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

Security Enhancement of Directional Modulation Scheme Against Hybrid Eavesdroppers

Bin Qiu, Ling Wang*, Xin Yang, Jian Xie
School of Electronics and Information, Northwestern Polytechnical University, Xi'an, China

Abstract

The goal of this paper is to address the physical layer security (PLS) problem for a hybrid wiretapping wireless system, where active eavesdroppers (AE) and passive eavesdroppers (PE) may coexist to intercept the confidential messages and disrupt traffic. To this end, we propose a directional modulation (DM) scheme that uses frequency diverse array (FDA) with aided artificial noise (AN) technique at the transmitter to achieve angle-range dependent secure transmission, and phased-array antennas at the receiver to eliminate the jamming signals. Simulation results verify the superiority of the proposed scheme.

1 Introduction

The phased-array directional modulation (DM) technique is one of effective approaches to enhance PLS. It can preserve the standard symbol constellation of the transmit signal over a predefined direction in free space while trying to debilitate the received signal of the eavesdroppers (Eve). Most of the previous work on PLS using DM focuses on passive eavesdroppers (PE) [1], where the Eve aims at intercepting information and not disrupting traffic. However, active eavesdroppers (AE) can actively attack and interfere the reception of legitimate user (LU), which leads to the security issues.

In this paper, we investigate a beamforming DM technique such that guarantees the PLS in the presence of hybrid Eve. The PE wiretap the confidential signal, but never transmit signals. The AE may wiretap the confidential signal and/or transmit a jamming signal, which can be discovered by the transmitter. However, AE may be too far away from the transmitter or high-dynamic jammers. The coordinate of AE is not available by the transmitter, precisely. Therefore, we assume a worst-case assumption that the positions of PE and AE are both unknown at the transmitter. In contrast to the secrecy rate optimization, where requires perfect or statistical information of the Eve, we design the transmit beamforming vector and artificial noise (AN) under unknown the information of Eve,

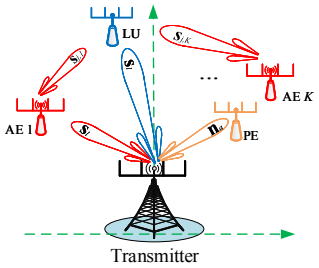

Figure 1. Model the of the DM with hybrid Eve.

which is more practical. The received signal-to-noise ratio (SNR) and phase at LU are taken into account to guarantee the valid reception of the LU with minimum transmit message power. The rest of total transmit power can be allocated to AN. Additionally, we design the weight vector at the LU by using the minimum variance distortionless response (MVDR) method to eliminate the interference of AE.

2 System Sketch and Signal Model

Let us consider a line-of-sight (LoS) communication system, as seen in Fig. 1, that consists of a transmitter equipped with an N-antenna, an M-antenna LU. Unless otherwise stated, multi-antenna array is assumed as an uniform linear array (ULA) in this paper. We assume that the coordinate of the LU is known at the transmitter. Without loss of generality, we set the first element of the transmitter and LU as a reference element. We utilize random frequency diverse array (FDA) due to its satisfactory decoupled performance between the range and angle [2]. Therefore, the radiated frequency of the nth antenna element is given by

$$f_n = f_c + \Delta f_n, n \in \mathcal{N}, \tag{1}$$

where $f_c \in \mathbb{R}$ represents the carrier frequency, $\mathcal{N} \triangleq \{1, 2, ..., N\}$, and frequency offsets $\Delta f_n = \eta_n \Delta f$. $\Delta f \in \mathbb{R}$ refers to the frequency increment. η_n is chosen as a random variable with i.i.d.

In the far-field assumption, i.e., parallel wavefront, the steering vector of FDA transmitted signal to (r, θ) and

phased-array antenna received signal from direction (θ) are defined as

$$\mathbf{h}(r,\theta) \triangleq \Big[e^{-j2\pi\Delta f_1(t-\frac{r}{c})},..., e^{-j2\pi\left\{\frac{f_c(N-1)d_t\sin\theta}{c}+\Delta f_N\left[t-\frac{r-(N-1)d_t\sin\theta}{c}\right]\right\}}\Big]^H, \quad (2)$$

and

$$\mathbf{a}(\theta) \triangleq \left[1, e^{-j2\pi\frac{f_c d_l\sin\theta}{c}},..., e^{-j2\pi\frac{f_c(M-1)d_l\sin\theta}{c}}\right]^H, \quad (3)$$

respectively, where c represents the speed of light, d_t and d_l refer to the inter-element spacing of the ULA at the transmitter and LU, respectively. As a result, the FDA beampattern with phased-array receiver in the free-space path loss model is given by [3]

$$\begin{aligned} &B(r,\theta,t) \\ &= \rho(r_n)\, e^{-j2\pi f_c\left(t-\frac{r}{c}\right)}[\mathbf{h}(r,\theta)\otimes\mathbf{a}(\theta)]^H[\mathbf{v}\otimes\mathbf{w}] \\ &\approx \rho(r)\, e^{-j2\pi f_c\left(t-\frac{r}{c}\right)}\mathbf{h}^H(r,\theta)\mathbf{v}\mathbf{a}^H(\theta)\mathbf{w}, \end{aligned} \quad (4)$$

where $\otimes$ is Kronker product, $\mathbf{v} = [v_1, v_2, ..., v_N]^T$ is the beamforming vector, $\mathbf{w} = [w_1, w_2, ..., w_M]^T$ is the beamforming weight vector, and $\rho(r)$ is the path loss in free space and approximate to $1/r^2$. Due to the far-field model, we present a reasonable approximation $r_n \approx r$ being the range between the transmitter and receiver.

Considering the strategy of AN-aided FDA beamforming, the instantaneous transmitted message is given by

$$\mathbf{s}_l = \mathbf{v}x + \mathbf{n}_a, \quad (5)$$

where x is the confidential symbol chosen from the constellation diagram with $\mathbb{E}[|x|^2] = 1$, $\mathbf{n}_a = \mathbf{T}_a\mathbf{z}$ is AN, $\mathbf{T}_a \in \mathbb{C}^{N\times(N-1)}$ refers to the AN projection matrix for forcing interference to the regions of Eve, and AN vector $\mathbf{z} \in \mathbb{C}^{(N-1)\times 1}$ consists of complex Gaussian variables with $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}_{N-1})$.

Assume (r_l, θ_l) and $(r_{j,k}, \theta_{j,k})$ as the positions of LU related to transmitter and AE k, $k \in \mathcal{K}$, $\mathcal{K} \triangleq \{1, 2, ..., K\}$, K is the number of AE, respectively. To simplify the notations, we define $\mathbf{h}_l \triangleq \mathbf{h}(r_l, \theta_l)$ and $\mathbf{a}_{j,k} \triangleq \mathbf{a}(\theta_{j,k})$. In addition, it is assumed that the AE knows the carrier frequency, or else the LU can eliminate the jamming signals from AE by a filtering in the frequency domain. It is assumed that the synchronization of time and frequency is perfect in the ideal scenario. Then, the down converted baseband signal at LU is given by

$$y_l = \rho(r_l)\mathbf{h}_l^H\mathbf{s}_l\mathbf{a}_l^H\mathbf{w} + \sum_{k=1}^{K}\rho(r_{j,k})\sqrt{E_{j,k}}s_{j,k}\mathbf{a}_{j,k}^H\mathbf{w} + n_l, \quad (6)$$

where $s_{j,k}$ is the jamming signal from AE k with $\mathbb{E}[|s_{j,k}|^2] = 1$, $E_{j,k}$ is the transmit power of AE k, $k \in \mathcal{K}$, and n_l is the complex additive white Gaussian noise (AWGN) with $n_l \sim \mathcal{CN}(0, \sigma_l^2)$.

For the Eve, we define $\mathbf{h}_e \triangleq \mathbf{h}(r_e, \theta_e)$ and $\mathbf{a}_e \triangleq \mathbf{a}(\theta_e)$. The beamforming weight vector of Eve is set to point to the transmitter, i.e.,$\mathbf{w} = \mathbf{a}_e/N$. We assume the interference from other Eve can be eliminated through cooperation. The signal received at Eve is given by

$$y_e = \rho(r_e)\mathbf{h}_e^H\mathbf{s}_l\mathbf{a}_e^H\mathbf{w} + n_e, \quad (7)$$

where n_e is the complex AWGN with $n_e \sim \mathcal{CN}(0, \sigma_e^2)$.

3 Proposed Secure Strategy

To achieve PLS, it is important to ensure the confidential messages can be received by the LU, precisely, but equally important to avoid eavesdropping. To this end, we propose an efficient secure communication strategy.

As is well known, the add of AN is able to interfere with Eve, but it also takes up total transmit power consumption. Hence, the rational transmit power allocation between the messages and AN is very crucial for security. Notice that we have assumed that the total transmit power at the transmitter is fixed. Less transmit power of messages means: 1). less message power is leaked to Eve, and 2). more power can be allocated to AN. We adopt a transmit message power minimization (MPM) criterion, subject to constraints on the received SNR and fixed phase, i.e.,

$$\min_{\mathbf{v}} \ \|\mathbf{v}\|_2^2 \quad (8a)$$

$$\text{s.t. } \rho^2(r_l)|\mathbf{h}_l^H\mathbf{v}|^2 \geq \zeta\sigma_l^2, \quad (8b)$$

$$\arg(\mathbf{h}_l^H\mathbf{v}) = \phi, \quad (8c)$$

where $\zeta \in \mathbb{R}$ is the desired SNR target for the LU, and ϕ is a fixed phase rotation. To solve above problem, it is equivalent to the following problem replaced with in-phase and quadrature constraints

$$\min_{\mathbf{v}} \ \|\mathbf{v}\|_2^2 \quad (9a)$$

$$\text{s.t. } \mathrm{Re}(\mathbf{h}_l^H\mathbf{v}) \geq \sigma_l\sqrt{\zeta/(1+\alpha^2)}/\rho(r_l), \quad (9b)$$

$$\alpha\mathrm{Re}(\mathbf{h}_l^H\mathbf{v}) - \mathrm{Im}(\mathbf{h}_l^H\mathbf{v}) = 0, \quad (9c)$$

where $\alpha = \tan(\phi)$. To remove the real and imaginary valued parts from (9), we can use $\mathbf{h}_l^H = \mathrm{Re}(\mathbf{h}_l^H) + j\mathrm{Im}(\mathbf{h}_l^H)$ and $\mathbf{v} = \mathrm{Re}(\mathbf{v}) + j\mathrm{Im}(\mathbf{v})$ to separate the real and imaginary valued parts as

$$\begin{aligned} \mathbf{h}_l^H\mathbf{v} =& \mathrm{Re}(\mathbf{h}_l^H)\mathrm{Re}(\mathbf{v}) - \mathrm{Im}(\mathbf{h}_l^H)\mathrm{Im}(\mathbf{v}) \\ &+ j[\mathrm{Im}(\mathbf{h}_l^H)\mathrm{Re}(\mathbf{v}) + \mathrm{Re}(\mathbf{h}_l^H)\mathrm{Im}(\mathbf{v})]. \end{aligned} \quad (10)$$

Then, we have

$$\mathrm{Re}(\mathbf{h}_l^H\mathbf{v})=\mathbf{h}_{l,1}^T\tilde{\mathbf{v}},\mathrm{Im}(\mathbf{h}_l^H\mathbf{v})=\mathbf{h}_{l,2}^T\tilde{\mathbf{v}}, \tag{11}$$

where $\tilde{\mathbf{v}} = [\mathrm{Re}(\mathbf{v})^T,\mathrm{Im}(\mathbf{v})^T]^T$, $\mathbf{h}_{l,1}^T = [\mathrm{Re}(\mathbf{h}_l^H),-\mathrm{Im}(\mathbf{h}_l^H)]$, $\mathbf{h}_{l,2}^T=[\mathrm{Im}(\mathbf{h}_l^H),\mathrm{Re}(\mathbf{h}_l^H)]$. Also, it is easy to see that $\|\mathbf{v}\|_2^2=\|\tilde{\mathbf{v}}\|_2^2$. Then, the optimal problem (9) is replaced by

$$\min_{\tilde{\mathbf{v}}} \ \|\tilde{\mathbf{v}}\|_2^2 \tag{12a}$$

$$\text{s.t. } \mathbf{h}_{l,1}^T\tilde{\mathbf{v}}\geq\xi, \tag{12b}$$

$$(\alpha\mathbf{h}_{l,1}^T-\mathbf{h}_{l,2}^T)\tilde{\mathbf{v}}=0, \tag{12c}$$

where $\xi=\sigma_l\sqrt{\zeta/(1+\alpha^2)}/\rho(r_l)$. Based on the singular value decomposition (SVD) characteristic [4], $\alpha\mathbf{h}_{l,1}^T-\mathbf{h}_{l,2}^T$=$\mathbf{U\Sigma V^H}$, we define $\tilde{\mathbf{v}}\triangleq\mathbf{Du}$, where $\mathbf{D}=[\mathbf{v}_2,\mathbf{v}_{2K+1},...,\mathbf{v}_{2N}]$, $\mathbf{u}\in\mathbb{R}^{(2N-1)\times1}$. Problem (12) can be replaced by

$$\min_{\mathbf{u}} \ \|\mathbf{u}\|_2^2 \tag{13a}$$

$$\text{s.t. } \mathbf{h}_{l,1}^T\mathbf{Du}\geq\xi, \tag{13b}$$

The optimal beamforming vector in (8) can be calculated from that of (13) via Lagrange Multiplier [5], i.e.,

$$\mathbf{u}^\star=(\mathbf{h}_{l,1}^T\mathbf{D})^T(\mathbf{h}_{l,1}^T\mathbf{D}\mathbf{D}^T\mathbf{h}_{l,1})^{-1}\xi. \tag{14}$$

We aim to calculate the AN projection matrix by forcing it to the null space of LU's steering vector to eliminate the AN interference with LU, i.e.,

$$\min_{\mathbf{T_a}}\|\mathbf{h}_l^H\mathbf{T}_a\|_2^2 \tag{15a}$$

$$\text{s.t. } \mathrm{tr}(\mathbf{T}_a\mathbf{T}_a^H)=E_t-\|\mathbf{v}\|_2^2. \tag{15b}$$

Based on the generalized Rayleigh-Ritz theorem [6], all columns of AN projection matrix consist of the eigenvectors corresponding to the $N-1$ least eigenvalues of the matrix given by

$$(E_t-\|\mathbf{v}\|_2^2)\mathbf{h}_l\mathbf{h}_l^H. \tag{16}$$

In order to eliminate the interference from AE, we adopt the minimum variance distortionless response (MVDR) method [7]. The purpose of MVDR is to minimize the interference-plus-noise power while maintaining a distortionless response to the direction of LU. The problem is then formulated as

$$\min_{\mathbf{w}} \ \mathbf{w}^H\mathbf{R}_y\mathbf{w} \tag{17a}$$

$$\text{s.t. } \mathbf{a}_l^H\mathbf{w}=1. \tag{17b}$$

The solution of problem (17) is given by

$$\mathbf{w}^\star=\mathbf{R}_y^{-1}\mathbf{a}_l(\mathbf{a}_l^H\mathbf{R}_y^{-1}\mathbf{a}_l)^{-1}. \tag{18}$$

where the covariance matrix $\mathbf{R}_y$ is hard to get. In practice, we used the sample covariance matrix of each antenna to replace the covariance matrix given by $\tilde{\mathbf{R}}_y=\frac{1}{L}\sum_{i=1}^{L}\mathbf{y}_i\mathbf{y}_i^H$, where $\{\mathbf{y}_i\}_1^l$ is the data snapshots, L is the length of snapshots.

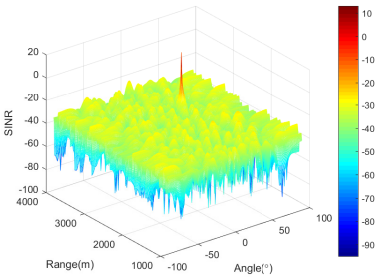

Figure 2. The SINR distribution versus angle-range.

4 Performance Analysis

According to (6) and (7), the signal to interference-plus-noise ratio (SINR) of LU and Eve are given by

$$\gamma_l=\frac{\left|\rho(r_l)\mathbf{h}_l^H\mathbf{v}\mathbf{a}_l^H\mathbf{w}\right|^2}{\left|\rho(r_l)\mathbf{h}_l^H\mathbf{n}_a\mathbf{a}_l^H\mathbf{w}\right|^2+\sum_{k=1}^{K}\left|\rho(r_{j,k})\sqrt{P_{j,k}}s_{j,k}\mathbf{a}_{j,k}^H\mathbf{w}\right|^2+\sigma_l^2}, \tag{19}$$

and

$$\gamma_e=\frac{\left|\rho(r_e)\mathbf{h}_e^H\mathbf{v}\right|^2}{\left|\rho(r_e)\mathbf{h}_e^H\mathbf{n}_a\right|^2+\sigma_e^2}. \tag{20}$$

respectively. Then, we define the average secrecy rate as [8]

$$R\triangleq\left[\log_2(1+\gamma_l)-\max\log_2(1+\gamma_e)\right]^+, \tag{21}$$

where $[\cdot]^+=\max\{0,\cdot\}$.

5 Numerical Results

We present the simulated performance in this section. The simulation parameters are as follows. $f_c=1$GHz, $N=16$, $M=12$, $K=2$, $d_t=d_l=c/2f_c$, $\Delta f=10$MHz, E_t=10dBm, $E_{j,1}=E_{j,2}$=50dBm, $\zeta=10$dB, and $(r_l,\theta_l)=(300\mathrm{m},30^\circ)$. $(r_{j,1},\theta_{j,1})=(600\mathrm{m},-20^\circ)$, $(r_{j,2},\theta_{j,2})=(400\mathrm{m},50^\circ)$. For simplicity, we assume all channel noise power is -100dBm, i.e., $10\log(\sigma_l^2)=10\log(\sigma_e^2)=-100$dBm.

Fig. 2 illustrates the SINR performance of the proposed scheme. As expected, a sharp SINR peak is synthesized at the position of LU whose value is roughly equal to the required SNR 10dB. Additionally, the SINR is uniformly distributed and very low in other regions due to a weak leak of message power and AN interference. As is well known, the closer gets to the transmitter, the stronger message power becomes for the free space path loss, so does the AN interference. This can achieve an uniform and low distribution of SINR in the regions where Eve may exist, which makes the Eve hard to intercept the confidential messages.

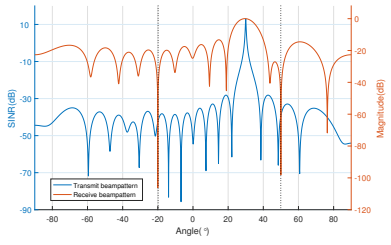

Figure 3. The transmit and receive patterns versus angle.

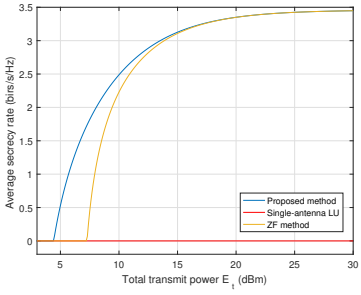

Figure 4. The average secrecy rate versus total transmit power.

In Fig. 3, we illustrate the transmit and receive patterns. From the pattern of transmit, we can see the SINR is about 10dB in the LU's direction, whereas it is low in other regions. For the reception of LU, two nulls are formed in the directions of the AE and the gain of the LU's direction is equal to 0dB, which means the interference from the AE can be effectively suppressed, while maintaining a distortionless response to the direction of the LU.

In Fig. 4, we compare the secrecy rate for different methods. As total transmit power increases, the secrecy rate is higher. The reception of single-antenna LU is broken by the interference from the AE. Therefore, the secrecy rate for single-antenna LU is zero. In addition, given a desired received SNR, the minimal transmit message power is determined for the proposed method, with the rest of total transmit power being allocated to the AN, which can enhance secure performance, and thus the secrecy rate of proposed method is better than that of zero-forcing (ZF) method to design the beamformer in [9].

6 Conclusion

In this paper, we consider the PLS problem in the presence of hybrid Eve by introducing FDA with aided AN technique at transmitter to achieve angle-range dependent secure transmission, and phased-array antennas at LU to eliminate the jamming signals. Finally, the secure performance is simulated, which verifies the superior security of the proposed scheme.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China under Grant Grant No. 61901390, No. 61771404, 61971355, and in part by the Innovation Foundation for Doctor Dissertation of Northwestern Polytechnical University under Grant CX202038.

References

[1] J. Lin, Q. Li, J. Yang, H. Shao, and W. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 671–684, March 2018.

[2] Y. Liu, H. Ruan, L. Wang, and 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*, vol. 11, no. 2, pp. 295–308, March 2017.

[3] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 2006–2021, 2014.

[4] G. Strang, G. Strang, G. Strang, and G. Strang, *Introduction to linear algebra*. Wellesley-Cambridge Press Wellesley, MA, 1993, vol. 3.

[5] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[6] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1987.

[7] H. L. Van Trees, *Optimum array processing: Part IV of detection, estimation, and modulation theory*. John Wiley & Sons, 2004.

[8] F. Shu, X. Wu, J. Hu, J. Li, R. Chen, and J. Wang, "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 890–904, 2018.

[9] X. Tao, Z. Jiang, and L. Yang, "Artificial-noise-aided zero-forcing synthesis approach for secure multi-beam directional modulation," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1–1, 2017.