Secure Precise Transmission with Multi-Relay-Aided Directional Modulation

Wei Zhu[1], Feng Shu[1,2,*], Tingting Liu[1], Xiaobo Zhou[1], Jinsong Hu[1],
Guangzu Liu[1], Linqing Gui[1], Jun Li[1] and Jinhui Lu[1]
[1]School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, 210094, China
[2]National Mobile Communication Research Laboratory, Southeast University, Nanjing, 210096, China
Email: wei.zhu@njust.edu.cn; shufeng@njust.edu.cn; liutt@njit.edu.cn; zxb@njust.edu.cn; jinsong_hu@njust.edu.cn;
liuguangzu@njust.edu.cn; guilinqing@163.com; jun.li@njust.edu.cn; ljh_412@sina.com

***Abstract*—In the conventional directional modulation (DM) system without relay aiding, when the eavesdropper locates within the main-beam of the desired direction, it can intercept the confidential message from source Alice. In this paper, we propose a strategy to enhance physical-layer security of direction modulation in wireless transmission with the help of multi-relay cooperation. In this scenario, the confidential messages are forwarded to the desired destination receiver, and the artificial noise (AN) is enforced to the eavesdroppers with the aid of multi-relays and direction modulation such that the eavesdropper can not successfully recover the useful information from its received signals. The simulation results show that the proposed method achieves a significantly higher signal-to-interference-plus-noise ratio (SINR) peak at the destination position than at other positions outside the main-beam of the desired position and its secrecy rate performance at undesired position is so poor that the secure transmission is guaranteed.**

***Index Terms*—Physical-layer security, directional modulation, multi-relay-aided, secure wireless communication, artificial noise**

I. Introduction

In recent years, the rapid development of mobile Internet has brought great convenience to our work and daily life. At the same time, security issues on wireless transmission are also increasingly serious. Encrypting of the confidential messages in the upper layer is a common means to guarantee security. However, deciphering complex encryption mechanism has gradually become possible due to the extremely high speed increase in computing capacity of the computer. As a result, the researchers turn their attentions to the bottom physical-layer security. The physical-layer security mainly studies the difference between the legitimate channel and the eavesdropping channel, aiming at enhancing the quality of the legitimate channel and reducing the quality of the eavesdropping channel, and achieving the purpose of secure communication [1]–[3].

Directional modulation (DM), as a promising physical-layer security technique, has been widely concerned in recent years. It is characterized by the ability to send useful signals to the specified desired direction while distort the constellation of useful signals in other directions so that the eavesdropper can not recover the useful signal [4], [5]. Subsequently, the concept of artificial noise (AN) is applied to the DM technique where the transmitter transmits AN and useful signals simultaneously, making the AN sent to eavesdropper direction but projected in the null space of the desired direction for further security in wireless communication [6]–[8]. In [9], a robust synthesis method for single-user DM system is designed based on the distribution of angle measurement errors and the minimum mean square error criterion, reducing the negative effect of the estimation error on the system performance. [10] extends the single-user DM system to the multi-user broadcast scenario.

Although existing DM systems can achieve security in the desired direction, it is under the assumption that the eavesdropper locates in the direction other than the desired direction, ignoring the scenario that the eavesdropper may lie in or move to the desired direction which results in potential security hazard. In [11], [12], the authors propose a random frequency diverse array-based directional modulation with artificial noise (RFDA-DM-AN) scheme to achieve 2-D (i.e., angle and range) secure transmissions. Nevertheless, the design of its receiver is with high complexity due to randomly allocating frequencies. To address these problems, this paper introduces multi-relay-aided technique, which is usually applied to the case that the channel between source and destination is no better than that between source and eavesdropper [13], [14]. In this paper, the enhanced physical-layer secure communication can be realized by using multi-relay-aided technique combined with the conventional DM system. A DM transmitter group is established with multiple DM relays. The desired direction of each DM relay points to the destination node, where the desired receiver is located and useful signals can be readily obtained. While the eavesdropper in other places is drowned in a large amount of superimposed AN transmitted from multiple relay stations.

Notations: throughout the paper, matrices, vectors, and scalars are denoted by letters of bold upper case, bold lower case, and lower case, respectively. Signs $(\cdot)^T$, $(\cdot)^H$, and $\mathrm{tr}(\cdot)$ denote matrix transpose, conjugate transpose, and trace, respectively. The symbol $\mathbf{I}_N$ denotes the $N \times N$ identity

This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 61771244, 61702258, 61472190, 61501238 and 61602245), the China Postdoctoral Science Foundation (2016M591852), the Postdoctoral research funding program of Jiangsu Province(1601257C), the Natural Science Foundation of Jiangsu Province (Grants No. BK20150791), and the open research fund of National Mobile Communications Research Laboratory, Southeast University, China (No.2013D02).

[*]Corresponding author

978-1-5386-2062-5/17/$31.00 ©2017 IEEE

matrix.

II. System Model

A schematic diagram of multi-relay-aided enhanced secure wireless communication based on directional modulation is shown in Fig. 1, where S, D and E denote the source node, the destination node and the eavesdropping node, respectively. Each of them is equipped with a single omni-directional antenna. The set $\{R_1, \ldots, R_m, \ldots, R_M\}$ denotes the DM transmitter group consisting of M relays. Each relay carries an N-element uniform liner antenna array and operates in half-duplex mode. As shown in Fig. 1, $\mathbf{h}_{SR_m}(m = 1, 2, \ldots, M)$ is the channel vector between the source and the m-th relay, $\mathbf{h}^H_{R_mD}(m = 1, 2, \ldots, M)$ is the channel vector between the m-th relay and the destination and $\mathbf{h}^H_{R_mE}(m = 1, 2, \ldots, M)$ is the channel vector between the m-th relay and the eavesdropper. Direct channels from S to D and E are not considered in this paper due to the path loss.

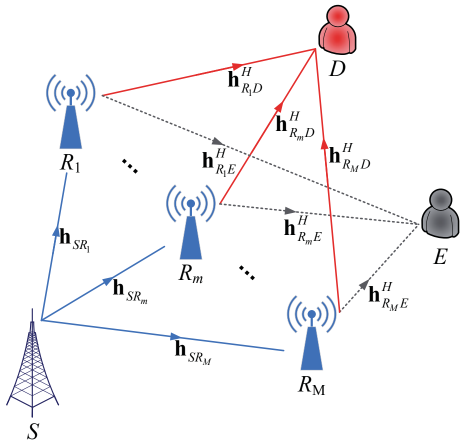


Fig. 1. Schematic diagram of multi-relay-aided enhanced secure wireless communication based on directional modulation

Each relay with an antenna array can operate as an independent DM transmitter in terms of the conventional DM system [7]. We call it DM relay. θ_{R_mD} and d_{R_mD} denote the desired direction from the m-th delay to the destination and the distance between these two nodes, respectively. Likewise, θ_{R_mE} and d_{R_mE} denote the eavesdropping direction from the m-th delay to the eavesdropper and the distance between these two nodes. Considering the free-space path loss model, the steering vector from the m-th relay to the destination can be expressed as

$$\mathbf{h}_{R_mD} = \frac{1}{\sqrt{N}}\left[e^{j2\pi\varphi_1(\theta_{R_mD})}, \cdots, e^{j2\pi\varphi_n(\theta_{R_mD})}, \cdots, e^{j2\pi\varphi_N(\theta_{R_mD})}\right]^T, \tag{1}$$

where

$$\varphi_n(\theta_{R_mD}) = -\frac{(n-(N+1)/2)l\cos\theta_{R_mD}}{\lambda}, \tag{2}$$

where l and λ denote the spacing between two adjacent element of antenna array and the wavelength of transmit carrier, respectively. Similarly, $\mathbf{h}_{R_mE}$ can be achieved by (1) and (2).

In this paper, decode-and-forward (DF) strategy is employed at each relay, hence there is a two-stage transmission from the source to the destination. In Stage 1, the source transmitter broadcasts its encoded symbol x with $\mathbb{E}\{xx^H\} = 1$ to M DM relays. The received signals at the m-th relay, stacked in a vector, are

$$\mathbf{y}_{R_m} = \sqrt{g(d_{SR_m})P_S}\mathbf{h}_{SR_m}x + \mathbf{n}_{R_m}, \tag{3}$$

where $g(d_{SR_m}) = \frac{\beta}{d^c_{SR_m}}$ denotes the path loss coefficient from the source to the m-th relay, β is the attenuation at $d_{SR_m} = 1$m and c is the path loss exponent. P_S is the transmit power at the source transmitter and $\mathbf{n}_{R_m}$ is the complex additive white Gaussian noise (AWGN) vector with distribution $\mathcal{CN}(0, \sigma^2_{R_m}\mathbf{I}_N)$.

It is assumed that all relays decode the symbol x from the source successfully. Then in Stage 2, M relays transmit the symbol x mixed with AN simultaneously. The beamforming vector of the useful message x at the m-th relay is denoted by $\mathbf{v}_m$ and the corresponding AN vector $\mathbf{z}_m$ is multiplied by the projection matrix $\mathbf{T}_{AN_m}$ forcing $\mathbf{z}_m$ to the eavesdropper. Thus, the transmit baseband signal at m-th relay can be written as

$$\mathbf{s}_m = \sqrt{\alpha_m P_{R_m}}\mathbf{v}_m x + \sqrt{(1-\alpha_m)P_{R_m}}\mathbf{T}_{AN_m}\mathbf{z}_m, \tag{4}$$

where α_m is power allocation between the useful messages and AN, P_{R_m} is the transmit power of the m-th relay and the total power constraint of M relays is fixed as $P_0 = \sum_{m=1}^{M} P_{R_m}$. The received signal at the destination is

$$\begin{aligned} y_D &= \sum_{m=1}^{M}\sqrt{g(d_{R_mD})}\mathbf{h}^H_{R_mD}\mathbf{s}_m + n_D \\ &= \sum_{m=1}^{M}\sqrt{g(d_{R_mD})\alpha_m P_{R_m}}\mathbf{h}^H_{R_mD}\mathbf{v}_m x \\ &+ \sum_{m=1}^{M}\sqrt{g(d_{R_mD})(1-\alpha_m)P_{R_m}}\mathbf{h}^H_{R_mD}\mathbf{T}_{AN_m}\mathbf{z}_m + n_D, \end{aligned} \tag{5}$$

where n_D is the complex AWGN at the destination receiver with the distribution $\mathcal{CN}(0, \sigma^2_D)$, while the signal intercepted by the eavesdropper is

$$\begin{aligned} y_E &= \sum_{m=1}^{M}\sqrt{g(d_{R_mE})}\mathbf{h}^H_{R_mE}\mathbf{s}_m + n_E \\ &= \sum_{m=1}^{M}\sqrt{g(d_{R_mE})\alpha_m P_{R_m}}\mathbf{h}^H_{R_mE}\mathbf{v}_m x \\ &+ \sum_{m=1}^{M}\sqrt{g(d_{R_mE})(1-\alpha_m)P_{R_m}}\mathbf{h}^H_{R_mE}\mathbf{T}_{AN_m}\mathbf{z}_m + n_E, \end{aligned} \tag{6}$$

$$C_D = \frac{1}{2}\log_2\left\{1+\frac{\sum\limits_{m=1}^{M} g(d_{R_m D})\alpha_m P_{R_m}\mathbf{v}_m^H\mathbf{R}_{R_m D}\mathbf{v}_m}{\sum\limits_{m=1}^{M} g(d_{R_m D})(1-\alpha_m)P_{R_m}\mathrm{tr}\left[\mathbf{T}_{AN_m}^H\mathbf{R}_{R_m D}\mathbf{T}_{AN_m}\right]+\sigma_D^2}\right\} \tag{8}$$

$$C_E = \frac{1}{2}\log_2\left\{1+\frac{\sum\limits_{m=1}^{M} g(d_{R_m E})\alpha_m P_{R_m}\mathbf{v}_m^H\mathbf{R}_{R_m E}\mathbf{v}_m}{\sum\limits_{m=1}^{M} g(d_{R_m E})(1-\alpha_m)P_{R_m}\mathrm{tr}\left[\mathbf{T}_{AN_m}^H\mathbf{R}_{R_m E}\mathbf{T}_{AN_m}\right]+\sigma_E^2}\right\} \tag{9}$$

where n_E is the complex AWGN at the eavesdropper with the distribution $\mathcal{CN}(0,\sigma_E^2)$.

Based on (3), (5) and (6), the rate at the m-th relay is

$$C_{R_m} = \frac{1}{2}\log_2\left\{1+\frac{g(d_{SR_m})P_S\mathbf{h}_{SR_m}^H\mathbf{h}_{SR_m}}{\sigma_{R_m}^2}\right\}, \tag{7}$$

and the rate at the destination and the eavesdropper are shown in (8) and (9), respectively, where

$$\mathbf{R}_{R_m D} = \mathbf{h}_{R_m D}\mathbf{h}_{R_m D}^H, \tag{10}$$

$$\mathbf{R}_{R_m E} = \mathbf{h}_{R_m E}\mathbf{h}_{R_m E}^H, \tag{11}$$

Since a relay can successfully decode signals from source when the achievable rate at the relay is no less than that at the destination, we assume that $\min\left(C_{R_m}\right) \geq C_D$ for successful decoding at all DM relays. Thus, the secrecy rate of the system can be defined as

$$C_{sec} = \max\left[0, C_D - C_E\right], \tag{12}$$

which is the objective function to be optimized in this paper.

III. Proposed Beamforming Scheme

The proposed synthesis approach in this paper includes the design of the useful message beamforming vector and AN projection matrix. In the following, we will describe the design in two different scenarios: the eavesdropper's location information is 1) unknown and 2) known, respectively.

A. Unknown eavesdropping location

In this case, the rate at the eavesdropper C_E is unknown without the knowledge of the eavesdropper's location. Therefore, the secrecy rate in (12) is not suitable for direct optimization and only the remaining C_D could be candidate objective function, i.e.,

$$\max_{\mathbf{v}_m,\mathbf{T}_{AN_m}} \quad C_D$$
$$\text{s.t.}\begin{cases}\mathbf{v}_m^H\mathbf{v}_m = 1\\ \mathrm{tr}[\mathbf{T}_{AN_m}^H\mathbf{T}_{AN_m}] = 1, \quad m\in\{1,2,\cdots,M\}.\end{cases} \tag{13}$$

From (8), the optimization problem in (13) can be solved by optimizing $\mathbf{v}_m$ and $\mathbf{T}_{AN_m}$ independently with each other. Hence, the problem can be divided into

$$\max_{\mathbf{v}_m} \sum_{m=1}^{M} g(d_{R_m D})\alpha_m P_{R_m}\mathbf{v}_m^H\mathbf{R}_{R_m D}\mathbf{v}_m,$$
$$\text{s.t. } \mathbf{v}_m^H\mathbf{v}_m = 1, \quad m\in\{1,2,\cdots,M\}, \tag{14}$$

and

$$\min_{\mathbf{T}_{AN_m}} \sum_{m=1}^{M} g(d_{R_m D})(1-\alpha_m)P_{R_m}\mathrm{tr}\left[\mathbf{T}_{AN_m}^H\mathbf{R}_{R_m D}\mathbf{T}_{AN_m}\right],$$
$$\text{s.t. } \mathrm{tr}[\mathbf{T}_{AN_m}^H\mathbf{T}_{AN_m}] = 1, \quad m\in\{1,2,\cdots,M\}. \tag{15}$$

As mentioned in the system model, each DM relay can operate as an independent DM transmitter. The maximum of the objective function in (14) can be achieved when each element of the summation is maximum. Based on the conventional DM system, the useful message beamforming vector at the m-th relay can be given by

$$\mathbf{v}_m = \mathbf{h}_{R_m D}. \tag{16}$$

Similarly, the minimum of each element in the summation results in the minimum of the objective function in (15). Utilizing the orthogonal projection (OP) method, the projection matrix $\mathbf{T}_{AN_m}$ is represented as

$$\mathbf{T}_{AN_m} = \frac{\mathbf{I}_N - \mathbf{R}_{R_m D}}{\|\mathbf{I}_N - \mathbf{R}_{R_m D}\|_F}. \tag{17}$$

It is noted that the essence of $\mathbf{T}_{AN_m}$ in (17) is to project AN to the null-space of $\mathbf{h}_{R_m D}^H$, such that the desired receiver will not be interfered by AN.

B. Known eavesdropping location

When eavesdropping location is available at the BS, the achievable rate at the eavesdropper C_E in (9) in known to the BS as well. The problem of maximizing the secrecy rate in (12) can be formulated as

$$\max_{\mathbf{v}_m,\mathbf{T}_{AN_m}} \quad C_D - C_E,$$
$$\text{s.t.}\begin{cases}\mathbf{v}_m^H\mathbf{v}_m = 1\\ \mathrm{tr}[\mathbf{T}_{AN_m}^H\mathbf{T}_{AN_m}] = 1, \quad m\in\{1,2,\cdots,M\}.\end{cases} \tag{18}$$

In this scenario, the desired receiver is still not expected to be interfered by AN, which can be realized by forcing AN sent by multiple DM relays to the null-space of their corresponding desired directions, i.e.,

$$\mathbf{h}_{R_m D}^H \mathbf{T}_{AN_m} = \mathbf{0}_{1\times N}, \quad m \in \{1, 2, \cdots, M\}. \tag{19}$$

Furthermore, with the knowledge of the eavesdropper, we can null the useful messages at the eavesdropper by introducing an additional constraint, i.e.,

$$\mathbf{h}_{R_m E}^H \mathbf{v}_m = 0, \quad m \in \{1, 2, \cdots, M\}. \tag{20}$$

Substituting constraints (19) and (20) in (18) yields

$$\max_{\mathbf{v}_m, \mathbf{T}_{AN_m}} \frac{1}{2}\log_2 \left\{ 1 + \frac{\sum\limits_{m=1}^{M} g(d_{R_m D})\alpha_m P_{R_m} \mathbf{v}_m^H \mathbf{R}_{R_m D} \mathbf{v}_m}{\sigma_D^2} \right\},$$

$$\text{s.t.} \begin{cases} \mathbf{h}_{R_m D}^H \mathbf{T}_{AN_m} = \mathbf{0}_{1\times N} \\ \mathbf{h}_{R_m E}^H \mathbf{v}_m = 0 \\ \mathbf{v}_m^H \mathbf{v}_m = 1 \\ \mathrm{tr}[\mathbf{T}_{AN_m}^H \mathbf{T}_{AN_m}] = 1, \quad m \in \{1, 2, \cdots, M\}. \end{cases}$$

It is apparent that the optimal solution of $\mathbf{T}_{AN_m}$ is the same as the expression in (17). On the other hand, the optimal $\mathbf{v}_m$ can be given by

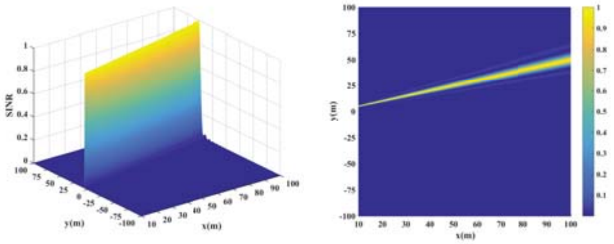
$$\mathbf{v}_m = \frac{(\mathbf{I}_N - \mathbf{h}_{R_m E}\mathbf{h}_{R_m E}^H)\mathbf{h}_{R_m D}}{\|(\mathbf{I}_N - \mathbf{h}_{R_m E}\mathbf{h}_{R_m E}^H)\mathbf{h}_{R_m D}\|_2}. \tag{21}$$

Until now, we have completed the design of the useful message beamforming vector and AN projection matrix for each DM relay when the eavesdropper's location information is unknown and known, respectively.

IV. Simulation and Discussion

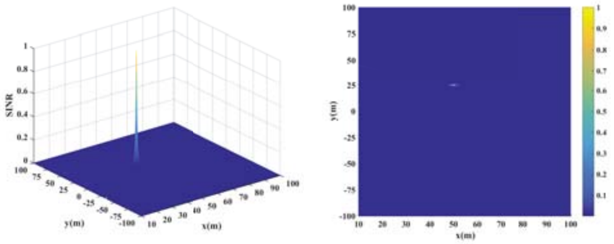
To evaluate the signal-to-interference-plus-noise ratio (SINR) and secrecy rate performance of the proposed synthesis approach, the parameters in our simulation are set as follows. Quadrature phase shift keying (QPSK) modulation is adopted at both the source transmitter and DM relays. All nodes are located in a two-dimensional plane, where the source node, the destination node and the eavesdropping node are fixed at S(-20,0), D(50,25) and E(40,20), respectively (unit: meters). All DM relays stand in a line on the ordinate axis with uniform spacing 50m. The attenuation factor $\beta = 1$ and the path loss exponent $c = 2$. The transmit power at the source and the m-th DM relay are $P_S = 0$dBm and $P_{R_m} = 10$dBm, respectively. The noise power at all receivers are $\sigma_{R_m}^2 = \sigma_D^2 = \sigma_E^2 = -60$dBm.

Fig. 2 demonstrates the normalized SINR versus x-y plane of the conventional DM system for a DM transmitter at the origin and power allocation $\alpha^2 = 0.5$. As indicated in Fig. 2, there is a well marked SINR ridge extending from the DM transmitter to the desired direction, meaning that the eavesdropper at E(40,20) and all other illegitimate receivers located in the desired direction are able to receive strong energy of useful signal excluding the desired receiver, which results in enormous hidden risks in the conventional DM system.



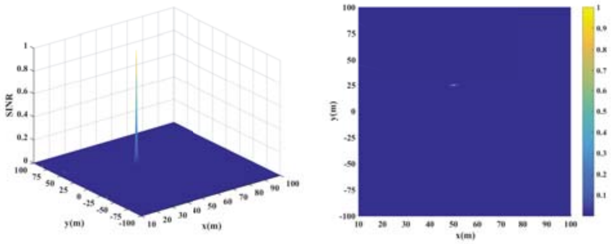
(a) (b)

Fig. 2. Normalized SINR versus x-y plane of the conventional DM system ($\alpha^2 = 0.5$).



(a) (b)

Fig. 3. Normalized SINR versus x-y plane of the proposed method without knowing eavesdropping location ($M = 5$, $\alpha_m^2 = 0.5$).



(a) (b)

Fig. 4. Normalized SINR versus x-y plane of the proposed method with known eavesdropping location ($M = 5$, $\alpha_m^2 = 0.5$).

Fig. 3 and Fig. 4 illustrate the normalized SINR versus x-y plane of the methods proposed in Section III.A and Section III.B for $M = 5$ and $\alpha_m^2 = 0.5$, respectively, where the middle DM relay R_3 locates at the origin and the eavesdropping node E(40,20) lies in its desired direction. From Fig. 3, it is seen that only one towering SINR peak appears at the desired node D(50,25), around which a small desired zone is formed, since that desired directions of all DM relays point to the desired receiver position where the power of useful signals is collected. While in the potential eavesdropping region apart from the desired zone, the receive SINR is much lower than that of the desired receiver due to the superimposed interference of AN on the weak useful signals. When the position of the eavesdropper is obtained by DM relays, Fig. 4 shows a similar single-peak feature as depicted in Fig. 3. It is evident that the proposed approach can provide secure wireless transmission at the

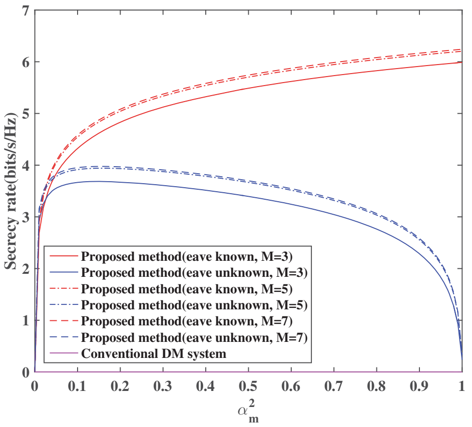


Fig. 5. Curves of secrecy rate versus power allocation α_m^2 for the proposed method and the conventional DM system.

predefined desired receiver whether or not the eavesdropping location is known to DM relays.

In the following, we will evaluate the performance of the proposed method from the secrecy rate aspect. Fig. 5 plots the curves of secrecy rate versus power allocation α_m^2 for the proposed methods in Section III.A and Section III.B and the conventional DM system, respectively. As can be seen in Fig. 5, with the increase in α_m^2, the secrecy rate of the proposed method in Section III.B increase continuously and monotonously when the position of eave (short for eavesdropper) is known to DM relays, which means that the more power allocation is applied to useful signals, the higher secrecy rate is available. However, without knowing the eave, the secrecy rate of the proposed method in Section III.A decreases in the medium and high α_m^2 region due to the lack of superimposed interference of AN on eave, and the optimal value of α_m^2 is around 0.15. In addition, as the number of DM relays increases ($M = 3, 5, 7$), the secrecy rate increases in both scenarios of the proposed method, but the gap between $M = 3$ and $M = 5$ is larger than that between $M = 5$ and $M = 7$. In other words, the improvement of secrecy rate performance achieved by multiple DM relays is becoming less significant when the number of relays is larger. For the conventional DM system, its secrecy rate is always 0, because the eavesdropper is located in its desired direction and closer to it than the desired user which causes that the eavesdropper can obtain better channel than the desired user.

V. Conclusion

In this paper, we designed a strategy of the enhanced physical-layer secure transmission using multi-relay-aided D-M. In the proposed strategy, each relay station acts as one DM transmitter, multiple relays form one group of DM transmitters. Each DM relay transmitter sends both confidential messages and AN simultaneously. The desired directions of multiple relay transmitters intersect at the desired position, called secure precise transmission. Only the desired receiver at the destination is able to detect the confidential message. While the eavesdroppers deviate from the desired receiver position, they are terribly disturbed and drowned by a large amount of superimposed ANs from multiple relay DM transmitters and cannot recover those confidential messages. Therefore, the security of wireless transmission using DM is improved, and the secure precise transmission is achieved.

References

[1] A. D. Wyner, “The wire-tap channel,” *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June. 2008.

[3] X. Chen, C. Zhong, C. Yuen, and H. H. Chen, “Multi-antenna relay aided wireless physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, Dec. 2015.

[4] A. Babakhani, D. B. Rutledge, and A. Hajimiri, “Transmitter architectures based on near-field direct antenna modulation,” *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[5] M. P. Daly, E. L. Daly, and J. T. Bernhard, “Directional modulation technique for phased arrays,” *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sept. 2009.

[6] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June. 2008.

[7] Y. Ding and V. Fusco, “A vector approach for the analysis and synthesis of directional modulation transmitters,” *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[8] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. Leung, “Physical layer security issues in interference-alignment-based wireless networks,” *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, Aug. 2016.

[9] J. Hu, F. Shu, and J. Li, “Robust synthesis method for secure directional modulation with imperfect direction angle,” *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, June. 2016.

[10] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, “Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems,” *IEEE Access*, vol. 4, pp. 6614–6623, 2016.

[11] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, “Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays,” *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[12] F. Shu, X. Wu, J. Hu, R. Chen, and J. Wang, “Secure precise wireless transmission with random-subcarrier-selection-based directional modulation transmit antenna array,” *arXiv preprint*, pp. 1–14, May 2017, arXiv:1704.07996v2.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[14] G. Zheng, L. C. Choo, and K. K. Wong, “Optimal cooperative jamming to enhance physical layer security using relays,” *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.