SECURE M-PSK COMMUNICATION VIA DIRECTIONAL MODULATION

Ashkan Kalantari[⋆]*, Mojtaba Soltanalian*[†]*, Sina Maleki*[⋆]*, Symeon Chatzinotas*[⋆]*, and Björn Ottersten*[⋆]

[⋆] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
[†] Dept. of Electrical and Computer Engineering, University of Illinois at Chicago

ABSTRACT

In this work, a directional modulation-based technique is devised to enhance the security of a multi-antenna wireless communication system employing M-PSK modulation to convey information. The directional modulation method operates by steering the array beam in such a way that the phase of the received signal at the receiver matches that of the intended M-PSK symbol. Due to the difference between the channels of the legitimate receiver and the eavesdropper, the signals received by the eavesdropper generally encompass a phase component different than the actual symbols. As a result, the transceiver which employs directional modulation can impose a high symbol error rate on the eavesdropper without requiring to know the eavesdropper's channel. The optimal directional modulation beamformer is designed to minimize the consumed power subject to satisfying a specific resulting phase and minimal signal amplitude at each antenna of the legitimate receiver. The simulation results show that the directional modulation results in a much higher symbol error rate at the eavesdropper compared to the conventional benchmark scheme, i.e., zero-forcing precoding at the transmitter.

***Index Terms*—** Array processing, beamforming, directional modulation, M-PSK modulation, physical layer security.

1. INTRODUCTION

Due to the broadcast nature of wireless communications, sensitive information can be exposed to unintended receivers. A recent effort in order to protect the information in the physical layer has been carried out by relying on the information-theoretic concept introduced in [1]. This type of coding helps achieving a specific rate, known as the secrecy rate, with which the transmission is completely secure. Secrecy rate was later extended to broadcast [2], Gaussian [3], and fading channels [4–6]. One drawback is that to calculate the secrecy rate, channel state information (CSI) of the eavesdropper is required, which is difficult to get in practice, specially for a passive eavesdropper.

We further note that many communication systems use finite-alphabet signals; in particular, M-PSK modulation has various applications in wireless networks [7], ZigBee protocol [8] and multi-user communications [9, 10]. Since finite-alphabet signals usually have a non-Gaussian distribution [11], they are not optimal in terms of the developed secrecy rates in [1–6]. There has been research interest on the security improvement when finite-alphabet signals are used. The authors in [12] devote some of the available power to add a randomly scaled version of the finite-alphabet signal to the signal itself without optimal beamforming. If the added random part rotates the M-PSK constellation enough, the eavesdropper detects the wrong symbol. In [13], suboptimal random beamforming is used to enhance the security without requiring the eavesdropper CSI when finite-alphabet signal is used. An external helper generating interference in the form of fine-alphabet signal is considered in [14]. Information-theoretic secrecy rate expressions are derived by approximating the helping interference distribution as sum of the Gaussian distributions and assuming the availability of the eavesdropper's CSI. The authors in [15] study the information-theoretic secrecy rate for finite-alphabet signals in a communication system with multi-antenna nodes by assuming the eavesdropper CSI availability at the transmitter. In another paradigm in [16], random and optimized antenna subset selection from a large uniform linear antenna array system without optimal beamforming is employed in order to improve the security in a milliliter-wave system with line-of-sight channel.

In this work, rather than relying on the information-theoretic security concept of [1], a signal processing approach based on the array-based directional modulation [17, 18] concept is utilized in order to enhance the security, without requiring the eavesdropper's CSI, when M-PSK modulation is used for communication. In this technique, instead of producing the symbols at the transmitter, the phase and amplitude of each element of the array is adjusted so that the resulting phase of the received signals on each antenna of the receiver is equal to the phase of a specific M-PSK symbol. We assume the eavesdropper channel is independent from the one of the legitimate receiver. Therefore, the received signals by the eavesdropper have a different resulting phase compared to the legitimate receiver. As shall be shown later, this increases the symbol error rate (SER) at the eavesdropper considerably.

The summarized contributions are as follows. The optimal beamformer for a multi-antenna transmitter is designed when directional modulation is used for M-PSK transmission. There are several works such as [19–28] which perform secrecy rate analysis by assuming the availability of the eavesdropper's CSI, which is difficult to acquire in practice. However, in the directional modulation, the security is enhanced without requiring the eavesdropper CSI while assuming that the eavesdropper is aware of the global CSI as well as the transmitter and receiver configurations, including the number of antennas and the modulation order. Although the information-theoretic secrecy rate provides perfect secrecy, i.e., zero bit leakage, it reduces the message transmission rate. Here, we rely on a signal processing-based approach, so the transmission rate does not need to be scarified in order to enhance the security. Finally, the transmission channel CSI is not required at the legitimate receiver when using the directional modulation, in addition, there is no need for zero-forcing (ZF) or minimum-mean-square-error (MMSE) multi-input and multi-output (MIMO) receiver implementation at the legitimate receiver side.

The remainder of the paper is organized as follows. In Section 2, the network configuration as well as the signal models are introduced. The security and the beamformer design for the directional modu-

This work was supported by the National Research Fund of Luxembourg under grant number 5798109 and SeMIGod.

[⋆] e-mails:{ashkan.kalantari, sina.maleki, symeon.chatzinotas, bjorn.ottersten}@uni.lu [†] e-mail: msol@uic.edu

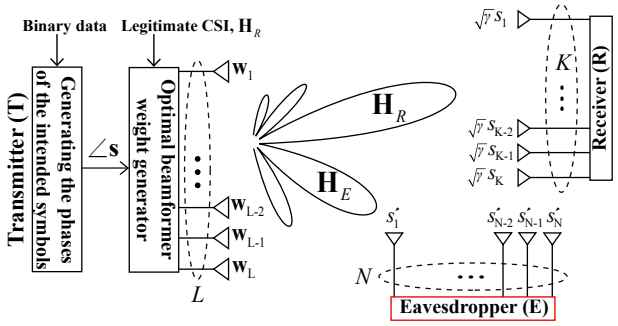

Fig. 1: Array-based directional modulation to enhance the security in a MIMO wiretap channel.

lation is mentioned in Section 3. In Section 4, the security of the directional modulation is evaluated using simulations. Finally, the conclusions are drawn in Section 5.

Notation: Upper-case and lower-case bold-faced letters are used to denote matrices and column vectors, respectively. Superscripts $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$ represent transpose, conjugate, and Hermitian operators, respectively. $\mathbf{I}_{N\times N}$ denotes an N by N identity matrix, $diag(\mathbf{a})$ denotes a diagonal matrix where the elements of $\mathbf{a}$ are its diagonal entries, $\mathbf{a}\circ\mathbf{b}$ is the element-wise Hadamard product, $\|\cdot\|$ is the Frobenius norm, and $|\cdot|$ represents the absolute value of a scalar. $\mathrm{Re}\,(\cdot)$, $\mathrm{Im}\,(\cdot)$, and $\arg(\cdot)$ represent the real part, imaginary part, and angle of a complex number, respectively.

2. SIGNAL AND SYSTEM MODEL

We consider a communication network with a multi-antenna transmitter denoted by T, a multi-antenna receiver denoted by R, and a multi-antenna eavesdropper denoted by E as shown in Fig. 1. Using the transmission channel CSI and the symbols' phases, the phase and the amplitude of each transmit antenna is designed so that the resulting phase of the received signals by each antenna of the legitimate receiver is equal to the phase of a specific M-PSK symbol. Here, all the communication channels are considered to be quasi-static block fading. After applying the optimal coefficients to array elements, the received signals at R and E are

$$\mathbf{y}_R = \mathbf{H}_R\mathbf{w} + \mathbf{n}_R, \tag{1}$$

$$\mathbf{y}_E = \mathbf{H}_E\mathbf{w} + \mathbf{n}_E, \tag{2}$$

where the random variables $\mathbf{n}_R$ and $\mathbf{n}_E$ denote the additive white Gaussian noise at R and E, respectively. The Gaussian random variables $\mathbf{n}_R$ and $\mathbf{n}_E$ are independent and identically distributed (i.i.d.) with $\mathbf{n}_R \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{n_R}\mathbf{I}_{K\times K})$, and $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{n_E}\mathbf{I}_{N\times N})$, respectively, where $\mathcal{CN}$ denotes the complex and circularly symmetric i.i.d. random variable. The signal $\mathbf{y}_R$ is a $K\times 1$ vector denoting the received signals by R, $\mathbf{y}_E$ is an $N\times 1$ vector denoting the received signals by E, $\mathbf{H}_R$ is a $K\times L$ matrix denoting the channel from T to R defined as $\mathbf{H}_R = [\mathbf{h}_1, ..., \mathbf{h}_i, ..., \mathbf{h}_R]^T$, $\mathbf{H}_E$ is an $N\times L$ matrix denoting the channel from T to E, and $\mathbf{w}$ is the beamforming vector. In the directional modulation scheme, the elements of the vector $\mathbf{H}_R\mathbf{w}$ are the M-PSK symbols. Hence, to detect the received symbols, R can directly apply a conventional detector, e.g., maximum-likelihood (ML) detector, on each individual element of the vector $\mathbf{y}_R$ without requiring to implement a ZF or MMSE receiver [29].

3. SECURITY VIA DIRECTIONAL MODULATION

In this section, first, the security benefits of the directional modulation is discussed, and then the optimal beamformer design problem is formulated and solved.

3.1. Security Advantages

As indicated earlier, the design of the beamformer in the directional modulation scheme is based on the phase of the symbols which are to be conveyed to R; in particular, to recover the symbols, it is necessary for E to somehow estimate $\mathbf{H}_R\mathbf{w}$. To this end, considering that E is aware of $\mathbf{H}_R$, E should begin by estimating $\mathbf{w}$ given by

$$\widehat{\mathbf{w}} = \left(\mathbf{H}_E^H\mathbf{H}_E\right)^{-1}\mathbf{H}_E^H\mathbf{y}_E = \mathbf{w} + \left(\mathbf{H}_E^H\mathbf{H}_E\right)^{-1}\mathbf{H}_E^H\mathbf{n}_E, \tag{3}$$

where $\widehat{\mathbf{w}}$ is the estimation of $\mathbf{w}$ at E. Note that E can compute (3) only in the case $N \geq L$ since $\left(\mathbf{H}_E^H\mathbf{H}_E\right)^{-1}\mathbf{H}_E^H\mathbf{H}_E \neq \mathbf{I}$ for $N < L$. Next, E needs to multiply $\widehat{\mathbf{w}}$ by $\mathbf{H}_R$ to calculate $\mathbf{H}_R\mathbf{w}$, viz.

$$\mathbf{H}_R\widehat{\mathbf{w}} = \mathbf{H}_R\mathbf{w} + \mathbf{H}_R\left(\mathbf{H}_E^H\mathbf{H}_E\right)^{-1}\mathbf{H}_E^H\mathbf{n}_E. \tag{4}$$

where $\mathbf{H}_R\widehat{\mathbf{w}}$ denotes the estimation of $\mathbf{H}_R\mathbf{w}$ at E. However, the first step of estimating $\mathbf{H}_R\mathbf{w}$ in (3) results in the noise enhancement at E [30]. Therefore, the SER at E will be higher than that of R, especially in a low signal-to-noise ratio regime due to the fact that R can directly detect the M-PSK symbols without channel equalization. Moreover, in the case of $N < L$, E cannot estimate $\mathbf{H}_R\mathbf{w}$. Therefore, E can not correctly decode the transmitted signal, and any attempt to do so leads to a high SER.

Remark 1. *It is interesting to observe that the condition $N < L$ is easily met in a massive MIMO scenario, hence, the directional modulation technique appears to be a good candidate for security enhancement in massive MIMO systems.* ■

In the next section, the optimal beamformer design problem for the directional modulation is formulated and solved from a power efficiency viewpoint.

3.2. Optimal Beamformer Design

In this section, the optimal beamformer design problem for the directional modulation is defined and transformed into a linearly constrained quadratic program which can be solved efficiently. Herein, the beamformer for the directional modulation will be designed to minimize the consumed power at the transmitter such that 1) the resulting phase of the signals received by each antenna of R is equal to the phase of a specific M-PSK symbol, and that 2) the required signal level for the in-phase and quadrature-phase components of the resulting M-PSK symbol on each antenna of R is preserved above a specific level. Note that in such a setup, by minimizing the power we actually increase the SER at E even when $N \geq L$ while keeping the quality of our own signal reception at the desired level.

Using the directional modulation signal model described in Section 2, the related beamformer design problem can be cast as

$$\min_{\mathbf{w}} \ \|\mathbf{w}\|^2$$

$$\text{s.t.} \quad \arg\left(\mathbf{h}_i^T\mathbf{w}\right) = \arg\left(s_i\right), \qquad \forall\, i \tag{5a}$$

$$\mathrm{Re}\left(s_i\right)\mathrm{Re}\left(\mathbf{h}_i^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Re}^2\left(s_i\right), \ \forall\, i \tag{5b}$$

$$\mathrm{Im}\left(s_i\right)\mathrm{Im}\left(\mathbf{h}_i^T\mathbf{w}\right) \geq \sqrt{\gamma}\mathrm{Im}^2\left(s_i\right), \ \forall\, i \tag{5c}$$

where s_i is the i-th M-PSK symbol possessing instantaneous unit energy, i.e., $|s_i|^2 = 1$, and $\sqrt{\gamma}$ is a scalar to adjust the required level for the in-phase and quadrature-phase components of the received signal at the corresponding antenna of R. Note that since the in-phase or quadrant-phase part of the symbol may be negative, both sides of the constraints (5b) and (5c) are multiplied by $\mathrm{Re}(s_i)$ and $\mathrm{Im}(s_i)$, respectively. Since (5a) holds at the optimal point, $\mathrm{Re}(s_i)$ and $\mathrm{Im}(s_i)$ have the same sign as $\mathrm{Re}\left(\mathbf{h}_i^T\mathbf{w}\right)$ and $\mathrm{Im}\left(\mathbf{h}_i^T\mathbf{w}\right)$ at the optimal point. As a result, the multiplication at both sides of (5b) and (5c) does not change the side of the inequality.

To simplify (5), let's write the constraint (5a) as

$$\mathrm{Re}\left(\mathbf{h}_i^T\mathbf{w}\right)\alpha_i - \mathrm{Im}\left(\mathbf{h}_i^T\mathbf{w}\right) = 0, \;\; i = 1, ..., K, \tag{6}$$

where $\alpha_i = \tan(s_i)$. Using the equations derived in (6) and by putting together the constraints (5b) and (5c), it is possible to reformulate (5) into a compact form as

$$\begin{aligned} \min_{\mathbf{w}} \quad & \|\mathbf{w}\|^2 \\ \text{s.t.} \quad & \mathbf{A}\mathrm{Re}\left(\mathbf{H}_R\mathbf{w}\right) - \mathrm{Im}\left(\mathbf{H}_R\mathbf{w}\right) = \mathbf{0}, && \text{(7a)} \\ & \mathrm{Re}\left(\mathbf{S}\right)\mathrm{Re}\left(\mathbf{H}_R\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_r, && \text{(7b)} \\ & \mathrm{Im}\left(\mathbf{S}\right)\mathrm{Im}\left(\mathbf{H}_R\mathbf{w}\right) \geq \sqrt{\gamma}\,\mathbf{s}_i, && \text{(7c)} \end{aligned}$$

where $\mathbf{S} = diag\left(\mathbf{s}\right)$, $\mathbf{s} = [s_1, ..., s_i, ..., s_K]^T$ is the vector bearing the M-PSK symbols, $\mathbf{s}_r = \mathrm{Re}\left(\mathbf{s}\right) \circ \mathrm{Re}\left(\mathbf{s}\right)$, $\mathbf{s}_i = \mathrm{Im}\left(\mathbf{s}\right) \circ \mathrm{Im}\left(\mathbf{s}\right)$, and $\mathbf{A} = diag\left(\alpha_1, ..., \alpha_K\right)$.

Note that applying $tan(\cdot)$ on the phases of the intended symbols causes ambiguity since symbols with different phases can have the same tan value, e.g., $\tan\left(\frac{\pi}{4}\right) = \tan\left(\frac{3\pi}{4}\right)$. Hence, the constraints $\mathrm{Re}\left(\mathbf{S}\right)\mathrm{Re}\left(\mathbf{H}_R\mathbf{w}\right) \geq 0$ and $\mathrm{Im}\left(\mathbf{S}\right)\mathrm{Im}\left(\mathbf{H}_R\mathbf{w}\right) \geq 0$ need to be added to the design problem (7) to resolve the phase ambiguity. Interestingly, these constraints are already present in (7b) and (7c).

To transform (7) into a familiar form, we represent $\mathbf{H}_R = \mathrm{Re}\left(\mathbf{H}_R\right) + i\mathrm{Im}\left(\mathbf{H}_R\right)$ and $\mathbf{w} = \mathrm{Re}\left(\mathbf{w}\right) + i\mathrm{Im}\left(\mathbf{w}\right)$ in order to write $\mathbf{H}_R\mathbf{w}$ as

$$\begin{aligned} \mathbf{H}_R\mathbf{w} =& \mathrm{Re}\left(\mathbf{H}_R\right)\mathrm{Re}\left(\mathbf{w}\right) - \mathrm{Im}\left(\mathbf{H}_R\right)\mathrm{Im}\left(\mathbf{w}\right) \\ & + i\left[\mathrm{Re}\left(\mathbf{H}_R\right)\mathrm{Im}\left(\mathbf{w}\right) + \mathrm{Im}\left(\mathbf{H}_R\right)\mathrm{Re}\left(\mathbf{w}\right)\right], \end{aligned} \tag{8}$$

which helps us to write the real and imaginary parts of $\mathbf{H}_R\mathbf{w}$ as

$$\mathrm{Re}\left(\mathbf{H}_R\mathbf{w}\right) = \mathbf{H}_{R_1}\widetilde{\mathbf{w}}, \;\; \mathrm{Im}\left(\mathbf{H}_R\mathbf{w}\right) = \mathbf{H}_{R_2}\widetilde{\mathbf{w}}, \tag{9}$$

where $\widetilde{\mathbf{w}} = \left[\mathrm{Re}\left(\mathbf{w}^T\right), \mathrm{Im}\left(\mathbf{w}^T\right)\right]^T$, $\mathbf{H}_{R_1} = \left[\mathrm{Re}\left(\mathbf{H}_R\right), -\mathrm{Im}\left(\mathbf{H}_\mathrm{R}\right)\right]$, $\mathbf{H}_{R_2} = \left[\mathrm{Im}\left(\mathbf{H}_\mathrm{R}\right), \mathrm{Re}\left(\mathbf{H}_\mathrm{R}\right)\right]$. Also, it is straightforward to see that $\|\widetilde{\mathbf{w}}\|^2 = \|\mathbf{w}\|^2$.

Using the derivations in (9), (7) can be reformulated as

$$\begin{aligned} \min_{\widetilde{\mathbf{w}}} \quad & \|\widetilde{\mathbf{w}}\|^2 \\ \text{s.t.} \quad & \left(\mathbf{A}\mathbf{H}_{R_1} - \mathbf{H}_{R_2}\right)\widetilde{\mathbf{w}} = 0, \\ & \mathrm{Re}\left(\mathbf{S}\right)\mathbf{H}_{R_1}\widetilde{\mathbf{w}} \geq \sqrt{\gamma}\,\mathbf{s}_r, \\ & \mathrm{Im}\left(\mathbf{S}\right)\mathbf{H}_{R_2}\widetilde{\mathbf{w}} \geq \sqrt{\gamma}\,\mathbf{s}_i. \end{aligned} \tag{10}$$

For (10) to be feasible, $\widetilde{\mathbf{w}}$ should lie in the null space of the matrix $\mathbf{A}\mathbf{H}_{R_1} - \mathbf{H}_{R_2}$. If the singular value decomposition of $\mathbf{A}\mathbf{H}_{R_1} - \mathbf{H}_{R_2}$ is shown by $\mathbf{U}\Sigma\mathbf{V}^H$, the orthonormal basis for the null space of $\mathbf{A}\mathbf{H}_{R_1} - \mathbf{H}_{R_2}$ are the last $2L - K$ columns of $\mathbf{V}$ which span $\widetilde{\mathbf{w}}$ [31]. This means that the vector $\widetilde{\mathbf{w}}$ can be written as $\widetilde{\mathbf{w}} = \mathbf{E}\boldsymbol{\lambda}$ where $\mathbf{E} = [\mathbf{v}_{K+1}, ..., \mathbf{v}_{2L}]$ and $\boldsymbol{\lambda} = [\lambda_1, ..., \lambda_{2L-K}]$. Therefore, (10) boils down into

$$\begin{aligned} \min_{\boldsymbol{\lambda}} \quad & \|\boldsymbol{\lambda}\|^2 \\ \text{s.t.} \quad & \mathrm{Re}\left(\mathbf{S}\right)\mathbf{H}_{R_1}\mathbf{E}\boldsymbol{\lambda} \geq \sqrt{\gamma}\,\mathbf{s}_r, \\ & \mathrm{Im}\left(\mathbf{S}\right)\mathbf{H}_{R_2}\mathbf{E}\boldsymbol{\lambda} \geq \sqrt{\gamma}\,\mathbf{s}_i, \end{aligned} \tag{11}$$

which is a convex linearly constrained quadratic programming and can be solved efficiently using standard convex optimization techniques.

Remark 2. *Since $\widetilde{\mathbf{w}}$ in* (10) *is spanned by the last $2L - K$ vectors of the matrix $\mathbf{V}$, a necessary condition for the existence of the optimal beamformer for the directional modulation is $L > \frac{K}{2}$ which means that the number of transmit antennas needs to be more than half of the number of antennas at the legitimate receiver. Provided that the latter condition is met, a sufficient condition can be proposed from a geometrical point of view; namely that the feasible set of* (11) *is not empty if and only if the intersection of the linear spaces in the constraint set constitutes a non-empty set.* ■

4. SIMULATION RESULTS

In this section, the performance of the secure directional modulation and a benchmark scheme are demonstrated and compared using different simulation scenarios. In all simulations, channels are considered to be quasi static block Rayleigh fading which are generated using i.i.d. complex Gaussian random variables with distribution$\sim \mathcal{CN}(0, \sigma^2)$ and remain fixed during the interval in which the M-PSK symbol is being conveyed to R. In addition, the noise is also generated using i.i.d. complex Gaussian random variables, and the modulation order used in all of the scenarios is 8-PSK. The acronym "DM" is used instead of the term "directional modulation" in the legend of the figures. Before proceeding, we first mention the benchmark scheme.

The ZF at the transmitter in order to neutralize the interference between received symbol streams at R [32] is used as the comparison benchmark. In contrast to the directional modulation scheme, the symbols in the benchmark scheme are generated and sent from the transmitter. The received signals at R and E are

$$\mathbf{y}_R = \mathbf{H}_R\mathbf{P}\mathbf{s} + \mathbf{n}_R, \tag{12}$$

$$\mathbf{y}_E = \mathbf{H}_E\mathbf{P}\mathbf{s} + \mathbf{n}_E, \tag{13}$$

where $\mathbf{P} = \mathbf{H}_\mathbf{R}^\mathbf{H}\left(\mathbf{H}_\mathbf{R}\mathbf{H}_\mathbf{R}^\mathbf{H}\right)^{-\mathbf{1}}\beta$, and β is the amplification factor for the symbols which acts similar as $\sqrt{\gamma}$ in the directional modulation scheme. After the signal is received by E, it estimates the transmitted symbols as

$$\begin{aligned} \widehat{\mathbf{s}} &= \left[\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{H}_E\mathbf{P}\right]^{-1}\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{y}_E \\ &= \mathbf{s} + \left[\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{H}_E\mathbf{P}\right]^{-1}\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{n}_E. \end{aligned} \tag{14}$$

The dimension of the matrix $\mathbf{H}_E\mathbf{P}$ is $N \times K$ which results in $\left[\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{H}_E\mathbf{P}\right]^{-1}\left(\mathbf{H}_E\mathbf{P}\right)^H\mathbf{H}_E\mathbf{P} = \mathbf{I}$ for $N \geq K$. This means that E can recover the symbols even with the condition $N < L$. Generally, satisfying the condition $N < L$ is easier than $N < K$ since the base station has usually more antennas than the users. Considering that the condition for E to estimate $\mathbf{H}_R\mathbf{w}$ and detect the M-PSK symbol in the directional modulation scheme is $N \geq L$, the directional modulation is much more probable to enhance the security compared to the benchmark scheme.

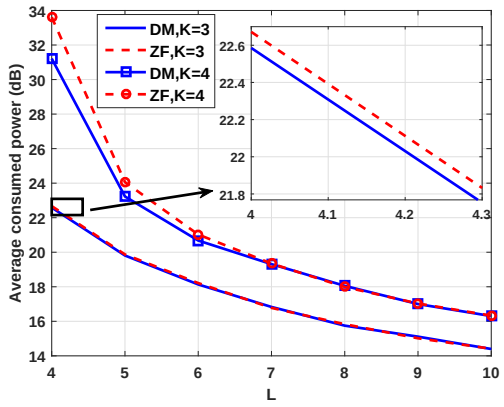

Fig. 2: Average consumed power with respect to the number of transmitting antennas for the directional modulation and the benchmark schemes when $N = 6$, $\sqrt{\gamma} = 8$, and $\beta = 8$.

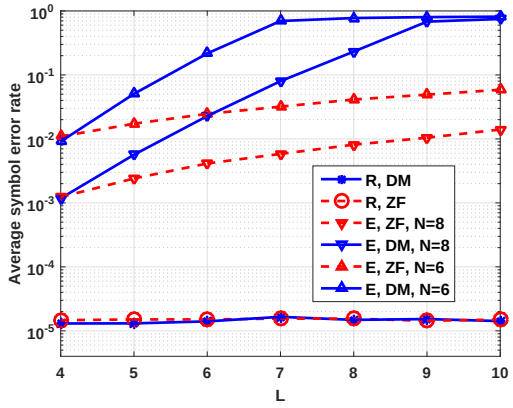

Fig. 3: Average SER versus the number of transmitting antennas for the directional modulation and the benchmark schemes when $K = 4$, $\sqrt{\gamma} = 8$, and $\beta = 8$.

In the first scenario, the effect of the number of transmission antennas, L, on the consumed power is investigated. The average consumed power with respect to L is shown in Fig. 2. As seen, for a specific range of L, the directional modulation consumes less power than the benchmark scheme. Furthermore, the difference in power consumption increases when the number of antennas at R increases.

The SER at R and E when using different number of transmitting antennas is studied in the second scenario. The average SER with respect to L is presented in Fig. 3. As it is seen, the directional modulation causes considerably more SER at E compared to the benchmark scheme. Furthermore, as the antennas of E increase, the difference between the SER caused at E by the directional modulation and benchmark scheme increases for specific values of L. For example, when $L = 9$ and $N = 8$, the difference between the SER caused by the directional modulation and ZF schemes is more than the case when $L = 9$ and $N = 6$.

In the last scenario, the relation between the required level, $\sqrt{\gamma}$, for the in-phase and quadrature-phase components of the induced symbols at R and the SER at R and E is studied. The average SER at R and E with respect to $\sqrt{\gamma}$ is shown in Fig. 4. As it is observed,

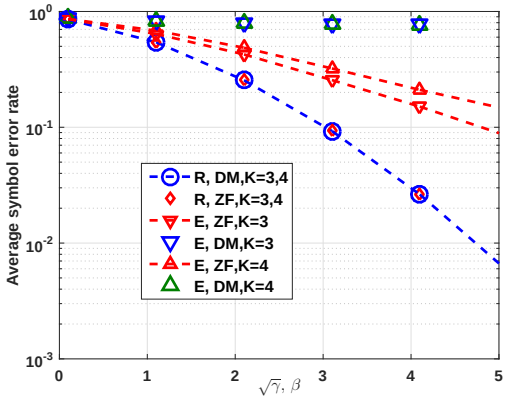

Fig. 4: Average SER versus the in-phase and the quadrature-phase required signal levels for directional modulation and benchmark schemes when $L = 8$ and $N = 6$.

when using the benchmark scheme, the SER at E decreases as $\sqrt{\gamma}$ increases. This reduction is more when the antennas of R decreases. On the other hand, when using the directional modulation scheme, the SER at E does not decrease as the required signal level at the legitimate increases. As mentioned, this is due to the fact that for $N \geq K$, E can remove the effect of precoder in the benchmark scheme and decrease its own SER. However, as explained in Section 3.1, E cannot estimate $\mathbf{H}_R\mathbf{w}$ when $N < L$ in the directional modulation. Therefore, assuming the independence of $\mathbf{H}_R$ and $\mathbf{H}_E$, E has to detect the symbols according to the phases of the vector $\mathbf{H}_E\mathbf{w}$ which are different from the phases of the vector $\mathbf{H}_R\mathbf{w}$.

5. CONCLUSIONS

The optimal beamformer for the secure directional modulation was designed without requiring the eavesdropper's CSI. It was seen that the eavesdropper cannot regenerate the beamformer and has to estimate the signal received by the legitimate receiver using the global CSI knowledge. However, this estimation enhances the noise and is only possible when the transmitter has less antennas than the eavesdropper. The directional modulation was compared with the ZF at the transmitter as the benchmark. In the ZF scheme, the eavesdropper had to have more antennas than the legitimate receiver to recover the symbol. The results showed that directional modulation leads into less power consumption and more SER at the eavesdropper compared to the conventional benchmark scheme. These observations confirm the reliability of the studied directional modulation approach from a security point of view.

6. REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, Mar. 2007, pp. 905–910.

[6] F. Oggier and B. Hassibi, "The MIMO wiretap channel," in *International Symposium on Communications, Control and Signal Processing (ISCCSP)*, Malta, Mar. 2008, pp. 213–218.

[7] "IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications: Amendment 6: Medium access control (MAC) security enhancements," *IEEE Std 802.11i*, pp. 1–190, Jul. 2004.

[8] "IEEE standard for a smart transducer interface for sensors and actuators wireless communication protocols and transducer electronic data sheet (TEDS) formats," *IEEE Std*, pp. C1–236, Oct. 2007.

[9] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.

[10] C. Masouros and G. Zheng, "Exploiting known interference as green signal power for downlink beamforming optimization," *IEEE Trans. Signal Process.*, vol. 63, no. 14, pp. 3628–3640, Jul. 2015.

[11] V. Madisetti, *The Digital Signal Processing Handbook*, ser. Electrical Engineering Handbook. Taylor & Francis, 1997.

[12] O. Bakr and R. Mudumbai, "A new jamming technique for secrecy in multi-antenna wireless networks," in *IEEE International Symposium on Information Theory (ISIT)*, Austin, TX, Jun. 2010, pp. 2513–2517.

[13] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, May 2007.

[14] A. Chorti, "Helping interferer physical layer security strategies for M-QAM and M-PSK systems," in *Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, Mar. 2012.

[15] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.

[16] N. Valliappan, A. Lozano, and R. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[17] M. Daly and J. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[18] M. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[19] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[20] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Improved wireless secrecy rate using distributed auction theory," in *International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, Dec. 2009, pp. 442–447.

[21] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

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

[23] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2010.

[24] J. Huang and A. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *Global Telecommunications Conference (GLOBECOM)*, Miami, FL, Dec. 2010.

[25] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[26] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.

[27] A. Kalantari, S. Maleki, G. Zheng, S. Chatzinotas, and B. Ottersten, "Joint power control in wiretap interference channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3810–3823, Jul. 2015.

[28] A. Kalantari, G. Zheng, Z. Gao, Z. Han, and B. Ottersten, "Secrecy analysis on network coding in bidirectional multibeam satellite communications," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1862–1874, Sep. 2015.

[29] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. Poor, *MIMO Wireless Communications*. Cambridge University Press, 2007.

[30] V. Arokiamary, *Mobile Communications*. Technical Publications, 2009.

[31] G. Strang, *Introduction to Linear Algebra*, 4th ed. Wellesley-Cambridge Press and SIAM, 2009.

[32] L.-U. Choi and R. Murch, "A transmit preprocessing technique for multiuser mimo systems using a decomposition approach," *Wireless Communications, IEEE Transactions on*, vol. 3, no. 1, pp. 20–24, Jan 2004.