

基于干扰机功率放大器特性的有源欺骗干扰识别方法

唐娟^{1,2} 冉智¹ 赵源¹ 唐斌¹

(1. 电子科技大学电子工程学院, 成都, 611731; 2. 国网内江供电公司信通分公司, 内江, 641100)

摘要: 针对对空情报雷达的有源欺骗干扰与目标回波高度相似, 导致识别有源欺骗干扰难度较大的现状, 提出了一种基于干扰机功率放大器非线性特性的有源欺骗干扰识别方法。提取分段自相关最大值方差和奇异谱熵两个特征, 用这两个特征联合识别有源欺骗干扰。仿真结果表明, 在信噪比大于等于 8 dB 时, 欺骗干扰识别概率能达到 100%, 能够满足实际工程需要。

关键词: 有源欺骗干扰识别; 功率放大器; 特征提取

中图分类号: TP391 **文献标志码:** A

Active Deceptive Jamming Identification Based on Jammer's Power Amplifier Character

Tang Juan^{1,2}, Ran Zhi¹, Zhao Yuan¹, Tang Bin¹

(1. College of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China;
2. State Grid Neijiang Power Supply Company Information & Telecommunication Branch, Neijiang, 641100, China)

Abstract: The high similarity between active deceptive jamming and echo of air surveillance radar results in the difficulty in identifying the active deception jamming. Based on jammer's power amplifier nonlinear characters, a new active deceptive jamming identification method is proposed by extracting piecewise autocorrelation maximum variance and singular value spectral entropy of radar receiving signal. Simulation shows that the recognition probability for deceptive jamming is 100% with signal-to-noise ratio of 8 dB, meeting the actual engineering needs.

Key words: active deceptive jamming recognition; power amplifier; feature extraction

引 言

雷达电子战的源头能够追溯至第二次世界大战。在二战期间, 双方战机损失很严重, 为了降低损失, 雷达就运用到各种各样的军事装备上, 这样就产生了雷达电子战。在以后的多次战争中, 雷达电子战都发挥了至关重要的作用, 所以雷达电子战不仅在当前而且在未来的各种军事战争中都将发挥至关重要的作用。数字储频技术的发展使对空情报雷达有源欺骗干扰与目标回波越来越相似, 研究有源欺骗干扰与目标回波的差异显得尤为重要。目前国内外针对有源欺骗干扰识别方法的研究主要集中在特征提取上。Berge S D^[1] 系统地分析了在数字射频频存储器(Digital radio frequency memory, DRFM) 数字特性的影响下, 拖引时延函数由理想情况下的线性函数改变为阶梯形函数, 并研究了此时线性距离拖引

干扰(Range gate pull-off, RGPO)信号的时域模型和频域特征。Greco M等^[2]在此基础上,进一步分析了由DRFM产生的RGPO干扰信号受DRFM相位量化及时延函数离散化后在频域上的特征,得出时延量化给干扰信号带来的影响与相位量化的影响相比可以忽略,尤其在相位量化位数较少时。然而,随着DRFM量化位数的提高,量化所带来的误差越来越小,只分析量化所带来的误差显然不能满足实际需求。李建勋^[3-6]研究了有源欺骗干扰的高阶累积量与双谱特征,在一定程度上能区分有源欺骗干扰和目标回波。粘朋雷^[7]提出了基于短时分数阶傅里叶变换的欺骗干扰识别方法,但此方法仅针对线性调频脉冲压缩引信。闫琰^[8]提出了基于多维特征处理识别欺骗干扰,在时域、频域、小波域和双谱域提取特征分析了有源欺骗干扰与目标回波,但未对这些特征的物理意义给出说明。甘一鸣^[9]提出了基于射频功放建模的欺骗干扰识别方法,利用Hammerstein模型对射频功放进行非线性建模,用模型参数作为提取的特征向量,但其只考虑了功放的非线性,没有考虑其记忆性。郭波^[10]提出了短时滑窗方式的分数阶傅里叶滤波方法,提供一种低信噪比情况下线性调频信号的检测准则,但该方法只能用于线性调频信号。祝宏^[11]研究了基于粒子滤波抗欺骗干扰,但该算法运算量比较大,不易工程实现。田晓^[12]分析了干扰机的指纹特征,研究了基于子空间的特征提取方法。因此,基于雷达有源欺骗干扰与目标回波之间差异的干扰识别方法可为后续干扰抑制提供先验信息,算法的有效性显得尤为重要。

本文首先给出基于干扰机功率放大器特性的有源欺骗干扰模型,然后对欺骗干扰与目标回波的分段自相关最大值方差和奇异谱熵两个特征进行分析比较。在此基础上,研究可以用于识别有源欺骗干扰的特征提取方法,最后仿真验证了所提取特征的有效性。

1 基于干扰机功率放大器特性的有源欺骗干扰模型

当对空情报雷达工作在跟踪状态时,干扰机在产生有源欺骗干扰时一般仅进行距离调制,通过转发截获的雷达信号形成干扰。设在没有噪声的情况下,干扰机截获到的雷达单次扫描期间发射的线性调频信号的解析形式为

$$x(n) = A \exp(j2\pi f_0 n + jk\pi n^2) \quad (1)$$

式中: A 为发射信号幅度, f_0 为发射信号中心频率, k 为调频斜率。

由文献[12]可知,在干扰机的模块电路中,功率放大器引入的非线性失真是所有器件中最大的。假定干扰机的其他模块都工作在理想情况,仅研究基于干扰机功率放大器特性的有源欺骗干扰模型,提取欺骗干扰的细微特征,用于欺骗式干扰的识别。

设干扰机功率放大器的输入和输出信号分别为 $x(n)$ 和 $y(n)$,由文献[13]可知,工作在丙类的干扰机功率放大器的离散记忆多项式模型可以表示为

$$y(n) = \sum_{k=1}^p \sum_{m=0}^q c_{km} x(n-m) |x(n-m)|^{k-1} \quad (2)$$

式中: p 和 q 分别为记忆多项式的阶次和记忆深度, c_{km} 为记忆多项式的复系数, $|x(n-m)|$ 为 $x(n-m)$ 的模。一旦记忆多项式的阶次和记忆深度确定,确定的功率放大器其 c_{km} 也就相应确定。

将干扰机接收到的雷达发射信号通过功率放大器,可以得到放大器的输出信号为

$$y(n) = \sum_{k=1}^p \sum_{m=0}^q c_{km} \exp(j\omega_0(n-m) + jk\pi(n-m)^2) A^k = x(n) \sum_{k=1}^p \sum_{m=0}^q c_{km} \exp(jk\pi m^2 - j\omega_0 m - j2\pi kmn) A^{k-1} \quad (3)$$

则雷达接收机接收到的欺骗干扰信号为

$$y_j(n) = A_j y(n) \otimes \delta(n - N_j) \quad (4)$$

式中: A_j 为干扰机电压放大器的放大倍数, N_j 为干扰信号延时产生的点数, \otimes 表示卷积。

对空情报雷达单次扫描期间接收机目标回波信号模型为

$$s(n) = A_r x(n) \exp(j2\pi f_r n) \otimes \delta(n - N_r) \quad (5)$$

式中: N_r 为目标回波延时对应的点数, f_r 为目标的多普勒频率, A_r 为目标回波幅度的衰减量。

由式(3)可以看出, 雷达有源欺骗干扰是多个频率很小的正弦信号与发射信号相乘之后的叠加, 且正弦信号的频率和幅度分别与干扰机功率放大器的记忆项、阶次和系数有关系, 这使有源欺骗干扰带有放大器的细微特征, 通过分析这些细微特征, 可为区分有源欺骗干扰和目标回波提供依据。

2 欺骗干扰与目标回波特征

2.1 分段自相关最大值方差

分段自相关最大值方差能反映信号时域能量分布的均衡性, 信号时域能量分布越均匀, 其值越小, 反之越大。由第1节分析可知, 欺骗干扰携带了干扰机的细微特征, 使得欺骗干扰时域能量分布不均匀, 所以可以通过分析欺骗干扰和目标回波在分段自相关最大值方差的差异来区分两者。

设目标回波信号脉内总长度为 N , 用长度为 M 的矩形窗将雷达接收的目标回波信号分为 L 段, 且 $N = M \times L$, 则目标回波的第 i 段数据为

$$s_r^i(n) = A_r x(n + (i-1)M) \exp(j\omega_r(n + (i-1)M)) \otimes \delta(n + (i-1)M - N_r) = A_r x(n + (i-1)M - N_r) \exp(j\omega_r(n + (i-1)M - N_r)) \quad (6)$$

式中 $1 \leq i \leq L$ 。令 $k_i(n) = n + (i-1)M - N_r$, 则有

$$s_r^i(n) = A_r x(k_i(n)) \exp(j\omega_r k_i(n)) \quad (7)$$

则回波信号每段的自相关最大值为

$$R_r^i(0) = \frac{1}{M} \sum_{n=0}^{M-1} s_r^i(n) (s_r^i(n))^* = \frac{1}{M} \sum_{n=0}^{M-1} A_r^2 x(k_i(n)) \exp(j\omega_r k_i(n)) (x(k_i(n))^* \exp(-j\omega_r k_i(n))) = A_r^2 A^2 \quad (8)$$

由式(8)可以看出, 目标回波分段的每一段自相关最大值都是恒定的, 且与目标回波幅度相关, 说明目标回波在时域上能量分布均匀, 则其分段自相关最大值方差应该为 0。

同理, 将脉内长度为 N 的欺骗干扰信号分成 L 段, 每一段长度为 M , 且 $N = M \times L$, 则欺骗干扰第 i 段信号为

$$y_j^i(n) = A_j x(f_i(n)) \sum_{k=1}^p \sum_{m=0}^q c_{km} \exp(jk\pi m^2 - j2\pi km f_i(n)) A^{k-1} \quad (9)$$

式中 $f_i(n) = n + (i-1)M - N_j$, 则其自相关最大值为

$$\begin{aligned} R_j^i(0) &= A_j^2 \frac{1}{M} \sum_{n=0}^{M-1} \left\{ x(f_i(n)) \sum_{k_1=1}^p \sum_{m_1=0}^q c_{k_1 m_1} \exp(jk_1 \pi m_1^2 - j2k_1 \pi m_1 f_i(n)) A^{k_1-1} \right\} \cdot \\ &\quad \left\{ x(f_i(n)) \sum_{k=1}^p \sum_{m=0}^q c_{km} \exp(jk\pi m^2 - j2k\pi m f_i(n)) A^{k-1} \right\}^* = \\ &= \frac{A^2 A_j^2}{M} \sum_{n=0}^{M-1} \left\{ \sum_{k_1=1}^p \sum_{m_1=0}^q c_{k_1 m_1} \exp(jk_1 \pi m_1^2 - j2k_1 \pi m_1 f_i(n)) A^{k_1-1} \right\} \cdot \\ &\quad \left\{ \sum_{k=1}^p \sum_{m=0}^q c_{km} \exp(jk\pi m^2 - j\omega_j m - j2k\pi m f_i(n)) A^{k-1} \right\}^* \end{aligned} \quad (10)$$

对式(10), 当 $k = k_1, m = m_1$ 时, 产生平方

$$A^2 A_j^2 \sum_{k=1}^p \sum_{m=0}^q c_{km}^2 A^{2k-2} \quad (11)$$

对于确定的干扰机, 式(11)为一常数, 与分段无关。

当 $k_1 m_1 \neq km$ 时, 产生交叉项

$$\frac{A^2 A_j^2}{M} \sum_{n=0}^{M-1} \left\{ \sum_{s=1}^{c_{pvq}} c_s \exp(j\vartheta_s - j2\pi s f_s(n) A^s) \right\} \quad (12)$$

由式(11,12)知,欺骗式干扰的自相关最大值为

$$R_j^i(0) = \begin{cases} A^2 A_j^2 \sum_{k=1}^p \sum_{m=0}^q c_{km}^2 A^{2k-2} & k = k_1, m = m_1 \\ \frac{1}{M} \sum_{n=0}^{M-1} \left\{ \sum_{s=1}^{c_{pvq}} c_s \exp(j\vartheta_s - j2\pi s f_s(n) (AA_j)^s) \right\} & k_1 m_1 \neq km \end{cases} \quad (13)$$

由式(13)可以看出,有源欺骗干扰的自相关最大值当 $k_1 m_1 \neq km$ 时会产生交叉项,该交叉项与分段有关,导致有源欺骗干扰分段每一段的自相关最大值不同。这样,各段自相关最大值的方差应该大于0,而目标回波各段自相关最大值的方差应该等于0。所以可以用自相关最大值方差来区分欺骗干扰和目标回波。

因此定义自相关最大值方差 v 为

$$v = \text{var} \left(\sum_{i=1}^L R_i(0) \right) \quad (14)$$

式中:var表示求各段自相关最大值的方差。

2.2 奇异谱熵

奇异谱信息熵可以表征信号所携带信息量的多少,信号所携带的信息越多,奇异谱信息熵值越大,说明信号越复杂。由于欺骗干扰携带了干扰机功率放大器的微弱信息,导致其携带的信息要比目标回波多,所以可以用奇异谱信息熵来区分目标回波和有源欺骗干扰。与2.1节类似,将雷达接收机接收的长度为 N 的脉内信号分成 L 段,每段长度为 M ,将这 L 段数据形成 $L \times M$ 维矩阵 \mathbf{C} ,求得 A 的奇异值谱 $\sigma_i (i=1, 2, \dots, k, k \leq L)$,奇异谱中非零特征值 σ_i 与信号频率分布情况有很大的联系,其维数越高,表示分布越复杂,维数越低,表示分布越简单。定义时域空间信息的奇异谱熵为

$$H = - \sum_{i=1}^k p_i \log p_i \quad (15)$$

式中: $p_i = \sigma_i / \sum_{i=1}^k \sigma_i$ 为单个奇异值在总奇异值中所占的比例。

由式(3)知,雷达有源欺骗干扰为多个频率很小的正弦信号与发射信号相乘之后的叠加,且这些正弦信号与干扰机功率放大器相关,这使有源欺骗干扰带有放大器的细微特征,所以雷达有源欺骗干扰携带的信息比目标回波丰富,其奇异谱熵比目标回波大,因此可以用奇异谱熵 H 区分目标回波和欺骗干扰。

2.3 特征组合

通过对有源欺骗干扰和目标回波的分析,定义分段自相关最大值方差和奇异谱熵这两组特征因子^[14],从此实现有源欺骗干扰和目标回波信号的识别。

由2.1节和2.2节定义,利用回波信号与欺骗干扰信号在 v 和 H 上的差异,用这两个特征联合来区分有源欺骗干扰与目标回波。设接收信号的脉内最大值为 ϵ ,定义联合特征 $\mu = \lambda \frac{v}{\max(\epsilon)^2} + (1 - \lambda)H$,其中 λ 用来控制 v 和 H 所占的权重且 $0 \leq \lambda \leq 1$ ^[15]。其算法流程如图1所示。图1中将雷达接收的脉内长度为 N 的信号分为 L 段,每段长度为 M ,用 L 段数据构造 $L \times M$ 维矩阵 \mathbf{C} ,求 A 的奇异谱,然后求其奇异谱熵 H ,同时对 L 段数据求自相关最大值,然后求 L 段自相关最大值的方差 v ,用 v 和 H 构造联合参数 μ ,用该参数实现目标回波与欺骗式干扰的识别。

3 仿真验证

设雷达工作在 L 波段,载频为 1 500 MHz,发射的线性调频信号带宽为 10 MHz,脉宽为 5 μs ,采样

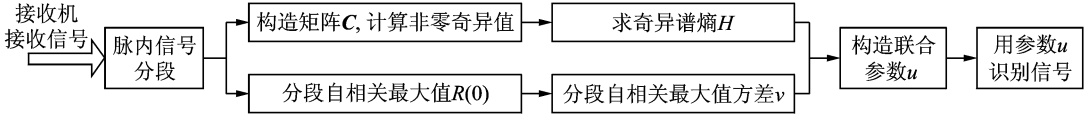


图1 算法流程

Fig. 1 Algorithmic flow

率为 100 MHz, 脉冲重复周期为 $500 \mu\text{s}$, 取 $5 \text{ dB} \leq \text{SNR} \leq 20 \text{ dB}$, 此信噪比为目标回波(或者欺骗干扰)与噪声的功率之比。

根据文献[13], 综合计算量与相似性考虑, 取功率放大器的记忆多项式模型阶数为 3, 记忆深度为 2, 根据某实测数据得到功率放大器记忆多项式模型参数, 用该模型仿真提取特征, 当欺骗干扰和目标回波信号不重叠时, 其分段自相关最大值方差和奇异谱熵值结果分别如图 2, 3 所示。

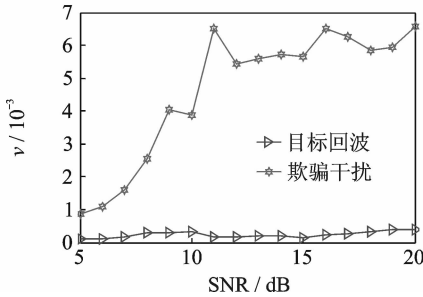


图2 分段自相关最大值方差

Fig. 2 Segmentation autocorrelation maximum variance

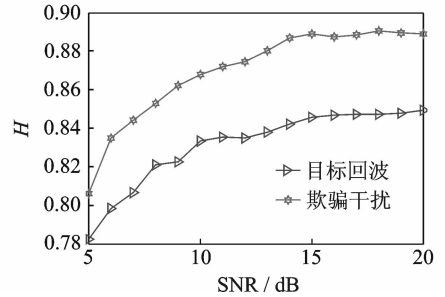


图3 奇异谱熵

Fig. 3 Singular spectrum entropy

由图 2 可以看出, 目标回波的分段自相关最大值方差在零附近, 而有源欺骗干扰的分段自相关最大值方差大于零, 两者有明显的区别。由图 3 可以看出, 奇异谱熵也能在一定程度上区分欺骗式干扰和目标回波, 而且随着信噪比的提高, 两者的差异趋向平稳, 所以可以通过这两个特征联合来区分目标回波和有源欺骗干扰。当目标回波和欺骗干扰重叠 30% 时, 其分段自相关最大值方差和奇异谱熵结果分别如图 4, 5 所示。

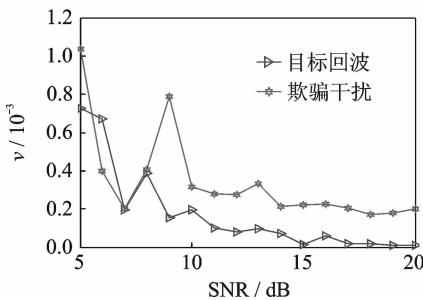


图4 分段自相关最大值方差

Fig. 4 Segmentation autocorrelation maximum variance

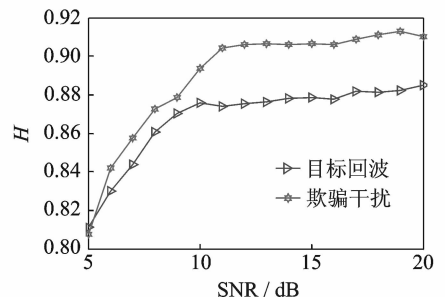


图5 奇异谱熵

Fig. 5 Singular spectrum entropy

当目标回波和欺骗干扰重叠 50% 时, 其分段自相关最大值方差和奇异谱熵结果分别如图 6, 7 所示。

由图 4~7 可以看出, 随着目标回波和欺骗干扰重叠部分的增多, 分段自相关最大值方差和奇异谱

熵区分目标回波和欺骗干扰的性能明显下降。这是因为当目标回波和欺骗干扰重叠时,可利用的信息变少,使得欺骗干扰所携带的一部分放大器的微弱特征丢失,导致欺骗干扰和目标回波更加相似,所以两个特征的性能下降。

利用上述两个特征联合来区分有源欺骗干扰和目标回波,能提高识别的稳定性。用特征 μ 来识别欺骗干扰和目标回波,取 $\lambda=0.5$ 。当目标回波和欺骗干扰不重叠时,做 400 次蒙特卡洛实验得到的有源欺骗干扰识别概率图形如图 8 所示。由图 8 可知,利用分段自相关最大值方差与奇异谱熵相结合来区分目标回波和欺骗干扰,在信噪比大于 8 dB,且目标回波和欺骗干扰不重叠时,识别概率可达到 100%,能有效识别出欺骗式干扰。但在信噪较小时,由于噪声的影响,使得联合特征区别不大,很难区分出目标回波和欺骗干扰,以至于在信噪比小于 5 dB 时,识别概率不高。

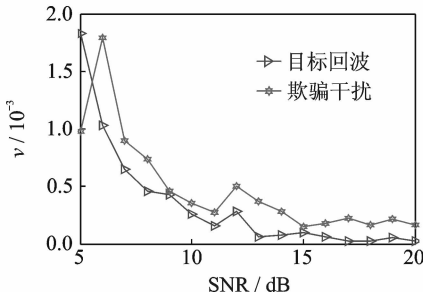


图 6 分段自相关最大值方差

Fig. 6 Segmentation autocorrelation maximum variance

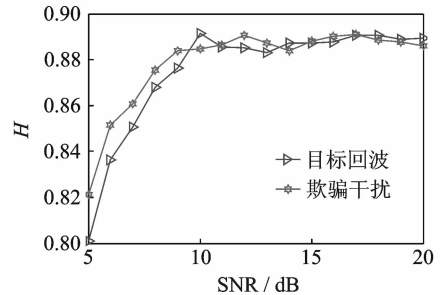


图 7 奇异谱熵

Fig. 7 Singular spectrum entropy

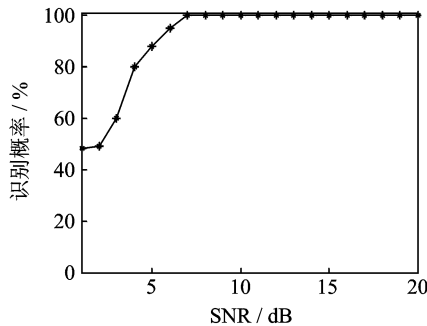


图 8 联合特征识别概率

Fig. 8 Joint feature recognition probability

4 结束语

本文基于干扰机功率放大器特性分析了有源欺骗干扰和目标回波,研究了目标回波和欺骗干扰在分段自相关最大值方差和奇异谱熵两个特征上的差异。仿真结果表明,提取的特征因子可以体现欺骗干扰和目标回波的区别。当目标回波和欺骗干扰不重叠时,在信噪比大于 8 dB 时,欺骗干扰的识别概率可以达到 100%,但在低信噪比下性能有待改进。下一步将在单个欺骗干扰特征提取的基础上研究低信噪比下识别欺骗干扰以及抗密集转发式干扰。

参考文献:

- [1] Berger S D. Digital radio frequency memory linear range gatestealer spectrum[J]. Aerospace and Electronic Systems, IEEE

Trans on, 2003, 39(2): 725-735.

- [2] Greco M, Gini F, Farina A, et al. Effect of phase and range gate pull off delay quantisation on jammer signal[J]. *IEE Proc Radar Sonar Navig*, 2006, 153(5): 454-459.
- [3] 李建勋, 唐斌, 吕强. 双谱特征提取在欺骗式干扰方式识别中的应用研究[J]. *电子科技大学学报*, 2009, 38(3): 329-332.
Li Jianxun, Tang Bin, Lü Qiang. Bispectrum feature extraction used in deceptive jamming modes recognition[J]. *Journal of University of Electronic Science and Technology of China*, 2009, 38(3): 329-332.
- [4] 吕强, 李建勋, 秦江敏, 等. 基于神经网络的雷达抗转发式距离欺骗干扰方法[J]. *系统工程与电子技术*, 2005, 27(2): 240-243.
Lü Qiang, Li Jianxun, Qin Jiangmin, et al. Method against radar's transmitting deceptive jamming in distance based on neural network[J]. *Systems Engineering and Electronics*, 2005, 27(2): 240-243.
- [5] 李建勋, 秦江敏, 马晓岩. 雷达抗应答式欺骗干扰中的特征提取研究[J]. *空军雷达学院学报*, 2004, 18(2): 4-7.
Li Jianxun, Qin Jiangmin, Ma Xiaoyan. Study of feature extraction in radar anti-answering-deception-jamming[J]. *Journal of Air Force Early Warning Academy*, 2004, 18(2): 4-7.
- [6] 李建勋, 秦江敏, 马晓岩. 基于神经网络的雷达抗应答式欺骗干扰方法[J]. *空军雷达学院学报*, 2003, 17(4): 19-21.
Li Jianxun, Qin Jiangmin, Ma Xiaoyan. A method of radar anti-deception-jamming based on neural network[J]. *Journal of Air Force Early Warning Academy*, 2003, 17(4): 19-21.
- [7] 粘朋雷, 李国林, 李飞. 基于 STFRFT 的 LFM 引信抗欺骗干扰方法[J]. *海军航空工程学院学报*, 2015, 30(2): 111-115.
Nian Penglei, Li Guolin, Li Fei. Deception jamming suppression method of LFM fuze based on STFRFT[J]. *Journal of Naval Aeronautical and Astronautical University*, 2015, 30(2): 111-115.
- [8] 闫琰. 基于多维特征处理的雷达有源干扰识别技术[D]. 西安: 西安电子科技大学, 2014.
Yan Yan. Multi-feature-based identification of active jamming[D]. Xi'an: Xidian University, 2014.
- [9] 甘一鸣, 孙闽红, 郑琴, 等. 基于射频功放非线性建模的欺骗干扰识别[J]. *舰船电子对抗*, 2014, 37(4): 1-9.
Gan Yiming, Sun Minhong, Zheng Qin, et al. Deception jamming identification based on nonlinear modeling of RF power amplifier[J]. *Shipboard Electronic Countermeasure*, 2014, 37(4): 1-9.
- [10] 郭波, 宋李彬, 周贵良. 分数阶傅里叶滤波在欺骗干扰中的应用研究[J]. *电子学报*, 2012, 40(7): 1328-1332.
Guo Bo, Song Libin, Zhou Guiliang. Application research on fractional fourier filtering in deception jamming[J]. *Acta Electronica Sinica*, 2012, 40(7): 1328-1332.
- [11] 祝宏, 张海, 唐高弟, 等. 一种基于粒子滤波的雷达抗欺骗干扰方法[J]. *强激光与粒子束*, 2014, 26(11): 1-5.
Zhu Hong, Zhang Hai, Tang Gaodi, et al. Method against radar's deception jamming based on particle filter[J]. *High Power Laser and Particle Beams*, 2014, 26(11): 1-5.
- [12] 田晓. 雷达有源欺骗干扰综合感知方法研究[D]. 成都: 电子科技大学, 2013.
Tian Xiao. Study on the method of radar active deception jamming integrated sensing[D]. Chengdu: University of Electronic Science and Technology of China, 2013.
- [13] 詹鹏. 射频功放数字预失真线性化技术研究[D]. 成都: 电子科技大学, 2012.
Zhan Peng. Study on digital predistortion linearization technique for radio frequency power amplifiers[D]. Chengdu: University of Electronic Science and Technology of China, 2012.
- [14] Lu G, Tang T, Gui G. Deception ECM signals cancellation processor with joint time-frequency pulse diversity[J]. *IEICE Electronics Express*, 2011, 8: 1608-1613.
- [15] Yongping L, Ying X, Tang B. SMSP jamming identification based on matched signal transform[C]//2011 International Conference on Computational Problem-Solving (ICCP). [S. l.]: IEEEEXPlore, 2011: 182-185.

作者简介:



唐娟(1989-), 女, 硕士研究生, 研究方向: 雷达有源欺骗干扰对抗技术。



赵源(1991-), 男, 博士研究生, 研究方向: 组网雷达抗有源干扰技术。



唐斌(1964-), 男, 博士, 教授, 博士生导师, 研究方向: 电子对抗技术与系统、雷达抗干扰技术等, E-mail: bint@uestc.edu.cn。

