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

Phased-Array Transmission for Secure mmWave Communication via Kronecker Decomposition

Ziyi Song, Xuejing Zhang*
University of Electronic Science and Technology of China, Chengdu 611731, China
E-mail: 2018190604003@std.uestc.edu.cn, xjzhang7@163.com

Abstract

This paper provides a secure communication algorithm based on Kronecker decomposition. The channel vector and gain are divided into Kronecker product form, and the corresponding weight vectors are calculated, then through Kronecker product of the subweight vectors, the weight vector can be generated. The security of the proposed algorithm is demonstrated by simulation.

1 Introduction

Wireless communication field is facing the contradiction between the shortage of traditional spectrum resources and the explosive growth of the demand of the communication industry. Therefore, millimeter-wave communication, which has a large number of under-utilized spectrum resources, has become one of the potential key technologies of 5G wireless communication system (see [1], [2] and [3]). In the field of wireless communication, the phased array antenna is superior to the general mechanical scanning array, thus has strong vitality and great practical application value.

Because of the broadcast characteristics of wireless communication, the signal is likely to be eavesdropped, so the security of wireless communication is a question deserving research. In the past few years, quite a number of algorithms have been proposed in the field of wireless secure communication. In the paper [4], a directional modulation algorithm based on the antenna subset modulation (ASM) is proposed. Different from other directional modulation methods, ASM projects clear constellations for all directions, while randomly selecting the antenna subset, additional points are added to the constellation. Which has no effect on the target receiver, however, for random directions, these additional points will randomize the signal along side lobe thus realize directional safe communication. The author of [5] presented a reliable approach to establish a non-zero secret capacity link in the side lobe direction, switching phased array (SPA) wireless transmission structure. SPA consists of a phased array emitter and an antenna with a switch, through randomly turning off an antenna, a well-defined constellation is emitted in the desired direction, on the contrary, for the undesired direction, phase and amplitude of the constellation are scrambled. A programmable weighted phased array (PWPA) algorithm supporting secure mmWave communication is proposed in [6], PWPA adjusts the weights of base station antenna with the aid of a traditional phased array and a programmable power amplifier. Compared with the traditional scheme, PWPA can generate more artificial noise in the non-target directions. In the paper [7], a effective approach for secure communication is developed. The phased array antenna is divided into several antenna subsets, each of which can transmit directional beam waves, at the same time, all the subsets are combined. In order to achieve directional modulation with a higher scheduling resolution, on the premise of maintaining coherent directional gain, even if the location of the eavesdroppers is unknown.

Motivated from these papers, a phased-array transmission algorithm for secure millimeter wave communication based on Kronecker decomposition is proposed in this paper. We consider the case of single path channel, when the number of element antenna is a power of 2. The channel gain and channel vector are Kronecker decomposed into a number of individual two-dimensional matrices, the corresponding matrices are calculated to obtain the subweight vector, then take the Kronecker product of subweight vectors to generate the weight vector.

2 Preliminaries

We consider a MISO communication system, where has channel vector $\mathbf{h}$ with N antennas. Assume that the signal received by the target at time k, $y(k)$ can be written as

$$y(k) = \mathbf{h}^H \mathbf{x}(k) + \eta(k) \tag{1}$$

where $\eta(k) \sim CN(0, \sigma^2)$ is the Gaussian noise and when considering the PSK modulation, the transmit vector $\mathbf{x}(k)$ equals to $\mathbf{w}(k)x(k)$, where $\mathbf{w}(k) \in C^N$ stands for the weight vector and $x(k)$ represents the signal after PSK modulation.

Define the beam gain of the single path channel as a given constant β, we have

$$\mathbf{h}^H \mathbf{w} = \beta. \tag{2}$$

the time variable k is omitted for the sake of simplification.

In particular, the channel vector $\mathbf{h}$ can be equivalently described as

$$\mathbf{h} = \alpha \mathbf{a}(\phi) \tag{3}$$

where α denotes the path gain and $\mathbf{a}(\phi)$ stands for the steering vector at departure angle ϕ. Moreover $\mathbf{a}(\phi)$ is often formulated as

$$\mathbf{a}(\phi) = [1, e^{j\varphi}, \ldots, e^{j(N-1)\varphi}]^T. \tag{4}$$

where $\varphi \triangleq 2\pi d \sin(\pi)/\lambda$, λ denotes the wavelength, d stands for the distance from one element to the next. The weight vector $\mathbf{w}$ satisfies the constant modulus constraint $|\mathbf{w}| = 1$, and denote the angle of $\mathbf{w}$ as ω_n, thus we get

$$\mathbf{w} = \left[e^{j\omega_1}, e^{j\omega_2}, \ldots, e^{j\omega_N}\right]^T. \tag{5}$$

3 Algorithms

We consider the case of a single path channel when the amount of antennas N equal to 2^M, where M is an arbitrary positive integer. The channel vector $\mathbf{h}$ satisfies

$$\mathbf{h} = [1, e^{j\varphi}, \ldots, e^{j(N-1)\varphi}]^T, \tag{6}$$

and the vector a can be decomposed as

$$\mathbf{h} = \mathbf{h}_M \otimes \mathbf{h}_{M-1} \otimes \cdots \otimes \mathbf{h}_m \otimes \cdots \otimes \mathbf{h}_1 \tag{7}$$

where $\otimes$ represents the Kronecker product, and the m_{th} element is

$$\mathbf{h}_m = [1, e^{j2^{(m-1)}\varphi}]^T, \tag{8}$$

where $m = 1, 2, \ldots, M$. In the same way, the weight vector $\mathbf{w}$ can be formulated into the Kronecker structure

$$\mathbf{w} = \mathbf{w}_M \otimes \mathbf{w}_{M-1} \otimes \cdots \otimes \mathbf{w}_m \otimes \cdots \otimes \mathbf{w}_1 \tag{9}$$

where the factor $\mathbf{w}_m$ is

$$\mathbf{w}_m = [e^{j\omega_{m,1}}, e^{j\omega_{m,2}}]^T. \tag{10}$$

According to the beam pattern $\mathbf{h}^H\mathbf{w} = \beta$ and

$$\begin{aligned}(\mathbf{h}_M \otimes \mathbf{h}_{M-1} \otimes \cdots \otimes \mathbf{h}_1)^H (\mathbf{w}_M \otimes \mathbf{w}_{M-1} \otimes \cdots \otimes \mathbf{w}_1) \\ = (\mathbf{h}_M^H \otimes \mathbf{w}_M)(\mathbf{h}_{M-1}^H \otimes \mathbf{w}_{M-1}) \ldots (\mathbf{h}_1^H \otimes \mathbf{w}_1)\end{aligned} \tag{11}$$

the received signal can be expressed as

$$(\mathbf{h}_M^H \mathbf{w}_M)(\mathbf{h}_{M-1}^H \mathbf{w}_{M-1}) \cdots (\mathbf{h}_1^H \mathbf{w}_1) = \mathbf{h}^H \mathbf{w} = \beta. \tag{12}$$

We construct the beam β into M sub-gain and written as

$$\beta = \beta_M \beta_{M-1} \cdots \beta_m \cdots \beta_1 \tag{13}$$

where

$$\beta_m = \mathbf{h}_m^H \mathbf{w}_m = e^{j\omega_{m,1}} + e^{j(\omega_{m,2} - 2^{(m-1)}\varphi)}. \tag{14}$$

In order to compute each $\mathbf{w}_m$, the corresponding β_m should be determined first. When $e^{j\omega_{m,1}}$ and $e^{j(\omega_{m,2}-2^{(m-1)}\varphi)}$ are of the same direction, β_m obtains the maximum value 2, on the contrary, when the two vectors are of the opposite direction β_m gets the minimum value 0. As a consequence, we conclude that $\beta_m \in [0,2]$ and it is easy to obtain the domain of β, where $\beta \in [0, 2^M]$. At the same time, in order to achieve reliable communication to target, the signal-noise ratio SNR need be larger than threshold Ω, where $SNR = E_s|\mathbf{h}^H\mathbf{w}(k)|^2/\sigma^2 > \Omega$, $\sqrt{E_s}$ represents amplitude modulation. We difine $\sqrt{\Omega\sigma^2/E_s} \triangleq \rho$, thus we conduct that $\beta > \rho$, so we express $\beta \in [\rho, 2^M]$. To be more mathematically precise, and make sure that there are M β_m that satisfy the equation (13), we assume the domain of the first $M-1$ β_m is β_m is $[\beta_{min}, \beta_{max}]$. Hence the last β_M is evaluate in the range $[\frac{\beta}{\beta_{max}^{M-1}}, \frac{\beta}{\beta_{min}^{M-1}}]$, it should satisfy $\beta_m \in [0,2]$, where $\frac{\beta}{\beta_{min}^{M-1}} < 2$ and $\beta_{min} > \sqrt[M-1]{\frac{\beta}{2}}$, thus the $[\beta_{min}, \beta_{max}]$ is derived as $[\sqrt[M-1]{\frac{\beta}{2}}, 2]$ and the last β_M is calculate $\beta_M = \frac{\beta}{\prod_{m=1}^{M-1}\beta_m}$. In the above discussions, we have specified the feasible set of β_m, note the equation(14), phase $\omega_{m,1}$ and $\omega_{m,2}$ of the weight vector are given by

$$\omega_{m,1} = \pm \arccos\left(\frac{\beta_m}{2}\right) \tag{15}$$

$$\omega_{m,2} = \mp \arccos\left(\frac{\beta_m}{2}\right) + 2^{(m-1)}\varphi \tag{16}$$

where $m = 1, 2, \ldots, M$, and it is easy to get the weight vector

$$\mathbf{w} = \mathbf{w}_M \otimes \mathbf{w}_{M-1} \otimes \cdots \mathbf{w}_m \cdots \otimes \mathbf{w}_1. \tag{17}$$

To make the above description clear, the procedure of algorithm is presented.

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

Input: $\mathbf{h} = [1, e^{j\varphi}, \ldots, e^{j(N-1)\varphi}]^T, M, \beta, \varphi$
Output: $\mathbf{w} = \left[e^{j\omega_1}, \ldots e^{j\omega_N}\right]^T$

for k=1, 2 ,… **do**
  calculate $[\beta_{min}, \beta_{max}]$, where $\beta_{min} = \sqrt[M-1]{\frac{\beta}{2}}$ and $\beta_{max} = 2$
  for m= $M, M-1, \ldots, 1$ **do**
    if m>1 **then**
      randomly select β_m in the range $[\beta_{min}, \beta_{max}]$
    else
      $\beta_m = \frac{\beta}{\prod_{m=2}^{M}\beta_m}$
    end if
    $\omega_{m,1} = \pm \arccos\left(\frac{\beta_m}{2}\right)$ and
    $\omega_{m,2} = \mp \arccos\left(\frac{\beta_m}{2}\right) + 2^{(m-1)}\varphi$
    $\mathbf{w}_m = [e^{j\omega_{m,1}}, e^{j\omega_{m,2}}]^T$
  end for
  $\mathbf{w} = \mathbf{w}_M \otimes \mathbf{w}_{M-1} \otimes \cdots \mathbf{w}_m \cdots \otimes \mathbf{w}_1$
end for

4 Numerical Results

Numerical simulations are exhibited in this section to demonstrate the performances of proposed algorithm. In all the simulation examples below, we consider the phased array structure with 20 uniform linear array elements. The departure angle ϕ is uniform distributed in the domain $[-\pi/2, \pi/2]$, and the *SNR* threshold Ω is assumed as 100, the baseband modulation amplitude $\sqrt{E_s}$ is set as 1 and variance σ^2 of the Gaussian noise is 0.01, thus we obtain $\rho = 1$. We assume that the noise power of target and eavesdropper are identical. The number of discrete transmission time k is 1000. We suppose that the base station does not know the channel vectors of eavesdroppers, if there are two eavesdroppers and are randomly selected from $[-\pi/2, \pi/2]$.

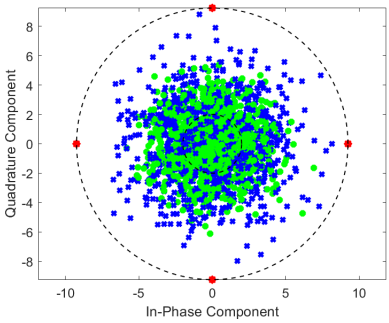

Figure 1. noiseless constellation with QPSK modulation

In this example, we simulate a scenario where QPSK modulation are used. The different patterns shown in the Figure1 illustrate the received signals, where the red points represent the synthesized constellation of the target receiver, the green points denote the received constellation of the first eavesdropper and the blue points stands for the resultant constellation of the second eavesdropper, respectively. Four red points with defined pattern are shown in the diagram, which illustrates that the algorithm can project a clear constellation in the desired direction; the disorganized blue and green points demonstrate that in the non-target directions, the algorithm transmits random signals.

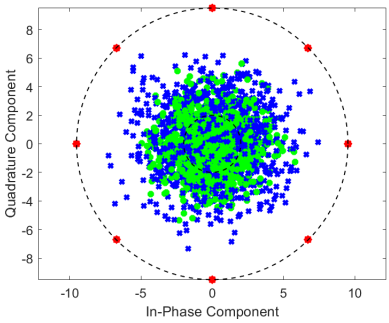

Figure 2. noiseless constellation with 8-PSK modulation

Our second example corresponds to the same setting with 8-PSK modulation. The noiseless constellations at target receiver and the two eavesdroppers with the proposed algorithm are presented in Figure2. There are eight red points arranged in a regular pattern, indicating that the receiver can receive a clear signal; the jumble blue and green points suggest that for non-target directions, a jumbled constellation will be received.

5 Conclusions

In this paper, a secure communication algorithm based on Kronecker decomposition is proposed. The channel gain and channel vector are divided into Kronecker subsets to obtain the corresponding weight vector, then the weight vector is obtained according to Kronecker product. Through simulation of QPSK and 8-PSK modulation, the defined pattern of the target and irregular constellations of the undesired directions are obtained, thus the security of the proposed algorithm is proved. For single-path channel, this algorithm realizes simple and reliable secure communication, on the other hand, it would be interesting to study multipath channel for further research.

References

[1] Xuejing Zhang, Xiang Gen Xia, Zishu He, and Xuepan Zhang. Phased-array transmission for secure mmwave wireless communication via polygon construction. *IEEE Transactions on Signal Processing*, 68:327–342, 2020.

[2] Sundeep Rangan, Theodore S. Rappaport, and Elza Erkip. Millimeter wave cellular wireless networks: Potentials and challenges. *Proceedings of the IEEE*, 102(3):366–385, 2014.

[3] T. S. Rappaport, Shu Sun, R. Mayzus, Hang Zhao, and F. Gutierrez. Millimeter wave mobile communications for 5g cellular: It will work! *IEEE Access*, 1(1):335–349, 2013.

[4] Valliappan, Nachiappan, Lozano, Angel, Heath, and W. Robert. Antenna subset modulation for secure millimeter-wave wireless communication. *IEEE Transactions on Communications*, 61(8):3231–3245, 2013.

[5] N., N., Alotaibi, K., A., and Hamdi. Switched phased-array transmission architecture for secure millimeter-wave wireless communication. *IEEE Transactions on Communications*, 64(3):1303–1312, 2016.

[6] Yuanquan Hong, Xiaojun Jing, and Hui Gao. Programmable weight phased-array transmission for secure millimeter-wave wireless communications. *IEEE Journal of Selected Topics in Signal Processing*, pages 1–1, 2018.

[7] Wen Qin Wang and Zhi Zheng. Hybrid mimo and phased-array directional modulation for physical layer security in mmwave wireless communications. *IEEE Journal on Selected Areas in Communications*, PP(7):1–1, 2018.