)$$

式中, λ_k 为判决门限, 基于式(38)计算求得, 表示为 $\lambda_k = \sigma_k Q^{-1}(P_{fa}) + \mu_k$, 其中 σ_k 和 μ_k 分别为基于所采集该带宽内背景迹线的信息熵, 所估计的方差与均值。由于带宽内可能存在两子带信号频谱重叠的现象, 为降低切分判决虚警率, 此处只进行单门限的功率谱熵检测。计算门限时, 设置虚警率 P_{fa} 为较小值(取值范围 $10^{-5} \sim 10^{-3}$), 以降低判决门限。若检验统计量小于门限值 λ_k , 则判决存在信号切分, 对两个子带进行合并。

对于被划分的 M 个子带, 若相邻两子带判决为有频段占用, 则进行上述切分判决。基于上述步骤, 实现信号的切分调整。

5 仿真与实验分析

5.1 双门限功率谱检测算法性能分析

5.1.1 仿真分析

(1) 检测性能分析

为验证算法在低信噪比下的检测性能, 本文以

常见的隐蔽通信方式——扩频通信为例, 设计相关仿真实验。参数设置如表 2 所示。

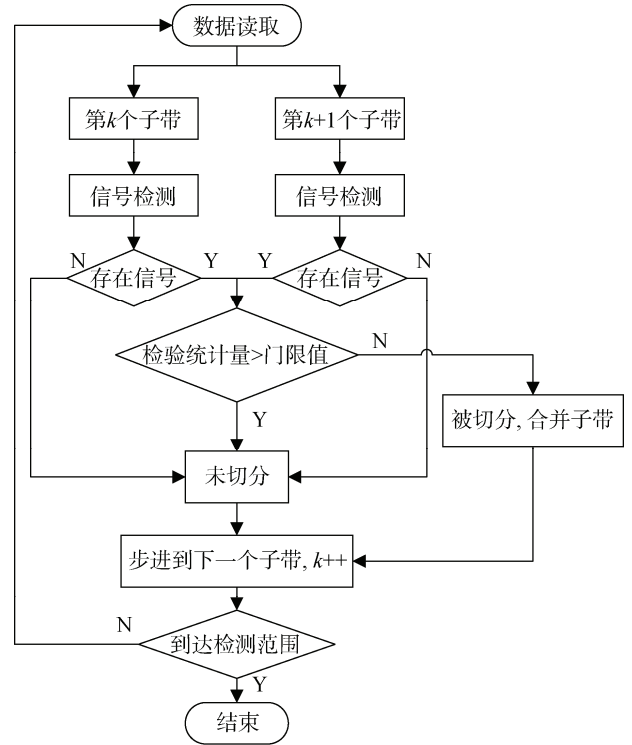


图 7 切分调整流程
Figure 7 Segmentation adjustment process

表 2 仿真参数设置
Table 2 Simulation parameter setup

参数	数值
信号类型	AWGN+DS-BPSK
信号功率	依信噪比而定
样本点数	6000
载频	128kHz
采样率	48kHz
码元速率	2000symbol/s

基于图 7 的算法流程图, 对上述扩频信号在 Gauss 白噪声信道下进行检测, 模拟非合作模式下对隐蔽通信信号的检测。每个实验结果进行 5000 次蒙特卡罗模拟。对实验信号进行功率谱估计, 求功率谱熵, 进行检测判决。本文所提算法参数设为: 虚警率 $P_{faH} = 0.1$, $P_{faL} = 0.01$, 调节系数 $\varepsilon = 0.01$, $m = 2$ 。

由图 8 结果可见, 在不存在噪声不确定度的条件下, 本文算法在 -16dB 信噪比下检测率大于 80%, 优于能量检测法^[19]和其他基于熵的算法^[20-21]。本文算法在 -14dB 信噪比下, 能达到其他文献^[20-21]中基于熵的检测方法在 -8dB 下的检测性能, 算法性能提升了约 6dB。证明了基于功率谱熵的方法, 与其他基

于熵的方法相比, 更好地反映了信号和噪声间的差异特征, 更适合对低功率的隐蔽通信信号检测。

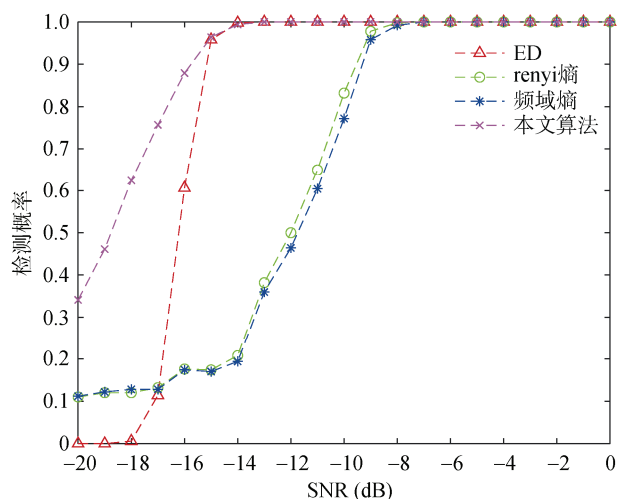


图 8 本文算法与其他文献算法的检测性能比较

Figure 8 Comparison of detection performance between proposed algorithm and algorithms in other literature

接着, 仿真分析了不同样本点数和信噪比下本文算法的 ROC 曲线。为便于分析, 算法虚警率 $P_{faH} = P_{faL}$, 其余参数设置不变。由图 9 结果可见, 样本长度越大, 算法检测性能越高, 当样本点数 $N \geq 6500$, 虚警率 0.1 时, 检测率大于 80%。由图 10 结果可见, 当样本长度一定时, 随着信噪比降低, 算法性能出现了一定程度的下降, 当 $SNR \geq -10\text{dB}$, 虚警率 0.1 时, 检测率大于 80%, 证明了本文算法在低信噪比下仍具有较好的检测性能。

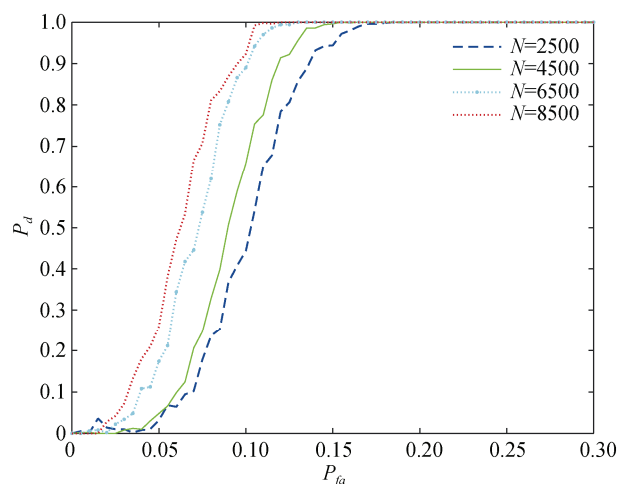


图 9 信噪比 $SNR = -15\text{dB}$ 下, 不同样本点数下本文算法的 ROC 曲线

Figure 9 Under $SNR = -15\text{dB}$, the ROC curve of proposed algorithm under different sample points

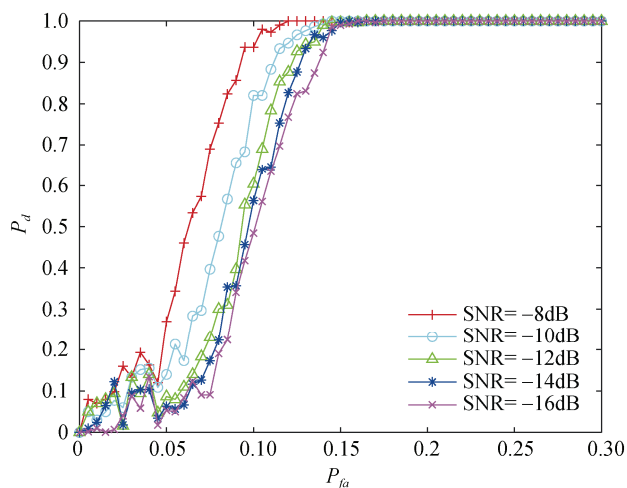


图 10 样本点数 $N = 3000$, 不同信噪比下本文算法的 ROC 曲线

Figure 10 Under $N=3000$, the ROC curve of proposed algorithm under different SNR

调节系数是本文算法中决定检测性能的一个重要参数。图 11 分析了在不同调节系数与 DFT 点数下, 本文算法与文献[22]的单门限频域熵检测器性能对比。文献中方法为典型的基于信号 DFT 的信息熵特征构造的检测算子, 原理与本文类似。本文所提算法参数设置为: 虚警率 $P_{faH} = 0.1$, $P_{faL} = 0.01$, $m = 1$ 。

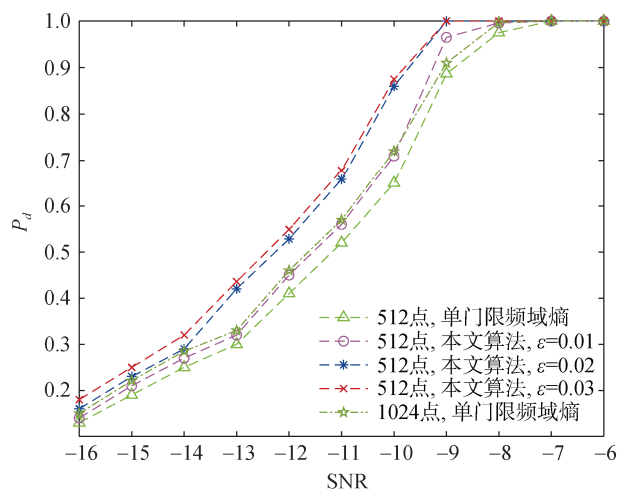


图 11 不同调节系数与 DFT 点数下本文算法与单门限频域熵检测性能对比

Figure 11 Performance comparison between proposed detector and single-threshold frequency entropy detector under different adjustment factors and DFT points

由图 11 结果可见, 当调节系数 $\epsilon > 0.01$ 时, 检测性能有了明显的提升, 但当调节系数为 0.02 和 0.03 时, 曲线近乎重合, 两者的检测性能相当。在算法实

际应用中, 调节系数应设置为一个合理的范围, 调节系数过大, 虽然能提升一定的检测概率, 但会使检验统计量更多地落在二次判决的区间范围内, 增加判决的计算量, 导致更多的时间开销。由图中结果, 调节系数 $\varepsilon = 0.01$ 时, 本文算法作 512 点 DFT 时的检测性能与文献[22]算法作 1024 点 DFT 时的检测性能相当, 且计算复杂度更小。

(2) 抗噪声不确定度分析

由于实际环境中无线信道的复杂性, 往往需要考虑到噪声不确定度的影响, 噪声不确定度^[23]的模型可表示为

$$\hat{\sigma}^2 \in [\sigma^2, \alpha\sigma^2] \quad (47)$$

式中, σ^2 表示噪声功率的估计值, $\hat{\sigma}^2$ 表示实际的噪声功率, α 表示噪声的不确定度 ($\alpha > 1$), 以 dB 的形式表示为 $\beta = 10 \lg \alpha$ 。

为验证算法抗噪声不确定度的性能, 仿真实验参数设置如表 3 所示, 将本文算法与目前频谱监测中应用最广泛的能量检测法进行对比, 信噪比固定为 -15dB, 算法参数设置为: 虚警率 $P_{faH} = P_{faL} = 0.1$, $\varepsilon = 0.01$, $m = 2$ 。

表 3 仿真参数设置

Table 3 Simulation parameter setup

参数	数值
信噪比	-15dB
背景噪声功率区间	-87~-83dBmW
信号类型	AWGN+DS-BPSK
信号功率	依信噪比而定
样本点数	5000
载频	256kHz
采样率	96kHz
码元速率	3000symbol/s

图 12 为本文算法与能量检测法的结果对比。由结果可见, 当背景噪声功率 -85dBmW (噪声不确定度 0) 时, 能量检测法检测率和虚警率为正常值, 但当噪声功率波动大于 0.5dBmW 时, 性能严重下降, 而本文算法在背景噪声功率变化时, 检测率和虚警率均维持在一个恒定的水平, 对噪声不确定度的鲁棒性更好。

5.1.2 隐蔽通信场景实测分析

(1) 实验布置

为验证本文所提算法在实际环境中的检测效果, 利用 R&S 公司 SMW200A 信号源发射宽带测试信号, 模拟隐蔽通信信号的信息传输。在非屏蔽的实验环

境中, 除测试信号外, 待测频段内无其他电子设备的干扰, 模拟实际的频谱监测场景。实验布置如图 13 所示, 发射天线连接信号源, 利用实验室自研的频谱监测设备进行信号接收。通过配套的频谱分析软件, 采集迹线数据进行分析。

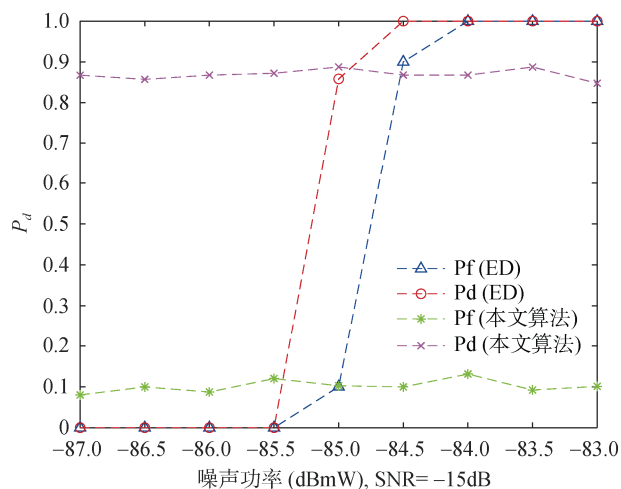


图 12 本文算法与能量检测法在存在噪声不确定度时的性能比较

Figure 12 The performance comparison between proposed algorithm and the energy detection method in the presence of noise uncertainty

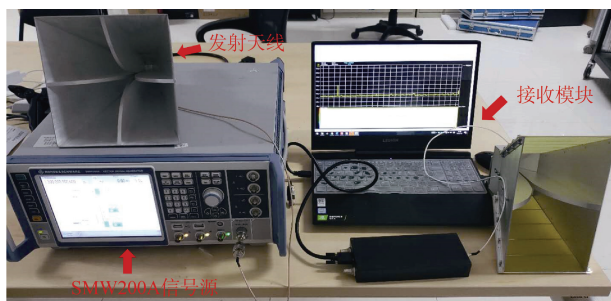


图 13 实验布置图

Figure 13 Experiment layout

对于实际环境下接收信号的信噪比, 采用文献[24]基于谱分析的平均信噪比估计方法进行计算, 其步骤如下:

(1) 接收机采集待测频段范围的时域 IQ 数据, 根据 Welch 法计算接收信号的功率谱 $X(f)$ 。

(2) 对功率谱 $X(f)$ 进行均值滤波, 由于发射的信号是预先设定的, 可求得发射信号所对应的频率带宽 $B = f_H - f_L$ 。

(3) 对测试信号频段外的功率谱图进行直方图分析, 计算得出噪声功率谱的均值 N , 最后将信号频率范围内的功率谱值减去噪声谱均值, 得到信号的谱值, 接收信号信噪比可表示为

$$\hat{\rho}_{dB} = 10\lg(\frac{\int_{f_L}^{f_H} X(f)df - N_0B}{N_0f_s/2}) \tag{48}$$

式中, f_s 为接收信号的采样频率。

(2) 无干扰背景下实验结果分析

如图 14, 为信号源 SMW200A 发射的测试信号在接收端频谱分析软件上所显示的迹线。测试信号参数为: 码元速率 100Mbyte/s, 脉冲成型方式为根升余弦, 载频 2.8GHz, 调制方式为 BPSK。

如图 15, 设置检测带宽 150MHz, 分辨率带宽 30kHz, 调节信号源发射功率和与接收机的距离, 此时图 14 中的信号逐渐淹没在噪声中。在接收信噪比 -6.32dB 下, 利用本文所提双门限功率谱熵检测算法, 基于采集的迹线数据, 判决得到此时该频段有信号占用, 证明了该方法在负信噪比下, 对可能存在信息传输的隐蔽通信信号检测的有效性。

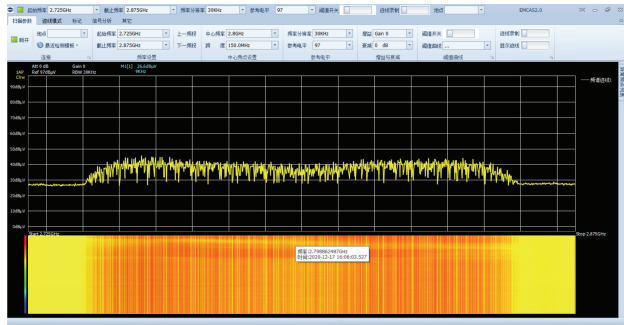


图 14 信号源发射带宽约 100MHz 的宽带信号
Figure 14 Signal source emits a wideband signal with a bandwidth of about 100MHz

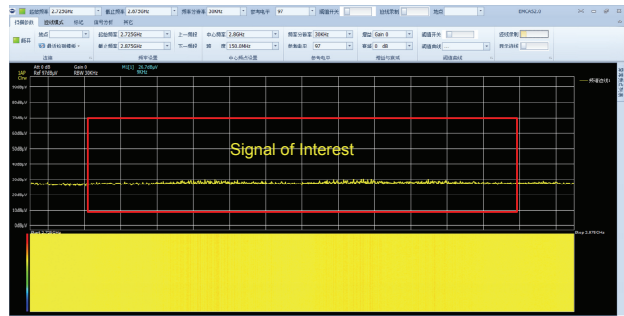


图 15 信号逐渐淹没在噪声中
Figure 15 The signal is gradually submerged in noise

为进一步验证算法的检测性能, 信号源发射调制方式集合为 {2FSK、QPSK、MSK、2ASK、BPSK、16QAM} 的测试信号, 模拟非合作频谱监测下的隐蔽通信信号传输, 参数如表 4 所示。算法参数设为: 虚警率 $P_{faH} = P_{faL} = 0.1$, $\varepsilon=0.01$, $m=2$ 。采集迹线进行检测, 每个实验结果进行了 500 次的实验。

表 4 实验参数设置

Table 4 Experiment parameter setup

参数	数值
信号类型	{2FSK、QPSK、MSK、2ASK、BPSK、16QAM}
码元速率	100Msymbol/s
发射功率	依信噪比而定
载频	2.8GHz
脉冲成型方式	根升余弦
检测带宽	150MHz
分辨率带宽	30kHz

图 16 为不同信噪比下六种调制方式信号的检测概率, 以及各信噪比下的平均虚警率。由实验结果可见, 信噪比较低时, 每种调制方式的信号检测性能有所差异, 其中 2FSK 信号的检测性能最好, BPSK、16QAM 信号的检测性能略差。由于信号调制方式的复杂程度不同, 相同条件下功率谱熵也会有较为显著的差异, 从而造成算法检测性能的差别。此外, 实际实验的检测效果不如仿真实验的结果, 这是由于噪底不平坦、频谱泄露和接收信号谱估计误差等因素造成的, 但仍在可接受的范围内。从图中结果可见, 当信噪比 $SNR = -15\text{dB}$ 时, 六种调制信号的检测率都大于 60%, 证明了该检测算法在实际环境中的有效性。

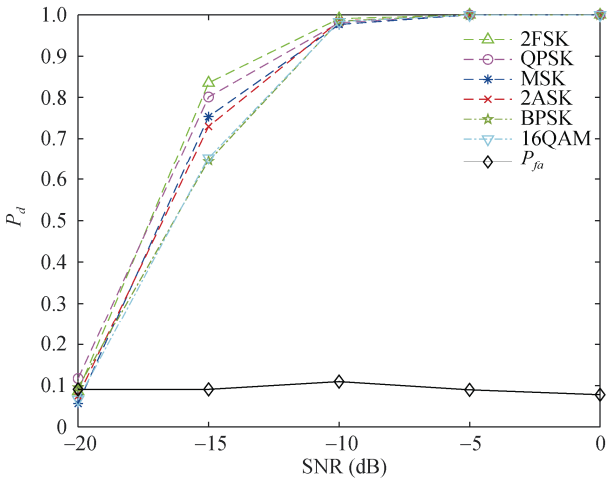


图 16 不同调制方式信号的检测性能
Figure 16 Detection performance of signals with different modulation methods

(3) 干扰背景下实验结果分析

如图 17 所示, 1.2~1.4GHz 频谱范围内, 存在时变的信号干扰, 噪底动态变化的情况。基于该背景, 利用信号源发射信号, 模拟隐蔽通信的信息传输, 参数设置如表 5 所示。检测算法参数设置与图 16 相同, 采集该频段迹线进行实验。

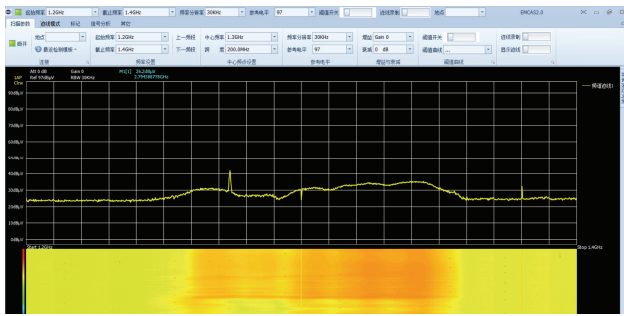


图 17 不平坦噪声底下对宽带信号的检测

Figure 17 Wideband signal detection under uneven noise floor

表 5 实验参数设置

Table 5 Experiment parameter setup

参数	数值
信号类型	{2FSK、QPSK、MSK、2ASK、BPSK、16QAM}
码元速率	100Msymbol/s
发射功率	依信噪比而定
载频	1.3GHz
脉冲成型方式	根升余弦
检测带宽	200MHz
分辨率带宽	30kHz

图 18 为在上述背景和实验参数设置下,不同调制方式的信号在不同信噪比下的检测性能,每个实验结果进行了 500 次的实验。与图 16 结果相比,算法的检测性能有所降低,但在信噪比 $SNR = -10dB$ 时,不同调制信号的检测率仍然大于 90%,证明了在实际环境下,该算法对噪声不确定度的鲁棒性。

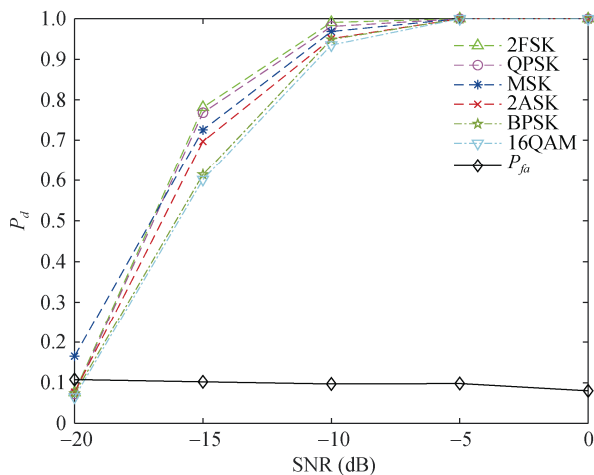


图 18 不平坦噪声底下,不同调制信号的检测性能

Figure 18 Detection performance of different modulation signals under uneven noise floor

在实际的电磁频谱监测环境中,往往存在定频干扰的情况。广播信号、WiFi 信号、对讲机信号都

是常用的定频信号,当某些信号和已知的定频信号的频段重叠时,常规的能量检测法往往难以检测到其存在,造成可能的安全风险。如图 19 所示,在 2.785~2.815GHz 频段范围内,发射一背景信号。在背景信号带宽范围内,发射不同调制方式的测试信号,实验参数设置如表 6 所示,此时图 19 中的迹线包络没有显著变化。

表 6 实验参数设置

Table 6 Experiment parameter setup

参数	数值
背景信号类型	QPSK
背景信号载频	2.8GHz
背景信号码元速率	6Msymbol/s
测试信号类型	{2FSK、QPSK、MSK、2ASK、BPSK、16QAM}
测试信号码元速率	5Msymbol/s
测试信号发射功率	依信干比而定
测试信号载频	2.8GHz
测试信号脉冲成型方式	根升余弦
检测带宽	30MHz
分辨率带宽	30kHz

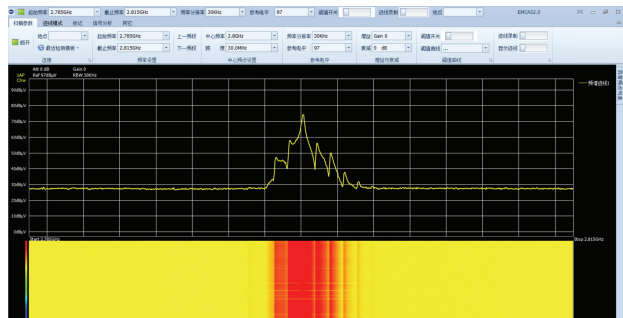


图 19 存在背景信号干扰时的检测场景

Figure 19 Detection scene when there is background signal interference

基于图 19 中的场景,采集迹线进行检测,检测算法参数设置与图 16 相同。图 20 为在不同信干比下算法的检测结果,每个实验结果进行 500 次的实验。在信干比 $SIR = -10dB$ 时,不同调制信号的检测概率大于 70%,证明了算法在存在定频干扰的情况下,仍可感知到背景信号下的隐蔽信息传输,具有较好的检测性能。

5.2 分阶段宽带频谱感知方法实测分析

5.2.1 实验布置

在对分阶段宽带频谱感知方法的性能实测中,利用矢量信号源 SMW200A 和 USRP 软件无线电平台产生若干不同调制类型的宽带信号和窄带信号,作为进行信息传输的隐蔽通信信号,模拟实际环境下

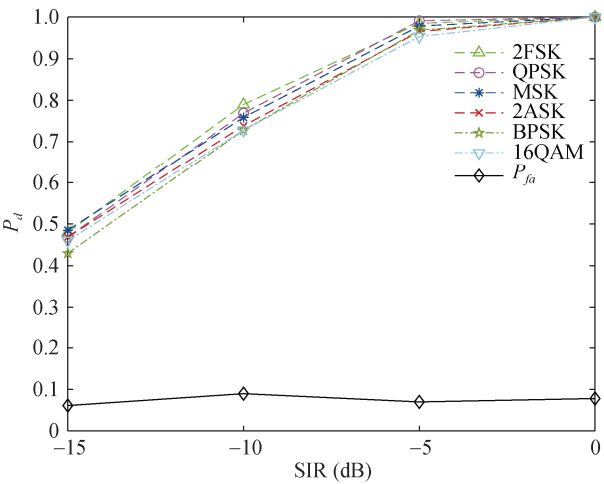


图 20 不同信干比时不同调制信号的检测性能
Figure 20 Detection performance of different modulated signals at different SIR ratios

的宽带频谱感知场景(如图 21 所示)。在非屏蔽实验室中,除测试信号外,待测频段内无其他电子设备的干扰。在本次实验中,利用两台 USRP X300 设备,通过 Gnuradio 软件^[25-26]编程实现信号的发射,利用矢量信号源 SMW200A 产生宽带信号。

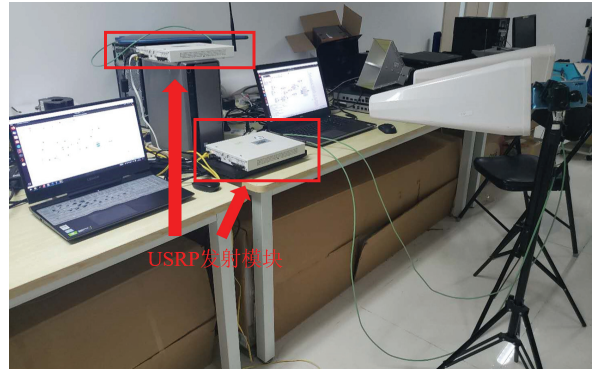


图 21 宽带频谱监测实验布置
Figure 21 Wideband spectrum monitoring experiment layout

5.2.2 无干扰背景下实验结果分析

如图 22 所示,在跨度 500MHz 的频段内,存在五个待测的隐蔽通信信号,实验参数如表 7 所示。调节信号源发射功率和与接收机的距离,降低接收信噪比,基于图 5 的方法流程图,采集迹线进行检测。参数设置为:子带划分数 $M = 50$,分辨率带宽分别取 $RBW_1 = 500\text{kHz}$, $RBW_2 = 2\text{kHz}$,双门限检测算法参数设置为: $P_{faH} = P_{faL} = 0.1$, $\varepsilon = 0.1$, $m = 2$ 。

如图 23 所示,基于图 22 的实验场景,将本文方法与常用于宽带多信号检测的单阈值频域前向连续均值去除(FCME)算法^[24]进行对比。检测率表示为:

检测出全部 5 个信号的次数/实验总次数,每个实验结果进行 500 次实验。由图 23 可见,本文方法表现出了比 FCME 算法更好的检测性能,在接收信噪比 $\text{SNR} = -5\text{dB}$ 时,检测率大于 80%,证明了算法的有效性。

表 7 实验参数设置	
Table 7 Experiment parameter setup	
参数	数值
信号类型	{2FSK、QPSK、MSK、2ASK、BPSK}
码元速率	2Msymbol/s、3Msymbol/s、100Msymbol/s、6Msymbol/s、5Msymbol/s
发射功率	依信噪比而定
载频	3.3GHz、3.45GHz、3.5GHz、3.65GHz、3.7GHz
脉冲成型方式	根升余弦
检测带宽	500MHz
分辨率带宽	500kHz、2kHz

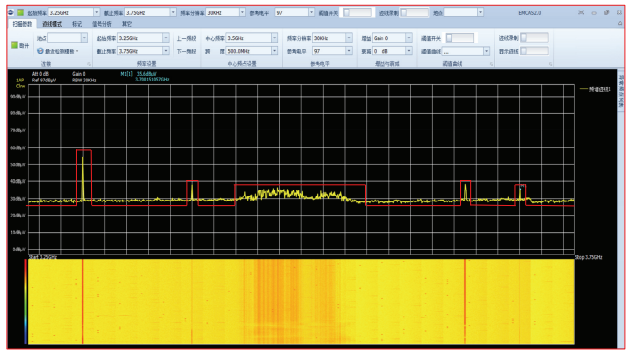


图 22 宽带多信号的检测场景
Figure 22 Wideband multi-signal detection scene

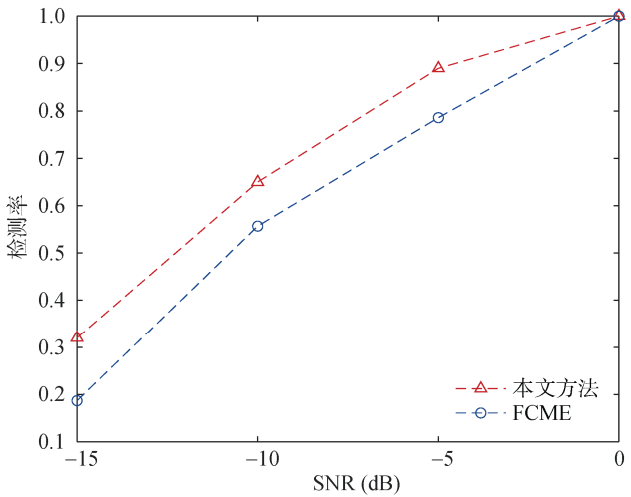


图 23 本文方法与其他算法的检测结果对比
Figure 23 Comparison of detection results between proposed method and other algorithm

5.2.3 干扰背景下实验结果分析

如图 24、图 25 所示,调节信号发射功率和与接

收机的距离,降低接收信噪比,在噪底动态变化,存在时变信号干扰的环境下,对宽带范围内多个信号进行检测,本文所提方法的参数设置与图 23 相同。与传统的单阈值 FCME 算法在低信噪比时存在漏检的现象(如图 24)相比,本文方法(如图 25)成功实现了对多个可能的隐蔽通信信号的感知。

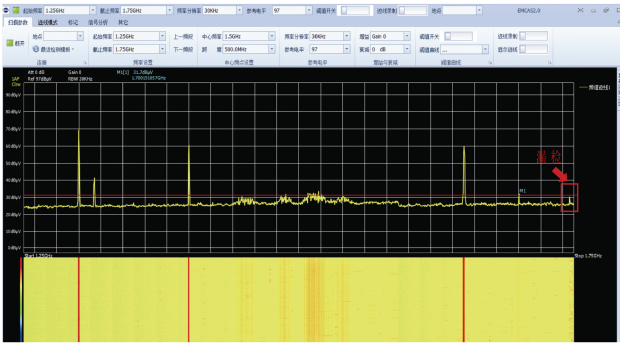


图 24 FCME 算法存在漏检现象

Figure 24 The FCME algorithm has missed detection

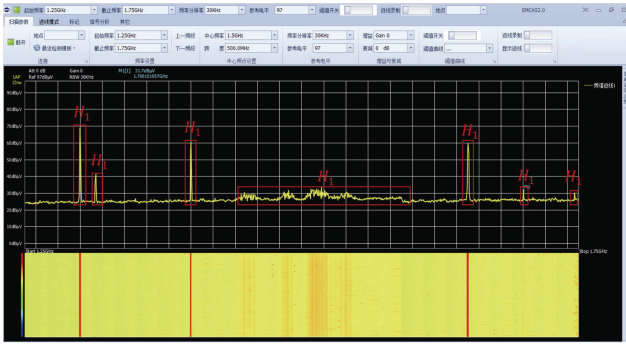


图 25 本文方法实现对宽带多信号的检测

Figure 25 The proposed method realizes the detection of wideband multi-signal

设置实验参数如表 8 所示,基于图 24、图 25 的检测场景,将本文方法与 FCME 算法在不同信噪比下的检测结果作对比,方法参数设置与图 23 相同,每个实验结果进行 500 次实验。由图 26 的实验结果可见,相比于 FCME 算法在干扰背景下性能下降明显,本文所提方法的检测性能没有明显下滑。在信噪比 $SNR = -10\text{dB}$ 时,检测率仍然大于 60%,证明该方法对噪声不确定度有较好的鲁棒性。

6 总结

本文针对电磁频谱监测中,某些进行信息传输的隐蔽通信信号淹没在背景噪声中难以检测,可能造成电磁安全风险的问题,提出了一种基于功率谱熵的改进双门限检测算法,仿真和不同场景下的实测实验证明了该算法在低信噪比下,能有效感知到

可能进行信息传输的隐蔽通信信号。基于该算法,提出了针对宽带内多个低功率隐蔽信号的分阶段功率谱熵检测方法,通过采集实际环境的频谱迹线进行实验,证明了该方法能在低信噪比下对宽带内多个可能的隐蔽通信信号进行有效感知,并能确定信号的个数和占用频段。下一步研究将在更复杂的电磁环境下进行实验,进一步验证该方法在实际场景下的性能,同时结合信号时域特征,对检出的可能存在信息传输隐蔽的通信信号进行相关参数估计,以更好地评估可能的电磁空间安全风险。

表 8 实验参数设置

Table 8 Experiment parameter setup

参数	数值
信号类型	{2FSK、QPSK、MSK、2ASK、BPSK}
码元速率	2Msymbol/s、3Msymbol/s、100Msymbol/s、6Msymbol/s、5Msymbol/s
发射功率	依信噪比而定
载频	1.3GHz、1.45GHz、1.5GHz、1.65GHz、1.7GHz
脉冲成型方式	根升余弦
检测带宽	500MHz
分辨率带宽	500kHz、2kHz

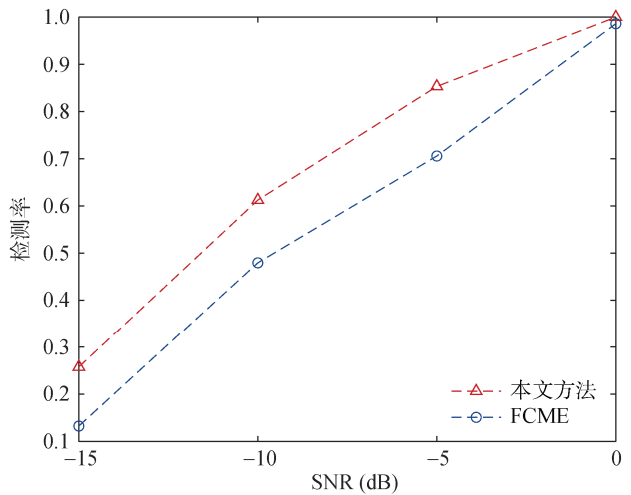


图 26 干扰下,本文方法与其他算法的检测结果对比

Figure 26 The performance comparison of proposed method with other algorithm under interference

参考文献

- [1] Urkowitz H. Energy Detection of Unknown Deterministic Signals[J]. *Proceedings of the IEEE*, 1967, 55(4): 523-531.
- [2] Robey F C, Fuhrmann D R, Kelly E J, et al. A CFAR Adaptive Matched Filter Detector[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 1992, 28(1): 208-216.
- [3] Lunden J, Kassam S A, Koivunen V. Robust Nonparametric Cyclic Correlation-Based Spectrum Sensing for Cognitive Radio[J]. *IEEE*

- Transactions on Signal Processing*, 2010, 58(1): 38-52.
- [4] Wang Y H, Zhang S C, Zhang Y W, et al. A Cooperative Spectrum Sensing Method Based on Signal Decomposition and K-Medoids Algorithm[J]. *International Journal of Sensor Networks*, 2019, 29(3): 171.
- [5] Tian Z, Giannakis G B. A Wavelet Approach to Wideband Spectrum Sensing for Cognitive Radios[C]. *2006 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2007: 1-5.
- [6] He D, Lin Y P, He C, et al. A Novel Spectrum-Sensing Technique in Cognitive Radio Based on Stochastic Resonance[J]. *IEEE Transactions on Vehicular Technology*, 2010, 59(4): 1680-1688.
- [7] Al-Badrawi M H, Kirsch N J. An EMD-Based Double Threshold Detector for Spectrum Sensing in Cognitive Radio Networks[C]. *2015 IEEE 82nd Vehicular Technology Conference*, 2016: 1-5.
- [8] Cover T M. Elements of information theory[M]. John Wiley & Sons, 1999:792.
- [9] Nagaraj S V. Entropy-Based Spectrum Sensing in Cognitive Radio[J]. *Signal Processing*, 2009, 89(2): 174-180.
- [10] Zhu Y Y, Zhu Y G. The Simulation Study of Entropy-Based Signal Detector over Fading Channel[C]. *2012 International Conference on Wireless Communications and Signal Processing*, 2013: 1-5.
- [11] Zhang Q T. An Entropy-Based Receiver for the Detection of Random Signals and Its Application to Radar[J]. *Signal Processing*, 1989, 18(4): 387-396.
- [12] Zhang Y, Zhang Q, Wu S. Entropy-Based Robust Spectrum Sensing in Cognitive Radio[J]. *IET Communications*, 2010, 4(4): 428.
- [13] Prieto G, Andrade Á G, Martínez D M. Numerical Analysis of Histogram-Based Estimation Techniques for Entropy-Based Spectrum Sensing[J]. *IETE Technical Review*, 2020, 37(1): 91-97.
- [14] Zhao N. A Novel Two-Stage Entropy-Based Robust Cooperative Spectrum Sensing Scheme with Two-Bit Decision in Cognitive Radio[J]. *Wireless Personal Communications*, 2013, 69(4): 1551-1565.
- [15] Barbe K, Pintelon R, Schoukens J. Welch Method Revisited: Nonparametric Power Spectrum Estimation via Circular Overlap[J]. *IEEE Transactions on Signal Processing*, 2010, 58(2): 553-565.
- [16] Prieto G, Andrade Á G, Martínez D M, et al. On the Evaluation of an Entropy-Based Spectrum Sensing Strategy Applied to Cognitive Radio Networks[J]. *IEEE Access*, 2018, 6: 64828-64835.
- [17] Xia W J, Cai Z M. Performance Analysis of Power Spectrum Entropy Detection for Unknown Sinusoidal Signals[J]. *Journal of Signal Processing*, 2018, 34(12): 1499-1507.
(夏文杰, 蔡志明. 未知正弦信号的功率谱熵检测性能分析[J]. *信号处理*, 2018, 34(12): 1499-1507.)
- [18] Haykin S. Cognitive Radio: Brain-Empowered Wireless Communications[J]. *IEEE Journal on Selected Areas in Communications*, 2005, 23(2): 201-220.
- [19] Zeng Y H, Liang Y C, Zhang R. Blindly Combined Energy Detection for Spectrum Sensing in Cognitive Radio[J]. *IEEE Signal Processing Letters*, 2008, 15: 649-652.
- [20] Srinu S, Sabat S L, Udgate S K. Spectrum Sensing Using Frequency Domain Entropy Estimation and Its FPGA Implementation for Cognitive Radio[J]. *Procedia Engineering*, 2012, 30: 289-296.
- [21] Cadena Muñoz E, Pedraza Martínez L F, Hernandez C A. Rényi Entropy-Based Spectrum Sensing in Mobile Cognitive Radio Networks Using Software Defined Radio[J]. *Entropy*, 2020, 22(6): 626.
- [22] Zhang Y L, Zhang Q Y, Melodia T. A Frequency-Domain Entropy-Based Detector for Robust Spectrum Sensing in Cognitive Radio Networks[J]. *IEEE Communications Letters*, 2010, 14(6): 533-535.
- [23] Tandra R, Sahai A. SNR Walls for Signal Detection[J]. *IEEE Journal of Selected Topics in Signal Processing*, 2008, 2(1): 4-17.
- [24] Peng G, Huang Z T, Lu F B, et al. Fast Blind SNR Estimation of IF Communication Signals[J]. *Journal of Electronics & Information Technology*, 2010, 32(1): 102-106.
(彭耿, 黄知涛, 陆风波, 等. 中频通信信号信噪比的快速盲估计[J]. *电子与信息学报*, 2010, 32(1): 102-106.)
- [25] Li X G, Pan K G, Yang Q, et al. Research and Implementation of Segmented Differential Dual Threshold Wideband Signal Detection Technology Based on GNURadio[J]. *Communications Technology*, 2018, 51(9): 2040-2046.
(李晓光, 潘克刚, 杨群, 等. 基于 GNURadio 分段差分双阈值的宽带信号检测技术研究及实现[J]. *通信技术*, 2018, 51(9): 2040-2046.)
- [26] Muslimin J, Asnawi A L, Ismail A F, et al. SDR-Based Transceiver of Digital Communication System Using USRP and GNU Radio[C]. *2016 International Conference on Computer and Communication Engineering*, 2017: 449-453.



洪泽坤 于 2018 年在中国农业大学电子信息工程专业获得学士学位。现在中国科学院大学信息工程研究所网络空间安全专业攻读硕士学位。研究领域为信号处理、超宽带信号检测。研究兴趣包括: 通信安全、电磁信息安全。Email: hongzekun@iie.ac.cn



徐艳云 于 2012 年在中国科学院研究生院电磁场与微波专业获得博士学位。现任中国科学院信息工程研究所高级工程师。研究领域为电磁信息安全、信号处理等。研究兴趣包括: 电磁泄漏发射检测、电磁指纹特征等。Email: xuyanyun@iie.ac.cn



黄伟庆 于 2002 年在北京邮电大学获得硕士学位。现任中国科学院信息工程研究所正研级高级工程师。研究领域为电磁信息安全、信号处理等。研究兴趣包括: 电磁泄漏发射检测、无线通信安全、电磁信息安全。Email: huangweiqing@iie.ac.cn



李婷婷 中国科学院信息工程研究所硕士研究生, 主要研究方向为超宽带信号检测。E-mail: litngting@iie.ac.cn



于超 2019 年在中国民航大学电子信息工程专业获得学士学位。现在中国科学院大学网络空间安全专业攻读硕士学位。研究领域为网络空间安全。研究兴趣包括: 图像处理、文本识别。Email: yuchao@iie.ac.cn