Fuzzy Chance-Constrained Programming Based Security Information Optimization for Low Probability of Identification Enhancement in Radar Network Systems

Chenguang SHI, Fei WANG, Jianjiang ZHOU, Jun CHEN

Key Laboratory of Radar Imaging and Microwave Photonics, Ministry of Education, Nanjing University of Aeronautics and Astronautics, No. 29, Yudao Street, Qinhuai District, Nanjing city, Jiangsu Province, Nanjing 210016, P. R. China

zjjee@nuaa.edu.cn

Abstract. *In this paper, the problem of low probability of identification (LPID) improvement for radar network systems is investigated. Firstly, the security information is derived to evaluate the LPID performance for radar network. Then, without any prior knowledge of hostile intercept receiver, a novel fuzzy chance-constrained programming (FCCP) based security information optimization scheme is presented to achieve enhanced LPID performance in radar network systems, which focuses on minimizing the achievable mutual information (MI) at interceptor, while the attainable MI outage probability at radar network is enforced to be greater than a specified confidence level. Regarding to the complexity and uncertainty of electromagnetic environment in the modern battlefield, the trapezoidal fuzzy number is used to describe the threshold of achievable MI at radar network based on the credibility theory. Finally, the FCCP model is transformed to a crisp equivalent form with the property of trapezoidal fuzzy number. Numerical simulation results demonstrating the performance of the proposed strategy are provided.*

Keywords

Security information, low probability of identification (LPID), power allocation, fuzzy chance-constrained programming (FCCP), radar network systems

1. Introduction

Radar network architecture, which often refers to distributed multiple-input multiple-output (MIMO) radar [1], is pioneered by Fisher in [2] and has drawn considerable attentions due to its advantage of signal and spatial diversities. Moreover, radar network outperforms traditional monostatic radar in target detection, localization accuracy and information extraction [3].

Recent years have witnessed an increasing interest on the radar network configuration which has been extensively studied from various perspectives. The authors in [4] consider the optimal waveform design for MIMO radar in colored noise based on maximization of mutual information (MI) and relative entropy. Yang and Blum present two radar waveform design schemes with constraints on waveform power [5]: the one is maximization of the MI between the target impulse response and the reflected waveform, the other is minimization of the minimum mean-square error (MMSE) in estimating the target impulse response. A novel two-stage waveform optimization algorithm for distributed MIMO radar is proposed in [6], where it is demonstrated that this method can provide great performance improvement in target information extraction. In [7], the authors present three power allocation criteria integrating propagation losses into distributed MIMO radar signal model: maximizing the MI, minimizing the MMSE and maximizing the echo energy. Shi et al. in [8], [9] investigate the low probability of intercept (LPI) optimization strategies in radar network configurations for the first time, which are shown to be effective to enhance the LPI performance for radar networks.

In recent years, pursing high physical-layer (PHY) security is becoming a central issue in wireless communications, in which secrecy capacity is utilized as a metric for secrecy communication performance [10]. In [11], the authors study the use of artificial interference in maximizing secrecy capacity, where a portion of the transmitting power is allocated to broadcast the information signal with enough power to guarantee a certain signal-to-interference-plus-noise ratio (SINR) for the intended receiver, while the rest of the power is utilized to broadcast artificial interference to jam the passive eavesdroppers. Zhou et al. in [12] investigate the problem of secure communication in fading channels. While [13] proposes an optimization strategy for achieving security over multiple-input single-output (MISO) channels by beamforming and artificial interference combined with the "protected zone". Mukherjee and Swindlehurst model the interactions between the legitimate transmitter and active eavesdropper as a two-person zero-sum game [14]. The authors in [15] present a multiuser scheduling algorithm to improve the cognitive transmission security. Further, Wang et al. in [16] propose security

information factor to evaluate radar radio frequency (RF) stealth, where it is illustrated airborne radar RF stealth effects based on security information factor concept under some conditions. Shi et al. extend the work in [16] and provide a security information based optimal power allocation scheme for LPID performance in radar networks [17], [18].

However, most researches on secrecy capacity are mainly towards maximizing the secrecy rate for communication with guaranteeing system requirements. The use of security information for LPID performance in radar network systems has rarely been studied previously, which motivates us to consider this problem. In addition, the modern electromagnetic environment is becoming more and more complicated, large difficulties for radar mission are caused by amounts of uncertain factors in electronic warfare, which cannot be completely solved by stochastic theory. The theory of fuzzy set has drawn considerable attentions since this concept was initiated by Zadeh [19] in 1965. In 2002, Liu [20] proposed the concept of credibility measure, and established the theory of fuzzy chance-constrained programming (FCCP) [21], which is a branch of mathematics for studying fuzzy phenomena.

This paper will investigate the FCCP based security information optimization for LPID enhancement in radar networks. The main contributions of this paper are summarized as follows. Firstly, we derive an analytical closed-form expression of security information. Secondly, when the prior knowledge of intercept receiver is unavailable, a novel FCCP based security information optimization algorithm is formulated to minimize the achievable MI at intercept receiver, while the achievable MI outage probability at radar network is enforced to be greater than a specified confidence level. Regarding to the complexity and uncertainty of electromagnetic environment in the modern electronic warfare, the trapezoidal fuzzy number is utilized to describe the threshold of achievable MI at radar network. Finally, the FCCP model is transformed to a crisp equivalent form with the property of credibility theory. Numerical simulations are provided to demonstrate that our proposed algorithm can improve the LPID performance for radar networks to defend against passive intercept receivers. To the best of authors' knowledge, no literature discussing FCCP based security information optimization for improved LPID performance in radar network systems was conducted prior to this work.

The remainder of this paper is organized as follows. Section 2 introduces the basic concepts of credibility theory and the system model for radar network. We first derive the analytical closed-form expression of security information with cooperative jamming (CJ) for radar network in Sec. 3 and formulate the FCCP based security information optimization algorithm for radar network system. Section 4 provides some numerical simulation results. Finally, conclusion remarks are drawn in Sec. 5.

2. Preliminaries and System Model

2.1 Credibility Theory

The theory of fuzzy set has received close attention by the scientific community over the last several decades, which was pioneered by Zadeh via membership function in 1965. In 1978, Zadeh presented the concept of possibility measure, which is utilized to measure a fuzzy set. Although possibility measure has been widely used in both theory and practice, it has no self-duality property. In 2002, Liu proposed the concept of credibility measure to define a self-dual measure. After that, Liu established the credibility theory in 2004, which is a branch of mathematics for studying fuzzy phenomena. Some basic concepts of credibility theory are provided in the following.

Definition 2.1: (Liu & Liu [20]) Let Θ be a nonempty set, and P the power set of Θ. The set function Cr is called a credibility measure if it satisfies the following four axioms:

Axiom 1: $Cr\{\Theta\}=1$.

Axiom 2: $Cr\{A\}\le Cr\{B\}$, whenever $A\subset B$.

Axiom 3: $Cr\{A\}+Cr\{A^c\}=1$ for any event $A\in P$.

Axiom 4: $Cr\{\cup_i A_i\}=\sup_i Cr\{A_i\}$ for any events $\{A_i\}$ with $\sup_i Cr\{A_i\}<0.5$.

Then, the triplet (Θ,P,Cr) is called a credibility space.

Definition 2.2: (Liu [21]) A fuzzy variable is a measurable function from a credibility space (Θ,P,Cr) to the set of real numbers $\Re$.

Definition 2.3: (Liu [21]) Let ξ be a fuzzy variable defined on the credibility space (Θ,P,Cr). Then its membership function is derived from the credibility measure by:

$$\mu(x)=\left(2Cr\{\xi=x\}\right)\wedge 1,\quad x\in\Re. \tag{1}$$

Theorem 2.1 (Credibility Inversion Theorem): (Liu [21]) Let ξ be a fuzzy variable with membership function $\mu(x)$. Then for any set B of real numbers, we have:

$$Cr\{\xi\in B\}=\frac{1}{2}\left(\sup_{x\in B}\mu(x)+1-\sup_{x\in B^c}\mu(x)\right). \tag{2}$$

Definition 2.4: (Liu [21]) The credibility distribution $\Phi:\Re\to[0,1]$ of a fuzzy variable ξ is defined by:

$$\Phi(x)=Cr\{\theta\in\Theta\mid\xi(\theta)\le x\}. \tag{3}$$

That is, $\Phi(x)$ is the credibility that the fuzzy variable ξ takes a value less than or equal to x.

2.2 Radar Network SNR Equation

Let us consider a radar network system with N_t transmitters and N_r receivers, which can be broken down into $N_t \times N_r$ transmitter-receiver pairs each with a bistatic component contributing to the entirety of the radar network signal-to-noise ratio (SNR), as depicted in Fig. 1. The radar network system has a common precise knowledge of space and time. In addition, it is worth pointing out that orthogonal polyphase codes are utilized in radar network system, which have a large main lobe-to-side lobe ratio. These codes have a more complicated signal structure making it harder to intercept and identify by a noncooperative intercept receiver.

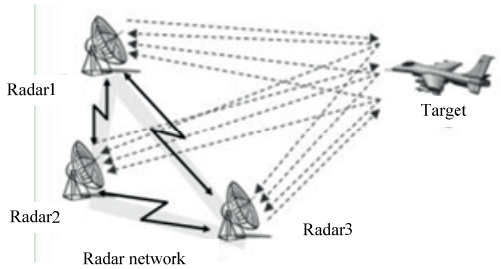

Fig. 1. Example of a radar network.

The radar network SNR can be calculated by summing up the SNR of each transmit-receive pair as in [1]:

$$SNR_{net} = \sum_{m=1}^{N_t}\sum_{n=1}^{N_r} \frac{P_{tm} G_{tm} G_{rn} \sigma_{tmn} \lambda_m^2}{(4\pi)^3 k T_{omn} B_{rm} F_{rn} R_{tm}^2 R_{rn}^2 L_{mn}} \tag{4}$$

where the P_{tm} is the m th transmitter power, G_{tm} is the mth transmit antenna gain, G_{rn} is the n th receive antenna gain, σ_{tmn} is the radar cross section (RCS) of the target for the mth transmitter and nth receiver, λ_m is the m th transmitted wavelength, k is Boltzmann's constant, T_{omn} is the receiving system noise temperature at the n th receiver, B_{rm} is the bandwidth of the matched filter for the mth transmitted waveform, F_{rn} is the noise factor for the nth receiver, L_{mn} is the system loss between the mth transmitter and nth receiver, R_{tm} is the distance from the mth transmitter to the target and R_{rn} is the distance from the target to the nth receiver.

2.3 Radar Network Signal Model

Let K denote the discrete time index, then we can express the radar network signal model as:

$$\boldsymbol{Y}_r = \boldsymbol{X}\boldsymbol{H}_r + \boldsymbol{W}_r \tag{5}$$

where $\boldsymbol{X} = [\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{N_t}] \in \mathbb{C}^{K \times N_t}$, is the set of transmission sequences, $\boldsymbol{H}_r = [\boldsymbol{h}_{r1}, \boldsymbol{h}_{r2}, \ldots, \boldsymbol{h}_{rN_t}] \in \mathbb{C}^{N_t \times N_r}$ refers to the path gain matrix for radar network system, $\boldsymbol{W}_r = [\boldsymbol{w}_{r1}, \boldsymbol{w}_{r2}, \ldots, \boldsymbol{w}_{rN_r}] \in \mathbb{C}^{K \times N_r}$ represents the system noise, and the received signal matrix can be written as $\boldsymbol{Y}_r = [\boldsymbol{y}_{r1}, \boldsymbol{y}_{r2}, \ldots, \boldsymbol{y}_{rN_t}] \in \mathbb{C}^{K \times N_r}$. For convenience, it is assumed that the noise matrix $\boldsymbol{W}_r$ does not depend on the transmitted waveform $\boldsymbol{X}$, and $\boldsymbol{H}_r$ and $\boldsymbol{W}_r$ are mutually independent.

According to the discussions in [7], the path gain $\boldsymbol{h}_{rn}$ contains the target reflection coefficient g_{mn} and the propagation loss factor p_{mn}. Based on the central limit theorem, $g_{mn} \sim CN(0, \sigma_g^2)$, where g_{mn} denotes the target reflection gain between the radar m and radar n. The propagation loss factor p_{mn} can be expressed as:

$$p_{mn} = \frac{\sqrt{G_{tm} G_{rn}}}{R_{tm} R_{rn}}. \tag{6}$$

Furthermore, with the consideration of propagation losses and target scattered matrix, the radar network signal model (5) can be rewritten as:

$$\boldsymbol{Y}_r = \boldsymbol{X}(\boldsymbol{G} \odot \boldsymbol{P}) + \boldsymbol{W}_r \tag{7}$$

where $\boldsymbol{G} = [\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_{N_r}]$, $\boldsymbol{P} = [\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_{N_r}]$, $\boldsymbol{w}_{rn} \sim \boldsymbol{CN}(0, \sigma_{w_r}^2 \boldsymbol{I}_K)$, and $\odot$ denotes the Hadamard product.

3. Problem Formulation

3.1 Security Information for Radar Network Systems

With the definition of MI in [17], [18], we can obtain the MI between the transmitting signal of radar network $\boldsymbol{X}$ and the backscatter signal $\boldsymbol{Y}_r$ as follows:

$$\begin{aligned} \boldsymbol{I}(\mathrm{X}, \mathrm{Y_r}) &= \boldsymbol{H}(\mathrm{Y_r}) - \boldsymbol{H}(\mathrm{Y_r} \mid \mathrm{X}) \\ &= \boldsymbol{H}(\mathrm{Y_r}) - \boldsymbol{H}(\mathrm{W_r}) \\ &= \sum_{m=1}^{N_t}\sum_{n=1}^{N_r} \ln\left(1 + \frac{P_{tm}\sigma_g^2 p_{mn}^2}{\sigma_{w_r}^2}\right) \\ &= \sum_{m=1}^{N_t}\sum_{n=1}^{N_r} \ln\left(1 + \frac{P_{tm}\sigma_g^2 G_{tm} G_{rn}}{\sigma_{w_r}^2 R_{tm}^2 R_{rn}^2}\right) \triangleq I_{net}(P_r) \end{aligned} \tag{8}$$

where $\boldsymbol{I}(\boldsymbol{X}, \boldsymbol{Y}_r)$ is the MI between $\boldsymbol{Y}_r$ and $\boldsymbol{X}$, $\boldsymbol{H}(\boldsymbol{Y}_r)$ is the entropy of backscatter signal, and $\boldsymbol{H}(\boldsymbol{W}_r)$ is the entropy of Gaussian white noise.

Similarly, we can express the MI between the transmitting signal of radar network $\boldsymbol{X}$ and the received signal of intercept receiver $\boldsymbol{Y}_i$ as:

$$\begin{aligned} I(\boldsymbol{X}, \boldsymbol{Y}_i) &= H(\boldsymbol{Y}_i) - H(\boldsymbol{Y}_i \mid \boldsymbol{X}) \\ &= \sum_{m=1}^{N_t} \ln\left(\boldsymbol{1} + \frac{P_{tm} G_{tm} G_{int}}{\sigma_{w_i}^2 R_{tm}^2}\right) \end{aligned} \tag{9}$$

where G_{int} is the antenna gain of intercept receiver, $\sigma_{w_i}^2$ denotes the noise covariance of intercept receiver.

As introduced in [17], [18], in modern electronic warfare, cooperative jammer is indispensable to keep the radar network in LPID state. This means that CJ is to jam the hostile intercept receiver so that the achievable MI at interceptor can be degraded by the CJ signals while the radar network system is unaffected. With the consideration of CJ, we can modify (12) as follows:

$$I\left(\boldsymbol{X},\boldsymbol{Y}_i\right)=\sum_{m=1}^{N_t}\ln\left[1+\frac{P_{tm}G_{tm}G_{\text{int}}}{\left(\sigma_{w_i}^2+\dfrac{P_jG_jG_{\text{int}}}{R_j^2}\right)R_{tm}^2}\right]\triangleq I_{\text{int}}\left(P_r,P_j\right)\quad(10)$$

where P_j is the total transmitting power for CJ signal, G_j is the antenna gain of cooperative jammer, R_j is the distance from the target to cooperative jammer.

For convenience, we assume that the radar network system can simultaneously transmit radar modulating signal to track target and CJ signal to interfere passive intercept receiver for simplicity of discussion, while the CJ signal is designed to be completely orthogonal to radar modulating signal and generated to jam the intercept receiver without affecting the radar network.

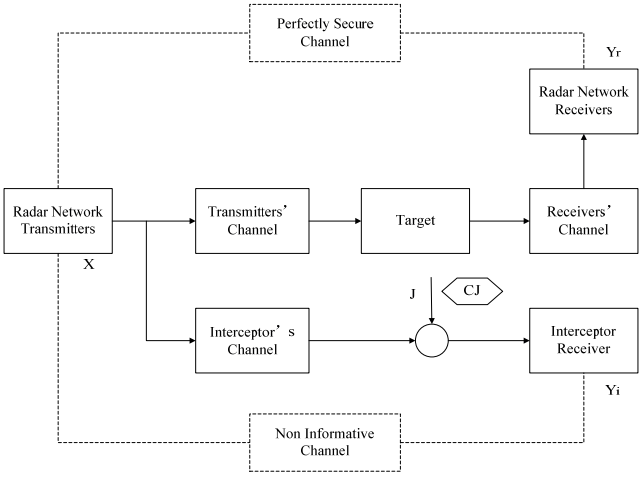

Fig. 2. The notional sketch of our proposed perfectly secure radar network system.

For simplicity of derivation, it is supposed that:

$$R_{net}^2\approx R_{ti}R_{rj}\left(\forall m=1,\ldots,N_t,n=1,\ldots,N_r\right),\quad(11)$$

$$P_{tm}=\frac{P_r}{N_t}\left(\forall m=1,\ldots,N_t\right)\quad(12)$$

where R_{net} is approximately the distance from target to radar network system, P_r is the total transmitting power for radar modulating signal. It is also assumed that each netted radar node in the network is the same. Therefore, originating from the secrecy capacity in wireless communications, we define security information to measure the LPID performance for radar network system [17], [18]:

$$\begin{aligned}&I_{\text{sec}}\left(P_r,P_j\right)\\&\triangleq\left[I_{net}\left(P_r\right)-I_{\text{int}}\left(P_r,P_j\right)\right]^+\\&\doteq\left\{\begin{array}{l}N_tN_r\ln\left(1+\dfrac{P_r\sigma_g^2G_tG_r}{N_t\sigma_{w_r}^2R_{net}^4}\right)\\-N_t\ln\left[1+\dfrac{P_rG_tG_{\text{int}}}{N_t\left(\sigma_{w_i}^2+\dfrac{P_jG_jG_{\text{int}}}{R_j^2}\right)R_{net}^2}\right]\end{array}\right\}^+\end{aligned}\quad(13)$$

where $[x]^+=\max(0,x)$. It has been pointed out in [17], [18] that $I_{\text{sec}}>0$ means that radar network is in completely secure state while tracking target, and that the larger the achievable security information I_{sec} obtained, the better LPID performance to finish the system mission.

The notional sketch of our proposed perfectly secure radar network system is illustrated in Fig. 2. This amounts to say that, if the radar network system experiences an SNR higher than that of the noncooperative intercept receiver, a positive rate can be sustained, while the intercept receiver gets maximally confused based on the utilized secrecy criterion in (13).

3.2 FCCP Based Security Information Optimization

In practical applications, it would be impossible to suppose that any prior information about the hostile intercept receiver is available, such as the sensitivity of interceptor, the processing gain, et al. The system model is illustrated in Fig. 3, where the target and the intercept receiver are separated at different places.

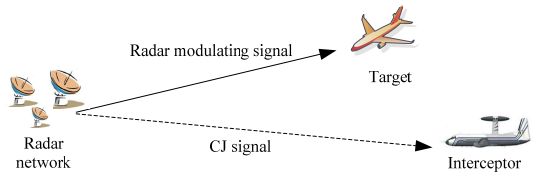

Fig. 3. The geometry of radar network, target and interceptor.

With the derivation of security information as (13), we can observe that security information is based on satisfying MI constraints both at radar network and at intercept receiver. With a proper choice of the power allocation, a perfectly securing channel can be devised such that:

$$\left.\begin{array}{l}I_{net}\left(P_r\right)\ge\delta^{th}\\I_{\text{int}}\left(P_r,P_j\right)\overset{P_j\to\infty}{\to}0\end{array}\right\}\quad(14)$$

where δ^{th} is the predefined threshold of MI at radar network. Equation (14) means asymptotically perfect security in radar network system.

In this paper, we focus on minimizing the achievable MI at intercept receiver $I_{\text{int}}(P_r, P_j)$ to guarantee a predefined threshold of MI at radar network δ^{th}. To be more specific, minimization of the achievable MI at noncooperative intercept receiver can significantly defend against interceptor, showing LPID performance enhancement of exploiting CJ when any prior knowledge about the intercept receiver is unavailable.

The security information optimization strategy can be summarized as follows:

1) Specify the desired MI threshold δ^{th} for radar network system, which is utilized as a metric for target detection performance.
2) Allocate some transmission power to achieve the desired MI threshold δ^{th} for target detection.
3) Minimize the achievable MI at intercept receiver $I_{\text{int}}(P_r, \mathrm{P}_j)$ by distributing the remaining transmission power to yield as much interference as possible, while guaranteeing that the CJ signal is designed to be completely orthogonal to radar modulating signal and generated to jam the intercept receiver without affecting the radar network.

Hence, the security information optimization for enhanced LPID performance can be formulated as:

$$\left.\begin{aligned} &\min_{P_r,P_j} \; I_{\text{int}}\left(P_r,P_j\right) \\ &s.t.:\; I_{net}\left(P_r\right) \ge \delta^{th} \\ &\quad P_r + P_j \le P_{tot}^{\max} \\ &\quad P_r \in \left(0, P_r^{\max}\right] \end{aligned}\right\} \tag{15}$$

where $P_{tot}{}^{\max}$ is the maximum transmitting power for radar network, $P_r{}^{\max}$ is the maximum transmitting power for radar modulating signal. While regarding to the complexity and uncertainty of electromagnetic environment in the modern electronic warfare, the predefined threshold of MI at radar network δ^{th} would be uncertain. Herein, a fuzzy variable δ^{th}_{fuzzy} is utilized to evaluate the predefined threshold of MI at radar network. Based on the concepts of credibility theory, the achievable MI outage probability at radar network is enforced to be greater than a specified confidence level α, that is:

$$Cr\left\{I_{net}\left(P_r\right) \ge \delta^{th}_{fuzzy}\right\} \ge \alpha \tag{16}$$

where $Cr\{\cdot\}$ indicates the credibility that $\{\cdot\}$ will occur. Therefore, we have the FCCP based security information optimization for LPID enhancement in radar network as:

$$\left.\begin{aligned} &\min_{P_r,P_j} \; I_{\text{int}}\left(P_r,P_j\right) \\ &s.t.:\; Cr\left\{I_{net}\left(P_r\right) \ge \delta^{th}_{fuzzy}\right\} \ge \alpha \\ &\quad P_r + P_j \le P_{tot}^{\max} \\ &\quad P_r \in \left(0, P_r^{\max}\right] \end{aligned}\right\} \tag{17}$$

With the FCCP model (17), we can observe that increasing the confidence level leads to enlarging the feasible set of the true problem, which in turn may result in decreasing of the optimal value of the true problem [22]. It is also worth pointing out that there exists a restrictive relationship between the confidence level and the achievable MI at intercept receiver.

3.3 The Crisp Equivalent Form of FCCP Model

The FCCP model (17) is a fuzzy linear programming, which can be transformed into the crisp equivalent form. In this paper, we set $\delta^{th}_{fuzzy} = (a, b, c, d)$ $(a < b \le c < d)$ to be a trapezoidal fuzzy variable.

Definition 3.1: (Liu, Zhao & Wang [23]) By a trapezoidal fuzzy variable, we mean that the fuzzy variable fully determined by the quadruplet $\left(r_1, r_2, r_3, r_4\right)$ of crisp numbers with $r_1 < r_2 \le r_3 < r_4$, whose membership function is given by:

$$\mu\left(x\right) = \begin{cases} \dfrac{x - r_1}{r_2 - r_1}, & \text{if } r_1 \le x \le r_2 \\ 1, & \text{if } r_2 \le x \le r_3 \\ \dfrac{x - r_4}{r_3 - r_4}, & \text{if } r_3 \le x \le r_4 \\ 0, & \text{else} \end{cases} \tag{18}$$

Definition 3.2: (Liu, Zhao & Wang [23]) The credibility distribution of a trapezoidal fuzzy variable $\left(r_1, r_2, r_3, r_4\right)$ is:

$$\Phi\left(x\right) = \begin{cases} 0, & \text{if } x \le r_1 \\ \dfrac{x - r_1}{2\left(r_2 - r_1\right)}, & \text{if } r_1 \le x \le r_2 \\ \dfrac{1}{2}, & \text{if } r_2 \le x \le r_3 \\ \dfrac{x - 2r_3 + r_4}{2\left(r_4 - r_3\right)}, & \text{if } r_3 \le x \le r_4 \\ 1, & \text{if } r_4 \le x \end{cases} \tag{19}$$

Theorem 3.1: (Liu [24]) If ξ is a trapezoidal fuzzy number $\xi = \left(r_1, r_2, r_3, r_4\right)\left(r_1 < r_2 \le r_3 < r_4\right)$, for the given confidence level $\alpha \in \left(0.5, 1\right]$, the following equivalent transformation can be derived as:

$$Cr\left\{\xi \ge x\right\} \ge \alpha \Leftrightarrow x \le \left(2\alpha - 1\right)r_1 + \left(2 - 2\alpha\right)r_2, \tag{20a}$$

$$Cr\left\{\xi \le x\right\} \ge \alpha \Leftrightarrow x \ge \left(2 - 2\alpha\right)r_3 + \left(2\alpha - 1\right)r_4. \tag{20b}$$

Based on the properties of trapezoidal fuzzy number, we have that:

$$Cr\left\{I_{net}\left(P_r\right) \ge \delta^{th}_{fuzzy}\right\} \ge \alpha \Leftrightarrow I_{net}\left(P_r\right) \ge 2\left(1 - \alpha\right)c + \left(2\alpha - 1\right)d \tag{21}$$

The proposed FCCP based security information algorithm (17) could be transformed into the following

crisp equivalent form:

$$\left.\begin{aligned} &\min_{P_r,P_j} \ I_{\text{int}}\left(P_r,P_j\right) \\ &s.t.:\ I_{net}\left(P_r\right)\geq 2\left(1-\alpha\right)c+\left(2\alpha-1\right)d \\ &P_r+P_j\leq P_{tot}^{\max} \\ &P_r\in\left(0,P_r^{\max}\right] \end{aligned}\right\} \tag{22}$$

Problem (17) takes radar network mission δ^{th}_{fuzzy} into consideration because radar network system must accomplish its mission in modern battlefield. To be specific, for the predetermined system detection probability P_d^{net} and false alarm probability P_{fa}^{net}, if $Cr\{I_{\text{net}}(P_r)\geq\delta^{th}_{fuzzy}\}\geq\alpha$ and $I_{\text{sec}}(P_r, P_j)>0$, the detection probability of intercept receiver P_d^{int} would be significantly less than 0.5, which means that the interceptor could not intercept and identify radar modulating signal, and that the radar network system is in completely LPID state [16].

Based on the above derivations as (13) and (22), it is worth pointing out the simplicity of the proposed algorithm which relies on basic mathematical calculations and does not require highly complex computation. Moreover, our proposed algorithm is significantly simple to implement.

So far, we have completed the achievable security information derivation and the FCCP based security information optimization for LPID enhancement in radar network systems. In what follows, some numerical simulations are provided to show the feasibility and effectiveness of our presented algorithm.

4. Numerical Simulations and Analysis

In this section, we evaluate the proposed algorithm through some numerical simulations. Let us consider a 4×4 radar network architecture ($N_t=N_r=4$), which is depicted in Fig. 4 that the netted radars in the network are spatially distributed in the surveillance area.

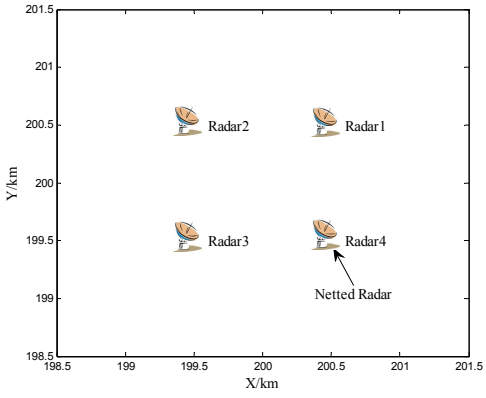

Fig. 4. The radar network system configuration in two dimensions.

Herein, we set the simulation parameters $P_{tot}^{\max}=P_r+P_j=25$ kW, $G_t=G_r=G_j=30$ dB, $G_i=0$ dB, $\sigma_{w_r}^2=4.57\times10^{-12}$ W, $\sigma_{w_i}^2=8.77\times10^{-8}$ W and $\sigma_g^2=1$. The radar network can detect the target whose RCS is 1 m^2 in the distance 180 km by transmitting the maximum power $P_r^{\max}=24$ kW. The sensitivity of intercept receiver $S_{i\min}$ is set to be –80 dBmW. Based on some experimental data, the trapezoidal fuzzy number is set to be $\delta^{th}_{fuzzy}=$ (4.4, 8.1, 13.0, 25.6)nats, which equals to the fuzzy SNR (7.0, 10.2, 13.0, 18.0) dB. This is because that the radar network system can track the target steadily when the SNR is between 10.0 dB and 13.0 dB, and the value of the membership function is set to be 1.

4.1 Security Information Analysis

As shown in Fig. 5, for all the cases $N_r=1$, $N_r=2$ and $N_r=4$, with an increasing N_t, the achievable security information is increased correspondingly. As the number of transmitters N_t continues increasing beyond a certain value, the achievable security information of (16) leads to approximate constant. Fig. 5 also demonstrates that as the number of receivers increases from $N_r=1$ to $N_r=4$, the achievable security information for radar network can be significantly increased. To be specific, increasing the number of radars can effectively improve security information for radar network. This is because that radar network can offer great transmit and receive diversities in terms of the achievable security information, which confirms the LPID benefits by exploiting radar network system to defend against passive intercept receiver attacks.

Figure 6 shows the achievable security information versus R_{net} with $P_r=25$ kW, $P_j=5$ kW and different R_j. It can be seen from Fig. 6 that as R_{net} and R_j decrease, the achievable security information is increased as theoretically proved in (16). Furthermore, it is depicted that with the same R_{net}, the available security information can be increased as R_j decreases, which shows the advantage of exploiting CJ to defend against intercept receiver.

Figure 7 illustrates achievable MI at intercept receiver versus the confidence level α at radar network for different sensitivities of intercept receiver $S_{i\min}$ with $R_{net}=$ 100 km and $R_j=300$ km. In Fig. 7, for all the cases, one can observe that the achievable MI at intercept receiver is

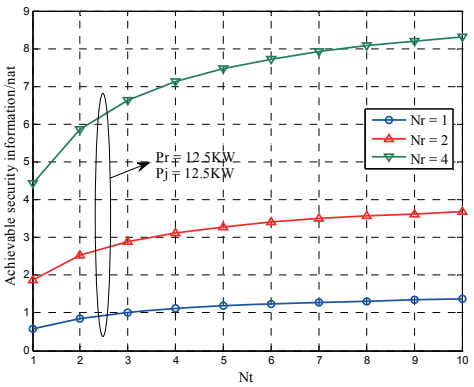

Fig. 5. Achievable security information versus the number of transmitters N_t for different number of receivers N_r with $R_{net}=150$ km, $R_j=250$ km, and $P_r=P_j=12.5$ kW.

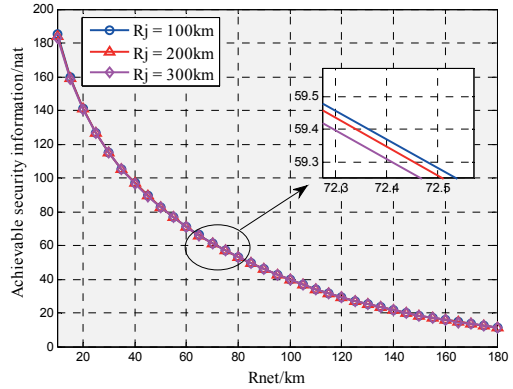

Fig. 6. Achievable security information versus R_{net} with P_r =20 kW, P_j =5 kW and different R_j .

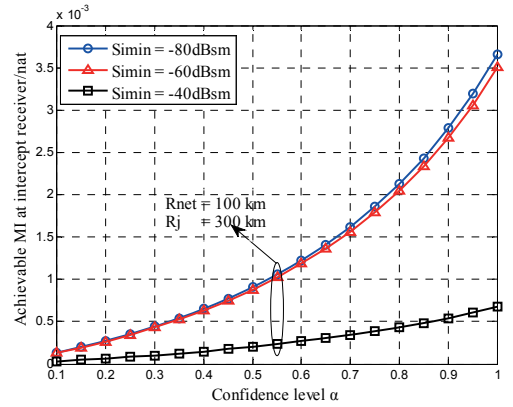

Fig. 7. Achievable MI at intercept receiver versus the confidence level α at radar network for different sensitivities of intercept receiver S_{imin} with R_{net} = 100 km and R_j = 300 km.

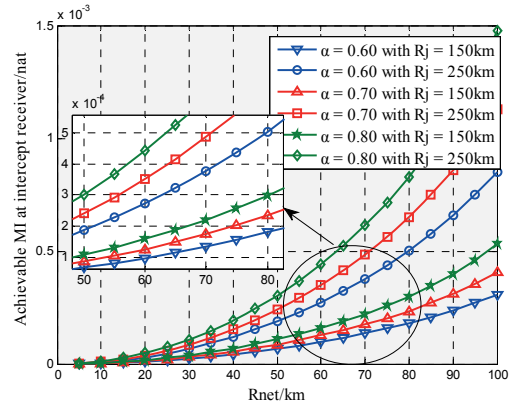

Fig. 8. Achievable MI at intercept receiver versus R_{net} for different confidence levels α and different R_j.

increased as the confidence level α at radar network increases, which shows that there exists a restrictive relationship between the confidence level α and the achievable MI at intercept receiver. This is due to the fact that more radar modulating signal would be transmitted to satisfy the system requirement with the increase of confidence level at radar network. The radar modulating signal could be intercepted by interceptor easily, and the achievable MI at intercept receiver will increase subsequently. Moreover, the achievable MI at intercept receiver is reduced as the sensitivity of intercept receiver S_{imin} decreases.

In Fig. 8, we depict the achievable MI at intercept receiver versus the distance between radar network and target R_{net} for different confidence levels at radar network α and different distances between radar network and intercept receiver R_j. One can observe from Fig. that for all the cases, the achievable MI at intercept receiver is increased as the distance between radar network and target increases from R_{net} = 5 km to R_{net} = 100 km. As mentioned before, this is because that more radar modulating signal is transmitted to satisfy the requirement for target detection as R_{net} increases, so less power is remained to generate CJ signal to jam the intercept receiver. Moreover, one can observe that as the distance between radar network and intercept receiver R_j decreases, the MI at interceptor is reduced, showing the LPID performance enhancement of exploiting CJ to defend against interceptors in radar network system.

4.2 Target Tracking with FCCP Based Security Information Optimization

This subsection presents the numerical results of our proposed security information optimization scheme in target tracking scenario. We track a single target by employing particle filtering (PF) method. For simplicity, it is assumed that the passive intercept receiver is carried by the target. Figure 9 shows one realization of the target trajectory for 50 s. Figure 10 illustrates the distance changing curve between radar network and target.

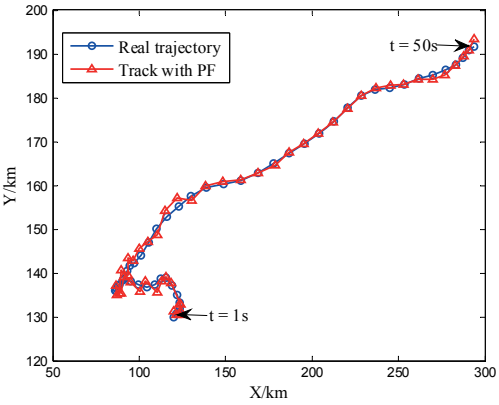

Fig. 9. Target tracking scenario.

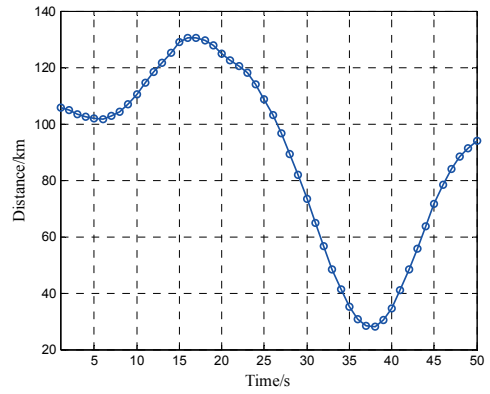

Fig. 10. The distance between the radar network and the target.

Figure 11 illustrates the achievable MI at intercept receiver with different confidence levels. We can see from Fig. 11 that the achievable MI at intercept receiver is increased as the confidence level increases. This is due to the fact that more radar modulating signal will be allocated to satisfy the system requirement with the increase of confidence level at radar network, in which way the radar signal would be intercepted and identified by hostile interceptor easily. It is also worth pointing out that the achievable MI at interceptor changes accordingly with the distance between radar network and target. To be specific, when the target is far away from the radar network, the network system would allocate more power for modulating signal to obtain a better capability of radar network to estimate the target. In contrast, as the distance decreases, more power for CJ signal could be transmitted to defend against the passive intercept receiver, which makes the achievable security information robust in terms of LPID performance.

In Fig. 12, we compare the performance of the proposed FCCP based security information optimization algorithm, the energy-efficiency based algorithm [17] and the adaptive security information optimization algorithm [18]. The algorithm provided in [17] aims at optimizing the energy-efficiency and will terminate to maintain certain security information, while the algorithm proposed in [18] aims at the optimization of the overall security information

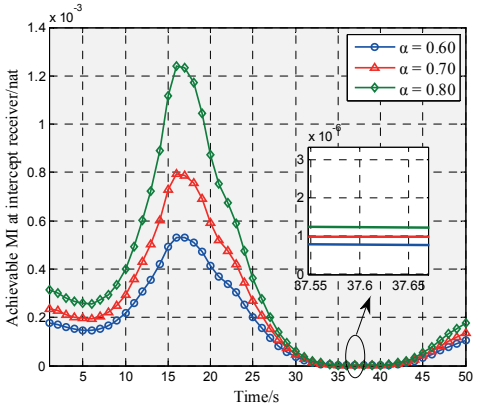

Fig. 11. Achievable MI at intercept receiver in the tracking process.

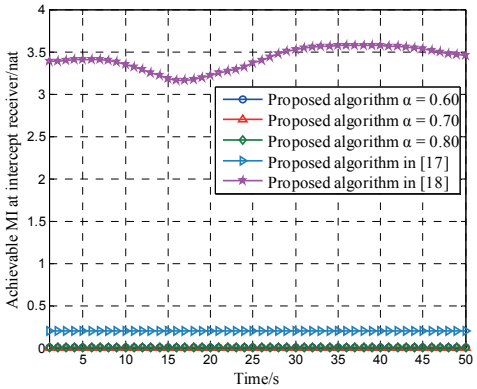

Fig. 12. Achievable MI at intercept receiver of various algorithms.

by optimizing the transmission power allocation between radar modulating signal and CJ signal. As Fig. 12 shows, the proposed algorithm significantly outperforms the algorithms proposed in [17] and [18], which is due to the fact that the achievable MI at interceptor is remarkable lower than that of the compared algorithms across the whole region. In addition, the proposed algorithm is more practical than the algorithm proposed in [18] because of the former's lower complexity.

4. Conclusions

This paper has proposed a novel FCCP based security information optimization algorithm to achieve improved LPID performance in radar network systems without any prior knowledge of noncooperative intercept receiver, whose purpose is to minimize the achievable MI at interceptor, while the achievable MI outage probability at radar network is enforced to be greater than a specified confidence level. It is worth pointing out that our proposed algorithm is presented by simple analytical closed-form expression. Simulation results demonstrate that our proposed algorithm is effective to enhance LPID performance for radar network to defend against passive interceptor attacks. For future research, other optimization criteria need to be addressed to improve LPID performance for radar network systems.

Acknowledgements

The authors would like to thank the anonymous reviewers for their comments that help to improve the quality of this article. The support provided by the National Natural Science Foundation of China (Grant No. 61371170), the Fundamental Research Funds for the Central Universities (Grant No. NJ20140010), Funding of Jiangsu Innovation Program for Graduate Education (CXLX13_154), the Fundamental Research Funds for the Central Universities, the Priority Academic Program Development of Jiangsu Higher Education Institutions (PADA) and Key Laboratory of Radar Imaging and Microwave Photonics (Nanjing Univ. Aeronaut. Astronaut.), Ministry of Education, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China are gratefully acknowledged.

References

[5] PACE, P. E. *Detecting and Classifying Low Probability of Intercept Radar*. Boston: Artech House, 2009, p. 342–352.

[6] FISHER, E., HAIMOVICH, A., BLUM, R. S., CIMINI, L. J., CHIZHIK, D., VALENZUELA, R. A. Spatial diversity in radars: models and detection performance. *IEEE Transactions on Signal Processing*, 2006, vol. 54, no. 3, p. 823–838. DOI: 10.1109/TSP.2005.862813

[3] HAIMOVICH, A. M., BLUM, R. S., CIMINI, L. J. JR. MIMO radar with widely separated antennas. *IEEE Signal Processing Magazine*, 2008, vol. 25, no. 1, p. 116–129. DOI: 10.1109/MSP.2008.4408448

[4] TANG, B., TANG, J., PENG, Y. N. MIMO radar waveform design in colored noise based on information theory. *IEEE Transactions on Signal Processing*, 2010, vol. 58, no. 9, p. 4684–4697. DOI: 10.1109/TSP.2010.2050885

[5] YANG, Y., BLUM, R. S. MIMO radar waveform design based on mutual information and minimum mean-square error estimation. *IEEE Transactions on Aerospace and Electronic System*, 2007, vol. 43, no. 1, p. 330–343. DOI: 10.1109/TAES.2007.357137

[6] CHEN, Y. F., NIJSURE, Y., YUEN, C., CHEW, Y. H., DING, Z. G. Adaptive distributed MIMO radar waveform optimization based on mutual information. *IEEE Transactions on Aerospace and Electronic System*, 2013, vol. 49, no. 2, p. 1374–1385. DOI: 10.1109/TAES.2013.6494422

[7] SONG, X. F., WILLETT, P., ZHOU, S. L. Optimal power allocation for MIMO radars with heterogeneous propagation losses. In *IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP 2012.* Kyoto (Japan), 2012, p. 2465–2468. DOI: 10.1109/ICASSP.2012.6288415

[8] SHI, C. G., ZHOU, J. J., WANG, F. Low probability of intercept optimization for radar network based on mutual information. In *2014 2nd IEEE China Summit & International Conference on Signal and Information Processing (ChinaSIP)*. Xi'an (China), 2014, p. 683–687. DOI: 10.1109/ChinaSIP.2014.6889331

[9] SHI, C. G., WANG, F., SELLATHURAI, M., ZHOU, J. J. LPI optimization framework for target tracking in radar network architectures using information-theoretic criteria. *International Journal of Antennas and Propagation*, 2014, 10 p. DOI: 10.1155/2014/654561

[10] WYNER, A. X. The wiretap channel. *The Bell System Technical Journal*, 1975, vol. 54, no. 8, p. 1355–1387. DOI: 10.1002/j.1538-7305.1975.tb02040.x

[11] SWINDLEHURST, A. L. Fixed SINR solutions for the MIMO wiretap channel. In *IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP 2009.* Taipei, 2009, p. 2437–2440. DOI: 10.1109/ICASSP.2009.4960114

[12] ZHOU, X. Y., MCKAY, M. R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. *IEEE Transactions on Vehicular Technology*, 2010, vol. 59, no. 8, p. 3831–3842. DOI: 10.1109/TVT.2010.2059057

[13] ROMERO-ZURITA, N., MCLERNON, D., GHOGHO, M., SWAMI, A. PHY layer security based on protected zone and artificial noise. *IEEE Signal Processing Letters*, 2013, vol. 20, no. 5, p. 487–490. DOI: 10.1109/LSP.2013.2252898

[14] MUKHERJEE, A., SWINDLEHURST, A. L. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Transactions on Signal Processing*, 2013, vol. 61, no. 1, p. 82–91. DOI: 10.1109/TSP.2012.2222386

[15] ZOU, Y. L., WANG, X. B., SHEN, W. M. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications*, 2013, vol. 61, no. 12, p. 5103 to 5113.

[16] WANG, F., SELLATHURAI, M., LIU, W. G., ZHOU, J. J. Security information factor based airborne radar RF stealth. *Journal of Systems Engineering and Electronics*, 2014. (Unpublished)

[17] SHI, C. G., ZHOU, J. J., WANG, F., CHEN, J. Optimal power allocation for low probability of identification in radar network based on security information with cooperative jamming. *ICIC Express Letters*, 2014, vol. 8, no. 12, p. 3401–3406.

[18] SHI, C. G., ZHOU, J. J., WANG, F., CHEN, J. LPID optimization with security information in radar network. *Industrial Electronics and Engineering*, 2014, vol. 93, p. 255–263. DOI: 10.2495/ICIEE140291

[19] ZADEH, L. A. Fuzzy sets. *Information and Control*, 1965, vol. 8, no. 3, p. 338–353. DOI: 10.1016/S0019-9958(65)90241-X

[20] LIU, B. D., LIU, Y. K. Expected value of fuzzy variable and fuzzy expected value models. *IEEE Transactions on Fuzzy Systems*, 2002, vol. 10, no. 4, p. 445–450. DOI: 10.1109/TFUZZ.2002.800692

[21] LIU, B. D. *Uncertainty Theory: An Introduction to Its Axiomatic Foundations*. Berlin: Springer-Verlag, 2004, p. 109–128.

[22] PAGNONCELLI, B. K., AHMED, S., SHAPIRO, A. Sample average approximation method for chance constrained programming: theory and application. *Journal of Optimization Theory and Application*, 2009, vol. 142, no. 2, p. 399–416. DOI: 10.1007/s10957-009-9523-6

[23] LIU, B. D., ZHAO, R. Q., WANG, G. *Uncertainty programming with Application.* Beijing: Tsinghua University Press, 2003, p. 138-187. (In Chinese)

[24] LIU, B. D. *Theory and Practice of Uncertainty Programming.* Heidelberg: Physical-Verlag, 2002, p. 53–74.

About the Authors ...

Chenguang SHI was born in 1989. He received B.S. from Nanjing University of Aeronautics and Astronautics (NUAA) in 2012, and he is currently working toward his Ph.D. degree in NUAA. His main research interest is aircraft radio frequency stealth, radar target tracking.

Jianjiang ZHOU (corresponding author) was born in 1962. He received M.S. and Ph.D. from Nanjing University of Aeronautics and Astronautics (NUAA) in 1988 and 2001 respectively, and then became a professor there. His main research interest is aircraft radio frequency stealth, radar signal processing.