ICIC Express Letters
Volume **11**, Number **7**, July **2017**

 ISSN 1881-803X
pp. 1185–1190

INSECURE ZONE BASED LOW PROBABILITY OF IDENTIFICATION IMPROVEMENT IN RADAR NETWORK ARCHITECTURES

Guangquan Kang*, Hanchu Xia and Lu Bian

School of Electronic Information Engineering
Sanjiang University
No. 10, Longxi Road, Yuhua District, Nanjing 210012, P. R. China
*Corresponding author: guangquankang_sju@163.com

Received January 2017; accepted April 2017

Abstract. *In this paper, a novel approach for ensuring low probability of identification (LPID) performance in radar network architectures is proposed and analyzed from a geometrical perspective. We first utilize the concept of insecure zone to characterize the LPID performance when no information about the hostile passive intercept receiver's location is available. The insecure zone is defined as the zone where the intercept receiver may intercept and identify the radar modulating signal. With the aim of minimizing the insecure zone, an optimal power allocation strategy between the radar modulating signal and the cooperative jamming (CJ) signal is presented for a specified threshold of achievable mutual information (MI) in radar network. Numerical results demonstrate that the proposed method can effectively achieve the optimal solution and bring a significantly enhanced LPID performance in practical scenarios.*
Keywords: Insecure zone, Security information, Low probability of identification (LPID), Power allocation, Radar network

1. **Introduction.** Radar network architecture, which often refers to distributed multiple-input multiple-output (MIMO) radar [1-3], is widely deployed in modern battlefield owing to its advantage of signal and spatial diversities. The research on radar network architecture has received increasing impetus in recent years, which has been extensively studied from various perspectives [1-6]. Song et al. in [5] investigate the optimal power allocation in distributed MIMO radar configuration. The authors in [6] study multi-static radar code design methods using information-theoretic criteria in the presence of clutter.

Currently, inspired by the fact that physical-layer (PHY) security is to keep passive eavesdropper ignorant of legitimate transmitter, the authors in [7] have presented security information originating from secrecy capacity to describe the LPID performance for radar network systems. However, the concise geometrical model was not given. When no information about the hostile passive intercept receiver's location is available, it is impossible to calculate the security information. In [8], the concept of protected zone is proposed from a geometrical perspective. The use of insecure zone for LPID performance in radar network systems has not been investigated previously, which motivates us to consider this problem for the first time.

This paper will investigate the insecure zone based LPID optimization strategy in radar network architectures. The main contributions of this paper are summarized as follows. Firstly, we define the concept of insecure zone to characterize the LPID performance when no information about the hostile passive interceptor's location is available, and an analytical closed-form expression of insecure zone is derived. Secondly, different from existing approaches, an optimal power allocation strategy between the radar modulating signal and the cooperative jamming (CJ) signal is presented, which aims to minimize the insecure zone for a given threshold of MI in radar network. The analytical closed-form expression for the optimal solution is derived. Finally, numerical simulations are

provided to demonstrate that our proposed algorithm can significantly improve the LPID performance of radar network to defend against passive intercept receivers. To the best of our knowledge, no literature discussing this issue was conducted prior to this work.

Regarding the paper structure, Section 2 describes the system model. In Section 3, with the proposed definition of insecure zone, a novel LPID improvement strategy is formulated, and the optimal solutions are derived by analytical closed-form expressions. The numerical simulations are presented in Section 4. Finally, conclusion remarks are drawn in Section 5.

2. **Radar Network Signal Model.** In this paper, we consider a fully coherent radar network, which means that the radars comprising the whole network have a common and highly precise knowledge of time and space. It is also assumed that the whole network is perfectly synchronized and works cooperatively such that each receiver is capable of receiving echoes of the signals from any of the transmitters in the network.

Let K denote the discrete time index, and we can express the radar network signal model as [5,7]:

$$\mathbf{Y}_r = \mathbf{X}\mathbf{H}_r + \mathbf{W}_r \tag{1}$$

where $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{N_t}]$ is the transmit sequence, $\mathbf{H}_r = [\mathbf{h}_{r,1}, \mathbf{h}_{r,2}, \ldots, \mathbf{h}_{r,N_t}]$ refers to the path gain matrix, $\mathbf{W}_r = [\mathbf{w}_{r,1}, \mathbf{w}_{r,2}, \ldots, \mathbf{w}_{r,N_r}]$ represents the system noise, and the received signal matrix is $\mathbf{Y}_r = [\mathbf{y}_{r,1}, \mathbf{y}_{r,2}, \ldots, \mathbf{y}_{r,N_t}]$. For convenience, we assume that the noise matrix $\mathbf{W}_r$ does not depend on the transmit sequence $\mathbf{X}$, and $\mathbf{H}_r$ and $\mathbf{W}_r$ are mutually independent.

With the discussions in [5,7], the path gain $\mathbf{h}_{rn}$ contains the target reflection coefficient g_{mn} and the propagation loss factor p_{mn}. Based on the central limit theorem, $g_{mn} \sim CN\left(0, \sigma_g^2\right)$, where g_{mn} denotes the target reflection gain between the transmitter m and receiver n, the propagation loss factor can be expressed as $p_{mn} = \frac{\sqrt{G_{t,m}G_{r,n}}}{R_{t,m}R_{r,n}}$.

Hence, the radar network signal model (1) can be rewritten as:

$$\mathbf{Y}_r = \mathbf{X}\left(\mathbf{G} \odot \mathbf{P}\right) + \mathbf{W}_r \tag{2}$$

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

3. **Problem Formulation.** The MI between the transmitted signal $\mathbf{X}$ and the backscattered signal $\mathbf{Y}_r$ is expressed as:

$$I\left(\mathbf{X}, \mathbf{Y}_r\right) = H\left(\mathbf{Y}_r\right) - H\left(\mathbf{W}_r\right) = \sum_{m=1}^{N_t}\sum_{n=1}^{N_r} \ln\left(1 + \frac{P_{t,m} \cdot \sigma_g^2 \cdot G_{t,m} \cdot G_{r,n}}{\sigma_{w_r}^2 \cdot R_{t,m}^2 \cdot R_{r,n}^2}\right) \triangleq I_{\text{net}} \tag{3}$$

where $I\left(\mathbf{X}, \mathbf{Y}_r\right)$ is the MI between $\mathbf{Y}_r$ and $\mathbf{X}$, $H\left(\mathbf{Y}_r\right)$ is the entropy of backscattered signal, $H\left(\mathbf{W}_r\right)$ is the entropy of noise, $P_{t,m}$ is the mth transmitter power, $G_{t,m}$ is the mth transmitting antenna gain, $G_{r,n}$ is the nth receiving antenna gain, $R_{t,m}$ is the distance from the mth transmitter to the target, and $R_{r,n}$ is the distance from the target to the nth receiver.

Similarly, the MI between the transmit signal of radar network $\mathbf{X}$ and the received signal of intercept receiver $\mathbf{Y}_i$ is:

$$I\left(\mathbf{X}, \mathbf{Y}_i\right) = H\left(\mathbf{Y}_i\right) - H\left(\mathbf{Y}_i|\mathbf{X}\right) = \sum_{m=1}^{N_t} \ln\left(1 + \frac{P_{t,m} \cdot G'_{t,m} \cdot G_{\text{int}}}{\sigma_{w_i}^2 \cdot R_{t,m}^2}\right) \tag{4}$$

where G_{int} is the antenna gain of interceptor, $G'_{t,m}$ is the gain of the mth radar's transmitting antenna in the direction of the interceptor, $\sigma_{w_i}^2$ is the noise covariance of interceptor. In modern electronic warfare, CJ is indispensable to keep radar network in LPID state [7], which means that CJ is to jam the hostile intercept receiver so that the achievable

MI at interceptor can be degraded by the CJ signal while the radar network system is unaffected. With the consideration of CJ, (4) can be modified as follows:

$$I\left(\mathbf{X},\mathbf{Y}_i\right)=\sum_{m=1}^{N_t}\ln\left[1+\frac{P_{t,m}\cdot G_{t,m}\cdot G_{\text{int}}}{\left(\sigma_{w_i}^2+\frac{P_j\cdot G_j\cdot G_{\text{int}}}{R_j^2}\right)\cdot R_{t,m}^2}\right]\triangleq I_{\text{int}} \tag{5}$$

where P_j is the total transmit 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 simplicity, we assume that the radar network can simultaneously transmit radar modulating signal to track target and CJ signal to interfere 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 interceptor without affecting the radar network.

Using the results of [7], the security information of radar network is defined as:

$$I_{\text{sec}}\left(P_r,P_j\right)\triangleq\left[I_{\text{net}}-I_{\text{int}}\right]^+=\left[\sum_{m=1}^{N_t}\sum_{n=1}^{N_r}\ln\left(1+\gamma_{\text{net}}^{mn}\right)-\sum_{m=1}^{N_t}\ln\left(1+\gamma_{\text{int}}^{m}\right)\right]^+ \tag{6}$$

where $\gamma_{\text{net}}^{mn}=\frac{P_{t,m}\cdot\sigma_g^2\cdot G_{t,m}\cdot G_{r,n}}{\sigma_{w_r}^2\cdot R_{t,m}^2\cdot R_{r,n}^2}$, $\gamma_{\text{int}}^{m}=\frac{P_{t,m}\cdot G_{t,m}\cdot G_{\text{int}}}{\left(\sigma_{w_i}^2+\frac{P_j\cdot G_j\cdot G_{\text{int}}}{R_j^2}\right)\cdot R_{t,m}^2}$, and $[x]^+=\max(0,x)$.

The notional sketch of our proposed perfectly secure radar network system is illustrated in Figure 1. It has been pointed out in [7] 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 [9].

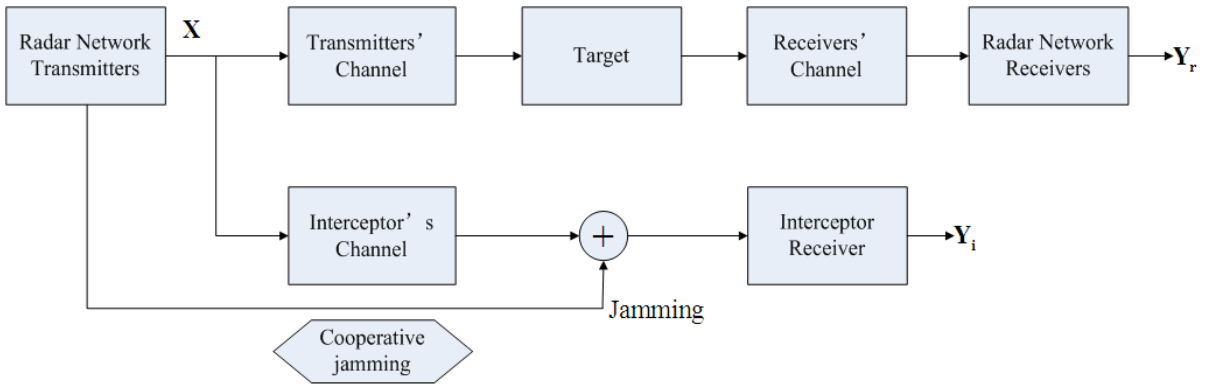

FIGURE 1. The notional sketch of our proposed perfectly secure radar network architecture

However, in practical applications, no information about the hostile passive intercept receiver's location is available; thus, we cannot calculate the security information. We define the insecure zone as follows.

Definition 3.1. (Insecure zone): *For a specified MI at intercept receiver C_{int}, transmit power and CJ power, the insecure zone is defined as the area where the passive interceptor may intercept and identify the radar network's modulating signal, and is formulated as:*

$$\left\{\xi_E\middle|\, I_{\text{int}}\geq C_{int}\right\} \tag{7}$$

where ξ_E is the geometrical coordinate vector for intercept receiver.

The motivation for deploying an insecure zone U is twofold. First, it contributes to LPID performance by defending against passive interceptor attacks at close quarters, and second, it allows us to make efficient use of the available power. In this paper, we aim

to minimize the insecure zone subject to constraints on power at a given MI in radar network. The design formulation can now be written as:

$$\left.\begin{array}{l}\min\limits_{P_{tm}(\forall m),P_j} U \\ \text{s.t.}: I_{\text{net}} \geq C_{\text{net}} \\ \quad \sum\limits_{m=1}^{N_t} P_{t,m} + P_j \leq P_{tot}^{\max} \\ \quad 0 < \sum\limits_{m=1}^{N_t} P_{t,m} \leq P_r^{\max}, \quad P_j \geq 0 \end{array}\right\} \tag{8}$$

Definition 3.2. (Insecure radius): *The insecure radius r_E is defined as the largest distance from radar network configuration where an passive intercept receiver can successfully intercept and identify the modulating signal.*

From the above discussions, it is obvious that the insecure zone U is an increasing function of the insecure radius r_E. Hence, problem (8) can be turned to:

$$\left.\begin{array}{l}\min\limits_{P_{tm}(\forall m),P_j} r_E \\ \text{s.t.}: I_{\text{net}} \geq C_{\text{net}} \\ \quad \sum\limits_{m=1}^{N_t} P_{t,m} + P_j \leq P_{tot}^{\max} \\ \quad 0 < \sum\limits_{m=1}^{N_t} P_{t,m} \leq P_r^{\max}, \quad P_j \geq 0 \end{array}\right\} \tag{9}$$

To make the problem have a feasible solution, some simplicity will be utilized to the formula of security information (6). Herein, it is supposed that $R_{\text{net}}^2 \approx R_{t,m} \cdot R_{r,n}\,(\forall m, n)$, $P_{t,m} = \frac{P_r}{N_t}\,(\forall m)$, where R_{net} is approximately the distance from target to radar network system, P_r is the total transmit power for radar modulating signal. We also assume that each radar in the network is the same. Thus, (6) can be rewritten as:

$$\begin{aligned} I_{\text{sec}}(P_r, P_j) = \Bigg\{ & N_t \cdot N_r \cdot \ln\left(1 + \frac{P_r \cdot \sigma_g^2 \cdot G_t \cdot G_r}{N_t \cdot \sigma_{w_r}^2 \cdot R_{\text{net}}^4}\right) \\ & - N_t \cdot \ln\left[1 + \frac{P_r \cdot G_t' \cdot G_{\text{int}}}{N_t \cdot \left(\sigma_{w_i}^2 + \frac{P_j \cdot G_j \cdot G_{\text{int}}}{r_E^2}\right) \cdot r_E^2}\right] \Bigg\}^+ \end{aligned} \tag{10}$$

Now, substituting (10) into the optimization problem (9) yields:

$$\begin{cases} P_r \geq \min\left\{P_r^{\max}, \frac{N_t \cdot \sigma_{w_r}^2 \cdot R_{\text{net}}^4}{\sigma_g^2 \cdot G_t \cdot G_r}\left[\exp\left(C_{\text{net}}/N_t N_r\right) - 1\right]\right\} \\ r_E \leq \sqrt{\frac{P_r \cdot G_t' \cdot G_{\text{int}}}{N_t \sigma_{w_i}^2 [\exp(C_{\text{int}}/N_t) - 1]} - \frac{P_j \cdot G_j \cdot G_{\text{int}}}{\sigma_{w_i}^2}} \end{cases} \tag{11}$$

We can see that to achieve the best performance for intercepting and identifying at a given distance from radar network, the intercept receiver should be located in the line from radar network system to target. This formulation is meaningful and gives us insights about the impact of the intercept receiver's location on LPID performance in radar network.

4. **Numerical Simulations.** In this section, we will present numerical simulations to verify our proposed scheme. We set $P_{tot} = P_r + P_j = 25$ KW, $G_t = G_r = G_j = 30$ dB, $G_t' = 10$ dB, $G_i = 0$ dB, $\sigma_{w_r}^2 = 4.57 \times 10^{-12}$ W, $\sigma_{w_i}^2 = 8.77 \times 10^{-8}$ W and $\sigma_g^2 = 1$. For convenience, we consider a 4×4 radar network architecture ($N_t = N_r = 4$), which 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 is set to be -80 dBmW.

Figure 2 illustrates the insecure zone and achievable MI at hostile intercept receiver, when the radar network is located at $(0, 0)$ km and the target is located at $(150, 0)$ km.

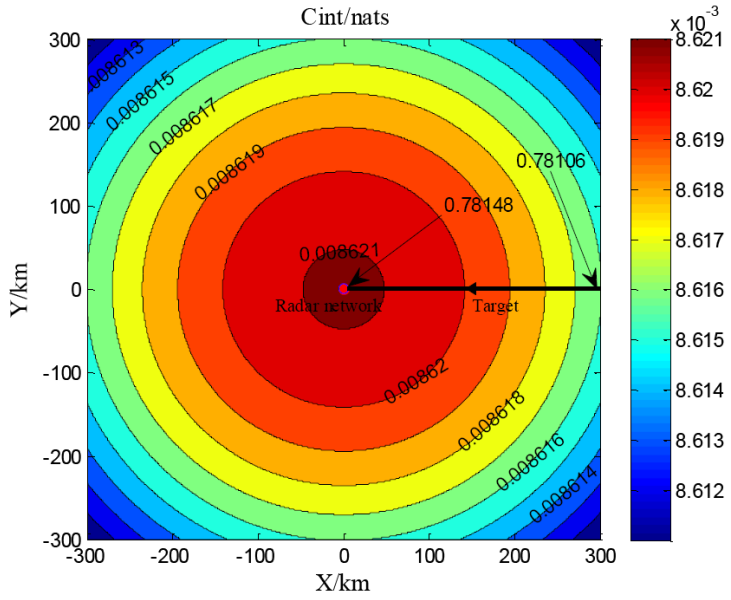

FIGURE 2. Insecure zone and achievable MI at intercept receiver

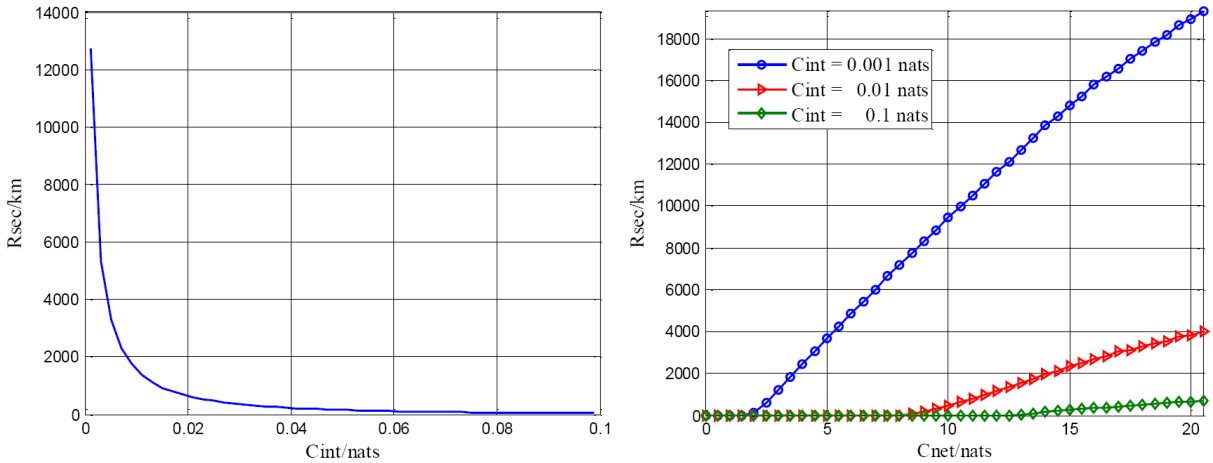

FIGURE 3. (a) The insecure radius versus C_{int}; (b) the insecure radius versus C_{net} for different C_{int}

The threshold of achievable MI in radar network C_{net} is 12.98 nats, which is minimum value of the basic performance requirement for target information extraction and can be calculated in the condition that the transmitting power of each radar node is 6 KW in the distance 180 km between the radar network and the target. We can see that for different values of C_{int}, the insecure zones are circles around radar network. When C_{int} is above 0.008621 nats, the insecure zone is zero, which means that wherever the hostile interceptor locates, it cannot intercept and identify the radar modulating signal, showing the advantage of exploiting CJ to defend against intercept receiver attacks [7,9].

To understand the LPID performance improvement of our proposed strategy, Figure 3(a) shows the insecure radius versus C_{int}, from which it is shown that the insecure zone can be reduced to a small area around radar network as C_{int} increases. In Figure 3(b), we depict the insecure radius versus the threshold of achievable MI in radar network for different C_{net}. As expected, the insecure zone is decreased to a small area around radar network system as C_{net} reduces. In Figure 3(b), it can be seen that the insecure radius is zero when C_{net} is low, and increases significantly when C_{net} is larger than a specific value

(i.e., the "=" in (11) is satisfied). It should be noted that when C_{net} is large we must keep the passive intercept receiver away from radar network to ensure LPID performance in the presence of a power constraint, highlighting that close intercept receivers represent the biggest threat to LPID performance in radar network.

5. **Conclusions.** In this paper, the problem of LPID improvement based on insecure zone in radar network systems is investigated, which minimizes the insecure zone by optimizing the power allocation between the radar modulating signal and CJ signal for a predefined threshold of MI in radar network. It should be noted that the optimal solution can be achieved by explicit closed-form expressions. Numerical simulations demonstrate that the presented strategy can improve the LPID performance for radar network remarkably to prevent hostile interceptor attacks. Future work will concentrate on other optimization criteria to improve LPID performance for radar network architectures.

Acknowledgment. The support provided by Top-notch Academic Programs Project of Jiangsu Higher Education Institutions is gratefully acknowledged.

REFERENCES

[1] A. M. Haimovich, R. S. Blum and L. J. Jr. Cimini, MIMO radar with widely separated antennas, *IEEE Signal Processing Magazine*, vol.25, no.1, pp.116-129, 2008.

[2] C. G. Shi, F. Wang, M. Sellathurai and J. J. Zhou, Transmitter subset selection in FM-based passive radar networks for joint target parameter estimation, *IEEE Sensors Journal*, vol.16, no.15, pp.6043-6052, 2016.

[3] C. G. Shi, F. Wang, M. Sellathurai, J. J. Zhou and H. Zhang, Robust transmission waveform design for distributed multiple-radar systems based on low probability of intercept, *ETRI Journal*, vol.38, no.1, pp.70-80, 2016.

[4] P. Chavali and A. Nehorai, Scheduling and power allocation in a cognitive radar network for multiple-target tracking, *IEEE Trans. Signal Processing*, vol.60, no.2, pp.715-728, 2012.

[5] X. F. Song, P. Willett and S. L. Zhou, Optimal power allocation for MIMO radars with heterogeneous propagation losses, *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp.2465-2468, 2012.

[6] 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. Signal Processing*, vol.61, no.21, pp.5401-5416, 2013.

[7] C. Shi, J. Zhou, F. Wang and J. Chen, Optimal power allocation for low probability of identification in radar network based on security information with cooperative jamming, *ICIC Express Letters*, vol.8, no.12, pp.3401-3406, 2014.

[8] 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.

[9] C. G. Shi, F. Wang, J. J. Zhou and J. Chen, Fuzzy chance-constrained programming based security information optimization for low probability of identification enhancement in radar network systems, *Radio Engineering*, vol.24, no.1, pp.199-207, 2015.