

## 基于统计相关差异的多基地雷达拖引欺骗干扰识别

孙闽红<sup>①</sup> 丁辰伟<sup>\*①</sup> 张树奇<sup>①</sup> 鲁加战<sup>②</sup> 邵鹏飞<sup>②</sup>

<sup>①</sup>(杭州电子科技大学通信工程学院 杭州 310018)

<sup>②</sup>(中国航天科工集团八五一一所 南京 210000)

**摘要:** 针对长基线多基地雷达系统在目标跟踪阶段的拖引欺骗干扰识别问题, 考虑到真实目标回波在不同节点雷达中的幅度相互独立, 而拖引欺骗干扰假设来自同一干扰机, 其在不同节点雷达中的幅度完全相关, 从而跟踪波门内只有目标回波与同时存在目标回波与拖引欺骗干扰这两种不同情形下的信号幅度存在统计相关差异。该文提出利用这一差异实现多基地雷达系统的拖引欺骗干扰识别。通过在分析统计相关差异的基础上, 对不同节点雷达接收到的回波信号幅度序列进行相关性度量及参数估计, 构建检验统计量, 在给定的虚警概率下实现了对欺骗干扰的识别。仿真实验结果表明, 该方法对欺骗干扰具有较好的识别效果, 相较于基于拟合优度的AD检测算法, 识别概率平均提高18.63%。

**关键词:** 欺骗干扰; 检测识别; 多基地雷达系统; 相关性

中图分类号: TN974

文献标识码: A

文章编号: 1009-5896(2020)12-2992-07

DOI: [10.11999/JEIT190634](https://doi.org/10.11999/JEIT190634)

## Recognition of Deception Jamming Based on Statistical Correlation Difference in a Multistatic Radar System

SUN Minghong<sup>①</sup> DING Chenwei<sup>①</sup> ZHANG Shuqi<sup>①</sup>

LU Jiazhan<sup>②</sup> SHAO Pengfei<sup>②</sup>

<sup>①</sup>(College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China)

<sup>②</sup>(China Aerospace Science and Technology Group 8511 Research Institute, Nanjing 210000, China)

**Abstract:** In multistatic radar system, the real target echoes are independent of each other in different node radars under long-term baseline conditions, but the amplitudes of the deception jamming signals in different node radars are completely correlated because of the jamming signals generated from the same jammer. This paper uses the difference to realize the recognition of deception jamming in multistatic radar system on the stage of tracking. Correlation measurement and parameter estimation are carried out on the amplitude sequence of the received signals by different nodes, and the test statistic is constructed to realize the recognition of deception jamming under the given false alarm probability. The simulation results show that the proposed method has a good performance on the recognition of deception jamming. Compared to the Anderson-Darling (AD) test based on goodness-of-fit, the recognition probability increases by an average of 18.63%.

**Key words:** Deception jamming; Detection and recognition; Multistatic radar system; Correlation

### 1 引言

数字射频存储器<sup>[1]</sup> (Digital Radio Frequency Memory, DRFM)通过对截获的雷达信号进行采样、存储、调制和转发, 能够准确快速地产生与雷达信号高度逼真的欺骗干扰信号, 使得雷达无法轻易地识别欺骗假目标。针对欺骗式干扰, 单站雷达可以利用发射信号优化<sup>[2]</sup>、物体表面散射强度<sup>[3]</sup>、极化特性差异<sup>[4,5]</sup>、DOA差异<sup>[6]</sup>以及DRFM量化误

差<sup>[7]</sup>来识别欺骗干扰。但是, 单站雷达的探测角度单一, 无法获得完整的环境信息, 其抗干扰能力受到限制, 面对高逼真度的有源欺骗干扰假目标, 往往无法发挥出预期的抗干扰效果。

多基地雷达可以发挥雷达集群的优势, 获得更多的信息。文献[8]利用同一空域目标的空间相关性有效地进行真假目标识别。文献[9]利用单站雷达与双基雷达观测到真假目标的多普勒信息的差异, 可对有源假目标进行识别。文献[10]结合分布式多雷达系统的目标定位问题, 对欺骗干扰产生的假目标识别问题进行了研究。文献[11]采用正交脉冲块的

收稿日期: 2019-08-26; 改回日期: 2020-05-24; 网络出版: 2020-07-02

\*通信作者: 丁辰伟 751745548@qq.com

方法<sup>[12,13]</sup>和基于时间脉冲分集的策略, 在组网雷达下实现了对欺骗干扰的抑制。然而, 该方法目前无法抑制先进DRFM欺骗干扰机产生的在同一脉冲重复间隔内的欺骗干扰。文献[14]提出了基于目标幅度比差异的有源假目标鉴别方法, 通过对目标在各接收站中幅度比的随机分布进行理论分析, 发现同一个虚假目标在不同雷达接收机内的幅度比近似相等, 而同一个真实目标在不同雷达接收机内的幅度比不相等。根据幅度比差异, 利用聚类分析的方法实现了欺骗干扰识别。文献[15]考虑多基地雷达接收机中存在多个假目标的接收信号模型, 通过接收信号在不同接收端的互相关检验, 得到假目标的传播时间延迟, 然后提出了一种基于局部密度的带噪声应用空间聚类方法(Local Density-Based Spatial clustering of applications with noise, LDBScan)实现了欺骗干扰识别。文献[16]在非完全正交波形的分频阵列多输入多输出雷达中采用非均匀采样检测, 利用时间延迟和距离差分在发射-接收频域联合空间中对真目标和假目标进行识别。文献[17]针对多基地雷达系统中存在的多距离假目标欺骗干扰, 提出了一种基于同源定位试验的抗干扰技术, 仿真结果表明该方法能有效地识别假目标。文献[18]提出一种基于奇异谱分析(Singular Spectral Analysis, SSA)的抗距离波门拖引干扰方法, 通过提取干扰信号谐波分量与目标回波经SSA分解后奇异值能量的分布差异特征, 实现对有源欺骗干扰的检测识别。文献[19]提出了一种捷变频联合Hough变换的抗欺骗干扰方法, 利用脉间频率捷变技术规避大部分欺骗式干扰, 然后通过Hough变换和峰值提取进行干扰识别, 仿真实验结果表明该方法具有良好的抗干扰性能。文献[20]利用目标的空间散射特性<sup>[21,22]</sup>来识别欺骗干扰, 实现了雷达在搜索阶段的欺骗干扰识别, 这种情况下目标回波与欺骗干扰在时域上可分。然而, 当雷达工作在目标跟踪阶段、干扰机产生拖引欺骗干扰时, 目标回波与欺骗干扰在时域上不可分, 该方法不再适用。

针对文献[20]只适应于各节点雷达各距离门内只存在真实目标回波, 或只存在欺骗干扰信号的场景, 即真实目标与欺骗干扰在时域上可分, 本文进一步考虑雷达工作于目标跟踪状态, 跟踪波门内同时存在目标回波信号与欺骗干扰信号时, 即真实目标和欺骗干扰无法在时域上可分的场景, 同样基于相关性差异, 提出了多雷达系统欺骗干扰的统计检测识别方法。

## 2 信号模型

多雷达系统由 $N$ 部节点雷达组成, 其中仅有雷

达1工作在收发状态, 其余各部雷达仅工作在接收状态, 如图1所示。该多雷达系统对存在目标的某一特定区域进行探测。欺骗干扰机为掩护真实目标而释放虚假欺骗干扰信号。

没有干扰时, 各部节点雷达仅接收到目标回波和接收机内部噪声; 存在干扰时, 各部节点雷达接收目标回波、欺骗干扰和接收机内部噪声。因此, 欺骗干扰的检测识别问题可以模型化为一个二元假设检验问题。这里将欺骗干扰检测识别看作是如式(1)的二元假设检验

$$\begin{aligned} H_0 : x(n) &= s(n) + w(n) \\ H_1 : x(n) &= s(n) + j(n) + w(n) \end{aligned} \quad (1)$$

其中,  $x(n)$ 为雷达接收机接收的回波序列,  $s(n)$ 为真实目标回波序列,  $j(n)$ 为距离拖引欺骗干扰信号序列,  $w(n)$ 为雷达接收机内部的噪声序列。

对于不同节点雷达, 真实目标回波的幅度间的相关性与节点雷达间的基线长度 $L$ 、雷达发射信号载波波长 $\lambda$ 、真实目标相对于节点雷达的径向距离 $R$ 以及目标尺寸 $D$ 有关, 目标回波幅度的空间独立性条件为<sup>[20]</sup>

$$L \geq \lambda R/D \quad (2)$$

该独立条件的物理解释可以表述为: 如果把真实目标看作一个天线, 那么空间位置上相互分开的节点雷达接收到的真实目标的回波信号相互独立的条件是两个节点雷达处于该天线的主波束范围之外。

假定雷达基线足够长, 以保证目标回波信号在各个节点雷达上的回波幅度相互独立。假设各部节点雷达检测概率为1时, 第 $n$ 个节点雷达接收到的第 $p$ 个目标的幅度序列表示为

$$\mathbf{A}_p^n = \mathbf{B}_p^n + \mathbf{W}^n \quad (3)$$

其中,  $\mathbf{W}^n$ 为接收机内部噪声序列,  $\mathbf{W}^n \sim \text{CN}(0, \sigma_{w,n}^2 \mathbf{I}_{Q \times Q})$ , CN表示复高斯分布,  $\sigma_{w,n}^2$ 为第 $n$ 个节点雷达的噪声方差,  $\mathbf{I}_{Q \times Q}$ 为维数 $Q \times Q$ 的单位矩阵,  $Q$ 为相干处理周期(CPI)中的PRT的个

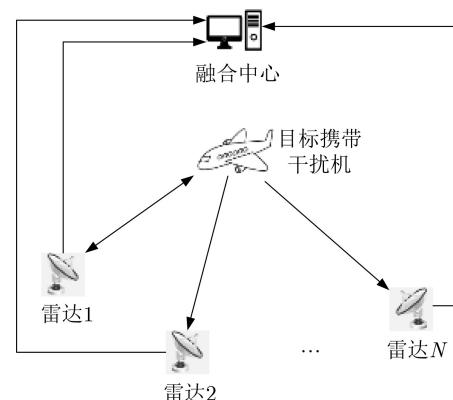


图1 多基地雷达系统探测目标示意图

数,  $\mathbf{B}_p^n$ 为目标回波信号幅度构成的慢时间幅度序列, 可表示为

$$\mathbf{B}_p^n = [\alpha_{p,n}^1, \alpha_{p,n}^2, \dots, \alpha_{p,n}^i, \dots, \alpha_{p,n}^Q]^T \quad (4)$$

其中,  $\alpha_{p,n}^i (i=1, 2, \dots, Q)$ 为第  $p$  个目标的回波信号在第  $n$  个节点雷达中的幅度。

### 3 相关性分析

#### 3.1 真实目标间的相关性

根据中心极限定理<sup>[23,24]</sup>,  $\alpha_{p,n}^i$ 服从复高斯分布, 即  $\alpha_{p,n}^i \sim \text{CN}(0, \sigma_{p,n}^2)$ 。同时幅度序列  $\mathbf{B}_p^n$  的各分量相互独立, 则可以得到

$$\mathbf{B}_p^n \sim \text{CN}(0, \sigma_{p,n}^2 \mathbf{I}_{Q \times Q}) \quad (5)$$

$$\mathbf{A}_p^n \sim \text{CN}(0, (\sigma_{p,n}^2 + \sigma_{w,n}^2) \mathbf{I}_{Q \times Q}) \quad (6)$$

由于同一目标的回波信号幅度在不同雷达接收机中相互独立, 对于  $\forall n \neq m$ , 可以得到  $\text{E}[(\mathbf{B}_p^n)^H(\mathbf{B}_p^m)] = 0$ , 不同雷达接收机中的噪声序列相互独立, 即  $\text{E}[(\mathbf{W}^n)^H(\mathbf{W}^m)] = 0$ , 不同节点雷达接收到的真实目标回波幅度序列之间的相关性可以表示为

$$\text{E}[(\mathbf{A}_p^n)^H(\mathbf{A}_p^m)] = 0 \quad (7)$$

$$\text{D}[(\mathbf{A}_p^n)^H(\mathbf{A}_p^m)] = Q \cdot (\sigma_{p,n}^2 + \sigma_{w,n}^2) \cdot (\sigma_{p,m}^2 + \sigma_{w,m}^2) \quad (8)$$

#### 3.2 欺骗干扰间的相关性

常规的转发式欺骗干扰是干扰机通过截获雷达发射信号进行直接储频转发来产生的。在一个 CPI 内, 干扰机发射的脉冲串中的各个脉冲的功率相差不大, 欺骗干扰信号可以近似看作在一个 CPI 内幅度不变。此时, 第  $n$  个节点雷达接收到的目标回波幅度序列为

$$\mathbf{A}_p^n = \mathbf{B}_p^n + \mathbf{J}_p^n + \mathbf{W}^n \quad (9)$$

$$\mathbf{A}_p^n \sim \text{CN}(\beta_{p,n}, (\sigma_{p,n}^2 + \sigma_{w,n}^2) \mathbf{I}_{Q \times Q}) \quad (10)$$

其中, 干扰功率相同的干扰幅度序列  $\mathbf{J}_p^n = [\beta_{p,n}, \beta_{p,n}, \dots, \beta_{p,n}]^T$ , 不同节点雷达中接收到的干扰回波来自于同一干扰机, 干扰幅度序列在各个不同

节点雷达中完全相关。尽管干扰机到各个节点雷达的传播衰减不同、雷达接收天线增益不同, 导致干扰在不同节点雷达中的功率不同, 但是并不影响其相关性。对于  $\forall n \neq m$ , 有  $\mathbf{J}_p^n = k \cdot \mathbf{J}_p^m$ ,  $\beta_{p,n} = k \cdot \beta_{p,m}$ , 不同节点雷达接收到的回波信号幅度序列之间的相关性表示为

$$\text{E}[(\mathbf{A}_p^n)^H(\mathbf{A}_p^m)] = Q \cdot \beta_{p,n} \cdot \beta_{p,m} \quad (11)$$

$$\begin{aligned} \text{D}[(\mathbf{A}_p^n)^H(\mathbf{A}_p^m)] &= Q \cdot [(\sigma_{p,n}^2 + \sigma_{w,n}^2) \cdot (\sigma_{p,m}^2 + \sigma_{w,m}^2) \\ &\quad + (\sigma_{p,n}^2 + \sigma_{w,n}^2) \cdot \beta_{p,m}^2 \\ &\quad + (\sigma_{p,m}^2 + \sigma_{w,m}^2) \cdot \beta_{p,n}^2] \end{aligned} \quad (12)$$

### 4 相关性检测

根据以上描述的相关性差异, 利用相关性差异来识别欺骗干扰目标。不失一般性, 以两个节点雷达为例介绍基于相关性的检测方法来识别真假目标。

为了衡量真假目标相关性上的差异, 定义相关性度量

$$\mu = (\mathbf{A}_p^1)^H \mathbf{A}_p^2 \quad (13)$$

式(1)表示的二元假设检验可以转化为

$$\left. \begin{aligned} H_0 : \mu &\sim \text{CN}(0, Q\zeta_{p,1}^2\zeta_{p,2}^2) \\ H_1 : \mu &\sim \text{CN}(Q\beta_{p,1}\beta_{p,2}, Q(\zeta_{p,1}^2\zeta_{p,2}^2 \\ &\quad + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2)) \end{aligned} \right\} \quad (14)$$

其中,  $\zeta_1^2 = \sigma_{p,1}^2 + \sigma_{w,1}^2$ ,  $\zeta_2^2 = \sigma_{p,2}^2 + \sigma_{w,2}^2$ 。

根据检测理论可知, 构建广义似然比检测如式(15)所示

$$\frac{p(\mu | H_1)}{p(\mu | H_0)} \stackrel{H_1}{\gtrless} \Lambda \quad (15)$$

式(15)又可以表示为

$$e^{-\frac{(\mu - Q\beta_{p,1}\beta_{p,2})^2}{2Q(\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2)} + \frac{\mu^2}{2Q\zeta_{p,1}^2\zeta_{p,2}^2}} \stackrel{H_1}{\gtrless} \Delta \quad (16)$$

$$\text{其中, } \Delta = \Lambda \cdot \frac{\sqrt{\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2}}{\sqrt{\zeta_{p,1}^2\zeta_{p,2}^2}}.$$

将式(16)两端取对数可得

$$\begin{aligned} \frac{\mu^2(\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2) - (\mu - Q\beta_{p,1}\beta_{p,2})^2\zeta_{p,1}^2\zeta_{p,2}^2}{2Q \cdot \zeta_{p,1}^2\zeta_{p,2}^2(\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2)} &\stackrel{H_1}{\gtrless} \ln \Delta \\ (\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2) \ln \Delta - \left( \frac{Q\beta_{p,1}\beta_{p,2}\zeta_{p,1}\zeta_{p,2}}{\zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2} \right)^2 \\ (\zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2 - \zeta_{p,1}^2\zeta_{p,2}^2). \end{aligned} \quad (17)$$

由式(18)可以得到, 在假设  $H_0$  条件下, 检测统计量  $l$  服从自由度为 1, 非中心参数为  $D^2$  的非中心卡

化简式(17)可以得到

$$l = (\mu + D)^2 \stackrel{H_1}{\gtrless} \eta \quad (18)$$

$$\text{其中, } D = \frac{Q\beta_{p,1}\beta_{p,2}\zeta_{p,1}\zeta_{p,2}}{\zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2}, \eta = 2Q\zeta_{p,1}\zeta_{p,2}(\zeta_{p,1}^2\zeta_{p,2}^2$$

方分布; 在假设  $H_1$  条件下, 检测统计量  $l$  服从自由度为 1, 非中心参数为  $(Q\beta_{p,1}\beta_{p,2} + D)^2$  的非中心卡方分布。对于自由度为 1 的非中心卡方分布, 可以根据正态分布的性质得到卡方分布的累积分布函数

$$F(l|H_0) = \frac{1}{2} \left[ \operatorname{erf} \left( \frac{\sqrt{l} - D}{\sqrt{2Q\zeta_{p,1}^2\zeta_{p,2}^2}} \right) - \operatorname{erf} \left( \frac{-\sqrt{l} - D}{\sqrt{2Q\zeta_{p,1}^2\zeta_{p,2}^2}} \right) \right] \quad (19)$$

$$\begin{aligned} F(l|H_1) &= \frac{1}{2} \left[ \operatorname{erf} \left( \frac{\sqrt{l} - Q\beta_{p,1}\beta_{p,2} - D}{\sqrt{2Q(\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2)}} \right) - \operatorname{erf} \left( \frac{-\sqrt{l} - Q\beta_{p,1}\beta_{p,2} - D}{\sqrt{2Q(\zeta_{p,1}^2\zeta_{p,2}^2 + \zeta_{p,1}^2\beta_{p,2}^2 + \zeta_{p,2}^2\beta_{p,1}^2)}} \right) \right] \end{aligned} \quad (20)$$

其中,  $\operatorname{erf}(\cdot)$  代表误差函数, 表示为  $\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-z^2} dz$ 。

根据 Neyman-Pearson 准则, 在恒定的虚警概率  $P(H_1|H_0) = P_{fa}$  下, 式(18)中的检测阈值  $\eta$  可由式(20)得到

$$\eta = F^{-1}(1 - P_{fa}|H_0) \quad (21)$$

二元假设检验中的参数  $\sigma_{w,1}$  和  $\sigma_{w,2}$  分别为节点雷达 1 和节点雷达 2 接收机中的热噪声功率, 可以在节点雷达锁闭期得到估计值  $\hat{\sigma}_{w,1}$  和  $\hat{\sigma}_{w,2}$ 。由于节点雷达 1 和节点雷达 2 中接收到的信号幅度序列可以分别为  $\mathbf{A}_p^1 = [\gamma_{p,1}^1, \gamma_{p,1}^2, \dots, \gamma_{p,1}^Q]^T$ ,  $\mathbf{A}_p^2 = [\gamma_{p,2}^1, \gamma_{p,2}^2, \dots, \gamma_{p,2}^Q]^T$ , 根据极大似然估计可以得到

$$\left. \begin{aligned} \hat{\beta}_{p,1} &= \frac{1}{Q} \sum_{i=1}^Q \gamma_{p,1}^i \\ \hat{\beta}_{p,2} &= \frac{1}{Q} \sum_{i=1}^Q \gamma_{p,2}^i \end{aligned} \right\} \quad (22)$$

$$\left. \begin{aligned} \hat{\sigma}_{p,1} &= \frac{1}{Q} \sum_{i=1}^Q (\gamma_{p,1}^i - \hat{\beta}_{p,1})^2 - \hat{\sigma}_{w,1}^2 \\ \hat{\sigma}_{p,2} &= \frac{1}{Q} \sum_{i=1}^Q (\gamma_{p,2}^i - \hat{\beta}_{p,2})^2 - \hat{\sigma}_{w,2}^2 \end{aligned} \right\} \quad (23)$$

则可以得到  $\hat{\zeta}_{p,1}^2 = \hat{\sigma}_{p,1}^2 + \hat{\sigma}_{w,1}^2$  和  $\hat{\zeta}_{p,2}^2 = \hat{\sigma}_{p,2}^2 + \hat{\sigma}_{w,2}^2$ 。

通过对不同节点雷达接收到的目标回波信号进行预处理和相关性参数估计, 进行相关性检测, 实现对欺骗干扰的识别。基于相关性的多雷达系统欺骗干扰识别算法的算法步骤如图 2 所示。

步骤 1 信号预处理。对节点雷达 1 和节点雷达 2 接受到的目标回波信号进行预处理得到目标信号幅度序列;

步骤 2 计算相关性度量和参数估计。根据式(13)计算相关性度量  $\mu$  以及根据式(22)和式(23)进行参数估计得到  $\hat{\beta}_{p,1}$ ,  $\hat{\beta}_{p,2}$ ,  $\hat{\sigma}_{p,1}$  和  $\hat{\sigma}_{p,2}$ ;

步骤 3 检测统计量  $l$ 。利用得到的相关性度量和估计所得参数计算检测统计量  $l$ ;

步骤 4 检测阈值。根据给定的虚警概率和式(21)确定检测阈值;

步骤 5 检测判决。根据式(18)进行检测判决, 实现欺骗干扰识别。

## 5 仿真实验与分析

为了验证该算法的有效性, 以由两部节点雷达和融合中心组成的多雷达系统为例进行性能仿真实验。该多雷达系统的探测空域中存在 1 个真实目标, 目标携带自卫式干扰机, 两部节点雷达的检测

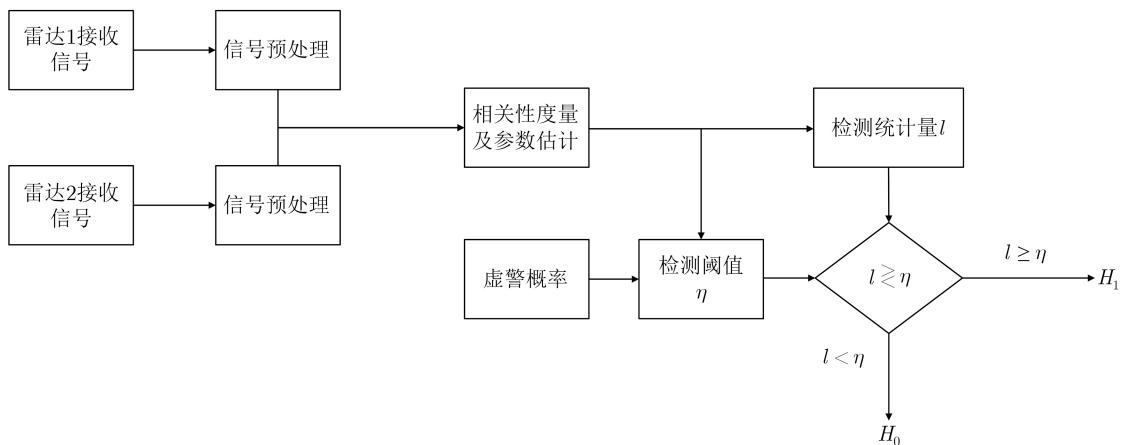


图 2 基于相关性的欺骗干扰检测识别算法流程图

概率均为1。实验设置不同条件下的仿真场景，验证不同仿真条件下的检测识别性能。

设置干信比JSR=3 dB, 虚警概率 $P_{fa}=10^{-3}$ 时, 一个CPI内含有不同脉冲数目场景下, 欺骗干扰检测识别概率随信噪比(SNR)的变化如图3所示。

从图3的实验结果可以看出, 当脉冲数目一定时, 随着SNR的增加, 欺骗干扰的检测识别性能也在提升。在该仿真实验设置的不同脉冲数目下, 当 $SNR > 9$  dB时, 欺骗干扰检测识别概率都能达到90%以上。在相同SNR下, 脉冲数目越多, 欺骗干扰的检测识别性能越高, 这是由于1个CPI内含有的脉冲数目越多, 相关性度量等参数的估计更加有效, 对欺骗干扰的检测识别性能越好。

设置干信比JSR=3 dB, 1个CPI内含有的脉冲数目恒定为50时, 在不同的虚警概率下, 欺骗干扰检测识别概率随SNR的变化如图4所示。

从图4的实验结果可以看出, 当虚警概率一定时, 随着SNR的增加, 欺骗干扰的检测识别性能也在提升, 当 $SNR > 9$  dB时, 欺骗干扰检测识别概率达到90%。在相同SNR下, 随着虚警概率减小, 欺骗干扰的检测识别性能下降, 这是由于虚警概率越小, 检测阈值会越大, 使得检测统计量不能过阈值, 欺骗干扰的检测识别性能就会下降。

设置虚警概率 $P_{fa}=10^{-3}$ , 1个CPI内含有的脉

冲数目恒定为50时, 在不同JSR下, 欺骗干扰的检测识别概率随SNR的变化如图5所示。

从图5的实验结果可以看出, 当JSR一定时, 随着SNR的增加, 欺骗干扰的检测识别性能也在提升。在仿真实验设置的不同JSR下, 当SNR大于9 dB时, 欺骗干扰检测识别概率都超过90%。在相同SNR下, 随着JSR增大, 欺骗干扰的检测识别性能越高, 这是由于JSR越大, 使得二元假设检验下的检测统计量差异增大, 欺骗干扰的检测识别性能就会越好。

设置虚警概率 $P_{fa}=10^{-3}$ , 干信比JSR=3 dB, 1个CPI内含有的脉冲数目恒定为50时, 节点雷达数目不同时, 欺骗干扰的检测识别概率随SNR的变化如图6所示。

从图6的实验结果可以看出, 当节点雷达数目一定时, 随着SNR的增加, 欺骗干扰的检测识别性能也在提升。在仿真实验设置的不同节点雷达数目下, 当 $SNR > 9$  dB时, 欺骗干扰检测识别概率都超过90%。节点雷达数目越多, 雷达测得的目标之间相关性的判决更加准确, 欺骗干扰的检测识别性能就会越好。

鉴于现有检测雷达拖引欺骗干扰的参考文献不多, 而文献[25]提出了一种基于拟合优度的AD检测算法可以实现检测未知参数的欺骗性干扰, 且在

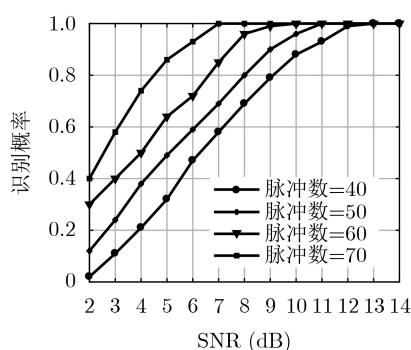


图3 不同脉冲数目下欺骗干扰目标检测识别概率

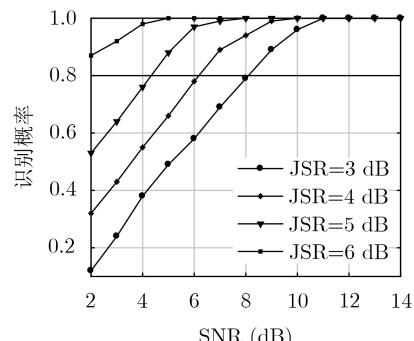


图5 不同干信比下欺骗干扰目标检测识别概率

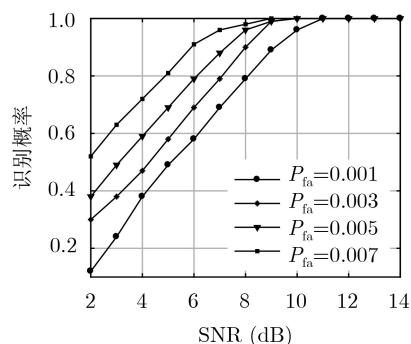


图4 不同虚警概率下欺骗干扰目标检测识别概率

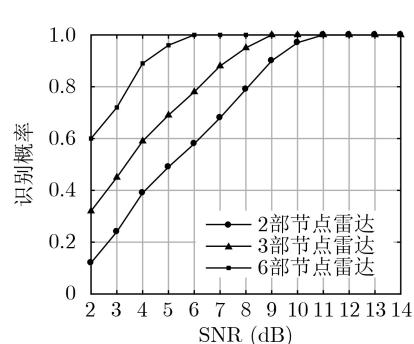


图6 不同节点雷达数目下欺骗干扰目标检测识别概率

SNR大于5 dB和JSR为6 dB时, 欺骗干扰识别概率优于90%, 具有较好的识别性能。因此, 本文与该算法进行了性能比较。通过设置与文献[25]相同的仿真场景, 比较本文算法与AD算法的欺骗干扰识别性能, 得到的识别概率曲线如图7所示。

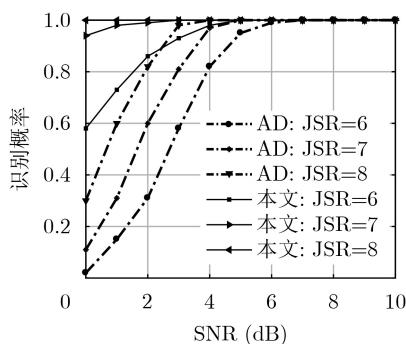


图 7 本文算法与AD检测算法的性能比较

从图7的实验结果可以看出, 当JSR为6 dB时, 本文采用的算法达到90%识别率时较AD检测算法性能平均提高了2 dB, 在JSR为7 dB时平均提高4 dB, 在JSR为8 dB时平均提高5 dB。本文算法的检测识别概率平均比AD检测算法的识别概率高18.63%, 可以发现本文的基于相关性的欺骗干扰识别算法优于基于拟合优度的AD检测识别算法。

## 6 结论

本文利用真实目标和欺骗干扰间的相关性差异, 提出了基于相关性的多基地雷达系统欺骗干扰识别算法。通过对不同节点雷达接收到的回波信号幅度序列进行相关性度量及参数估计, 构建检验统计量, 在给定的虚警概率下实现欺骗干扰的识别。通过仿真实验表明, 该算法在较低的SNR下具有良好的检测识别性能, 从而验证了本文算法的有效性。

## 参 考 文 献

- [1] ZHOU Chao, LIU Quanhua, and CHEN Xinliang. Parameter estimation and suppression for DRFM-based interrupted sampling repeater jammer[J]. *IET Radar, Sonar & Navigation*, 2018, 12(1): 56–63. doi: [10.1049/iet-rsn.2017.0114](https://doi.org/10.1049/iet-rsn.2017.0114).
- [2] LIU Zhen, SUI Jinping, WEI Zhenhua, et al. A sparse-driven anti-velocity deception jamming strategy based on pulse-Doppler radar with random pulse initial phases[J]. *Sensors*, 2018, 18(4): 1249. doi: [10.3390/s18041249](https://doi.org/10.3390/s18041249).
- [3] LIU Jieyi, ZHANG Linrang, ZHAO Shanshan, et al. Correlation characteristic analysis in diversity multiple-input multiple-output radar[J]. *Electronics Letters*, 2017, 53(5): 349–351. doi: [10.1049/el.2016.3535](https://doi.org/10.1049/el.2016.3535).
- [4] HUANG Can, CHEN Zhuming, and DUAN Rui. Novel Discrimination Algorithm for Deceptive Jamming in Polarimetric Radar[M]. Berlin, Germany, 2013: 359–365. doi: [10.1007/978-3-642-34528-9\\_38](https://doi.org/10.1007/978-3-642-34528-9_38).
- [5] ZHANG Zhaojian, XIE Junwei, SHENG Chuan, et al. Deceptive jamming discrimination based on range-angle localization of a frequency diverse array[J]. *Frontiers of Information Technology & Electronic Engineering*, 2017, 18(9): 1437–1446.
- [6] 王珊珊, 刘峰, 谢荣, 等. 有源欺骗干扰环境下的DOA估计[J]. 电子与信息学报, 2019, 41(5): 1040–1046. doi: [10.11999/JEIT180488](https://doi.org/10.11999/JEIT180488).
- [7] WANG Shanshan, LIU Zheng, XIE Rong, et al. DOA estimation under active deception jamming environment[J]. *Journal of Electronics & Information Technology*, 2019, 41(5): 1040–1046. doi: [10.11999/JEIT180488](https://doi.org/10.11999/JEIT180488).
- [8] RAO Bin, XIAO Shunping, and WANG Xuesong. Joint tracking and discrimination of exoatmospheric active decoys using nine-dimensional parameter-augmented EKF[J]. *Signal Processing*, 2011, 91(10): 2247–2258. doi: [10.1016/j.sigpro.2011.04.005](https://doi.org/10.1016/j.sigpro.2011.04.005).
- [9] GRIFFITHS H. Multistatic, MIMO and networked radar: The future of radar sensors?[C]. The 7th European Radar Conference, Paris, France, 2010: 81–84.
- [10] BUTT F A, NAQVI I H, and NAJAM A I. Radar ECCM against deception jamming: A novel approach using bi-static and mono-static radars[C]. The 15th International Multitopic Conference (INMIC), Islamabad, Pakistan, 2012: 137–141. doi: [10.1109/INMIC.2012.6511482](https://doi.org/10.1109/INMIC.2012.6511482).
- [11] ZHAO Shanshan and LIU Ziwei. Deception parameter estimation and discrimination in distributed multiple-radar architectures[J]. *IEEE Sensors Journal*, 2017, 17(19): 6322–6330. doi: [10.1109/JSEN.2017.2737654](https://doi.org/10.1109/JSEN.2017.2737654).
- [12] ABDALLA A, YUAN Zhao, and TANG Bin. ECCM schemes in netted radar system based on temporal pulse diversity[J]. *Journal of Systems Engineering and Electronics*, 2016, 27(5): 1001–1009. doi: [10.21629/JSEE.2016.05.08](https://doi.org/10.21629/JSEE.2016.05.08).
- [13] ALAMOUTI S M. A simple transmit diversity technique for wireless communications[J]. *IEEE Journal on Selected Areas in Communications*, 1998, 16(8): 1451–1458. doi: [10.1109/49.730453](https://doi.org/10.1109/49.730453).
- [14] AKHTAR J. Orthogonal block coded ECCM schemes against repeat radar jammers[J]. *IEEE Transactions on Aerospace and Electronic Systems*, 2009, 45(3): 1218–1226. doi: [10.1109/TAES.2009.5259195](https://doi.org/10.1109/TAES.2009.5259195).
- [15] ZHAO Shanshan, LIU Nan, ZHANG Linrang, et al. Discrimination of deception targets in multistatic radar based on clustering analysis[J]. *IEEE Sensors Journal*, 2016, 16(8): 2500–2508. doi: [10.1109/JSEN.2016.2516000](https://doi.org/10.1109/JSEN.2016.2516000).

- [15] ABDALLA A, SHOKRALLAH A M G, YUAN Z, et al. Deceptive jamming suppression in multistatic radar based on coherent clustering[J]. *Journal of Systems Engineering and Electronics*, 2018, 29(2): 269–277. doi: [10.21629/JSEE.2018.02.07](https://doi.org/10.21629/JSEE.2018.02.07).
- [16] LAN Lan, LIAO Guisheng, XU Jingwei, et al. Suppression approach to main-beam deceptive jamming in FDA-MIMO radar using nonhomogeneous sample detection[J]. *IEEE Access*, 2018, 6: 34582–34597. doi: [10.1109/ACCESS.2018.2850816](https://doi.org/10.1109/ACCESS.2018.2850816).
- [17] HUANG Datong, CUI Guolong, GE Mengmeng, et al. A suppression method against range deception jamming based on homologous localisation test[J]. *The Journal of Engineering*, 2019, 2019(20): 6961–6965. doi: [10.1049/joe.2019.0474](https://doi.org/10.1049/joe.2019.0474).
- [18] 卢云龙, 李明, 陈洪猛, 等. 基于奇异谱分析的抗数字射频存储距离波门拖引干扰[J]. 电子与信息学报, 2016, 38(3): 600–606. doi: [10.11999/JEIT150550](https://doi.org/10.11999/JEIT150550).
- LU Yunlong, LI Ming, CHEN Hongmeng, et al. Countering DRFM range gate pull-off jamming based on singular spectrum analysis[J]. *Journal of Electronics & Information Technology*, 2016, 38(3): 600–606. doi: [10.11999/JEIT150550](https://doi.org/10.11999/JEIT150550).
- [19] 全英汇, 陈侠达, 阮锋, 等. 一种捷变频联合Hough变换的抗密集假目标干扰算法[J]. 电子与信息学报, 2019, 41(11): 2639–2645. doi: [10.11999/JEIT190010](https://doi.org/10.11999/JEIT190010).
- QUAN Yinghui, CHEN Xiada, RUAN Feng, et al. An anti-dense false target jamming algorithm based on agile frequency joint Hough transform[J]. *Journal of Electronics & Information Technology*, 2019, 41(11): 2639–2645. doi: [10.11999/JEIT190010](https://doi.org/10.11999/JEIT190010).
- [20] ZHAO Shanshan, ZHANG Linrang, ZHOU Yu, et al. Study of multistatic radar against false targets jamming using spatial scattering properties[C]. 2014 IEEE International Conference on Computer and Information Technology, Xi'an, China, 2014: 129–133. doi: [10.1109/CIT.2014.132](https://doi.org/10.1109/CIT.2014.132).
- [21] LI Qiang, ZHANG Linrang, ZHOU Yu, et al. Discrimination of active false targets based on Hermitian distance for distributed multiple-radar architectures[J]. *IEEE Access*, 2019, 7: 71872–71883. doi: [10.1109/ACCESS.2019.2920365](https://doi.org/10.1109/ACCESS.2019.2920365).
- [22] LI Qiang, ZHANG Linrang, ZHOU Yu, et al. Hermitian distance-based method to discriminate physical targets and active false targets in a distributed multiple-radar architecture[J]. *IEEE Sensors Journal*, 2019, 19(22): 10432–10442. doi: [10.1109/JSEN.2019.2926414](https://doi.org/10.1109/JSEN.2019.2926414).
- [23] ZHOU Shenghua, LIU Hongwei, ZHAO Yongbo, et al. Target spatial and frequency scattering diversity property for diversity MIMO radar[J]. *Signal Processing*, 2011, 91(2): 269–276. doi: [10.1016/j.sigpro.2010.07.004](https://doi.org/10.1016/j.sigpro.2010.07.004).
- [24] ZHANG Qiliang, GAO Feifei, SUN Qing, et al. Single source self-screen jamming elimination and target detection for distributed dual antennas radar system[J]. *China Communications*, 2017, 14(11): 112–125. doi: [10.1109/CC.2017.8233655](https://doi.org/10.1109/CC.2017.8233655).
- [25] XIAO Tian. Radar deceptive jamming detection based on goodness-of-fit testing[J]. *Journal of Information & Computational Science*, 2012, 9(13): 3839–3847.

孙闽红: 男, 1974年生, 教授, 研究方向为雷达通信信号处理及抗干扰。

丁辰伟: 男, 1995年生, 硕士生, 研究方向为信号与信息处理。

张树奇: 男, 1993年生, 硕士生, 研究方向为信号与信息处理。

鲁加战: 男, 1987年生, 工程师, 研究方向为信号处理。

邵鹏飞: 男, 1994年生, 助理工程师, 研究方向为信号分析与处理。

责任编辑: 马秀强