SECURITY INFORMATION FACTOR BASED LOW PROBABILITY OF IDENTIFICATION IN DISTRIBUTED MULTIPLE-RADAR SYSTEM

Chenguang Shi, Fei Wang, Jianjiang Zhou, Huan Zhang

Key Laboratory of Radar Imaging and Microwave Photonics, Ministry of Education, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China

ABSTRACT

In this study, the problem of low probability of identification (LPID) performance improvement for distributed multiple-radar system (DMRS) is addressed. Firstly, we propose security information factor originating from secrecy capacity to evaluate the LPID performance for DMRS, and derive an explicit closed-form expression of security information factor. Then, a novel LPID enhancement scheme based on security information factor is presented, whose purpose is to maximize the achievable security information factor by optimizing the transmission waveforms and the cooperative jamming spectra with the predefined total transmission energy and cooperative jamming power constraints. Numerical simulations demonstrate that the proposed strategy can effectively achieve the optimal solutions and bring remarkable improvement on the LPID performance for DMRS.

Index Terms—Low probability of identification (LPID), security information factor, distributed multiple-radar system (DMRS), transmission waveform, cooperative jamming

1. INTRODUCTION

In recent years, distributed multiple-radar system (DMRS) is widely used in modern battlefield owing to its ability to increase signal and spatial diversity gains [1]-[3].

The waveform design for DMRS has been a long term research topic for many years [4]-[13]. Friedlander in [4] investigates the problem of waveform design for multiple-input multiple-output (MIMO) radars, where the transmission waveforms are optimized to maximize the signal-to-interference-plus-noise ratio (SINR).

In 1993, Bell first introduced information theory to radar waveform design in his work [7]. Subsequently, the authors in [8] present the MIMO radar waveform design criteria based on mutual information (MI) and minimum mean square error (MMSE). The work of [9] investigates the design of matched waveforms based on maximization of signal-to-noise ratio (SNR) and MI. Other existing studies [10]-[13] also utilize similar waveform optimization criteria.

Following from the above discussions, it should be noted that most cases on waveform design are mainly towards system performance improvement for DMRS, while the low probability of identification (LPID) optimization is scarcely considered [1]. Currently, with the continuously growing demand for security in wireless communications, physical-layer (PHY) security is emerging as an effective secure communication method to defend against passive eavesdropper by employing the physical characteristics of wireless channel [14]-[18]. Inspired by the fact that PHY security is to have hostile eavesdropper got nothing of emitter, we present security information factor originating from secrecy capacity to describe the LPID performance for DMRS, which hasn't been studied previously.

Furthermore, this paper will investigate the security information factor based LPID performance improvement strategy in DMRS. The main contributions of the current work can be summarized as follows. Firstly, we define security information factor to evaluate the LPID performance for DMRS, and derive an analytical closed-form expression of security information factor. Secondly, a novel optimal LPID enhancement scheme is developed to maximize the achievable security information factor by optimizing the transmission waveforms and the cooperative jamming spectra in DMRS. To the best of our knowledge, no literature investigating the security information factor based LPID performance optimization in DMRS was prior to this work.

The remainder of this paper is organized as follows. Section 2 introduces the known target signal model. In Section 3, with the proposed definition of security information factor, a novel LPID improvement strategy based on security information factor is formulated, and the optimal solutions are derived by analytical closed-form expressions. The numerical simulations are given in Section 4. Finally, Section 5 concludes this paper.

2. SIGNAL MODEL

The work is supported by the National Natural Science Foundation of China under grant number 61371170, the Fundamental Research Funds for the Central Universities, Funding of Jiangsu Innovation Program for Graduate Education under grant number CXLX13_154 and the Priority Academic Program Development of Jiangsu Higher Education Institutions (PADA).

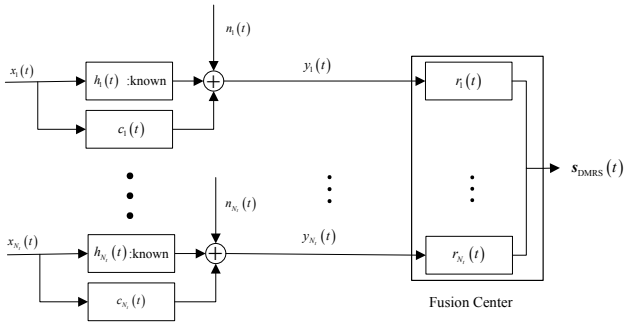

Fig.1 Known target signal model in signal-dependent interference

The known target model in signal-dependent interference is depicted in Fig.1, where $x_i(t)$ is the i th complex-valued baseband transmit waveform with finite duration T_i, $h_i(t)$ is the i th known complex-valued baseband target impulse response of finite duration T_{h_i}. Let $X_i(f)$ and $H_i(f)$ be the Fourier transforms of $x_i(t)$ and $h_i(t)$, respectively. Let $\boldsymbol{n}_i(t)$ denote the i th complex-valued, zero-mean channel noise process with the power spectral density (PSD) $S_{nni}(f)$. Likewise, $\boldsymbol{c}_i(t)$ is the i th complex-valued, zero-mean Gaussian random process representing the signal-dependent interference with PSD $S_{cci}(f)$. $y_i(t)$ denotes the i th scattered signal, $r_i(t)$ denotes the i th complex-valued receiver filter impulse response, and $s_{DMRS}(t)$ denotes the overall output signal. The variables in boldface letters represent random processes. It is important to note that the fusion center can process all the echoes reflected from the target with the matched filter bank.

Here, we consider a DMRS where each of N_t radar nodes individually and independently extracts information about the target. The information about the target at each radar node is sent to a fusion center, which combines the local observations $y_i(t)$ in order to improve the overall system performance.

3. PROBLEM FORMULATION

The MI between the DMRS return and the estimated target impulse response can be used as a metric for target estimation performance [7]. We assume that the transmission signal is essentially limited to the bandwidth BW. Then, the achievable MI of DMRS is written as [9]:

$$\mathrm{I}_{\mathrm{DMRS}} \simeq \sum_{i=1}^{N_t} T_{y_i} \bullet \int_{\mathrm{BW}} \ln\left\{1+\frac{|H_i(f)|^2 \bullet |X_i(f)|^2 \bullet L^2_{\mathrm{DMRS}}(i)}{T_{y_i} \bullet \left[S_{cci}(f) \bullet |X_i(f)|^2 \bullet L^2_{\mathrm{DMRS}}(i) + S_{nni}(f)\right]}\right\} df \quad (1)$$

where $T_y = T_h + T$ denotes the duration of the echo $y_i(t)$, $L_{\mathrm{DMRS}}(i)$ denotes the attenuation from the i th radar node in DMRS to the target, that is:

$$L_{\mathrm{DMRS}}(i) = \frac{\sqrt{G_{ti} \bullet G_{ri}}}{R_i^2} \quad (2)$$

where G_{Ti} is the gain of the i th radar's transmitting antenna, G_{Ri} is the gain of the i th radar's receiving antenna, R_{Ti} is the range from the i th radar node to the target.

Similarly, the MI between the transmission signal of DMRS $x_i(t)$ and the received signal of intercept receiver $z_i(t)$ can be expressed as:

$$\begin{aligned} \mathrm{I}_{\mathrm{INRE}}(i) &\triangleq \mathrm{MI}\left(x_i(t), z_i(t)\right) \\ &= T_y^{'} \bullet \int_{\mathrm{BW}^{'}} \ln\left\{1+\frac{|X_i(f)|^2 \bullet L^2_{\mathrm{INRE}}(i)}{T_y^{'} \bullet S_{nni}^{'}(f)}\right\} df \end{aligned} \quad (3)$$

where $T_y^{'}$ is the processing time of intercept receiver, $\mathrm{BW}^{'}$ is the effective bandwidth of intercept receiver, $S_{nni}^{'}(f)$ is the intercept receiver noise PSD, $L_{\mathrm{INRE}}(i)$ is the attenuation from the i th radar node in DMRS to the intercept receiver, that is:

$$L_{\mathrm{INRE}}(i) = \frac{\sqrt{G_{Ti} \bullet G_I}}{R_{Ti}} \quad (4)$$

where G_{Ti} is the gain of the i th radar's transmitting antenna in the direction of the intercept receiver, G_I is the gain of the intercept receiver's antenna, R_{Ti} is the range from the i th radar node to the intercept receiver.

What's more, the cooperative jamming techniques can be employed to jam the passive intercept receiver so that the achievable MI of interceptor would be degraded by the cooperative jamming signals while the DMRS is unaffected [19]. Thus, (3) can be modified as:

$$\begin{aligned} \mathrm{I}_{\mathrm{INRE}}(i) &\triangleq \mathrm{MI}\left(x_i(t), z_i(t)\right) \\ &= T_y^{'} \bullet \int_{\mathrm{BW}^{'}} \ln\left\{1+\frac{|X_i(f)|^2 \bullet L^2_{\mathrm{INRE}}(i)}{T_y^{'} \bullet \left\{J_i(f) \bullet L^2_{\mathrm{JAM}}(i) + S_{nni}^{'}(f)\right\}}\right\} df \end{aligned} \quad (5)$$

where $J_i(f)$ represents the PSD of the i th cooperative jammer, $L_{\mathrm{JAM}}(i)$ is the attenuation from the i th cooperative jammer to the intercept receiver, which can be described as:

$$L_{\mathrm{JAM}}(i) = \frac{\sqrt{G_{Ji} \bullet G_I}}{R_{Ji}} \quad (6)$$

where G_{Ji} is the gain of the i th cooperative jammer's transmitting antenna in the direction of the intercept receiver, R_{Ji} is the range from the i th cooperative jammer to the intercept receiver. For simplicity of derivation, we suppose that $T_y = T_y^{'}$ and $\mathrm{BW} = \mathrm{BW}^{'}$. Thus, (5) can be further rewritten as follows:

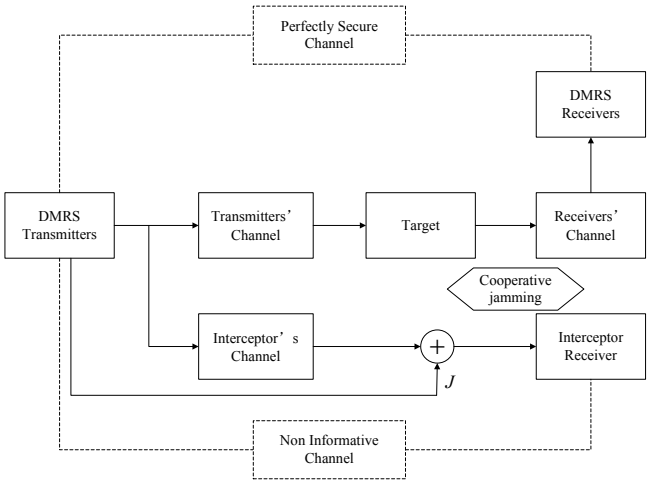

Fig.2 The notional sketch of the completely secure DMRS

$$\mathrm{I}_{\mathrm{INRE}}(i)=T_y\bullet\int_{\mathrm{BW}}\ln\left\{1+\frac{\left|X_i(f)\right|^2\bullet L_{\mathrm{INRE}}^2(i)}{T_y\bullet\left\{J_i(f)\bullet L_{\mathrm{JAM}}^2(i)+S_{nni}^{'}(f)\right\}}\right\}df \quad (7)$$

In this paper, for convenience, it is assumed that the radar nodes in DMRS can simultaneously transmit radar modulating signal to extract information about the target and cooperative jamming signal to jam the passive intercept receivers, while the cooperative jamming signal is designed to jam the intercept receiver without affecting the radar nodes in DMRS. Therefore, originating from the definition of secrecy capacity in wireless communications, we propose security information factor F_{SE} for DMRS as:

$$F_{\mathrm{SE}}\triangleq\frac{\mathrm{I}_{\mathrm{DMRS}}-\sum_{i=1}^{N_t}\mathrm{I}_{\mathrm{INRE}}(i)}{\mathrm{I}_{\mathrm{DMRS}}} \quad (8)$$

which can be utilized to evaluate the LPID performance for DMRS.

The notional sketch of the completely secure DMRS is plotted in Fig.2. It is important to note that $0<F_{\mathrm{SE}}\le 1$ means that the DMRS is in completely secure state while estimating the target features, and that the larger the achievable security information factor F_{SE}, the better LPID performance of DMRS to finish the system task.

Herein, we will formulate the security information factor based LPID improvement approach. To this end, the proposed LPID optimization scheme can be written as:

$$\left.\begin{aligned}&\max_{|X_i(f)|^2,J_i(f)}\quad F_{\mathrm{SE}}=1-\frac{\sum_{i=1}^{N_t}\mathrm{I}_{\mathrm{INRE}}(i)}{\mathrm{I}_{\mathrm{DMRS}}}\\ &s.t.:\ \mathrm{C1}:\ \sum_{i=1}^{N_t}\int_{\mathrm{BW}}\left|X_i(f)\right|^2df\le\mathrm{E}_{\mathrm{DMRS}}\\ &\qquad\mathrm{C2}:\ \int_{\mathrm{BW}}J_i(f)df\le P_i\ (\forall i)\end{aligned}\right\} \quad (9)$$

where $\mathrm{E}_{\mathrm{DMRS}}$ denotes the total energy constraint of DMRS, P_i denotes the cooperative jamming power constraint of the i th radar node. In (9), the security information factor F_{SE} is maximized by optimizing the transmission waveforms and the cooperative jamming spectra subjected to the predefined total transmission energy and the cooperative jamming power constraints. It is also worth mentioning that if the security information factor is maximized, the intercept probability of the transmission waveforms would be much less than 0.5, in which case the DMRS is in perfectly LPID state.

Theorem 3.1: The optimal transmission waveforms that maximize the MI (1) under the total energy constraint C1 should satisfy:

$$\left|X_i(f)\right|^2\simeq\max\left[0,B_i(f)\left(A-D_i(f)\right)\right] \quad (10)$$

where $B_i(f)$ and $D_i(f)$ can be given by:

$$B_i(f)=\frac{\left|H_i(f)\right|^2\bullet L_{\mathrm{DMRS}}^2(i)/T_y}{2S_{cci}(f)\bullet L_{\mathrm{DMRS}}^2(i)+\left|H_i(f)\right|^2/T_y} \quad (11)$$

and

$$D_i(f)=\frac{S_{nni}(f)}{\left|H_i(f)\right|^2\bullet L_{\mathrm{DMRS}}^2(i)/T_y} \quad (12)$$

respectively. The constant A can be calculated by the total energy constraint C1.

The optimal cooperative jamming spectra that minimize the MI (7) under the jamming power constraint C2 should satisfy:

$$J_i(f)\simeq\max\left[0,\overline{B_i}(f)\left(\overline{A_i}-\overline{D_i}(f)\right)\right] \quad (13)$$

where $\overline{B_i}(f)$, and $\overline{D_i}(f)$ can be given by:

$$\overline{B_i}(f)=\frac{\frac{\left|X_i(f)\right|^2\bullet L_{\mathrm{INRE}}^2(i)}{T_y\bullet L_{\mathrm{JAM}}^2(i)}}{2\frac{S_{nni}^{'}(f)}{L_{\mathrm{JAM}}^2(i)}+\frac{\left|X_i(f)\right|^2\bullet L_{\mathrm{INRE}}^2(i)}{T_y\bullet L_{\mathrm{JAM}}^2(i)}} \quad (14)$$

and

$$\overline{D_i}(f)=\frac{\left(\frac{S_{nni}^{'}(f)}{L_{\mathrm{JAM}}^2(i)}\right)^2+\frac{\left|X_i(f)\right|^2\bullet L_{\mathrm{INRE}}^2(i)}{T_y\bullet L_{\mathrm{JAM}}^2(i)}\bullet\frac{S_{nni}^{'}(f)}{L_{\mathrm{JAM}}^2(i)}}{\frac{\left|X_i(f)\right|^2\bullet L_{\mathrm{INRE}}^2(i)}{T_y\bullet L_{\mathrm{JAM}}^2(i)}} \quad (15)$$

respectively, and $\overline{A_i}$ is a constant which can be determined by the cooperative jamming power constraint C2.

4. SIMULATION RESULTS

In this sequel, simulation results are provided to demonstrate the effectiveness of employing the optimal transmission waveforms and cooperative jamming spectra given in **Theorem 3.1**. Here, we assume that the PSDs of the additive Gaussian white noise in DMRS and intercept receiver are 6.0×10^{-16} W/Hz and 6.0×10^{-13} W/Hz, respectively. The to-

Table 1 The comparison of security information factor for different jamming strategies

Jamming strategies	Security information factor
Optimal cooperative jamming spectra	0.9875
Predefined cooperative jamming spectra	0.9854
Without cooperative jamming	-8.5278

tal energy of DMRS is $200\,\mathrm{J}$, the total power of each cooperative jammer is $500\,\mathrm{W}$, and T_y is set to be $0.01\,\mathrm{s}$.

Table 1 presents the comparison of security information factor for different jamming strategies. It is observed that the optimal cooperative jamming spectra can result in the largest security information factor, which in turn means that it achieves the best LPID performance for DMRS. The predefined cooperative jamming spectra is the uniform jamming power allocation in the whole frequency band, and it has a worse LPID performance. This is reasonable due to the fact that the predefined cooperative jamming has no prior knowledge about the transmission waveforms [20]. However, it is better than the case without cooperative jamming. This again shows that the proposed optimal transmission waveforms and cooperative jamming spectra based on security information factor achieves indeed good solution for LPID improvement in DMRS.

The achievable MI curves of the DMRS for different transmission waveforms are shown in Fig.3, which are obtained by conducting 10000 Monte Carlo trials. For both cases, it is obvious that the achievable MI is increased as the transmitting energy increases. While for a given total transmitting energy constraint, the larger MI can be achieved when using the optimal transmission waveforms. This is due to the fact that the predefined waveforms distribute uniform energy over the whole frequency band with no prior knowledge about the target spectra, which have the worse target estimation performance.

Similarly, the achievable MI of the intercept receiver when utilizing the optimal jamming spectra and the predefined jamming spectra are compared in Fig.4. The numerical results illustrate that the achievable MI of the intercept receiver is reduced as the jamming power increases, which again shows that employing cooperative jamming can undoubtedly improve the LPID performance for DMRS to defend against noncooperative interceptors. This is not surprising that the predefined jamming spectra has a larger MI of the intercept receiver than the optimal cooperative jamming spectra, which is because of the lack of the information about the transmission waveforms.

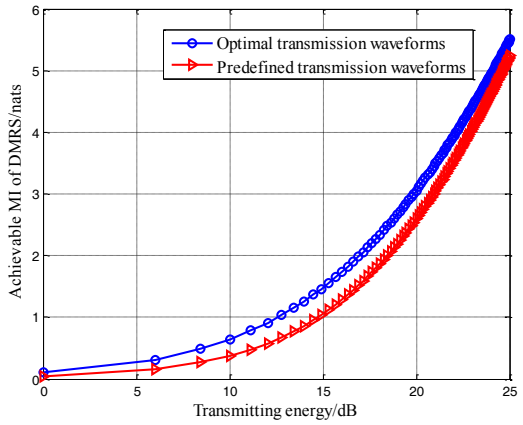

Fig.3 Achievable MI curves of the DMRS for different transmission waveforms

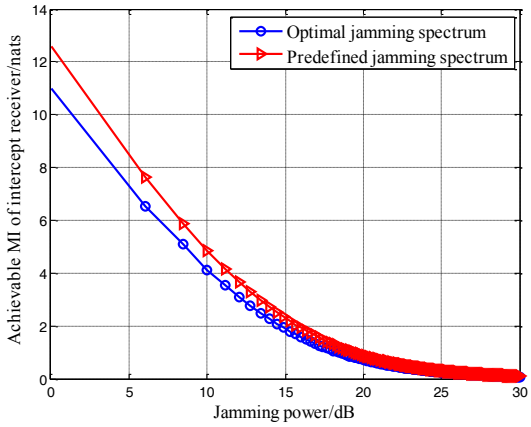

Fig.4 Achievable MI curves of the intercept receiver for different cooperative jamming spectra

5. CONCLUSION

In this paper, the problem of LPID performance improvement for DMRS based on security information factor is investigated, which maximizes the security information factor by optimizing the transmission waveforms and the cooperative jamming spectra for the given total transmission energy and cooperative jamming power constraints. It is worth pointing out that the optimal solutions can be achieved by explicit closed-form expressions. Numerical simulations are conducted to demonstrate that our presented strategy can improve the LPID performance for DMRS remarkably to defend against the hostile intercept receiver attacks, which provides useful guidance on the design of optimal transmission waveforms and cooperative jamming spectra for LPID enhancement. Future work will concentrate on other optimization criteria to facilitate improved LPID performance for DMRS.

6. REFERENCES

[1] E.P. Phillip, *Detecting and classifying low probability of intercept radar*, Boston: Artech House, 2009.

[2] E. Fisher, A. Haimovich, R.S. Blum, L.J. Cimini, D. Chizhik, and R.A. Valenzuela, "Spatial diversity in radars–models and detection performance," *IEEE Trans. on Signal Processing*, vol. 54, no. 3, pp. 823-836, 2006.

[3] C.G. Shi, F. Wang, M. Sellathurai, and J.J. Zhou, "LPI optimization framework for target tracking in radar network architectures using information-theoretic criteria," *International Journal of Antennas and Propagation*, vol. 2014, pp. 1-10, 2014.

[4] B. Friedlander, "Waveform design of MIMO radar," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 43, no. 3, pp. 1227-1238, 2007.

[5] P. Stoica, J. Li, and Y. Xie, "On probing signal design for MIMO radar," *IEEE Trans. on Signal Processing*, vol. 55, no. 8, pp. 4151-4161, 2007.

[6] B. Jiu, H.W. Liu, D.Z. Feng, and Z. Liu, "Minimax robust transmission waveform and receiving filter design for extended target detection with imprecise prior knowledge," *Signal Processing*, vol. 92, no. 1, pp. 210-218, 2012.

[7] M.R. Bell, "Information theory and radar waveform design," *IEEE Trans. on Information Theory*, vol. 39, no. 5, pp. 1578-1597, 1993.

[8] Y. Yang, and R. S. Blum, "MIMO radar waveform design based on mutual information and minimum mean-square error estimation," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 43, no. 1, pp. 330-343, 2007.

[9] R.A. Romero, J. Bae, and N.A. Goodman, "Theory and application of SNR and mutual information matched illumination waveforms," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 47, no. 2, pp. 912-926, 2011.

[10] Y.F. Chen, Y. Nijsure, C. Yuen, Y.H. Chew, and Z.G. Ding, "Adaptive distributed MIMO radar waveform optimization based on mutual information," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1374-1385, 2013.

[11] L. Xu, and Q. L. Liang, "Waveform design and optimization in radar sensor network," *2010 IEEE Conference on Global Telecommunication (GLOBECOM 2010)* , pp. 1-5, 2010.

[12] B. Tang, J. Tang, and Y.N. Peng, "MIMO radar waveform design in colored noise based on information theory," *IEEE Trans. on Signal Processing*, vol. 58, no. 9, pp. 4684-4697, 2010.

[13] M.M. Naghsh, M.H. Mahmoud, S.P. Shahram, M. Soltanalian, and P. Stoica, "Unified optimization framework for multi-static radar code design using information-theoretic criteria," *IEEE Trans. on Signal Processing*, vol. 61, no. 21, pp. 5401-5416, 2013.

[14] X.Y. Zhou, and M.R. Mckay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. on Vehicular Technology*, vol. 59, no. 8, pp. 3831-3842, 2010.

[15] J.P. Vilela, M. Bloch, J. Barros, and S.W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 2, pp. 256-266, 2011.

[16] Y.L. Zou, X.B. Wang, and W.M. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. on Communications*, vol. 61, no. 12, pp. 5103-5113, 2013.

[17] A. Mukherjee, and A.L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. on Signal Processing*, vol. 61, no. 1, pp. 82-91, 2013.

[18] R.Z. Nabil, D. Mclernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487-490, 2013.

[19] Y.Q. Zhao, C.L. Yu, and H.P. Yin, "Research into the anti-common-frequency interference technology based on code agility," *Shipboard electronic countermeasure*, vol. 36, no. 1, pp. 14-19, 32, 2013. (In Chinese)

[20] C.G. Shi, J. J. Zhou, and F. Wang, "Low probability of intercept optimization for radar network based on mutual information," *2014 IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)* , pp. 683-687, 2014.

[21] L.L. Wang, H.Q. Wang, K.K. Wong, and P.V. Brennan, "Minimax robust jamming techniques based on signal-to-interference-plus-noise ratio and mutual information criteria," *IET Communications*, vol. 8, no. 10, pp. 1859-1867, 2014.