Linear Swept-Frequency Jamming Detection Algorithms and Anti-Jamming Methods: Postprint

Authors: Han Chen, Niú Yīngtāo, Xia Zhi, Pang Tianyang

Date: 2018-11-29T00:00:00+00:00

Abstract

Linear frequency sweep interference is one of the commonly employed jamming patterns in battlefield environments, and its timely detection along with efficient anti-jamming decision-making is of significant importance. A low-complexity linear frequency sweep interference detection algorithm is proposed that incorporates metrics of false alarm probability and missed detection probability, with theoretical performance analysis conducted to provide a decision basis for actual communication systems to assess interference conditions. Subsequently, a Q-learning-based anti-frequency-sweep-jamming algorithm is proposed, enabling autonomous selection of optimal communication channels and maximum dwell times when wireless communication systems encounter sweep interference. Finally, simulation results demonstrate that the proposed detection algorithm can effectively detect linear frequency sweep interference signals, achieving detection performance closely matching theoretical analysis results at low complexity. The proposed anti-frequency-sweep-jamming learning algorithm can autonomously select communication channels in interference environments, efficiently evade sweep interference, and realize continuous and reliable information transmission.

Full Text

Preamble

Vol. 37 No. 1
Application Research of Computers
ChinaXiv Cooperative Journal

Detection Algorithm and Anti-Jamming Method for Linear Sweeping Jamming with Low Complexity

Han Chen[1], Niu Yingtao[2], Xia Zhi[1], Pang Tianyang[1]
(1. Army Engineering University, Nanjing 210000, China; 2. Nanjing Telecommunication Technology Institute, Nanjing 210007, China)

Abstract: Linear sweeping jamming is one of the commonly employed jamming patterns in battlefield environments, making its timely detection and effective anti-jamming decision-making critically important. This paper proposes a low-complexity linear sweeping jamming detection algorithm that considers both false alarm probability and missed detection probability metrics, and provides a theoretical performance analysis to serve as a basis for actual communication systems to determine jamming conditions. Subsequently, a Q-learning-based anti-sweeping jamming algorithm is proposed, which enables wireless communication systems to autonomously select the optimal communication channel and maximum dwell time when encountering sweeping jamming. Simulation results demonstrate that the proposed detection algorithm can effectively detect linear sweeping jamming signals, achieving detection performance closely matching theoretical analysis results at low complexity. The proposed anti-sweeping jamming learning algorithm can autonomously select communication channels in jamming environments, efficiently evade sweeping jamming, and achieve continuous and reliable information transmission.

Keywords: linear sweeping jamming; communication anti-jamming; probability of missed detection; probability of false alarm; Q-learning; channel selection

0 Introduction

Military wireless communication has become a key factor in determining the outcome of modern warfare, with its reliability and effectiveness directly determining the degree of battlefield information sharing. Malicious jamming from adversaries is one of the primary factors affecting wireless communication reliability and effectiveness. Linear sweeping jamming, with its advantages of simple generation, large jamming bandwidth, and high jamming efficiency, has become one of the commonly used jamming patterns by adversaries. Therefore, timely and effective detection of linear sweeping jamming is of great significance.

Currently, several mature analysis methods and approaches exist for linear sweeping jamming detection. The Wigner-Ville distribution exhibits good time-frequency concentration for linear sweeping jamming detection, but suffers from cross-term interference when the number of jamming signals increases. References [4–6] propose the Wigner-Hough transform algorithm combined with Hough transform, which further improves detection performance. Reference [7] presents a hidden Markov model recognition algorithm based on likelihood gradient, with real-time parameter estimation to solve the sweeping jamming

suppression problem in spread spectrum communications. Reference [9] utilizes fractional Fourier transform methods for jamming detection of sweeping signals in the fractional domain. These studies provide valuable contributions to sweeping signal detection and suppression. However, existing algorithms still suffer from high complexity, focus primarily on weak sweeping signal detection, lack theoretical analysis of detection performance, and struggle to meet the requirements of military wireless communication systems for sweeping jamming awareness.

Reinforcement learning techniques, represented by Q-learning, have been widely applied in wireless communications. Reference [11] investigates spectrum and power allocation in distributed dynamic spectrum access networks, first solving spectrum allocation through Q-learning and then treating power allocation as an optimization problem to reduce computational complexity and enhance real-time performance. Reference [12] proposes a Q-learning-based real-time routing algorithm to address routing instability caused by node mobility in mobile ad hoc networks. Reference [13] employs minimax Q-learning within an anti-jamming game framework to solve spectrum allocation problems under cognitive jamming threats. However, research on applying reinforcement learning techniques for anti-sweeping jamming decision-making remains limited. For wireless communication systems under jamming attacks, reinforcement learning technology can be introduced to perceive and learn from jamming patterns, effectively predict jamming behavior, enable dynamic adaptation to the electromagnetic environment, and achieve efficient and reliable data transmission.

This paper investigates effective detection of linear sweeping jamming under constraints of performance metrics such as false alarm probability and missed detection probability, derives theoretical detection performance, and provides a theoretical basis for actual communication systems to determine jamming conditions. Subsequently, Q-learning is employed to achieve reliable transmission under sweeping jamming. Finally, based on military wireless communication requirements, simulation verification is conducted for the theoretical detection performance analysis and anti-jamming learning algorithm.

1 System Model

Linear sweeping jamming is a jamming pattern where a jamming signal performs periodic linear scanning across a target frequency band, thereby effectively degrading the reliability or effectiveness of wireless communications within that band. The considered jamming signal is a narrowband Gaussian white noise signal following a normal distribution with signal bandwidth W_{chirp}. Within one scanning period T, the jamming signal' s center frequency moves from the lowest frequency f_L to the highest frequency f_H, forming sweeping jamming across the target band.

The sweeping jamming signal is expressed as:

$$J_{\text{chirp}}(t) = \text{Filter}[w(t) \cdot J_0(t)]$$

where Filter[·] represents narrowband filtering, $w(t)$ represents a zero-mean Gaussian white noise signal following a normal distribution with variance σ^2, and $J_0(t)$ represents the instantaneous center frequency of the narrowband filter during the h-th sweeping period.

When linear sweeping jamming exists, the received sampled signal in an AWGN channel is:

$$x(n) = J_{\text{chirp}}(n) + n_0(n)$$

where $x(n)$ represents the received signal and $n_0(n)$ represents zero-mean Gaussian white noise in the channel with variance σ^2.

For research convenience, the following assumptions are made:

a) The target spectrum consists of N non-overlapping channels in the frequency domain, each with bandwidth W_{ch}, giving a target spectrum bandwidth of $W = N \cdot W_{\text{ch}}$.

b) The broadband detector has a detection bandwidth of W and can detect energy values within these N channels, requiring $2NL$ samples per detection. The sweeping jamming bandwidth satisfies $W_{\text{chirp}} \leq W$.

c) During the entire detection process, detection is performed at most M times, with each detection duration being T_d, and total detection duration $T_{\text{total}} = M \cdot T_d \leq T$.

d) Each detection duration T_d is sufficiently short, allowing the sweeping signal to be approximated as a fixed-frequency signal during detection.

e) Reliable transmission time is defined as the transmission duration from the start of communication until communication interruption due to jamming.

---

2 Low-Complexity Linear Sweeping Jamming Detection Algorithm

This section proposes a low-complexity linear sweeping jamming detection algorithm that considers false alarm probability and missed detection probability metrics, providing criteria for actual communication systems to determine jamming conditions. The specific algorithm steps are as follows:

a) Calculate the power spectrum of the target band. At time m, the NP energy detector computes the power spectrum of the target band using the modified periodogram method. The power spectrum value at frequency point f obtained from the m-th detection is:

$$P_m(f) = \frac{1}{2NL}\left|\sum_{l=0}^{2NL-1} w(l)x(l)e^{-j2\pi fl}\right|^2$$

where $2NL$ is the number of sampling points, $x(l)$ are the sampled values, and $w(l)$ is the window function. This paper selects the Hamming window.

b) Calculate energy values in each channel. The power spectrum obtained in equation (3) contains NL points, which are equally divided into N segments in order. Each segment contains L power spectrum points corresponding to one channel. The energy value in the i-th channel during the m-th detection can be calculated as:

$$E_{m,i} = \sum_{k=(i-1)L+1}^{iL} P_m(f_k) \cdot \frac{W}{NL}$$

c) Determine if any channel is jammed in the m-th detection. Compare the energy value $E_{m,i}$ of the i-th channel in the m-th detection with the detection threshold γ. The threshold value is determined by the false alarm probability indicator P_{FA}:

$$\gamma = \frac{\sigma^2}{2L} Q_{\chi^2}^{-1}(P_{\mathrm{FA}})$$

If $E_{m,i} > \gamma$, it is determined that channel i is jammed at time m, denoted as $I_{m,i} = 1$; otherwise, it is determined that channel i is not jammed in the m-th detection, denoted as $I_{m,i} = 0$.

d) Perform M detections on the target band using the above method. If channel i is not jammed at time $m-1$, is jammed at time m, and the jamming disappears at time $m+1$, then it is determined that channel i experiences dynamic jamming:

$$\{I_{m-1,i} = 0; I_{m,i} = 1; I_{m+1,i} = 0\}$$

e) Calculate the channel threshold value M for the number of detected channels based on the given missed detection probability indicator P_{MD}:

$$M = \arg \min_{k\in\{1,2,\ldots,N\}} \left|\sum_{m=k}^{N} C_N^m P_{\mathrm{D}}^m (1-P_{\mathrm{D}})^{N-m} - (1-P_{\mathrm{MD}})\right|$$

where P_{D} is the single-channel dynamic jamming detection probability. If at least M out of N channels are detected as experiencing dynamic jamming during

M detections, it is determined that the band is subject to dynamic jamming. The missed detection probability P_{MD} is defined as the probability that jamming actually exists but is not detected.

f) Divide the detected jammed frequency points into odd and even groups, and fit them into straight lines using the least squares method: $y_e = A_e x + B_e$, $y_o = A_o x + B_o$. If the similarity between the parameters of the two fitted lines exceeds the threshold value η, i.e.,

$$\Delta = (A_e - A_o)^2 + (B_e - B_o)^2 < \eta$$

then it is determined that linear sweeping jamming is present.

---

3 Detection Algorithm Performance Analysis

This section provides a theoretical analysis of the proposed low-complexity linear sweeping jamming detection algorithm that considers false alarm probability and missed detection probability metrics.

3.1 NP Detector

The jamming signal detection problem can be viewed as a binary hypothesis selection problem. According to the NP theorem, the NP detector is constructed as:

$$\mathcal{H}_0 : x(n) = n_0(n), \quad n = 0, 1, ..., 2NL - 1$$
$$\mathcal{H}_1 : x(n) = n_0(n) + J_{\mathrm{chirp}}(n), \quad n = 0, 1, ..., 2NL - 1$$

where $\mathcal{H}_0$ assumes only noise in the observations, and $\mathcal{H}_1$ assumes both jamming signal and noise in the observations. With $2NL$ independent samples, the likelihood ratio function is constructed as:

$$L(x) = \frac{p(x|\mathcal{H}_1)}{p(x|\mathcal{H}_0)} > \gamma'$$

If the likelihood ratio exceeds the threshold value γ', the NP detector decides $\mathcal{H}_1$ (jamming present); otherwise, it decides $\mathcal{H}_0$. Here $p(x|\mathcal{H}_1)$ represents the probability density function of observations under $\mathcal{H}_1$, and $p(x|\mathcal{H}_0)$ represents the probability density function under $\mathcal{H}_0$.

According to the model assumptions, as shown in equation (9), under $\mathcal{H}_0$, $x(n) \sim \mathcal{N}(0, \sigma^2)$; under $\mathcal{H}_1$, $x(n) \sim \mathcal{N}(0, \sigma_s^2 + \sigma^2)$. The log-likelihood ratio function is:

$$\ln L(x) = \sum_{n=0}^{2NL-1} \left[\ln \frac{1}{\sqrt{2\pi(\sigma_s^2+\sigma^2)}} - \frac{x^2(n)}{2(\sigma_s^2+\sigma^2)} - \ln \frac{1}{\sqrt{2\pi\sigma^2}} + \frac{x^2(n)}{2\sigma^2} \right]$$

Simplifying and combining constants independent of observations with the threshold γ' into a new threshold γ, we obtain the detection statistic:

$$T(x) = \sum_{n=0}^{2NL-1} x^2(n) > \gamma$$

If $T(x)$ exceeds the new threshold γ, it is decided that $\mathcal{H}_1$ holds (jamming present).

$T(x)$ follows a Gaussian distribution and is the sum of squares of $2NL$ independent and identically distributed Gaussian random variables. Under $\mathcal{H}_0$, $T(x)$ follows a chi-square distribution with $2NL$ degrees of freedom; under $\mathcal{H}_1$, $T(x)$ follows a non-central chi-square distribution with $2NL$ degrees of freedom. A chi-square distribution with ν degrees of freedom is denoted as χ^2_ν.

3.2 Jamming Signal Detection Performance Analysis

The false alarm probability P_{FA} represents errors where jamming is detected when none exists:

$$P_{\mathrm{FA}} = \Pr\{T(x) > \gamma | \mathcal{H}_0\} = Q_{\chi^2_{2NL}}\left(\frac{\gamma}{\sigma^2}\right)$$

where $Q_{\chi^2_\nu}$ is the complementary cumulative distribution function of the chi-square distribution with ν degrees of freedom. Therefore, the final detection threshold γ is calculated from the given false alarm probability:

$$\gamma = \sigma^2 Q^{-1}_{\chi^2_{2NL}}(P_{\mathrm{FA}})$$

The single-channel dynamic jamming detection probability P_{D} is the probability that jamming actually exists and is correctly detected:

$$P_{\mathrm{D}} = \Pr\{T(x) > \gamma | \mathcal{H}_1\} = Q_{\chi^2_{2NL}}\left(\frac{\gamma}{\sigma_s^2+\sigma^2}\right)$$

The missed detection probability is:

$$P_{\mathrm{MD}} = \Pr\{T(x) < \gamma | \mathcal{H}_1\} = 1 - P_{\mathrm{D}}$$

3.3 Single-Channel Dynamic Interference Detection Probability

From the algorithm, the detection probability $P_{i,\mathrm{D}}$ that dynamic jamming exists on channel i is:

$$P_{i,\mathrm{D}} = P_{\mathrm{D}}^2 \times (1 - P_{\mathrm{D}}) \times P_{\mathrm{D}}^2$$

3.4 Linear Sweeping Jamming Detection Performance

Given the premise that jamming exists, the communication system's final missed detection probability $P_{\mathrm{MD,total}}$ and detection probability $P_{\mathrm{D,total}}$ for dynamic jamming are:

$$P_{\mathrm{D,total}} = \sum_{m=M}^{N} C_N^m P_{i,\mathrm{D}}^m (1 - P_{i,\mathrm{D}})^{N-m}$$

Given the missed detection probability indicator, the channel threshold value M for determining whether the band is subject to dynamic jamming can be obtained from equation (7). If after M detections, at least M out of N channels are detected as experiencing dynamic jamming, it is determined that the band is subject to dynamic jamming. The missed detection probability $P_{\mathrm{MD,total}}$ is defined as the probability that dynamic jamming actually exists but is not detected.

Analysis from equation (7) shows that a larger channel threshold value M leads to smaller P_{FA} and larger $P_{\mathrm{MD,total}}$, resulting in lower detection probability for dynamic jamming. However, under unknown adversary jamming conditions, if the final detector determines that jamming exists, the credibility of this result is higher.

The detected jammed frequency points are divided into odd and even groups, and linear fitting is performed using the least squares method. If the fitted result approximates a straight line, it is determined that linear sweeping jamming is present.

---

4 Q-Learning-Based Anti-Sweeping Jamming Algorithm

Q-learning is a typical reinforcement learning algorithm where an agent can adjust its execution strategy based on environmental feedback, achieving adaptive interaction between the agent and environment to improve environmental adaptability. As shown in [Figure 1: see original paper], in the current state s, the agent selects an action a according to the current selection policy π, applies it to the unknown environment, and simultaneously receives an environmental feedback signal r, thereby updating the Q-function and guiding the next round

of action selection. Through continuous learning, the agent can eventually find the optimal action selection policy π^*.

Based on the detection algorithm results, the state space S is defined as $S = [1, 2, ..., N]$, where S_t represents the channel where the sweeping jamming resides at time t.

The action space A is defined as $A = [1, 2, ..., N]$, where a_t represents the communication channel selected by the user at time t.

The reward function is defined as:

$$r_t = T_2 - T_1$$

where T_1 is the communication start time and T_2 is the time when communication is interrupted due to jamming.

The user' s communication selection policy π is defined as a probability distribution over various possible actions in the current state s. The user' s optimization objective is to find the optimal selection policy π^* that maximizes reliable transmission time.

Traditional Q-learning algorithms generally use a fixed ε-greedy model to balance "exploration" and "exploitation" :

$$a = \begin{cases} \text{random}(A) & \text{if Num} \leq \varepsilon \\ \arg\max_{a'} Q(s, a') & \text{if Num} > \varepsilon \end{cases}$$

where Num represents a random number generated between [0,1]. If Num $> \varepsilon$, a random action is selected from the action set to "explore" better strategies; if Num $\leq \varepsilon$, the Q-table is "exploited" to select the action that maximizes the Q-value. For communication anti-jamming, after both communication parties obtain anti-jamming decision knowledge, they need to establish stable communication behavior to meet communication requirements. Therefore, the method of using a fixed ε value to balance "exploration" and "exploitation" is not conducive to stable convergence of the learning process. In anti-jamming scenarios, this paper implements a smooth transition between "exploration" and "exploitation" based on a simulated annealing model. After obtaining complete anti-jamming decision knowledge, stable communication behavior can be established to better achieve intelligent communication anti-jamming learning.

The communication selection policy is updated as:

$$\pi_t(a|s_t) = \frac{\exp(\xi_t(s_t, a)/\tau_t)}{\sum_{a' \in A} \exp(\xi_t(s_t, a')/\tau_t)}$$

where a' represents channels other than the current communication channel a_t, and ξ_t, τ_t are parameters related to the Boltzmann model. ξ_t is positively correlated with "exploration" time, ξ_{final} represents the termination condition of the "exploration" phase, and τ, υ affect the transition between the "exploration" and "exploitation" phases.

Based on the Q-learning algorithm, the anti-sweeping jamming algorithm is proposed as follows:

a) Initialize Q as a zero matrix, initial learning rate α_0, annealing initial temperature ξ_0, final temperature ξ_{final}, Boltzmann parameter τ, and annealing rate υ in the learning rule. Initialize the communication selection policy π_0 and randomly select a channel from the state set A as the current communication channel.

b) At each time slot t, repeat the following process:

(a) Select action a_t according to the current communication policy, calculate the received reward r_t, and observe the next state s_{t+1}.

(b) Update the Q-table:

$$Q_{t+1}(s_t, a_t) = (1 - \alpha_t)Q_t(s_t, a_t) + \alpha_t[r_t + \max_{a'} Q_t(s_{t+1}, a')]$$

(c) Update the communication selection policy according to equation (27).

(d) Update the Boltzmann coefficient ξ_t and learning rate α_t according to equations (28) and (30):

$$\xi_{t+1} = \begin{cases} \xi_t - \upsilon & \text{if } \xi_t \geq \xi_{\text{final}} \\ \xi_{\text{final}} & \text{if } \xi_t < \xi_{\text{final}} \end{cases}$$

$$\alpha_t = \frac{\alpha_0}{\log(\mu(s_t, a_t) + 1)}$$

where α_0 represents the learning step size at the initial stage, and $\mu(s_t, a_t)$ represents the number of times the state-action pair (s_t, a_t) has been visited. Literature [16] has proven that if $\sum_{t=0}^{\infty} \alpha_t = \infty$ and $\sum_{t=0}^{\infty} \alpha_t^2 < \infty$, the Q-learning algorithm can converge.

(e) Determine whether the maximum number of iterations K has been reached. If not, return to step **b)**.

5 Simulation Results

To verify the performance of the proposed algorithms, MATLAB simulation experiments were conducted.

The experimental parameters were set as: sampling frequency $F_s = 20\,\text{MHz}$, detection time per interval $T_d = 0.5\,\text{ms}$, sweeping signal period $T = 0.05\,\text{s}$. The sweeping signal' s lowest frequency, highest frequency, and sweeping jamming bandwidth were $f_L = 2\,\text{MHz}$, $f_H = 10\,\text{MHz}$, and $W_{\text{chirp}} = 8\,\text{MHz}$, respectively. The broadband detector' s detection bandwidth was $W = 8\,\text{MHz}$, with $N = 100$ channels. The Gaussian white noise variance was $\sigma^2 = 0.5$, and the jamming-to-noise ratio (JNR) ranged from $-15\,\text{dB}$ to $6\,\text{dB}$. This paper generates sweeping jamming signals using narrowband Gaussian noise amplitude-modulated sweeping signals. First, narrowband Gaussian noise $n_{\text{Gauss}}(n)$ with $50\,\text{kHz}$ bandwidth is generated. Then, this noise amplitude-modulates the sweeping signal $J_{\text{chirp}}(n)$. The final jamming signal is $J(n) = n_{\text{Gauss}}(n) \times J_{\text{chirp}}(n) + n_0(n)$, where $n_0(n)$ is channel environment Gaussian white noise, satisfying a JNR of $-15\,\text{dB}$ to $6\,\text{dB}$.

Fig. 2 shows the detection probability of a single interference detection. With false alarm probabilities P_{FA} set to 10^{-2}, 10^{-3}, and 10^{-4}, the single detection probability P_{D} from the simulation matches the theoretical value $P_{\text{D,th}}$ well. The proposed detection algorithm achieves detection performance close to theoretical analysis results with low complexity of $\mathcal{O}(\log n)$. When $\text{JNR} > -4\,\text{dB}$, the energy detector performs well, with single detection probability approaching 1.

Fig. 3 shows the detection probability under different false alarm probability constraints. With constant $\text{JNR} = -5\,\text{dB}$, the relationship between system detection probability $P_{\text{D,total}}$ and channel threshold value M is compared. When JNR is constant, detection probability gradually decreases as the channel threshold value increases. A higher channel threshold setting results in lower detection probability for dynamic jamming, but higher detection credibility when jamming status is unknown. A smaller false alarm probability indicator leads to lower single detection probability, and with the same channel threshold setting, the achievable detection probability is lower.

Fig. 4 compares theoretical values $P_{\text{D,th}}$ and actual simulation values P_{D} under different JNR conditions with fixed false alarm probability $P_{\text{FA}} = 10^{-3}$. With constant false alarm probability, detection probability and detection channel threshold value have a one-to-one correspondence. As the channel threshold value increases, detection probability decreases while detection credibility under unknown jamming status increases. When JNR gradually decreases, with the same channel threshold setting, system detection probability decreases.

In each detection period, channel frequency points experiencing dynamic jamming are divided into odd and even groups for least squares linear fitting. The fitted curves are shown as blue dashed lines in **Fig. 5** (for demonstration purposes, $N = 10$ is used in this simulation). **Fig. 5** illustrates the time-frequency

jamming pattern of sweeping jamming signals over two periods. Based on detection results, the anti-sweeping jamming learning algorithm finds channel selection strategies that guarantee maximum reliable transmission time, shown as red solid lines in **Fig. 5**. Based on the current jamming state, the wireless communication system autonomously selects a communication channel that lags one channel behind the sweeping signal' s location. When the sweeping signal jams the lowest frequency channel, the selected channel is the highest frequency channel. This allows the communication system to guarantee maximum transmission dwell time through autonomous channel selection.

Fig. 6 compares the average reliable transmission time performance of the proposed anti-jamming algorithm against blind frequency hopping and traditional Q-learning algorithm ($\varepsilon = 0.8$). The results show that the proposed algorithm ensures higher reliable transmission time and demonstrates superior anti-jamming performance.

---

6 Conclusion

Timely and effective detection of linear sweeping jamming signals and the development of corresponding efficient anti-jamming strategies constitute an important research topic in military communication anti-jamming. This paper proposes a broadband detection algorithm for effective detection of linear sweeping jamming signals and provides performance analysis. Simulation results demonstrate that the proposed detection algorithm can meet given false alarm probability and missed detection probability metrics, achieving good detection performance with low complexity, which satisfies military wireless communication system requirements for sweeping jamming awareness and validates the correctness of the fundamental theoretical analysis. Based on detection results, a Q-learning-based anti-sweeping jamming algorithm is proposed. Simulation results show that this algorithm can select optimal channels to achieve continuous and efficient reliable transmission under sweeping jamming.

References

[1] Yao Fuqiang. Communication anti-jamming engineering and practice [M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2012: 2-71.

[2] Kong Zhijie, Hao Xinhong, Li Ping, et al. Research on anti-frequency sweeping jamming method for frequency modulation fuze based on timing sequence and correlation detection [J]. Acta Armamentarii, 2017, 38(8): 1575-1582.

[3] Lu Dandan. Interference detection and blind source separation technology in the frequency hopping system [D]. Chengdu: University of Electronic Science & Technology, 2016: 16-21.

[4] Barbarossa S, Zanalda A. A combined wigner-ville and hough transform for cross-terms suppression and optimal detection and parameter estimation [C]// Proc. of Acoustics, Speech, and Signal Processing. 1992: 173-176.

[5] Barbarossa S. Analysis of multicomponent LFM signals by a combined wigner-hough transform [J]. IEEE Trans on Signal Processing, 1995, 43(6): 1511-1515.

[6] Xia Caijie, Wang Aihua, An Jianping. Research on adaptive time-varying suppression of frequency sweeping interference [J]. Computer Engineering, 2008, 34(4): 37-39.

[7] Yang Jipin, Zheng Zhi, Zhang Xiongwei. Sweeping interference suppression based on the HMM in spread spectrum communication systems [J]. Journal of PLA University of Science & Technology: Natural Science Edition, 2004, 5(4): 25-28.

[8] Zhao Huizi, Sun Kewen. The sweep jamming detection for GNSS receiver based on fractional fourier transform [J]. China Computer & Communication, 2017(1): 78-81.

[9] Dong Pinhong, Du Yang, Zhou Lanlin, et al. The performance analysis of the FH/MFSK system under the broadband sweep jamming [J]. Journal of Electronic Science and Technology, 2014, 43(5): 659-662.

[10] Lyu Zaixing. Research on jamming detection algorithm in communication countermeasures [D]. Chengdu: University of Electronic Science and Technology, 2011.

[11] Ghorbel M B, Hamdaoui B, Guizani M, et al. Distributed learning-based cross-layer technique for energy-efficient multicarrier dynamic spectrum access with adaptive power allocation [J]. IEEE Trans on Wireless Communications, 2016, 15(3): 1665-1674.

[12] Ali Ghaffari. Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms [J]. Wireless Networks, 2017, 23(3): 703-714.

[13] Wang Beibei, Wu Yongle, Liu K J R, et al. An anti-jamming stochastic game for cognitive radio networks [J]. IEEE Journal on Selected Areas in Communications, 2011, 29(4): 877-889.

[14] Jia Luliang, Yao Fuqiang, Sun Youming, et al. A hierarchical learning solution for anti-jamming Stackelberg game with discrete power strategies [J]. IEEE Wireless Communications Letters, 2017, PP(99): 1-1.

[15] Sudharman K. Jayaweera. Signal processing for cognitive radios [M]. Wiley Publishing, 2014: 429-471.

[16] Wang Wenbo, Kwasinski Andres, Niyato Dusit, et al. A survey on applications of model-free strategy learning in cognitive wireless networks [J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 1717-1757.