AUT Journal of Electrical Engineering

AUT J. Elec. Eng., 52(1) (2020) 97-106
DOI: 10.22060/eej.2019.15573.5263

Distance-Aware Beamforming for Multiuser Secure Communication Systems

Nasrin Ravansalar, Vahid Pourahmadi*

Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran

ABSTRACT: Typical cryptography schemes are not well suited for low complexity types of equipment, e.g. Internet of things (IoT) devices, as they may need high power or impose high computational complexity. Physical (PHY) layer security techniques such as beamforming (in multiple antennas systems) are possible alternatives to provide security for such applications. In this paper, we consider a network with multiple groups of users as receivers and a transmitter that intends to send different messages to each group. There are also some eavesdroppers (Eavs) at known locations of the environment. The goal of this paper is to find the beamforming vectors that minimize the total transmitting power while keeping the signal level above a threshold at the exact locations of the legitimate receivers (both angle and range) and keeping it less than another threshold at eavesdropping points. We use frequency diverse arrays (FDA) at the transmitter; thus, the transmitter also needs to determine the frequency that each antenna element must use for data transmission. This condition makes the problem non-convex and so we propose an approximate solution for solving this optimization problem. Simulation results show the performance of the scheme in a particular network setting.

Review History:
Received: 2019-01-06
Revised: 2019-11-04
Accepted: 2019-11-04
Available Online: 2020-06-01

Keywords:
Secure Communication
Beamforming
Optimization
Frequency Diverse Multi-antenna Array
CVX

1. INTRODUCTION

Security plays an important role in wireless communications due to the nature of the wireless medium. One approach to meet the security problems is the conventional use of encryption employed in the application layer. This approach needs a secret key agreement which itself is not possible always because the number of secret keys is limited and transceivers need a secure channel to exchange those keys which are not always accessible. Hence, recently physical (PHY) layer security has attracted a wide range of studies [1, 2]. Despite the cryptographic approaches which are based on secret key exchanges, the principle concept behind the PHY layer security is the use of channels' physical characteristics for secure transmission. In [3], Wyner showed that perfect secrecy between a transmitter and a legitimate receiver at a strictly positive data rate is possible only if the source-destination channel has better conditions than the source-eavesdropper one.

One way to improve the channels' conditions of the legitimate receivers is to deploy multiple antennas at the transmitter and benefit from the spatial multiplexing gain. Multiple antennas at the transmitter can concentrate the secret signal to the predefined legitimate directions by *directional modulation* (DM) [4] or *transmit beamforming* [5]. By applying phase shifts on each antenna element, directional modulation can commix the constellation of the modulated signal at undesired points in order to confuse eavesdroppers [6, 7]. On the other hand, transmit beamforming can strengthen the signal power at desired points while weaken it at illegal ones by solving an optimization problem [8, 9].

Another way to ensure security is to inject *artificial noise* to the communication channels such that it degrades the received signal to noise and interference ratio (SINR) at the eavesdropping points [10-12]. Also, some authors, like in [13-15] used both beamforming and artificial noise techniques and optimized the joint problem. The drawback of such studies is that under far-field conditions their beamformers only depend on the direction angle and do not consider the distance from the transmitter. It is important especially for security purposes when an eavesdropper locates along the same direction as the legitimate user but in the different distance from the transmitter. In such cases, we assume that the eavesdropper receives path loss is almost similar to the legitimate user. This is because on the far-field conditions, the relative distance between two receivers is much smaller than their distances to the transmitter, so the path loss effect on the power amplitude is almost identical for both of them.

To have a method considering both range and angle, frequency diverse array antenna (FDA) was introduced which applies a frequency shift on each antenna element. Primary studies on FDA have applied linear shifts to the elements

*Corresponding author's email: v.pourahmadi@aut.ac.ir

called linear frequency diverse array (LFDA) [16-18] using which the received signal strength are maximized on range-angle pairs which are linearly coupled. Randomly assigning frequency shifts to antenna elements decouples range-angle pairs so the transmitted signal only reaches to the exact desired location in the area. Random frequency diverse array (RFDA) has been introduced in the context of Radar as they need to locate the exact location of the object [19, 20]. Reference [21] uses RFDA-based scheme directional modulation with the aid of artificial noise to enhance physical layer security of wireless communications.

RFDA-related studies, such as the work in [21], use random frequency assignment, and they do not explore if the random frequency assignment is the best strategy or not. In [22, 23], authors have tried to look into this problem but they only consider scenarios when there is only one legitimate receiver. In the case of more than one user or more than one group of users, the problem changes to a multicasting problem which is discussed in [24] in the near-field conditions where path loss is an important factor. To the best of our knowledge, the problem of multicast transmission to exact user locations under far-field conditions knowing eavesdropping locations without the aid of artificial noise has not been investigated in literature.

In this work, we assume that there are multiple groups of users in the network, and there could be multiple users in each group. The transmitter needs to transmit different messages to different groups, while aiming to perform beamforming considering the exact users' locations including the ranges and angles of the receivers. We use the concept of FDA to optimize the transmit beamforming on the desired angle-range couples, i.e.; we jointly optimize the transmit beamforming and the frequency assignment to the transmit antenna elements. As the resulted optimization problem is non-convex, we approximate it and propose a two-step optimization problem to find the solution. At the first step, we solve a convex problem minimizing the total transmitting power under SINR limitations in different points to find the best beamformers, and at the second step, we find an acceptable suboptimal frequency assignment during a non-convex optimization searching algorithm also minimizing the total transmitting power.

The rest of this paper is organized as follows. In section 2, we detail our system model and derive the optimization problem. Section 3 presents our approximation scheme. In section 4 numerical results and performance evaluations are illustrated. Finally, section 5 concludes the paper.

2. SYSTEM MODEL AND PROBLEM FORMULATION

Consider a wireless system composed of a single transmitter with a uniform linear array (ULA) of N antennas and M single antenna receivers in G groups, $\{g_k\}_{k=1}^{G}$. In fact g_k consists of indices of users locating in the k^{th} group. The number of users in different groups can be different, and users of the same group can be located at different range-angle pairs. The goal is to send G independent messages $\{x_k\}_{k=1}^{G}$ simultaneously to the G groups with no leakage to the undesired receivers and no interference with each other. Also, there are J eavesdroppers located at known locations. We note that there is no limitation on the number of eavesdroppers that exist in the system, i.e., we can solve the problem with many EAVs. This property may help to use this method for real scenarios that we do not know the exact location of actual EAVs, but we can assume that we can identify some locations in our area that potentially an EAV can be located there. Then, to protect our data, we add an EAV to our model for each of these potential locations and design the network such that low power gets to them.

Let $\{\mathbf{w}_k\}_{k=1}^{G}$ be $N\times 1$ complex beamforming vectors of groups $\{g_k\}_{k=1}^{G}$ which shape the signal intended for each group, $\{x_k\}_{k=1}^{G}$. So, the transmitted signal from the base station (BS) is $\mathbf{s}=\sum_{k=1}^{G}\mathbf{w}_k x_k$, and the received signal at the i^{th} receiver is:

$$\mathbf{y}_i=\mathbf{h}_i^H\mathbf{s}+n_i=\sum_{k=1}^{G}\mathbf{h}_i^H\mathbf{w}_k x_k+n_i,\quad 1\le i\le M, \tag{1}$$

where $n_i\sim\mathcal{CN}(0,\sigma_i^2)$ is the additive white Gaussian noise at i^{th} receiver. In (1), $\mathbf{h}_i$ denotes the $N\times 1$ complex vector modeling the channel from transmitter to the i^{th} receiver located at range-angle pair (R_i,θ_i) from the reference antenna element.

Under free space and far-field conditions, the only factor determining the channel vectors is the delay of the received signals that causes phase shifts on the received signals of each antenna element relative to the reference element. So the channel vector of the i^{th} receiver is [21]:

$$\mathbf{h}_i(R_i,\theta_i)=\frac{1}{\sqrt{N}}[e^{j\Psi_{0,i}(R_i,\theta_i)},e^{j\Psi_{1,i}(R_i,\theta_i)},\ldots,e^{j\Psi_{N-1,i}(R_i,\theta_i)}]^T,\quad i=1,\ldots,M. \tag{2}$$

$\{\Psi_{n,i}(R_i,\theta_i)\}_{n=0}^{N-1}$ are the phase shifts from the reference antenna element (element of number zero), i.e., [21]:

$$\Psi_{n,i}(R_i,\theta_i)=\phi_{n,i}(R_i,\theta_i)-\phi_{0,i}(R_i,\theta_i)=-2\pi f_n\frac{R_{n,i}}{c}+2\pi f_c\frac{R_i}{c}, \tag{3}$$

where $\phi_{0,i}(R_i,\theta_i)$ and $\phi_{n,i}(R_i,\theta_i)$ are the phases received at the i^{th} receiver from the reference and the n^{th} antenna elements, respectively. R_i and $R_{n,i}$ are the ranges of the i^{th} receiver from the reference and n^{th} element of the antenna array respectively, as shown in Fig. 1. Assuming $d=\lambda/2$, i.e., half of the wavelength, as the spacing between the antenna elements. Such spacing between antenna elements makes the received signals from antenna array independent of each other so causes spatial diversity. Furthermore, $b_n=n-\frac{N-1}{2}$, under far-field conditions $R_{n,i}$ can be approximated as [21]:

$$R_{n,i}\approx R_i-b_n d\cos\theta_i,\quad n=0,1,\ldots,N-1. \tag{4}$$

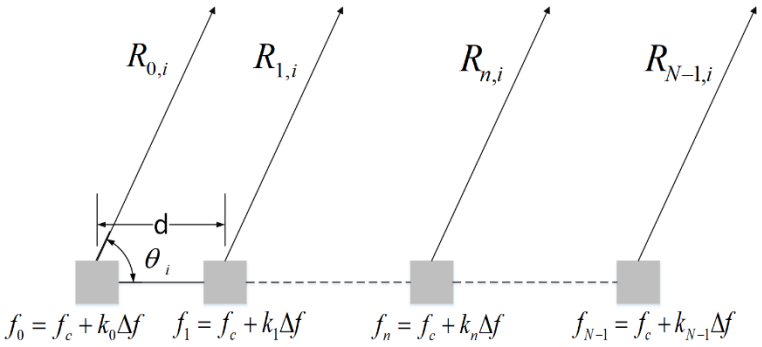


Fig. 1. Uniform antenna array (ULA)

This is because under far-field conditions $\theta_{n,i} \approx \theta_i$ and the arc subtended between reference element, i^{th} receiver and n^{th} element, centered at i^{th} receiver with the radius of R_i is approximately linear, so the second term of (4) is the length of other perpendicular edge of the orthogonal triangle it makes since its hypotenuse length is $b_n d$. Adding this term, considering the sign of b_n, to the radius of the arc makes $R_{n,i}$.

In (3), f_n denotes the carrier frequency assigned to the n^{th} antenna element and f_c is the central frequency. Assuming Δf as the frequency increment such that $N\Delta f \ll f_c$ we have [21]:

$$f_n = f_c + k_n \Delta f\ , \quad n = 0,1,\ldots,N-1. \tag{5}$$

In equation (5), $\{k_n\}_{n=0}^{N-1}$ are the frequency increment coefficients for transmit antenna elements.

In the previous studies where the direction of transmission is the only concern [5, 8], $\{k_n\}_{n=0}^{N-1}$ are equal to zero, i.e. all antenna elements transmit over the same frequency. By applying randomly chosen $\{k_n\}_{n=0}^{N-1}$, transmitted signal can be received only at some spots according to angles and ranges of the receivers [21].

Similar to [21], in this study, $\{k_n\}_{n=0}^{N-1}$ are not zero, but they are not selected randomly as [21], instead we assume $\{k_n\}_{n=0}^{N-1}$ are chosen from a predefined set of discrete values during an optimization problem. Substituting (4) and (5) in (3) we have [21]:

$$\Psi_{n,i}(R_i,\theta_i) = -2\pi(-b_n \frac{f_c d\cos\theta_i}{c} + k_n \frac{\Delta f R_i}{c} - b_n k_n \frac{\Delta f d\cos\theta_i}{c}). \tag{6}$$

The third term in (6) is negligible (because of $\Delta f \ll f_c$ and $d\cos\theta_i \ll R_i$), so it can be approximated as [21]:

$$\Psi_{n,i}(R_i,\theta_i) \approx -\frac{2\pi}{c}(-b_n f_c d\cos\theta_i + k_n \Delta f R_i), \tag{7}$$

which is then replaced in (2).

Assuming x_k to be temporally white with zero mean and unit variance and $\{x_k\}_{k=1}^{G}$ to be mutually uncorrelated, then the total transmit power becomes $P_t = \sum_{k=1}^{G} \| \mathbf{w}_k \|_2^2$.

Mathematically representing the problem, we should jointly determine the best frequency increment coefficients $\{k_n\}_{n=0}^{N-1}$ and design the beamforming vectors $\{\mathbf{w}_k\}_{k=1}^{G}$, indirect functions of $\{k_n\}_{n=0}^{N-1}$, for all groups spending minimum possible total transmit power such that they guarantee a minimum SINR at all legitimate users of each group, $\{\gamma_k\}_{k=1}^{G}$, and keep each group message secret from the users of other groups and the eavesdroppers, i.e. SINRs received at all receivers not in group k must be lower than a threshold, $\{\gamma_{sec_k}\}_{k=1}^{G}$, in order not to be detectable. Considering the SINR of the signal of group k received at the i^{th} receiver as:

$$SINR_{i,k} = \frac{\left|\mathbf{h}_i^H \mathbf{w}_k\right|^2}{\sum_{l\neq k}\left|\mathbf{h}_i^H \mathbf{w}_l\right|^2 + \sigma_i^2}, \tag{8}$$

We can write this problem as:

$$\begin{aligned} \mathcal{Q}: & \min_{\substack{\{\mathbf{w}_k \in \mathbb{C}^N\}_{k=1}^{G}, \\ \{k_n \in S\}_{n=0}^{N-1}}} \sum_{k=1}^{G} \| \mathbf{w}_k \|_2^2 \\ s.t.: & \frac{\left|\mathbf{h}_i^H \mathbf{w}_k\right|^2}{\sum_{l\neq k}\left|\mathbf{h}_i^H \mathbf{w}_l\right|^2 + \sigma_i^2} \geq \gamma_k, \quad \forall i \in g_k, \quad \forall k \in \{1,\ldots,G\}, \\ & \frac{\left|\mathbf{h}_j^H \mathbf{w}_k\right|^2}{\sum_{l\neq k}\left|\mathbf{h}_j^H \mathbf{w}_l\right|^2 + \sigma_j^2} \leq \gamma_{sec_k}, \quad \forall j \notin g_k, \quad \forall k \in \{1,\ldots,G\}, \end{aligned} \tag{9}$$

where $S = [-L, -L+1, \ldots, L-1, L]$ and L is a positive integer value.

It should be noted that $\mathbf{h}_i$ is a function of $\{k_n\}_{n=0}^{N-1}$ and $\{\mathbf{w}_k\}_{k=1}^{G}$ depend on channels' conditions $\{\mathbf{h}_i\}_{i=1}^{M}$, so frequency increment coefficients also affect beamforming vectors.

The first condition in problem $\mathcal{Q}$ is for all legitimate receivers in the k^{th} group ensuring that SINR associated with the message intended for group k should be larger than γ_k for all users in that group. Additionally, the second condition is that the SINR corresponding to the message of the group k for all other legitimate users not in the k^{th} group and illegitimate receivers, i.e. Eavs, should be less than γ_{sec_k}.

It's worth mentioning that each receiver knows its channels' condition $\mathbf{h}_i$ and by multiplying it to the received signal, it can obtain a message which for legal receivers is their own secret message and for illegal ones is undetectable. SINR

is a measure of the quality of the message that receivers get.

According to [8], by defining $\{\mathbf{U}_k := \mathbf{w}_k \mathbf{w}_k^H\}_{k=1}^G$ and adding $rank(\mathbf{U}_k)=1$ constraint, problem in (9) can be equivalently written as:

$$
\begin{aligned}
&\mathcal{Q}: \min_{\substack{\{\mathbf{U}_k\in\mathbb{C}^{N\times N}\}_{k=1}^G,\{k_n\in S\}_{n=0}^{N-1},\\ \{s_i\in\mathbb{R}\}_{i=1}^M,\{s_j\in\mathbb{R}\}_{j=1}^{M(G-1)+J\times G}}} \sum_{k=1}^G tr(\mathbf{U}_k)\\
&s.t.: tr(\mathbf{Q}_i\mathbf{U}_k)-\gamma_k\sum_{l\neq k} tr(\mathbf{Q}_i\mathbf{U}_l)-s_i=\gamma_k\sigma_i^2,\\
&\forall i\in g_k,\quad \forall k,l\in\{1,\dots,G\},\\
&\quad tr(\mathbf{Q}_j\mathbf{U}_k)-\gamma_{sec_k}\sum_{l\neq k} tr(\mathbf{Q}_j\mathbf{U}_l)+s_j=\gamma_{sec_k}\sigma_j^2,\\
&\forall j\notin g_k,\quad \forall k,l\in\{1,\dots,G\},\\
&\quad \ddot{u}_i\geq 0,\quad \forall\in\{1,\dots,\quad\},\\
&\quad s_j\geq 0,\quad \forall j\in\{1,\dots,M(G-1)+J\times G\},\\
&\quad \mathbf{U}_k\succeq\mathbf{0},\quad \forall k\in\{1,\dots,G\},\\
&\quad rank(\mathbf{U}_k)=1,\quad \forall k\in\{1,\dots,G\},
\end{aligned}
\tag{10}
$$

where $\mathbf{Q}_i := \mathbf{h}_i\mathbf{h}_i^H$, $\{s_i\}_{i=1}^M$ are the real nonnegative slack variables related to the conditions of the legitimate users in each group and $\{s_j\}_{j=1}^{M(G-1)+J\times G}$ are real nonnegative slack variables related to the legitimate and illegal receivers, i.e. $M(G-1)$ conditions to ensure the message of one group is not detectable at legitimate users of other groups and $J\times G$ conditions to be sure of low SINRs of all messages at locations of J eavesdroppers.

3. APPROXIMATING THE OPTIMAL DESIGN

Optimization problem in (10) is non-convex for two reasons: a) $\{k_n\}_{n=0}^{N-1}$, which are appeared in a complex sinusoidal function $\mathbf{Q}_i$, take only discrete values so they make the problem non-convex, b) condition $rank(\mathbf{U}_k)=1$ is non-convex.

To find an approximate solution for (10), we rewrite $\mathcal{Q}$ as a two-step optimization problem. The inner problem, $\mathcal{Q}_{in}$, approximated as a semidefinite program (SDP) that is solvable by convex solvers like CVX, determines the best beamforming vectors, outer problem, $\mathcal{Q}_{out}$, tries to find the best frequency increment coefficients among all possible choices for $\{k_n\}_{n=0}^{N-1}$. Subsections 3-1 and 3-2 discuss these two problems respectively.

3-1- The Inner Problem

The goal of this problem is to find the beamforming vectors, $\{\mathbf{w}_k\}_{k=1}^G$, subject to guarantee minimum SINRs, $\{\gamma_k\}_{k=1}^G$, at each group and maximum secure SINRs, $\{\gamma_{sec_k}\}_{k=1}^G$, at receivers not in that group such that they consume minimum total transmit power. In this step, we assume $\{k_n\}_{n=0}^{N-1}$ are known and fixed (by the outer problem), and we find the best beamforming vectors according to them. Despite of excluding variables $\{k_n\}_{n=0}^{N-1}$ from the inner problem, it remains non-convex due to the last condition, $rank(\mathbf{U}_k)=1$. As suggested by [8], one way to try to solve this problem is to discard the last condition and solve the relaxed version of it. Then, use the solution of the relaxed problem to find the solution to the inner optimization problem. The relaxed inner optimization problem $\mathcal{Q}_{in}$ is:

$$
\begin{aligned}
&\mathcal{Q}_{in}: \min_{\substack{\{\mathbf{U}_k\in\mathbb{C}^{N\times N}\}_{k=1}^G,\{s_i\in\mathbb{R}\}_{i=1}^M,\\ \{s_j\in\mathbb{R}\}_{j=1}^{M(G-1)+J\times G}}} \sum_{k=1}^G tr(\mathbf{U}_k)\\
&s.t.: tr(\mathbf{Q}_i\mathbf{U}_k)-\gamma_k\sum_{l\neq k} tr(\mathbf{Q}_i\mathbf{U}_l)-s_i=\gamma_k\sigma_i^2\\
&\forall i\in g_k,\quad \forall k,l\in\{1,\dots,G\},\\
&\quad tr(\mathbf{Q}_j\mathbf{U}_k)-\gamma_{sec_k}\sum_{l\neq k} tr(\mathbf{Q}_j\mathbf{U}_l)+s_j=\gamma_{sec_k}\sigma_j^2,\\
&\forall j\in g_l,\quad \forall k,l\in\{1,\dots,G\},\\
&\quad s_i\geq 0,\quad \forall i\in\{1,\dots,M\},\\
&\quad s_j\geq 0,\quad \forall j\in\{1,\dots,M(G-1)+JG\},\\
&\quad \mathbf{U}_k\succeq\mathbf{0}\quad \forall k\in\{1,\dots,G\}.
\end{aligned}
\tag{11}
$$

Problem in (11) is a semidefinite program (SDP) and is solvable using SDP solvers like CVX, [25].

Because we have dropped the constraint $rank(\mathbf{U}_k)=1$, in general, the optimal solution of (11), $\{\mathbf{U}_k^{opt}\}_{k=1}^G$, might not be rank one. In such cases, *randomization* procedure can be applied on $\{\mathbf{U}_k^{opt}\}_{k=1}^G$ to obtain the best approximate solutions for (11) [5]. Reference [5] presented three methods of randomization in which it uses $\{\mathbf{U}_k^{opt}\}_{k=1}^G$ to generate a number of candidate beamforming vectors $\{\{\mathbf{w}_k^{cdt}\}_{cdt}\}_{k=1}^G$, and then among the candidate vectors chooses the one which consumes less transmit power, $\{\mathbf{w}_k^{opt}\}_{k=1}^G$.

3-2- The Outer Problem

In this step, we assume for any selection of $\{k_n\}_{n=0}^{N-1}$, $\{\mathbf{w}_k^{opt}\}_{k=1}^G$ can be obtained by $\mathcal{Q}_{in}$ and therefore using

(8) the effective SINRs can be calculated at any desirable points of the area. The outer optimization problem aims to find $\{k_n\}_{n=0}^{N-1}$ that best direct the signal power towards the desired locations and tries to make low SINRs at undesired points. In other words, it tries to satisfy all conditions of $\mathcal{Q}_{in}$ while consumes minimum total power.

So the outer optimization problem, $\mathcal{Q}_{out}$, can be defined as:

$$
\begin{aligned}
&\mathcal{Q}_{out}: \min_{\{k_n\}_{n=0}^{N-1}} \sum_{k=1}^G \| \mathbf{w}_k^{opt} \|_2^2\\
&s.t.: k_n\in S,\quad \forall n\in\{0,\dots,N-1\},
\end{aligned}
\tag{12}
$$

where, $S=[-L,-L+1,\dots,L-1,L]$ and, as discussed before, $\{\mathbf{w}_k^{opt}\}_{k=1}^G$ are indirect functions of $\{k_n\}_{n=0}^{N-1}$ i.e. the frequency increment coefficients. It is because $\{\mathbf{w}_k^{opt}\}_{k=1}^G$ are selected by the inner optimization problem such that it minimizes the total transmit power which depends on $\{\mathbf{h}_i\}_{i=}^M$, in (2). Dependency of $\{\mathbf{h}_i\}_{i=1}^M$ on $\{k_n\}_{n=0}^{N-1}$ is through $\Psi_{n,i}(R_i,\theta_i)$ in (3) which itself depends on the frequency assigned to each antenna in (5).

Problem $\mathcal{Q}_{out}$ is a discrete optimization problem, and its optimum result can be determined using discrete optimization techniques like *Branch and Bound* (BnB) which has high computational complexity. To clarify the computational cost of obtaining optimal solutions, consider an N-dimensional Boolean variable; It needs at most 2^N calculations to reach the optimum. In the outer problem, we have an array of antennas ($N\geq 10$) each have a choice of $2L+1\geq N$ frequencies which causes at most $(2L+1)^N$ calculations that are infeasible. To have a low

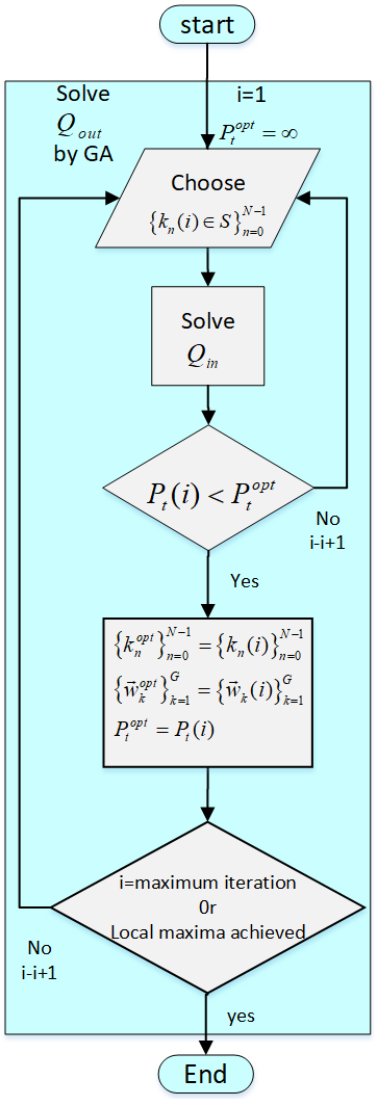


Fig. 2. Flowchart of the problem $\mathcal{Q}$ decomposition

complexity scheme, in this paper, we use *Genetic Algorithm* (GA) to determine the approximate solution of the above integer-valued nonlinear constrained optimization problem.

Here we have used the standard GA procedure, where $P_t=\sum_{k=1}^{G}\|\mathbf{w}_k^{opt}\|_2^2$, obtained from solving the inner problem, is used as the fitness function of GA, i.e., for all $\{k_n\}_{n=0}^{N-1}$ which are in the population set of the current GA generation, we find P_t and then choose the ones resulted in better power consumptions (mating pool). The members of the mating pool are then combined to make next set of $\{k_n\}_{n=0}^{N-1}$ candidates, i.e. next GA generation. This process is repeated several times and each time better coefficient sets are produced which make lower use of P_t. The GA algorithm is summarized in Alg. 1. We note that GA may get to the optimal point but the final result might be a suboptimal solution; so in general it is a suboptimal procedure but it has much lower computational loads than BnB. Such approximate GA-based results are more of interest when the number of antenna elements increases, and optimal methods become very complex. The flowchart of these two steps is shown in Fig. 2.

4. SIMULATION RESULTS

In this section, we provide simulation results on a hemispheric area with a radius of $r=30m$. There are one transmitter with $N=10$ antennas locating at the center of the hemisphere and J illegal receiver(s), Eav(s), locating at range-angle pairs $\{(R_j,\theta_j)\}_{j=1}^{J}$ in the supporting area. For clarification, we first study a single legitimate user network. Then, we present the results when there are more than one legitimate users.

In order to compare our proposed method against the others, we consider three schemes for the frequency increment coefficients, $\{k_n\}_{n=0}^{N-1}$, and beamforming vectors, $\{\mathbf{w}_k\}_{k=1}^{G}$:

I. Based on [8], all antenna elements use the same

Algorithm 1: Genetic Algorithm for solving $\mathcal{Q}_{out}$

Data: Number of Generations ($\mathcal{K}$), Population size of each Generation ($\mathcal{P}$)

Result: P_t^{opt} , $\{\mathbf{w}_k^{opt}\}_{k=1}^{G}$ and $\{k_n^{opt}\}_{n=0}^{N-1}$

Initialize: $i=1$, $\mathcal{G}_i=\left\{\{k_n\}_{n=0}^{N-1}\right\}_{\mathcal{P}}^{i}$

While $i \le \mathcal{K}$ **do**

Eval step: Solve $\mathcal{Q}_{in}$ for each member of $\mathcal{G}_i$

Mating pool generation: From $\mathcal{G}_i$, select $\{k_n\}_{n=0}^{N-1}$ which resulted to lower transmit powers (i.e., $\mathcal{Q}_{in}$)

Next GA Generation: Create the next GA generation by combining the members of the mating pool $\mathcal{G}_{i+1}=\left\{\{k_n\}_{n=0}^{N-1}\right\}_{\mathcal{P}^{i+1}}$

Iterate: $i=i+1$

end

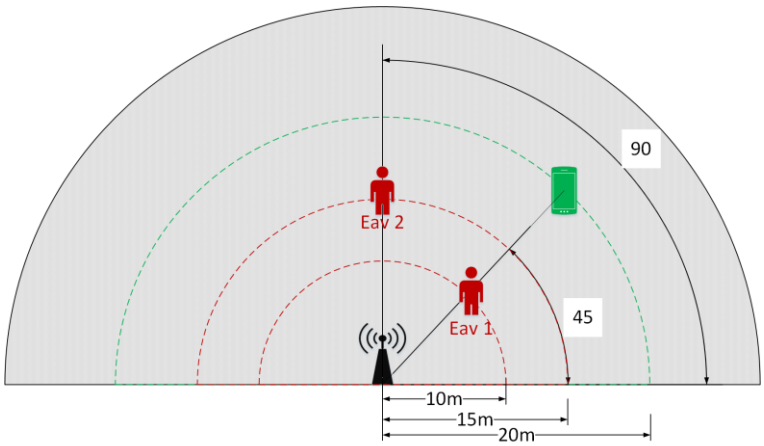


Fig. 3. System model of the first scenario

carrier frequency i.e. $k_n=0,\forall n\in\{0,1,\ldots,N-1\}$) and $\{\mathbf{w}_k\}_{k=1}^{G}$ are optimized to minimize the total transmit power;

II. Based on[21], all antenna elements are provided with random frequency increments, and $\{\mathbf{w}_k\}_{k=1}^{G}$ are optimized to minimize the total transmit power;

III. Proposed method, when the antennas' frequency increments $\{k_n\}_{n=0}^{N-1}$, and the beamforming vectors, $\{\mathbf{w}_k\}_{k=1}^{G}$, are determined by solving $\mathcal{Q}_{out}$ and $\mathcal{Q}_{in}$ respectively.

Discussion on Complexity: The computational complexity of schemes I and III are similar, i.e. they just solve $\mathcal{Q}_{in}$ with preset values for the frequency shifts. The proposed approach consists of two optimization problems where $\mathcal{Q}_{in}$ has the same complexity of schemes I and III. As discussed in section 3-2, $\mathcal{Q}_{out}$ is an NP hard problem if we want to find its optimal solution. However, since we have used GA, its computational complexity is similar to GA methods [26] and depends on the number of GA generations, the populations size and the complexity of solving the inner optimization problem. In short, thus, for a scenario with $\mathcal{K}$ generations and populations size of $\mathcal{P}$, the complexity of the proposed scheme is $\mathcal{K}\times\mathcal{P}$ times more than the complexity of schemes I and III.

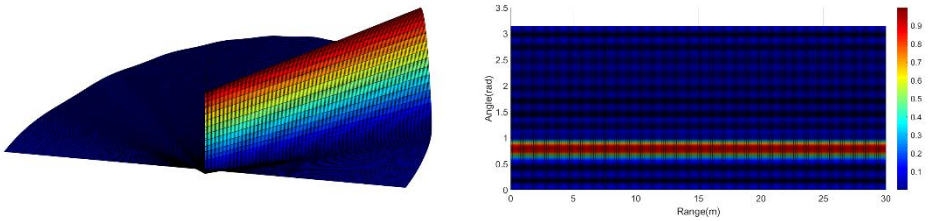
We now examine two scenarios in these schemes.

4-1- Simple Single-user Scenario

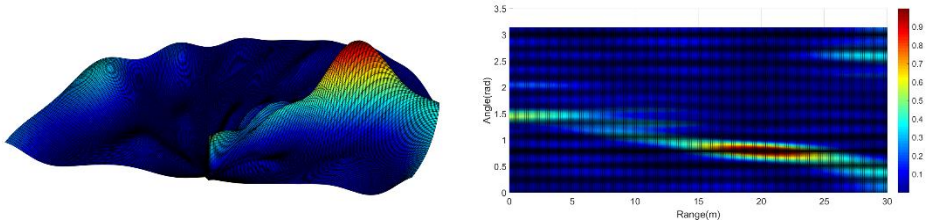
The first scenario is that there is only one legitimate receiver, i.e. one group and one user, Bob, at $(R_b,\theta_b)=(20m,45^\circ)$ and the transmitter sends a single message to Bob. There are also two eavesdroppers at $(R_{e_1},\theta_{e_1})=(10m,45^\circ)$ and $(R_{e_2},\theta_{e_2})=(15m,90^\circ)$. The system model of this scenario is depicted in Fig. 3.

Fig. 4 shows the received SINR at each point of the supporting area defined in (8) with $\gamma=1$, $\gamma_{sec}=0.01$ and $\sigma_i^2=\sigma_j^2=\sigma^2=0.001,\forall i,j$.

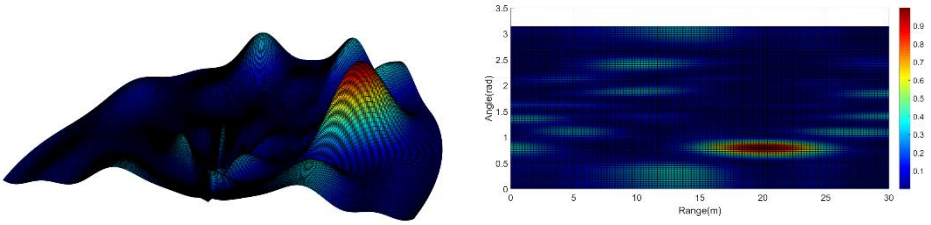
- Fig. 4-(a) shows the results of scheme I. Simulations show the same SINRs at all distances from the transmitter when $\theta=\theta_b=45^\circ$. So Eav1 locating in the same direction as Bob can easily overhear the messages.



(a) Scheme I



(b) Scheme II, $P_{total} = 0.14dBm$



(c) Scheme III, $P_{total} \approx 0.001dBm$

Fig. 4. Received SINRs in the first scenario, $N = 10$, $\gamma = 1$, $\gamma_{sec} = 0.01$ and $\sigma_i^2 = \sigma_j^2 = \sigma^2 = 0.001, \forall i, j$. Left figures are the qualitative polar views and the right ones show the exact angles (rad) and ranges (m) of the SINRs

- In Fig. 4-(b) results of scheme II are presented. Similar to [21], simulations show that there is just one point that can receive the largest SINR, which is the legitimate receiver's location, and the active eavesdroppers get the SINRs lower than γ_{sec} . In this scheme $P_{total} = 0.14dBm$.

• Results of our method, i.e. scheme III, is depicted in Fig. 4-(c). In this scheme $P_{total} \approx .001$, i.e. about zero dBm, which is very smaller than the scheme II.

Fig. 5 shows the 2D plots of SINRs at directions $\theta = 45^\circ = \pi/4$ and $\theta = 90^\circ = \pi/2$ where Eavs locate. As can be seen in Fig. 5, schemes II and III satisfy all conditions on desired and undesired receivers but scheme I can't guarantee maximum SINR, γ_{sec} , at Eav1 who is in the same direction as Bob. The green boxes show the SINRs that are satisfied at all desired and undesired receivers and the red box shows the violated SINR of Eav1 in scheme I.

Note that Fig. 5 only shows the SINRs at angles $\theta = \pi/4$ and $\theta = \pi/2$, and the complete performance can be observed by looking at Fig. 4.

4-2- Multi-user Multi-group Scenario

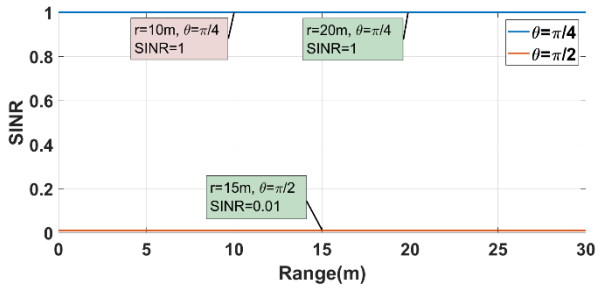
In the second scenario, there are three legitimate receivers in two groups ($G = 2, M = 3$). Two of them are in the first group at locations $(10m, 30^\circ)$ and $(15m, 60^\circ)$. The third one is in the second group located at $(25m, 90^\circ)$. There are two eavesdroppers at the same locations as the first scenario. Transmitter sends two different messages to both groups simultaneously by $N = 10$ antennas, and the SINR requirements of users are $\gamma_1 = 8, \gamma_2 = 6$. The maximum allowable SINRs for each group which can guarantee the security against other users and eavesdroppers are $\gamma_{sec_1} = 3$ and $\gamma_{sec_2} = 2$. The system model of the second scenario is shown in Fig. 6.

Fig. 7 shows the received SINRs, obtained from (8), at all points of the area assuming the three schemes.

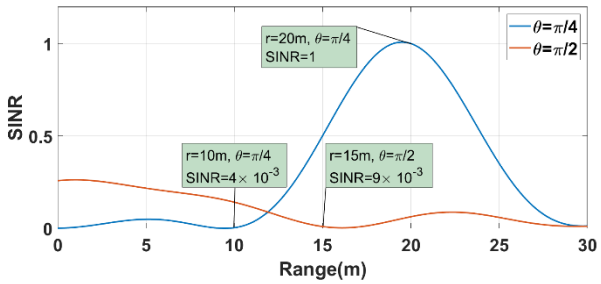
• Results of scheme I is shown in Fig. 7-(a). The result is generally similar to Fig. 4-(a) but the main lobs are in three directions where the legitimate receivers are located. The same eavesdropping issue exists in this scenario as well, where it can be seen that Eav2 can easily eavesdrop messages of the second group.

• Fig. 7-(b) depicts the SINRs at different locations of the area if we use the proposed scheme while we assign random frequency increments to antenna elements, i.e. no $\mathcal{Q}_{out}$, and optimal beamformer is selected based on $\mathcal{Q}_{in}$. We can see that there are three points at the desired locations that have the maximum SINRs and also each group has its own level of required SINR. Note that [21] was restricted to single user case so we can say scheme III is in fact the extension of [21] to the multiuser scenarios. In this scheme $P_{total} = 12.62dBm$.

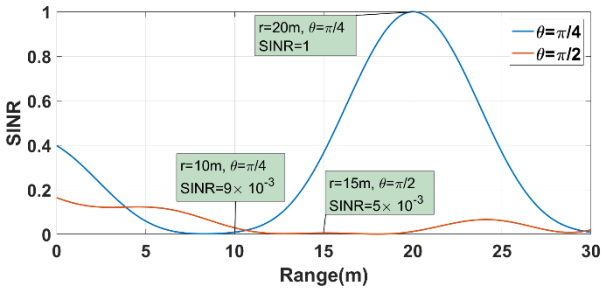
• Fig. 7-(c) illustrates the simulation results when we use the proposed scheme (scheme III), that is the optimization on beamforming vectors and frequency increments simultaneously. As can be seen (compared to Fig. 7-(b)), optimizing over $\{k_n\}_{n=0}^{N-1}$ can reduce total power effectively and



(a) Scheme I



(b) Scheme II



(c) Scheme III

Fig. 5. Received SINRs at all ranges of $\theta = \pi / 4$ (blue line) and $\theta = \pi / 2$ (red line). $N = 10$, $\gamma = 1$, $\gamma_{sec} = 0.01$ and $\sigma_i^2 = \sigma_j^2 = \sigma^2 = 0.001, \forall i, j$.

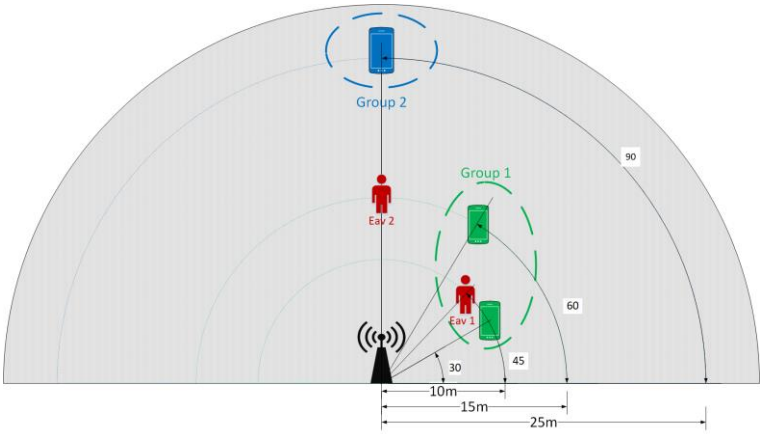
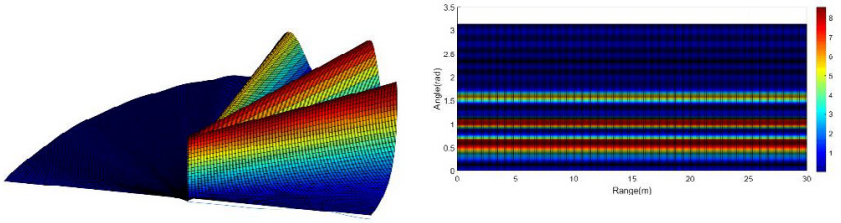


Fig. 6. System model of the second scenario

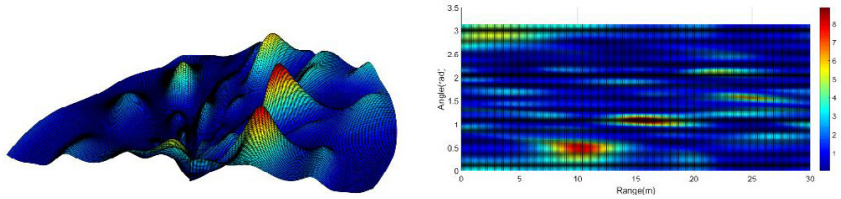
$P_{total} = 11.82 dBm$ in this scheme.

To see the effect of different number of antennas, we have simulated the network with different number of antennas. The results are presented in Fig. 8 and Fig. 9.

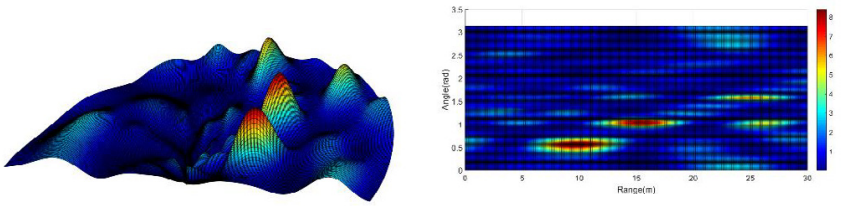
First, increasing N from 10 to 30, Fig. 8 shows the received SINR patterns when we have $N = 30$ antenna elements. As can be seen, this case has almost the same transmit power as $N = 10$ but the received beam-widths are much smaller and also the number and width of sidelobes are less than their counter-part in Fig. 7-(c). Similar behavior can be seen if we further change the number of antennas. Fig. 9 shows the effect of applying the frequency search optimization, i.e., comparing scheme III and scheme II, but for different number of antennas. As can be seen while number of antennas are not affecting the required power, scheme III always considerably reduces the required power. We note that scheme I is not included in this chart as that scheme is not capable of supporting multi-user multi-agent scenarios. If we look at the generated antenna patterns of each case, that we have presented for only $N = 30$ in Fig. 8, we see a more precise SINR pattern when increasing the number of antennas which, of course, incur higher computational complexity.



(a) Scheme I



(b) Scheme II, $P_{total} = 12.62dBm$



(c) Scheme III, $P_{total} = 11.82dBm$

Fig. 7. Received SINRs in the second scenario, $N = 10$, , $\gamma_2 = 6$, $\gamma_{sec_1} = 3$, $\gamma_{sec_2} = 2$ and $\sigma_i^2 = \sigma_j^2 = \sigma^2 = 0.001, \forall i, j$. Left figures are the qualitative polar views and the right ones show the exact angles (rad) and ranges (m) of the SINRs

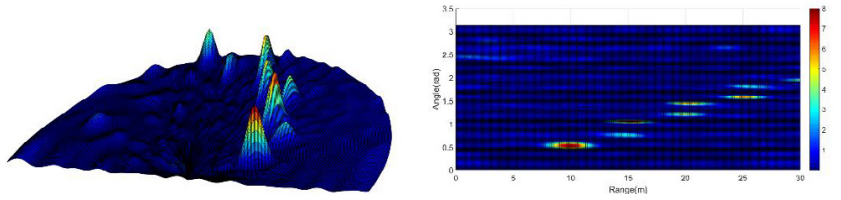


Fig. 8. Received SINRs from $N = 30$ transmit antenna elements using scheme III, $P_{total} = 11.80dBm$. $\gamma_1 = 8$, $\gamma_2 = 6$, $\gamma_{sec_1} = 3$, $\gamma_{sec_2} = 2$ and $\sigma_i^2 = \sigma_j^2 = \sigma^2 = 0.001, \forall i, j$. Left figure is the qualitative polar view and the right one shows the exact angles (rad) and ranges (m) of the SINRs.

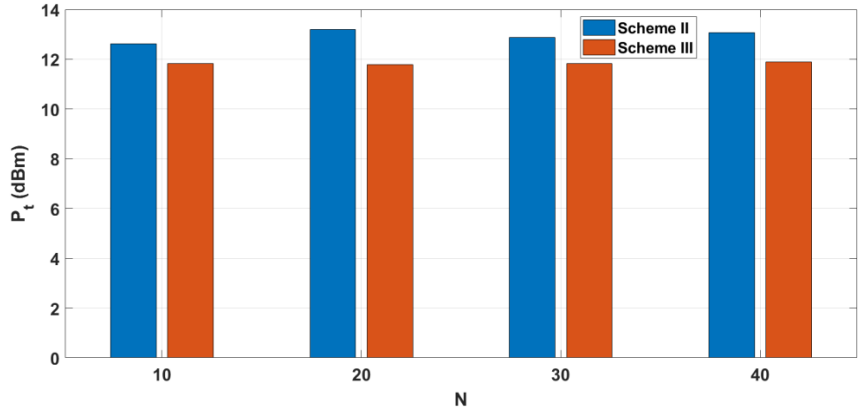


Fig. 9. Total transmit power used in schemes II and III with different number of transmit antenna elements, N . $\gamma_1 = 8$, $\gamma_2 = 6$, $\gamma_{sec_1} = 3$, $\gamma_{sec_2} = 2$ and $\sigma_i^2 = \sigma_j^2 = \sigma^2 = 0.001, \forall i, j$.

5. CONCLUSION

Beamforming is one of the techniques to provide secure communication for users which cannot afford high complexity cryptographic schemes. In this paper, in order to send different messages to multiple groups of users securely, against eavesdroppers or among each other, we proposed a scheme in which a two-step optimization problem is solved to approximate the optimal beamforming vectors and carrier frequency increment coefficients simultaneously. By jointly optimizing beamformers and frequency increments, the transmitted power can be directed to the desired range-angle pairs consuming less transmit power than just optimizing on beamformers. The effect of a higher number of antenna elements has been investigated and verified that increasing the number of transmit antenna elements reduces the total transmit power and enhances security.

REFERENCES

[1] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Communications Surveys & Tutorials, 19(1) (2016) 347-376.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE Journal on Selected Areas in Communications, 36(4) (2018) 679-695.

[3] A.D. Wyner, The wire-tap channel, Bell system technical journal, 54(8) (1975) 1355-1387.

[4] M.P. Daly, J.T. Bernhard, Directional modulation technique for phased arrays, IEEE Transactions on Antennas and Propagation, 57(9) (2009) 2633-2640.

[5] N.D. Sidiropoulos, T.N. Davidson, Z.-Q. Luo, Transmit beamforming for physical-layer multicasting, IEEE Trans. Signal Processing, 54(6-1) (2006) 2239-2251.

[6] M.P. Daly, E.L. Daly, J.T. Bernhard, Demonstration of directional modulation using a phased array, IEEE Transactions on Antennas and Propagation, 58(5) (2010) 1545-1550.

[7] Y. Ding, V.F. Fusco, A vector approach for the analysis and synthesis of directional modulation transmitters, IEEE Transactions on Antennas and Propagation, 62(1) (2013) 361-370.

[8] E. Karipidis, N.D. Sidiropoulos, Z.-Q. Luo, Far-field multicast beamforming for uniform linear antenna arrays, IEEE Transactions on Signal Processing, 55(10) (2007) 4916-4927.

[9] D. Wang, B. Bai, W. Zhao, Z. Han, A survey of optimization approaches for wireless physical layer security, IEEE Communications Surveys & Tutorials, 21(2) (2018) 1878-1911.

[10] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE transactions on wireless communications, 7(6) (2008) 2180-2189.

[11] F. Shu, L. Xu, J. Wang, W. Zhu, Z. Xiaobo, Artificial-noise-aided secure multicast precoding for directional modulation systems, IEEE Transactions on Vehicular Technology, 67(7) (2018) 6658-6662.

[12] R. Soltani, D. Goeckel, D. Towsley, B.A. Bash, S. Guha, Covert wireless communication with artificial noise generation, IEEE Transactions on Wireless Communications, 17(11) (2018) 7252-7267.

[13] A. Al-Nahari, G. Geraci, M. Al-Jamali, M.H. Ahmed, N. Yang, Beamforming with artificial noise for secure MISOME cognitive radio transmissions, IEEE Transactions on Information Forensics and Security, 13(8) (2018) 1875-1889.

[14] M.A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, M.-S. Alouini, Artificial Noise-Based Beamforming for the MISO VLC Wiretap Channel, IEEE Transactions on Communications, 67(4) (2018) 2866-2879.

[15] W.-C. Liao, T.-H. Chang, W.-K. Ma, C.-Y. Chi, QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach, IEEE Transactions on Signal Processing, 59(3) (2010) 1202-1216.

[16] P. Antonik, An investigation of a frequency diverse array, UCL (University College London), 2009.

[17] P.F. Sammartino, C.J. Baker, H.D. Griffiths, Frequency diverse MIMO techniques for radar, IEEE Transactions on Aerospace and Electronic Systems, 49(1) (2013) 201-222.

[18] W.-Q. Wang, Frequency diverse array antenna: New opportunities, IEEE Antennas and Propagation Magazine, 57(2) (2015) 145-152.

[19] P. Antonik, M.C. Wicks, H.D. Griffiths, C.J. Baker, Frequency diverse array radars, in: 2006 IEEE Conference on Radar, IEEE, 2006, pp. 3 pp.

[20] Y. Liu, H. Ruan, L. Wang, A. Nehorai, The random frequency diverse array: A new antenna structure for uncoupled direction-range indication in active sensing, IEEE Journal of Selected Topics in Signal Processing, 11(2) (2016) 295-308.

[21] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, Y. Zhang, Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays, IEEE Access, 5 (2017) 1658-1667.

[22] J. Lin, Q. Li, J. Yang, H. Shao, W.-Q. Wang, Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach, IEEE Transactions on Information Forensics and Security, 13(3) (2017) 671-684.

[23] B. Qiu, J. Xie, L. Wang, Y. Wang, Artificial-noise-aided secure transmission for proximal legitimate user and eavesdropper based on frequency diverse arrays, IEEE Access, 6 (2018) 52531-52543.

[24] B. Qiu, M. Tao, L. Wang, J. Xie, Y. Wang, Multi-beam directional modulation synthesis scheme based on frequency diverse array, IEEE Transactions on Information Forensics and Security, (2019).

[25] M. Grant, S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, in, 2014.

[26] U. ADEEC, Time complexity of genetic algorithms on exponentially scaled problems, Urbana, 51 (2000) 61,801.

HOW TO CITE THIS ARTICLE

N. Ravansalar, V. Pourahmadi, Distance-Aware Beamforming for Multiuser Secure Communication Systems, AUT J. Elec. Eng., 52(1) (2020) 97-106.

DOI: 10.22060/eej.2019.15573.5263