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

A Simple Secure Transmission Algorithm for mmWave Communication

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

In this paper, a simple phased-array transmission algorithm for secure millimeter-wave wireless communication is proposed. The essence is to use the permutation matrix to replace the element of a known weight vector, therefore a new weight vector is obtained as the identical gain is maintained for the single channel. Clear constellations are projected to the target, on the other hand, random constellations are transmitted for undesired directions. Compared with other algorithms, this algorithm exhibits significant computational advantages as well as the ability of flexible combination with the existing algorithms to expand the solution set of the original algorithm. The simulation results show that the proposed algorithm can generate time-varying weight vectors thus realize the secure mmWave communication in a simple way.

1 Introduction

Over the last several decades, there has been an upsurge of interest in millimeter wave wireless communication. It is caused by the huge demand for data services brought by the mobile Internet and the Internet of Things (IOT), which makes the traditional mobile communication spectrum resources tend to be saturated; see the literature such as [1], [2] and [3]. One of the most classical methods in the field of wireless communication is the phased array antenna, of which the transmission weight vector are changed with time, for the sake of secure transmission.

There are several existing transmission algorithms for secure millimeter wave communication. The author of [4] has developed a point-to-point antenna subset modulation (ASM) algorithm of low complexity. Briefly speaking, in order to transmit data in target direction and to project random constellations in undesirable directions, ASM only uses the specific subset of antennas to modulate radiation in the direction of the target at a symbol rate; while for the undesired direction, a random subset of the antenna is selected for information transmission. In order to enhance the physical layer security, a new transmit structure switched phased-array (SPA) is proposed in [5]. Direction-dependent information can be realized through a conventional phased array transmitter along with an antenna with switch. More specifically, clear information is transmitted in the direction of the target while a constellation with distorted amplitude and phase is projected in undesired direction. In [6], a programmable weighted phased array (PWPA) structure is proposed. In PWPA, a conventional phased array structure and a programmable power amplifier are used to modulate the amplitude weight of the antenna for the sake of generating more artificial noise in non-target directions. For MIMO, phased-array time-modulated directional modulation scheme is proposed in [7]. In this scheme, the transmitting array is divided into subsets, and each of which forms a directional beam. By combining all the subsets, the angular resolution can be improved. It is worth mentioning that under the condition of not knowing the position of eavesdropper, the physical layer secure communication of millimeter wave can be realized. Besides, to achieve secure communication for general multi-path channels, a transmission algorithm using polygon construction approach is presented in [8], while the signal emitted by the array element are treated as vectors on the complex plane and through generating a geometric polygon that satisfies the channel constraint the time-varying weight vectors are obtained.

Inspired by the above paper, a simple secure transmission algorithm is proposed in this paper. Based on a set of weight vector, the new time-varying weight vectors can be obtained by a simple permutation operation. In addition, this method can also combine with the existing weight vector algorithms, which achieve the purpose of increasing the possible solutions of weight vector, and improve the security of the physical layer of wireless communication.

2 Preliminaries

For a MISO communication system, we assume that the base station contains N transmitting antennas, at discrete time k, the target receiver receives the data

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

where $\mathbf{h} \in C^N$ denotes the channel vector, $\mathbf{x}(k)$ stands for the transmit vector, $\eta(k) \sim CN(0, \sigma_t^2)$ represents the Gaussian noise and $\mathbf{x}(k) = \mathbf{w}(k)x(k)$, where $\mathbf{w}(k) \in C^N$ denotes the weight vector, $x(k)$ is the modulated signal, when considering the PSK modulation.

For single path channel, the channel vector $\mathbf{h}$ satisfies

$$\mathbf{h} = \alpha \mathbf{a}(\phi) \tag{2}$$

where α represents the gain of the path, $\mathbf{a}$ denotes the array response vector at the angle of departure ϕ, $\mathbf{a}(\phi)$ is given by

$$\mathbf{a}(\phi) = [1, e^{j\varphi}, \ldots, e^{j(N-1)\varphi}]^T. \tag{3}$$

where λ is the wavelength, d represents the distance between adjacent matrix elements, and denote $2\pi d \sin(\pi)/\lambda$ as φ. $\mathbf{w}(k)$ is the emission weight vector at time k, where k is omitted in the later sections for the sake of simplicity, and $\mathbf{w}$ satisfies the constant modulus constraint, where

$$|w_n(k)| = 1, n = 1, \ldots, N. \tag{4}$$

Denote $\omega_n = \angle w_n$, thus $\mathbf{w}$ can be expressed as

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

The beam gain of the target receiver is a prespecified constant β,

$$\mathbf{h}^H \mathbf{w} = \beta. \tag{6}$$

which indicates that there are multiple groups of weight vectors to make the target get the same gain. Besides, to the guarantee a reliable communication, the instantaneous receiving SNR_k (signal-noise ratio) at time k should be greater than a given threshold(denotes by Ω_t). For which $E_s|\mathbf{h}^H \mathbf{w}(k)|^2/\sigma_t^2$, where $\sqrt{E_s}$ stands for the amplitude modulation. Using this representation, we have $SNR_k = E_s|\mathbf{h}^H \mathbf{w}(k)|^2/\sigma_t^2 > \Omega_t$, and we define $\sqrt{\Omega_t \sigma_t^2/E_s}$ as ρ, thus the beam gain of the target should satisfy

$$\beta > \rho. \tag{7}$$

3 Algorithms

Suppose that a set of weight vector $\mathbf{w}_{initial}$, where $\mathbf{w}_{initial} = \left[e^{j\omega_{initial,1}}, \ldots e^{j\omega_{initial,N}}\right]^T$, has already been obtained based on the algorithm proposed in [8] via polygon construction. Denote the product of $\mathbf{h}^* \odot \mathbf{w}_{initial}$ as $\mathbf{v}_{initial}$,

$$\mathbf{v}_{initial} = \mathbf{h}^* \odot \mathbf{w}_{initial}. \tag{8}$$

Since the summation order does not affect the result, we could change the calculate order of β through the permutation matrix $\mathbf{P}$, where

$$\sum_{n=1}^{N} e^{j\left(\omega_{initial,n} - (n-1)\varphi\right)} = \beta. \tag{9}$$

where $v_{initial,n}$ stands for the nth element of the vector $\mathbf{v}_{initial}$. Denote the vector after random arrangement $\mathbf{P}\mathbf{v}_{initial}$ as $\mathbf{p}$, where $\mathbf{p} = \mathbf{P}\mathbf{v}_{initial}$, we have

$$\mathbf{p} = [e^{j\theta_1}, e^{j\theta_2}, \ldots, e^{j\theta_N}]^T \tag{10}$$

and throuth backward extrapolation, the new weight vector $\mathbf{w}_{new}$ can be obtained. Define the product of $\mathbf{h}^* \odot \mathbf{w}_{new}$ as $\mathbf{v}_{new}$, we get

$$\mathbf{v}_{new} = \mathbf{h}^* \odot \mathbf{w}_{new}. \tag{11}$$

Because the new weight vector $\mathbf{w}_{new}$ also accords with the beam gain,

$$\sum_{n=1}^{N} e^{j\left(\omega_{new,n} - (n-1)\varphi\right)} = \beta, \tag{12}$$

we conclude that

$$\mathbf{v}_{new} = \mathbf{p}, \tag{13}$$

thus it is easy to obtain the phase of $\mathbf{v}_{new}$

$$v_{new,n} = \theta_n, \tag{14}$$

where $n \in [1, 2, \ldots, N]$ and $v_{new,n}$ represent the nth element of the vector $\mathbf{v}_{new}$, and we express the phase of $\mathbf{w}_{new}$ as

$$\omega_{new,n} = \theta_n + (n-1)\varphi, \tag{15}$$

Therefore, we could generate the new weight vector $\mathbf{w}_{new}$, as $\mathbf{w}_{new} = \left[e^{j\omega_{new,1}}, \ldots, e^{j\omega_{new,n}}, \ldots, e^{j\omega_{new,N}}\right]^T$.

To make the above derivation clearer, the corresponding pseudocode is listed below.

Algorithm A Simple Secure Transmission Algorithm for mmWave Communication

Input: $\mathbf{w}_{initial} = \left[e^{j\omega_{initial,1}}, \ldots e^{j\omega_{initial,N}}\right]^T$
$\mathbf{h} = [1, e^{j\varphi}, \ldots, e^{j(N-1)\varphi}]^T$
Output: $\mathbf{w}_{new} = \left[e^{j\omega_{new,1}}, \ldots e^{j\omega_{new,N}}\right]^T$

for k=1,2,... **do**
  calculate $\mathbf{v}_{initial} = \mathbf{h}^* \odot \mathbf{w}_{initial}$, where $\mathbf{v}_{initial} = [e^{j\omega_{initial,1}}, e^{j\left(\omega_{initial,2} - \varphi\right)}, \ldots, e^{j\left(\omega_{initial,N} - (N-1)\varphi\right)}]^T$
  randomly generate a $N \times N$ dimensional permutation matrix $\mathbf{P}$
  calculate $\mathbf{p} = \mathbf{P}\mathbf{v}_{initial}$
  the vector after permutation $\mathbf{p}$ is obtained, where $\mathbf{p} = [e^{j\theta_1}, e^{j\theta_2}, \ldots e^{j\theta_{N-1}}, e^{j\theta_N}]^T$.
  for $n = 1, 2, \ldots, N$ **do**
    solve $v_{new,n} = \omega_{new,n} - (n-1)\varphi = \theta_n$
    where $\omega_{new,n} = \theta_n + (n-1)\varphi$
  end for
  generate $\mathbf{w}_{new} = \left[e^{j\omega_{new,1}}, \ldots, e^{j\omega_{new,n}}, \ldots, e^{j\omega_{new,N}}\right]^T$
end for

4 Numerical Results

In this section, several sets of simulation results will be provided to demonstrate the performance of the proposed algorithm. Considering the single-path millimeter wave channel with 20 uniform linear elements, and the angle of departure ϕ is randomly distributed in $[-\pi/2, \pi/2]$. Assume that the threshold SNR_k, Ω_t is 320, the base band modulation amplitude $\sqrt{E_s}$ is 1 and the variance σ_t^2 of Gaussian noise to the target is 0.05, therefore, we get $\rho = 4$. Besides, the noise power at target and eavesdropper are assumed to be the same and the number of emission is chosen as 1000. Suppose there are two eavesdroppers and the base station

does not know their channel vectors, so their channel vectors are randomly selected in $[-\pi/2, \pi/2]$.

In the first example, we simulate the algorithm under QPSK modulation. The figure1 shows the constellations received at the target and two eavesdroppers using the proposed algorithmwhere red points represent the constellation received by the target and blue and green points stand for the signals received by the two eavesdroppers. We can see from the figure that four distinct points are received at the target receiver, which indicates the algorithm can transmit clear constellation. However, at the undesired location, signals with disordered pattern are received, which means the algorithm will project random signals.

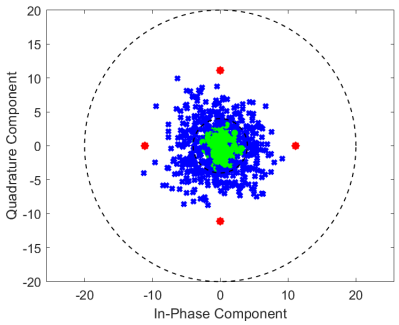

Figure 1. noiseless constellation with QPSK modulation

The other simulation settings are the same as previous. Based on the 8-PSK modulation, we get the constellations at target and two eavesdroppers as figure2. There are eight defined red points in figure2, revealing that at the target receiver, clear constellation is received. In contrast, the constellations received at the two eavesdropper locations are distorted.

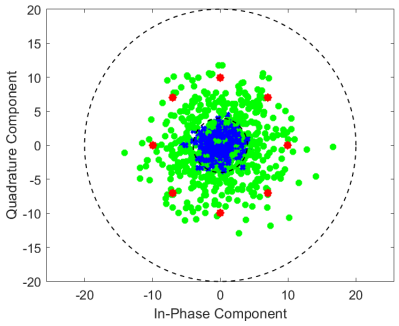

Figure 2. noiseless constellation with 8-PSK modulation

5 Conclusions

This paper presents a simple secure transmission algorithm for millimeter wave wireless communication using permutation matrix. When a set of weight vectors is known, time-varying weight vectors can be obtained by simple permutation operation. The algorithm has a fast computing speed, at the same time, when this algorithm is combined with other secrecy algorithms, the analytical solutions of the original algorithm can be increased to a large extent, for the sake of enhancing the confidentiality. Simulation results for QPSK and 8PSK modulation show that the proposed algorithm can obtain time-varying weight vectors, thus the secure communication of physical layer is realized. Since the theoretical foundation of the algorithm is that for single-path channels, which the gain of each transmitting array element is identical. However, for multiple path channels, this limitation is not satisfied, therefore, this algorithm is only applicable to single-path channel transmission. As future directions, we shall consider extension to multiple path channel communication.

References

[1] Sridhar Rajagopal, Shadi Abu-Surra, Zhouyue Pi, and Farooq Khan. Antenna array design for multi-gbps mmwave mobile broadband communication. *IEEE Global Telecommunications Conference*, pages 5–9, 2011.

[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.

[8] 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.