Advances in Computer Science Research (ACRS), volume 54
International Conference on Computer Networks and Communication Technology (CNCT2016)

Physical-Layer Secure Transmission Method with Random Sparse Array

Min WU[1] and Meng WU[2]

[1]Nanjing University of Posts and Telecommunication, Nanjing,210003, China

[2]Nanjing University of Posts and Telecommunication, Nanjing,210003, China

[1]wumincmm@163.com

Keywords: Physical Layer Security, Sparse Array, Genetic Algorithm, Codebook, Random Selection

Abstract. With the characteristics of narrow scanning beam and high spatial resolution, sparse array becames a research hotspot. However, it can produce higher side lobes which leads to the information leakage easily. A physical layer secure transmission method based on sparse array was proposed in this paper to achieve secure communications. We used the genetic algorithm with two objective functions to produce multiple sparse array structures with low sidelobes, and then created a codebook. When transmitting signals, we selected a sparse array structure randomly for each symbol from the codebook. Both theoretical analysis and simulation results show that the proposed method can ensure the communication security.

Introduction

Wireless mobile communication is experiencing a huge change in data business with the popularity of variety intelligent and the increasing demand for future wireless applications in recent years, which speeds up the research on the fifth generation(5G) network[1] and providing a more safe and reliable service is a primary task in the design and implementation of the 5G network [2].Compared to traditional wireless communication network, physical layer security is identified as a promising strategy to safeguard data confidentiality by smartly exploiting the imperfections of the communications medium, and it can reap the benefits offered by promising technologies, e.g massive multiple-input multiple-output[3]. Massive MIMO technology has these characteristics of increasing frequency efficiency, reducing transmission power and forming a narrow beam communications.

Small array element spacing leads to serious mutual coupling effect which degrades the system performance, So sparse array[4] with fewer array elements has weak mutual coupling effect, which are more suitable for Massive MIMO system. Periodic thinning of the antenna array produces high sidelobes, causes some interference to security communication. We can use intelligent optimization algorithms[5], such as genetic algorithm, simulated annealing algorithm, to optimize the sparse array structure , However, it only can overcome the large sidelobe levels, and cannot prevent the eavesdroppers from acquiring sensitive information from the received signal.

Recently, Several approaches related to antenna subset modulation have been proposed for achieving enhanced security. In [6], according to the training sequence for estimating channel parameters from the desired receiver, selecting randomly part of array elements in order to achieve the purpose of equivalent random channel change, so as to ensure the eavesdropper's low probability of intercept. While [7] proposed a technique to select an antenna subset randomly for every symbol.

Randomly switching antenna subsets effectively randomizes the constellation of the received symbol for an eavesdropper in other directions, while doesn't affect the radiation pattern in the desired direction. But random antenna subset switching may lead to large sidelobes and the signal constellation distortion in undesired direction may not be so serious that sensitive eavesdroppers can get correct information.

To overcome these security problems, this paper proposes a sparse array random selection scheme based on codebook, Using genetic algorithm to optimize the structure of sparse array, and random selecting sparse array to transmit information.

Sparse Array Model

The antenna array consists of linear array, planar array and three-dimensional array, both of which can be divided into uniform and non-uniform array. According to principle of pattern multiplication, the uniform linear array pattern E with M RF chains along any direction θ can be written as:

$$E(\theta)=\sum_{m=0}^{M-1} I_m \cdot e^{j\varphi} \cdot e^{jkdm\,(cos\theta - cos\theta_0)} \cdot elis(m) \quad (1)$$

where elis(m) is the pattern function of every array element, I_m and φ respectively refers to the excitation amplitude and phase. d is the distance between the adjacent elements, and we specify $\mathrm{d} \leq \lambda/2$, where λ is the wavelength; θ_0 is the desired direction.

Figure 1 shows the structure of a sparse linear array with N($< M$) array elements.

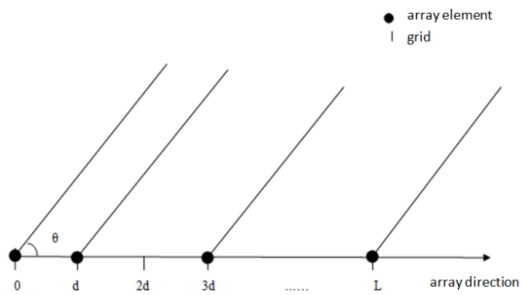


Fig.1 The structure of sparse linear array

We consider uniform linear arrays with isotropic antennas, that is,elis$(m) = 1$. All array elements are excited with the same amplitude and phase, that is I_m=1,φ=0.Using (1), the pattern function of sparse array with a binary bit CC_m,which indicates whether the array is excited:

$$E(\theta)=\sum_{m=0}^{M-1} CC_m \cdot I_m \cdot e^{j\varphi} \cdot e^{jkdm\,(cos\theta - cos\theta_0)} \cdot elis(m) \quad (2)$$

Optimizing Sparse Array based on Genetic Algorithm

In [7], a random selection scheme based on simulated annealing algorithm is proposed, the cost function of which is minimizing the sidelobe level, but without considering the distortion degree of the signal constellation in the undesired direction. However, QPSK demodulation determines information bits based on the quadrant that the constellation points locates in. If the distortion isn't serious, such as every constellation point still falls in the correct quadrant, the sensitive eavesdroppers can restore information. Here we use genetic algorithm[8](GA) with multi-objective functions to optimize sparse array, including minimizing the sidelobe level and maximizing the signal constellation distortion in undesired directions. According to the pattern of the sparse array (2), we can define the cost functions as follows:

$$\min\left\{f_1 = \left|\frac{\sum_{m=0}^{M-1} CC_m \cdot e^{jkdm\,(cos\theta - cos\theta_0)}}{FF_{max}} \cdot \mathrm{elis}(m)\right|\right\} \quad (3-1)$$

$$\max\left\{\mathrm{f}_2 = \int_{\theta_0-10}^{\theta_0+10} \left|\frac{F}{M}\sum_{m=0}^{M-1} CC_m \cdot e^{jkdm\,(cos\theta - cos\theta_0)} - F\right| d\theta\right\} \quad (3-2)$$

(3-1) denotes the first optimization function, the FF_{max} represents the mainlobe peak;

(3-2) denotes the second optimization function, it maximizes the signal constellation distortion within $\pm 10^{\circ}$ range of the desired direction.

Fig.2 depicts the radiation patterns of a synthesized sparse array using genetic algorithm and of a conventional array without optimization.The optimized one exhibits a lower sidelobe level of -15.86 dB, as expected, while the other one's sidelobe level is -13.51 dB when steered to broadside, which is improved 2.35 dB .

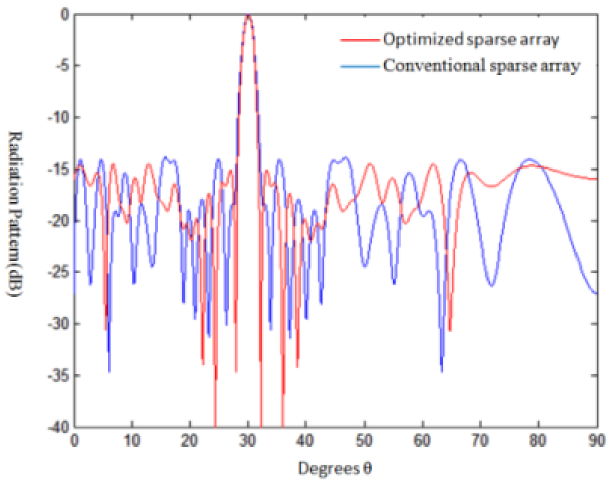
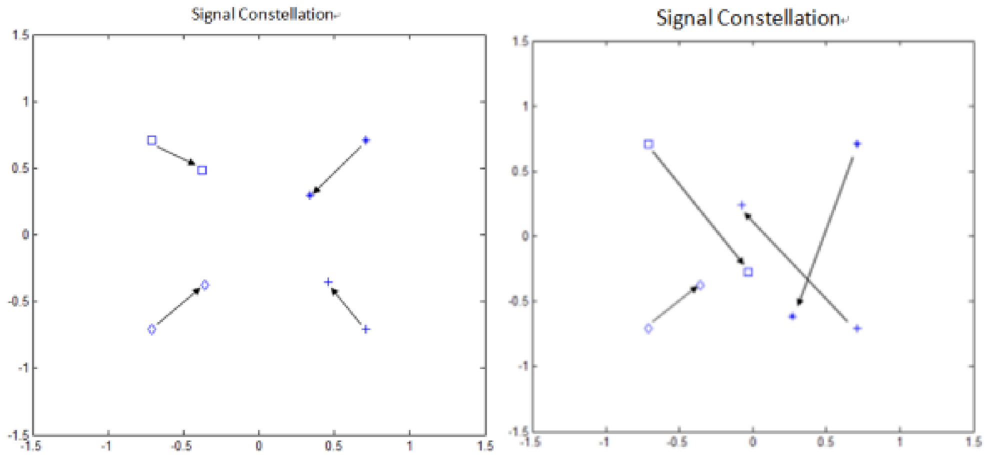


Fig.2 radiation patterns of a synthesized and a conventional sparse array

In Fig.3, (a) (b) repectively depicts the signal constellation in 40° from a synthesized sparse array and of a conventional array. It is not difficult to see that the distortion of signal constellation is random, if the constellation points only move a limited distance towards the coordinate origin (as (a) shown), where the receiver can restore the correct information; while severe distortion of the constellation points have moved to other quadrants(as (b) shown), which further strengthens the security of information transmission.



(a) (b)

Fig.3 diagram of distorted signal constellations

Secure Performance Analysis

Considering that the array transmits a complex phase-modulated symbol $e^{j\varphi(i)}$ to a target receiver using conventional baseband modulation.By beamforming on the original signal, the noiseless symbol received along an arbitrary direction θ is:

$$f(i,\theta) = e^{j\varphi(i)} \cdot \frac{\sum_{m=0}^{M-1} e^{jkdm(\cos\theta-\cos\theta_0)}}{M} \quad (4)$$

As we can see from formula (4), when $\theta = \theta_0$, the received signal in desired direction is the same as the original one, that is , $f(i,\theta) = e^{j\varphi(i)}$;when the undesired direction $\theta \neq \theta_0$ ($cos\theta \neq cos\theta_0$), the signal can be abbreviated as $f(i,\theta) = e^{j\varphi(i)}.e^{j\sigma}$, which is equivalent to the original signal phase rotated a fixed angle. While the shape of the signal constellation does not change, therefore, the traditional phase modulation isn't safe enough.Therefore this paper proposed that randomly selecting a sparse array from the codebook for each symbol, the formula (4) can be rewritten as:

$$f(i,\theta) = e^{j\varphi(i)} \cdot \frac{\sum_{n\in\mathcal{P}} e^{jkdm\,(cos\theta - cos\theta_0)}}{M} \tag{5}$$

Where $\mathcal{P}$ represents the optimized sparse array set ,namely codebook. when $\theta = \theta_0$, the received signal in desired direction is the same as the original one, that is , $f(i,\theta) = e^{j\varphi(i)}$; when the undesired direction $\theta \neq \theta_0(cos\theta \neq cos\theta_0)$, the signal can be abbreviated as $f(i,\theta) = e^{j\varphi(i)}.e^{j\sigma(\theta,p(i))}$, now the received signal not only related to the direction θ , but also to the sparse array structure. Received signal and original signal have a random phase difference $\sigma(\theta, p(i))$ ($p(i)$ is one structure of the codebook $\mathcal{P}$).Thus it distorts the received signal constellation in undesirable direction, from the physical layer level increases the difficulty for the eavesdropper to decode and strengthens the system security.

As you can see in Fig.4 (a)(b), the signal constellation synthesized in the desired direction ($\theta_0 = 30°$) is undistorted, while the received constellation in undesired direction($\theta = 50°$) appears randomized because of the random choice of a sparse array for each symbol, where constellation points wrongly fall in the other quadrants. The randomized selection procedure synthesizes a multi-point constellation to confuse undesired receivers. Also shown in Fig.4 (b)(c) is that under the premise of a fixed thinning rate, the greater of the antenna base, the more serious of signal constellation distortion in the undesired direction.

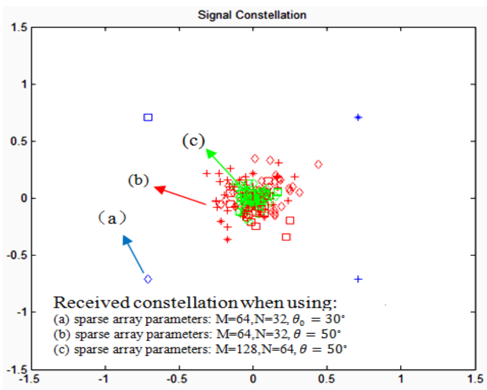


Fig.4 Signal constellations along desired(($\theta_0 = 30°$) and undesired direction（$\theta = 50°$）

Conclusions

This paper proposes a sparse array random selection scheme based on genetic algorithm, which can achieve secure transmission goal from the physical layer level.

On one hand, using intelligent algorithm optimizes sparse array with the optimal performance and maximizing the signal constellation distortion in undesired direction, which can reduce the risk of information leakage from the sidelobes in a certain extent; on the other hand, sparse array random selection artificially introduces randomness to distort the received constellation, making it more difficult for the eavesdropper to recover information, and further improving the security performance. Theoretical analysis and simulation results show that the sparse array not only reduces the deployment cost, but also achieves the secure transmission goal.

Future work will be extended to multidimensional periodic arrays, such as planar array and three-dimensional array, Incorporating multidirectional and multiusers transmission capabilities to the proposed scheme using array partitioning techniques is also an interesting research problem that merits further study.

Acknowledgement

In this paper, the research was sponsored by the Nature Science Foundation of Jiangsu Province (Project No.BK20151507)

References

[1] Soldani D and Manzalini A. Horizon 2020 and beyond: On the 5G operating system for a true digital society[J]. IEEE Vehicular Technology Magazine, 2015,10(1):32-42.

[2] Yang Nan and Wang Lifeng. Safeguarding 5G wireless communication networks using physical layer security[J].IEEE Communications Magazine, 2015, AP-15(4): 0163-6804.

[3] Larsson E G, Tufvesson F, Edfors O,et al.. Massive MIMO for next generation wireless systems[J]. IEEE Communications Magazine, 2014, 52(2): 186-195.

[4] Roberts W, Xu L,LiJ,et al.. Sparse antenna array design for MIMO active sensing applications[J]. IEEET ransactions on Antennas and Propagation, 2011,59(3): 846-858.

[5] BV Ha，RE Zich，M Mussetta，et al..Thinning array using improved compact Genetic Algorithm[J]. IEEE International Symposium on Antennas, 2013,9(6):592-593.

[6] H. Alves, R. D. Souza, M. Debbah, et al.. Performance of transmit antenna selection physical layer security schemes[J]. IEEE Signal Process, 2012, 19(6): 372–375.

[7] Nachiappan Valliappan, Angel Lozano, Robert W. Heath Jr, et al.. Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication[J]. IEEE Transactions on Communication，2013, 61(8):3231-3244.

[8] Ha Bui-van, Zich R E, Mussetta M, et al.. Improved compact Genetic Algorithm for thinned array design[C]. Proceedings of the 7th European Conference on Antennas and Propagation (EuCAP), Gothenburg, Sweder, 2013 :1807-18