URSI GASS 2021, Rome, Italy, 28 August - 4 September 2021

Phased-Array Transmission for Secure Multiuser mmWave Communication via Kronecker Decomposition

Chentao Liang, Xuejing Zhang*
University of Electronic Science and Technology of China, Chengdu 611731, China
Email: 610074045@QQ.com; xjzhang7@163.com

Abstract

This paper considers the problem of security in phase-array transmission for multiple receivers. In the proposed algorithm, the phased-array transmission structure is considered, and we mainly concentrate on phase shift keying (PSK) and quadrature amplitude modulation (QAM). Specifically, in our problem formulation we assume 1) The proposed structure of antenna is uniform linear array (ULA); 2) The legitimate receivers are precisely known by the transmitter; 3) All channel vectors have a Vandermonde structures. Under the assumptions above and by judiciously examining the structures of phased array and corresponding mathematical model, we develop an approach to design the weight vector for each legitimate receiver based on Kronecker decomposition, which provides a relatively good randomness in designing weight vectors. Simulations are presented to demonstrate the effectiveness of the proposed algorithms under various types of modulation.

1 Introduction

Millimeter-wave (mmWave) wireless communication is regarded as a promising technology for mobile devices [1]. The small wavelength minimizes the eligible antenna space, making it possible for implementing large-scale arrays in both transmitter and receiver side. Similar to the conventional wireless communication system, communication via mmWave wireless system is able to be accessed by eavesdroppers illegally as well. Securing the whole process during transmission has become an indispensable part in order to avoid information disclosure.

Over the past several years, a wide range of measures have been developed to enhance the security in physical layer and achieve secure transmission. The basic approach is to form a deep nulls towards the direction of unexpected eavesdroppers under the condition that transmitter acknowledges the precise information of channel state information (CSI). However, such approach might not perform well in practical situation, since the eavesdroppers will not cooperate obediently, it is a difficult task to fully master their CSI [2]. In order to realize secure transmission with unknown eavesdropper channel or CSI partially known, the concept of artificial noise (AN) is proposed in [3], in which artificial noise is imposed on the information carrying signal to cover the confidential messages up. With AN being added on the orthogonal subspace of the main channel, the eavesdropper channel is degraded, which deteriorates the channel of eavesdropper efficiently as well. However, this might impair the data transmission power and decrease the signal-to-interference-plus-noise ratio (SINR) at the destination [4].

In recent years, the study of secure transmission using directional modulation (DM) technique gradually walks onto the stage. It produces an expected constellation towards the preset direction, scrambling received constellation at other undesired direction simultaneously. Particularly, the authors of [5] used a phased array at the transmitter to enhance the transmission security by altering the phase rate at symbol rate. In addition, this technique is also implemented in [6] by using a four-element patch array. The phase value is conducted by genetic algorithm, in order to modulate the symbols of quadratic phase shift keying (QPSK) modulation directionally. However, only approximate solutions can be obtained by the such methods, and the time-consuming of the phase value calculation is relatively high with large-scale array.

Based on existing work, we propose an algorithm for secure multiuser mmWave communication via Kronecker decomposition. The weight vectors of each legitimate receiver is designed by decomposing into sub-vectors, and then make the sub-vectors satisfy the constraints proposed below. This algorithm provides a relatively good randomness in designing weight vectors, which increases the difficulty for illegal access by eavesdroppers.

2 SYSTEM MODEL AND CONSTRAINTS FORMULATION

2.1 System model

The base station is equipped with N transmission antenna. Assume that there are K desired receivers and Q eavesdroppers. For simplicity, The legitimate receivers and eavesdroppers are all equipped with a single antenna. At each

discrete time t, the signals received by legitimate receivers and eavesdroppers are given respectively as follows:

$$\begin{aligned} y_k(t) &= \mathbf{h}_k^T \mathbf{x}_k(t) + \eta_k(t), k = 1,2,...,K \\ y_q(t) &= \mathbf{g}_q^T \mathbf{x}_k(t) + \kappa_q(t), Q = 1,2,...,Q \end{aligned} \tag{1}$$

where $\mathbf{h_k} \in \mathbb{C}^N$, is the channel vector that reflects the channel state of the k-th legitimate receiver, while $\mathbf{g_q} \in \mathbb{C}^N$ stands for that of the q-th eavesdropper, $\mathbf{x}$ represents the transmit signal vector, η_k and κ_q signify the additive Gaussian noise at the k-th receiver and the q-th eavesdropper respectively.

We consider an extended Saleh-Valenzuela geometric model [7] with single-path channel. Specifically, the Channel vector can be simplified to

$$\mathbf{h}_k = \alpha_k \mathbf{a}_k(\gamma_k) \tag{2}$$

where $\alpha_k \sim \mathscr{CN}(0,1)$ is the gain of the single path of the k-th receiver, γ_k is the angle of departure (AoD) of the single path to the k-th receiver, and $\mathbf{a}(\gamma_k) \in \mathbb{C}^N$ denotes the antenna array response vector at γ_k. It is the same situation for channel state of eavesdroppers.

2.2 The constraints

For the sake of simplification, the PSK modulated signal is considered. The transmitted vector at time t is given By

$$\mathbf{x}_k(t) = \mathbf{w}_k(t) x_k(t) \tag{3}$$

where $\mathbf{w}(t) \in \mathbb{C}^N$ is the transmitted weight vector, $x(k) = \sqrt{E_s} e^{j\xi(t)}$ denotes the modulated signal, where $\sqrt{E_s}$ is the baseband modulation amplitude, $\xi(t)$ represents the phase for transmitted message. Because the two phase shifters are the only parts that can be manipulated in the architecture mentioned above, the transmitting vector is constrained. Under such circumstances, without the loss of generality, it is assumed that

$$|\bar{\mathbf{w}}(t)| \leq 2 \tag{4}$$

where $\bar{\mathbf{w}}(t)$ is the total set of the weight vector corresponding to all channels, which is given by

$$\bar{\mathbf{w}}(t) = [\mathbf{w}_1(t) + \mathbf{w}_2(t) + ... + \mathbf{w}_k(t)]^T, k = 1,2,...,K \tag{5}$$

in fact, the total set of weight vector can be multiplied with a factor in order to satisfy the constraint (4) at any time, that is

$$|\bar{\mathbf{w}}(t)| \cdot \frac{2}{K} \leq 2 \tag{6}$$

Specifically, it is crucial to find the weight vectors $\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_k$ belonging to the null space of the unexpected receiver's channel and send valid message to the corresponding legitimate receiver. In other words, when subscript $i \neq j$, the transmitted vector should be 0, while when $i = j$, the result should be a constant that corresponds to each receiver (The time variable t is omitted for convenience in the following content), i.e.,

$$\mathbf{h}_{k_1}^T \mathbf{w}_{k_2} = 0, \text{for } k_1 \neq k_2 \tag{7}$$

$$\mathbf{h}_{k_1}^T \mathbf{w}_{k_2} = \alpha_k, \text{for } k_1 = k_2 \tag{8}$$

where α_k is the information that should be received at the $k-$th legitimate receiver, depending on the specific modulation. And $k_1 = 1,2,...,K, k_2 = 1,2,...,K$ respectively.

3 Using kronecker decomposition to solve phase equation

3.1 The structure of channel vector and weight vector

Based on the property of Kronecker decomposition [8], the channel vector h_{k_1} for the k_1-th legitimate receiver can be conducted as

$$\mathbf{h}_{k_1} = [1, e^{j2\pi d \cdot \sin(\gamma_{k_1})/\lambda}, ..., e^{(N-1)\{j2\pi d \cdot \sin(\gamma_{k_1})/\lambda\}}]^T \tag{9}$$

which satisfies the Vandermonde structure. To obtain the kronecker decomposed vector of channel vector, first the number of antenna should be decomposed as

$$N = n_D \cdot n_{D-1} \cdot ... \cdot n_m \cdot ... \cdot n_1 \tag{10}$$

where D equals to the number of prime factors that the antenna number N can be decomposed, n_m denotes one of the prime factors. Although the number type of n_m is not restricted in *Lemma 1*, the prime factor constraint is imposed to specify the decomposition process. Thus, the channel vector of the k-th legitimate receiver can be decomposed as follows

$$\mathbf{h}_{k_1} = \mathbf{u}_{D,k_1} \otimes \mathbf{u}_{D-1,k_1} \otimes ... \otimes \mathbf{u}_{m,k_1} \otimes ... \otimes \mathbf{u}_{1,k_1} \tag{11}$$

where each $\mathbf{u}_{m,k_1}$ has dimension of $n_m \times 1$. On the other hand, the weight vector for the k_2-th legitimate receiver $\mathbf{w}_{k_2}$ could also be written as the form of (11), with the m-th subvector of the k_2-th legitimate user denoted as $\mathbf{a}_{m,k_2}$,where $m = 1,...,D, k_2 = 1,...,K$.

3.2 Design of weight vector

Substituting $\mathbf{h}_{k_1}$, $\mathbf{w}_{k_2}$ with their corresponding equations, the equations (12) and (13) can be obtained.

The expected weight vector elements in weight vector set $\bar{\mathbf{w}} = [\mathbf{w}_1 + ... + \mathbf{w}_K]$ are supposed to satisfy constraint (7) firstly that mentioned above. And the randomly chosen product term in every row for each k_2 can form a new function set

$$\mathbf{u}_{r+m,k_1}^T \mathbf{a}_{r+m,k_2} = 0 \tag{14}$$

where $r \in \{1,2,...,j-1,j+1,...,K\}, k_2 = 1,...,K$. By substituting each $\mathbf{u}_{r+m,k_1}^T$ and $\mathbf{a}_{r+m,k_2}$ into the equation (14)

above, a function set for an $\mathbf{a}_{r+m,k_2}$ with n_m unknown phase variable is obtained as equation (15). To solve equation (15), the unknown phase variables in E part should be settled with random numbers at every time scale t and phase variable $\psi_{1,r+m,k_2}$ can obtained by moving E to the right side of the equation as well.

Having settled the $K-1$ terms in every $\mathbf{w}_{k_2}, k_2 = 1,...,K$ under the constraint (7), there are still $D-(K-1)$ degree of freedom for each $\mathbf{w}_{k_2}$ awaiting to be designed, i.e. $D-(K-1)$ subterms in every $\mathbf{w}_{k_2}, k_2 = 1,...,K$ haven't been settled, and they need to be fixed by satisfying condition (8). To obtain the rest of the unfixed phase variable in every $\mathbf{w}_{k_2}$, the terms $\mathbf{a}_{m,k_2}$ with fixed phase variable are put together and the same procedure with unfixed terms, that is, resequence the Kronecker decomposition equation of $\mathbf{w}_{k_2}$. In fact, this process is executed in expansion of $\mathbf{h}_{k_1}^T\mathbf{w}_{k_2} = \alpha_k, k_1 = k_2 = k = 1,2...,K$ below instead of with $\mathbf{w}_{k_2}$ alone. Based on the property of kronecker product that has been used in (12) and (13) above, the expansion of $\mathbf{h}_{k_1}^T\mathbf{w}_{k_2} = \alpha_k$ can be written as

$$(\mathbf{u}_{D,k_1}^T\mathbf{a}_{D,k_2})(\mathbf{u}_{D-1,k_1}^T\mathbf{a}_{D-1,k_2})...(\mathbf{u}_{1,k_1}^T\mathbf{a}_{1,k_2}) = \alpha_k \quad (16)$$

Under the circumstance of (16), the sequence of subvector for $\mathbf{h}_{k_1}^T\mathbf{w}_{k_2}$ is able to be changed at will, since every subvector $(\mathbf{u}_{m,k_1}^T\mathbf{a}_{m,k_2})$ represents a number that is connected by ordinary product sign. The resequenced expansion of (16) should follow the form that given in (17). Where r and f denote the randomly selected sub-product terms and free-sub-product terms respectively, $\mathbf{u}_{f+m,k_1}^T\mathbf{a}_{f+m,k_2}$ represents the degree of freedom part of $\mathbf{h}_{k_1}^T\mathbf{w}_{k_2}$. The previous randomly selected sub-product terms r can be moved to the right side of the equation, and free terms are able to be rewritten as in (18). By using the polygon construction algorithm[9], the phase of free terms in (18) can be solved. Having solved the phase for both randomly chosen part and free part, the new weight vector can be obtained by using kronecker product to both parts as showen in (19). Comparing (19) with its original sequence, there always exists a permutation to resequence (19). To reorganize the sequence, the communication matrix $\mathbf{K}_{mn}$ [10] can be conducted based on its property. And the proposed weight vector for each legitimate user is given as

$$\mathbf{w}_{k_2} = \mathbf{K}_{mn}\tilde{\mathbf{w}}_{k_2} \quad (20)$$

Eventually, the final weight vector $\bar{\mathbf{w}}_{k_2}$ could be obtained by adding all the weight vectors $\mathbf{w}_{k_2}$ of each legitimate receiver together.

Based on the description above, the procedure is summarized in Algorithm 1.

Algorithm 1: Using Kronecker decomposition to design weight vectors $\mathbf{w}_j$

Input: N, K, $\{\mathbf{h}_1^T, \mathbf{h}_2^T, ..., \mathbf{h}_K^T\}$
Output: $\mathbf{w}_{k_2}, k_2 = 1,2,...,K$

$N = n_D \cdot n_{D-1} \cdot ... \cdot n_1$
for $k_1 = 1,2...,K$ **do**
  $\mathbf{h}_{k_1}^T = \mathbf{u}_{D,k_1} \otimes \mathbf{u}_{D-1,k_1} \otimes ... \otimes \mathbf{u}_{1,k_1}$
end
for $k = 1,2...,K$ **do**
  Randomly select a group of $K-1$ sub-vectors sequentially from (19), Use random numbers to determine the phases E except the first, and the first unknown phase can be obtained by solving (15)
end
for $k_1 = k_2 = k = 1,2...,K$ **do**
  $\mathbf{h}_{k_1}^T\mathbf{w}_{k_2} = \alpha_k$, resequence the order of both $\mathbf{h}_{k_1}^T$ and $\mathbf{w}_{k_2}$ by using the properties of the Kronecker product. Move the randomly selected part to right side of the equation, solve the phase of the free terms.
end
for $k_1 = k_2 = k = 1,2...,K$ **do**
  $\mathbf{K}_{mn} = \sum_{j=1}^{n}(\mathbf{e}_j^T \otimes \mathbf{I}_m \otimes \mathbf{e}_j)$
  Obtain $\tilde{\mathbf{w}}_{k_2}$ by using kronecker product for the randomly selected terms and free terms.
  $\mathbf{w}_{k_2} = \mathbf{K}_{mn}\tilde{\mathbf{w}}_{k_2}$
end
$\bar{\mathbf{w}} = \sum_{k_2=1}^{K}\mathbf{w}_{k_2}$

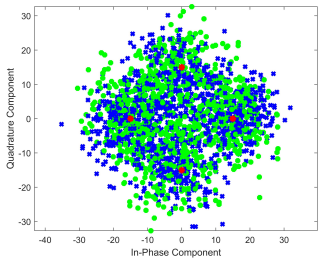
4 Numerical Results

The sections above elaborates the proposed Kronecker-decomposition-based algorithm for design weight vectors of multiuser. In order to verify the effectiveness of the proposed secure transmission algorithm, simulations are presented in this section. For simplicity, the number of legitimate receivers is chosen as $K = 3$, phase array element number $N = 64$, and modulation of QPSK, 8PSK and 16QAM are imposed to corresponding legal receivers respectively in 600 time intervals. The channel vectors can be obtained for all of three legitimate users by executing Algorithm 1. Thus, the constellation can be obtained. Figure 1 illustrates the noiseless received constellations results for the all of the three legal users and at two eavesdroppers respectively. What needs to be clarified is that during the process of simulation, the results of some time interval is abandoned for the sake of the stability of the final results, since the product of random selected subterms of both channel vector and weight vector are small, which may probably lead to the absence of solution when using polygon con-

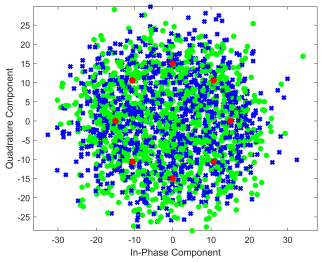
$$\mathbf{h}_{k_1}^T\mathbf{w}_{k_2} = (\mathbf{u}_{D,k_1}^T \otimes \mathbf{u}_{D-1,k_1}^T \otimes ... \otimes \mathbf{u}_{1,k_1}^T)(\mathbf{a}_{D,k_2} \otimes \mathbf{a}_{D-1,k_2} \otimes ... \otimes \mathbf{a}_{1,k_2}) \quad (12)$$

$$\mathbf{h}_{k_1}^T\mathbf{w}_{k_2} = (\mathbf{u}_{D,k_1}^T\mathbf{a}_{D,k_2})(\mathbf{u}_{D-1,k_1}^T\mathbf{a}_{D-1,k_2})...(\mathbf{u}_{m+1,k_1}^T\mathbf{a}_{m+1,k_2})(\mathbf{u}_{m,k_1}^T\mathbf{a}_{m,k_2})...(\mathbf{u}_{1,k_1}^T\mathbf{a}_{1,k_2}) \quad (13)$$

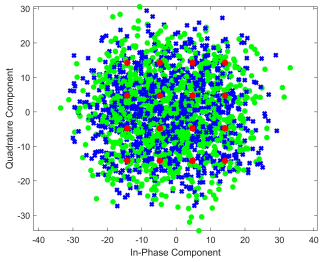
$$e^{j\psi_{1,r+m,k_2}} + \underbrace{e^{\{jn_{m-1}...n_1n_0\Theta_{k_1}+j\psi_{2,r+m,k_2}\}} + ... + e^{\{j(n_m-1)n_{m-1}...n_1n_0\Theta_{k_1}+j\psi_{n_m,r+m,k_2}\}}}_{\triangleq \mathsf{E}} = 0 \quad (15)$$



(a) Constellation of the first legitimate receiver based on QPSK



(b) Constellation of the second legitimate receiver based on 8PSK



(c) Constellation of the third legitimate receiver based on 16-QAM

Figure 1. The constellation result

struction algorithm to solve the phase.

5 Conclusion

In this paper, we have presented a algorithm of phase-array security transmission for multiple legitimate receivers based on the Kronecker decomposition and its related property. The orthogonality between weight vector and channel vector of different users is achieved, and it also provides a relatively good randomness in designing weight vectors for each legitimate user, increasing the complexity to the access of illegal eavesdroppers. The simulation is then conducted with different means of modulation for each legitimate receiver and eavesdroppers. However, there still exists some limitation. The algorithm consumes a relatively high degree of freedom, which may results in no phase solutions under certain circumstances. Based on the current work, study will be conducted to further improve the performance of this algorithm in the future.

References

[1] M. R. Akdeniz et al., "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1164-1179, Jun. 2014.

[2] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[4] Y. P. Hong, P. Lan, and C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[5] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[6] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[7] X. Yu, J. Shen, J. Zhang, and K. B. Letaief, "Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 485–500, Apr. 2016.

[8] G. Zhu, K. Huang, V. K. N. Lau, B. Xia, X. Li and S. Zhang, "Hybrid beamforming via the kronecker decomposition for the millimeter-wave massive MIMO systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 9, pp. 2097-2114, Sept. 2017.

[9] X. Zhang, X. Xia, Z. He and X. Zhang, "Phased-Array transmission for secure mmWave wireless communication via polygon construction," *IEEE Transactions on Signal Processing.*, vol. 68, pp. 327-342, 2020.

[10] Magnus J R, Neudecker H. The commutation matrix: Some properties and applications. Ann Ststist, 1979.7:381 394.

$$\underbrace{[(\mathbf{u}_{r+K-2,k_1}^T\mathbf{a}_{r+K-2,k_2})(\mathbf{u}_{r+K-3,k_1}^T\mathbf{a}_{r+K-3,k_2})\ldots(\mathbf{u}_{r,k_1}^T\mathbf{a}_{r,k_2})]}_{\triangleq \mathsf{r}}\overbrace{[(\mathbf{u}_{f+m,k_1}^T\mathbf{a}_{f+m,k_2})\ldots(\mathbf{u}_{f+1,k_1}^T\mathbf{a}_{f+1,k_2})(\mathbf{u}_{f,k_1}^T\mathbf{a}_{f,k_2})]}^{\triangleq \mathsf{f}} = \alpha_k \tag{17}$$

$$\hat{\mathbf{h}}_{k_1}^T\hat{\mathbf{w}}_{k_2} \equiv \underbrace{[\mathbf{u}_{f+m,k_1}^T\ldots\otimes\mathbf{u}_{f+1,k_1}^T\otimes\mathbf{u}_{f,k_1}^T][\mathbf{a}_{f+m,k_2}\ldots\otimes\mathbf{a}_{f+1,k_2}\otimes\mathbf{a}_{f,k_2}]}_{\triangleq \mathsf{f}} = \frac{\alpha_k}{\mathsf{r}} \tag{18}$$

$$\tilde{\mathbf{w}}_{k_2} = [\mathbf{a}_{r+K-2,k_2}\otimes\mathbf{a}_{r+K-3,k_2}\otimes\ldots\otimes\mathbf{a}_{r,k_2}]\otimes[\mathbf{a}_{f+m,k_2}\otimes\mathbf{a}_{f+m-1,k_2}\otimes\ldots\otimes\mathbf{a}_{f,k_2}] \tag{19}$$