SCIENCE CHINA
Information Sciences

• LETTER •

January 2022, Vol. 65 119302:1–119302:2
https://doi.org/10.1007/s11432-020-3232-4

Low-complexity and high-performance receive beamforming for secure directional modulation networks against an eavesdropping-enabled full-duplex attacker

Yin TENG[1], Jiayu LI[1], Mengxing HUANG[2], Lin LIU[1], Guiyang XIA[1], Xiaobo ZHOU[3], Feng SHU[2*] & Jiangzhou WANG[4]

[1]*School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing* 210094*, China;*
[2]*School of Information and Communication Engineering, Hainan University, Haikou* 570228*, China;*
[3]*School of Physics and Electronic Engineering, Fuyang Normal University, Fuyang* 236037*, China;*
[4]*School of Engineering and Digital Arts, University of Kent, Canterbury* CT2 7NT*, U.K.*

Received 2 December 2020/Revised 10 March 2021/Accepted 25 March 2021/Published online 17 December 2021

Citation Teng Y, Li J Y, Huang M X, et al. Low-complexity and high-performance receive beamforming for secure directional modulation networks against an eavesdropping-enabled full-duplex attacker. Sci China Inf Sci, 2022, 65(1): 119302, https://doi.org/10.1007/s11432-020-3232-4

Dear editor,

Directional modulation (DM), as an advanced physical-layer security (PLS) transmission technique, is suitable for the line-of-sight (LoS) propagation channel. In [1], the authors presented a DM technique that uses the phased arrays to generate modulation and provides security by deliberately distorting the received signals in other directions. An orthogonal vector approach was proposed in [2] for the synthesis of multi-beam DM transmitters. A robust hybrid analog-digital (HAD) plus DM transmitter was presented in [3], where the authors utilized the probability density function (PDF) of the measured direction of arrival (DOA) to achieve a secure and robust physical-layer transmission.

However, the aforementioned existing studies only focused on the scenarios in the face of a passive eavesdropper (Eve) without an active malicious attacker. In such a situation, it is hard for the base station (Alice) to obtain the channel state information (CSI) from Alice to Eve. If Eve behaves like Mallory, as an active malicious attacker, this problem naturally disappears. With the aid of channel estimation, Alice may obtain the CSI from Alice to Mallory and Bob can obtain the CSI from Mallory to Bob. A hybrid wiretapping wireless system against a half-duplex adversary was considered in [4], where the adversary can decide to either jam or eavesdrop on the transmitter-to-receiver channel.

In this study, our focus is on how to suppress the malicious jamming and improve the security performance by designing the receive beamforming (RBF) at Bob in the presence of a full-duplex (FD) malicious attacker Mallory. Apart from delivering the interference signal, Mallory also eavesdrops on the confidential message (CM) conveyed from Alice to Bob. To reduce the impact of jamming from Mallory on Bob, three RBF methods are proposed for strengthening the security performance.

System model. The proposed DM system consists of an N_A-antennas base station (Alice), a legitimate N_B-antennas user (Bob), and an illegal N_M-antennas malicious attacker (Mallory). Here, Alice conveys a CM to Bob. Additionally, there exists a malicious FD attacker Mallory with a ability to intercept the CM. Therefore, the baseband transmit signal can be expressed as $\boldsymbol{s}_A = \sqrt{\beta_1 P_A}\boldsymbol{v}_A d_A + \sqrt{(1-\beta_1)P_A}\boldsymbol{T}_{A,\mathrm{AN}}\boldsymbol{z}_{A,\mathrm{AN}}$, where P_A, β_1, and $\boldsymbol{v}_A$ denote the total transmit power, the power allocation factor, and the beamforming vector of the CM with $\boldsymbol{v}_A^{\mathrm{H}}\boldsymbol{v}_A = 1$, respectively. Moreover, $\boldsymbol{T}_{A,\mathrm{AN}}$ is the projection matrix for forcing artificial noise (AN) to the undesired direction with $\mathrm{tr}[\boldsymbol{T}_{A,\mathrm{AN}}\boldsymbol{T}_{A,\mathrm{AN}}^{\mathrm{H}}] = 1$. d_A means the CM with $\mathbb{E}[\|d_A\|^2] = 1$ and $\boldsymbol{z}_{A,\mathrm{AN}}$ denotes the AN vector following a complex Gaussian distribution, i.e., $\boldsymbol{z}_{A,\mathrm{AN}} \sim \mathcal{CN}(0, \boldsymbol{I}_{N_A})$. As such, the malicious attacking signal at Mallory can be expressed as $\boldsymbol{s}_M = \sqrt{P_M}\boldsymbol{T}_{M,\mathrm{AN}}\boldsymbol{z}_{M,\mathrm{AN}}$, where P_M, $\boldsymbol{T}_{M,\mathrm{AN}}$, and $\boldsymbol{z}_{M,\mathrm{AN}}$ denote the transmit power at Mallory, the projection matrix for forcing the jamming signal imposing on Bob and AN vector following a complex Gaussian distribution, respectively. Therefore the received signals at Bob and Mallory can be respectively written as $r_B = \boldsymbol{v}_{BR}^{\mathrm{H}}(\sqrt{g_{AB}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{s}_A + \sqrt{g_{MB}}\boldsymbol{H}^{\mathrm{H}}(\theta_{MB})\boldsymbol{s}_M + \boldsymbol{n}_B)$, and $r_M = \boldsymbol{v}_{MR}^{\mathrm{H}}(\sqrt{g_{AM}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AM})\boldsymbol{s}_A + \sqrt{\rho}\boldsymbol{H}_M^{\mathrm{H}}\boldsymbol{s}_M + \boldsymbol{n}_M)$, where $\boldsymbol{H}^{\mathrm{H}}(\theta_{AB}) = \boldsymbol{h}(\theta_{r,AB})\boldsymbol{h}^{\mathrm{H}}(\theta_{t,AB})$, $\boldsymbol{H}^{\mathrm{H}}(\theta_{MB}) = \boldsymbol{h}(\theta_{r,MB})\boldsymbol{h}^{\mathrm{H}}(\theta_{t,MB})$, and $\boldsymbol{H}^{\mathrm{H}}(\theta_{AM}) = \boldsymbol{h}(\theta_{r,AM})\boldsymbol{h}^{\mathrm{H}}(\theta_{t,AM})$ denote the channel matrix from Alice to Bob, Mallory to Bob, and Alice to Mallory. Naturally, the normalized steering vector $\boldsymbol{h}(\theta)$ can be given by $\boldsymbol{h}(\theta) = \frac{1}{\sqrt{N}}[\mathrm{e}^{\mathrm{j}2\pi\Psi_\theta(1)}, \ldots, \mathrm{e}^{\mathrm{j}2\pi\Psi_\theta(n)}, \ldots, \mathrm{e}^{\mathrm{j}2\pi\Psi_\theta(N)}]^{\mathrm{T}}$,

[*] Corresponding author (email: shufeng0101@163.com)

where the phase function $\Psi_\theta(n)$ is defined by [5]. Herein, $\boldsymbol{n}_B$ and $\boldsymbol{n}_M$ are the complex additive white Gaussian noise (AWGN) vectors. Notably, g_{AB} and g_{AM} represent the path loss from Alice to Bob and Alice to Mallory, while $\boldsymbol{v}_{BR}$ and $\boldsymbol{v}_{MR}$ represent the receive beamforming vector of Bob and Mallory. Moreover, $\sqrt{\rho}\boldsymbol{H}_M^{\mathrm{H}}$ is the residual self-interference channel matrix of Mallory and $\rho \in [0,1]$ is the residual self-interference parameter of the Mallory after self-interference cancelation.

Proposed methods. To enhance the performance of traditional maximum ratio combining (MRC) receive beamformer at Bob, a whitening-filter-based MRC (WFMRC) is proposed as follows:

$$\boldsymbol{v}_{BR}^{\mathrm{H}}=(\boldsymbol{W}_{\mathrm{WF}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A)^{\mathrm{H}}\|(\boldsymbol{W}_{\mathrm{WF}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A)^{\mathrm{H}}\|_2^{-1}, \quad (1)$$

where $\boldsymbol{W}_{\mathrm{WF}} = \mathbb{E}\{\overline{\boldsymbol{n}}_B\overline{\boldsymbol{n}}_B^{\mathrm{H}}\}^{-1/2}$ refers to the whitening filter (WF) matrix, $\overline{\boldsymbol{n}}_B$ denotes the colored interference plus noise at Bob. The above WFMRC converts $\overline{\boldsymbol{n}}_B$ into a white one with its covariance matrix being a multiple of identity matrix. To completely remove the jamming from Mallory on Bob, the problem of maximizing the receive power at Bob can be expressed as

$$\begin{aligned} &\max_{\boldsymbol{v}_{BR}} \quad \boldsymbol{v}_{BR}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\boldsymbol{v}_A^{\mathrm{H}}\boldsymbol{H}(\theta_{AB})\boldsymbol{v}_{BR} \\ &\text{s.t.} \quad (\text{C1}) \quad \boldsymbol{v}_{BR}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}(\theta_{MB}) = \boldsymbol{0}_{1\times N_M}, \end{aligned} \quad (2)$$

where constraint (C1) forces the malicious jamming onto the null-space of the channel from Mallory to Bob and $\boldsymbol{v}_{BR}^{\mathrm{H}}\boldsymbol{v}_{BR} = 1$. To enhance its performance, a new RBF of maximizing the WF-based receive power (Max-WFRP) at Bob is also proposed by converting the colored interference plus noise at Bob into a white one with its covariance matrix being a multiple of identity matrix. As such, the optimization problem of Max-WFRP can be simplified to maximize $\widetilde{\boldsymbol{v}}_{BR}^{\mathrm{H}}\boldsymbol{J}\widetilde{\boldsymbol{v}}_{BR}$, where $\boldsymbol{J} = \widetilde{\boldsymbol{W}}_{\mathrm{WF}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\boldsymbol{v}_A^{\mathrm{H}}\boldsymbol{H}(\theta_{AB})\boldsymbol{G}\widetilde{\boldsymbol{W}}_{\mathrm{WF}}^{\mathrm{H}}$, $\boldsymbol{G} = \boldsymbol{I}_{N_B} - \boldsymbol{H}^{\mathrm{H}}(\theta_{MB})[\boldsymbol{H}(\theta_{MB})\boldsymbol{H}^{\mathrm{H}}(\theta_{MB})]^{-1}\boldsymbol{H}(\theta_{MB})$, and $\widetilde{\boldsymbol{W}}_{\mathrm{WF}}$ denotes WF matrix. Then, the closed-form expression of $\widetilde{\boldsymbol{v}}_{BR}$ is directly given by

$$\widetilde{\boldsymbol{v}}_{BR}=\widetilde{\boldsymbol{W}}_{\mathrm{WF}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\|\widetilde{\boldsymbol{W}}_{\mathrm{WF}}\boldsymbol{G}^{\mathrm{H}}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\|_2^{-1}. \quad (3)$$

In the following, a low-complexity minimum mean square error (MMSE) algorithm is further proposed. The solution $\boldsymbol{v}_{BR}$ to the traditional MMSE method is

$$\boldsymbol{v}_{BR} = \sqrt{g_{AB}\beta_1 P_A}\boldsymbol{O}^{-1}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A, \quad (4)$$

where $\boldsymbol{O} = \sigma_B^2\boldsymbol{I}_{N_B} + g_{AB}\beta_1 P_A\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\boldsymbol{v}_A^{\mathrm{H}}\boldsymbol{H}(\theta_{AB}) + \mathbb{E}\{\boldsymbol{n}_A\boldsymbol{n}_A^{\mathrm{H}}\} + \mathbb{E}\{\boldsymbol{n}_M\boldsymbol{n}_M^{\mathrm{H}}\} = \boldsymbol{K} + \mathbb{E}\{\boldsymbol{n}_M\boldsymbol{n}_M^{\mathrm{H}}\}$, $\boldsymbol{n}_A = \sqrt{g_{AB}(1-\beta_1)P_A}\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{T}_{A,\mathrm{AN}}\boldsymbol{z}_{A,\mathrm{AN}}$, $\boldsymbol{n}_M = \sqrt{g_{MB}}\boldsymbol{H}^{\mathrm{H}}(\theta_{MB})\boldsymbol{s}_M$. Interestingly, all the ranks of matrices $\boldsymbol{H}^{\mathrm{H}}(\theta_{AB})\boldsymbol{v}_A\boldsymbol{v}_A^{\mathrm{H}}\boldsymbol{H}(\theta_{AB})$, $\mathbb{E}\{\boldsymbol{n}_A\boldsymbol{n}_A^{\mathrm{H}}\}$, and $\mathbb{E}\{\boldsymbol{n}_M\boldsymbol{n}_M^{\mathrm{H}}\}$ in matrix $\boldsymbol{O}$ are unit, the Sherman-Morrison formula can be elaborately applied to compute the inverse of matrix $\boldsymbol{O}^{-1}$ as follows:

$$\begin{aligned} \boldsymbol{O}^{-1} &= (\boldsymbol{K}+\boldsymbol{u}\boldsymbol{u}^{\mathrm{T}})^{-1} \\ &= \boldsymbol{K}^{-1} - \boldsymbol{K}^{-1}\boldsymbol{u}\boldsymbol{u}^{\mathrm{T}}\boldsymbol{K}^{-1}(1+\boldsymbol{u}^{\mathrm{T}}\boldsymbol{K}^{-1}\boldsymbol{u})^{-1}, \end{aligned} \quad (5)$$

where $\boldsymbol{u} = \sqrt{g_{MB}P_M}\boldsymbol{H}^{\mathrm{H}}(\theta_{MB})\boldsymbol{T}_{M,\mathrm{AN}}$. Similarly, by repeatedly making use of the Sherman-Morrison formula four times, we obtain $\boldsymbol{K}^{-1}$. Due to the space limitation, the specific derivation for (5) is omitted here. The above recursive scheme provides a low-complexity version when compared with the traditional MMSE.

Computational complexity analysis. The computational complexities of the MRC, WFMRC, NSP-based Max-WFRP, traditional MMSE, and the low-complexity MMSE are respectively given by $C_{\mathrm{MRC}} = \mathcal{O}(3N_AN_B + 2N_B)$, $C_{\mathrm{WFMRC}} = \mathcal{O}(N_B^3 + 7N_B^2 + 5N_AN_B + 3N_BN_M + 4N_A^2)$, $C_{\text{Max-WFRP}} = \mathcal{O}(4N_B^3 + 7N_B^2 + N_M^3 + 4N_A^2 + 4N_AN_B + 3N_BN_M + 3N_M^2)$, $C_{\text{Traditional MMSE}} = \mathcal{O}(N_B^3 + 2N_B^2N_A + 2N_A^2N_B + 7N_B^2 + N_AN_B + 2N_BN_M)$, and $C_{\text{Low-complexity MMSE}} = \mathcal{O}(36N_B^2 + 12N_AN_B + 6N_BN_M + 3N_A + N_M)$ float-point operations. We find the fact: as N_B tends to large-scale, the computational complexities of MRC, low-complexity MMSE, and remaining methods perform in the orders $\mathcal{O}(N_B)$, $\mathcal{O}(N_B^2)$, and $\mathcal{O}(N_B^3)$, respectively.

Simulation. System parameters are set as follows: quadrature phase shift keying (QPSK) modulation, $P_A = 10$ W, $N_A = 4$, $N_B = 4$, $N_M = 4$, $\rho = 10^{-11}$, $\beta_1 = 0.9$, $\theta_{t,AB} = 90°$, $\theta_{t,AM} = 155°$, $d_{AB} = 1$ km, $d_{AM} = 3$ km, and $\sigma_B^2 = \sigma_M^2$.

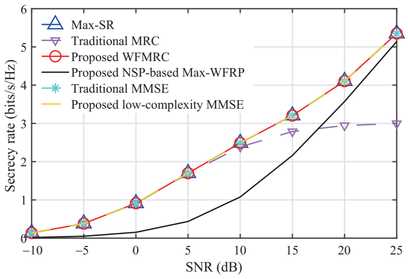

Figure 1 (Color online) Curves of SR versus SNR with $P_M = 10$ W.

Figure 1 plots the curves of SR versus SNR of the three proposed methods with $P_M = 10$ W, where the traditional MRC and MMSE are used as the performance benchmarks. It can be observed that the proposed WFMRC and low-complexity MMSE have the same SR performance as the secrecy rate maximization (Max-SR) scheme, and achieve the best SR performance among all the six methods. More specifically, in the medium and high-SNR regions, the proposed NSP-based Max-WFRP performs much better than MRC and worse than the proposed WFMRC, and low-complexity MMSE in terms of the SR performance. Additionally, the computational complexity of the proposed low-complexity MMSE is lower than that of the Max-SR scheme without performance loss as N_B tends to be large-scale.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62071234, 61771244, 61901121).

References

1 Daly M P, Bernhard J T. Directional modulation technique for phased arrays. IEEE Trans Antenn Propag, 2009, 57: 2633–2640
2 Ding Y, Fusco V. Orthogonal vector approach for synthesis of multi-beam directional modulation transmitters. Antenn Wirel Propag Lett, 2015, 14: 1330–1333
3 Zhuang Z H, Xu L, Li J Y, et al. Machine-learning-based high-resolution DOA measurement and robust directional modulation for hybrid analog-digital massive MIMO transceiver. Sci China Inf Sci, 2020, 63: 180302
4 Basciftci Y O, Gungor O, Koksal C E, et al. On the secrecy capacity of block fading channels with a hybrid adversary. IEEE Trans Inform Theory, 2015, 61: 1325–1343
5 Tse D, Viswanath P. Fundamentals of Wireless Communication. Cambridge: Cambridge University Press, 2005